Manual do usuário

AWS IAM Identity Center

AWS IAM Identity Center: Manual do usuário

Table of Contents

O que é o IAM Identify Center?

AWS IAM Identity Center é o recomendado AWS service (Serviço da AWS) para gerenciar o acesso de usuários humanos aos AWS recursos. É um único lugar em que você pode atribuir aos usuários da força de trabalho, também conhecidos como workforce identities, acesso consistente a várias aplicações da Contas da AWS . O IAM Identity Center é oferecido sem custo adicional.

Com o IAM Identity Center, você pode criar ou conectar usuários da força de trabalho e gerenciar centralmente seu acesso em todos os aplicativos Contas da AWS . Você pode usar permissões de várias contas para atribuir acesso aos usuários da sua força de trabalho às Contas da AWS. Você pode usar as atribuições de aplicativos para atribuir aos usuários acesso a aplicativos AWS gerenciados e gerenciados pelo cliente.

> **Note**
>
> Embora o nome do serviço AWS Single Sign-On tenha sido retirado, o termo single sign-on ainda é usado neste guia para descrever o esquema de autenticação que permite que os usuários façam login uma vez para acessar vários aplicativos e sites.

Recursos do IAM Identity Center

O IAM Identity Center inclui os seguintes recursos e atributos básicos:

Gerenciar identidades da força de trabalho

Usuários humanos que criam ou operam cargas de trabalho em também AWS são conhecidos como usuários da força de trabalho ou identidades da força de trabalho. Os usuários da força de trabalho são funcionários ou prestadores de serviços que você permite acessar Contas da AWS em sua organização e em aplicativos comerciais internos. Eles podem ser as pessoas que desenvolvem os sistemas internos e os sistemas de interface com o cliente, ou usuários dos sistemas e aplicações de banco de dados internos. Você pode criar usuários e grupos da força de trabalho no IAM Identity Center ou conectar-se e sincronizar com um conjunto existente de usuários e grupos em sua própria fonte de identidade para uso em todos os seus aplicativos Contas da AWS . Para ter mais informações, consulte Gerencie sua fonte de identidade.

Gerenciar instâncias do IAM Identity Center

O IAM Identity Center é compatível com dois tipos de instâncias: instâncias de organização e instâncias de conta. Usa uma instância da organização é a prática recomendada. É a única instância que permite gerenciar o acesso Contas da AWS e é recomendada para todo o uso de aplicativos em produção. Uma instância da organização é implantada na conta AWS Organizations de gerenciamento e fornece um único ponto para gerenciar o acesso do usuário em todo o AWS ambiente.

As instâncias da conta estão vinculadas ao Conta da AWS local em que estão habilitadas. Use instâncias de conta do IAM Identity Center somente para oferecer suporte a implantações isoladas de aplicativos AWS gerenciados selecionados. Para ter mais informações, consulte Gerenciar instâncias de organização e de conta do IAM Identity Center.

Gerencie o acesso a vários Contas da AWS

Com as permissões de várias contas, você pode planejar e implementar centralmente permissões em várias Contas da AWS ao mesmo tempo, sem precisar configurar cada uma de suas contas manualmente. Você pode criar permissões refinadas com base nas funções de trabalho comuns ou definir permissões personalizadas que atendam às suas necessidades de segurança. Em seguida, você pode atribuir essas permissões aos usuários da força de trabalho para controlar o acesso a contas específicas.

Este atributo opcional só está disponível para instâncias de organização. Se você estiver usando o gerenciamento de perfis do IAM por conta em seu ambiente, os dois sistemas podem coexistir. Se quiser experimentar as permissões multicontas, você pode começar implementando esse sistema de forma limitada e, com o tempo, migrar uma porção maior do ambiente para usar esse sistema.

Gerenciar o acesso a aplicações

O IAM Identity Center permite que você simplifique o gerenciamento do acesso a aplicações. Com o IAM Identity Center, você pode conceder aos usuários da força de trabalho do IAM Identity Center acesso de logon único às aplicações.

AWS aplicativos gerenciados

AWS fornece aplicativos como Amazon Redshift Amazon Managed Grafana e Amazon Monitron, que se integram ao IAM Identity Center. Essas aplicações podem usar o IAM Identity Center para autenticação, serviços de diretório e propagação de identidades confiáveis. Os usuários usufruem de uma experiência de logon único consistente e, como as aplicações compartilham uma visão comum de usuários, grupos e associações a grupos, os

usuários também têm uma experiência consistente quando compartilham os recursos das aplicações com outras pessoas. Você pode configurar aplicativos AWS gerenciados para trabalhar com o IAM Identity Center diretamente dos consoles de aplicativos relevantes ou por meio das APIs.

Aplicações gerenciadas pelo cliente

Você pode conceder aos usuários da força de trabalho do IAM Identity Center acesso de logon único a aplicações compatíveis com federação de identidades com o SAML 2.0. Muitas aplicações SAML 2.0 usadas comumente, como o Salesforce e o Microsoft 365, funcionam com o IAM Identity Center e estão disponíveis no catálogo de aplicações no console do IAM Identity Center. Esse é um atributo opcional que pode ser útil se você usar essas aplicações e criar usuários e grupos no IAM Identity Center ou usar o Microsoft Active Directory Domain Service como fonte de identidades.

Trusted identity propagation across applications

A propagação confiável de identidade fornece uma experiência simplificada de login único para usuários de ferramentas de consulta e aplicativos de business intelligence (BI) que precisam de acesso aos dados nos serviços. AWS O gerenciamento de acesso aos dados é baseado na identidade do usuário, portanto, os administradores podem conceder acesso com base no usuário e nas associações a grupo dos usuários. O acesso do usuário aos AWS serviços e a outros eventos é registrado em registros e CloudTrail eventos específicos do serviço, para que os auditores saibam quais ações os usuários realizaram e quais recursos os usuários acessaram.

AWS acesso ao portal de acesso para seus usuários

O portal de AWS acesso é um portal web simples que fornece aos usuários acesso contínuo a todos os aplicativos Contas da AWS e atribuídos.

Renomeação do IAM Identity Center

Em 26 de julho de 2022, o AWS Single Sign-On foi renomeado para. AWS IAM Identity Center Para clientes existentes, a tabela seguinte serve para descrever algumas das mudanças de termos mais comuns que foram atualizadas ao longo deste guia como resultado da renomeação.

Termo legado	Termo atual
AWS Usuário SSO ou usuário SSO	usuário da força de trabalho ou usuário

Termo legado	Termo atual
AWS Portal do usuário SSO ou portal do usuário	AWS portal de acesso
AWS Aplicativos integrados ao SSO	AWS aplicativos gerenciados
AWS Diretório SSO	Diretório do Identity Center
AWS Armazenamento SSO ou armazenamento de AWS identidade SSO	Armazenamento de identidade pelo IAM Identity Center

A tabela a seguir descreve as alterações de nome do guia de referência de usuário, desenvolvedor e API aplicáveis que também ocorreram como resultado dessa renomeação.

Guia legado	Guia atual
AWS Guia do usuário de login único	Usuários do IAM Identity Center
AWS Guia do desenvolvedor da implement ação do SCIM de login único	Guia do desenvolvedor de implementação do IAM Identity Center SCIM
AWS Guia de referência da API de login único	Referência da API do IAM Identity Center
AWS Guia de referência da API Single Sign-On Identity Store	Referência de API do Repositório de identidad es
AWS Guia de referência da API OIDC de login único	Referência da API OIDC do IAM Identity Center
AWS Guia de referência da API do portal de login único	Referência da API do portal do IAM Identity Center

Os namespaces legados permanecem os mesmos

Os namespaces `sso` e `identitystore` da API, juntamente com os seguintes namespaces relacionados, permanecem inalterados para fins de compatibilidade com versões anteriores.

- Comandos da CLI
  - `aws configure sso`
  - `identitystore`
  - `sso`
  - `sso-admin`
  - `sso-oidc`
- Políticas gerenciadas contendo prefixos `AWSSSO` e `AWSIdentitySync`
- Endpoints de serviço contendo `sso` e `identitystore`
- Recursos AWS CloudFormation contendo prefixos `AWS::SSO`
- Função vinculada ao serviço contendo `AWSServiceRoleForSSO`
- URLs do console contendo `sso` e `singlesignon`
- URLs de documentação contendo `singlesignon`

Habilitando AWS IAM Identity Center

Conclua as etapas a seguir para fazer login AWS Management Console e habilitar uma instância organizacional do IAM Identity Center.

1. Realize um dos procedimentos a seguir para entrar no AWS Management Console.
   - Novo em AWS (usuário root) — Faça login como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.
   - Já está usando AWS (credenciais do IAM) — Faça login usando suas credenciais do IAM com permissões administrativas.
2. Abra o console do Centro de Identidade do IAM.
3. Em Habilitar o IAM Identity Center, escolha Habilitar com o AWS Organizations.
4. Opcional Adicione as tags que deseja associar a essa instância de organização.
5. Opcional Configure a administração delegada.

> **Note**
>
> Se você estiver usando um ambiente com várias contas, recomendamos que você configure a administração delegada. Com a administração delegada, você pode limitar o número de pessoas que precisam de acesso à conta de gerenciamento no AWS Organizations. Para ter mais informações, consulte Administradores delegados.

> **Important**
>
> A capacidade de criar instâncias de conta do IAM Identity Center está habilitada por padrão. As instâncias de conta do IAM Identity Center incluem um subconjunto de atributos disponíveis para uma instância de organização. Você pode controlar se os usuários podem acessar esse atributo usando uma política de controle de serviços.

Você precisa atualizar firewalls e gateways?

Se você filtrar o acesso a AWS domínios ou endpoints de URL específicos usando uma solução de filtragem de conteúdo da Web, como firewalls de próxima geração (NGFW) ou Secure Web

Gateways (SWG), deverá adicionar os seguintes domínios ou endpoints de URL às suas listas de permissões da solução de filtragem de conteúdo da web. Isso permite que você acesse seu portal de AWS acesso.

- *[Directory ID or alias]*.awsapps.com
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

Considerações sobre a lista de permissões de domínios e endpoints de URL

Entenda o impacto da lista de domínios permitidos além do portal de AWS acesso.

- Para acessar Contas da AWS o console do AWS Management Console IAM Identity Center e o console do IAM a partir do seu portal de AWS acesso, você deve incluir domínios adicionais na lista de permissões. Consulte Solução de problemas no Guia de introdução para AWS Management Console obter uma lista de AWS Management Console domínios.
- Para acessar aplicativos AWS gerenciados do seu portal de AWS acesso, você deve permitir seus respectivos domínios. Consulte a respectiva documentação de serviço para obter orientação.
- Essas listas de permissão abrangem AWS serviços. Se você usa software externo, como externo IdPs (por exemplo, Okta eMicrosoft Entra ID), precisará incluir seus domínios nas suas listas de permissões.

Agora você está pronto para configurar o IAM Identity Center. Quando você habilita o IAM Identity Center, ele é configurado automaticamente com um diretório do Identity Center como a fonte de

identidades padrão, que é o modo mais rápido de começar a usar o IAM Identity Center. Para obter instruções, consulte Configurar acesso de usuário com o diretório padrão do IAM Identity Center.

Se você quiser saber mais sobre como o IAM Identity Center trabalha com o Organizations, fontes de identidades e perfis do IAM, consulte os tópicos a seguir.

Tópicos

Pré-requisitos e considerações

Os tópicos seguintes fornecem informações sobre os pré-requisitos e outras considerações para a configuração do IAM Identity Center.

Considerações para escolher um Região da AWS

Você pode habilitar uma instância do IAM Identity Center em uma única instância compatível Região da AWS de sua escolha. A escolha de uma região exige uma avaliação de suas prioridades com base nos casos de uso e nas políticas da empresa. O acesso Contas da AWS e os aplicativos em nuvem do seu IAM Identity Center não dependem dessa escolha; no entanto, o acesso aos aplicativos AWS gerenciados e a capacidade de usá-los AWS Managed Microsoft AD como fonte de identidade podem depender dessa escolha. Consulte os endpoints e cotas do AWS IAM Identity Center no Referência geral da AWS para obter uma lista de regiões compatíveis com o IAM Identity Center.

Principais considerações para escolher um Região da AWS.

- Localização geográfica — Quando você seleciona uma região geograficamente mais próxima da maioria dos seus usuários finais, eles terão menor latência de acesso ao portal de acesso e AWS aos aplicativos AWS gerenciados, como a Amazon. SageMaker Studio
- Disponibilidade de aplicativos AWS AWS gerenciados — aplicativos gerenciados, como a Amazon SageMaker, podem operar somente nas áreas em Regiões da AWS que oferecem suporte. Ative o IAM Identity Center em uma região suportada pelo (s) aplicativo (s) AWS gerenciado (s) que você deseja usar com ele. Muitos aplicativos AWS gerenciados também podem operar somente na mesma região em que você ativou o IAM Identity Center.
- Soberania digital — Os regulamentos de soberania digital ou as políticas da empresa podem exigir o uso de um determinado. Região da AWS Consulte o departamento jurídico da sua empresa.

- Fonte de identidade — Se você estiver usando nosso AWS Managed Microsoft AD AD Connector como fonte de identidade, sua região de origem deverá corresponder à Região da AWS na qual você habilitou o IAM Identity Center.
- Regiões desativadas por padrão — AWS originalmente habilitava todas as novas Regiões da AWS para uso Contas da AWS por padrão, o que permitia automaticamente que seus usuários criassem recursos em qualquer região. Agora, ao AWS adicionar uma nova região, seu uso é desativado por padrão em todas as contas. Se você implantar o IAM Identity Center em uma região desativada por padrão, deverá habilitar essa região em todas as contas para as quais deseja gerenciar o acesso ao IAM Identity Center. Isso é necessário mesmo que você não planeje criar nenhum recurso nessa região nessas contas.

  Você pode habilitar uma região para as contas atuais em sua organização e deve repetir essa ação para novas contas que você possa adicionar posteriormente. Para obter instruções, consulte Habilitar ou desabilitar uma região em sua organização no guia AWS Organizations do usuário. Para evitar a repetição dessas etapas adicionais, você pode optar por implantar sua Central de Identidade do IAM em uma região habilitada por padrão. Para referência, as seguintes regiões estão habilitadas por padrão:

  - Leste dos EUA (Ohio)
  - Leste dos EUA (N. da Virgínia)
  - Oeste dos EUA (Oregon)
  - Oeste dos EUA (N. da Califórnia)
  - Europa (Paris)
  - América do Sul (São Paulo)
  - Ásia-Pacífico (Mumbai)
  - Europa (Estocolmo)
  - Ásia-Pacífico (Seul)
  - Ásia-Pacífico (Tóquio)
  - Europa (Irlanda)
  - Europa (Frankfurt)
  - Europa (Londres)
  - Ásia-Pacífico (Singapura)
  - Ásia-Pacífico (Sydney)
  - Canadá (Central)

  - Asia Pacific (Osaka)
- Chamadas entre regiões — Em algumas regiões, o IAM Identity Center pode ligar para o Amazon Simple Email Service em uma região diferente para enviar e-mails. Nessas chamadas entre regiões, o IAM Identity Center envia determinados atributos do usuário para a outra região. Para obter mais informações sobre regiões, consulte AWS IAM Identity Center Disponibilidade da região.

Trocando Regiões da AWS

Você só pode mudar sua região do IAM Identity Center excluindo a instância atual e criando uma nova instância em outra região. Se você já habilitou um aplicativo AWS gerenciado com sua instância existente, você deve excluí-lo primeiro antes de excluir seu IAM Identity Center. Você deve recriar usuários, grupos, conjuntos de permissões, aplicativos e exercícios na nova instância. Você pode usar a conta do IAM Identity Center e as APIs de atribuição de aplicativos para obter um instantâneo da sua configuração e, em seguida, usar esse instantâneo para reconstruir sua configuração em uma nova região. Talvez você também precise recriar algumas configurações do IAM Identity Center por meio do console de gerenciamento da sua nova instância. Para obter instruções sobre como excluir o IAM Identity Center, consulteExclua a configuração do IAM Identity Center.

Cota para funções do IAM criadas pelo IAM Identity Center

O IAM Identity Center cria perfis do IAM para dar aos usuários permissões para usar os recursos. Quando você atribui um conjunto de permissões, o IAM Identity Center cria os perfis do IAM controlados pelo IAM Identity Center correspondentes em cada conta e anexa as políticas especificadas no conjunto de permissões a esses perfis. O IAM Identity Center gerencia a função e permite que os usuários autorizados que você definiu assumam a função usando o portal de AWS acesso ou. AWS CLI Conforme você modificar o conjunto de permissões, o IAM Identity Center garantirá que as políticas e perfis do IAM correspondentes sejam devidamente atualizados.

Se você já configurou funções do IAM no seu Conta da AWS, recomendamos que verifique se sua conta está se aproximando da cota para funções do IAM. A cota padrão de perfis do IAM por conta é de 1.000 perfis. Para obter mais informações, consulte Cotas de objetos do IAM.

Se você estiver se aproximando da cota, considere solicitar um aumento de cota. Caso contrário, você poderá ter problemas com o Centro de Identidade do IAM ao provisionar conjuntos de permissões para contas que excederam a cota de perfis do IAM. Para obter informações sobre como

solicitar o aumento da cota, consulte Solicitar um aumento de cota no Guia do usuário do Service Quotas.

> **Note**
>
> Se você estiver revisando os perfis do IAM de uma conta que já está usando o IAM Identity Center, poderá notar nomes de perfil começando com “AWSReservedSSO_”. Esses são os perfis que o serviço do IAM Identity Center criou na conta e vieram da atribuição de um conjunto de permissões à conta.

Centro de identidade do IAM e AWS Organizations

AWS Organizations é recomendado, mas não obrigatório, para uso com o IAM Identity Center. Se você não configurou uma organização, não é necessário fazer isso. Ao ativar o IAM Identity Center, você escolherá se deseja ativar o serviço com AWS Organizations. Quando você configura uma organização, o Conta da AWS que configura a organização se torna a conta de gerenciamento da organização. O usuário raiz do Conta da AWS agora é o proprietário da conta de gerenciamento da organização. Todas as contas adicionais Contas da AWS que você convidar para sua organização são contas de membros. A conta de gerenciamento cria os recursos, as unidades organizacionais e as políticas da organização que gerenciam as contas-membros. As permissões são delegadas às contas-membros pela conta de gerenciamento.

> **Note**
>
> Recomendamos que você habilite o IAM Identity Center com AWS Organizations, que cria uma instância organizacional do IAM Identity Center. Uma instância de organização é a prática recomendada porque é compatível com todos os atributos do IAM Identity Center e fornece recursos de gerenciamento central. Para ter mais informações, consulte Gerenciar instâncias de organização e de conta do IAM Identity Center.

Se você já configurou AWS Organizations e vai adicionar o IAM Identity Center à sua organização, verifique se todos os AWS Organizations recursos estão habilitados. Quando você cria uma organização, a habilitação de todos os recursos é o padrão. Para obter mais informações, consulte Enabling all features in your organization no Manual do usuário do AWS Organizations .

Para habilitar o IAM Identity Center, você deve entrar no AWS Management Console fazendo login na sua conta de AWS Organizations gerenciamento como um usuário com credenciais administrativas ou como usuário raiz (não recomendado, a menos que não existam outros usuários administrativos). Você não pode ativar o IAM Identity Center enquanto estiver conectado com as credenciais administrativas de uma conta de AWS Organizations membro. Para obter mais informações, consulte Criação e gerenciamento de uma AWS organização no Guia AWS Organizations do usuário.

Confirme suas fontes de identidade no IAM Identity Center

Sua fonte de identidade no IAM Identity Center define onde seus usuários e grupos são gerenciados. Depois de habilitar o IAM Identity Center, confirme se você está usando a fonte de identidades de sua escolha.

Confirmar a fonte de identidades

1. Abra o console do Centro de Identidade do IAM.
2. Na página Painel, abaixo da seção Etapas de configuração recomendadas, escolha Confirmar sua fonte de identidade. Você também pode acessar essa página escolhendo Configurações e depois a guia Fonte de identidades.
3. Não será necessária nenhuma ação se você quiser manter sua fonte de identidades atribuída. Se você preferir alterá-la, escolha Ações e depois Alterar fonte de identidades.

   Você pode escolher uma das seguintes opções como fonte de identidade:

   Diretório do Identity Center

   Quando você habilita o IAM Identity Center pela primeira vez, ele é configurado automaticamente com um diretório do Identity Center como sua fonte de identidades padrão. Se você não estiver usando outro provedor de identidades externo, pode começar a criar os usuários e os grupos, e a definir seu nível de acesso às suas aplicações e Contas da AWS . Para obter um tutorial sobre o uso dessa fonte de identidades, consulte Configurar acesso de usuário com o diretório padrão do IAM Identity Center.

   Active Directory

   Se você já estiver gerenciando usuários e grupos em seu AWS Managed Microsoft AD diretório usando AWS Directory Service ou em seu diretório autogerenciado emActive Directory (AD), recomendamos que você conecte esse diretório ao habilitar o IAM Identity

Center. Não crie nenhum usuário ou grupo no diretório padrão do Identity Center. O IAM Identity Center usa a conexão fornecida pelo AWS Directory Service para sincronizar informações de usuário, grupo e associação do seu diretório de origem no Active Directory com o repositório de identidades do IAM Identity Center. Para ter mais informações, consulte Conectar-se a um diretório Microsoft AD.

> **Note**
>
> O IAM Identity Center não é compatível com o Simple AD baseado no SAMBA4 como fonte de identidades.

Provedores de identidade externos

Para provedores de identidade externos (IdPs), como Okta ouMicrosoft Entra ID, você pode usar o IAM Identity Center para autenticar identidades IdPs por meio do padrão Security Assertion Markup Language (SAML) 2.0. O protocolo SAML não oferece um modo de consultar o IdP para obter informações sobre usuários e grupos. Você informa o IAM Identity Center sobre esses usuários e grupos provisionando-os para o IAM Identity Center. O IAM Identity Center é compatível com o provisionamento automático (sincronização) de informações de usuários e grupos do IdP para o IAM Identity Center usando o protocolo System for Cross-domain Identity Management (SCIM) v2.0. Caso contrário, você pode provisionar manualmente os usuários e os grupos inserindo os nomes de usuário, os endereços de e-mail e os grupos no IAM Identity Center.

Para obter instruções detalhadas sobre como configurar sua fonte de identidade, consulteTutoriais de introdução.

> **Note**
>
> Se você planejar usar um provedor de identidades externo, observe que o IdP externo, não o IAM Identity Center, gerenciará as configurações de autenticação multifator (MFA). O MFA no IAM Identity Center não é suportado para uso externo. IdPs Para ter mais informações, consulte Solicite aos usuários o MFA.

A fonte de identidade que você escolhe determina onde o Centro de Identidade do IAM pesquisa usuários e grupos que precisam de acesso de login único. Após confirmar ou altear a fonte de

identidades, você criará ou especificará um usuário e atribuirá a ele permissões administrativas na sua Conta da AWS.

> **Important**
>
> Se você já gerencia usuários e grupos no Active Directory ou em um provedor de identidades (IdP) externo, recomendamos que considere conectar essa fonte de identidade ao habilitar o IAM Identity Center e escolher sua fonte de identidade. Isso deve ser feito antes de você criar qualquer usuário e grupo no diretório padrão do Identity Center e fazer qualquer atribuição. Se você já estiver gerenciando usuários e grupos em uma fonte de identidade no IAM Identity Center, mudar para uma fonte de identidade diferente pode remover todas as atribuições de usuários e grupos que você configurou no IAM Identity Center. Se isso ocorrer, todos os usuários, incluindo o usuário administrativo no IAM Identity Center, perderão o acesso de login único a seus aplicativos Contas da AWS e aplicativos. Para ter mais informações, consulte Considerações para alterar sua fonte de identidade.

Depois de configurar sua fonte de identidade, você pode pesquisar usuários ou grupos para conceder a eles acesso de login único a Contas da AWS aplicativos em nuvem ou ambos.

Tutoriais de introdução

Você só pode ter uma fonte de identidade por organização, por isso é importante dedicar um tempo a testar os recursos de cada uma delas.

Nesta seção, você pode escolher um dos tutoriais a seguir para configurar o IAM Identity Center com sua fonte de identidades preferida, criar um usuário administrativo e configurar conjuntos de permissões para conceder aos usuários acesso aos recursos.

Antes de iniciar qualquer um desses tutoriais, ative o IAM Identity Center. Para ter mais informações, consulte Habilitando AWS IAM Identity Center.

Tópicos

- Configurar acesso de usuário com o diretório padrão do IAM Identity Center
- Usar o Active Directory como uma fonte de identidades
- Setting up SCIM provisioning between CyberArk and IAM Identity Center
- Configurar SAML e SCIM com o Google Workspace e o IAM Identity Center
- Usar o IAM Identity Center para conectar com a plataforma de diretórios do JumpCloud
- Configurar SAML e SCIM com o Microsoft Entra ID e o IAM Identity Center
- Configurar SAML e SCIM com o Okta e o IAM Identity Center
- Configurar o provisionamento SCIM entre o OneLogin e o IAM Identity Center
- Usar produtos de Ping Identity com o IAM Identity Center

Configurar acesso de usuário com o diretório padrão do IAM Identity Center

Quando você habilita o IAM Identity Center pela primeira vez, ele é configurado automaticamente com um diretório do Identity Center como sua fonte de identidades padrão, portanto não é necessário escolher uma fonte de identidades. Se sua organização usa outro provedor de identidade AWS Directory Service for Microsoft Active Directory, como,Microsoft Entra ID, ou Okta considere integrar essa fonte de identidade com o IAM Identity Center em vez de usar a configuração padrão.

Objetivo

Neste tutorial, você usará o diretório padrão como fonte de identidades e configurará e testará o acesso do usuário. Nesse cenário, você gerencia todos os usuários e grupos do IAM Identity Center. Os usuários fazem login por meio do portal de AWS acesso. Este tutorial é destinado a usuários iniciantes AWS ou que já estão usando o IAM para gerenciar usuários e grupos. Nas próximas etapas, você criará o seguinte:

- Um usuário administrativo chamado *Nikki Wolf*
- Um grupo chamado *Equipe de administração*
- Um conjunto de permissões chamado *AdminAccess*

Para verificar se tudo foi criado corretamente, você fará login e definirá a senha do usuário administrativo. Depois de concluir este tutorial, você pode usar o usuário administrativo para adicionar mais usuários ao IAM Identity Center, criar conjuntos de permissões adicionais e configurar o acesso organizacional às aplicações.

Se você ainda não habilitou o IAM Identity Center, consulte Habilitando AWS IAM Identity Center.

Antes de começar

Realize um dos procedimentos a seguir para entrar no AWS Management Console.

- Novo em AWS (usuário root) — Faça login como proprietário da conta escolhendo o usuário Conta da AWS root e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.
- Já está usando AWS (credenciais do IAM) — Faça login usando suas credenciais do IAM com permissões administrativas.

Abra o console do Centro de Identidade do IAM.

Etapa 1: adicionar um usuário

1. No painel de navegação do IAM Identity Center, escolha Usuários e selecione Adicionar usuário.
2. Na página Especar detalhes do usuário, preencha as seguintes informações:
   - Nome de usuário: para este tutorial, insira *nikkiw*.

Ao criar usuários, escolha nomes de usuário fáceis de lembrar. Os usuários devem lembrar o nome de usuário para fazer login no Portal de acesso do AWS e você não pode alterá-lo posteriormente.

- Senha: escolha Enviar um e-mail para este usuário com instruções de configuração de senha (recomendado).

  Essa opção envia ao usuário um endereço de e-mail da Amazon Web Services, com a linha de assunto Convite para ingressar no IAM Identity Center (sucessor do AWS Single Sign-On). O e-mail vem de `no-reply@signin.aws` ou de `no-reply@login.awsapps.com`. Adicione esses endereços de e-mail à sua lista de remetentes aprovados.
- Endereço de e-mail: insira um endereço de e-mail para o usuário no qual você possa receber o e-mail. Em seguida, insira-o novamente para confirmar. Cada usuário deve ter um endereço de e-mail exclusivo.
- Nome: insira o nome do usuário. Para este tutorial, insira *`Nikki`*.
- Sobrenome: insira o sobrenome do usuário. Para este tutorial, insira *`Wolf`*.
- Nome de exibição: o valor padrão é nome e sobrenome do usuário. Se quiser alterar o nome de exibição, você pode inserir algo diferente. O nome de exibição é visível no portal de login e na lista de usuários.
- Preencha as informações opcionais, se desejar. Elas não são usadas durante este tutorial e você pode alterá-las posteriormente.

3. Escolha Próximo. A página Adicionar usuário a grupos é exibida. Nós vamos criar um grupo ao qual atribuir permissões administrativas em vez de concedê-las diretamente a *`Nikki`*.

   Escolha Criar grupo.

   Uma nova guia do navegador é aberta para exibir a página Criar grupo.

   a. Em Detalhes do grupo, em Nome do grupo, insira um nome para o grupo. Recomendamos um nome de grupo que identifique a função do grupo. Para este tutorial, insira *`Equipe de administração`*.

   b. Escolha Criar grupo.

   c. Feche a guia Grupos do navegador para retornar à guia Adicionar usuário do navegador

4. Na área Grupos, selecione o botão Atualizar. O grupo *`Equipe de administração`* aparece na lista.

Marque a caixa de seleção ao lado de *Equipe de administração* e escolha Avançar.

5. Na página Revisar e adicionar usuário, confirme o seguinte:

   - As informações primárias aparecem como você pretendia
   - Grupos mostra o usuário adicionado ao grupo que você criou

   Se precisar fazer alterações, escolha Editar. Quando todos os detalhes estiverem corretos, escolha Adicionar usuário.

   Uma mensagem notifica você de que o usuário foi adicionado.

Em seguida, você adicionará permissões administrativas para o grupo *Equipe de administração* para que *Nikki* tenha acesso aos recursos.

Etapa 2: adicionar permissões administrativas

1. No painel de navegação do IAM Identity Center, em Permissões multicontas, escolha Contas da AWS.
2. Na página Contas da AWS, a Estrutura organizacional exibe a organização com as contas abaixo dela na hierarquia. Marque a caixa de seleção da sua conta de gerenciamento e selecione Atribuir usuários ou grupos.
3. O fluxo de trabalho Atribuir usuários e grupos é exibido. Ele consiste em três etapas:

   a. Em Etapa 1: selecionar usuários e grupos, escolha o grupo *Equipe de administração* que você criou. Em seguida, escolha Próximo.

   b. Em Etapa 2: selecionar conjuntos de permissões, escolha Criar conjunto de permissões para abrir uma nova guia que orienta você pelas três subetapas envolvidas na criação de um conjunto de permissões.

      i. Em Etapa 1: selecionar o tipo de conjunto de permissões, preencha o seguinte:

         - Em Tipo de conjunto de permissões, escolha Conjunto de permissões predefinido.
         - Em Política para conjunto de permissões predefinido, escolha AdministratorAccess.

         Escolha Próximo.

ii. Em Etapa 2: especificar detalhes do conjunto de permissões, mantenha as configurações padrão e escolha Avançar.

As configurações padrão criam um conjunto de permissões chamado *AdministratorAccess*com a duração da sessão definida em uma hora. Você pode alterar o nome do conjunto de permissões inserindo um novo nome no campo Nome do conjunto de permissões.

iii. Para a Etapa 3: revisar e criar, verifique se o tipo de conjunto de permissões usa a política AWS gerenciada AdministratorAccess. Escolha Criar. Na página Conjuntos de permissões, aparece uma notificação informando que o conjunto de permissões foi criado. Você agora pode fechar essa guia do navegador.

Na guia Atribuir usuários e grupos do navegador, você ainda está na Etapa 2: selecionar conjuntos de permissões na qual você iniciou o fluxo de trabalho de criação do conjunto de permissões.

Na área Conjuntos de permissões, escolha o botão Atualizar. O conjunto de *AdministratorAccess*permissões que você criou aparece na lista. Marque a caixa de seleção desse conjunto de permissões e escolha Avançar.

c. Na página Etapa 3: revisar e enviar exercícios, confirme se o grupo da *equipe de administradores* está selecionado e se o conjunto de *AdministratorAccess*permissões está selecionado e, em seguida, escolha Enviar.

A página é atualizada com uma mensagem informando que a sua Conta da AWS está sendo configurada. Aguarde a conclusão do processo.

Você retornará à Contas da AWS página. Uma mensagem de notificação informa que a sua Conta da AWS foi reprovisionada e que o conjunto de permissões atualizado foi aplicado.

> Parabéns!
>
> Você configurou com sucesso seu primeiro usuário, grupo e conjunto de permissões.

Na próxima parte deste tutorial, você testará o acesso *de Nikki* entrando no portal de AWS acesso com suas credenciais administrativas e definindo sua senha. Saia do console agora.

Etapa 3: Testar o acesso do usuário

Agora que *Nikki Wolf* é um usuário da organização, ela pode fazer login e acessar os recursos para os quais recebeu permissão de acordo com seu conjunto de permissões. Para verificar se o usuário está configurado corretamente, na próxima etapa, você usará as credenciais *de Nikki* para fazer login e configurar a senha dela. Ao adicionar o usuário *Nikki Wolf* na etapa 1, você optou por fazer com que *Nikki* recebesse um e-mail com instruções de configuração de senha. É hora de abrir esse e-mail e fazer o seguinte:

1. No e-mail, selecione o link Aceitar convite para aceitar o convite.

   > **Note**
   >
   > O e-mail também inclui o nome de usuário de *Nikki* e o URL do Portal de acesso do AWS que ela usará para fazer login na organização. Registre essas informações para uso futuro.

   Você é levado para a página Inscrição de novo usuário onde pode definir a senha de *Nikki*.
2. Depois de definir a senha de *Nikki*, você será direcionado para a página Fazer login. Insira *nikkiw* e escolha Avançar, depois insira senha de *Nikki* e escolha Fazer login.
3. O portal de AWS acesso é aberto exibindo a organização e os aplicativos que você pode acessar.

   Selecione a organização para expandi-la em uma lista e, em Contas da AWS seguida, selecione a conta para exibir as funções que você pode usar para acessar os recursos na conta.

   Cada conjunto de permissões tem dois métodos de gerenciamento que você pode usar, chaves de função ou de acesso.

   - Função, por exemplo *AdministratorAccess*- Abre AWS Console Home o.
   - Chaves de acesso: fornecem credenciais que você pode usar com o AWS CLI ou e o AWS SDK. Inclui as informações para usar credenciais de curto prazo que são atualizadas automaticamente ou chaves de acesso de curto prazo. Para ter mais informações, consulte Obter credenciais de usuário do IAM Identity Center para o AWS CLI ou AWS SDKs.
4. Escolha o link Função para fazer login no AWS Console Home.

Você está conectado e navegou até a AWS Console Home página. Explore o console e confirme se você tem o acesso esperado.

Próximas etapas

Agora que você criou um usuário administrativo no IAM Identity Center, você pode:

- Atribuir uma aplicação
- Adicionar outros usuários
- Atribuir usuários a contas
- Configurar conjuntos de permissões adicionais

> **Note**
>
> Você também pode atribuir vários conjuntos de permissões ao mesmo usuário. Para seguir as melhores práticas de aplicar permissões com privilégio mínimo, após criar seu usuário administrativo, crie um conjunto de permissões mais restritivo e atribua-o ao mesmo usuário. Dessa forma, você pode acessar o seu Conta da AWS com apenas as permissões necessárias, em vez de permissões administrativas.

Depois que seus usuários aceitarem o convite para ativar sua conta e entrarem no portal de AWS acesso, os únicos itens que aparecem no portal são para as Contas da AWS funções e os aplicativos aos quais estão atribuídos.

> **Important**
>
> Recomendamos muito que você habilite a autenticação multifator (MFA) para os seus usuários. Para ter mais informações, consulte Autenticação multifator para usuários do Identity Center.

Usar o Active Directory como uma fonte de identidades

Se estiver gerenciando usuários no diretório do AWS Managed Microsoft AD usando o AWS Directory Service ou em seu diretório autogerenciado no Active Directory (AD), você poderá alterar sua fonte de identidades do IAM Identity Center para trabalhar com esses usuários. Recomendamos

que você considere conectar essa fonte de identidades quando habilitar o IAM Identity Center e escolher a fonte de identidade. Fazer isso antes de criar qualquer usuário e grupo no diretório padrão do Centro de Identidade ajudará a evitar a configuração adicional necessária se você alterar sua fonte de identidade posteriormente.

Se você quiser usar o Active Directory como a fonte de identidades, a configuração deverá atender aos seguintes pré-requisitos:

- Se você estiver usando o AWS Managed Microsoft AD, deve habilitar o Centro de Identidade do IAM na mesma Região da AWS em que seu diretório AWS Managed Microsoft AD estiver configurado. O Centro de Identidade do IAM armazena os dados de atribuição na mesma região do diretório. Para administrar o Centro de Identidade do IAM, talvez seja necessário mudar para a região em que ele estiver configurado. Além disso, observe que o portal de acesso da AWS usa o mesmo URL de acesso que o diretório.
- Use um Active Directory residente na conta de gerenciamento:

  Você deve ter um AD Connector ou um diretório do AWS Managed Microsoft AD configurado no AWS Directory Service e residente na conta de gerenciamento do AWS Organizations. Você pode conectar somente um diretório do AD Connector ou um diretório por AWS Managed Microsoft AD vez. Se você precisar oferecer suporte a vários domínios ou florestas, use AWS Managed Microsoft AD. Para obter mais informações, consulte:

  - Conecte um diretório AWS Managed Microsoft AD ao IAM Identity Center
  - Conecte um diretório autogerenciado no Active Directory ao IAM Identity Center
- Use um Active Directory residente na conta do administrador delegado:

  Se você planejar habilitar o administrador delegado do IAM Identity Center e usar o Active Directory como a fonte de identidades do IAM Identity Center, poderá usar um AD Connector ou diretório do AWS Managed Microsoft AD existente configurado no AWS Directory residente na conta do administrador delegado.

  Se você decidir alterar a fonte de identidade do IAM Identity Center de qualquer outra fonte para o Active Directory ou alterá-la do Active Directory para qualquer outra fonte, o diretório deverá residir (pertencer à) conta de membro do administrador delegado do IAM Identity Center, se houver; caso contrário, deverá estar na conta de gerenciamento.

Este tutorial orienta você na configuração básica para usar o Active Directory como uma fonte de identidades do IAM Identity Center.

Etapa 1: conectar o Active Directory ou outro IdP e especificar um usuário

Se já estiver usando o Active Directory, os tópicos a seguir ajudarão você a conectar o diretório ao IAM Identity Center.

> **Note**
>
> Como uma prática recomendada de segurança, habilite a autenticação multifator. Se você planeja conectar um diretório AWS Managed Microsoft AD ou um diretório autogerenciado no Active Directory e não está usando o RADIUS MFA com o AWS Directory Service, habilite a MFA no Centro de Identidade do IAM.

AWS Managed Microsoft AD

1. Revise as orientações em Conectar-se a um diretório Microsoft AD.
2. Siga as etapas em Conecte um diretório AWS Managed Microsoft AD ao IAM Identity Center.
3. Configure o Active Directory para sincronizar o usuário ao qual você deseja conceder permissões administrativas no IAM Identity Center. Para obter mais informações, consulte Sincronizar um usuário administrativo para o IAM Identity Center.

Diretório autogerenciado no Active Directory

1. Revise as orientações em Conectar-se a um diretório Microsoft AD.
2. Siga as etapas em Conecte um diretório autogerenciado no Active Directory ao IAM Identity Center.
3. Configure o Active Directory para sincronizar o usuário ao qual você deseja conceder permissões administrativas no IAM Identity Center. Para obter mais informações, consulte Sincronizar um usuário administrativo para o IAM Identity Center.

Etapa 2: sincronizar um usuário administrativo com o IAM Identity Center

Depois de conectar seu diretório ao Centro de Identidade do IAM, você pode especificar um usuário ao qual deseja conceder permissões administrativas e, em seguida, sincronizá-lo do seu diretório com o Centro de Identidade do IAM.

1. Abra o console do Centro de Identidade do IAM.

2. Escolha Settings.
3. Na página Configurações, escolha a guia Origem da identidade, escolha Ações e, em seguida, Gerenciar sincronização.
4. Na página Gerenciar sincronização , escolha a guia Usuários e Adicionar usuários e grupos.
5. Na guia Usuários, em Usuário, insira o nome do usuário exato e escolha Adicionar.
6. Em Usuários e grupos adicionados, faça o seguinte:
    a. Confirme se o usuário para o qual você deseja conceder permissões administrativas foi especificado.
    b. Marque a caixa de seleção à esquerda do nome do usuário.
    c. Selecione Enviar.
7. Na página Gerenciar sincronização, o usuário que você especificou aparece na lista Usuários no escopo de sincronização.
8. No painel de navegação, escolha Users.
9. Na página Usuários, pode levar algum tempo para que o usuário que você especificou apareça na lista. Escolha o ícone de atualização para atualizar a lista de usuários.

Neste momento, seu usuário não tem acesso à conta de gerenciamento. Você configurará o acesso administrativo a essa conta criando um conjunto de permissões administrativas e atribuindo o usuário a esse conjunto de permissões. Para obter mais informações, consulte Criar um conjunto de permissões.

Setting up SCIM provisioning between CyberArk and IAM Identity Center

O IAM Identity Center oferece suporte ao provisionamento automático (sincronização) das informações do usuário a partir CyberArk Directory Platform para o IAM Identity Center. Esse provisionamento usa o protocolo System for Cross-domain Identity Management (SCIM) v2.0. Você configura essa conexão no CyberArk usando seu endpoint e token de acesso do IAM Identity Center SCIM. Ao configurar a sincronização do SCIM, você cria um mapeamento dos atributos do usuário no CyberArk para os atributos nomeados no IAM Identity Center. Isso faz com que os atributos esperados correspondam entre o IAM Identity Center e CyberArk.

Este guia é baseado no CyberArk em agosto de 2021. As etapas para versões mais recentes podem variar. Este guia contém algumas notas sobre a configuração da autenticação do usuário por meio do SAML.

> **Note**
>
> Antes de começar a implantar o SCIM, é recomendável que você analise Considerações sobre o uso do provisionamento automático antes. Em seguida, continue analisando considerações adicionais na próxima seção.

Tópicos

Pré-requisitos

Você precisará do seguinte antes de começar:

- Assinatura ou teste gratuito do CyberArk. Para se inscrever para um teste gratuito, acesse CyberArk.
- Uma conta habilitada para o IAM Identity Center (gratuita). Para obter mais informações, consulte Habilitar o IAM Identity Center.
- Uma conexão SAML da sua conta do CyberArk com o IAM Identity Center, conforme descrito na documentação do CyberArk do IAM Identity Center.
- Associe o conector do IAM Identity Center às funções, usuários e organizações às quais você deseja permitir acesso a Contas da AWS.

Considerações SCIM

As seguintes considerações devem ser observadas ao usar a federação do CyberArk para o IAM Identity Center:

- Somente as funções mapeadas na seção Provisionamento do aplicativo serão sincronizadas com o IAM Identity Center.
- O script de provisionamento é suportado somente em seu estado padrão. Uma vez alterado, o provisionamento do SCIM pode falhar.
  - Somente um atributo de número de telefone pode ser sincronizado e o padrão é “telefone comercial”.
- Se o mapeamento de funções no aplicativo IAM Identity Center do CyberArk for alterado, o comportamento abaixo é esperado:
  - Se os nomes das funções forem alterados, não haverá alterações nos nomes dos grupos no IAM Identity Center.
  - Se os nomes dos grupos forem alterados, novos grupos serão criados no IAM Identity Center, os grupos antigos permanecerão, mas não terão membros.
- O comportamento de sincronização e desprovisionamento do usuário pode ser configurado a partir do aplicativo IAM Identity Center do CyberArk. Certifique-se de configurar o comportamento certo para sua organização. Estas são as opções que você tem:
  - Substitua (ou não) usuários no diretório do Identity Center com o mesmo nome de entidade principal.
  - Desprovisione usuários do IAM Identity Center quando o usuário for removido da função CyberArk.
  - Desprovisione o comportamento do usuário – desative ou exclua.

Etapa 1: Habilitar provisionamento no IAM Identity Center

Nesta primeira etapa, você usa o console do IAM Identity Center para ativar o provisionamento automático.

Para habilitar o provisionamento automático no IAM Identity Center

1. Depois de concluir os pré-requisitos, abra o console do IAM Identity Center.
2. Escolha Configurações no painel de navegação à esquerda.

3. Na página Configurações, localize a caixa de informações Provisionamento automático e selecione Habilitar. Isso habilita imediatamente o provisionamento automático no IAM Identity Center e exibe as informações necessárias do endpoint SCIM e do token de acesso.
4. Na caixa de diálogo Provisionamento automático de entrada, copie cada um dos valores para as opções a seguir. Você precisará colá-los posteriormente ao configurar o provisionamento em seu IdP.

    a. Endpoint do SCIM

    b. Token de acesso
5. Escolha Fechar.

Agora que você configurou o provisionamento no console do IAM Identity Center, precisa concluir as tarefas restantes usando o aplicativo IAM Identity Center do CyberArk. Essas etapas são descritas no procedimento a seguir.

Etapa 2: Configure o provisionamento no CyberArk

Use o procedimento a seguir no aplicativo IAM Identity Center do CyberArk para habilitar o provisionamento com o IAM Identity Center. Esse procedimento pressupõe que você já tenha adicionado o aplicativo IAM Identity Center do CyberArk ao seu console de administração do CyberArk em Aplicativos Web. Se você ainda não tiver feito isso, consulte Pré-requisitos e, em seguida, conclua este procedimento para configurar o provisionamento do SCIM.

Para configurar o provisionamento no CyberArk

1. Abra o aplicativo IAM Identity Center do CyberArk que você adicionou como parte da configuração do SAML para o CyberArk (Aplicativos > Aplicativo Web). Consulte Pré-requisitos.
2. Escolha o aplicativo IAM Identity Center e vá para a seção Provisionamento.
3. Marque a caixa Ativar provisionamento para este aplicativo e escolha Modo em tempo real.
4. No procedimento anterior, você copiou o valor do endpoint SCIM do IAM Identity Center. Cole esse valor no campo URL do serviço SCIM, no aplicativo CyberArk IAM Identity Center, defina o Tipo de autorização como Cabeçalho de autorização. Certifique-se de remover a barra final no final do URL.
5. Defina o Tipo de cabeçalho como Token do portador.
6. No procedimento anterior, você copiou o valor do Token de acesso do IAM Identity Center. Cole esse valor no campo Token do portador no aplicativo IAM Identity Center do CyberArk.

