



Guia do administrador

Cadeia de Suprimentos AWS



Cadeia de Suprimentos AWS: Guia do administrador

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

O que é Cadeia de Suprimentos AWS?	1
Navegadores compatíveis	1
Idiomas compatíveis	2
.....	2
Configurando uma AWS conta	3
Inscreva-se para um Conta da AWS	3
Criar um usuário com acesso administrativo	3
Pré-requisitos para usar Cadeia de Suprimentos AWS	6
Começando com Cadeia de Suprimentos AWS	7
Etapa 1: atribuir um perfil de usuário do IAM Identity Center	7
Etapa 2: Criar uma instância	8
Use a configuração padrão	9
Use a configuração avançada	11
Etapa 3: escolha o proprietário do Cadeia de Suprimentos AWS aplicativo	17
Faça login no aplicativo Cadeia de Suprimentos AWS da web	19
Usando o Cadeia de Suprimentos AWS	20
Usando o Cadeia de Suprimentos AWS console	20
Atualizando seu perfil	24
Atualizando o perfil da sua conta	25
Atualizando o perfil da sua organização	25
Gerenciando funções de permissão do usuário	25
Adição de usuários	26
Atualização de permissões de usuários	27
Exclusão de usuários	27
Criação de funções de permissão de usuário personalizadas	28
Excluir uma instância	29
Segurança	30
Proteção de dados	31
Dados com que o Cadeia de Suprimentos AWS lida	32
Preferência de exclusão	32
Criptografia em repouso	32
Criptografia em trânsito	33
Gerenciamento de chaves	33
Privacidade do tráfego entre redes	33

Como Cadeia de Suprimentos AWS usa subsídios em AWS KMS	33
AWS PrivateLink	37
Considerações	37
Como criar um endpoint de interface	38
Criar uma política de endpoint	38
IAM	39
Público	39
Autenticar com identidades	40
Gerenciar o acesso usando políticas	44
Como Cadeia de Suprimentos AWS funciona com o IAM	47
Exemplos de políticas baseadas em identidade	52
Solução de problemas	54
AWS políticas gerenciadas	56
AWSSupplyChainFederationAdminAccess	57
Atualizações da política	58
Validação de conformidade	59
Resiliência	60
Registro e monitoramento da cadeia AWS de suprimentos	61
Cadeia de Suprimentos AWS eventos de dados em CloudTrail	62
Cadeia de Suprimentos AWS eventos de gerenciamento em CloudTrail	63
Aplicativo web APIs	63
Gerenciando eventos usando EventBridge	69
Cadeia de Suprimentos AWS eventos	70
Enviar eventos do Cadeia de Suprimentos AWS	71
Referência detalhada de eventos	72
Cotas	74
Perguntas frequentes (FAQs)	76
Suporte administrativo	78
Histórico de documentos	79
.....	lxxxii

O que é Cadeia de Suprimentos AWS?

Cadeia de Suprimentos AWS é um aplicativo de gerenciamento da cadeia de suprimentos baseado em nuvem que unifica dados e fornece métodos de previsão baseados em ML para melhorar a previsão de demanda e a visibilidade do estoque, insights acionáveis, colaboração contextual integrada, planejamento de demanda, planejamento de suprimentos, visibilidade de fornecedores de vários níveis e gerenciamento de informações de sustentabilidade. Cadeia de Suprimentos AWS pode se conectar aos seus sistemas existentes de planejamento de recursos corporativos (ERP) e gerenciamento da cadeia de suprimentos e usa ML e IA generativa para transformar e integrar dados diferentes no data lake da cadeia de suprimentos (SCDL). O AWS Supply Chain pode melhorar o gerenciamento de riscos da cadeia de suprimentos sem reformulação de plataforma, taxas de licenciamento antecipadas ou compromissos de longo prazo.

Tópicos

- [Navegadores compatíveis com Cadeia de Suprimentos AWS](#)
- [Idiomas suportados pelo Cadeia de Suprimentos AWS](#)

Navegadores compatíveis com Cadeia de Suprimentos AWS

Antes de trabalhar com o AWS Supply Chain, verifique se seu navegador é compatível usando a tabela a seguir.

Navegador	Versões compatíveis
Google Chrome	Últimas três versões.
Mozilla Firefox ESR	As versões são suportadas até a end-of-lifedata do Firefox. Para obter detalhes, consulte o Calendário de lançamentos do Firefox ESR .
Mozilla Firefox	Últimas três versões.
Microsoft Edge e Edge Chromium	Versão 84 e superiores.
Safari	Safari 10 ou posterior para macOS.

Idiomas suportados pelo Cadeia de Suprimentos AWS

Cadeia de Suprimentos AWS suporta os seguintes idiomas:

- Inglês (EUA)
- Inglês (Reino Unido)
- Alemão
- Espanhol
- Francês
- Italiano
- Português
- Chinês (simplificado)
- Chinês (tradicional)
- Japonês
- Coreano

Configurando uma AWS conta

Use esta seção para criar uma AWS conta e criar um usuário do IAM. Para obter informações sobre as melhores práticas para criar uma AWS conta, consulte [Estabelecendo seu AWS ambiente de melhores práticas](#).

Tópicos

- [Inscreva-se para um Conta da AWS](#)
- [Criar um usuário com acesso administrativo](#)

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 ligação ou mensagem de texto e inserir um código de verificação no teclado do telefone.

Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWS é 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 Console](#) como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

Para obter ajuda 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 .

Pré-requisitos para usar Cadeia de Suprimentos AWS

Antes de criar uma Cadeia de Suprimentos AWS instância, certifique-se de concluir as seguintes etapas:

- Você tem um Conta da AWS. Para criar um Conta da AWS, consulte [Configurando uma AWS conta](#).
- Certifique-se de que o IAM Identity Center esteja ativado. Para ativar o IAM Identity Center, consulte [Habilitar o IAM Identity Center](#).
- Você tem as permissões administrativas necessárias. Para obter mais informações sobre permissões, consulte Configuração avançada.
- Uma instância do IAM Identity Center deve ser ativada na mesma região em que você deseja criar sua Cadeia de Suprimentos AWS instância. Cadeia de Suprimentos AWS só é compatível com as regiões Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Europa (Frankfurt), Ásia-Pacífico (Sydney) e Europa (Irlanda).

Se a Cadeia de Suprimentos AWS instância não estiver na mesma região da Central de Identidades do IAM, [entre em contato conosco](#) para obter mais assistência.

- Você deve ter pelo menos um usuário na instância do IAM Identity Center para designar como Cadeia de Suprimentos AWS administrador. Você pode conectar seu Active Directory ao IAM Identity Center. Para obter mais informações, consulte [Conectar-se a um diretório do Microsoft AD](#).
- Adicione outros usuários que precisem Cadeia de Suprimentos AWS acessar o IAM Identity Center.
- Você precisa AWS Key Management Service (AWS KMS) para criar uma instância. Cadeia de Suprimentos AWS usa isso AWS KMS key para criptografar todos os dados que chegam Cadeia de Suprimentos AWS. Para obter informações sobre AWS KMS chaves, consulte [Criação de chaves](#).

Começando com Cadeia de Suprimentos AWS

Nesta seção, você pode aprender a criar uma Cadeia de Suprimentos AWS instância, conceder funções de permissão de usuário, fazer login no aplicativo Cadeia de Suprimentos AWS web e criar funções de permissão de usuário personalizadas. Um Conta da AWS pode ter até 10 Cadeia de Suprimentos AWS instâncias no estado ativo ou de inicialização.

Tópicos

- [Etapa 1: atribuir um perfil de usuário do IAM Identity Center](#)
- [Etapa 2: Criar uma instância](#)
- [Etapa 3: escolha o proprietário do Cadeia de Suprimentos AWS aplicativo](#)
- [Faça login no aplicativo Cadeia de Suprimentos AWS da web](#)

Etapa 1: atribuir um perfil de usuário do IAM Identity Center

Para criar uma instância e usar o Cadeia de Suprimentos AWS serviço, você precisa conectar um perfil de usuário existente do IAM Identity Center ou criar um novo.

1. Abra o [console de Cadeia de Suprimentos AWS](#). Você também pode pesquisar por "Cadeia de Suprimentos AWS" no principal AWS Management Console.
2. Se necessário, altere a AWS região selecionando Selecionar uma região localizada na parte superior do console. Escolha sua região na lista suspensa.
3. Selecione Criar Cadeia de Suprimentos AWS instância. Uma notificação aparecerá.

Continue with email



We'll check if you have an existing user and help create one if you don't.

AWS Supply Chain

Email address

Continue

4. Insira seu endereço de e-mail e selecione Continuar. O iDC verificará se o e-mail corresponde a um usuário existente.
5. Execute um destes procedimentos:
 - Se o iDC corresponder ao endereço de e-mail de um usuário, selecione Conectar sua fonte de identidade e integre sua equipe.

 Note

Isso pode ser usado se sua organização tiver uma instância de IDC estabelecida para Cadeia de Suprimentos AWS a qual você gostaria de usar.

- Se o iDC não encontrar uma correspondência com um usuário existente, a notificação Criar um novo usuário será exibida. Prossiga para a próxima etapa.
6. Na notificação, digite o seguinte e selecione Continuar:
 - Endereço de e-mail
 - Nome
 - Sobrenome

O iDC cria o usuário automaticamente e o adiciona como Cadeia de Suprimentos AWS administrador.

7. Execute um destes procedimentos:
 - Para criar uma instância usando a configuração padrão, selecione Criar. Consulte [the section called “Use a configuração padrão”](#).
 - Para criar uma instância usando uma configuração personalizada, selecione Editar na configuração avançada. Consulte [the section called “Use a configuração avançada”](#).

Etapa 2: Criar uma instância

A criação de uma instância Cadeia de Suprimentos AWS estabelece um ambiente dedicado para gerenciamento e análise da cadeia de suprimentos. Para configurar uma instância, você configura detalhes básicos, estabelece configurações e define as permissões iniciais de acesso do usuário.

Note

Somente o AWS Management Console administrador pode criar uma instância. O AWS Management Console administrador que cria a Cadeia de Suprimentos AWS instância deve ter todas as permissões listadas abaixo [Usando o Cadeia de Suprimentos AWS](#). Esse administrador deve convidar um usuário do IAM como Cadeia de Suprimentos AWS administrador para gerenciar Cadeia de Suprimentos AWS.

Você cria uma instância usando um dos dois métodos, configuração padrão ou configuração avançada. A configuração padrão usa um processo automatizado que cria sua instância rapidamente usando parâmetros predefinidos. A configuração avançada permite que você personalize sua instância definindo seus próprios parâmetros.

Tópicos

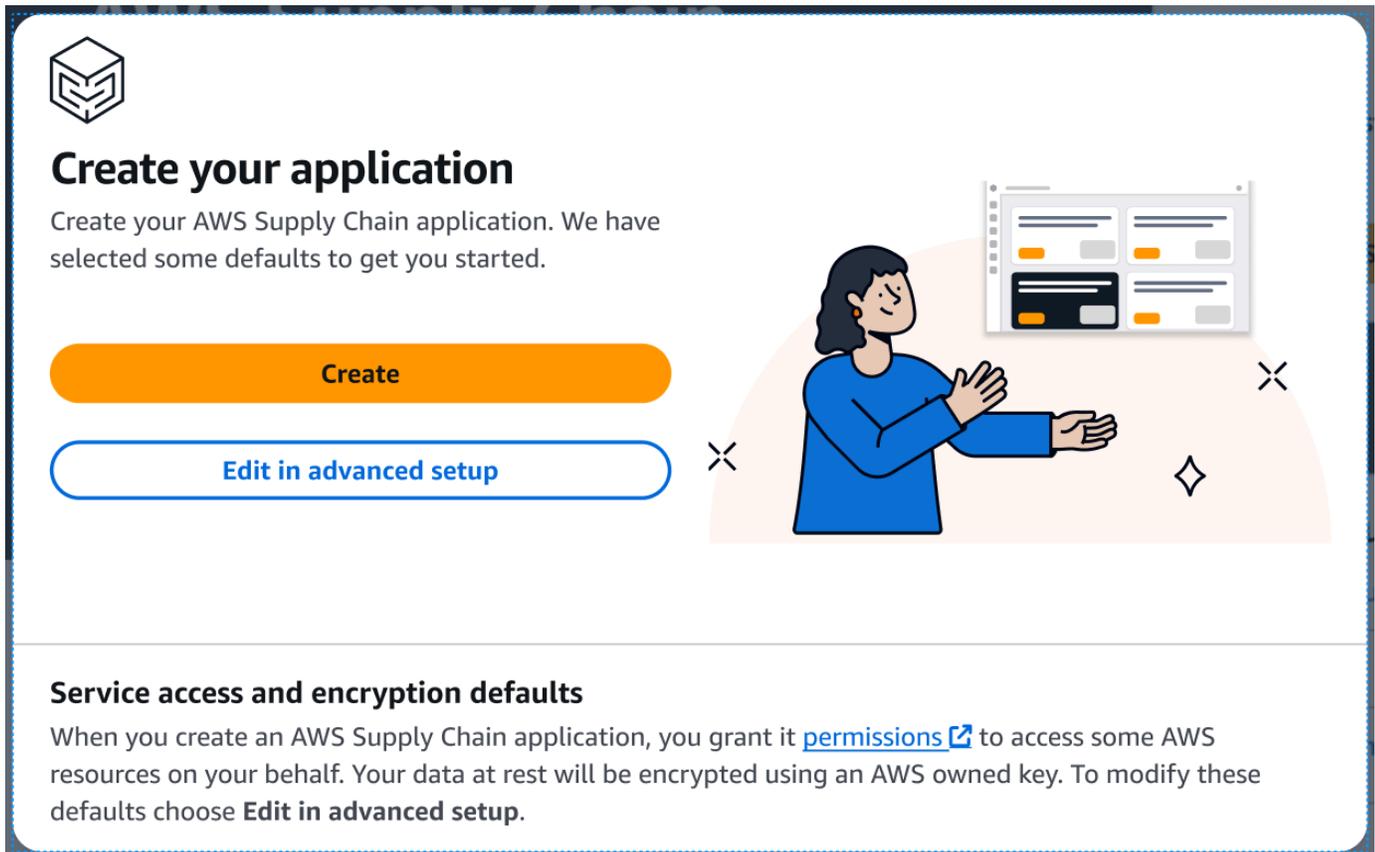
- [Use a configuração padrão](#)
- [Use a configuração avançada](#)

Use a configuração padrão

A configuração padrão cria sua Cadeia de Suprimentos AWS instância usando as configurações padrão de segurança e criptografia. As instâncias operam em regiões AWS geográficas. Para obter mais informações sobre regiões, consulte [Regiões e endpoints](#) no Guia do usuário do IAM e [Endpoints regionais](#) no. Referência geral da AWS

Para criar uma Cadeia de Suprimentos AWS instância usando uma configuração padrão de parâmetros predefinidos, siga estas etapas.

