Guia do administrador

Cadeia de Suprimentos AWS

Cadeia de Suprimentos AWS: Guia do administrador

Table of Contents

O que é o Cadeia de Suprimentos AWS?

Cadeia de Suprimentos AWS é um aplicativo de gerenciamento da cadeia de suprimentos baseado em nuvem que funciona com suas soluções existentes, como planejamento de recursos corporativos (ERP) e sistemas de gerenciamento da cadeia de suprimentos. Usando Cadeia de Suprimentos AWS, você pode conectar e extrair seus dados relacionados ao inventário, fornecimento e demanda dos sistemas existentes de ERP ou cadeia de suprimentos em um modelo de Cadeia de Suprimentos AWS dados unificado.

Tópicos

Navegadores compatíveis com o Cadeia de Suprimentos AWS

Antes de trabalhar com a cadeia de suprimentos AWS, verifique se o 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 data de fim da vida útil 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 compatíveis com o Cadeia de Suprimentos AWS

O Cadeia de Suprimentos AWS oferece suporte aos seguintes idiomas:

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

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

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 https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

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

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

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

Proteja seu Usuário raiz da conta da AWS

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

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Signing in as the root user (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. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo para 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 seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  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 Create a permission set 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 Add groups no Guia do usuário do AWS IAM Identity Center .

Fechando uma AWS conta

Para obter informações sobre como fechar uma AWS conta, consulte Fechando uma conta.

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

Pré-requisitos

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

- Você criou um Conta da AWS. Para ter mais informações, consulte Configurando uma AWS conta.

> **Note**
>
> Se você não tiver ativado AWS IAM Identity Center, crie uma AWS organização e ative o IAM Identity Center. Para obter mais informações sobre como criar uma AWS organização, consulte Criando uma organização.

- Ative o IAM Identity Center no mesmo Região da AWS local em que você deseja criar sua Cadeia de Suprimentos AWS instância. Cadeia de Suprimentos AWS só é suportado nas regiões Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Europa (Frankfurt) e Europa (Irlanda). Para ter mais informações, consulte Habilitar o IAM Identity Center .

  > **Note**
  >
  > Cadeia de Suprimentos AWS O Planejamento da Demanda e o Planejamento do Suprimento não são suportados na região Europa (Irlanda).

  > **Note**
  >
  > Se você não ativou o IAM Identity Center em uma região diferente das listadas aqui, não é possível criar uma Cadeia de Suprimentos AWS instância.

- Você pode criar usuários do IAM a partir do console AWS Identity and Access Management (IAM). Para ter mais informações, consulte Configurando uma AWS conta.
- Adicione usuários que precisam Cadeia de Suprimentos AWS acessar o IAM Identity Center. Para ter mais informações, consulte Adicionar usuários no IAM Identity Center. Você também pode conectar seu Active Directory ao IAM Identity Center. Para obter mais informações, consulte Conectar ao diretório do Microsoft AD no Guia do usuário do AWS IAM Identity Center .
- Ao usar o Microsoft Active Directory, verifique se a sincronização do active directory está ativada.
- 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.

Usar o console do Cadeia de Suprimentos AWS

> **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. Se você criar uma política baseada em identidade que seja mais restritiva do 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 a operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o Cadeia de Suprimentos AWS console, anexe também a política Cadeia de Suprimentos AWS `ConsoleAccess` ou a política `ReadOnly` AWS gerenciada às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

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:DescribeOrganization",
                "organizations:CreateOrganization",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:CreateGrant",
                "kms:RetireGrant",
                "kms:DescribeKey",
                "kms:ListAliases"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:CreateRole",
                "iam:CreatePolicy",
                "iam:GetRole",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "sso:StartPeregrine",
                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
```

```
                "sso:GetPeregrineStatus",
                "sso:GetSSOStatus",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:AssociateProfile",
                "sso:AssociateDirectory",
                "sso:RegisterRegion",
                "sso:StartSSO",
                "sso:CreateManagedApplicationInstance",
                "sso:DeleteManagedApplicationInstance",
                "sso:GetManagedApplicationInstance",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Criação de uma instância

> **Note**
>
> É possível criar até 10 instâncias em um Conta da AWS. As 10 instâncias incluem instâncias ativas e de inicialização. Se você já ativou o IAM Identity Center (sucessor do AWS Single Sign-On), você deve criar sua Cadeia de Suprimentos AWS instância no mesmo Região da AWS local em que ativou o IAM Identity Center. Cadeia de Suprimentos AWS não é compatível com chamadas do IAM Identity Center em todas as regiões.