7. Clique em Verificar para testar e aplicar a configuração.
8. Em Opções de sincronização, escolha o comportamento correto para o qual você deseja que o provisionamento de saída do CyberArk funcione. Você pode optar por substituir (ou não) os usuários existentes do IAM Identity Center por um nome de entidade principal semelhante e pelo comportamento de desprovisionamento.
9. Em Mapeamento de funções, configure o mapeamento das funções do CyberArk, no campo Nome, para o grupo do IAM Identity Center, no Grupo de destino.
10. Clique em Salvar na parte inferior quando terminar.
11. Para verificar se os usuários foram sincronizados com sucesso com o IAM Identity Center, retorne ao console do IAM Identity Center e escolha Usuários. Os usuários sincronizados do CyberArk aparecerão na página Usuários. Agora, esses usuários podem ser atribuídos a contas e se conectar ao IAM Identity Center.

(Opcional) Etapa 3: Configure os atributos do usuário CyberArk para controle de acesso (ABAC) no IAM Identity Center

Esse é um procedimento opcional CyberArk caso você opte por configurar atributos para o IAM Identity Center gerenciar o acesso aos seus AWS recursos. Os atributos que você define no CyberArk são passados em uma declaração de SAML para o IAM Identity Center. Em seguida, você cria um conjunto de permissões no IAM Identity Center para gerenciar o acesso com base nos atributos dos quais você passou do CyberArk.

Antes de iniciar este procedimento, você deve primeiro habilitar o atributo Atributos para controle de acesso. Para obter mais informações sobre como fazer isso, consulte Habilite e configure atributos para controle de acesso.

Para configurar atributos do usuário emCyberArk para controle de acesso no IAM Identity Center

1. Abra o aplicativo IAM Identity Center do CyberArk que você instalou como parte da configuração do SAML para o CyberArk (Aplicativos > Aplicativo Web).
2. Acesse a opção Resposta SAML.
3. Em Atributos, adicione os atributos relevantes à tabela seguindo a lógica abaixo:

    a. Nome do atributo é o nome do atributo original do CyberArk.

    b. O Valor do atributo é o nome do atributo enviado na declaração SAML para o IAM Identity Center.

4. Escolha Salvar.

(Opcional) Passar atributos para controle de acesso

Opcionalmente, você pode usar o atributo Atributos para controle de acesso no IAM Identity Center para passar um elemento `Attribute` com o atributo `Name` definido como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento permite que você passe atributos como tags de sessão na declaração do SAML. Para obter mais informações sobre tags de sessão, consulte Passar tags de sessão AWS STS no Guia de usuário do IAM.

Para passar atributos como tags de sessão, inclua o elemento `AttributeValue` que especifica o valor da tag. Por exemplo, para passar o par chave-valor de tag `CostCenter = blue`, use o atributo a seguir.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se você precisar adicionar vários atributos, inclua um elemento separado `Attribute` para cada tag.

Configurar SAML e SCIM com o Google Workspace e o IAM Identity Center

Se sua organização estiver usando, Google Workspace você pode integrar seus usuários e grupos Google Workspace no IAM Identity Center para dar a eles acesso aos AWS recursos. Você pode obter essa integração alterando sua fonte de identidade do IAM Identity Center da fonte de identidade padrão do IAM Identity Center paraGoogle Workspace.

As informações dos usuários do Google Workspace são sincronizados com o IAM Identity Center usando o protocolo System for Cross-domain Identity Management (SCIM) v2.0. Você configura essa conexão no Google Workspace usando o endpoint SCIM para o IAM Identity Center e um token ao portador do IAM Identity Center. Ao configurar a sincronização do SCIM, você cria um mapeamento dos atributos do usuário no Google Workspace para os atributos nomeados no IAM Identity Center. Esse mapeamento faz a correspondência dos atributos de usuário esperados entre o IAM Identity

Center e o Google Workspace. Para fazer isso, você precisa configurar o Google Workspace como um provedor de identidades do IAM e um provedor de identidades do IAM Identity Center.

Objetivo

As etapas deste tutorial ajudam você a estabelecer a conexão SAML entre Google Workspace e. AWS Posteriormente, você sincronizará os usuários do Google Workspace usando o SCIM. Para verificar se tudo está configurado corretamente, depois de concluir as etapas de configuração, você fará login como Google Workspace usuário e verificará o acesso aos AWS recursos. Observe que este tutorial é baseado em um ambiente de teste de um pequeno diretório do Google Workspace. As estruturas do diretório, como grupos e unidades organizacionais, não estão incluídas. Depois de concluir este tutorial, seus usuários poderão acessar o portal de AWS acesso com suas Google Workspace credenciais.

> **Note**
>
> Para se cadastrar para fazer um teste gratuito do Google Workspace, visite Google Workspace no site da Goggle.
> Se você ainda não habilitou o IAM Identity Center, consulte Habilitando AWS IAM Identity Center.

Considerações

- Antes de configurar o provisionamento do SCIM entre Google Workspace e o IAM Identity Center, recomendamos que você primeiro analise. Considerações sobre o uso do provisionamento automático
- Atualmente, a sincronização automática do SCIM Google Workspace está limitada ao provisionamento de usuários. O aprovisionamento automático de grupos não é suportado no momento. Os grupos podem ser criados manualmente com o comando create-group ou a API AWS Identity and Access Management (IAM) do AWS CLI Identity Store. CreateGroup Como alternativa, você pode usar o ssosync para sincronizar Google Workspace usuários e grupos no IAM Identity Center.
- Todo usuário do Google Workspace deve ter um valor especificado de Nome, Sobrenome, Nome de usuário e Nome de exibição.
- Todo usuário do Google Workspace tem apenas um valor por atributo de dados, como endereço de e-mail ou número de telefone. Qualquer usuário que tenha vários valores não conseguirá

sincronizar. Se houver usuários com vários valores em seus atributos, remova os atributos duplicados antes de tentar provisionar o usuário no IAM Identity Center. Por exemplo, somente um único atributo de número de telefone pode ser sincronizado, já que o atributo de número de telefone padrão é "telefone comercial", use o atributo "telefone comercial" para armazenar o número de telefone do usuário, mesmo que o telefone do usuário seja residencial ou celular.

- Os atributos ainda serão sincronizados se o usuário estiver desativado no IAM Identity Center, mas ainda estiver ativo no Google Workspace.
- Se houver um usuário existente no diretório do Identity Center com o mesmo nome de usuário e e-mail, o usuário será sobrescrito e sincronizado usando o SCIM de. Google Workspace
- Há considerações adicionais ao alterar sua fonte de identidade. Para ter mais informações, consulte the section called “Mudar do IAM Identity Center para um IdP externo”.

Etapa 1Google Workspace: Configurar o aplicativo SAML

1. Faça login no GoogleAdmin Console usando uma conta com privilégios de superadministrador.
2. No painel de navegação esquerdo do GoogleAdmin Console, escolha Aplicativos e, em seguida, escolha Aplicativos Web e Móveis.
3. Na lista suspensa Adicionar aplicativo, selecione Pesquisar aplicativos.
4. Na caixa de pesquisa, insira Amazon Web Services e selecione o aplicativo Amazon Web Services (SAML) na lista.
5. Na página Detalhes do provedor de Google identidade - Amazon Web Services, você pode fazer o seguinte:

   a. Baixe os metadados do IdP.

   b. Copie o URL do SSO, o URL do ID da entidade e as informações do certificado.

   Você precisará do arquivo XML ou das informações do URL na Etapa 2.
6. Antes de passar para a próxima etapa no Google Admin Console, deixe essa página aberta e vá para o console do IAM Identity Center.

Etapa 2: Centro de Identidade do IAM eGoogle Workspace: Alterar a fonte de identidade do IAM Identity Center e a configuração Google Workspace como um provedor de identidade SAML

1. Faça login no console do IAM Identity Center usando uma função com permissões administrativas.
2. Escolha Configurações no painel de navegação à esquerda.
3. Na página Configurações, escolha Ações e depois Alterar fonte de identidades.

   - Se você não ativou o IAM Identity Center, consulte Habilitar o IAM Identity Center para obter mais informações. Depois de ativar e acessar o IAM Identity Center pela primeira vez, você chegará ao painel onde poderá selecionar Escolha sua fonte de identidade.
4. Em Escolher fonte de identidades, selecione Provedor de identidades externo e escolha Avançar.
5. A página Configurar provedor de identidades externo é aberta. Para concluir esta página e a Google Workspace página na Etapa 1, você precisará concluir o seguinte:

   - Na seção de metadados do provedor de identidade no console do IAM Identity Center, você precisará fazer o seguinte:

     i. Faça upload dos metadados do GoogleSAML como metadados do IdP SAML no console do IAM Identity Center.

     ii. Copie e cole o URL do GoogleSSO no campo URL de login do IdP Google, o URL do emissor no campo URL do emissor do IdP e faça o upload do certificado como o certificado do IdP. Google
6. Depois de fornecer os Google metadados na seção de metadados do provedor de identidade do console do IAM Identity Center, copie o URL de login do portal de AWS acesso, o URL do IAM Identity Assertion Consumer Service (ACS) e o URL do emissor do IAM Identity Center. Você precisará fornecer esses URLs no Google Admin Console na próxima etapa.
7. Deixe a página aberta com o console do IAM Identity Center e retorne ao Google Admin Console. Você deve estar na página de detalhes do Amazon Web Services - Service Provider. Selecione Continuar.
8. Na página de detalhes do provedor de serviços, insira os valores de URL do ACS, ID da entidade e URL inicial. Você copiou esses valores na etapa anterior e eles podem ser encontrados no console do IAM Identity Center.

- Cole o URL do IAM Identity Center Assertion Consumer Service (ACS) no campo URL do ACS
- Cole o URL do emissor do IAM Identity Center no campo ID da entidade.
- Cole a URL de login do portal de AWS acesso no campo URL inicial.

9. Na página de detalhes do provedor de serviços, preencha os campos em ID do nome da seguinte forma:
   - Em Formato do ID do nome, selecione EMAIL
   - Em ID do nome, selecione Informações básicas > E-mail principal
10. Escolha Continuar.
11. Na página Mapeamento de atributos, em Atributos, escolha ADICIONAR MAPEAMENTO e configure esses campos em Atributo Google do diretório:
    - Para o atributo do **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`** aplicativo, selecione o campo Informações básicas, E-mail principal nos Google Directoryatributos.
    - Para o atributo do **`https://aws.amazon.com/SAML/Attributes/Role`** aplicativo, selecione qualquer Google Directoryatributo. Um atributo de Google diretório pode ser Departamento.
12. Escolha Concluir
13. Volte para o console do IAM Identity Center e escolha Avançar. Na página Revisar e confirmar, revise as informações e digite ACEITAR no espaço fornecido. Escolha Alterar origem de identidade.

Agora você está pronto para habilitar o aplicativo Amazon Web Services Google Workspace para que seus usuários possam ser provisionados no IAM Identity Center.

Etapa 3Google Workspace: ativar os aplicativos

1. Retorne ao GoogleAdmin Console e ao seu AWS IAM Identity Center aplicativo, que podem ser encontrados em Aplicativos e Aplicativos Web e Móveis.
2. No painel de acesso do usuário ao lado de Acesso do usuário, escolha a seta para baixo para expandir Acesso do usuário e exibir o painel Status do serviço.
3. No painel Status do serviço, escolha ATIVADO para todos e escolha SALVAR.

> **Note**
>
> Para ajudar a manter o princípio do privilégio mínimo, recomendamos que, após concluir este tutorial, você altere o status do serviço para DESLIGADO para todos. Somente usuários que precisam acessar AWS devem ter o serviço ativado. Você pode usar os grupos ou as unidades organizacionais do Google Workspace para conceder acesso de usuário a um subconjunto específico de usuários.

Etapa 4: IAM Identity Center: configurar o provisionamento automático do IAM Identity Center

1. Volte para o console do IAM Identity Center.
2. Na página Configurações, localize a caixa de informações Provisionamento automático e selecione Habilitar. Isso habilita imediatamente o provisionamento automático no IAM Identity Center e exibe as informações necessárias do endpoint SCIM e do token de acesso.
3. Na caixa de diálogo Provisionamento automático de entrada, copie cada um dos valores para as opções a seguir. Na Etapa 5 deste tutorial, você inserirá esses valores para configurar o provisionamento automático. Google Workspace

   - Endpoint do SCIM
   - Token de acesso

   > **Warning**
   >
   > Essa é a única vez em que você pode obter o endpoint e o token de acesso do SCIM. Certifique-se de copiar esses valores antes de prosseguir.

4. Escolha Fechar.

   Agora que você configurou o provisionamento no console do IAM Identity Center, na próxima etapa, você configurará o provisionamento automático em. Google Workspace

Etapa 5Google Workspace: Configurar o provisionamento automático

1. Retorne ao Google Admin Console e ao seu AWS IAM Identity Center aplicativo, que podem ser encontrados em Aplicativos e Aplicativos Web e Móveis. Na seção Provisionamento automático, escolha Configurar provisionamento automático.
2. No procedimento anterior, você copiou o valor do token de acesso no console do IAM Identity Center. Cole esse valor no campo Token de acesso e escolha Continuar. Além disso, no procedimento anterior, você copiou o valor do endpoint do SCIM no console do IAM Identity Center. Cole esse valor no campo URL do endpoint. Certifique-se de remover a barra no final do URL e escolha Continuar.
3. Verifique se todos os atributos obrigatórios do IAM Identity Center (os que estão marcados com *) estão mapeados para os atributos do Google Cloud Directory. Caso contrário, escolha a seta para baixo e mapeie para o atributo apropriado. Escolha Continuar.
4. Na seção Escopo de provisionamento, você pode escolher um grupo com seu Google Workspace diretório para fornecer acesso ao aplicativo Amazon Web Services. Pule esta etapa e selecione Continuar.
5. Na seção Desprovisionamento, você pode escolher como responder a diferentes eventos que removem o acesso de um usuário. Para cada situação, você pode especificar a quantidade de tempo antes do início do desprovisionamento como:

   - 24 horas
   - 1 dia
   - 7 dias
   - depois de 30 dias

   Cada situação tem uma configuração de tempo para quando suspender o acesso de uma conta e para quando excluir a conta.

   > **Tip**
   >
   > Sempre defina mais tempo para excluir uma conta de usuário do que para suspender uma conta de usuário.

6. Escolha Terminar. Você será levado de volta à página da aplicação Amazon Web Services.
7. Na seção Provisionamento automático, ative a chave seletora para alterá-la de Inativa para Ativa.

> **Note**
>
> O controle deslizante de ativação será desativado se o IAM Identity Center não estiver ativado para os usuários. Escolha Acesso do usuário e ative o aplicativo para ativar o controle deslizante.

8. Na caixa de diálogo de confirmação, escolha Ligar.
9. Para verificar se os usuários estão sincronizados com sucesso com o IAM Identity Center, retorne ao console do IAM Identity Center e escolha Usuários. A página Usuários lista os usuários do diretório do Google Workspace que foram criados pelo SCIM. Se os usuários ainda não estiverem listados, pode ser que o provisionamento ainda esteja em andamento. O provisionamento pode levar até 24 horas, embora, na maioria dos casos, seja concluído em minutos. Certifique-se de atualizar a janela do navegador a cada poucos minutos.

   Selecione um usuário e visualize seus detalhes. As informações devem corresponder às informações do Google Workspace diretório.

> **Parabéns!**
>
> Você configurou com êxito uma conexão SAML entre Google Workspace e AWS e verificou se o provisionamento automático está funcionando. Agora você pode atribuir esses usuários a contas no IAM Identity Center. Para este tutorial, na próxima etapa, vamos designar um dos usuários como administrador do IAM Identity Center, concedendo a ele permissões administrativas para a conta de gerenciamento.

Etapa 6: IAM Identity Center: conceder Google Workspace aos usuários acesso às contas

1. Retorne ao console do IAM Identity Center. No painel de navegação do IAM Identity Center, em Permissões multicontas, escolha Contas da AWS.
2. Na página Contas da AWS, a Estrutura organizacional exibe a raiz organizacional com as contas abaixo dela na hierarquia. Marque a caixa de seleção da conta de gerenciamento e selecione Atribuir usuários ou grupos.
3. O fluxo de trabalho Atribuir usuários e grupos é exibido. Ele consiste em três etapas:

a. Em Etapa 1: selecionar usuários e grupos, escolha o usuário que desempenhará a função de administrador. Em seguida, escolha Próximo.

b. Em Etapa 2: selecionar conjuntos de permissões, escolha Criar conjunto de permissões para abrir uma nova guia que orienta você pelas três subetapas envolvidas na criação de um conjunto de permissões.

   i. Em Etapa 1: selecionar o tipo de conjunto de permissões, preencha o seguinte:

      - Em Tipo de conjunto de permissões, escolha Conjunto de permissões predefinido.
      - Em Política para conjunto de permissões predefinido, escolha AdministratorAccess.

      Escolha Próximo.

   ii. Em Etapa 2: especificar detalhes do conjunto de permissões, mantenha as configurações padrão e escolha Avançar.

      As configurações padrão criam um conjunto de permissões chamado *AdministratorAccess*com a duração da sessão definida em uma hora.

   iii. Para a Etapa 3: revisar e criar, verifique se o tipo de conjunto de permissões usa a política AWS gerenciada AdministratorAccess. Escolha Criar. Na página Conjuntos de permissões, aparece uma notificação informando que o conjunto de permissões foi criado. Você agora pode fechar essa guia do navegador.

   iv. Na guia Atribuir usuários e grupos do navegador, você ainda está na Etapa 2: selecionar conjuntos de permissões na qual você iniciou o fluxo de trabalho de criação do conjunto de permissões.

   v. Na área Conjuntos de permissões, escolha o botão Atualizar. O conjunto de *AdministratorAccess*permissões que você criou aparece na lista. Marque a caixa de seleção do conjunto de permissões e escolha Avançar.

c. Em Etapa 3: revisar e enviar, revise o usuário e o conjunto de permissões selecionados e escolha Enviar.

   A página é atualizada com uma mensagem informando que a sua Conta da AWS está sendo configurada. Aguarde a conclusão do processo.

   Você retornará à Contas da AWS página. Uma mensagem de notificação informa que a sua Conta da AWS foi reprovisionada e que o conjunto de permissões

atualizado foi aplicado. Quando o usuário fizer login, ele terá a opção de escolher a *AdministratorAccess*função.

> **Note**
>
> A sincronização automática do SCIM Google Workspace só oferece suporte ao provisionamento de usuários. O aprovisionamento automático de grupos não é suportado no momento. Você não pode criar grupos para os usuários do Google Workspace usando o AWS Management Console. Depois de provisionar usuários, você pode criar grupos usando o comando create-group do AWS CLI Identity Store ou a API IAM. CreateGroup

Etapa 7Google Workspace: confirmar o acesso Google Workspace dos usuários aos AWS recursos

1. Faça login Google usando uma conta de usuário de teste. Para saber como adicionar usuários aoGoogle Workspace, consulte a Google Workspacedocumentação.
2. Selecione o ícone do iniciador (waffle) do Google apps.
3. Role para o fim da lista de aplicações em que as aplicações personalizadas do Google Workspace se encontram. Duas aplicações são exibidas: Amazon Web Services e Portal de acesso do AWS .
4. Selecione a aplicação Portal de acesso do AWS . Você está conectado ao portal e pode ver o Conta da AWS ícone. Expanda esse ícone para ver a lista Contas da AWS que o usuário pode acessar. Neste tutorial, você só trabalhou com uma conta, portanto, a expansão do ícone só mostra uma conta.

   > **Note**
   >
   > Se você selecionar a aplicação Amazon Web Services, receberá um erro de SAML. Essa aplicação é usada para usuários do Google Workspace que foram provisionados como usuários do IAM e este tutorial está provisionando os usuários do Google Workspace como usuários no IAM Identity Center.

5. Selecione a conta para exibir os conjuntos de permissões disponíveis para o usuário. Neste tutorial, você criou o conjunto de AdministratorAccesspermissões.

6. Ao lado do conjunto de permissões, há links para o tipo de acesso disponível para aquele conjunto de permissões. Ao criar o conjunto de permissões, você especificou que o console de gerenciamento e o acesso programático fossem habilitados, assim sendo, essas duas opções estão presentes. Selecione Console de gerenciamento para abrir o AWS Management Console.
7. O usuário fez login no console.

(Opcional) Passar atributos para controle de acesso

Opcionalmente, você pode usar o atributo Atributos para controle de acesso no IAM Identity Center para passar um elemento `Attribute` com o atributo `Name` definido como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento permite que você passe atributos como tags de sessão na declaração do SAML. Para obter mais informações sobre tags de sessão, consulte Passar tags de sessão AWS STS no Guia de usuário do IAM.

Para passar atributos como tags de sessão, inclua o elemento `AttributeValue` que especifica o valor da tag. Por exemplo, para passar o par chave-valor de tag `CostCenter = blue`, use o atributo a seguir.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se você precisar adicionar vários atributos, inclua um elemento separado `Attribute` para cada tag.

Próximas etapas

Agora que você configurou o Google Workspace como provedor de identidades e provisionou usuários no IAM Identity Center, você pode:

- Use o comando create-group do AWS CLI Identity Store ou a API IAM CreateGrouppara criar grupos para seus usuários.

  Os grupos são úteis ao atribuir acesso a aplicativos Contas da AWS e aplicativos. Em vez de atribuir cada usuário individualmente, você concede permissões a um grupo. Posteriormente, à medida que você adiciona ou remove usuários de um grupo, o usuário obtém ou perde dinamicamente o acesso às contas e aplicações que você atribuiu ao grupo.

- Configure as permissões baseadas nas funções do trabalho; consulte Criar um conjunto de permissões.

  Os conjuntos de permissões definem o nível de acesso que os usuários e grupos têm a uma Conta da AWS. Os conjuntos de permissões são armazenados no IAM Identity Center e podem ser provisionados para um ou mais Contas da AWS. Você pode atribuir mais de um conjunto de permissões a um usuário.

> **Note**
>
> Como administrador do IAM Identity Center, você ocasionalmente precisará substituir certificados IdP antigos por outros mais novos. Por exemplo, talvez seja necessário substituir um certificado IdP quando a data de expiração do certificado se aproximar. O processo de substituição de um certificado antigo por um mais recente é conhecido como rodízio de certificados. Certifique-se de revisar como gerenciar os certificados SAML para o Google Workspace.

Usar o IAM Identity Center para conectar com a plataforma de diretórios do JumpCloud

O IAM Identity Center oferece suporte ao provisionamento automático (sincronização) das informações do usuário da plataforma de diretórios do JumpCloud para o IAM Identity Center. Esse provisionamento usa o protocolo System for Cross-domain Identity Management (SCIM) v2.0. Você configura essa conexão no JumpCloud usando seu endpoint e token de acesso do IAM Identity Center SCIM. Ao configurar a sincronização do SCIM, você cria um mapeamento dos atributos do usuário no JumpCloud para os atributos nomeados no IAM Identity Center. Isso faz com que os atributos esperados correspondam entre o IAM Identity Center e JumpCloud.

Este guia é baseado no JumpCloud em junho de 2021. As etapas para versões mais recentes podem variar. Este guia contém algumas notas sobre a configuração da autenticação do usuário por meio do SAML.

As etapas a seguir explicam como habilitar o provisionamento automático de usuários e grupos do JumpCloud para o IAM Identity Center usando o protocolo SCIM.

> **Note**
>
> Antes de começar a implantar o SCIM, é recomendável que você analise Considerações sobre o uso do provisionamento automático antes. Em seguida, continue analisando considerações adicionais na próxima seção.

Tópicos

Pré-requisitos

Você precisará do seguinte antes de começar:

- Assinatura ou teste gratuito do JumpCloud. Para se inscrever para um teste gratuito, acesse JumpCloud.
- Uma conta habilitada para o IAM Identity Center (gratuita). Para obter mais informações, consulte Habilitar o IAM Identity Center.
- Uma conexão SAML da sua conta do JumpCloud com o IAM Identity Center, conforme descrito na documentação do JumpCloud do IAM Identity Center.
- Associe o conector do IAM Identity Center aos grupos para os quais você deseja permitir o acesso às contas da AWS.

Considerações SCIM

As seguintes considerações devem ser observadas ao usar a federação do JumpCloud para o IAM Identity Center.

- Somente grupos associados ao AWS conector de login único no JumpCloud serão sincronizados com o SCIM.
- Somente um atributo de número de telefone pode ser sincronizado e o padrão é “telefone comercial”.
- Os usuários no diretório JumpCloud devem ter nomes e sobrenomes configurados para serem sincronizados com o IAM Identity Center com o SCIM.
- Os atributos ainda serão sincronizados se o usuário estiver desativado no IAM Identity Center, mas ainda estiver ativo no JumpCloud.
- Você pode optar por ativar a sincronização do SCIM somente para informações do usuário desmarcando a opção “Habilitar gerenciamento de grupos de usuários e associação a grupos” no conector.
- Se houver um usuário existente no diretório do Identity Center com o mesmo nome de usuário e e-mail, o usuário será sobrescrito e sincronizado com o SCIM a partir do JumpCloud.

Etapa 1: Habilitar provisionamento no IAM Identity Center

Nesta primeira etapa, você usa o console do IAM Identity Center para ativar o provisionamento automático.

Para habilitar o provisionamento automático no IAM Identity Center

1. Depois de concluir os pré-requisitos, abra o console do IAM Identity Center.
2. Escolha Configurações no painel de navegação à esquerda.
3. Na página Configurações, localize a caixa de informações Provisionamento automático e selecione Habilitar. Isso habilita imediatamente o provisionamento automático no IAM Identity Center e exibe as informações necessárias do endpoint SCIM e do token de acesso.
4. Na caixa de diálogo Provisionamento automático de entrada, copie cada um dos valores para as opções a seguir. Você precisará colá-los posteriormente ao configurar o provisionamento em seu IdP.
    a. Endpoint do SCIM
    b. Token de acesso
5. Escolha Fechar.

Agora que você configurou o provisionamento no console do IAM Identity Center, precisa concluir as tarefas restantes usando o conector IAM Identity Center do JumpCloud. Essas etapas são descritas no procedimento a seguir.

Etapa 2: Configure o provisionamento no JumpCloud

Use o procedimento a seguir no conector IAM Identity Center do JumpCloud para habilitar o provisionamento com o IAM Identity Center. Esse procedimento pressupõe que você já tenha adicionado o conector IAM Identity Center do JumpCloud ao seu portal e grupos de administração do JumpCloud. Se você ainda não tiver feito isso, consulte Pré-requisitos e conclua este procedimento para configurar o provisionamento do SCIM.

Para configurar o provisionamento no JumpCloud

1. Abra o conector do IAM Identity Center do JumpCloud que você instalou como parte da configuração do SAML para o JumpCloud (Autenticação de usuário > IAM Identity Center). Consulte Pré-requisitos.
2. Escolha o conector do IAM Identity Center e, em seguida, escolha a terceira guia Gestão de identidade.
3. Marque a caixa Habilitar gerenciamento de grupos de usuários e membros de grupos neste aplicativo se quiser que os grupos sejam sincronizados com o SCIM.
4. Clique em Configurar.
5. No procedimento anterior, você copiou o valor do endpoint SCIM do IAM Identity Center. Cole esse valor no campo Base URL no conector do JumpCloud IAM Identity Center. Certifique-se de remover a barra final no final do URL.
6. No procedimento anterior, você copiou o valor do Token de acesso do IAM Identity Center. Cole esse valor no campo Chave token no conector do IAM Identity Center do JumpCloud.
7. Clique em Ativar para aplicar a configuração.
8. Verifique se você tem um indicador verde ao lado do Single Sign-On ativado.
9. Vá para a quarta guia Grupos de usuários e marque os grupos que você deseja que sejam provisionados com o SCIM.
10. Clique em Salvar na parte inferior quando terminar.
11. Para verificar se os usuários foram sincronizados com sucesso com o IAM Identity Center, retorne ao console do IAM Identity Center e escolha Usuários. Os usuários sincronizados do JumpCloud aparecem na página Usuários. Esses usuários agora podem ser atribuídos a contas no IAM Identity Center.

(Opcional) Etapa 3: configure atributos do usuário no JumpCloud para controle de acesso no IAM Identity Center

Esse é um procedimento opcional para o JumpCloud caso você opte por configurar atributos para o IAM Identity Center gerenciar o acesso aos seus recursos da AWS. Os atributos que você define no JumpCloud são passados em uma declaração de SAML para o IAM Identity Center. Em seguida, você cria um conjunto de permissões no IAM Identity Center para gerenciar o acesso com base nos atributos dos quais você passou do JumpCloud.

Antes de iniciar esse procedimento, você deve ativar primeiro o recurso Atributos para controle de acesso. Para obter mais informações sobre como fazer isso, consulte Habilitar e configurar atributos para controle de acesso.

Para configurar atributos do usuário em JumpCloud para controle de acesso no IAM Identity Center

1. Abra o conector do IAM Identity Center do JumpCloud que você instalou como parte da configuração do SAML para o JumpCloud (Autenticação de usuário > IAM Identity Center).
2. Escolha o conector do IAM Identity Center. Em seguida, escolha a segunda guia IAM Identity Center.
3. Na parte inferior dessa guia, você tem Mapeamento de atributos de usuário, escolha Adicionar novo atributo e faça o seguinte: Você deve executar essas etapas para cada atributo que adicionará para uso no IAM Identity Center para controle de acesso.
    a. No campo Nome do atributo do provedor de serviço, insira `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**`.` Substituir **`AttributeName`** pelo nome do atributo que você está esperando no IAM Identity Center. Por exemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**.
    b. No campo JumpCloud Nome do atributo, escolha os atributos do usuário em seu JumpCloud diretório. Por exemplo, E-mail (trabalho).
4. Escolha Salvar.

(Opcional) Passar atributos para controle de acesso

Opcionalmente, você pode usar o atributo Atributos para controle de acesso no IAM Identity Center para passar um elemento `Attribute` com o atributo `Name` definido como `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**. Este elemento permite que

você passe atributos como tags de sessão na declaração do SAML. Para obter mais informações sobre tags de sessão, consulte Passar tags de sessão AWS STS no Guia de usuário do IAM.

Para passar atributos como tags de sessão, inclua o elemento `AttributeValue` que especifica o valor da tag. Por exemplo, para passar o par chave-valor de tag `CostCenter = blue`, use o atributo a seguir.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se você precisar adicionar vários atributos, inclua um elemento separado `Attribute` para cada tag.

Configurar SAML e SCIM com o Microsoft Entra ID e o IAM Identity Center

O AWS IAM Identity Center é compatível com a integração com o Security Assertion Markup Language (SAML) 2.0, bem como com o provisionamento automático (sincronização) de informações de usuários e grupos do Microsoft Entra ID (antes conhecido como Azure Active Directory ou Azure AD) para o IAM Identity Center usando o protocolo System for Cross-domain Identity Management (SCIM) 2.0.

Objetivo

Neste tutorial, você configurará um laboratório de teste e uma conexão SAML e um provisionamento SCIM entre o Microsoft Entra ID e o IAM Identity Center. Durante as etapas iniciais de preparação, você criará um usuário de teste (Nikki Wolf) no Microsoft Entra ID e no IAM Identity Center que será usado para testar a conexão SAML nas duas direções. Posteriormente, como parte das etapas do SCIM, você criará um usuário de teste diferente (Richard Roe) para verificar se os novos atributos do Microsoft Entra ID estão sendo sincronizados com o IAM Identity Center como esperado.

Pré-requisitos

Antes de começar este tutorial, você precisará definir o seguinte:

- Um locatário do Microsoft Entra ID. Para obter mais informações, consulte Início rápido: configurar um tenant no site da Microsoft.

- Uma conta habilitada para o AWS IAM Identity Center. Para obter mais informações, consulte What is IAM Identity Center (O que é o Centro de Identidade do IAM?) no Guia do usuário do AWS IAM Identity Center.

Etapa 1: preparar o locatário da Microsoft

Nesta etapa, você aprenderá a instalar e configurar a aplicação empresarial AWS IAM Identity Center e a atribuir acesso a um usuário de teste do Microsoft Entra ID recém-criado.

Step 1.1 >

Etapa 1.1: configurar a aplicação empresarial AWS IAM Identity Center no Microsoft Entra ID

Neste procedimento, você instala a aplicação empresarial AWS IAM Identity Center no Microsoft Entra ID. Mais tarde, você precisará dessa aplicação para configurar a conexão SAML com a AWS.

1. Faça login no Centro de administração do Microsoft Entra como, no mínimo, administrador de aplicações de nuvem.
2. Navegue até Identidade > Aplicações > Aplicações empresariais e escolha Nova aplicação.
3. Na página Procurar na galeria do Microsoft Entra, insira **`AWS IAM Identity Center`** na caixa de pesquisa.
4. Selecione AWS IAM Identity Center na área de resultados.
5. Escolha Create (Criar).

Step 1.2 >

Etapa 1.2: criar um usuário de teste do Microsoft Entra ID

Nikki Wolf é o nome do usuário de teste do Microsoft Entra ID que você criará neste procedimento.

1. No console do Centro de administração do Microsoft Entra, navegue até Identidade > Usuários > Todos os usuários.
2. Selecione Novo usuário e escolha Criar novo usuário na parte superior da tela.
3. Em Nome da entidade principal do usuário, insira **`NikkiWolf`** e selecione o domínio e a extensão de sua preferência. Por exemplo, NikkiWolf@*`exemplo.org`*.
4. Em Nome de exibição, insira **`NikkiWolf`**.

5. Em Senha, insira uma senha forte ou selecione o ícone de olho para mostrar a senha que foi gerada automaticamente e copie ou anote o valor exibido.
6. Escolha Propriedades, em Nome, insira **`Nikki`**. Em Sobrenome, insira **`Wolf`**.
7. Selecione Revisar + criar e depois Criar.

Step 1.3

Etapa 1.3: testar a experiência de Nikki antes de atribuir a ela permissões ao AWS IAM Identity Center

Neste procedimento, você verificará se Nikki consegue fazer login no portal Minha conta da Microsoft.

1. No mesmo navegador, abra uma nova guia, vá até página de login do portal Minha conta e insira o endereço de e-mail completo de Nikki. Por exemplo, NikkiWolf@*`exemplo.org`*.
2. Quando solicitado, insira a senha de Nikki e escolha Fazer login. Se essa for uma senha gerada automaticamente, será solicitado que você a altere.
3. Na página Ação necessária, escolha Perguntar mais tarde para ignorar a solicitação de métodos de segurança adicionais.
4. Na página Minha conta, no painel de navegação esquerdo, escolha Minhas aplicações. Observe que, além dos complementos, nenhuma aplicação é exibida no momento. Você adicionará uma aplicação do AWS IAM Identity Center que aparecerá aqui em uma etapa posterior.

Step 1.4

Etapa 1.4: atribuir permissões a Nikki no Microsoft Entra ID

Agora que você verificou que Nikki pode acessar com sucesso o portal Minha conta, use este procedimento para atribuir o usuário dela à aplicação AWS IAM Identity Center.

1. No console do Centro de administração do Microsoft Entra, navegue até Identidade > Aplicações > Aplicações empresariais e escolha AWS IAM Identity Center na lista.
2. No lado esquerdo, escolha Usuários e grupos.
3. Escolha Add user/group (Adicionar usuário/grupo). Você pode ignorar a mensagem informando que os grupos não estão disponíveis para atribuição. Este tutorial não usa grupos para atribuição.

4. Na página Adicionar atribuição, em Usuários, escolha Nenhum selecionado.
5. Selecione NikkiWolf e escolha Selecionar.
6. Na página Add Assignment (Adicionar atribuição), escolha Assign (Atribuir). NikkiWolf agora aparece na lista de usuários atribuídos à aplicação AWS IAM Identity Center.

Etapa 2: preparar a conta da AWS

Nesta etapa, você aprenderá a usar o IAM Identity Center para configurar permissões de acesso (via conjunto de permissões), criar manualmente um usuário Nikki Wolf correspondente e atribuir a ela as permissões necessárias para administrar recursos na AWS.

Step 2.1 **>**

Etapa 2.1: criar um conjunto de permissões RegionalAdmin no IAM Identity Center

Esse conjunto de permissões será usado para conceder a Nikki as permissões da conta da AWS necessárias para gerenciar regiões na página Conta no AWS Management Console. Todas as outras permissões para visualizar ou gerenciar qualquer outra informação da conta de Nikki são negadas por padrão.

1. Abra o console do IAM Identity Center.
2. Em Permissões de várias contas, escolha Conjuntos de permissões.
3. Escolha Create permission set (Criar conjunto de permissões).
4. Em Selecionar tipo de conjunto de permissões, selecione Conjunto de permissões personalizado e escolha Avançar.
5. Selecione Política em linha para expandi-la e crie uma política para o conjunto de permissões usando as seguintes etapas:

   a. Escolha Adicionar nova instrução para criar uma instrução de política.
   b. Em Editar instrução, selecione Conta na lista e escolha as caixas de seleção a seguir.

      - **`ListRegions`**
      - **`GetRegionOptStatus`**
      - **`DisableRegion`**
      - **`EnableRegion`**

   c. Ao lado de Add a resource (Adicionar um recurso), escolha Add (Adicionar).