1. Escolha Criar.





Create your application

Create your AWS Supply Chain application. We have selected some defaults to get you started.

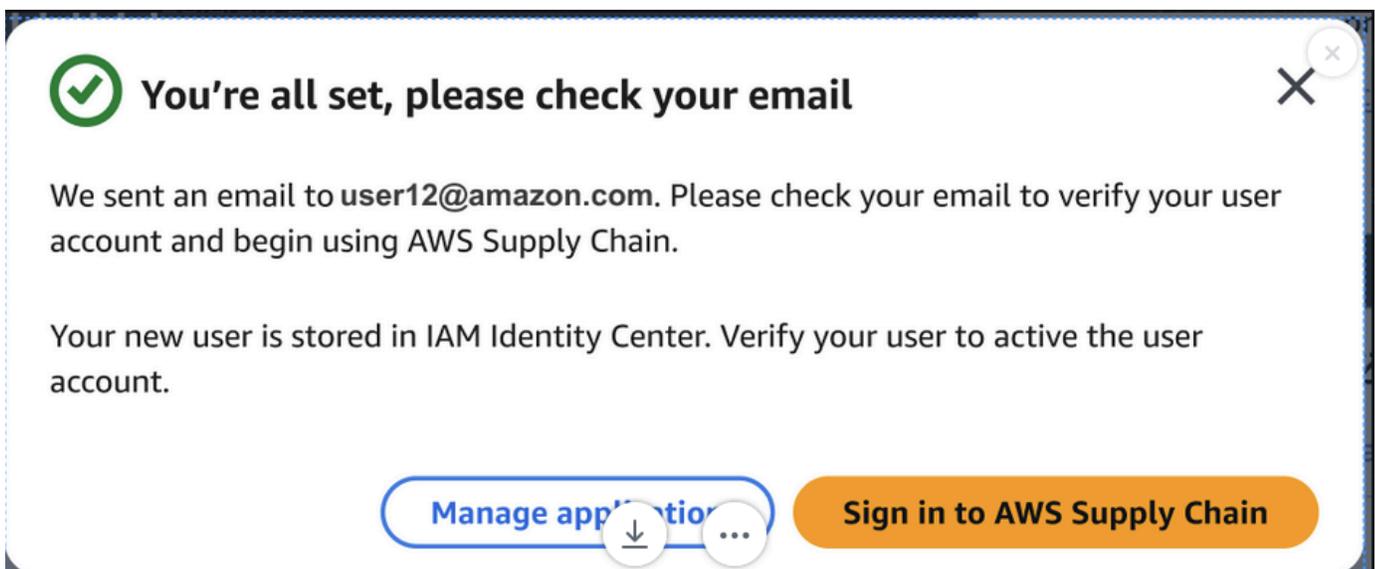
Create

Edit in advanced setup

Service access and encryption defaults

When you create an AWS Supply Chain application, you grant it [permissions](#) to access some AWS resources on your behalf. Your data at rest will be encrypted using an AWS owned key. To modify these defaults choose **Edit in advanced setup**.

Uma confirmação aparecerá.



 **You're all set, please check your email** 

We sent an email to `user12@amazon.com`. Please check your email to verify your user account and begin using AWS Supply Chain.

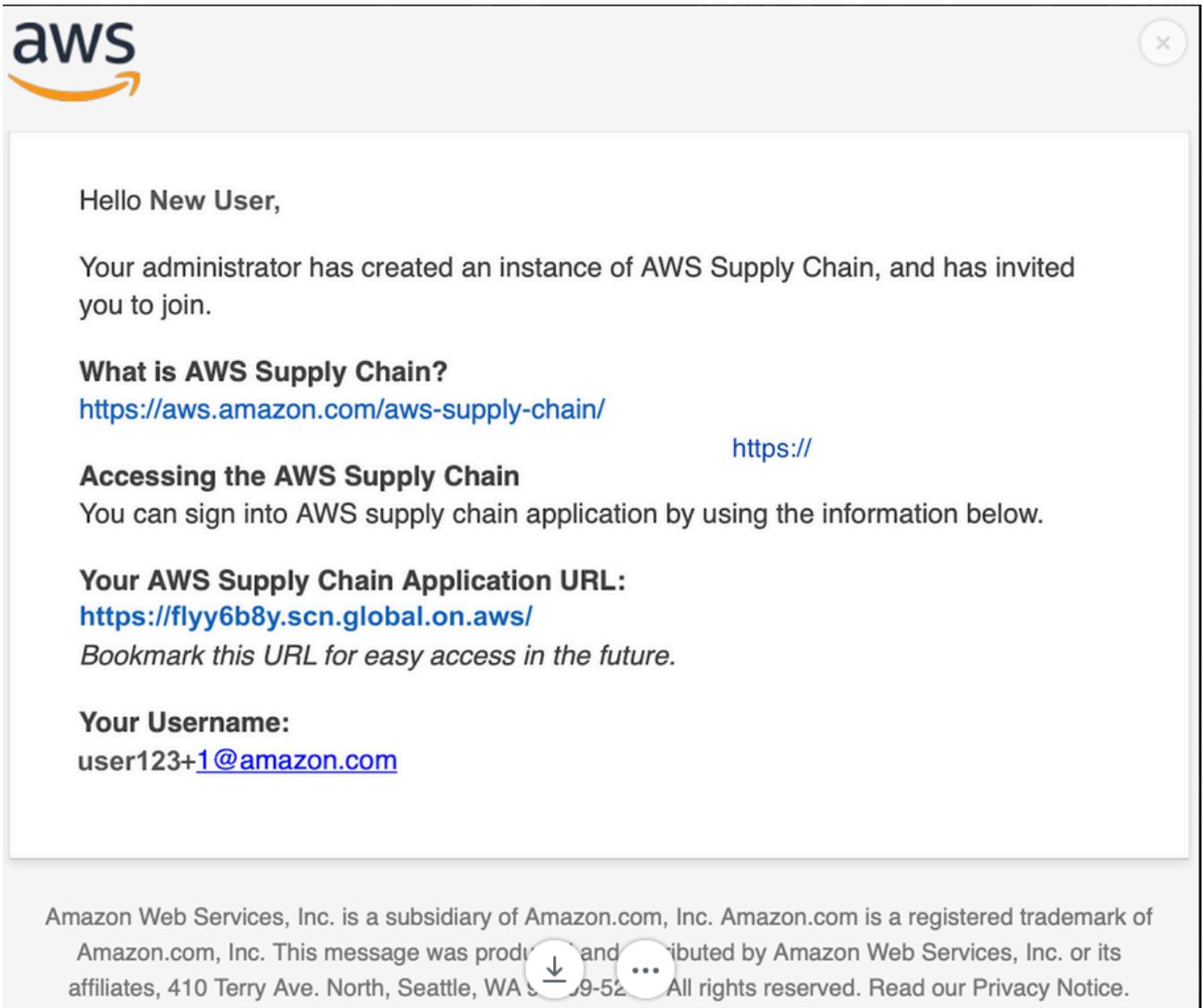
Your new user is stored in IAM Identity Center. Verify your user to active the user account.

Manage application  

Sign in to AWS Supply Chain

2. Verifique seu e-mail para saber o seguinte:

- Um e-mail da equipe do iDC.
- Um e-mail da equipe de gerenciamento de identidade.



3. Depois de receber o e-mail de convite, faça login em Cadeia de Suprimentos AWS. Veja [the section called “Faça login no aplicativo Cadeia de Suprimentos AWS da web”](#).

Use a configuração avançada

A configuração avançada permite que você personalize sua instância definindo seus próprios parâmetros. Para criar uma Cadeia de Suprimentos AWS instância usando uma configuração avançada de parâmetros predefinidos, siga estas etapas.

1. Selecione Editar na configuração avançada.



Create your application

Create your AWS Supply Chain application. We have selected some defaults to get you started.

Create

Edit in advanced setup



Service access and encryption defaults

When you create an AWS Supply Chain application, you grant it [permissions](#) to access some AWS resources on your behalf. Your data at rest will be encrypted using an AWS owned key. To modify these defaults choose **Edit in advanced setup**.

A página de propriedades da instância será exibida.

The screenshot shows the 'Specify instance details' page in the AWS console. It is divided into three main sections:

- Instance properties**: Includes a dropdown for 'AWS Region' (currently set to 'Europe (Ireland) eu-west-1'), a text input for 'Enter an instance name' (with a note: '1 to 62 characters including spaces, underscores, and dashes.'), and a text area for 'Enter a description - optional' (with a note: '256 characters max.').
- AWS KMS Key - Optional**: Includes a search input for 'Choose an AWS KMS Key' (with a placeholder: 'Choose an AWS KMS key or enter an ARN') and a 'Create' button.
- Instance tags - optional**: The top of this section is visible, with a note: 'A tag is a label that you assign to an AWS resource (such as an instance). Each tag consists of a key and an optional value. You can use tags to identify your instances, for example.'

2. Insira o seguinte na página de propriedades da instância:

- Nome — insira um nome de instância.
- Descrição — Insira uma descrição da sua Cadeia de Suprimentos AWS instância (por exemplo, instância de produção, instância de teste etc.).
- Chave do AWS KMS (opcional) — Você pode escolher usar a AWS KMS chave padrão (recomendada) ou fornecer sua própria AWS KMS chave. Consulte [the section called “Usando uma AWS KMS chave personalizada”](#) para obter mais informações.
- Tags de instância — Você pode adicionar tags à sua instância que podem ser usadas para identificação. Por exemplo, você pode adicionar uma tag para definir o tipo de instância que você está criando (por exemplo, produção, teste, UAT etc.).

Note

Se você planeja usar uma conexão de dados S/4 Hana, certifique-se de que a AWS KMS chave que você forneceu tenha a `aws-supply-chain-access` tag com um valor associado de `true`

3. Selecione Criar instância.
4. (Opcional) Depois que sua Cadeia de Suprimentos AWS instância for criada e se você optar por usar sua própria AWS KMS chave em AWS KMS Chave, atualize sua política do KMS para permitir o acesso Cadeia de Suprimentos AWS à sua AWS KMS chave.

 Note

YourInstanceID substitua *YourAccountNumber* e por sua Conta da AWS ID de Cadeia de Suprimentos AWS instância.

```
{
  "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::YourAccountNumber:role/service-role/scn-instance-
role-YourInstanceID"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*"
}
```

Usando uma AWS KMS chave personalizada

Você pode usar sua própria AWS KMS chave ao criar instâncias. Se você quiser gerenciar sua própria chave, mas não quiser usar uma chave existente, você pode criar uma nova chave.

 Note

Usar uma AWS chave própria é a configuração padrão recomendada para Cadeia de Suprimentos AWS instâncias.

Usando uma AWS KMS chave existente

1. Escolha Personalizar configurações de criptografia.
2. Vá para Escolher uma AWS KMS chave.
3. Insira sua chave no campo fornecido.
4. Selecione Atualizar.