Para criar uma Cadeia de Suprimentos AWS instância, siga estas etapas.

> **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 abaixoUsar o console do Cadeia de Suprimentos AWS. Esse administrador deve convidar um usuário do IAM como Cadeia de Suprimentos AWS administrador para gerenciar Cadeia de Suprimentos AWS.

1. Abra o Cadeia de Suprimentos AWS console emhttps://console.aws.amazon.com/scn/home.
2. Se necessário, altere a Região da AWS. Na barra na parte superior da janela do console, abra a lista Selecionar uma região e escolha uma região. Para obter mais informações sobre Regiões e endpoints, consulte o Guia do usuário do IAM. Além disso, consulte Regiões e endpoints no Referência geral da Amazon Web Services.

   > **Note**
   >
   > Cadeia de Suprimentos AWS só é suportado nas regiões Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Europa (Frankfurt) Ásia-Pacífico (Sydney) e Europa (Irlanda).
   > Cadeia de Suprimentos AWS O Planejamento da Demanda e o Planejamento do Suprimento não são suportados na região Europa (Irlanda).

3. No Cadeia de Suprimentos AWS painel, escolha Criar instância.
4. Na página Propriedades da instância, insira as seguintes informações:

   - AWS Região — Escolha a região em que você ativou o IAM Identity Center. Para alterar a região, escolha Selecionar uma região no menu suspenso no canto superior direito. Não é possível alterar a região depois de criar a instância.
   - Nome – Insira o nome da instância.
   - (Opcional) Descrição – Insira uma descrição para a instância.

5. Em Chave do AWS KMS, insira sua chave KMS e atualize sua política de chaves KMS com o seguinte:

   > **Note**
   >
   > Como administrador do aplicativo, quando você adiciona usuários a instância do Cadeia de Suprimentos AWS , 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 Funções de permissão do usuário.

> **Note**
>
> Substitua *Região YourAccountNumber*, *YourInstanceID* e *YourKmsKeyArn*por sua AWS Região Conta da AWS, ID da Cadeia de Suprimentos AWS Instância e AWS KMS Chave.

```
   {
   "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"
                }

            }
        }
    ]
}
```

Se você não tiver uma chave KMS, escolha Criar para acessar o console do AWS KMS , no qual você pode criar essa chave. Use a política de chaves KMS anterior. Para obter informações sobre como criar chaves KMS, consulte Criar chaves no Guia do desenvolvedor do AWS Key Management Service .

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

6. (Opcional) Em Tags de instância, escolha Adicionar nova tag para atribuir uma tag à sua instância. Você pode usar essas etiquetas para identificar sua instância. Para obter informações sobre como criar tags, consulte Criar tags.
7. Selecione Criar instância.

   A criação da Cadeia de Suprimentos AWS instância leva aproximadamente de 2 a 3 minutos. Depois que a instância é criada, o campo Status no Cadeia de Suprimentos AWS painel é exibido como Ativo.
8. Depois que sua Cadeia de Suprimentos AWS instância for criada, atualize sua política do KMS para permitir Cadeia de Suprimentos AWS o acesso à sua AWS KMS chave.

> **Note**
>
> Substitua o *YourInstanceID* pelo ID da sua Cadeia de Suprimentos AWS instância. Você pode encontrar o ID da sua instância no painel do console do Cadeia de Suprimentos AWS .

```
{
```

```
    "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": "*"
},
{
    "Sid": "Enable ASC to backfill KMS permissions",
    "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":"YourKmsKeyArn"
}
```

Habilitar o IAM Identity Center

Antes de começar a usar Cadeia de Suprimentos AWS, você deve se conectar a uma fonte de identidade. Para obter mais informações, consulte Conceitos básicos do IAM no Guia do usuário do IAM.

Adicionar usuários no IAM Identity Center

Você pode gerenciar usuários para Cadeia de Suprimentos AWS usar o serviço IAM Identity Center. O IAM Identity Center é um serviço do IAM Identity Center baseado em nuvem que facilita o gerenciamento centralizado do acesso ao IAM Identity Center a todos os seus aplicativos Contas da AWS e aplicativos na nuvem. Para adicionar usuários do IAM, consulte Criar um usuário do IAM em sua conta da AWS no Guia do usuário do IAM.