d. Na página Adicionar recurso, em Tipo de recurso, selecione Todos os recursos e escolha Adicionar recurso. Confirme se a política é semelhante à seguinte:

```
{
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "account:ListRegions",
                "account:DisableRegion",
                "account:EnableRegion",
                "account:GetRegionOptStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. Escolha Next (Próximo).
7. Na página Especificar detalhes do conjunto de permissões, em Nome do conjunto de permissões, insira **`RegionalAdmin`** e escolha Avançar.
8. Na página Review and create (Revisar e criar), escolha Create (Criar). Você deve ver RegionalAdmin exibido na lista de conjuntos de permissões.

Step 2.2 >

Etapa 2.2: criar um usuário NikkiWolf correspondente no IAM Identity Center

Como o protocolo SAML não fornece um mecanismo para consultar o IdP (Microsoft Entra ID) e criar usuários automaticamente aqui no IAM Identity Center, use o procedimento a seguir para criar manualmente um usuário no IAM Identity Center que espelhe os principais atributos do usuário Nikki Wolfs no Microsoft Entra ID.

1. Abra o console do Centro de Identidade do IAM.
2. Escolha Usuários, depois Adicionar usuário e forneça as seguintes informações:

a. Em nome de usuário e endereço de e-mail, insira o mesmo **NikkiWolf@*yourcompanydomain.extension*** que você usou ao criar seu usuário Microsoft Entra ID. Por exemplo, NikkiWolf@*exemplo.org*.

b. Confirmar o endereço de e-mail: insira novamente o endereço de e-mail da etapa anterior

c. Primeiro nome: insira **Nikki**

d. Sobrenome: insira **Wolf**

e. Nome de exibição: insira **Nikki Wolf**

3. Escolha Avançar e depois Adicionar usuário.
4. Selecione Fechar.

Step 2.3

Etapa 2.3: atribuir Nikki ao conjunto de permissões RegionalAdmin no IAM Identity Center

Aqui você localiza a região da Conta da AWS na qual Nikki administrará as regiões e, em seguida, atribua as permissões necessárias para ela acessar com sucesso o Portal de acesso do AWS.

1. Abra o console do IAM Identity Center.
2. Em Permissões de várias contas, escolha Contas da AWS.
3. Marque a caixa de seleção ao lado do nome da conta (por exemplo, *Sandbox*), à qual você deseja conceder a Nikki acesso para gerenciar regiões e depois escolha Atribuir usuários e grupos.
4. Na página Atribuir usuários e grupos, escolha a guia Usuários, localize e marque a caixa ao lado de Nikki e escolha Avançar.

Etapa 3: configurar e testar a conexão SAML

Nesta etapa, você configura a conexão SAML usando a aplicação empresarial AWS IAM Identity Center no Microsoft Entra ID junto com as configurações de IdP externo no IAM Identity Center.

Step 3.1 >

Etapa 3.1: coletar os metadados necessários do provedor de serviços do IAM Identity Center

Nesta etapa, você iniciará o assistente Alterar fonte de identidades no console do IAM Identity Center e recuperará o arquivo de metadados e o URL específico de login da AWS que você precisará inserir ao configurar a conexão com o Microsoft Entra ID na próxima etapa.

1. No console do IAM Identity Center, escolha Configurações.
2. Na página Configurações, escolha a guia Origem da identidade e, em seguida, escolha Ações > Alterar origem da identidade.
3. Em Escolher fonte de identidades, selecione Provedor de identidades externo e escolha Avançar.
4. Na página Configurar provedor de identidades externo, em Metadados do provedor de serviços, escolha Baixar arquivo de metadados para baixá-lo em seu sistema.
5. Na mesma seção, localize e copie o valor da URL de login do Portal de acesso do AWS. Você precisará inserir esse valor quando solicitado na próxima etapa.
6. Deixe essa página aberta e passe para a próxima etapa (**`Step 3.2`**) para configurar a aplicação empresarial AWS IAM Identity Center no Microsoft Entra ID. Posteriormente, você retornará a essa página para concluir o processo.

Step 3.2 >

Etapa 3.2: configurar a aplicação empresarial AWS IAM Identity Center no Microsoft Entra ID

Esse procedimento estabelece metade da conexão SAML do lado da Microsoft usando os valores do arquivo de metadados e o URL de logon único que você obteve na última etapa.

1. No console do Centro de administração do Microsoft Entra, navegue até Identidade > Aplicações > Aplicações empresariais e escolha AWS IAM Identity Center.
2. Do lado esquerdo, escolha Logon único.
3. Na página Configurar logon único com SAML, escolha Carregar arquivo de metadados, escolha o ícone de pasta, selecione o arquivo de metadados do provedor de serviços que você baixou na etapa anterior e escolha Adicionar.
4. Na página Configuração básica do SAML, verifique se os valores Identificador e URL de resposta agora apontam para endpoints na AWS que começam com `https://<REGION>.signin.aws.amazon.com/platform/saml/`.
5. Em URL de login (opcional), cole o valor do URL de login do Portal de acesso do AWS que você copiou na etapa anterior (**`Step 3.1`**), escolha Salvar e depois X para fechar a janela.

6. Se for solicitado que você teste o logon único com o AWS IAM Identity Center, escolha Não, testarei mais tarde. Você fará essa verificação em uma etapa posterior.
7. Na página Configurar logon único com SAML, na seção Certificados SAML, ao lado de XML dos metadados da federação, escolha Baixar para salvar o arquivo de metadados em seu sistema. Você precisará inserir esse arquivo quando solicitado na próxima etapa.

Step 3.3 >

Etapa 3.3: configurar o IdP externo do Microsoft Entra ID no AWS IAM Identity Center

Aqui, você retornará ao assistente Alterar fonte de identidades no console do IAM Identity Center para concluir a segunda metade da conexão SAML na AWS.

1. Retorne à sessão do navegador que você deixou aberta na **`Step 3.1`** no console do IAM Identity Center.
2. Na página Configurar provedor de identidades externo, na seção Metadados do provedor de identidade em Metadados SAML do IdP, escolha o botão Escolher arquivo e selecione o arquivo de metadados do provedor de identidades que você baixou do Microsoft Entra ID na etapa anterior e escolha Abrir.
3. Escolha Next (Próximo).
4. Depois de ler a isenção de responsabilidade e estar pronto para continuar, insira **`ACCEPT`**.
5. Escolha Alterar fonte de identidades para aplicar as alterações.

Step 3.4 >

Etapa 3.4: testar se Nikki é redirecionada para o Portal de acesso do AWS

Neste procedimento, você testará a conexão SAML fazendo login no portal Minha conta da Microsoft com as credenciais de Nikki. Depois da autenticação, você selecionará a aplicação AWS IAM Identity Center que redirecionará Nikki para o Portal de acesso do AWS.

1. Vá até página de login do portal Minha conta e insira o endereço de e-mail completo de Nikki. Por exemplo, ***`NikkiWolf`***`@`*`exemplo.org`*.
2. Quando solicitado, insira a senha de Nikki e escolha Fazer login.
3. Na página Minha conta, no painel de navegação esquerdo, escolha Minhas aplicações.
4. Na página Minhas aplicações, selecione a aplicação denominada AWS IAM Identity Center. Deve ser solicitado que você faça uma autenticação adicional.

5. Na página de login da Microsoft, escolha as credenciais de NikkiWolf. Se for solicitada mais uma autenticação, escolha as credenciais de NikkiWolf novamente. Isso deve redirecioná-lo automaticamente para o Portal de acesso do AWS.

   > **Tip**
   >
   > Se você não for redirecionado com sucesso, verifique se o valor do URL de login do Portal de acesso do AWS inserido na **`Step 3.2`** corresponde ao valor que você copiou da **`Step 3.1`**.

6. Verifique se você vê um ícone de conta da AWS

   exibido.

   > **Tip**
   >
   > Se a página estiver vazia e nenhum ícone de conta da AWS for exibido, confirme que Nikki foi atribuída com sucesso ao conjunto de permissões RegionalAdmin (consulte **`Step 2.3`**).

Step 3.5

Etapa 3.5: testar o nível de acesso de Nikki para gerenciar sua Conta da AWS

Nesta etapa, você verificará o nível de acesso de Nikki para gerenciar as configurações de região para sua Conta da AWS. Nikki só deve ter privilégios de administrador suficientes para gerenciar regiões na página Contas.

1. No Portal de acesso do AWS, escolha o ícone de conta da AWS

   para expandir a lista de contas. Depois de escolher o ícone, os nomes das contas, os IDs das contas e os endereços de e-mail associados às contas nas quais você definiu conjuntos de permissões são exibidos.

2. Escolha o nome da conta (por exemplo, *Sandbox*) em que você aplicou o conjunto de permissões (consulte **`Step 2.3`**). Isso expandirá a lista de conjuntos de permissões que Nikki pode escolher para gerenciar sua conta.

3. Ao lado de RegionalAdmin, escolha Console de gerenciamento para assumir o perfil que você definiu no conjunto de permissões RegionalAdmin. Isso redirecionará você para a página inicial do AWS Management Console.
4. No canto superior direito do console, escolha o nome da sua conta e depois Conta. Isso levará você para a página Conta. Observe que todas as outras seções desta página exibem uma mensagem informando que você não tem as permissões necessárias para visualizar ou modificar essas configurações.
5. Na página Conta, role para baixo até a seção Regiões da AWS. Marque uma caixa de seleção de qualquer região disponível na tabela. Observe que Nikki tem as permissões necessárias para habilitar ou desabilitar a lista de regiões de sua conta como pretendido.

> Muito bem!
>
> As etapas de 1 a 3 ajudaram você a implementar e testar com sucesso a conexão SAML. Agora, para concluir o tutorial, recomendamos que você passe para a etapa 4 para implementar o provisionamento automático.

Etapa 4: configurar e testar a sincronização SCIM

Nesta etapa, você configurará o provisionamento automático (sincronização) das informações de usuário do Microsoft Entra ID para o IAM Identity Center usando o protocolo SCIM v2.0. Você configura essa conexão no Microsoft Entra ID usando seu endpoint SCIM para o IAM Identity Center e um token de portador que é criado automaticamente pelo IAM Identity Center.

Ao configurar a sincronização do SCIM, você cria um mapeamento dos atributos de usuário no Microsoft Entra ID para os atributos nomeados no IAM Identity Center. Isso faz com que os atributos esperados correspondam entre o IAM Identity Center e Microsoft Entra ID.

As etapas a seguir explicam como habilitar o provisionamento automático de usuários e grupos que residem primariamente no Microsoft Entra ID para o IAM Identity Center usando a aplicação IAM Identity Center no Microsoft Entra ID.

Step 4.1 >

Etapa 4.1: criar um segundo usuário de teste no Microsoft Entra ID

Para fins de teste, você criará um novo usuário (Richard Roe) no Microsoft Entra ID. Posteriormente, depois de configurar a sincronização SCIM, você testará se esse usuário e todos os atributos relevantes foram sincronizados com sucesso com o IAM Identity Center.

1. No console do Centro de administração do Microsoft Entra, navegue até Identidade > Usuários > Todos os usuários.
2. Selecione Novo usuário e escolha Criar novo usuário na parte superior da tela.
3. Em Nome da entidade principal do usuário, insira **`RichRoe`** e selecione o domínio e a extensão de sua preferência. Por exemplo, RichRoe@*`exemplo.org`*.
4. Em Nome de exibição, insira **`RichRoe`**.
5. Em Senha, insira uma senha forte ou selecione o ícone de olho para mostrar a senha que foi gerada automaticamente e copie ou anote o valor exibido.
6. Selecione Propriedades e forneça os seguintes valores:
   - Nome: insira **`Richard`**
   - Sobrenome: insira **`Roe`**
   - Cargo: insira **`Marketing Lead`**
   - Departamento: insira **`Sales`**
   - ID do funcionário: insira **`12345`**
7. Selecione Revisar + criar e depois Criar.

Step 4.2 >

Etapa 4.2: habilitar provisionamento no IAM Identity Center

Neste procedimento, você usará o console do IAM Identity Center para habilitar o provisionamento automático de usuários e grupos originários do Microsoft Entra ID para o IAM Identity Center.

1. Abra o console do IAM Identity Center e escolha Configurações no painel de navegação esquerdo.
2. Na página Configurações, na guia Fonte de identidades, observe que Método de aprovisionamento está definido como Manual.
3. Localize a caixa de informações Provisionamento automático e escolha Habilitar. Isso habilita imediatamente o provisionamento automático no IAM Identity Center e exibe as informações necessárias do endpoint SCIM e do token de acesso.

4. Na caixa de diálogo Provisionamento automático de entrada, copie cada um dos valores para as opções a seguir. Você precisará colá-los na próxima etapa quando configurar o provisionamento no Microsoft Entra ID.

   a. Endpoint SCIM: por exemplo, https://scim.*us-east-2*.amazonaws.com/*11111111111-2222-3333-4444-555555555555*/scim/v2/

   b. Token de acesso: escolha Mostrar token para copiar o valor.

5. Escolha Fechar.

6. Na guia Fonte de identidades, observe que Método de provisionamento agora está definido como SCIM.

Step 4.3 >

Etapa 4.3: configurar o provisionamento automático no Microsoft Entra ID

Agora que você tem o usuário de teste RichRoe configurado e o SCIM habilitado no IAM Identity Center, pode prosseguir com a configuração da sincronização SCIM no Microsoft Entra ID.

1. No console do Centro de administração do Microsoft Entra, navegue até Identidade > Aplicações > Aplicações empresariais e escolha AWS IAM Identity Center.

2. Escolha Provisionamento em Gerenciar e depois escolha Provisionamento novamente.

3. Em Modo de aprovisionamento, selecione Automático.

4. Em Credenciais do administrador, em URL do locatário, cole o valor da URL do endpoint SCIM que você copiou anteriormente na **`Step 4.1`**. Em Token secreto, cole o valor do token de acesso.

5. Escolha Test Connection (Testar conexão). Você deve ver uma mensagem indicando que as credenciais testadas foram autorizadas com sucesso a habilitar o provisionamento.

6. Escolha Save (Salvar).

7. Em Gerenciar, escolha Usuários e grupos e depois escolha Adicionar usuário/grupo.

8. Na página Adicionar atribuição, em Usuários, escolha Nenhum selecionado.

9. Selecione RichRoe e escolha Selecionar.

10. Na página Add Assignment (Adicionar atribuição), escolha Assign (Atribuir).

11. Escolha Visão geral e depois Iniciar provisionamento.

Step 4.4

Etapa 4.4: verificar se a sincronização ocorreu

Nesta seção, você verificará se o usuário de Richard foi provisionado com sucesso e se todos os atributos são exibidos no IAM Identity Center.

1. No console do IAM Identity Center, escolha Usuários.
2. Na página Usuários, você deve ver o usuário RichRoe exibido. Observe que na coluna Criado por, o valor está definido como SCIM.
3. Escolha RichRoe, em Perfil, verifique se os atributos a seguir foram copiados do Microsoft Entra ID.

   - Nome: **`Richard`**
   - Sobrenome: **`Roe`**
   - Departamento: **`Sales`**
   - Cargo: **`Marketing Lead`**
   - Número do funcionário: **`12345`**

   Agora que o usuário de Richard foi criado no IAM Identity Center, você pode atribuí-lo a qualquer conjunto de permissões para poder controlar o nível de acesso que ele tem aos recursos da AWS. Por exemplo, você pode atribuir RichRoe ao conjunto de permissões **`RegionalAdmin`** usado anteriormente para conceder a Nikki as permissões para gerenciar as regiões (consulte **`Step 2.3`**) e depois testar seu nível de acesso usando a **`Step 3.5`**.

> Parabéns!
>
> Você configurou com sucesso uma conexão SAML entre a Microsoft e a AWS, e verificou que o provisionamento automático está trabalhando para manter tudo sincronizado. Agora você pode aplicar o que aprendeu para configurar seu ambiente de produção com mais facilidade.

Considerações sobre o uso do SCIM com o Microsoft Entra ID em um ambiente de produção

Estas são considerações importantes sobre o Microsoft Entra ID que podem afetar a forma como você planeja implementar o provisionamento automático com o IAM Identity Center em seu ambiente de produção usando o protocolo SCIM v2.

> **Note**
>
> Antes de começar a implantar o SCIM, é recomendável que você revise as Considerações sobre o uso do provisionamento automático.

Atributos para controle de acesso

Os atributos para controle de acesso são usados nas políticas de permissão que determinam quem em sua fonte de identidades pode acessar seus recursos da AWS. Se um atributo for removido de um usuário em Microsoft Entra ID, esse atributo não será removido do usuário correspondente no IAM Identity Center. Esta é uma limitação conhecida do Microsoft Entra ID. Se um atributo for alterado para um valor diferente (não vazio) em um usuário, essa alteração será sincronizada com o IAM Identity Center.

Grupos aninhados

O serviço de provisionamento de usuários do Microsoft Entra ID não pode ler nem provisionar usuários em grupos aninhados. Somente usuários que são membros imediatos de um grupo atribuído explicitamente podem ser lidos e provisionados. O Microsoft Entra ID não descompacta recursivamente as associações de grupos ou usuários atribuídos indiretamente (usuários ou grupos que são membros de um grupo atribuído diretamente). Para obter mais informações, consulte Assignment-based scoping na documentação do Microsoft Entra ID.

Grupos dinâmicos

O serviço de provisionamento de usuários do Microsoft Entra ID não pode ler nem provisionar usuários em grupos dinâmicos. Veja abaixo um exemplo que mostra a estrutura de usuários e grupos ao usar grupos dinâmicos e como eles são exibidos no IAM Identity Center. Esses usuários e grupos foram provisionados do IAM Identity Center do Microsoft Entra ID via SCIM.

Por exemplo, se a estrutura do Microsoft Entra ID para grupos dinâmicos for a seguinte:

1. Grupo A com membros ua1, ua2

2. Grupo B com membros ub1
3. Grupo C com membros uc1
4. Grupo K com uma regra para incluir membros do Grupo A, B, C
5. Grupo L com uma regra para incluir membros do Grupo B e C

Depois que as informações do usuário e do grupo forem provisionadas do Microsoft Entra ID para o IAM Identity Center por meio do SCIM, a estrutura será a seguinte:

1. Grupo A com membros ua1, ua2
2. Grupo B com membros ub1
3. Grupo C com membros uc1
4. Grupo K com membros ua1, ua2, ub1, uc1
5. Grupo L com membros ub1, uc1

Ao configurar o provisionamento automático usando grupos dinâmicos, mantenha as seguintes considerações em mente.

- Um grupo dinâmico pode incluir um grupo aninhado. No entanto, o serviço de provisionamento do Microsoft Entra ID não nivela o grupo aninhado. Por exemplo, se a seguinte estrutura do Microsoft Entra ID para grupos dinâmicos:
  - O grupo A é pai do grupo B.
  - O Grupo A tem ua1 como membro.
  - O grupo B tem ub1 como membro.

O grupo dinâmico que inclui o Grupo A incluirá apenas os membros diretos do grupo A (ou seja, ua1). Não incluirá recursivamente membros do grupo B.

- Os grupos dinâmicos não podem conter outros grupos dinâmicos. Para obter mais informações, consulte Preview limitations na documentação do Microsoft Entra ID.

Solução de problemas do SCIM com o Microsoft Entra ID

Se você estiver enfrentando problemas com usuários do Microsoft Entra ID que não estão sincronizando com o IAM Identity Center, talvez seja devido a um problema de sintaxe que o IAM Identity Center sinalizou que acontece quando um novo usuário está sendo adicionado ao IAM

Identity Center. Você pode confirmar isso verificando os eventos com falha registrados nos logs de auditoria do Microsoft Entra ID, como uma `'Export'`. O Motivo do status para este evento indicará:

```
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is
 unparsable, syntactically incorrect, or violates schema.","status":"400"}
```

Você também pode verificar se o evento AWS CloudTrail falhou. Isso pode ser feito pesquisando no console Histórico de eventos do CloudTrail usando o seguinte filtro:

```
"eventName":"CreateUser"
```

O erro no evento do CloudTrail indicará o seguinte:

```
"errorCode": "ValidationException",
        "errorMessage": "Currently list attributes only allow single item“
```

Em última análise, essa exceção significa que um dos valores passados do Microsoft Entra ID continha mais valores do que previsto. A solução aqui é revisar os atributos do usuário em Microsoft Entra ID, garantindo que nenhum contenha valores duplicados. Um exemplo comum de valores duplicados é ter vários valores presentes para números de contato, como celular, trabalho e fax. Embora sejam valores separados, todos eles são passados para o IAM Identity Center sob o atributo ascendente único PhoneNumbers.

Para obter dicas de solução de problemas em geral, consulte Solução de problemas do IAM Identity Center.

Etapa 5: (opcional) configurar o ABAC

Agora que você configurou o SAML e o SCIM com sucesso, pode optar por configurar o controle de acesso por atributo (ABAC). ABAC é uma estratégia de autorização que define permissões com base em atributos.

Com o Microsoft Entra ID, você pode usar qualquer dos dois métodos a seguir para configurar o ABAC para uso com o IAM Identity Center.

Method 1

Método 1: configurar atributos de usuário no Microsoft Entra ID para controle de acesso no IAM Identity Center

No procedimento a seguir, você determinará quais atributos do Microsoft Entra ID devem ser usados pelo IAM Identity Center para gerenciar o acesso aos seus recursos do AWS. Depois de definidos, Microsoft Entra ID envie esses atributos para o IAM Identity Center por meio de asserções SAML. Em seguida, você precisará acessar Criar um conjunto de permissões no IAM Identity Center para gerenciar o acesso com base nos atributos dos quais você passou do Microsoft Entra ID.

Antes de iniciar este procedimento, você deve primeiro habilitar o atributo Atributos para controle de acesso. Para obter mais informações sobre como fazer isso, consulte Habilite e configure atributos para controle de acesso.

1. No console do Centro de administração do Microsoft Entra, navegue até Identidade > Aplicações > Aplicações empresariais e escolha AWS IAM Identity Center.
2. Escolha Logon único.
3. Na seção Atributos e declarações, escolha Editar.
4. Na página Atributos e declarações, faça o seguinte:
    a. Escolha Adicionar nova reivindicação
    b. Em Nome, insira `AccessControl:`*`AttributeName`*. Substitua *`Nome do atributo`* pelo nome do atributo que você espera no IAM Identity Center. Por exemplo, `AccessControl:`**`Department`**.
    c. Em Namespace, insira **`https://aws.amazon.com/SAML/Attributes`**.
    d. Em Origem, escolha Atributo.
    e. Para Atributo de fonte, use a lista suspensa para escolher os atributos do Microsoft Entra ID usuário. Por exemplo, `user.`**`department`**.
5. Repita a etapa anterior para cada atributo que você precisa enviar para o IAM Identity Center na declaração SAML.
6. Escolha Salvar.

Method 2

Método 2: configurar o ABAC usando o IAM Identity Center

Com esse método, você usa o recurso Atributos para controle de acesso no IAM Identity Center para passar um elemento `Attribute` com o atributo `Name` definido como `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**. Você pode usar esse

elemento para passar atributos como tags de sessão na asserção SAML. Para obter mais informações sobre tags de sessão, consulte Passar tags de sessão AWS STS no Guia de usuário do IAM.

Para passar atributos como tags de sessão, inclua o elemento `AttributeValue` que especifica o valor da tag. Por exemplo, para passar o par de valores-chave da tag `CostCenter = blue`, use o seguinte atributo:

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/
AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se você precisar adicionar vários atributos, inclua um elemento `Attribute` separado para cada tag.

Configurar SAML e SCIM com o Okta e o IAM Identity Center

Você pode provisionar automaticamente (sincronizar) informações de usuários e grupos do Okta para o IAM Identity Center usando o protocolo System for Cross-domain Identity Management (SCIM) v2.0. Para configurar essa conexão no Okta, você usa seu endpoint SCIM para o IAM Identity Center e um token de portador que é criado automaticamente pelo IAM Identity Center. Ao configurar a sincronização do SCIM, você cria um mapeamento dos atributos de usuário no Okta para os atributos nomeados no IAM Identity Center. Esse mapeamento faz a correspondência dos atributos de usuário esperados entre o IAM Identity Center e o Okta.

O Okta oferece suporte aos seguintes recursos de provisionamento quando conectado ao IAM Identity Center por meio do SCIM:

- Criar usuários – Os usuários atribuídos ao aplicativo IAM Identity Center no Okta são provisionados no IAM Identity Center.
- Atualizar atributos do usuário – As alterações de atributos para usuários atribuídos ao aplicativo IAM Identity Center no Okta são atualizadas no IAM Identity Center.
- Desativar usuários – Os usuários que não estão atribuídos ao aplicativo IAM Identity Center no Okta são desativados no IAM Identity Center.

- Push de grupo – Os grupos (e seus membros) no Okta são sincronizados com o IAM Identity Center.

> **Note**
>
> Para minimizar a sobrecarga administrativa no Okta e no IAM Identity Center, recomendamos que você atribua e envie por push para grupos em vez de usuários individuais.

Se você ainda não habilitou o IAM Identity Center, consulte Habilitando AWS IAM Identity Center.

Objetivo

Neste tutorial, você aprenderá passo a passo como configurar uma conexão SAML com o Okta IAM Identity Center. Posteriormente, você sincronizará os usuários do Okta usando o SCIM. Nesse cenário, você gerencia todos os usuários e grupos no Okta. Os usuários fazem login pelo Portal de acesso do Okta. Para verificar se tudo está configurado corretamente, depois de concluir as etapas de configuração, você fará login como Okta usuário e verificará o acesso aos AWS recursos.

> **Note**
>
> Você pode se cadastrar em uma conta do Okta (teste gratuito) que tem a aplicação IAM Identity Center do Okta's instalada. Para produtos da Okta pagos, talvez seja necessário confirmar se sua licença do Okta é compatível com gerenciamento do ciclo de vida ou recursos similares que permitam o provisionamento externo. Esses recursos podem ser necessários para configurar o SCIM do Okta para o IAM Identity Center.

Antes de começar

Antes de configurar o provisionamento do SCIM entre Okta e o IAM Identity Center, recomendamos que você primeiro analise. Considerações sobre o uso do provisionamento automático

Confirme os seguintes itens antes de começar:

- Todo usuário do Okta deve ter um valor especificado de Nome, Sobrenome, Nome de usuário e Nome de exibição.

- Todo usuário do Okta tem apenas um valor por atributo de dados, como endereço de e-mail ou número de telefone. Qualquer usuário que tenha vários valores não conseguirá sincronizar. Se houver usuários com vários valores em seus atributos, remova os atributos duplicados antes de tentar provisionar o usuário no IAM Identity Center. Por exemplo, somente um único atributo de número de telefone pode ser sincronizado, já que o atributo de número de telefone padrão é "telefone comercial", use o atributo "telefone comercial" para armazenar o número de telefone do usuário, mesmo que o telefone do usuário seja residencial ou celular.
- Se você atualizar o endereço do usuário, é preciso especificar o valor streetAddress, city, state, zipCode e countryCode. Se algum desses valores não for especificado para o usuário do Okta no momento da sincronização, o usuário (ou as alterações feitas no usuário) não será provisionado.

> **Note**
>
> Os direitos e os atributos de perfil não são compatíveis e não podem ser sincronizados com o IAM Identity Center.
> Atualmente não é possível usar o mesmo grupo do Okta para atribuições e envio automático de grupos. Para manter as associações dos grupos consistentes entre o Okta e o IAM Identity Center, crie um grupo separado e configure-o para enviar automaticamente os grupos para o IAM Identity Center.

Etapa 1: obter os metadados SAML da sua conta do Okta

1. Faça login no Okta admin dashboard, expanda Aplicações e selecione Aplicações.
2. Na página Applications (Aplicações), escolha Browse App Catalog (Navegar pelo App Catalog).
3. Na caixa de pesquisa AWS IAM Identity Center, digite e selecione o aplicativo para adicionar o aplicativo IAM Identity Center.
4. Selecione a guia Fazer login.
5. Em Certificados de assinatura SAML, selecione Ações e depois Visualizar metadados do IdP. Uma nova guia de navegador é aberta mostrando a árvore de documentos de um arquivo XML. Selecione todo o XML de `<md:EntityDescriptor>` a `</md:EntityDescriptor>` e copie-o em um arquivo de texto.
6. Salve o arquivo de texto como `metadata.xml`.

Deixe o Okta admin dashboard aberto, você continuará usando esse console nas etapas posteriores.

Etapa 2: configurar o Okta como fonte de identidades para o IAM Identity Center

1. Abra o console do IAM Identity Center como um usuário com privilégios administrativos.
2. Escolha Configurações no painel de navegação à esquerda.
3. Na página Configurações, escolha Ações e depois Alterar fonte de identidades.
4. Em Escolher fonte de identidade, selecione Escolher fonte de identidade e, depois, Próximo.
5. Em Configurar provedor de identidades externo, faça o seguinte:

   a. Em Metadados do provedor de serviços, escolha Baixar arquivo de metadados para baixar o arquivo de metadados do IAM Identity Center e salvá-lo em seu sistema. Você fornecerá o arquivo de metadados SAML do IAM Identity Center ao Okta posteriormente neste tutorial.

      Copie os seguintes itens em um arquivo de texto para facilitar o acesso:

      - URL do Assertion Consumer Service (ACS) do IAM Identity Center
      - URL do emissor do IAM Identity Center

      Você vai precisar desses valores mais adiante neste tutorial.

   b. Em Metadados do provedor de identidade, em IdP SAML meta, selecione Escolher arquivo e selecione `metadata.xml` o arquivo que você criou na etapa anterior.

   c. Escolha Próximo.
6. Depois de ler a isenção de responsabilidade e estar pronto para continuar, insira ACEITAR.
7. Escolha Alterar origem de identidade.

   Deixe o AWS console aberto, você continuará usando esse console na próxima etapa.
8. Volte para o Okta admin dashboard e selecione a guia Fazer login da aplicação AWS IAM Identity Center e clique em Editar.
9. Em Configurações avançadas de login, insira o seguinte:

   - Em URL do ACS, insira o valor que você copiou para URL do Center Assertion Consumer Service (ACS) do IAM Identity
   - Em URL do emissor, insira o valor que você copiou para URL do emissor do IAM Identity Center
   - Em Formato do nome de usuário da aplicação, selecione uma das opções no menu suspenso.

Faça com que o valor escolhido seja exclusivo para cada usuário. Para este tutorial, selecione o Nome de usuário do Okta

10. Escolha Salvar.

Agora você está pronto para provisionar usuários do Okta no IAM Identity Center. Deixe a Okta admin dashboard janela aberta e retorne ao console do IAM Identity Center para a próxima etapa.

Etapa 3: provisionar usuários do Okta

1. Na página Configurações do console do IAM Identity Center, localize a caixa de informações Provisionamento automático e escolha Habilitar. Isso habilita o provisionamento automático no IAM Identity Center e exibe as informações necessárias do endpoint SCIM e as informações do token de acesso.
2. Na caixa de diálogo Provisionamento automático de entrada, copie os valores para as seguintes opções:

   - Endpoint do SCIM
   - Token de acesso

   Posteriormente neste tutorial, você inserirá esses valores para configurar o provisionamento. Okta
3. Escolha Fechar.
4. Volte para o Okta admin dashboard e navegue até a aplicação IAM Identity Center.
5. Na página do aplicativo IAM Identity Center, escolha a guia Provisionamento e, no painel de navegação à esquerda, em Configurações, escolha Integração.
6. Escolha Editar e, em seguida, marque a caixa de seleção ao lado de Habilitar a integração da API para ativar o provisionamento.
7. Configure Okta com os valores de provisionamento SCIM do IAM Identity Center que você copiou anteriormente neste tutorial:

   a. No campo URL da base, insira o valor do Endpoint SCIM. Certifique-se de remover a barra final no final do URL.

   b. No campo Token da API, insira o valor do Token de acesso.
8. Escolha Testar credenciais da API para verificar se as credenciais inseridas são válidas.

A mensagem O AWS IAM Identity Center foi verificado com sucesso! é exibida.

9. Escolha Salvar. Você será direcionado até a área Configurações, com a opção Integração selecionada.
10. Em Configurações, escolha Para aplicativo e marque a caixa de seleção Habilitar para cada um dos recursos de Provisionamento para aplicativo que você deseja ativar. Para este tutorial, selecione todas as opções.
11. Escolha Salvar.

Agora você está pronto para sincronizar os usuários do Okta com o IAM Identity Center.

Etapa 4: sincronizar os usuários do Okta com o IAM Identity Center

Por padrão, nenhum usuário ou grupo está atribuído à aplicação IAM Identity Center do Okta. Os grupos de aprovisionamento provisionam os usuários que são membros do grupo. Conclua as etapas a seguir para sincronizar os grupos e os usuários com o IAM Identity Center.

1. Na página do aplicativo Okta IAM Identity Center, escolha a guia Atribuições. Você pode atribuir pessoas e grupos à aplicação IAM Identity Center.

   a. Para atribuir pessoas:

      - Na página Atribuições, escolha Atribuir e, em depois, escolha Atribuir a pessoas.
      - Escolha os usuários do Okta que você deseja que tenham acesso à aplicação IAM Identity Center. Escolha Atribuir, Salvar e voltar e escolha Concluído.

      Isso inicia o processo de provisionamento de usuários para o IAM Identity Center.

   b. Para atribuir grupos:

      - Na página Atribuições, escolha Atribuir e depois Atribuir a grupos.
      - Escolha os grupos do Okta que você deseja que tenham acesso à aplicação IAM Identity Center. Escolha Atribuir, Salvar e voltar e escolha Concluído.

      Isso inicia o processo de provisionamento dos usuários do grupo no IAM Identity Center.

> **Note**
>
> Talvez seja necessário especificar atributos adicionais para o grupo se eles não estiverem presentes em todos os registros de usuário. Os atributos especificados para o grupo substituirão os valores dos atributos individuais.

2. Escolha a guia Enviar por push para grupos. Escolha o grupo do Okta que contém todos os grupos que você atribuiu à aplicação IAM Identity Center. Escolha Salvar.

   O status do grupo muda para Ativo depois que o grupo e seus membros são enviados automaticamente para o IAM Identity Center.

3. Volte para a guia Atribuições.

4. Se você tiver usuários que não são membros dos grupos que você enviou automaticamente para o IAM Identity Center, adicione-os individualmente usando as seguintes etapas:

   Na página Atribuições, escolha Atribuir e, em seguida, escolha Atribuir a pessoas.

5. Escolha os usuários do Okta que você deseja que tenham acesso à aplicação IAM Identity Center. Escolha Atribuir, Salvar e voltar e escolha Concluído.

   Isso inicia o processo de provisionamento de usuários individuais para o IAM Identity Center.

   > **Note**
   >
   > Você também pode atribuir usuários e grupos ao AWS IAM Identity Center aplicativo, na página Aplicativos doOkta admin dashboard. Para fazer isso, selecione o ícone de Configurações e escolha Atribuir a usuários ou Atribuir a grupos e especifique o usuário ou o grupo.

6. Volte para o console do IAM Identity Center. No painel de navegação esquerdo, selecione Usuários. Você deve ver a lista de usuários preenchida com seus usuários do Okta.

> **Parabéns!**
>
> Você configurou com êxito uma conexão SAML entre Okta e AWS e verificou se o provisionamento automático está funcionando. Agora você pode atribuir esses usuários a contas no IAM Identity Center. Para este tutorial, na próxima etapa, vamos designar um

dos usuários como administrador do IAM Identity Center, concedendo a ele permissões administrativas para a conta de gerenciamento.

Etapa 5: conceder aos usuários do Okta acesso a contas

1. No painel de navegação do IAM Identity Center, em Permissões multicontas, escolha Contas da AWS.
2. Na página Contas da AWS, a Estrutura organizacional exibe a raiz organizacional com as contas abaixo dela na hierarquia. Marque a caixa de seleção da conta de gerenciamento e selecione Atribuir usuários ou grupos.
3. O fluxo de trabalho Atribuir usuários e grupos é exibido. Ele consiste em três etapas:

   a. Em Etapa 1: selecionar usuários e grupos, escolha o usuário que desempenhará a função de administrador. Em seguida, escolha Próximo.

   b. Em Etapa 2: selecionar conjuntos de permissões, escolha Criar conjunto de permissões para abrir uma nova guia que orienta você pelas três subetapas envolvidas na criação de um conjunto de permissões.

      i. Em Etapa 1: selecionar o tipo de conjunto de permissões, preencha o seguinte:

         - Em Tipo de conjunto de permissões, escolha Conjunto de permissões predefinido.
         - Em Política para conjunto de permissões predefinido, escolha AdministratorAccess.

         Escolha Próximo.

      ii. Em Etapa 2: especificar detalhes do conjunto de permissões, mantenha as configurações padrão e escolha Avançar.

         As configurações padrão criam um conjunto de permissões chamado *`AdministratorAccess`*com a duração da sessão definida em uma hora.

      iii. Para a Etapa 3: revisar e criar, verifique se o tipo de conjunto de permissões usa a política AWS gerenciada AdministratorAccess. Escolha Criar. Na página Conjuntos de permissões, aparece uma notificação informando que o conjunto de permissões foi criado. Você agora pode fechar essa guia do navegador.

Na guia Atribuir usuários e grupos do navegador, você ainda está na Etapa 2: selecionar conjuntos de permissões na qual você iniciou o fluxo de trabalho de criação do conjunto de permissões.

Na área Conjuntos de permissões, escolha o botão Atualizar. O conjunto de *AdministratorAccess*permissões que você criou aparece na lista. Marque a caixa de seleção do conjunto de permissões e escolha Avançar.

c. Em Etapa 3: revisar e enviar, revise o usuário e o conjunto de permissões selecionados e escolha Enviar.

A página é atualizada com uma mensagem informando que a sua Conta da AWS está sendo configurada. Aguarde a conclusão do processo.

Você retornará à Contas da AWS página. Uma mensagem de notificação informa que a sua Conta da AWS foi reprovisionada e que o conjunto de permissões atualizado foi aplicado. Quando o usuário fizer login, ele terá a opção de escolher a *AdministratorAccess*função.

> **Note**
>
> A sincronização automática SCIM do Okta só é compatível com o provisionamento de usuários; os grupos não são provisionados automaticamente. Você não pode criar grupos para os usuários do Okta usando o AWS Management Console. Após provisionar os usuários, você pode criar grupos usando uma operação da CLI ou da API

Etapa 6: confirmar o acesso Okta dos usuários aos AWS recursos

1. Faça login no Okta dashboard usando uma conta de usuário de teste.
2. Em Minhas aplicações, selecione o ícone do AWS IAM Identity Center.
3. Você está conectado ao portal e pode ver o Conta da AWS ícone. Expanda esse ícone para ver a lista Contas da AWS que o usuário pode acessar. Neste tutorial, você só trabalhou com uma conta, portanto, a expansão do ícone só mostra uma conta.
4. Selecione a conta para exibir os conjuntos de permissões disponíveis para o usuário. Neste tutorial, você criou o conjunto de AdministratorAccesspermissões.

5. Ao lado do conjunto de permissões, há links para o tipo de acesso disponível para aquele conjunto de permissões. Ao criar o conjunto de permissões, você especificou que o console de gerenciamento e o acesso programático fossem habilitados, assim sendo, essas duas opções estão presentes. Selecione Console de gerenciamento para abrir o AWS Management Console.
6. O usuário fez login no console.

(Opcional) Passar atributos para controle de acesso

Opcionalmente, você pode usar o atributo Atributos para controle de acesso no IAM Identity Center para passar um elemento `Attribute` com o atributo `Name` definido como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento permite que você passe atributos como tags de sessão na declaração do SAML. Para obter mais informações sobre tags de sessão, consulte Passar tags de sessão AWS STS no Guia de usuário do IAM.

Para passar atributos como tags de sessão, inclua o elemento `AttributeValue` que especifica o valor da tag. Por exemplo, para passar o par chave-valor de tag `CostCenter = blue`, use o atributo a seguir.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se você precisar adicionar vários atributos, inclua um elemento separado `Attribute` para cada tag.

Próximas etapas

Agora que você configurou o Okta como provedor de identidades e provisionou usuários no IAM Identity Center, você pode:

- Conceda acesso a Contas da AWS, vejaAtribuir acesso de usuário a Contas da AWS.
- Conceder acesso a aplicações na nuvem, consulte Atribuir acesso de usuário às aplicações no console do IAM Identity Center.
- Configurar permissões baseadas nas funções do trabalho, consulte Criar um conjunto de permissões

Configurar o provisionamento SCIM entre o OneLogin e o IAM Identity Center

O IAM Identity Center oferece suporte ao provisionamento automático (sincronização) de informações de usuários e grupos do seu OneLogin no IAM Identity Center usando o protocolo System for Cross-domain Identity Management (SCIM) v2.0. Você configura essa conexão em OneLogin usando seu endpoint SCIM para o IAM Identity Center e um token portador que é criado automaticamente pelo IAM Identity Center. Ao configurar a sincronização do SCIM, você cria um mapeamento dos atributos do usuário no OneLogin para os atributos nomeados no IAM Identity Center. Isso faz com que os atributos esperados correspondam entre o IAM Identity Center e OneLogin.

As etapas a seguir explicam como habilitar o provisionamento automático de usuários e grupos do OneLogin para o IAM Identity Center usando o protocolo SCIM.

> **Note**
>
> Antes de começar a implantar o SCIM, é recomendável que você analise Considerações sobre o uso do provisionamento automático antes.

Tópicos

Pré-requisitos

Você precisará do seguinte antes de começar:

- Uma conta do OneLogin. Se você não tiver uma conta existente, poderá obter uma conta de teste gratuita ou de desenvolvedor no site do OneLogin.

- Uma conta habilitada para o IAM Identity Center (gratuita). Para obter mais informações, consulte Habilitar o IAM Identity Center.
- Uma conexão SAML da sua conta do OneLogin com o IAM Identity Center. Para obter mais informações, consulte Habilitando o login único entre OneLogin e AWS no blog AWS Partner Network.

Etapa 1: Habilitar provisionamento no IAM Identity Center

Nesta primeira etapa, você usa o console do IAM Identity Center para ativar o provisionamento automático.

Para habilitar o provisionamento automático no IAM Identity Center

1. Depois de concluir os pré-requisitos, abra o console do IAM Identity Center.
2. Escolha Configurações no painel de navegação à esquerda.
3. Na página Configurações, localize a caixa de informações Provisionamento automático e selecione Habilitar. Isso habilita imediatamente o provisionamento automático no IAM Identity Center e exibe as informações necessárias do endpoint SCIM e do token de acesso.
4. Na caixa de diálogo Provisionamento automático de entrada, copie cada um dos valores para as opções a seguir. Você precisará colá-los posteriormente ao configurar o provisionamento em seu IdP.
    a. Endpoint do SCIM
    b. Token de acesso
5. Escolha Fechar.

Você já configurou provisionamento no console do IAM Identity Center. Agora você precisa executar as tarefas restantes usando o console administrativo OneLogin conforme descrito no procedimento a seguir.

Etapa 2: Configure o provisionamento no OneLogin

Use o procedimento a seguir no console de admin do OneLogin para permitir a integração entre o IAM Identity Center e o aplicativo IAM Identity Center. Esse procedimento pressupõe que você já tenha configurado o aplicativo AWS Single Sign-On no OneLogin para autenticação SAML. Se você ainda não criou essa conexão SAML, faça isso antes de continuar e depois volte aqui para concluir o

processo de provisionamento do SCIM. Para obter mais informações sobre como configurar o SAML com OneLogin, consulte Habilitando o login único entre OneLogin e AWS no AWS Partner Network Blog.

Para configurar o provisionamento no OneLogin

1. Faça login em OneLogin, e em seguida navegue até Aplicativos > Aplicativos.
2. Na página Aplicativos, pesquise o aplicativo que você criou anteriormente para formar sua conexão SAML com o IAM Identity Center. Escolha isso e depois escolhaConfiguration na barra de navegação esquerda.
3. No procedimento anterior, você copiou o valor do endpoint SCIM do IAM Identity Center. Cole esse valor no campo URL base do SCIM em OneLogin. Certifique-se de remover a barra final no final do URL. Além disso, no procedimento anterior, você copiou o valor do Token de acesso do IAM Identity Center. Cole esse valor no campo SCIM Bearer Token no OneLogin.
4. Ao lado de Conexão de API, clique em Ativar e, em seguida, clique em Salvar para concluir a configuração.
5. Na barra de navegação à esquerda, escolha Provisionamento.
6. Marque as caixas de seleção Ativar provisionamento, Criar usuário, Excluir usuário e Atualizar usuário e, em seguida, escolha Salvar.
7. Na barra de navegação esquerda, selecione Usuários.
8. Clique em Mais ações e escolha Sincronizar logins. Você deve receber a mensagem Sincronizando usuários com AWS login único.
9. Clique em Mais ações novamente e escolha Reaplicar mapeamentos de direitos. Você deve receber a mensagem Mapeamentos estão sendo reaplicados.
10. Nesse ponto, o processo de provisionamento deve começar. Para confirmar isso, navegue até Atividade > Eventos e monitore o progresso. Eventos de provisionamento bem-sucedidos, bem como erros, devem aparecer no fluxo de eventos.
11. Para verificar se seus usuários e grupos foram sincronizados com sucesso com o IAM Identity Center, retorne ao console do IAM Identity Center e escolha Usuários. Seus usuários sincronizados do OneLogin aparecem na página Usuários. Você também pode ver seus grupos sincronizados na página Grupos.
12. Para sincronizar automaticamente as alterações do usuário no IAM Identity Center, navegue até a página Provisionamento, localize a seção Exigir aprovação do administrador antes que essa ação seja executada, desmarque Criar usuário, Excluir usuário, e/ou Atualizar usuário, e clique em Salvar.

(Opcional) Etapa 3: configure atributos do usuário no OneLogin para controle de acesso no IAM Identity Center

Esse é um procedimento opcional para o OneLogin se você escolher configurar atributos que usará no IAM Identity Center para gerenciar o acesso aos seus recursos da AWS. Os atributos que você define no OneLogin são passados em uma declaração de SAML para o IAM Identity Center. Em seguida, você criará um conjunto de permissões no IAM Identity Center para gerenciar o acesso com base nos atributos que você passou do OneLogin.

Antes de iniciar este procedimento, você deve primeiro habilitar o atributo Atributos para controle de acesso. Para obter mais informações sobre como fazer isso, consulte Habilite e configure atributos para controle de acesso.

Para configurar atributos do usuário em OneLogin para controle de acesso no IAM Identity Center

1. Faça login em OneLogin, e em seguida navegue até Aplicativos > Aplicativos.
2. Na página Aplicativos, pesquise o aplicativo que você criou anteriormente para formar sua conexão SAML com o IAM Identity Center. Selecione e, depois, escolha Parâmetros na barra de navegação à esquerda.
3. Na seção Parâmetros obrigatórios, faça o seguinte para cada atributo que você deseja usar no IAM Identity Center:
   a. Escolha +.
   b. Em Nome do campo, insira `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**, e substitua **`AttributeName`** pelo nome do atributo que você está esperando no IAM Identity Center. Por exemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**.
   c. Em Sinalizadores, marque a caixa ao lado de Incluir na declaração SAML e escolha Salvar.
   d. No campo Valor, use a lista suspensa para escolher os atributos do usuário OneLogin. Por exemplo, Departamento.
4. Escolha Salvar.

(Opcional) Passar atributos para controle de acesso

Opcionalmente, você pode usar o atributo Atributos para controle de acesso no IAM Identity Center para passar um elemento `Attribute` com o atributo `Name` definido como `https://`

`aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento permite que você passe atributos como tags de sessão na declaração do SAML. Para obter mais informações sobre tags de sessão, consulte Passar tags de sessão AWS STS no Guia de usuário do IAM.

Para passar atributos como tags de sessão, inclua o elemento `AttributeValue` que especifica o valor da tag. Por exemplo, para passar o par chave-valor de tag `CostCenter = blue`, use o atributo a seguir.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se você precisar adicionar vários atributos, inclua um elemento separado `Attribute` para cada tag.

Solução de problemas

O seguinte pode ajudá-lo a solucionar alguns problemas comuns que você pode encontrar ao configurar o provisionamento automático com o OneLogin.

Os grupos não são provisionados para o IAM Identity Center

Por padrão, os grupos não podem ser provisionados a partir do IAM Identity Center do OneLogin. Certifique-se de ter habilitado o provisionamento de grupos para seu aplicativo IAM Identity Center no OneLogin. Para fazer isso, faça login no console de administrador do OneLogin e verifique se a opção Incluir no provisionamento de usuários está selecionada nas propriedades do aplicativo IAM Identity Center (aplicativo IAM Identity Center > Parâmetros > Grupos). Para obter mais detalhes sobre como criar grupos no OneLogin, incluindo como sincronizar funções do OneLogin como grupos no SCIM, consulte o site do OneLogin site.

Nada é sincronizado do OneLogin para o IAM Identity Center, apesar de todas as configurações estarem corretas

Além da observação acima sobre a aprovação do administrador, você precisará reaplicar os mapeamentos de direitos para que muitas alterações de configuração entrem em vigor. Isso pode ser encontrado em Aplicativos > Aplicativos > Aplicativo IAM Identity Center > Mais ações. Você pode ver detalhes e registros da maioria das ações no OneLogin, incluindo eventos de sincronização, em Atividade > Eventos.

Excluí ou desativei um grupo no OneLogin, mas ele ainda aparece no IAM Identity Center

Atualmente, o OneLogin não suporta a operação SCIM DELETE para grupos, o que significa que o grupo continua existindo no IAM Identity Center. Portanto, você deve remover o grupo diretamente do IAM Identity Center para garantir que todas as permissões correspondentes no IAM Identity Center desse grupo sejam removidas.

Excluí um grupo no IAM Identity Center sem primeiro excluí-lo no OneLogin, e agora estou tendo problemas de sincronização de usuários/grupos

Para corrigir essa situação, primeiro verifique se você não tem nenhuma regra ou configuração redundante de provisionamento de grupos. no OneLogin Por exemplo, um grupo atribuído diretamente a um aplicativo junto com uma regra que publica no mesmo grupo. Em seguida, exclua todos os grupos indesejáveis no IAM Identity Center. Por fim, no OneLogin, atualize os direitos (aplicativo IAM Identity Center > Provisionamento > Direitos) e, em seguida, reaplique os mapeamentos de direitos (Aplicativo IAM Identity Center > Mais ações). Para evitar esse problema no futuro, primeiro faça a alteração para parar de provisionar o grupo no OneLogin, em seguida, exclua o grupo do IAM Identity Center.

Usar produtos de Ping Identity com o IAM Identity Center

Os produtos Ping Identity a seguir foram testados com o IAM Identity Center.

Tópicos

PingFederate

O IAM Identity Center oferece suporte ao provisionamento automático (sincronização) das informações do usuário e grupo a partir do produto PingFederate do Ping Identity (doravante “Ping“) para o IAM Identity Center. Esse provisionamento usa o protocolo System for Cross-domain Identity Management (SCIM) v2.0. Você configura essa conexão no PingFederate usando seu endpoint e token de acesso do IAM Identity Center SCIM. Ao configurar a sincronização do SCIM, você cria um mapeamento dos atributos do usuário no PingFederate para os atributos nomeados no IAM Identity Center. Isso faz com que os atributos esperados correspondam entre o IAM Identity Center e PingFederate.

Este guia é baseado na versão 10.2 do PingFederate. As etapas para outras versões podem variar. Entre em contato com o Ping para obter mais informações sobre como configurar o provisionamento no IAM Identity Center para outras versões do PingFederate.

As etapas a seguir explicam como habilitar o provisionamento automático de usuários e grupos do PingFederate para o IAM Identity Center usando o protocolo SCIM.

> **Note**
>
> Antes de começar a implantar o SCIM, é recomendável que você analise Considerações sobre o uso do provisionamento automático antes. Em seguida, continue analisando considerações adicionais na próxima seção.

Tópicos

Pré-requisitos

Você precisará do seguinte antes de começar:

- Um servidor do PingFederate em funcionamento. Se você não tiver um servidor do PingFederate, poderá obter uma conta de teste gratuita ou de desenvolvedor no site do Ping Identity. O teste inclui licenças e downloads de software e documentação associada.
- Uma cópia do software IAM Identity Center Connector do PingFederate instalado em seu servidor do PingFederate. Para obter mais informações sobre como obter esse software, consulte IAM Identity Center Connector no site do Ping Identity.
- Uma conta habilitada para o IAM Identity Center (gratuita). Para obter mais informações, consulte Habilitar o IAM Identity Center.

- Uma conexão SAML da sua instância do PingFederate com o IAM Identity Center. Para obter mais instruções sobre como configurar essa conexão, consulte a documentação PingFederate. Em resumo, o caminho recomendado é usar o IAM Identity Center Connector para configurar o "SSO do navegador" no PingFederate, usando os recursos de "baixar" e "importar" metadados em ambas as extremidades para trocar metadados SAML entre o PingFederate e o IAM Identity Center.

Considerações adicionais

A seguir estão considerações importantes sobre o PingFederate isso que podem afetar a forma como você implementa o provisionamento com o IAM Identity Center.

- Se um atributo (como um número de telefone) for removido de um usuário no armazenamento de dados configurado no PingFederate, esse atributo não será removido do usuário correspondente no IAM Identity Center. Essa é uma limitação conhecida na implementação do provisionador do PingFederate's. Se um atributo for alterado para um valor diferente (não vazio) em um usuário, essa alteração será sincronizada com o IAM Identity Center.

Etapa 1: Habilitar provisionamento no IAM Identity Center

Nesta primeira etapa, você usa o console do IAM Identity Center para ativar o provisionamento automático.

Para habilitar o provisionamento automático no IAM Identity Center

1. Depois de concluir os pré-requisitos, abra o console do IAM Identity Center.
2. Escolha Configurações no painel de navegação à esquerda.
3. Na página Configurações, localize a caixa de informações Provisionamento automático e selecione Habilitar. Isso habilita imediatamente o provisionamento automático no IAM Identity Center e exibe as informações necessárias do endpoint SCIM e do token de acesso.
4. Na caixa de diálogo Provisionamento automático de entrada, copie cada um dos valores para as opções a seguir. Você precisará colá-los posteriormente ao configurar o provisionamento em seu IdP.
    a. Endpoint do SCIM
    b. Token de acesso
5. Escolha Fechar.

Agora que você configurou o provisionamento no console do IAM Identity Center, você deve concluir as tarefas restantes usando o console administrativo do PingFederate. As etapas estão descritas no procedimento a seguir.

Etapa 2: Configure o provisionamento no PingFederate

Use o procedimento a seguir no console administrativo do PingFederate para permitir a integração entre o IAM Identity Center e o IAM Identity Center Connector. Esse procedimento pressupõe que você já instalou o software do IAM Identity Center Connector. Se você ainda não tiver feito isso, consulte Pré-requisitos e conclua este procedimento para configurar o provisionamento do SCIM.

> **Important**
>
> Se seu servidor do PingFederate não tiver sido configurado anteriormente para provisionamento SCIM de saída, talvez seja necessário fazer uma alteração no arquivo de configuração para habilitar o provisionamento. Para obter mais informações, consulte a documentação do Ping. Em resumo, você deve modificar a configuração `pf.provisioner.mode` no arquivo pingfederate-<version>/pingfederate/bin/run.properties com um valor diferente de `OFF` (que é o padrão) e reiniciar o servidor se ele estiver em execução. Por exemplo, você pode optar por usar `STANDALONE` se não tiver uma configuração de alta disponibilidade no PingFederate.

Para configurar o provisionamento no PingFederate

1. Faça login no console administrativo do PingFederate.
2. Selecione Aplicativos na parte superior da página e clique em Conexões SP.
3. Localize o aplicativo que você criou anteriormente para formar sua conexão SAML com o IAM Identity Center e clique no nome da conexão.
4. Selecione Tipo de conexão nos cabeçalhos de navegação escuros próximos à parte superior da página. Você verá o SSO do navegador já selecionado na configuração anterior do SAML. Caso contrário, você deve concluir essas etapas primeiro antes de continuar.
5. Marque a caixa de seleção Provisionamento de saída, escolha IAM Identity Center Cloud Connector como o tipo e clique em Salvar. Se o IAM Identity Center Cloud Connector não aparecer como uma opção, verifique se você instalou o IAM Identity Center Connector e reiniciou seu servidor do PingFederate.

6. Clique em Próximo repetidamente até chegar à página Provisionamento de saída e, em seguida, clique no botão Configurar provisionamento.
7. No procedimento anterior, você copiou o valor do endpoint SCIM do IAM Identity Center. Cole esse valor no campo URL do SCIM no PingFederate console. Certifique-se de remover a barra final no final do URL. Além disso, no procedimento anterior, você copiou o valor do Token de acesso do IAM Identity Center. Cole esse valor no campo Token de acesso no PingFederate console. Clique em Salvar.
8. Na página Configuração de canais (Configurar canais), clique em Criar.
9. Insira o Nome de canal desse novo canal de provisionamento (como**`AWSIAMIdentityCenterchannel`**) e clique em Próximo.
10. Na página Fonte, escolha o Armazenamento de dados ativo que você deseja usar para sua conexão com o IAM Identity Center e clique em Próximo.

> **Note**
>
> Se você ainda não configurou uma fonte de dados, faça isso agora. Consulte a documentação do produto Ping para obter informações sobre como escolher e configurar uma fonte de dados no PingFederate.

11. Na página Configurações de fonte, confirme se todos os valores estão corretos para sua instalação e clique em Próximo.
12. Na página Localização da Fonte, insira as configurações apropriadas à sua fonte de dados e clique em Próximo. Por exemplo, se estiver usando o Active Directory como um diretório LDAP:
    a. Insira o DN base da sua floresta do AD (por exemplo, **`DC=myforest,DC=mydomain,DC=com`**).
    b. Em Usuários > DN do Grupo, especifique um único grupo que contenha todos os usuários que você deseja provisionar para o IAM Identity Center. Se esse grupo único não existir, crie esse grupo no AD, retorne a essa configuração e insira o DN correspondente.
    c. Especifique se deseja pesquisar subgrupos (Pesquisa aninhada) e qualquer filtro LDAP necessário.
    d. Em Grupos > DN do Grupo, especifique um único grupo que contenha todos os grupos que você deseja provisionar para o IAM Identity Center. Em muitos casos, esse pode ser o mesmo DN que você especificou na seção Usuários. Insira os valores de Pesquisa aninhada e Filtro conforme necessário.

13. Na página Mapeamento de atributos, verifique o seguinte e clique em Próximo:

    a. O campo Nome de usuário deve ser mapeado para um Atributo formatado como um e-mail (user@domain.com). Ele também deve corresponder ao valor que o usuário usará para fazer login no Ping. Esse valor, por sua vez, é preenchido na declaração SAML `nameId` durante a autenticação federada e usado para corresponder ao usuário no IAM Identity Center. Por exemplo, ao usar o Active Directory, você pode optar por especificar o `UserPrincipalName` como o Nome de usuário.

    b. Outros campos com o sufixo * devem ser mapeados para atributos que não sejam nulos para seus usuários.

14. Na página Ativação e resumo, defina o Status do canal como Ativo para fazer com que a sincronização comece imediatamente após a configuração ser salva.
15. Confirme se todos os valores de configuração na página estão corretos e clique em Concluído.
16. Na página Gerenciar canais, clique em Salvar.
17. Nesse ponto, o provisionamento começa. Para confirmar a atividade, você pode visualizar o arquivo provisioner.log, localizado por padrão no diretório pingfederate-<version>/pingfederate/log do seu servidor do PingFederate.
18. Para verificar se os usuários e grupos foram sincronizados com sucesso com o IAM Identity Center, retorne ao console do IAM Identity Center e escolha Usuários. Os usuários sincronizados do PingFederate aparecem na página Usuários. Você também pode ver os grupos sincronizados na página Grupos.

(Opcional) Etapa 3: configurar os atributos do usuário em PingFed erate para controle de acesso no IAM Identity Center

Esse é um procedimento opcional para o PingFederate se você escolher configurar atributos que usará no IAM Identity Center para gerenciar o acesso aos seus recursos da AWS. Os atributos que você define no PingFederate são passados em uma declaração de SAML para o IAM Identity Center. Em seguida, você criará um conjunto de permissões no IAM Identity Center para gerenciar o acesso com base nos atributos que você passou do PingFederate.

Antes de iniciar este procedimento, você deve primeiro habilitar o atributo Atributos para controle de acesso. Para obter mais informações sobre como fazer isso, consulte Habilite e configure atributos para controle de acesso.

Para configurar atributos do usuário em PingFederate para controle de acesso no IAM Identity Center

1. Faça login no console administrativo do PingFederate.
2. Escolha Aplicativos na parte superior da página e clique em Conexões SP.
3. Localize o aplicativo que você criou anteriormente para formar sua conexão SAML com o IAM Identity Center e clique no nome da conexão.
4. Selecione SSO do navegador nos cabeçalhos de navegação escuros próximos à parte superior da página. Em seguida, clique em Configurar SSO do navegador.
5. Na página Configurar SSO do Navegador, escolha Criação de asserção e clique em Configurar criação de asserção.
6. Na página Configurar criação de asserção, escolha Contrato de atributo.
7. Na página Contrato de atributo, na seção Estender o contrato, adicione um novo atributo executando as seguintes etapas:

   a. No campo de texto, digite `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`** e substitua **`AttributeName`** pelo nome do atributo que você está esperando no IAM Identity Center. Por exemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**.

   b. Em Formato do nome do atributo, escolha urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

   c. Escolha Adicionar e a seguir Próximo.
8. Na página Mapeamento da fonte de autenticação, escolha a instância do adaptador configurada com seu aplicativo.
9. Na página Atendimento ao Contrato de Atributo, escolha a Fonte (armazenamento de dados) e o Valor (atributo do armazenamento de dados) para o Contrato de Atributo `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**.

   > **Note**
   >
   > Se você ainda não configurou uma fonte de dados, será necessário fazer isso agora. Consulte a documentação do produto Ping para obter informações sobre como escolher e configurar uma fonte de dados no PingFederate.

10. Clique em Próximo repetidamente até chegar à página Ativação e Resumo e, em seguida, clique em Salvar.

(Opcional) Passar atributos para controle de acesso

Opcionalmente, você pode usar o atributo Atributos para controle de acesso no IAM Identity Center para passar um elemento `Attribute` com o atributo `Name` definido como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento permite que você passe atributos como tags de sessão na declaração do SAML. Para obter mais informações sobre tags de sessão, consulte Passar tags de sessão AWS STS no Guia de usuário do IAM.

Para passar atributos como tags de sessão, inclua o elemento `AttributeValue` que especifica o valor da tag. Por exemplo, para passar o par chave-valor de tag `CostCenter = blue`, use o atributo a seguir.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se você precisar adicionar vários atributos, inclua um elemento separado `Attribute` para cada tag.

PingOne

O IAM Identity Center oferece suporte ao provisionamento automático (sincronização) das informações do usuário a partir do produto PingOne do Ping Identity (doravante “Ping“) para o IAM Identity Center. Esse provisionamento usa o protocolo System for Cross-domain Identity Management (SCIM) v2.0. Você configura essa conexão no PingOne usando seu endpoint e token de acesso do IAM Identity Center SCIM. Ao configurar a sincronização do SCIM, você cria um mapeamento dos atributos do usuário no PingOne para os atributos nomeados no IAM Identity Center. Isso faz com que os atributos esperados correspondam entre o IAM Identity Center e PingOne.

Este guia é baseado no PingOne em outubro de 2020. As etapas para versões mais recentes podem variar. Entre em contato com o Ping para obter mais informações sobre como configurar o provisionamento no IAM Identity Center para outras versões do PingOne. Este guia também contém algumas notas sobre a configuração da autenticação do usuário por meio do SAML.

As etapas a seguir explicam como ativar o provisionamento automático de usuários do PingOne para o IAM Identity Center usando o protocolo SCIM.

> **Note**
>
> Antes de começar a implantar o SCIM, é recomendável que você analise Considerações sobre o uso do provisionamento automático antes. Em seguida, continue analisando considerações adicionais na próxima seção.

Tópicos

Pré-requisitos

Você precisará do seguinte antes de começar:

- Uma assinatura ou teste gratuito do PingOne, com recursos de autenticação federada e provisionamento. Para obter mais informações sobre como obter um teste gratuito, consulte o site do Ping Identity.
- Uma conta habilitada para o IAM Identity Center (gratuita). Para obter mais informações, consulte Habilitar o IAM Identity Center.
- O aplicativo IAM Identity Center do PingOne foi adicionado ao seu portal de administrador do PingOne. Você pode obter o aplicativo IAM Identity Center do PingOne no catálogo de aplicativos do PingOne. Para obter informações gerais, consulte Adicionar um aplicativo do catálogo de aplicativos no site do Ping Identity.
- Uma conexão SAML da sua instância do PingOne com o IAM Identity Center. Depois que o aplicativo IAM Identity Center do PingOne for adicionado ao seu portal administrativo do PingOne, você deverá usá-lo para configurar uma conexão SAML da sua instância do PingOne com o IAM Identity Center. Use o recurso de “baixar” e “importar” metadados nas duas extremidades para trocar metadados SAML entre o PingOne e o IAM Identity Center. Para obter mais instruções sobre como configurar essa conexão, consulte a documentação PingOne.

Considerações adicionais

A seguir estão considerações importantes sobre o PingOne isso que podem afetar a forma como você implementa o provisionamento com o IAM Identity Center.

- Em outubro de 2020, o PingOne não oferece suporte ao provisionamento de grupos por meio do SCIM. Entre em contato com o Ping para obter as informações mais recentes sobre suporte de grupo no SCIM do PingOne.
- Os usuários podem continuar sendo provisionados no PingOne após a desativação do provisionamento no portal administrativo do PingOne. Se você precisar encerrar o provisionamento imediatamente, exclua o token portador do SCIM relevante e/ou desative Provisionamento automático no IAM Identity Center.
- Se um atributo for removido de um usuário no armazenamento de dados configurado no PingOne, esse atributo não será removido do usuário correspondente no IAM Identity Center. Essa é uma limitação conhecida na implementação do provisionador do PingOne's. Se um atributo for modificado, a alteração será sincronizada com o IAM Identity Center.
- A seguir estão observações importantes sobre sua configuração de SAML no PingOne:
  - O IAM Identity Center é compatível somente como `emailaddress` no formato `NameId`. Isso significa que você precisa escolher um atributo de usuário que seja exclusivo em seu diretório no PingOne, não nulo e formatado como um e-mail/UPN (por exemplo, user@domain.com) para seu mapeamento SAML_SUBJECT no PingOne. E-mail (comercial) é um valor razoável para usar em configurações de teste com o diretório integrado do PingOne.
  - Usuários do PingOne com um endereço de e-mail contendo um caractere + podem não conseguir entrar no IAM Identity Center, apresentando erros como `'SAML_215'` ou `'Invalid input'`. Para corrigir isso, no PingOne, escolha a opção Avançado para o mapeamento SAML_SUBJECT em Mapeamentos de atributos. Em seguida, defina o Formato de ID do Nome para enviar para SP: para urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress no menu suspenso.

Etapa 1: Habilitar provisionamento no IAM Identity Center

Nesta primeira etapa, você usa o console do IAM Identity Center para ativar o provisionamento automático.

Para habilitar o provisionamento automático no IAM Identity Center

1. Depois de concluir os pré-requisitos, abra o console do IAM Identity Center.

2. Escolha Configurações no painel de navegação à esquerda.
3. Na página Configurações, localize a caixa de informações Provisionamento automático e selecione Habilitar. Isso habilita imediatamente o provisionamento automático no IAM Identity Center e exibe as informações necessárias do endpoint SCIM e do token de acesso.
4. Na caixa de diálogo Provisionamento automático de entrada, copie cada um dos valores para as opções a seguir. Você precisará colá-los posteriormente ao configurar o provisionamento em seu IdP.

    a. Endpoint do SCIM

    b. Token de acesso
5. Escolha Fechar.

Agora que você configurou o provisionamento no console do IAM Identity Center, precisa concluir as tarefas restantes usando o aplicativo IAM Identity Center do PingOne. Essas etapas são descritas no procedimento a seguir.

Etapa 2: Configure o provisionamento no PingOne

Use o procedimento a seguir no aplicativo IAM Identity Center do PingOne para habilitar o provisionamento com o IAM Identity Center. Esse procedimento pressupõe que você já tenha adicionado o aplicativo IAM Identity Center do PingOne ao seu console de administração do PingOne. Se você ainda não tiver feito isso, consulte Pré-requisitos e conclua este procedimento para configurar o provisionamento do SCIM.

Para configurar o provisionamento no PingOne

1. Abra o aplicativo IAM Identity Center do PingOne que você instalou como parte da configuração do SAML para o PingOne (Aplicativos > Meus aplicativos). Consulte Pré-requisitos.
2. Role até o final da página. Em Provisionamento de usuários, escolha o link completo para navegar até a configuração de provisionamento de usuários da sua conexão.
3. Na página Instruções de provisionamento, escolha Continuar para a próxima etapa.
4. No procedimento anterior, você copiou o valor do endpoint SCIM do IAM Identity Center. Cole esse valor no campo URL do SCIM no aplicativo IAM Identity Center do PingOne. Certifique-se de remover a barra final no final do URL. Além disso, no procedimento anterior, você copiou o valor do Token de acesso do IAM Identity Center. Cole esse valor no campo ACCESS_TOKEN no aplicativo IAM Identity Center do PingOne.

5. Para REMOVE_ACTION, escolha Desabilitado ou Excluído (consulte o texto descritivo na página para obter mais detalhes).
6. Na página Mapeamento de atributos, escolha um valor a ser usado para a declaração SAML_SUBJECT (`NameId`), seguindo as orientações do Considerações adicionais início desta página. Em seguida, selecione Avançar para a próxima etapa.
7. Na página PingOne App Customization - IAM Identity Center, faça as alterações de personalização desejadas (opcional) e clique em Continuar para a próxima etapa.
8. Na página Acesso ao grupo, escolha os grupos que contêm os usuários que você gostaria de habilitar para provisionamento e login único no IAM Identity Center. Selecione Avançar para a próxima etapa.
9. Navegue até o final da página e escolha Finalizar para iniciar o provisionamento.
10. Para verificar se os usuários foram sincronizados com sucesso com o IAM Identity Center, retorne ao console do IAM Identity Center e escolha Usuários. Os usuários sincronizados do PingOne aparecerão na página Usuários. Agora, esses usuários podem ser atribuídos a contas e e aplicativos no IAM Identity Center.

    Lembre-se de que o PingOne não oferece suporte ao provisionamento de grupos ou associações de grupos por meio do SCIM. Entre em contato Ping para obter mais informações.

(Opcional) Etapa 3: configure atributos do usuário no PingOne para controle de acesso no IAM Identity Center

Esse é um procedimento opcional PingOne se você optar por configurar atributos do IAM Identity Center para gerenciar o acesso aos seus AWS recursos. Os atributos que você define no PingOne são passados em uma declaração de SAML para o IAM Identity Center. Em seguida, você cria um conjunto de permissões no IAM Identity Center para gerenciar o acesso com base nos atributos dos quais você passou do PingOne.

Antes de iniciar este procedimento, você deve primeiro habilitar o atributo Atributos para controle de acesso. Para obter mais informações sobre como fazer isso, consulte Habilite e configure atributos para controle de acesso.

Para configurar atributos do usuário em PingOne para controle de acesso no IAM Identity Center

1. Abra o aplicativo IAM Identity Center do PingOne que você instalou como parte da configuração do SAML para o PingOne (Aplicativos > Meus aplicativos).

2. Escolha Editar e, em seguida, escolha Avançar para a próxima etapa até chegar à página Mapeamentos de atributos.
3. Na página Mapeamentos de atributos, escolha Adicionar novo atributo e faça o seguinte. Você deve executar essas etapas para cada atributo que adicionar para usar no IAM Identity Center para controle de acesso.

    a. No campo Atributo do aplicativo, insira `https://aws.amazon.com/SAML/Attributes/AccessControl:`*`AttributeName`*. Substitua *`AttributeName`* pelo nome do atributo que você espera no IAM Identity Center. Por exemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**.

    b. No campo Atributo da ponte de identidade ou Valor literal, escolha os atributos do usuário em seu diretório do PingOne. Por exemplo, E-mail (trabalho).
4. Escolha Próximo algumas vezes e, em seguida, escolha Finalizar.

(Opcional) Passar atributos para controle de acesso

Opcionalmente, você pode usar o atributo Atributos para controle de acesso no IAM Identity Center para passar um elemento `Attribute` com o atributo `Name` definido como `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**. Este elemento permite que você passe atributos como tags de sessão na declaração do SAML. Para obter mais informações sobre tags de sessão, consulte Passar tags de sessão AWS STS no Guia de usuário do IAM.

Para passar atributos como tags de sessão, inclua o elemento `AttributeValue` que especifica o valor da tag. Por exemplo, para passar o par chave-valor de tag `CostCenter = blue`, use o atributo a seguir.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Se você precisar adicionar vários atributos, inclua um elemento separado `Attribute` para cada tag.

Introdução às tarefas comuns do IAM Identity Center

Se você for um novo usuário do IAM Identity Center, o fluxo de trabalho básico para começar a usar o serviço é:

1. Faça login no console da sua conta de gerenciamento se estiver usando uma instância organizacional do IAM Identity Center ou Conta da AWS se estiver usando uma instância de conta do IAM Identity Center e navegue até o console do IAM Identity Center.
2. Selecione o diretório que você usa para armazenar as identidades dos usuários e grupos no console do IAM Identity Center. O IAM Identity Center fornece um diretório padrão que você pode usar para configurar o acesso de usuários. Se preferir usar outra fonte de identidades, você pode conectar o Active Directory ou um provedor de identidades externo.
3. Para instâncias de organização, atribua acesso de usuário a Contas da AWS selecionando as contas da organização e depois os usuários ou grupos no seu diretório e as permissões que você deseja conceder a eles.
4. Conceda aos usuários acesso a aplicações da seguinte maneira:
   a. Configure aplicações SAML 2.0 gerenciadas pelo cliente escolhendo no catálogo de aplicações uma das aplicações pré-integradas ou adicionando sua própria aplicação SAML 2.0.
   b. Configure as propriedades da aplicação.
   c. Atribua aos usuários acesso à aplicação. Recomendamos que você atribua acesso aos usuários por meio da associação a um grupo, em vez de adicionar permissões de usuário individuais. Com grupos, você pode conceder ou negar permissões para grupos de usuários, em vez de ter de aplicar essas permissões a cada indivíduo. Se um usuário se mudar para uma organização diferente, basta mover esse usuário para um grupo diferente. Em seguida, o usuário recebe automaticamente as permissões necessárias para a nova organização.
5. Se você estiver usando o diretório padrão do IAM Identity Center, diga aos usuários como fazer login no portal de AWS acesso. Novos usuários no IAM Identity Center devem ativar suas credenciais de usuário antes que elas possam ser usadas para entrar no portal de AWS acesso. Para obter mais informações, consulte Entrar no portal de AWS acesso no Guia do Início de Sessão da AWS usuário

Os tópicos desta seção ajudam você a se familiarizar com as tarefas comuns realizadas depois que concluir a configuração inicial do IAM Identity Center.

Se você ainda não habilitou o IAM Identity Center, consulte Habilitando AWS IAM Identity Center.

Tópicos

Criar um conjunto de permissões

Os conjuntos de permissões são armazenadas no IAM Identity Center e definem o nível de acesso que os usuários e grupos têm a uma conta da Conta da AWS. O primeiro conjunto de permissões que você cria é o conjunto de permissões administrativas. Se você já concluiu um dos Tutoriais de introdução, já criou seu conjunto de permissões administrativas. Use esse procedimento para criar conjuntos de permissões como descrito no tópico AWS managed policies for job functions no IAM User Guide.

1. Realize um dos procedimentos a seguir para entrar no AWS Management Console.
   - Novo em AWS (usuário root) — Faça login como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.
   - Já está usando AWS (credenciais do IAM) — Faça login usando suas credenciais do IAM com permissões administrativas.
2. Abra o console do Centro de Identidade do IAM.
3. No painel de navegação do Centro de Identidade do IAM, em Permissões de várias contas, escolha Conjuntos de permissões.
4. Escolha Create permission set (Criar conjunto de permissões).
   a. Na página Selecionar tipo de conjunto de permissões, na seção Tipo de conjunto de permissões, escolha Conjunto de permissões predefinido.
   b. Na seção Política para um conjunto de permissões predefinido, escolha uma das seguintes opções:
      - AdministratorAccess
      - Faturamento

- DatabaseAdministrator
- DataScientist
- NetworkAdministrator
- PowerUserAccess
- ReadOnlyAccess
- SecurityAudit
- SupportUser
- SystemAdministrator
- ViewOnlyAccess

5. Na página Especificar detalhes do conjunto de permissões, mantenha as configurações padrão e escolha Próximo. A configuração padrão limita sua sessão a uma hora.
6. Na página Revisar e criar, confirme o seguinte:
    1. Para Etapa 1: Selecionar tipo de conjunto de permissões, exibe o tipo de conjunto de permissões que você escolheu.
    2. Para a Etapa 2: Definir detalhes do conjunto de permissões, exibe o nome do conjunto de permissões que você escolheu.
    3. Escolha Criar.

Criar um conjunto de permissões que aplica permissões de privilégio mínimo

Para seguir as práticas recomendadas para aplicar permissões de privilégio mínimo, depois de criar um conjunto de permissões administrativas, crie um conjunto de permissões mais restritivo e o atribua a um ou mais usuários. Os conjuntos de permissões criados no procedimento anterior fornecem um ponto de partida para você avaliar de quanto acesso aos recursos os usuários precisam. Para alternar para permissões de privilégio mínimo, você pode executar o IAM Access Analyzer para monitorar as entidades principais com políticas gerenciadas pela AWS . Depois de descobrir quais permissões elas estão usando, você pode escrever uma política personalizada ou gerar uma política apenas com as permissões necessárias para sua equipe.

Com o IAM Identity Center, você pode atribuir vários conjuntos de permissões para o mesmo usuário. Ao usuário administrativo também devem ser atribuídos conjuntos de permissões adicionais,

mais restritivos. Dessa forma, eles podem acessar você somente Conta da AWS com as permissões necessárias, em vez de sempre usar suas permissões administrativas.

Por exemplo, se você for um desenvolvedor, após criar seu usuário administrativo no IAM Identity Center, poderá criar um novo conjunto de permissões que conceda permissões de `PowerUserAccess` e atribuir esse conjunto de permissões a si mesmo. Ao contrário do conjunto de permissões administrativas, que usa `AdministratorAccess` permissões, o conjunto de `PowerUserAccess` permissões não permite o gerenciamento de usuários e grupos do IAM. Ao entrar no portal de AWS acesso para acessar sua AWS conta, você pode escolher, `PowerUserAccess` em vez de `AdministratorAccess` realizar tarefas de desenvolvimento na conta.

Lembre-se das seguintes considerações:

- Para começar rapidamente a criar um conjunto de permissões mais restritivo, use um conjunto de permissões predefinido em vez de um conjunto de permissões personalizado.

  Com um conjunto de permissões predefinido, que usa permissões predefinidas, você escolhe uma única política AWS gerenciada em uma lista de políticas disponíveis. Cada política concede um nível específico de acesso a AWS serviços e recursos ou permissões para uma função de trabalho comum. Para obter informações sobre cada uma dessas políticas, consulte políticas gerenciadas pela AWS para funções de trabalho.
- Você pode configurar a duração da sessão de um conjunto de permissões para controlar o período de tempo que um usuário fica conectado a uma. Conta da AWS.

  Quando os usuários se federam Conta da AWS e usam o AWS Management Console ou a Interface de Linha de AWS Comando (AWS CLI), o IAM Identity Center usa a configuração de duração da sessão no conjunto de permissões para controlar a duração da sessão. Por padrão, o valor da duração da sessão, que determina o período de tempo em que um usuário pode se Conta da AWS conectar AWS e antes de sair da sessão, é definido como uma hora. Você pode especificar um valor máximo de 12 horas. Para ter mais informações, consulte Definir duração da sessão.
- Você também pode configurar a duração da sessão do portal de AWS acesso para controlar o período de tempo em que um usuário da força de trabalho está conectado ao portal.

  Por padrão, o valor da duração máxima da sessão, que determina o período de tempo em que um usuário da força de trabalho pode entrar no portal de AWS acesso antes de precisar se autenticar novamente, é de oito horas. Você pode especificar um valor máximo de 90 dias. Para ter mais

informações, consulte Configure a duração da sessão do portal de AWS acesso e dos aplicativos integrados do IAM Identity Center.

- Ao entrar no portal de AWS acesso, escolha a função que fornece permissões de privilégio mínimo.

  Cada conjunto de permissões que você cria e atribui ao seu usuário aparece como uma função disponível no portal de AWS acesso. Ao entrar no portal como esse usuário, escolha a função que corresponde ao conjunto de permissões mais restritivo que você pode utilizar para realizar tarefas na conta, em vez `AdministratorAccess` de.
- Você pode adicionar outros usuários ao IAM Identity Center e atribuir conjuntos de permissões novos ou existentes a esses usuários.

  Para obter mais informações, consulte Atribuir Conta da AWS acesso a grupos.

Atribuir Conta da AWS acesso a um usuário do IAM Identity Center

Para configurar o Conta da AWS acesso de um usuário do IAM Identity Center, você deve atribuir ao usuário o conjunto de permissões Conta da AWS e.

1. Realize um dos procedimentos a seguir para entrar no AWS Management Console.
   - Novo em AWS (usuário root) — Faça login como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.
   - Já está usando AWS (credenciais do IAM) — Faça login usando suas credenciais do IAM com permissões administrativas.
2. Abra o console do IAM Identity Center.
3. No painel de navegação, em Permissões de várias contas, escolha Contas da AWS.
4. Na página Contas da AWS, uma lista de visualização em árvore da sua organização é exibida. Marque a caixa de seleção ao lado da Conta da AWS qual você deseja atribuir acesso. Se você estiver configurando o acesso administrativo para o IAM Identity Center, marque a caixa de seleção ao lado da conta de gerenciamento.
5. Escolha Atribuir usuários ou grupos.
6. Para a Etapa 1: Selecionar usuários e grupos, na página Atribuir usuários e grupos ao "***Conta da AWS nome***", faça o seguinte:

1. Na guia Usuários, selecione o usuário para o qual você deseja conceder permissões administrativas.

   Para filtrar os resultados, comece a digitar o nome do usuário que você quer na caixa de pesquisa.

2. Após confirmar que o usuário correto foi selecionado, escolha Próximo.

7. Para a Etapa 2: Selecionar conjuntos de permissões, na página Atribuir conjuntos de permissões a "***`Conta da AWS nome`***", em Conjuntos de permissões, selecione um conjunto de permissões para definir o nível de acesso que usuários e grupos têm a ele Conta da AWS.
8. Escolha Próximo.
9. Para a Etapa 3: Revisar e enviar, na página Revisar e enviar exercícios para "***`Conta da AWS nome`***", faça o seguinte:

   1. Revise o usuário selecionado e o conjunto de permissões.
   2. Depois de confirmar que o usuário correto foi atribuído ao conjunto de permissões, escolha Enviar.

   > **Important**
   >
   > O processo de atribuição de usuário pode demorar alguns minutos para ser concluído. Mantenha a página aberta até que o processo seja concluído com êxito.

10. Se alguma das opções a seguir se aplicar, siga as etapas em Solicite aos usuários o MFA para habilitar a MFA para o IAM Identity Center:

    - Você está usando o diretório padrão do Identity Center como sua fonte de identidade.
    - Você está usando um AWS Managed Microsoft AD diretório ou um diretório autogerenciado no Active Directory como sua fonte de identidade e não está usando o RADIUS MFA com. AWS Directory Service

    > **Note**
    >
    > Se você estiver usando um provedor de identidades externo, observe que o IdP externo, e não o Centro de Identidade do IAM, gerencia as configurações de MFA. O MFA no IAM Identity Center não é suportado para uso externo. IdPs

Quando você configura o acesso à conta para o usuário administrativo, o IAM Identity Center cria um perfil do IAM correspondente. Essa função, que é controlada pelo IAM Identity Center, é criada no local relevante Conta da AWS e as políticas especificadas no conjunto de permissões são anexadas à função.

Faça login no portal de AWS acesso com suas credenciais do IAM Identity Center

O portal de AWS acesso fornece aos usuários do IAM Identity Center acesso único a todos os seus aplicativos Contas da AWS e atribuídos por meio de um portal da web.

Conclua as etapas a seguir para confirmar se o usuário do IAM Identity Center pode entrar no AWS portal de acesso e acessar Conta da AWS o.

1. Realize um dos procedimentos a seguir para entrar no AWS Management Console.

   - Novo em AWS (usuário root) — Faça login como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.
   - Já está usando AWS (credenciais do IAM) — Faça login com suas credenciais do IAM e selecione uma função de administrador.
2. Abra o console do IAM Identity Center.
3. No painel de navegação, escolha Painel.
4. Na página Painel, em Resumo das configurações, escolha a URL do portal de AWS acesso.
5. Faça login com uma destas opções:

   - Se você estiver usando o Active Directory ou um provedor de identidades (IdP) externo como fonte de identidades, faça login usando as credenciais de usuário do Active Directory ou do IdP.
   - Se você estiver usando o diretório padrão do Identity Center como sua fonte de identidades, faça o login usando o nome de usuário que você especificou ao criar o usuário e a nova senha que especificou para o usuário.

1. Na guia Contas, Conta da AWS localize sua e expanda-a.
2. Os perfis disponíveis para você são exibidos. Por exemplo, se você receber o conjunto de AdministratorAccesspermissões e os conjuntos de permissões de cobrança, essas funções

serão exibidas no portal de AWS acesso. Escolha o nome do perfil do IAM que você deseja usar para a sessão.

3. Se você for redirecionado para o AWS Management Console, você concluiu com êxito a configuração do acesso ao Conta da AWS.

> **Note**
>
> Se você não vê Contas da AWS listadas, é provável que o usuário ainda não tenha sido atribuído a um conjunto de permissões para essa conta. Para obter instruções sobre como atribuir usuários a um conjunto de permissões, consulte Atribuir acesso de usuário a Contas da AWS.

Agora que você confirmou que pode fazer login usando as credenciais do IAM Identity Center, mude para o navegador que você usou para fazer login AWS Management Console e sair de suas credenciais de usuário raiz ou de usuário do IAM.

> **Important**
>
> É altamente recomendável que você use as credenciais do usuário administrativo do IAM Identity Center ao entrar no portal de AWS acesso para realizar tarefas administrativas em vez de usar as credenciais de usuário raiz ou usuário do IAM. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele pode executar. Para permitir que outros usuários acessem suas contas e aplicações, e administrem o IAM Identity Center, crie e atribua conjuntos de permissões somente por meio do IAM Identity Center.

Atribuir Conta da AWS acesso a grupos

Depois de criar um usuário administrativo no IAM Identity Center e criar conjuntos de permissões adicionais que você pode usar para realizar tarefas com permissões menos privilegiadas, você pode fornecer acesso aos seus Contas da AWS dois grupos de usuários.

Recomendados que você atribua acesso diretamente aos grupos, em vez de a usuários individuais. Por exemplo, se criar grupos e conjuntos de permissões com base em unidades organizacionais, se um usuário for transferido para outra unidade organizacional, você só precisará passar esse usuário para um outro grupo e ele receberá automaticamente as permissões necessárias para a nova unidade organizacional e perderá as permissões da unidade organizacional anterior.

Para atribuir acesso ao grupo de usuários a Contas da AWS

1. Abra o console do Centro de Identidade do IAM.

   > **Note**
   >
   > Se sua fonte de identidade for, AWS Managed Microsoft AD certifique-se de que o console do IAM Identity Center esteja usando a região em que seu AWS Managed Microsoft AD diretório está localizado antes de passar para a próxima etapa.

2. No painel de navegação, em Permissões de várias contas, escolha Contas da AWS.
3. Na página Contas da AWS, aparece uma lista de visualização em árvore da sua organização. Marque a caixa de seleção ao lado de uma ou mais Contas da AWS às quais você deseja atribuir acesso de logon único.

   > **Note**
   >
   > Você pode selecionar até 10 Contas da AWS por conjunto de permissões.

4. Escolha Atribuir usuários ou grupos.
5. Em Etapa 1: selecionar usuários e grupos, na página Atribuir usuários e grupos a "***AWS-account-name***", selecione a guia Grupos e escolha um ou mais grupos.

   Para filtrar os resultados, comece a digitar o nome do grupo que deseja na caixa de pesquisa.

   Para exibir os usuários e grupos selecionados, escolha o triângulo virado ao lado de Usuários e grupos selecionados.

   Depois de confirmar que os usuários e grupos corretos foram selecionados, escolha Avançar.
6. Em Etapa 2: selecionar conjuntos de permissões, na página Atribuir conjuntos de permissões a "***AWS-account-name***", selecione um ou mais conjuntos de permissões

   > **Note**
   >
   > Se você não criou o conjunto de permissões desejado antes de iniciar esse procedimento, escolha Criar conjunto de permissões e siga as etapas em Criar um conjunto de permissões. Depois de criar os conjuntos de permissões que você deseja aplicar, no console do IAM Identity Center, retorne a Contas da AWS e siga as

instruções até chegar à Etapa 2: Selecionar conjuntos de permissões. Ao chegar a essa etapa, selecione os novos conjuntos de permissões que você criou e vá para a próxima etapa desse procedimento.

Depois de confirmar que os conjuntos de permissões corretos foram selecionados, escolha Avançar.

7. Na Etapa 3: Revisar e enviar, na página Revisar e enviar exercícios para "***AWS-account-name***", faça o seguinte:

   1. Revise os grupos e os conjuntos de permissões selecionados.
   2. Depois de confirmar que os grupos e conjuntos de permissões corretos estão selecionados, escolha Enviar.

      Important

      O processo de atribuição de grupo pode levar alguns minutos para ser concluído. Mantenha a página aberta até que o processo seja concluído com êxito.

      Note

      Talvez seja necessário conceder permissões aos usuários ou grupos para operar na conta AWS Organizations de gerenciamento. Por ser uma conta altamente privilegiada, restrições de segurança adicionais exigem que você tenha a FullAccess política do IAM ou permissões equivalentes antes de poder configurá-la. Essas restrições de segurança adicionais não são necessárias para nenhuma das contas dos membros em sua AWS organização.

Como alternativa, você pode usar o AWS CloudFormation para criar e atribuir conjuntos de permissões e atribuir usuários a esses conjuntos de permissões. Os usuários podem então entrar no portal de acesso da AWS ou usar os comandos da AWS Command Line Interface (AWS CLI).

Configurar o acesso de logon único às aplicações

O IAM Identity Center oferece suporte a dois tipos de aplicativos: aplicativos AWS gerenciados e aplicativos gerenciados pelo cliente.

AWS os aplicativos gerenciados são configurados diretamente dos consoles de aplicativos relevantes ou por meio das APIs do aplicativo.

As aplicações gerenciadas pelo cliente devem ser adicionadas ao IAM Identity Center e configuradas com os metadados apropriados tanto para o IAM Identity Center quanto para o provedor de serviços. Você pode escolher em um catálogo das aplicações mais usadas que são compatíveis com o SAML 2.0 ou pode configurar suas próprias aplicações SAML 2.0 ou OAuth 2.0.

As etapas de configuração para configurar o acesso de login único às aplicações variam com base no tipo de aplicação.

Configurar um aplicativo AWS gerenciado

AWS aplicativos gerenciados, como o Amazon Managed Grafana e o Amazon Monitron, se integram ao IAM Identity Center e podem usá-lo para serviços de autenticação e diretório. Para configurar um aplicativo AWS gerenciado para funcionar com o IAM Identity Center, você deve configurar o aplicativo diretamente do console para o serviço aplicável ou usar as APIs do aplicativo.

Configurar uma aplicação do catálogo de aplicações

Você pode selecionar uma aplicação SAML 2.0 em um catálogo das aplicações mais usadas no console do IAM Identity Center. Use este procedimento para configurar uma relação de confiança SAML 2.0 entre o IAM Identity Center e o provedor de serviços da aplicação.

Para configurar uma aplicação do catálogo de aplicações

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Escolha a guia Gerenciada pelo cliente.
4. Escolha Adicionar aplicação.
5. Na página Selecionar tipo de aplicação, em Preferências de configuração, escolha Quero selecionar uma aplicação do catálogo.
6. Em Catálogo de aplicações, comece a digitar, na caixa de pesquisa, o nome da aplicação que você deseja adicionar.

7. Escolha o nome da aplicação na lista quando ele aparecer nos resultados da pesquisa e depois escolha Avançar.
8. Na página Configurar aplicação, os campos Nome de exibição e Descrição já estão preenchidos com os detalhes relevantes da aplicação. Você pode editar essas informações.
9. Em Metadados do IAM Identity Center, faça o seguinte:

    a. Ao lado do Arquivo de metadados de SAML do IAM Identity Center, escolha Download para fazer download dos metadados do provedor de identidades.

    b. Ao lado de Certificado do IAM Identity Center, escolha Fazer download do certificado para baixar o certificado do provedor de identidades.

> **Note**
>
> Você precisará desses arquivos mais tarde ao configurar a aplicação no site do provedor de serviços. Siga as instruções desse provedor.

10. (Opcional) Em Propriedades da aplicação, você pode especificar URL de início da aplicação, Estado de retransmissão e Duração da sessão. Para ter mais informações, consulte Configurar as propriedades da aplicação no console do IAM Identity Center.
11. Em Metadados da aplicação, faça o seguinte:

    a. Se você tiver um arquivo de metadados, escolha Carregar o arquivo de metadados SAML da aplicação. Em seguida, selecione Escolher arquivo para encontrar e selecionar o arquivo de metadados.

    b. Se você não tiver um arquivo de metadados, escolha Digitar manualmente os valores dos metadados e forneça os valores de URL do ACS da aplicação e Público do SAML da aplicação.
12. Selecione Enviar. Você é direcionado para a página de detalhes da aplicação que acabou de adicionar.

Configurar sua própria aplicação SAML 2.0

Use este procedimento para configurar uma relação de confiança SAML 2.0 entre o IAM Identity Center e o provedor de serviços da sua própria aplicação SAML 2.0. Antes de iniciar este procedimento, verifique se você tem o certificado e os arquivos de troca de metadados do provedor de serviços, para que possa terminar de configurar a confiança.

Para configurar sua própria aplicação SAML 2.0

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Escolha a guia Gerenciada pelo cliente.
4. Escolha Adicionar aplicação.
5. Na página Selecionar tipo de aplicação, em Preferências de configuração, escolha Eu tenho uma aplicação que quero configurar.
6. Em Tipo de aplicação, escolha SAML 2.0.
7. Escolha Próximo.
8. Na página Configurar aplicação, em Configurar aplicação, insira um nome de exibição para a aplicação, como **`MyApp`**. Insira uma Descrição.
9. Em Metadados do IAM Identity Center, faça o seguinte:

    a. Ao lado do Arquivo de metadados de SAML do IAM Identity Center, escolha Download para fazer download dos metadados do provedor de identidades.

    b. Em Certificado do IAM Identity Center, escolha Baixar para baixar o certificado do provedor de identidades.

    > **Note**
    >
    > Você precisará desses arquivos mais tarde ao configurar a aplicação personalizada no site do provedor de serviços.

10. (Opcional) Em Propriedades da aplicação, você também pode especificar URL de início da aplicação, Estado de retransmissão e Duração da sessão. Para ter mais informações, consulte Configurar as propriedades da aplicação no console do IAM Identity Center.
11. Em Metadados da aplicação, escolha Digite manualmente seus valores de metadados. Em seguida, forneça os valores de URL do ACS da aplicação e Público do SAML da aplicação.
12. Selecione Enviar. Você é direcionado para a página de detalhes da aplicação que acabou de adicionar.

Depois de configurar seus aplicativos, seus usuários podem acessar seus aplicativos de dentro do portal de AWS acesso com base nas permissões que você atribuiu.

Se você tem aplicativos gerenciados pelo cliente que oferecem suporte ao OAuth 2.0 e seus usuários precisam acessar esses aplicativos aos AWS serviços, você pode usar a propagação de identidade confiável. Com a propagação de identidade confiável, um usuário pode entrar em um aplicativo e esse aplicativo pode transmitir a identidade dos usuários em solicitações para acessar dados em AWS serviços. Para ter mais informações, consulte Usar a propagação de identidades confiáveis com aplicações gerenciadas pelo cliente.

Para obter mais informações sobre os tipos de aplicação, consulte Gerenciar o acesso a aplicações.

Exibir exercícios de usuários e grupos

Você pode ver quem tem acesso ao quê no IAM Identity Center nas páginas Usuários e Grupos. Use esse procedimento para visualizar o nível de acesso que os usuários têm às AWS contas, conjuntos de permissões, aplicativos e grupos.

1. Abra o console do Centro de Identidade do IAM.
2. Escolha Usuários ou Grupos com base em se você deseja editar um grupo de usuários ou um usuário que foi atribuído individualmente.
3. Escolha um usuário ou grupo na lista.
4. Escolha se você deseja visualizar as atribuições da conta, as atribuições do aplicativo ou as tarefas em grupo:

   - AWS atribuições de contas e conjuntos de permissões
     1. Selecione a guia Accounts.
     2. Selecione uma conta na lista para ver as atribuições do conjunto de permissões de usuários e grupos.
     3. Selecione um conjunto de permissões para visualizar os detalhes da política e da atribuição.
   - Atribuições de aplicativos
     1. Escolha a guia Aplicativos para ver quais aplicativos estão atribuídos a um usuário ou grupo.
     2. Selecione um aplicativo na lista para ver os detalhes do exercício.
   - Tarefas em grupo
     1. Na página Usuários, escolha a guia Grupos.
     2. Selecione um grupo para ver os exercícios em grupo de um usuário.

Gerenciar instâncias de organização e de conta do IAM Identity Center

Uma instância é uma implantação única do IAM Identity Center. Há dois tipos de instâncias disponíveis para o IAM Identity Center: instâncias de organização e instâncias de conta.

Conta da AWS tipos que podem ativar o IAM Identity Center

Para habilitar o IAM Identity Center, faça login no AWS Management Console usando uma das seguintes credenciais, dependendo do tipo de instância que você deseja criar:

- Sua conta AWS Organizations de gerenciamento (recomendada) — necessária para criar uma instância organizacional do IAM Identity Center. Use uma instância de organização para permissões multicontas e atribuições de aplicações em toda a organização.
- Sua conta de AWS Organizations membro — Use para criar uma instância de conta do IAM Identity Center para permitir atribuições de aplicativos dentro dessa conta de membro. Pode haver uma ou mais contas com uma instância de nível de membro em uma organização.
- Autônomo Conta da AWS — Use para criar uma instância organizacional ou instância de conta do IAM Identity Center. O autônomo Conta da AWS não é gerenciado por AWS Organizations. Somente uma instância do IAM Identity Center pode ser associada a uma instância autônoma Conta da AWS e você pode usar a instância para atribuições de aplicativos dentro dessa instância autônoma. Conta da AWS

Recurso	Instância na conta AWS Organizations de gerenciamento (recomendado)	Instância em uma conta-membro	Instância em uma instância autônoma Conta da AWS
Gerenciar usuários	 S	 S	 Sim
AWS portal de acesso para acesso com login único aos seus	 S	 S	 Sim

Recurso	Instância na conta AWS Organizations de gerenciamento (recomendado)	Instância em uma conta-membro	Instância em uma instância autônoma Conta da AWS
aplicativos AWS gerenciados			
Aplicativos gerenciados pelo cliente OAuth 2.0 (OIDC)	 S	 S	 Sim
Permissões multicontas	 S	 N	 Não
AWS portal de acesso para acesso com login único ao seu Contas da AWS	 S	 N	 Não
Aplicativos gerenciados pelo cliente SAML 2.0	 S	 N	 Não
O administrador delegado pode gerenciar a instância	 S	 N	 Não

Tópicos

- Instâncias de organização do IAM Identity Center
- Instâncias de conta do IAM Identity Center
- Ative as instâncias da conta no console do IAM Identity Center
- Controlar a criação de instâncias de conta com políticas de controle de serviço
- Criar uma instância de conta do IAM Identity Center

Instâncias de organização do IAM Identity Center

Ao ativar o IAM Identity Center em conjunto com AWS Organizations, você está criando uma instância organizacional do IAM Identity Center. A instância de organização deve estar habilitada em sua conta de gerenciamento e você pode gerenciar centralmente o acesso de usuários e grupos com uma única instância de organização. Você só pode ter uma instância de organização para cada conta de gerenciamento no AWS Organizations.

Se habilitou o IAM Identity Center antes de 15 de novembro de 2023, você já tem uma instância de organização do IAM Identity Center.

Quando usar uma instância de organização

Uma instância da organização é o principal método para habilitar o IAM Identity Center e, na maioria dos casos, uma instância da organização é recomendada. As instâncias de organização oferecem os seguintes benefícios:

- Support para todos os recursos do IAM Identity Center — incluindo o gerenciamento de permissões para vários Contas da AWS em sua organização e a atribuição de acesso a aplicativos gerenciados pelo cliente.
- Redução do número de pontos de gerenciamento: uma instância de organização tem um único ponto de gerenciamento, a conta de gerenciamento. Recomendamos que você habilite uma instância de organização, em vez de uma instância de conta, para reduzir o número de pontos de gerenciamento.
- Controle a criação de instâncias de conta — Você pode controlar se as instâncias de conta podem ser criadas por contas membros em sua organização, desde que você não tenha implantado uma instância do IAM Identity Center em sua organização em uma região opcional (Região da AWS que é desativada por padrão).

Instâncias de conta do IAM Identity Center

Com uma instância de conta do IAM Identity Center, você pode implantar aplicativos AWS gerenciados compatíveis e aplicativos gerenciados pelo cliente baseados em OIDC. As instâncias de conta oferecem suporte a implantações isoladas de aplicativos em um único aplicativo Conta da AWS, aproveitando os recursos do portal de acesso e identidade da força de trabalho do IAM Identity Center.

As instâncias da conta estão vinculadas a uma única Conta da AWS e são usadas somente para gerenciar o acesso de usuários e grupos a aplicativos compatíveis na mesma conta Região da AWS e. Você está limitado a uma instância de conta por Conta da AWS. Você pode criar uma instância de conta em:

- Uma conta de membro em AWS Organizations.
- Um autônomo Conta da AWS que não é gerenciado pelo AWS Organizations.

Restrições de disponibilidade para contas-membro

Você pode implantar uma instância de conta em uma conta-membro de uma organização se o seguinte for verdadeiro:

- Você não tinha uma instância do IAM Identity Center implantada em sua organização antes de 15 de novembro de 2023.
- Você tem uma instância do IAM Identity Center já implantada em sua organização antes de 15 de novembro de 2023, e seu administrador habilitou contas de membros para criar instâncias de conta do IAM Identity Center.
- Seu administrador não criou uma Política de Controle de Serviços que impeça que as contas dos membros criem instâncias da conta.
- Você ainda não tem uma instância do IAM Identity Center nessa mesma conta, independentemente de Região da AWS.
- Você está trabalhando em um Região da AWS local onde o IAM Identity Center não está disponível. Para obter mais informações sobre regiões, consulte AWS IAM Identity Center Disponibilidade da região.

Tópicos

Quando usar instâncias de conta

Na maioria dos casos, uma instância da organização é recomendada. As instâncias de conta só devem ser usadas se um dos seguintes cenários se aplicar:

- Você deseja executar um teste temporário de um aplicativo AWS gerenciado compatível para determinar se o aplicativo atende às suas necessidades comerciais.
- Você não tem planos de adotar o IAM Identity Center em toda a sua organização, mas deseja oferecer suporte a um ou mais aplicativos AWS gerenciados.
- Você tem uma instância organizacional do IAM Identity Center, mas deseja implantar um aplicativo AWS gerenciado compatível em um conjunto isolado de usuários que são distintos dos usuários na instância da sua organização.

> **Important**
>
> Se você planeja usar o IAM Identity Center para compatibilidade com aplicações em várias contas, crie uma instância de organização e não use instâncias de conta.

Considerações sobre instâncias de conta

Uma instância de conta destina-se a casos de uso especializados, oferecendo um subconjunto dos atributos disponíveis para uma instância de organização. Considere o seguinte antes de criar uma instância de conta:

- As instâncias da conta não oferecem suporte a conjuntos de permissões e, portanto, não oferecem suporte ao acesso Contas da AWS a.
- Você não pode converter uma instância de conta em uma instância de organização.
- Você não pode mesclar uma instância de conta com uma instância de organização.
- Selecione somente instâncias da conta de AWS aplicativos gerenciados suporte.
- Use instâncias de conta para usuários isolados que só usarão as aplicações em uma única conta e durante toda a vida útil das aplicações usadas.
- As aplicações vinculadas a uma instância de conta devem permanecer vinculadas até que você exclua a aplicação junto com seus recursos.
- Uma instância da conta deve permanecer no Conta da AWS local em que foi criada.

AWS aplicativos gerenciados que oferecem suporte a instâncias de contas

Veja AWS aplicativos gerenciados para saber quais aplicativos AWS gerenciados oferecem suporte às instâncias da conta do IAM Identity Center. Verifique a disponibilidade da criação da instância da conta com seu aplicativo AWS gerenciado.

Ative as instâncias da conta no console do IAM Identity Center

Se você ativou o IAM Identity Center antes de 15 de novembro de 2023, você tem uma instância organizacional do IAM Identity Center e a capacidade de as contas membros criarem instâncias de conta está desativada por padrão. Você pode escolher se as contas-membros podem criar instâncias de conta habilitando o atributo de instância de conta no AWS Management Console.

> **Note**
>
> As contas dos membros podem criar uma instância de conta, desde que você não tenha implantado uma instância do IAM Identity Center em sua organização em uma região opcional (Região da AWS que é desativada por padrão), independentemente da data de implantação. Qualquer instância organizacional do IAM Identity Center implantada em um opt-in Região da AWS impedirá a criação de instâncias de conta. Para obter mais informações sobre regiões, consulte AWS IAM Identity Center Disponibilidade da região.

Para habilitar a criação de instâncias de contas-membro na organização

1. Abra o console do Centro de Identidade do IAM.
2. Escolha Configurações e depois escolha a guia Gerenciamento.
3. Na seção Instâncias de conta do IAM Identity Center, escolha Habilitar instâncias de conta do IAM Identity Center.
4. Na caixa de diálogo Habilitar instâncias de conta do IAM Identity Center, confirme que você deseja permitir que as contas-membros da organização criem instâncias de conta ao escolher Habilitar.

> **Important**
>
> Habilitar instâncias de conta do IAM Identity Center para contas de membros é uma operação única. Isso significa que essa operação não pode ser revertida. Depois

de ativado, você pode limitar a criação de instâncias da conta criando uma política de controle de serviço (SCP). Para obter instruções, consulte Controlar a criação de instâncias de conta com políticas de controle de serviços.

Controlar a criação de instâncias de conta com políticas de controle de serviço

Os usuários podem criar uma instância do IAM Identity Center vinculada a uma única Conta da AWS, chamada instância de conta do IAM Identity Center. Você pode controlar a criação de instâncias de conta com políticas de controle de serviços (SCP).

1. Abra o console do Centro de Identidade do IAM.
2. No Painel, na seção Gerenciamento central, escolha o botão Evitar instâncias de conta.
3. Na caixa de diálogo Anexar SCP para evitar a criação de novas instâncias de conta, uma SCP é fornecida a você. Copie a SCP e escolha o botão Ir para o painel de SCP. Você será levado ao console do AWS Organizations para criar a SCP ou anexá-la como uma instrução a uma SCP existente.

   As políticas de controle de serviços são uma característica do AWS Organizations. Para obter instruções sobre como anexar uma SCP, consulte Attaching and detaching service control policies no AWS Organizations User Guide.

Em vez de impedir a criação de instâncias de conta, você pode limitar a criação de instâncias de conta a uma Conta da AWS situação específica da sua organização:

Example : SCP para controlar a criação de instâncias