Criando uma AWS KMS chave

1. Escolha Criar.
2. Siga as etapas em [Criar uma chave KMS](#).
3. Atualize a nova chave com as seguintes permissões.
 - Defina as principais permissões administrativas: deixe desmarcado
 - Defina as permissões de uso da chave: deixe desmarcada
 - Atualize a política de chaves: edite a política de chaves e substitua-a por:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::YourAccountNumber:root"
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow access through SecretManager for all principals in the
account that are authorized to use SecretManager",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
```

```

        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "secretsmanager.Region.amazonaws.com",
            "kms:CallerAccount": "YourAccountNumber"
        }
    }
},
{
    "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
    "Effect": "Allow",
    "Principal": {
        "Service": "scn.Region.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:RetireGrant"
    ],
    "Resource": "*"
}
]
}

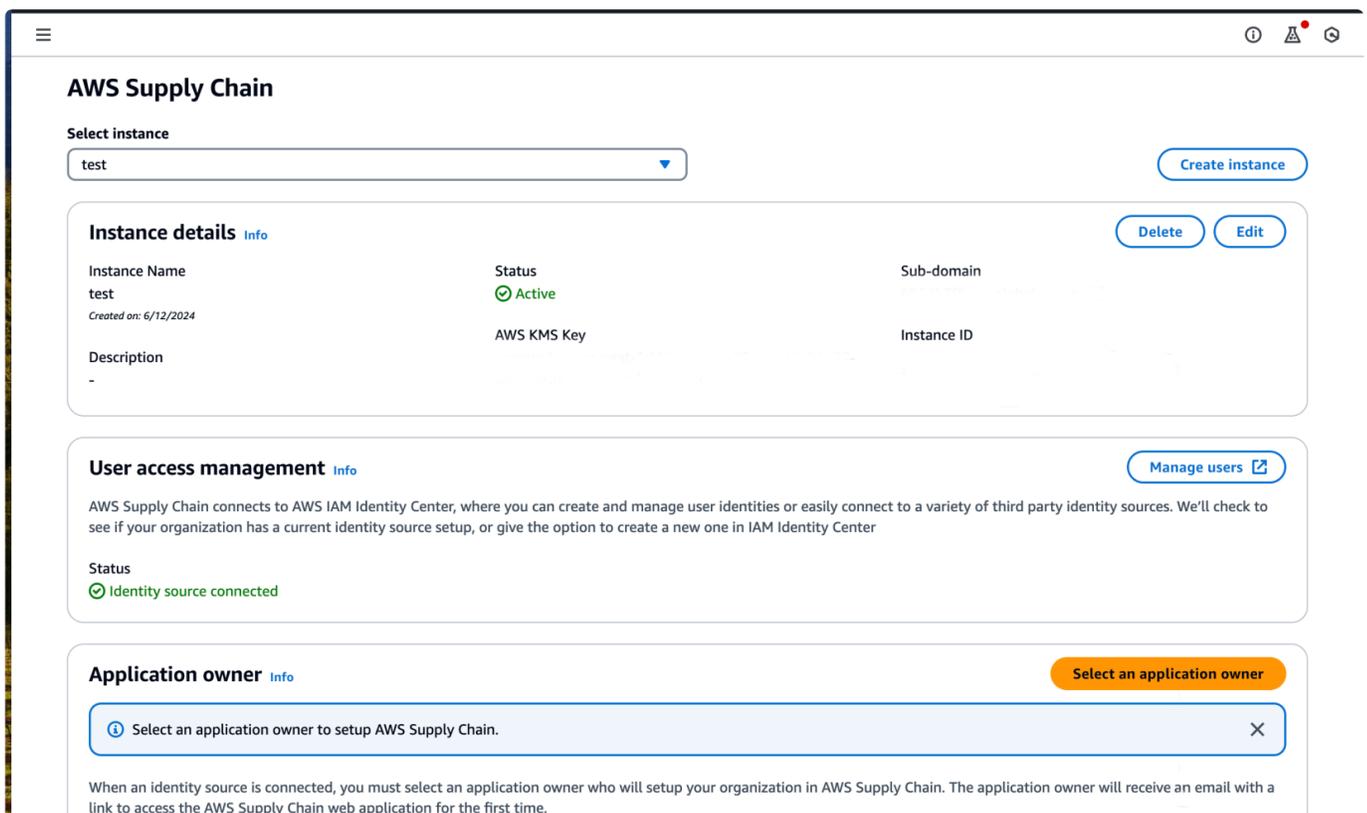
```

Etapa 3: escolha o proprietário do Cadeia de Suprimentos AWS aplicativo

Como administrador AWS do console, você escolhe o proprietário do Cadeia de Suprimentos AWS aplicativo para gerenciar o acesso ao aplicativo Cadeia de Suprimentos AWS web. O proprietário do aplicativo Cadeia de Suprimentos AWS pode adicionar ou remover funções de permissão do usuário no aplicativo web Cadeia de Suprimentos AWS .

Depois que a instância for criada e uma fonte de identidade estiver conectada, siga estas etapas para escolher o proprietário do Cadeia de Suprimentos AWS aplicativo.

1. Abra o painel Cadeia de Suprimentos AWS do console.
2. Vá para Selecionar proprietário do aplicativo e selecione um usuário para ser proprietário do Cadeia de Suprimentos AWS aplicativo. Os resultados da pesquisa mostram somente usuários que correspondem aos critérios de pesquisa.

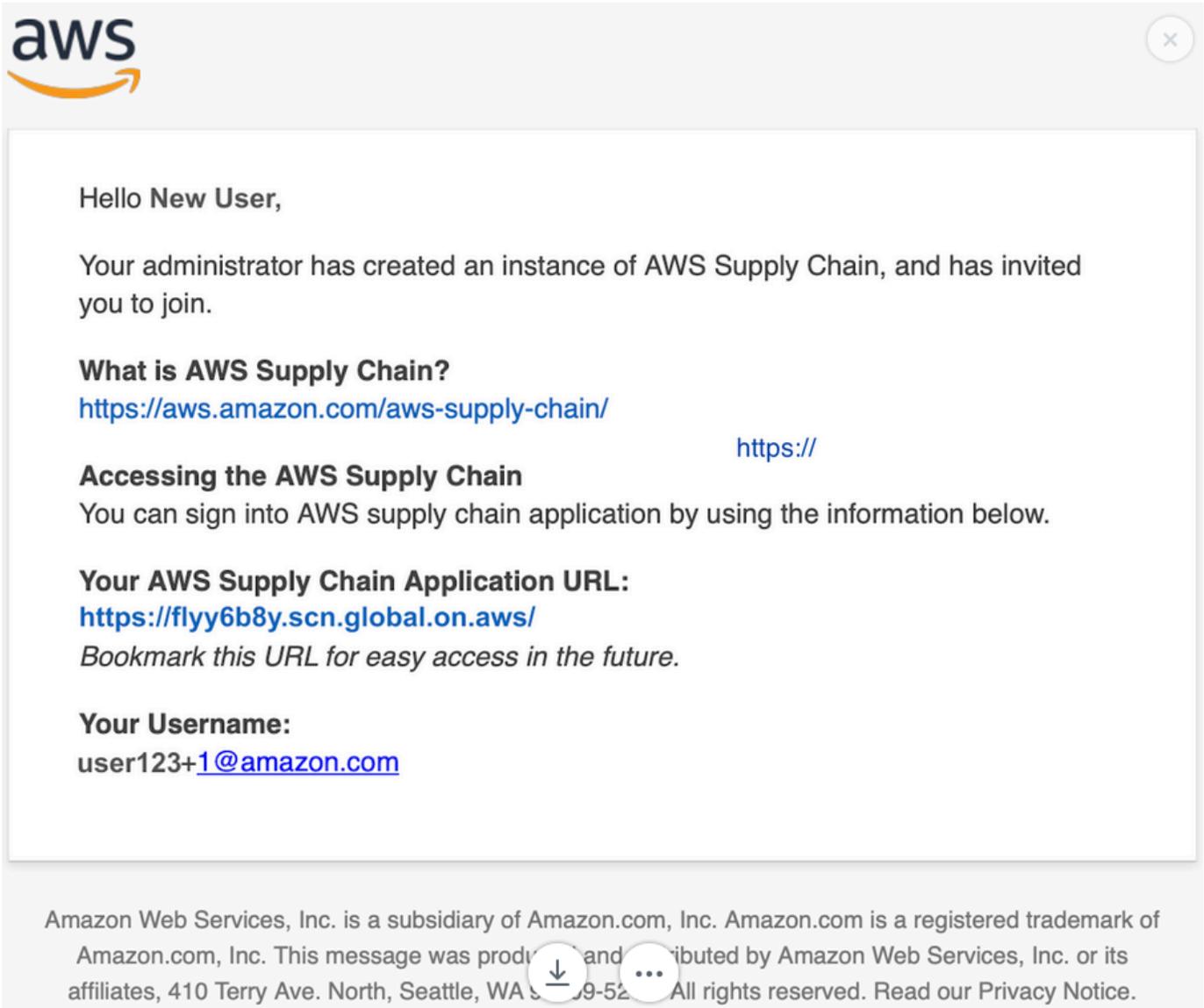


3. (Opcional) Escolha Ir para o IAM Identity Center para adicionar mais usuários. Para obter mais informações sobre a adição de usuários, consulte [Gerenciar sua fonte de identidade](#) no Guia do usuário do AWS IAM Identity Center e, para obter mais informações sobre funções de permissão de usuário, consulte [Funções de permissão de usuário](#).

Note

Você só pode adicionar um usuário por vez a partir do Cadeia de Suprimentos AWS console. Você não pode adicionar um grupo como proprietário do aplicativo no Cadeia de Suprimentos AWS.

- Escolha Enviar convite. Um e-mail é enviado para o administrador do aplicativo web. Depois que o administrador do aplicativo web receber o e-mail de convite, ele poderá selecionar o URL do aplicativo e fazer login no Cadeia de Suprimentos AWS.



No painel do Cadeia de Suprimentos AWS console, você verá o usuário listado em Proprietário do aplicativo.

Escolha Gerenciar na cadeia de suprimentos da AWS para adicionar e remover usuários no aplicativo Cadeia de Suprimentos AWS web

Faça login no aplicativo Cadeia de Suprimentos AWS da web

Como Cadeia de Suprimentos AWS administrador, você deve ter recebido um convite por e-mail para o aplicativo Cadeia de Suprimentos AWS web.

1. Você pode escolher o link no e-mail ou no painel do console do Cadeia de Suprimentos AWS , em Subdomínio, escolha URL da web.

A página de login do aplicativo web Cadeia de Suprimentos AWS é exibida.

2. Insira as credenciais de usuário do AWS IAM Identity Center e escolha Entrar.

Note

Você só precisará preencher os perfis de sua conta e organização quando fizer login pela primeira vez.

3. Na página Complete seu perfil, insira seu Cargo e fuso horário. Escolha Próximo.
4. Na página Vamos adicionar as informações da sua organização, insira o nome da organização e escolha a localização da sede. Opcionalmente, é possível adicionar o logotipo da empresa. Escolha Próximo.
5. Na página Configurar seus colegas de equipe em Cadeia de Suprimentos AWS, selecione os usuários que você deseja que tenham acesso ao aplicativo web Cadeia de Suprimentos AWS . Escolha Invite Users. Para obter informações sobre as funções de permissão Cadeia de Suprimentos AWS do usuário, consulte [Gerenciando funções de permissão do usuário](#).
6. Se quiser adicionar usuários posteriormente, você pode escolher Ignorar por enquanto.

A página de integração completa é exibida.
7. Cada usuário que você adicionou recebe uma mensagem de e-mail com um link que vai para Cadeia de Suprimentos AWS, ou você pode escolher Copiar link e enviar o link para os usuários.
8. Escolha Continuar na página inicial para ver o painel do Cadeia de Suprimentos AWS .

Usando o Cadeia de Suprimentos AWS

Cadeia de Suprimentos AWS é um aplicativo baseado em nuvem que ajuda você a obter visibilidade da sua rede de cadeia de suprimentos, tomar decisões informadas rapidamente e melhorar a resiliência da cadeia de suprimentos. Usando Cadeia de Suprimentos AWS, você pode conectar fontes de dados diferentes, gerar insights usando aprendizado de máquina e colaborar com equipes internas e parceiros externos. Esta seção o guiará por algumas das funções Cadeia de Suprimentos AWS básicas.

Tópicos

- [Usando o Cadeia de Suprimentos AWS console](#)
- [Atualizando seu perfil](#)
- [Gerenciando funções de permissão do usuário](#)
- [Excluir uma instância](#)

Usando o Cadeia de Suprimentos AWS console

Usar o console é a maneira mais fácil de gerenciar seus recursos e configurações de serviço. O console fornece uma interface intuitiva baseada na Web, na qual você pode visualizar, criar, modificar e monitorar seus recursos. Esta seção mostra como acessar e navegar no console para realizar tarefas comuns de gerenciamento.

Note

Se sua AWS conta for uma conta membro de uma AWS organização e incluir uma Política de Controle de Serviços (SCP), certifique-se de que o SCP da organização conceda as seguintes permissões à conta do membro. Se as permissões a seguir não estiverem incluídas na política de SCP da organização, a criação da Cadeia de Suprimentos AWS instância falhará.

Para acessar o Cadeia de Suprimentos AWS console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os Cadeia de Suprimentos AWS recursos 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.

As permissões a seguir são necessárias pelo administrador do console para criar e atualizar instâncias do Cadeia de Suprimentos AWS com sucesso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "scn:*",
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutBucketOwnershipControls",
        "s3:PutBucketNotification",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketLogging",
        "s3:PutBucketTagging"
      ],
      "Resource": "arn:aws:s3:::aws-supply-chain-*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "cloudtrail:CreateTrail",
        "cloudtrail:PutEventSelectors",
        "cloudtrail:GetEventSelectors",
```

```
"cloudtrail:StartLogging"
],
"Resource": "*",
"Effect": "Allow"
},
{
"Action": [
"events:DescribeRule",
"events:PutRule",
"events:PutTargets"
],
"Resource": "*",
"Effect": "Allow"
},
{
"Action": [
"chime:CreateAppInstance",
"chime>DeleteAppInstance",
"chime:PutAppInstanceRetentionSettings",
"chime:TagResource"
],
"Resource": "*",
"Effect": "Allow"
},
{
"Action": [
"cloudwatch:PutMetricData",
"cloudwatch:Describe*",
"cloudwatch:Get*",
"cloudwatch:List*"
],
"Resource": "*",
"Effect": "Allow"
},
{
"Action": [
"organizations:CreateOrganization",
"organizations:DescribeAccount",
"organizations:DescribeOrganization",
"organizations:EnableAWSServiceAccess",
"organizations:ListDelegatedAdministrators"
],
"Resource": "*",
"Effect": "Allow"
```

```
},
{
  "Action": [
    "kms:CreateGrant",
    "kms:RetireGrant",
    "kms:DescribeKey"
  ],
  "Resource": key_arn,
  "Effect": "Allow"
},
{
  "Action": [
    "kms:ListAliases"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "iam:CreateRole",
    "iam:CreatePolicy",
    "iam:GetRole",
    "iam:PutRolePolicy",
    "iam:AttachRolePolicy",
    "iam:CreateServiceLinkedRole"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "sso:AssociateDirectory",
    "sso:AssociateProfile",
    "sso:CreateApplication",
    "sso:CreateApplicationAssignment",
    "sso:CreateInstance",
    "sso:CreateManagedApplicationInstance",
    "sso>DeleteApplication",
    "sso>DeleteApplicationAssignment",
    "sso>DeleteManagedApplicationInstance",
    "sso:DescribeApplication",
    "sso:DescribeDirectories",
    "sso:DescribeInstance",
    "sso:DescribeRegisteredRegions",
```

```

"sso:DescribeTrusts",
"sso:DisassociateProfile",
"sso:GetManagedApplicationInstance",
"sso:GetPeregrineStatus",
"sso:GetProfile",
"sso:GetSharedSsoConfiguration",
"sso:GetSsoConfiguration",
"sso:GetSSOStatus",
"sso:ListApplicationAssignments",
"sso:ListApplicationTemplates",
"sso:ListDirectoryAssociations",
"sso:ListInstances",
"sso:ListProfileAssociations",
"sso:ListProfiles",
"sso:PutApplicationAuthenticationMethod",
"sso:PutApplicationGrant",
"sso:RegisterRegion",
"sso:SearchDirectoryGroups",
"sso:SearchDirectoryUsers",
"sso:SearchGroups",
"sso:SearchUsers",
"sso:StartPeregrine",
"sso:StartSSO",
"sso:UpdateSsoConfiguration",
"sso-directory:SearchUsers"
],
"Resource": "*",
"Effect": "Allow"
}
]
}

