Guia do usuário

AWS Organizations

AWS Organizations: Guia do usuário

Table of Contents

O que AWS Organizationsé

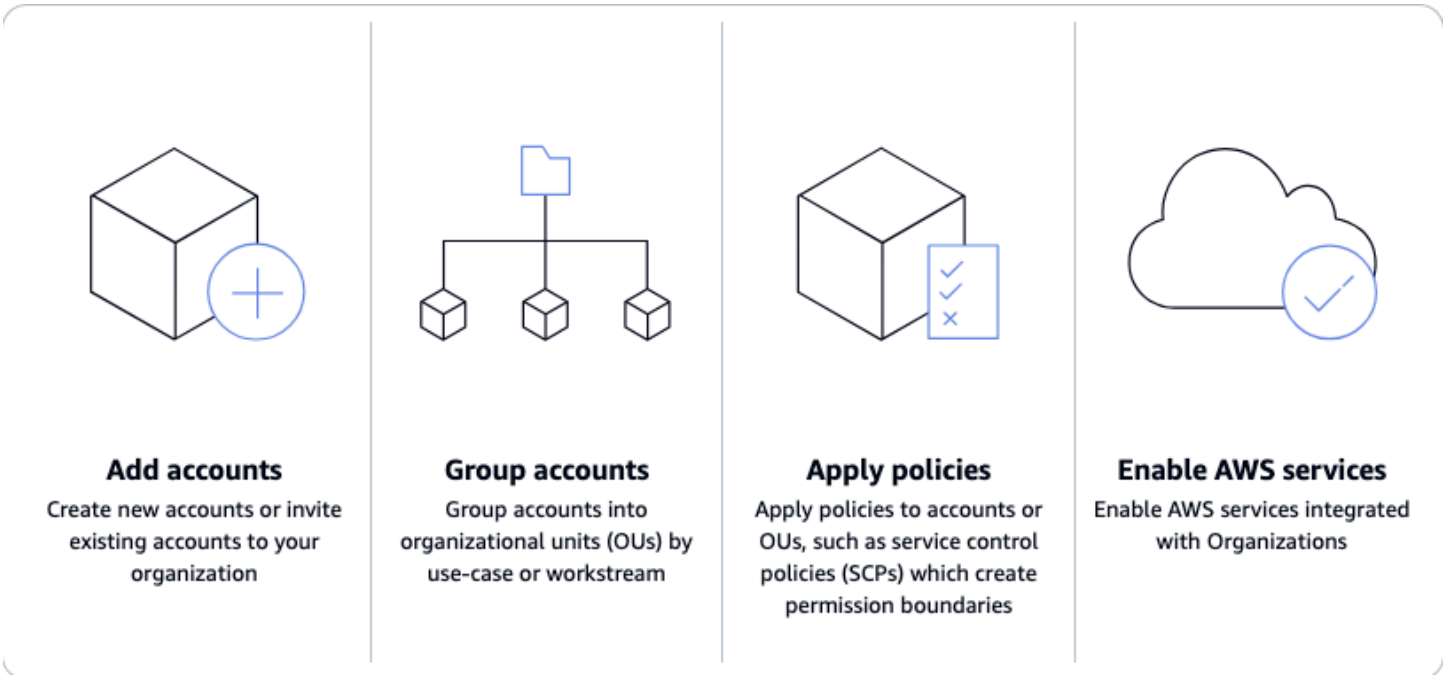
Gerencie centralmente seu ambiente à medida que você expande seus recursos AWS

AWS Organizations ajuda você a gerenciar e governar centralmente seu ambiente à medida que você cresce e escala seus AWS recursos. Usando o Organizations, você pode criar contas e alocar recursos, agrupar contas para organizar seus fluxos de trabalho, aplicar políticas para fins de governança e simplificar o faturamento usando um único método de pagamento para todas as suas contas.

O Organizations é integrado a outros Serviços da AWS para que você possa definir configurações centrais, mecanismos de segurança, requisitos de auditoria e compartilhamento de recursos entre contas em sua organização. Para obter mais informações, consulte Usando AWS Organizations com outros Serviços da AWS.

O diagrama a seguir mostra uma explicação de alto nível de como você pode usar o AWS Organizations:

- Adicionar contas
- Agrupar contas
- Aplicar políticas
- Habilitar Serviços da AWS.



Tópicos

Características para AWS Organizations

AWS Organizations oferece os seguintes recursos:

Gerencie seu Contas da AWS

Contas da AWS são limites naturais para permissão, segurança, custos e cargas de trabalho. Usar um ambiente de várias contas é uma prática recomendada ao escalar seu ambiente de nuvem. Você pode simplificar a criação de contas criando programaticamente novas contas usando o AWS Command Line Interface (AWS CLI), ou SDKs APIs, e provisionando centralmente

os recursos e permissões recomendados para essas contas com. AWS CloudFormation StackSets

Defina e gerencie sua organização

Ao criar novas contas, você pode agrupá-las em unidades organizacionais (OUs) ou grupos de contas que servem a um único aplicativo ou serviço. Aplique políticas de tags para classificar ou rastrear recursos em sua organização e forneça controle de acesso baseado em atributos para usuários ou aplicações. Além disso, você pode delegar a responsabilidade pelo suporte Serviços da AWS às contas para que os usuários possam gerenciá-las em nome da sua organização.

Proteja e monitore suas contas

Você pode fornecer ferramentas e acesso centralizados para que sua equipe de segurança gerencie as necessidades de segurança em nome da organização. Por exemplo, você pode fornecer acesso de segurança somente para leitura em todas as contas, detectar e mitigar ameaças com a Amazon GuardDuty, analisar o acesso não intencional aos recursos com o IAM Access Analyzer e proteger dados confidenciais com o Amazon Macie.

Controle o acesso e as permissões

Configure o AWS IAM Identity Center para fornecer acesso às Contas da AWS e aos recursos usando seu Active Directory e personalize as permissões com base em diferentes funções de trabalho. Você também pode aplicar políticas da organização a usuários, contas ou OUs. Por exemplo, as políticas de controle de serviços (SCPs) permitem que você controle o acesso a AWS recursos, serviços e regiões em sua organização. As políticas de controle de recursos (RCPs) permitem que você evite centralmente o uso não intencional de seus AWS recursos. As políticas de aplicativos de bate-papo permitem que você controle o acesso às contas da sua organização a partir de aplicativos de bate-papo, como Slack e Microsoft Teams.

Compartilhe recursos entre contas

Você pode compartilhar AWS recursos em sua organização usando AWS Resource Access Manager (AWS RAM). Por exemplo, crie sub-redes da Amazon Virtual Private Cloud (Amazon VPC) uma vez e as compartilhe-as em toda a organização. Você também pode concordar centralmente com licenças de software usando o AWS License Manager e compartilhar um catálogo de serviços de TI e produtos personalizados entre contas com o AWS Service Catalog.

Audite seu ambiente para verificar a conformidade

Você pode ativar várias contas do AWS CloudTrail, o que cria um log de todas as atividades em seu ambiente de nuvem que não podem ser desativadas ou modificadas pelas contas dos

membros. Além disso, você pode definir políticas para impor backups na cadência especificada ou definir as configurações recomendadas para recursos em todas as contas e Regiões da AWS com AWS Backup. AWS Config

Gerencie centralmente o faturamento e os custos

O Organizations fornece uma única fatura consolidada. Além disso, você pode visualizar o uso de recursos em todas as contas, monitorar os custos usando o AWS Cost Explorer e otimizar o uso dos recursos de computação com o AWS Compute Optimizer.

Casos de uso para AWS Organizations

A seguir estão alguns casos de uso para AWS Organizations:

Automatize a criação Contas da AWS e categorize as cargas de trabalho

Você pode automatizar a criação de Contas da AWS para lançar rapidamente novas cargas de trabalho. Adicione as contas a grupos definidos pelo usuário para aplicação instantânea de políticas de segurança, implantações de infraestrutura sem contato e auditoria. Crie grupos separados para categorizar as contas de desenvolvimento e produção e use AWS CloudFormation StackSetspara provisionar serviços e permissões para cada grupo.

Definir e aplicar políticas de auditoria e conformidade

Você pode aplicar políticas de controle de serviço (SCPs) para garantir que seus usuários realizem somente as ações que atendam aos seus requisitos de segurança e conformidade. Crie um log central de todas as ações realizadas em sua organização usando o AWS CloudTrail. Visualize e aplique configurações de recursos padrão em todas as contas e Regiões da AWS usando. AWS Config Aplique automaticamente backups regulares usando o AWS Backup. Use AWS Control Towerpara aplicar regras de governança predefinidas para segurança, operações e conformidade de suas AWS cargas de trabalho.

Forneça ferramentas e acesso para suas equipes de segurança e, ao mesmo tempo, incentive o desenvolvimento

Crie um grupo de segurança e forneça a ele acesso somente de leitura a todos os seus recursos para identificar e mitigar problemas de segurança. Você pode permitir que esse grupo gerencie a Amazon para que eles GuardDuty possam monitorar e mitigar ativamente as ameaças às suas cargas de trabalho, e o IAM Access Analyzer identifique rapidamente o acesso não intencional aos seus recursos.

Compartilhe recursos comuns entre contas

O Organizations facilita o compartilhamento de recursos centrais essenciais em todas as contas. Por exemplo, você pode compartilhar sua AWS Directory Service for Microsoft Active Directory central para que as aplicações possam acessar seu armazenamento central de identidades.

Compartilhe recursos centrais essenciais em suas contas

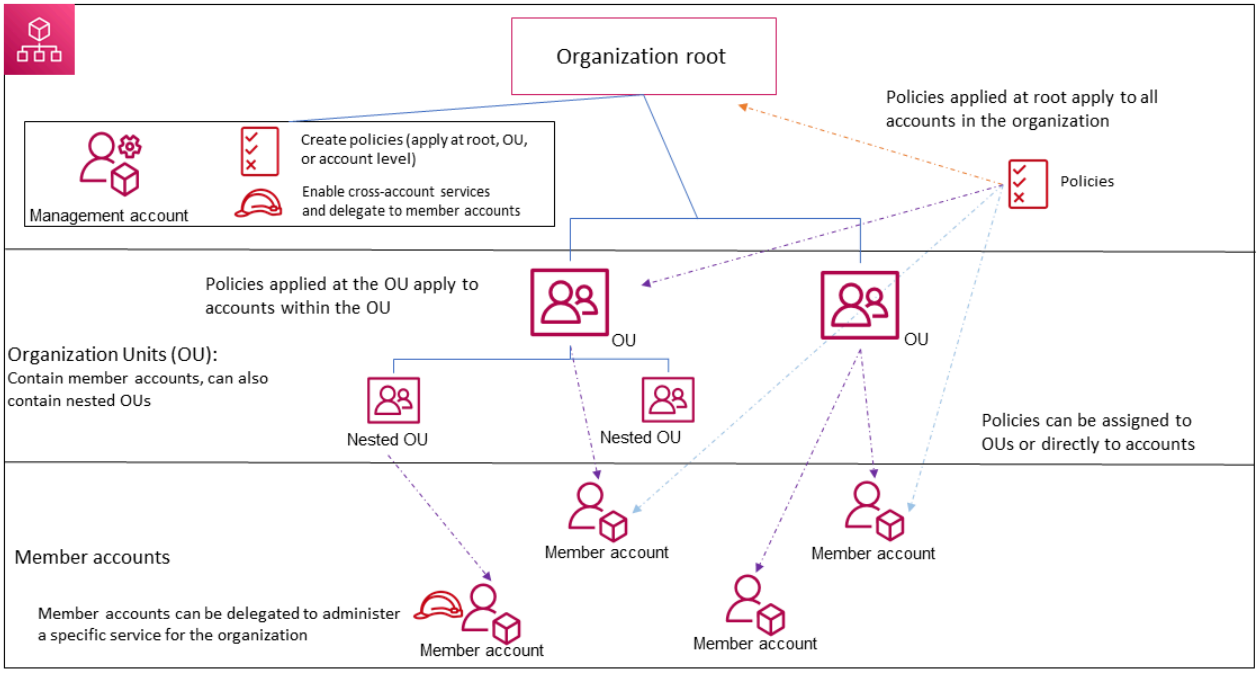
Compartilhe seu AWS Directory Service for Microsoft Active Directory como um armazenamento central de identidades para suas aplicações. Use o AWS Service Catalog para compartilhar serviços de TI em contas designadas para que os usuários possam descobrir e implantar rapidamente os serviços aprovados. Garanta que os recursos de aplicação sejam criados em suas sub-redes da Amazon Virtual Private Cloud (Amazon VPC) definindo-as centralmente uma vez e compartilhando-as em toda a organização usando o AWS Resource Access Manager (AWS RAM).

Terminologia e conceitos para AWS Organizations

Este tópico explica alguns dos principais conceitos do AWS Organizations.

O diagrama a seguir mostra uma organização que consiste em cinco contas organizadas em quatro unidades organizacionais (OUs) abaixo da raiz. A organização também tem várias políticas vinculadas a algumas OUs ou diretamente às contas.

Para obter uma descrição de cada um desses itens, consulte as definições neste tópico.



Tópicos

- Conjuntos de recursos disponíveis
- Estrutura da organização
- Convites e handshakes
- Políticas organizacionais

Conjuntos de recursos disponíveis

Todos os recursos (recomendado)

Todos os recursos são o conjunto de recursos padrão que está disponível para AWS Organizations. Você pode definir políticas centrais e requisitos de configuração para uma organização inteira, criar permissões ou recursos personalizados dentro da organização, gerenciar e organizar suas contas em uma única fatura e delegar responsabilidades a outras contas em nome da organização. Você também pode usar integrações com outros Serviços da AWS para definir configurações centrais, mecanismos de segurança, requisitos de auditoria e compartilhamento de recursos em todas as contas-membro em sua organização. Para obter mais informações, consulte Usando AWS Organizations com outros Serviços da AWS.

O modo Todos os recursos fornece todos os recursos de faturamento consolidado junto com os recursos administrativos.

Faturamento consolidado

O faturamento consolidado é o conjunto de recursos que fornece a funcionalidade de cobrança compartilhada, mas não inclui os recursos mais avançados do. AWS Organizations Por exemplo, você não pode permitir que outros AWS serviços se integrem à sua organização para funcionar em todas as contas, nem usar políticas para restringir o que usuários e funções em diferentes contas podem fazer.

Você pode habilitar 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. Para obter mais informações, consulte Habilitando todos os recursos de uma organização com AWS Organizations.

Estrutura da organização

Organização

Uma organização é um conjunto de Contas da AWS que você pode gerenciar centralmente e organizar em uma estrutura hierárquica em forma de árvore com uma raiz na parte superior e unidades organizacionais aninhadas sob a raiz. Cada conta pode estar diretamente na raiz ou colocada em uma das da OUs hierarquia.

Cada organização consiste em:

- Uma conta de gerenciamento
- Zero ou mais contas-membro
- Zero ou mais unidades organizacionais (OUs)
- Zero ou mais políticas

Uma organização tem a funcionalidade que é determinada pelo conjunto de recursos que você ativar.

Raiz

Uma raiz administrativa (raiz) está contida na conta de gerenciamento e é o ponto de partida para organizar suas Contas da AWS. A raiz é o contêiner mais alto na hierarquia da sua organização.

Sob essa raiz, você pode criar unidades organizacionais (OUs) para agrupar logicamente suas contas e organizá-las OUs em uma hierarquia que melhor atenda às suas necessidades.

Se você aplicar uma política de gerenciamento à raiz, ela se aplicará a todas as unidades organizacionais (OUs) e contas, incluindo a conta de gerenciamento da organização.

Se você aplicar uma política de autorização (por exemplo, uma política de controle de serviço (SCP)) à raiz, ela se aplicará a todas as unidades organizacionais (OUs) e contas de membros na organização. Ela não se aplica à conta de gerenciamento da organização.

> **Note**
>
> Você só pode ter uma raiz. AWS Organizations cria automaticamente a raiz para você quando você cria uma organização.

Unidade organizacional (UO)

Uma unidade organizacional (OU) é um grupo de Contas da AWSdentro de uma organização. Uma OU também pode conter outras, OUs permitindo que você crie uma hierarquia. Por exemplo, você pode agrupar todas as contas que pertencem ao mesmo departamento em uma OU departamental. Da mesma forma, você pode agrupar todas as contas que executam serviços de segurança em uma OU de segurança.

OUs são úteis quando você precisa aplicar os mesmos controles a um subconjunto de contas em sua organização. O aninhamento OUs permite unidades menores de gerenciamento. Por exemplo, você pode criar OUs para cada carga de trabalho e, em seguida, criar duas aninhadas OUs em cada OU de carga de trabalho para dividir as cargas de trabalho de produção da pré-produção. Eles OUs herdam as políticas da OU principal, além de quaisquer controles atribuídos diretamente à OU em nível de equipe. Incluindo a raiz e Contas da AWS criada na mais baixa OUs, sua hierarquia pode ter cinco níveis de profundidade.

Conta da AWS

An Conta da AWSé um contêiner para seus AWS recursos. Você cria e gerencia seus AWS recursos em um Conta da AWS, e Conta da AWS fornece recursos administrativos para acesso e cobrança.

Usar vários Contas da AWS é uma prática recomendada para escalar seu ambiente, pois fornece um limite de faturamento para custos, isola recursos para fins de segurança, oferece flexibilidade para indivíduos e equipes, além de ser adaptável a novos processos.

> **Note**
>
> Uma AWS conta é diferente de um usuário. Um usuário é uma identidade que você cria usando o AWS Identity and Access Management (IAM), sendo um usuário do IAM com credenciais de longo prazo ou um perfil do IAM com credenciais de curto prazo. Uma única AWS conta 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.

Conta de gerenciamento

Uma conta de gerenciamento é aquela Conta da AWS que você usa para criar sua organização. Na conta de gerenciamento, é possível fazer o seguinte:

- Criar outras contas em sua organização
- Convidar e gerenciar convites para que outras contas ingressem na sua organização
- Designar contas de administrador delegado
- Remover contas da organização
- Anexe políticas a entidades como raízes, unidades organizacionais (OUs) ou contas em sua organização
- Habilite a integração com AWS os serviços suportados para fornecer funcionalidade de serviço em todas as contas da organização.

A conta de gerenciamento é a proprietária final da organização, com controle final sobre as políticas de segurança, infraestrutura e finanças. Essa conta tem o papel de uma conta pagadora e é responsável pelo pagamento de todos as cobranças acumuladas pelas contas em sua organização.

> **Note**
>
> Você não pode alterar qual conta em sua organização é a conta de gerenciamento.

Conta-membro

Uma conta de membro é uma conta Conta da AWS, diferente da conta de gerenciamento, que faz parte de uma organização. Como um administrador de uma organização, você pode criar contas-

membro em sua organização e convidar contas existentes a participarem da organização. Você também pode aplicar políticas a contas-membro.

> **Note**
>
> Uma conta-membro pode pertencer a apenas uma organização por vez. Você pode designar contas-membro para serem contas de administrador delegado.

Administrador delegado

Recomendamos usar a conta de gerenciamento do 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 ocorre porque os recursos de segurança, como as políticas de controle de serviços (SCPs) do Organizations, não restringem nenhum usuário ou função 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 para Organizations: A partir dessas contas, você pode gerenciar as políticas da organização e anexar políticas às entidades (raízes ou contas) dentro da organização. OUs A conta de gerenciamento pode controlar as permissões de delegação em níveis granulares. Para obter mais informações, consulte Administrador delegado para AWS Organizations.
- Administrador delegado de um AWS serviço: a partir dessas contas, você pode gerenciar AWS serviços que se integram ao Organizations. 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. Para obter mais informações, consulte Administrador delegado para Serviços da AWS esse trabalho com Organizations.

Convites e handshakes

Convite

Um convite é uma solicitação feita pela conta de gerenciamento de uma organização para outra conta. Por exemplo, o processo de solicitar que uma conta independente participe de uma organização é um convite.

Os convites são implementados como apertos de mão. Talvez você não veja handshakes quando trabalha no console do AWS Organizations . Mas se você usa a AWS Organizations API AWS CLI or, deve trabalhar diretamente com apertos de mão.

Handshake

Um aperto de mão é a troca segura de informações entre duas AWS contas: um remetente e um destinatário.

Os seguintes apertos de mão são compatíveis:

- CONVITE: O Handshake é enviado para uma conta independente para que ele se junte à organização do remetente.
- ENABLE_ALL_FEATURES: aperto de mão enviado às contas dos membros convidados para ativar todos os recursos da organização.
- APPROVE_ALL_FEATURES: aperto de mão enviado para a conta de gerenciamento quando todas as contas de membros convidados tiverem sido aprovadas para habilitar todos os recursos.

Geralmente, você precisa interagir diretamente com os apertos de mão somente se trabalhar com a AWS Organizations API ou com ferramentas de linha de comando, como o. AWS CLI

Políticas organizacionais

Uma política é um “documento” com uma ou mais declarações que definem os controles que você deseja aplicar a um grupo de Contas da AWS. AWS Organizations suporta políticas de autorização e políticas de gerenciamento.

Políticas de autorização

As políticas de autorização ajudam você a gerenciar centralmente a segurança de Contas da AWS toda a organização.

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

Uma política de controle de serviço é um tipo de política que oferece controle central sobre o máximo de permissões disponíveis para usuários e funções do IAM em uma organização.

Isso significa que SCPs especifique controles centrados no principal. SCPs crie uma barreira de permissões ou defina limites para o máximo de permissões disponíveis para os diretores em suas contas de membros. Você usa um SCP quando deseja aplicar centralmente controles de acesso consistentes aos diretores da sua organização.

Isso pode incluir especificar quais serviços seus usuários e funções do IAM podem acessar, quais recursos eles podem acessar ou as condições sob as quais eles podem fazer solicitações (por exemplo, de regiões ou redes específicas). Para obter mais informações, consulte SCPs.

Política de controle de recursos (RCP)

Uma política de controle de recursos é um tipo de política que oferece controle central sobre o máximo de permissões disponíveis para recursos em uma organização.

Isso significa que RCPs especifique controles centrados em recursos. RCPs crie uma barreira de permissões ou defina limites para o máximo de permissões disponíveis para recursos em suas contas de membros. Use um RCP quando quiser aplicar centralmente controles de acesso consistentes em todos os recursos da sua organização.

Isso pode incluir restringir o acesso aos seus recursos para que eles só possam ser acessados por identidades pertencentes à sua organização ou especificar as condições sob as quais identidades externas à sua organização podem acessar seus recursos. Para obter mais informações, consulte RCPs.

Políticas de gerenciamento

As políticas de gerenciamento ajudam você a configurar Serviços da AWS e gerenciar centralmente seus recursos em toda a organização.

Política declarativa

Uma política declarativa é um tipo de política que permite declarar e aplicar centralmente as configurações desejadas para uma determinada empresa em grande escala AWS service (Serviço da AWS) em toda a organização. Depois de anexada, a configuração é sempre mantida quando o serviço adiciona novos recursos ou, para obter mais informações, consulte a política declarativa APIs.

Política de backup

Uma política de backup é um tipo de política que permite gerenciar e aplicar centralmente planos de backup aos AWS recursos nas contas de uma organização. Para obter mais informações, consulte a política de backup.

Política de tag

Uma política de tags é um tipo de política que permite padronizar as tags anexadas aos AWS recursos nas contas de uma organização. Para obter mais informações, consulte a política de tags.

Política de aplicativos de bate-papo

Uma política de aplicativos de bate-papo é um tipo de política que permite controlar o acesso às contas de uma organização a partir de aplicativos de bate-papo, como Slack e Microsoft Teams. Para obter mais informações, consulte a política de aplicativos do Chat.

Política de cancelamento de serviços de IA

Uma política de exclusão de serviços de IA é um tipo de política que permite controlar a coleta de dados de serviços de AWS IA para todas as contas em uma organização. Para obter mais informações, consulte a política de exclusão de serviços de IA.

Cotas e limites de serviço para AWS Organizations

Este tópico descreve cotas e limites de serviço para 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:

- Os nomes devem ser compostos por caracteres Unicode.
- O comprimento máximo da sequência para nomes varia de acordo com o objeto. Para obter informações sobre o limite real de cada objeto, consulte a Referência de API do AWS Organizations, encontre a operação da API que cria o objeto e veja os detalhes do parâmetro `Name` dessa operação. Por exemplo: Account name (Nome da conta) ou UO name (Nome da UO).

Considerações

Os códigos de cota de serviço podem mudar com o tempo devido às atualizações. Isso não afeta os valores nem os nomes das cotas. Para encontrar o código de cota para uma cota específica, use a ListServiceQuotasoperação e procure a `QuotaCode` resposta na saída da cota desejada.

Valores máximo e mínimo

A seguir estão os valores máximos padrão para entidades em AWS Organizations.

> **Note**
>
> Considere as seguintes informações sobre AWS Organizations cotas:
>
> - Você pode solicitar o aumento de alguns desses valores usando o console do Service Quotas.
> - AWS Organizations os limites se aplicam no nível da organização, a menos que especificado de outra forma. Muitas cotas se aplicam somente às ações realizadas na conta AWS Organizations de gerenciamento.
> - AWS Organizations é um serviço global hospedado fisicamente na região Leste dos EUA (Norte da Virgínia) (`us-east-1`). Portanto, você deve usar `us-east-1` para acessar essas cotas ao usar o console Service Quotas, AWS CLI o ou AWS um SDK.

Descrição	Limite
Número máximo padrão de contas	10: o número máximo padrão de contas permitidas em uma organizaç ão. Essa cota é ajustável e pode ser aumentada usando o console Service Quotas. Nota: somente a conta de gerenciamento de uma organização pode enviar essa solicitação de aumento de cota. Os aumentos de limite podem ser concedidos para até 10.000 contas com base nas qualifica ções e requisitos do cliente. As contas e organizações recém-criadas podem ter uma cota abaixo do padrão de 10 contas.

Descrição	Limite
	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. Quando uma conta é fechada, ela não para de contar com essa cota até que seja fechada permanentemente. Para obter mais informaçõ es sobre quando uma conta é encerrada permanentemente, consulte Período pós-encerramento no Guia de referência do AWS Gerenciam ento de contas . Alguns serviços têm limites de conta diferentes do número máximo de contas permitidas em uma organização. Para obter mais informações, consulte Limites por AWS serviço.
Período mínimo para remoção das contas criadas	Cada região suportada: 7 — O número mínimo de dias em que uma conta criada deve existir antes que você possa removê-la da organização.
Número de raízes em uma organização	1
Número de OUs em uma organização	2000
Número de políticas de cada tipo em uma organização	Políticas de controle de serviço: 10.000 Políticas de controle de recursos: 1000 Políticas declarativas: 1000 Políticas de backup: 1000 Políticas de tag: 1000 Políticas de aplicativos de bate-papo: 1000 Políticas de recusa de serviços de IA: 1000 Políticas do Security Hub: 1000

Descrição	Limite
Tamanho máximo de um documento de política	Políticas de controle de serviço: 5120 caracteres Políticas de controle de recursos: 5120 caracteres Políticas declarativas: 10.000 caracteres Políticas de backup: 10.000 caracteres Políticas de aplicativos de bate-papo: 10.000 caracteres Políticas de exclusão de serviços de IA: 2500 caracteres Políticas de tag: 10.000 caracteres Políticas do Security Hub: 10.000 caracteres Observação: se você salvar a política usando o AWS Managemen t 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 OUs profundidade abaixo de 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. 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.

Descrição	Limite
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 que você pode fechar em um período de 30 dias	10% das contas-membro em uma organização, com um máximo de 1000. Esta cota não é ajustável. • < 100 contas — Você pode fechar até 10 contas de membros • 100 a 10.000 contas — Você pode fechar até 10% de suas contas-membro • > 10.000 contas — Você pode fechar até 1000 contas-membro Depois de atingir essa cota, você pode fechar contas adicionais ou aguardar até que sua cota seja redefinida. Para obter mais informações, consulte Fechar uma AWSAWS 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

Limites por AWS serviço

A maioria Serviços da AWS suporta o número máximo declarado de contas que você pode ter em uma organização. Contudo, alguns serviços têm limites de conta diferentes do número máximo de contas permitidas em uma organização.

As tabelas a seguir mostram serviços com limites de conta diferentes.

AWS serviço	Limite	Pode ser aumentada
AWS IAM Identity Center	3000	Sim
AWS Application Migration Service	5000	Não
AWS Directory Service	250	Sim

Para obter mais informações, consulte as AWS IAM Identity Center quotas no IAM Identity Center User Guide e os AWS MGN service quota limits no Application Migration Service User Guide.

Tempos de expiração para handshakes

A seguir estão os tempos limite para apertos de mão. AWS Organizations

Descrição	Limite
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. Todos os limites de políticas são limites fixos.

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 pelo menos um SCP anexado o tempo todo quando você habilita SCPs. Não é possível remover a última SCP de uma entidade.	5	5	5
Política de controle de recursos	1 — A `RCPFullAWSAccess` política é anexada automaticamente à raiz, a cada UO e a cada conta da sua organização quando você a habilita RCPs. Você não pode separar essa política e ela	5	5	5

Tipo de política	Mínimo anexado a uma entidade	Máximo anexado à raiz	Máximo anexado por UO	Máximo anexado por conta
	conta para a cota de 5 políticas.			
Política declarativa	0	10	10	10
Política de backup	0	10	10	10
Política de tag	0	10	10	10
Política de aplicativos de bate-papo	0	5	5	5
Política de exclusão dos serviços de IA	0	5	5	5
Política do Security Hub	0	10	10	10

> **Note**
>
> Você pode ter apenas uma raiz em uma organização.

Limites de controle de utilização

As tabelas a seguir listam AWS Organizations APIs por categoria de gerenciamento e mostram suas respectivas taxas de aceleração no nível da conta e da organização.

AWS Organizations usa o algoritmo de token bucket para implementar a limitação de API. Com esse algoritmo, sua conta tem um bucket que contém um número específico de tokens. O número de tokens no bucket representa sua cota de controle de utilização a qualquer segundo.

A taxa é o ritmo fixo em que os tokens são adicionados ao token bucket por segundo.

Burst é o número máximo de tokens que podem ser adicionados e o número máximo de tokens que podem ser usados por segundo.

Por exemplo, a `DescribeAccount` API é limitada a uma Conta da AWS a 20 solicitações por segundo como taxa básica e a 30 solicitações por segundo como taxa de intermitência. A taxa de intermitência de 30 solicitações por segundo permite que você exceda temporariamente a taxa básica de 20 solicitações por segundo.

Você pode fazer 20 solicitações no primeiro segundo, que é a taxa básica. No próximo segundo, você pode fazer 30 solicitações, excedendo a linha de base, mas permanecendo dentro da taxa de intermitência de 30. No entanto, no terceiro segundo, se você tentar fazer mais de 20 solicitações, você será limitado, pois excedeu a taxa básica e a capacidade de intermitência foi usada.

A taxa de intermitência permite lidar com picos temporários no tráfego sem ser limitado, desde que a média de solicitações por segundo permaneça dentro do limite básico ao longo do tempo.

Limites de gerenciamento da conta

A tabela a seguir lista os AWS Organizations APIs para gerenciamento de contas.

AWS Organizations API	Por limite por conta (taxa, pico)	Por limite por organização (taxa, pico)
CloseAccount	,05, 1	
CreateAccount, CreateGov CloudAccount	0,1, 3	
DescribeAccount	20, 30	24, 36
DescribeCreateAccountStatus	2, 2	2, 3
LeaveOrganization	1, 1	
ListCreateAccountStatus	5, 8	6, 10

Limites de gerenciamento de handshake

A tabela a seguir lista o AWS Organizations APIs handshake da conta.

AWS Organizations API	Por limite por conta (taxa, pico)	Por limite por organização (taxa, pico)
AcceptHandshake	1, 2	5, 5
DescribeHandshake	1, 2	6, 10
CancelHandshake	2, 3	
DeclineHandshake	1, 1	5, 5
InviteAccountToOrganization	3, 5	
ListHandshakesForAccount, ListHandshakesForOrganization	5, 8	6, 10

Limites de gerenciamento da organização

A tabela a seguir lista os AWS Organizations APIs para o gerenciamento da organização.

AWS Organizations API	Por limite por conta (taxa, pico)	Por limite por organização (taxa, pico)
CreateOrganization, DeleteOrganization, EnableFullControl	1, 1	
CreateOrganizationalUnit, DescribeOrganization	1, 2	
MoveAccount, UpdateOrganizationalUnit, DeleteOrganizationalUnit	2, 3	

AWS Organizations API	Por limite por conta (taxa, pico)	Por limite por organização (taxa, pico)
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	

Limites de gerenciamento de políticas

A tabela a seguir lista os AWS Organizations APIs para gerenciamento de políticas.

AWS Organizations API	Por limite por conta (taxa, pico)	Por limite por organização (taxa, pico)
CreatePolicy, DeletePolicy, AttachPolicy, DetachPolicy	2, 3	
DescribePolicy	2, 2	2, 3
DisablePolicyType, EnablePolicyType	1, 1	
ListPolicies, ListPoliciesForTarget, ListTargetsForPolicy	5, 8	6, 10

AWS Organizations API	Por limite por conta (taxa, pico)	Por limite por organização (taxa, pico)
UpdatePolicy	2, 3	

Limites de gerenciamento do serviço

A tabela a seguir lista os AWS Organizations APIs para gerenciamento de serviços.

AWS Organizations API	Por limite por conta (taxa, pico)	Por limite por organização (taxa, pico)
Ativar AWSService acesso, desativar AWSService acesso	1, 2	
Lista AWSServiceAccessForOrganization, ListDelegatedServicesForAccount	1, 3	1, 4
ListDelegatedAdministrators	5, 8	6, 10
RegisterDelegatedAdministrator, DeregisterDelegatedAdministrator	1, 2	

Suporte regional para AWS Organizations

AWS Organizations está disponível em todas as regiões AWS comerciais AWS GovCloud (US) Regions e regiões da China.

Para obter uma lista das diferenças de funcionalidade em AWS GovCloud (US) Regions, consulte AWS Organizations em AWS GovCloud (US).

Para obter uma lista das diferenças de funcionalidade nas regiões da China, consulte AWS Organizations na China.

Os endpoints de serviço para o Organizations estão localizados:

- No Leste dos EUA (Norte da Virgínia) para organizações comerciais
- Em AWS GovCloud (Oeste dos EUA) para organizações AWS GovCloud (US)
- Na China (Ningxia) para organizações chinesas, operadas pela Ningxia Western Cloud Data Technology Co. Ltd (NWCD).

Todas as entidades organizacionais são acessíveis globalmente, exceto as organizações gerenciadas na China, da mesma forma que o AWS Identity and Access Management (IAM) funciona atualmente. Você não precisa especificar uma Região da AWS ao criar e gerenciar sua organização, mas precisará criar uma organização separada para contas usadas na China. Os usuários em sua região Contas da AWS podem usar Serviços da AWS em qualquer região geográfica em que esse serviço esteja disponível.

> **Note**
>
> As políticas de tags são aceitas somente em um subconjunto de regiões
> Aspolíticas de tag são um tipo de política que pode ajuda você a padronizar tags entre recursos nas contas da organização. As políticas de tags são aceitas somente em um subconjunto de regiões em que Organizations é suportado. Para ver uma lista das regiões em que as políticas de tags são aceitas, consulte Políticas de tags | Regiões compatíveis.

Lista de disponíveis Regiões da AWS

A tabela a seguir lista todas as Regiões da AWS disponíveis.

Nome da região	Região	Endpoint	Protocolo	
Leste dos EUA (Ohio)	us-east-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	
Leste dos EUA (Norte da Virgínia)	us-east-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS	

Nome da região	Região	Endpoint	Protocolo
Oeste dos EUA (N. da Califórnia)	us-west-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Oeste dos EUA (Oregon)	us-west-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
África (Cidade do Cabo)	af-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Ásia-Pacífico (Hong Kong)	ap-east-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Ásia-Pacífico (Hyderabad)	ap-south-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Ásia-Pacífico (Jacarta)	ap-southeast-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Ásia-Pacífico (Malásia)	ap-southeast-5	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS

Nome da região	Região	Endpoint	Protocolo
Ásia-Pacífico (Melbourne)	ap-southeast-4	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Ásia-Pacífico (Mumbai)	ap-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Ásia-Pacífico (Osaka)	ap-northeast-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Ásia-Pacífico (Seul)	ap-northeast-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Ásia-Pacífico (Singapura)	ap-southeast-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Ásia-Pacífico (Sydney)	ap-southeast-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Ásia-Pacífico (Taipei)	ap-east-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Ásia-Pacífico (Tailândia)	ap-southeast-7	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS

Nome da região	Região	Endpoint	Protocolo
Ásia-Pacífico (Tóquio)	ap-northeast-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Canadá (Central)	ca-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Oeste do Canadá (Calgary)	ca-west-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (Frankfurt)	eu-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (Irlanda)	eu-west-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (Londres)	eu-west-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (Milão)	eu-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (Paris)	eu-west-3	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (Espanha)	eu-south-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS

Nome da região	Região	Endpoint	Protocolo
Europa (Estocolmo)	eu-north-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Europa (Zurique)	eu-central-2	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Israel (Tel Aviv)	il-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
México (Central)	mx-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Oriente Médio (Barém)	me-south-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
Oriente Médio (Emirados Árabes Unidos)	me-central-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
América do Sul (São Paulo)	sa-east-1	organizations.us-east-1.amazonaws.com organizations-fips.us-east-1.amazonaws.com	HTTPS HTTPS
AWS GovCloud (Leste dos EUA)	us-gov-east-1	organizations.us-gov-west-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo	
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	organizations.us-gov-west-1.amazonaws.com	HTTPS	

Cobrança e preços para AWS Organizations

AWS Organizations é oferecido sem custo adicional. Você é cobrado somente pelos AWS recursos que os usuários e funções em suas contas de membros usam. Por exemplo, são cobradas as taxas padrão das EC2 instâncias da Amazon que são usadas por usuários ou funções em suas contas de membros. Para obter informações sobre os preços de outros AWS serviços, consulte AWS Preços.

Quem paga pelo uso incorrido pelos usuários em uma conta de AWS membro na minha organização?

O proprietário da conta de gerenciamento é responsável por pagar por todo o uso, dados e recursos usados pelas contas na organização.

Minha fatura refletirá a estrutura da unidade organizacional que eu criei na minha organização?

Sua fatura não refletirá a estrutura que você definiu em sua organização. Você pode usar etiquetas de alocação de custos individualmente Contas da AWS para categorizar e rastrear seus AWS custos, e essa alocação ficará visível na fatura consolidada de sua organização.

Support e feedback para 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 AWS Support, consulte a Ajuda do Forums.

Outros AWS recursos

- AWS Treinamento e cursos — Links para cursos especializados e baseados em funções, bem como laboratórios individualizados para ajudar a aprimorar suas AWS habilidades e ganhar experiência prática.
- 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.
- AWS Support Center — O hub para criar e gerenciar seus casos de AWS Support. Também inclui links para outros recursos úteis, como fóruns, informações técnicas FAQs, status de integridade do serviço e AWS Trusted Advisor.
- AWS Support — A principal página da web com informações sobre o AWS Support one-on-one, um canal de suporte de resposta rápida para ajudá-lo a criar e executar aplicativos na nuvem.
- Fale conosco — Um ponto de contato central para consultas sobre AWS faturamento, conta, eventos, abuso e outros problemas.
- AWS Termos do site — Informações detalhadas sobre nossos direitos autorais e nossa marca registrada; sua conta, licença e acesso ao site; e outros tópicos.

Práticas recomendadas para ambiente com várias contas

Siga estas recomendações para ajudar você a configurar e gerenciar um ambiente com várias contas no AWS Organizations.

Tópicos

Conta e credenciais

Habilite o gerenciamento de acesso raiz para simplificar o gerenciamento de credenciais de usuário raiz para contas de membros

Recomendamos que você ative o gerenciamento de acesso raiz para ajudá-lo a monitorar e remover as credenciais do usuário raiz das contas dos membros. O gerenciamento do acesso raiz impede a recuperação das credenciais do usuário raiz, melhorando a segurança da conta em sua organização.

- Remova as credenciais do usuário raiz das contas dos membros para impedir o login no usuário raiz. Isso também impede que as contas dos membros recuperem o usuário root.
- Suponha uma sessão privilegiada para realizar as seguintes tarefas nas contas dos membros:
  - Remova uma política de bucket mal configurada que negue a todas as entidades principais o acesso ao bucket do Amazon S3.
  - Exclua uma política baseada em recursos do Amazon Simple Queue Service que negue a todas as entidade principais acesso a uma fila do Amazon SQS.
  - Permita que uma conta de membro recupere suas credenciais de usuário raiz. A pessoa com acesso à caixa de entrada de e-mail do usuário raiz para a conta do membro pode redefinir a senha do usuário raiz e fazer login como usuário raiz da conta do membro.

Depois que o gerenciamento do acesso raiz é ativado, as contas de membros recém-criadas não têm secure-by-default credenciais de usuário raiz, o que elimina a necessidade de segurança adicional, como MFA após o provisionamento.

Para obter mais informações, consulte Centralizar as credenciais do usuário raiz para contas de membros no Guia do AWS Identity and Access Management usuário.

Mantenha o número de telefone de contato atualizado

Para recuperar o acesso ao seu Conta da AWS, é fundamental 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 AWS possamos 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 por meio do AWS Management Console ou Gerenciamento de contas APIs.

Existem várias maneiras de obter um número de telefone dedicado que garanta que você 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 AWS contato e compartilhe seus detalhes com as equipes específicas que precisam conhecê-lo em sua organização. 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. No caso de precisar AWS entrar em contato com o proprietário da conta, por exemplo, para confirmar o acesso, a mensagem de e-mail é 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.

Estrutura organizacional e workloads

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.

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

Recomendamos que você isole os ambientes e os dados da carga de trabalho de produção em seu nível superior orientado à carga de trabalho. OUs Você OUs deve se basear em um conjunto comum de controles, em vez de espelhar a estrutura de relatórios da sua empresa. Além da produção OUs, recomendamos que você defina um ou mais ambientes de não-produção OUs que contenham contas e ambientes de carga de trabalho usados para desenvolver e testar cargas de trabalho. Para obter orientação adicional, consulte Organização orientada à carga de trabalho OUs.

Use várias contas para organizar suas workloads

E Conta da AWS fornece segurança natural, acesso e limites de cobrança para seus AWS recursos. 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.

Serviços e gerenciamento de custos

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

Como prática recomendada, recomendamos ativar ou desativar todos os serviços com os quais você gostaria de integrar AWS Organizations usando o console desse serviço ou os equivalentes

de operações de API/comando da CLI. Usando esse método, o AWS serviço pode executar todas as etapas de inicialização necessárias para sua organização, como criar os recursos necessários e limpá-los ao desativar o serviço. AWS Gerenciamento de contas é o único serviço que requer o uso do AWS Organizations console ou APIs a ativação. Para revisar a lista de serviços que estão integrados com AWS Organizations, consulteServiços da AWS 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 marcar estratégias de nomenclatura, siga as orientações em Como marcar seus recursos. AWS Além dos recursos, você pode criar tags na raiz, nas contas e nas políticas da organização. OUs Consulte Criar sua estratégia de tags para obter informações adicionais.

Começando com AWS Organizations

Os tópicos a seguir fornecem informações para ajudar você a começar a usar o AWS Organizations. Você também pode usar os seguintes tutoriais para começar a executar tarefas usando o AWS Organizations.

Tutorial: criar e configurar uma organização

Comece a usar step-by-step as instruções para criar sua organização, convidar suas primeiras contas de membros, criar uma hierarquia de UO que contenha suas contas e aplicar algumas políticas de controle de serviço (SCPs).

Tutorial: Monitore mudanças importantes em sua organização com a Amazon EventBridge

Monitore as principais mudanças em sua organização configurando EventBridge a Amazon para acionar um alarme na forma de um e-mail, mensagem de texto SMS ou entrada de registro 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.

Tópicos

Inscrevendo-se para AWS

Tópicos

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Fazer login como usuário-raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

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

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

   Para obter instruções, consulte Habilitar o AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

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

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Criar um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do AWS IAM Identity Center .

Acessando AWS Organizations

Você pode trabalhar com AWS Organizations 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 AWS recursos. Você pode executar qualquer tarefa da sua organização usando o console.

AWS Ferramentas de linha de comando

Com as ferramentas de linha de AWS comando, você pode emitir comandos na linha de comando do seu sistema para executar AWS Organizations AWS tarefas. 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 .

AWS fornece dois conjuntos de ferramentas de linha de comando:

- AWS Command Line Interface

  O AWS Command Line Interface (AWS CLI) é uma ferramenta unificada para gerenciar seu Serviços da AWS. Com apenas uma ferramenta para baixar e configurar, você pode controlar várias na linha Serviços da AWS de comando e automatizá-las por meio de scripts.

  Para obter informações sobre como instalar e usar o AWS CLI, consulte o Guia AWS Command Line Interface do usuário.

- AWS Tools for Windows PowerShell

  As Ferramentas para Windows PowerShell permitem que desenvolvedores e administradores gerenciem seus recursos Serviços da AWS e recursos no ambiente PowerShell de script. Você pode gerenciar seus AWS recursos com as mesmas PowerShell ferramentas que usa para gerenciar seus ambientes Windows, Linux e macOS.

  Para obter informações sobre como instalar e usar as Ferramentas para Windows PowerShell, consulte o Guia AWS Tools for Windows PowerShell do Usuário.

AWS SDKs

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

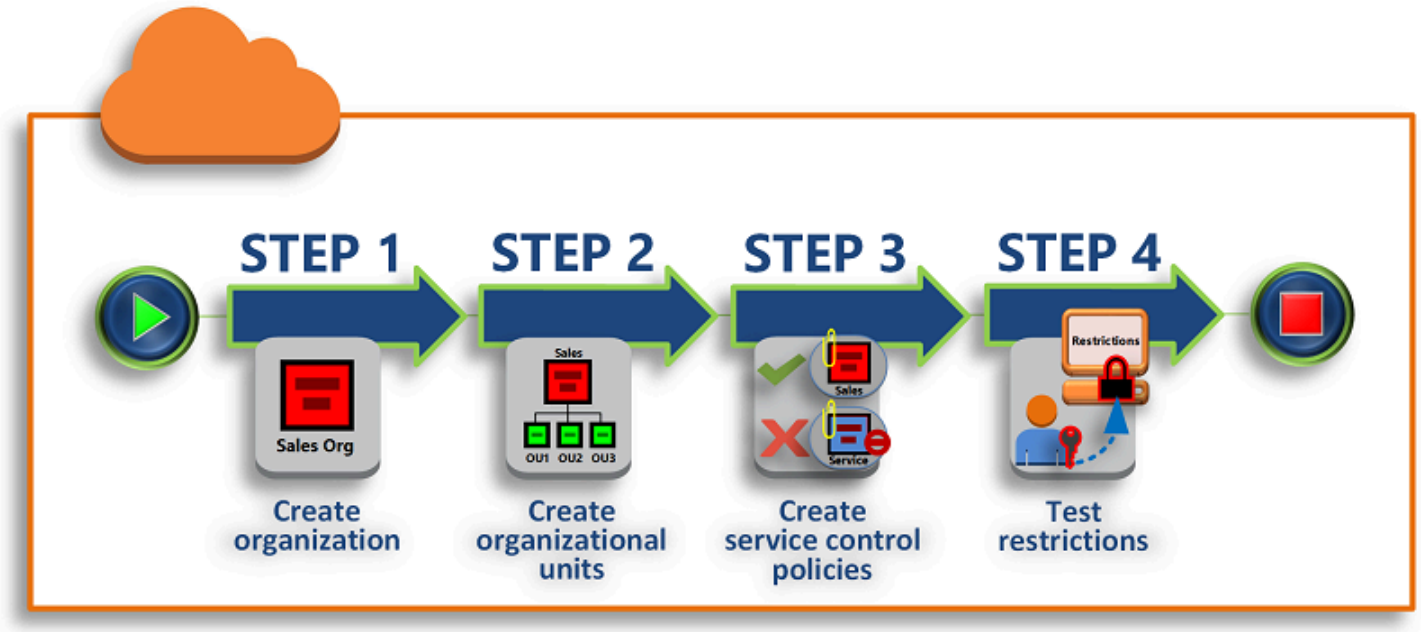
AWS Organizations API de consulta HTTPS

A API de consulta AWS Organizations HTTPS fornece acesso programático a AWS Organizations e. AWS A API de consulta HTTPS permite que você execute solicitações HTTPS diretamente para o serviço. Quando você usa a API HTTPS, deve incluir código para assinar digitalmente solicitações usando suas credenciais. Para obter mais informações, consulte Chamada de API fazendo solicitações de consulta HTTP e Referência da API do AWS Organizations.

Tutorial: criar e configurar uma organização

Neste tutorial, você cria sua organização e a configura com duas contas de AWS membros. 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 AWS introduzido antes de permitir seu uso por qualquer outra pessoa em sua empresa. Dessa forma, se AWS introduzir um novo serviço, ele permanecerá proibido até que um administrador adicione o serviço à lista de permissões na política apropriada. O tutorial também mostra como usar uma lista de negação para garantir que nenhum usuário em uma conta membro possa alterar a configuração dos registros de auditoria AWS CloudTrail criados.

A seguinte ilustração mostra as etapas principais do tutorial.



[Etapa 1: criar sua organização]

Nesta etapa, você cria uma organização com sua conta atual Conta da AWS como conta de gerenciamento. Você também convida alguém Conta da AWS para se juntar à sua organização e cria uma segunda conta como conta de membro.

[Etapa 2: criar as unidades organizacionais]

Em seguida, você cria duas unidades organizacionais (OUs) na sua nova organização e coloca as contas dos membros nelas OUs.

[Etapa 3: criar as políticas de controle de serviço]

Você pode aplicar restrições às ações que podem ser delegadas aos usuários e funções nas contas dos membros usando políticas de controle de serviço (SCPs). Nesta etapa, você cria dois SCPs e os anexa ao OUs em sua organização.

[Etapa 4: testar suas políticas da organização]

Você pode entrar como usuário de cada uma das contas de teste e ver os efeitos que SCPs elas têm nas contas.

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

Pré-requisitos

Este tutorial pressupõe que você tenha acesso a dois existentes Contas da AWS (crie um terceiro como parte deste tutorial) e que você possa entrar em cada um 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 AWS como administrador da conta 111111111111 e abra o console.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.

   AWS cria a organização e mostra a Contas da AWSpágina. 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 de endereço de e-mail com AWS Organizations.

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 Conta da AWS página Adicionar uma, escolha Convidar um existente Conta da AWS.
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`**. Como alternativa, se você souber o número de Conta da AWS identificação, poderá inseri-lo.
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 Enviar convite. AWS Organizations envia o convite para o responsável pela 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 AWS enviado pela 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 de membro

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

AWS Management Console

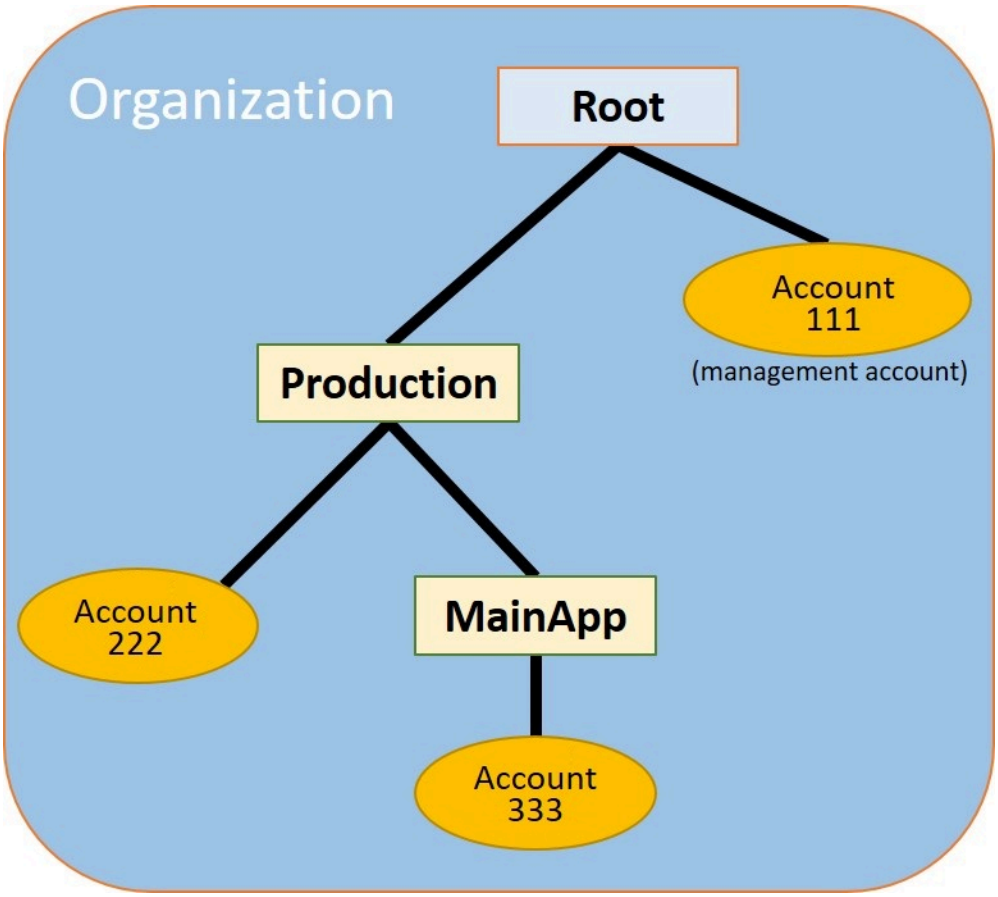
Para criar uma conta-membro

1. No AWS Organizations console, na Contas da AWSpágina, escolha Adicionar Conta da AWS.
2. Na página Adicionar uma Conta 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 Criar Conta 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 (OUs) e coloca suas contas de membros nelas. Quando terminar, a hierarquia será semelhante à seguinte ilustração. A conta de gerenciamento permanece na raiz. Uma conta membro é movida para a OU de Produção e a outra conta de membro é movida para a MainApp OU, que é filha da Produção.



AWS Management Console

Para criar e preencher o OUs

> **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. Selecione o menu suspenso Ações, depois, em Unidade organizacional, escolha 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 de membros para elas OUs.

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 MainAppOU como filha da 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 Mover Conta da AWS '333333333333', escolha o triângulo ao lado de Produção para expandi-lo. Ao lado de MainApp, escolha o botão de rádio  (não seu nome) e, em seguida, escolha 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 Mover Conta da AWS '2222222222', ao lado de Produção, escolha o botão de opção (não seu nome) e, em seguida, escolha 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 as anexa à raiz e à OUs para restringir o que os usuários nas contas da organização podem fazer. O primeiro SCP impede que qualquer pessoa em qualquer uma das contas dos membros crie ou modifique AWS CloudTrail os registros que você configurar. A conta de gerenciamento não é afetada por nenhum SCP, portanto, depois de aplicar o CloudTrail SCP, você deve criar todos os registros da 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 sua 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 aparece para informar que agora você pode criar SCPs em sua organização.

Crie seu 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 o primeiro SCP que bloqueia as ações CloudTrail de configuração

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 Política, na lista de serviços à direita, selecione CloudTrail o serviço. Em seguida, escolha as seguintes ações: AddTagsCreateTrailDeleteTrail, RemoveTags, StartLogging, StopLogging,, UpdateTraile.
5. Ainda no painel direito, escolha Adicionar recurso e especificar CloudTraile 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 negação de serviços que estão bloqueados de serem usados na MainApp OU. Neste tutorial, você bloqueia o acesso ao Amazon DynamoDB em qualquer conta que esteja na OU. MainApp

AWS Management Console

Para criar a terceira política que nega acesso a serviços que não podem ser usados na MainApp OU

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 o SCPs ao seu OUs

Agora que eles SCPs existem e estão habilitados para sua raiz, você pode anexá-los à raiz OUs e.

AWS Management Console

Para anexar as políticas à raiz e ao OUs

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 o anexa à raiz para que ele afete todas as contas dos membros para impedir que alguém altere a forma como você configurou CloudTrail.

   A página de detalhes da raiz, guia Políticas, agora mostra que duas SCPs estão anexadas à raiz: a que você acabou de anexar e a `FullAWSAccess` SCP padrão.
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 Políticas novamente para ver se duas SCPs estão anexadas à OU: a que você acabou de conectar e a `FullAWSAccess` SCP padrão. 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 OU de produção, escolha o botão de rádio para Completo AWSAccess, escolha Desanexar e, na caixa de diálogo de confirmação, escolha Desanexar 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 o SCP nomeado `Deny List for MainApp Prohibited services` para impedir que qualquer pessoa nas contas da MainApp OU use qualquer um dos serviços restritos.

    Para fazer isso, navegue até a Contas da AWSpágina, escolha o ícone de triângulo para expandir a ramificação da OU de produção e, em seguida, escolha a MainAppOU (seu nome, não o botão de rádio) para navegar até seu conteúdo.

12. Na página de MainAppdetalhes, escolha a guia Políticas.

13. Em Políticas de Controle de Serviços, escolha Anexar e, na lista de políticas disponíveis, escolha o botão de opção ao lado de Negar Lista de Serviços MainApp Proibidos e, em seguida, escolha 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. Eles SCPs não afetam nenhum usuário ou função na conta de gerenciamento, não importa em qual raiz ou OU a conta esteja localizada.
- Se você entrar como usuário na conta 222222222222, poderá realizar qualquer ação permitida pela lista de permissões. AWS Organizations nega qualquer tentativa de realizar uma ação em

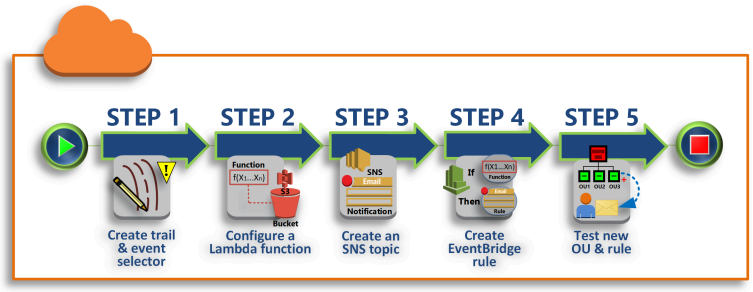
qualquer serviço que não esteja na lista de permissões. Além disso, AWS Organizations nega qualquer tentativa de realizar uma das ações de CloudTrail configuração.

- 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, AWS Organizations nega qualquer tentativa de realizar uma das ações de CloudTrail configuração.

Tutorial: Monitore mudanças importantes em sua organização com a Amazon EventBridge

Este tutorial mostra como configurar a Amazon EventBridge, antiga Amazon CloudWatch Events, para monitorar mudanças 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 EventBridge a Amazon para executar uma AWS Lambda função 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 registro, chamado de trilha, em AWS CloudTrail. Você configura-o para capturar todas as chamadas de API.

[Etapa 2: Configurar uma função do Lambda]

Crie uma AWS Lambda função que registre detalhes sobre o evento em 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 EventBridge regra da Amazon

Crie uma regra que diga EventBridge à Amazon que transmita detalhes de chamadas de API especificadas para a função Lambda e para os assinantes de tópicos do SNS.

Etapa 5: Teste sua EventBridge regra da Amazon

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 a Amazon AWS CloudTrail e EventBridge com AWS Organizations ela, consulteRegistro e monitoramento em AWS Organizations.

Pré-requisitos

Este tutorial assume o seguinte:

- Você pode entrar no AWS Management Console como usuário do IAM a partir da conta de gerenciamento da sua organização. O usuário do IAM deve ter permissões para criar e configurar um login CloudTrail, uma função no Lambda, um tópico no Amazon SNS e uma regra na 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 existente do Amazon Simple Storage Service (Amazon S3) (ou você tem permissões para criar um bucket) para receber CloudTrail o log que você configurou na etapa 1.

> **Important**
>
> Atualmente, AWS Organizations está hospedado somente na região Leste dos EUA (Norte da Virgínia) (embora esteja disponível globalmente). Para executar as etapas deste 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/gravação para que a Amazon EventBridge tenha chamadas para ativar.

Para criar uma trilha

1. Faça login AWS como administrador da conta de gerenciamento da organização e abra o CloudTrail console emhttps://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, AWS Organizations não aparece como uma opção nas EventBridge configurações da Amazon e CloudTrail não captura informações sobre 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 opções a seguir para especificar onde CloudTrail os registros devem ser entregues:

   - 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 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 Próximo.
10. Verifique suas seleções e escolha Create trail (Criar trilha).

A Amazon EventBridge permite que você escolha entre várias maneiras diferentes de enviar alertas quando uma regra de alarme corresponde 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 Lambda que registra a atividade da API que é enviada a ela pela EventBridge regra da Amazon que você configura posteriormente.

Para criar uma função Lambda que registra eventos da Amazon EventBridge

1. Abra o AWS Lambda console emhttps://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 a opção 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 faz desse tópico um alvo da EventBridge regra da Amazon que você criará 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 Criar assinatura. AWS envia um e-mail para o 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 EventBridge regra da Amazon

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

Para criar uma EventBridge regra

1. Abra o EventBridge console da Amazon emhttps://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 a criação de regras, consulte Regras na Amazon EventBridge no guia EventBridge do usuário da Amazon.

Etapa 5: Teste sua EventBridge regra da Amazon

Nesta etapa, você cria uma unidade organizacional (OU) e observa a EventBridge regra da Amazon, gera uma entrada de registro e envia um e-mail para si mesmo com detalhes sobre o evento.

AWS Management Console

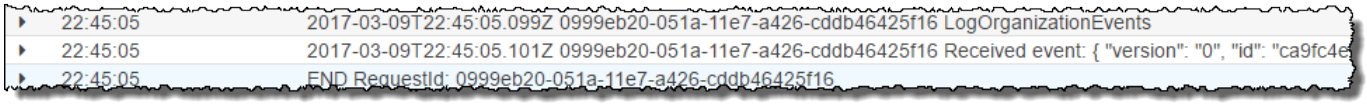
Para criar uma OU

1. Abra o AWS Organizations console na Contas da AWSpágina.
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 do EventBridge registro

1. Abra o CloudWatch console emhttps://console.aws.amazon.com/cloudwatch/.
2. Na página de navegação, escolha Logs.
3. Em Grupos de registros, escolha o grupo associado à sua função 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 há uma mensagem de Orgs em sua conta de e-mail CWEvnt (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 cobranças, você deve excluir todos AWS os recursos que você criou como parte deste tutorial e que não deseja manter.

Para limpar seu AWS ambiente

1. Use o CloudTrail console 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 CloudWatch console para excluir a EventBridge regra chamada **`OrgsMonitorRule`** que você criou 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 EventBridge para monitorar mudanças 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.

Usando AWS Organizations com um AWS SDK

AWS kits de desenvolvimento de software (SDKs) estão disponíveis para muitas linguagens de programação populares. Cada SDK fornece uma API, exemplos de código e documentação que permitem que os desenvolvedores criem facilmente aplicações em seu idioma de preferência.

Documentação do SDK	Exemplos de código
AWS SDK para C++	AWS SDK para C++ exemplos de código
AWS CLI	AWS CLI exemplos de código
AWS SDK para Go	AWS SDK para Go exemplos de código
AWS SDK para Java	AWS SDK para Java exemplos de código
AWS SDK para JavaScript	AWS SDK para JavaScript exemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin exemplos de código
AWS SDK para .NET	AWS SDK para .NET exemplos de código
AWS SDK para PHP	AWS SDK para PHP exemplos de código
Ferramentas da AWS para PowerShell	Ferramentas para exemplos PowerShell de código
AWS SDK para Python (Boto3)	AWS SDK para Python (Boto3) exemplos de código
AWS SDK para Ruby	AWS SDK para Ruby exemplos de código

Documentação do SDK	Exemplos de código
AWS SDK para Rust	AWS SDK para Rust exemplos de código
SDK da AWS para SAP ABAP	SDK da AWS para SAP ABAP exemplos de código
AWS SDK for Swift	AWS SDK for Swift exemplos de código

Exemplo de disponibilidade

Não consegue encontrar o que precisa? Solicite um exemplo de código usando o link Fornecer feedback na parte inferior desta página.

Gerenciando uma organização com AWS Organizations

Uma organização é uma coleção Contas da AWS que você pode gerenciar centralmente e organizar em uma estrutura hierárquica em forma de árvore com uma raiz na parte superior e unidades organizacionais aninhadas sob a raiz. Cada conta pode estar diretamente na raiz ou colocada em uma das da OUs hierarquia.

Cada organização consiste em:

- Uma conta de gerenciamento
- Zero ou mais contas-membro
- Zero ou mais unidades organizacionais (OUs)
- Zero ou mais políticas

Uma organização tem a funcionalidade que é determinada pelo conjunto de recursos que você ativar.

Tópicos

Criando uma organização com AWS Organizations

Você pode criar uma organização com a sua Conta da AWS 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. Por padrão, uma organização que você cria oferece suporte a todos os recursos.

Criar uma organização

Você pode criar uma organização usando o AWS Management Console ou usando um comando do SDK AWS CLI APIs ou de um deles.

Permissões mínimas

Para criar uma organização com a sua atual Conta da AWS, 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 obter mais informações, consulte Verificação de endereço de e-mail com AWS Organizations. 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

Os exemplos de código a seguir mostram como usar o `CreateOrganization`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates an organization in AWS Organizations.
/// </summary>
```

```
    public class CreateOrganization
    {
        /// <summary>
        /// Creates an Organizations client object and then uses it to create
        /// a new organization with the default user as the administrator, and
        /// then displays information about the new organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
            {
                FeatureSet = "ALL",
            });

            Organization newOrg = response.Organization;

            Console.WriteLine($"Organization: {newOrg.Id} Main Accoount:
{newOrg.MasterAccountId}");
        }
    }
```

- Para obter detalhes da API, consulte CreateOrganizationa Referência AWS SDK para .NET da API.

CLI

AWS CLI

Exemplo 1: como criar uma organização

Bill quer criar uma organização usando as credenciais da conta 111111111111. O exemplo a seguir mostra que a conta se torna a conta principal na nova organização. Como ele não especificou um conjunto de recursos, a nova organização usa como padrão todos os recursos habilitados e as políticas de controle de serviços são habilitadas na raiz.

```
aws organizations create-organization
```

A saída inclui um objeto de organização com detalhes sobre a nova organização:

```
{
        "Organization": {
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
                ],
                "MasterAccountId": "111111111111",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "FeatureSet": "ALL",
                "Id": "o-exampleorgid",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
        }
}
```

Exemplo 2: como criar uma organização apenas com os recursos de faturamento consolidados

O seguinte exemplo cria uma organização compatível apenas com os recursos de faturamento consolidados:

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

A saída inclui um objeto de organização com detalhes sobre a nova organização:

```
{
        "Organization": {
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [],
                "Id": "o-exampleorgid",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "MasterAccountId": "111111111111",
                "FeatureSet": "CONSOLIDATED_BILLING"
```

```
        }
}
```

Para obter informações, consulte Criar uma organização no Guia do usuário do AWS Organizations.

- Para obter detalhes da API, consulte CreateOrganizationem Referência de AWS CLI Comandos.

Depois de ter criado 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.

Verificação de endereço de e-mail com AWS Organizations

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, envia AWS 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.

Verificar o endereço de e-mail

Em 24 horas, siga as instruções no e-mail para verificar o seu endereço de e-mail. Se tiverem passado mais de 24 horas, consulte Como reenviar o e-mail de verificação.

Reenvie o e-mail de verificação com AWS Organizations

Se você não confirmar seu endereço de e-mail em até 24 horas, poderá reenviar a solicitação de verificação. Depois de verificar seu endereço de e-mail, você pode convidar outras pessoas Contas da AWS para 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 Como visualizar 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 obter mais informações, consulte Gerenciando convites de conta com AWS Organizations.

Alterando seu endereço de e-mail para uma organização com AWS Organizations

Para alterar o endereço de e-mail associado à sua conta de gerenciamento, consulte Atualizar o Conta da AWS nome, endereço de e-mail ou senha do usuário root no Guia de AWS Gerenciamento de contas referência.

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. Primeiro, você deve reenviar a solicitação de verificação. Depois de concluir o processo respondendo ao e-mail, suas contas convidadas poderão aceitar os convites.

Habilitando todos os recursos de uma organização com AWS Organizations

AWS Organizations tem dois conjuntos de recursos disponíveis:

- Todos os recursos — Esse conjunto de recursos é a forma preferida e padrão de trabalhar com AWS Organizations ele e inclui todos os recursos de consolidação do faturamento. 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 de gerenciamento de contas disponíveis em Organizations, como integração com AWS serviços suportados e políticas da organização.
- Recursos de faturamento consolidado: este conjunto de recursos se limita à geração de uma única fatura em toda a organização. Nenhum outro recurso de gerenciamento está disponível com o faturamento consolidado.

Se você criar uma organização apenas com conjunto de recursos de faturamento consolidado, poderá habilitar todos os recursos posteriormente. No entanto, você não pode migrar de todos os recursos para o faturamento consolidado depois que todos os recursos estiverem habilitados.

Migração padrão e migração assistida

As duas abordagens para migrar para todos os recursos são a migração padrão e a migração assistida.

A migração padrão é o processo de autoatendimento disponível para todos os AWS Organizations clientes para ativar o modo de todos os recursos.

A migração assistida é um processo disponível para os clientes do plano Enterprise Support solicitarem a AWS migração de sua organização para o modo de todos os recursos em seu nome.

> **Note**
>
> Processos unidirecionais e processos de reversão

- 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.
- Depois de ter iniciado o processo de migração assistida, ele não poderá ser revertido. Você precisará esperar 90 dias até que o processo expire se quiser passar pelo processo padrão.

Tópicos

Considerações

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:

As contas convidadas devem aprovar a migração

Quando você inicia o processo para ativar todos os recursos, AWS Organizations envia uma solicitação para cada conta de membro que você convidou para participar da 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.

As contas convidadas são notificadas sobre qual conjunto de recursos está habilitado no momento

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. Você pode continuar convidando contas para sua organização enquanto habilita todos os recursos.

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.

O processo de criação de contas em uma organização não é afetado pela migração

Você pode continuar criando contas na organização. Esse processo não é afetado por essa alteração.

O perfil vinculado ao serviço **`AWSServiceRoleForOrganizations`** é necessário

AWS Organizations verifica se cada conta de membro tem 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 receberá um convite específico para recriar essa função. Todos esses convites devem ser aceitos para a organização concluir o processo de habilitação de todos os recursos.

Processo de migração padrão para habilitar todos os atributos com o Organizations

Este tópico descreve como habilitar todos os atributos com o processo de migração padrão.

Etapa 1: solicitar que as contas convidadas aprovem a migração (conta de gerenciamento)

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).

   AWS Organizations envia uma solicitação para cada conta convidada (não criada) na organização solicitando aprovação para habilitar todos os recursos da organização. Se você tiver alguma conta criada usando AWS Organizations e o administrador da conta do membro tiver excluído a função vinculada ao serviço chamada`AWSServiceRoleForOrganizations`, AWS Organizations envia a essa 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 Etapa 3: finalizar o processo de migração para habilitar todos os atributos (conta de gerenciamento).

Etapa 2: aprovar a solicitação para habilitar todos os atributos ou recriar a função vinculada ao serviço (conta vinculada)

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, em vez disso, sua conta foi criada usando AWS Organizations e você excluiu a função `AWSServiceRoleForOrganizations` vinculada ao serviço, você 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 habilitar todos os atributos para a sua conta-membro, o membro da conta deve ter as seguintes permissões:

- `organizations:AcceptHandshake`
- `organizations:DescribeOrganization` – necessária 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 AWS Organizations console no AWS Organizations console. 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

Etapa 3: finalizar o processo de migração para habilitar todos os atributos (conta de gerenciamento)

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:
  - ListHandshakesForOrganization
  - AcceptHandshake

Processo de migração assistida para habilitar todos os recursos com o Organizations

Se você for um cliente Enterprise, pode ser difícil concluir o processo de migração padrão devido ao grande número de contas que você pode gerenciar. Por exemplo, você pode ter dificuldade em obter aprovação para migrar todas as contas convidadas em grandes organizações.

A migração assistida ajuda nesse processo, permitindo que clientes com um plano de Enterprise Support solicitem a AWS migração de sua organização para todos os recursos em seu nome. Esse processo exige que você assine um contrato afirmando que é proprietário de todas as contas,

seguido por um período de espera de 14 dias. Esse período de espera permite que as contas saiam da organização, se quiserem, antes que a migração para todos os recursos entre em vigor.

AWS Management Console

Para migrar para todos os recursos com migração assistida

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, escolha Enable all feature e selecione Assisted migration.
3. Leia os termos e condições do contrato, escolha Accept e escolha Begin process to enable all features para iniciar a migração.

> **Note**
>
> O início do processo de migração assistida substitui o processo de migração padrão
> Se você estiver habilitando todos os recursos usando o processo de migração padrão, ele será cancelado e o processo de migração assistida será iniciado.
> O processo de migração assistida é unidirecional e não pode ser revertido
> Depois de ter iniciado o processo de migração assistida, ele não poderá ser revertido. Você precisará esperar 90 dias até que o processo expire se quiser passar pelo processo padrão.

Se você usa a migração assistida, não precisa se preocupar em acessar sua conta convidada como usuário-raiz para aceitar a migração para todos os recursos.

Você pode entrar em contato com seu gerente técnico de contas (TAM) para obter detalhes exatos, andamento e cronogramas da migração assistida.

Como visualizar 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

Excluindo uma organização com AWS Organizations

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 antiga conta de gerenciamento se torna autônoma e Conta da AWS não é mais gerenciada pelo AWS Organizations. Você tem três opções:

- Você pode continuar a usá-la como uma conta independente.
- Você pode usá-la para criar uma organização diferente.
- Você pode aceitar um convite de outra organização para adicionar a conta a essa organização como uma conta-membro.

Tópicos

Considerações

Organizações excluídas não podem ser recuperadas

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.

As organizações só poderão ser excluídas depois que todas as contas-membro forem removidas

Você pode excluir uma organização somente depois que remover todas as contas-membro da organização. Se você criou algumas de suas contas de membros usando AWS Organizations, você pode 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 Saindo de uma organização a partir de uma conta de membro com AWS Organizations.

Contas-membro em estado “suspenso” não podem ser removidas de uma organização

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.

Remover conta de gerenciamento de uma organização ao excluir a organização pode afetar a conta 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, AWS IAM Identity Center exige que uma organização opere, portanto, se você remover uma conta de uma organização que ofereça suporte ao IAM Identity Center, os usuários dessa conta não poderão mais usar esse serviço.

A conta de gerenciamento de uma organização nunca é afetada pelas políticas de controle de serviços (SCPs), portanto, não há alteração nas permissões depois de não SCPs estarem mais disponíveis.

Faça backup de todos os relatórios

Não se esqueça de exportar ou fazer backup dos relatórios da conta de gerenciamento, especialmente dos relatórios de faturamento. Relatórios e históricos de nível organizacional não são armazenados quando você exclui uma organização. Todos os dados de custo (como o conjunto de dados do Cost Explorer) são excluídos. É recomendável que você faça uma exportação completa de todo o histórico de faturamento.

Para obter mais informações, consulte os Relatórios de uso e de custo, os Relatórios do Cost Explorer, os Relatórios dos Savings Plans e a Utilização e cobertura da Instância reservada (IR).

Excluir uma organização.

Use o procedimento a seguir para excluir uma organização que reverte a antiga conta de gerenciamento para uma conta autônoma Conta da AWS que não é mais gerenciada pela. 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 Removendo uma conta de membro de uma organização com AWS Organizations.
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 Fechando uma conta de membro em uma organização com AWS Organizations.

AWS CLI & AWS SDKs

Os exemplos de código a seguir mostram como usar o `DeleteOrganization`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Shows how to delete an existing organization using the AWS
    /// Organizations Service.
    /// </summary>
    public class DeleteOrganization
    {
        /// <summary>
        /// Initializes the Organizations client and then calls
        /// DeleteOrganizationAsync to delete the organization.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine("Successfully deleted organization.");
            }
            else
            {
```

```
                Console.WriteLine("Could not delete organization.");
            }
        }
    }
```

- Para obter detalhes da API, consulte DeleteOrganizationa Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como excluir uma organização

O exemplo a seguir mostra como excluir uma organização. Você deve ser administrador da conta principal na organização para poder realizar essa operação. O exemplo pressupõe que você removeu anteriormente todas as contas e políticas dos membros da organização: OUs

```
aws organizations delete-organization
```

- Para obter detalhes da API, consulte DeleteOrganizationem Referência de AWS CLI Comandos.