Para obter mais informações sobre a criação de grupos de usuários do IAM, consulte Criação de grupos de usuários do IAM no Guia do usuário do IAM.

> **Note**
>
> Para adicionar um usuário Cadeia de Suprimentos AWS, os usuários devem fazer parte de um grupo do IAM Identity Center.

Escolhendo o proprietário do Cadeia de Suprimentos AWS aplicativo

> **Note**
>
> Como administrador do AWS console, você está escolhendo um 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. No painel do Cadeia de Suprimentos AWS console, em Proprietário do aplicativo, escolha Atribuir proprietário do aplicativo.
2. Em Selecionar proprietário do aplicativo, selecione um usuário que atuará como proprietário do Cadeia de Suprimentos AWS aplicativo. Você só pode pesquisar o nome de usuário e os usuários que correspondem aos critérios de pesquisa são exibidos.

Para adicionar mais usuários, escolha Ir para o IAM Identity Center. Para obter mais informações sobre como adicionar usuários, consulte Adicionar usuários no IAM Identity Center; e para obter mais informações sobre funções de permissão de usuário, consulte Funções de permissão do 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.

3. escolha Enviar teste.

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

4. Escolha Gerenciar em Cadeia de Suprimentos AWS para adicionar e remover usuários no aplicativo Cadeia de Suprimentos AWS web.

Atribuir grupos

Como proprietário ou Cadeia de Suprimentos AWS administrador do aplicativo, você só pode adicionar usuários que façam parte de um grupo do IAM Identity Center Cadeia de Suprimentos AWS.

1. No painel do Cadeia de Suprimentos AWS console, em Grupos, escolha Atribuir grupos.

   A página Grupos é exibida.

2. Em Nome do grupo, selecione o grupo com usuários que podem acessar Cadeia de Suprimentos AWS e escolha Atribuir.

   Você verá o grupo listado em Grupos no Cadeia de Suprimentos AWS painel.

3. Você pode escolher Gerenciar grupos para adicionar um novo grupo no IAM Identity Center. Depois que o grupo for adicionado ao IAM Identity Center, o grupo será listado em Nome do grupo no Cadeia de Suprimentos AWS.

Fazendo login no aplicativo web da AWS Supply Chain

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.

Fazendo login Cadeia de Suprimentos AWS pela primeira vez

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

Depois de fazer login no aplicativo Cadeia de Suprimentos AWS web como Cadeia de Suprimentos AWS administrador, siga estas etapas para concluir a configuração.

1. Na página Complete seu perfil, insira seu Cargo e fuso horário. Escolha Próximo.
2. 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.
3. 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 como adicionar usuários ao IAM Identity Center, consulte Adicionar usuários no IAM Identity Center. Para obter informações sobre as funções de permissão Cadeia de Suprimentos AWS do usuário, consulteFunções de permissão do usuário.
4. Se quiser adicionar usuários posteriormente, você pode escolher Ignorar por enquanto.

   A página de integração completa é exibida.
5. 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.

6. Escolha Continuar na página inicial para ver o painel do Cadeia de Suprimentos AWS .

Atualizando o perfil da sua conta

Você pode atualizar o perfil da sua conta a qualquer momento no aplicativo da Cadeia de Suprimentos AWS web. Siga estas etapas para atualizar a conta.

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

Você pode atualizar o perfil da organização a qualquer momento no aplicativo web Cadeia de Suprimentos AWS . Siga estas etapas para atualizar o perfil da organização.

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.

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 — Acesso para criar, visualizar e gerenciar previsões e substituições, além de publicar planejamentos 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

> **Note**
>
> Antes de adicionar usuários, verifique se o usuário faz parte de um grupo do IAM Identity Center e ao qual o grupo está atribuído Cadeia de Suprimentos AWS.

Como Cadeia de Suprimentos AWS administrador, você pode adicionar usuários para acessar o aplicativo Cadeia de Suprimentos AWS web. Para criar um usuário, siga as 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. Escolha Adicionar novo usuário.

   A página Adicionar usuário é exibida.
4. No menu suspenso Adicionar usuário(s), selecione o usuário e, em Selecionar função, selecione a função do usuário.
5. Escolha Adicionar.