```

key_arn especifica a chave que você gostaria de usar para a Cadeia de Suprimentos AWS instância. Para ver as melhores práticas e restringir o acesso somente às chaves que você gostaria de usar Cadeia de Suprimentos AWS, consulte [Especificação de chaves do KMS nas declarações de política do IAM](#). Para representar todas as chaves KMS, use apenas um caractere curinga (“*”).

Atualizando seu perfil

Você pode atualizar sua conta e o perfil da organização a qualquer momento no aplicativo Cadeia de Suprimentos AWS web.

Atualizando o perfil da sua conta

Para atualizar o perfil da sua conta, siga estas etapas.

1. No painel do aplicativo Cadeia de Suprimentos AWS web, no painel de navegação esquerdo, escolha o ícone Configurações.
2. Escolha Perfil da conta.

A página Perfil da conta é exibida.
3. Atualize as informações do contato, conforme apropriado, e escolha Salvar.

Atualizando o perfil da sua organização

Para atualizar o perfil da organização, siga estas etapas.

1. No painel do aplicativo Cadeia de Suprimentos AWS web, no painel de navegação esquerdo, escolha o ícone Configurações.
2. Escolha Organização e, em seguida, escolha Perfil da organização.

A página Perfil da organização é exibida.
3. Atualize o logotipo da organização ou a localização da sede e escolha Salvar.

Gerenciando funções de permissão do usuário

Como Cadeia de Suprimentos AWS administrador, você pode usar as funções de permissão de usuário padrão ou criar funções de permissão personalizadas. Cadeia de Suprimentos AWS tem as seguintes funções de permissão de usuário padrão:

- Administrador: acesso para criar, visualizar e gerenciar todos os dados e permissões do usuário.
- Analista de dados: acesso para criar, visualizar e gerenciar todas as conexões de dados.
- Gerenciador de inventário: acesso para criar, visualizar e gerenciar Insights.
- Planejador de Demanda — Acesso para criar, visualizar e gerenciar previsões, substituições e publicar planos de demanda.
- Gerenciador de dados de parceiros — Acesso para gerenciar e visualizar parceiros, gerenciar e visualizar solicitações de dados e visualizar dados de sustentabilidade.
- Planejador de suprimentos — Acesso para gerenciar e visualizar planos de suprimentos.

Note

Como Cadeia de Suprimentos AWS administrador, antes de adicionar usuários, observe o seguinte:

- Cada função de permissão de usuário padrão é definida com um conjunto de permissões. Você pode adicionar usuários às funções de permissão de usuário padrão ou criar funções de permissão personalizadas.
- Um usuário só pode ser atribuído a uma função de permissão de usuário.
- Você não pode editar nem excluir funções de permissão de usuário padrão.
- Quando você edita uma função de permissão personalizada que você criou, as permissões de todos os usuários sob a função de permissão personalizada são atualizadas.
- Quando você exclui uma função de permissão personalizada que você criou, todos os usuários sob a função de permissão personalizada perderão acesso Cadeia de Suprimentos AWS a.
- A adição de grupos não é suportada no Cadeia de Suprimentos AWS.

Tópicos

- [Adição de usuários](#)
- [Atualização de permissões de usuários](#)
- [Exclusão de usuários](#)
- [Criação de funções de permissão de usuário personalizadas](#)

Adição de usuários

Como Cadeia de Suprimentos AWS administrador, você pode adicionar usuários para acessar o aplicativo Cadeia de Suprimentos AWS web. Primeiro, os usuários devem ser adicionados ao IAM Identity Center (iDC) e, em seguida, podem ser adicionados Cadeia de Suprimentos AWS. Para obter mais informações sobre como adicionar usuários ao IdC, consulte [Atribuir acesso de usuário](#).

Depois que os usuários forem adicionados ao iDC, siga estas etapas para adicionar um usuário.

1. Escolha o ícone Configurações no Cadeia de Suprimentos AWS painel.
2. Selecione Usuários e permissões.

3. Selecione Usuários, Usuários. A página Gerenciar usuários é exibida.
4. Selecione Adicionar novo usuário. A página Adicionar usuário é exibida.
5. Selecione o usuário no menu suspenso Adicionar usuário (s).
6. Selecione a função do usuário no menu suspenso Selecionar função.
7. Selecione Adicionar.

Atualização de permissões de usuários

Para atualizar a função de permissão do usuário para os Cadeia de Suprimentos AWS usuários atuais, siga estas etapas.

1. No Cadeia de Suprimentos AWS painel, no painel de navegação esquerdo, escolha o ícone Configurações.
2. Escolha Permissões e Criar usuário.

A página Gerenciar usuários é exibida.

3. Na página Gerenciar usuários, selecione o usuário ou grupo para o qual você deseja atualizar a função de permissão do usuário e, no menu suspenso Função de permissões, selecione uma das funções de permissão.

Note

Dependendo das permissões de função que você atribuiu, o painel do Cadeia de Suprimentos AWS é personalizado. Para obter mais informações, consulte [Criação de funções de permissão de usuário personalizadas](#).

4. Escolha Salvar.

Exclusão de usuários

Como Cadeia de Suprimentos AWS administrador, você pode excluir usuários do aplicativo Cadeia de Suprimentos AWS web. Siga estas etapas para excluir a tabela.

1. No Cadeia de Suprimentos AWS painel, no painel de navegação esquerdo, escolha o ícone Configurações.
2. Escolha Permissões e Criar usuário.

A página Gerenciar usuários é exibida.

3. Na página Gerenciar usuários, selecione o usuário que você deseja excluir e escolha o ícone Excluir.

Criação de funções de permissão de usuário personalizadas

Além das funções de permissão de usuário padrão, você pode criar funções de permissão de usuário personalizadas para incluir várias funções de permissão e adicionar locais e produtos específicos. Siga estas etapas para criar novas funções de permissão.

1. No Cadeia de Suprimentos AWS painel, no painel de navegação esquerdo, escolha o ícone Configurações. Escolha Permissões e, em seguida, Funções de permissão.

A página Funções de permissão é exibida.

2. Escolha Criar nova função.
3. Na página Gerenciar função de permissão, em Nome da função, insira um nome.
4. Mova o controle deslizante para selecionar a função de permissão do usuário.
 - Gerenciar — A atribuição de permissões de gerenciamento aos usuários pode adicionar, editar e gerenciar informações.
 - Exibir — A atribuição de permissões de visualização aos usuários só pode visualizar as informações atuais.

5.  Note

Você só pode escolher os produtos e locais em Acesso à localização e Acesso ao produto se sua instância estiver conectada a uma fonte de dados. Por exemplo, você pode criar um usuário administrador personalizado apenas para gerenciar abacates no local de Seattle ou um usuário do Insight apenas para gerenciar os insights sobre abacates no local de Seattle.

Em Acesso à localização, pesquise as regiões enquanto digita na barra de pesquisa e selecione as regiões.

6. Em Acesso ao produto, pesquise os produtos enquanto digita na barra de pesquisa e selecione os produtos.

7. Escolha Salvar.

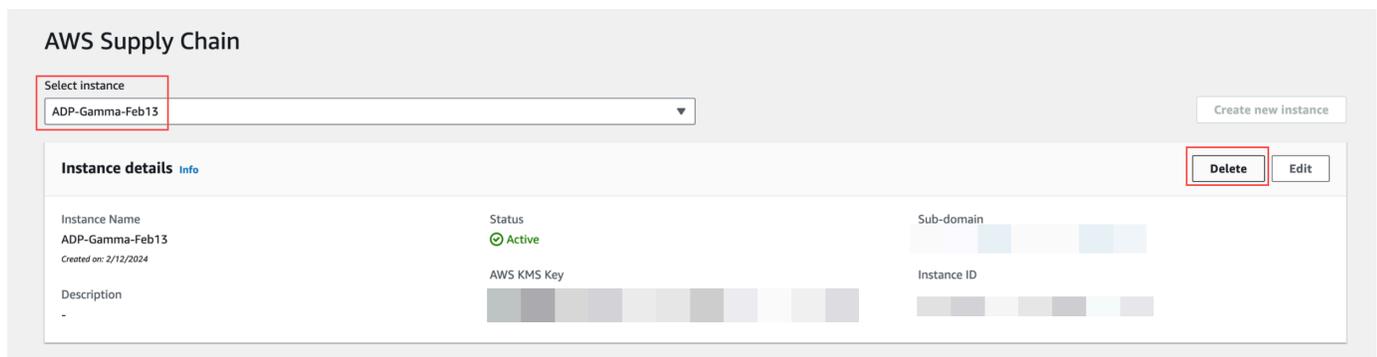
Excluir uma instância

Para excluir uma instância, siga estas etapas.

Note

Quando você exclui uma instância, as informações do bucket do Amazon S3 não são excluídas automaticamente.

1. Abra o Cadeia de Suprimentos AWS console em <https://console.aws.amazon.com/scn/home>.
2. No painel do Cadeia de Suprimentos AWS console, no menu suspenso, selecione a instância que você deseja excluir.



3. Escolha Excluir.
4. Na página Excluir Cadeia de Suprimentos AWS instância, em Confirmação, digite **delete** para confirmar que você deseja excluir a instância.
5. Escolha Excluir. A exclusão da instância começa e, quando a instância for excluída, você verá uma mensagem de confirmação.

Note

Depois que a instância é excluída, as informações relacionadas ao Amazon Q in Cadeia de Suprimentos AWS são excluídas automaticamente.