Gerenciando contas em uma organização com AWS Organizations

An Conta da AWSé um contêiner para seus AWS recursos. Você cria e gerencia seus AWS recursos em um Conta da AWS.

Este tópico descreve como gerenciar contas para AWS Organizations.

Tópicos

Gerenciando a conta de gerenciamento com AWS Organizations

Uma conta de gerenciamento é aquela Conta da AWS que você usa para criar sua organização.

A conta de gerenciamento é a proprietária final da organização, com controle final sobre as políticas de segurança, infraestrutura e finanças. Essa conta tem o papel de uma conta pagadora e é responsável pelo pagamento de todos as cobranças acumuladas pelas contas em sua organização.

Este tópico descreve como gerenciar a conta de gerenciamento com AWS Organizations.

Tópicos

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

A conta de gerenciamento é fundamental para todas as tarefas administrativas mencionadas, como gerenciamento de contas, políticas, integração com outros AWS serviços, 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 AWS recursos Contas da AWS em outras partes 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 serviços (SCPs) da Organizations não funcionam para restringir nenhum usuário ou função na conta de gerenciamento. Separar seus recursos da conta de gerenciamento também ajuda a entender os lançamentos em suas faturas.

Para obter uma lista de tarefas que devem ser chamadas da conta de gerenciamento, consulte Operations you can call from only the organization's management account .

Evite implantar workloads na conta de gerenciamento da organização

As operações privilegiadas podem ser realizadas na conta de gerenciamento de uma organização e 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, você pode registrar vários administradores delegados para serviços que oferecem suporte a essa funcionalidade, como compartilhamento AWS Service Catalog de software em toda a organização ou criação e implantação AWS CloudFormation StackSets de pilhas.

Para obter mais informações, consulte Arquitetura de referência de segurança, Organizando seu AWS ambiente usando várias contas e Serviços da AWS que você pode usar com AWS Organizations sugestões sobre como registrar contas de membros como administrador delegado para vários AWS serviços.

Para obter mais informações sobre como configurar administradores delegados, consulte Habilitar uma conta de administrador delegado para o AWS Gerenciamento de contas e Administrador delegado para AWS Organizations.

Como encerrar uma conta-membro em sua organização

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

Encerrar a conta de gerenciamento

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

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

AWS Management Console

Para encerrar uma conta de gerenciamento na página Contas

> **Note**
>
> Você não pode encerrar uma conta de gerenciamento diretamente no console do AWS Organizations .

1. Faça login AWS Management Console como usuário root da conta de gerenciamento que você deseja fechar. Você não poderá encerrar uma conta se tiver feito login como usuário ou perfil do IAM.
2. Verifique se não há contas-membro ativas restantes em sua organização. Para fazer isso, acesse o AWS Organizations console. Se você tiver uma conta de membro que ainda esteja ativa, você precisará seguir as orientações fornecidas em Fechando uma conta de membro em uma organização com AWS Organizations ou Para remover uma conta-membro de uma organização antes de passar para a próxima etapa.
3. No canto superior direito da barra de navegação, selecione o nome ou número da conta e, em seguida, selecione Conta.
4. Na página Conta, escolha o botão Encerrar conta. Leia e certifique-se de que entendeu as orientações para o encerramento da conta.
5. Escolha o botão Encerrar conta para iniciar o processo de encerramento da conta.
6. Em alguns minutos, você receberá uma confirmação por e-mail de que a conta foi encerrada.

AWS CLI & AWS SDKs

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

Gerenciando contas de membros com AWS Organizations

Uma conta de membro é uma conta Conta da AWS, diferente da conta de gerenciamento, que faz parte de uma organização.

Este tópico descreve como gerenciar contas de membros com AWS Organizations.

Tópicos

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

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. Contas da AWS devem basear-se em requisitos comuns de acesso. 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 e limites de serviço 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 o alcance dos limites CloseAccount da API.

Habilite o gerenciamento de acesso raiz para simplificar o gerenciamento de credenciais de usuário raiz para contas de membros

Recomendamos que você ative o gerenciamento de acesso raiz para ajudá-lo a monitorar e remover as credenciais do usuário raiz das contas dos membros. O gerenciamento do acesso raiz impede a recuperação das credenciais do usuário raiz, melhorando a segurança da conta em sua organização.

- Remova as credenciais do usuário raiz das contas dos membros para impedir o login no usuário raiz. Isso também impede que as contas dos membros recuperem o usuário root.
- Suponha uma sessão privilegiada para realizar as seguintes tarefas nas contas dos membros:
  - Remova uma política de bucket mal configurada que negue a todas as entidades principais o acesso ao bucket do Amazon S3.
  - Exclua uma política baseada em recursos do Amazon Simple Queue Service que negue a todas as entidade principais acesso a uma fila do Amazon SQS.

- Permita que uma conta de membro recupere suas credenciais de usuário raiz. A pessoa com acesso à caixa de entrada de e-mail do usuário raiz para a conta do membro pode redefinir a senha do usuário raiz e fazer login como usuário raiz da conta do membro.

Depois que o gerenciamento do acesso raiz é ativado, as contas de membros recém-criadas não têm secure-by-default credenciais de usuário raiz, o que elimina a necessidade de segurança adicional, como MFA após o provisionamento.

Para obter mais informações, consulte Centralizar as credenciais do usuário raiz para contas de membros no Guia do AWS Identity and Access Management usuário.

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, o SCP a seguir impede que o usuário raiz em qualquer conta membro faça qualquer chamada de API de AWS serviço, exceto “Atualizar uma política de bucket do S3 que foi configurada incorretamente e nega acesso a todos os principais” (uma das ações que exige credenciais 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.

Criação de uma conta de membro em uma organização com AWS Organizations

Este tópico descreve como criar Contas da AWS em sua organização em AWS Organizations. Para obter informações sobre como criar um single Conta da AWS, consulte o Centro de recursos de introdução.

Considerações antes de criar uma conta-membro

O Organizations cria automaticamente o perfil do IAM **`OrganizationAccountAccessRole`** para a conta-membro

Quando você cria uma conta-membro em sua organização, o Organizations cria automaticamente um perfil do IAM `OrganizationAccountAccessRole` na conta-membro, permitindo que os usuários e perfis na conta de gerenciamento exerçam controle administrativo completo sobre a conta-membro. Todas as contas adicionais vinculadas à mesma política gerenciada sejam atualizadas automaticamente sempre que a política for atualizada. Essa função está sujeita a qualquer política de controle de serviço (SCPs) que se aplique à conta do membro.

Organizations cria automaticamente a função vinculada ao serviço **`AWSServiceRoleForOrganizations`** para a conta do membro

Quando você cria uma conta-membro em sua organização, o Organizations automaticamente cria um perfil vinculado ao serviço `AWSServiceRoleForOrganizations` na conta-membro, permitindo a integração com serviços específicos da AWS . Você deve configurar os outros serviços para permitir a integração. Para obter mais informações, consulte AWS Organizations e funções vinculadas ao serviço.

As contas-membro só podem ser criadas na raiz de uma organização

As contas de membros em uma organização só podem ser criadas na raiz de uma organização. Depois de criar uma conta de membro raiz de uma organização, você pode movê-la entre OUs. Para obter mais informações, consulte Movendo contas para uma unidade organizacional (OU) ou entre a raiz e OUs com AWS Organizations.

As políticas vinculadas à raiz se aplicam imediatamente

Se você tiver alguma política anexada à raiz, essa política será aplicada imediatamente a todos os usuários e funções na conta criada.

Se você habilitou a confiança de serviço para outro AWS serviço da sua organização, esse serviço confiável pode criar funções vinculadas ao serviço ou realizar ações em qualquer conta membro da organização, incluindo sua conta criada.

As contas-membro devem optar por receber e-mails de marketing

As contas de membros que você cria como parte de uma organização não são automaticamente inscritas em e-mails AWS de marketing. Para inscrever suas contas para receber e-mails de marketing, consulte https://pages.awscloud.com/communication-preferences.

As contas de membros de organizações gerenciadas por AWS Control Tower devem ser criadas em AWS Control Tower

Se sua organização for gerenciada por AWS Control Tower, recomendamos que você crie suas contas de membros usando a fábrica de AWS Control Tower contas no AWS Control Tower console ou usando AWS Control Tower APIs o.

Se você criar uma conta de membro em Organizations quando a organização for gerenciada por AWS Control Tower, a conta não será cadastrada com AWS Control Tower. Para obter mais informações, consulte Referência a recursos fora do AWS Control Tower no Manual do usuário do AWS Control Tower .

Crie uma conta de membro

Depois de fazer login na conta de gerenciamento da organização, você pode criar contas-membro que são parte de sua organização.

Ao criar uma conta usando o procedimento a seguir, copia AWS Organizations automaticamente as seguintes informações de contato principal da conta de gerenciamento para a nova conta de membro:

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

O Organizations também copia a linguagem de comunicação e as informações do Marketplace (fornecedor da conta em alguns Regiões da AWS casos) da conta de gerenciamento.

> **Permissões mínimas**
>
> Para criar uma conta membro em sua organização, você deve ter as seguintes permissões:
>
> - `organizations:DescribeOrganization` – necessário somente ao usar o console do Organizations
> - `organizations:CreateAccount`
> - `iam:CreateServiceLinkedRole`

AWS Management Console

Para criar um Conta da AWS que seja automaticamente parte 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, 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. Esse endereço de e-mail ainda não pode estar associado a outro Conta da AWS porque se torna a credencial do nome de usuário do 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, AWS Organizations atribua à função um 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 Criar Conta da AWS.

   - 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 AWS CloudTrail registro para obter informações sobre se a criação da conta foi bem-sucedida. Para obter mais informações, consulte Registro e monitoramento em 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 Acessando contas de membros em uma organização com AWS Organizations.

AWS CLI & AWS SDKs

Os exemplos de código a seguir mostram como usar o `CreateAccount`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations account.
/// </summary>
public class CreateAccount
{
    /// <summary>
    /// Initializes an Organizations client object and uses it to create
    /// the new account with the name specified in accountName.
    /// </summary>
    public static async Task Main()
    {
        IAmazonOrganizations client = new AmazonOrganizationsClient();
        var accountName = "ExampleAccount";
        var email = "someone@example.com";

        var request = new CreateAccountRequest
        {
            AccountName = accountName,
            Email = email,
        };

        var response = await client.CreateAccountAsync(request);
        var status = response.CreateAccountStatus;
```

```
            Console.WriteLine($"The staus of {status.AccountName} is
 {status.State}.");
        }
    }
```

- Para obter detalhes da API, consulte CreateAccounta Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como criar uma conta de membro que automaticamente faça parte da organização

O exemplo a seguir mostra como criar uma conta de membro em uma organização. A conta de membro é configurada com o nome Production Account e o endereço de e-mail susan@example.com. Organizations cria automaticamente uma função do IAM usando o nome padrão de OrganizationAccountAccessRole porque o parâmetro roleName não está especificado. Além disso, a configuração que permite que usuários ou funções do IAM com permissões suficientes acessem os dados de faturamento da conta é definida com o valor padrão de ALLOW porque o IamUserAccessToBilling parâmetro não foi especificado. Organizations envia automaticamente a Susan um e-mail de “Bem-vindo a AWS”:

```
aws organizations create-account --email susan@example.com --account-
name "Production Account"
```

A saída inclui um objeto de solicitação que mostra que o status agora é `IN_PROGRESS`:

```
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

Posteriormente, você pode consultar o status atual da solicitação fornecendo o valor de resposta Id ao describe-create-account-status comando como o valor do create-account-request-id parâmetro.

Para obter mais informações, consulte Criando uma AWS conta em sua organização no Guia do Usuário do AWS Organizations.

- Para obter detalhes da API, consulte CreateAccountem Referência de AWS CLI Comandos.

Acessando contas de membros em uma organização com AWS Organizations

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 criá-lo, mas recomendamos que você o nomeie de forma consistente em todas as suas contas. AWS Organizations não cria nenhum outro usuário ou função.

Para acessar as contas em sua organização, você deve usar um dos seguintes métodos:

Permissões mínimas

Para acessar e Conta da AWS de qualquer outra conta em sua organização, você deve ter a seguinte permissão:

- `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

Using the root user (Not recommended for everyday tasks)

Quando você cria uma nova conta de membro em sua organização, a conta não tem credenciais de usuário raiz por padrão. As contas-membro não podem fazer login com o usuário-raiz nem realizar a recuperação da senha do usuário-raiz, a menos que a recuperação de conta esteja habilitada.

Você pode centralizar o acesso root às contas dos membros para remover as credenciais do usuário root das contas existentes na sua organização. A exclusão das credenciais do usuário raiz remove a senha do usuário raiz, as chaves de acesso, os certificados de assinatura e desativa a autenticação multifator (MFA). Essas contas-membro não têm credenciais de usuário-raiz, não podem fazer login como usuário-raiz e são impedidas de recuperar a senha do usuário-raiz. As novas contas que você criar no Organizations não terão credenciais de usuário-raiz por padrão.

Entre em contato com seu administrador se precisar realizar uma tarefa que exija credenciais de usuário raiz em uma conta de membro em que as credenciais do usuário raiz não estejam presentes.

Para acessar sua conta de membro como usuário root, você deve passar pelo processo de recuperação de senha. Consulte Esqueci a senha de usuário-raiz da minha Conta da AWS no Guia do usuário do AWS Sign-In para obter mais informações.

Se você precisar acessar uma conta de membro usando o usuário root, siga estas melhores práticas:

- Não use o usuário root para acessar sua conta, exceto para criar outros usuários e funções com permissões mais limitadas. Em seguida, faça login como um desses usuários ou funções.
- Ative a autenticação multifator (MFA) no usuário raiz. Redefina a senha e atribua um dispositivo MFA ao usuário raiz.

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 recomendações adicionais de segurança do usuário root, consulte as melhores práticas do usuário root para você Conta da AWS no Guia do usuário do IAM.

Using trusted access for IAM Identity Center

Use AWS IAM Identity Centere habilite o acesso confiável para o IAM Identity Center com AWS Organizations. Isso permite que os usuários entrem no portal de AWS acesso com suas credenciais corporativas e acessem recursos na conta de gerenciamento atribuída ou nas contas de membros.

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.

Using the IAM role OrganizationAccountAccessRole

Se você criar uma conta usando as ferramentas fornecidas como parte do AWS Organizations, poderá acessar a conta usando a função pré-configurada chamada `OrganizationAccountAccessRole` que existe em todas as novas contas que você cria dessa forma. Para obter mais informações, consulte Acessando uma conta de membro que tem OrganizationAccountAccessRole com AWS Organizations.

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 Criação OrganizationAccountAccessRole de uma conta convidada com AWS Organizations.

Depois de criar a função, acesse-a usando as etapas em Acessando uma conta de membro que tem OrganizationAccountAccessRole com AWS Organizations.

Tópicos

Criação OrganizationAccountAccessRole de uma conta convidada com AWS Organizations

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 Acessando uma conta de membro que tem OrganizationAccountAccessRole com AWS Organizations.

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 AWS Organizations administrador em uma conta de 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 acesse Perfis e, em seguida, escolha Criar perfil.
3. Escolha e Conta da AWS, em seguida, selecione Outro Conta da AWS.
4. Insira o número de ID de 12 dígitos da conta de gerenciamento 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 externo, consulte Quando devo usar um ID externo? 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 MFA, consulte Uso da autenticação multifator (MFA) na AWS no Guia do usuário do IAM.
5. Escolha Próximo.
6. Na página Adicionar permissões, selecione a política gerenciada da AWS denominada `AdministratorAccess` e, em seguida, selecione Próximo.
7. Na página Nomear, revisar e criar, especifique um nome de perfil 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. Acesse 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 de ID AWS da conta do membro e, em seguida, insira o nome da função que você criou anteriormente nas etapas de 1 a 8. Escolha Add (Adicionar) 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 selecione Criar política para salvar suas alterações.
18. Escolha Grupos de usuário no painel de navegação e escolha o nome do grupo (não a caixa de seleção) que você deseja usar para delegar a administração da conta-membro.
19. Escolha a aba Permissões.
20. Escolha Adicionar permissões, Anexar política e selecione a política que criou nas etapas 11–18.

Os usuários que são membros do grupo selecionado agora podem usar o URLs que você capturou na etapa 9 para acessar a função de cada conta de 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 Acessando uma conta de membro que tem OrganizationAccountAccessRole com AWS Organizations.

Acessando uma conta de membro que tem OrganizationAccountAccessRole com AWS Organizations

Quando você cria uma conta de membro usando o AWS Organizations console, cria AWS Organizations automaticamente uma função do IAM nomeada `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 Criação OrganizationAccountAccessRole de uma conta convidada com AWS Organizations.

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 https://console.aws.amazon.com/iam/como um 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, escolha Choose a service, digite **STS** na caixa de pesquisa para filtrar a lista e escolha a opção STS.
4. Na seção Ações, insira **assume** na caixa de pesquisa para filtrar a lista e escolha a AssumeRoleopção.
5. Na seção Recursos, escolha Específico, escolha Adicionar ARNs
6. Na seção Specify ARN(s), escolha Other account para o recurso.
7. Insira o ID da conta-membro que você acabou de criar
8. Em Resource role name with path, insira o nome do perfil criado na seção anterior (recomendamos dar a ele o nome `OrganizationAccountAccessRole`).
9. Escolha Adicionar ARNs quando a caixa de diálogo exibir o ARN correto.
10. (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.
11. Escolha Próximo.

12. Na página Review and create, insira um nome para a política. Por exemplo: **`GrantAccessToOrganizationAccountAccessRole`**. Você também pode adicionar uma descrição opcional.
13. Escolha Criar política para salvar a nova política gerenciada.
14. Agora que você tem a política disponível, poderá associá-la a um grupo.

    No painel de navegação, escolha Groups e selecione o nome do grupo (não a caixa de seleção) cujos membros você deseja que assumam a função na conta-membro. Se necessário, você poderá criar outro grupo.
15. Escolha a guia Permissões, escolha Adicionar permissões e depois Anexar políticas.
16. (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 13. Você também pode filtrar todas as políticas gerenciadas da AWS selecionando Policy Type e Customer Managed.
17. Marque a caixa ao lado da política e selecione Attach policies.

Os usuários do IAM que são membros do grupo agora têm permissões para mudar para a nova função no AWS Organizations console usando o procedimento a seguir.

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 AWS Organizations console, escolha o link que contém seu nome de login atual e escolha Trocar 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*

Fechando uma conta de membro em uma organização com AWS Organizations

Se não precisar mais de uma conta-membro em sua organização, é possível encerrá-la no console do AWS Organizations seguindo as instruções apresentadas neste tópico. 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 encerrar uma conta de gerenciamento, consulte Como encerrar uma conta-membro em sua organização.

Encerrar 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 encerrar sua conta-membro, é altamente recomendável que você analise as considerações e entenda o impacto do encerramento de uma conta. Para obter mais informações, consulte O que você precisa saber antes de encerrar a conta e O que esperar depois de encerrar a conta no Guia de gerenciamento de contas da AWS .

AWS Management Console

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

1. Faça login no console do AWS Organizations. Você deve entrar como usuário do IAM ou como usuário raiz (não recomendado) na conta de gerenciamento da organização.

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. Essa opção só está disponível quando uma AWS organização está no modo Todos os recursos.

> **Note**
>
> Se sua organização estiver usando o modo de cobrança consolidada, você não conseguirá ver o botão Fechar no console. Para fechar uma conta no modo de cobrança consolidada, faça login na conta que você deseja fechar como usuário root. Na página Contas, escolha o botão Fechar conta, insira o ID da sua conta e, em seguida, escolha o botão Fechar conta.

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

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

Para encerrar uma conta-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

Protegendo as contas dos membros contra o encerramento com AWS Organizations

Para proteger as contas dos membros contra o encerramento acidental, crie uma política do IAM que especifique quais contas estão isentas. Essa política impede o encerramento de contas de membros protegidas.

Crie uma política do IAM para negar o encerramento da conta usando um destes métodos:

- Liste explicitamente as contas protegidas no `Resource` elemento da política usando suas. ARNs
- Marque contas individuais e use a chave de condição `aws:ResourceTag` global para evitar o encerramento de contas marcadas.

> **As políticas de controle de serviços não podem proteger as contas dos membros**
>
> As políticas de controle de serviço (SCPs) não podem proteger as contas dos membros porque SCPs não afetam os diretores do IAM na conta de gerenciamento.

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-membro encerrem suas contas.

Prevent member accounts with tags from getting closed

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"}
            }
        }
    ]
}
```

Prevent member accounts listed in this policy from getting closed

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"
            ]
        }
    ]
}
```

Removendo uma conta de membro de uma organização com AWS Organizations

A remoção de uma conta-membro não encerra a conta, mas remove a conta-membro da organização. A antiga conta de membro se torna autônoma e Conta da AWS não é mais gerenciada por 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.

Considerações

Os perfis de acesso do IAM criados pela conta de gerenciamento não são excluídas automaticamente

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.

Você pode remover uma conta de sua organização somente se a conta tem as informações necessárias para operar como uma conta autônoma

Você pode remover uma conta de sua organização somente se a conta tem as informações necessárias para operar como uma conta autônoma. Quando você cria uma conta em uma organização usando o AWS Organizations console, a API ou os AWS CLI comandos, todas as informações exigidas das contas independentes não são coletadas automaticamente.

Para cada conta que você deseja tornar independente, você deve escolher um plano de suporte, fornecer e verificar as informações de contato necessárias e fornecer uma forma de pagamento atual. AWS usa a forma de pagamento para cobrar por qualquer AWS atividade faturável (não de nível AWS gratuito) que ocorra enquanto a conta não está vinculada a uma organização. Para remover uma conta que ainda não tem essas informações, siga as etapas em Saindo de uma organização a partir de uma conta de membro com AWS Organizations.

Você deve aguardar pelo menos sete dias após a criação da conta

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.

O proprietário da conta que sai se torna responsável por todos os novos custos acumulados

No momento em que a conta deixa a organização com sucesso, o proprietário da Conta da AWS se torna responsável por todos os novos AWS custos acumulados e a forma de pagamento da conta é usada. A conta de gerenciamento da organização não é mais responsável.

A conta não pode ser uma conta de administrador delegado para nenhum AWS serviço habilitado para a organização

A conta que você deseja remover não deve ser uma conta de administrador delegado para nenhum AWS serviço 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 de um AWS serviço, consulte a documentação desse serviço.

A conta não tem mais acesso aos dados de custo e uso

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.

As tags anexadas à conta são excluídas

Quando uma conta-membro sai de uma organização, todas as tags anexadas à conta são excluídas.

As entidades principais da conta não são mais afetadas por nenhuma política da organização

As entidades primárias da conta não são mais afetadas pelas políticas que se aplicavam na organização. Isso significa que as restrições SCPs impostas por desapareceram e que os usuários e funções na conta podem ter mais permissões do que tinham antes. Outros tipos de política da organização não podem mais ser aplicados ou processados.

A conta não está mais coberta pelos contratos da organização

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 acordos organizacionais ativos pode ser visualizada no AWS Artifact console na página Acordos AWS Artifact Organizacionais.

A integração com outros serviços pode ser desabilitado

A integração com outros serviços pode ser desativada. Se você remover uma conta de uma organização que tenha a integração com um AWS serviço habilitada, os usuários dessa conta não poderão mais usar esse serviço.

Para remover uma conta-membro de uma 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.

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 OU ou ativar a opção Exibir Contas da AWS somente para ver uma lista simples de contas sem a estrutura da OU. 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 OUs (escolher a) para encontrar a conta que você deseja.
3. Selecione Actions (Ações), então, em Conta da AWS, escolha Remove from organization (Remover da organização).
4. Na seção Remover conta “nome da conta” (# account-id-num) da organização? caixa de diálogo, escolha Remover conta.
5. Se AWS Organizations não conseguir remover uma ou mais contas, normalmente é porque você não forneceu todas as informações necessárias para que a conta funcione como uma conta independente. 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 ver o link Copiar, use este link para acessar a página Inscrever-se na AWS e concluir as etapas de registro que restam. 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 de concluir a última etapa de inscrição, redireciona AWS automaticamente seu navegador para o AWS Organizations console da conta do 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 Saindo de uma organização a partir de uma conta de membro com AWS Organizations.

Saindo de uma organização a partir de uma conta de membro com AWS Organizations

Quando faz login em uma conta-membro, você pode sair de uma organização. A conta de gerenciamento não pode deixar a organização usando essa técnica. Para remover a conta de gerenciamento, é necessário excluir a organização.

Considerações

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.

A conta não está mais coberta pelos contratos da organização que foram aceitos em seu nome

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 acordos organizacionais no AWS Artifact console na página Acordos AWS Artifact da Organização. 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.

Sair de uma organização como uma conta-membro

Para sair de uma organização, siga o procedimento a seguir.

Permissões mínimas

Para sair de uma organização 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 AWS Organizations console no AWS Organizations console. 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 root em uma conta de membro que foi criada usando AWS Organizations. Se necessário, recupere a senha do usuário root seguindo as etapas em Usando o usuário root (não recomendado para tarefas diárias) emAcessando contas de membros em uma organização com AWS Organizations.
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. Depois de confirmar, você será redirecionado para a página de introdução do AWS Organizations console, onde poderá ver todos os convites pendentes da sua conta para participar de 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 for esse o caso, prosseguir 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.

   Se você não vir o link Complete the account sign-up steps, use este link para acessar a página Inscrever-se na AWS e concluir as etapas de registro restantes.
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 de introdução do AWS Organizations console, onde poderá ver todos os convites pendentes da sua conta para participar de 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 dos membros também podem ser removidas por um usuário na conta de gerenciamento remove-account-from-organizationcom. Para obter mais informações, consulte Para remover uma conta-membro de uma organização.

Atualizando o nome da conta de uma conta de membro com AWS Organizations

Ao entrar na conta de gerenciamento da sua organização, você pode atualizar o nome da conta de um membro. Para saber como atualizar o nome da conta de um membro, siga as etapas em Atualizar o nome da conta de qualquer Conta da AWS membro da sua organização no Guia de AWS Gerenciamento de contas referência.

Atualizando o endereço de e-mail do usuário raiz O endereço para uma conta de membro com AWS Organizations

Para aumentar a segurança e a resiliência administrativa, os diretores do IAM na conta de gerenciamento (que têm as permissões necessárias do IAM) podem atualizar centralmente o endereço de e-mail do usuário raiz do (também chamado de endereço de e-mail principal) para

qualquer uma de suas contas membros sem precisar entrar em cada conta individualmente. Isso dá aos administradores na conta de gerenciamento (ou em uma conta de administrador delegado) mais controle sobre suas contas-membro. Também garante que os endereços de e-mail do usuário raiz Os endereços de de qualquer conta membro em toda a sua conta AWS Organizations possam ser mantidos atualizados, mesmo quando você pode ter perdido o acesso ao endereço de e-mail do usuário raiz original ou às credenciais administrativas .

Quando o endereço de e-mail do usuário raiz (endereço de) é alterado centralmente pelo administrador da conta de gerenciamento, a senha e a configuração de MFA permanecerão as mesmas de antes da alteração. Observe que o MFA pode ser ignorado por um usuário com controle do endereço de e-mail do usuário raiz da conta, endereço de e-mail de contato principal.

Para atualizar o endereço de e-mail do usuário raiz (endereço de) de uma conta membro em sua organização, sua organização deve ter habilitado anteriormente o modo de todos os recursos. AWS Organizations no modo de cobrança consolidada ou em contas que não fazem parte de uma organização, não podem atualizar o endereço de e-mail do usuário raiz do de forma centralizada. Os usuários que desejam alterar o endereço de e-mail do usuário raiz O endereço de para contas que não são suportadas pela API devem continuar usando o Billing Console para gerenciar seu endereço de e-mail do usuário raiz. O endereço de e-mail do .

Para step-by-step obter instruções sobre como atualizar o endereço de e-mail do usuário raiz da sua conta membro (endereço de), consulte Atualizar o e-mail do usuário raiz para qualquer Conta da AWS pessoa da sua organização no Guia de AWS Gerenciamento de contas referência.

Gerenciando convites de conta com AWS Organizations

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. Use o AWS Organizations console para iniciar e gerenciar os convites que você envia para outras contas. Só é possível enviar um convite para outras contas pela conta de gerenciamento de sua organização.

Quando você convida uma conta, AWS Organizations envia um convite para o proprietário da conta, que pode decidir aceitar ou recusar o convite.

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.

Para criar uma conta que faça parte de uma organização automaticamente, consulte Criação de uma conta de membro em uma organização com AWS Organizations.

> **Important**
>
> 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 de Regiões da China ou contas na partição de AWS GovCloud (US) Regiões.

Tópicos

Considerações

Limitações no número de convites que você pode enviar por dia

Para saber as limitações no 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.

Uma conta só pode se juntar a uma organização

Uma conta só pode se juntar a uma organização. Se receber vários convites, você só poderá aceitar um.

O histórico de faturamento e os relatórios permanecem com a conta de gerenciamento

O histórico de faturamento e os relatórios de todas as contas permanecem com a conta de gerenciamento em uma organização. Antes de mover a conta para uma nova organização, exporte

ou faça o backup de todos os históricos de faturamento e relatório relativos a todas as contas-membro que você queira manter. Isso pode incluir Relatórios de uso e de custo, Relatórios do Cost Explorer, Relatórios dos Savings Plans e a Utilização e cobertura da Instância reservada (IR).

A conta de gerenciamento é responsável por todas as despesas acumuladas pelas contas-membro

Depois 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.

O Organizations cria automaticamente o perfil vinculado ao serviço **`AWSServiceRoleForOrganizations`**

AWS Organizations cria uma função vinculada a serviços chamada `AWSServiceRoleForOrganizations` para oferecer suporte a integrações entre AWS Organizations e outros serviços. AWS Para obter mais informações, consulte AWS Organizations e funções vinculadas ao serviço. A conta convidada deverá ter esse perfil se a organização for compatível com todos os recursos. É possível excluir esse perfil se a organização oferecer suporte apenas ao conjunto de recursos de faturamento consolidado. Se você excluir essa função e depois ativar todos os recursos em sua organização, AWS Organizations recriará essa função para a conta.

O Organizations não cria automaticamente o perfil do IAM **`OrganizationAccountAccessRole`**

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 obter mais informações, consulte Criação OrganizationAccountAccessRole de uma conta convidada com AWS Organizations.

> **Note**
>
> Quando você cria uma conta na sua organização em vez de convidar uma conta existente para participar, cria AWS Organizations automaticamente a função do IAM `OrganizationAccountAccessRole` por padrão.

As políticas vinculadas à raiz ou à OU que contêm a conta são aplicadas imediatamente

Se você tiver alguma política vinculada à raiz ou à unidade organizacional (OU) que contenha a conta convidada, essas políticas serão aplicadas imediatamente a todos os usuários e perfis na conta convidada.

Você pode habilitar a confiança de serviço para outro AWS serviço da 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.

Organizações com apenas o conjunto de recursos de faturamento consolidado ainda podem convidar contas

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.

Enviando convites para contas com AWS Organizations

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 obter mais informações, consulte Verificação de endereço de e-mail com AWS Organizations. 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 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

Gerenciando convites de contas pendentes com AWS Organizations

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.

   Se você não conseguir ver um convite, verifique se a conta convidada é a conta de gerenciamento de outra organização. Somente contas de membros e contas autônomas podem receber convites. As contas de gerenciamento não podem receber convites.

   Se você quiser convidar uma conta que seja uma conta de gerenciamento em outra organização, é recomendável que você torne essa conta uma conta independente.

   > **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

Aceitando ou recusando convites para contas com AWS Organizations

Se você receber um convite para participar de uma organização, pode aceitar ou recusá-lo.

Considerações

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.

Somente contas-membro e contas independentes podem aceitar ou recusar um convite

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 uma organização, essa conta não poderá ver o convite até remover todas as contas membros da organização e excluir a organização.

Aceitar ou recusar um convite de conta

Para aceitar ou recusar o convite, conclua as etapas a seguir.

Permissões mínimas

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

- `organizations:ListHandshakesForAccount`— Necessário para ver a lista de convites no AWS Organizations console.
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.
- `iam:CreateServiceLinkedRole`: necessária apenas quando a aceitação do convite requer a criação de uma função vinculada ao serviço para dar suporte à integração com outros Serviços da AWS. Para obter 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 outras AWS Organizations . Serviços da AWS Para obter 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

Migre uma conta para outra organização com AWS Organizations

Você pode migrar e Conta da AWS de uma organização para outra a qualquer momento. Por exemplo, migrar uma conta pode ser útil no caso de uma fusão e aquisição, quando você precisa consolidar uma ou mais Contas da AWS de várias organizações em uma organização.

Seja qual for o seu caso de uso, a migração de uma conta entre organizações exige que você remova a conta da organização antiga, transforme-a em uma conta independente e que a conta aceite o convite da nova organização para ingressar na nova organização. Suas workloads e serviços continuarão operando de acordo com suas especificações durante a migração. No entanto, é importante estar ciente de quaisquer dependências que você possa usar em sua organização.

> **Note**
>
> Contas encerradas ou suspensas não podem ser migradas

Contas encerradas ou suspensas não podem ser migradas. Para reativar uma conta, entre em contato com o Suporte.

Requisito de espera de sete dias

Para migrar uma conta que você criou na organização, deve aguardar pelo menos sete dias após a criação da conta. As contas convidadas não estão sujeitas a esse período de espera.

Replicação de dados entre contas

A seguinte orientação AWS prescritiva fornece informações sobre estratégias para replicar dados entre Contas da AWS: Replicação de recursos ou migração entre. Contas da AWS

O que você precisa fazer antes de migrar uma conta

Antes de migrar seu Conta da AWS de uma organização para outra, verifique se você concluiu as etapas a seguir.

Etapa 1: verificar se você tem as permissões necessárias do IAM para migrar uma conta

Etapa 1

Verifique se você aplicou as permissões necessárias para migrar uma conta para as respectivas organizações.

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

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

Para obter mais informações, consulte Sair de uma organização com sua conta-membro.

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

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

Para obter mais informações, consulte Convidar um homem Conta da AWS para se juntar à sua organização.

Para migrar uma conta, você não pode ter políticas de IAM ou políticas de controle de serviços que impeçam a migração

Se você for a conta de gerenciamento ou um administrador delegado, poderá controlar o acesso aos AWS recursos anexando políticas de permissões às identidades do IAM (usuários, grupos e funções) dentro de uma organização. Para obter mais informações, consulte as Políticas do IAM para o AWS Organizations.

Antes de migrar uma conta:

- Verifique se não há políticas do IAM ou políticas de controle de serviço (SCPs) que impeçam você de migrar a conta.
- Identifique as políticas do IAM e as políticas de controle de serviços (SCPs) existentes que você precisa replicar na organização para a qual está migrando a conta.
- Identifique as políticas do IAM existentes que especificam o ID da sua organização. Por exemplo, .`aws:PrincipalOrgID`

Para obter mais informações, consulte Gerenciamento de políticas do IAM no Guia do usuário do IAM e nas políticas de controle de serviços (SCPs).

Etapa 2: verificar se você removeu as permissões do IAM que permitem o acesso à conta de gerenciamento antiga

Etapa 2

Verifique se você removeu as permissões do IAM que permitem o acesso à conta de gerenciamento antiga, como a `OrganizationAccountAccessRole`.

Quando você remove uma conta-membro da organização, nenhum perfil do IAM criado para permitir o acesso pela conta de gerenciamento da organização 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.

Etapa 3: conferir o método de verificação do telefone e pagamento

Etapa 3

A conta a ser migrada deve operar como uma conta independente por um período antes de migrar para a nova organização.

Para permitir que uma conta opere como uma conta independente, verifique o seguinte:

- Verifique se a verificação do seu telefone é up-to-date.
- Confirme se foi adicionada uma forma de pagamento válida para a conta para lidar com quaisquer cobranças incorridas durante a migração da conta.
- Se você usa o faturamento como forma de pagamento, verifique se a fatura é. up-to-date

Etapa 4: fazer backup de todos os relatórios

Etapa 4

Não se esqueça de exportar ou fazer backup dos relatórios da conta de gerenciamento, especialmente dos relatórios de faturamento. Relatórios e históricos de nível organizacional não são armazenados quando você migra uma conta. É recomendável que você faça uma exportação completa de todo o histórico de faturamento. Você ainda pode acessar relatórios da conta do membro, como histórico de AWS CloudTrail eventos e histórico de faturamento da conta.

> **Important**
>
> Todos os relatórios e históricos de nível organizacional, como informações de faturamento organizacional na conta de gerenciamento, serão excluídos depois que uma conta for removida de uma organização.

Para obter mais informações, consulte os Relatórios de uso e de custo, os Relatórios do Cost Explorer, os Relatórios dos Savings Plans e a Utilização e cobertura da Instância reservada (IR).

Etapa 5: verificar se há dependências da organização

Etapa 5

Confirme se a conta a ser migrada não tem dependências relacionadas à organização.

Dependências a serem verificadas:

- Se a conta for um administrador delegado, será necessário cancelar o registro das permissões do administrador delegado antes de migrar a conta. Para obter mais informações, consulte Serviços com os quais você pode usar AWS Organizations.
- Se a conta for a conta de gerenciamento, será necessário remover todas as contas-membro da organização e excluir a organização antes de migrar. Depois de excluir a organização, sua conta de gerenciamento funcionará como uma conta independente. Após a migração, a conta de gerenciamento será uma conta-membro da nova organização. Para obter mais informações, consulte Excluir uma organização.
- Se quaisquer permissões do IAM dependerem da conta, será necessário ajustar as permissões da organização antiga depois de migrar a conta para a nova organização, para que a organização antiga funcione como antes. Para obter mais informações, consulte Gerenciar permissões de acesso para a organização.
- Se você estiver usando qualquer tag de conta ou unidade organizacional (OU), precisará recriar as tags na nova organização.

(Opcional) Etapa 6: revise a orientação se você usar AWS Control Tower

(Opcional) Etapa 6

Se você estiver migrando uma conta de ou para uma organização gerenciada por AWS Control Tower, consulte a seguinte orientação AWS prescritiva: Migrar uma conta de AWS membro de para. AWS Organizations AWS Control Tower

O que você precisa fazer para migrar uma conta

O processo de migração exige que a nova organização envie um convite para a conta a ser migrada, para que a organização antiga remova a conta de migração e a conta a ser migrada aceite o convite da nova organização para ingressar na nova organização.

Para migrar uma conta

1. Envie um convite da conta de gerenciamento da nova organização para a conta a ser migrada. Você deve enviar o convite para a conta antes que ela saia da organização antiga. Isso ajuda a minimizar os custos incorridos quando a conta a ser migrada opera temporariamente como uma conta independente. Para obter informações sobre como convidar contas, consulte Convidar um homem Conta da AWS para participar da sua organização.

2. Remova a conta a ser migrada da organização antiga. Você pode remover uma conta-membro da sua organização usando a conta de gerenciamento ou sair de uma organização como conta-membro.
3. Aceite o convite para se juntar à nova organização. Para obter mais informações, consulte Accepting an invitation from an organization. As contas migradas de uma outra organização para outra serão automaticamente adicionadas à raiz da nova organização. Antes de mover uma conta para uma unidade organizacional (OU) na nova organização, é recomendável verificar se a conta a ser migrada tem as políticas organizacionais e as permissões de OU apropriadas.
4. Se quiser migrar a conta de gerenciamento, deverá remover todas as contas-membro da organização e excluir a organização antes de migrar a conta de gerenciamento para a nova organização. Depois de excluir a organização antiga, sua conta de gerenciamento operará como uma conta independente e poderá aceitar o convite da nova organização para ingressar na nova organização. Se você aceitar um convite, sua conta de gerenciamento se tornará uma conta-membro da organização.

O que você precisa fazer depois de migrar uma conta

Depois de migrar sua conta de uma organização para outra, confirme se as etapas a seguir foram concluídas.

Revisão pós-migração

1. Avalie todas as configurações da ferramenta de cobrança da conta migrada, como categorias de custo, orçamentos e alarmes de cobrança.
2. Revise e atualize as seguintes informações monetárias de todas as contas que você migrou de uma organização para outra:
   a. Se necessário, atualize as configurações fiscais na conta.
   b. Confirme se o plano do Suporte de migração da conta corresponda à conta do pagador da nova organização.
   c. Analise todas as possíveis isenções fiscais que você queira aplicar à conta que você migrou.
3. Valide e confirme as políticas existentes do IAM e as políticas de controle de serviços (SCPs) para a conta migrada. Por exemplo, talvez seja necessário atualizar o ID da organização para que algumas políticas do IAM reflitam a nova organização.

4. Atualize as tags de alocação de custos para a nova organização para a qual você migrou a conta. Você precisará atualizar todas as tags de alocação de custos anteriores coletadas pela conta que você migrou.
5. Todas as Instâncias reservadas e Saving Plans migrarão junto com a conta. Elas não são mantidas na organização antiga. Entre em contato Suporte se eles precisarem ser transferidos para a organização antiga.

Exibir detalhes de uma conta em AWS Organizations

Ao entrar na conta de gerenciamento da organização no AWS Organizations console, você pode ver detalhes sobre suas contas de membros.

> **Permissões mínimas**
>
> Para ver os detalhes de um Conta da AWS, você deve ter as seguintes permissões:
>
> - `organizations:DescribeAccount`
> - `organizations:DescribeOrganization` – necessária somente ao usar o console do Organizations
> - `organizations:ListAccounts` – necessária somente ao usar o console do Organizations

AWS Management Console

Para ver detalhes de um 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 ver detalhes de um 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

Exportar detalhes de todas as contas em AWS Organizations

Com AWS Organizations, os usuários da conta de gerenciamento e os administradores delegados de uma organização podem exportar um arquivo.csv com todos os detalhes da conta dentro 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.

> **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 todos Contas da AWS em 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.

Atualize os contatos alternativos de uma conta no AWS Organizations

Você pode atualizar contatos alternativos para contas em sua organização usando o console AWS Organizations ou programaticamente usando a CLI AWS ou. AWS SDKs Para saber como atualizar contatos alternativos, consulte Atualizar os contatos alternativos de qualquer pessoa Conta da AWS da sua organização na Referência de gerenciamento de AWS contas.

Atualize as informações de contato principais de uma conta no AWS Organizations

Você pode atualizar as informações de contato primárias das contas em sua organização usando o console AWS Organizations ou programaticamente usando a CLI AWS ou. AWS SDKs Para saber como atualizar as informações de contato principais, consulte Atualizar o contato principal de qualquer pessoa Conta da AWS da sua organização na Referência de gerenciamento de AWS contas.

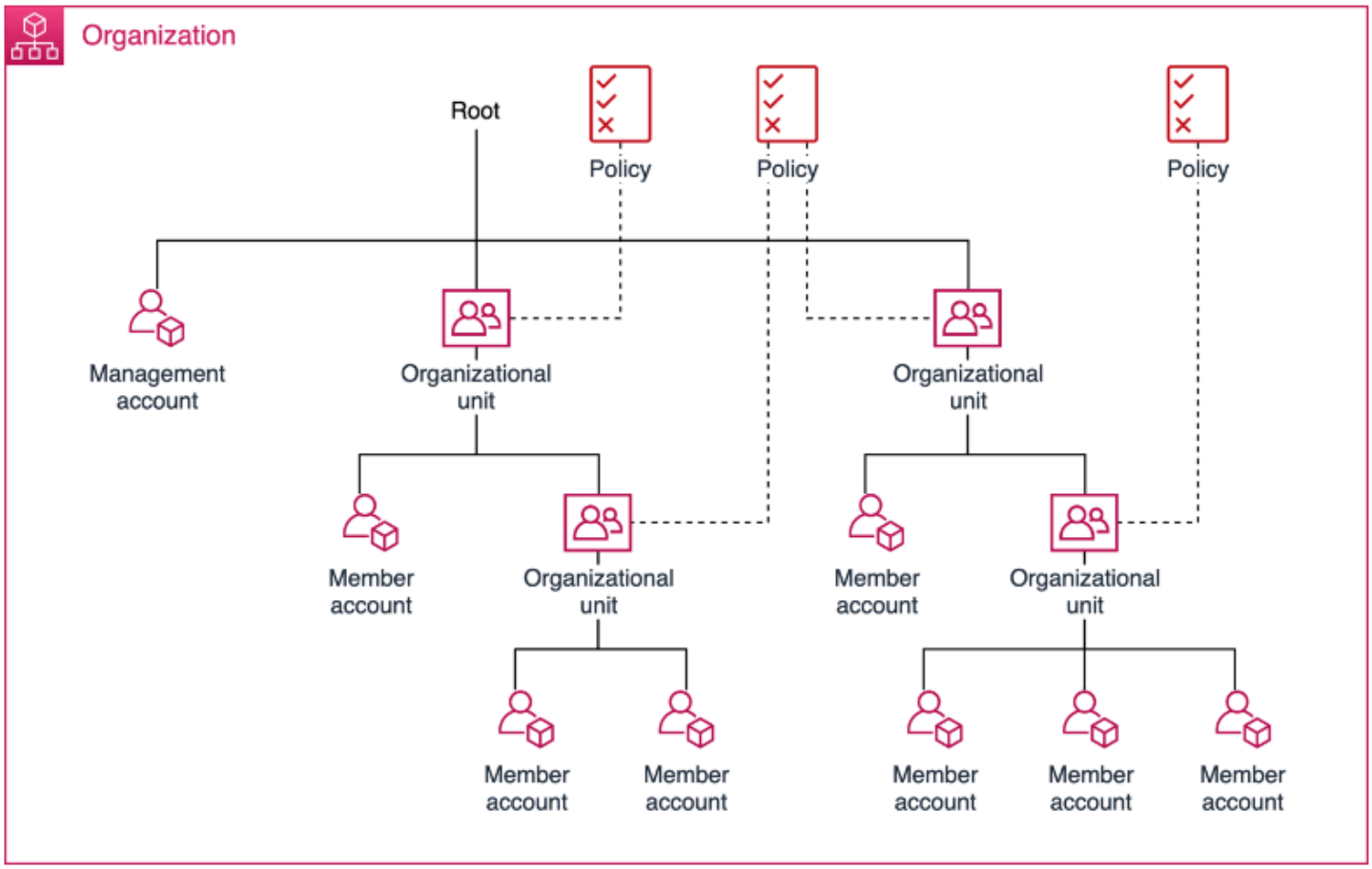
Atualização Regiões da AWS para uma conta em AWS Organizations

Você pode atualizar Regiões da AWS as contas habilitadas em sua organização usando o AWS Organizations console. Para saber como ativar a atualização Regiões da AWS, consulte Ativar ou desativar Regiões da AWS em sua AWS conta na Referência de gerenciamento de contas.

Gerenciando unidades organizacionais (OUs) com AWS Organizations

Você pode usar unidades organizacionais (OUs) para agrupar contas e administrá-las como uma única unidade. 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 OUs dentro de uma única organização, e você pode criar OUs dentro de outra OUs. 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.

O diagrama a seguir mostra uma organização que consiste em sete contas organizadas em quatro OUs abaixo da raiz. A organização também tem algumas políticas que são aplicadas OUs a.



> **Note**
>
> Há uma raiz na organização, que é AWS Organizations criada para você quando você configura sua organização pela primeira vez.

Tópicos

Melhores práticas para gerenciar unidades organizacionais (OUs) com AWS Organizations

Siga estas recomendações para ajudar você a gerenciar um ambiente com várias contas AWS Organizations usando unidades organizacionais (OUs).

Tópicos

Compreensão AWS Organizations

A base de um AWS ambiente de várias contas bem arquitetado é AWS Organizations que permite que você gerencie e administre várias contas de forma centralizada. Uma unidade organizacional (OU) é um agrupamento lógico de contas em uma organização. OUs permitem que você organize suas contas em uma hierarquia e o ajude a aplicar controles de gerenciamento. As políticas da Organizations definem os controles que você pode aplicar a um grupo de Contas da AWS. Por exemplo, uma política de controle de serviços (SCP) é uma política que define as AWS service (Serviço da AWS) ações, como Amazon EC2 Run Instance, que as contas da sua organização podem realizar.

Embora você possa começar sua AWS jornada com uma única conta, AWS recomenda que você configure várias contas à medida que suas cargas de trabalho aumentam em tamanho e complexidade. Usar um ambiente com várias contas é uma prática AWS recomendada que pode oferecer vários benefícios:

- Inovação rápida com vários requisitos: você pode alocar Contas da AWS para diferentes equipes, projetos ou produtos em sua empresa para ajudar a garantir que cada um deles possa inovar rapidamente e, ao mesmo tempo, atender aos seus próprios requisitos de segurança.
- Faturamento simplificado: o uso de vários Contas da AWS pode simplificar a forma como você aloca seus AWS custos, ajudando a identificar qual produto ou linha de serviço é responsável por uma AWS cobrança.
- Controles de segurança flexíveis: você pode usar vários Contas da AWS para isolar cargas de trabalho ou aplicativos que tenham requisitos de segurança específicos ou que precisem atender a diretrizes rígidas de conformidade, como HIPAA ou PCI.
- Adapte-se aos processos de negócios: você pode organizar vários Contas da AWS da maneira que melhor reflita as diversas necessidades dos processos de negócios da sua empresa, que têm diferentes requisitos operacionais, regulatórios e orçamentários.

Unidade organizacional fundamental recomendada () OUs

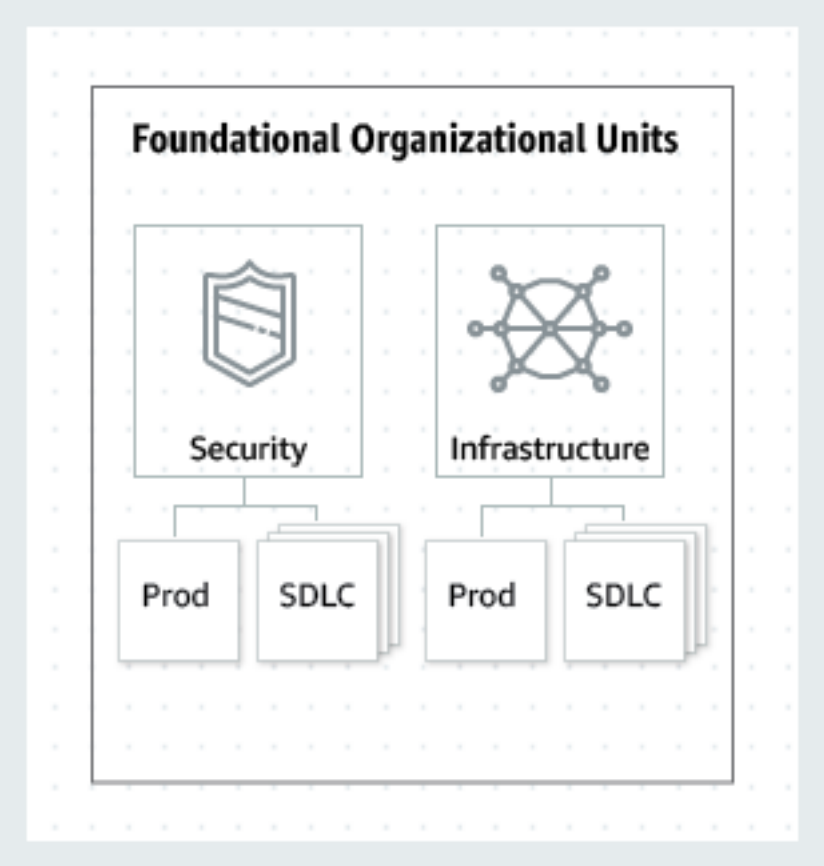
Sua unidade organizacional (OUs) deve ser baseada na função ou no conjunto comum de controles, em vez de espelhar a estrutura de relatórios da sua empresa. AWS recomenda que você comece pensando na segurança e na infraestrutura. A maioria das empresas tem equipes centralizadas que atendem a toda a organização para essas necessidades. Recomendamos criar um conjunto básico OUs para essas funções específicas:

- Segurança: usada para serviços de segurança. Crie contas para arquivos de log, acesso de segurança somente para leitura, ferramentas de segurança e de emergência.
- Infraestrutura: usada para serviços de infraestrutura compartilhada, como serviços de rede e TI. Crie contas para cada tipo de serviço de infraestrutura que você precisar.

Como a maioria das empresas tem requisitos de políticas diferentes para cargas de trabalho de produção, a infraestrutura e a segurança podem ter sido aninhadas OUs para não produção (SDLC) e produção (Prod). As contas na OU do SDLC hospedam workloads que não sejam de produção e não devem ter dependências de produção de outras contas. Se houver variações nas políticas de OU entre os estágios do ciclo de vida, o SDLC poderá ser dividido em vários OUs (por exemplo, desenvolvimento e pré-produção). As contas na OU de Prod hospedam as workloads de produção.

Aplique políticas no nível da OU para governar o ambiente Prod e SDLC de acordo com seus requisitos. Em geral, aplicar políticas no nível da OU é uma prática melhor do que no nível da conta individual, pois simplifica o gerenciamento de políticas e qualquer possível solução de problemas.

O diagrama a seguir mostra a base OUs (Prod e SDLC) para segurança e infraestrutura:



Unidade organizacional adicional recomendada (OUs)

Depois que os serviços centrais estiverem prontos, recomendamos criar OUs algo diretamente relacionado à criação ou execução de seus produtos ou serviços. Muitos AWS clientes criam o seguinte OUs depois de estabelecer uma base:

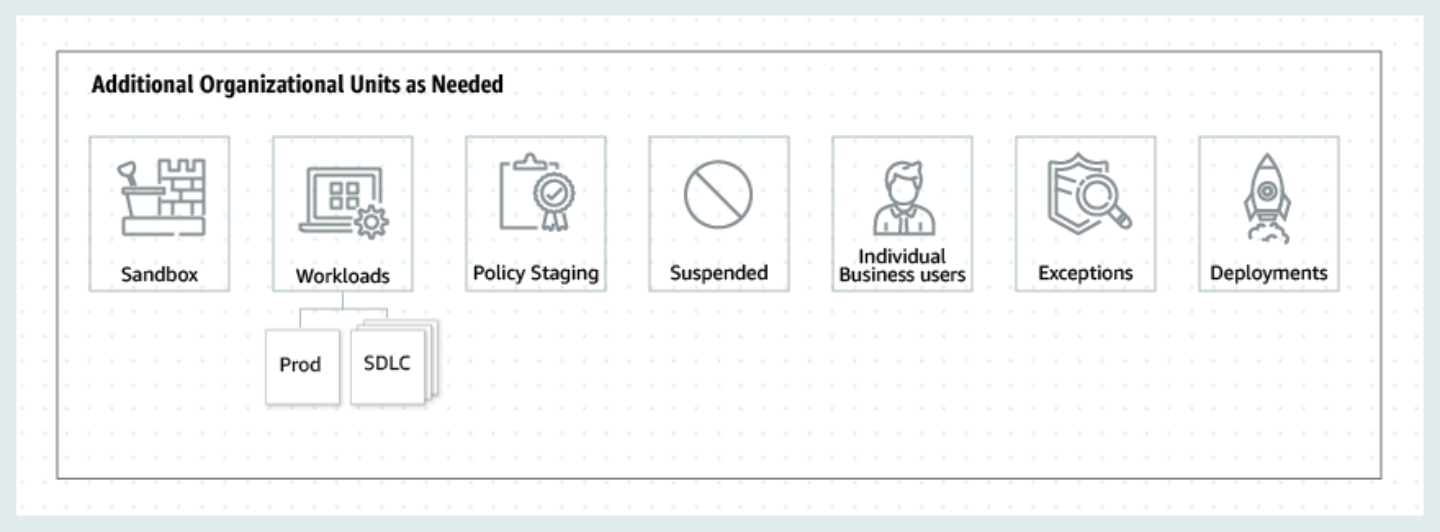
- Sandbox: Contém Contas da AWS conteúdo que desenvolvedores individuais podem usar para experimentar Serviços da AWS. Certifique-se de que essas contas possam ser desvinculadas das redes internas.
- Cargas de trabalho: contém aquelas Contas da AWS que hospedam seus serviços de aplicativos externos. Você deve se estruturar OUs em ambientes SDLC e Prod (semelhantes aos básicos OUs) para isolar e controlar rigorosamente as cargas de trabalho de produção.

Também recomendamos adicionar mais OUs para manutenção e expansão contínua, dependendo de suas necessidades específicas. A seguir estão alguns temas comuns baseados nas práticas de AWS clientes existentes:

- Preparação de políticas: mantém AWS contas nas quais você pode testar as alterações de política propostas antes de aplicá-las amplamente à organização. Comece implementando mudanças no nível da conta na UO pretendida e, lentamente, OUs trabalhe em outras contas e em todo o resto da organização.
- Suspenso: contém Contas da AWS conteúdos que foram fechados e estão aguardando para serem excluídos da organização. Anexe um SCP a essa OU que negue todas as ações. Certifique-se de que as contas estejam marcadas com detalhes para rastreabilidade, caso precisem ser restauradas.
- Usuários corporativos individuais: uma OU de acesso limitado que contém Contas da AWS para usuários corporativos (não desenvolvedores) que talvez precisem criar aplicativos relacionados à produtividade comercial, por exemplo, configurar um bucket do S3 para compartilhar relatórios ou arquivos com um parceiro.
- Exceções: retenções Contas da AWS usadas para casos de uso de negócios que têm requisitos de segurança ou auditoria altamente personalizados, diferentes daqueles definidos na OU de cargas de trabalho. Por exemplo, configurar um aplicativo ou recurso Conta da AWS específico para um novo aplicativo ou recurso confidencial. Use SCPs no nível da conta para atender às necessidades personalizadas. Considere configurar um sistema Detect and React usando a Amazon EventBridge e AWS Config as regras.

- Implantações: Contém Contas da AWS conteúdo destinado à integração contínua e contínua delivery/deployment (CI/CD deployments). You can create this OU if you have a different governance and operational model for CI/CD deployments as compared to accounts in the Workloads OUs (Prod and SDLC). Distribution of CI/CD helps reduce the organizational dependency on a shared CI/CD environment operated by a central team. For each set of SDLC/ Prod Contas da AWS para um aplicativo na OU de cargas de trabalho. Crie uma conta para CI/CD em UO de implantações.
- Transitório: é usado como uma área de retenção temporária para contas e workloads existentes antes de transferi-las para áreas padrão da sua organização. As contas podem fazer parte de uma aquisição, serem anteriormente gerenciadas por terceiros, ou serem contas legadas de uma estrutura organizacional antiga.

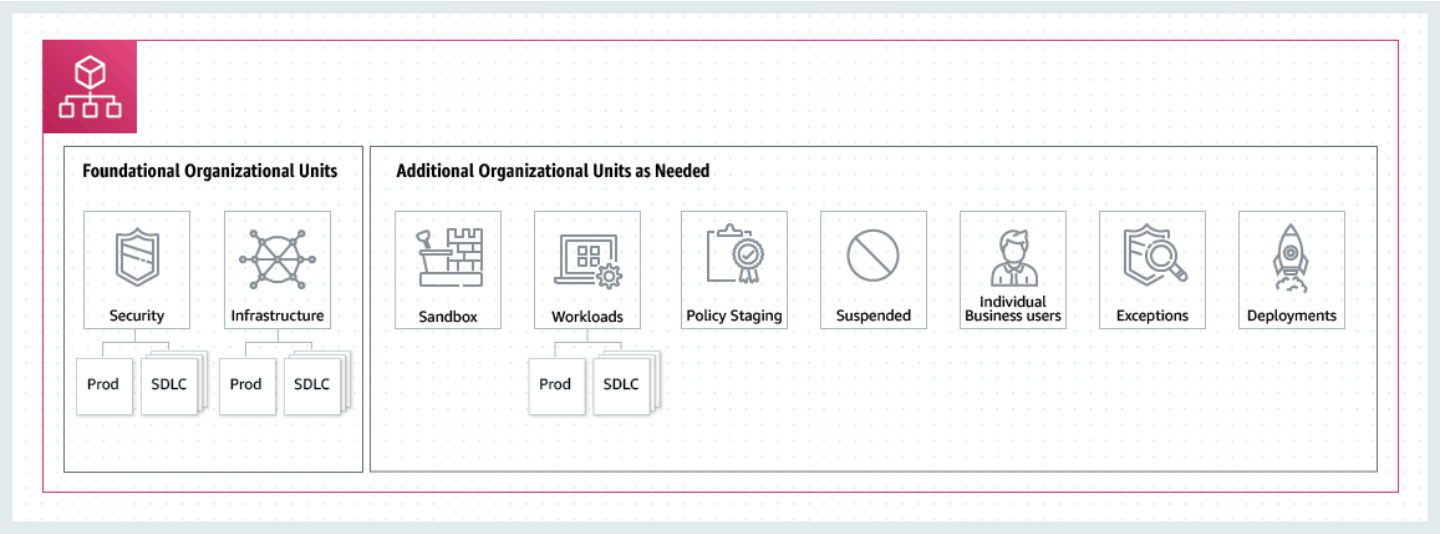
O diagrama a seguir mostra mais informações OUs sobre sandbox, cargas de trabalho, preparação de políticas, suspensos, usuários corporativos individuais, exceções, implantações e contas transitórias:



Conclusão

Uma estratégia de várias contas bem arquitetada pode ajudá-lo a inovar e AWS, ao mesmo tempo, a garantir que você atenda às suas necessidades de segurança e escalabilidade. A estrutura descrita neste tópico representa as AWS melhores práticas que você deve usar como ponto de partida para sua AWS jornada.

O diagrama a seguir mostra os fundamentos OUs e os adicionais OUs recomendados:



Navegando pela hierarquia raiz e da unidade organizacional (OU) com AWS Organizations

Para navegar para diferentes OUs ou até a raiz ao mover contas ou anexar políticas, você pode usar a visualização em “árvore” padrão.

AWS Management Console

Para navegar na organização como uma "árvore"

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, na parte superior da seção Organization (Organização), selecione Hierarchy (Hierarquia) em vez de List (Lista).
3. A árvore aparece inicialmente mostrando a raiz, exibindo somente o primeiro nível de filho OUs e contas. 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. Nessa visualização, você não pode ver OUs 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 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 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.

Visualizando detalhes de uma unidade organizacional (OU) com AWS Organizations

Ao entrar na conta de gerenciamento da organização no AWS Organizations console, você pode ver os detalhes da OUs em 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

Criando uma unidade organizacional (OU) com AWS Organizations

Ao entrar na conta de gerenciamento da sua organização, você pode criar uma OU na raiz da sua organização. OUs pode ser aninhado até cinco níveis de profundidade. Para criar uma UO, conclua as seguintes etapas.

Important

Se essa organização for gerenciada com AWS Control Tower, crie a sua OUs com o AWS Control Tower console ou 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 do AWS 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 OU

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 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 já criou OUs e transferiu contas para elas, o console mostra somente as contas de nível superior OUs e todas as contas que você ainda não transferiu para uma OU.
3. (Opcional) Se você quiser criar uma OU dentro de uma UO existente, navegue até a UO secundária escolhendo o nome (não a caixa de seleção) da UO secundária ou escolhendo a

   próxima na exibição OUs em árvore até ver a que deseja e, em seguida, 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 OU

Os exemplos de código a seguir mostram como usar o `CreateOrganizationalUnit`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new organizational unit in AWS Organizations.
/// </summary>
public class CreateOrganizationalUnit
{
    /// <summary>
    /// Initializes an Organizations client object and then uses it to call
    /// the CreateOrganizationalUnit method. If the call succeeds, it
    /// displays information about the new organizational unit.
```

```
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var orgUnitName = "ProductDevelopmentUnit";

            var request = new CreateOrganizationalUnitRequest
            {
                Name = orgUnitName,
                ParentId = "r-0000",
            };

            var response = await client.CreateOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully created organizational unit:
{orgUnitName}.");
                Console.WriteLine($"Organizational unit {orgUnitName} Details");
                Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
{response.OrganizationalUnit.Id}");
            }
            else
            {
                Console.WriteLine("Could not create new organizational unit.");
            }
        }
    }
```

- Para obter detalhes da API, consulte CreateOrganizationalUnita Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como criar uma unidade organizacional em uma unidade organizacional raiz ou pai

O seguinte exemplo mostra como criar uma UO chamada AccountingOU:

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

A saída inclui um objeto organizationalUnit que contém detalhes sobre a nova UO:

```
{
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
                "Name": "AccountingOU"
        }
}
```

- Para obter detalhes da API, consulte CreateOrganizationalUnitem Referência de AWS CLI Comandos.

Renomeando uma unidade organizacional (OU) com AWS Organizations

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 UO dentro uma raiz em sua organização da , você precisa 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 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 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

Marcar uma unidade organizacional (OU) com AWS Organizations

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 UO dentro uma raiz em sua organização da , você precisa 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 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 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: TagResource e UntagResource

Movendo contas para uma unidade organizacional (OU) ou entre a raiz e OUs com AWS Organizations

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 OU a torna sujeita a todas as políticas vinculadas à OU principal e a qualquer outra OUs na cadeia principal 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 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 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 contas 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 você deve especificar os IDs contêineres de origem e 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

Visualizando detalhes da raiz com AWS Organizations

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

> **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 das unidades organizacionais (OUs) e geralmente se comporta como uma UO. No entanto, como o contêiner no topo da hierarquia, as mudanças na raiz afetam todas as outras UOs e todas as partes 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

Excluindo uma unidade organizacional (OU) com AWS Organizations

Ao entrar na conta de gerenciamento da sua organização, você pode excluir qualquer uma OUs que não seja mais necessária.

Primeiro, você deve remover todas as contas da OU e de qualquer criança e OUs, em seguida, excluir a criança OUs.

> **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 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 Contas da AWSpágina, localize o OUs que você deseja excluir e escolha a caixa de seleção ☑ ao lado do nome de cada OU.
3. Selecione Actions (Ações) e, em Organizational unit (Unidade organizacional), escolha Delete (Excluir).
4. Para confirmar que você deseja excluir o OUs, insira o nome da OU (se você optou por excluir somente uma) ou a palavra 'excluir' (se você escolheu mais de uma) e escolha Excluir.

   AWS Organizations exclui os OUs e os remove da lista.

AWS CLI & AWS SDKs

Como excluir uma UO

Os exemplos de código a seguir mostram como usar o `DeleteOrganizationalUnit`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing AWS Organizations organizational unit.
/// </summary>
public class DeleteOrganizationalUnit
{
    /// <summary>
    /// Initializes the Organizations client object and calls
    /// DeleteOrganizationalUnitAsync to delete the organizational unit
    /// with the selected ID.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var orgUnitId = "ou-0000-00000000";

        var request = new DeleteOrganizationalUnitRequest
        {
            OrganizationalUnitId = orgUnitId,
        };
```

```
            var response = await client.DeleteOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
            }
        }
    }
```

- Para obter detalhes da API, consulte DeleteOrganizationalUnita Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como excluir uma UO

O exemplo a seguir mostra como excluir uma UO. O exemplo pressupõe que você removeu anteriormente todas as contas e outras OUs da OU:

```
aws organizations delete-organizational-unit --organizational-unit-id ou-
examplerootid111-exampleouid111
```

- Para obter detalhes da API, consulte DeleteOrganizationalUnitem Referência de AWS CLI Comandos.

Gerenciando políticas da organização com 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.

Tópicos

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 o máximo de permissões disponíveis para usuários e funções do IAM em uma organização.
- As políticas de controle de recursos (RCPs) oferecem controle central sobre o máximo de permissões disponíveis para recursos em uma organização.

Políticas de gerenciamento

As políticas de gerenciamento ajudam você a configurar Serviços da AWS e gerenciar centralmente seus recursos em toda a organização.

- As políticas declarativas permitem que você declare e aplique centralmente as configurações desejadas para uma determinada empresa em grande escala AWS service (Serviço da AWS) em toda a organização. Uma vez conectada, a configuração é sempre mantida quando o serviço adiciona novos recursos ou APIs.
- As políticas de backup permitem que você gerencie e aplique centralmente os planos de backup aos AWS recursos nas contas de uma organização.
- As políticas de tags permitem padronizar as tags anexadas aos AWS recursos nas contas de uma organização.
- As políticas de aplicativos de bate-papo permitem que você controle o acesso às contas de uma organização a partir de aplicativos de bate-papo, como Slack e Microsoft Teams.
- As políticas de exclusão de serviços de IA permitem que você controle a coleta de dados para serviços de AWS IA em todas as contas de uma organização.
- As políticas do Security Hub permitem que você resolva as lacunas de cobertura de segurança que se alinham aos requisitos de segurança da sua organização e as aplique centralmente em toda a 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 e limites de serviço para AWS Organizations.

Tipo de política	Categoria 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	Autorização	 Não	5	2500 caracteres	 Não
RCP	Autorização	 Não	5	2500 caracteres	 Não
Política declarativa	Gerenciamento	 Sim	10	10 mil caracteres	 Sim
Política de backup	Gerenciamento	 Sim	10	10 mil caracteres	 sim
Política de tag	Gerenciamento	 Sim	10	10 mil caracteres	 Sim
Política de aplicativos de bate-papo	Gerenciamento	 Sim	5	10 mil caracteres	 Sim

Tipo de política	Categoria 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
Política de cancelamento de serviços de IA	Gerenciamento	 Sim	5	2500 caracteres	 Sim
Política do Security Hub	Gerenciamento	 Sim	10	10 mil caracteres	 Sim

Políticas de autorização em AWS Organizations

As políticas de autorização AWS Organizations permitem que você configure e gerencie centralmente o acesso de diretores e recursos em suas contas de membros. A forma como essas políticas afetam as unidades organizacionais (OUs) e as contas às quais você as aplica depende do tipo de política de autorização que você aplica.

Há dois tipos diferentes de políticas de autorização em AWS Organizations: políticas de controle de serviços (SCPs) e políticas de controle de recursos (RCPs).

Tópicos

- Diferenças entre SCPs e RCPs
- Usando SCPs e RCPs
- Políticas de controle de serviços (SCPs)
- Políticas de controle de recursos (RCPs)

Diferenças entre SCPs e RCPs

SCPs são controles centrados no principal. SCPs crie uma barreira de permissões ou defina limites para o máximo de permissões disponíveis para diretores em suas contas de membros. Você pode usar um SCP quando quiser aplicar centralmente controles de acesso consistentes aos diretores da sua organização. Isso pode incluir especificar quais serviços seus usuários e funções do IAM podem acessar, quais recursos eles podem acessar ou as condições sob as quais eles podem fazer solicitações (por exemplo, de regiões ou redes específicas).

RCPs são controles centrados em recursos. RCPs crie uma barreira de permissões ou defina limites para o máximo de permissões disponíveis para recursos em suas contas de membros. Você pode usar um RCP quando quiser aplicar centralmente controles de acesso consistentes em todos os recursos da sua organização. Isso pode restringir o acesso aos seus recursos para que eles só possam ser acessados por identidades que pertencem à sua organização ou especificando as condições sob as quais identidades externas à sua organização podem acessar seus recursos.

Alguns controles podem ser aplicados de forma semelhante por meio de SCPs RCPs e. Por exemplo, talvez você queira impedir que seus usuários enviem objetos não criptografados para o S3, que podem ser gravados como um SCP para impor um controle sobre as ações que seus diretores podem realizar nos buckets do S3. Esse controle também pode ser escrito como um RCP para exigir criptografia sempre que algum principal fizer upload de objetos para seu bucket do S3. A segunda opção pode ser preferida se seu bucket permitir que diretores de fora da sua organização, como fornecedores terceirizados, façam upload de objetos para seu bucket do S3. No entanto, alguns controles só podem ser implementados em um RCP, e alguns controles só podem ser implementados em um SCP. Para obter mais informações, consulte Casos de uso geral para SCPs e RCPs.

Usando SCPs e RCPs

SCPs e RCPs são controles independentes. Você pode optar por habilitar somente SCPs ou RCPs usar os dois tipos de política juntos. Usando ambos SCPs RCPs, você pode criar um perímetro de dados em torno de suas identidades e seus recursos.

SCPs forneça a capacidade de controlar quais recursos suas identidades podem acessar. Por exemplo, talvez você queira permitir que suas identidades acessem recursos em sua AWS organização. No entanto, talvez você queira impedir que suas identidades acessem recursos fora da sua organização. Você pode aplicar esse controle usando SCPs.

RCPs forneça a capacidade de controlar quais identidades podem acessar seus recursos. Por exemplo, talvez você queira permitir que identidades em sua organização possam acessar recursos em sua organização. No entanto, talvez você queira impedir que identidades externas à sua organização acessem seus recursos. Você pode aplicar esse controle usando RCPs. RCPs forneça a capacidade de impactar as permissões efetivas para diretores externos à sua organização que estão acessando seus recursos. SCPs só pode afetar as permissões efetivas para diretores em sua AWS organização.