Atualização de permissões de usuários

Você pode atualizar a função de permissão do usuário para os Cadeia de Suprimentos AWS usuários atuais. Siga estas etapas para atualizar a função de permissões do usuário.

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 abaixo:

> **Note**
>
> Dependendo das permissões de função que você atribui, o painel do Cadeia de Suprimentos AWS é personalizado. Para ter mais informações, consulte Criação de funções de permissão de usuário personalizadas.

- 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 — Acesso para criar, visualizar e gerenciar previsões e substituições, além de publicar planejamentos de demanda.

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.

> **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.

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

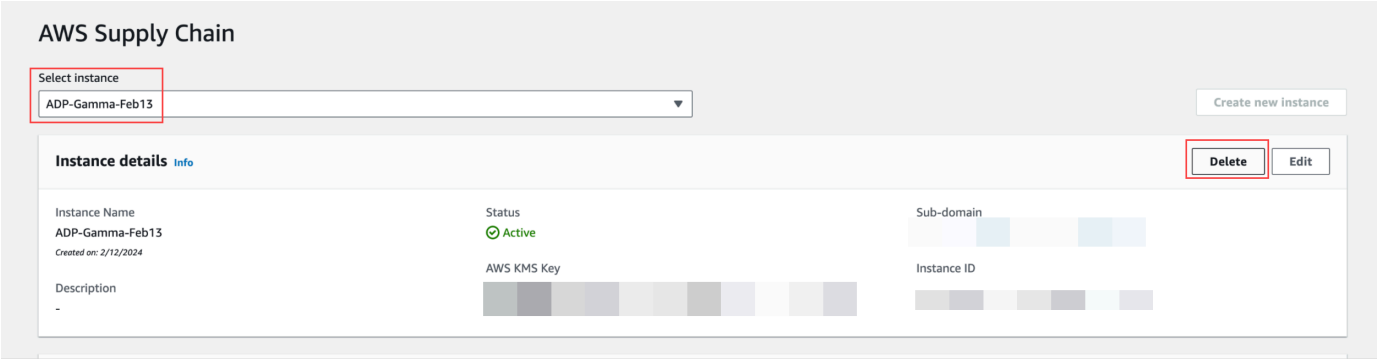
   A página Funções de permissão é exibida.
2. Escolha Criar nova função.
3. Na página Gerenciar função de permissão, em Nome da função, insira um nome.
4. Mova o controle deslizante para selecionar a função de permissão do usuário.
   - Gerenciar — A atribuição de permissões de gerenciamento aos usuários pode adicionar, editar e gerenciar informações.
   - Exibir — A atribuição de permissões de visualização aos usuários só pode visualizar as informações atuais.
5. 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.

Exclusão de uma instância

Para excluir uma instância, use as etapas a seguir.

> **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 emhttps://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.

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:

- 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

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 seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR 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.
- 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 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com Cadeia de Suprimentos AWS ou Serviços da AWS usa o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou

de diagnóstico. Se você fornecer um URL para um servidor externo, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse 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 inativa

Os dados de contato classificados como PII, ou dados que representam o conteúdo do cliente que está sendo armazenado por 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 AWS Key Management Service chave de dados 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 trocados com a AWS Supply Chain são protegidos em trânsito entre o navegador do usuário e a AWS Supply Chain 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. Criação de 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 CreateInstanceoperação. Cadeia de Suprimentos AWS cria uma concessão em seu nome enviando CreateGrantsolicitações 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 GenerateDataKeysolicitações 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 RetireGrantpermissões 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 Cadeia de Suprimentos AWS.

Você estabelece essa conectividade privada criando um endpoint de interface, desenvolvido 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`.

Criar uma política de endpoint para o endpoint da interface

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 AWSusuários 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 a Serviços Usando Políticas de Endpoint no AWS PrivateLink Guia.

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

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 realizar 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. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com Cadeia de Suprimentos AWS, consulteComo 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

Autenticando com identidades

A autenticação é 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 assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação Multifator no Guia do Usuário do AWS IAM Identity Center . Usar a autenticação multifator (MFA) na AWS 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, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas

da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Manual 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, recomendamos 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, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne 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 IAMAdmins e 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 Quando criar um usuário do IAM (em vez de um perfil) 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. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. 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 o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais

informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você 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 Manual 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 saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- 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 no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um 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 Encaminhar sessões de acesso.
  - Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar 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 a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS

e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como 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 funções não têm permissões. Para conceder aos usuários permissões 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.