Segurança em Cadeia de Suprimentos AWS

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

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

- **Segurança da nuvem** — AWS é responsável por proteger a infraestrutura que funciona Serviços da AWS no Nuvem AWS. 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 Cadeia de Suprimentos AWS, consulte [AWS Serviços no escopo do programa de conformidade AWS](#).
- **Segurança na nuvem** — O AWS service (Serviço da AWS) que você usa determina sua responsabilidade. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Cadeia de Suprimentos AWS. Os tópicos a seguir mostram como configurar para atender Cadeia de Suprimentos AWS aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros Serviços da AWS que o ajudem a monitorar e proteger seus Cadeia de Suprimentos AWS recursos.

Tópicos

- [Proteção de dados em Cadeia de Suprimentos AWS](#)
- [Acesso Cadeia de Suprimentos AWS usando um endpoint de interface \(\)AWS PrivateLink](#)
- [IAM para Cadeia de Suprimentos AWS](#)
- [AWS políticas gerenciadas para Cadeia de Suprimentos AWS](#)
- [Validação de conformidade para Cadeia de Suprimentos AWS](#)
- [Resiliência em Cadeia de Suprimentos AWS](#)
- [Registro e monitoramento Cadeia de Suprimentos AWS](#)
- [Gerenciando Cadeia de Suprimentos AWS eventos usando Amazon EventBridge](#)

Proteção de dados em Cadeia de Suprimentos AWS

O modelo de [responsabilidade AWS compartilhada modelo](#) se aplica à proteção de dados em Cadeia de Suprimentos AWS. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as [Data Privacy FAQ](#). Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog [AWS Shared Responsibility Model and RGPD](#) no Blog de segurança da AWS .

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

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como [trabalhar com CloudTrail trilhas](#) no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para obter mais informações sobre os endpoints FIPS disponíveis, consulte [Federal Information Processing Standard \(FIPS\) 140-3](#).

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

livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Dados com que o Cadeia de Suprimentos AWS lida

Para limitar os dados que podem ser acessados por usuários autorizados de uma instância específica da AWS Supply Chain, os dados mantidos na AWS Supply Chain são segregados pelo ID da sua AWS conta e pelo ID da instância do AWS Supply Chain.

AWS A cadeia de suprimentos lida com uma variedade de dados da cadeia de suprimentos, como informações do usuário, informações extraídas do conector de dados e detalhes do inventário.

Preferência de exclusão

Podemos usar e armazenar Seu Conteúdo que é processado por Cadeia de Suprimentos AWS, conforme observado nos [Termos de Serviço da AWS](#). Se você quiser optar por não usar ou armazenar seu conteúdo, você pode criar uma política de exclusão no AWS Organizations. Cadeia de Suprimentos AWS Para obter mais informações sobre como criar uma política de exclusão, consulte exemplos e sintaxe da política de [exclusão de serviços de IA](#).

Criptografia em repouso

Os dados de contato classificados como PII, ou dados que representam o conteúdo do cliente, incluindo o conteúdo usado no Amazon Q ao Cadeia de Suprimentos AWS ser armazenado pelo Cadeia de Suprimentos AWS, são criptografados em repouso (ou seja, antes de serem colocados, armazenados ou salvos em um disco) com uma chave limitada no tempo e específica para a Cadeia de Suprimentos AWS instância.

A criptografia do lado do servidor Amazon S3 é usada para criptografar todos os dados do console e do aplicativo web com uma chave de dados AWS Key Management Service exclusiva para cada conta de cliente. Para obter informações sobre AWS KMS keys, consulte [O que é AWS Key Management Service?](#) no Guia do AWS Key Management Service desenvolvedor.

Note

Cadeia de Suprimentos AWS features Supply Planning and N-Tier Visibility não suporta criptografia data-at-rest com o KMS-CMK fornecido.

Criptografia em trânsito

Os dados, incluindo o conteúdo usado no Amazon Q em Cadeia de Suprimentos AWS troca com a cadeia AWS de suprimentos, são protegidos em trânsito entre o navegador da web do usuário e a cadeia de AWS suprimentos usando criptografia TLS padrão do setor.

Gerenciamento de chaves

Cadeia de Suprimentos AWS suporta parcialmente o KMS-CMK.

Para obter informações sobre como atualizar a chave do AWS KMS Cadeia de Suprimentos AWS, consulte. [Etapa 2: Criar uma instância](#)

Privacidade do tráfego entre redes

Note

Cadeia de Suprimentos AWS não suporta PrivateLink.

Um endpoint de nuvem privada virtual (VPC) para Cadeia de Suprimentos AWS é uma entidade lógica dentro de uma VPC que permite conectividade somente com o. Cadeia de Suprimentos AWS A VPC encaminha as solicitações Cadeia de Suprimentos AWS e as respostas de volta para a VPC. Para obter mais informações, consulte [VPC Endpoints no Guia do usuário](#) da VPC.

Como Cadeia de Suprimentos AWS usa subsídios em AWS KMS

Cadeia de Suprimentos AWS exige uma [concessão](#) para usar sua chave gerenciada pelo cliente.

Cadeia de Suprimentos AWS cria várias concessões usando a AWS KMS chave que é passada durante a CreateInstance operação. Cadeia de Suprimentos AWS cria uma concessão em seu nome enviando [CreateGrant](#) solicitações para AWS KMS. As concessões AWS KMS são usadas para dar Cadeia de Suprimentos AWS acesso à AWS KMS chave em uma conta de cliente.

Note

Cadeia de Suprimentos AWS usa seu próprio mecanismo de autorização. Depois que um usuário é adicionado Cadeia de Suprimentos AWS, você não pode negar a lista do mesmo usuário usando a AWS KMS política.

Cadeia de Suprimentos AWS usa a concessão para o seguinte:

- Para enviar `GenerateDataKey` solicitações AWS KMS para [criptografar](#) os dados armazenados na sua instância.
- Para enviar solicitações do `Decrypt` para AWS KMS ler seus dados criptografados associados à instância.
- Para adicionar `DescribeKey`, `CreateGrant`, e `RetireGrant` permissões para manter seus dados protegidos ao enviá-los para outros AWS serviços, como o Amazon Forecast.

É possível revogar o acesso à concessão, ou remover o acesso do serviço à chave gerenciada pelo cliente a qualquer momento. Se você fizer isso, Cadeia de Suprimentos AWS não conseguirá acessar nenhum dos dados criptografados pela chave gerenciada pelo cliente, o que afeta as operações que dependem desses dados.

Monitorando sua criptografia para Cadeia de Suprimentos AWS

Os exemplos a seguir são AWS CloudTrail eventos para `Encrypt`, `GenerateDataKey`, e `Decrypt` para monitorar operações KMS chamadas por Cadeia de Suprimentos AWS para acessar dados criptografados pela chave gerenciada pelo cliente:

Encrypt

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "scn.amazonaws.com"
  },
  "eventTime": "2024-03-06T22:39:32Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Encrypt",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "172.12.34.56"
  "userAgent": "Example/Desktop/1.0 (V1; OS)",
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "keyId": "arn:aws:kms:us-east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
  },
}
```

```

"responseElements": null,
"requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
"eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
"readOnly": true,
"resources": [
  {
    "accountId": account ID,
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "112233445566",
"sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
"eventCategory": "Management"
}

```

GenerateDataKey

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "scn.amazonaws.com"
  },
  "eventTime": "2024-03-06T22:39:32Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "172.12.34.56"
  "userAgent": "Example/Desktop/1.0 (V1; OS)",
  "requestParameters": {
    "encryptionContext": {
      "aws:s3:arn": "arn:aws:s3:::test/rawEvent/bf6666c1-111-48aaca-b6b0-
dsadsadsa3432423/noFlowName/scn.data.inboundorder/20240306_223934_536"
    },
    "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
    "keySpec": "AES_222"
  }
}

```

```

},
"responseElements": null,
"requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
"eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
"readOnly": true,
"resources": [
  {
    "accountId": account ID,
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "112233445566",
"sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
"eventCategory": "Management"
}

```

Decrypt

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "scn.amazonaws.com"
  },
  "eventTime": "2024-03-06T22:39:32Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "172.12.34.56"
  "userAgent": "Example/Desktop/1.0 (V1; OS)",
  "requestParameters": {
    "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
  },
  "responseElements": null,
  "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",

```

```
"eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
"readOnly": true,
"resources": [
  {
    "accountId": account ID,
    "type": "AWS::KMS::Key",
    "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "112233445566",
"sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
"eventCategory": "Management"
}
```

Acesso Cadeia de Suprimentos AWS usando um endpoint de interface ()AWS PrivateLink

Você pode usar AWS PrivateLink para criar uma conexão privada entre sua VPC e Cadeia de Suprimentos AWS. Você pode acessar Cadeia de Suprimentos AWS como se estivesse em sua VPC, sem o uso de um gateway de internet, dispositivo NAT, conexão VPN ou conexão. AWS Direct Connect As instâncias na sua VPC não precisam de endereços IP públicos para acessar o Cadeia de Suprimentos AWS.

Estabeleça essa conectividade privada criando um endpoint de interface, habilitado pelo AWS PrivateLink. Criaremos um endpoint de interface de rede em cada sub-rede que você habilitar para o endpoint de interface. Estas são interfaces de rede gerenciadas pelo solicitante que servem como ponto de entrada para o tráfego destinado ao Cadeia de Suprimentos AWS.

Para obter mais informações, consulte [Acesso Serviços da AWS por meio AWS PrivateLink](#) do AWS PrivateLink Guia.

Considerações para Cadeia de Suprimentos AWS

Antes de configurar um endpoint de interface para Cadeia de Suprimentos AWS, consulte [as Considerações](#) no AWS PrivateLink Guia.

Cadeia de Suprimentos AWS suporta fazer chamadas para todas as suas ações de API por meio do endpoint da interface.

Crie um endpoint de interface para Cadeia de Suprimentos AWS

Você pode criar um endpoint de interface para Cadeia de Suprimentos AWS usar o console Amazon VPC ou AWS Command Line Interface o AWS CLI(). Para obter mais informações, consulte [Criar um endpoint de interface](#) no Guia do usuário do AWS PrivateLink .

Crie um endpoint de interface para Cadeia de Suprimentos AWS usar o seguinte nome de serviço:

```
com.amazonaws.region.scn
```

Se você habilitar o DNS privado para o endpoint da interface, poderá fazer solicitações de API a Cadeia de Suprimentos AWS usando seu nome DNS regional padrão. Por exemplo, *scn.region*.amazonaws.com.

Crie uma política de endpoint para seu endpoint de interface.

Uma política de endpoint é um recurso do IAM que você pode anexar ao endpoint de interface. A política de endpoint padrão permite acesso total Cadeia de Suprimentos AWS por meio do endpoint da interface. Para controlar o acesso Cadeia de Suprimentos AWS permitido pela sua VPC, anexe uma política de endpoint personalizada ao endpoint da interface.

Uma política de endpoint especifica as seguintes informações:

- Os diretores que podem realizar ações (Contas da AWS usuários do IAM e funções do IAM)
- As ações que podem ser executadas
- Os recursos nos quais as ações podem ser executadas

Para obter mais informações, consulte [Controlar o acesso aos serviços usando políticas de endpoint](#) no Guia do AWS PrivateLink .

Exemplo: política de VPC endpoint para ações Cadeia de Suprimentos AWS

O exemplo a seguir refere-se a uma política de endpoint personalizada. Quando anexada ao endpoint da sua interface, essa política concede acesso às ações do Cadeia de Suprimentos AWS listadas para todas as entidades principais em todos os recursos.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "scn:action-1",
        "scn:action-2",
        "scn:action-3"
      ],
      "Resource": "*"
    }
  ]
}
```

IAM para Cadeia de Suprimentos AWS

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

Tópicos

- [Público](#)
- [Autenticar com identidades](#)
- [Gerenciar o acesso usando políticas](#)
- [Como Cadeia de Suprimentos AWS funciona com o IAM](#)
- [Exemplos de políticas baseadas em identidade para o Cadeia de Suprimentos AWS](#)
- [Solução de problemas Cadeia de Suprimentos AWS de identidade e acesso](#)

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz Cadeia de Suprimentos AWS.

Usuário do serviço — Se você usar o Cadeia de Suprimentos AWS serviço para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais Cadeia de Suprimentos AWS recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no Cadeia de Suprimentos AWS, consulte [Solução de problemas Cadeia de Suprimentos AWS de identidade e acesso](#).

Administrador de serviços — Se você é responsável pelos Cadeia de Suprimentos AWS recursos da sua empresa, provavelmente tem acesso total Cadeia de Suprimentos AWS a. É seu trabalho determinar quais Cadeia de Suprimentos AWS recursos e recursos seus 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 sua empresa pode usar o IAM com Cadeia de Suprimentos AWS, consulte [Como Cadeia de Suprimentos AWS funciona com o IAM](#).

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar acesso ao Cadeia de Suprimentos AWS. Para ver exemplos de políticas Cadeia de Suprimentos AWS baseadas em identidade que você pode usar no IAM, consulte. [Exemplos de políticas baseadas em identidade para o Cadeia de Suprimentos AWS](#)

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 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 ao armazenamento de chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que 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 várias 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 Cadeia de Suprimentos AWS funciona com o IAM

Antes de usar o IAM para gerenciar o acesso Cadeia de Suprimentos AWS, saiba com quais recursos do IAM estão disponíveis para uso Cadeia de Suprimentos AWS.