Casos de uso geral para SCPs e RCPs

A tabela a seguir detalha os casos de uso gerais para o uso de um SCP e RCPs

		Impactos			
Caso de uso	Tipo de política	Suas identidades	Identidades externas	Seus recursos	Recursos externos (alvo da solicitação)
Restrinja quais serviços ou ações suas identidades podem usar	SCP	X		X	X
Restrinja quais recursos suas identidades podem acessar	SCP	X		X	X
Imponha requisitos sobre como suas identidad	SCP	X		X	X

		Impactos		
es podem acessar recursos				
Restrinja quais identidades podem acessar seus recursos	RCP	X	X	X
Proteja recursos confidenciais em sua organização	RCP	X	X	X
Imponha requisitos sobre como seus recursos podem ser acessados	RCP	X	X	X

Políticas de controle de serviços (SCPs)

As políticas de controle de serviço (SCPs) são um tipo de política organizacional que você pode usar para gerenciar permissões em sua organização. SCPs ofereça controle central sobre o máximo de permissões disponíveis para os usuários do IAM e as funções do IAM em sua organização. SCPs ajudam você a garantir que suas contas permaneçam dentro das diretrizes de controle de acesso da sua organização. SCPsestão disponíveis somente em uma organização que tenha todos os recursos habilitados. SCPs não estão disponíveis se sua organização tiver ativado somente os recursos de cobrança consolidada. Para obter instruções sobre como habilitar SCPs, consulteHabilitação de um tipo de política.

SCPs não conceda permissões aos usuários do IAM e às funções do IAM em sua organização. Nenhuma permissão é concedida por uma SCP. Uma SCP define uma barreira de proteção de permissões — ou define limites — nas ações que os usuários e perfis do IAM em sua organização podem realizar. Para conceder permissões, o administrador deve vincular políticas para controlar o acesso, como políticas baseadas em identidade que são anexadas a usuários e perfis do IAM, e políticas baseadas em recursos que estão vinculadas aos recursos em suas contas. Para obter mais informações, consulte Políticas baseadas em identidade e em recurso no Guia do usuário do IAM.

As permissões efetivas são a interseção lógica entre o que é permitido pelo SCP e pelas políticas de controle de recursos (RCPs) e o que é permitido pelas políticas baseadas em identidade e recursos.

> ⚠ SCPs não afetam usuários ou funções na conta de gerenciamento
>
> SCPs não afetam usuários ou funções na conta de gerenciamento. Elas afetam apenas as contas-membro de sua organização. Isso também significa que SCPs se aplicam às contas de membros designadas como administradores delegados.

Tópicos nesta página

Testando os efeitos do SCPs

AWS recomenda fortemente que você não se vincule 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 de SCPs

Todos os caracteres em sua conta de SCP contam em relação ao seu tamanho máximo. Os exemplos deste guia mostram o SCPs formato com espaço em branco extra para melhorar sua 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-se SCPs a diferentes níveis da organização

Para obter uma explicação detalhada de como SCPs funciona, consulteAvaliação do SCP.

Efeitos de SCP sobre permissões

SCPs são semelhantes às políticas de AWS Identity and Access Management permissão e usam quase a mesma sintaxe. No entanto, uma SCP nunca concede permissões. Em vez disso, SCPs são controles de acesso que especificam o máximo de permissões disponíveis 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.

- SCPs afetam somente usuários e funções do IAM que são gerenciados por contas que fazem parte da organização. 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 somente as contas dos membros na organização. Eles não têm efeito sobre os usuários ou funções na conta de gerenciamento. Isso também significa que SCPs se aplicam às contas de membros designadas como administradores delegados. Para obter mais informações, consulte Práticas recomendadas para a 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 o aplicável SCPs permita todos os serviços e todas as ações.
- Se um usuário ou função tiver uma política de permissão do IAM que concede acesso a uma ação que também é permitida pelo aplicável SCPs, o usuário ou função poderá realizar essa ação.
- Se um usuário ou função tiver uma política de permissão do IAM que concede acesso a uma ação que não é permitida ou explicitamente negada pelo aplicável SCPs, o usuário ou a função não poderá realizar essa ação.
- SCPs afetam todos os usuários e funções nas contas anexadas, incluindo o usuário root. As únicas exceções são aquelas descritas em Tarefas e entidades não restritas por SCPs.
- SCPs não afetam nenhuma função vinculada ao serviço. As funções vinculadas ao serviço permitem que outras pessoas Serviços da AWS se integrem AWS Organizations e não possam ser restringidas por elas. SCPs
- Quando você desabilita o tipo de política SCP em uma raiz, todas SCPs são automaticamente separadas de todas as AWS Organizations entidades nessa raiz. AWS Organizations as entidades incluem unidades organizacionais, organizações e contas. Se você reativar SCPs em uma raiz, essa raiz será revertida somente para a `FullAWSAccess` política padrão anexada automaticamente a todas as entidades na raiz. Todos os anexos de AWS Organizations entidades anteriores SCPs à desativação são perdidos e não podem ser SCPs recuperados 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.

Usando dados de acesso para melhorar 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 utilizadas, a fim de refiná-las SCPs para melhor aderir ao princípio do privilégio mínimo.

Por exemplo, você pode ter uma SCP de lista de negações que impede o acesso a três Serviços da AWS. Todos os serviços que não são listados na declaração `Deny` da SCP são permitidos. Os últimos dados acessados do serviço no IAM informam quais Serviços da AWS 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 restritas 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
- Forneça funcionalidade de assinante confiável para conteúdo CloudFront privado
- Configure o DNS reverso para um servidor de e-mail Amazon Lightsail e uma instância EC2 da Amazon como 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

Avaliação do SCP

> **Note**
>
> As informações nesta seção não se aplicam aos tipos de políticas de gerenciamento, incluindo políticas de backup, políticas de tags, políticas de aplicativos de bate-papo ou políticas de exclusão de serviços de IA. Para obter mais informações, consulte Entendendo a herança da política de gerenciamento.

Como você pode anexar várias políticas de controle de serviço (SCPs) em diferentes níveis AWS Organizations, entender como SCPs são avaliadas pode ajudá-lo SCPs a escrever o resultado certo.

Tópicos

Como SCPs trabalhar 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 ativa SCPs, AWS Organizations anexa uma política SCP AWS gerenciada chamada Full, AWSAccess que permite todos os serviços e ações. Se essa política for removida e não substituída em nenhum nível da organização, todas as contas OUs e contas desse nível serão impedidas de realizar qualquer ação.

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 do SCP segue um deny-by-default modelo, o que significa que todas as permissões não permitidas explicitamente no SCPs são negadas. Se uma instrução de permissão não estiver presente SCPs em nenhum dos níveis, como Raiz, OU 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`.

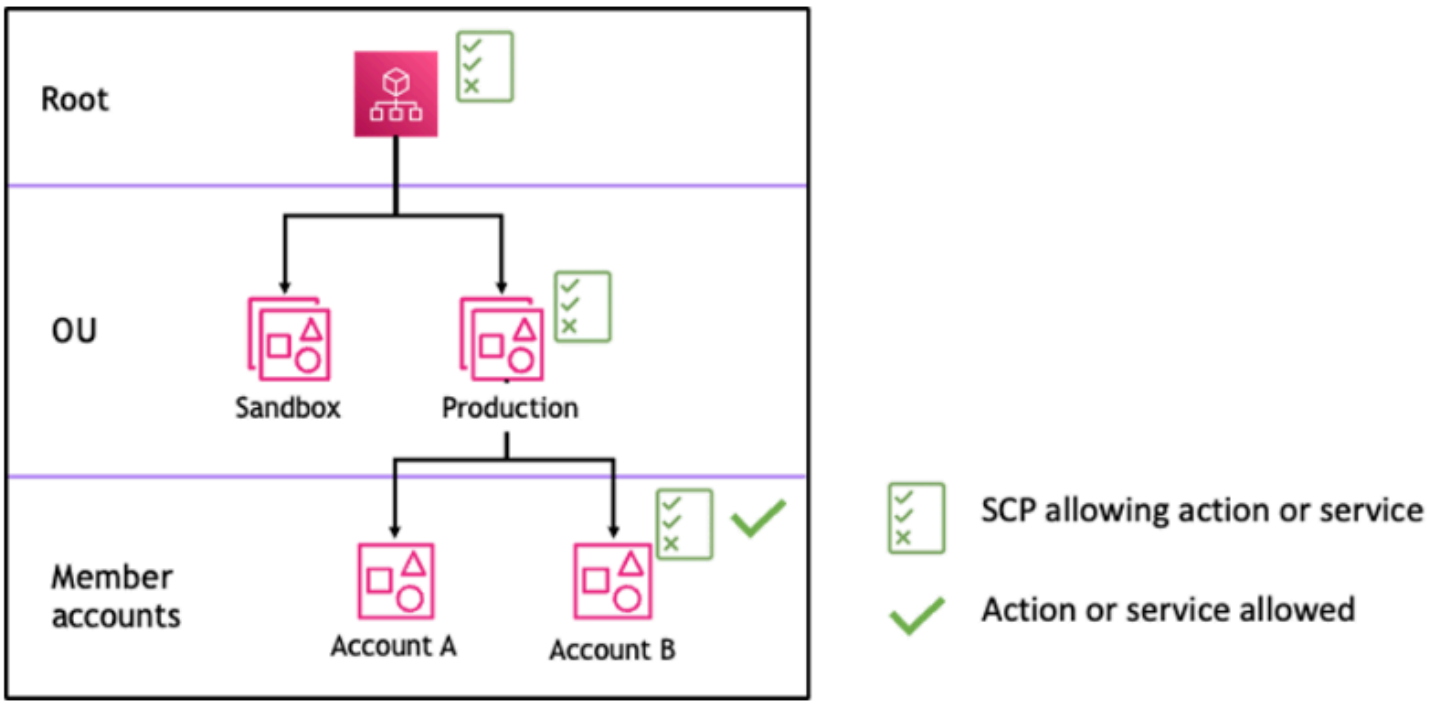


Figura 1: exemplo de estrutura organizacional com uma declaração *`Allow`* anexada na Raiz, UO de Produção e Conta B

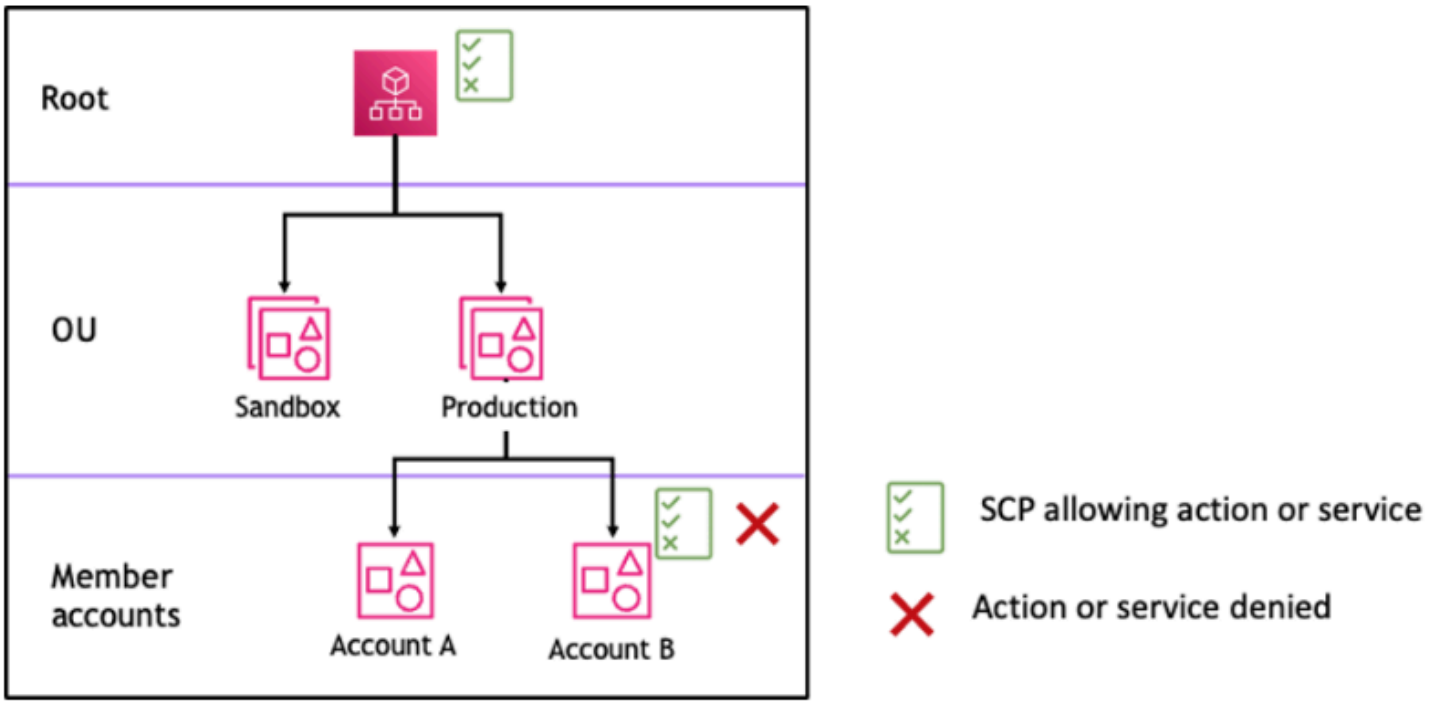


Figura 2: exemplo de estrutura organizacional com uma declaração *Allow* faltando na UO de Produção e seu impacto na Conta B

Como SCPs trabalhar com Deny

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 contas OUs e membros abaixo dela.

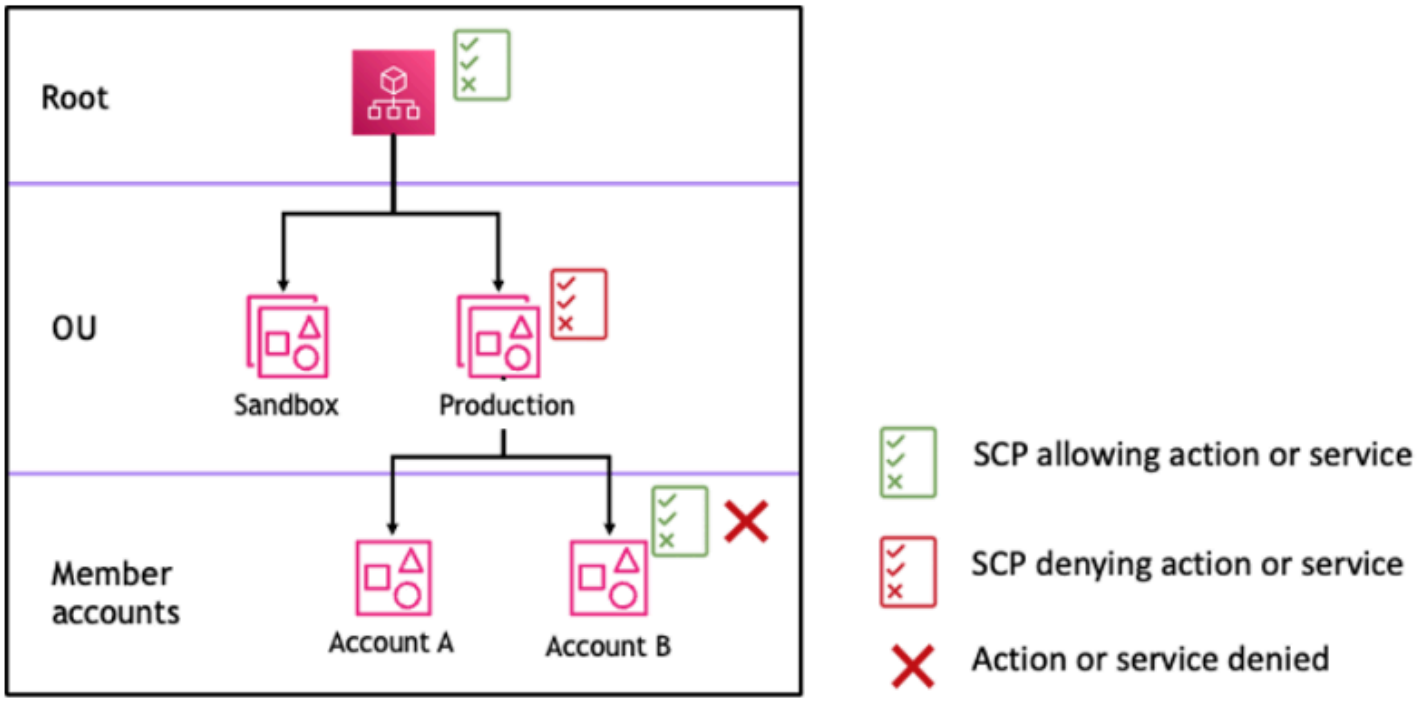


Figura 3: exemplo de estrutura organizacional com uma declaração *Deny* anexada na UO de Produção e seu impacto na Conta B

Estratégia para usar SCPs

Ao escrever, SCPs você pode usar uma combinação de `Allow` `Deny` declarações para permitir ações e serviços pretendidos em sua organização. `Deny`as declarações são uma forma poderosa de implementar restrições que devem ser verdadeiras para uma parte mais ampla de sua organização ou OUs porque, quando aplicadas na raiz ou no nível da UO, elas afetam todas as contas sob ela.

Por exemplo, você pode implementar uma política usando instruções de `Deny` para 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 do último acesso do serviço no IAM para atualizar seus SCPs dados e restringir o acesso somente ao Serviços da AWS que você precisa. Para obter mais informações, consulte Visualizar os dados de serviço da organização acessados mais recentemente da organização no Guia do usuário do IAM.

AWS Organizations anexa um SCP AWS gerenciado chamado Full AWSAccess a cada raiz, UO e conta quando ele é criado. Esta política permite todos os serviços e ações. Você pode AWSAccess substituir Full por uma política que permita somente um conjunto de serviços para que novos não Serviços da AWS sejam permitidos, a menos que sejam explicitamente permitidos pela atualização 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.

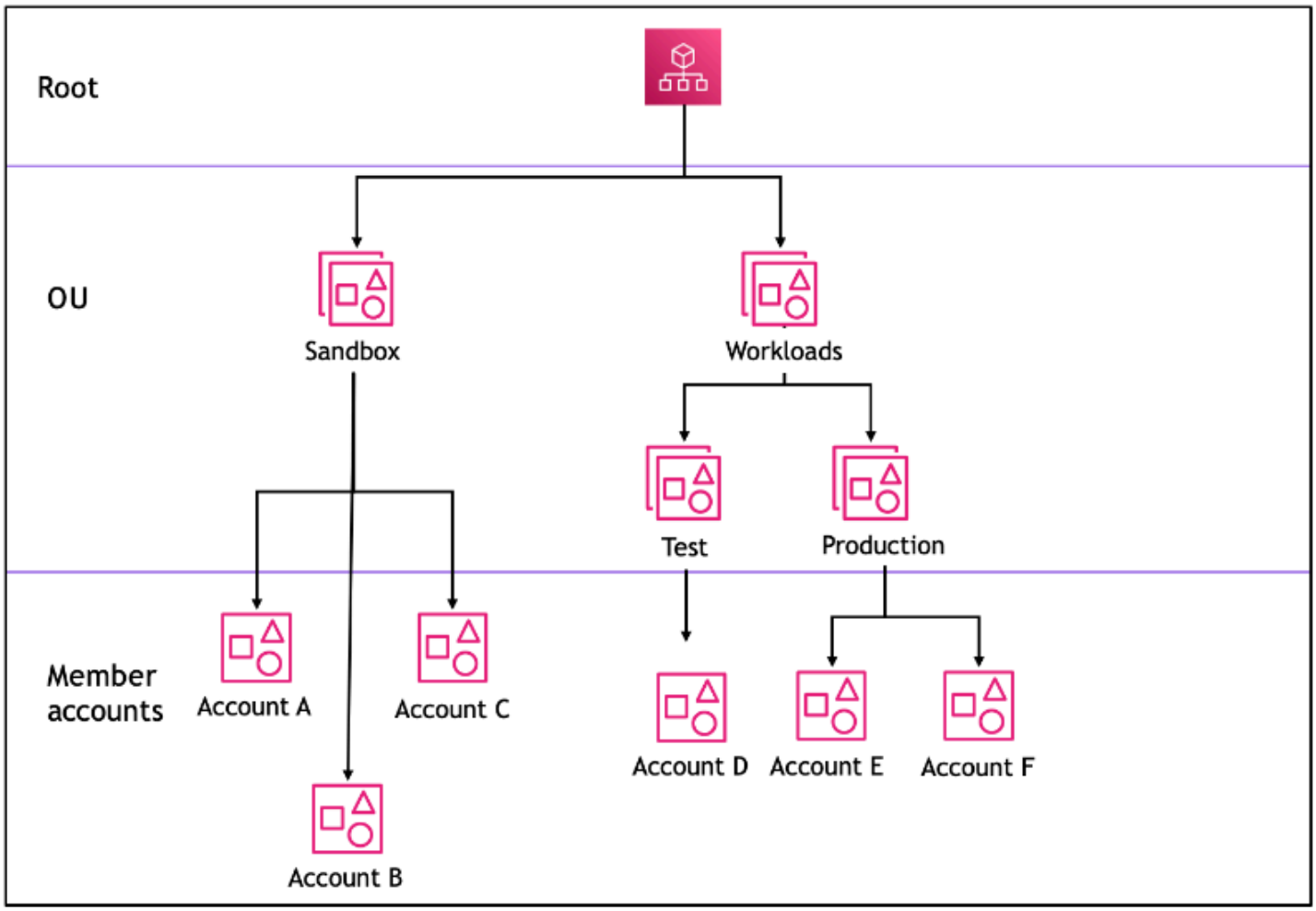
```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

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 separar a AWSAccess política completa e, em vez disso, anexar esta.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Deny",
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

Agora, considere o exemplo de estrutura organizacional a seguir para entender como você pode aplicar várias 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	AWS Acesso total	AWS Acesso total + negar acesso ao S3	AWS Acesso total + negar EC2 acesso	Sem S3, sem acesso EC2	Sem acesso ao S3
2	AWS Acesso total	Permitir EC2 acesso	Permitir EC2 acesso	Permitir EC2 acesso	Permitir EC2 acesso
3	Negar acesso ao S3	Permitir acesso ao S3	AWS Acesso total	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	AWS Acesso total	AWS Acesso total	AWS Acesso total + negar EC2 acesso	Sem EC2 acesso	AWS Acesso total
2	AWS Acesso total	AWS Acesso total	Permitir EC2 acesso	Permitir EC2 acesso	AWS Acesso total
3	Negar acesso ao S3	AWS Acesso total	Permitir acesso ao S3	Sem acesso ao serviço	Sem acesso ao S3

Sintaxe de SCP

As políticas de controle de serviço (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 o SCPs formato com espaço em branco extra para melhorar sua 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, consultePolíticas de controle de serviços (SCPs).

Resumo de elementos

A tabela a seguir resume os elementos de política que você pode usar em SCPs. Alguns elementos da política estão disponíveis somente nas ações SCPs de negação. A coluna Efeitos suportados lista o tipo de efeito que você pode usar com cada elemento de política em SCPs.

Elemento	Finalidade	Efeitos com suporte
Ação	Especifica o AWS serviço e as ações que o SCP permite ou nega.	`Allow`, `Deny`

Elemento	Finalidade	Efeitos com suporte
Efeito	Define se a instrução da SCP permite ou nega o acesso principal a usuários e funções do IAM em uma conta.	`Allow`, `Deny`
Instrução	Serve como o contêiner para elementos de políticas. Você pode incluir várias declarações em SCPs.	`Allow`, `Deny`
ID da instrução (Sid)	(Opcional) Fornece um nome amigável para a instrução.	`Allow`, `Deny`

Elemento	Finalidade	Efeitos com suporte
Versão	Especifica as regras da sintaxe da linguagem a serem usadas para processar a política.	`Allow`, `Deny`
Condição	Especifica as condições em que a instrução está em vigor.	`Deny`
NotAction	Especifica AWS serviços e ações que estão isentos do SCP. Usado em vez do elemento `Action`.	`Deny`

Elemento	Finalidade	Efeitos com suporte
Recurso	Especifica os AWS recursos aos quais o SCP se aplica.	`Deny`

As seções a seguir fornecem mais informações e exemplos de como os elementos da política são usados em SCPs.

Tópicos

- Elementos Action e NotAction
- Elemento Condition
- Elemento Effect
- Elemento Resource
- Elemento Statement
- Elemento ID da instrução (Sid)
- Elemento Version
- Elementos sem suporte

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

notações não diferenciam maiúsculas de minúsculas. Geralmente, todos eles são inseridos com cada palavra começando com uma letra maiúscula e o resto com minúscula. 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 `"ec2:Describe*"` corresponde somente às EC2 ações que começam com “Descrever”.
- 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"` ambos `"servicename:some*action"` são inválidos em SCPs.

Para obter uma lista de todos os serviços e as ações que eles suportam nas AWS Organizations SCPs políticas de permissão do IAM, 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 exemplo a seguir mostra um SCP com uma declaração que permite aos administradores da conta delegar permissões de descrição, início, interrupção e encerramento para EC2 instâncias 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 o padrão ainda `"Allow *"` SCPs esteja anexado a tudo OUs e à raiz. Esse exemplo de política impede que os administradores de contas em contas anexadas deleguem quaisquer permissões para os serviços IAM EC2, Amazon 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 **`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.

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, SCPs atue como filtros que especificam as permissões máximas para as contas em uma organização, unidade organizacional (OU) ou conta. 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 declaração em que o `Effect` elemento tem um valor de`Deny`, você também pode restringir o acesso a recursos específicos ou definir condições para quando SCPs estão 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 declaração em um SCP define uma barreira para evitar que contas afetadas (onde o SCP está vinculado à própria conta ou à raiz da organização ou UO que contém a conta) iniciem instâncias da Amazon EC2 se a EC2 instância da Amazon não estiver configurada como. `t2.micro` Mesmo que uma política do IAM que permite essa ação seja anexada à conta, a proteção criada pela SCP impedirá isso.

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 um recurso individual Amazon Resource Names (ARNs).

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.

Nas declarações em que o `Effect` elemento tem um valor de`Deny`, você pode especificar individual ARNs, conforme mostrado no exemplo a seguir.

```
{
```

```
  "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 **`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 declaração permite todas as ações, enquanto a segunda nega qualquer EC2 ação. O resultado é que um administrador na conta pode delegar qualquer permissão, exceto aquelas da 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 `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.

Elementos sem suporte

Os seguintes elementos não são compatíveis com SCPs:

- `Principal`
- `NotPrincipal`
- `NotResource`

Exemplos de política de controle de serviço

O exemplo de políticas de controle de serviço (SCPs) exibido neste tópico serve apenas para fins informativos.

> **Antes de usar esses exemplos**
>
> Antes de usar esses exemplos SCPs em sua organização, faça o seguinte:
>
> - Analise e personalize cuidadosamente o SCPs de acordo com seus requisitos exclusivos.
> - Teste minuciosamente o SCPs em seu ambiente com o Serviços da 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. Políticas de controle de serviço baseadas em negação podem, sem querer, limitar ou bloquear seu uso, Serviços da AWS a menos que você adicione as exceções necessárias à política. Para ver um exemplo dessa exceção, veja o primeiro exemplo que isenta os serviços globais das regras que bloqueiam o acesso a serviços indesejados. Regiões da AWS

- Lembre-se de que uma SCP afeta cada usuário e perfil, inclusive o usuário raiz, em cada conta à qual ela é anexada.
- Lembre-se de que um SCP não afeta os perfis vinculados ao serviço. As funções vinculadas ao serviço permitem que outras pessoas Serviços da AWS se integrem AWS Organizations e não possam ser restringidas por elas. SCPs

> **Tip**
>
> Você pode usar os dados do último acesso do serviço no IAM para atualizar seus SCPs dados e restringir o acesso somente ao Serviços da AWS que você precisa. 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 à raiz, a todas as unidades organizacionais (OUs) e a todas as contas. Na verdade, não concede as permissões; nenhuma SCP faz isso. Em vez disso, ele permite que os administradores dessa conta deleguem acesso a essas ações anexando políticas de permissões padrão 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
  - Negar acesso a AWS com base no solicitado Região da AWS
  - Evite que usuários e funções do IAM façam determinadas alterações
  - Impedir que usuários e funções do IAM façam alterações especificadas, com uma exceção para uma função de administrador especificada
  - Exigir MFA para executar uma operação de API
  - Bloquear o acesso ao serviço para o usuário root
  - Impedir que a conta membro saia da organização
- Exemplo SCPs para o Amazon Q Developer em aplicativos de bate-papo

Exemplos gerais

Negar acesso a AWS com base no solicitado Região da AWS

Este SCP nega o acesso a quaisquer operações fora das regiões especificadas. Substitua `eu-central-1` e `eu-west-1` pelo que Regiões da AWS 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 com a qual negar SCP AWS Control Tower, consulte Negar acesso AWS com base na solicitação Região da AWS no Guia de Referência de AWS Control Tower Controles.

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 NotActionelemento permite que você liste 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**
>
> Esse exemplo pode não incluir todas as operações Serviços da AWS ou operações globais mais recentes. 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 ofereça suporte a 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 serviços globais no exemplo a seguir, SCP. Um serviço global como a Amazon CloudFront normalmente requer acesso a AWS KMS um ACM na mesma região, que para um serviço global é a Região Leste dos EUA (Norte da Virgínia) (`us-east-1`).
- Por padrão, AWS STS é um serviço global e deve ser incluído na lista global de exclusão de serviços. No entanto, você pode AWS STS habilitar o uso de endpoints regionais 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 Gerenciando AWS STS em um 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": {
        "ArnNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
      }
    }
  ]
}
```

Exigir MFA para executar uma operação 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 EC2 instância da Amazon.

```
{
  "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 SCPs para o Amazon Q Developer em aplicativos de bate-papo

Exemplos nesta categoria

- Negar todas as operações do IAM
- Negar solicitações put do bucket do S3 de um canal específico do Slack

Negar todas as operações do IAM

O SCP a seguir nega todas as operações do IAM invocadas por todo o Amazon Q Developer nas configurações de aplicativos de bate-papo.

```
{
    "Effect": "Deny",
    "Action": "iam:*",
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:ChatbotSourceArn": "arn:aws:chatbot::*:*"
        }
    }
}
```

Negar solicitações put do bucket do S3 de um canal específico do Slack

A política a seguir nega as solicitações de put do S3 no bucket especificado para todas as solicitações originadas em canal do Slack.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExampleS3Deny",
            "Effect": "Deny",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringLike": {
                      "aws:ChatbotSourceArn": "arn:aws:chatbot::*:chat-configuration/
slack-channel/*"
                }
            }
        }
    ]
}
```

Exemplo SCPs para a Amazon CloudWatch

Exemplos nesta categoria

- Impedir que os usuários desativem CloudWatch ou alterem sua configuração

Impedir que os usuários desativem CloudWatch ou alterem sua configuração

Um CloudWatch operador 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. Esse SCP impede que usuários ou funções em qualquer conta afetada executem qualquer um dos CloudWatch comandos que possam 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 SCPs para AWS Config

Exemplos nesta categoria

- Impedir que os usuários desativem AWS Config ou alterem suas regras

Impedir que os usuários desativem AWS Config ou alterem suas regras

Esse SCP impede que usuários ou funções em qualquer conta afetada executem AWS Config operações que possam desativar AWS Config ou alterar suas regras ou gatilhos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemplo SCPs para Amazon Elastic Compute Cloud (Amazon EC2)

Exemplos nesta categoria

- Exija que EC2 as instâncias da Amazon usem um tipo específico
- Evite o lançamento de EC2 instâncias sem IMDSv2
- Evitar a desativação da criptografia padrão do Amazon EBS
- Evite criar e anexar volumes não gp3

Exija que EC2 as instâncias da Amazon 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"
        }
      }
    }
  ]
}
```

Evite o lançamento de EC2 instâncias sem IMDSv2

A política a seguir impede que todos os usuários iniciem EC2 instâncias sem 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":"2"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"*",
      "Resource":"*",
      "Condition":{
         "NumericLessThan":{
            "ec2:RoleDelivery":"2.0"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:ModifyInstanceMetadataOptions",
      "Resource":"*"
   }
]
```

A política a seguir restringe que todos os usuários iniciem EC2 instâncias sem 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": "2"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
      "ArnNotLike": {
        "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": "*"
```

```
}
```

Evite criar e anexar volumes não gp3

A política a seguir restringe que todos os usuários criem ou anexem quaisquer volumes do Amazon EBS que não sejam do tipo de volume gp3. Para obter mais informações, consulte Tipos de volumes do Amazon EBS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreationAndAttachmentOfNonGP3Volumes",
      "Effect": "Deny",
      "Action": [
        "ec2:AttachVolume",
        "ec2:CreateVolume",
        "ec2:RunInstances"
      ],
      "Resource": "arn:aws:ec2:*:*:volume/*",
      "Condition": {
        "StringNotEquals": {
          "ec2:VolumeType": "gp3"
        }
      }
    }
  ]
}
```

Isso pode ajudar a impor uma configuração de volume padronizada em toda a organização.

> **As modificações do tipo de volume não são evitadas**
>
> Você não pode restringir a ação de modificar um volume gp3 existente para um volume Amazon EBS de outro tipo usando. SCPs Por exemplo, esse SCP não impediria que você modificasse um volume gp3 existente para um volume gp2. Isso ocorre porque a chave de condição `ec2:VolumeType` verifica o tipo de volume antes de ser modificado.

Exemplo SCPs para a Amazon GuardDuty

Exemplos nesta categoria

- Impedir que os usuários desativem GuardDuty ou modifiquem sua configuração

Impedir que os usuários desativem GuardDuty ou modifiquem sua configuração

Esse SCP impede que usuários ou funções em qualquer conta afetada desativem GuardDuty ou alterem sua configuração, diretamente como um comando ou por meio do console. Ele permite efetivamente o acesso somente de leitura às GuardDuty informações e aos recursos.

```
{
    "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 SCPs para AWS Resource Access Manager

Exemplos nesta categoria

- Evitar compartilhamento externo
- Permitir que contas específicas compartilhem apenas tipos de recursos especificados
- Impedir o compartilhamento com organizações ou unidades organizacionais (OUs)
- 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"
                }
            }
        }
    ]
}
```

Impedir o compartilhamento com organizações ou unidades organizacionais (OUs)

O SCP a seguir impede que os usuários criem compartilhamentos de recursos que compartilhem recursos com uma organização ou OUs.

```
{
    "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:StringEquals": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
                        "111111111111"
```

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

Exemplo SCPs de Amazon Application Recovery Controller (ARC)

Exemplos nesta categoria

- Impedir que os usuários atualizem os estados de controle de roteamento do ARC

Impedir que os usuários atualizem os estados de controle de roteamento do ARC

Um operador do ARC de nível mais baixo precisa monitorar painéis e visualizar informações do ARC. No entanto, o operador não deve ser capaz de atualizar os controles de roteamento para transferir o aplicativo de um Região da AWS para outro, como pode ser permitido a um operador sênior. Esta SCP impede que usuários ou perfis em qualquer conta afetada executem operações do ARC que atualizam os controles de roteamento do 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"
                    ]
                }
            }
        }
    ]
```

```
}
```

Exemplo SCPs para o Amazon S3

> **Note**
>
> O Amazon Simple Storage Service (Amazon S3) aplica automaticamente criptografia do lado do servidor (SSE-S3) para cada novo objeto, a menos que você especifique uma opção de criptografia diferente. Para obter mais informações, consulte O Amazon S3 agora criptografa automaticamente todos os objetos novos no Guia do usuário do 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 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 SCPs de 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 não marcados ou execução de EC2 instâncias não marcadas da Amazon e não inclui nenhuma exceção.
> O exemplo de política a seguir não é compatível com AWS CloudFormation a versão escrita, porque esse serviço cria um segredo e o marca como duas etapas separadas. Esse exemplo de política efetivamente AWS CloudFormation impede a criação de um segredo como parte de uma pilha, porque tal ação resultaria, ainda que brevemente, em um segredo que não está marcado como obrigatório.

```
{
  "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/*"
      ],
      "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/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    }
  ]
}
```

Para obter uma lista de todos os serviços e ações que eles suportam nas AWS Organizations SCPs políticas de permissão do IAM, consulte Ações, recursos e chaves de condição 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 atributos (ABAC) como parte de sua estratégia de segurança AWS na nuvem. 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 esteja bloqueado por essa política ainda precisa ter uma política de IAM separada que conceda explicitamente a `Allow` permissão na marcação APIs relevante. 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 SCPs de 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

Esse SCP impede que usuários ou funções em qualquer conta afetada excluam registros de fluxo, grupos ou CloudWatch fluxos de registros do Amazon Elastic Compute Cloud (Amazon EC2).

```
{
  "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

Esse SCP impede que usuários ou funções em qualquer conta afetada alterem a configuração de suas nuvens privadas EC2 virtuais da Amazon (VPCs) para conceder a eles 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": "*"
```

```
    }
  ]
}
```

Solução de problemas de políticas de controle de serviço (SCPs) com AWS Organizations

Use as informações aqui para ajudá-lo a diagnosticar e corrigir erros comuns encontrados nas políticas de controle de serviço (SCPs).

As políticas de controle de serviço (SCPs) em AWS Organizations são semelhantes às políticas do IAM e compartilham uma sintaxe comum. Essa sintaxe começa com as regras da Notação de JavaScript Objetos (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.

AWS Organizations usa um subconjunto da sintaxe e gramática do IAM. Para obter 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 está incorreto porque contém dois objetos no nível superior (indicados em*red*):

```
{
  "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.

> **Note**
>
> Se você salvar a política usando o AWS Management Console, o espaço em branco extra entre os 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.

Políticas de controle de recursos (RCPs)

> **Note**
>
> Políticas de controle de serviços (SCPs) e políticas de controle de recursos (RCPs)
> Use um SCP quando precisar limitar as permissões dos diretores do IAM nas contas dos membros da sua organização.
> Use um RCP quando precisar restringir os diretores do IAM que são externos às contas da sua organização, fazendo solicitações para acessar recursos nas contas dos membros da sua organização.
> Para obter mais informações, consulte Compreendendo SCPs RCPs e.

As políticas de controle de recursos (RCPs) são um tipo de política organizacional que você pode usar para gerenciar permissões em sua organização. RCPs ofereça controle central sobre o máximo de permissões disponíveis para recursos em sua organização. RCPs ajudam você a garantir que os recursos em suas contas permaneçam dentro das diretrizes de controle de acesso da sua organização. RCPs estão disponíveis somente em uma organização que tenha todos os recursos habilitados. RCPs não estão disponíveis se sua organização tiver ativado somente os recursos de

cobrança consolidada. Para obter instruções sobre como habilitar RCPs, consulteHabilitação de um tipo de política.

RCPs sozinhos, não são suficientes para conceder permissões aos recursos em sua organização. Nenhuma permissão é concedida por um RCP. Um RCP define uma barreira de permissões, ou define limites, sobre as ações que as identidades podem realizar em relação aos recursos em suas organizações. O administrador ainda deve anexar políticas baseadas em identidade aos usuários ou funções do IAM, ou políticas baseadas em recursos aos recursos em suas contas para realmente conceder permissões. Para obter mais informações, consulte Políticas baseadas em identidade e em recurso no Guia do usuário do IAM.

As permissões efetivas são a interseção lógica entre o que é permitido pelas RCPs políticas de controle de serviços (SCPs) e o que é permitido pelas políticas baseadas em identidade e recursos.

> **RCPs não afetam os recursos na conta de gerenciamento**
>
> RCPs não afetam os recursos na conta de gerenciamento. Eles afetam apenas os recursos nas contas dos membros da sua organização. Isso também significa que RCPs se aplicam às contas de membros designadas como administradores delegados.

Tópicos nesta página

Lista Serviços da AWS desse suporte RCPs

RCPs aplicam-se às ações para o seguinte Serviços da AWS:

- Amazon S3
- AWS Security Token Service
- AWS Key Management Service
- Amazon SQS
- AWS Secrets Manager
- Amazon Elastic Container Registry
- Amazon sem OpenSearch servidor

Testando os efeitos do RCPs

AWS recomenda fortemente que você não se vincule RCPs à raiz da sua organização sem testar minuciosamente o impacto que a política tem sobre os recursos em suas contas. Você pode começar RCPs anexando contas de teste individuais, movendo-as para um OUs nível inferior na hierarquia e, em seguida, subindo na estrutura organizacional conforme necessário. Uma forma de determinar o impacto é analisar os AWS CloudTrail registros em busca de erros de acesso negado.

Tamanho máximo de RCPs

Todos os caracteres em seu RCP contam em relação ao tamanho máximo. Os exemplos deste guia mostram o RCPs formato com espaço em branco extra para melhorar sua 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 seu RCP. Ele remove automaticamente os espaços em branco.

Vinculando-se RCPs a diferentes níveis da organização

Você pode se vincular RCPs diretamente a contas individuais ou à raiz da organização. OUs Para obter uma explicação detalhada de como RCPs funciona, consulteAvaliação do RCP.

Efeitos do RCP nas permissões

RCPs são um tipo de política AWS Identity and Access Management (IAM). Eles estão mais intimamente relacionados às políticas baseadas em recursos. No entanto, um RCP nunca concede

permissões. Em vez disso, RCPs são controles de acesso que especificam o máximo de permissões disponíveis para recursos em sua organização. Para obter mais informações, consulte Lógica da avaliação de política no Guia do usuário do IAM.

- RCPs aplicam-se aos recursos de um subconjunto de. Serviços da AWS Para obter mais informações, consulte Lista Serviços da AWS desse suporte RCPs.
- RCPs afetam somente os recursos gerenciados por contas que fazem parte da organização que anexou RCPs o. Eles não afetam os recursos de contas externas à 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 um RCP anexado. Esse RCP se aplica ao bucket do S3 na Conta A, mesmo quando acessado por usuários da Conta B. No entanto, esse RCP não se aplica aos recursos na Conta B quando acessados por usuários na Conta A.
- Um RCP restringe as permissões para recursos nas contas dos membros. Qualquer recurso em uma conta tem somente as permissões permitidas por todos os pais acima dela. Se uma permissão for bloqueada em qualquer nível acima da conta, um recurso na conta afetada não terá essa permissão, mesmo que o proprietário do recurso anexe uma política baseada em recursos que permita acesso total a qualquer usuário.
- RCPs aplicam-se aos recursos autorizados como parte de uma solicitação de operação. Esses recursos podem ser encontrados na coluna “Tipo de recurso” da tabela Ação na Referência de Autorização de Serviço. Se um recurso for especificado na coluna “Tipo de recurso”, a RCPs conta principal chamadora será aplicada. Por exemplo, `s3:GetObject` autoriza o recurso do objeto. Sempre que uma `GetObject` solicitação for feita, um RCP aplicável será aplicado para determinar se o principal solicitante pode invocar a operação. `GetObject` Um RCP aplicável é um RCP que foi anexado a uma conta, a uma unidade organizacional (OU) ou à raiz da organização proprietária do recurso que está sendo acessado.
- RCPs afetam somente os recursos nas contas dos membros da organização. Eles não afetam os recursos na conta de gerenciamento. Isso também significa que RCPs se aplicam às contas de membros designadas como administradores delegados. Para obter mais informações, consulte Práticas recomendadas para a conta de gerenciamento.
- Quando um principal faz uma solicitação para acessar um recurso em uma conta que tem um RCP anexado (um recurso com um RCP aplicável), o RCP é incluído na lógica de avaliação da política para determinar se o principal tem acesso permitido ou negado.
- RCPs afetam as permissões efetivas dos diretores que tentam acessar recursos em uma conta membro com um RCP aplicável, independentemente de os diretores pertencerem às mesmas organizações ou não. Isso inclui usuários root. A exceção é quando os principais são funções

vinculadas ao serviço porque RCPs não se aplicam às chamadas feitas por funções vinculadas ao serviço. As funções vinculadas ao serviço permitem Serviços da AWS realizar as ações necessárias em seu nome e não podem ser restringidas por. RCPs

- Os usuários e funções ainda precisam receber permissões com as políticas de permissão apropriadas do IAM, incluindo políticas baseadas em identidade e recursos. Um usuário ou função sem nenhuma política de permissão do IAM não tem acesso, mesmo que um RCP aplicável permita todos os serviços, todas as ações e todos os recursos.

Recursos e entidades não restritos por RCPs

Você não pode usar RCPs para restringir o seguinte:

- Qualquer ação sobre recursos na conta de gerenciamento.
- RCPs não afetam as permissões efetivas de nenhuma função vinculada ao serviço. As funções vinculadas ao serviço são um tipo exclusivo de função do IAM vinculada diretamente a um AWS serviço e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome. As permissões das funções vinculadas ao serviço não podem ser restringidas por. RCPs RCPs também não afetam a capacidade AWS dos serviços de assumir uma função vinculada ao serviço; ou seja, a política de confiança da função vinculada ao serviço também não é afetada pela. RCPs
- RCPs não se inscreva Chaves gerenciadas pela AWS para AWS Key Management Service. Chaves gerenciadas pela AWS são criados, gerenciados e usados em seu nome por um AWS service (Serviço da AWS). Você não pode alterar ou gerenciar suas permissões.
- RCPs não impacte as seguintes permissões:

Serviço	API	Recursos não autorizados pelo RCPs
AWS Key Management Service	`kms:RetireGrant`	RCPs não afetem a `kms:RetireGrant` permissão. Para obter mais informações sobre como a permissão `kms:RetireGrant` é determinada, consulte Aposentadoria e revogação de concessões no

Serviço	API	Recursos não autorizados pelo RCPs
		Guia do AWS KMS desenvolvedor.

Avaliação do RCP

> **Note**
>
> As informações nesta seção não se aplicam aos tipos de políticas de gerenciamento, incluindo políticas de backup, políticas de tags, políticas de aplicativos de bate-papo ou políticas de exclusão de serviços de IA. Para obter mais informações, consulte Entendendo a herança da política de gerenciamento.

Como você pode anexar várias políticas de controle de recursos (RCPs) em diferentes níveis AWS Organizations, entender como RCPs são avaliadas pode ajudá-lo RCPs a escrever o resultado certo.

Estratégia para usar RCPs

A `RCPFullAWSAccess` política é uma política AWS gerenciada. Ele é automaticamente anexado à raiz da organização, a cada UO e a cada conta da sua organização, quando você ativa as políticas de controle de recursos (RCPs). Você não pode desanexar essa política. Esse RCP padrão permite que o acesso de todos os diretores e ações passe pela avaliação do RCP, ou seja, até você começar a criar e anexar RCPs, todas as suas permissões existentes do IAM continuarão funcionando da mesma forma. Essa política AWS gerenciada não concede acesso.

Você pode usar `Deny` declarações para bloquear o acesso aos recursos em sua organização. Para que uma permissão seja negada para um recurso em uma conta específica, qualquer RCP da raiz até cada OU no caminho direto para a conta (incluindo a própria conta de destino) pode negar essa permissão.

`Deny`as declarações são uma forma poderosa de implementar restrições que devem ser verdadeiras para uma parte mais ampla da sua organização. Por exemplo, você pode anexar uma política para ajudar a impedir que identidades externas à sua organização acessem seus recursos no nível raiz, e isso será efetivo para todas as contas da organização. AWS recomenda fortemente que você não se vincule RCPs à raiz da sua organização sem testar minuciosamente o impacto que a política tem

sobre os recursos em suas contas. Para obter mais informações, consulte Testando os efeitos do RCPs.

Na Figura 1, há um RCP anexado à OU de produção que tem uma `Deny` declaração explícita especificada para um determinado serviço. 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 contas OUs e membros abaixo dela.

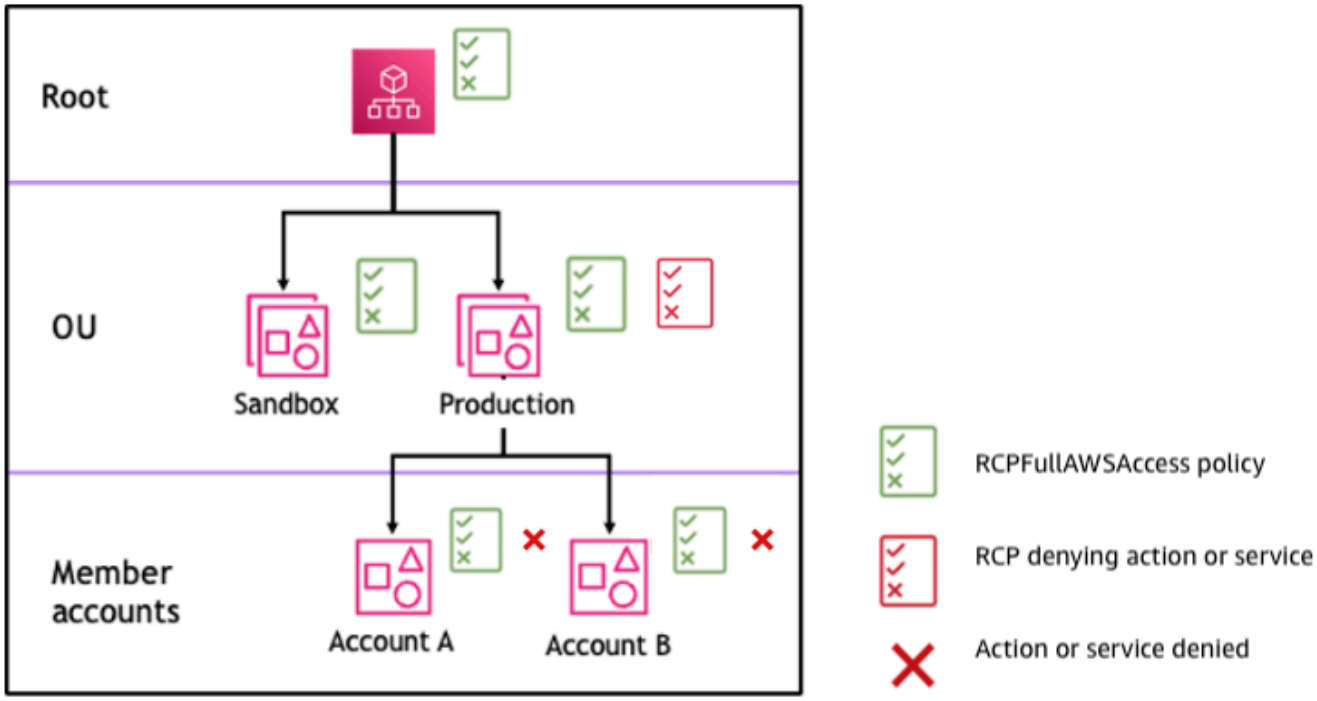


Figura 1: Exemplo de estrutura organizacional com uma *Deny* declaração anexada na OU de produção e seu impacto na Conta A e na Conta B

Sintaxe de RCP

As políticas de controle de recursos (RCPs) usam uma sintaxe semelhante à usada pelas políticas baseadas em recursos. 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.

Um RCP é estruturado de acordo com as regras do JSON. Ela usa os elementos que são descritos neste tópico.

> **Note**
>
> Todos os caracteres em seu RCP contam em relação ao tamanho máximo. Os exemplos deste guia mostram o RCPs formato com espaço em branco extra para melhorar sua

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 RCPs, consulte Políticas de controle de recursos (RCPs).

Resumo de elementos

A tabela a seguir resume os elementos de política que você pode usar em RCPs.

> **Note**
>
> O efeito de só **`Allow`** é suportado pela **`RCPFullAWSAccess`** política
> O efeito de só `Allow` é suportado pela `RCPFullAWSAccess` política. Essa política é anexada automaticamente à raiz da organização, a cada UO e a cada conta da sua organização, quando você ativa as políticas de controle de recursos (RCPs). Você não pode desanexar essa política. Esse RCP padrão permite que o acesso de todos os diretores e ações passe pela avaliação do RCP, ou seja, até você começar a criar e anexar RCPs, todas as suas permissões existentes do IAM continuarão funcionando da mesma forma. Isso não concede acesso.

Elemento	Finalidade	
Versão	Especifica as regras da sintaxe da linguagem a serem usadas para processar a política.	
Instrução	Serve como o contêiner para elementos de políticas. Você pode incluir várias	

Elemento	Finalidade
	declarações em RCPs.
ID da instrução (Sid)	(Opcional) Fornece um nome amigável para a instrução.
Efeito	Define se a instrução RCP nega acesso aos recursos em uma conta.
Principal	Especifica o principal ao qual é permitido ou negado o acesso aos recursos em uma conta.
Ação	Especifica o AWS serviço e as ações que o RCP permite ou nega.
Recurso	Especifica os AWS recursos aos quais o RCP se aplica.
NotResource	Especifica os AWS recursos que estão isentos do RCP. Usado em vez do elemento `Resource`.

Elemento	Finalidade	
Condição	Especifica as condições em que a instrução está em vigor.	

Tópicos

- Elemento Version
- Elemento Statement
- Elemento ID da instrução (Sid)
- Elemento Effect
- Elemento Principal
- Elemento Action
- Elementos Resource e NotResource
- Elemento Condition
- Elementos sem suporte

Elemento **`Version`**

Cada RCP deve incluir um `Version` elemento 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`**

Um RCP consiste em um ou mais `Statement` elementos. 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 declaração que consiste em `Resource` elementos únicos `Effect` `PrincipalAction`,, e.

```
 {
    "Statement": {
        "Effect": "Deny",
        "Principal": "*",
        "Action": "*",
        "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. O exemplo de RCP a seguir mostra um exemplo de `Sid` declaração.

```
{
    "Statement": {
        "Sid": "DenyAllActions",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "*",
        "Resource": "*"
    }
}
```

Para obter mais informações, consulte Elementos de política JSON do IAM: Sid no Guia do usuário do IAM.

Elemento **`Effect`**

Cada instrução deve conter um elemento `Effect`. Usando o valor de `Deny` no `Effect` elemento, você pode restringir o acesso a recursos específicos ou definir condições para quando RCPs estão em vigor. Para RCPs que você crie, o valor deve ser`Deny`. Para obter mais informações, consulte Avaliação do RCP e Elementos da política JSON do IAM: efeito no Guia do usuário do IAM.

Elemento **`Principal`**

Cada declaração deve conter o `Principal` elemento. Você só pode especificar “`*`” no `Principal` elemento de um RCP. Use o `Conditions` elemento para restringir princípios específicos.

Para obter mais informações, consulte Elementos de política JSON do IAM: principal no Guia do usuário do IAM.

Elemento **`Action`**

Cada declaração deve conter o `Action` elemento.

O valor do `Action` elemento é uma string ou lista (uma matriz JSON) de strings que identifica AWS serviços e ações que são permitidos ou negados pela instrução.

Cada string consiste na abreviatura do serviço (como “s3", “sqs” ou “sts”), em letras minúsculas, seguida por dois pontos e, em seguida, por uma ação desse serviço. Geralmente, todos eles são inseridos com cada palavra começando com uma letra maiúscula e o resto com minúscula. Por exemplo: `"s3:ListAllMyBuckets"`.

Você também pode usar caracteres curinga, como asterisco (*) ou ponto de interrogação (?) em um RCP:

- 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 `"sts:Get*"` corresponde somente às AWS STS ações que começam com “Obter”.
- Use o curinga ponto de interrogação (?) para corresponder a um único caractere.

> **Note**
>
> Curingas (*) e pontos de interrogação (?) pode ser usado em qualquer lugar no nome da ação
> Ao contrário de SCPs, você pode usar caracteres curinga, como asterisco (*) ou ponto de interrogação (?) em qualquer lugar no nome da ação.

Para obter uma lista dos serviços que oferecem suporte RCPs, consulteLista Serviços da AWS desse suporte RCPs. Para obter uma lista das ações e dos AWS service (Serviço da AWS) suportes, consulte Ações, recursos e chaves de condição para AWS serviços na Referência de autorização de serviço.

Para obter mais informações, consulte Elementos da política JSON do IAM: ação no Manual do usuário do IAM.

Elementos **`Resource`** e **`NotResource`**

Cada declaração deve conter o `NotResource` elemento `Resource` ou.

Você pode usar caracteres curinga, como asterisco (*) ou ponto de interrogação (?) no elemento de recurso:

- Use um asterisco (*) como curinga para combinar vários recursos que compartilham parte de um nome.
- Use o curinga ponto de interrogação (?) para corresponder a um único caractere.

Para obter mais informações, consulte Elementos de política JSON do IAM: recurso e Elementos da política JSON do IAM: NotResource no Guia do usuário do IAM.

Elemento **`Condition`**

Você pode especificar um `Condition` elemento nas instruções de negação em um RCP.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition:": {
                "BoolIfExists": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

Esse RCP nega acesso às operações e recursos do Amazon S3, a menos que a solicitação ocorra por meio de transporte seguro (a solicitação foi enviada por TLS).

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 com RCPs:

- `NotPrincipal`
- `NotAction`

Exemplos de políticas de controle de recursos

Os exemplos de políticas de controle de recursos (RCPs) exibidos neste tópico são apenas para fins informativos. Para exemplos de perímetro de dados, consulte Exemplos de políticas de perímetro de dados em. GitHub

> **Antes de usar esses exemplos**
>
> Antes de usar esses exemplos RCPs em sua organização, faça o seguinte:
>
> - Analise e personalize cuidadosamente o RCPs de acordo com seus requisitos exclusivos.
> - Teste minuciosamente o RCPs em seu ambiente com os AWS serviços que você usa.
>
> Os exemplos de políticas nesta seção demonstram a implementação e o uso de RCPs. 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 todas as políticas para verificar se elas são adequadas para resolver os requisitos comerciais de seu ambiente. Políticas de controle de recursos baseadas em negação podem, sem querer, limitar ou bloquear o uso de AWS serviços, a menos que você adicione as exceções necessárias à política.

Exemplos gerais

Tópicos

- RCPFullAWSAccess
- Proteção delegada confusa entre serviços
- Restrinja o acesso somente a conexões HTTPS aos seus recursos
- Controles consistentes de políticas de bucket do Amazon S3

RCPFullAWSAccess

A política a seguir é uma política AWS gerenciada e é automaticamente anexada à raiz da organização, a cada UO e a cada conta da sua organização, quando você ativa as políticas de controle de recursos (RCPs). Você não pode desanexar essa política. Esse RCP padrão permite que todos os diretores e ações acessem seus recursos, ou seja, até você começar a criar e anexar RCPs, todas as suas permissões existentes do IAM continuarão funcionando da mesma forma. Você não precisa testar o efeito dessa política, pois ela permitirá que o comportamento de autorização existente continue para seus recursos.

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

Proteção delegada confusa entre serviços

Alguns Serviços da AWS (serviços de chamada) usam seu AWS service (Serviço da AWS) principal para acessar AWS recursos de outros Serviços da AWS (chamados serviços). Quando um ator que não pretendia ter acesso a um AWS recurso tenta usar a confiança de um AWS service (Serviço da AWS) diretor para interagir com recursos aos quais ele não deveria ter acesso, isso é conhecido como o problema do substituto confuso entre serviços. Para obter mais informações, consulte O problema confuso do deputado no Guia do usuário do IAM

A política a seguir exige que AWS service (Serviço da AWS) os diretores que acessam seus recursos só o façam em nome das solicitações da sua organização. Essa política aplica o controle somente às solicitações `aws:SourceAccount` presentes, para que as integrações de serviços que não exijam o uso de `aws:SourceAccount` não sejam afetadas. Se o `aws:SourceAccount` estiver presente no contexto da solicitação, a `Null` condição será avaliada como`true`, fazendo com que a `aws:SourceOrgID` chave seja aplicada.

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

```
    "Statement": [
        {
            "Sid": "EnforceConfusedDeputyProtection",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:*",
                "sqs:*",
                "kms:*",
                "secretsmanager:*",
                "sts:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceOrgID": "my-org-id",
                    "aws:SourceAccount": [
                        "third-party-account-a",
                        "third-party-account-b"
                    ]
                },
                "Bool": {
                    "aws:PrincipalIsAWSService": "true"
                },
                 "Null": {
                    "aws:SourceArn": "false"
                }
            }
        }
    ]
}
```

Restrinja o acesso somente a conexões HTTPS aos seus recursos

A política a seguir exige que o acesso aos seus recursos ocorra somente em conexões criptografadas via HTTPS (TLS). Isso pode ajudar a evitar que possíveis invasores manipulem o tráfego da rede.

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

```
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "sts:*",
                "s3:*",
                "sqs:*",
                "secretsmanager:*",
                "kms:*"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

Controles consistentes de políticas de bucket do Amazon S3

O RCP a seguir contém várias declarações para impor controles de acesso consistentes nos buckets do Amazon S3 em sua organização.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceS3TlsVersion",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "s3:TlsVersion": [
                        "1.2"
                    ]
                }
            }
        },
        {
            "Sid": "EnforceKMSEncryption",
```

```
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
                }
            }
        }
    ]
}
```

- O ID da declaração `EnforceS3TlsVersion` — Exigir uma versão mínima de TLS 1.2 para acessar os buckets do S3.
- O ID da declaração `EnforceKMSEncryption` — Exija que os objetos sejam criptografados no lado do servidor com chaves KMS.

Políticas de gestão em AWS Organizations

As políticas de gerenciamento permitem que você configure e Serviços da AWS gerencie centralmente seus recursos. A forma como essas políticas afetam OUs as contas que as herdam depende do tipo de política de gerenciamento à qual você se aplica. AWS Organizations Revise os tópicos desta seção para compreender termos e conceitos relevantes sobre políticas de gerenciamento.

Tópicos

- Pré-requisitos e permissões para políticas de gerenciamento para AWS Organizations
- Entendendo a herança da política de gerenciamento
- Como visualizar políticas de gerenciamento em vigor
- Políticas declarativas
- Políticas de backup
- Políticas de tag
- Políticas de aplicativos de bate-papo
- Políticas de recusa de serviços de IA
- Políticas do Security Hub

Pré-requisitos e permissões para políticas de gerenciamento para AWS Organizations

Esta página descreve os pré-requisitos e as permissões necessárias para políticas de gerenciamento no AWS Organizations.

Tópicos

Pré-requisitos para as políticas de gerenciamento

Para usar políticas de gerenciamento em uma organização, é necessário o seguinte:

- A organização deve ter todos os recursos habilitados.
- É necessário estar conectado à conta de gerenciamento da organização ou ser um administrador delegado.
- Seu usuário ou função AWS Identity and Access Management (IAM) deve ter as permissões listadas na seção a seguir.

Permissões para políticas de gerenciamento

O exemplo de política do IAM a seguir fornece permissões para usar todos os aspectos das políticas de gerenciamento em uma organização.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationPolicies",
            "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 Guia do usuário do IAM.

Entendendo a herança da política de gerenciamento

> **Important**
>
> As informações nesta seção não se aplicam às políticas de autorização: políticas de controle de serviços (SCPs) e políticas de controle de recursos (RCPs). Para obter mais informações sobre como RCPs trabalhar SCPs e como trabalhar em uma AWS Organizations hierarquia, consulte Avaliação do SCP e. Avaliação do RCP

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 OUs as contas da 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.

Os tópicos a seguir explicam como as políticas pai e as políticas filho são processadas na política em vigor 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 OUs, às 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. Para obter mais informações, consulte Como visualizar políticas de gerenciamento em vigor.

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

A forma exata como as políticas afetam OUs as contas que as herdam depende do tipo de política de gerenciamento que você escolher. Os tipos de políticas de gerenciamento incluem:

- Políticas declarativas
- Políticas de backup

- Políticas de tag
- Políticas de aplicativos de bate-papo
- Políticas de recusa de serviços de IA

A sintaxe dos tipos de política de gerenciamento inclui Operadores de herança, que permite especificar com grande granularidade quais elementos das políticas principais são aplicados e quais elementos podem ser substituídos ou modificados quando herdados por filhos e contas. OUs

A política efetiva é o conjunto de regras que são herdadas da raiz da organização e OUs junto com aquelas diretamente vinculadas 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 Como visualizar políticas de gerenciamento em vigor.

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.

Ao usar o editor visual no AWS Organizations console, você pode usar somente o `@@assign` operador. 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.

Para obter informações sobre como a herança de políticas funciona em uma organização, consulte. Exemplos de herança

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.

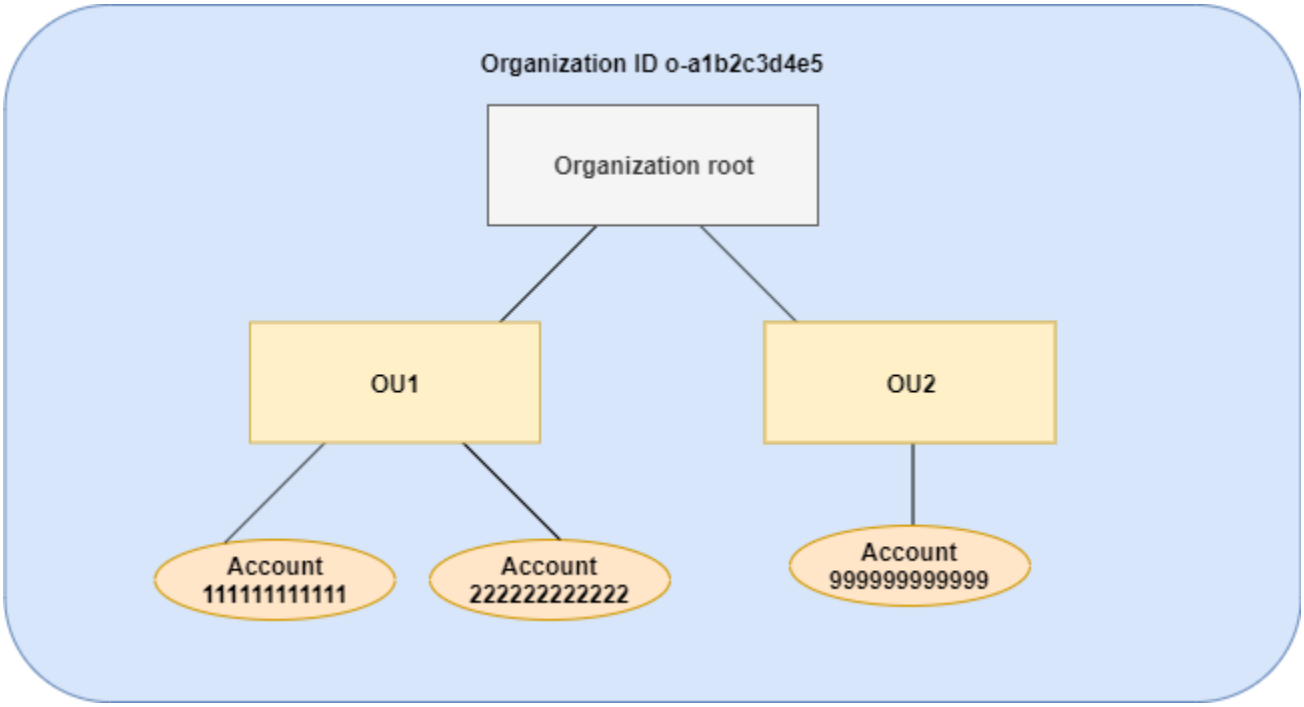
- `"@@operators_allowed_for_child_policies": ["@@all"]` — Crianças OUs e contas podem usar qualquer operador nas políticas. Por padrão, todos os operadores são permitidos em políticas filho.
- `"@@operators_allowed_for_child_policies": ["@@assign", "@@append", "@@remove"]` — A criança OUs e as contas podem usar somente os operadores especificados nas políticas secundárias. Você pode especificar um ou mais operadores de definição de valor neste operador de controle filho.
- `"@@operators_allowed_for_child_policies": ["@@none"]` — Crianças OUs e contas não podem usar operadores nas 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"
                ]
            }
        }
    }
}
```

Suponha que você queira que os usuários usem OU1 um valor de tag diferente para uma chave e imponha a política de tags para 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 `@@assign` operador e criar uma política de tag como a seguinte para anexar OU1.

Política B — política de OU1 tags

```
{
    "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.

Conforme mostrado no diagrama, OU1 inclui duas contas: 111111111111 e 2222222222.

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"
                ]
            }
        }
    }
}
```

Neste exemplo, anexe a política C OU2 a. 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 OU2 tags para anexar valores

```
{
```

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

Anexar a política C à OU2 tem os seguintes efeitos quando a política A e a política C se fundem 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.

Conforme mostrado no diagrama, OU2 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 tenha executado todos os exemplos anteriores, as políticas B, C e C são políticas secundárias de A. A política B está apenas vinculada OU1, 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 você adicionar mais contas posteriormente OU2, suas políticas de tags 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"
```

```
            ]
        }
    }
}
```

Como visualizar políticas de gerenciamento em vigor

Determine a política de gerenciamento em vigor para uma conta em sua organização.

O que é uma política de gerenciamento em vigor?

A política efetiva especifica as regras finais que se aplicam a um Conta da AWS tipo de política de gerenciamento. É a agregação de uma política de gerenciamento que a conta herda, além de quaisquer políticas para esse tipo de política de gerenciamento que estejam diretamente anexadas à conta. Quando você anexa uma política de gerenciamento à raiz da organização, ela se aplica a todas as contas da organização. Quando você anexa uma política de gerenciamento a uma unidade organizacional (OU), ela se aplica a todas as contas OUs que pertencem à OU. Quando você anexa uma política de gerenciamento diretamente a uma conta, ela se aplica somente a essa conta Conta da AWS.

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.

Exemplo de políticas de backup

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.

Exemplo da política de tags

A política de tag vinculada 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.

Exemplo de política de aplicativos de bate-papo

O Amazon Q Developer em aplicativos de bate-papo reavaliará qualquer configuração de Amazon Q Developer criado anteriormente em relação às políticas efetivas de aplicativos de bate-papo e negará quaisquer ações permitidas anteriormente se elas forem consistentes com as configurações permitidas e as barreiras de proteção na política efetiva. A política em vigor para uma conta-membro define as configurações e barreiras de proteção permitidas. Por exemplo, se uma política de aplicativos de bate-papo com negação de acesso a canais públicos do Slack for aplicada a uma conta de membro, o Amazon Q Developer existente nas configurações de aplicativos de bate-papo para canais públicos do Slack na conta do membro será desativado. O Amazon Q Developer em aplicativos de bate-papo não entregará notificações e os membros do canal não poderão executar nenhuma tarefa no canal bloqueado. O Amazon Q Developer no console de aplicativos de bate-papo marcará os canais afetados como desativados com uma mensagem de erro apropriada ao lado.

Exemplo de recusa dos serviços de IA

A política de exclusão de serviços de IA anexada à raiz da organização pode especificar que todas as contas da organização optem por não usar o conteúdo por todos os serviços de aprendizado AWS de máquina. 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 da organização são excluídas de todas Serviços da AWS, com exceção de uma conta que opta pelo Amazon Rekognition.

Como ver a política de gerenciamento em vigor

Você pode visualizar a política efetiva de um tipo de política de gerenciamento para uma conta na AWS Management Console AWS API ou AWS Command Line Interface.

> **Permissões mínimas**
>
> Para ver a política em vigor de um tipo de política de gerenciamento para uma conta, você deve ter permissão para executar as seguintes ações:
>
> - `organizations:DescribeEffectivePolicy`

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

AWS Management Console

Para ver a política em vigor de um tipo de política de gerenciamento 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 em vigor. Talvez seja necessário expandir OUs (escolher a) para encontrar a conta que você deseja.
3. Na guia Políticas, escolha o tipo de política de gerenciamento para o qual você deseja visualizar a política em vigor.
4. Escolha Exibir a política efetiva para isso 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 sem alterações significativas. Documentos de política devem incluir os operadores de herança que especificam como cada configuração é mesclada na política em vigor final.

AWS CLI & AWS SDKs

Para ver a política em vigor de um tipo de política de gerenciamento para uma conta

Você pode usar uma das seguintes opções para visualizar a política 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

Políticas declarativas

As políticas declarativas do permitem que você declare e aplique centralmente a configuração desejada para um determinado AWS service (Serviço da AWS) em grande escala em uma organização. Uma vez conectada, a configuração é sempre mantida quando o serviço adiciona novos recursos ou APIs. Use políticas declarativas para evitar ações não conformes. Por exemplo, você pode bloquear o acesso público à Internet aos recursos da Amazon VPC em toda a sua organização.

Veja os principais benefícios do uso de políticas declarativas:

- Facilidade de uso: você pode aplicar a configuração básica para um AWS service (Serviço da AWS) com algumas seleções nos AWS Control Tower consoles AWS Organizations e ou com alguns comandos usando o &. AWS CLI AWS SDKs
- Defina uma vez e esqueça: a configuração básica de um AWS service (Serviço da AWS) é sempre mantida, mesmo quando o serviço introduz novos recursos ou. APIs A configuração básica também é mantida quando novas contas são adicionadas a uma organização ou quando novos diretores e recursos são criados.
- Transparência: o relatório de status da conta permite que você revise o status atual de todos os atributos suportados pelas políticas declarativas das contas no escopo. Você também pode criar mensagens de erro personalizáveis, que podem ajudar os administradores a redirecionar os usuários finais para páginas wiki internas ou fornecer uma mensagem descritiva que pode ajudar os usuários finais a entender por que uma ação falhou.

Para obter uma lista completa de atributos Serviços da AWS e compatíveis, consulteSuporte Serviços da AWS e atributos.

Tópicos

- Como as políticas declarativas funcionam
- Mensagens de erro personalizadas para políticas declarativas
- Relatório de status da conta para políticas declarativas
- Suporte Serviços da AWS e atributos
- Conceitos básicos de políticas declarativas
- Práticas recomendadas para usar políticas declarativas
- Gerando o relatório de status da conta para políticas declarativas
- Sintaxe e exemplos de políticas declarativas

Como as políticas declarativas funcionam

As políticas declarativas são aplicadas no plano de controle do serviço, o que é uma distinção importante das políticas de autorização, como políticas de controle de serviço (SCPs) e políticas de controle de recursos (RCPs). Embora as políticas de autorização regulem o acesso ao APIs, as políticas declarativas são aplicadas diretamente no nível do serviço para impor uma intenção duradoura. Isso garante que a configuração básica seja sempre aplicada, mesmo quando novos recursos ou APIs são introduzidos pelo serviço.

A tabela a seguir ajuda a ilustrar essa distinção e fornece alguns casos de uso.