As políticas do IAM definem permissões para uma ação independente 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 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 Criando políticas do IAM no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte 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 que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

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

Listas de controle de acesso (ACLs)

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

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte 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 atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do Usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as 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 o Organizações e SCPs, consulte Como os SCPs Funcionam no Manual do Usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia 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 recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de políticas	Sim
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Perfis vinculados ao 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, 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 Criando políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou 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 elementos da 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

Suporte a 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 que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

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

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo 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 (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 mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para Cadeia de Suprimentos AWS

Suporte ao 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 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 Encaminhamento de sessões de acesso.

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 realizar 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 a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas 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 aos usuários permissão para executar ações nos recursos de que 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

- Melhores práticas de política

Melhores práticas 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 seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para 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 atributos 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 gravar 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 100 verificações de política e recomendações acionáveis para ajudá-lo 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

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com 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, consulteComo 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 saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Políticas gerenciadas pela AWS para o Cadeia de Suprimentos AWS

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

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

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

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

AWS política gerenciada: AWSSupplyChainFederationAdminAccess

O AWSSupplychainFederationAdminAccess fornece aos Cadeia de Suprimentos AWS usuários federados acesso ao Cadeia de Suprimentos AWSaplicativo, 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. Não é possível anexar a política do AWSSupplychainFederationAdminAccess 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 as APIs administrativas.

Detalhes da permissão

Esta política inclui as seguintes permissões:

- `Chime` — Fornece acesso para criar ou excluir usuários em uma instância de aplicativo do Amazon Chime; 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 e perfis de lista associados à instância do aplicativo 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 acesso a GetBucketPolicy, PutObject, GetObject e ListBucket aos buckets com o recurso arn arn:aws:s3:::aws-supply-chain-data-*.
- `SecretsManager` — Fornece acesso à criação de segredos e à atualização da política secreta.
- `KMS` — Fornece ao serviço Amazon AppFlow o acesso às chaves da lista e ao alias da chave. Fornece permissões DescribeKey, CreateGrant e ListGrants para chaves KMS marcadas com o valor-chave aws-suply-chain-access: true; fornece acesso para criar segredos e atualizar políticas secretas.

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

Para visualizar as permissões para esta política, consulte AWSSupplyChainFederationAdminAccess no AWS Management Console.

Atualizações do Cadeia de Suprimentos AWS para políticas gerenciadas pela AWS

A tabela a seguir detalha as atualizações em AWS políticas gerenciadas para Cadeia de Suprimentos AWS desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página de histórico de documentos do Cadeia de Suprimentos AWS.

Alteração	Descrição	Data
AWSSupplyChainFederationAdminAccess – Política atualizada	Cadeia de Suprimentos AWS atualizou a política gerenciada para permitir que usuários federados acessem as operações ListProfileAssociations no IAM Identity Center.	1º de novembro de 2023
AWSSupplyChainFederationAdminAccess – Política atualizada	Cadeia de Suprimentos AWS atualizou a política gerenciada para permitir que usuários federados acessem as operações PutObject e GetObject no bucket S3 dedicado com o recurso arn arn:aws:s3:::aws-supply-chain-data-*.	21 de setembro de 2023

Alteração	Descrição	Data
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 Cadeia de Suprimentos AWS aplicativo.	1 de março de 2023
O Cadeia de Suprimentos AWS iniciou o rastreamento das alterações	O Cadeia de Suprimentos AWS começou a monitorar as alterações para as políticas gerenciadas da AWS.	1 de março de 2023

Validação de conformidade do Cadeia de Suprimentos AWS

Auditores de terceiros avaliam a segurança e a conformidade do Cadeia de Suprimentos AWS como parte de vários programas de conformidade da AWS. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para obter uma lista de serviços da Serviços da AWS que estão no escopo de programas de conformidade específicos, consulte AWSServiços no escopo pelo programa de conformidade. Para obter informações gerais, consulte Programas de conformidade da AWS.

É possível fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Downloading Reports in AWS Artifact.

Sua responsabilidade de conformidade ao usar o Cadeia de Suprimentos AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar com a 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.