Recursos do IAM que você pode usar com Cadeia de Suprimentos AWS

Atributo do IAM	Cadeia de Suprimentos AWS apoio
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Perfis vinculados a serviço	Não

Para ter uma visão de alto nível de como Cadeia de Suprimentos AWS 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 Cadeia de Suprimentos AWS

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 de políticas baseadas em identidade para Cadeia de Suprimentos AWS

Para ver exemplos de políticas Cadeia de Suprimentos AWS baseadas em identidade, consulte [Exemplos de políticas baseadas em identidade para o Cadeia de Suprimentos AWS](#)

Políticas baseadas em recursos dentro Cadeia de Suprimentos AWS

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. 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.

Ações políticas para Cadeia de Suprimentos AWS

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.

As ações de política Cadeia de Suprimentos AWS usam o seguinte prefixo antes da ação:

```
scn
```

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

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

Para ver exemplos de políticas Cadeia de Suprimentos AWS baseadas em identidade, consulte [Exemplos de políticas baseadas em identidade para o Cadeia de Suprimentos AWS](#)

Recursos políticos para Cadeia de Suprimentos AWS

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 exemplos de políticas Cadeia de Suprimentos AWS baseadas em identidade, consulte [Exemplos de políticas baseadas em identidade para o Cadeia de Suprimentos AWS](#)

Chaves de condição de política para Cadeia de Suprimentos AWS

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 exemplos de políticas Cadeia de Suprimentos AWS baseadas em identidade, consulte [Exemplos de políticas baseadas em identidade para o Cadeia de Suprimentos AWS](#)

Usando credenciais temporárias com Cadeia de Suprimentos AWS

Compatível com credenciais temporárias: sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “[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 Cadeia de Suprimentos AWS

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](#).

Funções de serviço para Cadeia de Suprimentos AWS

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

Alterar as permissões de uma função de serviço pode interromper Cadeia de Suprimentos AWS a funcionalidade. Edite as funções de serviço somente quando Cadeia de Suprimentos AWS fornecer orientação para fazer isso.

Funções vinculadas a serviços para Cadeia de Suprimentos AWS

Compatível com perfis vinculados ao serviço: Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um [AWS service \(Serviço da AWS\)](#). O serviço pode 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.

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

Exemplos de políticas baseadas em identidade para o Cadeia de Suprimentos AWS

Por padrão, usuários e funções não têm permissão para criar ou modificar Cadeia de Suprimentos AWS recursos. Eles também não podem executar tarefas usando o Console de Gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) ou uma API da AWS. 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 presumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte [Criação de políticas do IAM](#) no Guia do usuário do IAM.

Tópicos

- [Práticas recomendadas de política](#)

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir Cadeia de Suprimentos AWS recursos 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.

Solução de problemas Cadeia de Suprimentos AWS de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com Cadeia de Suprimentos AWS um IAM.

Tópicos

- [Não estou autorizado a realizar uma ação em Cadeia de Suprimentos AWS](#)
- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero permitir que pessoas fora da minha Conta da AWS acessem meus Cadeia de Suprimentos AWS recursos](#)

Não estou autorizado a realizar uma ação em Cadeia de Suprimentos AWS

Se o AWS Management Console informar que você não está autorizado a executar uma ação, você deverá entrar em contato com o administrador para obter assistência. O administrador é a pessoa que forneceu o seu nome de usuário e senha.

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 `scn:GetWidget` fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:  
  scn: GetWidget on resource: my-example-widget
```

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

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não está autorizado a executar a ação iam:PassRole, as suas políticas devem ser atualizadas para permitir que você passe uma função para o Cadeia de Suprimentos AWS.

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 fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada marymajor tenta utilizar o console para executar uma ação no Cadeia de Suprimentos AWS. 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 Conta da AWS acessem meus Cadeia de Suprimentos AWS recursos

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 é Cadeia de Suprimentos AWS compatível com esses recursos, consulte [Como Cadeia de Suprimentos AWS 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.

AWS políticas gerenciadas para Cadeia de Suprimentos AWS

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

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

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

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

AWS política gerenciada: AWSSupply ChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess fornece aos usuários Cadeia de Suprimentos AWS federados acesso ao Cadeia de Suprimentos AWS aplicativo, incluindo as permissões necessárias para realizar ações dentro do Cadeia de Suprimentos AWS aplicativo. A política fornece permissões administrativas para usuários e grupos do IAM Identity Center e está vinculada a uma função criada Cadeia de Suprimentos AWS por você. Você não deve vincular a AWSSupply ChainFederationAdminAccess política a nenhuma outra entidade do IAM.

Embora essa política forneça todo o acesso Cadeia de Suprimentos AWS por meio das permissões `scn: *`, a Cadeia de Suprimentos AWS função determina suas permissões. A Cadeia de Suprimentos AWS função inclui apenas as permissões necessárias e não tem permissões para o administrador APIs.

Detalhes de permissões

Esta política inclui as seguintes permissões:

- **Chime**— Fornece acesso para criar ou excluir usuários em um Amazon Chime AppInstance; Fornece acesso para gerenciar canais, membros do canal e moderadores; Fornece acesso para enviar mensagens para o canal. As operações do Chime têm como escopo as instâncias do aplicativo marcadas com "SCNInstanceID".
- **AWS IAM Identity Center (AWS SSO)**— Fornece as permissões necessárias para associar e desassociar perfis de usuário, listar associações de perfis, listar atribuições de aplicativos, descrever aplicativos, descrever instâncias e obter a configuração de atribuição de aplicativos no IAM Identity Center.
- **AppFlow** — Fornece acesso para criar, atualizar e excluir perfis de conexão; fornece acesso para criar, atualizar, excluir, iniciar e interromper fluxos; fornece acesso para marcar e desmarcar fluxos e descrever registros de fluxo.
- **Amazon S3** — Fornece acesso para listar todos os buckets. Fornece `GetBucketLocation`, `GetBucketPolicy` `PutObject` `GetObject`, e `ListBucket` acesso aos buckets com o recurso `arn:aws:s3:::*.aws-supply-chain-data`
- **SecretsManager** — Fornece acesso à criação de segredos e à atualização da política secreta.
- **KMS**— Fornece ao AppFlow serviço Amazon o acesso às chaves da lista e ao alias da chave. `DescribeKey` `CreateGrant` Fornece `ListGrants` permissões para chaves KMS marcadas com

chave-valor `aws-suply-chain-access: true`; fornece acesso para criar segredos e atualizar políticas secretas.

As permissões (`kms:ListKeys`, `kms:`, `kms: ListAliases` e `kms:Decrypt`) não estão restritas à AppFlow Amazon e essas permissões podem ser concedidas a qualquer chave em sua conta. `GenerateDataKey AWS KMS`

Para ver as permissões dessa política, consulte [AWSSupplyChainFederationAdminAccess](#) no AWS Management Console.

Cadeia de Suprimentos AWS atualizações nas políticas AWS gerenciadas

A tabela a seguir lista detalhes sobre as atualizações nas políticas AWS gerenciadas Cadeia de Suprimentos AWS desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do Cadeia de Suprimentos AWS documento.

Alteração	Descrição	Data
AWSSupplyChainFederationAdminAccess : política atualizada	Cadeia de Suprimentos AWS atualizou a política gerenciada para permitir que usuários federados acessem <code>ListApplicationAssignments</code> , <code>DescribeApplication</code> , <code>DescribeInstance</code> , e <code>GetApplicationAssignmentConfiguration</code> operações no IAM Identity Center.	10 de dezembro de 2024
AWSSupplyChainFederationAdminAccess : política atualizada	Cadeia de Suprimentos AWS atualizou a política gerenciada para permitir que usuários federados acessem as <code>ListProfileAssociations</code>	1º de novembro de 2023

Alteração	Descrição	Data
	operações no IAM Identity Center.	
AWSSupplyChainFederationAdminAccess : política atualizada	Cadeia de Suprimentos AWS atualizou a política gerenciada para permitir que usuários federados acessem GetObject as operações PutObject e no bucket S3 dedicado com o recurso <code>arn:aws:s3:::aws-supply-chain-data-*</code> .	21 de setembro de 2023
AWSSupplyChainFederationAdminAccess – Nova política	Cadeia de Suprimentos AWS adicionou uma nova política para permitir que usuários federados acessem o Cadeia de Suprimentos AWS aplicativo. Isso inclui as permissões necessárias para realizar ações dentro do aplicativo Cadeia de Suprimentos AWS.	1º de março de 2023
Cadeia de Suprimentos AWS começou a rastrear alterações	Cadeia de Suprimentos AWS começou a rastrear as mudanças em suas políticas AWS gerenciadas.	1º de março de 2023

Validação de conformidade para Cadeia de Suprimentos AWS

Audidores terceirizados avaliam a segurança e a conformidade Cadeia de Suprimentos AWS como parte de vários programas de AWS conformidade. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para obter uma lista dos Serviços da AWS que se enquadram no escopo de programas de conformidade específicos, consulte [AWS Serviços no escopo do programa de conformidade AWS](#). Para obter informações gerais, consulte Programas de [AWS conformidade Programas AWS](#) de .

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

Sua responsabilidade de conformidade quando você usa Cadeia de Suprimentos AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade da sua empresa e pelas leis e regulamentos aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- [Guias de início rápido de segurança e compatibilidade](#): estes guias de implantação abordam as considerações de arquitetura e fornecem etapas para implantação de ambientes de linha de base focados em compatibilidade e segurança na AWS.
- Documento técnico [sobre arquitetura para segurança e conformidade com a HIPAA — Este whitepaper](#) descreve como as empresas podem usar para criar aplicativos compatíveis com a HIPAA. AWS
- 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.
- [Avaliar recursos com regras](#) no Guia do desenvolvedor da AWS Config : esse guia avalia como suas configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- [AWS Security Hub](#) — Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS para ajudá-lo a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.

Resiliência em Cadeia de Suprimentos AWS

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS forneça várias zonas de disponibilidade fisicamente separadas e isoladas. Conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

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

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

Registro e monitoramento Cadeia de Suprimentos AWS

O registro e o monitoramento são uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho da cadeia de AWS suprimentos e de suas outras AWS soluções. AWS fornece a ferramenta de AWS CloudTrail monitoramento para monitorar a cadeia AWS de suprimentos, relatar quando algo está errado e tomar ações automáticas quando apropriado.

Note

APIs chamadas somente do Cadeia de Suprimentos AWS console são capturadas em AWS CloudTrail.

O AWS CloudTrail captura chamadas de API e eventos relacionados feitos por sua conta da Conta da AWS ou em nome dela e entrega os arquivos de log a um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas chamaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. Você pode ver os eventos da cadeia AWS de suprimentos em scn.amazonaws.com. Para obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).

Note

Observe o seguinte com Cadeia de Suprimentos AWS:

- Quando você convida usuários que não têm acesso Cadeia de Suprimentos AWS, esses usuários não recebem informações nas notificações que recebem do aplicativo web. Os usuários convidados recebem uma notificação por e-mail com um link para o aplicativo web. Eles só podem fazer login e visualizar o conteúdo na notificação se tiverem as permissões de usuário necessárias.
- Todos os usuários com ou sem permissões de usuário para um determinado Insight podem ver as mensagens de bate-papo do Insights.
- Como administrador do aplicativo, quando você adiciona usuários à Cadeia de Suprimentos AWS instância, eles têm acesso ao AWS KMS key. Você pode gerenciar as

permissões do usuário para adicionar ou remover usuários. Para obter mais informações sobre as permissões de usuário, consulte [Gerenciando funções de permissão do usuário](#).

Cadeia de Suprimentos AWS eventos de dados em CloudTrail

Note

Os aplicativos web APIs listados abaixo [Cadeia de Suprimentos AWS aplicativo web APIs](#) estão listados nos eventos de dados em CloudTrail.

Os [Eventos de dados](#) fornecem informações sobre as operações de recursos realizadas em um recurso (por exemplo, leitura ou gravação em um objeto do Amazon S3). Também são conhecidas como operações de plano de dados. Eventos de dados geralmente são atividades de alto volume. Por padrão, CloudTrail não registra eventos de dados. O histórico de CloudTrail eventos não registra eventos de dados.

Há cobranças adicionais para eventos de dados. Para obter mais informações sobre CloudTrail preços, consulte [AWS CloudTrail Preços](#).

Você pode registrar eventos de dados para os tipos de Cadeia de Suprimentos AWS recursos usando o CloudTrail console ou AWS CLI as operações CloudTrail da API.

- Para registrar eventos de dados usando o CloudTrail console, crie um [armazenamento de dados de trilhas ou eventos](#) para registrar eventos de dados ou [atualize um armazenamento de dados de trilhas ou eventos existente](#) para registrar eventos de dados.
 1. Selecione Eventos de dados para registrar eventos de dados em log.
 2. Em Tipo de evento de dados, escolha o tipo de recurso para o qual você deseja registrar eventos de dados em log.
 3. Selecione o modelo de seletor de logs que deseja usar. Você pode registrar todos os eventos de dados para o tipo de recurso, registrar todos os eventos `readOnly`, registrar todos os eventos `writeOnly` ou criar um modelo de seletor de logs personalizado para filtrar os campos `readOnly`, `eventName` e `resources.ARN`.
- Para registrar eventos de dados usando o AWS CLI, configure o `--advanced-event-selector` parâmetro para definir o `eventCategory` campo igual `Data` e o `resources.type`

campo igual ao valor do tipo de recurso. É possível adicionar condições para filtrar os valores dos campos `readOnly`, `eventName` e `resources.ARN`.

- Para configurar uma trilha para registrar eventos de dados, execute o [put-event-selectorscomando](#) . Para ter mais informações, consulte [Registrar em log eventos de dados para trilhas com a AWS CLI](#).
- Para configurar um armazenamento de dados de eventos para registrar eventos de dados, execute o [create-event-data-storecomando](#) para criar um novo armazenamento de dados de eventos para registrar eventos de dados ou executar o [update-event-data-storecomando](#) para atualizar um armazenamento de dados de eventos existente. Para obter mais informações, consulte [Log em log de eventos de dados para trilhas AWS CLI](#).

*É possível configurar seletores de eventos avançados para filtrar os campos `eventName`, `readOnly` e `resources.ARN` e registrar em log somente os eventos que são importantes para você. Para obter mais informações sobre esses campos, consulte [AdvancedFieldSelector](#).

Cadeia de Suprimentos AWS eventos de gerenciamento em CloudTrail

[Os eventos de gerenciamento](#) fornecem informações sobre as operações de gerenciamento que são realizadas nos recursos AWS da sua conta. Também são conhecidas como operações de ambiente de gerenciamento. Por padrão, CloudTrail registra eventos de gerenciamento.

O AWS Supply Chain registra todas as operações do plano de controle CloudTrail como eventos de gerenciamento.

Cadeia de Suprimentos AWS aplicativo web APIs

Os APIs listados nesta seção são chamados por Cadeia de Suprimentos AWS aplicativos em nome de usuários federados. Eles não APIs são visíveis nos CloudTrail registros e não são capturados no documento de referência de autorização de serviço, consulte [Cadeia de Suprimentos AWS](#). O acesso a eles APIs é controlado por Cadeia de Suprimentos AWS aplicativos com base nas permissões federadas da função de usuário. Você não deve tentar controlar o acesso a eles APIs para evitar a interrupção dos Cadeia de Suprimentos AWS aplicativos.

Perfis de usuário

APIs Os itens a seguir são usados para gerenciar usuários, funções de usuário, notificações de usuários e mensagens de bate-papo em Cadeia de Suprimentos AWS.