	Políticas de controle de serviço	Políticas de controle de recursos	Políticas declarativas		
Por quê?	Definir e aplicar de forma centralizada controles de acesso consistentes sobre	Definir e aplicar centralmente controles de acesso consistentes sobre recursos	Definir e aplicar centralmente a configuração básica para AWS serviços		

	Políticas de controle de serviço	Políticas de controle de recursos	Políticas declarativas		
	entidades principais (como usuários do IAM e funções do IAM) em grande escala.	em grande escala	em grande escala.		
Como?	Controlando o máximo de permissões de acesso disponíveis dos diretores em um nível de API.	Controlando o máximo de permissões de acesso disponíveis para recursos no nível da API.	Ao aplicar a configuração desejada de um AWS service (Serviço da AWS) sem usar ações de API.		
Governa funções vinculadas ao serviço?	Não	Não	Sim		

	Políticas de controle de serviço	Políticas de controle de recursos	Políticas declarativas		
Mecanismo de feedback	Erro de SCP não personalizável de acesso negado.	Erro de RCP de acesso negado não personalizável.	Mensagem de erro personalizável. Para obter mais informações, consulte Mensagens de erro personalizadas para políticas declarativas.		
Exemplo de política	Negar acesso a AWS com base no solicitado Região da AWS	Restrinja o acesso somente a conexões HTTPS aos seus recursos	Configurações de imagens permitidas		

Depois de criar e anexar uma política declarativa, ela é aplicada e aplicada em toda a sua organização. As políticas declarativas podem ser aplicadas a uma organização inteira, unidades organizacionais (OUs) ou contas. As contas que ingressam em uma organização herdarão automaticamente a política declarativa na organização. Para obter mais informações, consulte Entendendo a herança da política de gerenciamento.

A política efetiva é o conjunto de regras que são herdadas da raiz da organização e OUs junto com aquelas diretamente vinculadas à conta. A política em vigor especifica as regras que se aplicam à conta. Para obter mais informações, consulte Como visualizar políticas de gerenciamento em vigor.

Se uma política declarativa for desanexada, o estado do atributo voltará ao estado anterior antes da anexação da política declarativa.

Mensagens de erro personalizadas para políticas declarativas

As políticas declarativas permitem que você crie mensagens de erro personalizadas. Por exemplo, se uma operação de API falhar devido a uma política declarativa, você pode definir a mensagem de erro ou fornecer uma URL personalizada, como um link para um wiki interno ou um link para uma mensagem que descreva a falha. Se você não especificar uma mensagem de erro personalizada, AWS Organizations fornece a seguinte mensagem de erro padrão:`Example: This action is denied due to an organizational policy in effect.`

Você também pode auditar o processo de criação de políticas declarativas, atualização de políticas declarativas e exclusão de políticas declarativas com. AWS CloudTrail CloudTrail pode sinalizar falhas na operação da API devido a políticas declarativas. Para obter mais informações, consulte Registro e monitoramento.

> **Important**
>
> Não inclua informações de identificação pessoal (PII) nem outras informações confidenciais em uma mensagem de erro personalizada. As PII incluem informações gerais que podem ser usadas para identificar ou localizar um indivíduo. Abrange registros como financeiros, médicos, educacionais ou trabalhistas. Exemplos de PII incluem endereços, números de contas bancárias e números de telefone.

Relatório de status da conta para políticas declarativas

O relatório de status da conta permite que você revise o status atual de todos os atributos suportados pelas políticas declarativas das contas no escopo. Você pode escolher as contas e as unidades organizacionais (OUs) a serem incluídas no escopo do relatório ou escolher uma organização inteira selecionando a raiz.

Esse relatório ajuda você a avaliar a prontidão fornecendo um detalhamento por região e se o estado atual de um atributo é uniforme em todas as contas (por meio do`numberOfMatchedAccounts`) ou inconsistente (por meio do`numberOfUnmatchedAccounts`). Você também pode ver o valor mais frequente, que é o valor de configuração observado com mais frequência para o atributo.

Na Figura 1, há um relatório de status da conta gerado, que mostra a uniformidade entre as contas para os seguintes atributos: VPC Block Public Access e Image Block Public Access. Isso significa que, para cada atributo, todas as contas no escopo têm a mesma configuração para esse atributo.

O relatório de status da conta gerado mostra contas inconsistentes para os seguintes atributos: Configurações de imagens permitidas, padrões de metadados da instância, acesso ao console serial e acesso público ao bloco de instantâneos. Neste exemplo, cada atributo com uma conta inconsistente se deve ao fato de haver uma conta com um valor de configuração diferente.

Se houver um valor mais frequente, ele será exibido em sua respectiva coluna. Para obter informações mais detalhadas sobre o que cada atributo controla, consulte Sintaxe de política declarativa e exemplos de políticas.

Você também pode expandir um atributo para ver um detalhamento da região. Neste exemplo, o Image Block Public Access é expandido e, em cada região, você pode ver que também há uniformidade entre as contas.

A opção de anexar uma política declarativa para aplicar uma configuração básica depende do seu caso de uso específico. Use o relatório de status da conta para ajudá-lo a avaliar sua prontidão antes de anexar uma política declarativa.

Para obter mais informações, consulte Geração do relatório de status da conta.

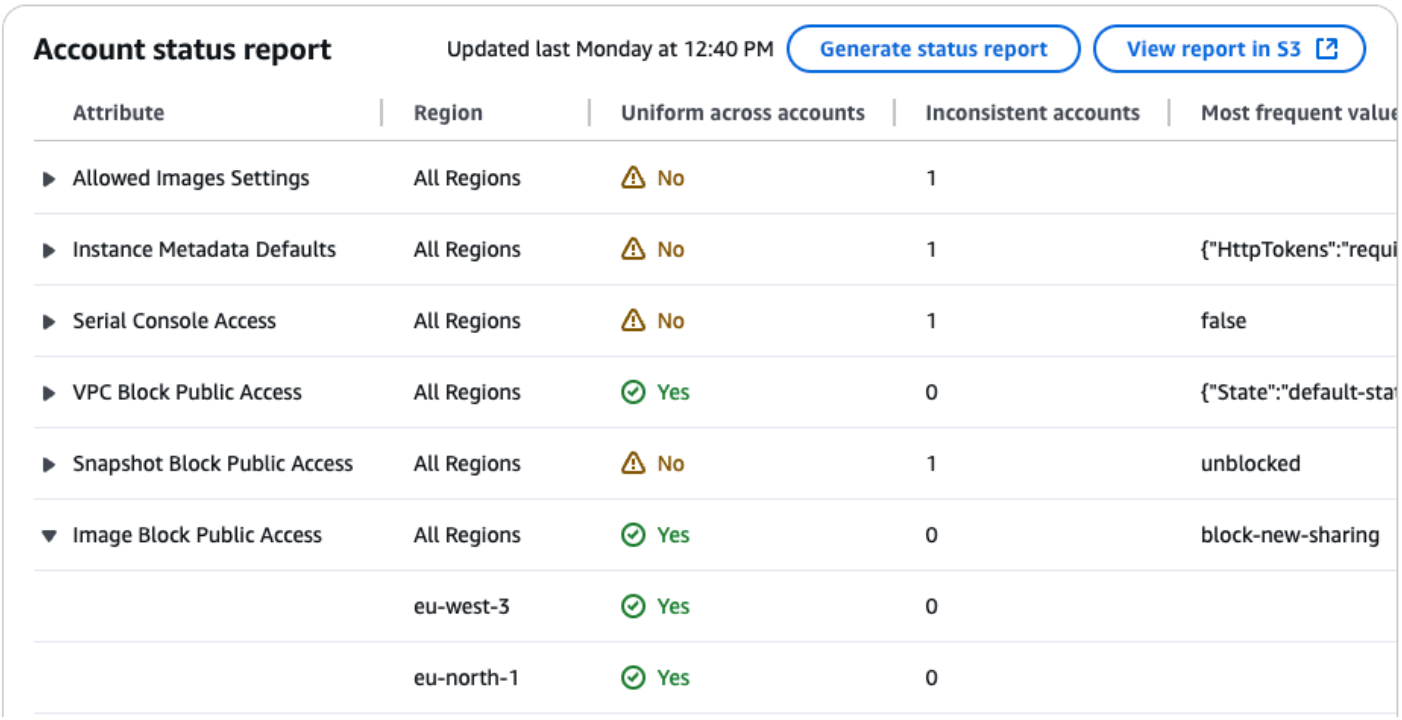


Figura 1: Exemplo de relatório de status de conta com uniformidade entre contas para VPC Block Public Access e Image Block Public Access.

Suporte Serviços da AWS e atributos

Atributos compatíveis com políticas declarativas para EC2

A tabela a seguir mostra os atributos suportados pelos serviços EC2 relacionados à Amazon.

Políticas declarativas para EC2

AWS serviço	Atributo	Efeito político	Conteúdo da política	Mais informaçõ es
Amazon VPC	Bloqueio de acesso público da VPC	Controla se os recursos na Amazon VPCs e nas sub-redes podem acessar a Internet por meio de gateways da Internet (). IGWs	Exibir política	Para obter mais informaçõ es, consulte Bloquear o acesso público VPCs e as sub-redes no Guia do usuário da Amazon VPC.
Amazon EC2	Acesso ao console serial	Controla se o console EC2 serial está acessível.	Exibir política	Para obter mais informaçõ es, consulte Configurar o acesso ao console EC2 serial no Guia do usuário do Amazon Elastic Compute Cloud.
	Bloqueio de imagem de acesso público	Controla se as Amazon Machine Images (AMIs) podem	Exibir política	Para obter mais informaçõ es, consulte Entenda o

AWS serviço	Atributo	Efeito político	Conteúdo da política	Mais informaçõ es
		ser compartil hadas publicame nte.		bloqueio do acesso público AMIs no Guia do usuário do Amazon Elastic Compute Cloud.
	Configurações de imagem permitidas	Controla a descoberta e o uso de Amazon Machine Images (AMI) na Amazon EC2 com Allowed AMIs.	Exibir política	Para obter mais informações, consulte Amazon Machine Images (AMIs) no Guia do usuário do Amazon Elastic Compute Cloud.
	Encaminha mentos de metadados de instância	Controla os padrões do IMDS para todas as novas EC2 instâncias lançadas.	Exibir política	Para obter mais informaçõ es, consulte Configurar opções de metadados de instância para novas instância s no Guia do usuário do Amazon Elastic Compute Cloud.

AWS serviço	Atributo	Efeito político	Conteúdo da política	Mais informaçõ es
Amazon EBS	Bloqueio de instantâneo de acesso público	Controla se os instantâneos do Amazon EBS estão acessíveis ao público.	Exibir política	Para obter mais informaçõ es, consulte Bloquear o acesso público para snapshots do Amazon EBS no Guia do usuário do Amazon Elastic Block Store.

Conceitos básicos de políticas declarativas

Siga essas etapas para começar a usar políticas declarativas.

1. Saiba mais sobre as permissões que você deve ter para executar qualquer tarefas de política declarativa.
2. Habilite políticas declarativas para sua organização.

> **Note**
>
> É necessário habilitar o acesso confiável
> Você deve habilitar o acesso confiável para o serviço em que a política declarativa aplicará uma configuração de linha de base. Isso cria uma função vinculada ao serviço somente para leitura que é usada para gerar o relatório de status da conta sobre qual é a configuração existente para contas em sua organização.
> Como usar o console
> Se você usa o console Organizations, essa etapa faz parte do processo para habilitar políticas declarativas.
> Usando o AWS CLI
> Se você usar o AWS CLI, há dois separados APIs:
>
> - EnablePolicyType, que você usa para habilitar políticas declarativas.

- Habilite o AWSService Access, que você usa para habilitar o acesso confiável.

Para obter mais informações sobre como habilitar o acesso confiável para um serviço específico com o AWS CLI consulte, Serviços da AWS que você pode usar com AWS Organizations.

3. Execute o relatório de status da conta.
4. Crie uma política declarativa.
5. Vincule a política declarativa à raiz, OU ou conta da sua organização.
6. Veja a política declarativa em vigor 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 a sintaxe da política declarativa e veja exemplos de políticas

Práticas recomendadas para usar políticas declarativas

AWS A recomenda as seguintes práticas recomendadas para o uso de políticas declarativas.

Aproveite as avaliações de prontidão

Use o relatório de status da conta de política declarativa para avaliar o status atual de todos os atributos suportados pelas políticas declarativas para as contas no escopo. Você pode escolher as contas e as unidades organizacionais (OUs) a serem incluídas no escopo do relatório ou escolher uma organização inteira selecionando a raiz.

Esse relatório ajuda você a avaliar a prontidão fornecendo um detalhamento por região e se o estado atual de um atributo é uniforme em todas as contas (por meio do`numberOfMatchedAccounts`) ou inconsistente (por meio do`numberOfUnmatchedAccounts`). Você também pode ver o valor mais frequente, que é o valor de configuração observado com mais frequência para o atributo.

A opção de anexar uma política declarativa para impor uma configuração de linha de base depende do seu caso de uso específico.

Para obter mais informações e um exemplo ilustrativo, consulteRelatório de status da conta para políticas declarativas.

Comece pequeno e depois escale

Para simplificar a depuração, comece com uma política de teste. 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 ocorre.

Por exemplo, você pode começar com uma política de teste vinculada a uma única conta em um ambiente de teste não crítico. Depois de confirmar que ela funciona de acordo com suas especificações, você pode mover incrementalmente a política na estrutura organizacional para mais contas e mais unidades organizacionais (OUs).

Estabelecer processos de revisão

Implemente processos para monitorar novos atributos declarativos, avaliar exceções de políticas e fazer ajustes para manter o alinhamento com seus requisitos operacionais e de segurança organizacional.

Validar alterações usando **`DescribeEffectivePolicy`**

Depois de fazer uma alteração em uma política declarativa, verifique as políticas efetivas para contas representativas abaixo do nível em que você fez a alteração. Você pode visualizar a política efetiva usando a AWS Management Console, ou usando a operação da DescribeEffectivePolicyAPI ou uma de suas variantes AWS CLI ou do AWS SDK. Certifique-se de que a alteração feita tenha o impacto pretendido na política efetiva.

Comunique-se e treine

Garanta que suas organizações entendam o propósito e o impacto de suas políticas declarativas. Forneça orientações claras sobre os comportamentos esperados e como lidar com falhas devido à aplicação de políticas.

Gerando o relatório de status da conta para políticas declarativas

O relatório de status da conta permite que você revise o status atual de todos os atributos suportados pelas políticas declarativas das contas no escopo. Você pode escolher as contas e as unidades organizacionais (OUs) a serem incluídas no escopo do relatório ou escolher uma organização inteira selecionando a raiz.

Esse relatório ajuda você a avaliar a prontidão fornecendo um detalhamento por região e se o estado atual de um atributo é uniforme em todas as contas (por meio do`numberOfMatchedAccounts`) ou

inconsistente (por meio do`numberOfUnmatchedAccounts`). Você também pode ver o valor mais frequente, que é o valor de configuração observado com mais frequência para o atributo.

A opção de anexar uma política declarativa para aplicar uma configuração de linha de base depende do seu caso de uso específico.

Para obter mais informações e um exemplo ilustrativo, consulteRelatório de status da conta para políticas declarativas.

Pré-requisitos

Antes de gerar um relatório do status da conta, você deve executar as seguintes etapas

1. A `StartDeclarativePoliciesReport` API só pode ser chamada pela conta de gerenciamento ou pelos administradores delegados de uma organização.
2. Você deve ter um bucket do S3 antes de gerar o relatório (criar um novo ou usar um existente), ele deve estar na mesma região em que a solicitação é feita e deve ter uma política de bucket do S3 apropriada. Para obter um exemplo de política do S3, consulte Exemplo de política do Amazon S3 em Exemplos na Amazon API Reference EC2
3. Você deve habilitar o acesso confiável para o serviço em que a política declarativa aplicará uma configuração de linha de base. Isso cria uma função vinculada ao serviço somente para leitura que é usada para gerar o relatório de status da conta sobre qual é a configuração existente para contas em sua organização.

   Como usar o console

   Para o console Organizations, essa etapa faz parte do processo de habilitação de políticas declarativas.

   Usando o AWS CLI

   Para o AWS CLI, use a API Enable AWSService Access.

   Para obter mais informações sobre como habilitar o acesso confiável para um serviço específico com o AWS CLI consulte, Serviços da AWS que você pode usar com AWS Organizations.
4. Somente um relatório por organização pode ser gerado por vez. A tentativa de gerar um relatório enquanto outro estiver em andamento resultará em um erro.

Acesse o relatório de status de conformidade

> **Permissões mínimas**
>
> Para gerar um relatório do status de conformidade, você precisa de permissão para executar as seguintes ações:
>
> - `ec2:StartDeclarativePoliciesReport`
> - `ec2:DescribeDeclarativePoliciesReports`
> - `ec2:GetDeclarativePoliciesReportSummary`
> - `ec2:CancelDeclarativePoliciesReport`
> - `organizations:DescribeAccount`
> - `organizations:DescribeOrganization`
> - `organizations:DescribeOrganizationalUnit`
> - `organizations:ListAccounts`
> - `organizations:ListDelegatedAdministrators`
> - `organizations:ListAWSServiceAccessForOrganization`
> - `s3:PutObject`

> **Note**
>
> Se seu bucket do Amazon S3 usa criptografia SSE-KMS, você também deve incluir a permissão na `kms:GenerateDataKey` política.

AWS Management Console

Use o procedimento a seguir para gerar um relatório do status da conta.

Para gerar um relatório de status da 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 Políticas, escolha Políticas declarativas para EC2.

3. Na EC2 página Políticas declarativas para, escolha Exibir relatório de status da conta no menu suspenso Ações.
4. Na página Exibir relatório de status da conta, escolha Gerar relatório de status.
5. No widget Estrutura organizacional, especifique quais unidades organizacionais (OUs) você deseja incluir no relatório.
6. Selecione Enviar.

AWS CLI & AWS SDKs

Para gerar um relatório de status da conta

Use as operações a seguir para gerar um relatório do status de conformidade, verificar seu status e visualizar o relatório:

- `ec2:start-declarative-policies-report`: gera um relatório de status da conta. O relatório é gerado de forma assíncrona e pode levar algumas horas para ser concluído. Para obter mais informações, consulte StartDeclarativePoliciesReporta Amazon EC2 API Reference.
- `ec2:describe-declarative-policies-report`: descreve os metadados de um relatório de status da conta, incluindo o estado do relatório. Para obter mais informações, consulte DescribeDeclarativePoliciesReportsa Amazon EC2 API Reference.
- `ec2:get-declarative-policies-report-summary`: recupera um resumo do relatório de status da conta. Para obter mais informações, consulte GetDeclarativePoliciesReportSummarya Amazon EC2 API Reference.
- `ec2:cancel-declarative-policies-report`: cancela a geração de um relatório de status da conta. Para obter mais informações, consulte CancelDeclarativePoliciesReporta Amazon EC2 API Reference.

Antes de gerar um relatório, conceda às políticas EC2 declarativas acesso principal ao bucket do Amazon S3 onde o relatório será armazenado. Para fazer isso, anexe a política a seguir ao bucket. `amzn-s3-demo-bucket`Substitua pelo nome real do bucket do Amazon S3 e `identity_ARN` pela identidade do IAM usada para chamar a `StartDeclarativePoliciesReport` API.

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

```
        {
            "Sid": "DeclarativePoliciesReportDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "report.declarative-policies-
ec2.amazonaws.com"
                }
            }
        }
    ]
}
```

Sintaxe e exemplos de políticas declarativas

Esta página fornece sintaxe exemplos das políticas declarativas.

Considerações

- Quando você configura um atributo de serviço usando uma política declarativa, isso pode afetar vários APIs. Qualquer ação não compatível falhará.
- Os administradores da conta não poderão modificar o valor do atributo de serviço no nível da conta individual.

Sintaxe para políticas declarativas

Uma política declarativa é um arquivo de texto sem formatação estruturado de acordo com as regras de JSON. A sintaxe para políticas declarativas 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 declarativa.

O exemplo a seguir mostra a sintaxe da política declarativa:

```
{
    "ec2_attributes": {
        "exception_message": {
            "@@assign": "Your custom error message.https://myURL"
        },

        ...

        [Insert supported service attributes]

        ...
    }
}
```

- O nome da chave de campo `ec2_attributes`. As políticas declarativas sempre começam com um nome de chave fixo para o determinado AWS service (Serviço da AWS). É a linha superior na política de exemplo acima. Atualmente, as políticas declarativas só oferecem suporte EC2 aos serviços relacionados à Amazon.
- Em`ec2_attributes`, você pode usar `exception_message` para definir uma mensagem de erro personalizada. Para obter mais informações, consulte Mensagens de erro personalizadas para políticas declarativas.
- Em`ec2_attributes`, você pode inserir uma ou mais das políticas declarativas suportadas. Para esses esquemas, consultePolíticas declarativas suportadas.

Políticas declarativas suportadas

A seguir estão os atributos Serviços da AWS e que as políticas declarativas suportam. Em alguns dos exemplos a seguir, a formatação de espaço em branco JSON pode ser compactada para economizar espaço.

- Bloquear o Acesso Público da VPC
- Acesso ao console serial
- Bloquear o Acesso Público de Imagem
- Configurações de imagem permitidas
- Padrões de metadados da instância
- Bloquear o Acesso Público do Snapshot

VPC Block Public Access

Efeito político

Controla se os recursos na Amazon VPCs e nas sub-redes podem acessar a Internet por meio de gateways da Internet (). IGWs Para obter mais informações, consulte Configuração para acesso à Internet no Guia do usuário da Amazon Virtual Private Cloud.

Conteúdo da política

```
"vpc_block_public_access": {
    "internet_gateway_block": { // (optional)
        "mode": { // (required)
            "@@assign": "block_ingress" // off | block_ingress | block_bidirectional
        },
        "exclusions_allowed": { // (required)
            "@@assign": "enabled" // enabled | disabled
        }
    }
}
```

Estes são os campos disponíveis para esse atributo:

- `"internet_gateway"`:
  - `"mode"`:
    - `"off"`: o VPC BPA não está ativado.
    - `"block_ingress"`: todo o tráfego de Internet para o VPCs (exceto VPCs para as sub-redes excluídas) é bloqueado. Apenas o tráfego de e para gateways NAT e gateways da Internet somente de saída é permitido porque esses gateways só permitem o estabelecimento de conexões de saída.
    - `"block_bidirectional"`: todo o tráfego de e para os gateways da Internet e os gateways da Internet (exceto os gateways da Internet e os gateways da Internet somente de saída) é VPCs bloqueado.
- `"exclusions_allowed"`: uma exclusão é um modo que pode ser aplicado a uma única VPC ou sub-rede que a isenta do modo BPA da VPC da conta e permitirá acesso bidirecional ou somente de saída.
  - `"enabled"`: as exclusões podem ser criadas pela conta.
  - `"disabled"`: as exclusões não podem ser criadas pela conta.

> **Note**
>
> É possível usar o atributo para configurar se as exclusões são permitidas, mas não é possível criar exclusões com esse atributo em si. Para criar exclusões, é necessário fazê-lo na conta proprietária da VPC. Para obter mais informações sobre como criar exclusões do BPA da VPC, consulte Criar e excluir exclusões no Manual do usuário da Amazon VPC.

Considerações

Se você usar esse atributo em uma política declarativa, não poderá usar as operações a seguir para modificar a configuração imposta para as contas no escopo. Essa lista não é exaustiva:

- `ModifyVpcBlockPublicAccessOptions`
- `CreateVpcBlockPublicAccessExclusion`
- `ModifyVpcBlockPublicAccessExclusion`

Serial Console Access

Efeito político

Controla se o console EC2 serial está acessível. Para obter mais informações sobre o console EC2 serial, consulte o console EC2 serial no Guia do usuário do Amazon Elastic Compute Cloud.

Conteúdo da política

```
"serial_console_access": {
    "status": { // (required)
        "@@assign": "enabled" // enabled | disabled
    }
}
```

Estes são os campos disponíveis para esse atributo:

- `"status"`:
  - `"enabled"`: o acesso ao console EC2 serial é permitido.
  - `"disabled"`: o acesso ao console EC2 serial está bloqueado.

Considerações

Se você usar esse atributo em uma política declarativa, não poderá usar as operações a seguir para modificar a configuração imposta para as contas no escopo. Essa lista não é exaustiva:

- `EnableSerialConsoleAccess`
- `DisableSerialConsoleAccess`

Image Block Public Access

Efeito político

Controla se as Amazon Machine Images (AMIs) podem ser compartilhadas publicamente. Para obter mais informações sobre AMIs, consulte Amazon Machine Images (AMIs) no Guia do usuário do Amazon Elastic Compute Cloud.

Conteúdo da política

```
"image_block_public_access": {
    "state": { // (required)
        "@@assign": "block_new_sharing" // unblocked | block_new_sharing
    }
}
```

Estes são os campos disponíveis para esse atributo:

- `"state"`:
  - `"unblocked"`: Sem restrições ao compartilhamento público de AMIs.
  - `"block_new_sharing"`: Bloqueia o novo compartilhamento público de AMIs. AMIs que já foram compartilhados publicamente permanecem disponíveis publicamente.

Considerações

Se você usar esse atributo em uma política declarativa, não poderá usar as operações a seguir para modificar a configuração imposta para as contas no escopo. Essa lista não é exaustiva:

- `EnableImageBlockPublicAccess`
- `DisableImageBlockPublicAccess`

Allowed Images Settings

Efeito político

Controla a descoberta e o uso de Amazon Machine Images (AMI) na Amazon EC2 com Allowed AMIs.. Para obter mais informações sobre AMIs, consulte Amazon Machine Images (AMIs) no Guia do usuário do Amazon Elastic Compute Cloud.

Conteúdo da política

Estes são os campos disponíveis para esse atributo:

```
"allowed_images_settings": {
    "state": { // (required)
        "@@assign": "enabled" // enabled | disabled | audit_mode
    },
    "image_criteria": { // (optional)
        "criteria_1": {
            "allowed_image_providers": { // limit 200
                "@@append": [
                    "amazon" // amazon | aws_marketplace | aws_backup_vault | 12
 digit account ID
                ]
            }
        }
    }
}
```

- `"state"`:
  - `"enabled"`: O atributo está ativo e obrigatório.
  - `"disabled"`: o atributo está inativo e não é obrigatório.
  - `"audit_mode"`: O atributo está no modo de auditoria. Isso significa que ele identificará imagens não compatíveis, mas não bloqueará seu uso.
- `"image_criteria"`: uma lista de `allowed_image_providers` objetos que definem as fontes de AMI permitidas.
  - `"allowed_image_providers"`: uma lista separada por vírgulas de nomes de provedores ou contas. IDs

Considerações

Se você usar esse atributo em uma política declarativa, não poderá usar as operações a seguir para modificar a configuração imposta para as contas no escopo. Essa lista não é exaustiva:

- `EnableAllowedImagesSettings`
- `ReplaceImageCriteriaInAllowedImagesSettings`
- `DisableAllowedImagesSettings`

Instance Metadata Defaults

Efeito político

Controla os padrões do IMDS para todas as novas EC2 execuções de instâncias. Observe que essa configuração define somente padrões e não impõe as configurações de versão do IMDS. Para obter mais informações sobre os padrões do IMDS, consulte o IMDS no Guia do usuário do Amazon Elastic Compute Cloud.

Conteúdo da política

Estes são os campos disponíveis para esse atributo:

```
"instance_metadata_defaults": {
    "http_tokens": { // (required)
        "@@assign": "required" // no_preference | required | optional
    },
    "http_put_response_hop_limit": { // (required)
        "@@assign": "4" // -1 | 1 -> 64
    },
    "http_endpoint": { // (required)
        "@@assign": "enabled" // no_preference | enabled | disabled
    },
    "instance_metadata_tags": { // (required)
        "@@assign": "enabled" // no_preference | enabled | disabled
    }
}
```

- `"http_tokens"`:
  - `"no_preference"`: Outros padrões se aplicam. Por exemplo, a AMI usa como padrão, se aplicável.
  - `"required"`: IMDSv2 deve ser usado. IMDSv1 não é permitido.

- `"optional"`: Ambos IMDSv1 IMDSv2 são permitidos.

> **Note**
>
> Versão de metadados
> Antes de `http_tokens` configurar como `required` (IMDSv2 deve ser usado), certifique-se de que nenhuma das suas instâncias esteja fazendo IMDSv1 chamadas.

- `"http_put_response_hop_limit"`:
  - `"Integer"`: valor inteiro de -1 a 64, representando o número máximo de saltos que o token de metadados pode percorrer. Para indicar que não há preferência, especifique -1.

> **Note**
>
> Limite de salto
> Se `http_tokens` estiver definido como`required`, é recomendável `http_put_response_hop_limit` definir no mínimo 2. Para obter mais informações, consulte Considerações sobre o acesso aos metadados da instância no Guia do usuário do Amazon Elastic Compute Cloud.

- `"http_endpoint"`:
  - `"no_preference"`: Outros padrões se aplicam. Por exemplo, a AMI usa como padrão, se aplicável.
  - `"enabled"`: o endpoint do serviço de metadados da instância está acessível.
  - `"disabled"`: o endpoint do serviço de metadados da instância não está acessível.
- `"instance_metadata_tags"`:
  - `"no_preference"`: Outros padrões se aplicam. Por exemplo, a AMI usa como padrão, se aplicável.
  - `"enabled"`: as tags de instância podem ser acessadas a partir dos metadados da instância.
  - `"disabled"`: as tags da instância não podem ser acessadas a partir dos metadados da instância.

Snapshot Block Public Access

Efeito político

Controla se os snapshots do Amazon EBS são acessíveis publicamente. Para obter mais informações sobre os snapshots do EBS, consulte os snapshots do Amazon EBS no Guia do usuário do Amazon Elastic Block Store.

Conteúdo da política

```
"snapshot_block_public_access": {
    "state": { // (required)
        "@@assign": "block_new_sharing" // unblocked | block_new_sharing |
 block_all_sharing
    }
}
```

Estes são os campos disponíveis para esse atributo:

- `"state"`:
  - `"block_all_sharing"`: bloqueia todos os compartilhamentos de snapshots. Os snapshots que já foram compartilhados publicamente são tratados como privados e não estão mais disponíveis publicamente.
  - `"block_new_sharing"`: bloqueia o novo compartilhamento público de instantâneos. Os snapshots que já foram compartilhados publicamente permanecem disponíveis publicamente.
  - `"unblocked"`: sem restrições ao compartilhamento público dos snapshots.

Considerações

Se você usar esse atributo em uma política declarativa, não poderá usar as operações a seguir para modificar a configuração imposta para as contas no escopo. Essa lista não é exaustiva:

- `EnableSnapshotBlockPublicAccess`
- `DisableSnapshotBlockPublicAccess`

Políticas de backup

As políticas de backup permitem que você gerencie e aplique centralmente os planos de backup aos AWS recursos nas contas de uma organização.

AWS Backuppermite que você crie planos de backup que definam como fazer backup de seus AWS recursos. As regras do plano incluem uma variedade de configurações, como a frequência do backup, a janela de tempo durante a qual o backup ocorre, a Região da AWS contenção dos recursos para backup e o cofre no qual armazenar o backup. Em seguida, você pode aplicar um plano de backup a grupos de AWS recursos identificados usando tags. Você também deve identificar uma função AWS Identity and Access Management (IAM) que conceda AWS Backup permissão para realizar a operação de backup em seu nome.

As políticas de backup AWS Organizations combinam todas essas peças em documentos de texto JSON. Você pode anexar uma política de backup a qualquer um dos elementos da estrutura da sua organização, como a raiz, as unidades organizacionais (OUs) e as contas individuais. Organizations aplica regras de herança para combinar as políticas na raiz da organização, em qualquer pai OUs ou vinculadas à conta. Isso resulta em uma política de backup efetiva para cada conta. Essa política eficaz instrui AWS Backup como fazer backup automático de seus AWS recursos.

Como as políticas de backup funcionam

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. Em seguida, você pode anexar uma política de backup OUs que substitua a frequência de backup de acordo com os requisitos de cada OU. 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. Você pode anexar essas políticas a diferentes partes da árvore organizacional, como a raiz ou a UO principal, com a intenção de que essas políticas parciais sejam herdadas por contas e níveis inferiores OUs . 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, AWS Backup considera que a política não é válida e não faz backup dos recursos afetados.

> **Important**
>
> AWS Backup só pode realizar um backup bem-sucedido quando invocado por uma política completa e eficaz 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 efetivo para cada um Conta da AWS na organização aparece no AWS Backup console como um plano imutável para essa conta. Você pode visualizá-lo, mas não alterá-lo. No entanto, você pode adicionar ou remover etiquetas do plano de backup usando TagResourceUntagResource APIse.

Quando AWS Backup inicia um backup com base em um plano de backup criado pela política, você pode ver o status da tarefa de backup no AWS Backup console. 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 o acesso a serviços confiáveis com AWS Backup, um usuário na conta de gerenciamento da organização poderá ver o status e os erros de todas as tarefas de backup na 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

Melhores práticas para usar políticas de backup

AWS recomenda as seguintes práticas recomendadas para o uso de 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 efetiva usando a AWS Management Console, ou usando a operação da GetEffectivePolicyAPI ou uma de suas variantes 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 contas Regiões da AWS e em sua organização

Para melhorar sua posição na recuperação de desastres, você pode armazenar cópias de seus backups.

- Uma região diferente — Se você armazenar cópias do backup em outros lugares Regiões da AWS, ajudará a proteger o backup contra corrupção 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 você armazenar cópias do backup em adição Contas da AWS, você adiciona uma barreira de segurança que ajuda a proteger contra um agente mal-intencionado que compromete 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 de conjuntos de AWS CloudFormation pilhas com Organizations para criar automaticamente os cofres de backup e as funções AWS Identity and Access Management (IAM) necessárias em cada uma das contas membros da sua organização. Você pode criar um conjunto de pilhas que inclua os recursos que você deseja disponibilizar automaticamente Conta da AWS em cada um 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 efetiva e garante que ela AWS Backup interprete suas políticas e implemente os planos de backup da maneira pretendida.

Usando AWS CloudTrail eventos para monitorar políticas de backup em sua organização

Você pode usar AWS CloudTrail eventos para monitorar quando as políticas de backup são criadas, atualizadas ou excluídas de qualquer conta em sua organização ou quando há um plano de backup organizacional inválido. Para obter mais informações, consulte Registrar eventos de gerenciamento entre contas no AWS Backup Guia 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 ter mais informações, consulte Sintaxe de política e 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.

Para obter mais informações sobre AWS Backup planos, consulte CreateBackupPlano Guia do AWS Backup desenvolvedor.

Considerações

Sintaxe da política

Nomes de chave duplicados serão rejeitados em JSON.

As políticas devem especificar os recursos Regiões da AWS e os recursos a serem copiados.

As políticas devem especificar a função do IAM que ela AWS Backup assume.

Usar o `@@assign` operador no mesmo nível pode substituir as configurações existentes. Para obter mais informações, consulte Uma política secundária substitui as configurações em uma política principal.

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.

Para obter mais informações, consulte Operadores de herança e exemplos de políticas de Backup.

Perfis do IAM

A função do IAM deve existir ao criar um plano de backup pela primeira vez.

A função do IAM deve ter permissão para acessar recursos identificados pela consulta de tag.

A função do IAM também deve ter permissão para executar o backup.

Cofres de backup

Os cofres devem existir em cada um deles para que um plano Regiões da AWS de backup possa ser executado.

Devem existir cofres para cada AWS conta que recebe a política efetiva. Para obter mais informações, consulte Criação e exclusão de cofres de backup no Guia do AWS Backup desenvolvedor.

Recomendamos que você use os conjuntos de AWS CloudFormation pilhas 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 Criar um conjunto de pilhas com permissões autogerenciadas no Guia do usuário do AWS CloudFormation .

Cotas

Para obter uma lista de cotas, consulte AWS Backup cotas no Guia do AWS Backup desenvolvedor.

Sintaxe de backup: visão geral

A sintaxe da política de backup inclui os seguintes componentes:

```
{
    "plans": {
        "PlanName": {
            "rules": { ... },
            "regions": { ... },
            "selections": { ... },
            "advanced_backup_settings": { ... },
            "backup_plan_tags": { ... }
        }
    }
```

```
}
```

Elementos de políticas de backup

Elemento	Descrição	Obrigatório
regras	Lista de regras de backup. Cada regra define quando os backups são iniciados e a janela de execução dos recursos especificados nos `selections` elementos `regions` e.	Sim
regiões	Lista de Regiões da AWS onde uma política de backup pode proteger os recursos.	Sim
seleções	Um ou mais tipos de recursos dentro do especificado `regions` que o backup `rules` protege.	Sim
configurações_de backup avançadas	Opções de configuração para cenários de backup específicos. No momento, a única configuração de backup avançada compatível é habilitar os backups do Microsoft Volume Shadow Copy Service (VSS) para Windows ou SQL Server em execução em uma EC2 instância da Amazon.	Não
etiquetas_do_plano de backup	Tags que deseja associar a um plano de backup. Cada tag é um rótulo que consiste em um valor e uma chave definida pelo usuário. As tags podem ajudar você a gerenciar, identificar, organizar, pesquisar e filtrar seus planos de backup.	Não

Sintaxe de backup: regras

A chave `rules` de política especifica as tarefas de backup agendadas que são AWS Backup executadas nos recursos selecionados.

Elementos de regra de backup

Elemento	Descrição	Obrigatório
`schedule_expression`	Expressão Cron em UTC que especifica quando o AWS Backup inicia um trabalho de backup. Para ter informações sobre expressão cron, consulte Using cron and rate expressions to schedule rules in the Amazon EventBridge User Guide.	Sim
`target_backup_vault_name`	Cofre de backup onde os backups são armazenados. Os cofres de backup são identificados por nomes que são exclusivos da conta usada para criá-los e da Região da AWS em que são criados.	Sim
`start_backup_window_minutes`	O número de minutos a aguardar antes de cancelar um trabalho de backup será cancelado se ele não for iniciado com êxito. Se esse valor for incluído, deve ser de pelo menos 60 minutos para evitar erros.	Não
`complete_backup_window_minutes`	Quantidade de minutos após um trabalho de backup ser iniciado com êxito antes que ele seja concluído ou ele será cancelado pelo. AWS Backup	Não
`enable_continuous_backup`	Especifica se o AWS Backup cria backups contínuos. `True`faz com AWS Backup que o crie backups contínuos capazes de point-in-time restauração (PITR). `False`(ou não especificado) faz com que AWS Backup o crie backups de snapshot.	Não

Elemento	Descrição	Obrigatório
	Para obter mais informações sobre backups contínuos, consulte P oint-in-time recovery no Guia do AWS Backup desenvolvedor. Observação: os backups habilitados para PITR têm retenção máxima de 35 dias.	

Elemento	Descrição	Obrigatório
`lifecycle`	Especifica quando o faz a AWS Backup transição de um backup para armazenamento de baixa atividade e quando ele expira. Os tipos de recursos que podem ser transferi dos para armazenamento a frio estão listados na tabela Disponibilidade de recursos por recurso no Guia do AWS Backup desenvolv edor. Cada ciclo de vida contém os seguintes elementos: • `move_to_cold_storage_after_ days` : Número de dias após a realização do backup antes de o AWS Backup mover o ponto de recuperação para o armazenam ento frio. • `delete_after_days` : Número de dias após a ocorrência de um backup antes de AWS Backup excluir o ponto de recuperação. • `opt_in_to_archive_for_suppo rted_resources` : Se o valor for definido como`true`, um plano de backup faz a transição dos recursos compatíveis para o nível de armazenamento de arquivos (frio) de acordo com as suas configurações de ciclo de vida. Observação: Os backups transferidos para armazenamento “frio” devem ficar armazenad os lá por no mínimo 90 dias.	Não

Elemento	Descrição	Obrigatório
	Isso significa que `delete_after_days` deve ser 90 dias maior que `move_to_cold_storage_after_days` .	

Elemento	Descrição	Obrigatório

`copy_actions`	Especifica se AWS Backup copia um backup para um ou mais locais adicionais.
	
	Cada ação de cópia contém os seguintes elementos:
	
	• `target_backup_vault_arn` : Cofre onde o AWS Backup armazena uma cópia adicional do backup.
	  • Use `$account` para cópias da mesma conta
	  • Use o ID de conta real para cópias entre contas
	• `lifecycle` : especifica quando o faz a AWS Backup transição de um backup para armazenamento de baixa atividade e quando ele expira.
	
	Cada ciclo de vida contém os seguintes elementos:
	  • `move_to_cold_storage_after_days` : Número de dias após a realizaçã o do backup antes de o AWS Backup mover o ponto de recuperação para o armazenamento frio.
	  • `delete_after_days` : Número de dias após a ocorrência de um backup antes de AWS Backup excluir o ponto de recuperaç ão.
	
	Observação: Os backups transferidos para armazenamento “frio” devem ficar armazenad os lá por no mínimo 90 dias.
		Não

Elemento	Descrição	Obrigatório
	Isso significa que `delete_after_days` deve ser 90 dias maior que`move_to_cold_storage_after_days` .	
`recovery_point_tags`	Tags que deseja atribuir aos recursos restaurados do backup. Cada tag contém os seguintes elementos: • `tag_key`: Nome da tag (com distinção entre maiúsculas e minúsculas) • `tag_value` : valor da tag (com distinção entre maiúsculas e minúsculas)	Não
`index_actions`	Especifica se AWS Backup cria um índice de backup de seus snapshots do Amazon EBS e/ou backups do Amazon S3. Os índices de backup são criados para pesquisar os metadados de seus backups. Para obter mais informações sobre criação de índice de backup e pesquisa de backup, consulte Pesquisa de backup. Observação: permissões adicionais de função do IAM são necessárias para a criação do índice de backup de snapshots do Amazon EBS. Cada ação de índice contém o seguinte elemento: `resource_types` onde os tipos de recursos suportados para indexação são Amazon EBS e Amazon S3. Esse parâmetro especifica qual tipo de recurso será incluído na indexação.	Não

Sintaxe de backup: regiões

A chave `regions` de política especifica quais o Regiões da AWS AWS Backup examina para localizar os recursos que correspondem às condições da `selections` chave.

Elementos de regiões de backup

Elemento	Descrição	Obrigatório
`regions`	Especifica os Região da AWS códigos. Por exemplo: `["us-east-1", "eu-north -1"]` .	Sim

Sintaxe de backup: seleções

A chave `selections` de política especifica os recursos que são apoiados pelas regras em uma política de backup.

Existem dois elementos mutuamente exclusivos: `tags` e. `resources` Uma política eficaz deve estar marcada `have` ou estar `resources` na seleção para ser válida.

Se você quiser uma seleção com condições de tag e condições de recursos, use as `resources` teclas.

Elementos de seleção de backup: tags

Elemento	Descrição	Obrigatório
`iam_role_arn`	Função do IAM que AWS Backup pressupõe consultar, descobrir e fazer backup de recursos nas regiões especificadas. A função deve ter permissões suficientes para consultar recursos com base nas condições da tag e realizar operações de backup nos recursos correspondentes.	Sim
`tag_key`	Marque o nome da chave a ser pesquisada.	Sim
`tag_value`	Valor que deve ser associado à tag_key correspondente.	Sim

Elemento	Descrição	Obrigatório
	AWS Backup inclui o recurso somente se tag_key e tag_value corresponderem (diferenc ia maiúsculas de minúsculas).	
`conditions`	Marque chaves e valores que você deseja incluir ou excluir Use string_equals ou string_not_equals para incluir ou excluir tags de uma correspondência exata. Use string_like e string_not_like para incluir ou excluir tags que contenham ou não caracteres específicos Nota: Limitado a 30 condições para cada seleção.	Não

Elementos de seleção de backup: recursos

Elemento	Descrição	Obrigatório
`iam_role_arn`	Função do IAM que AWS Backup pressupõe consultar, descobrir e fazer backup de recursos nas regiões especificadas. A função deve ter permissões suficientes para consultar recursos com base nas condições da tag e realizar operações de backup nos recursos correspondentes. Nota: Em AWS GovCloud (US) Regions, você deve adicionar o nome da partição ao ARN. Por exemplo, "`arn:aws:ec2:*:*:volume/*` " deve ser "`arn:aws-us-gov:ec2:*:*:volume/*` ".	Sim

Elemento	Descrição	Obrigatório
`resource_types`	Tipos de recursos a serem incluídos em um plano de backup.	Sim
`not_resource_types`	Tipos de recursos a serem excluídos de um plano de backup.	Não
`conditions`	Marque chaves e valores que você deseja incluir ou excluir Use string_equals ou string_not_equals para incluir ou excluir tags de uma correspondência exata. Use string_like e string_not_like para incluir ou excluir tags que contenham ou não caracteres específicos Nota: Limitado a 30 condições para cada seleção.	Não

Tipos de recursos compatíveis

O Organizations oferece suporte aos seguintes tipos de recursos para os `not_resource_types` elementos `resource_types` e:

- AWS Backup gateway máquinas virtuais: `"arn:aws:backup-gateway:*:*:vm/*"`
- AWS CloudFormation pilhas: `"arn:aws:cloudformation:*:*:stack/*"`
- Tabelas do Amazon DynamoDB: `"arn:aws:dynamodb:*:*:table/*"`
- EC2 Instâncias da Amazon: `"arn:aws:ec2:*:*:instance/*"`
- Volumes do Amazon EBS: `"arn:aws:ec2:*:*:volume/*"`
- Sistemas de arquivos do Amazon EFS: `"arn:aws:elasticfilesystem:*:*:file-system/*"`
- Clusters do Amazon Aurora/Amazon DocumentDB/Amazon Neptune: `"arn:aws:rds:*:*:cluster:*"`
- Bancos de dados do Amazon RDS: `"arn:aws:rds:*:*:db:*"`

- Clusters do Amazon Redshift: `"arn:aws:redshift:*:*:cluster:*"`
- Amazon S3: `"arn:aws:s3:::*"`
- AWS Systems Manager para SAP Bancos de dados HANA: `"arn:aws:ssm-sap:*:*:HANA/*"`
- AWS Storage Gateway gateways: `"arn:aws:storagegateway:*:*:gateway/*"`
- Bancos de dados Amazon Timestream: `"arn:aws:timestream:*:*:database/*"`
- Sistemas de FSx arquivos da Amazon: `"arn:aws:fsx:*:*:file-system/*"`
- FSx Volumes da Amazon: `"arn:aws:fsx:*:*:volume/*"`

Exemplos de código

Para obter mais informações, consulte Especificação de recursos com o bloco de tags e Especificação de recursos com o bloco de recursos.

Sintaxe de backup: configurações avançadas de backup

A `advanced_backup_settings` chave especifica as opções de configuração para cenários de backup específicos. Cada configuração contém os seguintes elementos:

Elementos avançados de configurações de backup

Elemento	Descrição	Obrigatório
`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: No momento, a única configuração de backup avançada compatível é habilitar os backups do Microsoft Volume Shadow Copy Service (VSS) para Windows ou SQL Server	Não

Elemento	Descrição	Obrigatório
	em execução em uma EC2 instância da Amazon. Cada configuração de backup avançada contém os seguintes elementos: • `Object key name`: sequência que especifica o tipo de recurso ao qual as configurações avançadas a seguir se aplicam. O nome da chave deve ser o tipo `"ec2"` de recurso • `Object value`: sequência que contém uma ou mais configurações de backup específicas do tipo de recurso associado. O valor especifica que o `"windows_vss"` suporte é `enabled` ou `disabled` para backups realizado s nas EC2 instâncias da Amazon.	

Exemplo:

```
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
            "@@assign": "enabled"
        }
```

```
    }
},
```

Sintaxe de backup: etiquetas do plano de backup

A chave `backup_plan_tags` de política especifica as tags anexadas ao plano de backup propriamente dito. Isso não afeta as tags especificadas para `rules` ou`selections`.

Elementos de tag do plano de backup

Elemento	Descrição	Obrigatório
`backup_plan_tags`	Cada tag é um rótulo que consiste em uma chave e um valor definidos pelo usuário: • `tag_key`: Marque o nome da chave a ser pesquisado. O valor diferencia maiúsculas de minúsculas. • `tag_value` : Valor anexado ao plano de backup e associado a`tag_key`. O valor diferencia maiúsculas de minúsculas.	Não

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 principal
- Exemplo 2: uma política principal é mesclada com uma política secundária
- Exemplo 3: Uma política para pais impede qualquer alteração feita por uma política para crianças
- Exemplo 4: Uma política principal impede alterações em um plano de backup por uma política secundária
- Exemplo 5: uma política secundária substitui as configurações em uma política principal
- Exemplo 6: especificando recursos com o bloco de tags
- Exemplo 7: Especificação de recursos com o bloco de recursos

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"
                        },
                        "opt_in_to_archive_for_supported_resources": {
                            "@@assign": "false"
                        }
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "index_actions": {
                        "resource_types": {
```

```
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                    },
                    "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"
                                },
                                "opt_in_to_archive_for_supported_resources": {
                                    "@@assign": "false"
                                }
                            }
                        },
                        "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"
                                },
                                "opt_in_to_archive_for_supported_resources": {
                                    "@@assign": "false"
                                }
                            }
                        }
                    }
```

```
                }
            },
            "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 em vigor processada em cada 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",
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": "false"
                    },
                    "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": {
                                "delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        },
                        "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": {
                                "delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        }
```

```
                    }
                }
            },
            "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 superior herdada e uma política subordinada herdada ou diretamente anexada a uma se Conta da AWS mesclam para formar a política em vigor.

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" },
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
```

```
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "delete_after_days": { "@@assign": "180" },
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "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":
 "28" },
                                "delete_after_days": { "@@assign": "180" },
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "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" },
                        "delete_after_days": { "@@assign": "365" },
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
                                "delete_after_days": { "@@assign": "365" },
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                },
            "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",
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "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": "28",
```

```
                                "delete_after_days": "180",
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [ "PII", "RED" ]
                    }
                }
            }
        },
        "Monthly_Backup_Plan": {
            "regions": [ "us-east-1", "eu-central-1" ],
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30",
                        "opt_in_to_archive_for_supported_resources": { "@@assign":
 "false" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:$account:backup-
vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "30",
                                "delete_after_days": "365",
                                "opt_in_to_archive_for_supported_resources":
 { "@@assign": "false" }
                            }
                        }
```

```
                    }
                }
            },
            "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"
                    },
                    "index_actions": {
                       "@@operators_allowed_for_child_policies": ["@@none"],
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
                        },
                        "delete_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
                        },
                        "opt_in_to_archive_for_supported_resources": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "false"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
```

```
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "delete_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "28"
                                },
                                "move_to_cold_storage_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "180"
                                },
                                 "opt_in_to_archive_for_supported_resources": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "false"
                                }
                            }
                        }
                    }
                }
            },
            "selections": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "tags": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "datatype": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "iam_role_arn": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "arn:aws:iam::$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",
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
```

```
                    },
                    "lifecycle": {
                        "delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180",
                        "opt_in_to_archive_for_supported_resources": "false"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:backup-vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "delete_after_days": "180",
                            "opt_in_to_archive_for_supported_resources": "false"
                        }
                    }
                }
            },
            "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"},
                    "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
```

```
                                "S3"
                            ]
                        }
                    },
                    "lifecycle": {
                        "delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:t2": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:backup-vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "delete_after_days": {"@@assign": "180"},
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        }
                    }
                }
            },
            "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"},
                        "delete_after_days": {"@@assign": "365"},
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    }
                }
            }
        }
    }
}
```

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 O executa a cada duas horas em vez de hora em 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",
                     "index_actions": {
                        "resource_types": {
                            "@@assign": [
                                "EBS",
                                "S3"
                            ]
                        }
                     },
                    "lifecycle": {
                        "delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30",
                        "opt_in_to_archive_for_supported_resources": "false"

                    },
                    "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": "28",
                                "delete_after_days": "180",
                                "opt_in_to_archive_for_supported_resources": "false"
                            }
                        }
                    }
```

```
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        }
    }
}
```

Exemplo 6: Especificando recursos com o bloco **`tags`**

O exemplo a seguir inclui todos os recursos com `tag_key` `tag_value` = “`env`” `"prod"` e = `"gamma"` e. Este exemplo exclui recursos com o `tag_key` = `"backup"` e o `tag_value` =`"false"`.

```
...
"selections":{
    "tags":{
        "selection_name":{
            "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/IAMRole"},
            "tag_key":{"@@assign": "env"},
            "tag_value":{"@@assign": ["prod", "gamma"]},
            "conditions":{
                "string_not_equals":{
                    "condition_name1":{
                        "condition_key": { "@@assign": "aws:ResourceTag/backup"  },
                        "condition_value": {  "@@assign": "false" }
                    }
                }
            }
        }
    }
},
...
```

Exemplo 7: especificando recursos com o bloco **`resources`**

Veja a seguir exemplos do uso do `resources` bloco para especificar recursos.

Example: Select all resources in my account

A lógica booleana é semelhante à que você pode usar nas políticas do IAM. O `"resource_types"` bloco usa um booleano `AND` para combinar os tipos de recursos.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        }
    }
},
...
```

Example: Select all resources in my account, but exclude Amazon EBS volumes

A lógica booleana é semelhante à que você pode usar nas políticas do IAM. Os `"not_resource_types"` blocos `"resource_types"` e usam um booleano `AND` para combinar os tipos de recursos.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "not_resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        }
```

```
    }
},
...
```

Example: Select all resources tagged with "backup" : "true", but exclude Amazon EBS volumes

A lógica booleana é semelhante à que você pode usar nas políticas do IAM. Os `"not_resource_types"` blocos `"resource_types"` e usam um booleano `AND` para combinar os tipos de recursos. O `"conditions"` bloco usa um booleano`AND`.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "not_resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key": { "@@assign":"aws:ResourceTag/backup"},
                    "condition_value": {  "@@assign":"true" }
                }
            }
        }
    }
},
...
```

Example: Select all Amazon EBS volumes and Amazon RDS DB instances tagged with both "backup" : "true" and "stage" : "prod"

A lógica booleana é semelhante à que você pode usar nas políticas do IAM. O `"resource_types"` bloco usa um booleano `AND` para combinar os tipos de recursos. O `"conditions"` bloco usa um booleano `AND` para combinar tipos de recursos e condições de tag.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:rds:*:*:db:*"
            ]
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                },
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/stage"},
                    "condition_value":{"@@assign":"prod"}
                }
            }
        }
    }
},
...
```

Example: Select all Amazon EBS volumes and Amazon RDS instances tagged with "backup" : "true" but not "stage" : "test"

A lógica booleana é semelhante à que você pode usar nas políticas do IAM. O `"resource_types"` bloco usa um booleano `AND` para combinar os tipos de recursos. O `"conditions"` bloco usa um booleano `AND` para combinar tipos de recursos e condições de tag.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:rds:*:*:db:*"
            ]
```

```
        },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                  }
            },
            "string_not_equals":{
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/stage"},
                    "condition_value":{"@@assign":"test"}
                }
            }
        }
    }
},
...
```

Example: Select all resources tagged with "key1" and a value which begins with "include" but not with "key2" and value that contains the word "exclude"

A lógica booleana é semelhante à que você pode usar nas políticas do IAM. O `"resource_types"` bloco usa um booleano AND para combinar os tipos de recursos. O `"conditions"` bloco usa um booleano AND para combinar tipos de recursos e condições de tag.

Neste exemplo, observe o uso do caractere curinga (`*`) em `include**exclude*`, e. `arn:aws:rds:*:*:db:*` Você pode usar o caractere curinga (`*`) no início, no final e no meio de uma string.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
        "resource_types":{
            "@@assign": [
                "*"
            ]
        },
        "conditions":{
            "string_like":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/key1"},
```

```
                    "condition_value":{"@@assign":"include*"}
                }
            },
            "string_not_like":{
                "condition_name2":{
                    "condition_key":{"@@assign":"aws:ResourceTag/key2"},
                    "condition_value":{"@@assign":"*exclude*"}
                }
            }
        }
    }
},
...
```

Example: Select all resources tagged with "backup" : "true" except Amazon FSx file systems and Amazon RDS resources

A lógica booleana é semelhante à que você pode usar nas políticas do IAM. Os `"not_resource_types"` blocos `"resource_types"` e usam um booleano `AND` para combinar os tipos de recursos. O `"conditions"` bloco usa um booleano `AND` para combinar tipos de recursos e condições de tag.

```
...
"resources":{
    "resource_selection_name":{
        "iam_role_arn":{"@@assign": "arn:aws:iam::$account:role/IAMRole"},
            "resource_types":{
                "@@assign": [
                    "*"
               ]
            },
            "not_resource_types":{
                "@@assign":[
                    "arn:aws:fsx:*:*:file-system/*",
                    "arn:aws:rds:*:*:db:*"
                ]
            },
        "conditions":{
            "string_equals":{
                "condition_name1":{
                    "condition_key":{"@@assign":"aws:ResourceTag/backup"},
                    "condition_value":{"@@assign":"true"}
                }
```

```
            }
        }
    }
},
...
```

Políticas de tag

As políticas de tags permitem padronizar as tags anexadas aos AWS recursos nas contas de uma 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.

O que são tags?

As tags são rótulos de atributos personalizados que você atribui ou AWS atribui aos AWS recursos. 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 marcar AWS recursos.
- Para obter informações sobre a atribuição de tags a recursos de Organizations, consulte Recursos de marcação AWS Organizations.

- Para obter informações sobre como marcar recursos em outros Serviços da AWS, 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.

O uso de políticas de tags 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 AWS serviço em que criou o recurso. Você também pode usar o Tag Editor e a API Resource Groups Tagging para marcar e desmarcar recursos de vários serviços.

  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 políticas de gerenciamento para AWS Organizations.

> **Important**
>
> Para começar com as políticas de tags, é AWS altamente recomendável que você siga o exemplo de fluxo de trabalho descrito em Conceitos básicos das políticas de tag antes de passar para políticas de tags 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.

Práticas recomendadas para usar políticas de tag

AWS recomenda as seguintes práticas recomendadas para o uso de políticas de tags.

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, talvez você queira especificar que, quando uma `CostCenter` tag é anexada a AWS Secrets Manager segredos, ela deve usar o tratamento de caso 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 encontrar e corrigir tags não compatíveis em recursos em suas contas usando o procedimento descrito em Avaliação da conformidade de uma conta no Guia do usuário de recursos de marcação. AWS 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 AWS serviço oferece suporte ao controle de acesso usando tags, consulte Serviços da AWS That Work with IAM no Guia do usuário do IAM. Procure os serviços que têm Sim na coluna ABAC (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 várias Serviços da AWS. 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 políticas de gerenciamento para AWS Organizations
- 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. Crie sua primeira política de tags de forma simples. Insira uma chave de tag no tratamento de maiúscula e minúscula que você deseja usar e deixe todas as outras opções com a configuração padrão.	A conta de gerenciamento da organização.[1]	AWS Organizations
Etapa 3: anexar uma política de tag a uma única conta-membro que você pode usar para teste. Será necessário fazer login nesta conta na próxima etapa.	A conta de gerenciamento da organização.[1]	AWS Organizations

Tarefa	Conta para fazer login	AWS console de serviço a ser usado
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. Se você criou recursos com tags compatíveis e não compatíveis, você verá as tags não compatíveis nos resultados.
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. 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. Você pode usar as informações em Entendendo a herança da política de gerenciamento e Sintaxe de política de tag para criar políticas de tag mais detalhadas.	A conta de gerenciamento da organização.[1]	AWS Organizations
Anexe políticas de tags a contas adicionais ou OUs. 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	A conta de gerenciamento da organização.[1]	AWS Organizations

Tarefa avançada	Conta para fazer login	AWS console de serviço a ser usado
criar novos recursos. Para obter um exemplo, consulte Exigir uma tag em recursos criados especificados.		
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 obter 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. 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
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.

Tarefas de aplicação	Conta para fazer login	AWS console de serviço a ser usado
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.

Usando EventBridge a Amazon para monitorar tags não compatíveis

Você pode usar a Amazon EventBridge, antiga Amazon CloudWatch Events, para monitorar quando tags não compatíveis 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 EventBridge, consulte o Guia EventBridge do usuário da Amazon.

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 Serviços da AWS 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, as tags nos grupos do Amazon EC2 Auto Scaling e nos clusters do Amazon EMR podem se propagar automaticamente para as instâncias da Amazon contidas. EC2 Você pode ter políticas de tags para a Amazon EC2 que sejam mais rígidas do que para grupos de Auto Scaling ou 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.

Tópicos

- Encontrar recursos não compatíveis para uma conta com AWS Organizations
- Corrigindo etiquetas não compatíveis em recursos com AWS Organizations
- Gerando um relatório de conformidade em toda a organização com AWS Organizations
- Serviços e tipos de recursos compatíveis com a aplicação

Encontrar recursos não compatíveis para uma conta com AWS Organizations

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 localizar recursos incompatíveis para uma conta usando uma política de tag, execute o seguinte comando para salvar os resultados em um arquivo:

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

Corrigindo etiquetas não compatíveis em recursos com AWS Organizations

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.