```
{
    "Version": "2012-10-17",
    "Statement" : [
        {
            "Sid": "DenyMemberAccountInstances",
            "Effect": "Deny",
            "Action": "sso:CreateInstance",
            "Resource": "*",
            "Condition": {
                 "StringNotEquals": {
```

```
                    "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
                }
            }
        }
    ]
}
```

Criar uma instância de conta do IAM Identity Center

Uma instância de organização é o método principal e recomendado para habilitar o IAM Identity Center. Verifique se seu caso de uso é compatível com a criação de uma instância de conta e se você está ciente das considerações.

Criar uma instância de conta a partir de uma conta-membro ou de uma Conta da AWS autônoma da organização

1. Realize um dos procedimentos a seguir para entrar no AWS Management Console.
   - Novo em AWS (usuário root) — Faça login como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.
   - Já está usando AWS (credenciais do IAM) — Faça login usando suas credenciais do IAM com permissões administrativas.
2. Abra o console do IAM Identity Center.
3. Em Habilitar o Centro de Identidade do IAM, escolha Habilitar.
4. Selecione Continuar criando a instância de conta e escolha Continuar.

   > **Note**
   >
   > Se já existir uma instância de organização do IAM Identity Center, certifique-se de que seu caso de uso exija sua própria instância de conta do IAM Identity Center. Caso contrário, escolha Cancelar e usar a instância de organização.

5. Opcional. Adicione as tags que deseja associar a essa instância de conta.

Uma notificação no console indica que uma instância de conta foi criada com sucesso e inclui o ID da instância. Você pode nomear a instância no Resumo das configurações.

> **Note**
>
> Por padrão, a autenticação multifator (MFA) não está habilitada para instâncias de conta. Os usuários são solicitados a fazer login com MFA quando seu dispositivo, navegador ou local são alterados. É uma prática de segurança altamente recomendável usar a MFA para as identidades da força de trabalho. Saiba mais sobre o Gerencie dispositivos MFA no IAM Identity Center.

Recursos de gerenciamento, como confirmar sua fonte de identidade, ajustar as configurações de autenticação multifatorial e adicionar aplicativos AWS gerenciados, devem ser preenchidos no console do IAM Identity Center.

Autenticação

Um usuário entra no portal de AWS acesso usando seu nome de usuário. Quando isso acontece, o IAM Identity Center redireciona a solicitação para o serviço de autenticação do IAM Identity Center com base no diretório associado ao endereço de e-mail do usuário. Depois de autenticados, os usuários têm acesso de login único a qualquer uma das AWS contas e aplicativos de terceiros (software-as-a-service SaaS) que aparecem no portal sem solicitações adicionais de login. Isso significa que os usuários não precisam mais acompanhar várias credenciais de conta para os vários AWS aplicativos atribuídos que eles usam diariamente.

Sessões de autenticação

Há dois tipos de sessões de autenticação mantidas pelo IAM Identity Center: uma para representar o login dos usuários no IAM Identity Center e outra para representar o acesso dos usuários aos aplicativos AWS gerenciados, como o Amazon SageMaker Studio ou o Amazon Managed Grafana. Toda vez que um usuário faz login no IAM Identity Center, uma sessão de login é criada com a duração configurada no Identity Center, que pode ser de até 90 dias. Para ter mais informações, consulte Gerencie a duração da sessão do portal de AWS acesso e dos aplicativos integrados do IAM Identity Center. Toda vez que o usuário acessa uma aplicação, a sessão de login do IAM Identity Center é usada para obter uma sessão de aplicação do IAM Identity Center para essa aplicação. As sessões da aplicação do IAM Identity Center têm uma vida útil atualizável de 1 hora, ou seja, as sessões da aplicação do IAM Identity Center são atualizadas automaticamente a cada hora, desde que a sessão de login do IAM Identity Center da qual foram obtidas ainda seja válida. Quando o usuário usa o IAM Identity Center para acessar o AWS Management Console ou CLI, a sessão de login do IAM Identity Center é usada para obter uma sessão do IAM, conforme especificado no conjunto de permissões correspondente do IAM Identity Center (mais especificamente, o IAM Identity Center assume uma função do IAM, gerenciada pelo IAM Identity Center, na conta de destino).

Quando você desabilita ou exclui um usuário no IAM Identity Center, esse usuário é imediatamente impedido de entrar para criar novas sessões de login no IAM Identity Center. As sessões de login do IAM Identity Center são armazenadas em cache por uma hora, o que significa que quando você desabilita ou exclui um usuário enquanto ele tem uma sessão ativa de login do IAM Identity Center, a sessão de login existente do IAM Identity Center continuará por até uma hora, dependendo de quando a sessão de login foi atualizada pela última vez. Durante esse período, o usuário pode iniciar novas sessões de aplicações do IAM Identity Center e de perfis do IAM.

Após a sessão de login do IAM Identity Center expirar, o usuário não poderá mais iniciar novas sessões de aplicação do IAM Identity Center ou de perfil do IAM. Porém, as sessões da aplicação do IAM Identity Center também podem ser armazenadas em cache por até uma hora, de modo que o usuário pode reter acesso a uma aplicação por até uma hora após a expiração da sessão de login do IAM Identity Center. Todas as sessões de perfil do IAM existentes continuarão com base na duração configurada no conjunto de permissões do IAM Identity Center (configurável pelo administrador, até 12 horas).

A tabela abaixo resume esses comportamentos:

Experiência do usuário/comportamento do sistema	Tempo após o usuário ser desativado/excluído
O usuário não consegue mais entrar no IAM Identity Center; o usuário não consegue obter uma nova sessão de login do IAM Identity Center	Nenhuma (efeito imediato)
O usuário não consegue mais iniciar novas sessões de aplicação ou de perfil do IAM por meio do IAM Identity Center	Até 1 hora
O usuário não consegue mais acessar nenhuma aplicação (todas as sessões da aplicação foram encerradas)	Até 2 horas (até 1 hora para a expiração da sessão de login do IAM Identity Center, mais até 1 hora para a expiração da sessão de aplicação do IAM Identity Center)
O usuário não pode mais acessar nenhum Contas da AWS por meio do IAM Identity Center	Até 13 horas (até 1 hora para a expiração da sessão de login do IAM Identity Center, mais até 12 horas para a expiração da sessão do perfil do IAM configurado pelo administrador com base nas configurações de duração da sessão do IAM Identity Center para o conjunto de permissões)

Para obter mais informações sobre sessões, consulte Definir duração da sessão.

Gerenciar identidades da força de trabalho

O AWS Identity and Access Management (IAM) ajuda você a gerenciar com segurança as identidades e o acesso aos serviços e recursos do AWS. Como um serviço do IAM, o AWS IAM Identity Center é onde você cria ou conecta suas identidades da força de trabalho na AWS uma só vez e gerencia o acesso centralmente às suas várias Contas da AWS e aplicativos.

Para os clientes do IAM Identity Center, não há mudança na forma como você gerencia centralmente o acesso a várias Contas da AWS ou aplicativos. Para novos clientes para o IAM Identity Center, você pode configurar com flexibilidade o IAM Identity Center para ser executado junto ou substituir o gerenciamento de Conta da AWS acesso único usando o IAM.

Tópicos

Casos de uso

A seguir estão os casos de uso que mostram como você pode usar o IAM Identity Center para atender às diferentes necessidades comerciais.

Tópicos

Habilite o acesso de login único para os seus AWS aplicativos (função de administrador do aplicativo)

Esse caso de uso fornece orientação se você for um administrador de aplicativos que gerencia AWS aplicativos gerenciados, como o Amazon SageMaker, AWS IoT SiteWise ou se precisar fornecer acesso de login único aos seus usuários.

Antes de começar, considere o seguinte:

- Você quer criar um ambiente de teste ou produção em uma organização separada no AWS Organizations?
- O IAM Identity Center já está habilitado em sua organização? Você tem permissões para ativar o IAM Identity Center na conta de gerenciamento do AWS Organizations?

Analise as diretrizes a seguir para determinar as próximas etapas com base nas necessidades de sua empresa.

Configurar meu aplicativo AWS em uma Conta da AWS independente

Se você precisar fornecer acesso de login único a um aplicativo AWS e souber que seu departamento de TI ainda não usa o IAM Identity Center, talvez seja necessário criar um aplicativo Conta da AWS independente para começar. Por padrão, ao criar sua própria Conta da AWS, você terá as permissões necessárias para criar e gerenciar sua própria organização AWS. Para habilitar o IAM Identity Center, você deve ter permissões de Usuário raiz da conta da AWS.

O IAM Identity Center e o AWS Organizations podem ser habilitados automaticamente durante a configuração de alguns aplicativos AWS (por exemplo, Amazon Managed Grafana). Se seu aplicativo AWS não fornecer a opção de ativar esses serviços, você deverá configurar o AWS Organizations e o IAM Identity Center antes de fornecer acesso de login único ao seu aplicativo.

O IAM Identity Center não está configurado na minha organização

Em sua função de administrador de aplicativos, talvez você não consiga habilitar o IAM Identity Center, dependendo de suas permissões. O IAM Identity Center exige permissões específicas na conta de gerenciamento do AWS Organizations. Nesse caso, entre em contato com o administrador apropriado para habilitar o IAM Identity Center na conta de gerenciamento do Organizations.

Se você tiver permissões suficientes para ativar o IAM Identity Center, faça isso primeiro e depois continue com a configuração do aplicativo. Para obter mais informações, consulte Introdução às tarefas comuns do IAM Identity Center.

O IAM Identity Center está configurado atualmente na minha organização

Nesse cenário, você pode continuar implantando seu aplicativo AWS sem realizar nenhuma ação adicional.

> **Note**
>
> Se sua organização habilitou o IAM Identity Center na conta de gerenciamento antes de 25 de novembro de 2019, você também deve habilitar as aplicações gerenciadas pela AWS na conta de gerenciamento e, opcionalmente, nas contas-membros. Se você ativá-los somente na conta de gerenciamento, poderá ativá-los nas contas dos membros posteriormente. Para habilitar essas aplicações, escolha Habilitar acesso na página Configurações do console do IAM Identity Center na seção de aplicações gerenciadas pela AWS. Para obter mais informações, consulte Configurar o IAM Identity Center para compartilhar informações de identidade .

Habilite o acesso de logon único em suas instâncias do Amazon EC2 Windows

Você pode habilitar o acesso de login único às suas instâncias Windows do Amazon EC2 se for um administrador de aplicativos que gerencia usuários no diretório do Identity Center (a fonte de identidade padrão para o IAM Identity Center) ou um provedor de identidades (IdP) externo compatível, e você deve fornecer acesso ao IAM Identity Center aos seus desktops do Amazon EC2 Windows a partir do console do Fleet Manager. AWS

Com essa configuração, você pode acessar com segurança suas instâncias do Amazon EC2 Windows com as credenciais corporativas existentes. Você não precisa compartilhar credenciais de administrador, acessar credenciais várias vezes ou configurar o software cliente de acesso remoto. Você pode conceder e revogar centralmente o acesso às suas instâncias do Amazon EC2 Windows em escala em várias Contas da AWS. Por exemplo, se você remover um funcionário da sua fonte de identidade integrada do IAM Identity Center, ele perderá automaticamente o acesso a todos os recursos AWS, incluindo instâncias Windows do Amazon EC2.

Para obter mais informações, consulte Como habilitar o login único seguro e contínuo nas instâncias do Amazon EC2 Windows com o IAM Identity Center.

Para uma demonstração de como configurar o IAM Identity Center para habilitar esse recurso, consulte Habilitar o login único no Amazon EC2 Windows com o IAM Identity Center.

Usuários, grupos e provisionamento

Tenha em mente as seguintes considerações ao trabalhar com usuários e grupos do IAM Identity Center.

Exclusividade do nome de usuário e endereço de e-mail

Os usuários do IAM Identity Center devem ser identificáveis de modo exclusivo. O IAM Identity Center implementa um nome de usuário que é o identificador principal dos seus usuários. Embora a maioria das pessoas defina o nome de usuário igual ao endereço de e-mail do usuário, o IAM Identity Center e o padrão SAML 2.0 não exigem isso. Porém, muitas das aplicações baseadas no SAML 2.0 usam um endereço de e-mail como identificador exclusivo dos usuários. Essas aplicações obtêm essas informações das asserções que um provedor de identidades SAML 2.0 envia durante a autenticação. Essas aplicações contam com a exclusividade dos endereços de e-mail de cada usuário. Por isso, o IAM Identity Center permite que você especifique outro dado que não o endereço de e-mail para login do usuário. O IAM Identity Center exige que todos os nomes de usuário e endereços de e-mail de seus usuários não sejam NULL e sejam exclusivos.

Grupos

Os grupos são uma combinação lógica de usuários que você define. Você pode criar grupos e adicionar de usuários aos grupos. O IAM Identity Center não é compatível com a adição de um grupo a um grupo (grupos aninhados). Os grupos são úteis ao atribuir acesso a Contas da AWS e aplicações. Em vez de atribuir cada usuário individualmente, você concede permissões a um grupo. Posteriormente, à medida que você adiciona ou remove usuários de um grupo, o usuário obtém ou perde dinamicamente o acesso às contas e aplicações que você atribuiu ao grupo.

Provisionamento de usuários e grupos

O provisionamento é o processo de disponibilização de informações de usuários e grupos para uso do IAM Identity Center ou de aplicações gerenciadas pela AWS e aplicações gerenciadas pelo cliente. Você pode criar usuários e grupos diretamente no IAM Identity Center ou trabalhar com os usuários e grupos que tem no Active Directory ou em outro provedor de identidades externo. Antes que o IAM Identity Center possa ser usado para atribuir permissões de acesso a usuários e grupos em uma Conta da AWS, o IAM Identity Center primeiro deve estar ciente dos usuários e grupos. Da mesma forma, as aplicações gerenciadas pela AWS e as aplicações gerenciadas pelo cliente podem trabalhar com os usuários e grupos de que o IAM Identity Center está ciente.

O provisionamento no IAM Identity Center varia com base na fonte de identidade que você usa. Para obter mais informações, consulte Gerencie sua fonte de identidade.

Gerencie sua fonte de identidade

Sua fonte de identidade no IAM Identity Center define onde seus usuários e grupos são gerenciados. Após configurar sua fonte de identidades, você pode pesquisar usuários ou grupos para conceder a eles acesso de logon único a Contas da AWS, aplicações ou ambas.

Você pode ter apenas uma fonte de identidade por organização no AWS Organizations. Você pode escolher uma das seguintes opções como fonte de identidade:

- Diretório do Identity Center: quando você ativa o IAM Identity Center pela primeira vez, ele é configurado automaticamente com um diretório do Identity Center como sua origem de identidade padrão. Aqui você cria seus usuários e grupos e atribui o nível de acesso deles às suas Contas da AWS e aplicações.
- Active Directory: escolha essa opção se quiser continuar gerenciando usuários em seu diretório AWS Managed Microsoft AD usando AWS Directory Service ou em seu diretório autogerenciado no Active Directory (AD).
- Provedor de identidades externo: escolha essa opção se quiser gerenciar usuários em um provedor de identidades (IdP) externo, como Okta ou Microsoft Entra ID.

> **Note**
>
> O IAM Identity Center não é compatível com o Simple AD baseado no SAMBA4 como fonte de identidade.

Tópicos

Considerações para alterar sua fonte de identidade

Embora você possa alterar sua fonte de identidade quando quiser, recomendamos que você considere como essa alteração pode afetar sua implantação atual.

Se você já estiver gerenciando usuários e grupos em uma fonte de identidade, mudar para outra fonte de identidade pode remover todas as atribuições de usuários e grupos que você configurou no Centro de Identidade do IAM. Se isso ocorrer, todos os usuários, incluindo o usuário administrativo no IAM Identity Center, perderão o acesso de login único a seus aplicativos Contas da AWS e aplicativos.

Antes de alterar a fonte de identidade do IAM Identity Center, revise as seguintes considerações antes de continuar. Se você quiser continuar com a alteração da fonte de identidade, consulte Alterar sua fonte de identidades para obter mais informações.

Alteração entre o IAM Identity Center e o Active Directory

Se você já estiver gerenciando usuários e grupos no Active Directory, recomendamos que considere a possibilidade de conectar o diretório ao habilitar o IAM Identity Center e escolher a fonte de identidade. Faça isso antes de você criar qualquer usuário e grupo no diretório padrão do Identity Center e fazer qualquer atribuição.

Se você já estiver gerenciando usuários e grupos no diretório padrão do Identity Center, considere o seguinte:

- Atribuições removidas e usuários e grupos excluídos – Alterar sua fonte de identidade para o Active Directory exclui seus usuários e grupos do diretório do Identity Center. Essa alteração também remove suas atribuições. Nesse caso, depois de mudar para o Active Directory, você deve sincronizar seus usuários e grupos do Active Directory no diretório do Identity Center e, em seguida, reaplicar suas atribuições.

  Se você optar por não usar o Active Directory, deverá criar seus usuários e grupos no diretório do Identity Center e, em seguida, fazer as atribuições.
- As atribuições não são excluídas quando as identidades são excluídas – Quando as identidades são excluídas no diretório do Identity Center, as atribuições correspondentes também são excluídas no IAM Identity Center. No entanto, no Active Directory, quando as identidades são excluídas (no Active Directory ou nas identidades sincronizadas), as atribuições correspondentes não são excluídas.

- Sem sincronização de saída para APIs – Se você usa o Active Directory como sua fonte de identidade, recomendamos que utilize as APIs Criar, Atualizar e Excluir com cuidado. O IAM Identity Center não oferece suporte à sincronização de saída, portanto, sua fonte de identidade não é atualizada automaticamente com as alterações que você faz nos usuários ou grupos usando essas APIs.
- A URL do portal de acesso mudará — Alterar sua fonte de identidade entre o IAM Identity Center e o Active Directory também altera a URL do portal de AWS acesso.

Para obter informações sobre a forma como o IAM Identity Center provisiona usuários e grupos, consulte Conectar-se a um diretório Microsoft AD.

Mudar do IAM Identity Center para um IdP externo

Se você alterar sua fonte de identidade do IAM Identity Center para um provedor de identidades (IdP) externo, considere o seguinte:

- As atribuições e associações funcionam com as afirmações corretas — suas atribuições de usuário, atividades em grupo e associações em grupo continuarão funcionando enquanto o novo IdP enviar as afirmações corretas (por exemplo, SAML NameIDs). Essas afirmações devem corresponder aos nomes de usuário e grupos no IAM Identity Center.
- Sem sincronização de saída — o IAM Identity Center não oferece suporte à sincronização de saída, portanto, seu IdP externo não será atualizado automaticamente com as alterações feitas nos usuários e grupos que você fizer no IAM Identity Center.
- Provisionamento do SCIM — se você estiver usando o provisionamento do SCIM, as alterações nos usuários e grupos no seu provedor de identidade só serão refletidas no IAM Identity Center depois que seu provedor de identidade enviar essas alterações para o IAM Identity Center. Consulte Considerações sobre o uso do provisionamento automático.
- Reversão — você pode reverter sua fonte de identidade para usar o IAM Identity Center a qualquer momento. Consulte Mudar de um IdP externo para o IAM Identity Center.

Para obter informações sobre a forma como o IAM Identity Center provisiona usuários e grupos, consulte Conecte-se a um provedor de identidades externo.

Mudar de um IdP externo para o IAM Identity Center

Se você alterar sua fonte de identidade de um provedor de identidades (IdP) externo para o IAM Identity Center, considere o seguinte:

- O IAM Identity Center preserva todas as suas atribuições.
- Forçar a redefinição de senha – Os usuários que tinham senhas no IAM Identity Center podem continuar fazendo login com suas senhas antigas. Para usuários que estavam no IdP externo e não estavam no IAM Identity Center, um administrador deve forçar uma redefinição de senha.

Para obter informações sobre a forma como o IAM Identity Center provisiona usuários e grupos, consulte Gerencie identidades no IAM Identity Center.

Mudar de um IdP externo para outro IdP externo

Se você já estiver usando um IdP externo como fonte de identidades para o IAM Identity Center e mudar para um IdP externo diferente, considere o seguinte:

- Atribuições e associações funcionam com afirmações corretas – O IAM Identity Center preserva todos as suas atribuições. As atribuições de usuário, as atribuições de grupo e as associações de grupos continuarão funcionando enquanto o novo IdP enviar as afirmações corretas (por exemplo, SAML NameIDs).

  Essas afirmações devem corresponder aos nomes de usuário no IAM Identity Center quando seus usuários se autenticam por meio do novo IdP externo.
- Provisionamento do SCIM – Se você estiver usando o SCIM para provisionamento no IAM Identity Center, recomendamos que você revise as informações específicas do IdP neste guia e a documentação fornecida pelo IdP para garantir que o novo provedor corresponda corretamente aos usuários e grupos quando o SCIM estiver ativado.

Para obter informações sobre a forma como o IAM Identity Center provisiona usuários e grupos, consulte Conecte-se a um provedor de identidades externo.

Alternar entre o Active Directory e um IdP externo

Se você alterar sua fonte de identidade de um IdP externo para o Active Directory ou do Active Directory para um IdP externo, considere o seguinte:

- Usuários, grupos e atribuições são excluídos – Todos os usuários, grupos e atribuições são excluídos do IAM Identity Center. Nenhuma informação de usuário ou grupo é afetada no IdP externo ou no Active Directory.

- Provisionamento de usuários – Se você mudar para um IdP externo, deverá configurar o IAM Identity Center para provisionar seus usuários. Como alternativa, você deve provisionar manualmente os usuários e grupos para o IdP externo antes de poder configurar as atribuições.
- Criar atribuições e grupos – Se você mudar para o Active Directory, deverá criar atribuições com os usuários e grupos que estão no seu diretório no Active Directory.

Para obter informações sobre a forma como o IAM Identity Center provisiona usuários e grupos, consulte Conectar-se a um diretório Microsoft AD.

Alterar sua fonte de identidades

O procedimento a seguir descreve como mudar de um diretório fornecido pelo IAM Identity Center (o diretório padrão do Identity Center) para o Active Directory ou um provedor de identidades externo, ou vice-versa. Antes de continuar, consulte as informações em Considerações para alterar sua fonte de identidade. Dependendo da sua implantação atual, essa alteração pode remover qualquer atribuição de usuário e grupo que você configurou no IAM Identity Center. Se isso ocorrer, todos os usuários, incluindo o usuário administrativo no IAM Identity Center, perderão o acesso de login único a seus aplicativos Contas da AWS e aplicativos.

Para alterar sua fonte de identidades

1. Abra o console do IAM Identity Center.
2. Escolha Configurações.
3. Na página Configurações, escolha a guia Origem da identidade. Escolha Ações e, em seguida, escolha Alterar fonte de identidades.
4. Em Escolher fonte de identidades, selecione a fonte para a qual você deseja alterar e, em seguida, escolha Próximo.

   Se você estiver mudando para o Active Directory, escolha o diretório disponível no menu na próxima página.

> **Important**
>
> Alterar sua fonte de identidade para ou a partir do Active Directory exclui usuários e grupos do diretório do Identity Center. Essa alteração também remove todas as atribuições que você configurou no IAM Identity Center.

Se estiver migrando para um provedor de identidades externo, recomendamos que você siga as etapas em Como se conectar a um provedor de identidades externo.

5. Depois de ler o aviso legal e estar pronto para prosseguir, digite ACCEPT.
6. Escolha Alterar origem de identidade. Se estiver alterando sua fonte de identidade para o Active Directory, vá para a próxima etapa.
7. Alterar sua fonte de identidade para o Active Directory leva você à página Configurações. Na página Configurações faça um dos seguintes:

   - Escolha Iniciar configuração guiada. Para obter informações sobre como concluir o processo de configuração guiada, consulte Configuração guiada.
   - Na seção Fonte de identidades, escolha Ações e, em seguida, escolha Gerenciar sincronização para configurar seu escopo de sincronização, a lista de usuários e grupos a serem sincronizados.

Gerencie o login e o uso de atributos para todos os tipos de fonte de identidade

O IAM Identity Center fornece o seguinte conjunto de recursos que permite aos administradores controlar o uso do portal de AWS acesso, definir durações de sessão para usuários no portal de AWS acesso e seus aplicativos e usar atributos para controle de acesso. Esses atributos funcionam com um diretório do Identity Center ou um provedor de identidades externo como sua fonte de identidade.

> **Note**
>
> Se você estiver usando o Active Directory como fonte de identidade para o IAM Identity Center, o gerenciamento de sessões não é aceito.

Tópicos

- Gerencie a duração da sessão do portal de AWS acesso e dos aplicativos integrados do IAM Identity Center
- Configure a duração da sessão do portal de AWS acesso e dos aplicativos integrados do IAM Identity Center

- Excluir sessões para o portal de AWS acesso e aplicativos AWS integrados
- Atributos de usuário e de grupo compatíveis

Gerencie a duração da sessão do portal de AWS acesso e dos aplicativos integrados do IAM Identity Center

O administrador do IAM Identity Center pode configurar a duração da sessão tanto para os aplicativos integrados ao IAM Identity Center quanto para Portal de acesso da AWS o. A configuração da duração das sessões determina com que frequência os usuários precisam se autenticar novamente. O administrador do IAM Identity Center pode encerrar uma sessão ativa do portal de AWS acesso e, ao fazer isso, também encerrar as sessões de aplicativos integrados.

Para ter mais informações, consulte Configure a duração da sessão do portal de AWS acesso e dos aplicativos integrados do IAM Identity Center. Para obter mais informações sobre como gerenciar e finalizar sessões de usuário, consulteExcluir sessões para o portal de AWS acesso e aplicativos AWS integrados.

> **Note**
>
> Modificar a AWS duração da sessão do portal de AWS acesso e encerrar as sessões do portal de acesso não tem efeito na duração da sessão do AWS Management Console que você define em seus conjuntos de permissões.

Configure a duração da sessão do portal de AWS acesso e dos aplicativos integrados do IAM Identity Center

A duração da sessão de autenticação nos aplicativos integrados do IAM Identity Center Portal de acesso da AWS e do IAM é o tempo máximo em que um usuário pode se conectar sem se autenticar novamente. A duração padrão da sessão é de 8 horas. O administrador do IAM Identity Center pode especificar uma duração diferente, de no mínimo 15 minutos a no máximo 90 dias. Para obter mais informações sobre a duração da sessão de autenticação e o comportamento do usuário, consulteAutenticação.

Os tópicos a seguir fornecem informações sobre como configurar a duração da sessão do portal de AWS acesso e dos aplicativos integrados do IAM Identity Center.

Tópicos

- Pré-requisitos e considerações
- Como configurar a duração da sessão

Pré-requisitos e considerações

A seguir estão os pré-requisitos e as considerações para configurar a duração da sessão para o portal de AWS acesso e os aplicativos integrados do IAM Identity Center.

Provedores de identidades externos

O IAM Identity Center usa `SessionNotOnOrAfter` atributos de afirmações de SAML para ajudar a determinar por quanto tempo a sessão pode ser válida.

- Se não `SessionNotOnOrAfter` for passada em uma declaração de SAML, a duração de uma sessão do portal de AWS acesso não será afetada pela duração da sua sessão externa de IdP. Por exemplo, se a duração da sessão do IdP for de 24 horas e você definir uma duração de sessão de 18 horas no IAM Identity Center, seus usuários deverão se autenticar novamente no portal de AWS acesso após 18 horas.
- Se `SessionNotOnOrAfter` for passado em uma declaração SAML, o valor da duração da sessão será definido como o menor entre a duração da sessão do portal de AWS acesso e a duração da sessão do SAML IdP. Se você definir uma duração de sessão de 72 horas no IAM Identity Center e seu IdP tiver uma duração de sessão de 18 horas, seus usuários terão acesso aos AWS recursos para as 18 horas definidas em seu IdP.
- Se a duração da sessão do seu IdP for maior do que a definida no IAM Identity Center, seus usuários poderão iniciar uma nova sessão do IAM Identity Center sem reinserir suas credenciais, com base na sessão de login ainda válida com seu IdP.

> **Note**
>
> Se você estiver usando o Active Directory como fonte de identidade para o IAM Identity Center, o gerenciamento de sessões não é aceito.

AWS CLI e sessões de SDK

Se você estiver usando os AWS Command Line Interface kits de desenvolvimento de AWS software (SDKs) ou outras ferramentas de AWS desenvolvimento para acessar AWS serviços de forma

programática, os seguintes pré-requisitos devem ser atendidos para definir a duração da sessão para o portal de AWS acesso e os aplicativos integrados do IAM Identity Center.

- Você deve configurar a duração da sessão do portal de AWS acesso no console do IAM Identity Center.
- Você deve definir um perfil para as configurações de login único em seu arquivo de configuração da AWS compartilhado. Esse perfil é usado para se conectar ao portal de AWS acesso. Recomendamos que você use a configuração do provedor de token do SSO. Com essa configuração, seu AWS SDK ou ferramenta pode recuperar automaticamente os tokens de autenticação atualizados. Para obter mais informações, consulte a configuração do provedor de token do SSO no Guia de referência do AWS SDK e ferramentas.
- Os usuários devem executar uma versão do AWS CLI ou um SDK que ofereça suporte ao gerenciamento de sessões.

Versões mínimas da AWS CLI que oferecem suporte ao gerenciamento de sessões

A seguir estão as versões mínimas do gerenciamento AWS CLI de sessões de suporte.

- AWS CLI V2 2.9 ou posterior
- AWS CLI V1 1.27.10 ou posterior

Para obter informações sobre como instalar ou atualizar a AWS CLI versão mais recente, consulte Instalando ou atualizando a versão mais recente do AWS CLI.

Se seus usuários estiverem executando o AWS CLI, se você atualizar seu conjunto de permissões pouco antes de a sessão do IAM Identity Center expirar e a duração da sessão estiver definida como 20 horas, enquanto a duração do conjunto de permissões estiver definida como 12 horas, a AWS CLI sessão será executada por no máximo 20 horas mais 12 horas, totalizando 32 horas. Para obter mais informações sobre a CLI do IAM Identity Center, consulte Referência de comandos da AWS CLI.

Versões mínimas de SDKs que oferecem suporte ao gerenciamento de sessões do IAM Identity Center

A seguir estão as versões mínimas dos SDKs que oferecem suporte ao gerenciamento de sessões do IAM Identity Center.

SDK	Versão mínima
Python	1.26.10
PHP	3.245,0
Ruby	aws-sdk-core 3.167.0
Java V2	AWS SDK para Java v2 (2.18.13)
Go V2	SDK completo: release-2022-11-11 e módulos Go específicos: credentials/v1.13.0, config/v1 .18.0
JS V2	2.1253.0
JS V3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

Como configurar a duração da sessão

Use o procedimento a seguir para configurar a duração da sessão do portal de AWS acesso e dos aplicativos integrados do IAM Identity Center.

1. Abra o console do Centro de Identidade do IAM.
2. Escolha Configurações.
3. Na página Configurações, escolha a guia Autenticação.
4. Em Autenticação, ao lado de Configurações da sessão, escolha Configurar. A caixa de diálogo Definir configurações da sessão é exibida.
5. Na caixa de diálogo Definir configurações da sessão, escolha a duração máxima da sessão em minutos, horas e dias para seus usuários selecionando a seta suspensa. Escolha a duração da sessão e escolha Salvar. Você retorna à página Configurações.

Excluir sessões para o portal de AWS acesso e aplicativos AWS integrados

Use o procedimento a seguir para visualizar e excluir sessões ativas de um usuário do IAM Identity Center.

Para excluir uma sessão ativa do portal de AWS acesso e dos aplicativos integrados do IAM Identity Center

1. Abra o console do IAM Identity Center.
2. Selecione Usuários.
3. Na página Usuários, escolha o nome de usuário do usuário cujas sessões você deseja gerenciar. Isso leva você a uma página com as informações do usuário.
4. Na página do usuário, escolha a aba Sessões ativas. O número entre parênteses ao lado de Sessões ativas indica o número de sessões ativas atuais desse usuário.
5. Marque a caixa de seleção ao lado das identidades a serem excluídas e selecione Excluir seção. É exibida uma caixa de diálogo que confirma que você está excluindo sessões ativas desse usuário. Leia as informações na caixa de diálogo e, se quiser continuar, escolha Excluir sessão.
6. Você retornará à página do usuário. Uma barra flash verde aparece para indicar que as sessões selecionadas foram excluídas com sucesso.

Para obter mais informações sobre o comportamento das sessões de autenticação revogadas, consulteSessões de autenticação.

Atributos de usuário e de grupo compatíveis

Os atributos são informações que ajudam a definir e identificar objetos do usuário ou do grupo, como `name`, `email` ou `members`. O IAM Identity Center oferece suporte aos atributos mais usados, independentemente de serem inseridos manualmente durante a criação do usuário ou quando provisionados automaticamente usando um mecanismo de sincronização, conforme definido na especificação do Sistema de gerenciamento de identidade entre domínios (SCIM). Para obter mais informações sobre essa especificação, consulte https://tools.ietf.org/html/rfc7642. Para obter mais informações sobre provisionamento manual e automático, consulte Provisionamento quando os usuários vêm de um IdP externo.

Como o IAM Identity Center oferece suporte ao SCIM para casos de uso de provisionamento automático, o diretório do Identity Center oferece suporte a todos os mesmos atributos de usuário e

grupo listados na especificação do SCIM, com algumas exceções. As seções a seguir descrevem quais atributos não são compatíveis com o IAM Identity Center.

Objetos do usuário

Todos os atributos do esquema de usuário do SCIM (https://tools.ietf.org/html/rfc7643#section-8.3) são compatíveis com o repositório de identidades do IAM Identity Center, exceto os seguintes:

- `password`
- `ims`
- `photos`
- `entitlements`
- `x509Certificates`

Todos os subatributos dos usuários são compatíveis, com exceção de:

- subatributo `'display'` de qualquer atributo de vários valores (por exemplo, `emails` ou `phoneNumbers`)
- subatributo `'version'` do atributo `'meta'`

Agrupar objetos

Todos os atributos do esquema do grupo SCIM (https://tools.ietf.org/html/rfc7643#section-8.4) são compatíveis.

Todos os subatributos dos grupos são compatíveis, com exceção de:

- subatributo `'display'` de qualquer atributo de vários valores (por exemplo, membros).

Gerencie identidades no IAM Identity Center

O IAM Identity Center fornece os seguintes recursos para seus usuários e grupos:

- Crie seus usuários e grupos.
- Adicione seus usuários como membros aos grupos.
- Atribua aos grupos o nível desejado de acesso aos seus Contas da AWS aplicativos.

Para gerenciar usuários e grupos na loja do IAM Identity Center, AWS oferece suporte às operações de API listadas em Ações do Identity Center.

Provisionamento quando os usuários estão no Centro de Identidade do IAM

Ao criar usuários e grupos diretamente no IAM Identity Center, o provisionamento é automático. Essas identidades estão disponíveis imediatamente para serem usadas na criação de atribuições e para uso por aplicações. Para ter mais informações, consulte Provisionamento de usuários e grupos.

Alterando sua origem de identidade

Se você preferir gerenciar usuários no AWS Managed Microsoft AD, você pode parar de usar seu diretório do Identity Center a qualquer momento e, em vez disso, conectar o IAM Identity Center ao seu diretório no Microsoft AD usando AWS Directory Service. Para obter mais informações, consulte considerações para Alteração entre o IAM Identity Center e o Active Directory.

Se você preferir gerenciar usuários em um provedor de identidades (IdP) externo, você pode conectar o IAM Identity Center ao seu IdP e ativar o provisionamento automático. Para obter mais informações, consulte considerações para Mudar do IAM Identity Center para um IdP externo.

Tópicos

Adicionar usuários

Os usuários e grupos criados no diretório do Identity Center estão disponíveis somente no IAM Identity Center. Use o procedimento a seguir para adicionar usuários ao seu diretório do Identity

Center usando o console do IAM Identity Center. Como alternativa, você pode chamar a operação AWS da API CreateUserpara adicionar usuários.

Para adicionar um usuário

1. Abra o console do IAM Identity Center.
2. Selecione Usuários.
3. Na página Add user, forneça as seguintes informações necessárias:

   a. Nome de usuário — Esse nome de usuário é necessário para entrar no portal de AWS acesso e não pode ser alterado posteriormente. Deve ter de 1 a 100 caracteres.

   b. Senha – Você pode enviar um e-mail com as instruções de configuração da senha (essa é a opção padrão) ou gerar uma senha de uso único. Se estiver criando um usuário administrativo escolher enviar um e-mail, especifique um endereço de e-mail que você possa acessar.

      i. Envie um e-mail para esse usuário com instruções de configuração de senha. — Essa opção envia automaticamente ao usuário um endereço de e-mail da Amazon Web Services, com a linha de assunto Convite para participar AWS IAM Identity Center (sucessor do AWS Single Sign-On). O e-mail convida o usuário em nome da sua empresa a acessar o portal de acesso ao IAM Identity Center AWS .

      > **Note**
      >
      > Em determinadas regiões, o IAM Identity Center envia e-mails para usuários usando o Amazon Simple Email Service de outra Região da AWS. Para obter informações sobre como os e-mails são enviados, consulte Chamadas entre regiões.
      > Todos os e-mails enviados pelo serviço IAM Identity Center virão do endereço `no-reply@signin.aws.com` ou `no-reply@login.awsapps.com`. Recomendamos que você configure seu sistema de e-mail para que ele aceite e-mails desses remetentes e não os trate como lixo eletrônico ou spam.

      ii. Gere uma senha de uso único que você possa compartilhar com esse usuário. — Essa opção fornece os detalhes da URL e da senha do portal de AWS acesso que você pode enviar manualmente ao usuário a partir do seu endereço de e-mail.

   c. Endereço de e-mail – O endereço de e-mail deve ser exclusivo.

d. Confirme o endereço de e-mail

e. Nome – Você deve inserir um nome aqui para que o provisionamento automático funcione. Para ter mais informações, consulte Provisionamento automático.

f. Sobrenome – Você deve inserir um sobrenome aqui para que o provisionamento automático funcione.

g. Nome de exibição

> **Note**
>
> (Opcional) Se aplicável, você pode especificar valores para atributos adicionais, como a ID imutável do Microsoft 365 do usuário, para ajudar a fornecer ao usuário acesso de login único a determinados aplicativos comerciais.

4. Escolha Próximo.
5. Se aplicável, selecione um ou mais grupos aos quais deseja adicionar o usuário e escolha Próximo.
6. Revise as informações que você especificou para a Etapa 1: Especificar detalhes do usuário e Etapa 2: Adicionar usuário aos grupos – opcional. Escolha Editar por qualquer uma das etapas para fazer alterações. Depois de confirmar que as informações corretas foram especificadas para ambas as etapas, escolha Adicionar usuário.

Adicionar grupos

Use o procedimento a seguir para adicionar grupos ao seu diretório do Identity Center usando o console do IAM Identity Center. Como alternativa, você pode chamar a operação AWS da API CreateGrouppara adicionar grupos.

Para adicionar um grupo

1. Abra o console do IAM Identity Center.
2. Selecione Grupos.
3. Escolha Criar grupo.
4. Insira um Nome de grupo e Descrição – opcional. A descrição deve fornecer detalhes sobre quais permissões foram ou serão atribuídas ao grupo. Em Adicionar usuários ao grupo – opcional, localize os usuários que você deseja adicionar como membros. Em seguida, marque a caixa de seleção ao lado de cada um deles.

5. Escolha Criar grupo.

Depois de adicionar esse grupo ao seu diretório do Identity Center, você pode atribuir acesso de login único a esse grupo. Para ter mais informações, consulte Atribuir acesso de usuário a Contas da AWS.

Adicionar usuários a grupos

Use o procedimento a seguir para adicionar usuários como membros de um grupo criado anteriormente no diretório do Identity Center usando o console do IAM Identity Center. Como alternativa, você pode chamar a operação da AWS API CreateGroupMembershippara adicionar um usuário como membro de um grupo.

Para adicionar um usuário como membro de um grupo

1. Abra o console do IAM Identity Center.
2. Selecione Grupos.
3. Escolha o nome do grupo que deseja atualizar.
4. Na página de detalhes do grupo, em Usuários neste grupo, escolha Adicionar usuários ao grupo.
5. Na página Adicionar usuários ao grupo, em Outros usuários, localize os usuários que você deseja adicionar como membros. Depois, marque a caixa de seleção ao lado de cada um deles.
6. Escolha Adicionar usuários.

Excluir grupos do IAM Identity Center

Quando você exclui um grupo no diretório do IAM Identity Center, ele remove o acesso a aplicações e Contas da AWS para todos os usuários que são membros desse grupo . Não é possível desfazer a ação de excluir um grupo. Use o procedimento a seguir para excluir um grupo do seu diretório do Identity Center usando o console do IAM Identity Center.

Excluir um grupo do IAM Identity Center

> **Important**
>
> As instruções nesta página aplicam-se a AWS IAM Identity Center. Elas não se aplicam ao AWS Identity and Access Management (IAM). Os usuários, grupos e credenciais de usuário

do IAM Identity Center são diferentes dos usuários, grupos e credenciais de usuário do IAM. Se você estiver procurando instruções sobre como excluir grupos no IAM, consulte Excluir um grupo de usuários do IAM no Guia do usuário do AWS Identity and Access Management .

1. Abra o console do IAM Identity Center.
2. Selecione Grupos.
3. Você pode excluir um grupo de duas maneiras:
   - Na página Grupos, você pode selecionar vários grupos para exclusão. Selecione o nome do grupo que deseja excluir, escolha Excluir grupo.
   - Escolha o nome do grupo que você deseja excluir. Na página de detalhes do grupo, escolha Excluir grupo.
4. Talvez você precise confirmar sua intenção de excluir o grupo.
   - Se você excluir vários grupos de uma vez, confirme sua intenção digitando **`Delete`** na caixa de diálogo Excluir grupo.
   - Se você excluir um único grupo que contém usuários, confirme sua intenção digitando o nome do grupo que você deseja excluir na caixa de diálogo Excluir grupo.
5. Selecione Excluir grupo. Se você selecionou vários grupos para exclusão, escolha Excluir # grupos.

Excluir usuários do IAM Identity Center

Quando você exclui um usuário do diretório do IAM Identity Center, ele remove seu acesso a aplicações e Contas da AWS . Não é possível desfazer a ação de excluir um usuário. Use o procedimento a seguir para excluir um usuário do seu diretório do Identity Center usando o console do IAM Identity Center.

> **Note**
>
> Quando você desabilita o acesso do usuário ou exclui um usuário no IAM Identity Center, esse usuário será imediatamente impedido de entrar no portal de AWS acesso e não poderá criar novas sessões de login. Para ter mais informações, consulte Sessões de autenticação.

Excluir um usuário do IAM Identity Center

> **Important**
>
> As instruções nesta página aplicam-se a AWS IAM Identity Center. Elas não se aplicam ao AWS Identity and Access Management (IAM). Os usuários, grupos e credenciais de usuário do IAM Identity Center são diferentes dos usuários, grupos e credenciais de usuário do IAM. Se você estiver procurando instruções sobre como excluir usuários no IAM, consulte Excluir um grupo de usuários do IAM no Guia do usuário do AWS Identity and Access Management .

1. Abra o console do IAM Identity Center.
2. Selecione Usuários.
3. Você pode excluir um usuário de duas maneiras:
   - Na página Usuários, você pode selecionar vários grupos para exclusão. Selecione o nome de usuário que deseja excluir e escolha Excluir usuários.
   - Escolha o nome de usuário que você deseja excluir. Na página detalhes do usuário, escolha Excluir usuário.
4. Se você excluir vários usuários de uma vez, confirme sua intenção digitando **`Delete`** na caixa de diálogo Excluir usuário.
5. Escolha Excluir usuário. Se você selecionou vários grupos para exclusão, escolha Excluir # usuários.

Desabilitar o acesso do usuário no IAM Identity Center

Ao desabilitar o acesso do usuário no diretório do IAM Identity Center, você não poderá editar os detalhes do usuário, redefinir a senha, adicionar o usuário a um grupo ou visualizar a associação ao grupo. Use o procedimento a seguir para desabilitar o acesso do usuário no diretório do Identity Center usando o console do IAM Identity Center.

> **Note**
>
> Quando você desabilita o acesso do usuário ou exclui um usuário no IAM Identity Center, esse usuário será imediatamente impedido de entrar no portal de AWS acesso e não poderá criar novas sessões de login. Para ter mais informações, consulte Sessões de autenticação.

Para desabilitar o acesso do usuário no IAM Identity Center

1. Abra o console do IAM Identity Center.

> **Important**
>
> As instruções nesta página aplicam-se a AWS IAM Identity Center. Elas não se aplicam ao AWS Identity and Access Management (IAM). Os usuários, grupos e credenciais de usuário do IAM Identity Center são diferentes dos usuários, grupos e credenciais de usuário do IAM. Se você estiver procurando instruções sobre como desativar usuários no IAM, consulte Gerenciar usuários do IAM no Guia do usuário do AWS Identity and Access Management .

2. Selecione Usuários.
3. Selecione o nome de usuário do usuário cujo acesso você deseja desabilitar.
4. Abaixo do nome de usuário do usuário cujo acesso você deseja desativar, na seção Informações gerais, escolha Desativar o acesso do usuário.
5. Na caixa de diálogo Desabilitar acesso do usuário, escolha Desabilitar acesso do usuário.

Editar propriedades do usuário

Use o procedimento a seguir para editar as propriedades de um usuário no diretório do Identity Center usando o console do IAM Identity Center. Como alternativa, você pode chamar a operação da AWS API UpdateUserpara atualizar as propriedades do usuário.

Para editar as propriedades do usuário no IAM Identity Center

1. Abra o console do IAM Identity Center.
2. Selecione Usuários.
3. Escolha o usuário que deseja editar.
4. Na página Perfil, ao lado de Detalhes do perfil, Escolha Editar.
5. Na página Editar detalhes do perfil, atualize as propriedades conforme necessário. Depois, escolha Salvar alterações.

> **Note**
>
> (Opcional) Você pode modificar atributos adicionais, como Número de funcionário e Office 365 Immutable ID para ajudar a mapear a identidade do usuário no IAM Identity Center com determinados aplicativos de negócios que os usuários precisam usar.

> **Note**
>
> O atributo Endereço de e-mail é um campo editável e o valor fornecido deve ser exclusivo.

Redefinir a senha de usuário do IAM Identity Center para um usuário final

Esse procedimento é para administradores que precisam redefinir a senha de um usuário no diretório do IAM Identity Center. Você usará o console do IAM Identity Center para redefinir senhas.

Considerações sobre provedores de identidade e tipos de usuários

- MicrosoftActive Directory ou provedor externo – Se você estiver conectando o IAM Identity Center no Microsoft Active Directory ou a um provedor externo, as redefinições de senha do usuário devem ser feitas de dentro do Active Directory ou do provedor externo. Isso significa que as senhas desses usuários não podem ser redefinidas no console do IAM Identity Center.
- Usuários no diretório do IAM Identity Center – Se você for um usuário do IAM Identity Center, poderá redefinir sua própria senha do IAM Identity Center, consulte Redefinir a senha de usuário do IAM Identify Center.

Redefinir a senha de um usuário final do IAM Identity Center

> **Important**
>
> As instruções nesta página aplicam-se a AWS IAM Identity Center. Elas não se aplicam ao AWS Identity and Access Management (IAM). Os usuários, grupos e credenciais de usuário do IAM Identity Center são diferentes dos usuários, grupos e credenciais de usuário do IAM. Se você estiver procurando instruções sobre como alterar senhas de usuários do IAM,

consulte Gerenciar senhas de usuários do IAM no Guia do usuário do AWS Identity and Access Management .

1. Abra o console do IAM Identity Center.
2. Selecione Usuários.
3. Selecione o nome de usuário do usuário cuja senha você deseja redefinir.
4. Na página detalhes do usuário, escolha Reset password.
5. Na caixa de diálogo Redefinir senha, selecione uma das seguintes opções e, em seguida, escolha Redefinir senha:

   a. Enviar um e-mail para o usuário com instruções para redefinir a senha – Esta opção envia automaticamente ao usuário um e-mail endereçado a partir do Amazon Web Services que o orienta sobre como redefinir sua senha.

      > **Warning**
      >
      > Como prática recomendada de segurança, verifique se o endereço de e-mail desse usuário está correto antes de selecionar essa opção. Se esse e-mail de redefinição de senha fosse enviado para um endereço de e-mail incorreto ou mal configurado, um destinatário mal-intencionado poderia usá-lo para obter acesso não autorizado ao seu AWS ambiente.

   b. Gerar uma senha de uso único e compartilhá-la com o usuário – Esta opção fornece os detalhes da senha que você pode enviar manualmente para o usuário por meio do seu endereço de e-mail.

Enviar e-mail OTP para usuários criados a partir da API

Quando você cria usuários com a operação CreateUserda API, eles não têm senhas. Você pode alterar isso optando por enviar aos usuários uma senha de uso único (OTP) por e-mail quando eles forem criados com a API. Os usuários recebem o e-mail OTP quando tentam fazer login pela primeira vez. Depois de receber o e-mail OTP, quando um usuário fizer login, ele deverá definir uma nova senha. Se você não habilitar essa configuração, deverá gerar e compartilhar OTP com os usuários que você cria usando a API CreateUser.

Enviar OTP por e-mail para usuários criados com a API CreateUser

1. Abra o console do IAM Identity Center.
2. Escolha Configurações.
3. Na página Configurações, escolha a guia Autenticação.
4. Na seção Autenticação padrão, escolha Configurar.
5. Uma caixa de diálogo aparece. Marque a caixa ao lado de Enviar OTP de e-mail Depois, escolha Salvar. O status é atualizado de Desabilitado para Habilitado.

Requisitos de senha ao gerenciar identidade no IAM Identity Center

> **Note**
>
> Esses requisitos se aplicam somente aos usuários criados no diretório do Identity Center. Se você configurou uma fonte de identidade diferente do IAM Identity Center para autenticação, como Active Directoryum provedor de identidade externo, as políticas de senha para seus usuários são definidas e aplicadas nesses sistemas, não no IAM Identity Center. Se sua fonte de identidade for AWS Managed Microsoft AD, consulte Gerenciar políticas de senha AWS Managed Microsoft AD para obter mais informações.

Quando você usa o IAM Identity Center como sua fonte de identidade, os usuários devem seguir os seguintes requisitos de senha para definir ou alterar sua senha:

- As senhas diferenciam maiúsculas de minúsculas.
- As senhas devem ter entre 8 e 64 caracteres.
- As senhas devem conter pelo menos um caractere de cada uma das quatro categorias a seguir:
  - Letras minúsculas (a-z)
  - Letras maiúsculas (A-Z)
  - Números (0-9)
  - Caracteres não alfanuméricos (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)
- As últimas três senhas não podem ser reutilizadas.
- Senhas conhecidas publicamente por meio de um conjunto de dados vazado de terceiros não podem ser usadas.

Conectar-se a um diretório Microsoft AD

Com AWS IAM Identity Center, você pode conectar um diretório autogerenciado no Active Directory (AD) ou um diretório AWS Managed Microsoft AD usando AWS Directory Service. Esse diretório do Microsoft AD define o grupo de identidades que os administradores podem extrair ao usar o console do IAM Identity Center para atribuir acesso de logon único. Depois de conectar seu diretório corporativo ao IAM Identity Center, você pode conceder aos usuários ou grupos do AD acesso a Contas da AWSaplicativos ou ambos.

AWS Directory Service ajuda você a configurar e executar um AWS Managed Microsoft AD diretório autônomo hospedado na AWS nuvem. Você também pode usar AWS Directory Service para conectar seus AWS recursos a um AD autogerenciado existente. Para configurar AWS Directory Service para funcionar com seu AD autogerenciado, você deve primeiro configurar relações de confiança para estender a autenticação para a nuvem.

O IAM Identity Center usa a conexão fornecida por AWS Directory Service para realizar a autenticação de passagem para a instância de origem do AD. Quando você usa AWS Managed Microsoft AD como fonte de identidade, o IAM Identity Center pode trabalhar com usuários de AWS Managed Microsoft AD ou de qualquer domínio conectado por meio de uma confiança do AD. Se você quiser localizar seus usuários em quatro ou mais domínios, os usuários devem usar a sintaxe `DOMAIN\user` como nome de usuário ao realizar logins no IAM Identity Center.

Observações

- Como etapa de pré-requisito, certifique-se de que seu AD Connector ou diretório in AWS Directory Service resida AWS Managed Microsoft AD em sua AWS Organizations conta de gerenciamento. Para ter mais informações, consulte Confirme suas fontes de identidade no IAM Identity Center.
- O IAM Identity Center não é compatível SAMBA 4-based Simple AD como diretório conectado.

Considerações sobre o uso do Active Directory

Se você quiser usar o Active Directory como sua fonte de identidade, sua configuração deve atender aos seguintes pré-requisitos:

- Se você estiver usando AWS Managed Microsoft AD, você deve habilitar o IAM Identity Center no mesmo Região da AWS local em que seu AWS Managed Microsoft AD diretório está configurado. O Centro de Identidade do IAM armazena os dados de atribuição na mesma região do diretório. Para administrar o Centro de Identidade do IAM, talvez seja necessário mudar para a região em que ele estiver configurado. Além disso, observe que o portal de AWS acesso usa a mesma URL de acesso do seu diretório.
- Use um Active Directory residente na conta de gerenciamento:

  Você deve ter um AD Connector ou AWS Managed Microsoft AD diretório existente configurado e ele deve residir em sua conta AWS Organizations de gerenciamento. AWS Directory ServiceVocê pode conectar somente um diretório do AD Connector ou um diretório por AWS Managed Microsoft AD vez. Se você precisar oferecer suporte a vários domínios ou florestas, use AWS Managed Microsoft AD. Para obter mais informações, consulte:

  - Conecte um diretório AWS Managed Microsoft AD ao IAM Identity Center
  - Conecte um diretório autogerenciado no Active Directory ao IAM Identity Center
- Use um Active Directory residente na conta de administrador delegado:

  Se você planeja habilitar o administrador delegado do IAM Identity Center e usar o Active Directory como sua fonte de identidade do IAM Identity Center, você pode usar um AD Connector ou AWS Managed Microsoft AD diretório existente configurado no AWS Diretório que reside na conta de administrador delegado.

  Se você decidir alterar a fonte de identidade do IAM Identity Center de qualquer outra fonte para o Active Directory ou alterá-la do Active Directory para qualquer outra fonte, o diretório deverá residir (pertencer à) conta de membro do administrador delegado do IAM Identity Center, se houver; caso contrário, deverá estar na conta de gerenciamento.

Conectar o Active Directory e especificar um usuário

Se já estiver usando o Active Directory, os tópicos a seguir ajudarão você a conectar o diretório ao IAM Identity Center.

Você pode conectar um AWS Managed Microsoft AD diretório ou um diretório autogerenciado no Active Directory com o IAM Identity Center. Se você planeja conectar um AWS Managed Microsoft AD diretório ou um diretório autogerenciado no Active Directory, verifique se a configuração do Active Directory atende aos pré-requisitos do. Confirme suas fontes de identidade no IAM Identity Center

> **Note**
>
> Como uma prática recomendada de segurança, habilite a autenticação multifator. Se você planeja conectar um AWS Managed Microsoft AD diretório ou um diretório autogerenciado no Active Directory e não está usando o RADIUS MFA com, AWS Directory Servicehabilite o MFA no IAM Identity Center.

AWS Managed Microsoft AD

1. Revise as orientações em Conectar-se a um diretório Microsoft AD.
2. Siga as etapas em Conecte um diretório AWS Managed Microsoft AD ao IAM Identity Center.
3. Configure o Active Directory para sincronizar o usuário ao qual você deseja conceder permissões administrativas no IAM Identity Center. Para ter mais informações, consulte Sincronizar um usuário administrativo para o IAM Identity Center.

Diretório autogerenciado no Active Directory

1. Revise as orientações em Conectar-se a um diretório Microsoft AD.
2. Siga as etapas em Conecte um diretório autogerenciado no Active Directory ao IAM Identity Center.
3. Configure o Active Directory para sincronizar o usuário ao qual você deseja conceder permissões administrativas no IAM Identity Center. Para ter mais informações, consulte Sincronizar um usuário administrativo para o IAM Identity Center.

IdP externo

1. Revise as orientações em Conecte-se a um provedor de identidades externo.
2. Siga as etapas em Como se conectar a um provedor de identidades externo.
3. Configure seu IdP para provisionar usuários no IAM Identity Center.

> **Note**
>
> Antes de configurar o provisionamento automático baseado em grupos de todas as identidades da sua força de trabalho do seu IdP no IAM Identity Center, recomendamos

que você sincronize o usuário ao qual deseja conceder permissões administrativas no IAM Identity Center.

Sincronizar um usuário administrativo para o IAM Identity Center

Depois de conectar seu diretório ao Centro de Identidade do IAM, você pode especificar um usuário ao qual deseja conceder permissões administrativas e, em seguida, sincronizá-lo do seu diretório com o Centro de Identidade do IAM.

1. Abra o console do Centro de Identidade do IAM.
2. Escolha Settings.
3. Na página Configurações, escolha a guia Origem da identidade, escolha Ações e, em seguida, Gerenciar sincronização.
4. Na página Gerenciar sincronização , escolha a guia Usuários e Adicionar usuários e grupos.
5. Na guia Usuários, em Usuário, insira o nome de usuário exato e escolha Adicionar.
6. Em Usuários e grupos adicionados, faça o seguinte:
    a. Confirme se o usuário para o qual você deseja conceder permissões administrativas foi especificado.
    b. Marque a caixa de seleção à esquerda do nome do usuário.
    c. Selecione Enviar.
7. Na página Gerenciar sincronização, o usuário que você especificou aparece na lista Usuários no escopo de sincronização.
8. No painel de navegação, escolha Users.
9. Na página Usuários, pode levar algum tempo para que o usuário que você especificou apareça na lista. Escolha o ícone de atualização para atualizar a lista de usuários.

Neste momento, seu usuário não tem acesso à conta de gerenciamento. Você configurará o acesso administrativo a essa conta criando um conjunto de permissões administrativas e atribuindo o usuário a esse conjunto de permissões. Para ter mais informações, consulte Criar um conjunto de permissões.

Provisioning when users come from Active Directory.

O IAM Identity Center usa a conexão fornecida pelo AWS Directory Service para sincronizar informações de usuário, grupo e associação do seu diretório de origem no Active Directory com o repositório de identidades do IAM Identity Center. Nenhuma informação de senha é sincronizada com o IAM Identity Center, pois a autenticação do usuário ocorre diretamente no diretório de origem no Active Directory. Esses dados de identidade são usados por aplicações para facilitar cenários de pesquisa, autorização e colaboração na aplicação sem passar a atividade de LDAP de volta ao diretório de origem no Active Directory.

Para obter mais informações sobre o provisionamento, consulte Provisionamento de usuários e grupos.

Tópicos

- Conecte um diretório AWS Managed Microsoft AD ao IAM Identity Center
- Conecte um diretório autogerenciado no Active Directory ao IAM Identity Center
- Mapeamentos de atributos para diretório AWS Managed Microsoft AD
- Provisionar usuários e grupos do Active Directory

Conecte um diretório AWS Managed Microsoft AD ao IAM Identity Center

Use o procedimento a seguir para conectar um diretório AWS Managed Microsoft AD que é gerenciado pelo AWS Directory Service IAM Identity Center.

Para se conectar AWS Managed Microsoft AD ao IAM Identity Center

1. Abra o console do Centro de Identidade do IAM.

   > **Note**
   >
   > Antes de passar para a etapa seguinte, confirme se o console do IAM Identity Center está usando uma das regiões em que seu diretório do AWS Managed Microsoft AD está localizado.

2. Escolha Settings.
3. Na página Configurações, escolha a guia Origem de identidade e, em seguida, escolha Actions > Change identity source.

4. Em Escolher origem de identidade, selecione Active Directory e, em seguida, escolha Next.
5. Em Connect active directory, escolha um diretório na AWS Managed Microsoft AD lista e, em seguida, escolha Next.
6. Em Confirmar alteração, revise as informações e, quando estiver pronto, digite ACCEPT e escolha Change identity source.

> **Important**
>
> Para especificar um usuário no Active Directory como usuário administrativo no IAM Identity Center, você deve primeiro sincronizar o usuário ao qual deseja conceder permissões administrativas do Active Directory no IAM Identity Center. Para isso, siga as etapas em Sincronizar um usuário administrativo para o IAM Identity Center.

Conecte um diretório autogerenciado no Active Directory ao IAM Identity Center

Os usuários em seu diretório autogerenciado no Active Directory (AD) também podem ter acesso de logon único Contas da AWS e aplicativos no AWS portal de acesso. Para configurar o acesso de logon único para esses usuários, você poderá seguir um destes procedimentos:

- Crie uma relação de confiança bidirecional — Quando relações de confiança bidirecionais são criadas entre AWS Managed Microsoft AD um diretório autogerenciado no AD, os usuários em seu diretório autogerenciado no AD podem entrar com suas credenciais corporativas em vários AWS serviços e aplicativos de negócios. Confianças unidirecionais não funcionam com o IAM Identity Center.

  AWS IAM Identity Center requer uma relação de confiança bidirecional para que tenha permissões para ler informações de usuários e grupos do seu domínio para sincronizar metadados de usuários e grupos. O IAM Identity Center usa esses metadados ao atribuir acesso a conjuntos de permissões ou aplicativos. Os metadados de usuários e grupos também são usados por aplicativos para colaboração, como quando você compartilha um painel com outro usuário ou grupo. A confiança do AWS Directory Service Microsoft Active Directory em seu domínio permite que o IAM Identity Center confie em seu domínio para autenticação. A confiança na direção oposta concede AWS permissões para ler metadados de usuários e grupos.

  Para obter mais informações sobre a configuração de uma confiança bidirecional, consulte Quando criar uma relação de confiança no AWS Directory Service Guia Administrativo.

- Criar um conector AD – O Conector AD é um gateway de diretório que pode redirecionar solicitações de diretório para seu AD autogerenciado sem armazenar nenhuma informação em cache na nuvem. Para obter mais informações, consulte Conectar a um Diretório no AWS Directory Service Guia de administração.

> **Note**
>
> Se você estiver conectando o IAM Identity Center a um diretório do AD Connector, qualquer futura redefinição de senha de usuário deverá ser feita de dentro do AD. Isso significa que os usuários não poderão redefinir suas senhas no portal de AWS acesso. Se você usa o AD Connector para conectar seu serviço de domínio do Active Directory ao IAM Identity Center, o IAM Identity Center só tem acesso aos usuários e grupos do único domínio ao qual o AD Connector está conectado. Se você precisar oferecer suporte a vários domínios ou florestas, use AWS Directory Service para o Microsoft Active Directory.

> **Note**
>
> O IAM Identity Center não funciona com diretórios Simple AD baseados em Samba4.

Mapeamentos de atributos para diretório AWS Managed Microsoft AD

Os mapeamentos de atributos são usados para mapear tipos de atributos que existem no IAM Identity Center com atributos semelhantes em um AWS Managed Microsoft AD diretório. O IAM Identity Center recupera os atributos do usuário do seu diretório do Microsoft AD e os mapeia para os atributos do usuário do IAM Identity Center. Esses mapeamentos de atributos de usuário do IAM Identity Center também são usados para gerar asserções SAML 2.0 para as aplicações. Cada aplicação determina a lista de atributos SAML 2.0 necessários para que o logon único tenha sucesso.

O IAM Identity Center preenche previamente um conjunto de atributos para você na guia Mapeamentos de atributo encontrada na página de configuração do seu aplicativo. O IAM Identity Center usa esses atributos de usuário para preencher as asserções SAML (como atributos SAML) que são enviadas à aplicação. Por sua vez, esses atributos de usuário são recuperados de seu diretório do Microsoft AD. Para ter mais informações, consulte Mapear atributos em sua aplicação para atributos do IAM Identity Center.

O IAM Identity Center também gerencia um conjunto de atributos para você na seção Mapeamentos de atributo da página de configuração do diretório. Para ter mais informações, consulte Mapeie atributos no IAM Identity Center para atributos em seu AWS Managed Microsoft AD diretório.

Atributos de diretório compatíveis

A tabela a seguir lista todos os atributos de AWS Managed Microsoft AD diretório que são compatíveis e que podem ser mapeados para os atributos do usuário no IAM Identity Center.

Atributos compatíveis em seu diretório do Microsoft AD
`${dir:email}`
`${dir:displayname}`
`${dir:distinguishedName}`
`${dir:firstname}`
`${dir:guid}`
`${dir:initials}`
`${dir:lastname}`
`${dir:proxyAddresses}`
`${dir:proxyAddresses:smtp}`
`${dir:proxyAddresses:SMTP}`
`${dir:windowsUpn}`

Você pode especificar qualquer combinação de atributos de diretório do Microsoft AD compatíveis para mapear para um único atributo no IAM Identity Center. Por exemplo, você pode escolher o atributo `subject` na coluna Atributo de usuário no IAM Identity Center. Em seguida, mapeie-o para `${dir:displayname}` ou `${dir:lastname}${dir:firstname }` ou qualquer atributo único suportado ou qualquer combinação arbitrária de atributos suportados. Para obter uma lista dos mapeamentos padrão para atributos do usuário no IAM Identity Center, consulte Mapeamentos padrão.

> **Warning**
>
> Alguns atributos do IAM Identity Center não podem ser modificados porque são imutáveis e mapeados por padrão para atributos específicos do diretório Microsoft AD.
> Por exemplo, “nome de usuário” é um atributo obrigatório no IAM Identity Center. Se você mapear “nome de usuário” para um atributo de diretório do AD com um valor vazio, o IAM Identity Center considerará o `windowsUpn` valor como o valor padrão para “nome de usuário”. Se você quiser alterar o mapeamento de atributos para “nome de usuário” do mapeamento atual, confirme se os fluxos do IAM Identity Center com dependência de “nome de usuário” continuarão funcionando conforme o esperado, antes de fazer a alteração.

Se você usar as ações da ListGroupsAPI ListUsersou os comandos list-userse da list-groups AWS CLI para atribuir aos usuários e grupos acesso aos Contas da AWS aplicativos, você deverá especificar o valor de `AttributeValue` como um FQDN. Esse valor deve estar no seguinte formato: user@example.com. No exemplo a seguir, `AttributeValue` é definido como `janedoe@example.com`.