```
scn:AddMembersToResourceBasedChat
scn:AssignGalaxyRoleToUser
scn:AssociateUser
scn:BatchGetUsers
scn:BatchMarkNotificationAsDelivered
scn:CreateRole
scn>DeleteRole
scn:DescribeChatForUser
scn:GetAccessDetailConfig
scn:GetChatPreferencesForUser
scn:GetMessagingSessionConnectionDetails
scn:GetNotificationsPreference
scn:GetOrCreateChimeUser
scn:GetOrCreateResourceBasedChat
scn:GetOrCreateUserBasedChat
scn:GetOrganizationInfo
scn:GetResourceBasedChatArn
scn:GetUserDetails
scn:ListChatMembers
scn:ListChatMessages
scn:ListChatModerators
scn:ListChats
scn:ListRoles
scn:ListUserNotifications
scn:ListUsersWithRole
scn:MarkNotificationAsDelivered
scn:MarkNotificationAsRead
scn:RemoveMemberFromResourceBasedChat
scn:RemoveUser
scn:SearchChimeUsers
scn:SearchUsers
scn:SendChatMessage
scn:SetNotificationsPreference
scn:UpdateChatPreferencesForUser
scn:UpdateChatReadMarker
scn:UpdateOrganizationInfo
scn:UpdateRole
scn:UpdateUser
```

Data lake

Os itens a seguir APIs são usados para criar e gerenciar fluxos de dados e conexões no data lake.

```
scn:CreateConnection
scn:CreateDataflow
scn:CreateDeleteDataByPartitionJob
scn:CreateExtractFlows
scn:CreatePresignedUrl
scn:CreateSampleParsingJob
scn:CreateSap0DataConnection
scn:CreateUpdateDatasetSchemaJob
scn>DeleteConnection
scn>DeleteDataflow
scn>DeleteExtractFlows
scn>DeleteSap0DataConnection
scn:describeDatasetGroup
scn:DescribeDataset
scn:DescribeJob
scn:GetConnection
scn:GetCreateExtractFlowsStatus
scn:GetDataflow
scn:ListConnections
scn:ListCustomerFiles
scn:ListDataflows
scn:ListDataflowStats
scn:ListDatasets
scn:UpdateConnection
scn:UpdateDataflow
scn:UpdateExtractFlow
```

Insights

APIs Os itens a seguir são usados pelo aplicativo Insights para gerenciar filtros, listas de observação e visualizar alterações no inventário.

```
scn:AddModeratorToResourceBasedChat
```

```
scn:ComputePostRebalancedQuantities
scn:ComputePostRebalancedQuantitiesV1
scn:CreateInsightFilter
scn:CreateInsightSubscription
scn>DeleteInsightFilter
scn>DeleteInsightSubscription
scn:GetInsightLineItem
scn:GetInsightSubscription
scn:GetInstanceAttribute
scn:GetInstanceRequiredDatasetAvailabilityStatus
scn:GetKpiData
scn:GetModelEndpointStatus
scn:GetPIVForProduct
scn:GetPIVForSite
scn:GetPIVForSiteAndProduct
scn:GetPIVForSitesAndProducts
scn:GetProducts
scn:GetProductSummaryAggregates
scn:GetSites
scn:GetSiteSummaryAggregates
scn:IsUserAuthorizedForInsightLineItem
scn:ListCustomAttributeValues
scn:ListGeographiesAsGalaxyAdmin
scn:ListInsightFilters
scn:ListInsightLineItems
scn:ListInsightSubscriptions
scn:ListInventoryQuantityAggregates
scn:ListInventoryRisksBySiteAndProduct
scn:ListInventorySummariesBySite
scn:ListPIVProductsBySite
scn:ListProductHierarchiesAsGalaxyAdmin
scn:ListProducts
scn:ListProductsAsGalaxyAdmin
scn:ListSites
scn:ListUsers
scn:PotentiallyComputeThenListRebalancingOptionsForInsightLineItem
scn:RegisterInstanceAttribute
scn:UpdateInsightFilter
scn:UpdateInsightLineItemStatus
scn:UpdateInsightSubscription
scn:UpdateRebalancingOptionStatus
scn:UpdateRebalancingOptionStatusV1
```

Planejamento de Demanda

Os itens a seguir APIs são usados Cadeia de Suprimentos AWS para criar e gerenciar previsões, planos de demanda ou pastas de trabalho.

```
scn:AssociateDatasetWithWorkbook
scn:CreateBaselineForecast
scn:CreateDemandPlan
scn:CreateDemandPlanningCycle
scn:CreateDemandPlanningDatasetExportJob
scn:CreateDerivedForecast
scn:CreateWorkbook
scn>DeleteDemandForecastConfig
scn>DeleteDemandPlanningCycle
scn>DeleteDerivedForecast
scn>DeleteWorkbook
scn:DescribeBaselineForecast
scn:DescribeDemandPlanningCycleAccuracyJob
scn:DescribeDerivedForecast
scn:DescribePlanningCycle
scn:DescribeWorkbook
scn:DisassociatePlanningCycle
scn:GetDemandForecastConfig
scn:GetDemandPlan
scn:GetDemandPlanningCycle
scn:GetDemandPlanningCycleAccuracy
scn:GetDemandPlanningDatasetJob
scn:ListDemandPlans
scn:ListDerivedForecasts
scn:ListForecastingJobs
scn:ListPlanningCycles
scn:ListWorkbooks
scn:PublishDemandPlan
scn:PutDemandForecastConfig
scn:StartDemandPlanningCycleAccuracyJob
scn:StartForecastingJob
scn:UpdateDemandPlan
scn:UpdateDemandPlanningCycleMetadata
scn:UpdateWorkbook
```

Planejamento de suprimentos

Os itens a seguir APIs são usados Cadeia de Suprimentos AWS para criar e gerenciar planos de suprimentos.

```
scn:CreateReplenishmentPipeline
scn:GetReplenishmentPipeline
scn:UpdateReplenishmentPipeline
scn:ListReplenishmentPipelinesByInstance
scn:GetInstanceReplenishmentConfig
scn:CreateBacktest
scn:CreateReplenishmentReviewInstanceConfig
scn:GetReplenishmentReviewInstanceConfig
scn:ListReplenishmentVendors
scn:GetExceptionsSupplyInsightsStatistics
scn:GetPorSupplyInsightsStatistics
scn:GetPlanToPOConversionAnalytics
scn:GetPurchasePlanStatistics
scn:ListPlanExceptions
scn:ListPurchaseOrderRequestLines
scn:UpdatePurchaseOrderRequestLines
scn:ListBomPurchasePlans
scn:ListBomProductionPlans
scn:ListBomTransferPlans
scn:ListBomInsights
scn:ListBomProcesses
scn:ExportBomPlans
scn:GetBomPlanSummary
scn:GetDashboardAnalytics
scn:GetPurchaseOrderRequestExplanation
scn:ListBomSupplyPlan
scn:GetBomPlanRecordDetails
scn:GetBomPlanSummaryAnalytics
scn:ListBomPurchaseOrders
scn:ListBomTransferOrders
scn:ListBomProductionOrders
scn:ExportAllExplodedBoms
scn:ExportBillOfMaterials
```

```
scn:ExportInventoryPolicy
scn:ExportProductionProcess
scn:ExportSourcingRule
scn:ExportTransportationLane
scn:ExportVendorLeadTime
scn:ImportBillOfMaterials
scn:ImportInventoryPolicy
scn:ImportProductionProcess
scn:ImportSourcingRule
scn:ImportTransportationLane
scn:ImportVendorLeadTime
```

Amazon Q em Cadeia de Suprimentos AWS

Os itens a seguir APIs são usados no Amazon Q em Cadeia de Suprimentos AWS.

```
scn:GetQMessage
scn:ListQMessages
scn:PutQMessageFeedback
scn:SendQMessage
scn:GetQEnablementStatus
scn:UpdateQEnablementStatus
```

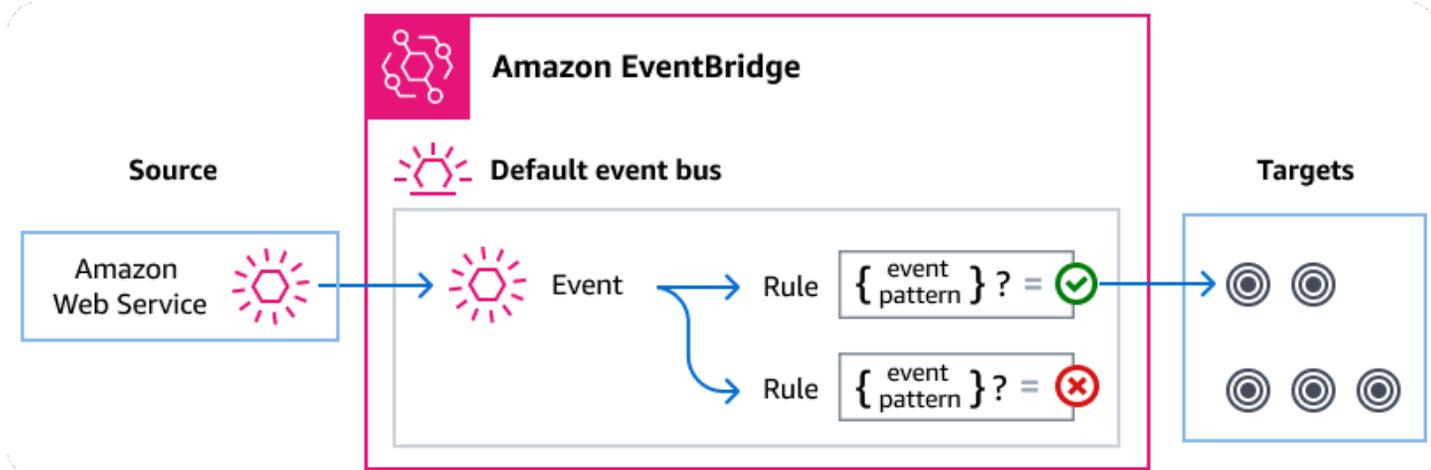
Gerenciando Cadeia de Suprimentos AWS eventos usando Amazon EventBridge

Usando EventBridge, você pode automatizar outros serviços para responder às mudanças de status de execução de um fluxo de trabalho Step Functions padrão.

Amazon EventBridge é um serviço sem servidor que usa eventos para conectar componentes do aplicativo, facilitando a criação de aplicativos escaláveis orientados por eventos. A arquitetura orientada a eventos é um estilo de criação de sistemas de software com acoplamento fraco que funcionam juntos emitindo e respondendo a eventos. Os eventos representam uma mudança em um recurso ou ambiente.

Como isso funciona:

Como acontece com muitos AWS serviços, Cadeia de Suprimentos AWS gera e envia eventos para o barramento de eventos EventBridge padrão. (O barramento de eventos padrão é provisionado automaticamente em todas as AWS contas.) Um barramento de eventos é um roteador que recebe eventos e os entrega a zero ou mais destinos, ou alvos. As regras especificadas para o barramento de eventos avaliam os eventos à medida que eles chegam. Cada regra verifica se um evento corresponde ao padrão do evento. Se o evento corresponder, o barramento de eventos enviará o evento para os destinos especificados.



Tópicos

- [Cadeia de Suprimentos AWS eventos](#)
- [Entregando Cadeia de Suprimentos AWS eventos usando EventBridge regras](#)
- [Cadeia de Suprimentos AWS referência de detalhes de eventos](#)

Cadeia de Suprimentos AWS eventos

Cadeia de Suprimentos AWS envia automaticamente os seguintes eventos para o barramento de EventBridge eventos padrão. Os eventos que correspondem ao padrão de eventos de uma regra são entregues aos alvos especificados em uma [base](#). Pode ser que os eventos sejam entregues fora da ordem.

Para obter mais informações, consulte [Eventos do EventBridge](#), no Guia do usuário do Amazon EventBridge .

Tipo de detalhe de evento	Descrição
Alteração do status de integração de dados da cadeia de suprimentos da AWS	Exibe o status de cada arquivo ingerido em Cadeia de Suprimentos AWS.

Entregando Cadeia de Suprimentos AWS eventos usando EventBridge regras

Para que o barramento de eventos EventBridge padrão envie Cadeia de Suprimentos AWS eventos para um destino, você deve criar uma regra. Cada regra contém um padrão de evento, que EventBridge corresponde a cada evento recebido no barramento de eventos. Se os dados do evento corresponderem ao padrão de evento especificado, EventBridge entregará esse evento ao (s) alvo (s) da regra.

Para obter instruções abrangentes de como criar regras de barramento de eventos, consulte [Criar regras que reagem a eventos](#) no Guia do usuário do EventBridge .

Criação de padrões de eventos que correspondam aos Cadeia de Suprimentos AWS eventos

Cada padrão de evento é um objeto JSON que contém:

- Um atributo `source` que identifica o serviço que envia o evento. Para Cadeia de Suprimentos AWS eventos, a fonte é `aws . supplychain`.
- (Opcional): um atributo `detail-type` que contém uma matriz dos tipos de eventos a serem correlacionados.
- (Opcional): um atributo `detail` que contém quaisquer outros dados relacionados aos eventos a serem correlacionados.

Por exemplo, o padrão de eventos a seguir corresponde a todos os AWS Supply Chain Data Integration Status Change eventos de Cadeia de Suprimentos AWS:

```
{
  "source": ["aws.supplychain"],
  "detail-type": ["AWS Supply Chain Data Integration Status Change"]
}
```

```
}
```

Para obter mais informações sobre como escrever padrões de eventos, consulte [Padrões de eventos](#) no Guia do usuário do EventBridge .

Cadeia de Suprimentos AWS referência de detalhes de eventos

Todos os eventos dos AWS serviços têm um conjunto comum de campos contendo metadados sobre o evento, como o AWS serviço que é a origem do evento, a hora em que o evento foi gerado, a conta e a região em que o evento ocorreu e outros. Para obter as definições desses campos gerais, consulte [Referência da estrutura de eventos](#) no Guia do usuário do Amazon EventBridge .

Além disso, cada evento tem um campo de `detail` que contém dados específicos desse determinado evento. A referência abaixo define os campos de detalhes dos vários eventos do Cadeia de Suprimentos AWS .

Ao usar EventBridge para selecionar e gerenciar Cadeia de Suprimentos AWS eventos, é útil ter em mente o seguinte:

- O `source` campo para todos os eventos de Cadeia de Suprimentos AWS está definido como `aws . supplychain`.
- O campo do `detail-type` especifica o tipo de evento.

Por exemplo, `AWS Supply Chain Data Integration Status Change`.

- O campo de `detail` contém os dados específicos desse determinado evento.

Para obter mais informações sobre a criação de padrões de eventos que habilitam regras para corresponder a eventos do Cadeia de Suprimentos AWS , consulte [Padrões de eventos](#) no Guia do usuário do Amazon EventBridge .

Para obter mais informações sobre eventos e como EventBridge os processa, consulte [Amazon EventBridge eventos](#) no Guia Amazon EventBridge do usuário.

Alteração do status de integração de dados da cadeia de suprimentos da AWS

Abaixo está um exemplo do `AWS Supply Chain Data Integration Status Change` event evento.

```
{
  "version": "0",
  "id": "instanceID",
  "detail-type": "AWS Supply Chain Data Integration Status Change",
  "source": "aws.supplychain",
  "account": "accountID",
  "time": "2024-03-30T12:26:13Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "version": "1.0",
    "instanceId": "instanceID",
    "flowArn": "arn:aws:scn:region:accountID:instance/instanceID/data-integration-
flows/flowname",
    "flowExecutionId": "flowExecutionId",
    "status": "IN_PROGRESS",
    "startTime": "2024-03-30T12:26:13Z",
    "endTime": "",
    "message": "",
    "sourceType": "S3",
    "sourceInfo": {
      "s3Source": {
        "bucketName": "aws-supply-chain-data-instanceID",
        "key": "flowname"
      }
    }
  }
}
```

endTime só está disponível quando o status é falha ou sucesso.

Cotas para Cadeia de Suprimentos AWS

Você Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada um. AWS service (Serviço da AWS) A menos que especificado de outra forma, cada cota é específica da região. Você pode solicitar o aumento das cotas de recursos definidos para o nível da sua conta. Para obter mais informações sobre cotas em nível de conta, consulte a tabela abaixo.

Para ver as cotas de Cadeia de Suprimentos AWS, abra o console [Service Quotas](#). No painel de navegação, escolha AWS services (Serviços da) e selecione Cadeia de Suprimentos AWS.

Para solicitar o aumento da cota, consulte [Solicitar um aumento de cota](#) no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível no serviço de cotas, use o [formulário de aumento de limite](#).

Você Conta da AWS tem as seguintes cotas relacionadas a. Cadeia de Suprimentos AWS

Recurso	Padrão	Ajustável
Número de instâncias	10	Não
<div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note Você pode criar até 10 instâncias em uma AWS conta.</p> </div>		
Número de buckets do Amazon S3	100	Não
Convites ativos e pendentes em uma conta AWS	30	Sim
Solicitações de dados em uma AWS conta	4.000	Sim
Itens da linha Insights por lista de observação	1.000	Não

Recurso	Padrão	Ajustável
Listas de observação do Insights por instância em uma conta AWS	1.000	Sim
Listas de observação do Insights por usuário em uma conta AWS	100	Sim
Fluxos de integração de dados por instância em uma AWS conta	100	Não
Namespaces de conjunto de dados personalizados por instância em uma conta AWS	20	Sim
Conjuntos de dados por namespace de conjunto de dados personalizado por instância em uma conta AWS	250	Sim
Conjuntos de dados no namespace padrão do conjunto de dados por instância em uma conta AWS	1.000	Não

Perguntas frequentes (FAQs)

As informações a seguir podem ajudá-lo a solucionar problemas comuns na ativação do IAM Identity Center.

Pergunta	Resposta
Por que a integração com o IAM Identity Center é necessária?	O IAM Identity Center é o recurso do IAM que gerencia a sincronização das fontes de identidade. O IAM Identity Center é a fonte de identidade da Cadeia de Suprimentos AWS instância. Você precisa configurar o IAM Identity Center para configurar o AWS console e o aplicativo Cadeia de Suprimentos AWS web. Para obter mais informações sobre o IAM Identity Center, consulte Habilitar o AWS IAM Identity Center no Guia AWS IAM Identity Center do usuário .
Por que usar uma instância organizacional do IAM Identity Center para Cadeia de Suprimentos AWS?	Ao criar uma instância organizacional, você pode habilitar o acesso ao IAM Identity Center em todas as AWS contas. Por exemplo, se sua Central de Identidade do IAM não estiver ativada na mesma AWS conta da conta da Cadeia de Suprimentos AWS instância. Para obter mais informações sobre os benefícios da criação de uma instância organizacional do IAM Identity Center, consulte Instâncias organizacionais do IAM Identity Center no Guia AWS IAM Identity Center do usuário .
Por que os privilégios de administrador delegado são necessários? Cadeia de Suprimentos AWS	Não é necessário ter um administrador delegado para usar, Cadeia de Suprimentos AWS mas é uma prática recomendada para uma configuração de AWS organização restringir o acesso à conta de gerenciamento da organização e gerenciar o IAM Identity

Pergunta	Resposta
	<p>Center. Para obter mais informações, consulte Delegated adminsitrotor for Organizations. AWS .</p> <p>Ao criar uma instância da organização, certifique-se de que a conta que será usada para criar uma Cadeia de Suprimentos AWS instância faça parte da mesma organização da conta do IAM Identity Center. Certifique-se de que as permissões necessárias estejam habilitadas para criar uma instância e que você possa criar uma Cadeia de Suprimentos AWS instância na mesma região da conta do IAM Identity Center. Para obter informações sobre as permissões necessárias para criar uma Cadeia de Suprimentos AWS instância, consulte Começando com Cadeia de Suprimentos AWS.</p>

AWS apoio

Se você for administrador e precisar entrar em contato com o suporte para Cadeia de Suprimentos AWS, escolha uma das seguintes opções:

- Se você tiver uma Suporte conta, acesse o [Support Center](#) e envie um ticket.
- Abra o [AWS Management Console](#) e escolha Cadeia de Suprimentos AWS , Suporte, Criar caso.

É útil fornecer as seguintes informações:

- Seu ID/ARN da instância da cadeia de AWS suprimentos.
- Sua AWS região.
- Uma descrição detalhada do problema.

Histórico de documentos do Guia do Cadeia de Suprimentos AWS Administrador

A tabela a seguir descreve as versões de documentação do Cadeia de Suprimentos AWS.

Alteração	Descrição	Data
Cadeia de Suprimentos AWS Cotas atualizadas	Atualizou as cotas de sua AWS conta relacionadas a Cadeia de Suprimentos AWS	12 de maio de 2025
Política AWS gerenciada atualizada	Cadeia de Suprimentos AWS atualizou a política gerenciada para permitir que usuários federados acessem ListApplicationAssignments, DescribeApplication DescribeInstance, e GetApplicationAssignmentConfiguration operações no IAM Identity Center.	10 de dezembro de 2024
Atualização da política KMS	Atualizou a política do KMS para permitir Cadeia de Suprimentos AWS o acesso à sua AWS KMS chave.	18 de março de 2024
PrivateLink apoio	Você pode acessar Cadeia de Suprimentos AWS usando um endpoint de interface (AWS PrivateLink).	26 de fevereiro de 2024
Adição de grupos	Os usuários devem fazer parte de um grupo do IAM Identity Center para acessar o Cadeia de Suprimentos AWS.	14 de novembro de 2023

Política AWS gerenciada atualizada	Cadeia de Suprimentos AWS atualizou a política gerenciada para permitir que usuários federados acessem as ListProfileAssociations operações no IAM Identity Center.	1º de novembro de 2023
Política AWS gerenciada atualizada	Cadeia de Suprimentos AWS atualizou a política gerenciada para permitir que usuários federados acessem GetObject as operações PutObject e no bucket dedicado do Amazon S3 com o recurso arn:aws:s3:::aws-supply-chain-data-*	21 de setembro de 2023
Informações atualizadas sobre o suporte de regiões	Cadeia de Suprimentos AWS O planejamento de demanda agora também é suportado na região Ásia-Pacífico (Sydney).	12 de setembro de 2023
Use o AWS console para ativar e desativar Cadeia de Suprimentos AWS	Cadeia de Suprimentos AWS Agora, os usuários podem usar o AWS console para se inscrever e optar Cadeia de Suprimentos AWS por não usar ou armazenar seu conteúdo no AWS Organizations.	7 de setembro de 2023
Informações atualizadas sobre o suporte de regiões	Cadeia de Suprimentos AWS agora também é suportado na região Ásia-Pacífico (Sydney) e na região Europa (Irlanda).	19 de julho de 2023

[Informações atualizadas sobre como entrar em contato com o AWS Support e criar uma instância](#)

Cadeia de Suprimentos AWS
Agora, os usuários podem entrar em contato com o AWS Support para obter ajuda e atualizar o conteúdo sobre como criar uma instância.

3 de abril de 2023

[Política AWS gerenciada adicionada](#)

AWS A Supply Chain adicionou uma nova política para permitir que usuários federados acessem o aplicativo o AWS Supply Chain, incluindo as permissões necessárias para realizar ações dentro do aplicativo AWS Supply Chain.

1 de março de 2023

[Lançamento inicial](#)

Versão inicial do Guia do Cadeia de Suprimentos AWS Administrador.

29 de novembro de 2022

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.