Gerando um relatório de conformidade em toda a organização com AWS Organizations

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 start-report-creation --region us-east-1
```

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 • Nomes de domínio • Novas operações de API REST • Estágios	• `"apigateway:apikeys"` • `"apigateway:domainnames"` • `"apigateway:restapis"` • `"apigateway:restapis/stages"`
AWS Amplify	• Componente • Tema	• `"amplifyuibuilder:app/environment/components"` • `"amplifyuibuilder:app/environment/themes"`
AWS AppConfig	• Aplicação • Perfil de configuração • Implantação • Estratégia de implantação • Environment	• `"appconfig:application"` • `"appconfig:application/configurationprofile"` • `"appconfig:application/environment/deployment"` • `"appconfig:deploymentstrategy"` • `"appconfig:application/environment"`
AWS App Mesh	• Todos • Rota de gateway • Mesh • Rota • Gateway virtual • Nó virtual • Roteador virtual • Serviço virtual	• `"appmesh:*"` • `"appmesh:mesh/virtualGateway/gatewayRoute"` • `"appmesh:mesh"` • `"appmesh:mesh/virtualRouter/route"` • `"appmesh:mesh/virtualGateway"` • `"appmesh:mesh/virtualNode"` • `"appmesh:mesh/virtualRouter"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
		• `"appmesh:mesh/virtualService"`
Amazon Athena	• Todos • WorkGroup	• `"athena:*"` • `"athena:workgroup"`
AWS Audit Manager	• Avaliação • Framework de avaliação • Controle	• `"auditmanager:assessment "` • `"auditmanager:assessmentFramework "` • `"auditmanager:control "`
AWS Backup	• Plano de backup • Cofre • Gateway • Hyper Visor • VM	• `"backup:backup-plan"` • `"backup:backup-vault"` • `"backup-gateway:gateway"` • `"backup-gateway:hypervisor"` • `"backup-gateway:vm"`
AWS Batch	• Trabalho • Definição do trabalho • Fila de trabalho	• `"batch:job"` • `"batch:job-definition"` • `"batch:job-queue"`
AWS BugBust	• Event	• `"bugbust:event"`
AWS Certificate Manager	• Todos • Certificados • Private Certificate Authority	• `"acm:*"` • `"acm:certificate"` • `"acm-pca:certificate-authority"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
Amazon Chime	• Instância da aplicação • Canal • Pipeline de mídia • Reunião • Aplicações de mídia de SIP • Instância do aplicativo do usuário • Conector de voz	• `"chime:app-instance"` • `"chime:app-instance/channel"` • `"chime:media-pipeline"` • `"chime:meeting"` • `"chime:sma"` • `"chime:app-instance/user"` • `"chime:vc"`
AWS Clean Rooms	• Colaboração • Tabela configurada • Associação • Associação de tabela configurada	• `"cleanrooms:collaboration"` • `"cleanrooms:configuredtable"` • `"cleanrooms:membership"` • `"cleanrooms:membership/configuredtableassociation"`
AWS Cloud9	• Environment	• `"cloud9:environment"`
Amazon CloudFront	• Todos • Distribuição	• `"cloudfront:*"` • `"cloudfront:distribution"`
AWS CloudTrail	• Todos • Trilha	• `"cloudtrail:*"` • `"cloudtrail:trail"`
Amazon CloudWatch	• Todos • Alarme • Regra do Contributor Insights • Fluxos de métricas	• `"cloudwatch:*"` • `"cloudwatch:alarm"` • `"cloudwatch:insight-rule"` • `"cloudwatch:metric-stream"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
Monitor de CloudWatch Internet da Amazon	• Monitorar	• `"internetmonitor:monitor"`
CloudWatch Registros da Amazon	• Destino • Grupo de logs	• `"logs:destination"` • `"logs:log-group"`
Gerenciador de acesso Amazon CloudWatch Observability	• Link • Sink	• `"oam:link"` • `"oam:sink"`
AWS CodeBuild	• Todos • Projeto	• `"codebuild:*"` • `"codebuild:project"`
Amazon CodeCatalyst	• Conexões	• `"codecatalyst:connections"`
AWS CodeCommit	• Todos • Repositório	• `"codecommit:*"` • `"codecommit:repository"`
AWS CodePipeline	• Todos • Tipo de ação • Pipeline • Webhook	• `"codepipeline:*"` • `"codepipeline:actiontype"` • `"codepipeline:pipeline"` • `"codepipeline:webhook"`
Identidade do Amazon Cognito	• Todos • Grupo de identidades	• `"cognito-identity:*"` • `"cognito-identity:identitypool"`
Grupos de usuários do Amazon Cognito	• Todos • Grupo de usuários	• `"cognito-idp:*"` • `"cognito-idp:userpool"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
Amazon Comprehend	• Todos • Classificador de documentos • Reconhecimento de entidade	• `"comprehend:*"` • `"comprehend:document-classifier"` • `"comprehend:entity-recognizer"`
AWS Config	• Todos • Agregação de autorização • Agregador de configuração • Regra do Config	• `"config:*"` • `"config:aggregation-authorization"` • `"config:config-aggregator"` • `"config:config-rule"`
CodeGuru Revisor da Amazon	• Associação	• `"codeguru-reviewer:association"`
CodeGuru Segurança da Amazon	• Verificar	• `"codeguru-security:scans"`
CodeConnections	• Conexão • Host	• `"codestar-connections:connection"` • `"codestar-connections:host"`
Amazon Connect	• Fluxo de contato • Associação de integração • Fila • Conexão rápida • Perfil de roteamento • Usuário	• `"connect:instance/contact-flow"` • `"connect:instance/integration-association"` • `"connect:instance/queue"` • `"connect:instance/transfer-destination"` • `"connect:instance/routing-profile"` • `"connect:instance/agent"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
Amazon Connect Wisdom	• Assistente • Associação • Conteúdo • Base de conhecimento • Sessão	• `"wisdom:assistant"` • `"wisdom:association"` • `"wisdom:content"` • `"wisdom:knowledge-base"` • `"wisdom:session"`
AWS Database Migration Service	• Todos • Endpoint • ES • Rep • Subgrp • Tarefa	• `"dms:*"` • `"dms:endpoint"` • `"dms:es"` • `"dms:rep"` • `"dms:subgrp"` • `"dms:task"`
Amazon Data Lifecycle Manager	• Política	• `"dlm:policy"`
AWS Direct Connect	• Todos • Dxcon • Dxlag • Dxvif	• `"directconnect:*"` • `"directconnect:dxcon"` • `"directconnect:dxlag"` • `"directconnect:dxvif"`
Amazon DynamoDB	• Todos • Tabela	• `"dynamodb:*"` • `"dynamodb:table"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
Amazon EC2	• Reserva de capacidade • Frota de reserva de capacidade • Gateway da operadora • Endpoint do cliente VPN • Grupo do CoIP • Gateway do cliente • Host dedicado • Opções do DHCP • Gateway da Internet somente de saída • Elastic IP • Janels de eventos • Tarefa de exportação de imagem • Tarefa de instância de exportação • Frota • Imagem de FPGA • Reserva de host • Imagem • Tarefa de importação de imagem • Tarefa de importação de snapshot • Instância	• `"ec2:capacity-reservation"` • `"ec2:capacity-reservation-fleet"` • `"ec2:carrier-gateway"` • `"ec2:client-vpn-endpoint"` • `"ec2:coip-pool"` • `"ec2:customer-gateway"` • `"ec2:dedicated-host"` • `"ec2:dhcp-options"` • `"ec2:egress-only-internet-gateway"` • `"ec2:elastic-ip"` • `"ec2:instance-event-window"` • `"ec2:export-image-task"` • `"ec2:export-instance-task"` • `"ec2:fleet"` • `"ec2:fpga-image"` • `"ec2:host-reservation"` • `"ec2:image"` • `"ec2:import-image-task"` • `"ec2:import-snapshot-task"` • `"ec2:instance"` • `"ec2:instance-connect-endpoint"` • `"ec2:internet-gateway"` • `"ec2:ipam"` • `"ec2:ipam-external-resource-verification-token"` • `"ec2:ipam-pool"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
	• Endpoint Instance Connect • Gateway da Internet • IP Address Manager • Token de verificação de recursos externos do IP Address Manager • Grupo do IP Address Manager • Descoberta de recursos do IP Address Manager • Associação de descoberta de recursos do gerenciador de endereços IP • Escopo do IP Address Manager • IPv4 Piscina • Par de chaves • Modelo de execução • Tabela de rotas do gateway local • Associação de grupos de interface virtual da tabela de	• `"ec2:ipam-resource-discovery"` • `"ec2:ipam-resource-discovery-association"` • `"ec2:ipam-scope"` • `"ec2:ipv4pool-ec2"` • `"ec2:key-pair"` • `"ec2:launch-template"` • `"ec2:local-gateway-route-table"` • `"ec2:local-gateway-route-table-virtual-interface-group-association"` • `"ec2:local-gateway-route-table-vpc-association"` • `"ec2:natgateway"` • `"ec2:network-acl"` • `"ec2:network-interface"` • `"ec2:network-insights-access-scope"` • `"ec2:network-insights-access-scope-analysis"` • `"ec2:network-insights-analysis"` • `"ec2:network-insights-path"` • `"ec2:placement-group"` • `"ec2:prefix-list"` • `"ec2:replace-root-volume-task"` • `"ec2:reserved-instances"` • `"ec2:route-table"` • `"ec2:security-group"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
	rotas do gateway local • Associação de VPC da tabela de rotas do gateway local • NAT gateway • Conexão ACL • Interface de rede • Escopo de acesso do Network Insights • Análise do escopo de acesso do Network Insights • Análise do Network Insights • Caminho do Network Insights • Grupo de posicionamento • Lista de prefixos • Tarefa de substituição de volume raiz • Instâncias reservadas • Tabela de rotas • Grupo de segurança • Snapshot • Solicitação de frota spot	• `"ec2:snapshot"` • `"ec2:spot-fleet-request"` • `"ec2:spot-instances-request"` • `"ec2:subnet"` • `"ec2:subnet-cidr-reservation"` • `"ec2:traffic-mirror-filter"` • `"ec2:traffic-mirror-session"` • `"ec2:traffic-mirror-target"` • `"ec2:transit-gateway"` • `"ec2:transit-gateway-attachment"` • `"ec2:transit-gateway-connect-peer"` • `"ec2:transit-gateway-multicast-domain"` • `"ec2:transit-gateway-policy-table"` • `"ec2:transit-gateway-route-table"` • `"ec2:transit-gateway-route-table-announcement"` • `"ec2:verified-access-endpoint"` • `"ec2:verified-access-group"` • `"ec2:verified-access-instance"` • `"ec2:verified-access-trust-provider"` • `"ec2:volume"` • `"ec2:vpc-flow-log"` • `"ec2:vpc"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
	• Solicitações de instância Spot • Sub-rede • Reserva do CIDR da sub-rede • Filtro de espelho de tráfego • Sessão de espelho de tráfego • Destino de espelho de tráfego • Gateway de trânsito • Anexo do gateway de trânsito • Par do Transit Gateway Connect • Domínio multicast do gateway de trânsito • Tabela de políticas de gateway de trânsito • Tabela de rotas do gateway de trânsito • Anúncio da tabela de rotas do gateway de trânsito • Endpoint de acesso verificado • Grupo de acesso verificado	• `"ec2:vpc-endpoint"` • `"ec2:vpc-endpoint-service"` • `"ec2:vpc-peering-connection"` • `"ec2:vpn-connection"` • `"ec2:vpn-gateway"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
	• Instância de acesso verificado • Provedor confiável de acesso verificado • Volume • Log do fluxo da VPC • VPC • Endpoint da VPC • Serviço de VPC endpoint • Conexão de emparelhamento de VPC • VPN connection (Conexão VPN) • gateway VPN	
EC2 Lixeira da Amazon	• Regra	• `"rbin:rule"`
AWS Elastic Beanstalk	• Aplicação • Versão da aplicação • Modelo de configuração • Plataforma	• `"elasticbeanstalk:application"` • `"elasticbeanstalk:applicationversion"` • `"elasticbeanstalk:configurationtemplate"` • `"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 • Cluster • Serviço • Definição de tarefa • Conjunto de tarefas	• `"ecs:capacity-provider"` • `"ecs:cluster"` • `"ecs:service"` • `"ecs:task-definition"` • `"ecs:task-set"`
Amazon Elastic File System	• Todos • Sistema de arquivos	• `"elasticfilesystem:*"` • `"elasticfilesystem:file-system"`
Amazon Elastic Kubernetes Service	• Cluster	• `"eks:cluster"`
Amazon ElasticSearch	• Domínio	• `"es:domain"`
Amazon EMR	• Cluster • Editor	• `"elasticmapreduce:cluster"` • `"elasticmapreduce:editor"`
Amazon EMR Sem Servidor	• Aplicação	• `"emr-serverless:applications"`
AWS Resolução de entidades	• Fluxo de trabalho de correspondência • Mapeamento de esquemas	• `"entityresolution:matchingworkflow"` • `"entityresolution:schemamapping"`
Amazon ElastiCache	• Cluster	• `"elasticache:cluster"`
Amazon EventBridge	• Todos • Barramento de eventos • Regra	• `"events:*"` • `"events:event-bus"` • `"events:rule"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
Amazon EventBridge Pipes	• Barra vertical	• `"pipes:pipe"`
Amazon EventBridge Scheduler	• Grupo de agendamento	• `"scheduler:schedule-group"`
Amazon Fraud Detector	• Detector • Versão do detector • Modelo • Regra • Variável	• `"frauddetector:detector"` • `"frauddetector:detector-version"` • `"frauddetector:model"` • `"frauddetector:rule"` • `"frauddetector:variable"`
Amazon Global Accelerator	• Accelerator	• `"globalaccelerator:accelerator"`
Elastic Load Balancing	• Todos • Receptor • Regra do receptor • Load balancer • Grupo de destino	• `"elasticloadbalancing:*"` • `"elasticloadbalancing:listener"` • `"elasticloadbalancing:listener-rule"` • `"elasticloadbalancing:loadbalancer"` • `"elasticloadbalancing:targetgroup"`
Amazon FSx	• Todos • Backup • Sistema de arquivos	• `"fsx:*"` • `"fsx:backup"` • `"fsx:file-system"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
Amazon GuardDuty	• Detector • Filtro • Conjunto de IPs • Conjuntos de inteligência de ameaças	• `"guardduty:detector"` • `"guardduty:detector/filter"` • `"guardduty:detector/ipset"` • `"guardduty:detector/threatintelset"`
AWS HealthLake	• Datastore	• `"healthlake:datastore  "`
AWS HealthOmics	• Armazenamento de anotações • Versão do armazenamento de anotações • Armazenamento de referência • Referência • Executar • Grupo de execução • Armazenamento de sequências • Conjunto de leitura • Armazenamento de variantes • Fluxo de trabalho	• `"omics:annotationStore"` • `"omics:annotationStore/version"` • `"omics:referenceStore"` • `"omics:referenceStore/reference"` • `"omics:run"` • `"omics:runGroup"` • `"omics:sequenceStore"` • `"omics:sequenceStore/readSet"` • `"omics:variantStore"` • `"omics:workflow"`
Amazon Inspector	• Filtro	• `"inspector2:filter "`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
AWS Identity and Access Management	• Perfil da instância • MFA • Provedor OIDC • Política • Provedor SAML • Certificado de servidor	• `"iam:instance-profile"` • `"iam:mfa"` • `"iam:oidc-provider"` • `"iam:policy"` • `"iam:saml-provider"` • `"iam:server-certificate"`
AWS IoT Analytics	• Todos • Canal • Conjunto de dados • Datastore • Pipeline	• `"iotanalytics:*"` • `"iotanalytics:channel"` • `"iotanalytics:dataset"` • `"iotanalytics:datastore"` • `"iotanalytics:pipeline"`
AWS IoT Events	• Todos • Modelo de detector • Entrada	• `"iotevents:*"` • `"iotevents:detectorModel"` • `"iotevents:input"`
AWS IoT Fleet Hub	• Aplicação	• `"iotfleethub:application"`
AWS IoT SiteWise	• Ativo • Modelo de ativo	• `"iotsitewise:asset"` • `"iotsitewise:asset-model  "`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
AWS IoT Greengrass	• Implantação em massa • Definição do Connector • Definição principal • Definição de dispositivo • Definição de função • Definição de logger • Definição de recurso • Definição de assinatura	• `"greengrass:bulk"` • `"greengrass:connectorsDefinition"` • `"greengrass:coresDefinition"` • `"greengrass:devicesDefinition"` • `"greengrass:functionsDefinition"` • `"greengrass:loggersDefinition"` • `"greengrass:resourcesDefinition"` • `"greengrass:subscriptionsDefinition"`
AWS Key Management Service	• Todos • Chave	• `"kms:*"` • `"kms:key"`
Amazon Kinesis	• Todos • Aplicação	• `"kinesisanalytics:*"` • `"kinesisanalytics:application"`
Amazon Data Firehose	• Todos • Fluxo de entrega	• `"firehose:*"` • `"firehose:deliverystream"`
AWS Lambda	• Todos • Função	• `"lambda:*"` • `"lambda:function"`
Amazon Macie	• Identificador de dados personalizado	• `"macie2:custom-data-identifier"`
Amazon MediaStore	• Contêiner	• `"mediastore:container"`
Amazon MQ	• Agente • Configuração	• `"mq:broker"` • `"mq:configuration"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
Amazon Network Firewall	• Firewall • Política de firewall • Grupo de regras com estado • Grupo de regras sem estado	• `"network-firewall:firewall"` • `"network-firewall:firewall-policy"` • `"network-firewall:stateful-rulegroup"` • `"network-firewall:stateless-rulegroup"`
Amazon sem OpenSearch servidor	• Coleta	• `"aoss:collection"`
AWS Organizations	• Conta • Unidade Organizacional • Política • Raiz	• `"organizations:account"` • `"organizations:ou"` • `"organizations:policy"` • `"organizations:root"`
Amazon Pinpoint SMS Voice V2	• Conjunto de configurações • Lista de exclusão • Número de telefone • Grupo • ID do remetente	• `"sms-voice:configuration-set"` • `"sms-voice:opt-out-list"` • `"sms-voice:phone-number"` • `"sms-voice:pool"` • `"sms-voice:sender-id"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
Amazon RDS	• Grupo de parâmetros do cluster • Endpoint do cluster • Assinatura de eventos • Grupo de opções do banco de dados • DB parameter group (grupo de parâmetros de banco de dados) • Proxy de banco de dados • Endpoint de proxy de banco de dados • Instância de banco de dados reservada • DB security group (grupo de segurança de banco de dados) • DB subnet group (Grupo de subredes do banco de dados) • Grupo de destino	• `"rds:cluster-pg"` • `"rds:cluster-endpoint"` • `"rds:es"` • `"rds:og"` • `"rds:pg"` • `"rds:db-proxy"` • `"rds:db-proxy-endpoint"` • `"rds:ri"` • `"rds:secgrp"` • `"rds:subgrp"` • `"rds:target-group"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
Amazon Redshift	• Todos • Cluster • Assinatura de eventos • Certificado do cliente HSM • Configuração de HSM • Grupo de parâmetros • Snapshot • Concessão de cópia de snapshot • Programação de snapshots. • Grupo de sub-rede	• `"redshift:*"` • `"redshift:cluster"` • `"redshift:eventsubscription"` • `"redshift:hsmclientcertificate"` • `"redshift:hsmconfiguration"` • `"redshift:parametergroup"` • `"redshift:snapshot"` • `"redshift:snapshotcopygrant"` • `"redshift:snapshotschedule"` • `"redshift:subnetgroup"`
Amazon Redshift sem servidor	• Namespace • WorkGroup	• `"redshift-serverless:namespace"` • `"redshift-serverless:workgroup"`
AWS Resource Access Manager	• Todos • Compartilhamento de recursos	• `"ram:*"` • `"ram:resource-share"`
AWS Resource Groups	• Todos • Grupo	• `"resource-groups:*"` • `"resource-groups:group"`
Amazon Route 53	• Zona hospedada	• `"route53:hostedzone"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
Amazon Route 53 Resolver	• Todos • Endpoint do resolvedor • Regra do resolvedor	• `"route53resolver:*"` • `"route53resolver:resolver-endpoint"` • `"route53resolver:resolver-rule"`
Amazon S3	• Bucket • Storage Lens • Grupos da Lente de Armazenamento	• `"s3:bucket"` • `"s3:storage-lens"` • `"s3:storage-lens-group"`
SageMaker IA da Amazon	• Config de imagem de aplicativo • Artifact • Contexto • Trabalho de treinamento • Processamento de trabalho • Grupo de pacotes modelo • UI de tarefa humana • Pacote de modelos • Ação • Pipeline • Experimento • Definição de fluxo • Projeto	• `"sagemaker:app-image-config"` • `"sagemaker:artifact"` • `"sagemaker:context"` • `"sagemaker:training-job"` • `"sagemaker:processing-job "` • `"sagemaker:model-package-group"` • `"sagemaker:human-task-ui"` • `"sagemaker:model-package"` • `"sagemaker:action"` • `"sagemaker:pipeline"` • `"sagemaker:experiment"` • `"sagemaker:flow-definition"` • `"sagemaker:project"`
AWS Secrets Manager	• Todos • Secreta	• `"secretsmanager:*"` • `"secretsmanager:secret"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
AWS Lago de Segurança	• Data lake • Assinante	• `"securitylake:data-lake"` • `"securitylake:subscriber"`
AWS Service Catalog	• Aplicação • Grupo de atributos • Portfólio • Produto	• `"servicecatalog:applications"` • `"servicecatalog:attribute-groups "` • `"catalog:portfolio "` • `"catalog:product "`
Amazon Simple Notification Service (SNS)	• Tópico	• `"sns:topic"`
Amazon Simple Queue Service (SQS)	• Fila	• `"sqs:queue"`
Amazon States Language	• Todos • Atividade • State Machine (Máquina de estado)	• `"states:*"` • `"states:activity "` • `"states:stateMachine  "`
AWS Step Functions	• Atividade	• `"states:activity"`
AWS Storage Gateway	• Todos • Gateway • Compartilhar • Fita • Volume	• `"storagegateway:*"` • `"storagegateway:gateway"` • `"storagegateway:share"` • `"storagegateway:tape"` • `"storagegateway:gateway/volume"`

Nome do serviço	Tipo de recurso	Sintaxe do JSON
AWS Systems Manager	• Associação • Execução de automação • Documento • Janela de manutenção • Instância gerenciada • Item de ops • Lista de referência de patches • Contatos	• `"ssm:association"` • `"ssm:automation-execution"` • `"ssm:document"` • `"ssm:maintenancewindow"` • `"ssm:managed-instance"` • `"ssm:opsitem"` • `"ssm:patchbaseline"` • `"ssm-contacts:contact"`
Amazon Textract	• Adaptadores • Versões	• `"textract:adapters"` • `"textract:adapters/versions"`
AWS Transfer Family	• Servidor • Usuário • Fluxo de trabalho	• `"transfer:server"` • `"transfer:user"` • `"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 • Alias de conexão • Diretório • WorkSpace • WorkSpaces pacote • WorkSpaces imagem • WorkSpaces Grupo IP	• `"workspaces:*"` • `"workspaces:connectionalias"` • `"workspaces:directory"` • `"workspaces:workspace"` • `"workspaces:workspacebundle"` • `"workspaces:workspaceimage"` • `"workspaces:workspaceipgroup"`

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. O valor da política diferencia maiúsculas de 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.

O exemplo de política de tags especifica que a `CostCenter` tag transmitida a todos os AWS Secrets Manager recursos deve estar em conformidade com essa política.

> **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.

AWS recomenda que você use esse exemplo como um guia para criar uma política de tag semelhante para as chaves de tag que você 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 em vigor, 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 do 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 Oeste dos EUA (N. da Califórnia)	us-west-1
Região Oeste dos EUA (Oregon)	us-west-2
Região África (Cidade do Cabo)[2]	af-south-1
Região Ásia-Pacífico (Hong Kong)[2]	ap-east-1

Nome da região	Parâmetro da região
Região Ásia-Pacífico (Mumbai)	`ap-south-1`
Asia Pacific (Hyderabad)[2]	`ap-south-2`
Região Ásia-Pacífico (Tóquio)	`ap-northeast-1`
Região Ásia-Pacífico (Seul)	`ap-northeast-2`
Região Ásia-Pacífico (Osaka)	`ap-northeast-3`
Região Ásia-Pacífico (Singapura)	`ap-southeast-1`
Região Ásia-Pacífico (Sydney)	`ap-southeast-2`
Região Ásia-Pacífico (Jacarta)[2]	`ap-southeast-3`
Região Ásia-Pacífico (Malásia)	`ap-southeast-5`
Ásia-Pacífico (Melbourne)[2]	`ap-southeast-4`
Ásia-Pacífico (Tailândia)	`ap-southeast-7`
Região Canadá (Central)	`ca-central-1`
Oeste do Canadá (Calgary)[2]	`ca-west-1`
Região da China (Pequim)	`cn-north-1`
Região da China (Ningxia)	`cn-northwest-1`
Região Europa (Frankfurt)	`eu-central-1`
Região Europa (Zurique)[2]	`eu-central-2`
Região Europa (Milão)	`eu-south-1`
Europa (Espanha)[2]	`eu-south-2`
Região Europa (Irlanda)	`eu-west-1`

Nome da região	Parâmetro da região
Região Europa (Londres)	`eu-west-2`
Região Europa (Paris)	`eu-west-3`
Região Europa (Estocolmo)	`eu-north-1`
Região México (Centro)	`mx-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`
AWS GovCloud Região (Leste dos EUA)	`us-gov-east-1`
AWS GovCloud Região (Oeste dos EUA)	`us-gov-west-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
- 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 como habilitar e desabilitar Regiões da AWS, consulte Especificar qual Regiões da AWS sua conta pode usar no Guia de referência de gerenciamento de conta da AWS . O console do Resource Groups não está disponível nessas regiões.

Políticas de aplicativos de bate-papo

As políticas de aplicativos de bate-papo AWS Organizations permitem que você controle o acesso às contas da sua organização a partir de aplicativos de bate-papo, como Slack e Microsoft Teams.

O Amazon Q Developer em aplicativos de bate-papo é um AWS serviço que permite DevOps que equipes de desenvolvimento de software usem salas de bate-papo de programas de mensagens para monitorar e responder a eventos operacionais em seus Nuvem AWS. O Amazon Q Developer em aplicativos de bate-papo processa AWS service (Serviço da AWS) notificações do Amazon Simple Notification Service (Amazon SNS) e as encaminha para salas de bate-papo para que as equipes possam analisá-las e agir imediatamente, independentemente da localização.

Como as políticas de aplicativos de bate-papo funcionam

Usando políticas de aplicativos de bate-papo, a conta de gerenciamento ou o administrador delegado de uma organização pode fazer o seguinte em toda a organização:

- Determinar quais aplicações de bate-papo compatíveis (Amazon Chime, Microsoft Teams e Slack) podem ser usadas.
- Restringir o acesso do cliente de bate-papo a espaços de trabalho específicos (Slack) e equipes (Microsoft Teams).
- Restringir a visibilidade do canal do Slack a canais públicos ou privados.
- Definir e aplicar configurações de função específicas.

As políticas de aplicativos de bate-papo restringem e têm precedência sobre as configurações no nível da conta, como configurações de função e políticas de proteção de canais. Você pode acessar e modificar as políticas de aplicativos de bate-papo do Amazon Q Developer em aplicativos de bate-papo ou no console Organizations.

Depois que as políticas forem anexadas às contas e unidades organizacionais (OU), as configurações atuais e futuras de aplicativos de bate-papo do Amazon Q Developer para as contas no escopo cumprirão automaticamente as configurações de governança e permissões. Para obter mais informações, consulte Entendendo a herança da política de gerenciamento.

Se você tentar realizar uma ação restrita por uma política de aplicativos de bate-papo, uma mensagem de erro o notificará de que a ação não é permitida devido à política de aplicativos de bate-papo com a recomendação de entrar em contato com a conta de gerenciamento ou com o administrador delegado da sua organização.

> **Note**
>
> As políticas de aplicativos de bate-papo são validadas em tempo de execução. Isso significa que os recursos existentes são continuamente verificados quanto à conformidade. Não há sobreposição com as permissões existentes do IAM, pois as permissões do IAM baseadas em tempo de execução para enviar notificações ou interagir com o Amazon Q Developer em aplicativos de bate-papo não são suportadas atualmente.

Introdução às políticas de aplicativos de bate-papo

Siga estas etapas para começar a usar as políticas de aplicativos de bate-papo.

1. Saiba mais sobre as permissões que você deve ter para realizar tarefas de política de aplicativos de bate-papo.
2. Ative as políticas de aplicativos de bate-papo para sua organização.
3. Crie uma política de aplicativos de bate-papo.
4. Anexe a política de aplicativos de bate-papo à raiz, UO ou conta da sua organização.
5. Veja a política combinada de aplicativos de bate-papo eficazes 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 a sintaxe da política de aplicativos de bate-papo e veja exemplos de políticas

Sintaxe e exemplos de políticas de aplicativos de bate-papo

Este tópico descreve a sintaxe da política de aplicativos de bate-papo e fornece exemplos.

Sintaxe para políticas de aplicativos de bate-papo

Uma política de aplicativos de bate-papo é um arquivo de texto simples estruturado de acordo com as regras do JSON. A sintaxe das políticas de aplicativos de bate-papo segue a sintaxe dos tipos de políticas 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 aplicativos de bate-papo.

O exemplo a seguir mostra a sintaxe básica de uma política de aplicativos de bate-papo:

```
{
    "chatbot":{
       "platforms":{
          "slack":{
             "client":{
                "@@assign":"enabled" // enabled | disabled
             },
             "workspaces": { // limit 255
                   "@@assign":[
                      "Slack-Workspace-Id"
                   ]
             },
             "default":{
                "supported_channel_types":{
                   "@@assign":[
                      "private" // public | private
                   ]
                },
                "supported_role_settings":{
                   "@@assign":[
                      "user_role" // user_role | channel_role
                   ]
                }
             },
```

```
            "overrides":{ // limit 255
               "Slack-Workspace-Id":{
                  "supported_channel_types":{
                     "@@assign":[
                        "public" // public | private
                     ]
                  },
                  "supported_role_settings":{
                     "@@assign":[
                        "user_role" // user_role | channel_role
                     ]
                  }
               }
            }
         },
         "microsoft_teams":{
            "client":{
               "@@assign":"enabled"
            },
            "tenants":{ // limit 36
               "Microsoft-Teams-Tenant-Id":{ // limit 36
                  "@@assign":[
                     "Microsoft-Teams-Team-Id"
                  ]
               }
            },
            "default":{
               "supported_role_settings":{
                  "@@assign":[
                     "user_role" // user_role | channel_role
                  ]
               }
            },
            "overrides":{ // limit 36
               "Microsoft-Teams-Tenant-Id":{ // limit 36
                  "Microsoft-Teams-Team-Id":{
                     "supported_role_settings":{
                        "@@assign":[
                           "user_role" // user_role | channel_role
                        ]
                     }
                  }
               }
            }
```

```
          },
          "chime":{
            "client":{
               "@@assign":"disabled" // enabled | disabled
            }
         }
      },
      "default":{
         "client":{
            "@@assign":"disabled" // enabled | disabled
         }
      }
   }
}
```

Essa política de aplicativos de bate-papo inclui os seguintes elementos:

- O nome da chave de campo `chatbot`. As políticas de aplicativos de bate-papo sempre começam com esse nome de chave fixo. É a linha superior nesta política de exemplo.
- Abaixo de `chatbot`, há um bloco de `platforms` que contém a configuração das diferentes aplicações de bate-papo compatíveis: Slack, Microsoft Teams e Amazon Chime.
  - Para o Slack, os seguintes campos estão disponíveis:
    - `"client"`:
      - `"enabled"`: o cliente do Slack está habilitado. Integrações com o Slack são permitidas.
      - `"disabled"`: o cliente do Slack está desabilitado. Integrações com o Slack não são permitidas.
    - `"workspaces"`: lista separada por vírgula dos espaços de trabalho permitidos do Slack. Neste exemplo, os espaços de trabalho permitidos do Slack são e. *`Slack-Workspace-Id1`* *`Slack-Workspace-Id2`*
    - `"default"`: as configurações padrão dos espaços de trabalho do Slack.
      - `"supported_channel_types"`:
        - `"public"`: os espaços de trabalho do Slack no escopo permitem canais públicos do Slack por padrão.
        - `"private"`: os espaços de trabalho do Slack no escopo permitem canais privados do Slack por padrão.
      - `supported_role_settings`:

        - `"user_role"`: os espaços de trabalho do Slack no escopo permitem perfis do IAM em nível de usuário por padrão.
        - `"channel_role"`: os espaços de trabalho do Slack no escopo permitem perfis de IAM em nível de canal por padrão.
    - `"overrides"`: as configurações de substituição dos espaços de trabalho do Slack.
        - *`Slack-Workspace-Id2`*: lista separada por vírgula dos espaços de trabalho do Slack aos quais a configuração de substituição se aplica. Neste exemplo, o espaço de trabalho do Slack é. *`Slack-Workspace-Id2`*
            - `"supported_channel_types"`:
                - `"public"`: substituir a configuração se os espaços de trabalho do Slack no escopo permitirem canais públicos do Slack.
                - `"private"`: substituir a configuração se os espaços de trabalho do Slack no escopo permitirem canais privados do Slack.
            - `supported_role_settings`:
                - `"user_role"`: substituir a configuração se os espaços de trabalho do Slack no escopo permitirem perfis do IAM em nível de usuário.
                - `"channel_role"`: substituir a configuração se os espaços de trabalho do Slack no escopo permitirem perfis do IAM no nível do canal.
- Para o Microsoft Teams, os seguintes campos estão disponíveis:
    - `"client"`:
        - `"enabled"`: o cliente do Microsoft Teams está habilitado. Integrações com o Microsoft Teams são permitidas.
        - `"disabled"`: o cliente do Microsoft Teams está desabilitado. Integrações com o Microsoft Teams não são permitidas.
    - `"tenants"`: lista separada por vírgula dos locatários permitidos do Microsoft Teams. Neste exemplo, o inquilino permitido é*`Microsoft-Teams-Tenant-Id`*.
        - *`Microsoft-Teams-Tenant-Id`*: lista separada por vírgulas de equipes dentro do locatário. Neste exemplo, a equipe permitida é*`Microsoft-Teams-Team-Id`*.
    - `"default"`: as configurações padrão para as equipes dentro do locatário.
        - `supported_role_settings`:
            - `"user_role"`: as equipes no escopo permitem perfis do IAM em nível de usuário por padrão.

        - `"channel_role"`: as equipes no escopo permitem perfis do IAM em nível de canal por padrão.
    - `"overrides"`: as configurações de substituição para os locatários do Microsoft Teams.
      - *`Microsoft-Teams-Tenant-Id`*: lista separada por vírgula dos locatários aos quais a configuração de substituição se aplica. Neste exemplo, o inquilino é*`Microsoft-Teams-Tenant-Id`*.
        - *`Microsoft-Teams-Team-Id`*: lista separada por vírgula das equipes do locatário. Neste exemplo, a equipe permitida é*`Microsoft-Teams-Team-Id`*.
          - `supported_role_settings`:
            - `"user_role"`: substituir a configuração se as equipes no escopo permitirem perfis do IAM em nível de usuário.
            - `"channel_role"`: substituir a configuração se as equipes no escopo permitirem perfis do IAM em nível de canal.
  - Para o Amazon Chime, os seguintes campos estão disponíveis:
    - `"client"`:
      - `"enabled"`: o cliente do Amazon Chime está habilitado. Integrações com o Amazon Chime são permitidas.
      - `"disabled"`: o cliente do Amazon Chime está desabilitado. Integrações com o Amazon Chime não são permitidas.
- Abaixo`chatbot`, há um `default` bloco que desativa o Amazon Q Developer em aplicativos de bate-papo em toda a organização, a menos que seja substituído em um nível inferior. Esse padrão também desativa qualquer novo aplicativo de bate-papo suportado pelo Amazon Q Developer em aplicativos de bate-papo. Por exemplo, se o Amazon Q Developer em aplicativos de bate-papo oferecer suporte a um novo aplicativo de bate-papo, esse padrão também desabilita esse aplicativo de bate-papo recém-suportado.

> **Note**
>
> Para obter mais informações sobre funções do IAM em nível de canal e funções de IAM em nível de usuário, consulte Entendendo as permissões do Amazon Q Developer em aplicativos de chat no Guia do administrador do Amazon Q Developer em aplicativos de bate-papo.

Exemplos de políticas de aplicativos de bate-papo

As políticas de exemplo a seguir são apenas para fins informativos.

Exemplo 1: permitir somente canais privados do Slack em um espaço de trabalho específico, desabilitar o Microsoft Teams, todos os modos de autenticação são compatíveis

A política a seguir se concentra em controlar as configurações permitidas para as integrações de chatbots do Slack e do Microsoft Teams.

```
{
   "chatbot": {
      "platforms": {
         "slack": {
            "client": {
               "@@assign": "enabled"
            },
            "workspaces": {
               "@@assign": [
                  "Slack-Workspace-Id"
               ]
            },
            "default": {
               "supported_channel_types": {
                  "@@assign": [
                     "private"
                  ]
               },
               "supported_role_settings": {
                  "@@assign": [
                     "channel_role",
                     "user_role"
                  ]
               }
            }
         },
         "microsoft_teams": {
            "client": {
               "@@assign": "disabled"
            }
         },
         "chime":{
            "client":{
```

```
                "@@assign":"disabled"
            }
         },
         "default":{
            "client":{
               "@@assign":"disabled"
            }
         }
      }
   }
}
```

Para Slack

- O cliente do Slack está habilitado.
- Somente o espaço de trabalho específico do Slack *`Slack-Workspace-Id`* é permitido.
- As configurações padrão são permitir somente canais privados do Slack, perfis do IAM no nível do canal e perfis do IAM no nível do usuário.

Para o Microsoft Teams

- O cliente do Microsoft Teams está desabilitado.

Para o Amazon Chime

- O cliente do Amazon Chime está desabilitado.

Outros detalhes

- O `default` bloco na parte inferior define que o cliente seja desativado, o que desativa o Amazon Q Developer em aplicativos de bate-papo em toda a organização, a menos que seja substituído em um nível inferior. Esse padrão também desativa qualquer novo aplicativo de bate-papo suportado pelo Amazon Q Developer em aplicativos de bate-papo. Por exemplo, se o Amazon Q Developer em aplicativos de bate-papo oferecer suporte a um novo aplicativo de bate-papo, esse padrão também desabilita esse aplicativo de bate-papo recém-suportado.

Exemplo 2: permitir apenas integrações do Slack com perfis do IAM de nível de usuário

A política a seguir adota uma abordagem mais permissiva ao Slack, permitindo todos os espaços de trabalho do Slack, mas restringindo o modo de autenticação somente aos perfis do IAM em nível de usuário.

```
{
   "chatbot":{
      "platforms":{
         "slack":{
            "client":{
               "@@assign":"enabled"
            },
            "workspaces":
               {
                  "@@assign":[
                     "*"
                  ]
               },
            "default":{
               "supported_role_settings":{
                  "@@assign":[
                     "user_role"
                  ]
               }
            }
         },
         "microsoft_teams":{
            "client":{
               "@@assign":"disabled"
            }
         },
         "chime":{
            "client":{
               "@@assign":"disabled"
            }
         }
      },
      "default":{
         "client":{
            "@@assign":"disabled"
         }
      }
```

```
    }
}
```

Para o Slack

- O cliente do Slack está habilitado.
- Nenhum espaço de trabalho específico do Slack é definido usando o caractere curinga `"*"`; portanto, todos os espaços de trabalho são permitidos.
- As configurações padrão são permitir somente perfis do IAM em nível de usuário.

Para o Microsoft Teams

- O cliente do Microsoft Teams está desabilitado.

Para o Amazon Chime

- O cliente do Amazon Chime está desabilitado.

Outros detalhes

- O `default` bloco na parte inferior define que o cliente seja desativado, o que desativa o Amazon Q Developer em aplicativos de bate-papo em toda a organização, a menos que seja substituído em um nível inferior. Esse padrão também desativa qualquer novo aplicativo de bate-papo suportado pelo Amazon Q Developer em aplicativos de bate-papo. Por exemplo, se o Amazon Q Developer em aplicativos de bate-papo oferecer suporte a um novo aplicativo de bate-papo, esse padrão também desabilita esse aplicativo de bate-papo recém-suportado.

Exemplo 3: permitir somente integrações do Microsoft Teams em locatários específicos

O exemplo de política a seguir bloqueia a organização para permitir apenas integrações de chatbot do Microsoft Teams dentro do locatário especificado, enquanto bloqueia completamente as integrações do Slack.

```
{
   "chatbot":{
      "platforms":{
         "slack":{
            "client": {
```

```
                "@@assign": "disabled"
            },
         },
         "microsoft_teams":{
            "client": {
               "@@assign": "enabled"
            },
            "tenants":{
               "Microsoft-Teams-Tenant-Id":{
                  "@@assign":[
                     "*"
                  ]
               }
            }
         },
         "chime": {
            "client":{
               "@@assign": "disabled"
            }
         }
      }
   }
}
```

Para o Slack

- O cliente do Slack está desabilitado.

Para o Microsoft Teams

- Somente o inquilino específico *Microsoft-Teams-Tenant-Id* é permitido, usando o curinga "*" para permitir todas as equipes desse inquilino.

Para o Amazon Chime

- O cliente do Amazon Chime está desabilitado.

Outros detalhes

- O `default` bloco na parte inferior define que o cliente seja desativado, o que desativa o Amazon Q Developer em aplicativos de bate-papo em toda a organização, a menos que seja substituído

em um nível inferior. Esse padrão também desativa qualquer novo aplicativo de bate-papo suportado pelo Amazon Q Developer em aplicativos de bate-papo. Por exemplo, se o Amazon Q Developer em aplicativos de bate-papo oferecer suporte a um novo aplicativo de bate-papo, esse padrão também desabilita esse aplicativo de bate-papo recém-suportado.

Exemplo 4: Permite o acesso restrito do Amazon Q Developer em aplicativos de bate-papo aos espaços de trabalho do Slack e a um inquilino do Microsoft Teams

A política a seguir permite o acesso restrito do Amazon Q Developer em aplicativos de bate-papo a espaços de trabalho selecionados do Slack e a um inquilino do Microsoft Teams.

```
{
    "chatbot":{
       "platforms":{
          "slack":{
             "client":{
                "@@assign":"enabled"
             },
             "workspaces": {
                   "@@assign":[
                      "Slack-Workspace-Id1",
                      "Slack-Workspace-Id2"
                   ]
             },
             "default":{
                "supported_channel_types":{
                   "@@assign":[
                      "private"
                   ]
                },
                "supported_role_settings":{
                   "@@assign":[
                      "user_role"
                   ]
                }
             },
             "overrides":{
                "Slack-Workspace-Id2":{
                   "supported_channel_types":{
                      "@@assign":[
                         "public",
                         "private"
```

```
                    ]
                },
                "supported_role_settings":{
                    "@@assign":[
                        "channel_role",
                        "user_role"
                    ]
                }
            }
        },
        "microsoft_teams":{
            "client":{
                "@@assign":"enabled"
            },
            "tenants":{
                "Microsoft-Teams-Tenant-Id":{
                    "@@assign":[
                        "Microsoft-Teams-Team-Id"
                    ]
                }
            },
            "default":{
                "supported_role_settings":{
                    "@@assign":[
                        "user_role"
                    ]
                }
            },
            "overrides":{
                "Microsoft-Teams-Tenant-Id":{
                    "Microsoft-Teams-Team-Id":{
                        "supported_role_settings":{
                            "@@assign":[
                                "channel_role",
                                "user_role"
                            ]
                        }
                    }
                }
            }
        },
        "default":{
```

```
          "client":{
             "@@assign":"disabled"
          }
       }
    }
}
```

Para o Slack

- O cliente do Slack está habilitado.
- Os espaços de trabalho permitidos do Slack são e. *Slack-Workspace-Id1* *Slack-Workspace-Id2*
- As configurações padrão do Slack são permitir apenas canais privados e perfis do IAM em nível de usuário.
- Há uma substituição para o espaço de trabalho *Slack-Workspace-Id2* que permite canais públicos e privados, bem como funções do IAM em nível de canal e funções de IAM em nível de usuário.

Para o Microsoft Teams

- O Microsoft Teams está habilitado.
- Os inquilinos permitidos do Teams estão *Microsoft-Teams-Tenant-Id* com a equipe*Microsoft-Teams-Team-Id*.
- As configurações padrão são para permitir somente perfis do IAM em nível de usuário.
- Há uma substituição para o locatário *Microsoft-Teams-Tenant-Id* que permite funções de IAM em nível de canal e funções de IAM em nível de usuário para a equipe. *Microsoft-Teams-Team-Id*

Outros detalhes

- O `default` bloco na parte inferior define que o cliente seja desativado, o que desativa o Amazon Q Developer em aplicativos de bate-papo em toda a organização, a menos que seja substituído em um nível inferior. Isso significa que o Amazon Chime está desabilitado neste exemplo. Esse padrão também desativa qualquer novo aplicativo de bate-papo suportado pelo Amazon Q Developer em aplicativos de bate-papo. Por exemplo, se o Amazon Q Developer em aplicativos de bate-papo oferecer suporte a um novo aplicativo de bate-papo, esse padrão também desabilita esse aplicativo de bate-papo recém-suportado.

Políticas de recusa de serviços de IA

As políticas de exclusão de serviços de IA permitem que você controle a coleta de dados para serviços de AWS IA em todas as contas de uma organização.

AWS Os serviços de IA podem usar e armazenar o conteúdo do cliente para melhorar o serviço. A melhoria do serviço é o uso e o armazenamento de conteúdo que não são dados pessoais para desenvolver, aprimorar AWS e afiliar tecnologias de aprendizado de máquina e inteligência artificial. Para esse fim, podemos armazenar conteúdo Região da AWS fora de Região da AWS onde você está usando o serviço. Como AWS cliente, você pode optar por não ter seu conteúdo usado para melhorias no serviço a qualquer momento.

Você pode criar políticas de exclusão para um serviço de IA individual ou para todos os serviços suportados pelas políticas de exclusão de serviços de IA. Você também pode consultar a política efetiva aplicável a cada conta para ver os efeitos de suas escolhas de configuração.

Para obter informações mais detalhadas, consulte Serviços AWS de Machine Learning e Inteligência Artificial nos Termos AWS de Serviço. Para ver uma lista dos serviços suportados pelas políticas de exclusão de serviços de IA, consulte Lista de serviços de IA compatíveis.

Tópicos

Considerações ao usar políticas de recusa de serviços de IA

A recusa exclui todo o conteúdo histórico associado

Quando você desativa o uso do conteúdo por um serviço de AWS IA, esse serviço exclui todo o conteúdo histórico associado com o qual foi compartilhado AWS antes de você definir a opção. Essa exclusão limita-se a dados armazenados que não são necessários para fornecer funções de serviço.

Por exemplo, você usa um serviço enquanto aceitou os termos. Esse serviço pode armazenar cópias do seu conteúdo para melhorar o serviço. Você opta pela recusa. Todas as cópias que foram armazenadas pelo serviço para aprimoramento do serviço são excluídas, mas os dados usados para fornecer o serviço a você não são.

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. Saiba mais sobre as permissões que você deve ter para executar qualquer tarefas de política de backup.
2. Habilitar políticas de exclusão dos serviços de IA para sua organização.
3. Criar uma política de exclusão dos serviços de IA.
4. Anexe a política de exclusão dos serviços de IA à raiz, UO ou conta da sua organização.
5. Visualize a política combinada de exclusão dos serviços de IA em vigor que se aplica a uma conta.

Em todas essas etapas, você faz login como usuário AWS Identity and Access Management (IAM), assume uma função do IAM ou faz 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

Recusar todos os serviços de AWS IA compatíveis

Neste tópico:

- Você pode recusar com a seleção de um botão no AWS Organizations console do.
- Você pode recusar vinculando a política de exemplo fornecida usando a AWS CLI e AWS SDKs.
- Você pode ver uma lista dos Serviços da AWS compatíveis com a política de recusa de serviços de IA.

Recusar todos os serviços de IA compatíveis

Você pode recusar que o conteúdo de sua organização seja usado para melhoria de serviços criando e vinculando uma política de recusa de serviços de IA. Essa política se aplica a todos os serviços de AWS IA da com suporte atual e futuro. As contas-membro não podem atualizar a política.

AWS Management Console

Para recusar todos os 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, selecione Opt out from all services.
3. Na página de confirmação Opt out from all services, selecione Opt out from all services.

AWS CLI & AWS SDKs

Para recusar todos os serviços de IA

1. Cópia do “exemplo 1: excluir todos os serviços de IA para todas as contas da organização” nos exemplos de recusa de serviços de IA.
2. Siga as instruções em Vinculação e desvinculação da recusa de serviços de IA.

> **Note**
>
> Etapas adicionais são necessárias para optar por não usar o Amazon Monitron. Para obter mais informações, consulte os Termos de Serviço da AWS.

Lista dos serviços abrangidos pela política de recusa de serviços de IA

Veja a seguir uma lista dos Serviços da AWS compatíveis com a política de recusa de serviços de IA:

- Operações de IA da Amazon
- Analytics de voz do SDK do Amazon Chime
- Amazon CloudWatch
- Amazon CodeGuru Profiler
- Amazon CodeWhisperer (agora parte do Amazon Q Developer)
- Amazon Comprehend
- Amazon Connect
- Otimização do Amazon Connect

- Amazon Connect Contact Lens
- AWS Database Migration Service
- Amazon DataZone
- AWS Entity Resolution
- Amazon Fraud Detector
- AWS Glue
- Amazon GuardDuty
- Amazon Lex
- Amazon Polly
- Amazon Q
- Amazon QuickSight
- Amazon Rekognition
- Amazon Security Lake
- Cadeia de Suprimentos AWS
- Amazon Textract
- Amazon Transcribe
- AWS Transform (Transformar)
- Amazon Translate

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 contas OUs ou diretamente a elas 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.
    - `aiops`
    - `awssupplychain`
    - `chimesdkvoiceanalytics`
    - `cloudwatch`
    - `codeguruprofiler`
    - `codewhisperer`
    - `comprehend`

- `connectamd`
- `connectoptimization`
- `contactlens`
- `datazone`
- `dms`
- `entityresolution`
- `frauddetector`
- `glue`
- `guardduty`
- `lex`
- `polly`
- `q`
- `quicksightq`
- `rekognition`
- `securitylake`
- `textract`
- `transcribe`
- `transform`
- `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 em vigor resultante para a Conta da AWS é que a conta opta pela inclusão apenas para o Amazon Lex, e opta pela exclusão para todos os outros serviços de AWS IA da por causa da configuração da `default` opção por exclusão herdada da política superior.

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 OUs ou contas.

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Políticas do Security Hub

AWS Security Hub as políticas fornecem às equipes de segurança uma abordagem centralizada para gerenciar as configurações de segurança em todos os seus. AWS Organizations Ao aproveitar essas políticas, você pode estabelecer e manter controles de segurança consistentes por meio de um mecanismo de configuração central. Essa integração permite que você resolva as lacunas de cobertura de segurança criando políticas alinhadas aos requisitos de segurança da sua organização e aplicando-as centralmente em todas as contas e unidades organizacionais ()OUs.

As políticas do Security Hub são totalmente integradas AWS Organizations, permitindo que contas de gerenciamento ou administradores delegados definam e apliquem configurações de segurança. Quando as contas ingressam na sua organização, elas herdam automaticamente as políticas aplicáveis com base em sua localização na hierarquia organizacional. Isso garante que seus padrões

de segurança sejam aplicados de forma consistente à medida que sua organização cresce. As políticas respeitam as estruturas organizacionais existentes e oferecem flexibilidade na forma como as configurações de segurança são distribuídas, mantendo o controle central sobre as configurações críticas de segurança.

Principais atributos e benefícios

As políticas do Security Hub fornecem um conjunto abrangente de recursos que ajudam você a gerenciar e aplicar configurações de segurança em toda a organização AWS . Esses recursos simplificam o gerenciamento de segurança e, ao mesmo tempo, garantem um controle consistente sobre seu ambiente de várias contas.

- Ative centralmente o Security Hub em todas as contas e regiões da sua organização
- Crie políticas de segurança que definam sua configuração de segurança em todas as contas e OUs
- Aplique automaticamente as configurações de segurança às novas contas quando elas ingressarem na sua organização
- Garanta configurações de segurança consistentes em toda a sua organização
- Impedir que as contas dos membros modifiquem as configurações de segurança no nível da organização

Quais são as políticas do Security Hub?

As políticas do Security Hub são AWS Organizations políticas que fornecem controle centralizado sobre as configurações de segurança nas contas da sua organização. Essas políticas funcionam perfeitamente AWS Organizations para ajudá-lo a estabelecer e manter padrões de segurança consistentes em todo o seu ambiente de várias contas.

Ao implementar as políticas do Security Hub, você ganha a capacidade de definir configurações de segurança específicas que se propagam automaticamente pela sua organização. Isso garante que todas as contas, inclusive as recém-criadas, estejam alinhadas aos requisitos de segurança e às melhores práticas da sua organização.

Essas políticas também ajudam você a manter a conformidade, aplicando controles de segurança consistentes e impedindo que contas individuais modifiquem as configurações de segurança no nível da organização. Essa abordagem centralizada reduz significativamente a sobrecarga administrativa do gerenciamento de configurações de segurança em ambientes grandes e complexos. AWS

Como as políticas do Security Hub funcionam

Quando você anexa uma política do Security Hub à sua organização ou unidade organizacional, avalia AWS Organizations automaticamente a política e a aplica com base no escopo definido. O processo de aplicação da política segue regras específicas de resolução de conflitos:

Quando as regiões aparecem nas listas de ativação e desativação, a configuração de desativação tem precedência. Por exemplo, se uma região estiver listada nas configurações de ativação e desativação, o Security Hub será desativado nessa região.

Quando `ALL_SUPPORTED` é especificado para ativação, o Security Hub é ativado em todas as regiões atuais e futuras, a menos que seja explicitamente desativado. Isso permite que você mantenha uma cobertura de segurança abrangente à medida que AWS se expande para novas regiões.

As políticas secundárias podem modificar as configurações da política principal usando operadores de herança, permitindo um controle granular em diferentes níveis organizacionais. Essa abordagem hierárquica garante que unidades organizacionais específicas possam personalizar suas configurações de segurança enquanto mantêm os controles básicos.

Terminologia

Este tópico usa os seguintes termos ao discutir as políticas do Security Hub.

Terminologia da política do Security Hub

Prazo	Definição
Política eficaz	A política final que se aplica a uma conta depois de combinar todas as políticas herdadas.
Herança de política	O processo pelo qual as contas herdam políticas das unidades organizac ionais principais.
Administrador delegado	Uma conta designada para gerenciar as políticas do Security Hub em nome da organização.
Perfil vinculado a serviço	Uma função do IAM que permite que o Security Hub interaja com outros AWS serviços.

Casos de uso das políticas do Security Hub

As políticas do Security Hub abordam desafios comuns de gerenciamento de segurança em ambientes com várias contas. Os casos de uso a seguir demonstram como as organizações normalmente implementam essas políticas para aprimorar sua postura de segurança.

Exemplo de caso de uso: requisitos regionais de conformidade

Uma empresa multinacional precisa de diferentes configurações do Security Hub para diferentes regiões geográficas. Eles criam uma política principal que habilita o Security Hub em todas as regiões usando e`ALL_SUPPORTED`, em seguida, usam políticas secundárias para desabilitar regiões específicas onde diferentes controles de segurança são necessários. Isso permite que eles mantenham a conformidade com os regulamentos regionais e, ao mesmo tempo, garantam uma cobertura de segurança abrangente.

Exemplo de caso de uso: padrões de segurança da equipe de desenvolvimento

Uma organização de desenvolvimento de software implementa políticas do Security Hub que permitem o monitoramento nas regiões de produção e, ao mesmo tempo, mantêm as regiões de desenvolvimento sem gerenciamento. Eles usam listas de regiões explícitas em suas políticas, em vez de `ALL_SUPPORTED` manter um controle preciso sobre a cobertura do monitoramento de segurança. Essa abordagem permite que eles apliquem controles de segurança mais rígidos em ambientes de produção e, ao mesmo tempo, mantenham a flexibilidade nas áreas de desenvolvimento.

Herança e aplicação de políticas

Entender como as políticas são herdadas e aplicadas é crucial para o gerenciamento eficaz da segurança em toda a organização. O modelo de herança segue a AWS Organizations hierarquia, garantindo uma aplicação previsível e consistente da política.

- As políticas anexadas no nível raiz se aplicam a todas as contas
- As contas herdam políticas de suas unidades organizacionais principais
- Várias políticas podem ser aplicadas a uma única conta
- Políticas mais específicas (mais próximas da conta na hierarquia) têm precedência

Validação de políticas

Ao criar políticas do Security Hub, as seguintes validações ocorrem:

- Os nomes das regiões devem ser identificadores de AWS região válidos
- As regiões devem ser suportadas pelo Security Hub
- A estrutura da política deve seguir as regras AWS Organizations de sintaxe da política
- Ambas `enable_in_regions` e `disable_in_regions` as listas devem estar presentes, embora possam estar vazias

Considerações regionais e regiões apoiadas

As políticas do Security Hub operam em várias regiões, exigindo uma análise cuidadosa de seus requisitos globais de segurança. Compreender o comportamento regional ajuda você a implementar controles de segurança eficazes em toda a presença global da sua organização.

- A aplicação da política ocorre em cada região de forma independente
- Você pode especificar quais regiões incluir ou excluir em suas políticas
- Novas regiões são incluídas automaticamente ao usar a `ALL_SUPPORTED` opção
- As políticas se aplicam somente às regiões em que o Security Hub está disponível

Próximas etapas

Para começar a usar as políticas do Security Hub:

1. Analise os pré-requisitos em Introdução às políticas do Security Hub
2. Planeje sua estratégia política usando nosso guia de melhores práticas
3. Saiba mais sobre a sintaxe de políticas e veja exemplos de políticas

Introdução às políticas do Security Hub

Antes de configurar as políticas do Security Hub, certifique-se de compreender os pré-requisitos e os requisitos de implementação. Este tópico orienta você pelo processo de configuração e gerenciamento dessas políticas em sua organização.

Antes de começar

Analise os seguintes requisitos antes de implementar as políticas do Security Hub:

- Sua conta deve fazer parte de uma AWS Organizations organização

- Você deve estar conectado como:
  - A conta de gerenciamento da organização
  - Uma conta de administrador delegado com permissões para gerenciar as políticas do Security Hub
- Você deve habilitar o acesso confiável para o Security Hub em sua organização
- Você deve habilitar o tipo de política do Security Hub na raiz da sua organização

Além disso, verifique se:

- O Security Hub é suportado nas regiões em que você deseja aplicar políticas
- Você tem a função `AWSServiceRoleForSecurityHubV2` vinculada ao serviço configurada em sua conta de gerenciamento. Para verificar se essa função existe, execute`aws iam get-role --role-name AWSServiceRoleForSecurityHubV2`. Se precisar criar essa função, você pode executá-la `aws securityhub enable-security-hub-v2` em qualquer região a partir da sua conta de gerenciamento ou criá-la diretamente executando`aws iam create-service-linked-role --aws-service-name securityhubv2.amazonaws.com`.

Etapas de implementação

Para implementar as políticas do Security Hub de forma eficaz, siga estas etapas em sequência. Cada etapa garante a configuração adequada e ajuda a evitar problemas comuns durante a configuração. A conta de gerenciamento ou o administrador delegado pode executar essas etapas por meio do AWS Organizations console, da Interface de Linha de AWS Comando (AWS CLI) ou. AWS SDKs

1. Habilite o acesso confiável para o Security Hub.
2. Ative as políticas do Security Hub para sua organização.
3. Crie uma política do Security Hub.
4. Anexe a política do Security Hub à raiz, UO ou conta da sua organização.
5. Veja a política combinada efetiva do Security Hub que se aplica a uma conta.

Em todas essas etapas, você faz login como usuário AWS Identity and Access Management (IAM), assume uma função do IAM ou faz login como usuário raiz (não recomendado) na conta de gerenciamento da organização.

Outras informações

- Aprenda a sintaxe das políticas do Security Hub e veja exemplos de políticas

Melhores práticas para usar as políticas do Security Hub

Ao implementar políticas do Security Hub em sua organização, seguir as melhores práticas estabelecidas ajuda a garantir a implantação e a manutenção bem-sucedidas de suas configurações de segurança. Essas diretrizes abordam especificamente os aspectos exclusivos do gerenciamento e aplicação de políticas do Security Hub AWS Organizations.

Princípios de design de políticas

Antes de criar políticas do Security Hub, estabeleça princípios claros para sua estrutura de políticas. Mantenha as políticas simples e evite regras complexas de atributos cruzados ou aninhadas que dificultam a determinação do resultado final. Comece com políticas amplas no nível raiz da organização e refine-as por meio de políticas secundárias, quando necessário.

Considere usar listas de regiões vazias de forma estratégica. Você pode deixar em `enable_in_regions` branco quando precisar apenas desativar o Security Hub em regiões específicas ou deixar em `disable_in_regions` branco para manter as regiões não gerenciadas pela política. Essa flexibilidade ajuda você a manter um controle preciso sobre sua cobertura de monitoramento de segurança.

Estratégias de gestão da região

Ao gerenciar regiões por meio de políticas do Security Hub, considere essas abordagens comprovadas. Use `ALL_SUPPORTED` quando quiser incluir automaticamente futuras regiões em sua cobertura de segurança. Para um controle mais granular, liste explicitamente as regiões em vez de confiar nelas`ALL_SUPPORTED`, especialmente quando regiões diferentes exigem configurações de segurança diferentes.

Documente os requisitos específicos de sua região, especialmente para:

- Regiões exigidas pela conformidade que exigem configurações específicas
- Diferenças entre desenvolvimento e ambiente de produção
- Regiões opcionais com considerações especiais
- Regiões em que o Security Hub deve permanecer desativado

Planejamento de herança de políticas

Planeje cuidadosamente sua estrutura de herança de políticas para manter um controle de segurança eficaz e, ao mesmo tempo, permitir a flexibilidade necessária. Documente quais unidades organizacionais podem modificar políticas herdadas e quais modificações são permitidas. Considere restringir os operadores de herança (@ @assign, @ @append, @ @remove) nos níveis principais quando precisar aplicar controles de segurança rígidos.

Monitoramento e validação

Implemente práticas regulares de monitoramento para garantir que suas políticas permaneçam efetivas. Revise os anexos da política periodicamente, especialmente após mudanças organizacionais. Valide se as configurações de região correspondem à cobertura de segurança pretendida, especialmente ao usar `ALL_SUPPORTED` ou ao gerenciar várias listas de regiões.

estratégias de solução de problemas

Ao solucionar problemas de políticas do Security Hub, concentre-se primeiro na precedência e herança das políticas. Lembre-se de que as configurações de desativação têm precedência sobre as configurações de ativação quando as regiões aparecem nas duas listas. Verifique as cadeias de herança de políticas para entender como as políticas de pais e filhos se combinam para criar uma política eficaz para cada conta.

Sintaxe e exemplos da política do Security Hub

As políticas do Security Hub seguem uma sintaxe JSON padronizada que define como o Security Hub é habilitado e configurado em toda a organização. Compreender a estrutura de políticas ajuda você a criar políticas eficazes para seus requisitos de segurança.

Considerações

Antes de criar políticas do Security Hub, entenda estes pontos-chave sobre a sintaxe da política:

- `enable_in_regions`Tanto as `disable_in_regions` listas quanto as listas são obrigatórias na política, embora possam estar vazias.
- Ao processar políticas efetivas, `disable_in_regions` tem precedência sobre `enable_in_regions`
- As políticas secundárias podem modificar as políticas principais usando operadores de herança, a menos que sejam explicitamente restritas

- A `ALL_SUPPORTED` designação inclui regiões atuais e futuras.
- Os nomes das regiões devem ser válidos e estar disponíveis no Security Hub

Estrutura política básica

Uma política do Security Hub usa essa estrutura básica:

```
{
   "securityhub":{
      "enable_in_regions":[
         "us-east-1",
         "us-west-2"
      ],
      "disable_in_regions":[
         "eu-central-1"
      ]
   }
}
```

Componentes da política

As políticas do Security Hub contêm esses componentes principais:

`securityhub`

O contêiner de nível superior para configurações de políticas

Obrigatório para todas as políticas do Security Hub

`enable_in_regions`

Lista de regiões em que o Security Hub deve ser ativado

Pode conter nomes de regiões específicos ou `ALL_SUPPORTED`

Campo obrigatório, mas pode estar vazio

Ao usar`ALL_SUPPORTED`, inclui futuras regiões

`disable_in_regions`

Lista de regiões onde o Security Hub deve ser desativado

Pode conter nomes de regiões específicos ou `ALL_SUPPORTED`

Campo obrigatório, mas pode estar vazio

Tem precedência sobre `enable_in_regions` quando as regiões aparecem nas duas listas

Operadores de herança

@ @assign - Substitui valores herdados

@ @append - Adiciona novos valores aos existentes

@ @remove - Remove valores específicos das configurações herdadas

Exemplos de políticas do Security Hub

Os exemplos a seguir demonstram configurações comuns de políticas do Security Hub.

O exemplo abaixo ativa o Security Hub em todas as regiões atuais e futuras. Ao usar `ALL_SUPPORTED` na `enable_in_regions` lista e deixar em `disable_in_regions` branco, essa política garante uma cobertura de segurança abrangente à medida que novas regiões se tornam disponíveis.

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "ALL_SUPPORTED"
         ]
      },
      "disable_in_regions":{
         "@@assign":[

         ]
      }
   }
}
```

Este exemplo desativa o Security Hub em todas as regiões, incluindo qualquer região futura, já que a `disable_in_regions` lista tem precedência. `enable_in_regions`

```
{
   "securityhub":{
```

```
      "enable_in_regions":{
         "@@assign":[
            "us-east-1",
            "us-west-2"
         ]
      },
      "disable_in_regions":{
         "@@assign":[
            "ALL_SUPPORTED"
         ]
      }
   }
}
```

O exemplo a seguir demonstra como as políticas secundárias podem modificar as configurações da política principal usando operadores de herança. Essa abordagem permite um controle granular enquanto mantém a estrutura geral da política. A política secundária adiciona uma nova região `enable_in_regions` e remove uma região de`disable_in_regions`.

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@append":[
            "eu-central-1"
         ]
      },
      "disable_in_regions":{
         "@@remove":[
            "us-west-2"
         ]
      }
   }
}
```

Este exemplo mostra como habilitar o Security Hub em várias regiões específicas sem usar`ALL_SUPPORTED`. Isso fornece controle preciso sobre quais regiões têm o Security Hub ativado, enquanto deixa regiões não especificadas não gerenciadas pela política.

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
```

```
            "us-east-1",
            "us-west-2",
            "eu-west-1",
            "ap-southeast-1"
         ]
      },
      "disable_in_regions":{
         "@@assign":[

         ]
      }
   }
}
```

O exemplo a seguir demonstra como lidar com os requisitos de conformidade regionais ativando o Security Hub na maioria das regiões e, ao mesmo tempo, desativando-o explicitamente em locais específicos. A `disable_in_regions` lista tem precedência, garantindo que o Security Hub permaneça desativado nessas regiões, independentemente de outras configurações de política.

```
{
   "securityhub":{
      "enable_in_regions":{
         "@@assign":[
            "ALL_SUPPORTED"
         ]
      },
      "disable_in_regions":{
         "@@assign":[
            "ap-east-1",
            "me-south-1"
         ]
      }
   }
}
```

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 ocorre porque os recursos de segurança, como as políticas

de controle de serviços (SCPs) do Organizations, não restringem usuários ou funções 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.

Para ver exemplos de políticas de delegação baseadas em recursos, consulte Exemplos de políticas baseadas em recursos para AWS Organizations.

Tópicos

Crie uma política de delegação baseada em recursos com AWS Organizations

Na conta de gerenciamento, crie 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 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 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.
4. Insira 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 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.
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.

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 do membro delegado pode anexar políticas à raiz da organização ou às unidades organizacionais (OUs), `Resources` defina. Você também deve selecionar `policy` como um tipo de recurso. 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 o recurso ARNs 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 o uso ARNs no elemento de recurso de uma política, consulte Elementos de política JSON do IAM: Recurso.
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`**. 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 uma política de delegação

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

- AWS CLI: put-resource-policy

  O exemplo a seguir cria 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`

Chaves de condição compatíveis

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 do AWS Organizations na Referência de autorização do serviço.

Atualize uma política de delegação baseada em recursos com AWS Organizations

Na conta de gerenciamento, 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 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 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 do AWS Organizations, escolha Editar para atualizar a política de delegação do Organizations.
4. Insira 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 de política e, depois, escolha Criar política.

Usar o editor visual para 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 do AWS Organizations, escolha Editar para atualizar a política de delegação do Organizations.
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.
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 do membro delegado pode anexar políticas à raiz da organização ou às unidades organizacionais (OUs), `Resources` defina. Você também deve selecionar `policy` como um tipo de recurso. 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 o recurso ARNs 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 o uso ARNs no elemento de recurso de uma política, consulte Elementos de política JSON do IAM: Recurso.

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`**. 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 de política e, depois, escolha Salvar política.

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

Chaves de condição compatíveis

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 do AWS Organizations na Referência de autorização do serviço.

Veja uma política de delegação baseada em recursos com AWS Organizations

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

Exclua uma política de delegação baseada em recursos com AWS Organizations

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

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. Você pode habilitar um tipo de política somente da conta de gerenciamento da organização ou de uma conta de membro designada como administrador delegado.

> **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 ***policy type***.

   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. Você pode desativar um tipo de política somente da conta de gerenciamento da organização ou de uma conta de membro designada como administrador delegado.

Considerações

As políticas desabilitadas são desvinculadas de todas as entidades, mas não são excluídas

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 para tipo de política de controle de serviço) Todas as entidades na raiz são inicialmente vinculadas apenas à SCP padrão do **`FullAWSAccess`**

(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. Os anexos de SCPs entidades são perdidos quando SCPs são desativados na organização. Se você quiser reativá-las posteriormente SCPs, deverá reconectá-las à raiz e às contas da organização OUs, conforme apropriado.

Desabilitar um tipo de política

Permissões mínimas

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

- `organizations:DisablePolicyType`
- `organizations:DescribeOrganization` – necessária 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 Desativar ***`policy type`***.
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

Criação de políticas organizacionais com AWS Organizations

Depois de habilitar políticas para sua organização, você pode criar uma política.

Este tópico descreve como criar políticas com AWS Organizations. Uma política define os controles que você deseja aplicar a um grupo de Contas da AWS.

Tópicos

- Criar uma política de controle de serviços (SCP)
- Crie uma política de controle de recursos (RCP)

- Crie uma política declarativa
- Criar uma política de backup
- Criar uma política de tags
- Crie uma política de aplicativos de bate-papo
- Criar uma política de recusa de serviços de IA
- Crie uma política do Security Hub

Criar uma política de controle de serviços (SCP)

> **Permissões mínimas**
>
> Para criar 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 Recursos de marcação 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 usa `Deny` instruções, você tem controle adicional porque pode restringir o acesso a recursos específicos, definir condições para quando SCPs elas estão em vigor e usar o NotActionelemento. Para obter detalhes sobre sintaxe de, consulte Sintaxe de SCP.

   Para adicionar uma instrução que nega acesso:

   a. No painel direito Editar declaração do editor, em Adicionar ações, escolha um AWS serviço.

      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).

- Chave de condição — Na lista, você pode escolher qualquer chave de condição que esteja disponível para todos os AWS serviços (por exemplo,`aws:SourceIp`) ou uma chave específica de serviço para somente um dos serviços que você selecionou para essa declaração.
- Qualificador — (Opcional) Quando a solicitação tem mais de um valor para uma chave de contexto de vários valores, você pode especificar um qualificador para testar as solicitações em relação aos valores. Para obter mais informações, consulte Chaves de contexto de valor único versus de valores múltiplos no Guia do usuário do IAM. Para verificar se uma solicitação pode ter vários valores, consulte as Ações, recursos e chaves de condição Serviços da AWS na Referência de autorização de serviço.

- 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 `Null` teste, você pode escolher a IfExistsopção.
- Value (Valor) – (opcional) especifique um ou mais valores para os quais você deseja testar a solicitação.

Escolha 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.

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 seu SCP à raiz OUs, ou 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**
>
> SCPs não têm efeito na conta de gerenciamento e em algumas outras situações. Para obter mais informações, consulte Tarefas e entidades não restritas por SCPs.

Crie uma política de controle de recursos (RCP)

> **Permissões mínimas**
>
> Para criar RCPs, você precisa de permissão para executar a seguinte ação:

- `organizations:CreatePolicy`

AWS Management Console

Para criar uma política de controle de 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 Política de controle de recursos, escolha Criar política.
3. Na página Criar nova política de controle de recursos, insira um nome da política e uma descrição opcional da política.
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 Recursos de marcação 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 adicionar uma declaração:

   a. No painel direito Editar declaração do editor, em Adicionar ações, escolha um AWS serviço.

      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.
- Preencha o Nome de recurso da Amazon (ARN) no 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).

- Chave de condição — Na lista, você pode escolher qualquer chave de condição que esteja disponível para todos os AWS serviços (por exemplo,`aws:SourceIp`) ou uma chave específica de serviço para somente um dos serviços que você selecionou para essa declaração.
- Qualificador — (Opcional) Quando a solicitação tem mais de um valor para uma chave de contexto de vários valores, você pode especificar um qualificador para testar as solicitações em relação aos valores. Para obter mais informações, consulte Chaves de contexto de valor único versus de valores múltiplos no Guia do usuário do IAM. Para verificar se uma solicitação pode ter vários valores, consulte as Ações, recursos e chaves de condição Serviços da AWS na Referência de autorização de serviço.
  - 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 `Null` teste, você pode escolher a IfExistsopção.

- Value (Valor) – (opcional) especifique um ou mais valores para os quais você deseja testar a solicitação.

Escolha 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 de política JSON do IAM: NotAction no Guia do usuário do IAM.

6. (Opcional) Para adicionar outra instrução à política, escolha Add Statement (Adicionar instrução) e use o editor visual para criar a próxima instrução.
7. Quando terminar de adicionar instruções, escolha Criar política para salvar o RCP concluído.

Seu novo RCP aparece na lista das políticas da organização. Agora você pode anexar seu RCP à raiz OUs, ou contas.

AWS CLI & AWS SDKs

Para criar uma política de controle de recursos

Você pode usar um dos seguintes comandos para criar um RCP:

- 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 recursos.

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMRCP \
```

```
    --type RESOURCE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
resource_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMRCP",
            "Description": "Deny all IAM actions",
            "Type": "RESOURCE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- AWS SDKs: CreatePolicy

> **Note**
>
> RCPs não têm efeito na conta de gerenciamento e em algumas outras situações. Para obter mais informações, consulte Recursos e entidades não restritos por RCPs.

Crie uma política declarativa

> **Permissões mínimas**
>
> Para criar uma política declarativa, você precisa de permissão para executar a seguinte ação:
>
> - `organizations:CreatePolicy`

AWS Management Console

Para criar uma política declarativa

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 Políticas declarativas, escolha Criar política.
3. Na EC2página Criar nova política declarativa para, insira um nome da política e uma descrição opcional da 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, consulte Recursos de marcação 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 da política declarativa, consulte. Sintaxe e exemplos de políticas declarativas

   Se você optar por usar o editor visual, selecione o atributo de serviço que deseja incluir na sua política declarativa. Para obter mais informações, consulte Suporte Serviços da AWS e atributos.
6. Escolha Adicionar atributo de serviço e configure o atributo de acordo com suas especificações. Para obter informações mais detalhadas sobre cada efeito, consulteSintaxe e exemplos de políticas declarativas.
7. 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 declarativa

Você pode usar uma das opções a seguir para criar uma política declarativa:

- AWS CLI: create-policy

  1. Crie uma política declarativa como a seguinte e armazene-a em um arquivo de texto.

     ```
     {
     ```

```
    "ec2_attributes": {
        "image_block_public_access": {
            "state": {
                "@@assign": "block_new_sharing"
            }
        }
    }
}
```

Essa política declarativa especifica que todas as contas afetadas pela política devem ser configuradas para que as novas Amazon Machine Images (AMIs) não possam ser compartilhadas publicamente. Para obter informações sobre a sintaxe da política declarativa, consulte. Sintaxe e exemplos de políticas declarativas

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 DECLARATIVE_POLICY_EC2 \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{"ec2_attributes":{"image_block_public_access":{"state":
{"@@assign":"block_new_sharing"}}}}".
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "DECLARATIVE_POLICY_EC2"
        }
    }
}
```

- AWS SDKs: CreatePolicy

O que fazer em seguida

Depois de criar uma política declarativa, avalie a prontidão usando o relatório de status da conta. Em seguida, você pode aplicar suas configurações de linha de base. Para fazer isso, você pode anexar a política à raiz da organização, às unidades organizacionais (OUs), Contas da AWS dentro da sua organização ou a uma combinação de todas elas.

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 AWS Management Console de 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 Recursos de marcação 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 AWS Backup console ou os AWS CLI comandos.
      - (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 AWS Backup usados para encontrar 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 dos afetados Contas da AWS que estão no especificado Regiões da AWS e que têm a tag `dataType` com um 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

Criar uma política de tags

Permissões mínimas

Para criar políticas de tag, você precisa de permissão para executar a seguinte ação:

- `organizations:CreatePolicy`

Você pode criar uma política de tags AWS Management Console de 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

Você pode criar uma política de tags AWS Management Console de 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.

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 Recursos de marcação 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.

   Se você optar por usar o Editor visual, especifique o seguinte:
6. Em New tag Key 1 (Nova chave de tag 1), especifique o nome de uma chave de tag a ser adicionada.
7. Em Compliance Options, você pode selecionar as seguintes opções:

   a. Use the capitalization that you've specified above for the tag key: deixe esta opção desmarcada (o padrão) para especificar que a política de tag pai herdada, caso exista, 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 tags OUs ou contas adicionais para criar regras de marcação adicionais.

b. Specify allowed values for this tag key: habilite esta opção se quiser adicionar valores permitidos para esta chave de tag a quaisquer valores herdados de uma política pai.

   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 Resource types to enforce, você pode selecionar Prevent noncompliant operations for this tag.

   Recomendamos deixar 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 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 tem a CostCenter tag anexada com ou sem um valor está em conformidade.

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

Crie uma política de aplicativos de bate-papo

> **Permissões mínimas**
>
> Para criar uma política de aplicativos de bate-papo, você precisa de permissão para executar a seguinte ação:
>
> - `organizations:CreatePolicy`

AWS Management Console

Você pode criar uma política de aplicativos de AWS Management Console bate-papo de 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 aplicativos de bate-papo

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 Chatbot policies, escolha Create policy.
3. Na página de política Criar novos aplicativos de bate-papo, insira o nome da política e uma descrição opcional da 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, consulte Recursos de marcação 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 da política de aplicativos de bate-papo, consulteSintaxe e exemplos de políticas de aplicativos de bate-papo.

   Se você optar por usar o editor visual, configure sua política de aplicativos de bate-papo especificando controles de acesso para clientes de bate-papo.

   a. Escolha uma das seguintes opções para Set Amazon Chime chat client access

- Negar o acesso ao Chime.
- Permitir o acesso ao Chime.

b. Escolha uma das seguintes opções para Set Microsoft Teams chat client access

- Negar acesso a tudo do Teams
- Permitir acesso a tudo do Teams
- Restringir acesso a Teams específicos

c. Escolha uma das seguintes opções para Set Slack chat client access

- Negar acesso a todos os espaços de trabalho do Slack
- Permitir acesso a todos os espaços de trabalho do Slack
- Restringir acesso a espaços de trabalho do Slack específicos

> **Note**
>
> Além disso, você pode selecionar Limitar o uso do Amazon Q Developer no uso de aplicativos de bate-papo somente a canais privados do Slack.

d. Selecione as seguintes opções para Set IAM permissions types

- Enable Channel level IAM role: todos os membros do canal compartilham as permissões do perfil do IAM para executar tarefas em um canal. Um perfil de canal será apropriado se os membros do canal precisarem das mesmas permissões.
- Enable User level IAM role: os membros do canal devem escolher um perfil de usuário do IAM para realizar ações (requer acesso ao console para escolher os perfis). Perfis de usuário serão apropriados se os membros do canal precisarem de permissões diferentes e puderem escolher seus perfis de usuário.

6. Quando terminar de criar sua política, escolha Create policy (Criar política). A política aparecerá na lista de políticas de backup de chatbot.

AWS CLI & AWS SDKs

Para criar uma política de aplicativos de bate-papo

Você pode usar uma das opções a seguir para criar uma política de aplicativos de bate-papo:

- AWS CLI: create-policy

Você pode usar qualquer editor de texto para criar uma política de aplicativos de bate-papo. Use a sintaxe JSON e salve a política de aplicativos de bate-papo como um arquivo com qualquer nome e extensão em um local de sua escolha. As políticas de aplicativos de bate-papo podem ter no máximo? caracteres, incluindo espaços. Para obter informações sobre sintaxe de política de tag, consulte Sintaxe e exemplos de políticas de aplicativos de bate-papo.

Para criar uma política de aplicativos de bate-papo

1. Crie uma política de aplicativos de bate-papo em um arquivo de texto semelhante ao seguinte:

   Conteúdo de `testpolicy.json`:

```
{
   "chatbot": {
      "platforms": {
         "slack": {
            "client": {
               "@@assign": "enabled"
            },
            "workspaces": {
               "@@assign": [
                  "Slack-Workspace-Id"
               ]
            },
            "default": {
               "supported_channel_types": {
                  "@@assign": [
                     "private"
                  ]
               }
            }
         },
         "microsoft_teams": {
            "client": {
               "@@assign": "disabled"
            }
         }
      }
   }
}
```

Essa política de aplicativos de bate-papo permite apenas canais privados do Slack em um espaço de trabalho específico, desativa o Microsoft Teams e oferece suporte a todas as configurações de função.

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 "MyTestChatbotPolicy" \
    --description "My Test policy" \
    --content file://testpolicy.json \
    --type CHATBOT_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-a1b2c3d4e5",
            "Name": "MyTestChatApplicationsPolicy",
            "Description": "My Test policy",
            "Type": "CHATBOT_POLICY",
            "AwsManaged": false
        },
        "Content": "{"chatbot":{"platforms":{"slack":{"client":
{"@@assign":"enabled"},"workspaces":{"@@assign":["Slack-Workspace-
Id"]},"supported_channel_types":{"@@assign":["private"]}},"microsoft_teams":
{"client":{"@@assign":"disabled"}}}}}"
    }
}
```

- AWS SDKs: CreatePolicy

Criar uma política de recusa de 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 obter mais informações, consulte Recursos de marcação 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

Crie uma política do Security Hub

Permissões mínimas

Para criar uma política do Security Hub, você precisa de permissão para executar a seguinte ação:

- `organizations:CreatePolicy`

AWS Management Console

Para criar uma política do Security Hub

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 de políticas do Security Hub, escolha Criar política.
3. Na página Criar nova política do Security Hub, insira o nome da política e uma descrição opcional da 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, consulte Recursos de marcação AWS Organizations.
5. Insira ou cole o texto da política na caixa do código JSON. Para obter informações sobre a sintaxe da política do Security Hub, consulteSintaxe e exemplos da política do Security Hub. Para obter exemplos de política que você pode usar como ponto de partida, consulte Exemplos de políticas do Security Hub.
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 do Security Hub

Você pode usar uma das opções a seguir para criar uma política do Security Hub:

- AWS CLI: create-policy

Exemplo: criar uma política que habilite o Security Hub em todas as regiões suportadas

O exemplo a seguir pressupõe que você tenha um arquivo chamado `testPolicy_enableAllSupportedRegions.json` com o texto da política JSON nele. Ele usa esse arquivo para criar uma nova política do Security Hub.

```
$ aws organizations create-policy \
    --content file://./testPolicy_enableAllSupportedRegions.json \
    --name "testPolicy_enableAllSupportedRegions" \
    --description "Test policy to enable securityhub in ALL_SUPPORTED Regions" \
    --type SECURITYHUB_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66ev7hgcvj",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
            "Name": "testPolicy_enableAllSupportedRegions",
            "Description": "Test policy to enable securityhub in ALL_SUPPORTED
 Regions",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[]\n    }\n  }\n}\n"
    }
}
```

Exemplo: Crie uma política que habilite o Security Hub em todas as regiões suportadas, mas desabilite na região us-east-1

O exemplo a seguir pressupõe que você tenha um arquivo chamado `testPolicy_enableAllSupportedRegions_Disable_us-east-1.json` com o texto da política JSON nele. Ele usa esse arquivo para criar uma nova política do Security Hub.

```
$ aws organizations create-policy \
    --content file://./testPolicy_enableAllSupportedRegions_Disable_us-east-1.json
 \
    --name "testPolicy_enableAllSupportedRegions_Disable_us-east-1" \
```

```
    --description "Test policy to enable securityhub in ALL_SUPPORTED Regions but
 disable in us-east-1 Region" \
    --type SECURITYHUB_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66217dwpos",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66217dwpos",
            "Name": "testPolicy_enableAllSupportedRegions_Disable_us-east-1",
            "Description": "Test policy to enable securityhub in ALL_SUPPORTED
 Regions but disable in us-east-1 Region",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[\n        \"us-east-1\"\n      ]\n
    }\n  }\n}\n"
    }
}
```

- AWS SDKs: CreatePolicy

Atualizando as políticas da organização com AWS Organizations

Quando os seus requisitos de política mudam, você pode atualizar uma política existente.

Este tópico descreve como atualizar políticas com AWS Organizations. Uma política define os controles que você deseja aplicar a um grupo de Contas da AWS.

Tópicos

- Atualizar uma política de controle de serviços (SCP)
- Atualizar uma política de controle de recursos (RCP)
- Atualizar uma política declarativa
- Atualizar uma política de backup
- Atualizar política de tag
- Atualizar uma política de aplicativos de bate-papo
- Atualizar uma política de recusa de serviços de IA

- Atualizar uma política do Security Hub

Atualizar uma política de controle de serviços (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 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

Atualizar uma política de controle de recursos (RCP)

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 um RCP afeta imediatamente todos os recursos em todas as contas anexadas.

Permissões mínimas

Para atualizar um RCP, 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 Política de controle de recursos, escolha o nome da política que você 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 o procedimento Criando um RCP anteriormente neste tópico.
5. Ao concluir, escolha 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 altera a descrição de uma política de controle de recursos.

```
$ 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 do RCP especificando um arquivo que contém o novo texto da 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

Atualizar uma política declarativa

Permissões mínimas

Para atualizar uma política declarativa, 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 declarativa

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 Políticas declarativas, 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 da política declarativa, consulte. Sintaxe e exemplos de políticas declarativas
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 declarativa.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "DECLARATIVE_POLICY_EC2",
```

```
            "AwsManaged": false
        },
        "Content": "{"ec2-configuration":{"ec2_attributes":
{"image_block_public_access":{"state":{"@@assign":"block_new_sharing"}}}}".
    }
}
```

O exemplo a seguir adiciona ou altera a descrição de uma política declarativa.

```
$ 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/
declarative_policy_ec2/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "DECLARATIVE_POLICY_EC2",
            "AwsManaged": false
        },
        "Content": "{"ec2_attributes":{"image_block_public_access":{"state":
{"@@assign":"block_new_sharing"}}}}".
    }
}
```

- AWS SDKs: UpdatePolicy

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" },
                        "opt_in_to_archive_for_supported_resources": {"@@assign":
 false}
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" },
                                "opt_in_to_archive_for_supported_resources":
 {"@@assign": false}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$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

Atualizar 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"
    }
}
```

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

Atualizar uma política de aplicativos de bate-papo

> **Permissões mínimas**
>
> Para atualizar uma política de aplicativos de bate-papo, 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 aplicativos de bate-papo

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 de políticas do Chatbot, escolha a política de aplicativos de bate-papo que você 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 aplicativos de bate-papo.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed chat applications policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
chatbot_policy/p-i9j8k7l6m5",
            "Name": "Renamed chat applications policy",
            "Type": "CHATBOT_POLICY",
            "AwsManaged": false
        },
        "Content": "{"chatbot":{"platforms":{"slack":{"client":
{"@@assign":"enabled"},"workspaces":{"@@assign":["Slack-Workspace-Id"]},"default":
{"supported_channel_types":{"@@assign":["private"]}}},"microsoft_teams":{"client":
{"@@assign":"disabled"}}}}}"
    }
}
```

- AWS SDKs: UpdatePolicy

Atualizar uma política de recusa de 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"}
}
```

- AWS SDKs: UpdatePolicy

Atualizar uma política do Security Hub

Permissões mínimas

Para atualizar uma política do Security Hub, 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 do Security Hub

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 de políticas do Security Hub, 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 da política do Security Hub, consulteSintaxe e exemplos da política do Security Hub. Para obter exemplos de política que você pode usar como ponto de partida, consulte Exemplos de políticas do Security Hub.
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 do Security Hub.