- Whitepaper Architecting for HIPAA Security and Compliance: este whitepaper descreve como as empresas podem usar a AWS para criar aplicações em conformidade com a HIPAA.
- Recursos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- Avaliar recursos com regras no AWS ConfigGuia do desenvolvedor - Este guia avalia como suas configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: esse AWS service (Serviço da AWS) fornece uma visão abrangente do estado de sua segurança na AWS que ajuda você a conferir sua conformidade com padrões e práticas recomendadas de segurança do setor.

Resiliência no Cadeia de Suprimentos AWS

A infraestrutura AWS global da é criada com base em Regiões da AWS e 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 mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

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

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

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**
>
> As 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 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 do, consulte Funções de permissão do usuário.

Cadeia de Suprimentos AWS 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). Elas 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. Escolha Eventos de dados para registrar eventos de dados.
  2. Na lista Tipo de evento de dados, escolha o tipo de recurso para o qual você deseja registrar eventos de dados.
  3. Escolha o modelo do seletor de registros que você deseja usar. Você pode registrar todos os eventos de dados do tipo de recurso, registrar todos os `readOnly` eventos, registrar todos os `writeOnly` eventos ou criar um modelo de seletor de registros personalizado para filtrar os `resources.ARN` campos `readOnlyeventName`, e.

- Para registrar eventos de dados usando o AWS CLI, configure o `--advanced-event-selectors` parâmetro para definir o `eventCategory` campo igual `Data` e o `resources.type` campo igual ao valor do tipo de recurso. Você pode adicionar condições para filtrar os valores dos `resources.ARN` campos `readOnlyeventName`, e.

  - Para configurar uma trilha para registrar eventos de dados, execute o put-event-selectorscomando. Para obter mais informações, consulte Registro de eventos de dados para trilhas com AWS CLI o.
  - 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 execute o update-event-data-storecomando para atualizar um armazenamento de dados de eventos existente. Para obter mais informações, consulte Registro de eventos de dados para armazenamentos de dados de eventos com AWS CLI o.

*Você pode configurar seletores de eventos avançados para filtrar os `resources.ARN` campos `eventNamereadOnly`, e e para registrar somente os eventos que são importantes para você. Consulte mais informações sobre esses campos em 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. Elas também são conhecidas como operações de plano de controle. 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 APIs de aplicativos web

As APIs listadas nesta seção são chamadas por Cadeia de Suprimentos AWS aplicativos em nome de usuários federados. Essas APIs não são visíveis nos CloudTrail registros e não são capturadas no documento de referência de autorização de serviço, consulte Cadeia de Suprimentos AWS.
O acesso a essas APIs é controlado por Cadeia de Suprimentos AWS aplicativos com base nas permissões de função de usuário federada. Você não deve tentar controlar o acesso a essas APIs para evitar a interrupção dos aplicativos. Cadeia de Suprimentos AWS

Perfis de usuário

As seguintes APIs são usadas 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

As seguintes APIs são usadas para criar e gerenciar fluxos e conexões de dados no data lake.

```
scn:CreateConnection
scn:CreateDataflow
scn:CreateDeleteDataByPartitionJob
scn:CreateExtractFlows
scn:CreatePresignedUrl
scn:CreateSampleParsingJob
scn:CreateSapODataConnection
scn:CreateUpdateDatasetSchemaJob
scn:DeleteConnection
scn:DeleteDataflow
scn:DeleteExtractFlows
scn:DeleteSapODataConnection
```

```
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

As seguintes APIs são usadas 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

As seguintes APIs são usadas 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

As seguintes APIs são usadas 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
```

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 **Note** Você pode criar até 10 instâncias em uma AWS conta.	10	Não
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

Obter suporte administrativo para o Cadeia de Suprimentos AWS

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

- Se você tiver uma AWS Support conta, acesse a Central de suporte, e envie um ticket.
- Abra AWS Management Console e escolha AWSCadeia e suprimentos, Suporte, Criar um caso.

É útil fornecer as seguintes informações:

- Seu AWS ID/ARN da instância da cadeia de 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
Atualização da política do 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 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.	1.º de novembro de 2023
Política AWS gerenciada atualizada	Cadeia de Suprimentos AWS atualizou a política gerenciad a para permitir que usuários federados acessem GetObject as operações PutObject e no bucket dedicado do Amazon S3 com o recurso	21 de setembro de 2023

	arn arn:aws:s3: ::aws-supply-chain-data-*.	
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 regional	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 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.