```
$ aws organizations update-policy \
    --policy-id p-66ev7hgcvj \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
```

```
            "Id": "p-66ev7hgcvj",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
            "Name": "Renamed policy",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[]\n    }\n  }\n}\n"
    }
}
```

O exemplo a seguir adiciona ou altera a descrição de uma política do Security Hub.

```
$ aws organizations update-policy \
    --policy-id p-66ev7hgcvj \
    --name "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-66ev7hgcvj",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
securityhub_policy/p-66ev7hgcvj",
            "Name": "My new description",
            "Type": "SECURITYHUB_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n  \"securityhub\": {\n    \"enable_in_regions\":
 {\n      \"@@assign\":[\n        \"ALL_SUPPORTED\"\n      ]\n    },\n
 \"disable_in_regions\": {\n      \"@@assign\":[]\n    }\n  }\n}\n"
    }
}
```

- AWS SDKs: UpdatePolicy

Editar tags anexadas às políticas da organização com o AWS Organizations

Este tópico descreve como editar tags anexadas às políticas com AWS Organizations. Uma política define os controles que você deseja aplicar a um grupo de Contas da AWS.

Tópicos

Editar tags anexadas a uma política de controle de serviços (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 Recursos de marcação AWS Organizations.

> **Permissões mínimas**
>
> Para editar as tags anexadas a uma SCP na sua organização da , 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 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

Editar tags anexadas a uma política de controle de recursos (RCP)

Ao entrar na conta de gerenciamento da sua organização, você pode adicionar ou remover as tags anexadas a um RCP. Para obter mais informações sobre marcação, consulte Recursos de marcação AWS Organizations.

Permissões mínimas

Para editar as tags anexadas a um RCP em sua AWS organização, 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 as tags anexadas a um RCP

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 Política de controle de recursos, escolha o nome da política com as tags que você deseja editar.
3. Na página de detalhes da política, escolha a guia Tags e, em seguida, escolha Gerenciar tags.
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 Salvar alterações.

AWS CLI & AWS SDKs

Para editar as tags anexadas a um RCP

Você pode usar um dos seguintes comandos para editar as tags anexadas a um RCP:

- AWS CLI: tag-resource e untag-resource
- AWS SDKs: TagResource e UntagResource

Editar tags anexadas a uma política declarativa

Ao entrar na conta de gerenciamento da sua organização, você pode adicionar ou remover as tags anexadas a uma política declarativa. Para obter mais informações sobre marcação, consulte Recursos de marcação AWS Organizations.

Permissões mínimas

Para editar as tags anexadas a uma política declarativa em sua AWS organização, 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 declarativa

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 Políticas declarativas, 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 declarativa

Você pode usar um dos comandos a seguir para editar as tags anexadas a uma política declarativa:

- AWS CLI: tag-resource e untag-resource
- AWS SDKs: TagResource e UntagResource

Editar 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 Recursos de marcação AWS Organizations.

Permissões mínimas

Para editar as tags anexadas a uma política de backup de sua organização da , 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

Editar tags anexadas a uma política de tags

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 , 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 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 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

Editar tags anexadas a uma política de aplicativos de bate-papo

Ao entrar na conta de gerenciamento da sua organização, você pode adicionar ou remover as tags anexadas a uma política de aplicativos de bate-papo. Para fazer isso, conclua as seguintes etapas:

> **Permissões mínimas**
>
> Para editar as tags anexadas a uma política de aplicativos de bate-papo em sua organização, 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 aplicativos de bate-papo

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 Chatbot policies, 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 aplicativos de bate-papo

Você pode usar um dos comandos a seguir para editar as tags anexadas a uma política de aplicativos de bate-papo:

- AWS CLI: tag-resource e untag-resource
- AWS SDKs: TagResource e UntagResource

Editar tags anexadas a uma política de recusa de 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 Recursos de marcação AWS Organizations.

Permissões mínimas

Para editar as tags anexadas a uma política de exclusão dos serviços de IA em sua organização da , 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

Editar tags anexadas a uma política do Security Hub

Ao entrar na conta de gerenciamento da sua organização, você pode adicionar ou remover as tags anexadas a uma política do Security Hub. Para obter mais informações sobre marcação, consulte Recursos de marcação AWS Organizations.

Permissões mínimas

Para editar as tags anexadas a uma política do Security Hub em sua organização, 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 do Security Hub

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 de políticas do Security Hub, 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 do Security Hub

Você pode usar um dos seguintes comandos para editar as tags anexadas a uma política do Security Hub:

- AWS CLI: tag-resource e untag-resource
- AWS SDKs: TagResource e UntagResource

Anexando políticas da organização com AWS Organizations

Este tópico descreve como vincular as políticas com o AWS Organizations. Uma política define os controles que você deseja aplicar a um grupo de Contas da AWS.

Tópicos

- Anexe políticas com AWS Organizations

Anexe políticas com AWS Organizations

Permissões mínimas

Para vincular políticas, você deve ter permissão para executar a seguinte ação:

- `organizations:AttachPolicy`

Permissões mínimas

Para anexar uma política de autorização (SCP ou RCP) a uma raiz, OU 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

Service control policies (SCPs)

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 OUs (escolher a ▶) para encontrar a OU 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 anexada SCPs na guia Políticas foi 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja.
5. Escolha Anexar política.

   A lista de alvos anexados SCPs na guia Alvos foi 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.

Resource control policies (RCPs)

Você pode anexar um RCP navegando até a política ou até a raiz, UO ou ou conta à qual deseja anexar a política.

Para anexar um RCP navegando até a raiz, a OU ou a 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 Contas da AWSpágina, navegue até e escolha a caixa de seleção ao lado da raiz, UO ou ou conta à qual você deseja anexar um RCP. Talvez seja necessário expandir OUs (escolher a) para encontrar a OU ou a conta que você deseja.
3. Na guia Políticas, na entrada de Políticas de controle de recursos, escolha Anexar.
4. Encontre a política que você deseja e escolha Attach policy (Anexar política).

   A lista anexada RCPs na guia Políticas foi atualizada para incluir a nova adição. A alteração da política entra em vigor imediatamente, afetando as permissões dos recursos na conta anexada ou em todas as contas na raiz ou UO anexada.

Para anexar um RCP 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 Política de controle de recursos, 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja.
5. Escolha Anexar política.

   A lista de alvos anexados RCPs na guia Alvos foi atualizada para incluir a nova adição. A alteração da política entra em vigor imediatamente, afetando as permissões dos recursos na conta anexada ou em todas as contas na raiz ou UO anexada.

Declarative policies

Você pode anexar uma política declarativa navegando até a política ou até a raiz, UO ou conta à qual deseja anexar a política.

Para anexar uma política declarativa navegando até a raiz, a OU ou a 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja.
3. Na guia Políticas, na entrada de Políticas declarativas, escolha Anexar.
4. Encontre a política que você deseja e escolha Attach policy (Anexar política).

   A lista de políticas declarativas anexadas na guia Políticas foi atualizada para incluir a nova adição. A política entra em vigor imediatamente.

Para anexar uma política declarativa 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 Políticas declarativas, 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja.
5. Escolha Anexar política.

   A lista de políticas declarativas anexadas na guia Metas foi atualizada para incluir a nova adição. A política entra em vigor imediatamente.

Backup policies

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 OUs (escolher a) para encontrar a OU 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja.
5. Escolha 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.

Tag policies

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 OUs (escolher a) para encontrar a OU 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 OUs (escolher a) para encontrar a OU 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.

Chat applications policies

Você pode anexar uma política de aplicativos de bate-papo navegando até a política ou até a raiz, UO ou ou conta à qual deseja anexar a política.

Para anexar uma política de aplicativos de bate-papo navegando até a raiz, OU 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja.
3. Na guia Políticas, na entrada de políticas de aplicativos do Chat, escolha Anexar.
4. Encontre a política que você deseja e escolha Attach policy (Anexar política).

   A lista de políticas de aplicativos de bate-papo anexadas na guia Políticas foi atualizada para incluir a nova adição. A política entra em vigor imediatamente.

Para anexar uma política de aplicativos de bate-papo 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 Chatbot policies, 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja.
5. Escolha Anexar política.

   A lista de políticas de aplicativos de bate-papo anexadas na guia Destinos foi atualizada para incluir a nova adição. A política entra em vigor imediatamente.

AI services opt-out policies

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 OUs (escolher a) para encontrar a OU 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja.
5. Escolha 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.

Security Hub policies

Você pode anexar uma política do Security Hub navegando até a política ou até a raiz, UO ou conta à qual deseja anexar a política.

Para anexar uma política do Security Hub navegando até a raiz, OU 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja.
3. Na guia Políticas, na entrada das políticas do Security Hub, escolha Anexar.
4. Encontre a política que você deseja e escolha Attach policy (Anexar política).

   A lista de políticas anexadas do Security Hub na guia Políticas foi atualizada para incluir a nova adição. A política entra em vigor imediatamente.

Para anexar uma política do Security Hub 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 de políticas do Security Hub, 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja.
5. Escolha Anexar política.

   A lista de políticas do Security Hub anexadas na guia Targets foi atualizada para incluir a nova adição. A política entra em vigor imediatamente.

AWS CLI & AWS SDKs

Anexar a política

Os exemplos de código a seguir mostram como usar o `AttachPolicy`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
```

```
    /// Shows how to attach an AWS Organizations policy to an organization,
    /// an organizational unit, or an account.
    /// </summary>
    public class AttachPolicy
    {
        /// <summary>
        /// Initializes the Organizations client object and then calls the
        /// AttachPolicyAsync method to attach the policy to the root
        /// organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new AttachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.AttachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully attached Policy ID {policyId} to
Target ID: {targetId}.");
            }
            else
            {
                Console.WriteLine("Was not successful in attaching the policy.");
            }
        }
    }
```

- Para obter detalhes da API, consulte AttachPolicya Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como anexar uma política a uma raiz, unidade operacional ou conta

Exemplo 1

O seguinte exemplo mostra com anexar uma política de controle de serviços (SCP) a uma unidade operacional (OU):

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id ou-examplerootid111-exampleouid111
```

Exemplo 2

O seguinte exemplo mostra como anexar uma política de controle de serviços a uma conta:

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id 333333333333
```

- Para obter detalhes da API, consulte AttachPolicyem Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
 or
    organizational unit.
```

```
    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
        raise
```

- Para obter detalhes da API, consulte a AttachPolicyReferência da API AWS SDK for Python (Boto3).

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

Separando as políticas da organização com AWS Organizations

Este tópico descreve como desvincular políticas com o AWS Organizations. Uma política define os controles que você deseja aplicar a um grupo de Contas da AWS.

Tópicos

- Separe as políticas com AWS Organizations

Separe as políticas com AWS Organizations

> **Permissões mínimas**
>
> Para desvincular uma política da raiz da organização, OU ou conta, você deve ter permissão para executar a seguinte ação:
>
> - `organizations:DetachPolicy`

> **Note**
>
> Você não pode separar a última política de autorização (SCP ou RCP) de uma raiz, de uma OU ou de uma conta. Deve haver pelo menos um SCP e um RCP conectados a cada raiz, UO e conta em todos os momentos.

AWS Management Console

Service control policies (SCPs)

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 OUs (escolher a) para encontrar a OU 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 anexos SCPs é 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja.
4. Escolha Detach (Desvincular).
5. Na caixa de diálogo de confirmação, escolha Detach (Desvincular).

   A lista de anexos SCPs é 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.

Resource control policies (RCPs)

Você pode desanexar um RCP navegando até a política ou até a raiz, UO ou ou conta da qual você deseja desanexar a política. Depois de separar um RCP de uma entidade, esse RCP não se aplica mais a nenhum recurso afetado pela entidade agora desanexada.

> **Note**
>
> Você não pode separar a política **`RCPFullAWSAccess`**
> A `RCPFullAWSAccess` política é anexada automaticamente à raiz, a cada UO e a cada conta em sua organização. Você não pode desanexar essa política.

Para desanexar um RCP navegando até a raiz, a OU ou a conta à qual ele está vinculado

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 OUs (escolher a) para encontrar a OU ou a conta que você deseja. Escolha o nome da raiz, UO ou conta.

3. Na guia Políticas, escolha o botão de rádio ao lado do RCP que você deseja desanexar e, em seguida, escolha Desanexar.
4. Na caixa de diálogo de confirmação, escolha Detach policy (Desvincular política).

   A lista de anexos RCPs é atualizada. A alteração de política causada pela separação do RCP entra em vigor imediatamente. Por exemplo, a desanexação de um RCP afeta imediatamente as permissões dos usuários e funções do IAM na conta ou contas anexadas anteriormente na raiz da organização ou OU anteriormente anexada.

Para desanexar um RCP 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 Política de controle de recursos, escolha o nome da política que você deseja separar 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja.
4. Escolha Detach (Desvincular).
5. Na caixa de diálogo de confirmação, escolha Detach (Desvincular).

   A lista de anexos RCPs é atualizada. A alteração de política causada pela separação do RCP entra em vigor imediatamente. Por exemplo, a desanexação de um RCP afeta imediatamente as permissões dos usuários e funções do IAM na conta ou contas anexadas anteriormente na raiz da organização ou OU anteriormente anexada.

Declarative policies

Você pode desanexar uma política declarativa navegando até a política ou até a raiz, UO ou conta da qual você deseja desanexar a política.

Para separar uma política declarativa navegando até a raiz, a OU ou a 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja. Escolha o nome da raiz, UO ou conta.
3. Na guia Políticas, escolha o botão de rádio ao lado da política declarativa que você deseja desanexar e, em seguida, escolha Desanexar.
4. Na caixa de diálogo de confirmação, escolha Detach policy (Desvincular política).

   A lista de políticas declarativas anexadas é atualizada. A política entra em vigor imediatamente.

Para separar uma política declarativa 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 Políticas declarativas, escolha o nome da política que você deseja separar 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja.
4. Escolha Detach (Desvincular).
5. Na caixa de diálogo de confirmação, escolha Detach (Desvincular).

   A lista de políticas declarativas anexadas é atualizada. A política entra em vigor imediatamente.

Backup policies

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 OUs (escolher a) para encontrar a OU 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 OUs (escolher a) para encontrar a OU 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.

Tag policies

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 OUs (escolher a) para encontrar a OU 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 OUs (escolher a) para encontrar a OU 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.

Chat applications policies

Você pode desanexar uma política de aplicativos de bate-papo navegando até a política ou até a raiz, UO ou ou conta da qual você deseja desanexar a política.

Para separar uma política de aplicativos de bate-papo navegando até a raiz, a OU ou a conta à qual ela está vinculada

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 OUs (escolher a) para encontrar a OU ou a conta que você deseja. Escolha o nome da raiz, UO ou conta.
3. Na guia Políticas, escolha o botão de opção ao lado da política de aplicativos de bate-papo que você deseja desanexar e, em seguida, escolha Desanexar.
4. Na caixa de diálogo de confirmação, escolha Detach policy (Desvincular política).

   A lista de políticas de aplicativos de bate-papo anexadas foi atualizada. A política entra em vigor imediatamente.

Para separar uma política de aplicativos de bate-papo 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 Chatbot policies, escolha o nome da política que você deseja desvincular de uma raiz, OU 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 OUs (escolher a) para encontrar a OU 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 aplicativos de bate-papo anexadas foi atualizada. A política entra em vigor imediatamente.

AI services opt-out policies

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 OUs (escolher a) para encontrar a OU 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 OUs (escolher a) para encontrar a OU 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.

Security Hub policies

Você pode desanexar uma política do Security Hub navegando até a política ou até a raiz, UO ou conta da qual você deseja desanexar a política.

Para desanexar uma política do Security Hub navegando até a raiz, a OU ou a 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 OUs (escolher a) para encontrar a OU ou a conta que você deseja. Escolha o nome da raiz, UO ou conta.
3. Na guia Políticas, escolha o botão de opção ao lado da política do Security Hub que você deseja desanexar e, em seguida, escolha Desanexar.
4. Na caixa de diálogo de confirmação, escolha Detach policy (Desvincular política).

   A lista de políticas anexadas do Security Hub é atualizada. A política entra em vigor imediatamente.

Para separar uma política do Security Hub 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 de políticas do Security Hub, escolha o nome da política que você deseja separar 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 OUs (escolher

a)
para encontrar a OU ou a conta que você deseja.

4. Escolha Detach (Desvincular).
5. Na caixa de diálogo de confirmação, escolha Detach (Desvincular).

   A lista de políticas anexadas do Security Hub é atualizada. A política entra em vigor imediatamente.

AWS CLI & AWS SDKs

Anexar a política

Os exemplos de código a seguir mostram como usar o `DetachPolicy`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to detach a policy from an AWS Organizations organization,
/// organizational unit, or account.
/// </summary>
public class DetachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and uses it to call
    /// DetachPolicyAsync to detach the policy.
    /// </summary>
    public static async Task Main()
```

```
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new DetachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.DetachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
            }
            else
            {
                Console.WriteLine("Could not detach the policy.");
            }
        }
    }
```

- Para obter detalhes da API, consulte DetachPolicya Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como separar uma política de uma raiz, UO ou conta

O seguinte exemplo mostra como separar uma política de uma UO:

```
aws organizations  detach-policy  --target-id ou-examplerootid111-exampleouid111
 --policy-id p-examplepolicyid111
```

- Para obter detalhes da API, consulte DetachPolicyem Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
 attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- Para obter detalhes da API, consulte a DetachPolicyReferência da API AWS SDK for Python (Boto3).

A alteração da política entra em vigor imediatamente, afetando as permissões dos usuários, funções e recursos do IAM, se aplicável, na conta anexada ou em todas as contas na raiz ou UO anexada.

Obter informações sobre as políticas da sua organização

Este tópico 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.

Tópicos

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 da sua organização no AWS Management Console ou usando um comando 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

Os exemplos de código a seguir mostram como usar o `ListPolicies`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to list the AWS Organizations policies associated with an
/// organization.
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        // The value for the Filter parameter is required and must must be
        // one of the following:
        //     AISERVICES_OPT_OUT_POLICY
        //     BACKUP_POLICY
        //     SERVICE_CONTROL_POLICY
        //     TAG_POLICY
        var request = new ListPoliciesRequest
        {
            Filter = "SERVICE_CONTROL_POLICY",
```

```
                MaxResults = 5,
            };

            var response = new ListPoliciesResponse();
            try
            {
                do
                {
                    response = await client.ListPoliciesAsync(request);
                    response.Policies.ForEach(p => DisplayPolicies(p));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about the Organizations policies associated
        /// with an organization.
        /// </summary>
        /// <param name="policy">An Organizations policy summary to display
        /// information on the console.</param>
        private static void DisplayPolicies(PolicySummary policy)
        {
            string policyInfo = $"{policy.Id}
{policy.Name}\t{policy.Description}";

            Console.WriteLine(policyInfo);
        }
    }
```

- Para obter detalhes da API, consulte ListPoliciesa Referência AWS SDK para .NET da API.

CLI

AWS CLI

Para recuperar uma lista de todas as políticas de um determinado tipo de uma organização

O exemplo a seguir mostra como obter uma lista de SCPs, conforme especificado pelo parâmetro filter:

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

A saída inclui uma lista de políticas com informações resumidas:

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllS3Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid111",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Enables account admins to delegate
 permissions for any S3 actions to users and roles in their accounts."
                },
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                },
                {
                        "AwsManaged": true,
                        "Description": "Allows access to every operation",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-FullAWSAccess",
                        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
                        "Name": "FullAWSAccess"
```

```
                }
        ]
}
```

- Para obter detalhes da API, consulte ListPoliciesem Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- Para obter detalhes da API, consulte a ListPoliciesReferência da API AWS SDK for Python (Boto3).

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 OUs (escolher a) para encontrar a OU 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

Listando todas as OUs raízes e contas às quais uma política está vinculada

> **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 OUs, e contas que têm uma política específica 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 OUs, e contas que têm uma política específica 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 de root, OUs, e contas da 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 Metas mostra uma lista das raízes e contas às quais a política está anexada. OUs
   - 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

Os exemplos de código a seguir mostram como usar o `DescribePolicy`.

CLI

AWS CLI

Como obter informações sobre uma política

O seguinte exemplo mostra como solicitar informações sobre uma política:

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

A saída inclui um objeto de política que contém detalhes sobre a política:

```
{
        "Policy": {
                "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement
\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n
 \"Resource\": \"*\"\n    }\n  ]\n}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-examplepolicyid111",
                        "AwsManaged": false,
                        "Name": "AllowAllS3Actions",
                        "Description": "Enables admins to delegate S3
 permissions"
                }
        }
}
```

- Para obter detalhes da API, consulte DescribePolicyem Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- Para obter detalhes da API, consulte a DescribePolicyReferência da API AWS SDK for Python (Boto3).

Excluindo políticas da organização com AWS Organizations

Quando você não precisar mais de uma política e depois de separá-la de todas as unidades organizacionais (OUs) e contas, poderá excluí-la.

Este tópico descreve como excluir políticas com AWS Organizations. Uma política define os controles que você deseja aplicar a um grupo de Contas da AWS.

Tópicos

Exclua políticas com AWS Organizations

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.

> **Note**
>
> - Você não pode excluir nenhum SCP AWS gerenciado, como o SCP chamado. `FullAWSAccess`
> - Você não pode excluir nenhum RCP AWS gerenciado, como o RCP chamado. `RCPFullAWSAccess`

> **Permissões mínimas**
>
> Para excluir uma política, você precisa de permissão para executar a seguinte ação:
>
> - `organizations:DeletePolicy`

AWS Management Console

Service control policies (SCPs)

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. Primeiro, você deve desanexar a política que deseja excluir de todas as raízes e contas. OUs 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).

Resource control policies (RCPs)

Para excluir um RCP

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 Políticas de controle de recursos, escolha o nome do RCP que você deseja excluir.
3. Primeiro, você deve desanexar a política que deseja excluir de todas as raízes e contas. OUs 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).

Declarative policies

Para excluir uma política declarativa

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 Políticas declarativas, escolha o nome da política que você deseja excluir.
3. Primeiro, você deve desanexar a política que deseja excluir de todas as raízes e contas. OUs 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).

Backup policies

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. Primeiro, você deve desanexar a política de backup que deseja excluir de todas as raízes e contas. OUs 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).

Tag policies

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. Na página Políticas de tags, escolha a política que você deseja excluir.
3. Primeiro, você deve desanexar a política que deseja excluir de todas as raízes e contas. OUs 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).

Chat applications policies

Para excluir uma política de aplicativos de bate-papo

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 Chatbot policies, escolha o nome da política que deseja excluir.
3. Primeiro, você deve desanexar a política que deseja excluir de todas as raízes e contas. OUs 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).

AI services opt-out policies

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. Primeiro, você deve desanexar a política que deseja excluir de todas as raízes e contas. OUs 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).

Security Hub policies

Para excluir uma política do Security Hub

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 de políticas do Security Hub, escolha o nome da política que você deseja excluir.
3. Primeiro, você deve desanexar a política que deseja excluir de todas as raízes e contas. OUs 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

Os exemplos de código a seguir mostram como usar o `DeletePolicy`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
```

```
public class DeletePolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var policyId = "p-00000000";

        var request = new DeletePolicyRequest
        {
            PolicyId = policyId,
        };

        var response = await client.DeletePolicyAsync(request);

        if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
        {
            Console.WriteLine($"Successfully deleted Policy: {policyId}.");
        }
        else
        {
            Console.WriteLine($"Could not delete Policy: {policyId}.");
        }
    }
}
```

- Para obter detalhes da API, consulte DeletePolicya Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como excluir uma política

O exemplo a seguir mostra como excluir uma política de uma organização. O exemplo pressupõe que você já separou a política de todas as entidades:

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- Para obter detalhes da API, consulte DeletePolicyem Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

```
def delete_policy(policy_id, orgs_client):
    """
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.delete_policy(PolicyId=policy_id)
        logger.info("Deleted policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't delete policy %s.", policy_id)
        raise
```

- Para obter detalhes da API, consulte a DeletePolicyReferência da API AWS SDK for Python (Boto3).

Recursos de marcação AWS Organizations

Uma tag é um rótulo de atributo personalizado que você adiciona a um AWS recurso para facilitar a identificação, a organização e a 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.

Tópicos

Considerações

AWS Organizations suporta as seguintes operações de marcação quando você está conectado à 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`.

Outras considerações

Você pode visualizar as tags em qualquer um dos recursos marcáveis AWS Organizations usando o console ou chamando a `ListTagsForResource` operação.

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 os recursos em sua organização, permitindo agrupá-los por 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 controle de serviço
  - Política de controle de recursos
  - Política declarativa
  - Política de backup
  - Política de tag
  - Política de aplicativos de bate-papo
  - Política de cancelamento de serviços de IA

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
- AWS SDKs: TagResource

Para excluir tags de um recurso na sua organização

Você pode usar um dos seguintes comandos para excluir tags:

- AWS CLI: untag-resource
- AWS SDKs: UntagResource

Aprovação multipartidária para AWS Organizations

A aprovação multipartidária é um recurso AWS Organizationsque permite proteger uma lista predefinida de operações por meio de um processo de aprovação distribuído. Use a aprovação multipartidária para estabelecer fluxos de trabalho de aprovação e transformar processos de segurança em decisões baseadas em equipe.

Quando usar a aprovação multipartidária:

- Você precisa se alinhar com o princípio Zero Trust de “nunca confie, sempre verifique”
- Você precisa garantir que os humanos certos tenham acesso às coisas certas da maneira certa.
- Você precisa de uma tomada de decisão distribuída para operações sensíveis ou críticas
- Você precisa se proteger contra operações não intencionais em recursos confidenciais ou críticos
- Você precisa de análises e aprovações formais por motivos de auditoria ou conformidade

Para obter mais informações, consulte O que é aprovação multipartidária no Guia do usuário da aprovação multipartidária.

Usando AWS Organizations com outros Serviços da AWS

Você pode usar o acesso confiável para permitir que um AWS serviço suportado especificado por você, chamado de serviço confiável, execute tarefas em sua organização e em 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

É altamente recomendável que, quando a opção estiver disponível, você ative e desative o acesso confiável usando somente o console do serviço confiável AWS CLI ou seus equivalentes de operação de 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 Serviços da AWS 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 requer permissões para dois serviços: AWS Organizations e o serviço confiável. Para permitir o acesso confiável, escolha um dos seguintes cenários:

- Se você tiver credenciais com permissões em ambos AWS Organizations e no serviço confiável, habilite o acesso usando as ferramentas (console ou AWS CLI) fornecidas pelo serviço confiável. Isso permite que o serviço habilite o acesso confiável AWS Organizations em seu nome e crie 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 AWS Organizations console.
  - 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 AWS Organizations , mas outra pessoa tiver credenciais com permissões no serviço confiável, execute essas etapas na seguinte ordem:
  1. A pessoa que tem credenciais com permissões AWS Organizations deve usar o AWS Organizations console AWS CLI, o ou um AWS SDK para permitir o acesso confiável ao serviço confiável. Isso concede permissão para que outros serviços executem sua configuração necessária na organização quando a etapa seguinte (etapa 2) é realizada.

As AWS Organizations permissões mínimas são as seguintes:

- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization`— Necessário somente se você usar o AWS Organizations console

Para obter as etapas para habilitar o acesso confiável AWS Organizations, consulteComo 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 Serviços da AWS 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 o acesso de usuários e funções a um AWS serviço, você pode remover as permissões do IAM que concedem esse acesso ou usar políticas de controle de serviço (SCPs) em AWS Organizations.
> Você pode se SCPs inscrever somente em contas de membros. 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 de membros, onde você pode controlar a segurança usando SCPs.

- Se você tiver credenciais com permissões em ambos AWS Organizations e no serviço confiável, desative o acesso usando as ferramentas (console ou AWS CLI) que estão 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 AWS Organizations console.
- 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 não AWS Organizations forem as credenciais com permissões no serviço confiável, execute essas 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 Serviços da AWS que você pode usar com AWS Organizations.
  2. A pessoa com permissões AWS Organizations pode então usar o AWS Organizations console ou um AWS SDK para desativar o acesso ao serviço confiável. AWS CLI Isso remove as permissões para o serviço confiável de sua organização e de suas contas.

     As AWS Organizations permissões mínimas são as seguintes:

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization`— Necessário somente se você usar o AWS Organizations console

     Para obter as etapas para desativar o acesso confiável em AWS Organizations, consulteComo habilitar ou desabilitar o acesso confiável.

Como habilitar ou desabilitar o acesso confiável

Se você tiver permissões somente para AWS Organizations e quiser habilitar ou desabilitar o acesso confiável à sua organização em nome do administrador do outro AWS serviço, use o procedimento a seguir.

Important

É altamente recomendável que, quando a opção estiver disponível, você ative e desative o acesso confiável usando somente o console do serviço confiável AWS CLI ou seus equivalentes de operação de 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 Serviços da AWS 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 outro AWS serviço.

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 o acesso, informe ao administrador do outro AWS serviço que agora ele pode habilitar o outro serviço para trabalhar com ele 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 Disable trusted access (Desabilitar acesso confiável).

AWS CLI, AWS API

Para habilitar ou desabilitar acesso a serviço confiável

Você pode usar os seguintes AWS CLI comandos ou operações de API para ativar ou desativar o acesso confiável a serviços:

- AWS CLI: AWS organizações enable-aws-service-access

- AWS CLI: AWS organizações disable-aws-service-access
- AWS API: Habilitar AWSService acesso
- AWS API: Desativar AWSService acesso

AWS Organizations e funções vinculadas ao serviço

AWS Organizations usa funções vinculadas ao serviço do IAM para permitir que serviços confiáveis realizem tarefas em seu nome nas contas dos membros da sua 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 AWS Organizations serviço em si pode assumir esse papel. A função tem permissões que permitem AWS Organizations criar funções vinculadas a serviços para outras pessoas. 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 concorda com a solicitação, AWS Organizations cria a função vinculada ao serviço, caso ela ainda 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**
>
> AWS Organizations SCPs nunca afetam as funções vinculadas ao serviço. Essas funções são isentas de quaisquer restrições da SCP.

Usando a função vinculada ao serviço de AWSService RoleForDeclarativePolicies EC2 relatório

A função `AWSServiceRoleForDeclarativePoliciesEC2Report` vinculada ao serviço é usada por Organizations para descrever os estados dos atributos da conta para que as contas dos membros criem relatórios de Políticas Declarativas. As permissões da função são definidas noAWS política gerenciada: DeclarativePoliciesEC2Report.

Serviços da AWS que você pode usar com AWS Organizations

O AWS Organizations permite executar atividades de gerenciamento de conta em grande escala, consolidando várias Contas da AWS em uma única organização. Consolidar contas simplifica a forma como você usa outros. Serviços da AWSÉ possível utilizar os serviços de gerenciamento de várias contas disponíveis no AWS Organizations com selecionados Serviços da AWS para executar tarefas em todas as contas que são membros de sua organização.

A tabela a seguir lista os Serviços da AWS que podem ser usados com AWS Organizations o e o benefício de usar cada serviço em toda a organização.

Acesso confiável: você pode habilitar um AWS serviço da compatível para realizar operações em todas as Contas da AWS da sua organização. Para obter mais informações, consulte Usando AWS Organizations com outros Serviços da AWS.

Administrador delegado para os Serviços da AWS: um AWS serviço compatível da pode registrar uma AWS conta-membro da da da organização como administrador para as contas da organização nesse serviço. Para obter mais informações, consulte Administrador delegado para Serviços da AWS esse trabalho com Organizations.

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
AWS Gerenciamento de contas Gerencie os detalhes e metadados de todas as da Contas da AWS sua organização.	Gerencie detalhes da conta, contatos alternativos e regiões para todos os Contas da AWS na sua organização.	 Sim Saiba mais	 Sim Saiba mais	
AWS Application Migration Service	Você pode gerenciar migrações	 Sim	 Sim	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
AWS Application Migration Service O permite que as empresas acessem lift-and-shift a AWS um grande número de servidores físicos, virtuais ou em nuvem sem problemas de compatibilidade, interrupção no desempenho ou longos períodos de substituição.	em grande escala em várias contas.	Saiba mais	Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
AWS Artifact 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 Saiba mais	 Não
AWS Audit Manager Automatize a coleta contínua de evidências para ajudá-lo a auditar seu uso de serviços de nuvem.	Audite continuamente o AWS uso da em várias contas de sua organização para simplificar a forma como você avalia risco e conformidade.	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
AWS Backup Gerencie e monitore backups em todas as contas da sua organização.	Você pode configurar e gerenciar planos de backup para toda a sua organização ou para grupos de contas em suas unidades organizacionais (OUs). Você pode monitorar centralmente backups de todas as suas contas.	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
Gerenciamento de Faturamento e Custos da AWS Fornece uma visão geral dos dados de gerenciamento financeiro AWS na nuvem da e ajuda a tomar decisões mais rápidas e informadas.	Permite que os dados de alocação de custos divididos recuperem AWS Organizations informações do, se aplicável, e coletem dados de telemetria para os serviços de dados de alocação de custos divididos pelos quais o cliente optou por aceitar.	 Sim Saiba mais	 Não

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	Para obter mais informações, consulte O que é Gerenciamento de Faturamento e Custos da AWS? no guia do usuário do Billing and Cost Management.			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
StackSets do AWS CloudFormation 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	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	organização.			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
AWS CloudTrail 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 Saiba mais	 Sim Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
Amazon CloudWatch Monitore seus AWS recursos da e as aplicações que você executa AWS na em tempo real. Você pode usar CloudWatch para coletar e monitorar métricas, que são as variáveis mensuráveis para avaliar seus recursos e aplicativos.	A integração com Organizations tem dois benefícios em CloudWatch. Primeiro, ao integrar ao Organizations, você pode usar CloudWatch para descobrir e entender o estado da configuração de telemetria dos AWS recursos	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	da de uma visualização central no console. CloudWatch Em segundo lugar, quando você pode usar o Network Flow Monitor CloudWatch para obter visibilidade das métricas de desempenho da rede, ao se integrar ao			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	Organizations, você pode visualizar as informações de desempenho da rede para recursos em várias contas em vez de apenas uma conta.			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
AWS Compute Optimizer Obtenha recomendações de otimização AWS computacional.	Você poderá analisar todos os recursos que estiverem nas contas da sua organização para obter recomendações de otimização. Para obter mais informações, consulte Contas suportadas pelo Compute Optimizer no	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	Guia do usuário do AWS Compute Optimizer.			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
AWS Config Avalie e audite as configurações dos recursos da AWS .	É possível obter uma visualização do status de conformidade de toda a organização. Também é possível usar as operações de AWS Config API do para gerenciar AWS Config regras e pacotes de conformidade do Contas da AWS	 Sim Saiba mais	 Sim Saiba mais: Config Rules Pacotes de conformidade Agregação de dados de várias regiões e várias contas

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	em todas as da sua organização. 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			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	obter mais informações, consulte Registrar um administrador delegado no Guia do desenvolvedor do AWS Config .			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
AWS Control Tower Configure e controle um ambiente multiconta da AWS seguro e compatível.	Você pode configurar uma landing zone, um ambiente multiconta para todos os seus AWS recursos da. Esse ambiente inclui uma organização e entidades da organização. Você pode usar esse ambiente para aplicar regulamentações de	 Sim Saiba mais	 Não	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	conformidade em todas as suas Contas da AWS. 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 o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
Hub de Otimização de Custos da AWS Reúna recomendações de custo em todos os produtos AWS de otimização da.	Você pode facilmente identificar, filtrar e agregar recomendações de otimização de AWS custos da em suas AWS Organizations contas-membro do e AWS regiões da. Para obter mais informações, consulte Hub de Otimização de	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	Custos no Guia do usuário do Hub de Otimização de Custos.			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
Amazon Detective 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 ao AWS Organizations para garantir que o gráfico de comportamento do Detective forneça visibilidade da atividade de todas as contas da sua organização.	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
DevOpsGuru da Amazon 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.	É possível integrar ao 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 organizaç	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
	ão de todas as aplicações monitoradas.		
AWS Directory Service Configurar e executar diretórios na AWS Nuvem da ou conectar AWS os recursos da a um Microsoft Active Directory existente on-premises.	Você pode se integrar AWS Organizations para AWS Directory Service compartilhar diretórios sem interrupções entre várias contas e qualquer VPC em uma região.	 Sim Saiba mais	 Não

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
Amazon EventBridge Monitore seus AWS recursos da e as aplicações que você executa AWS na em tempo real.	É possível habilitar o compartilhamento de todos os EventBridge eventos da Amazon, anteriormente Amazon CloudWatch Events, em todas as contas de sua organização. Para obter mais informações, consulte Enviar e	 Não	 Não

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	receber eventos da Amazon EventBridge Contas da AWS no Guia do usuário da Amazon EventBridge.			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
Amazon Elastic Compute Cloud O IP Address Manager (IPAM) da Amazon VPC oferece uma capacidade de computação escalável sob demanda na Nuvem. AWS	Permita que o administrador do Organizations crie um relatório de qual é a configuração existente para contas em toda a organização ao usar o recurso de políticas declarativas.	 Sim Saiba mais	 Não

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
Amazon Elastic Kubernetes Service O painel do Amazon EKS fornece visibilidade e gerenciamento agregados de clusters Kubernetes em toda a nuvem. AWS	Permita que o administrador do Organizations visualize dados consolidados do painel sobre os recursos do cluster, incluindo distribuição de versões, status de integridade e requisitos de atualização em toda a organização.	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
AWS Firewall Manager Configurar e gerenciar centralmente regras de firewall de aplicativos web entre contas e aplicativos.	Você pode configurar e gerenciar centralmente AWS WAF as regras dem todas as contas de sua organização.	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
Amazon GuardDuty 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-membro para visualizar e gerenciar GuardDuty todas as contas de sua organização. A adição de contas-membro habilita GuardDuty automaticamente essas contas na região da seleciona da Região da AWS.	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	Você também pode automatizar a GuardDuty ativação de novas contas adicionadas à sua organização. Para obter mais informações, consulte GuardDuty Organizations in the Amazon GuardDuty User Guide.			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
AWS Health Tenha visibilidade dos eventos que podem afetar a performance de seus recursos ou gerar problemas de disponibilidade dos Serviços da AWS.	Você pode agregar AWS Health eventos do em todas as contas de sua organização.	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
AWS Identity and Access Management Controle o acesso a recursos da com segurança. AWS	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)	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	que restringem o acesso apenas aos AWS serviços da que as contas de sua organização usam. 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 o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	O gerenciamento de acesso raiz do IAM permite que você gerencie centralmente as credenciais de usuário-raiz e execute tarefas privilegiadas nas contas-membro.			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
IAM Access Analyzer Analise as políticas baseadas em recursos no seu AWS ambiente da para identificar quaisquer políticas que concedam acesso a uma entidade primária fora da sua zona de confiança.	Você pode designar uma conta-membro como administrador do IAM Access Analyzer. Para obter mais informações, consulte Habilitar o Access Analyzer no Guia do usuário do IAM.	 Sim Saiba mais	 Sim Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
Amazon Inspector Examine automaticamente AWS workloads do quanto a vulnerabilidades para descobrir EC2 instâncias da Amazon e imagens de contêiner que residem no Amazon ECR para vulnerabilidades de software e exposição de rede não intencional.	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. Para obter mais informações, consulte	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
	Gerenciar várias contas com o AWS Organizations no Guia do usuário do Amazon Inspector.		
AWS License Manager 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 Saiba mais	 Saiba mais Sim

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
Amazon Macie 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	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	pode 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 o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	organização.			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
AWS Managed Services (AMS) Relatórios de autoatendimento (SSR) Coleta dados de vários AWS serviços nativos e fornece acesso a relatórios sobre as principais ofertas de AMS. O SSR fornece as informações que você pode usar para apoiar operações, gerenciamento de configuração, gerenciamento de ativos, gerenciamento de segurança	Você pode ativar o SSR agregado, um recurso que permite que os clientes visualizem relatórios consolidados de autoatendimento em toda a organização por meio de sua conta de gerenciamento ou de uma conta de administr	 Sim Saiba mais	 Sim Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
e conformidade.	ador delegado.		
AWS Marketplace 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 de suas AWS Marketplace assinaturas de compras do entre todas as contas de sua organização.	 Sim Saiba mais	 Não

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
AWS Marketplace Marketplace privado Fornece a você um amplo catálogo de produtos disponíveis no AWS Marketplace, junto com o controle otimizado desses produtos.	Permite que você crie múltiplas experiências de mercado privado associadas a uma ou mais contas em sua organização OUs, uma ou mais, ou toda a sua organização, cada uma com seu próprio conjunto de produtos aprovados. AWS Os	 Sim Saiba mais	 Sim Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	administradores da 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 o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
AWS Marketplace Painel de insights de compras do Permite que você visualize contratos e dados de análise de custos de todas as suas AWS Marketplace compras do nas AWS contas de sua organização.	AWS Marketplace O painel de insights de compras do escuta as mudanças da organização, como uma conta ingressando na organização, e agrega dados de seus contratos correspondentes para criar seus painéis.	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
Gerenciador de rede AWS Permite que você gerencie de forma centralizada a sua principal rede do WAN da AWS Nuvem e a sua rede do AWS Transit Gateway entre AWS contas, regiões e locais on-premises da.	Você pode gerenciar e monitorar centralmente as suas redes globais com gateways de trânsito e seus recursos conectados em várias AWS contas da na sua organização.	 Sim Saiba mais	 Sim Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
Amazon Q Developer O Amazon Q Developer é um assistente conversacional habilitado por IA generativa que pode ajudar você a entender, criar, ampliar e operar AWS aplicações da.	A versão de assinatura paga do Amazon Q Developer requer integração com o Organizations.	 Sim Saiba mais	 Não

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
AWS Resource Access Manager Compartilhe AWS recursos especificados da 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.	 Sim Saiba mais	 Não	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	Para obter informações sobre reservas de capacidade e de compartilhamento, consulte o Guia EC2 do usuário da Amazon ou o Guia EC2 do usuário da Amazon. Para obter uma lista de recursos compartilháveis, consulte Recursos			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
	compartilháveis no Guia do usuário do AWS RAM .		
Explorador de recursos da AWS 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 Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
AWS Security Hub Veja o estado de sua segurança na AWS e verifique o ambiente de acordo com os padrões e as práticas recomendadas de segurança do setor de segurança.	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,	 Sim Saiba mais	 Sim Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	o que fornece uma imagem mais precisa do seu procedimento de segurança em geral.			

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
Amazon S3 Storage Lens 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 Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
AWS Resposta a incidentes de segurança AWS serviço de segurança que fornece suporte a incidentes de segurança ao vivo e assistido por humanos 24 horas por dia, 7 dias por semana, para ajudar os clientes a responder rapidamente a incidentes de segurança cibernética, como roubo de credenciais e ataques de ransomware.	Cobertura de segurança para toda a organização.	 Sim Saiba mais	 Sim Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
Amazon Security Lake 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 Saiba mais	 Sim Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
AWS Service Catalog Crie e gerencie catálogos de serviços de TI aprovados para uso na AWS.	Você pode compartilhar portfólios e copiar produtos entre contas com mais facilidade, sem compartilhar portfólio IDs.	 Sim Saiba mais	 Sim Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
Service Quotas 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 Saiba mais	 Não

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
AWS IAM Identity Center Forneça acesso de logon único para todas as contas e aplicativos de nuvem.	Os usuários podem fazer login no portal de AWS acesso do com suas credenciais corporativas e acessar os recursos em sua conta de gerenciamento designada ou nas contas-membro.	 Sim Saiba mais	 Sim Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
AWS Systems Manager Permita visibilidade e controle dos AWS recursos da.	Você pode sincronizar dados de operações Contas da AWS em todas as da sua organização usando o Systems Manager Explorer. Você pode gerenciar modelos, aprovações e relatórios de alteração para todas as contas-membro	 Sim Saiba mais	 Sim Saiba mais

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
	de sua organização a partir de uma conta de administrador delegado usando o Change Manager do Systems Manager.			
Notificações de Usuários da AWS Um local central para suas AWS notificações.	Você pode configurar e visualizar notificações de forma centralizada em todas as contas de sua organização.	 Sim Saiba mais	 Sim Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
Políticas de tag 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 Saiba mais	 Não	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
AWS Trusted Advisor Trusted Advisor O inspecion a seu AWS ambiente da e faz recomendações quando existem oportunidades de poupar, melhorar a performance do sistema ou ajudar a corrigir falhas de segurança.	Execute Trusted Advisor verificações para todos Contas da AWS em sua organização.	 Sim Saiba mais	 Sim Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado
AWS Well-Architected Tool O AWS Well-Architected Tool ajuda você a documentar o estado de suas workloads e as compara com as práticas recomendadas AWS arquitetônicas mais recentes da.	Permite que AWS WA Tool tanto o como clientes do Organizations simplifiquem o processo de compartilhamento de AWS WA Tool recursos do com outros membros de sua organização.	 Sim Saiba mais	 Não

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
IP Address Manager (IPAM) da Amazon VPC O IPAM é um recurso de VPC que facilita o planejamento, o rastreamento e o monitoramento de endereços IP de suas workloads da. AWS	Monitore o uso de endereços IP em toda a organização e compartilhe grupos de endereços IP entre contas-membro.	 Sim Saiba mais	 Sim Saiba mais	

AWS serviço	Benefícios de usar com o AWS Organizations	Suporte a acesso confiável	Suporte a administrador delegado	
Amazon VPC Reachability Analyzer 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 Saiba mais	 Sim Saiba mais	

AWS Gerenciamento de contas e AWS Organizations

AWS Gerenciamento de contas ajuda você a gerenciar as informações da conta e os metadados de todos os 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 Gerenciamento de contas na sua organização no Guia do usuário do AWS Gerenciamento de contas .

Use as informações a seguir para ajudá-lo a se integrar AWS Gerenciamento de contas com 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 AWS Organizations antes que você possa designar uma conta de membro para ser o administrador delegado desse serviço para sua organização.

Você só pode habilitar o acesso confiável usando as ferramentas Organizations.

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Gerenciamento de contas na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de AWS Gerenciamento de contas diálogo Habilitar acesso confiável para, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Gerenciamento de contas que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitá-lo AWS Gerenciamento de contas como um serviço confiável com Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Habilitar AWSService acesso

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.

Somente um administrador na conta AWS Organizations de gerenciamento pode desativar o acesso confiável com AWS Gerenciamento de contas.

Você só pode desativar o acesso confiável usando as ferramentas 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Gerenciamento de contas na lista de serviços.
4. Escolha Desabilitar acesso confiável.

5. Na caixa de AWS Gerenciamento de contas diálogo Desabilitar acesso confiável para, digite desabilitar para confirmar e escolha Desabilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Gerenciamento de contas que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas.

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

  Execute o comando a seguir para desabilitar AWS Gerenciamento de contas como um serviço confiável com Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Desativar AWSService acesso

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 Crie uma política de delegação baseada em recursos com AWS Organizations.

AWS CLI, AWS API

Se você quiser configurar uma conta de administrador delegado usando a AWS CLI ou uma das, você pode usar AWS SDKs os seguintes comandos:

- AWS CLI:

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

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 Como configurar o 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. Esse perfil permite que o Application Migration Service realize as operações suportadas nas contas de sua organização.

Você só pode excluir ou modificar esse perfil se desabilitar o acesso confiável entre o Application Migration Service e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForApplicationMigrationService`

Entidades principais de serviço usadas 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. Os perfis vinculados ao serviço usados pelo Application Migration Service concedem acesso às seguintes entidades principais de serviço:

- `mgn.amazonaws.com`

Como habilitar o acesso confiável no Application Migration Service

Ao habilitar o acesso confiável com o Application Migration Service, você pode usar o atributo de visualização global, o qual 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 habilitar 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 habilitar 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Application Migration Service na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de AWS Application Migration Service diálogo Habilitar acesso confiável para, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Application Migration Service que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute 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: Habilitar AWSService acesso

Como desabilitar o acesso confiável no Application Migration Service

Apenas um administrador na conta de gerenciamento do Organizations pode desabilitar o acesso confiável no Application Migration Service.

Você pode desativar o acesso confiável usando as ferramentas AWS Application Migration Service ou as AWS Organizations ferramentas.

> **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. No painel de navegação, escolha Serviços.
3. Escolha AWS Application Migration Service na lista de serviços.
4. Escolha Desabilitar acesso confiável.
5. Na caixa de AWS Application Migration Service diálogo Desabilitar acesso confiável para, digite desabilitar para confirmar e escolha Desabilitar acesso confiável.

6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Application Migration Service que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas.

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

  Execute 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 AWSService acesso

Como habilitar uma conta de administrador delegado para o Application Migration Service

Quando você designa uma conta-membro como um administrador delegado para a organização, os usuários e os perfis dessa conta podem executar ações administrativas no Application Migration Service que, de outra forma, só poderiam ser realizadas por usuários ou perfis na conta de gerenciamento da organização. Isso ajuda você a separar o gerenciamento da organização do gerenciamento do Application Migration Service. Para obter mais informações, consulte Como configurar o AWS Organizations no Guia do usuário do Application Migration Service.

> **Permissões mínimas**
>
> Somente um usuário ou perfil na conta de gerenciamento do Organizations pode configurar uma conta-membro como um administrador delegado do Application Migration Service na organização

AWS CLI, AWS API

Se você quiser configurar uma conta de administrador delegado usando a AWS CLI ou uma das, você pode usar AWS SDKs 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.

Como desabilitar uma conta de 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 só pode habilitar o acesso confiável usando as ferramentas Organizations.

Você pode habilitar 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. No painel de navegação, escolha Serviços.

3. Escolha AWS Artifact na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de AWS Artifact diálogo Habilitar acesso confiável para, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Artifact que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute 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: Habilitar AWSService acesso

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 só pode desativar o acesso confiável usando as ferramentas 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 aceitos por você 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Artifact na lista de serviços.
4. Escolha Desabilitar acesso confiável.
5. Na caixa de AWS Artifact diálogo Desabilitar acesso confiável para, digite desabilitar para confirmar e escolha Desabilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Artifact que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas.

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

Execute 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 AWSService acesso

AWS Audit Manager e AWS Organizations

AWS Audit Manager ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você avalia o risco e a conformidade com as regulamentações e os 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.

Ao integrar o Audit Manager com AWS Organizations, você pode reunir evidências de uma fonte mais ampla incluindo várias Contas da AWS da sua organização no escopo de suas avaliações.

Para obter mais informações, consulte Enable AWS Organizations no Guia do usuário do Audit Manager.

Use as informações a seguir para ajudá-lo a se integrar AWS Audit Manager 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 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 exige acesso confiável AWS Organizations antes que você possa designar uma conta membro para ser o administrador delegado da sua organização.

Você pode habilitar o acesso confiável usando o AWS Audit Manager console ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Audit Manager console ou as ferramentas para permitir a integração com o Organizations. Isso permite AWS Audit Manager 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 Audit Manager. Para obter mais informações, consulte esta nota.
> Se você habilitar o acesso confiável usando o AWS Audit Manager console ou as ferramentas, não precisará concluir essas 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 AWS Audit Manager console, habilitará AWS Audit Manager automaticamente o acesso confiável para você.

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

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitá-lo AWS Audit Manager como um serviço confiável com Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Habilitar AWSService acesso

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.

Somente um administrador na conta AWS Organizations de gerenciamento pode desativar o acesso confiável com AWS Audit Manager.

Você só pode desativar o acesso confiável usando as ferramentas 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desabilitar AWS Audit Manager como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Desativar AWSService acesso

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 AWS Audit Manager console, 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 uma das, você pode usar AWS SDKs os seguintes comandos:

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- AWS SDK: chame a `RegisterAccount` operação e forneça `delegatedAdminAccount` como parâmetro para delegar a conta do administrador.

AWS Backup e AWS Organizations

AWS Backup é um serviço que permite gerenciar e monitorar os AWS Backup trabalhos em sua organização. Usando AWS Backup, se você fizer login como usuário na conta de gerenciamento da organização, poderá ativar a proteção e o monitoramento de backup em toda a organização. Ele ajuda você a alcançar a conformidade usando políticas de backup para aplicar centralmente os AWS Backup planos aos recursos em todas as contas da sua organização. Ao usar os dois AWS Backup e AWS Organizations juntos, você pode obter os seguintes benefícios:

Proteção

Você pode habilitar o tipo de política de backup em sua organização e, em seguida, criar políticas de backup para anexar à raiz ou às contas da organização. OUs Uma política de backup combina um AWS Backup plano com os outros detalhes necessários para aplicar o plano automaticamente às suas contas. As políticas diretamente vinculadas a uma conta são mescladas com as políticas herdadas da raiz da organização e de qualquer controladora OUs para criar uma política eficaz que se aplique à conta. A política inclui o ID de uma função do IAM que tem permissões para ser executada AWS Backup nos recursos em suas contas. AWS Backup usa a função do IAM para realizar o backup em seu nome, conforme especificado pelo plano de backup na política efetiva.

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 AWS Backup, consulte o Guia do AWS Backup desenvolvedor.

Use as informações a seguir para ajudá-lo a se integrar AWS Backup com 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 AWS Backup console ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Backup console ou as ferramentas para permitir a integração com o Organizations. Isso permite AWS Backup 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 Backup. Para obter mais informações, consulte esta nota. Se você habilitar o acesso confiável usando o AWS Backup console ou as ferramentas, não precisará concluir essas etapas.

Para habilitar o uso de acesso confiável AWS Backup, consulte Habilitar o backup Contas da AWS em vários no Guia do AWS Backup desenvolvedor.

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.

AWS Backup requer acesso confiável AWS Organizations para permitir o monitoramento de trabalhos de backup, restauração e cópia nas contas da sua organização. Se você desabilitar o acesso confiável AWS Backup, perderá a capacidade de visualizar trabalhos fora da conta atual. O AWS Backup papel que AWS Backup cria permanece. Se você reativar posteriormente o acesso confiável, AWS Backup continuará operando como antes, sem a necessidade de reconfigurar o serviço.

Você só pode desativar o acesso confiável usando as ferramentas 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desabilitar AWS Backup como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal backup.amazonaws.com
  ```

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

- AWS API: Desativar AWSService acesso

Habilitando uma conta de administrador delegado para AWS Backup

Consulte Administrador delegado no Guia do desenvolvedor do AWS Backup .

Gerenciamento de Faturamento e Custos da AWS e AWS Organizations

Gerenciamento de Faturamento e Custos da AWS 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 Gerenciamento de Faturamento e 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 Billing and Cost Management realize as operações suportadas nas contas de sua organização.

Você só pode excluir ou modificar essa função se desabilitar o acesso confiável entre o Billing and Cost Management e o Organizations, ou se remover a conta-membro da organização.

Para obter mais informações, consulte Service-linked role permissions for Billing and Cost Management no Guia de usuário do Billing and Cost Management.

- `AWSServiceRoleForSplitCostAllocationData`

Entidades principais 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. Os perfis vinculados ao serviço usados pelo Billing and Cost Management concedem acesso às seguintes entidades principais de serviço:

O Billing and Cost Management usa a entidade principal de serviço `billing-cost-management.amazonaws.com`.

Como habilitar o acesso confiável no 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 atributo de dados de alocação de custos fracionados no Billing and Cost Management. Quando os clientes habilitam os dados de alocação de custos fracionados para o Amazon Elastic Kubernetes Service com o Amazon Managed Service for Prometheus, o acesso confiável é invocado para criar perfis vinculados aos serviços para todas as contas-membro na organização. Isso permite que os dados de alocação de custos fracionados coletem dados de telemetria dos espaços de trabalho do Amazon Managed Service for Prometheus dos clientes e realizem a alocação de custos com base nessas métricas.

Você só pode habilitar o acesso confiável usando as ferramentas 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

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitá-lo Gerenciamento de Faturamento e Custos da AWS 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: Habilitar AWSService acesso

Desativação do acesso confiável

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você só pode desativar o acesso confiável usando as ferramentas 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

Execute o comando a seguir para desabilitar Gerenciamento de Faturamento e Custos da AWS 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 AWSService acesso

AWS CloudFormation StackSets e AWS Organizations

AWS CloudFormation StackSets permite criar, atualizar ou excluir pilhas em várias Contas da AWS e Regiões da AWS com uma única operação. StackSets a integração com AWS Organizations permite que você crie conjuntos de pilhas com permissões gerenciadas por serviços, usando uma função vinculada ao serviço que tem a permissão relevante em cada conta de membro. Isso permite implantar instâncias de pilha em todas as contas-membro de sua organização. Você não precisa criar as AWS Identity and Access Management funções necessárias; 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 o acesso confiável entre StackSets e Organizations ativado, 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 delegadas

do administrador para implantar em operações específicas OUs ou realizar operações específicas de conjunto de pilhas.

Para obter mais informações sobre a integração StackSets com Organizations, consulte Working with AWS CloudFormation StackSets no Guia do AWS CloudFormation Usuário.

Use as informações a seguir para ajudá-lo a se integrar AWS CloudFormation StackSets 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 AWS CloudFormation Stacksets realize operações compatíveis nas contas da sua organização em 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 Como trabalhar com AWS CloudFormation StackSets no Guia do AWS CloudFormation usuário.

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 aos seguintes diretores de serviço:

- Gerenciamento de contas: `stacksets.cloudformation.amazonaws.com`

  Você pode modificar ou excluir essa função somente se tiver desabilitado o acesso confiável entre StackSets e Organizations.
- Contas-membro: `member.org.stacksets.cloudformation.amazonaws.com`

  Você pode modificar ou excluir essa função de uma conta somente se primeiro desativar o acesso confiável entre StackSets e Organizations, ou se primeiro remover a conta da organização ou unidade organizacional (OU) de destino.

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 na conta de gerenciamento do Organizations tem permissões para habilitar o acesso confiável a outro AWS serviço. Você pode habilitar o acesso confiável usando o console do AWS CloudFormation ou o console do Organizations.

Você só pode habilitar o acesso confiável usando AWS CloudFormation StackSets.

Para ativar o acesso confiável usando o console AWS CloudFormation Stacksets, consulte Habilitar acesso confiável AWS Organizations no Guia do AWS CloudFormation usuário.

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.

Somente um administrador em uma conta de gerenciamento do Organizations tem permissões para desativar o acesso confiável com outro AWS serviço. Você pode desabilitar o acesso confiável apenas usando o console do Organizations. Se você desabilitar o acesso confiável com Organizations enquanto estiver usando 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 desativar o acesso confiável usando o AWS CloudFormation console ou o console Organizations.

> **Important**
>
> Se você desativar o acesso confiável programaticamente (por exemplo, com AWS CLI ou com uma API), saiba que isso removerá a permissão. É melhor desativar o acesso confiável com o AWS CloudFormation console.

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. No painel de navegação, escolha Serviços.
3. Escolha AWS CloudFormation StackSets na lista de serviços.
4. Escolha Desabilitar acesso confiável.
5. Na caixa de AWS CloudFormation StackSets diálogo Desabilitar acesso confiável para, digite desabilitar para confirmar e escolha Desabilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS CloudFormation StackSets que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas.

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

  Execute o comando a seguir para desabilitar AWS CloudFormation StackSets como um serviço confiável com 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: Desativar AWSService acesso

Habilitar uma conta de administrador delegado para Stacksets AWS CloudFormation

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 de 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 do AWS 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 Organizations no Guia AWS 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 do 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

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute 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: Habilitar AWSService acesso

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 da 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 nos armazenamentos de dados de eventos para aplicá-los à organização.

Para converter uma trilha no nível da conta ou um armazenamento de dados de eventos em uma trilha ou um 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-trailcomande e inclua o `--is-organization-trail` parâmetro.
  - Para atualizar um armazenamento de dados de eventos, execute o update-event-data-storecomande 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 do 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 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. No painel de navegação, escolha Serviços.
3. Escolha AWS CloudTrail na lista de serviços.
4. Escolha Desabilitar acesso confiável.
5. Na caixa de AWS CloudTrail diálogo Desabilitar acesso confiável para, digite desabilitar para confirmar e escolha Desabilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS CloudTrail que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas.

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

  Execute 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 AWSService acesso

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.

Amazon CloudWatch e AWS Organizations

Você pode usar AWS Organizations para a Amazon CloudWatch nos seguintes casos de uso:

- Descubra e entenda o estado da configuração de telemetria dos AWS recursos da de uma visualização central no console do CloudWatch . Isso simplifica o processo de auditoria das configurações de coleta de telemetria para vários tipos de recursos em toda a organização ou conta da. AWS Você deve ativar o acesso confiável para usar a configuração de telemetria em toda a sua organização.

  Para obter mais informações, consulte Auditoria de configurações de CloudWatch telemetria no Guia do usuário da Amazon. CloudWatch
- Trabalhe com várias contas no Network Flow Monitor, um recurso do Amazon CloudWatch Network Monitoring. O Network Flow Monitor fornece visibilidade quase em tempo real do desempenho da rede para tráfego entre EC2 instâncias da Amazon. Depois de ativar o acesso confiável para integração com o Organizations, você pode criar um monitor para visualizar os detalhes do desempenho da rede em várias contas.

  Para obter mais informações, consulte Initialize Network Flow Monitor para monitoramento de várias contas no Guia CloudWatch do usuário da Amazon.

Use as informações a seguir para ajudá-lo a integrar a Amazon CloudWatch ao AWS Organizations.

Funções vinculadas ao serviço, criadas quando você habilitou a integração

Crie a seguinte função vinculada ao serviço na conta de gerenciamento da sua organização. A função vinculada ao serviço é criada automaticamente nas contas dos membros quando você habilita o acesso confiável. Essa função CloudWatch permite que o realize as operações suportadas nas contas de sua organização. Você pode excluir ou modificar essa função apenas se desabilitar

o acesso confiável entre o CloudWatch e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForObservabilityAdmin`

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 CloudWatch concedem acesso às seguintes entidades de serviço primárias:

- `observabilityadmin.amazonaws.com`
- `networkflowmonitor.amazonaws.com`
- `topology.networkflowmonitor.amazonaws.com`

Habilitar o acesso confiável no CloudWatch

Para obter informações sobre as permissões de que você precisa para ativar o acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você pode habilitar o acesso confiável usando o CloudWatch console da Amazon ou o AWS Organizations console do.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do CloudWatch console ou das ferramentas da Amazon para habilitar a integração com o Organizations. Isso permite que a Amazon CloudWatch 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 pela Amazon CloudWatch. Para obter mais informações, consulte esta nota.
> Se você habilitar o acesso confiável usando o CloudWatch console ou as ferramentas da Amazon, não é necessário concluir estas etapas.

Para ativar o acesso confiável usando o CloudWatch console do

Consulte Como ativar a auditoria de CloudWatch telemetria no Guia do usuário da Amazon CloudWatch .

Ao ativar o acesso confiável CloudWatch, você ativa a auditoria de telemetria e pode trabalhar com várias contas no Monitor de Fluxo de Rede.

Você pode habilitar o acesso confiável usando o AWS Organizations console do, executando um AWS CLI comando da 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. No painel de navegação, escolha Serviços.
3. Escolha Amazon CloudWatch na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de CloudWatch diálogo Habilitar acesso confiável para a Amazon, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for o administrador apenas do AWS Organizations, informe ao administrador da Amazon CloudWatch que ele agora pode habilitar esse serviço a AWS Organizations partir do console do.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os AWS CLI comandos da ou as operações da API a seguir para habilitar o acesso ao serviço confiável:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitar a Amazon CloudWatch como um serviço confiável com o Organizations.

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal observabilityadmin.amazonaws.com
```

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

- AWS API: Habilitar AWSService acesso

Desative o acesso confiável com CloudWatch

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 a Amazon CloudWatch ou as AWS Organizations ferramentas do.

> **Important**
>
> É altamente recomendável, sempre que possível, o uso do CloudWatch console ou das ferramentas da Amazon para desabilitar a integração com o Organizations. Isso permite que a Amazon CloudWatch 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 pela Amazon CloudWatch.
> Se você desabilitar o acesso confiável usando o CloudWatch console ou as ferramentas da Amazon, não é necessário concluir estas etapas.

Para desabilitar o acesso confiável usando o CloudWatch console do

Consulte Desativar a auditoria de CloudWatch telemetria no Guia do usuário da Amazon CloudWatch

Quando você desativa o acesso confiável CloudWatch, a auditoria de telemetria não está mais ativa e você não pode mais trabalhar com várias contas no Monitor de Fluxo de Rede.

Você pode desabilitar o acesso confiável executando um AWS CLI comando da 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

Use os AWS CLI comandos da ou as operações da API a seguir para desabilitar o acesso ao serviço confiável:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desabilitar a Amazon CloudWatch como um serviço confiável com o Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal observabilityadmin.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Desativar AWSService acesso

Registrar uma conta de administrador delegado para CloudWatch

Quando você registra uma conta-membro como uma conta de administrador delegado para a organização, os usuários e funções dessa conta podem executar ações administrativas CloudWatch que, de outra forma, só podem ser executadas por usuários ou funções registrados com a conta de gerenciamento da organização. O uso de uma conta de administrador delegado ajuda você a separar o gerenciamento da organização do gerenciamento de recursos do. CloudWatch

> **Permissões mínimas**
>
> Somente um administrador na conta de gerenciamento do Organizations pode registrar uma conta-membro como uma conta de administrador delegado para o CloudWatch na organização.

É possível registrar uma conta de administrador delegado ao usar o CloudWatch console ou a operação da `RegisterDelegatedAdministrator` API do Organizations com o AWS Command Line Interface ou um SDK.

Para obter informações sobre como registrar uma conta de administrador delegado usando o CloudWatch console, consulte Ativando a auditoria de CloudWatch telemetria no Guia do usuário da Amazon. CloudWatch

Ao registrar uma conta de administrador delegado no CloudWatch, você pode usar a conta para operações de gerenciamento com auditoria de telemetria e com o Monitor de fluxo de rede.

Cancelar o registro de um administrador delegado para CloudWatch

> **Permissões mínimas**
>
> Somente um administrador conectado com a conta de gerenciamento do Organizations pode cancelar o registro de uma conta de administrador delegado para o CloudWatch na organização.

Você pode cancelar o registro da conta do administrador delegado ao usar o CloudWatch console ou a operação da `DeregisterDelegatedAdministrator` API do Organizations com o AWS Command Line Interface ou um SDK. Para obter mais informações, consulte Cancelamento do registro de uma conta de administrador delegado no Guia do usuário da Amazon. CloudWatch

Ao cancelar o registro de uma conta de administrador delegado CloudWatch, você não pode mais usar a conta para operações de gerenciamento com auditoria de telemetria e com o Monitor de fluxo de rede.

AWS Compute Optimizer e AWS Organizations

AWS Compute Optimizer é um serviço que analisa as métricas de configuração e utilização de seus AWS recursos. Exemplos de recursos incluem instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e grupos de 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 Optimizer Guia do usuário do .

Use as informações a seguir para ajudá-lo a se integrar AWS Compute Optimizer 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 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 AWS Compute Optimizer console ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Compute Optimizer console ou as ferramentas para permitir a integração com o Organizations. Isso permite AWS Compute Optimizer 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 Compute Optimizer. Para obter mais informações, consulte esta nota.
> Se você habilitar o acesso confiável usando o AWS Compute Optimizer console ou as ferramentas, não precisará concluir essas 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 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Compute Optimizer na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de AWS Compute Optimizer diálogo Habilitar acesso confiável para, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Compute Optimizer que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitá-lo AWS Compute Optimizer como um serviço confiável com 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: Habilitar AWSService acesso

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.

Somente um administrador na conta AWS Organizations de gerenciamento pode desativar o acesso confiável com AWS Compute Optimizer.

Você pode desativar o acesso confiável executando um AWS CLI comando do 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desabilitar AWS Compute Optimizer como um serviço confiável com 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: Desativar AWSService acesso

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 uma das, você pode usar AWS SDKs os seguintes comandos:

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal compute-optimizer.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.

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 o AWS AWS CLI, consulte deregister-delegated-administratorna Referência de AWS AWS CLI Comandos.

AWS Config e AWS Organizations

A agregação de dados de várias contas e várias regiões AWS Config permite agregar AWS Config dados de várias contas 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 AWS Config que coleta AWS Config dados de várias contas e regiões de origem. Crie um agregador na região em que você deseja ver os dados agregados AWS Config . Ao criar um agregador, você pode optar por adicionar uma conta individual IDs ou sua organização. Para obter mais informações sobre AWS Config, consulte o Guia do AWS Config desenvolvedor.

Você também pode usar AWS Config APIspara gerenciar AWS Config regras Contas da AWS em toda a sua organização. Para obter mais informações, consulte Como ativar AWS Config regras em todas as contas da sua organização no Guia do AWS Config desenvolvedor.

Use as informações a seguir para ajudá-lo a se integrar AWS Config com AWS Organizations.

Perfis vinculados ao serviço

A função vinculada ao serviço a seguir AWS Config permite realizar operações suportadas nas contas da sua organização.

- `AWSServiceRoleForConfig`

Saiba mais sobre como criar essa função em Permissões para a função do IAM atribuída AWS Config no Guia do AWS Config desenvolvedor.

Saiba mais sobre como AWS Config usar funções vinculadas a serviços em Como usar funções vinculadas a serviços no Guia do desenvolvedor AWS ConfigAWS Config

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 ativar o acesso confiável usando o AWS Config console ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Config console ou as ferramentas para permitir a integração com o Organizations. Isso permite AWS Config 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 Config. Para obter mais informações, consulte esta nota. Se você habilitar o acesso confiável usando o AWS Config console ou as ferramentas, não precisará concluir essas etapas.

Para habilitar o acesso confiável usando o AWS Config console

Para permitir o acesso confiável ao AWS Organizations uso AWS Config, crie um agregador de várias contas e adicione a organização. Para obter informações sobre como configurar um agregador de várias contas, consulte Criação de agregadores no Guia do desenvolvedor do AWS Config .

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Config na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de AWS Config diálogo Habilitar acesso confiável para, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Config que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitá-lo AWS Config como um serviço confiável com Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Habilitar AWSService acesso

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 só pode desativar o acesso confiável usando as ferramentas 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desabilitar AWS Config como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
  ```

```
    --service-principal config.amazonaws.com
```

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

- AWS API: Desativar AWSService acesso

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 Hub de Otimização de Custos no Guia do usuário do AWS Cost Management .

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 Hub de Otimização de Custos realize as operações compatíveis com as contas de sua organização.

Você só pode excluir ou modificar esse perfil se desabilitar o acesso confiável entre o Hub de Otimização de Custos e o Organizations, ou se você remover a conta-membro da organização.

Para obter mais informações, consulte Permissões de perfil vinculado ao serviço para o Hub de Otimização de Custos no Guia do usuário do AWS Cost Management .

- `AWSServiceRoleForCostOptimizationHub`

Entidades principais de serviço usadas pelo Hub de Otimização de Custos

O Hub de Otimização de Custos usa a entidade principal de serviço `cost-optimization-hub.bcm.amazonaws.com`.

Como habilitar o acesso confiável no Hub de Otimização de Custos

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 organização e inclui todas as contas-membro dela, o acesso confiável ao Hub de Otimização de Custos é habilitado automaticamente na conta da organização.

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Escolha Hub de Otimização de Custos da AWS na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de Hub de Otimização de Custos da AWS diálogo Habilitar acesso confiável para, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. 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 para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute 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: Habilitar AWSService acesso

Desativação do acesso confiável

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você só pode desativar o acesso confiável usando as ferramentas Organizations.

> **Important**
>
> Se você desabilitar o acesso confiável do Hub de Otimização de Custos depois de aceitar a opção, o Hub de Otimização de Custos negará o acesso às recomendações para as contas de membros da organização. Além disso, as contas-membro da organização não estão habilitadas para o Hub de Otimização de Custos. Saiba mais em Acesso confiável ao Hub de Otimização de Custos e Organizations no Guia do usuário do AWS Cost Management .

Você pode desativar o acesso confiável executando um AWS CLI comando do 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

Execute 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 AWSService acesso

Como habilitar uma conta de administrador delegado para o Hub de Otimização de Custos

Quando você designa uma conta-membro como administrador delegado para a organização, a conta designada pode recuperar as recomendações do Hub de Otimização de Custos para todas as contas da sua organização e gerenciar as preferências do Hub de Otimização de Custos, oferecendo maior flexibilidade para identificar centralmente as oportunidades de otimização 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 Hub de Otimização de Custos na organização:

Para obter instruções sobre como habilitar uma conta de administrador delegado para o Hub de Otimização de Custos, consulte Delegar uma conta de administrador no Guia do usuário do AWS Cost Management .

Como desabilitar uma conta de administrador delegado para o Hub de Otimização de Custos

Somente um administrador na conta de gerenciamento do Organizations pode remover um administrador delegado para o Hub de Otimização de Custos.

Para desabilitar a conta do administrador delegado do Hub de Otimização de Custos usando o console do Hub de Otimização de Custos , consulte Delegar uma conta de administrador no Guia do usuário AWS Cost Management .

Para remover um administrador delegado usando a AWS CLI, `deregister-delegated-administrator`consulte a Referência da AWS Config CLI.

AWS Control Tower e AWS Organizations

AWS Control Tower oferece uma maneira simples de configurar e administrar um ambiente com AWS várias contas, seguindo as melhores práticas prescritivas. AWS Control Tower a orquestração amplia as capacidades do. AWS Organizations AWS Control Tower aplica controles preventivos e de detetive (grades de proteção) para ajudar a evitar que suas organizações e contas se afastem das melhores práticas (deriva).

AWS Control Tower a orquestração amplia as capacidades do. AWS Organizations

Para obter mais informações, consulte o Guia do usuário do AWS Control Tower .

Use as informações a seguir para ajudá-lo a se integrar AWS Control Tower com AWS Organizations.

Funções necessárias para a integração

A função `AWSControlTowerExecution` deve estar presente em todas as contas cadastradas. Ele permite AWS Control Tower gerenciar suas contas individuais e relatar informações sobre elas às suas contas de Auditoria e Arquivo de Registros.

Para saber mais sobre as funções usadas por AWS Control Tower, consulte Como AWS Control Tower funciona com funções para criar e gerenciar contas e Como usar políticas baseadas em identidade (políticas do IAM) para. AWS Control Tower

Diretores de serviço usados por AWS Control Tower

AWS Control Tower usa o principal do `controltower.amazonaws.com` serviço.

Habilitar o acesso confiável no AWS Control Tower

AWS Control Tower usa acesso confiável para detectar desvios para 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 só pode habilitar o acesso confiável usando as ferramentas 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 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

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitá-lo AWS Control Tower como um serviço confiável com Organizations.

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

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

- AWS API: Habilitar AWSService acesso

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 só pode desativar o acesso confiável usando as ferramentas Organizations.

> **Important**
>
> A desativação AWS Control Tower do 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 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desabilitar AWS Control Tower como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

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

- AWS API: Desativar AWSService acesso

Detective da Amazon 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.

AWS Organizations O uso permite que você garanta 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 ajudá-lo a integrar o Amazon Detective 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. 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. Detective exige acesso confiável AWS Organizations antes que você possa designar uma conta de membro para ser o administrador delegado desse serviço em sua organização.

Você só pode habilitar o acesso confiável usando as ferramentas Organizations.

Você pode ativar o acesso confiável usando o AWS Organizations console.

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. No painel de navegação, escolha Serviços.
3. Escolha Amazon Detective na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de diálogo Enable trusted access for Amazon Detective, digite enable para confirmar e selecione Enable trusted access.
6. Se você for administrador do Only AWS Organizations, diga ao administrador do Amazon Detective que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviços.

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.

Somente um administrador na conta AWS Organizations de gerenciamento pode desativar o acesso confiável com o Amazon Detective.

Você só pode desativar o acesso confiável usando as ferramentas Organizations.

Você pode desativar o acesso confiável usando o AWS Organizations console.

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. No painel de navegação, escolha Serviços.
3. Escolha Amazon Detective na lista de serviços.
4. Escolha Desabilitar acesso confiável.

5. Na caixa de diálogo Desativar acesso confiável para Amazon Detective, digite desabilitar para confirmar e, em seguida, escolha Desativar acesso confiável.
6. Se você for administrador de apenas AWS Organizations, diga ao administrador do Amazon Detective que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas;.

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 uma das, você pode usar AWS SDKs os seguintes comandos:

- AWS CLI:

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

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, métricas e eventos de aplicativos 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 permite o suporte a várias contas com AWS Organizations, para que você possa designar uma conta de 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 Monitore contas em toda a sua organização no Guia do usuário do Amazon DevOps Guru.

Use as informações a seguir para ajudá-lo a integrar o Amazon DevOps Guru 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. Essa função permite que o DevOps Guru 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 DevOps Guru e o Organizations, ou se remover a conta do 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 aos seguintes diretores de serviço:

- `devops-guru.amazonaws.com`

Para obter mais informações, consulte Usando funções vinculadas a serviços 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 Guru habilita automaticamente o acesso confiável ao DevOps DevOps Guru para sua organização. DevOpsO Guru exige acesso confiável AWS Organizations antes que você possa designar uma conta de membro para ser o administrador delegado desse serviço para sua organização.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o console ou as ferramentas do Amazon DevOps Guru para permitir a integração com Organizations. Isso permite que o Amazon DevOps Guru execute qualquer configuração necessária, como criar os recursos necessários para o serviço. Prossiga com essas etapas somente se você não conseguir

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 AWS Organizations console ou o console 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 Serviços, encontre a linha do Amazon DevOps Guru, 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 Amazon DevOps Guru que agora ele pode habilitar esse serviço usando seu console para trabalhar com AWS Organizations ele.

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 Amazon DevOps Guru
2. Escolha Enable trusted access (Habilitar acesso confiável).

Para desativar 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.

Somente um administrador na conta AWS Organizations de gerenciamento pode desativar o acesso confiável com o Amazon DevOps Guru.

Você só pode desativar o acesso confiável usando as ferramentas Organizations.

Você pode desativar o acesso confiável usando o AWS Organizations console.

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. No painel de navegação, escolha Serviços.
3. Escolha Amazon DevOps Guru na lista de serviços.
4. Escolha Desabilitar acesso confiável.
5. Na caixa de diálogo Desativar acesso confiável para o Amazon DevOps Guru, digite desabilitar para confirmar e, em seguida, escolha Desativar acesso confiável.
6. Se você for administrador de apenas AWS Organizations, diga ao administrador do Amazon DevOps Guru que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas;.

Habilitando uma conta de administrador delegado para DevOps o Guru

A conta de administrador delegado do DevOps Guru pode ver os dados de insights de todas as contas de membros que estão integradas ao DevOps Guru pela organização. Para obter informações sobre como um administrador delegado gerencia as contas da organização, consulte Monitorar contas em toda a organização no Guia do usuário do Amazon DevOps Guru.

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado para o DevOps Guru.

Você pode especificar uma conta de administrador delegado no console do DevOps Guru ou usando a operação `RegisterDelegatedAdministrator` CLI ou SDK do Organizations.

> **Permissões mínimas**
>
> Somente um usuário ou função na conta de gerenciamento da Organizations pode configurar uma conta de 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 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 uma das, você pode usar AWS SDKs os seguintes comandos:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal devops-guru.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 Guru DevOps

Você pode remover o administrador delegado usando o console do DevOps Guru ou usando a operação `DeregisterDelegatedAdministrator` CLI ou SDK do Organizations. Para obter informações sobre como remover um administrador delegado usando o console do DevOps Guru, consulte Monitore contas em toda a sua organização no Guia do usuário do Amazon DevOps Guru.

AWS Directory Service e AWS Organizations

AWS Directory Service para Microsoft Active Directory, ou AWS Managed Microsoft AD, permite que você execute o Microsoft Active Directory (AD) como um serviço gerenciado. AWS Directory Service facilita a configuração e a execução de diretórios na AWS nuvem ou a conexão de seus AWS recursos a um Microsoft Active Directory local existente. AWS Managed Microsoft AD também se integra perfeitamente AWS Organizations para permitir o compartilhamento contínuo 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.

Para compartilhar um AWS Directory Service em toda a organização, a organização deve ter Todos os recursos habilitados e o diretório deve estar na conta de gerenciamento da organização.

Use as informações a seguir para ajudá-lo a se integrar AWS Directory Service com 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 AWS Directory Service console ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Directory Service console ou as ferramentas para permitir a integração com o Organizations. Isso permite AWS Directory 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 Directory Service. Para obter mais informações, consulte esta nota.
>
> Se você habilitar o acesso confiável usando o AWS Directory Service console ou as ferramentas, não precisará concluir essas etapas.

Para habilitar o acesso confiável usando o AWS Directory Service console

Para compartilhar um diretório, o que habilita automaticamente o acesso confiável, consulte Compartilhar seu diretório no Guia de administração do AWS Directory Service . Para step-by-step obter instruções, consulte Tutorial: Compartilhando seu diretório AWS gerenciado do Microsoft AD.

Você pode ativar o acesso confiável usando o AWS Organizations console.

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. No painel de navegação, escolha Serviços.
3. Escolha AWS Directory Service na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de diálogo Enable trusted access for AWS Directory Service, digite enable para confirmar e selecione Enable trusted access..
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Directory Service que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

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 AWS Organizations enquanto estiver usando 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 só pode desativar o acesso confiável usando as ferramentas Organizations.

Você pode desativar o acesso confiável usando o AWS Organizations console.

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. No painel de navegação, escolha Serviços.

3. Escolha AWS Directory Service na lista de serviços.
4. Escolha Desabilitar acesso confiável.
5. Na caixa de AWS Directory Service diálogo Desabilitar acesso confiável para, digite desabilitar para confirmar e escolha Desabilitar acesso confiável.
6. Se você for administrador de apenas AWS Organizations, informe ao administrador AWS Directory Service que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas;.

Amazon Elastic Compute Cloud e AWS Organizations

O Amazon Elastic Compute Cloud fornece capacidade de computação escalável e sob demanda na nuvem. AWS Ao usar a Amazon EC2 with Organizations, você permite que o administrador do Organizations crie um relatório de qual é a configuração existente para contas em toda a organização depois de usar o recurso Políticas Declarativas EC2 da Amazon.

Use as informações a seguir para ajudá-lo a integrar o Amazon Elastic Compute Cloud 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. Essa função permite que EC2 a Amazon 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 a Amazon EC2 e a Organizations ou se remover a conta do membro da organização.

- `AWSServiceRoleForDeclarativePoliciesEC2Report`

Princípios de serviço usados pela Amazon EC2

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 Amazon EC2 concedem acesso às seguintes entidades de serviço:

- `ec2.amazonaws.com`

Habilitando o acesso confiável com a Amazon EC2

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Para permitir que o administrador do Organizations crie um relatório sobre qual é a configuração existente para contas em toda a organização, você deve habilitar o acesso confiável.

Você só pode habilitar o acesso confiável usando as ferramentas Organizations.

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Escolha Amazon Elastic Compute Cloud na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de diálogo Habilitar acesso confiável para Amazon Elastic Compute Cloud, digite habilitar para confirmar e, em seguida, escolha Habilitar acesso confiável.
6. Se você for administrador de apenas AWS Organizations, diga ao administrador do Amazon Elastic Compute Cloud que agora ele pode permitir que esse serviço funcione a AWS Organizations partir do console de serviços.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

Execute o comando a seguir para habilitar o Amazon Elastic Compute Cloud como um serviço confiável com Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal ec2.amazonaws.com
```

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

- AWS API: Habilitar AWSService acesso

Desativação do acesso confiável

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você só pode desativar o acesso confiável usando as ferramentas Organizations.

Você pode desativar o acesso confiável executando um AWS CLI comando do 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desativar o Amazon Elastic Compute Cloud como um serviço confiável com Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal ec2.amazonaws.com
```

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

- AWS API: Desativar AWSService acesso

Amazon Elastic Kubernetes Service e AWS Organizations

O painel do Amazon Elastic Kubernetes Service é um painel consolidado que você pode usar para monitorar, gerenciar e obter visibilidade dos clusters do Kubernetes em várias regiões e contas. AWS AWS O EKS Dashboard fornece controle e insights abrangentes para sua infraestrutura do Amazon EKS por meio de uma interface centralizada.

O painel do Amazon Elastic Kubernetes Service permite que você acompanhe clusters programados para atualizações, controle os custos do plano do projeto, analise as informações do cluster e monitore as distribuições de grupos de nós em toda a sua organização. Seus AWS administradores podem visualizar dados agregados sobre recursos do cluster, incluindo status de integridade, distribuição de versões e configurações complementares por meio de diferentes opções de visualização, incluindo gráficos, listas de recursos e mapas geográficos. O painel se integra ao AWS Organizations para fornecer visibilidade segura entre contas e regiões de seus recursos do EKS.

Use as informações a seguir para integrar o Amazon Elastic Kubernetes Service 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 usando o console do Amazon Elastic Kubernetes Service. Esse perfil permite que o Amazon EKS realize operações válidas nas contas da sua organização. Você pode excluir ou modificar essa função apenas se desabilitar o acesso confiável entre o Amazon Elastic Kubernetes Service e o Organizations.

Se você habilitar o acesso confiável no console do Organizations, na CLI ou no SDK, o perfil vinculado ao serviço não é criado automaticamente.

- `AWSServiceRoleForAmazonEKSDashboard`

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 Amazon EKS concedem acesso às seguintes entidades principais de serviço:

- `dashboard.eks.amazonaws.com`

Habilitar o acesso confiável no Amazon EKS

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Para habilitar o acesso confiável usando o console do Amazon EKS

Consulte Habilitar acesso confiável no Guia do usuário do Amazon EKS.

Como desabilitar o acesso confiável no Amazon EKS

Para desabilitar o acesso confiável usando o console do Amazon EKS

Consulte Desativar o acesso confiável no Guia do usuário do Amazon EKS.

Como habilitar uma conta de administrador delegado para o Amazon EKS

O administrador da conta de gerenciamento pode delegar permissões administrativas do Amazon EKS a uma conta de membro designada, conhecida como administrador delegado.

Contas de gerenciamento e contas de administrador delegado podem visualizar o painel do Amazon EKS.

Para habilitar uma conta de administrador delegado

Consulte Habilitar uma conta de administrador delegado no Guia do usuário do Amazon EKS.

Como desabilitar um administrador delegado para o Amazon EKS

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado do Amazon EKS.

Para desabilitar uma conta de administrador delegado

Consulte Desativar uma conta de administrador delegado no Guia do usuário do Amazon EKS.

AWS Firewall Manager e AWS Organizations

AWS Firewall Manager é um serviço de gerenciamento de segurança que você usa para configurar e gerenciar centralmente as regras de firewall e outras proteções em todos os Contas da AWS

aplicativos da sua organização. Usando o Firewall Manager, você pode implantar AWS WAF regras, criar AWS Shield Advanced proteções, configurar e auditar grupos de segurança da Amazon Virtual Private Cloud (Amazon VPC) e AWS Network Firewall implantá-los. 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 AWS Firewall Manager, consulte o Guia do AWS Firewall Manager desenvolvedor.

Use as informações a seguir para ajudá-lo a se integrar AWS Firewall Manager 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 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 AWS Firewall Manager console ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Firewall Manager console ou as ferramentas para permitir a integração com o Organizations. Isso permite AWS Firewall Manager 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 Firewall Manager. Para obter mais informações, consulte esta nota.
> Se você habilitar o acesso confiável usando o AWS Firewall Manager console ou as ferramentas, não precisará concluir essas etapas.

Você deve entrar com sua conta AWS Organizations de gerenciamento e configurar uma conta dentro da organização como conta de AWS Firewall Manager administrador. 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 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Firewall Manager na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de AWS Firewall Manager diálogo Habilitar acesso confiável para, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Firewall Manager que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitá-lo AWS Firewall Manager como um serviço confiável com Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Habilitar AWSService acesso

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 desativar o acesso confiável usando as ferramentas AWS Firewall Manager ou as AWS Organizations ferramentas.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Firewall Manager console ou as ferramentas para desativar a integração com o Organizations. Isso permite AWS Firewall Manager 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 Firewall Manager.
> Se você desabilitar o acesso confiável usando o AWS Firewall Manager console ou as ferramentas, não precisará concluir essas etapas.

Para desabilitar acesso confiável usando o console do Firewall Manager

Você pode alterar ou revogar a conta do AWS Firewall Manager administrador seguindo as instruções em Como designar uma conta diferente como a conta do AWS Firewall Manager administrador no Guia do AWS Firewall Manager desenvolvedor.

Se você revogar a conta de administrador, deverá entrar na conta AWS Organizations de gerenciamento e definir uma nova conta de administrador para AWS Firewall Manager.

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. No painel de navegação, escolha Serviços.
3. Escolha AWS Firewall Manager na lista de serviços.
4. Escolha Desabilitar acesso confiável.
5. Na caixa de AWS Firewall Manager diálogo Desabilitar acesso confiável para, digite desabilitar para confirmar e escolha Desabilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Firewall Manager que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas.

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

  Execute o comando a seguir para desabilitar AWS Firewall Manager como um serviço confiável com Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal fms.amazonaws.com
```

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

- AWS API: Desativar AWSService acesso

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 administradora do Firewall Manager para a organização, consulte Definir a conta de AWS Firewall Manager administrador no Guia do AWS Firewall Manager desenvolvedor.

Amazon GuardDuty e AWS Organizations

GuardDuty A Amazon é um serviço contínuo de monitoramento de segurança que analisa e processa várias fontes de dados, usando feeds de inteligência de ameaças e aprendizado de máquina para identificar atividades inesperadas, potencialmente não autorizadas e maliciosas em seu ambiente. AWS Isso pode incluir problemas como escalonamento de privilégios, uso de credenciais expostas, comunicação com endereços IP ou domínios maliciosos ou presença de malware em suas instâncias do Amazon Elastic Compute Cloud e cargas de trabalho de contêineres. URLs

Você pode ajudar a simplificar o gerenciamento GuardDuty usando Organizations para gerenciar GuardDuty todas as contas da sua organização.

Para obter mais informações, consulte Gerenciamento de GuardDuty contas AWS Organizations no Guia do GuardDuty usuário da Amazon

Use as informações a seguir para ajudá-lo a integrar a Amazon GuardDuty com 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 GuardDuty realizar operações suportadas nas contas da sua organização em sua organização. Você pode excluir uma função somente se desativar o acesso confiável entre GuardDuty e Organizations ou se remover a conta do membro da organização.

- A função `AWSServiceRoleForAmazonGuardDuty` vinculada ao serviço é criada automaticamente em contas que foram integradas ao GuardDuty Organizations. Para obter mais informações, consulte Gerenciando GuardDuty contas com Organizations no Guia GuardDuty do usuário da Amazon
- A função `AmazonGuardDutyMalwareProtectionServiceRolePolicy` vinculada ao serviço é criada automaticamente em contas que ativaram a Proteção GuardDuty contra Malware. Para obter mais informações, consulte Permissões de funções vinculadas ao serviço para proteção contra GuardDuty malware no Guia do usuário da 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 só pode habilitar o acesso confiável usando a Amazon GuardDuty.

A Amazon GuardDuty exige acesso confiável AWS Organizations antes que você possa designar uma conta de membro para ser o GuardDuty administrador da sua organização. Se você configurar um administrador delegado usando o GuardDuty console, habilitará GuardDuty automaticamente o acesso confiável para você.

No entanto, se você quiser configurar uma conta de administrador delegado usando o AWS CLI ou um dos AWS SDKs, deverá chamar explicitamente a operação Habilitar AWSService Acesso e fornecer o principal de serviço como parâmetro. Em seguida, você pode ligar EnableOrganizationAdminAccountpara delegar a conta do GuardDuty administrador.

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 só pode desativar o acesso confiável usando as ferramentas 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desativar a Amazon GuardDuty como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal guardduty.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Desativar AWSService acesso

Habilitando uma conta de administrador delegado para GuardDuty

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 GuardDuty 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 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 da 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 suas Serviços da AWS 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.

Perfis vinculados ao serviço 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

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute 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: Habilitar AWSService acesso

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 ferramentas AWS Health ou as AWS Organizations ferramentas.

> **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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute 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 AWSService acesso

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

AWS Identity and Access Management and AWS Organizations

AWS Identity and Access Management é um serviço da web para controlar com segurança o acesso aos AWS serviços.

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 restringem o acesso somente aos AWS serviços que as contas da sua organização usam.

Para obter um exemplo, consulte Uso de dados para refinar permissões para uma unidade organizacional no Guia do usuário do IAM.

O IAM permite gerenciar centralmente as credenciais do usuário raiz e realizar tarefas privilegiadas nas contas dos membros. Depois de ativar o gerenciamento de acesso raiz, que permite acesso confiável para o IAM in AWS Organizations, você pode proteger centralmente as credenciais do usuário raiz das contas dos membros. As contas dos membros não podem fazer login com o usuário-raiz nem realizar a recuperação da senha do usuário-raiz. A conta de gerenciamento ou uma conta de administrador delegado do IAM também pode realizar algumas tarefas privilegiadas nas contas

dos membros usando acesso root de curto prazo. Sessões privilegiadas de curto prazo fornecem credenciais temporárias que podem ser usadas para realizar ações privilegiadas em uma conta-membro em sua organização.

Consulte mais informações em Gerencie centralmente o acesso raiz para contas-membro no Guia do usuário do IAM.

Use as informações a seguir para ajudá-lo a se integrar AWS Identity and Access Management com AWS Organizations.

Habilitando o acesso confiável com o IAM

Quando você ativa o gerenciamento de acesso raiz, o acesso confiável é habilitado para o IAM in AWS Organizations.

Desabilitando o acesso confiável com o IAM

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 Identity and Access Management.

Você só pode desativar o acesso confiável usando as ferramentas 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Identity and Access Management na lista de serviços.
4. Escolha Desabilitar acesso confiável.

5. Na caixa de AWS Identity and Access Management diálogo Desabilitar acesso confiável para, digite desabilitar para confirmar e escolha Desabilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Identity and Access Management que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas.

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

  Execute o comando a seguir para desabilitar AWS Identity and Access Management como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal iam.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Desativar AWSService acesso

Habilitar uma conta de administrador delegado para o IAM

Quando você designa uma conta de membro como administrador delegado da organização, os usuários e funções dessa conta podem realizar tarefas privilegiadas em contas de membros que, de outra forma, só poderiam ser executadas por usuários ou funções na conta de gerenciamento da organização. Para obter mais informações, consulte Executar uma tarefa privilegiada em uma conta membro do Organizations no Guia do usuário do IAM.

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado para o IAM.

Você pode especificar uma conta de administrador delegado no console ou na API do IAM ou usando a operação da CLI ou do SDK do Organizations.

Desabilitar um administrador delegado para o IAM

Somente um administrador na conta de gerenciamento do Organizations ou na conta de administrador delegado do IAM pode remover uma conta de administrador delegado da organização. Você pode desativar a administração delegada usando a operação Organizations `DeregisterDelegatedAdministrator` CLI ou SDK.

Amazon Inspector e AWS Organizations

O Amazon Inspector é um serviço automatizado de gerenciamento de vulnerabilidades que verifica continuamente as cargas de trabalho da Amazon EC2 e de contêineres em busca de vulnerabilidades de software e exposição não intencional na rede.

Usando o Amazon Inspector, você pode gerenciar várias contas associadas simplesmente delegando uma conta de administrador para o Amazon Inspector. AWS Organizations 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 ajudá-lo a integrar o Amazon Inspector 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 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 exige acesso confiável AWS Organizations antes que você possa designar uma conta membro para ser o administrador delegado desse serviço para 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 quiser configurar uma conta de administrador delegado usando a AWS CLI ou uma AWS SDKs das, deverá chamar explicitamente `EnableAWSServiceAccess` a operação e fornecer o principal de serviço como parâmetro. Você então poderá chamar `EnableDelegatedAdminAccount` para delegar a conta de administrador do Inspector.

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

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

Execute o comando a seguir para habilitar o Amazon Inspector como um serviço confiável com Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal inspector2.amazonaws.com
```

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

- AWS API: Habilitar AWSService acesso

> **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.

Somente um administrador na conta AWS Organizations de gerenciamento pode desativar o acesso confiável com o Amazon Inspector.

Você só pode desativar o acesso confiável usando as ferramentas 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desativar o Amazon Inspector como um serviço confiável com Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal inspector2.amazonaws.com
```

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

- AWS API: Desativar AWSService acesso

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 serviço. AWS Organizations

A conta AWS Organizations de gerenciamento designa uma conta dentro da organização como a conta de administrador delegado 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 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 uma das, você pode usar AWS SDKs os seguintes comandos:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.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.

Desabilitar um administrador delegado do Amazon Inspector

Somente um administrador na conta AWS Organizations de gerenciamento 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

AWS License Manager simplifica o processo de levar licenças de fornecedores de software para a nuvem. Ao criar uma infraestrutura de nuvem AWS, você pode economizar custos usando oportunidades bring-your-own-license (BYOL), ou seja, reaproveitando seu inventário de licenças existente para uso com 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 com AWS Organizations, você pode:

- 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 na AWS. Para obter mais informações, consulte Assinaturas Linux no AWS License Manager.

Use as informações a seguir para ajudá-lo a se integrar AWS License Manager com 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 só pode habilitar o acesso confiável usando 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 entrar no console do License Manager usando sua conta AWS Organizations de gerenciamento e associá-la à sua conta do License Manager. Para obter mais informações, consulte Configurações em 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 só pode desativar o acesso confiável usando as ferramentas Organizations.

Você pode desativar o acesso confiável executando um AWS CLI comando do 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 License Manager como um serviço confiável com 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: Desativar AWSService acesso

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.

AWS Managed Services (AMS) Relatórios de autoatendimento (SSR) e AWS Organizations

AWS Managed Services (AMS) O Self-Service Reporting (SSR) coleta dados de vários AWS serviços nativos e fornece acesso a relatórios sobre as principais ofertas do AMS. O SSR fornece as informações que você pode usar para apoiar operações, gerenciamento de configuração, gerenciamento de ativos, gerenciamento de segurança e conformidade.

Depois de fazer a integração com AWS Organizations, você pode ativar os relatórios de autoatendimento agregados (SSR). Esse é um recurso do AMS que permite que os clientes do Advanced e do Accelerate visualizem seus relatórios de autoatendimento existentes agregados no nível da organização, em todas as contas. Isso lhe dá visibilidade das principais métricas operacionais, como conformidade de patches, cobertura de backup e incidentes em todas as contas gerenciadas pela AMS. AWS Organizations

Use as informações a seguir para ajudá-lo a integrar AWS Managed Services (AMS) o Self-Service Reporting (SSR) 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. Essa função permite que o AMS 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 AMS e Organizations, ou se remover a conta do membro da organização.

- `AWSServiceRoleForManagedServices_SelfServiceReporting`

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 AMS concedem acesso aos seguintes diretores de serviço:

- `selfservicereporting.managedservices.amazonaws.com`

Habilitando acesso confiável com o AMS

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 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

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitar o AWS Managed Services (AMS) Self-Service Reporting (SSR) como um serviço confiável com Organizations.

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal selfservicereporting.managedservices.amazonaws.com
```

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

- AWS API: Habilitar AWSService acesso

Desabilitando o acesso confiável com o AMS

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você só pode desativar o acesso confiável usando as ferramentas 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desativar o AWS Managed Services (AMS) Self-Service Reporting (SSR) como um serviço confiável com Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal selfservicereporting.managedservices.amazonaws.com
```

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

- AWS API: Desativar AWSService acesso

Habilitando uma conta de administrador delegado para o AMS

As contas de administrador delegado podem visualizar relatórios do AMS (como patch e backup) em todas as contas em uma única visualização agregada no console do AMS.

Você pode adicionar um administrador delegado usando o console AMS ou a API, ou usando a operação `RegisterDelegatedAdministrator` CLI ou SDK do Organizations.

Desabilitando um administrador delegado para o AMS

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado para o AMS.

Você pode remover o administrador delegado usando o console do AMS ou a API, ou usando a operação `DeregisterDelegatedAdministrator` CLI ou SDK do Organizations.

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 com o. 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 exige acesso confiável para AWS Organizations designar uma conta membro para ser a administradora do Macie de 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 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

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitar o Amazon Macie como um serviço confiável com Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Habilitar AWSService acesso

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 exige acesso confiável para AWS Organizations designar uma conta membro para ser a administradora do Macie de 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

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.

AWS Marketplace cria e gerencia licenças usadas AWS License Manager para suas compras em 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 se integrar AWS Marketplace 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 Marketplace 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 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 pela AWS Marketplace concedem acesso aos seguintes diretores de serviço:

- `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 AWS Marketplace console ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Marketplace console ou as ferramentas para permitir a integração com o Organizations. Isso permite AWS Marketplace 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 Marketplace. Para obter mais informações, consulte esta nota.
>
> Se você habilitar o acesso confiável usando o AWS Marketplace console ou as ferramentas, não precisará concluir essas etapas.

Para habilitar o acesso confiável usando o AWS Marketplace console

Consulte Criação de um perfil vinculado ao serviço AWS Marketplace no Guia do comprador do AWS Marketplace .

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Marketplace na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).

5. Na caixa de AWS Marketplace diálogo Habilitar acesso confiável para, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Marketplace que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitá-lo AWS Marketplace como um serviço confiável com 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: Habilitar AWSService acesso

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 só pode habilitar o acesso confiável usando as ferramentas 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desabilitar AWS Marketplace como um serviço confiável com 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: Desativar AWSService acesso

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 Using roles to configure Private Marketplace in AWS Marketplace no Guia do comprador do AWS Marketplace .

Use as informações a seguir para ajudá-lo a integrar o AWS Marketplace Private Marketplace 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 da sua organização quando você ativa o acesso confiável usando o console do Private AWS Marketplace Marketplace. Esse perfil permite que o Private Marketplace realize as operações compatíveis nas contas de 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 no console do Organizations, na CLI ou no SDK, o perfil vinculado ao serviço não é criado 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. Os perfis vinculados ao serviço usados pelo Private Marketplace concedem acesso às seguintes entidades principais de serviço:

- `private-marketplace.marketplace.amazonaws.com`

Como habilitar o acesso confiável no 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 Getting started with Private Marketplace no Guia do comprador do AWS Marketplace .

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Selecione AWS Marketplace Private Marketplace na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de diálogo Habilitar acesso confiável para o AWS Marketplace Private Marketplace, digite enable para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador do Only AWS Organizations, informe ao administrador do AWS Marketplace Private Marketplace que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute 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: Habilitar AWSService acesso

Como desabilitar o acesso confiável no Private Marketplace

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você só pode desativar o acesso confiável usando as ferramentas 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute 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 AWSService acesso

Como habilitar 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-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.

As contas de gerenciamento e as contas de administrador delegado podem realizar tarefas administrativas do Private Marketplace, como criar experiências, atualizar configurações de

identidade visual, 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 Criar e gerenciar um mercado privado no Guia do comprador do AWS Marketplace .

Você também pode configurar um administrador delegado usando a API `RegisterDelegatedAdministrator` do Organizations. Para obter mais informações, consulte RegisterDelegatedAdministratorna Referência de Comandos do Organizations.

Como desabilitar uma conta de administrador delegado para o Private Marketplace

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado do Private Marketplace.

É possível remover a conta de administrador delegado usando o console Private Marketplace ou API ao usar a operação `DeregisterDelegatedAdministrator` da CLI ou o SDK do Organizations.

Para desabilitar a conta do Private Marketplace de administrador delegado usando o console do Private Marketplace, consulte Criar e gerenciar um mercado privado no Guia do comprador do AWS Marketplace .

AWS Marketplace painel de informações de compras e AWS Organizations

Você usa o painel AWS Marketplace de informações de aquisição para visualizar contratos e dados de análise de custos de todas as AWS contas da sua organização. Quando integrado ao Organizations, o painel de insights de AWS Marketplace compras escuta as mudanças da organização, como uma conta ingressando na organização, e agrega dados de seus contratos correspondentes para criar seus painéis.

Para obter mais informações, consulte Procurement insights no Guia do comprador do AWS Marketplace .

Use as informações a seguir para ajudá-lo a integrar o painel AWS Marketplace de insights de compras com AWS Organizations.

Perfis vinculados ao serviço e políticas gerenciadas criadas quando você habilita a integração

Quando você ativa o painel do painel AWS Marketplace de insights de aquisição, a função `AWSServiceRoleForProcurementInsightsPolicy`vinculada ao serviço e a política `AWSServiceRoleForProcurementInsightsPolicy` AWS gerenciada são criadas.

Como habilitar o acesso confiável ao insights de compras do AWS Marketplace

Habilitar o acesso confiável concede ao painel AWS Marketplace de insights de compras a capacidade de se integrar ao serviço Organizations do cliente. AWS Marketplace O painel de insights de compras escuta as mudanças da organização, como uma conta ingressando na organização, e agrega dados de seus contratos correspondentes para criar seus painéis.

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 painel AWS Marketplace de insights de compras ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o console ou as ferramentas do painel AWS Marketplace de insights de aquisição para permitir a integração com o Organizations. Isso permite que o painel de insights de AWS Marketplace compras execute qualquer configuração necessária, como criar os recursos necessários para o serviço. Prossiga com essas etapas somente se você não conseguir habilitar a integração usando as ferramentas fornecidas pelo painel AWS Marketplace de insights de compras. Para obter mais informações, consulte esta nota.
>
> Se você habilitar o acesso confiável usando o console ou as ferramentas do painel de insights de AWS Marketplace compras, não precisará concluir essas etapas.

Para permitir o acesso confiável ativando o painel AWS Marketplace de informações de aquisição

Consulte AWS Marketplace Ativação do painel de informações de compras no Guia do AWS Marketplace comprador.

Para habilitar o acesso confiável usando as ferramentas do Organizations

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Selecione AWS Marketplace procurement insights dashboard na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de diálogo Habilitar acesso confiável para o painel de informações de AWS Marketplace aquisição, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de apenas AWS Organizations, informe ao administrador do painel de informações de AWS Marketplace compras que agora ele pode permitir que esse serviço funcione a AWS Organizations partir do console de serviços.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitar o painel AWS Marketplace de insights de compras como um serviço confiável com Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal procurement-insights.marketplace.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Habilitar AWSService acesso

Como desabilitar o acesso confiável ao insights de compras do AWS Marketplace

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você só pode desativar o acesso confiável usando as ferramentas Organizations.

Você pode desativar o acesso confiável executando um AWS CLI comando do 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desativar o painel AWS Marketplace de insights de compras como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal procurement-insights.marketplace.amazonaws.com
  ```

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

- AWS API: Desativar AWSService acesso

Habilitar uma conta de administrador delegado para obter informações AWS Marketplace sobre compras

Para configurar um administrador delegado no console de insights AWS Marketplace de compras, consulte Registro de administradores delegados > no Guia do comprador.AWS Marketplace

Você também pode configurar um administrador delegado usando a API `RegisterDelegatedAdministrator` do Organizations. Para obter mais informações, consulte RegisterDelegatedAdministratorna Referência de Comandos do Organizations.

Desabilitando um administrador delegado para obter AWS Marketplace informações sobre compras

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado para obter informações AWS Marketplace sobre compras.

Para remover um administrador delegado por meio do console de insights AWS Marketplace de compras, consulte Cancelamento do registro de administradores delegados no Guia do comprador.AWS Marketplace

É possível remover a conta de administrador delegado usando a operação `DeregisterDelegatedAdministrator` da CLI ou SDK do Organizations.

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 as configurações de várias contas (administradores enable/disable trusted access and register/deregister 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-membros

- `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.

Amazon Q Developer e AWS Organizations

O Amazon Q Developer é um assistente conversacional generativo com inteligência artificial que pode ajudar você a entender, criar, ampliar e operar AWS aplicativos. Ele também é um gerador de código de uso geral baseado em machine learning que fornece recomendações de código em tempo real. A versão de assinatura paga do Amazon Q Developer requer integração com o Organizations. Para obter mais informações, consulte Account, IAM Identity Center, and Organizations setup 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

O perfil vinculado ao serviço do `AWSServiceRoleForAmazonQDeveloper` permite que o Amazon Q Developer realize as operações suportadas em sua organização. Crie o perfil usando o console, a

API ou a CLI do Amazon Q Developer, conforme descrito em Criar um perfil vinculado ao serviço no Guia do usuário do IAM.

Se você estiver usando uma conta-membro, poderá excluir ou modificar esse perfil somente se desabilitar o acesso confiável entre o Amazon Q Developer e o Organizations ou se remover a conta-membro da organização.

Entidades principais de serviço usadas pelo Amazon Q Developer

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 Amazon Q Developer concedem acesso às seguintes entidades principais de serviço:

- `q.amazonaws.com`

Como habilitar o acesso confiável no Amazon Q Developer

O Amazon Q Developer Pro usa acesso confiável para compartilhar as configurações feitas na conta de gerenciamento do Organizations com contas-membro da mesma organização.

Por exemplo, o administrador do Amazon Q Developer Pro, trabalhando na conta de gerenciamento do Organizations, pode habilitar sugestões com referências de código. Se o acesso confiável estiver ativado, as sugestões com referências de código também serão habilitadas para todas as contas de membros dessa organização.

Você só pode habilitar o acesso confiável usando o Amazon Q Developer.

Para habilitar o acesso confiável para o Amazon Q Developer, use este procedimento.

1. Na página Settings do Amazon Q Developer, em Member account settings, selecione Edit.
2. Na janela pop-up, selecione On.
3. Escolha Salvar.

Para obter mais informações, consulte Como habilitar o acesso confiável no Guia do usuário do Amazon Q Developer.

Como desabilitar o acesso confiável no Amazon Q Developer

Você só pode desativar o acesso confiável usando as ferramentas Amazon Q Developer.

Para desabilitar o acesso confiável para o Amazon Q Developer, use este procedimento.

1. Na página Settings do Amazon Q Developer, em Member account settings, selecione Edit.
2. Na janela pop-up, selecione Off.
3. Escolha Salvar.

Para obter mais informações, consulte Como habilitar o acesso confiável no Guia do usuário do Amazon Q Developer.

AWS Resource Access Manager e AWS Organizations

AWS Resource Access Manager (AWS RAM) permite que você compartilhe AWS recursos específicos que você possui com outras pessoas Contas da AWS. É um serviço centralizado que fornece uma experiência consistente para compartilhar diferentes tipos de AWS recursos em várias contas.

Para obter mais informações sobre AWS RAM, consulte o Guia AWS RAM do usuário.

Use as informações a seguir para ajudá-lo a se integrar AWS Resource Access Manager 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 RAM 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 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 pela AWS RAM concedem acesso aos seguintes diretores de serviço:

- `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 AWS Resource Access Manager console ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Resource Access Manager console ou as ferramentas para permitir a integração com o Organizations. Isso permite AWS Resource Access Manager 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 Resource Access Manager. Para obter mais informações, consulte esta nota.
> Se você habilitar o acesso confiável usando o AWS Resource Access Manager console ou as ferramentas, não precisará concluir essas etapas.

Para habilitar o acesso confiável usando o AWS RAM console ou a CLI

Consulte Habilitar o compartilhamento com o AWS Organizations no Guia do usuário do AWS RAM .

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Resource Access Manager na lista de serviços.

4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de AWS Resource Access Manager diálogo Habilitar acesso confiável para, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Resource Access Manager que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitá-lo AWS Resource Access Manager como um serviço confiável com Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Habilitar AWSService acesso

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 desativar o acesso confiável usando as ferramentas AWS Resource Access Manager ou as AWS Organizations ferramentas.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Resource Access Manager console ou as ferramentas para desativar a integração com o Organizations. Isso permite AWS Resource Access Manager 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 Resource Access Manager.
Se você desabilitar o acesso confiável usando o AWS Resource Access Manager console ou as ferramentas, não precisará concluir essas etapas.

Para desativar o acesso confiável usando o AWS Resource Access Manager console ou a CLI

Consulte Habilitar o compartilhamento com o AWS Organizations no Guia do usuário do AWS RAM .

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. No painel de navegação, escolha Serviços.
3. Escolha AWS Resource Access Manager na lista de serviços.
4. Escolha Desabilitar acesso confiável.
5. Na caixa de AWS Resource Access Manager diálogo Desabilitar acesso confiável para, digite desabilitar para confirmar e escolha Desabilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Resource Access Manager que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas.

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

  Execute o comando a seguir para desabilitar AWS Resource Access Manager como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Desativar AWSService acesso

Explorador de recursos da AWS e AWS Organizations

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 Resource Explorer funciona em todas AWS as regiões da sua conta para simplificar suas cargas de trabalho entre regiões.

Ao integrar o Resource Explorer com AWS Organizations, você pode coletar evidências de uma fonte mais ampla incluindo várias Contas da AWS da sua organização no escopo de suas avaliações.

Use as informações a seguir para ajudá-lo a se integrar Explorador de recursos 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. 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 Resource Explorer exige acesso confiável AWS Organizations antes que você possa designar uma conta de membro para ser o administrador delegado da 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 Explorador de recursos da AWS realizar qualquer configuração necessária, como criar os recursos necessários ao 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 Explorador de recursos da AWS console, habilitará Explorador de recursos da AWS automaticamente o acesso confiável para você.

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

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitá-lo Explorador de recursos da AWS como um serviço confiável com 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: Habilitar AWSService acesso

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.

Somente um administrador na conta AWS Organizations de gerenciamento pode desativar o acesso confiável com Explorador de recursos da AWS.

Você pode desativar o acesso confiável usando as ferramentas Explorador de recursos da AWS ou as AWS Organizations ferramentas.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o Explorador de recursos da AWS console ou as ferramentas para desativar a integração com o Organizations. Isso permite Explorador de recursos da AWS 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 Explorador de recursos da AWS.
> Se você desabilitar o acesso confiável usando o Explorador de recursos da AWS console ou as ferramentas, não precisará concluir essas etapas.

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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desabilitar Explorador de recursos da AWS como um serviço confiável com 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: Desativar AWSService acesso

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. Você pode compartilhar visualizações de várias contas com qualquer conta da sua organização AWS Resource Access Manager por meio da criação de 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 Explorador de recursos da AWS console, o Resource Explorer 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 uma das, você pode usar AWS SDKs os seguintes comandos:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.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 `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 Contas da AWS produtos de parceiros terceirizados, usados por Serviços da AWS você e 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 do AWS 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.

Desabilitar o acesso confiável com o Security Hub

Para obter informações sobre as permissões necessárias para desabilitar o acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável no Guia do usuário do AWS Organizations .

Antes de desabilitar o acesso confiável, recomendamos trabalhar com o administrador delegado da sua organização para desabilitar o Security Hub em contas-membro e limpar os recursos do Security Hub nessas contas.

Você pode desativar o acesso confiável usando o AWS Organizations console, a API Organizations ou AWS CLI o. Apenas um administrador na conta de gerenciamento Organizations pode desabilitar o acesso confiável com o Security Hub.

Para obter instruções sobre como desabilitar o acesso confiável com o Security Hub, consulte Desabilitação da integração do Security Hub com o AWS Organizations.

Como habilitar um 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 do AWS 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 habilitado, no console do Security Hub, selecione Settings em General.
3. Em Delegated Administrator (Administrador delegado), insira o ID da conta.

Como desabilitar um administrador delegado para o Security Hub

Somente a conta de gerenciamento da organização pode remover uma conta de administrador delegado do Security Hub.

Para alterar o administrador delegado do Security Hub, você deve primeiro remover a conta atual do administrador delegado e depois designar outra.

Se você usar o console do Security Hub para remover o administrador delegado em uma região, ele será removido automaticamente em todas as regiões.

A API do Security Hub só remove a conta de administrador delegado do Security Hub da região em que o comando ou a chamada de API são emitidos. Você deve repetir a ação em outras regiões.

Se você usar a API do Organizations para remover a conta de administrador delegado do Security Hub, ela será removida automaticamente de todas as regiões.

Para obter instruções sobre como desabilitar o administrador delegado do Security Hub, consulte Remover ou alterar o administrador delegado.

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 Ativando o acesso confiável para a Lente de Armazenamento do S3 no Guia do usuário do Amazon Simple Storage Service.

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Escolha Lente de Armazenamento do Amazon S3 na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de diálogo Habilitar acesso confiável para Amazon S3 Storage Lens, digite enable para confirmar e, em seguida, escolha Enable trust access.
6. Se você for administrador somente do AWS Organizations, diga ao administrador do Amazon S3 Storage Lens que agora ele pode permitir que esse serviço funcione a AWS Organizations partir do console de serviços.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitar o Amazon S3 Storage Lens como um serviço confiável com a 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: Habilitar AWSService acesso

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 só pode desativar o acesso confiável usando as ferramentas Amazon S3 Storage Lens.

Você pode desativar o acesso confiável usando o console Amazon S3, o AWS CLI ou qualquer um dos. AWS SDKs

Para desabilitar o acesso confiável usando o console do Amazon S3

Consulte Desativação do acesso confiável para a Lente de Armazenamento do S3 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 Amazon S3, AWS CLI o ou qualquer um dos. AWS SDKs Para registrar uma conta-membro como uma conta de administrador

delegado para sua organização usando o console do Amazon S3, consulte Registro de um administrador delegado para a Lente de Armazenamento do S3 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 ou qualquer um dos AWS CLI . AWS SDKs Para cancelar o registro de um administrador delegado usando o console do Amazon S3, consulte Cancelamento do registro de um administrador delegado para a Lente de Armazenamento do S3 no Guia do usuário do Amazon Simple Storage Service.

AWS Resposta a incidentes de segurança e AWS Organizations

AWS O Security Incident Response é um serviço de segurança que fornece suporte a incidentes de segurança 24 horas por dia, 7 dias por semana, ao vivo e assistido por humanos para ajudar os clientes a responder rapidamente a incidentes de segurança cibernética, como roubo de credenciais e ataques de ransomware. Ao se integrar ao Organizations, você habilita a cobertura de segurança para toda a sua organização. Para obter mais informações, consulte Gerenciando contas do AWS Security Incident Response AWS Organizations no Guia do Usuário do Security Incident Response.

Use as informações a seguir para ajudá-lo a integrar o AWS Security Incident Response com 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.

- `AWSServiceRoleForSecurityIncidentResponse`- usado para criar uma associação ao Security Incident Response - sua assinatura do serviço por meio de AWS Organizations.
- `AWSServiceRoleForSecurityIncidentResponse_Triage`- usado somente quando você ativa o recurso de triagem durante a inscrição.

Princípios de serviço usados pelo Security Incident Response

As funções vinculadas ao serviço na seção anterior só podem ser assumidas pelos diretores de serviço autorizados pelas relações de confiança definidas para a função. As funções vinculadas ao serviço usadas pelo Security Incident Response concedem acesso ao seguinte principal de serviço:

- `security-ir.amazonaws.com`

Permitindo acesso confiável ao Security Incident Response

Habilitar o acesso confiável ao Security Incident Response permite que o serviço acompanhe a estrutura da sua organização e garanta que todas as contas da organização tenham cobertura ativa de incidentes de segurança. Também permite que o serviço use uma função vinculada ao serviço nas contas dos membros para recursos de triagem quando você ativa o recurso de triagem.

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 Security Incident Response ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o console ou as ferramentas do AWS Security Incident Response para permitir a integração com o Organizations. Isso permite que o AWS Security Incident Response execute qualquer configuração necessária, como criar os recursos necessários ao serviço. Prossiga com essas etapas somente se você não conseguir habilitar a integração usando as ferramentas fornecidas pelo AWS Security Incident Response. Para obter mais informações, consulte esta nota.
> Se você habilitar o acesso confiável usando o console ou as ferramentas do AWS Security Incident Response, não precisará concluir essas etapas.

O Organizations ativa automaticamente o acesso confiável do Organizations quando você usa o console do Security Incident Response para configuração e gerenciamento. Se você usar o CLI/SDK do Security Incident Response, precisará habilitar manualmente o acesso confiável usando a API Enable AWSService Access. Para saber como habilitar o acesso confiável por meio do console do Security Incident Response, consulte Habilitando o acesso confiável para o gerenciamento de AWS contas no Guia do usuário do Security Incident Response.

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Escolha Resposta a incidentes de AWS segurança na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de diálogo Habilitar acesso confiável para Resposta a Incidentes de AWS Segurança, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, diga ao administrador do AWS Security Incident Response que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitar o AWS Security Incident Response como um serviço confiável com Organizations.

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

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

- AWS API: Habilitar AWSService acesso

Desabilitando o acesso confiável com o Security Incident Response

Somente um administrador na conta de gerenciamento do Organizations pode desativar o acesso confiável com o Security Incident Response.

Você só pode desativar o acesso confiável usando as ferramentas 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. No painel de navegação, escolha Serviços.
3. Escolha Resposta a incidentes de AWS segurança na lista de serviços.
4. Escolha Desabilitar acesso confiável.
5. Na caixa de diálogo Desabilitar acesso confiável para Resposta a Incidentes de AWS Segurança, digite desabilitar para confirmar e escolha Desabilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, diga ao administrador do AWS Security Incident Response que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas.

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

  Execute o comando a seguir para desativar o AWS Security Incident Response como um serviço confiável com Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal security-ir.amazonaws.com
```

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

- AWS API: Desativar AWSService acesso

Habilitando uma conta de administrador delegado para o Security Incident Response

Quando você designa uma conta membro como administrador delegado da organização, os usuários e funções dessa conta podem realizar ações administrativas para o Security Incident Response 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 Security Incident Response. Para obter mais informações, consulte Gerenciando contas do AWS Security Incident Response AWS Organizations no Guia do Usuário do Security Incident Response.

> **Permissões mínimas**
>
> Somente um usuário ou função na conta de gerenciamento da Organizations pode configurar uma conta de membro como administrador delegado para o Security Incident Response na organização.

Para saber como configurar um administrador delegado por meio do console do Security Incident Response, consulte Designando uma conta delegada de administrador do Security Incident Response no Guia do Usuário do Security Incident Response.

AWS CLI, AWS API

Se você quiser configurar uma conta de administrador delegado usando a AWS CLI ou uma das, você pode usar AWS SDKs os seguintes comandos:

- AWS CLI:

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

Desabilitando um administrador delegado para o Security Incident Response

> **Important**
>
> Se a associação foi criada a partir da conta do administrador delegado, cancelar o registro do administrador delegado é uma ação destrutiva e causará a interrupção do serviço. Para registrar novamente o DA:
>
> 1. Faça login no console do Security Incident Response em https://console.aws.amazon.com/security-ir/ home#/membership/settings
> 2. Cancele a associação no console de serviço. A associação permanece ativa até o final do ciclo de cobrança.
> 3. Depois que a associação for cancelada, desative o acesso ao serviço por meio do console do Organizations, da CLI ou do SDK.

Somente um administrador na conta de gerenciamento do Organizations pode remover um administrador delegado do Security Incident Response. É possível remover a conta de administrador delegado usando a operação `DeregisterDelegatedAdministrator` da CLI ou SDK do Organizations.

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 da sua organização quando você chama a RegisterDataLakeDelegatedAdministratorAPI. Esse perfil permite que o Amazon Security Lake realize operações válidas nas contas da sua organização.

Você só poderá excluir ou modificar esse perfil se desabilitar o acesso confiável entre o Amazon Security Lake e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForSecurityLake`

> ⚠ Recomendação: use a RegisterDataLakeDelegatedAdministrator API do Security Lake para permitir que o Security Lake acesse sua organização e para registrar o administrador delegado da organização
>
> Se você usar 'Organizations' APIs para registrar um administrador delegado, as funções vinculadas ao serviço das Organizations podem não ser criadas com êxito. Para garantir a funcionalidade total, use o Security Lake APIs.

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 Amazon Security Lake concedem acesso às seguintes entidades principais de serviço:

- `securitylake.amazonaws.com`

Como habilitar o acesso confiável ao 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 só pode habilitar o acesso confiável usando as ferramentas Organizations.

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Selecione Amazon Security Lake na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de diálogo Habilitar acesso confiável para o Amazon Security Lake, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador do Only AWS Organizations, informe ao administrador do Amazon Security Lake que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviços.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitar o Amazon Security Lake como um serviço confiável com Organizations.

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

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

- AWS API: Habilitar AWSService acesso

Como desabilitar o acesso confiável ao Amazon Security Lake

Apenas um administrador na conta de gerenciamento Organizations pode desabilitar o acesso confiável com o Amazon Security Lake.

Você só pode desativar o acesso confiável usando as ferramentas 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. No painel de navegação, escolha Serviços.
3. Selecione Amazon Security Lake na lista de serviços.
4. Escolha Desabilitar acesso confiável.
5. Na caixa de diálogo Desativar acesso confiável para o Amazon Security Lake, digite desabilitar para confirmar e, em seguida, escolha Desativar acesso confiável.
6. Se você for administrador do Only AWS Organizations, diga ao administrador do Amazon Security Lake que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas.

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

  Execute o comando a seguir para desativar o Amazon Security Lake como um serviço confiável com 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 AWSService acesso

Como habilitar uma conta de administrador delegado para o Amazon Security Lake

O administrador delegado do Amazon Security Lake adiciona outras contas na organização como contas-membro. O administrador delegado pode ativar o Amazon Security Lake e definir as configurações do Amazon Security Lake para as contas-membro. 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 logs e eventos nas contas-membro associadas. Assim, você pode configurar o Amazon Security Lake para coletar dados pertencentes às contas-membro 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 do Organizations pode configurar uma conta-membro como um administrador delegado para o Amazon Security Lake na organização

É possível especificar uma conta de administrador delegado usando o console do Amazon Security Lake, a ação `CreateDatalakeDelegatedAdmin` da API do Amazon Security Lake ou

o comando `create-datalake-delegated-admin` da 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 Designar o administrador delegado do Security Lake e adicionar contas-membro no Guia do usuário do Amazon Security Lake.

AWS CLI, AWS API

Se você quiser configurar uma conta de administrador delegado usando a AWS CLI ou uma das, você pode usar AWS SDKs 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.

Desabilitar um administrador delegado para o Amazon Security Lake

Somente um administrador na conta de gerenciamento do Organizations ou a conta de administrador delegado do Amazon Security Lake podem remover uma conta de administrador delegado da organização.

É possível remover a conta de administrador delegado usando a operação `DeregisterDataLakeDelegatedAdministrator` da API do Amazon Security Lake, o comando `deregister-data-lake-delegated-administrator` da CLI ou a operação `DeregisterDelegatedAdministrator` da CLI ou SDK do Organizations. Para remover um administrador delegado usando o Amazon Security Lake, consulte Removing the Amazon Security Lake delegated administrator 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 Service Catalog com AWS Organizations simplifica o compartilhamento de portfólios e a cópia de produtos em toda a organização. Os administradores do Service Catalog podem fazer referência a uma organização existente 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 o portfólio IDs e de a conta de recebimento referenciar manualmente o ID do portfólio ao importar o portfólio. 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 se integrar AWS Service Catalog com AWS Organizations.

Funções vinculadas ao serviço, criadas quando você habilitou a integração

AWS Service Catalog não cria nenhuma função vinculada ao serviço como parte da habilitação do 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 AWS Service Catalog console ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Service Catalog console ou as ferramentas para permitir a integração com o Organizations. Isso permite AWS Service Catalog 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 Service Catalog. Para obter mais informações, consulte esta nota.

Se você habilitar o acesso confiável usando o AWS Service Catalog console ou as ferramentas, não precisará concluir essas etapas.

Para habilitar o acesso confiável usando o Service Catalog CLI ou o SDK AWS

Chame um dos seguintes comandos ou operações:

- AWS CLI: catálogo de serviços aws enable-aws-organizations-access
- AWS SDKs: AWSServiceCatálogo: :Habilitar acesso AWSOrganizations

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Service Catalog na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de AWS Service Catalog diálogo Habilitar acesso confiável para, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Service Catalog que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

Execute o comando a seguir para habilitá-lo AWS Service Catalog como um serviço confiável com Organizations.

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

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

- AWS API: Habilitar AWSService acesso

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 Service Catalog AWS Organizations enquanto estiver usando o Service Catalog, isso não excluirá seus compartilhamentos atuais, mas impedirá que você crie novos compartilhamentos em toda a organização. Os compartilhamentos atuais não serão sincronizados com a estrutura da sua organização se ela for alterada depois que você chamar essa ação.

Para desativar o acesso confiável usando o Service Catalog CLI ou o SDK AWS

Chame um dos seguintes comandos ou operações:

- AWS CLI: catálogo de serviços aws disable-aws-organizations-access
- AWS SDKs: Desativar AWSOrganizations acesso

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. No painel de navegação, escolha Serviços.
3. Escolha AWS Service Catalog na lista de serviços.
4. Escolha Desabilitar acesso confiável.
5. Na caixa de AWS Service Catalog diálogo Desabilitar acesso confiável para, digite desabilitar para confirmar e escolha Desabilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Service Catalog que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas.

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

  Execute o comando a seguir para desabilitar AWS Service Catalog como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Desativar AWSService acesso

Service Quotas e AWS Organizations

O Service Quotas é um AWS serviço que permite que você visualize e gerencie suas cotas a partir de 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 é associado a 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 as Service Quotas 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. 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 só pode habilitar o acesso confiável usando Service Quotas.

Você pode habilitar o acesso confiável usando o console Service Quotas AWS CLI ou o SDK:

- Para habilitar o acesso confiável usando o console do Service Quotas

  Faça login com sua conta AWS Organizations de gerenciamento e configure o modelo no console 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 o Service Quotas AWS CLI ou o SDK

  Chame o seguinte comando ou operação:

- AWS CLI: cotas de serviço da AWS associate-service-quota-template
- AWS SDKs: AssociateServiceQuotaTemplate

AWS IAM Identity Center e AWS Organizations

AWS IAM Identity Center fornece acesso de login único para todos os seus aplicativos Contas da AWS e aplicativos na nuvem. Ele se conecta ao Microsoft Active Directory AWS Directory Service para permitir que os usuários desse diretório entrem em um portal de AWS acesso personalizado usando seus nomes de usuário e senhas existentes do Active Directory. No portal de AWS acesso, os usuários têm acesso a todos Contas da AWS os aplicativos na nuvem para os quais têm permissões.

Para obter mais informações sobre o Centro de Identidade do IAM, consulte o Guia do usuário do AWS IAM Identity Center.

Use as informações a seguir para ajudá-lo a se integrar AWS IAM Identity Center 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 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 AWS IAM Identity Center console ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS IAM Identity Center console ou as ferramentas para permitir a integração com o Organizations. Isso permite AWS IAM Identity Center 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 IAM Identity Center. Para obter mais informações, consulte esta nota.
>
> Se você habilitar o acesso confiável usando o AWS IAM Identity Center console ou as ferramentas, não precisará concluir essas etapas.

O IAM Identity Center requer acesso confiável 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 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. No painel de navegação, escolha Serviços.
3. Escolha AWS IAM Identity Center na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).

5. Na caixa de AWS IAM Identity Center diálogo Habilitar acesso confiável para, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS IAM Identity Center que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitá-lo AWS IAM Identity Center como um serviço confiável com Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Habilitar AWSService acesso

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 AWS Organizations para operar. Se você desativar o acesso confiável usando o IAM Identity Center AWS Organizations enquanto estiver usando o IAM Identity Center, ele deixará de funcionar porque não poderá 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 só pode desativar o acesso confiável usando as ferramentas 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. No painel de navegação, escolha Serviços.
3. Escolha AWS IAM Identity Center na lista de serviços.
4. Escolha Desabilitar acesso confiável.
5. Na caixa de AWS IAM Identity Center diálogo Desabilitar acesso confiável para, digite desabilitar para confirmar e escolha Desabilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS IAM Identity Center que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas.

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

  Execute o comando a seguir para desabilitar AWS IAM Identity Center como um serviço confiável com Organizations.

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal sso.amazonaws.com
```

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

- AWS API: Desativar AWSService acesso

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

AWS Systems Manager é um conjunto de recursos que permitem a visibilidade e o controle de seus AWS recursos. Os seguintes recursos do Systems Manager funcionam com o Organizations em todas as Contas da AWS em sua organização:

- O Systems Manager Explorer é um painel de operações personalizável que relata informações sobre seus AWS recursos. Você pode sincronizar dados de operações Contas da AWS em toda a sua organização usando o Organizations and 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 onde engenheiros de operações e profissionais de TI podem visualizar, investigar e resolver itens de trabalho operacionais (OpsItems) relacionados aos AWS recursos. Quando você usa OpsCenter com o Organizations, ele suporta trabalhar com uma conta OpsItems de gerenciamento (uma conta de gerenciamento do Organizations ou uma conta de administrador delegado do Systems Manager) e outra conta durante uma única sessão. Após configurados, os usuários podem realizar os seguintes tipos de ações:
  - Crie, visualize e atualize OpsItems em outra conta.
  - Visualize informações detalhadas sobre AWS os recursos especificados OpsItems em outra conta.
  - Inicie os runbooks do Systems Manager Automation para corrigir problemas com AWS recursos em outra conta.

  Consulte mais informações em AWS Systems Manager OpsCenter no Guia de Usuário AWS Systems Manager .
- Use a Configuração rápida para configurar rapidamente AWS serviços e recursos usados com frequência com as melhores práticas recomendadas. Para obter mais informações, consulte AWS Systems Manager Quick Setup no Guia do usuário do AWS Systems Manager .

  Ao registrar uma conta de administrador AWS Organizations delegado no Systems Manager, você pode criar, atualizar, visualizar e excluir gerenciadores de configuração do Quick Setup que têm como alvo unidades organizacionais em uma organização. Saiba mais em Usando um administrador delegado para configuração rápida no Guia do AWS Systems Manager usuário.
- Ao configurar o console integrado do Systems Manager, você insere uma conta de administrador delegado. Essa conta é usada para registrar contas de administrador AWS Organizations delegado com Quick Setup CloudFormation StackSets, Explorer e Resource Explorer. Saiba mais no Guia do AWS Systems Manager usuário de configuração do console integrado do Systems Manager para uma organização.

Use as informações a seguir para ajudá-lo a se integrar AWS Systems Manager 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 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 só pode habilitar o acesso confiável usando as ferramentas Organizations.

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Systems Manager na lista de serviços.

4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de AWS Systems Manager diálogo Habilitar acesso confiável para, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Systems Manager que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitá-lo AWS Systems Manager como um serviço confiável com Organizations.

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

  Esse comando não gera nenhuma saída quando é bem-sucedido.
- AWS API: Habilitar AWSService acesso

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 AWS Organizations para sincronizar os dados operacionais Contas da AWS em toda a sua organização. Se você desativar o acesso confiável, o Systems Manager não sincroniza os dados das operações e reporta um erro.

Você só pode desativar o acesso confiável usando as ferramentas 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Systems Manager na lista de serviços.
4. Escolha Desabilitar acesso confiável.
5. Na caixa de AWS Systems Manager diálogo Desabilitar acesso confiável para, digite desabilitar para confirmar e escolha Desabilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Systems Manager que agora ele pode impedir que esse serviço funcione AWS Organizations usando o console de serviço ou as ferramentas.

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

  Execute o comando a seguir para desabilitar AWS Systems Manager como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

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

- AWS API: Desativar AWSService acesso

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. Essa é a Conta da AWS que foi designada como a conta para gerenciar modelos de alteração, solicitações de alteração, registros de alterações 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 Explorer e OpsCenter, consulte Configurando 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).
- Para a Configuração rápida, consulte Registrar um administrador delegado para a Configuração rápida.

Desabilitando uma conta de administrador delegado para Systems Manager

Para cancelar o registro de um administrador delegado, consulte os seguintes tópicos no Guia do AWS Systems Manager usuário:

- Para Explorer e OpsCenter, consulte Cancelar o registro de um administrador delegado do Explorer.
- 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).

- Para a Configuração rápida, consulte Cancelar o registro de um administrador delegado para a Configuração rápida.

Notificações de Usuários da AWS e AWS Organizations

Notificações de Usuários da AWSé um local central para suas AWS notificações.

Depois de fazer a integração com AWS Organizations, você pode configurar e visualizar as notificações de forma centralizada em todas as contas da sua organização.

Use as informações a seguir para ajudá-lo a se integrar Notificações de Usuários 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 Notificações de Usuários 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 Notificações de Usuários e o Organizations, ou se remover a conta-membro da organização.

- `AWSServiceRoleForAWSUserNotifications`

Para obter mais informações, consulte Usando funções vinculadas ao serviço no Guia do Notificações de Usuários da AWS usuário.

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 Notificações de Usuários concedem acesso aos seguintes diretores de serviço:

- `notifications.amazon.com`

Habilitar o acesso confiável no Notificações de Usuários

Para obter informações sobre as permissões necessárias para habilitar acesso confiável, consulte Permissões necessárias para habilitar o acesso confiável.

Você só pode habilitar o acesso confiável usando Notificações de Usuários da AWS.

Para ativar o acesso confiável usando o Notificações de Usuários console, consulte Ativação AWS OrganizationsNotificações de Usuários da AWS no Guia Notificações de Usuários do usuário.

Desabilitar o acesso confiável no Notificações de Usuários

Para obter informações sobre as permissões necessárias para desabilitar acesso confiável, consulte Permissões necessárias para desabilitar o acesso confiável.

Você só pode habilitar o acesso confiável usando Notificações de Usuários da AWS.

Para desativar o acesso confiável usando o Notificações de Usuários console, consulte Ativação AWS OrganizationsNotificações de Usuários da AWS no Guia Notificações de Usuários do usuário.

Habilitando uma conta de administrador delegado para Notificações de Usuários

O administrador da conta de gerenciamento pode delegar permissões Notificações de Usuários administrativas 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.

As contas de gerenciamento e as contas de administrador delegado podem realizar tarefas Notificações de Usuários administrativas, como criar experiências, atualizar configurações de identidade visual, associar ou desassociar públicos, adicionar ou remover produtos e aprovar ou recusar solicitações pendentes.

Para configurar um administrador delegado usando o Notificações de Usuários console, consulte Registro de administradores delegados Notificações de Usuários da AWS no Guia do usuário.Notificações de Usuários

Você também pode configurar um administrador delegado usando a API `RegisterDelegatedAdministrator` do Organizations. Para obter mais informações, consulte RegisterDelegatedAdministratorna Referência de Comandos do Organizations.

Desabilitando um administrador delegado para Notificações de Usuários

Somente um administrador na conta de gerenciamento da organização pode configurar um administrador delegado para Notificações de Usuários.

Você pode remover o administrador delegado usando o Notificações de Usuários console ou a API, ou usando a operação `DeregisterDelegatedAdministrator` CLI ou SDK do Organizations.

Para desativar a Notificações de Usuários conta de administrador delegado usando o Notificações de Usuários console, consulte Remoção de administradores delegados Notificações de Usuários da AWS no Guia do Notificações de Usuários usuário.

Políticas de tag e AWS Organizations

As políticas de tags são um tipo de política AWS Organizations que pode ajudar você a padronizar as tags nos recursos das contas da sua organização. Para obter mais informações sobre políticas de tag, consulte Políticas de tag.

Use as informações a seguir para ajudá-lo a integrar políticas de tags com 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 ativando políticas de tags na organização ou usando o AWS Organizations console.

> **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 obter mais informações, consulte Habilitação de um tipo de política.

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Escolha tag policies na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de diálogo Habilitar acesso confiável para políticas de tag, digite enable para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador das políticas de tags que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitar políticas de tags como um serviço confiável com 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: Habilitar AWSService acesso

Desabilitar o acesso confiável com políticas de tag

Você pode desativar o acesso confiável às políticas de tags desativando o tipo de política de tags no AWS Organizations console. Para obter mais informações, consulte Desabilitar um tipo de política.

AWS Trusted Advisor e AWS Organizations

AWS 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. Quando integrado ao Organizations, você pode receber os resultados dos Trusted Advisor cheques de todas as contas da sua organização e baixar relatórios para ver os resumos de suas verificações e de quaisquer 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 se integrar AWS Trusted Advisor 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 Trusted Advisor 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 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 pela Trusted Advisor concedem acesso aos seguintes diretores de serviço:

- `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 só pode ativar o acesso confiável usando AWS Trusted Advisor.

Para habilitar o acesso confiável usando o Trusted Advisor console

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 de desativar esse recurso, Trusted Advisor interrompe o registro das informações de cheques de todas as outras contas em sua organização. Não é possível exibir ou baixar relatórios existentes nem criar novos relatórios.

Você pode desativar o acesso confiável usando as ferramentas AWS Trusted Advisor ou as AWS Organizations ferramentas.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Trusted Advisor console ou as ferramentas para desativar a integração com o Organizations. Isso permite AWS Trusted Advisor 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 Trusted Advisor.
> Se você desabilitar o acesso confiável usando o AWS Trusted Advisor console ou as ferramentas, não precisará concluir essas etapas.

Para desativar o acesso confiável usando o Trusted Advisor console

Consulte Desabilitar a visualização organizacional no Guia do usuário do AWS Support .

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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desabilitar AWS Trusted Advisor como um serviço confiável com 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: Desativar AWSService acesso

Habilitando uma conta de administrador delegado para 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 função na conta de gerenciamento da Organizations pode configurar uma conta de membro como administrador delegado Trusted Advisor na organização.

Para obter instruções sobre como habilitar uma conta de administrador delegado para Trusted Advisor, consulte Registrar administradores delegados no Guia do Suporte usuário.

AWS CLI, AWS API

Se você quiser configurar uma conta de administrador delegado usando a AWS CLI ou uma das, você pode usar AWS SDKs os seguintes comandos:

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal reporting.trustedadvisor.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 Trusted Advisor

Você pode remover o administrador delegado usando o Trusted Advisor console ou usando a operação Organizations `DeregisterDelegatedAdministrator` CLI ou SDK. Para obter informações sobre como desativar a Trusted Advisor conta de administrador delegado usando o Trusted Advisor console, consulte Cancelar o registro de administradores delegados no guia do usuário.Suporte

AWS Well-Architected Tool e AWS Organizations

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.

O uso AWS Well-Architected Tool com o Organizations permite que AWS Well-Architected Tool tanto os clientes quanto os clientes da Organizations simplifiquem o processo de compartilhamento de AWS Well-Architected Tool recursos com outros membros da organização.

Para obter mais informações, consulte Compartilhar seus recursos da AWS Well-Architected Tool no Guia do usuário do AWS Well-Architected Tool .

Use as informações a seguir para ajudá-lo a se integrar AWS Well-Architected Tool 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 WA Tool 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 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 pela AWS WA Tool concedem acesso aos seguintes diretores de serviço:

- `wellarchitected.amazonaws.com`

Habilitar o acesso confiável no AWS WA Tool

Permite a atualização de AWS WA Tool para refletir as 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 AWS Well-Architected Tool console ou o AWS Organizations console.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Well-Architected Tool console ou as ferramentas para permitir a integração com o Organizations. Isso permite AWS Well-Architected Tool 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 Well-Architected Tool. Para obter mais informações, consulte esta nota.

Se você habilitar o acesso confiável usando o AWS Well-Architected Tool console ou as ferramentas, não precisará concluir essas etapas.

Para habilitar o acesso confiável usando o AWS WA Tool console

Consulte Compartilhamento de seus AWS Well-Architected Tool recursos no Guia AWS Well-Architected Tool do usuário.

Você pode habilitar 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. No painel de navegação, escolha Serviços.
3. Escolha AWS Well-Architected Tool na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de AWS Well-Architected Tool diálogo Habilitar acesso confiável para, digite habilitar para confirmar e escolha Habilitar acesso confiável.
6. Se você for administrador de somente AWS Organizations, informe ao administrador AWS Well-Architected Tool que agora ele pode habilitar esse serviço para funcionar a AWS Organizations partir do console de serviço.

AWS CLI, AWS API

Para habilitar o acesso ao serviço confiável usando a CLI/SDK do Organizations

Use os seguintes AWS CLI comandos ou operações de API para habilitar o acesso confiável ao serviço:

- AWS CLI: enable-aws-service-access

  Execute o comando a seguir para habilitá-lo AWS Well-Architected Tool como um serviço confiável com Organizations.

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

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

- AWS API: Habilitar AWSService acesso

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 desativar o acesso confiável usando as ferramentas AWS Well-Architected Tool ou as AWS Organizations ferramentas.

> **Important**
>
> É altamente recomendável que, sempre que possível, você use o AWS Well-Architected Tool console ou as ferramentas para desativar a integração com o Organizations. Isso permite AWS Well-Architected Tool 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 Well-Architected Tool.
>
> Se você desabilitar o acesso confiável usando o AWS Well-Architected Tool console ou as ferramentas, não precisará concluir essas etapas.

Para desativar o acesso confiável usando o AWS WA Tool console

Consulte Compartilhamento de seus AWS Well-Architected Tool recursos no Guia AWS Well-Architected Tool 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desabilitar AWS Well-Architected Tool como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

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

- AWS API: Desativar AWSService acesso

Gerenciador de endereços IP da Amazon VPC (IPAM) e AWS Organizations

O Amazon VPC IP Address Manager (IPAM) é um recurso de VPC que facilita o planejamento, o rastreamento e o monitoramento de endereços IP para suas cargas de trabalho. AWS

AWS Organizations O uso permite monitorar o uso do endereço IP em toda a organização e compartilhar pools de endereços IP entre as contas dos membros.

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 Amazon VPC IP Address Manager (IPAM) com o. 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 exige acesso confiável AWS Organizations antes que você possa designar uma conta de membro para ser o administrador delegado desse serviço para 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 uso do console do IPAM ou da `EnableIpamOrganizationAdminAccount` API 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 os recursos EC2 de rede CIDRs associados à sua organização e armazenar métricas relacionadas ao IPAM na 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 AWS Organizations console ou com a `EnableAWSServiceAccess`API.

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.

Somente um administrador na conta AWS Organizations de gerenciamento pode desativar o acesso confiável com o IPAM usando a AWS Organizations `disable-aws-service-access` API.

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 desativar o acesso confiável executando um AWS CLI comando do 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

Use os seguintes AWS CLI comandos ou operações de API para desativar o acesso confiável ao serviço:

- AWS CLI: disable-aws-service-access

  Execute o comando a seguir para desativar o Amazon VPC IP Address Manager (IPAM) como um serviço confiável com Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ipam.amazonaws.com
  ```

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

- AWS API: Desativar AWSService acesso

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 AWS AWS CLI Comandos.

> **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 o AWS AWS CLI, consulte disable-ipam-organization-admin-account na Referência de AWS AWS CLI comandos.

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 permite realizar testes de conectividade entre um recurso de origem e um recurso de destino em suas nuvens privadas virtuais (). VPCs

O uso AWS Organizations com o Reachability Analyzer permite traçar caminhos entre contas em suas organizações.

Para obter mais informações, consulte Manage delegated administrator accounts in Reachability Analyzer no Guia do usuário do Reachability Analyzer.

Use as informações a seguir para ajudá-lo 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 antes que você possa designar uma conta membro AWS Organizations para ser 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 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 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 do only AWS Organizations, diga ao administrador do Reachability Analyzer que agora ele pode habilitar esse serviço usando o 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 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: Habilitar AWSService acesso

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 RegisterDelegatedAdministratorna 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 esse trabalho com 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

que você armazene seus AWS recursos em outras contas de membros na organização e os mantenha fora da conta de gerenciamento. Isso ocorre porque os recursos de segurança, como as políticas de controle de serviços (SCPs) do Organizations, não restringem usuários ou funções 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 que você reduza 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 Serviços da AWS 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 Serviços da AWS 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 Serviços da AWS 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 organizacional, todas as contas e OUs políticas organizacionais
- Associações
- Todas as contas OUs e.
- 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 funciona Serviços da AWS 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 programas de conformidade da AWS. Para saber mais sobre os programas de conformidade aplicáveis AWS Organizations, consulte Serviços da AWS 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 aprende a usar outros Serviços da AWS que ajudam você 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 mais informações sobre 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) às quais são atribuídos 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
- Criação de um VPC endpoint para AWS Organizations
- Criando uma política de endpoint da VPC para o AWS Organizations

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:

- Somente disponível na região `us-east-1`
- Não oferece suporte ao Transport Layer Security (TLS) 1.1

Criação de um VPC endpoint para AWS Organizations

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 VPCEndpoint recurso AWS::EC2:: no Guia do AWS CloudFormation usuário.

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

É possível anexar uma política de endpoint ao endpoint da VPC que controla o acesso ao Organizations. Essa política especifica as seguintes informações:

- A entidade principal que pode realizar ações.
- As ações que podem ser realizadas.
- Os recursos aos quais as ações podem ser aplicadas.

Para obter mais informações, consulte Controlar 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":"*"
      }
   ]
}
```

Identity and Access Management para AWS Organizations

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

Tópicos

Público

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

Usuário do serviço: se você usar o serviço do Organizations para fazer o trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que mais recursos do Organizations forem usados para realizar o trabalho, talvez sejam necessárias permissões adicionais. Compreenda como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador. Se você não conseguir acessar um atributo no Organizations, consulte Solução de problemas AWS Organizations de identidade e acesso.

Administrador do serviço: se você for o responsável pelos recursos do Organizations em sua empresa, você provavelmente terá acesso total ao Organizations. Cabe a você determinar quais

funcionalidades e atributos do Organizations os usuários do serviço devem acessar. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com o Organizations, consulte Como AWS Organizations funciona com o IAM.

Administrador do IAM: se você é um administrador do IAM, talvez queira saber detalhes sobre como pode escrever políticas para gerenciar o acesso ao Organizations. Para visualizar exemplos de políticas baseadas em identidade do Organizations que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o AWS Organizations.

Autenticar com identidades

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

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

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

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte Versão 4 do AWS Signature para solicitações de API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator

no Guia do usuário do AWS IAM Identity Center e Usar a autenticação multifator da AWS no IAM no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele 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.

Identidade federada

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

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

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

Usuários e grupos do IAM

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

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

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

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode alternar de um usuário para uma função do IAM (console). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Métodos para assumir um perfil no Guia do usuário do IAM.

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

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidade de terceiros (federação) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Guia do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para conhecer a

diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que os programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

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

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

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

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

Políticas baseadas em identidade

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

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

Políticas baseadas em recursos

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

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

Listas de controle de acesso (ACLs)

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

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

Outros tipos de política

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

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.
- Políticas de controle de recursos (RCPs) — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

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

Como AWS Organizations funciona com o IAM

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

Atributo do IAM	Suporte do Organizations
Políticas baseadas em identidade	Sim
Políticas baseadas em atributos	Sim
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Não
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Perfis vinculados a serviço	Sim

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

Políticas baseadas em identidade para o Organizations

Compatível com políticas baseadas em identidade: sim

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

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

Exemplos d políticas baseadas em identidade para o Organizations

Para exibir exemplos de políticas baseadas em identidade do Organizations, consulte Exemplos de políticas baseadas em identidade para o AWS Organizations.

Políticas baseadas em recursos no Organizations

Compatível com políticas baseadas em recursos: sim

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

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

O serviço do Organizations oferece suporte somente a um tipo de política baseada em recurso, denominada política de delegação baseada em recursos, que especifica 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.

Para obter mais informações, consulte Administrador delegado para AWS Organizations.

Exemplos de políticas baseadas em recursos no Organizations

Para exibir exemplos de políticas baseadas em recursos do Organizations, consulte Exemplos de políticas baseadas em recursos para AWS Organizations.

Ações de políticas para o Organizations

Compatível com ações de políticas: sim

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

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

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

Para ver uma lista das ações do Organizations, consulte Actions defined by AWS Organizations na Referência de autorização do serviço.

As ações de política no Organizations usam o seguinte prefixo antes da ação:

```
organizations
```

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

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

Para exibir exemplos de políticas baseadas em identidade do Organizations, consulte Exemplos de políticas baseadas em identidade para o AWS Organizations.

Recursos de políticas para o Organizations

Compatível com recursos de políticas: sim

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

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

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

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

Para ver uma lista dos tipos de recursos de Organizations e seus ARNs, consulte Recursos definidos por AWS Organizations na Referência de Autorização de Serviço. Para saber com quais ações é possível especificar o ARN de cada atributo, consulte Ações definidas pelo AWS Organizations.

Para exibir exemplos de políticas baseadas em identidade do Organizations, consulte Exemplos de políticas baseadas em identidade para o AWS Organizations.

Chaves de condição de políticas do Organizations

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

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

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões

condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

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

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

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

Para ver uma lista de chaves de condição do Organizations, consulte Condition keys for AWS Organizations na Service Authorization Reference. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS Organizations.

Para exibir exemplos de políticas baseadas em identidade do Organizations, consulte Exemplos de políticas baseadas em identidade para o AWS Organizations.

ACLs em Organizations

Suportes ACLs: Não

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

ABAC com o Organizations

Compatível com ABAC (tags em políticas): sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. Marcar de entidades e atributos é

a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

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

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

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usar credenciais temporárias com o Organizations

Compatível com credenciais temporárias: não

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

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

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para o Organizations

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

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Perfis de serviço do Organizations

Compatível com perfis de serviço: sim

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

> **Warning**
>
> A alteração das permissões de um perfil de serviço pode interromper a funcionalidade do Organizations. Edite perfis de serviço somente quando o Organizations fornecer orientação para isso.

Perfis vinculados ao serviço no Organizations

Compatibilidade com perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a esse serviço .

Gerenciando permissões de acesso para uma organização com AWS Organizations

Todos os AWS recursos, incluindo raízes OUs, contas e políticas em uma organização, são de propriedade de um Conta da AWS, e as permissões para criar ou acessar um recurso são regidas por políticas de permissões. No caso de uma organização, a conta de gerenciamento possui todos os recursos. Um administrador da conta pode controlar o acesso aos AWS recursos anexando políticas de permissões às 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 as melhores práticas de segurança no IAM no Guia de AWS Gerenciamento de contas referência.

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.

AWS Organizations recursos e operações

Esta seção discute como os AWS Organizations conceitos são mapeados para seus conceitos equivalentes ao IAM.

Recursos

Em AWS Organizations, você pode controlar o acesso aos seguintes recursos:

- A raiz e o OUs 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 em AWS Organizations, consulte Tipos de recursos definidos por AWS Organizations na Referência de Autorização de Serviço.

Operações

AWS fornece um conjunto de operações para trabalhar com os recursos em 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 obter uma lista de operações do AWS Organizations que podem ser usadas como permissões em uma política do IAM, consulte Actions defined by organizations na Referência de autorização do serviço.

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

AWS fornece chaves de condição que você pode consultar para fornecer um controle mais granular 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 seguintes chaves de condição são especialmente úteis com AWS Organizations:

- `aws:PrincipalOrgID` – Simplifica especificando o elemento `Principal` em uma política baseada em recursos. Essa chave global fornece uma alternativa para listar todas as contas IDs de todos Contas da AWS em 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 de `PrincipalOrgID` em Chaves de contexto de condição global da AWS 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 em texto da estrutura de uma AWS Organizations entidade. 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 elemento de condição a seguir corresponde aos membros de qualquer um dos dois 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:

  - `SERVICE_CONTROL_POLICY`
  - `RESOURCE_CONTROL_POLICY`
  - `DECLARATIVE_POLICY_EC2`

- `BACKUP_POLICY`
- `TAG_POLICY`
- `CHATBOT_POLICY`
- `AISERVICES_OPT_OUT_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 operações Ativar AWSService Acesso ou Desativar AWSService Acesso 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 somente AWS Firewall Manager ao ativar e desativar o acesso confiável com 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

Ele Conta da AWS possui os recursos que são criados na conta, independentemente de quem criou os recursos. Especificamente, o proprietário Conta da AWS do recurso é a entidade principal (ou seja, o usuário raiz, um usuário do IAM ou uma função do IAM) que autentica a solicitação de criação do recurso. Para uma organização, 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 OU).
- 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.

Gerenciar acesso aos recursos da

Uma 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 de 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 da política do IAM, consulte a Referência da política JSON do IAM no Manual 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 chamadas de políticas baseadas em recursos.

Tópicos

- Políticas de permissão baseadas em identidade (políticas do IAM)

Políticas de permissão baseadas em identidade (políticas do IAM)

Você pode anexar políticas às identidades do IAM para permitir que essas identidades realizem operações em AWS recursos. Por exemplo, você pode fazer o seguinte:

- Anexe uma política de permissões a um usuário ou grupo em sua conta — Para conceder a um usuário permissões para criar um AWS Organizations recurso, como uma política de controle de serviços (SCP) ou uma OU, você pode anexar uma política de permissões a um usuário ou 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 diretor na política de confiança também pode ser um diretor de AWS serviço se você quiser conceder permissões a um AWS serviço para assumir a função.

Para obter mais informações sobre o uso do IAM para delegar permissões, consulte Gerenciamento de acesso no Guia 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 perfis) no Guia do usuário do IAM.

Especificação de elementos da política: ações, condições, efeitos e recursos

Para cada AWS Organizations recurso, o serviço define um conjunto de operações ou ações de API que podem interagir ou manipular esse recurso de alguma forma. Para conceder permissões para essas operações, AWS Organizations define um conjunto de ações que você pode especificar em uma política. Por exemplo, para o recurso OU, 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 especificado`Effect`, `organizations:CreateAccount` permite ou nega ao usuário permissões para realizar a AWS Organizations `CreateAccount` operação. Para obter mais informações, consulte Elementos da política JSON do IAM: Action no Manual 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: Resource 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 da política JSON do IAM: condição no Guia 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 de política JSON do IAM: Effect 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 (isso se aplica somente a políticas baseadas em recursos).

Para saber mais sobre a sintaxe e as descrições de políticas do IAM, consulte a Referência da política JSON do IAM no Manual do usuário do IAM.

Exemplos de políticas baseadas em identidade para o AWS Organizations

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Organizations. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O

administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

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

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

Tópicos

- Práticas recomendadas de política
- Usar o console do Organizations
- Permitir que os usuários visualizem suas próprias permissões
- Concessão de permissões administrativas completas a um usuário
- Concessão de acesso limitado por ações
- Concessão de acesso a recursos específicos
- Concessão da capacidade de habilitar acesso confiável para entidades de serviço primárias limitadas

Práticas recomendadas de política

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

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

conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.

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

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

Usar o console do Organizations

Para acessar o AWS Organizations console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos da Organizations em seu Conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

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

Para garantir que usuários e funções ainda possam usar o console Organizations, anexe também as Organizations `AWSOrganizationsFullAccess`ou a política `AWSOrganizationsReadOnlyAccess` AWS gerenciada às entidades. Para obter informações, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Concessão de permissões administrativas completas a um usuário

Você pode criar uma política do IAM que conceda permissões totais de AWS Organizations administrador 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 Políticas.

   Se essa for a primeira vez que você escolhe Políticas, a página Bem-vindo às políticas gerenciadas será exibida. Escolha Começar.
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 Criação de políticas do IAM no Manual 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"` ambos `"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 disponíveis para atribuição em uma política do IAM, consulte Ações definidas por 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 nenhuma criança OUs. Nenhum acesso de cobrança é concedido. Observe que isso não lhe dá acesso administrativo ao Contas da AWS na OU. Ele concede somente permissões para realizar AWS Organizations operações nas contas dentro da OU 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 o IDs para a OU e a organização a partir do AWS Organizations console ou chamando `List*` APIs o. 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 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 daquele para AWS IAM Identity Center, essa política não corresponderá 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 vários recursos, consulte Tipos de recursos definidos por AWS Organizations na Referência de Autorização de Serviço.

Exemplos de políticas baseadas em recursos para AWS Organizations

Os exemplos de código a seguir mostram como é possível usar políticas de delegação baseadas em recursos. Para obter mais informações, consulte Administrador delegado para AWS Organizations.

Tópicos

Exemplo: Exibir organização OUs, contas e políticas

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

Este exemplo mostra como você pode incluir essas permissões em sua política de delegação baseada em recursos para a conta do 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 a partir da AWS API ou. AWS CLI Para usar essa política de delegação, substitua o texto AWS do espaço *AccountId* reservado 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::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: criar, ler, atualizar e excluir políticas

Você pode criar uma política de delegação baseada em recursos que permita que a conta de gerenciamento delegue ações de `create`, `read`, `update` e `delete` para qualquer tipo de política. Este exemplo mostra como você pode delegar essas ações para políticas de controle de serviço à conta do membro,*`MemberAccountId`*. Os dois recursos mostrados no exemplo concedem acesso às políticas de controle de serviços AWS gerenciados e gerenciados pelo cliente, respectivamente.

> **Important**
>
> Esta política permite que os administradores delegados executem as ações especificadas nas políticas criadas por qualquer conta na organização, incluindo a conta de gerenciamento. Ela não permite que administradores delegados vinculem ou desvinculem políticas porque não inclui as permissões necessárias para realizar e realizar ações de `organizations:AttachPolicy` e `organizations:DetachPolicy`.

Este exemplo de política de delegação concede as permissões necessárias para concluir ações programaticamente a partir da AWS API ou. AWS CLI Substitua o texto AWS do espaço reservado

para *MemberAccountIdManagementAccountId*, e *OrganizationId* 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": "SERVICE_CONTROL_POLICY"
        }
      }
    },
    {
      "Sid": "DelegatingMinimalActionsForSCPs",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
```

```
        "organizations:CreatePolicy",
        "organizations:DescribePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy"
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
service_control_policy/*",
        "arn:aws:organizations::aws:policy/service_control_policy/*"
      ]
    }
  ]
}
```

Exemplo: políticas de marcar e desmarcar

Este exemplo mostra como criar uma política de delegação baseada em recursos que permita que administradores delegados marquem ou desmarquem as políticas de backup. Ele 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*, e *OrganizationId* 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": "DelegatingTaggingBackupPolicies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:TagResource",
        "organizations:UntagResource"
      ],
      "Resource": "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
    }
  ]
}
```

Exemplo: vincular políticas a uma única OU ou conta

Este exemplo mostra como você pode criar uma política de delegação baseada em recursos que permita que administradores delegados `attach` ou `detach` políticas do Organizations de uma unidade organizacional (OU) especificada ou de uma conta específica. Antes de delegar essas ações, você deve delegar as permissões para navegar na estrutura de uma organização e visualizar as contas abaixo dela. Para obter detalhes, consulte Exemplo: Exibir organização OUs, contas e políticas

> **Important**
>
> - Embora essa política permita anexar ou desanexar políticas da OU ou conta especificada, ela exclui crianças OUs e contas menores de idade. OUs
> - 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 *TargetAccountId* 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": "*"
    },
    {
      "Sid": "AttachDetachPoliciesSpecifiedAccountOU",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:AttachPolicy",
        "organizations:DetachPolicy"
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/ou-OUId",
        "arn:aws:organizations::ManagementAccountId:account/
o-OrganizationId/TargetAccountId",
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ]
    }
  ]
}
```

Para delegar a vinculação ou desvinculação de políticas a qualquer OU ou conta nas organizações, substitua o recurso no exemplo anterior pelos seguintes recursos:

```
"Resource": [
    "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
    "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
    "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/backup_policy/
*"
]
```

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`.

> **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:ListRoots",
            "organizations:ListOrganizationalUnitsForParent",
            "organizations:ListParents",
            "organizations:ListChildren",
            "organizations:ListAccounts",
            "organizations:ListAccountsForParent",
            "organizations:ListTagsForResource"
        ],
      "Resource": "*"
    },
    {
      "Sid": "DelegatingNecessaryDescribeListActionsForSpecificPolicyType",
      "Effect": "Allow",
      "Principal": {
```

```
            "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
            "organizations:DescribePolicy",
            "organizations:DescribeEffectivePolicy",
            "organizations:ListPolicies",
            "organizations:ListPoliciesForTarget",
            "organizations:ListTargetsForPolicy"
      ],
      "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/*"
      ],
      "Condition": {
            "StringLikeIfExists": {
                "organizations:PolicyType": "BACKUP_POLICY"
            }
      }
```

```
    }
  ]
}
```

AWS políticas gerenciadas para AWS Organizations

Esta seção identifica as políticas AWS gerenciadas fornecidas para seu uso no gerenciamento de sua organização. Você não pode modificar ou excluir uma política AWS gerenciada, mas pode anexá-la ou desanexá-la às entidades da sua organização conforme necessário.

AWS Organizations políticas gerenciadas para uso com 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 sozinho e, ao AWS atualizar a política conforme apropriado para oferecer suporte a novos serviços, você obtém automaticamente e imediatamente os benefícios da atualização.

Você pode ver a lista de políticas gerenciadas pela AWS na página Policies (Políticas) no console do IAM. Use a lista suspensa Filter policies para selecionar AWS managed.

Você pode usar as seguintes políticas gerenciadas para conceder permissões a usuários da sua organização.

AWS política gerenciada: AWSOrganizationsFullAccess

Fornece todas as permissões necessárias para criar e administrar totalmente uma organização.

Veja esta política: `AWSOrganizationsFullAccess`.

AWS política gerenciada: AWSOrganizationsReadOnlyAccess

Fornece acesso somente de leitura a informações sobre a organização. Não permite que o usuário faça nenhuma alteração.

Veja esta política: `AWSOrganizationsReadOnlyAccess`.

AWS política gerenciada: DeclarativePoliciesEC2Report

Essa política é usada pela função vinculada ao serviço AWSServiceRoleForDeclarativePoliciesEC2Report para permitir que ela descreva os estados dos atributos da conta das contas dos membros.

Veja a política: DeclarativePoliciesEC2Relatório.

Atualizações nas políticas AWS gerenciadas da Organizations

A tabela a seguir detalha as atualizações das políticas AWS gerenciadas 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 .

Alteração	Descrição	Data
AWSOrganizationsFullAccess— atualizado para permitir as permissões de API da conta necessárias para visualizar ou modificar o nome de uma conta por meio do console do Organizations.	Foi adicionada a `account:GetAccountInformation` ação para permitir o acesso para visualizar o nome da conta de qualquer conta em uma organização e a `account:PutAccountName` ação para ativar o acesso para modificar qualquer nome de conta em uma organização.	22 de abril de 2025
DeclarativePoliciesEC2Relatório — Nova política gerenciada	Foi adicionada a `DeclarativePoliciesEC2Report` política para habilitar a funcionalidade da função `AWSServiceRoleForDeclarativePoliciesEC2Report` vinculada ao serviço.	22 de novembro de 2024
AWSOrganizationsReadOnlyAccess— atualizado para permitir que as permissões de API da conta sejam necessárias para visualizar	Foi adicionada a `account:GetPrimaryEmail` ação para permitir o acesso para visualizar o endereço de e-mail do usuário raiz, o para qualquer conta membro em	6 de junho de 2024

Alteração	Descrição	Data
um endereço de e-mail de usuário raiz (endereço de).	uma organização e a `account:GetRegionOptStatus` ação para permitir o acesso para visualizar as regiões habilitadas para qualquer conta membro em uma organização.	
AWSOrganizationsFullAccess— atualizado para incluir `Sid` elementos que descrevam a declaração de política.	`Sid`Elementos adicionados para a política `AWSOrganizationsFullAccess` gerenciada.	6 de fevereiro de 2024
AWSOrganizationsReadOnlyAccess— atualizado para incluir `Sid` elementos que descrevam a declaração de política.	`Sid`Elementos adicionados para a política `AWSOrganizationsReadOnlyAccess` gerenciada.	6 de fevereiro de 2024
AWSOrganizationsFullAccess— atualizado para permitir as permissões de API da conta necessárias para ativar ou desativar Regiões da AWS por meio do console do Organizations.	A `account:ListRegions` `account:DisableRegion` ação `account:EnableRegion` e foi adicionada à política para habilitar o acesso de gravação para ativar ou desativar regiões de 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.	A `account:ListRegions` ação foi adicionada à política para permitir o acesso à visualização das regiões de uma conta.	22 de dezembro de 2022
AWSOrganizationsFullAccess— atualizado para permitir as permissões de API da conta necessárias para adicionar ou editar contatos da conta por meio do console do Organizations.	A `account:PutContactInformation` ação `account:GetContactInformation` e foi adicionada à política para permitir o acesso de gravação para modificar os contatos de uma conta.	21 de outubro de 2022

Alteração	Descrição	Data
AWSOrganizationsReadOnlyAccess— atualizado para permitir as permissões de API da conta necessárias para visualizar os contatos da conta por meio do console do Organizations.	A `account:GetContactInformation` ação foi adicionada à política para permitir o acesso à visualização dos contatos de uma conta.	21 de outubro de 2022
AWSOrganizationsFullAccess— atualizado para permitir a criação de uma organização.	Foi adicionada a `CreateServiceLinkedRole` permissão à política para permitir 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 Organizations.	Foram adicionadas as `account:PutAlternateContact` ações `account:GetAlternateContact` `account:DeleteAlternateContact` ,, à política para permitir o acesso de gravação para modificar contatos alternativos de uma conta.	7 de fevereiro de 2022
AWSOrganizationsReadOnlyAccess— atualizado para permitir as permissões de API da conta necessárias para visualizar contatos alternativos da conta por meio do console do Organizations.	A `account:GetAlternateContact` ação foi adicionada à política para permitir o acesso à visualização de contatos alternativos de uma conta.	7 de fevereiro de 2022

AWS políticas de autorização gerenciadas

As políticas de autorização são semelhantes às políticas de permissão do IAM, mas são um recurso e AWS Organizations não do IAM. Você usa políticas de autorização para configurar e gerenciar centralmente o acesso de diretores e recursos em suas contas de membros.

Você pode ver a lista de políticas de sua organização na página Policies (Políticas) no console do Organizations.

Nome da política	Descrição	ARN
FullAWSAccess	Permite acesso a todas as operações.	arn:aws:organizations: :aws: - Completo policy/service_control_policy/p AWSAccess
RCPFullAWSAccess	Permite acesso a todos os recursos.	arn:aws:organizations: :aws: - policy/resource_control_policy/p RCPFullAWSAccess

Controle de acesso baseado em atributo com tags para AWS Organizations

O controle de acesso baseado em atributos permite que você use atributos gerenciados pelo administrador, como tags anexadas a AWS recursos e AWS identidades, 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.

AWS Organizations os recursos marcáveis incluem a raiz da organização Contas da AWS, as unidades organizacionais (OUs) ou as políticas. Quando anexa tags a recursos do Organizations, você pode usar essas tags para controlar quem pode acessar esses recursos. Você faz isso adicionando `Condition` elementos às suas declarações de política de permissões 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 efetivamente diz “Permitir que o usuário gerencie somente aqueles OUs que têm uma tag com uma chave X e um valorY” ou “Permitir que o usuário gerencie somente aqueles OUs que estão marcados com uma chave Z que tenha o mesmo valor da chave de tag anexada do 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

Ao fazer uma solicitação usando o AWS Management Console, o AWS Command Line Interface (AWS CLI) ou um dos AWS SDKs, você especifica quais recursos 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 Controlando o acesso ao recurso e à AWS: ResourceTag no Guia 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 chamador pode iniciar e interromper uma EC2 instância da Amazon somente se a instância estiver marcada com o mesmo `cost-center` valor do 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, a política de exemplo a seguir permite qualquer operação do Organizations somente se todas as tags presentes na solicitação forem um subconjunto das três tags nesta política.

```
{
    "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 em que a solicitação não tenha a `costcenter` tag ou forneça a essa tag um valor diferente de `12`, 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 Guia do usuário do IAM.

Solução de problemas AWS Organizations de identidade e acesso

Use as informações a seguir para ajudar a diagnosticar e corrigir problemas comuns que você possa encontrar ao trabalhar com o Organizations e o IAM.

Tópicos

- Não tenho autorização para executar uma ação no Organizations
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha tenham acesso Conta da AWS aos recursos da minha Organização

Não tenho autorização para executar uma ação no Organizations

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `organizations:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 organizations:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `organizations:`*`GetWidget`*.

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

Não estou autorizado a realizar iam: PassRole

Se receber uma mensagem de erro informando que você não tem autorização para realizar a ação `iam:PassRole`, suas políticas deverão ser atualizadas para permitir a transmissão de um perfil para o Organizations.

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

O erro exemplificado a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no Organizations. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

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

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

Quero permitir que pessoas fora da minha tenham acesso Conta da AWS aos recursos da minha Organização

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

Para saber mais, consulte:

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

Registro e monitoramento em AWS Organizations

Como uma prática recomendada, você deve monitorar a sua organização para garantir que as alterações sejam registradas. Isso ajuda você a garantir que qualquer alteração inesperada possa ser investigada e que alterações indesejadas possam ser revertidas. AWS Organizations atualmente suporta dois Serviços da AWS que permitem monitorar sua organização e a atividade que acontece dentro dela.

Tópicos

- Registro de chamadas de API com AWS CloudTrail for AWS Organizations
- Amazon EventBridge e AWS Organizations

Registro de chamadas de API com AWS CloudTrail for AWS Organizations

AWS Organizations é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço em AWS Organizations. CloudTrail captura todas as chamadas de API para eventos AWS Organizations as, incluindo chamadas do AWS Organizations console e de chamadas de código para o. AWS Organizations APIs Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para. AWS Organizations Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita AWS Organizations, o endereço IP de onde foi feita, quem a fez, quando foi feita e detalhes adicionais.

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

> **Important**
>
> Você pode ver todas as CloudTrail informações AWS Organizations somente na região Leste dos EUA (Norte da Virgínia). Se você não vê sua AWS Organizations atividade no CloudTrail console, defina-o para Leste dos EUA (Norte da Virgínia) usando o menu no canto superior direito. Se você consultar CloudTrail com as ferramentas do SDK AWS CLI ou SDK, direcione sua consulta para o endpoint do Leste dos EUA (Norte da Virgínia).

AWS Organizations informações em CloudTrail

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

Para obter um registro contínuo de eventos na sua Conta da AWS, incluindo eventos para o AWS Organizations, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Quando o CloudTrail registro está ativado em seu Conta da AWS, as chamadas de API feitas para AWS Organizations ações são rastreadas em arquivos de CloudTrail log, onde são gravadas com outros registros AWS de serviço. Você pode configurar outros Serviços da AWS para analisar e agir com base nos dados do evento coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão Geral para Criar uma Trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando notificações do Amazon SNS para CloudTrail

Todas AWS Organizations as ações são registradas CloudTrail e documentadas na Referência da AWS Organizations API. Por exemplo, chamadas para `CreateAccount` (incluindo o `CreateAccountResult` evento), `ListHandshakesForAccountCreatePolicy`, e `InviteAccountToOrganization` geram entradas nos arquivos de CloudTrail log.

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 AWS serviço

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Entendendo as entradas do arquivo de AWS Organizations log

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

Exemplos de entradas de registro: CloseAccount

O exemplo a seguir mostra uma entrada de CloudTrail registro para uma `CloseAccount` chamada de amostra que é gerada quando a API é chamada e o fluxo de trabalho para fechar a conta começa a ser processado 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 CloudTrail registro para uma `CloseAccountResult` chamada após a conclusão bem-sucedida do fluxo de trabalho em segundo plano para fechar a conta.

```
{
```

```
  "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"
}
```

Exemplos de entradas de registro: CreateAccount

O exemplo a seguir mostra uma entrada de CloudTrail registro para uma `CreateAccount` chamada de amostra que é gerada quando a API é chamada e o fluxo de trabalho para criar a conta começa a ser processado 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 CloudTrail registro para uma `CreateAccount` chamada após a conclusão bem-sucedida do fluxo de trabalho em segundo plano para criar a conta.

```
{
  "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 CloudTrail registro que é gerada após a falha de um fluxo de trabalho em `CreateAccount` segundo plano 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 registro: CreateOrganizationalUnit

O exemplo a seguir mostra uma entrada de CloudTrail registro para uma `CreateOrganizationalUnit` chamada de amostra.

```
{
    "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 registro: InviteAccountToOrganization

O exemplo a seguir mostra uma entrada de CloudTrail registro para uma `InviteAccountToOrganization` chamada de amostra.

```
{
    "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 registro: AttachPolicy

O exemplo a seguir mostra uma entrada de CloudTrail registro para uma `AttachPolicy` chamada de amostra. 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 e AWS Organizations

AWS Organizations pode trabalhar com a Amazon EventBridge, antiga Amazon CloudWatch Events, para gerar eventos quando ações especificadas pelo administrador ocorrem 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 EventBridge regras que buscam essas ações e, em seguida, enviam 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 obter um tutorial que mostra como EventBridge habilitar o monitoramento das principais atividades em sua organização, consulteTutorial: Monitore mudanças importantes em sua organização com a Amazon EventBridge.

> **Important**
>
> Atualmente, AWS Organizations está hospedado somente na região Leste dos EUA (Norte da Virgínia) (embora esteja disponível globalmente). Para executar as etapas deste tutorial, você deve configurar o AWS Management Console para usar essa região.

Para saber mais sobre EventBridge, inclusive como configurá-lo e habilitá-lo, consulte o Guia EventBridge do usuário da Amazon.

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:

- Governança e conformidade de segurança: esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- Referência de serviços qualificados para HIPAA: lista os serviços qualificados para HIPAA. Nem todos Serviços da AWS são elegíveis para a 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 recursos 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 em AWS Organizations

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

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

Segurança da infraestrutura em AWS Organizations

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

Você usa chamadas de API AWS publicadas para acessar Organizations pela rede. Os clientes devem oferecer compatibilidade com:

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

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível 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 AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

Solução de problemas AWS Organizations

Se você encontrar problemas ao trabalhar com o AWS Organizations, consulte os tópicos desta seção.

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. AWS Organizations

Tópicos

Eu recebo uma mensagem de “acesso negado” quando faço uma solicitação para 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 quaisquer condições, como

time-of-day restrições de endereço IP, você também deverá atender a 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 assina solicitações de API manualmente (sem usar o 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 kit de ferramentas do SDK escolhido ou Como usar credenciais de segurança temporárias para solicitar acesso aos AWS recursos no Guia 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. Ao criar uma conta em uma organização usando o AWS Organizations console do, a API ou AWS CLI os comandos da, essas informações não são coletadas automaticamente. Para uma conta que você desejar tornar autônoma, é

necessário aceitar o Contrato do AWS Cliente, escolher um plano de suporte, fornecer e confirmar as informações de contato exigidas, bem como informar o método de pagamento atual. AWS usa o método de pagamento para cobrar por qualquer AWS atividade faturável (fora do nível AWS gratuito da) da que ocorra enquanto a conta não estiver anexada a uma organização. Para obter mais informações, consulte Saindo de uma organização a partir de uma conta de membro com AWS Organizations.

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 devido às cotas da conta. Por exemplo, não é possível remover contas recém-criadas. Tente fazer isso novamente em alguns dias.

Para problemas com a adição de contas, consulte a cota Número máximo padrão de contas. Para problemas com a remoção de contas, consulte a cota Número de contas que é possível encerrar em um período de 30 dias.

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 AWS Organizations leva tempo para se tornar visível em todos os endpoints possíveis. Parte do atraso resulta do tempo necessário para enviar os dados de um servidor para outro ou de uma zona de replicação para outra. AWS Organizations também usa o armazenamento em cache para melhorar o desempenho, porém, em alguns casos, isso pode aumentar o 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
- Garantir consistência ao usar o Amazon S3 e o Amazon Elastic MapReduce para fluxos de trabalho de ETL no blog sobre big data da AWS
- EC2 Consistência eventual na Amazon EC2 API Reference.

Recebo uma mensagem de “Inscrição completa” quando tento acessar uma conta que já faz parte de uma organização

- Pode levar até 48 horas para que a conta do membro herde os detalhes de cobrança da conta de gerenciamento.

- Se o problema persistir após 48 horas, você poderá abrir um caso de suporte para a equipe de suporte de Conta e Cobrança. Para obter mais informações, consulte Criar um caso de suporte.

Chamar a API por meio de solicitações de consulta HTTP

Esta seção contém informações gerais sobre como usar a API de consulta para 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 AWS Organizations Query, você pode usar um dos AWS SDKs. Eles AWS SDKs consistem em bibliotecas e exemplos de código para várias linguagens e plataformas de programação (Java, Ruby, .NET, iOS, Android e muito mais). Eles SDKs fornecem uma maneira conveniente de criar acesso programático a AWS Organizations e. AWS Por exemplo, SDKs cuidar de tarefas como assinar criptograficamente solicitações, gerenciar erros e repetir solicitações automaticamente. Para obter informações sobre o AWS SDKs, incluindo como baixá-los e instalá-los, consulte Ferramentas para Amazon Web Services.

A API de consulta AWS Organizations permite que você chame ações de serviço. As solicitações da API de consulta são solicitações HTTPS que devem conter um `Action` parâmetro para indicar a operação a ser executada. AWS Organizations suporta 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

AWS Organizations tem um único endpoint de API global 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.

Assinatura AWS Organizations de solicitações de API

As solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta. É altamente recomendável que você não use suas Usuário raiz da conta da AWS credenciais para trabalhar diariamente com AWS Organizations. Em vez disso, use as credenciais de um usuário ou perfil do IAM.

Para assinar suas solicitações de API, você deve usar o AWS Signature versão 4. Para obter informações sobre como usar o Signature versão 4, consulte Solicitações de AWS API de assinatura no Guia do usuário do IAM.

AWS Organizations não oferece suporte a versões anteriores, como a Signature Version 2.

Para obter mais informações, consulte:

- AWS Credenciais de segurança — Fornece informações gerais sobre os tipos de credenciais que você pode usar para acessar. AWS
- Práticas recomendadas de segurança no IAM — Oferece sugestões para usar o serviço IAM para ajudar a proteger seus AWS recursos, incluindo aqueles em AWS Organizations.
- Credenciais de segurança temporárias no IAM: descreve como criar e usar credenciais de segurança temporárias.

Exemplos de código para organizações que usam AWS SDKs

Os exemplos de código a seguir mostram como usar o Organizations com um kit AWS de desenvolvimento de software (SDK).

Ações são trechos de código de programas maiores e devem ser executadas em contexto. Embora as ações mostrem como chamar perfis de serviço individuais, você pode ver as ações no contexto em seus cenários relacionados.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Exemplos de código

- Exemplos básicos para organizações que usam AWS SDKs
  - Ações para organizações usando AWS SDKs
    - Use AttachPolicy com um AWS SDK ou CLI
    - Use CreateAccount com um AWS SDK ou CLI
    - Use CreateOrganization com um AWS SDK ou CLI
    - Use CreateOrganizationalUnit com um AWS SDK ou CLI
    - Use CreatePolicy com um AWS SDK ou CLI
    - Use DeleteOrganization com um AWS SDK ou CLI
    - Use DeleteOrganizationalUnit com um AWS SDK ou CLI
    - Use DeletePolicy com um AWS SDK ou CLI
    - Use DescribePolicy com um AWS SDK ou CLI
    - Use DetachPolicy com um AWS SDK ou CLI
    - Use ListAccounts com um AWS SDK ou CLI
    - Use ListOrganizationalUnitsForParent com um AWS SDK ou CLI
    - Use ListPolicies com um AWS SDK ou CLI

Exemplos básicos para organizações que usam AWS SDKs

Os exemplos de código a seguir mostram como usar o básico do AWS Organizations with AWS SDKs.

Exemplos

- Ações para organizações usando AWS SDKs
  - Use AttachPolicy com um AWS SDK ou CLI
  - Use CreateAccount com um AWS SDK ou CLI
  - Use CreateOrganization com um AWS SDK ou CLI
  - Use CreateOrganizationalUnit com um AWS SDK ou CLI
  - Use CreatePolicy com um AWS SDK ou CLI
  - Use DeleteOrganization com um AWS SDK ou CLI
  - Use DeleteOrganizationalUnit com um AWS SDK ou CLI
  - Use DeletePolicy com um AWS SDK ou CLI
  - Use DescribePolicy com um AWS SDK ou CLI
  - Use DetachPolicy com um AWS SDK ou CLI
  - Use ListAccounts com um AWS SDK ou CLI
  - Use ListOrganizationalUnitsForParent com um AWS SDK ou CLI
  - Use ListPolicies com um AWS SDK ou CLI

Ações para organizações usando AWS SDKs

Os exemplos de código a seguir demonstram como realizar ações individuais da Organizations com AWS SDKs. Cada exemplo inclui um link para GitHub, onde você pode encontrar instruções para configurar e executar o código.

Os exemplos a seguir incluem apenas as ações mais utilizadas. Para obter uma lista completa, consulte a Referência de APIs do AWS Organizations.

Exemplos

- Use AttachPolicy com um AWS SDK ou CLI
- Use CreateAccount com um AWS SDK ou CLI
- Use CreateOrganization com um AWS SDK ou CLI

- Use CreateOrganizationalUnit com um AWS SDK ou CLI
- Use CreatePolicy com um AWS SDK ou CLI
- Use DeleteOrganization com um AWS SDK ou CLI
- Use DeleteOrganizationalUnit com um AWS SDK ou CLI
- Use DeletePolicy com um AWS SDK ou CLI
- Use DescribePolicy com um AWS SDK ou CLI
- Use DetachPolicy com um AWS SDK ou CLI
- Use ListAccounts com um AWS SDK ou CLI
- Use ListOrganizationalUnitsForParent com um AWS SDK ou CLI
- Use ListPolicies com um AWS SDK ou CLI

Use **`AttachPolicy`** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `AttachPolicy`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to attach an AWS Organizations policy to an organization,
/// an organizational unit, or an account.
/// </summary>
public class AttachPolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then calls the
```

```
        /// AttachPolicyAsync method to attach the policy to the root
        /// organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new AttachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.AttachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully attached Policy ID {policyId} to
Target ID: {targetId}.");
            }
            else
            {
                Console.WriteLine("Was not successful in attaching the policy.");
            }
        }
    }
```

- Para obter detalhes da API, consulte AttachPolicya Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como anexar uma política a uma raiz, unidade operacional ou conta

Exemplo 1

O seguinte exemplo mostra com anexar uma política de controle de serviços (SCP) a uma unidade operacional (OU):

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id ou-examplerootid111-exampleouid111
```

Exemplo 2

O seguinte exemplo mostra como anexar uma política de controle de serviços a uma conta:

```
aws organizations attach-policy
                --policy-id p-examplepolicyid111
                --target-id 333333333333
```

- Para obter detalhes da API, consulte AttachPolicyem Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
def attach_policy(policy_id, target_id, orgs_client):
    """
    Attaches a policy to a target. The target is an organization root, account,
 or
    organizational unit.

    :param policy_id: The ID of the policy to attach.
    :param target_id: The ID of the resources to attach the policy to.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.attach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Attached policy %s to target %s.", policy_id, target_id)
    except ClientError:
        logger.exception(
            "Couldn't attach policy %s to target %s.", policy_id, target_id
        )
```

```
        raise
```

- Para obter detalhes da API, consulte a AttachPolicyReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`CreateAccount`** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `CreateAccount`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Creates a new AWS Organizations account.
/// </summary>
public class CreateAccount
{
    /// <summary>
    /// Initializes an Organizations client object and uses it to create
    /// the new account with the name specified in accountName.
    /// </summary>
    public static async Task Main()
```

```
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var accountName = "ExampleAccount";
            var email = "someone@example.com";

            var request = new CreateAccountRequest
            {
                AccountName = accountName,
                Email = email,
            };

            var response = await client.CreateAccountAsync(request);
            var status = response.CreateAccountStatus;

            Console.WriteLine($"The staus of {status.AccountName} is
{status.State}.");
        }
    }
```

- Para obter detalhes da API, consulte CreateAccounta Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como criar uma conta de membro que automaticamente faça parte da organização

O exemplo a seguir mostra como criar uma conta de membro em uma organização. A conta de membro é configurada com o nome Production Account e o endereço de e-mail susan@example.com. Organizations cria automaticamente uma função do IAM usando o nome padrão de OrganizationAccountAccessRole porque o parâmetro roleName não está especificado. Além disso, a configuração que permite que usuários ou funções do IAM com permissões suficientes acessem os dados de faturamento da conta é definida com o valor padrão de ALLOW porque o IamUserAccessToBilling parâmetro não foi especificado. Organizations envia automaticamente a Susan um e-mail de “Bem-vindo a AWS”:

```
aws organizations create-account --email susan@example.com --account-
name "Production Account"
```

A saída inclui um objeto de solicitação que mostra que o status agora é `IN_PROGRESS`:

```
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

Posteriormente, você pode consultar o status atual da solicitação fornecendo o valor de resposta Id ao describe-create-account-status comando como o valor do create-account-request-id parâmetro.

Para obter mais informações, consulte Criando uma AWS conta em sua organização no Guia do Usuário do AWS Organizations.

- Para obter detalhes da API, consulte CreateAccountem Referência de AWS CLI Comandos.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`CreateOrganization`** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `CreateOrganization`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;
```

```
    /// <summary>
    /// Creates an organization in AWS Organizations.
    /// </summary>
    public class CreateOrganization
    {
        /// <summary>
        /// Creates an Organizations client object and then uses it to create
        /// a new organization with the default user as the administrator, and
        /// then displays information about the new organization.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.CreateOrganizationAsync(new
CreateOrganizationRequest
            {
                FeatureSet = "ALL",
            });

            Organization newOrg = response.Organization;

            Console.WriteLine($"Organization: {newOrg.Id} Main Accoount:
{newOrg.MasterAccountId}");
        }
    }
```

- Para obter detalhes da API, consulte CreateOrganizationa Referência AWS SDK para .NET da API.

CLI

AWS CLI

Exemplo 1: como criar uma organização

Bill quer criar uma organização usando as credenciais da conta 111111111111. O exemplo a seguir mostra que a conta se torna a conta principal na nova organização. Como ele não especificou um conjunto de recursos, a nova organização usa como padrão todos os recursos habilitados e as políticas de controle de serviços são habilitadas na raiz.

```
aws organizations create-organization
```

A saída inclui um objeto de organização com detalhes sobre a nova organização:

```
{
        "Organization": {
                "AvailablePolicyTypes": [
                        {
                                "Status": "ENABLED",
                                "Type": "SERVICE_CONTROL_POLICY"
                        }
                ],
                "MasterAccountId": "111111111111",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
                "FeatureSet": "ALL",
                "Id": "o-exampleorgid",
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid"
        }
}
```

Exemplo 2: como criar uma organização apenas com os recursos de faturamento consolidados

O seguinte exemplo cria uma organização compatível apenas com os recursos de faturamento consolidados:

```
aws organizations create-organization --feature-set CONSOLIDATED_BILLING
```

A saída inclui um objeto de organização com detalhes sobre a nova organização:

```
{
        "Organization": {
                "Arn": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
                "AvailablePolicyTypes": [],
                "Id": "o-exampleorgid",
                "MasterAccountArn": "arn:aws:organizations::111111111111:account/
o-exampleorgid/111111111111",
                "MasterAccountEmail": "bill@example.com",
```

```
                "MasterAccountId": "111111111111",
                "FeatureSet": "CONSOLIDATED_BILLING"
        }
}
```

Para obter informações, consulte Criar uma organização no Guia do usuário do AWS Organizations.

- Para obter detalhes da API, consulte CreateOrganizationem Referência de AWS CLI Comandos.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`CreateOrganizationalUnit`** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `CreateOrganizationalUnit`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Creates a new organizational unit in AWS Organizations.
    /// </summary>
    public class CreateOrganizationalUnit
    {
        /// <summary>
        /// Initializes an Organizations client object and then uses it to call
```

```
        /// the CreateOrganizationalUnit method. If the call succeeds, it
        /// displays information about the new organizational unit.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var orgUnitName = "ProductDevelopmentUnit";

            var request = new CreateOrganizationalUnitRequest
            {
                Name = orgUnitName,
                ParentId = "r-0000",
            };

            var response = await client.CreateOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully created organizational unit:
{orgUnitName}.");
                Console.WriteLine($"Organizational unit {orgUnitName} Details");
                Console.WriteLine($"ARN: {response.OrganizationalUnit.Arn} Id:
{response.OrganizationalUnit.Id}");
            }
            else
            {
                Console.WriteLine("Could not create new organizational unit.");
            }
        }
    }
```

- Para obter detalhes da API, consulte CreateOrganizationalUnita Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como criar uma unidade organizacional em uma unidade organizacional raiz ou pai

O seguinte exemplo mostra como criar uma UO chamada AccountingOU:

```
aws organizations create-organizational-unit --parent-id r-examplerootid111 --
name AccountingOU
```

A saída inclui um objeto organizationalUnit que contém detalhes sobre a nova UO:

```
{
        "OrganizationalUnit": {
                "Id": "ou-examplerootid111-exampleouid111",
                "Arn": "arn:aws:organizations::111111111111:ou/o-exampleorgid/ou-
examplerootid111-exampleouid111",
                "Name": "AccountingOU"
        }
}
```

- Para obter detalhes da API, consulte CreateOrganizationalUnitem Referência de AWS CLI Comandos.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use `CreatePolicy` com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `CreatePolicy`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
```

```
    using Amazon.Organizations.Model;

    /// <summary>
    /// Creates a new AWS Organizations Policy.
    /// </summary>
    public class CreatePolicy
    {
        /// <summary>
        /// Initializes the AWS Organizations client object, uses it to
        /// create a new Organizations Policy, and then displays information
        /// about the newly created Policy.
        /// </summary>
        public static async Task Main()
        {
            IAmazonOrganizations client = new AmazonOrganizationsClient();
            var policyContent = "{" +
                "   \"Version\": \"2012-10-17\"," +
                " \"Statement\" : [{" +
                    " \"Action\" : [\"s3:*\"]," +
                    " \"Effect\" : \"Allow\"," +
                    " \"Resource\" : \"*\"" +
                "}]" +
            "}";

            try
            {
                var response = await client.CreatePolicyAsync(new
CreatePolicyRequest
                {
                    Content = policyContent,
                    Description = "Enables admins of attached accounts to
delegate all Amazon S3 permissions",
                    Name = "AllowAllS3Actions",
                    Type = "SERVICE_CONTROL_POLICY",
                });

                Policy policy = response.Policy;
                Console.WriteLine($"{policy.PolicySummary.Name} has the following
content: {policy.Content}");
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
```

```
        }
    }
```

- Para obter detalhes da API, consulte CreatePolicya Referência AWS SDK para .NET da API.

CLI

AWS CLI

Exemplo 1: como criar uma política com um arquivo de origem de texto na política JSON

O exemplo a seguir mostra como criar uma política de controle de serviço (SCP) chamada `AllowAllS3Actions`. O conteúdo da política provém de um arquivo chamado `policy.json` presente no computador local.

```
aws organizations create-policy --content file://policy.json --
name AllowAllS3Actions, --type SERVICE_CONTROL_POLICY --description "Allows
 delegation of all S3 actions"
```

A saída inclui um objeto de política com detalhes sobre a nova política:

```
{
        "Policy": {
                "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource\":[\"*\"]}]}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::o-exampleorgid:policy/
service_control_policy/p-examplepolicyid111",
                        "Description": "Allows delegation of all S3 actions",
                        "Name": "AllowAllS3Actions",
                        "Type":"SERVICE_CONTROL_POLICY"
                }
        }
}
```

Exemplo 2: como criar uma política tendo uma política JSON como parâmetro

O exemplo a seguir mostra como criar a mesma SCP, mas, desta vez, incorporando o conteúdo da política como uma string JSON no parâmetro. A string deve ser recuada com barras invertidas antes das aspas duplas para garantir que ela seja tratada como literal no parâmetro (que está entre aspas duplas):

```
aws organizations create-policy --content "{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Action\":[\"s3:*\"],\"Resource
\":[\"*\"]}]}" --name AllowAllS3Actions --type SERVICE_CONTROL_POLICY --
description "Allows delegation of all S3 actions"
```

Para obter mais informações sobre como criar e usar políticas em sua organização, consulte Gerenciamento de políticas organizacionais no Guia do usuário do AWS Organizations.

- Para obter detalhes da API, consulte CreatePolicyem Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
def create_policy(name, description, content, policy_type, orgs_client):
    """
    Creates a policy.

    :param name: The name of the policy.
    :param description: The description of the policy.
    :param content: The policy content as a dict. This is converted to JSON
 before
                    it is sent to AWS. The specific format depends on the policy
 type.
    :param policy_type: The type of the policy.
    :param orgs_client: The Boto3 Organizations client.
    :return: The newly created policy.
    """
    try:
        response = orgs_client.create_policy(
```

```
            Name=name,
            Description=description,
            Content=json.dumps(content),
            Type=policy_type,
        )
        policy = response["Policy"]
        logger.info("Created policy %s.", name)
    except ClientError:
        logger.exception("Couldn't create policy %s.", name)
        raise
    else:
        return policy
```

- Para obter detalhes da API, consulte a CreatePolicyReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DeleteOrganization`** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `DeleteOrganization`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
```

```
    using Amazon.Organizations.Model;

    /// <summary>
    /// Shows how to delete an existing organization using the AWS
    /// Organizations Service.
    /// </summary>
    public class DeleteOrganization
    {
        /// <summary>
        /// Initializes the Organizations client and then calls
        /// DeleteOrganizationAsync to delete the organization.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var response = await client.DeleteOrganizationAsync(new
DeleteOrganizationRequest());

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine("Successfully deleted organization.");
            }
            else
            {
                Console.WriteLine("Could not delete organization.");
            }
        }
    }
```

- Para obter detalhes da API, consulte DeleteOrganizationa Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como excluir uma organização

O exemplo a seguir mostra como excluir uma organização. Você deve ser administrador da conta principal na organização para poder realizar essa operação. O exemplo pressupõe que você removeu anteriormente todas as contas e políticas dos membros da organização: OUs

```
aws organizations delete-organization
```

- Para obter detalhes da API, consulte DeleteOrganizationem Referência de AWS CLI Comandos.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DeleteOrganizationalUnit`** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `DeleteOrganizationalUnit`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Shows how to delete an existing AWS Organizations organizational unit.
/// </summary>
public class DeleteOrganizationalUnit
{
    /// <summary>
    /// Initializes the Organizations client object and calls
    /// DeleteOrganizationalUnitAsync to delete the organizational unit
```

```
        /// with the selected ID.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var orgUnitId = "ou-0000-00000000";

            var request = new DeleteOrganizationalUnitRequest
            {
                OrganizationalUnitId = orgUnitId,
            };

            var response = await client.DeleteOrganizationalUnitAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted the organizational unit
with ID: {orgUnitId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete the organizational unit with
ID: {orgUnitId}.");
            }
        }
    }
```

- Para obter detalhes da API, consulte DeleteOrganizationalUnita Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como excluir uma UO

O exemplo a seguir mostra como excluir uma UO. O exemplo pressupõe que você removeu anteriormente todas as contas e outras OUs da OU:

```
aws organizations delete-organizational-unit --organizational-unit-id ou-
examplerootid111-exampleouid111
```

- Para obter detalhes da API, consulte DeleteOrganizationalUnitem Referência de AWS CLI Comandos.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DeletePolicy`** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `DeletePolicy`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Deletes an existing AWS Organizations policy.
/// </summary>
public class DeletePolicy
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// delete the policy with the specified policyId.
    /// </summary>
    public static async Task Main()
    {
```

```
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var policyId = "p-00000000";

            var request = new DeletePolicyRequest
            {
                PolicyId = policyId,
            };

            var response = await client.DeletePolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully deleted Policy: {policyId}.");
            }
            else
            {
                Console.WriteLine($"Could not delete Policy: {policyId}.");
            }
        }
    }
```

- Para obter detalhes da API, consulte DeletePolicya Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como excluir uma política

O exemplo a seguir mostra como excluir uma política de uma organização. O exemplo pressupõe que você já separou a política de todas as entidades:

```
aws organizations delete-policy --policy-id p-examplepolicyid111
```

- Para obter detalhes da API, consulte DeletePolicyem Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
def delete_policy(policy_id, orgs_client):
    """
    Deletes a policy.

    :param policy_id: The ID of the policy to delete.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.delete_policy(PolicyId=policy_id)
        logger.info("Deleted policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't delete policy %s.", policy_id)
        raise
```

- Para obter detalhes da API, consulte a DeletePolicyReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribePolicy`** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `DescribePolicy`.

CLI

AWS CLI

Como obter informações sobre uma política

O seguinte exemplo mostra como solicitar informações sobre uma política:

```
aws organizations describe-policy --policy-id p-examplepolicyid111
```

A saída inclui um objeto de política que contém detalhes sobre a política:

```
{
        "Policy": {
                "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement
\": [\n    {\n      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n
 \"Resource\": \"*\"\n    }\n  ]\n}",
                "PolicySummary": {
                        "Arn": "arn:aws:organizations::111111111111:policy/o-
exampleorgid/service_control_policy/p-examplepolicyid111",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-examplepolicyid111",
                        "AwsManaged": false,
                        "Name": "AllowAllS3Actions",
                        "Description": "Enables admins to delegate S3
 permissions"
                }
        }
}
```

- Para obter detalhes da API, consulte DescribePolicyem Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
def describe_policy(policy_id, orgs_client):
    """
    Describes a policy.

    :param policy_id: The ID of the policy to describe.
    :param orgs_client: The Boto3 Organizations client.
    :return: The description of the policy.
    """
    try:
        response = orgs_client.describe_policy(PolicyId=policy_id)
        policy = response["Policy"]
        logger.info("Got policy %s.", policy_id)
    except ClientError:
        logger.exception("Couldn't get policy %s.", policy_id)
        raise
    else:
        return policy
```

- Para obter detalhes da API, consulte a DescribePolicyReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DetachPolicy`** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `DetachPolicy`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Shows how to detach a policy from an AWS Organizations organization,
    /// organizational unit, or account.
    /// </summary>
    public class DetachPolicy
    {
        /// <summary>
        /// Initializes the Organizations client object and uses it to call
        /// DetachPolicyAsync to detach the policy.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var policyId = "p-00000000";
            var targetId = "r-0000";

            var request = new DetachPolicyRequest
            {
                PolicyId = policyId,
                TargetId = targetId,
            };

            var response = await client.DetachPolicyAsync(request);

            if (response.HttpStatusCode == System.Net.HttpStatusCode.OK)
            {
                Console.WriteLine($"Successfully detached policy with Policy Id:
{policyId}.");
            }
            else
            {
                Console.WriteLine("Could not detach the policy.");
            }
        }
    }
```

- Para obter detalhes da API, consulte DetachPolicya Referência AWS SDK para .NET da API.

CLI

AWS CLI

Como separar uma política de uma raiz, UO ou conta

O seguinte exemplo mostra como separar uma política de uma UO:

```
aws organizations  detach-policy  --target-id ou-examplerootid111-exampleouid111
 --policy-id p-examplepolicyid111
```

- Para obter detalhes da API, consulte DetachPolicyem Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
def detach_policy(policy_id, target_id, orgs_client):
    """
    Detaches a policy from a target.

    :param policy_id: The ID of the policy to detach.
    :param target_id: The ID of the resource where the policy is currently
 attached.
    :param orgs_client: The Boto3 Organizations client.
    """
    try:
        orgs_client.detach_policy(PolicyId=policy_id, TargetId=target_id)
        logger.info("Detached policy %s from target %s.", policy_id, target_id)
    except ClientError:
```

```
        logger.exception(
            "Couldn't detach policy %s from target %s.", policy_id, target_id
        )
        raise
```

- Para obter detalhes da API, consulte a DetachPolicyReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`ListAccounts`** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `ListAccounts`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Uses the AWS Organizations service to list the accounts associated
/// with the default account.
/// </summary>
public class ListAccounts
{
    /// <summary>
```

```
        /// Creates the Organizations client and then calls its
        /// ListAccountsAsync method.
        /// </summary>
        public static async Task Main()
        {
            // Create the client object using the default account.
            IAmazonOrganizations client = new AmazonOrganizationsClient();

            var request = new ListAccountsRequest
            {
                MaxResults = 5,
            };

            var response = new ListAccountsResponse();
            try
            {
                do
                {
                    response = await client.ListAccountsAsync(request);
                    response.Accounts.ForEach(a => DisplayAccounts(a));
                    if (response.NextToken is not null)
                    {
                        request.NextToken = response.NextToken;
                    }
                }
                while (response.NextToken is not null);
            }
            catch (AWSOrganizationsNotInUseException ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about an Organizations account.
        /// </summary>
        /// <param name="account">An Organizations account for which to display
        /// information on the console.</param>
        private static void DisplayAccounts(Account account)
        {
            string accountInfo = $"{account.Id}
{account.Name}\t{account.Status}";

            Console.WriteLine(accountInfo);
```

```
        }
    }
```

- Para obter detalhes da API, consulte ListAccountsa Referência AWS SDK para .NET da API.

CLI

AWS CLI

Para recuperar uma lista de todas as contas de uma organização

O seguinte exemplo mostra como solicitar uma lista das contas de uma organização:

```
aws organizations list-accounts
```

A saída inclui uma lista de objetos de resumo da conta.

```
{
        "Accounts": [
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/111111111111",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481830215.45,
                        "Id": "111111111111",
                        "Name": "Master Account",
                        "Email": "bill@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/222222222222",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835741.044,
                        "Id": "222222222222",
                        "Name": "Production Account",
                        "Email": "alice@example.com",
                        "Status": "ACTIVE"
                },
```

```
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/333333333333",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835795.536,
                        "Id": "333333333333",
                        "Name": "Development Account",
                        "Email": "juan@example.com",
                        "Status": "ACTIVE"
                },
                {
                        "Arn": "arn:aws:organizations::111111111111:account/o-
exampleorgid/444444444444",
                        "JoinedMethod": "INVITED",
                        "JoinedTimestamp": 1481835812.143,
                        "Id": "444444444444",
                        "Name": "Test Account",
                        "Email": "anika@example.com",
                        "Status": "ACTIVE"
                }
        ]
}
```

- Para obter detalhes da API, consulte ListAccountsem Referência de AWS CLI Comandos.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`ListOrganizationalUnitsForParent`** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `ListOrganizationalUnitsForParent`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
using System;
using System.Threading.Tasks;
using Amazon.Organizations;
using Amazon.Organizations.Model;

/// <summary>
/// Lists the AWS Organizations organizational units that belong to an
/// organization.
/// </summary>
public class ListOrganizationalUnitsForParent
{
    /// <summary>
    /// Initializes the Organizations client object and then uses it to
    /// call the ListOrganizationalUnitsForParentAsync method to retrieve
    /// the list of organizational units.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        var parentId = "r-0000";

        var request = new ListOrganizationalUnitsForParentRequest
        {
            ParentId = parentId,
            MaxResults = 5,
        };

        var response = new ListOrganizationalUnitsForParentResponse();
        try
        {
            do
            {
                response = await
client.ListOrganizationalUnitsForParentAsync(request);
                response.OrganizationalUnits.ForEach(u =>
DisplayOrganizationalUnit(u));
                if (response.NextToken is not null)
                {
                    request.NextToken = response.NextToken;
                }
            }
```

```
                while (response.NextToken is not null);
            }
            catch (Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /// <summary>
        /// Displays information about an Organizations organizational unit.
        /// </summary>
        /// <param name="unit">The OrganizationalUnit for which to display
        /// information.</param>
        public static void DisplayOrganizationalUnit(OrganizationalUnit unit)
        {
            string accountInfo = $"{unit.Id} {unit.Name}\t{unit.Arn}";

            Console.WriteLine(accountInfo);
        }
    }
```

- Para obter detalhes da API, consulte ListOrganizationalUnitsForParenta Referência AWS SDK para .NET da API.

CLI

AWS CLI

Para recuperar uma lista de OUs em uma OU principal ou raiz

O exemplo a seguir mostra como obter uma lista de OUs em uma raiz especificada:

```
aws organizations list-organizational-units-for-parent --parent-id r-
examplerootid111
```

A saída mostra que a raiz especificada contém duas OUs e mostra detalhes de cada uma:

```
{
        "OrganizationalUnits": [
                {
```

```
                        "Name": "AccountingDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid111"
                },
                {
                        "Name": "ProductionDepartment",
                        "Arn": "arn:aws:organizations::o-exampleorgid:ou/r-
examplerootid111/ou-examplerootid111-exampleouid222"
                }
        ]
}
```

- Para obter detalhes da API, consulte ListOrganizationalUnitsForParentem Referência de AWS CLI Comandos.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`ListPolicies`** com um AWS SDK ou CLI

Os exemplos de código a seguir mostram como usar o `ListPolicies`.

.NET

SDK para .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
    using System;
    using System.Threading.Tasks;
    using Amazon.Organizations;
    using Amazon.Organizations.Model;

    /// <summary>
    /// Shows how to list the AWS Organizations policies associated with an
    /// organization.
```

```
/// </summary>
public class ListPolicies
{
    /// <summary>
    /// Initializes an Organizations client object, and then calls its
    /// ListPoliciesAsync method.
    /// </summary>
    public static async Task Main()
    {
        // Create the client object using the default account.
        IAmazonOrganizations client = new AmazonOrganizationsClient();

        // The value for the Filter parameter is required and must must be
        // one of the following:
        //     AISERVICES_OPT_OUT_POLICY
        //     BACKUP_POLICY
        //     SERVICE_CONTROL_POLICY
        //     TAG_POLICY
        var request = new ListPoliciesRequest
        {
            Filter = "SERVICE_CONTROL_POLICY",
            MaxResults = 5,
        };

        var response = new ListPoliciesResponse();
        try
        {
            do
            {
                response = await client.ListPoliciesAsync(request);
                response.Policies.ForEach(p => DisplayPolicies(p));
                if (response.NextToken is not null)
                {
                    request.NextToken = response.NextToken;
                }
            }
            while (response.NextToken is not null);
        }
        catch (AWSOrganizationsNotInUseException ex)
        {
            Console.WriteLine(ex.Message);
        }
    }
```

```
        /// <summary>
        /// Displays information about the Organizations policies associated
        /// with an organization.
        /// </summary>
        /// <param name="policy">An Organizations policy summary to display
        /// information on the console.</param>
        private static void DisplayPolicies(PolicySummary policy)
        {
            string policyInfo = $"{policy.Id}
 {policy.Name}\t{policy.Description}";

            Console.WriteLine(policyInfo);
        }
    }
```

- Para obter detalhes da API, consulte ListPoliciesa Referência AWS SDK para .NET da API.

CLI

AWS CLI

Para recuperar uma lista de todas as políticas de um determinado tipo de uma organização

O exemplo a seguir mostra como obter uma lista de SCPs, conforme especificado pelo parâmetro filter:

```
aws organizations list-policies --filter SERVICE_CONTROL_POLICY
```

A saída inclui uma lista de políticas com informações resumidas:

```
{
        "Policies": [
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllS3Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid111",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid111",
```

```
                        "Description": "Enables account admins to delegate
 permissions for any S3 actions to users and roles in their accounts."
                },
                {
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Name": "AllowAllEC2Actions",
                        "AwsManaged": false,
                        "Id": "p-examplepolicyid222",
                        "Arn": "arn:aws:organizations::111111111111:policy/
service_control_policy/p-examplepolicyid222",
                        "Description": "Enables account admins to delegate
 permissions for any EC2 actions to users and roles in their accounts."
                },
                {
                        "AwsManaged": true,
                        "Description": "Allows access to every operation",
                        "Type": "SERVICE_CONTROL_POLICY",
                        "Id": "p-FullAWSAccess",
                        "Arn": "arn:aws:organizations::aws:policy/
service_control_policy/p-FullAWSAccess",
                        "Name": "FullAWSAccess"
                }
        ]
}
```

- Para obter detalhes da API, consulte ListPoliciesem Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
def list_policies(policy_filter, orgs_client):
    """
    Lists the policies for the account, limited to the specified filter.

    :param policy_filter: The kind of policies to return.
```

```
    :param orgs_client: The Boto3 Organizations client.
    :return: The list of policies found.
    """
    try:
        response = orgs_client.list_policies(Filter=policy_filter)
        policies = response["Policies"]
        logger.info("Found %s %s policies.", len(policies), policy_filter)
    except ClientError:
        logger.exception("Couldn't get %s policies.", policy_filter)
        raise
    else:
        return policies
```

- Para obter detalhes da API, consulte a ListPoliciesReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Organizations com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Histórico do documento para AWS Organizations

A tabela a seguir descreve as principais atualizações da documentação do AWS Organizations.

- Versão da API: 28/11/2016
- Última atualização da documentação: 17 de junho de 2025

Alteração	Descrição	Data
Políticas do Security Hub adicionadas	Você pode usar as políticas do Security Hub para gerenciar centralmente as configurações do Security Hub em todo o seu. AWS Organizations Essas políticas ajudam você a habilitar recursos e manter controles de segurança consistentes em várias contas em sua organização.	17 de junho de 2025
Atualizou a política AWSOrganizations FullAccess gerenciada	Foi adicionada a `account:GetAccountInformation` ação para permitir o acesso para visualizar o nome da conta de qualquer conta em uma organização e a `account:PutAccountName` ação para ativar o acesso para modificar qualquer nome de conta em uma organização.	22 de abril de 2025
Integração de organizações com Notificações de Usuários da AWS	Você pode se integrar Notificações de Usuários AWS Organizations para configurar e visualizar notificações	24 de janeiro de 2025

	centralmente em todas as contas da sua organização.	
Integração de organizações com AWS Managed Services (AMS) Self-Service Reporting (SSR)	Você pode integrar o AMS SSR AWS Organizations para habilitar os relatórios de autoatendimento agregados (SSR). Esse é um recurso do AMS que permite que os clientes do Advanced e do Accelerate visualizem seus relatórios de autoatendimento existentes agregados no nível da organização, em todas as contas.	21 de janeiro de 2025
Políticas declarativas adicionadas	Você pode usar políticas declarativas para declarar e aplicar centralmente as configurações desejadas para uma determinada empresa em grande escala AWS service (Serviço da AWS) em toda a organização. Uma vez conectada, a configuração é sempre mantida quando o serviço adiciona novos recursos ou APIs.	1.º de dezembro de 2024
Nova política AWS gerenciada	Foi adicionada a `DeclarativePoliciesEC2Report` política para ativar a funcionalidade da função vinculada ao serviço declarative-policies-ec2.amazonaws.com.	22 de novembro de 2024

Políticas de backup atualizadas	AWS Backup as políticas atualizaram a chave de `selections` política para incluir uma chave de `conditions` política e adicionaram uma nova chave de `resources` política ao esquema. Com o novo esquema, você tem mais flexibilidade na seleção de recursos para suas políticas de backup.	14 de novembro de 2024
Gerencie centralmente o acesso raiz para contas-membro	Agora é possível gerenciar credenciais de usuário-raiz privilegiado em todas as contas-membro do AWS Organizations com acesso raiz centralizado. Proteja centralmente as credencias do usuário raiz do seu uso Contas da AWS gerenciado AWS Organizations para remover e impedir a recuperação e o acesso às credencias do usuário raiz em grande escala.	14 de novembro de 2024
Políticas de controle de recursos adicionadas (RCPs)	Você pode usar políticas de controle de recursos (RCPs) para controlar o máximo de permissões disponíveis para recursos em uma organização.	13 de novembro de 2024

Políticas de aplicativos de bate-papo adicionadas	Você pode usar as políticas de aplicativos de bate-papo para controlar o acesso às contas da sua organização a partir de aplicativos de bate-papo, como Slack e Microsoft Teams.	26 de setembro de 2024
Atualizações de conteúdo baseadas em cenários	A AWS Organizations documentação foi atualizad a para ser mais orientada por cenários em todo o guia e o conteúdo foi reorganiz ado para melhorar a legibilid ade e a descoberta. Se você tiver comentários sobre essas alterações, use o botão Envie seu feedback na parte inferior da página.	4 de setembro de 2024
Novo tópico de recusa de todos os serviços de IA	Foi adicionada documenta ção sobre como optar por não participar de todos os serviços de AWS IA compatíveis.	16 de agosto de 2024
O Organizations já oferece suporte a 10.000 contas em uma organização	Agora você pode gerenciar até 10.000 contas-membro em uma organização, dobrando o limite anterior de 5.000 contas. Se você tiver um requisito válido e uma necessidade comercial, poderá solicitar e ter aprovação ara uma cota de 10.000 contas sem a verificaç ão do limite de serviço do Organizations ou de outros Serviços da AWS integrados.	14 de agosto de 2024

Novo tópico de migração de conta	Adicionamos documentação sobre como migrar uma conta de uma organização para outra.	1.º de agosto de 2024
Políticas de backup atualizadas	AWS Backup as políticas agora oferecem suporte aos arquivos de snapshot do Amazon Elastic Block Store (Amazon EBS). Para obter exemplos atualizados, consulte Atualização de uma política de backup e Sintaxe e exemplos de políticas de backup.	9 de julho de 2024
Atualizou a política AWSOrganizations ReadOnlyAccess gerenciada	Adicionou a `account:GetPrimaryEmail` ação à AWSOrganizations ReadOnlyAccess política que permite o acesso para visualizar o endereço de e-mail do usuário raiz de qualquer conta membro em uma organização e adicionou a `account:GetRegionOptStatus` ação para permitir o acesso à visualização das regiões habilitadas para qualquer conta membro em uma organização.	6 de junho de 2024

Novo tópico de atualização do endereço de e-mail do usuário root	O Organizations agora fornece a capacidade de atualizar centralmente o endereço de e-mail do usuário raiz (endereço de) para qualquer conta membro em uma organização.	6 de junho de 2024
Declarações de política atualizadas	Foram adicionados novos `Sid` elementos às declarações de políticas AWS Organizations gerenciadas.	6 de fevereiro de 2024
Novo tópico sobre como encerrar contas de gerenciamento	Foram adicionados links para considerações e etapas detalhadas que explicam como fechar uma conta de gerenciamento.	1.º 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 AWSOrganizations ReadOnlyAccess atualizadas AWSOrganizations FullAccess 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 AWSOrganizations FullAccess gerenciada	A política gerenciada foi atualizada para permitir a criação de uma organizaç ão adicionando a permissão requerida para criar a função vinculada ao serviço de que uma nova organização precisa.	24 de agosto de 2022
Organizations fecham a capacidade da conta a partir do AWS Organizations console	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 alternati vos com o console do AWS Organizations	O Organizations agora oferece a capacidade de atualizar contatos alternativos para contas em sua organização usando o AWS Organizat ions console. Anuncie novos recursos e pontos para a Referência de gerenciamento de contas para obter instruçõe s.	8 de fevereiro de 2022

Atualizações de política gerenciada pelo Organizations: atualização em uma política existente	As políticas foram AWSOrganizations ReadOnlyAccess atualizadas AWSOrganizations FullAccess 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 AWS Organizations para garantir que seu gráfico de comportamento de detetive forneça visibilidade da atividade de todas as contas da sua organização.	16 de dezembro de 2021

A integração do Organizations AWS Config agora oferece suporte à agregação de dados multicontas e multirregionais.	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
A integração da Organizations com AWS Firewall Manager agora 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 AWS Backup contínuos com as políticas de backup da sua organização.	10 de março de 2021
A integração da Organizations com AWS CloudFormation StackSets agora 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 organização.	18 de fevereiro de 2021

Continuar convidando contas enquanto você habilita todos os recursos	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 AWS Organizations	AWS introduziu uma nova versão do AWS console. Toda a documentação foi atualizada para refletir a nova maneira de executar as tarefas.	21 de janeiro de 2021
O Organizations agora oferece suporte à integração com AWS Marketplace	Agora você pode AWS Marketplace compartilhar mais facilmente suas licenças de software em todas as contas da 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 administr ador 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	Ao usar políticas de backup para fazer backup dos recursos em sua organização, agora você pode armazenar cópias do seu backup Contas da AWS em outras partes da organização.	18 de novembro de 2020
Regiões da AWS na China, agora o suporte AWS Resource Access Manager é um serviço confiável da Organizations	Agora você pode usar AWS RAM recursos que se integram ao Organizations como um serviço confiável ao usar o Organizations e AWS RAM na China.	18 de novembro de 2020
O Organizations agora oferece suporte à integração com 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	AWS Organizations alterou o nome da “conta principal ” 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 recomendadas para o AWS Organizations. 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

As políticas de backup da Organization agora oferecem suporte a backups consistentes com aplicativos em EC2 instâncias do Windows 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 suporta tag-on-create e controla o 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
Adicionado AWS Health como um serviço confiável	Você pode agregar AWS Health eventos em todas as contas da 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 AWS IA podem armazenar e usar o conteúdo do cliente processado por esses serviços (conteúdo de IA) para o desenvolvimento e a melhoria contínua dos serviços e AWS tecnologias de IA.	8 de julho de 2020
Políticas de backup adicionadas e integração com 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 toda a sua organização Contas da AWS no Systems Manager Explorer.	26 de novembro de 2019
leis: PrincipalOrgPaths	A nova chave de condição global verifica o AWS Organizations caminho do usuário do IAM, da função do IAM ou do usuário Conta da AWS raiz que está fazendo a solicitação.	20 de novembro de 2019
Integração com AWS Config regras	Você pode usar operações de AWS Config API para gerenciar AWS Config regras Contas da AWS em toda a 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 a AWS Control Tower	AWS O Control Tower foi adicionado como um serviço que pode funcionar com as contas da sua organização.	24 de junho de 2019

Integração com AWS Identity and Access Management	O IAM fornece os dados do último acesso do serviço para as entidades da sua organizaç ão (a raiz da organização e as contas). OUs Você pode usar esses dados para restringir o acesso somente ao Serviços da AWS que você precisa.	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
Recursos, condições e o `NotAction` elemento nas políticas de controle de serviços (SCPs)	Agora você pode especific ar recursos, condições e o `NotAction` elemento SCPs para negar o acesso entre contas em sua organização ou unidade organizacional (OU).	25 de março de 2019
Novos serviços para acesso confiável	AWS License Manager e Service Catalog adicionados como serviços que podem funcionar com as contas em sua organização.	21 de dezembro de 2018
Novos serviços para acesso confiável	AWS CloudTrail e AWS RAM adicionados como serviços que podem funcionar com as contas em sua organização.	4 de dezembro de 2018
Novo serviço para acesso confiável	AWS Directory Service 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 notifications	`CreateAccount` as notificações são publicadas nos CloudTrail registros da conta de gerenciamento.	28 de junho de 2018
Novo serviço para acesso confiável	AWS Artifact adicionado como um serviço que pode funcionar com as contas em sua organização.	20 de junho de 2018
Novos serviços para acesso confiável	AWS Config e AWS Firewall Manager adicionados como serviços que podem funcionar com as contas em sua organização.	18 de abril de 2018
Acesso ao serviço confiável	Agora você pode ativar ou desativar o acesso Serviços da AWS para selecionar trabalhar nas contas da 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	Agora você pode remover contas que foram criadas internamente AWS Organizations sem entrar em contato AWS Support.	19 de dezembro de 2017

Suporte adicionado para novos serviços AWS IAM Identity Center	AWS Organizations agora oferece suporte à integração com AWS IAM Identity Center (IAM Identity Center).	7 de dezembro de 2017
AWS adicionou uma função vinculada ao serviço a todas as contas da organização	Uma função vinculada ao serviço chamada `AWSServiceRoleForOrganizations` é adicionada a todas as contas em uma organização para permitir a integração entre outras AWS Organizations . 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 AWS Organizations documentação que acompanhou o lançamento do novo serviço.	17 de fevereiro de 2017

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.