```
aws identitystore list-users --identity-store-id d-12345a678b --filters
 AttributePath=UserName,AttributeValue=janedoe@example.com
```

Atributos do Centro de Identidade do IAM compatíveis

A tabela a seguir lista todos os atributos do IAM Identity Center que são compatíveis e que podem ser mapeados para os atributos do usuário em seu AWS Managed Microsoft AD diretório. Posteriormente, quando você configurar os mapeamentos de atributos de aplicativo, poderá usar os mesmos atributos do IAM Identity Center para mapear para atributos reais usados por esse aplicativo.

Atributos do Centro de Identidade do IAM compatíveis
`${user:AD_GUID}`
`${user:email}`
`${user:familyName}`
`${user:givenName}`

Atributos do Centro de Identidade do IAM compatíveis
`${user:middleName}`
`${user:name}`
`${user:preferredUsername}`
`${user:subject}`

Atributos de provedor de identidade externo compatíveis

A tabela a seguir lista todos os atributos do provedor de identidades (IdP) externo que são compatíveis e que podem ser mapeados para atributos que você pode usar ao configurar Atributos para controle de acesso no IAM Identity Center. Ao usar asserções SAML, você pode usar quaisquer atributos compatíveis com seu IdP.

Atributos compatíveis em seu IdP
`${path:userName}`
`${path:name.familyName}`
`${path:name.givenName}`
`${path:displayName}`
`${path:nickName}`
`${path:emails[primary eq true].value}`
`${path:addresses[type eq "work"].streetAddress}`
`${path:addresses[type eq "work"].locality}`
`${path:addresses[type eq "work"].region}`
`${path:addresses[type eq "work"].postalCode}`
`${path:addresses[type eq "work"].country}`

Atributos compatíveis em seu IdP
`${path:addresses[type eq "work"].formatted}`
`${path:phoneNumbers[type eq "work"].value}`
`${path:userType}`
`${path:title}`
`${path:locale}`
`${path:timezone}`
`${path:enterprise.employeeNumber}`
`${path:enterprise.costCenter}`
`${path:enterprise.organization}`
`${path:enterprise.division}`
`${path:enterprise.department}`
`${path:enterprise.manager.value}`

Mapeamentos padrão

A tabela a seguir lista os mapeamentos padrão dos atributos do usuário no IAM Identity Center para os atributos do usuário no seu AWS Managed Microsoft AD diretório. O IAM Identity Center só é compatível com a lista de atributos na coluna User attribute in IAM Identity Center.

> **Note**
>
> Se você não tiver nenhuma atribuição para seus usuários e grupos no IAM Identity Center ao ativar a sincronização configurável do AD, os mapeamentos padrão na tabela a seguir serão usados. Para obter informações sobre como personalizar esses mapeamentos, consulte Configure mapeamentos de atributos para sua sincronização.

Atributo de usuário no IAM Identity Center	Mapeia para este atributo em seu diretório do Microsoft AD
AD_GUID	${dir:guid}
email *	${dir:windowsUpn}
familyName	${dir:lastname}
givenName	${dir:firstname}
middleName	${dir:initials}
name	${dir:displayname}
preferredUsername	${dir:displayname}
subject	${dir:windowsUpn}

* O atributo de e-mail no IAM Identity Center deve ser exclusivo dentro do diretório. Caso contrário, o processo de login do JIT poderá falhar.

Você pode alterar os mapeamentos padrão ou adicionar mais atributos às asserções SAML 2.0 de acordo com suas necessidades. Por exemplo, suponha que sua aplicação exija que o e-mail do usuário no atributo `User.Email` do SAML 2.0. Além disso, suponha que os endereços de e-mail estejam armazenados no atributo `windowsUpn` em seu diretório do Microsoft AD. Para conseguir esse mapeamento, você deve fazer alterações nos dois lugares a seguir no console do IAM Identity Center:

1. Na página Directory, na seção Attribute mappings (Mapeamentos de atributos), você precisaria mapear o atributo de usuário **`email`** para o atributo **`${dir:windowsUpn}`** (na coluna Maps to this attribute in your directory [Mapeia para este atributo em seu diretório])
2. Na página Aplicativos, escolha o nome do aplicativo da tabela. Escolha a guia Attribute mapping. Em seguida, mapeie o `User.Email` atributo para o **`${user:email}`**atributo (na coluna Mapas para esse valor de string ou atributo de usuário na coluna IAM Identity Center).

Observe que é necessário fornecer cada atributo de diretório no formato ${dir:**`AttributeName`**}. Por exemplo, o atributo `firstname` em seu diretório do Microsoft AD torna-se `${dir:firstname}`. É

importante que cada atributo de diretório tenha um valor real atribuído. Os atributos que não tiverem um valor depois de `${dir:` provocarão problemas de login de usuário.

Mapeie atributos no IAM Identity Center para atributos em seu AWS Managed Microsoft AD diretório

Você pode usar o procedimento a seguir para especificar como seus atributos de usuário no IAM Identity Center devem ser mapeados para atributos correspondentes em seu diretório do Microsoft AD.

Mapear atributos no IAM Identity Center para atributos em seu diretório

1. Abra o console do IAM Identity Center.
2. Escolha Settings.
3. Na página Configurações, escolha a guia Attributes for access control e, em seguida, escolha Manage Attributes.
4. Na página Edit attribute mappings for access control (Editar mapeamentos de atributos para controle de acesso), localize o atributo no IAM Identity Center que deseja mapear e, em seguida, digite um valor na caixa de texto. Por exemplo, talvez você queira mapear o atributo de usuário do IAM Identity Center para o **`email`** atributo de diretório do Microsoft AD**`${dir:windowsUpn}`**.
5. Escolha Save changes.

Provisionar usuários e grupos do Active Directory

O IAM Identity Center fornece as duas maneiras a seguir de provisionar usuários e grupos do Active Directory.

- Sincronização configurável do Active Directory (AD) do IAM Identity Center (recomendada) — Com esse método de sincronização, você pode fazer o seguinte:
  - Controle os limites dos dados definindo explicitamente os usuários e grupos no Microsoft Active Directory que são sincronizados automaticamente no IAM Identity Center. Você pode adicionar usuários e grupos ou remover usuários e grupos para alterar o escopo da sincronização a qualquer momento.
  - Atribua a usuários e grupos sincronizados acesso de logon único Contas da AWS ou acesso a aplicativos. Os aplicativos podem ser aplicativos AWS gerenciados ou aplicativos gerenciados pelo cliente.

- Controle o processo de sincronização pausando e retomando a sincronização conforme necessário. Isso ajuda você a regular a carga nos sistemas de produção.
- Sincronização do IAM Identity Center AD — Com esse método de sincronização, você usa o IAM Identity Center para atribuir acesso a contas e aplicativos AWS . Todas as identidades com atribuições são sincronizadas automaticamente no IAM Identity Center.

Sincronização configurável no AD do IAM Identity Center

A sincronização configurável do Active Directory (AD) do IAM Identity Center permite que você configure explicitamente as identidades no Microsoft Active Directory que são sincronizadas automaticamente com o IAM Identity Center e controle o processo de sincronização.

Os tópicos a seguir fornecem informações para permitir que você configure e administre a sincronização configurável do AD.

Tópicos

- Pré-requisitos e considerações
- Como funciona a sincronização configurável do AD
- Configure e gerencie seu escopo de sincronização

Pré-requisitos e considerações

Antes de usar o AD Sync configurável, esteja ciente dos seguintes pré-requisitos e considerações:

- Como especificar usuários e grupos no Active Directory para sincronização

  Antes de usar o IAM Identity Center para atribuir a novos usuários e grupos acesso Contas da AWS e aos aplicativos AWS gerenciados ou aplicativos gerenciados pelo cliente, você deve especificar os usuários e grupos no Active Directory para sincronizar e depois sincronizá-los com o IAM Identity Center.
  - Sincronização do AD — Quando você faz atribuições para novos usuários e grupos usando o console do IAM Identity Center ou ações relacionadas da API de atribuição, o IAM Identity Center pesquisa diretamente no controlador de domínio os usuários ou grupos especificados, conclui a atribuição e sincroniza periodicamente os metadados do usuário ou do grupo no IAM Identity Center.
  - Sincronização configurável do AD — o IAM Identity Center não pesquisa usuários e grupos diretamente em seu controlador de domínio. Em vez disso, você deve primeiro especificar a

lista de usuários e grupos a serem sincronizados. Você pode configurar essa lista, também conhecida como escopo de sincronização, de uma das seguintes formas, dependendo se você tem usuários e grupos que já estão sincronizados com o IAM Identity Center ou se tem novos usuários e grupos que você está sincronizando pela primeira vez usando a sincronização configurável do AD.

- Usuários e grupos existentes: se você tiver usuários e grupos que já estão sincronizados com o IAM Identity Center, o escopo de sincronização na sincronização configurável do AD é pré-preenchido com uma lista desses usuários e grupos. Para atribuir novos usuários ou grupos, você deve adicioná-los especificamente ao escopo de sincronização. Para ter mais informações, consulte Adicione usuários e grupos ao escopo de sincronização.
- Novos usuários e grupos: se você quiser atribuir a novos usuários e grupos acesso a Contas da AWS e aos aplicativos, você deve especificar quais usuários e grupos adicionar ao escopo de sincronização na sincronização configurável do AD antes de usar o IAM Identity Center para fazer a atribuição. Para ter mais informações, consulte Adicione usuários e grupos ao escopo de sincronização.

- Fazendo atribuições para grupos aninhados no Active Directory

  Os grupos que são membros de outros grupos são chamados de grupos aninhados (ou grupos secundários). Quando você faz atribuições em um grupo no Active Directory que contém grupos aninhados, a forma como as atribuições são aplicadas depende se você usa a sincronização do AD ou a sincronização configurável do AD.

  - Sincronização AD — Quando você faz atribuições para um grupo no Active Directory que contém grupos aninhados, somente os membros diretos do grupo podem acessar a conta. Por exemplo, se você atribuir acesso ao Grupo A e o Grupo B for membro do Grupo A, somente os membros diretos do Grupo A poderão acessar a conta. Nenhum membro do Grupo B herda o acesso.
  - Sincronização configurável do AD — Usar a sincronização configurável do AD para fazer atribuições a um grupo no Active Directory que contém grupos aninhados pode aumentar o escopo dos usuários que têm acesso ou aos Contas da AWS aplicativos. Nesse caso, o exercício se aplica a todos os usuários, incluindo aqueles em grupos aninhados. Por exemplo, se você atribuir acesso ao Grupo A e o Grupo B for membro do Grupo A, somente os membros diretos do Grupo A poderão acessar a conta.
- Atualização de fluxos de trabalho automatizados

Se você tiver fluxos de trabalho automatizados que usam as ações da API de armazenamento de identidades do IAM Identity Center e as ações da API de atribuição do IAM Identity Center para atribuir a novos usuários e grupos acesso a contas e aplicativos e sincronizá-los com o IAM Identity Center, você deve ajustar esses fluxos de trabalho até 15 de abril de 2022 para que funcionem conforme o esperado com a sincronização configurável do AD. A sincronização configurável do AD altera a ordem na qual a atribuição e o provisionamento de usuários e grupos ocorrem e a forma como as consultas são realizadas.

- Sincronização do AD — O processo de atribuições ocorre primeiro. Você atribui aos usuários e grupos acesso aos Contas da AWS aplicativos. Depois que os usuários e grupos recebem acesso, eles são automaticamente provisionados (sincronizados com o IAM Identity Center). Se você tem um fluxo de trabalho automatizado, isso significa que, ao adicionar um novo usuário ao Active Directory, seu fluxo de trabalho automatizado pode consultar o Active Directory para o usuário usando a ação da `ListUser` API do repositório de identidades e, em seguida, atribuir o acesso ao usuário usando as ações da API de atribuição do IAM Identity Center. Como o usuário tem uma atribuição, esse usuário é automaticamente provisionado no IAM Identity Center.
- Sincronização configurável do AD — O provisionamento ocorre primeiro e não é executado automaticamente. Em vez disso, primeiro você deve adicionar explicitamente usuários e grupos ao repositório de identidades adicionando-os ao seu escopo de sincronização. Para obter informações sobre as etapas recomendadas para automatizar sua configuração de sincronização para sincronização configurável do AD, consulte Automatize sua configuração de sincronização para sincronização configurável do AD.

Como funciona a sincronização configurável do AD

O IAM Identity Center atualiza os dados de identidade baseados em AD no repositório de identidades usando o processo a seguir.

Criação

Depois de conectar seu diretório autogerenciado no Active Directory ou seu AWS Managed Microsoft AD diretório gerenciado pelo AWS Directory Service ao IAM Identity Center, você pode configurar explicitamente os usuários e grupos do Active Directory que você deseja sincronizar no repositório de identidades do IAM Identity Center. As identidades que você escolher serão sincronizadas a cada três horas ou mais no repositório de identidades do IAM Identity Center. Dependendo do tamanho do seu diretório, o processo de sincronização pode demorar mais.

Grupos que são membros de outros grupos (chamados grupos aninhados ou grupos secundários) também são gravados no repositório de identidades. Quando você faz atribuições em um grupo no Active Directory que contém grupos aninhados, a forma como as atribuições são aplicadas depende se você usa a sincronização do AD ou a sincronização configurável do AD. Para ter mais informações, consulte Making assignments to nested groups in Active Directory.

Você só pode atribuir acesso a novos usuários ou grupos depois que eles forem sincronizados no repositório de identidades do IAM Identity Center.

Atualizar

Os dados de identidade no repositório de identidades do IAM Identity Center permanecem atualizados por meio da leitura periódica dos dados do diretório de origem no Active Directory. O IAM Identity Center sincroniza dados do seu Active Directory a cada hora em um ciclo de sincronização por padrão. Pode levar de 30 minutos a 2 horas para que os dados sejam sincronizados com o IAM Identity Center, com base no tamanho do seu Active Directory.

Os objetos de usuário e grupo que estão no escopo de sincronização e suas associações são criados ou atualizados no IAM Identity Center para mapear os objetos correspondentes no diretório de origem no Active Directory. Para atributos do usuário, somente o subconjunto de atributos listados na seção Attributes for access control do console do IAM Identity Center é atualizado no IAM Identity Center. Pode ser necessário um ciclo de sincronização para que qualquer atualização de atributo feita no Active Directory seja refletida no IAM Identity Center.

Você também pode atualizar o subconjunto de usuários e grupos que você sincroniza no repositório de identidades do IAM Identity Center. Você pode optar por adicionar novos usuários ou grupos a esse subconjunto ou removê-los. Todas as identidades que você adicionar serão sincronizadas na próxima sincronização agendada. As identidades que você remover do subconjunto deixarão de ser atualizadas no armazenamento de identidades do IAM Identity Center. Qualquer usuário que não estiver sincronizado por mais de 28 dias será desativado no repositório de identidades do IAM Identity Center. Os objetos de usuário correspondentes serão automaticamente desativados no repositório de identidades do IAM Identity Center durante o próximo ciclo de sincronização, a menos que façam parte de outro grupo que ainda faça parte do escopo da sincronização.

Exclusão

Usuários e grupos são excluídos do repositório de identidades do IAM Identity Center quando os objetos de usuário ou grupo correspondentes são excluídos do diretório de origem no Active Directory. Como alternativa, você pode excluir explicitamente objetos de usuário do repositório de

identidades do IAM Identity Center usando o console do IAM Identity Center. Se você usa o console do IAM Identity Center, também deve remover os usuários do escopo de sincronização para garantir que eles não sejam sincronizados novamente com o IAM Identity Center durante o próximo ciclo de sincronização.

Você também pode pausar e reiniciar a sincronização a qualquer momento. Se você pausar a sincronização por mais de 28 dias, todos os seus usuários serão desativados.

Configure e gerencie seu escopo de sincronização

É possível configurar o escopo de sincronização de uma das seguintes formas:

- Configuração guiada: se você estiver sincronizando seus usuários e grupos do Active Directory no IAM Identity Center pela primeira vez, siga as etapas em Configuração guiada para configurar seu escopo de sincronização. Depois de concluir a configuração guiada, você pode modificar seu escopo de sincronização a qualquer momento seguindo os outros procedimentos desta seção.
- Se você já tem usuários e grupos sincronizados no IAM Identity Center ou não quer seguir a configuração guiada, escolha Manage sync. Ignore o procedimento de configuração guiada e siga os outros procedimentos desta seção, conforme necessário, para configurar e gerenciar seu escopo de sincronização.

Procedimentos

- Configuração guiada
- Adicione usuários e grupos ao escopo de sincronização
- Remova usuários e grupos ao escopo de sincronização
- Interromper e retomar a sincronização
- Configure mapeamentos de atributos para sua sincronização
- Automatize sua configuração de sincronização para sincronização configurável do AD

Configuração guiada

1. Abra o console do IAM Identity Center.

> **Note**
>
> Certifique-se de que o console do IAM Identity Center esteja usando um dos Regiões da AWS locais em que seu AWS Managed Microsoft AD diretório está localizado antes de passar para a próxima etapa.

2. Escolha Settings.
3. Na parte superior da página, na mensagem de notificação, escolha Start guided setup.
4. Na Etapa 1 — opcional: Configurar mapeamentos de atributos, revise os mapeamentos padrão de atributos de usuário e grupo. Se nenhuma alteração for necessária, escolha Next. Se forem necessárias alterações, faça as alterações e escolha Save changes.
5. Na Etapa 2 — opcional: Configurar o escopo da sincronização, escolha a guia Users. Em seguida, insira o nome de usuário exato do usuário que você deseja adicionar ao seu escopo de sincronização e escolha Add. Em seguida, escolha a guia Groups. Insira o nome exato do grupo que você deseja adicionar ao seu escopo de sincronização e escolha Add. Em seguida, escolha Next. Se você quiser adicionar usuários e grupos ao seu escopo de sincronização posteriormente, não faça alterações e escolha Next.
6. Na Etapa 3: Revise e salve a configuração, confirme seus mapeamentos de atributos na Etapa 1: Mapeamentos de atributos e seus usuários e grupos na Etapa 2: Escopo de sincronização. Escolha Save configuration. Isso o levará para a página Gerenciar Sincronização.

Adicione usuários e grupos ao escopo de sincronização

Como adicionar usuários

1. Abra o console do IAM Identity Center.
2. Escolha Settings.
3. Na página Configurações, escolha a guia Origem da identidade, escolha Ações e, em seguida, Gerenciar sincronização.
4. Na página Gerenciar sincronização , escolha a guia Usuários e Adicionar usuários e grupos.
5. Na guia User, em User, insira o nome de usuário exato e escolha Adicionar.
6. Em Usuários e grupos adicionados, revise o usuário que você deseja adicionar.
7. Selecione Submit.
8. No painel de navegação, escolha Users.

9. Na página Usuários, pode levar algum tempo para que o usuário que você especificou apareça na lista. Escolha o ícone de atualização para atualizar a lista de usuários.

Para adicionar grupos

1. Abra o console do IAM Identity Center.
2. Escolha Settings.
3. Na página Configurações, escolha a guia Identity source, escolha Actions e, em seguida, escolha Manage Sync.
4. Na página Manage Sync, escolha a guia Groups e, em seguida, escolha Add users and groups.
5. Escolha a guia Groups. Em Grupo, insira o nome exato do grupo e escolha Add.
6. Em Added Users and Groups, revise o grupo que você deseja adicionar.
7. Selecione Submit.
8. No painel de navegação, escolha Groups.
9. Na página Groups, pode levar algum tempo para que o grupo que você especificou apareça na lista. Escolha o ícone de atualização para atualizar a lista de grupos.

Remova usuários e grupos ao escopo de sincronização

Para obter mais informações sobre o que acontece quando você remove usuários e grupos do seu escopo de sincronização, consulte Como funciona a sincronização configurável do AD.

Para remover um usuário

1. Abra o console do IAM Identity Center.
2. Escolha Settings.
3. Na página Configurações, escolha a guia Identity source, escolha Actions e, em seguida, escolha Manage Sync.
4. Escolha a guia Users.
5. Em Usuários no escopo de sincronização, marque a caixa de seleção ao lado do usuário que você deseja excluir. Para excluir todos os usuários, marque a caixa de seleção ao lado do Username.
6. Escolha Remover.

Para remover grupos

1. Abra o console do IAM Identity Center.
2. Escolha Settings.
3. Na página Configurações, escolha a guia Identity source, escolha Actions e, em seguida, escolha Manage Sync.
4. Escolha a guia Groups.
5. Em Groups in sync scope, marque a caixa de seleção ao lado do usuário que você deseja excluir. Para excluir todos os grupos, marque a caixa de seleção ao lado Group name.
6. Escolha Remover.

Interromper e retomar a sincronização

Pausar sua sincronização pausa todos os ciclos de sincronização futuros e impede que as alterações feitas nos usuários e grupos no Active Directory sejam refletidas no IAM Identity Center. Depois de retomar a sincronização, o ciclo de sincronização seleciona essas alterações na próxima sincronização agendada.

Para pausar a sincronização

1. Abra o console do IAM Identity Center.
2. Escolha Settings.
3. Na página Configurações, escolha a guia Identity source, escolha Actions e, em seguida, escolha Manage Sync.
4. Em Manage Sync, escolha Pause sync.

Para retomar a sincronização

1. Abra o console do IAM Identity Center.
2. Escolha Settings.
3. Na página Configurações, escolha a guia Identity source, escolha Actions e, em seguida, escolha Manage Sync.
4. Em Manage Sync, escolha Resume sync.

> **Note**
>
> Se você vir Pause sync em vez de Resume sync, a sincronização do Active Directory com o IAM Identity Center já foi retomada.

Configure mapeamentos de atributos para sua sincronização

Para obter mais informações sobre atributos disponíveis, consulte Mapeamentos de atributos para diretório AWS Managed Microsoft AD.

Mapear atributos no IAM Identity Center para atributos em seu diretório

1. Abra o console do IAM Identity Center.
2. Escolha Settings.
3. Na página Configurações, escolha a guia Identity source, escolha Actions e, em seguida, escolha Manage Sync.
4. Em Manage Sync, escolha View attribute mapping.
5. Em Active Directory user attributes do IAM Identity Center identity store attributes de Active Directory user attributes. Por exemplo, talvez você queira mapear o atributo de usuário do IAM Identity Center para o `email` atributo de diretório do Microsoft AD`${objectguid}`.

   > **Note**
   >
   > Em Atributos de Group attributes do IAM Identity Center identity store attributes Active Directory group attributes não podem ser alterados.

6. Escolha Save changes. Isso o levará de volta à página Manage Sync.

Automatize sua configuração de sincronização para sincronização configurável do AD

Para garantir que seu fluxo de trabalho automatizado funcione conforme o esperado com a sincronização configurável do AD, recomendamos que você execute as etapas a seguir para automatizar sua configuração de sincronização.

Automatize sua configuração de sincronização para sincronização configurável do AD

1. No Active Directory, crie um grupo de sincronização principal para conter todos os usuários e grupos que você deseja sincronizar no IAM Identity Center. Por exemplo, você pode nomear o grupo IAM IdentityCenterAllUsersAndGroups.
2. No IAM Identity Center, adicione o grupo de sincronização principal à sua lista de sincronização configurável. O IAM Identity Center sincronizará todos os usuários, grupos, subgrupos e membros de todos os grupos contidos no grupo de sincronização principal.
3. Use as ações da API de gerenciamento de usuários e grupos do Active Directory fornecidas pela Microsoft para adicionar ou remover usuários e grupos do grupo de sincronização principal.

IAM Identity Center e Sincronização

Com o IAM Identity Center AD sync, você usa o IAM Identity Center para atribuir aos usuários e grupos no Active Directory acesso a Contas da AWS e aos aplicativos AWS gerenciados ou aplicativos gerenciados pelo cliente. Todas as identidades com atribuições são sincronizadas automaticamente no IAM Identity Center.

Como a sincronização do IAM Identity Center AD funciona

O IAM Identity Center atualiza os dados de identidade baseados em AD no repositório de identidades usando o processo a seguir.

Criação

Quando você atribui usuários, grupos Contas da AWS ou aplicativos usando o AWS console ou as chamadas da API de atribuição, as informações sobre os usuários, grupos e membros são sincronizadas periodicamente no repositório de identidades do IAM Identity Center. Os usuários ou grupos adicionados às atribuições do IAM Identity Center geralmente aparecem no repositório de AWS identidades em duas horas. Dependendo da quantidade de dados que estão sendo sincronizados, esse processo pode levar mais tempo. Somente usuários e grupos aos quais foi atribuído acesso diretamente, ou que são membros de um grupo ao qual foi atribuído acesso, são sincronizados.

Grupos que são membros de outros grupos (chamados de grupos aninhados) também são gravados no repositório de identidades. Quando você faz atribuições em um grupo no Active Directory que contém grupos aninhados, a forma como as atribuições são aplicadas depende se você usa a sincronização do AD ou a sincronização configurável do AD.

- Sincronização AD — Quando você faz atribuições para um grupo no Active Directory que contém grupos aninhados, somente os membros diretos do grupo podem acessar a conta. Por exemplo, se você atribuir acesso ao Grupo A e o Grupo B for membro do Grupo A, somente os membros diretos do Grupo A poderão acessar a conta. Nenhum membro do Grupo B herda o acesso.
- Sincronização configurável do AD — Usar a sincronização configurável do AD para fazer atribuições a um grupo no Active Directory que contém grupos aninhados pode aumentar o escopo dos usuários que têm acesso ou aos Contas da AWS aplicativos. Nesse caso, o exercício se aplica a todos os usuários, incluindo aqueles em grupos aninhados. Por exemplo, se você atribuir acesso ao Grupo A e o Grupo B for membro do Grupo A, somente os membros diretos do Grupo A poderão acessar a conta.

Se um usuário acessar o IAM Identity Center antes que seu objeto de usuário tenha sido sincronizado pela primeira vez, o objeto de armazenamento de identidades desse usuário será criado sob demanda usando o provisionamento just-in-time (JIT). Os usuários criados pelo provisionamento do JIT não são sincronizados, a menos que tenham direitos do IAM Identity Center atribuídos diretamente ou baseados em grupos. As associações de grupos para usuários provisionados pelo JIT ficam indisponíveis até depois da sincronização.

Para obter instruções sobre como atribuir acesso aos usuários Contas da AWS, consulteAcesso com login único a Contas da AWS.

Atualizar

Os dados de identidade no repositório de identidades do IAM Identity Center permanecem atualizados por meio da leitura periódica dos dados do diretório de origem no Active Directory. Os dados de identidade que são alterados no Active Directory geralmente aparecem no repositório de AWS identidades em quatro horas. Dependendo da quantidade de dados que estão sendo sincronizados, esse processo pode levar mais tempo.

Os objetos de usuário e grupo que estão no escopo de sincronização e suas associações são criados ou atualizados no IAM Identity Center para mapear os objetos correspondentes no diretório de origem no Active Directory. Para atributos do usuário, somente o subconjunto de atributos listados na seção Manage attributes for access control do console do IAM Identity Center é atualizado no IAM Identity Center. Além disso, os atributos do usuário são atualizados com cada evento de autenticação do usuário.

Exclusão

Usuários e grupos são excluídos do repositório de identidades do IAM Identity Center quando os objetos de usuário ou grupo correspondentes são excluídos do diretório de origem no Active Directory.

Conecte-se a um provedor de identidades externo

Se você estiver usando um diretório autogerenciado no Active Directory ou em um AWS Managed Microsoft AD, consulteConectar-se a um diretório Microsoft AD. Para outros provedores de identidade externos (IdPs), você pode usar AWS IAM Identity Center para autenticar identidades IdPs por meio do padrão Security Assertion Markup Language (SAML) 2.0. Isso permite que seus usuários entrem no portal de AWS acesso com suas credenciais corporativas. Eles podem então navegar até suas contas, funções e aplicativos atribuídos hospedados externamente IdPs.

Por exemplo, você pode conectar um IdP externo, como o Okta ou o Microsoft Entra ID (AD), ao IAM Identity Center. Seus usuários podem então entrar no portal de AWS acesso com suas Microsoft Entra ID credenciais Okta ou existentes. Para controlar o que seus usuários podem fazer depois de entrarem, você pode atribuir a eles permissões de acesso centralmente em todas as contas e aplicativos AWS da sua organização. Além disso, os desenvolvedores podem simplesmente entrar no AWS Command Line Interface (AWS CLI) usando suas credenciais existentes e se beneficiar da geração e rotação automáticas de credenciais de curto prazo.

O protocolo SAML não fornece uma forma de consultar o IdP para aprender sobre usuários e grupos. Portanto, você deve informar o IAM Identity Center sobre esses usuários e grupos, provisionando-os no IAM Identity Center.

Provisionamento quando os usuários vêm de um IdP externo

Ao usar um IdP externo, você deve provisionar todos os usuários e grupos aplicáveis no IAM Identity Center antes de poder fazer qualquer atribuição ou aplicativo. Contas da AWS Para fazer isso, você pode configurar o Provisionamento automático para usuários e grupos ou usar o Provisionamento manual. Independentemente de como você provisiona usuários, o IAM Identity Center redireciona a interface da AWS Management Console linha de comando e a autenticação do aplicativo para seu IdP externo. Em seguida, o IAM Identity Center concede acesso a esses recursos com base nas políticas que você cria no IAM Identity Center. Para obter mais informações sobre provisionamento, consulte Provisionamento de usuários e grupos.

Como se conectar a um provedor de identidades externo

Há step-by-step tutoriais disponíveis para os apoiados: IdPs

- CyberArk
- Google Workspace
- JumpCloud
- Microsoft Entra ID
- Okta
- OneLogin
- Ping Identity

Existem diferentes pré-requisitos, considerações e procedimentos de provisionamento para os diferentes dispositivos externos suportados. IdPs O procedimento a seguir apresenta uma visão geral do procedimento usado com todos os provedores de identidades externos.

Conectar-se a um provedor de identidades externo

1. Abra o console do IAM Identity Center.
2. Escolha Configurações.
3. Na página Configurações, escolha a guia Origem da identidade e, em seguida, escolha Ações > Alterar origem da identidade.
4. Em Escolher fonte de identidade, selecione Escolher fonte de identidade e, depois, Próximo.
5. Em Configurar provedor de identidades externo, faça o seguinte:

    a. Em Metadados do provedor de serviços, escolha Baixar arquivo de metadados para baixar o arquivo de metadados e salvá-lo em seu sistema. O arquivo de metadados SAML do IAM Identity Center é exigido pelo seu provedor de identidades externo.

    b. Em Metadados do provedor de identidades, selecione Escolher arquivo e localize o arquivo de metadados que você baixou do seu provedor de identidades externo. Em seguida, faça upload do arquivo. Esse arquivo de metadados contém o certificado x509 público necessário usado para confiar em mensagens enviadas do IdP.

    c. Escolha Próximo.

> **Important**
>
> Alterar sua fonte para ou do Active Directory remove todas as atribuições existentes de usuários e grupos. Você deve reaplicar manualmente os exercícios depois de alterar sua fonte com sucesso.

6. Depois de ler a isenção de responsabilidade e estar pronto para continuar, insira ACEITAR.
7. Escolha Alterar origem de identidade. Uma mensagem de status informa que você alterou com sucesso a fonte de identidades.

Tópicos

- Usando a federação de identidades SAML e SCIM com provedores de identidade externos
- Perfil do SCIM e implementação SAML 2.0

Usando a federação de identidades SAML e SCIM com provedores de identidade externos

O IAM Identity Center implementa os seguintes protocolos baseados em padrões para federação de identidades:

- SAML 2.0 para autenticação do usuário
- SCIM para provisionamento

Espera-se que qualquer provedor de identidades (IdP) que implemente esses protocolos padrão interopere com sucesso com o IAM Identity Center, com as seguintes considerações especiais:

- SAML
  - O IAM Identity Center exige um formato SAML NameID de endereço de e-mail (ou seja, `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`).
  - O valor do campo NameID nas asserções deve ser uma string (“”) compatível com RFC 2822 (https://tools.ietf.org/html/rfc2822) (https://tools.ietf.org/html/rfc2822#section-3.4.1). `name@domain.com`
  - O arquivo de metadados não pode ter mais de 75.000 caracteres.

  - Os metadados devem conter um EntityID, certificado X509 e SingleSignOnService como parte da URL de login.
  - Uma chave de criptografia não é compatível.

- SCIM
  - A implementação do IAM Identity Center SCIM é baseada nos RFCs 7642 (https://tools.ietf.org/html/rfc7642), 7643 (https://tools.ietf.org/html/rfc7643) e 7644 (https://tools.ietf.org/html/rfc7644) do SCIM e nos requisitos de interoperabilidade estabelecidos no rascunho de março de 2020 do Basic SCIM Profile 1.0 (https://openid.net/specs/fastfed-scim-1_0-02.html#rfc.section.4). FastFed Todas as diferenças entre esses documentos e a implementação atual no IAM Identity Center estão descritas na seção Operações de API suportadas do Guia do desenvolvedor de implementação do IAM Identity Center SCIM.

IdPs que não estejam em conformidade com os padrões e as considerações mencionadas acima não são suportadas. Entre em contato com seu IdP para perguntas ou esclarecimentos sobre a conformidade de seus produtos com esses padrões e considerações.

Se você tiver problemas para conectar seu IdP ao IAM Identity Center, recomendamos que você verifique:

- AWS CloudTrail registra filtrando o nome do evento P ExternalId DirectoryLogin
- Registros específicos do IdP e/ou registros de depuração
- Solução de problemas do IAM Identity Center

> **Note**
>
> Alguns IdPs, como os doTutoriais de introdução, oferecem uma experiência de configuração simplificada para o IAM Identity Center na forma de um “aplicativo” ou “conector” criado especificamente para o IAM Identity Center. Se o seu IdP fornecer essa opção, recomendamos que a utilize, tomando cuidado ao escolher o item criado especificamente para o IAM Identity Center. Outros itens chamados “AWS”, “AWS federação” ou nomes genéricos de "AWS" semelhantes podem usar outras abordagens de federação e/ou endpoints e podem não funcionar conforme o esperado com o IAM Identity Center.

Perfil do SCIM e implementação SAML 2.0

Tanto o SCIM quanto o SAML são considerações importantes para configurar o IAM Identity Center.

Implementação SAML 2.0

O IAM Identity Center é compatível com federação de identidades com SAML (Security Assertion Markup Language) 2.0. Isso permite que o IAM Identity Center autentique identidades de provedores de identidade externos ()IdPs. O SAML 2.0 é um padrão aberto usado para trocar afirmações SAML com segurança. O SAML 2.0 transmite informações sobre um usuário entre uma autoridade SAML (chamada de provedor de identidades ou IdP) e um consumidor de SAML (chamado de provedor de serviços ou SP). O serviço IAM Identity Center usa essas informações para fornecer login único federado. O login único permite que os usuários acessem Contas da AWS e configurem aplicativos com base em suas credenciais de provedor de identidade existentes.

O IAM Identity Center adiciona recursos de SAML IdP à sua loja AWS Managed Microsoft AD do IAM Identity Center ou a um provedor de identidade externo. Os usuários podem então fazer login único em serviços que oferecem suporte ao SAML, incluindo aplicativos AWS Management Console de terceirosMicrosoft 365, como, e. Concur Salesforce

No entanto, o protocolo SAML não fornece uma forma de consultar o IdP para aprender sobre usuários e grupos. Portanto, você deve informar o IAM Identity Center sobre esses usuários e grupos, provisionando-os no IAM Identity Center.

Perfil do SCIM

O IAM Identity Center fornece suporte para o padrão System for Cross-domain Identity Management (SCIM) v2.0. O SCIM mantém as identidades do IAM Identity Center sincronizadas com as identidades do seu IdP. Isso inclui qualquer provisionamento, atualizações e desprovisionamento de usuários entre seu IdP e o IAM Identity Center.

Para obter mais informações sobre como implementar o SCIM, consulteProvisionamento automático. Para obter mais detalhes sobre a implementação do SCIM do IAM Identity Center, consulte o Guia do desenvolvedor de implementação do IAM Identity Center do SCIM.

Tópicos

- Provisionamento automático
- Provisionamento manual
- Gerenciar certificados SAML 2.0

Provisionamento automático

O IAM Identity Center oferece suporte ao provisionamento automático (sincronização) de informações de usuários e grupos do seu provedor de identidades (IdP) no IAM Identity Center usando o protocolo System for Cross-domain Identity Management (SCIM) v2.0. Ao configurar a sincronização do SCIM, você cria um mapeamento dos atributos de usuário do seu provedor de identidades (IdP) para os atributos nomeados no IAM Identity Center. Isso faz com que os atributos esperados correspondam entre o IAM Identity Center e seu IdP. Você configura essa conexão em seu IdP usando seu endpoint SCIM para o IAM Identity Center e um token de portador que você cria no IAM Identity Center.

Tópicos

Considerações sobre o uso do provisionamento automático

Antes de começar a implantar o SCIM, recomendamos que você primeiro analise as seguintes considerações importantes sobre como ele funciona com o IAM Identity Center. Para considerações adicionais sobre provisionamento, consulte o Tutoriais de introdução aplicável ao seu IdP.

- Se você estiver provisionando um endereço de e-mail principal, esse valor de atributo deverá ser exclusivo para cada usuário. Em alguns casos IdPs, o endereço de e-mail principal pode não ser um endereço de e-mail real. Por exemplo, pode ser um Universal Principal Name (UPN) que só se parece com um e-mail. Eles IdPs podem ter um endereço de e-mail secundário ou “outro” que contém o endereço de e-mail real do usuário. Você deve configurar o SCIM em seu IdP para mapear o endereço de e-mail exclusivo não NULL para o atributo de endereço de e-mail principal do IAM Identity Center. E você deve mapear o identificador de login exclusivo não NULL do usuário para o atributo de nome de usuário do IAM Identity Center. Verifique se o seu IdP tem um valor único que seja o identificador de login e o nome de e-mail do usuário. Nesse caso, você

pode mapear esse campo IdP para o e-mail principal do IAM Identity Center e para o nome de usuário do IAM Identity Center.

- Para que a sincronização do SCIM funcione, cada usuário deve ter um valor especificado de nome, sobrenome, nome de usuário e nome de exibição. Se algum desses valores estiver ausente de um usuário, esse usuário não será provisionado.
- Se você precisar usar aplicativos de terceiros, primeiro precisará mapear o atributo de assunto SAML de saída para o atributo de nome de usuário. Se o aplicativo de terceiros precisar de um endereço de e-mail roteável, você deverá fornecer o atributo de e-mail ao seu IdP.
- Os intervalos de provisionamento e atualização do SCIM são controlados pelo seu provedor de identidades. As alterações nos usuários e grupos em seu provedor de identidade só são refletidas no IAM Identity Center depois que seu provedor de identidades envia essas alterações para o IAM Identity Center. Consulte seu provedor de identidades para obter detalhes sobre a frequência das atualizações de usuários e grupos.
- Atualmente, atributos de vários valores (como vários e-mails ou números de telefone de um determinado usuário) não são provisionados com o SCIM. As tentativas de sincronizar atributos de vários valores no IAM Identity Center com o SCIM falharão. Para evitar falhas, certifique-se de que somente um único valor seja passado para cada atributo. Se você tiver usuários com atributos de vários valores, remova ou modifique os mapeamentos de atributos duplicados no SCIM em seu IdP para a conexão com o IAM Identity Center.
- Verifique se o mapeamento `externalId` SCIM em seu IdP corresponde a um valor exclusivo, sempre presente e com menor probabilidade de alteração para seus usuários. Por exemplo, seu IdP pode fornecer um identificador `objectId` garantido ou outro que não seja afetado por alterações nos atributos do usuário, como nome e e-mail. Nesse caso, você pode mapear esse valor para o campo `externalId` do SCIM. Isso garante que seus usuários não percam AWS direitos, atribuições ou permissões se você precisar alterar o nome ou o e-mail deles.
- Usuários que ainda não foram atribuídos a um aplicativo ou que Conta da AWS não podem ser provisionados no IAM Identity Center. Para sincronizar usuários e grupos, certifique-se de que eles estejam atribuídos ao aplicativo ou a outra configuração que represente a conexão do seu IdP com o IAM Identity Center.
- O comportamento de desprovisionamento do usuário é gerenciado pelo provedor de identidade e pode variar de acordo com sua implementação. Consulte seu provedor de identidade para obter detalhes sobre o desprovisionamento de usuários.

Para obter mais informações sobre a implementação do SCIM do IAM Identity Center, consulte o Guia do desenvolvedor de implementação do IAM Identity Center do SCIM.

Como monitorar a expiração do token de acesso

Os tokens de acesso ao SCIM são gerados com validade de um ano. Quando seu token de acesso ao SCIM está configurado para expirar em 90 dias ou menos, AWS envia lembretes no console do IAM Identity Center e no AWS Health painel para ajudá-lo a alternar o token. Ao fazer rodízio do token de acesso do SCIM antes que ele expire, você protege continuamente o provisionamento automático das informações do usuário e do grupo. Se o token de acesso do SCIM expirar, a sincronização das informações do usuário e do grupo do seu provedor de identidades no IAM Identity Center será interrompida, portanto, o provisionamento automático não poderá mais fazer atualizações ou criar e excluir informações. A interrupção do provisionamento automático pode impor riscos de segurança mais graves e afetar o acesso aos seus serviços.

Os lembretes do console do Identity Center persistem até que você faça rodízio do token de acesso do SCIM e exclua todos os tokens de acesso não utilizados ou expirados. Os eventos do AWS Health Dashboard são renovados semanalmente entre 90 a 60 dias, duas vezes por semana de 60 a 30 dias, três vezes por semana de 30 a 15 dias e diariamente a partir de 15 dias até que os tokens de acesso ao SCIM expirem.

Como habilitar provisionamento automático

Use o procedimento a seguir para ativar o provisionamento automático de usuários e grupos do seu IdP para o IAM Identity Center usando o protocolo SCIM.

> **Note**
>
> Antes de iniciar esse procedimento, recomendamos que você analise antes as considerações de provisionamento que sejam aplicáveis ao seu IdP. Para obter mais informações, consulte o Tutoriais de introdução para seu IdP.

Para habilitar o provisionamento automático no IAM Identity Center

1. Depois de concluir os pré-requisitos, abra o console do IAM Identity Center.
2. Escolha Configurações no painel de navegação à esquerda.
3. Na página Configurações, localize a caixa de informações Provisionamento automático e selecione Habilitar. Isso habilita imediatamente o provisionamento automático no IAM Identity Center e exibe as informações necessárias do endpoint SCIM e do token de acesso.

4. Na caixa de diálogo Provisionamento automático de entrada, copie cada um dos valores para as opções a seguir. Você precisará colá-los posteriormente ao configurar o provisionamento em seu IdP.

   a. Endpoint do SCIM

   b. Token de acesso

5. Escolha Fechar.

Depois de concluir este procedimento, você deve configurar o provisionamento automático em seu IdP. Para obter mais informações, consulte o Tutoriais de introdução para seu IdP.

Como desabilitar provisionamento automático

Use o procedimento a seguir para desabilitar o provisionamento automático no console do IAM Identity Center.

> **Important**
>
> Você deve excluir o token de acesso antes de iniciar esse procedimento. Para ter mais informações, consulte Como excluir um token de acesso.

Para desabilitar o provisionamento automático no console do IAM Identity Center

1. No console do IAM Identity Center, escolha Configurações no painel de navegação à esquerda.
2. Na página Configurações, escolha a guia Origem da identidade e escolha Ações > Gerenciar provisionamento.
3. Na página Provisionamento automático, escolha Desabilitar.
4. Na caixa de diálogo Desabilitar provisionamento automático, revise as informações, digite DESABILITAR e escolha Desabilitar provisionamento automático.

Como gerar um novo token de acesso

Use o procedimento a seguir para gerar um novo token de acesso no console do IAM Identity Center.

> **Note**
>
> Esse procedimento exige que você tenha habilitado antes o provisionamento automático. Para ter mais informações, consulte Como habilitar provisionamento automático.

Para gerar um novo token de acesso

1. No console do IAM Identity Center, escolha Configurações no painel de navegação à esquerda.
2. Na página Configurações, escolha a guia Origem da identidade e escolha Ações > Gerenciar provisionamento.
3. Na página Provisionamento automático, em Tokens de acesso, escolha Gerar token.
4. Na caixa de diálogo Gerar novo token de acesso, copie o novo token de acesso e salve-o em um local seguro.
5. Escolha Fechar.

Como excluir um token de acesso

Use o procedimento a seguir para excluir um token de acesso existente no console do IAM Identity Center.

Para excluir um token de acesso

1. No console do IAM Identity Center, escolha Configurações no painel de navegação à esquerda.
2. Na página Configurações, escolha a guia Origem da identidade e escolha Ações > Gerenciar provisionamento.
3. Na página Provisionamento automático, em Tokens de acesso, exclua e selecione Excluir.
4. Na caixa de diálogo Excluir token de acesso, revise as informações, digite EXCLUIR e escolha Excluir token de acesso.

Como fazer rodízio de um token de acesso

Um diretório do IAM Identity Center suporta até dois tokens de acesso por vez. Para gerar um token de acesso adicional antes de qualquer rodízio, exclua todos os tokens de acesso expirados ou não utilizados.

Se seu token de acesso SCIM estiver prestes a expirar, você poderá usar o procedimento a seguir para alternar um token de acesso existente no console do IAM Identity Center.

Para fazer rodízio de um token de acesso

1. No console do IAM Identity Center, escolha Configurações no painel de navegação à esquerda.
2. Na página Configurações, escolha a guia Origem da identidade e escolha Ações > Gerenciar provisionamento.
3. Na página Provisionamento automático, em Tokens de acesso, anote o ID do token que você deseja alternar.
4. Siga as etapas em Como gerar um novo token de acesso para criar um novo token. Se você já criou o número máximo de tokens de acesso ao SCIM, primeiro precisará excluir um dos tokens existentes.
5. Acesse o site do seu provedor de identidades e configure o novo token de acesso para provisionamento do SCIM e, em seguida, teste a conectividade com o IAM Identity Center usando o novo token de acesso do SCIM. Depois de confirmar que o provisionamento está funcionando com êxito usando o novo token, continue com a próxima etapa desse procedimento.
6. Siga as etapas em Como excluir um token de acesso para excluir o token de acesso antigo que você anotou anteriormente. Você também pode usar a data de criação do token como uma dica de qual token remover.

Provisionamento manual

Alguns IdPs não têm suporte ao System for Cross-domain Identity Management (SCIM) ou têm uma implementação de SCIM incompatível. Nesses casos, você pode provisionar usuários manualmente por meio do console do IAM Identity Center. Ao adicionar usuários ao IAM Identity Center, certifique-se de definir o nome de usuário para ser idêntico ao nome de usuário que você tem no seu IdP. No mínimo, você deve ter um endereço de e-mail e nome de usuário exclusivos. Para ter mais informações, consulte Exclusividade do nome de usuário e endereço de e-mail.

Você também deve gerenciar todos os grupos manualmente no IAM Identity Center. Para fazer isso, você cria os grupos e os adiciona usando o console do IAM Identity Center. Esses grupos não precisam corresponder ao que existe em seu IdP. Para ter mais informações, consulte Grupos.

Gerenciar certificados SAML 2.0

O IAM Identity Center usa certificados para configurar uma relação de confiança SAML entre seu provedor de identidades (IdP) e o IAM Identity Center. Ao adicionar um IdP externo no IAM Identity Center, você também deve obter pelo menos um certificado SAML 2.0 X.509 público do IdP externo. Esse certificado geralmente é instalado automaticamente durante a troca de metadados SAML do IdP durante a criação da confiança.

Como administrador do IAM Identity Center, você ocasionalmente precisará substituir certificados IdP antigos por outros mais novos. Por exemplo, talvez seja necessário substituir um certificado IdP quando a data de expiração do certificado se aproximar. O processo de substituição de um certificado antigo por um mais recente é conhecido como rodízio de certificados.

Tópicos

Alterar um certificado SAML 2.0

Talvez seja necessário importar certificados periodicamente para alternar certificados inválidos ou expirados emitidos pelo seu provedor de identidades. Isso ajuda a evitar a interrupção da autenticação ou o tempo de inatividade da autenticação. Todos os certificados importados são automaticamente ativos. Os certificados só devem ser excluídos depois de garantir que não estejam mais em uso com o provedor de identidades associado.

Você também deve considerar que alguns IdPs podem não oferecer suporte a vários certificados. Nesse caso, o ato de alternar certificados com eles IdPs pode significar uma interrupção temporária do serviço para seus usuários. O serviço é restaurado quando a confiança com esse IdP é restabelecida com sucesso. Planeje essa operação com cuidado fora do horário de pico, se possível.

> **Note**
>
> Como prática recomendada de segurança, em caso de qualquer sinal de comprometimento ou manuseio incorreto de um certificado SAML existente, você deve remover e alternar o certificado imediatamente.

A rotação de um certificado do IAM Identity Center é um processo de várias etapas que envolve o seguinte:

- Obtendo um novo certificado do IdP
- Importação do novo certificado para o IAM Identity Center
- Ativando o novo certificado no IdP
- Excluindo o certificado antigo

Use todos os procedimentos a seguir para concluir o processo de rotação de certificados e, ao mesmo tempo, evitar qualquer tempo de inatividade da autenticação.

Etapa1: Obter um novo certificado do IdP

Acesse o site do IdP e baixe o certificado SAML 2.0. Certifique-se de que o arquivo do certificado seja baixado no formato codificado PEM. A maioria dos provedores permite que você crie vários certificados SAML 2.0 no IdP. É provável que sejam marcados como desativados ou inativos.

Etapa 2: Importar o novo certificado para o IAM Identity Center

Use o procedimento a seguir para importar o novo certificado usando o console do IAM Identity Center.

1. No console do IAM Identity Center, escolha Configurações.
2. Na página Configurações, escolha a guia Origem da identidade e escolha Ações > Gerenciar autenticação.
3. Na página Gerenciar certificados SAML 2.0 escolha Importar certificado.
4. Na caixa de diálogo Importar certificado SAML 2.0, selecione Escolher arquivo, navegue até seu arquivo de certificado, selecione-o e, em seguida, escolha Importar certificado.

Nesse ponto, o IAM Identity Center confiará em todas as mensagens SAML recebidas assinadas pelos dois certificados que você importou.

Etapa 3: Ativar o novo certificado no IdP

Volte ao site do IdP e marque o novo certificado que você criou anteriormente como primário ou ativo. Nesse ponto, todas as mensagens SAML assinadas pelo IdP devem estar usando o novo certificado.

Etapa 4: Excluir o certificado antigo

Use o procedimento a seguir para concluir o processo de rodízio de certificados do seu IdP. Sempre deve haver pelo menos um certificado válido listado e ele não pode ser removido.

> **Note**
>
> Certifique-se de que seu provedor de identidades não esteja mais assinando respostas SAML com esse certificado antes de excluí-lo.

1. Na página Gerenciar certificados SAML 2.0, escolha o certificado que você quer excluir. Escolha Excluir.
2. Na caixa de diálogo Excluir certificado SAML 2.0, digite **DELETE** para confirmar e escolha Excluir.
3. Volte ao site do IdP e execute as etapas necessárias para remover o certificado inativo antigo.

Indicadores de status de expiração do certificado

Enquanto estiver na página Gerenciar certificados SAML 2.0, você poderá observar ícones indicadores de status coloridos. Esses ícones aparecem na coluna Expira em ao lado de cada certificado na lista. A seguir, descrevemos os critérios que o IAM Identity Center usa para determinar qual ícone é exibido para cada certificado.

- Vermelho – Indica que um certificado está expirado no momento.
- Amarelo: indica que um certificado expirará em 90 dias ou menos.
- Verde – Indica que um certificado está atualmente válido e permanecerá válido por pelo menos mais 90 dias.

Para verificar o status atual de um certificado

1. No console do IAM Identity Center, escolha Configurações.
2. Na página Configurações, escolha a guia Origem da identidade e escolha Ações > Gerenciar autenticação.
3. Na página Gerenciar autenticação SAML 2.0, em Gerenciar certificados SAML 2.0, revise o status dos certificados na lista, conforme indicado na coluna Expira em.

Usando o portal de AWS acesso

O portal de AWS acesso fornece a você (usuários finais) acesso de login único a todos os seus aplicativos de nuvem mais usados, como Office 365, Concur, Salesforce Contas da AWS e muitos outros. Você pode executar rapidamente vários aplicativos simplesmente escolhendo a conta da Conta da AWS ou o ícone do aplicativo no portal. A presença de ícones de aplicativos em seu portal de AWS acesso significa que um administrador da sua empresa concedeu a você acesso a esses Contas da AWS ou aplicativos. Isso também significa que você pode acessar todas essas contas ou aplicativos a partir do portal de AWS acesso sem solicitações adicionais de login.

Entre em contato com o administrador ou helpdesk para solicitar acesso adicional nas seguintes situações:

- Você não vê um aplicativo Conta da AWS ou que precisa acessar.
- O acesso que você tem a uma determinada conta ou aplicativo não é o que você esperava.

Tópicos

Aceitando o convite para ingressar no IAM Identity Center

Se esta é a primeira vez que você entra no portal de AWS acesso, verifique seu e-mail para obter instruções sobre como ativar suas credenciais de usuário.

Para habilitar suas credenciais de usuário

1. Dependendo do e-mail que você recebeu da sua empresa, escolha um dos métodos a seguir para ativar suas credenciais de usuário para que você possa começar a usar o portal de AWS acesso.

a. Se você recebeu um e-mail com o assunto Convite para ingressar no AWS IAM Identity Center (sucessor do AWS Single Sign-On), abra-o e escolha Aceitar convite. Na página de Registro de novo usuário, insira e confirme uma senha e escolha Definir nova senha. Você usará essa senha sempre que fizer login no portal.

b. Se você recebeu um e-mail do suporte de TI ou do administrador de TI da sua empresa, siga as instruções fornecidas para habilitar suas credenciais de usuário.

2. Depois de ativar suas credenciais de usuário fornecendo uma nova senha, o portal de AWS acesso conectará você automaticamente. Se isso não ocorrer, você poderá fazer login manualmente no portal de acesso da AWS , usando as instruções fornecidas na próxima etapa.

Entrando no portal de AWS acesso

Nesse momento, você deve ter recebido uma URL de login específica para o portal de AWS acesso por um administrador. Assim que você tiver esse URL, poderá prosseguir com as etapas a seguir para fazer login no portal. Para obter mais informações, consulte Entrar no portal de AWS acesso.

> **Note**
>
> Depois de entrar, a duração padrão da sua sessão do portal de AWS acesso é de 8 horas. Esteja ciente de que um administrador pode alterar a duração dessa sessão.

Dispositivos confiáveis

Quando você escolhe a opção Este é um dispositivo confiável na página de login, o IAM Identity Center considera todos os logins futuros desse dispositivo como autorizados. Isso significa que o IAM Identity Center não apresentará a opção de inserir um código de MFA enquanto você estiver usando esse dispositivo confiável. No entanto, há algumas exceções, inclusive fazer login em um novo navegador ou quando seu dispositivo recebe um endereço IP desconhecido.

Dicas de login para o portal de AWS acesso

Aqui estão algumas dicas para ajudá-lo a gerenciar sua experiência no portal de AWS acesso.

- Ocasionalmente, talvez você precise sair e entrar novamente no portal de AWS acesso. Isso pode ser necessário para acessar novos aplicativos que o administrador atribuiu recentemente a você.

No entanto, isso não é necessário, porque todos os novos aplicativos são atualizadas de hora em hora.

- Ao entrar no portal de AWS acesso, você pode abrir qualquer um dos aplicativos listados no portal escolhendo o ícone do aplicativo. Depois de terminar de usar o aplicativo, você pode fechar o aplicativo ou sair do portal de AWS acesso. Quando você fecha o aplicativo, sai somente desse aplicativo. Todos os outros aplicativos que você abriu no portal de AWS acesso permanecem abertos e em execução.
- Para fazer login como um usuário diferente, você deve primeiro sair do portal de acesso da AWS . Ao sair do portal, suas credenciais são removidas completamente da sessão do navegador.
- Depois de entrar no portal de AWS acesso, você pode alternar para uma função. Isso separa, temporariamente, as permissões originais de usuário e, em vez disso, oferece a você as permissões atribuídas à função. Para obter mais informações, consulte Alternar para uma função (console).

Sair do portal de AWS acesso

Quando você sai do portal, suas credenciais são removidas completamente da sessão do navegador. Para obter mais informações, consulte Sair do portal de AWS acesso no Início de Sessão da AWSguia.

Para sair do portal de AWS acesso

- No portal de AWS acesso, escolha Sair na barra de navegação.

> **Note**
>
> Se desejar fazer login como um usuário diferente, deverá primeiro sair do portal de acesso da AWS .

Redefinir a senha de usuário do IAM Identify Center

O portal de AWS acesso fornece aos usuários do IAM Identity Center acesso único a todas as AWS contas e aplicativos em nuvem atribuídos por meio de um portal da web. O portal de AWS acesso é diferente do AWS Management Console, que é uma coleção de consoles de serviço para gerenciar AWS recursos.

Use esse procedimento para redefinir sua senha de usuário do IAM Identity Center para o portal de AWS acesso. Saiba mais sobre User types no Início de Sessão da AWS User Guide.

Considerações

A funcionalidade de redefinição de senha para seu portal de AWS acesso está disponível somente para usuários de instâncias do Identity Center que estão usando o diretório do Identity Center ou AWS Managed Microsoft ADcomo sua fonte de identidade. Se seu usuário estiver conectado a um provedor de identidade externo ou ao AD Connector, as redefinições de senha do usuário deverão ser feitas a partir do provedor de identidade externo ou conectadoActive Directory.

- Se sua fonte de identidade for um diretório do IAM Identity Center, consulteRequisitos de senha ao gerenciar identidade no IAM Identity Center.
- Se sua fonte de identidade for uma AWS Managed Microsoft AD, consulte Requisitos de senha ao redefinir uma senha em AWS Managed Microsoft AD.

Para redefinir sua senha no portal de AWS acesso

1. Abra um navegador da web e vá até a página de login do seu portal de AWS acesso.

   Se você não tiver sua URL do portal de AWS acesso, verifique seu e-mail. Você deve ter recebido um convite por e-mail para participar AWS do IAM Identity Center, que inclui uma URL de login específica para o AWS portal de acesso. Como alternativa, seu administrador pode ter fornecido diretamente a você uma senha de uso único e a URL do portal de AWS acesso. Se você não conseguir localizar essas informações, peça ao administrador que as envie para você.

   Para obter mais informações sobre como entrar no portal de AWS acesso, consulte Entrar no portal de AWS acesso no Guia do Início de Sessão da AWS usuário.
2. Insira seu nome de usuário e escolha Avançar.
3. Em Senha, escolha Esqueci a senha.

   Forneça seu Nome de usuário e digite os caracteres da imagem fornecida para confirmar que você não é um robô. Em seguida, escolha Próximo. Talvez seja necessário desabilitar o software bloqueador de anúncios se não conseguir inserir caracteres.
4. Uma mensagem aparece para confirmar que um e-mail de redefinição de senha foi enviado. Escolha Continuar.
5. Você receberá um e-mail `no-reply@signin.aws` com o assunto Solicitação de redefinição de senha. Em seu e-mail, escolha Redefinir senha.

6. Na página Redefinir senha, verifique seu nome de usuário, especifique uma nova senha para o portal de AWS acesso e escolha Definir nova senha.
7. Você receberá um e-mail de `no-reply@signin.aws` com a linha de assunto Senha atualizada.

> **Note**
>
> Um administrador pode redefinir sua senha enviando um e-mail com instruções para redefini-la ou gerando uma senha única e compartilhando-a com você. Se você for administrador, consulte Redefinir a senha de usuário do IAM Identity Center para um usuário final.

Obter credenciais de usuário do IAM Identity Center para o AWS CLI ou AWS SDKs

Você pode acessar AWS os serviços programaticamente usando os AWS Command Line Interface kits de desenvolvimento de AWS software (SDKs) com credenciais de usuário do IAM Identity Center. Este tópico descreve como obter credenciais temporárias para um usuário no IAM Identity Center.

O portal de AWS acesso fornece aos usuários do IAM Identity Center acesso único a seus aplicativos Contas da AWS e à nuvem. Depois de entrar no portal de AWS acesso como usuário do IAM Identity Center, você pode obter credenciais temporárias. Em seguida, você pode usar as credenciais, também conhecidas como credenciais de usuário do IAM Identity Center, no AWS CLI ou AWS SDKs para acessar recursos em um. Conta da AWS

Se você estiver usando o AWS CLI para acessar AWS serviços de forma programática, você pode usar os procedimentos neste tópico para iniciar o acesso ao. AWS CLI Para obter informações sobre o AWS CLI, consulte o Guia AWS Command Line Interface do usuário.

Se você estiver usando os AWS SDKs para acessar AWS serviços de forma programática, seguir os procedimentos neste tópico também estabelecerá diretamente a autenticação dos SDKs. AWS Para obter informações sobre os AWS SDKs, consulte o Guia de referência de AWS SDKs e ferramentas.

> **Note**
>
> Os usuários do IAM Identity Center são diferentes dos usuários do IAM. Os usuários do IAM recebem credenciais de longo prazo para os AWS recursos. São concedidas credenciais

temporárias aos usuários no IAM Identity Center. Recomendamos que você use credenciais temporárias como uma prática recomendada de segurança para acessar suas, Contas da AWS pois essas credenciais são geradas toda vez que você faz login.

Pré-requisitos

Para obter credenciais temporárias para seu usuário do IAM Identity Center, você precisará do seguinte:

- Um usuário do IAM Identity Center — Você entrará no portal de acesso da AWS como esse usuário. Você ou seu administrador podem criar esse usuário. Para obter informações sobre como habilitar o IAM Identify Center e criar um usuário do IAM Identify Center, consulteIntrodução às tarefas comuns do IAM Identity Center.
- Acesso do usuário a um Conta da AWS — Para conceder a um usuário do IAM Identity Center permissão para recuperar suas credenciais temporárias, você ou um administrador deve atribuir ao usuário do IAM Identity Center um conjunto de permissões. Os conjuntos de permissões são armazenados no IAM Identity Center e definem o nível de acesso que um usuário do IAM Identity Center tem a um Conta da AWS. Se seu administrador criou o usuário do IAM Identity Center para você, peça que ele adicione esse acesso para você. Para ter mais informações, consulte Atribuir acesso de usuário a Contas da AWS.
- AWS CLI instalado — Para usar as credenciais temporárias, você deve instalar o. AWS CLI Para obter mais instruções, consulte Instalar ou atualizar a versão mais recente da AWS CLI no Guia do usuário do AWS CLI .

Considerações

Antes de concluir as etapas para obter credenciais temporárias para o usuário do IAM Identify Center, tenha em mente as seguintes considerações:

- O IAM Identity Center cria funções do IAM — Quando você atribui um usuário no IAM Identity Center a um conjunto de permissões, o IAM Identity Center cria uma função do IAM correspondente a partir do conjunto de permissões. Os papéis do IAM criados por conjuntos de permissões diferem dos papéis do IAM criados das seguintes maneiras: AWS Identity and Access Management
  - O IAM Identity Center possui e protege as funções criadas pelos conjuntos de permissões. Somente o IAM Identity Center pode modificar essas funções.

- Somente usuários no IAM Identity Center podem assumir as funções que correspondem aos conjuntos de permissões designados. Você não pode atribuir acesso ao conjunto de permissões a usuários do IAM, usuários federados do IAM ou contas de serviço.
- Você não pode modificar uma política de confiança de funções nessas funções para permitir acesso às entidades principais fora do IAM Identity Center.

Para obter informações sobre como obter credenciais temporárias para uma função que você cria no IAM, consulte Como usar credenciais de segurança temporárias com o AWS CLI no Guia do usuário AWS Identity and Access Management .

- Você pode definir a duração da sessão para os conjuntos de permissões — Depois de entrar no portal de AWS acesso, o conjunto de permissões ao qual seu usuário do IAM Identity Center está atribuído aparece como uma função disponível. O IAM Identity Center cria uma sessão separada para essa função. Essa sessão pode durar de uma a 12 horas, dependendo da duração da sessão configurada para o conjunto de permissões. Por padrão, a duração da sessão é de uma hora. Para ter mais informações, consulte Definir duração da sessão.

Obtendo e atualizando credenciais temporárias

Você pode obter e atualizar as credenciais temporárias do usuário do IAM Identity Center de forma automática ou manual.

Tópicos

- Atualização automática de credenciais (recomendada)
- Atualização manual de credenciais

Atualização automática de credenciais (recomendada)

A atualização automática de credenciais usa o padrão de autorização de código de dispositivo Open ID Connect (OIDC). Com esse método, você inicia o acesso diretamente usando o comando `aws configure sso` no AWS CLI. Você pode usar esse comando para acessar automaticamente qualquer função associada a qualquer conjunto de permissões ao qual você esteja atribuído para qualquer um Conta da AWS.

Para acessar a função criada para o usuário do IAM Identity Center, execute o `aws configure sso` comando e, em seguida, autorize o em uma janela AWS CLI do navegador. Desde que você tenha uma sessão ativa do portal de AWS acesso, o recupera AWS CLI automaticamente as credenciais temporárias e atualiza as credenciais automaticamente.

Para obter mais informações, consulte Configure your profile with the `aws configure sso wizard` no AWS Command Line Interface User Guide.

Para obter credenciais temporárias que são atualizadas automaticamente

1. Entre no portal de AWS acesso usando o URL de login específico fornecido pelo seu administrador. Se você criou o usuário do IAM Identity Center, AWS enviou um convite por e-mail que inclui sua URL de login. Para obter mais informações, consulte Entrar no portal de AWS acesso no Guia do usuário AWS de login.
2. Na guia Contas, localize a Conta da AWS partir da qual você deseja recuperar as credenciais. Quando você escolhe a conta, o nome da conta, o ID da conta e o endereço de e-mail associados à conta aparecem.

   > **Note**
   >
   > Se você não vê as Contas da AWS listadas, é provável que o usuário ainda não tenha sido designado a um conjunto de permissões para essa conta. Nesse caso, entre em contato com seu administrador e peça que ele adicione esse acesso para você. Para ter mais informações, consulte Atribuir acesso de usuário a Contas da AWS.

3. Abaixo do nome da conta, o conjunto de permissões ao qual seu usuário do IAM Identity Center foi designado aparece como uma função disponível. Por exemplo, se o usuário do IAM Identity Center for atribuído ao conjunto de PowerUserAccesspermissões da conta, a função aparecerá no portal de AWS acesso como PowerUserAccess.
4. Dependendo da sua opção ao lado do nome da função, escolha Teclas de acesso ou escolha Linha de comando ou acesso programático.
5. Na caixa de diálogo Obter credenciais, escolha macOS e Linux, Windows PowerShellou, dependendo do sistema operacional no qual você instalou o. AWS CLI
6. Em Credenciais AWS do IAM Identity Center (Recomendado), seu `SSO Start URL` e `SSO Region` são exibidos. Esses valores são exigidos para configurar um perfil compatível com o IAM Identity Center e `sso-session` para a sua AWS CLI Para concluir essa configuração, siga as instruções em Configurar seu perfil com o `aws configure sso wizard` no Guia do usuário AWS Command Line Interface .

Continue usando o AWS CLI conforme necessário Conta da AWS até que as credenciais tenham expirado.

Atualização manual de credenciais

Você pode usar o método de atualização manual de credenciais para obter credenciais temporárias para uma função associada a um conjunto de permissões específico em uma função específica. Conta da AWS Para fazer isso, você copia e cola os comandos necessários para as credenciais temporárias. Com esse método, você deve atualizar as credenciais temporárias manualmente.

Você pode executar AWS CLI comandos até que suas credenciais temporárias expirem.

Para obter credenciais que você atualiza manualmente

1. Entre no portal de AWS acesso usando o URL de login específico fornecido pelo seu administrador. Se você criou o usuário do IAM Identity Center, AWS enviou um convite por e-mail que inclui sua URL de login. Para obter mais informações, consulte Entrar no portal de AWS acesso no Guia do usuário AWS de login.
2. Na guia Contas, localize aquelas Conta da AWS das quais você deseja recuperar as credenciais de acesso e expanda-as para mostrar o nome da função do IAM (por exemplo, Administrador). Dependendo da sua opção ao lado do nome da função do IAM, escolha Teclas de acesso ou escolha Linha de comando ou acesso programático.

   > **Note**
   >
   > Se você não vê as Contas da AWS listadas, é provável que o usuário ainda não tenha sido designado a um conjunto de permissões para essa conta. Nesse caso, entre em contato com seu administrador e peça que ele adicione esse acesso para você. Para ter mais informações, consulte Atribuir acesso de usuário a Contas da AWS.

3. Na caixa de diálogo Obter credenciais, escolha macOS e Linux, Windows PowerShellou, dependendo do sistema operacional no qual você instalou o. AWS CLI
4. Escolha uma das seguintes opções:

   - Opção 1: definir variáveis de AWS ambiente

     Escolha essa opção para substituir todas as configurações de credenciais, incluindo todas as configurações nos `credentials` arquivos e `config` arquivos. Para obter mais informações, consulte Variáveis de ambiente para configurar no AWS CLI no Guia do usuário AWS CLI .

Para usar essa opção, copie os comandos na área de transferência, cole os comandos na janela do AWS CLI terminal e pressione Enter para definir as variáveis de ambiente necessárias.

- Opção 2: adicionar um perfil ao seu arquivo de AWS credenciais

  Escolha essa opção para executar comandos com diferentes conjuntos de credenciais.

  Para usar essa opção, copie os comandos na área de transferência e cole os comandos no AWS `credentials` arquivo compartilhado para configurar um novo perfil nomeado. Para obter mais informações, consulte Shared config and credentials files (“Arquivos compartilhados de configuração e de credenciais”) no Guia de referência de AWS SDKs e ferramentas. Para usar essa credencial, especifique a `--profile` opção em seu AWS CLI comando. Isso afeta todos os ambientes que usam o mesmo arquivo de credenciais.

- Opção 3: use valores individuais em seu cliente AWS de serviço

  Escolha essa opção para acessar AWS recursos de um cliente AWS de serviço. Para obter mais informações, consulte Ferramentas para desenvolver AWS.

  Para usar essa opção, copie os valores para sua área de transferência, cole os valores em seu código e atribua-os às variáveis apropriadas para seu SDK. Para obter mais informações, consulte a documentação específica para sua API do SDK.

Criação de links de atalho para destinos AWS Management Console

Os links de atalho criados no portal de AWS acesso levam os usuários do IAM Identity Center a um destino específico no AWS Management Console, com um conjunto de permissões específico e em um determinado Conta da AWS.

Links de atalho economizam tempo para você e seus colaboradores. Em vez de navegar até o URL de destino desejado AWS Management Console (por exemplo, uma página de instância de bucket do Amazon S3) em várias páginas, AWS incluindo o portal de acesso, você pode usar um link de atalho para chegar ao mesmo destino automaticamente.

Opções de destino do link de atalho

Os links de atalho têm três opções de destino, listadas aqui por prioridade:

- (Opcional) Qualquer URL de destino no AWS Management Console especificado no link de atalho. Por exemplo, a página de instância de bucket do Amazon S3.
- (Opcional) URL de estado de retransmissão configurada pelo administrador para o conjunto de permissões em questão. Para obter mais informações sobre como definir o estado do relé, consulteDefinir estado de retransmissão.
- AWS Management Console casa. O destino padrão se você não especificar um.

> **Note**
>
> A navegação automática até um destino só é bem-sucedida quando você está autenticado no IAM Identity Center e tem o conjunto de permissões necessário atribuído à AWS conta e ao URL de destino.

O portal de AWS acesso inclui um botão Criar atalho que ajuda você a criar um link de atalho compartilhável. Se você planeja especificar um URL de destino (a primeira opção na lista anterior), você pode copiar o URL em uma área de transferência para compartilhá-lo.

Crie um link de atalho no portal de AWS acesso

1. Enquanto estiver conectado ao portal de AWS acesso, escolha a guia Contas e, em seguida, escolha o botão Criar atalho.
2. Na caixa de diálogo:
   a. Escolha um Conta da AWS usando o ID da conta ou o nome da conta. Conforme você digita, um menu suspenso exibe IDs e nomes de contas correspondentes que você pode acessar. Você pode escolher somente uma conta à qual tenha acesso.
   b. Opcionalmente, escolha uma função do IAM na lista suspensa. Esses são os conjuntos de permissões atribuídos a você para a conta selecionada. Se você omitir a escolha da função, os usuários serão solicitados a selecionar uma atribuída a eles para a conta escolhida ao usar o link de atalho.

      > **Note**
      >
      > Você não pode conceder novos acessos com links de atalho. Os links de atalho funcionam somente com os conjuntos de permissões já atribuídos ao usuário. Se o

usuário não tiver os conjuntos de permissões necessários atribuídos à conta e ao URL de destino, o acesso será negado.

c. Opcionalmente, insira a URL de destino do portal de AWS acesso. Se você omitir a inserção de um URL, o destino será determinado automaticamente ao usar o link de atalho, com base nas opções de destino do link de atalho mencionadas anteriormente.

d. Seu link de atalho é gerado na parte inferior da caixa de diálogo, com base na sua entrada. Escolha o botão Copiar URL. Agora você pode criar um marcador com o link de atalho copiado ou compartilhá-lo com seus colaboradores que têm acesso à mesma conta com o mesmo conjunto de permissões ou outro conjunto de permissões suficiente.

Construindo links de AWS Management Console atalho seguros com codificação de URL

Todos os valores de parâmetros do URL, incluindo o ID da conta, o nome do conjunto de permissões e o URL de destino, devem ser codificados em URL.

Os links de atalho estendem a URL do portal de AWS acesso com o seguinte caminho:

```
/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

O URL completo na AWS partição clássica segue esse padrão:

```
https://[your_subdomain].awsapps.com/start/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

Aqui está um exemplo de link de atalho que conecta um usuário à conta `123456789012` com o conjunto de `S3FullAccess` permissões e o leva à página inicial do console S3:

- `https://example.awsapps.com/start/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) `https://start.us-gov-west-1.us-gov-home.awsapps.com/directory/example/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`

Registrando um dispositivo como MFA

Use o procedimento a seguir no portal de AWS acesso para registrar seu novo dispositivo para autenticação multifator (MFA).

> **Note**
>
> Recomendamos que você primeiro baixe a aplicação autenticadora apropriada em seu dispositivo antes de iniciar as etapas deste procedimento. Para obter uma lista de aplicativos que você pode usar para dispositivos com MFA, consulte Aplicativos de autenticação virtual.

Para registrar o dispositivo para usar com MFA

1. Entre no seu portal de AWS acesso. Para ter mais informações, consulte Entrando no portal de AWS acesso.
2. Próximo do canto superior direito da página, escolha MFA devices.
3. Na página Dispositivos Multi-Factor Authentication (MFA), escolha Registrar dispositivo.

   > **Note**
   >
   > Se a opção Registrar dispositivo com MFA estiver esmaecida, entre em contato com o administrador para obter ajuda com o registro do dispositivo.

4. Na página Registrar dispositivo com MFA, selecione um dos seguintes tipos de dispositivos de MFA e siga as instruções:

   - Aplicação autenticadora

     1. Na página Configurar o aplicativo autenticador, você pode observar informações de configuração para o novo dispositivo de MFA, inclusive um código QR gráfico. O gráfico é uma representação da chave secreta que está disponível para entrada manual em dispositivos que não suportam códigos QR.
     2. Usando o dispositivo MFA físico, faça o seguinte:

        a. Abra uma aplicação autenticadora com MFA compatível. Para obter uma lista de aplicativos testados que você pode usar com dispositivos com MFA, consulte Aplicativos de autenticação virtual. Se o aplicativo de MFA virtual oferecer suporte a várias contas

(vários dispositivos MFA virtuais), selecione a opção para criar uma nova conta (um novo dispositivo MFA virtual).

b. Determine se o aplicativo MFA suporta códigos QR e, em seguida, execute uma das seguintes ações na página Set up the authenticator app:

i. No assistente, escolha Show QR code e, em seguida, use o app para digitalizar o código de QR. Por exemplo, você pode escolher o ícone da câmera ou escolher uma opção semelhante a Scan code. Em seguida, use a câmera do dispositivo para digitalizar o código.

ii. Escolha mostrar chave secreta e, em seguida, insira essa chave secreta em seu aplicativo de MFA.

> **Important**
>
> Quando você configura um dispositivo MFA virtual para funcionar com o IAM Identity Center, recomendamos salvar uma cópia do código de QR ou da chave secreta em um local seguro. Isso pode ajudar se você perder o telefone ou precisar reinstalar a aplicação autenticadora com MFA. Se alguma dessas coisas acontecer, você poderá reconfigurar rapidamente o aplicativo para usar a mesma configuração de MFA.

3. Na página Configurar o aplicativo autenticador, em Código do autenticador, insira a senha de uso único que atualmente é exibida no dispositivo MFA físico.

> **Important**
>
> Envie sua solicitação imediatamente após gerar o código. Se você gerar os códigos e esperar muito tempo para enviar a solicitação, o dispositivo MFA se associa com êxito ao seu usuário, mas o dispositivo MFA está fora de sincronia. Isso ocorre porque as senhas únicas baseadas em tempo (time-based one-time passwords, TOTP) expiram após um curto período. Caso isso ocorra, você pode ressincronizar o dispositivo.

4. Escolha Assign MFA. O dispositivo de MFA agora pode começar a gerar senhas de uso único e agora está pronto para uso com. AWS

- Chave de segurança ou autenticador integrado

1. Na página Registrar a chave de segurança do usuário, siga as instruções fornecidas pelo seu navegador ou plataforma.

> **Note**
>
> A experiência varia de acordo com o navegador ou a plataforma. Depois que seu dispositivo for registrado com sucesso, você poderá associar um nome de exibição amigável ao seu dispositivo recém-cadastrado. Para alterar o nome, escolha Renomear, insira o novo nome e escolha Salvar.

Personalizando a URL do portal de AWS acesso

Por padrão, você pode acessar o portal de AWS acesso usando uma URL que segue este formato:`d-xxxxxxxxxx.awsapps.com/start`. É possível personalizar o plugin conforme a seguir: `your_subdomain.awsapps.com/start`.

> **Important**
>
> Se você alterar a URL do portal de AWS acesso, não poderá editá-la posteriormente.

Para personalizar seu URL

1. Abra o AWS IAM Identity Center console em https://console.aws.amazon.com/singlesignon/.
2. No console do IAM Identity Center, escolha Painel no painel de navegação e localize a seção Resumo das configurações.
3. Escolha o botão Personalizar abaixo da URL do seu portal de AWS acesso.

> **Note**
>
> Se o botão Personalizar não for exibido, significa que o portal de AWS acesso já foi personalizado. A personalização da URL do portal de AWS acesso é uma operação única que não pode ser revertida.

4. Insira o nome do subdomínio desejado e escolha Salvar.

Agora você pode entrar no AWS Console por meio do seu portal de AWS acesso com sua URL personalizada.

Autenticação multifator para usuários do Identity Center

A autenticação multifator (MFA) fornece uma maneira simples e segura de adicionar uma camada extra de proteção ao mecanismo de autenticação padrão do nome de usuário e senha.

Quando os administradores habilitam o MFA, os usuários devem entrar no portal de acesso AWS com dois fatores:

- Nome de usuário e Senha. Esse é o primeiro fator e é algo que os usuários conhecem.
- Um código, chave de segurança ou biometria. Esse é o segundo fator e é algo que os usuários têm (posse) ou são (biométrico). O segundo fator pode ser um código de autenticação gerado a partir do dispositivo móvel, uma chave de segurança conectada ao computador ou a verificação biométrica do usuário.

Juntos, esses vários fatores fornecem maior segurança ao impedir o acesso não autorizado aos seus atributos AWS, a menos que um desafio válido de MFA tenha sido concluído com sucesso.

Cada usuário pode registrar até dois aplicativos autenticadores virtuais, que são aplicativos autenticadores de senha únicos instalados em seu dispositivo móvel ou tablet, e seis autenticadores FIDO, que incluem autenticadores e chaves de segurança integrados, totalizando oito dispositivos de MFA. Saiba mais sobre Tipos de MFA disponíveis para o IAM Identity Center.

> **Important**
>
> Como prática recomendada de segurança, recomendamos habilitar a MFA.

Tópicos

Tipos de MFA disponíveis para o IAM Identity Center

A autenticação multifator (MFA) é um mecanismo simples e eficaz para aumentar sua segurança. O primeiro fator, sua senha, é um segredo que você memoriza, também conhecido como fator de conhecimento. Outros fatores podem ser fatores de posse (algo que você tem, como uma chave de segurança) ou fatores de inerência (algo que você é, como um escaneamento biométrico). É altamente recomendável configurar a MFA para adicionar uma camada adicional de segurança à sua conta.

O IAM Identity Center MFA é compatível com os seguintes tipos de dispositivos. Todos os tipos de MFA são compatíveis tanto para o acesso ao console baseado em navegador quanto para o uso da AWS CLI v2 com o IAM Identity Center.

- Autenticadores FIDO2, incluindo autenticadores e chaves de segurança integrados
- Aplicativos de autenticação virtual
- A implementação de sua própria RADIUS MFA conectada por meio de AWS Managed Microsoft AD

Um usuário pode ter até oito dispositivos de MFA, que incluem até dois aplicativos autenticadores virtuais e seis autenticadores FIDO, registrados em uma conta. Você também pode definir as configurações de habilitação de MFA para exigir MFA sempre que seus usuários fizerem login ou para habilitar dispositivos confiáveis que não exigem MFA a cada login. Para obter mais informações sobre como configurar seu servidor RADIUS para funcionar com Escolha os tipos de MFA e MFA, consulte Configurar a imposição de dispositivos de MFA.

Autenticadores FIDO2

O FIDO2 é um padrão que inclui CTAP2 e WebAuthn, além de ser baseado na criptografia de chave pública. As credenciais FIDO são resistentes ao phishing porque são exclusivas do site em que as credenciais foram criadas, como a AWS.

A AWS suporta os dois formatos mais comuns dos autenticadores FIDO: autenticadores integrados e chaves de segurança. Veja abaixo mais informações sobre os tipos mais comuns de autenticadores FIDO.

Tópicos

- Autenticadores integrados

- Chaves de segurança
- Gerenciadores de senhas, fornecedores de chaves de acesso e outros autenticadores FIDO

Autenticadores integrados

Alguns dispositivos têm autenticadores integrados, como o TouchID no MacBook ou uma câmera compatível com o Windows Hello. Se seu dispositivo tiver um autenticador integrado compatível com FIDO, você poderá usar sua impressão digital, rosto ou pin do dispositivo como um segundo fator.

Chaves de segurança

As chaves de segurança são autenticadores de hardware externos compatíveis com FIDO que você pode comprar e conectar ao seu dispositivo via USB, BLE ou NFC. Quando você é solicitado a inserir o MFA, basta concluir um gesto com o sensor da chave. Alguns exemplos de chaves de segurança incluem chaves YubiKeys e Feitian, e as chaves de segurança mais comuns criam credenciais FIDO vinculadas ao dispositivo. Para obter uma lista de todas as chaves de segurança certificadas pela FIDO, consulte FIDO Certified Products.

Gerenciadores de senhas, fornecedores de chaves de acesso e outros autenticadores FIDO

Vários provedores terceirizados oferecem suporte à autenticação FIDO em aplicativos móveis, como atributos em gerenciadores de senhas, cartões inteligentes com modo FIDO, entre outros formatos. Esses dispositivos compatíveis com FIDO podem funcionar com o IAM Identity Center, mas recomendamos que você mesmo teste um autenticador FIDO antes de ativar essa opção para MFA.

> **Note**
>
> Alguns autenticadores FIDO podem criar credenciais FIDO detectáveis, conhecidas como chaves de acesso. As chaves de acesso podem estar vinculadas ao dispositivo que as criou, ou podem ser sincronizadas e armazenadas em uma nuvem. Por exemplo, você pode registrar uma chave de acesso usando o Apple Touch ID em um Macbook compatível e, em seguida, fazer login em um site a partir de um laptop Windows usando o Google Chrome com sua chave de acesso no iCloud, seguindo as instruções na tela ao fazer login. Para obter mais informações sobre quais dispositivos suportam chaves de acesso sincronizáveis e a interoperabilidade atual de chaves de acesso entre sistemas operacionais e navegadores, consulte Device Support em passkeys.dev, um recurso mantido pela FIDO Alliance And World Wide Web Consortium (W3C).

Aplicativos de autenticação virtual

Os aplicativos autenticadores são autenticadores terceirizados baseados em senha de uso único (OTP). Você pode usar um aplicativo autenticador instalado em seu dispositivo móvel ou tablet como um dispositivo de MFA autorizado. O aplicativo autenticador de terceiros deve estar em conformidade com RFC 6238, que é um algoritmo de senha de uso único com marcação temporal (TOTP) padrão capaz de gerar códigos de autenticação de seis dígitos.

Quando a MFA for solicitada, você deve inserir um código válido do seu aplicativo autenticador na caixa de entrada apresentada. Cada dispositivo MFA atribuído a um usuário deve ser exclusivo. Dois aplicativos autenticadores podem ser registrados para qualquer usuário.

Aplicativo autenticador testado

Qualquer aplicativo compatível com TOTP funcionará com o IAM Identity Center MFA. Você pode escolher entre os seguintes aplicativos autenticadores de terceiros conhecidos.

Sistema operacional	Aplicativo autenticador testado
Android	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

RADIUS MFA

O Remote Authentication Dial-In User Service (RADIUS) é um protocolo cliente-servidor padrão da indústria que fornece autenticação, autorização e gestão de contabilidade para que os utilizadores possam ligar-se a serviços de rede. AWS Directory Service inclui um cliente RADIUS que liga ao servidor RADIUS no qual implementou a sua solução MFA. Para obter mais informações, consulte Enable Multi-Factor Authentication for AWS Managed Microsoft AD.

Você pode usar o RADIUS MFA ou o MFA no IAM Identity Center para fazer login do usuário no portal do usuário, mas não ambos. O MFA no IAM Identity Center é uma alternativa ao RADIUS MFA nos casos em que você deseja a autenticação nativa AWS de dois fatores para acessar o portal.

Quando você ativa a MFA no IAM Identity Center, seus usuários precisam de um dispositivo de MFA para entrar no portal de acesso AWS. Se você já usou o RADIUS MFA, habilitar o MFA no IAM

Identity Center substitui efetivamente o RADIUS MFA para usuários que fazem login no portal de acesso AWS. No entanto, o RADIUS MFA continua desafiando os usuários quando eles se conectam a todos os outros aplicativos AWS Directory Service com os quais funcionam, como o Amazon WorkDocs.

Se seu MFA estiver desativado no console do IAM Identity Center e você tiver configurado o RADIUS MFA comAWS Directory Service, o RADIUS MFA controla AWS o login no portal de acesso. Isso significa que o IAM Identity Center retornará à configuração RADIUS MFA se o MFA estiver desativado.

Configure o MFA

Os tópicos a seguir fornecem instruções para configurar dispositivos de MFA no IAM Identity Center.

Tópicos

Considerações antes de habilitar a MFA no IAM Identity Center

Antes de configurar a MFA, considere o seguinte:

- Os usuários são incentivados a registrar vários autenticadores de backup para todos os tipos de MFA habilitados. Essa prática pode evitar a perda de acesso no caso de um dispositivo de MFA quebrado ou extraviado.
- Não escolha a opção Require Them to Provide a One-Time Password Sent by Email se seus usuários precisarem entrar no portal de AWS acesso para acessar seus e-mails. Por exemplo, seus usuários podem usar Microsoft 365 no portal de AWS acesso para ler seus e-mails. Nesse caso, os usuários não conseguirão recuperar o código de verificação e não conseguirão entrar no portal de AWS acesso. Para obter mais informações, consulte Configurar a imposição de dispositivos de MFA.
- Se você já estiver usando o RADIUS MFA AWS Directory Service com o qual você configurou, não precisa habilitar o MFA no IAM Identity Center. O MFA no IAM Identity Center é uma alternativa

ao RADIUS MFA Microsoft Active Directory para usuários do IAM Identity Center. Para obter mais informações, consulte RADIUS MFA.

- Você pode usar os recursos de MFA no IAM Identity Center quando sua fonte de identidade está configurada com o repositório de identidades do IAM Identity Center, AWS Managed Microsoft AD ou o AD Connector. Atualmente, o MFA no IAM Identity Center não é compatível com provedores de identidade externos.

Habilitar MFA o IAM Identity Center

Você pode habilitar o acesso seguro ao portal de acesso AWS, aos aplicativos integrados do IAM Identity Center e AWS CLI ao habilitar a autenticação multifator (MFA).

Tópicos

- Solicite aos usuários o MFA
- Desativar MFA para o diretório do IAM Identity Center

Solicite aos usuários o MFA

Use as etapas a seguir para habilitar a MFA no console do IAM Identity Center. Antes de começar, recomendamos que você entenda o Tipos de MFA disponíveis para o IAM Identity Center.

> **Note**
>
> Se você estiver usando um IdP externo, a seção Autenticação multifatorial não estará disponível. Seu IdP externo gerencia as configurações de MFA, em vez de gerenciá-las pelo IAM Identity Center.

Para habilitar a MFA

1. Abra o console do IAM Identity Center.
2. No painel de navegação à esquerda, escolha Settings.
3. Na página Configurações, escolha a guia Autenticação.
4. Na seção Autenticação multifator, escolha Configure.
5. Na página Configurar autenticação multifator, em Solicitar aos usuários o MFA, escolha um dos seguintes modos de autenticação com base no nível de segurança que sua empresa precisa:

- Somente quando o contexto de login muda (sensível ao contexto)

  Nesse modo (o padrão), o IAM Identity Center oferece aos usuários a opção de confiar em seus dispositivos durante o login. Depois que um usuário indica que deseja confiar em um dispositivo, o IAM Identity Center solicita ao usuário a MFA uma vez e analisa o contexto de login (como dispositivo, navegador e localização) para os logins subsequentes do usuário. Para logins subsequentes, o IAM Identity Center determina se o usuário está fazendo login com um contexto anteriormente confiável. Se o contexto de login do usuário mudar, o IAM Identity Center solicitará ao usuário o MFA, além de suas credenciais de endereço de e-mail e senha.

  Esse modo oferece facilidade de uso para usuários que fazem login com frequência no local de trabalho, para que não precisem concluir o MFA a cada login. Eles só receberão uma solicitação de MFA se o contexto de login mudar.

- Toda vez que eles fazem login (sempre ativo)

  Nesse modo, o IAM Identity Center exige que os usuários com um dispositivo de MFA registrado sejam avisados sempre que fizerem login. Você deve usar esse modo se tiver políticas organizacionais ou de conformidade que exijam que seus usuários concluam o MFA sempre que entrarem no portal de acesso AWS. Por exemplo, o PCI DSS recomenda fortemente o MFA durante cada login para acessar aplicativos que oferecem suporte a transações de pagamento de alto risco.

- Nunca (desativado)

  Nesse modo, todos os usuários entrarão somente com seu nome de usuário e senha padrão. A escolha dessa opção desativa o IAM Identity Center MFA.

  > **Note**
  >
  > Se você já estiver usando o RADIUS MFA AWS Directory Service com e quiser continuar a usá-lo como seu tipo de MFA padrão, poderá deixar o modo de autenticação como desativado para ignorar os recursos de MFA no IAM Identity Center. A mudança do modo Desativado para o modo sensível ao contexto ou Sempre ativo substituirá as configurações existentes do RADIUS MFA. Para obter mais informações, consulte RADIUS MFA.

6. Escolha Save changes.

Related Topics

- Escolha os tipos de MFA
- Configurar a imposição de dispositivos de MFA
- Permita que os usuários registrem seus próprios dispositivos de MFA

Desativar MFA para o diretório do IAM Identity Center

Quando você desativa a autenticação multifator (MFA) para seu diretório do IAM Identity Center, ela permite que os usuários façam login somente com seu nome de usuário e senha padrão. Embora a MFA esteja desativada em seu diretório do Identity Center para usuários, você não pode gerenciar dispositivos de MFA em seus detalhes de usuário, e os usuários do diretório do Identity Center não podem gerenciar dispositivos de MFA a partir do portal de acesso AWS.

Desativar MFA para o diretório do IAM Identity Center

> **Important**
>
> s instruções da presente secção aplicam-se a AWS IAM Identity Center. Elas não se aplicam ao AWS Identity and Access Management (IAM). Os usuários, grupos e credenciais de usuário do IAM Identity Center são diferentes dos usuários, grupos e credenciais de usuário do IAM. Se você estiver procurando instruções sobre como desativar a MFA para usuários do IAM, consulte Deactivating MFA devices no User GuideAWS Identity and Access Management.

1. Abra o console do IAM Identity Center.
2. No painel de navegação à esquerda, escolha Settings.
3. Na página Configurações, escolha a guia Autenticação.
4. Na seção Multi-factor authentication, escolha Configure.
5. Na página Configure multi-factor authentication, na seção Solicitar MFA aos usuários, escolhao botão de opção rádioNever (disabled).
6. Escolha Save changes.

Escolha os tipos de MFA

Use o procedimento a seguir para escolher os tipos de dispositivos com os quais seus usuários podem se autenticar quando solicitados a fornecer MFA no portal de acesso AWS.

Para configurar os tipos de MFA para seus usuários

1. Abra o console do IAM Identity Center.
2. No painel de navegação à esquerda, escolha Settings.
3. Na página Configurações, escolha a guia Autenticação.
4. Na seção Multi-factor authentication, escolha Configure.
5. Na página Configure multi-factor authentication, em Users can authenticate with these MFA types, escolha um dos seguintes tipos de MFA com base nas necessidades de sua empresa. Para obter mais informações, consulte Tipos de MFA disponíveis para o IAM Identity Center.
   - Autenticadores FIDO2, incluindo autenticadores e chaves de segurança integrados
   - Aplicativos de autenticação virtual
6. Escolha Save changes.

Configurar a imposição de dispositivos de MFA

Use o procedimento a seguir para determinar se seus usuários devem ter um dispositivo de MFA registrado ao entrar no portal de acesso AWS.

Para configurar a imposição de dispositivos de MFA para seus usuários

1. Abra o console do IAM Identity Center.
2. No painel de navegação à esquerda, escolha Settings.
3. Na página Configurações, escolha a guia Autenticação.
4. Na seção Multi-factor authentication, escolha Configure.
5. Na página Configure multi-factor authentication, em If a user does not yet have a registered MFA device, escolha uma das seguintes opções com base nas necessidades de sua empresa:
   - Exija que eles registrem um dispositivo de MFA no login

     Essa é a configuração padrão quando você configura o MFA pela primeira vez para o IAM Identity Center. Use essa opção quando quiser exigir que os usuários que ainda não têm

um dispositivo de MFA registrado inscrevam automaticamente um dispositivo durante o login após uma autenticação de senha bem-sucedida. Isso permite que você proteja os ambientes AWS da sua organização com MFA sem precisar inscrever e distribuir dispositivos de autenticação individualmente para seus usuários. Durante a autoinscrição, seus usuários podem registrar qualquer dispositivo a partir dos Tipos de MFA disponíveis para o IAM Identity Center disponíveis que você ativou anteriormente. Depois de concluir o registro, os usuários têm a opção de dar um nome amigável ao dispositivo de MFA recém-inscrito, após o qual o IAM Identity Center redireciona o usuário para o destino original. Se o dispositivo do usuário for perdido ou roubado, você pode simplesmente remover esse dispositivo da conta, e o IAM Identity Center exigirá que ele inscreva automaticamente um novo dispositivo durante o próximo login.

- Exija que eles forneçam uma senha única enviada por e-mail para fazer login

  Use essa opção quando quiser que os códigos de verificação sejam enviados aos usuários por e-mail. Como o e-mail não está vinculado a um dispositivo específico, essa opção não atende aos padrões da autenticação multifator padrão do setor. Mas isso melhora a segurança do que ter apenas uma senha. A verificação por e-mail só será solicitada se o usuário não tiver registrado um dispositivo de MFA. Se o método de autenticação Context-aware tiver sido ativado, o usuário terá a oportunidade de marcar o dispositivo no qual recebeu o e-mail como confiável. Posteriormente, eles não precisarão verificar um código de e-mail em futuros logins a partir dessa combinação de dispositivo, navegador e endereço IP.

  > **Note**
  >
  > Se você estiver usando o Active Directory como sua fonte de identidade habilitada para o IAM Identity Center, o endereço de e-mail sempre será baseado no `email` atributo do Active Directory. Os mapeamentos personalizados de atributos do Active Directory não substituirão esse comportamento.

- Block their sign-in

  Use a opção Block Their Sign-In quando quiser impor o uso de MFA por todos os usuários antes que eles possam fazer login em AWS.

  > **Important**
  >
  > Se seu método de autenticação estiver definido como Context-aware, um usuário poderá marcar a caixa de seleção Este é um dispositivo confiável na página de login.

Nesse caso, esse usuário não receberá uma solicitação de MFA, mesmo que você tenha a configuração Block their sign in ativada. Se você quiser que esses usuários sejam avisados, altere seu método de autenticação para Always On.

- Permita que eles façam login

  Use essa opção para indicar que os dispositivos de MFA não são necessários para que seus usuários entrem no portal de acesso AWS. Os usuários que optarem por registrar dispositivos de MFA ainda receberão uma solicitação de MFA.

6. Escolha Save changes.

Permita que os usuários registrem seus próprios dispositivos de MFA

Use o procedimento a seguir para permitir que seus usuários registrem automaticamente seus próprios dispositivos de MFA.

Permita que os usuários registrem seus próprios dispositivos de MFA

1. Abra o console do IAM Identity Center.
2. No painel de navegação à esquerda, escolha Settings.
3. Na página Configurações, escolha a guia Autenticação.
4. Na seção Multi-factor authentication, escolha Configure.
5. Na página Configure multi-factor authentication, em Who can manage MFA devices, escolha Users can add and manage their own MFA devices.
6. Escolha Save changes.

> **Note**
>
> Depois de configurar o autorregistro para seus usuários, talvez você queira enviar a eles um link para o procedimento Registrando um dispositivo como MFA. Este tópico fornece instruções sobre como configurar os próprios dispositivos MFA.

Gerencie dispositivos MFA no IAM Identity Center

Os tópicos a seguir fornecem instruções para configurar dispositivos de MFA no IAM Identity Center.

Tópicos

Registrar um dispositivo de MFA

Use o procedimento a seguir para configurar um novo dispositivo de MFA para acesso por um usuário específico no console do IAM Identity Center. Você deve ter acesso físico ao dispositivo MFA do usuário para registrá-lo. Por exemplo, se você configurar a MFA para um usuário que usará um dispositivo MFA executado em um smartphone, você precisará de acesso físico ao smartphone para concluir o processo de registro. Ou então, você pode permitir que os usuários configurem e gerenciem os próprios dispositivos MFA. Para obter mais informações, consulte Permita que os usuários registrem seus próprios dispositivos de MFA.

Registrar um dispositivo de MFA

1. Abra o console do IAM Identity Center.
2. No painel de navegação à esquerda, escolha Users. Na lista, escolha um usuário. Não marque a caixa de seleção ao lado do usuário para essa etapa.
3. Na página de detalhes do usuário, escolha a guia MFA devices e, em seguida, escolha Register MFA device.
4. Na página Registrar dispositivo com MFA, selecione um dos seguintes tipos de dispositivos de MFA e siga as instruções:

    - Authenticator app

        1. Na página Set up the authenticator app, o IAM Identity Center exibe informações de configuração para o novo dispositivo MFA, incluindo um código QR gráfico. O gráfico é uma representação da chave de configuração secreta que está disponível para entrada manual em dispositivos que não suportam códigos de QR.
        2. Usando o dispositivo MFA físico, faça o seguinte:

            a. Abra uma aplicação autenticadora com MFA compatível. Para obter uma lista de aplicativos testados que você pode usar com dispositivos com MFA, consulte Aplicativos de autenticação virtual. Se o aplicativo de MFA virtual oferecer suporte a várias contas (vários dispositivos MFA virtuais), selecione a opção para criar uma nova conta (um novo dispositivo MFA virtual).

b. Determine se o aplicativo MFA suporta códigos QR e, em seguida, execute uma das seguintes ações na página Set up the authenticator app:

   i. No assistente, escolha Show QR code e, em seguida, use o app para digitalizar o código de QR. Por exemplo, você pode escolher o ícone da câmera ou escolher uma opção semelhante a Scan code. Em seguida, use a câmera do dispositivo para digitalizar o código.

   ii. Escolha Show secret key e digite a chave secreta em sua aplicação de MFA.

> **Important**
>
> Ao configurar um dispositivo MFA para o IAM Identity Center, recomendamos que você salve uma cópia do código QR ou da chave secreta em um local seguro. Isso pode ajudar se o usuário designado perder o telefone ou precisar reinstalar o aplicativo autenticador de MFA. Se alguma dessas coisas acontecer, você poderá reconfigurar rapidamente o aplicativo para usar a mesma configuração de MFA. Isso evita a necessidade de criar um novo dispositivo MFA virtual no IAM Identity Center para o usuário.

3. Na página Set up the authenticator app, em Authenticator code, digite a senha única que atualmente é exibida no dispositivo MFA físico.

> **Important**
>
> Envie sua solicitação imediatamente após gerar o código. Se você gerar os códigos e esperar muito tempo para enviar a solicitação, o dispositivo MFA conseguirá se associar ao usuário. No entanto, o dispositivo MFA estará fora de sincronia. Isso ocorre porque as senhas únicas baseadas em tempo (TOTP) expiram após um curto período. Caso isso ocorra, você pode ressincronizar o dispositivo.

4. Escolha Assign MFA. O dispositivo MFA agora pode começar a gerar senhas únicas e agora está pronto para uso com AWS.

- Chave de segurança

1. Na página Register your user's security key, siga as instruções fornecidas pelo seu navegador ou plataforma.

> **Note**
>
> A experiência aqui varia de acordo com os diferentes sistemas operacionais e navegadores, portanto, siga as instruções exibidas pelo seu navegador ou plataforma. Depois que o dispositivo do usuário for registrado com sucesso, você terá a opção de associar um nome de exibição amigável ao dispositivo recém-inscrito do usuário. Se você quiser alterar isso, escolha Rename, insira o novo nome e escolha Save. Se você tiver habilitado a opção de permitir que os usuários gerenciem seus próprios dispositivos, o usuário verá esse nome amigável no portal de acesso AWS.

Gerenciar o dispositivo de MFA de um usuário

Use os procedimentos a seguir quando precisar renomear ou excluir o dispositivo de MFA de um usuário.

Como renomear seu dispositivo de MFA

1. Abra o console do IAM Identity Center.
2. No painel de navegação à esquerda, escolha Users. Escolha o nome de usuário na lista. Não marque a caixa de seleção ao lado do usuário para essa etapa.
3. Na página de detalhes do usuário, escolha a guia MFA devices, selecione o dispositivo e escolha Rename.
4. Quando solicitado, insira o novo nome e escolha Rename.

Como excluir um dispositivo de MFA

1. Abra o console do IAM Identity Center.
2. No painel de navegação à esquerda, escolha Users. Escolha o nome de usuário na lista.
3. Na página de detalhes do usuário, escolha a guia MFA devices, selecione o dispositivo e escolha Delete.
4. Selecione DELETE e depois escolha Delete para confirmar.

Gerencie o acesso ao Contas da AWS

AWS IAM Identity Center é integrado com AWS Organizations, o que permite gerenciar centralmente as permissões em várias Contas da AWS sem configurar cada uma de suas contas manualmente. Você pode definir permissões e atribuir essas permissões aos usuários da força de trabalho para controlar seu acesso a informações específicas Contas da AWS.

Conta da AWS tipos

Existem dois tipos de Contas da AWS tinta AWS Organizations:

- Conta de gerenciamento - A Conta da AWS que é usada para criar a organização.
- Contas de membros - O restante pertence Contas da AWS a uma organização.

Para obter mais informações sobre Conta da AWS tipos, consulte AWS Organizations Terminologia e conceitos no Guia do AWS Organizations usuário.

Você também pode optar por registrar uma conta de membro como administrador delegado do IAM Identity Center. Os usuários dessa conta podem realizar a maioria das tarefas administrativas do IAM Identity Center. Para ter mais informações, consulte Administradores delegados.

Para cada tarefa e tipo de conta, a tabela a seguir indica se a tarefa administrativa do IAM Identity Center pode ser executada pelos usuários na conta.

Tarefas administrativas do IAM Identity Center	Conta-membro	Conta de administrador delegado	Conta de gerenciamento
Leia usuários ou grupos (lendo o próprio grupo e os membros do grupo)	 Yes (Sim)	 Yes (Sim)	 Yes (Sim)

Tarefas administrativas do IAM Identity Center	Conta-membro	Conta de administrador delegado	Conta de gerenciamento
Adicionar, editar ou excluir usuários ou grupos	 No (Não)	 Yes (Sim)	 Yes (Sim)
Habilite ou desative o acesso do usuário	 No (Não)	 Yes (Sim)	 Yes (Sim)
Ative, desative ou gerencie os atributos de entrada	 No (Não)	 Yes (Sim)	 Yes (Sim)
Altere ou gerencie fontes de identidade	 No (Não)	 Yes (Sim)	 Yes (Sim)
Crie, edite ou exclua aplicativos	 No (Não)	 Yes (Sim)	 Yes (Sim)
Configure o MFA	 No (Não)	 Yes (Sim)	 Yes (Sim)

Tarefas administrativas do IAM Identity Center	Conta-membro	Conta de administrador delegado	Conta de gerenciamento
Gerencie conjuntos de permissões não provisionados na conta de gerenciamento	 No (Não)	 Yes (Sim)	 Yes (Sim)
Gerencie conjuntos de permissões provisionados na conta de gerenciamento	 Não	 No (Não)	 Yes (Sim)
Habilitar o IAM Identity Center	 Não	 No (Não)	 Yes (Sim)
Exclua a configuração do IAM Identify Center	 Não	 No (Não)	 Yes (Sim)
Ative ou desative o acesso do usuário na conta de gerenciamento	 Não	 No (Não)	 Yes (Sim)
Registre ou cancele o registro de uma conta-membro como administrador delegado	 Não	 No (Não)	 Yes (Sim)

Atribuindo acesso Conta da AWS

Você pode usar conjuntos de permissões para simplificar a forma como você atribui acesso aos usuários e grupos da sua organização às Contas da AWS. Os conjuntos de permissões são armazenadas no IAM Identity Center e definem o nível de acesso que os usuários e grupos têm a uma conta da Conta da AWS. Você pode criar um único conjunto de permissões e atribuí-lo a vários Contas da AWS dentro da sua organização. Você também pode atribuir vários conjuntos de permissões ao mesmo usuário.

Para obter mais informações sobre esses conjuntos de permissões, consulte Criar, gerenciar e excluir conjuntos de permissões.

> **Note**
>
> Você também pode atribuir aos usuários acesso de logon único aos aplicativos. Para mais informações, consulte Gerenciar o acesso a aplicações.

Experiência do usuário final

O portal de AWS acesso fornece aos usuários do IAM Identity Center acesso único a todos os seus aplicativos Contas da AWS e atribuídos por meio de um portal da web. O portal de AWS acesso é diferente do AWS Management Console, que é uma coleção de consoles de serviço para gerenciar AWS recursos.

Quando você cria um conjunto de permissões, o nome que você especifica para o conjunto de permissões aparece no portal de AWS acesso como uma função disponível. Os usuários entram no portal de AWS acesso, escolhem um e Conta da AWS, em seguida, escolhem a função. Depois de escolherem a função, eles podem acessar AWS os serviços usando AWS Management Console ou recuperar as credenciais temporárias para acessar os AWS serviços de forma programática.

Para abrir AWS Management Console ou recuperar as credenciais temporárias para acesso AWS programático, os usuários concluem as seguintes etapas:

1. Os usuários abrem uma janela do navegador e usam a URL de login fornecida por você para navegar até o portal de AWS acesso.
2. Usando suas credenciais de diretório, eles entram no portal de AWS acesso.

3. Após a autenticação, na página do portal de AWS acesso, eles escolhem a guia Contas para exibir a lista Contas da AWS à qual têm acesso.
4. Em seguida, os usuários escolhem o Conta da AWS que desejam usar.
5. Abaixo do nome do Conta da AWS, todos os conjuntos de permissões aos quais os usuários estão atribuídos aparecem como funções disponíveis. Por exemplo, se você atribuiu um usuário `john_stiles` ao conjunto de `PowerUser` permissões, a função será exibida no portal de AWS acesso como`PowerUser/john_stiles`. Os usuários com vários conjuntos de permissões escolhem qual função deve ser usada. Os usuários podem escolher sua função para acessar AWS Management Console o.
6. Além da função, os usuários do portal de AWS acesso podem recuperar credenciais temporárias para acesso programático ou de linha de comando escolhendo as teclas de acesso.

Para step-by-step obter orientação que você pode fornecer aos usuários da sua força de trabalho, consulte Usando o portal de AWS acesso e. Obter credenciais de usuário do IAM Identity Center para o AWS CLI ou AWS SDKs

Imposição e limite de acesso

Quando você ativa o IAM Identity Center, ele cria uma função vinculada ao serviço. Você também pode usar políticas de controle de serviço (service control policies, SCPs).

Delegar e impor o acesso

Uma função vinculada ao serviço é um tipo de função do IAM vinculada diretamente a um AWS serviço. Depois de habilitar o IAM Identity Center, o IAM Identity Center pode criar uma função vinculada ao serviço em cada um Conta da AWS em sua organização. Essa função fornece permissões predefinidas que permitem que o IAM Identity Center delegue e imponha quais usuários têm acesso de login único a pessoas específicas Contas da AWS da sua organização em. AWS Organizations Você precisa atribuir a um ou mais usuários acesso a uma conta para usar essa função. Para obter mais informações, consulte Perfis vinculados ao serviço e As funções vinculadas ao serviço do IAM Identity Center permanecem..

Limitar o acesso ao repositório de identidades das contas dos membros

Para o serviço de armazenamento de identidades usado pelo IAM Identity Center, os usuários que têm acesso a uma conta de membro podem usar ações de API que exigem permissões de leitura. As contas dos membros têm acesso às ações de leitura nos namespaces sso-directory e identitystore.

Para obter mais informações, consulte Ações, recursos e chaves de condição para AWS IAM Identity Center diretório e Ações, recursos e chaves de condição para o AWS Identity Store na Referência de Autorização de Serviço.

Para evitar que usuários nas contas membro usem as operações de API no repositório de identidades, você pode anexar uma política de controle de serviços (SCP). As políticas de controle de serviço (SCPs) são um tipo de política organizacional que você pode usar para gerenciar permissões na sua organização. O exemplo de SCP a seguir impede que usuários em contas de membros acessem qualquer operação de API no repositório de identidades.

```
{
    "Sid": "ExplicitlyBlockIdentityStoreAccess",
    "Effect": "Deny",
    "Action": "identitystore:*", "sso-directory:*"],
    "Resource": "*"
}
```

> **Note**
>
> Limitar o acesso das contas dos membros pode prejudicar a funcionalidade nos aplicativos habilitados para o IAM Identity Center.

Para obter mais informações, consulte Políticas de controle de serviços (SCPs) no Guia do usuário do AWS Organizations .

Administradores delegados

A administração delegada fornece uma maneira conveniente para os usuários designados em uma conta de membro registrada realizarem a maioria das tarefas administrativas do IAM Identity Center. Quando você ativa o IAM Identity Center, sua instância do IAM Identity Center é criada na conta de gerenciamento AWS Organizations por padrão. Ele foi originalmente projetado dessa forma para que o IAM Identity Center possa provisionar, desprovisionar e atualizar funções em todas as contas dos membros da sua organização. Mesmo que sua instância do IAM Identity Center deva sempre residir na conta de gerenciamento, você pode optar por delegar a administração do IAM Identity Center a uma conta membro AWS Organizations, ampliando assim a capacidade de gerenciar o IAM Identity Center de fora da conta de gerenciamento.

Habilitar a administração delegada oferece os seguintes benefícios:

- Minimiza o número de pessoas que precisam de acesso à conta de gerenciamento para ajudar a mitigar as preocupações de segurança
- Permite que administradores selecionados atribuam usuários e grupos aos aplicativos e às contas dos membros da sua organização

Para obter mais informações sobre como o IAM Identity Center funciona com AWS Organizations, consulteGerencie o acesso ao Contas da AWS. Para obter informações adicionais e analisar um exemplo de cenário da empresa que mostra como configurar a administração delegada, consulte Introdução à administração delegada do IAM Identity Center no blog de segurança AWS .

Tópicos

Práticas recomendadas

Veja a seguir algumas práticas recomendadas a serem consideradas antes de configurar a administração delegada.

- Conceda o privilégio mínimo à conta de gerenciamento — Sabendo que a conta de gerenciamento é uma conta altamente privilegiada e para aderir ao princípio do privilégio mínimo, recomendamos que você restrinja o acesso à conta de gerenciamento ao menor número possível de pessoas. O atributo de administrador delegado tem como objetivo minimizar o número de pessoas que precisam de acesso à conta de gerenciamento.
- Crie conjuntos de permissões para uso somente na conta de gerenciamento — Isso facilita a administração de conjuntos de permissões personalizados apenas para usuários que acessam sua conta de gerenciamento e ajuda a diferenciá-los dos conjuntos de permissões gerenciados por sua conta de administrador delegado.
- Considere sua localização no Active Directory — Se você planeja usar o Active Directory como sua fonte de identidade do IAM Identity Center, localize o diretório na conta do membro em que você habilitou o atributo de administrador delegado do IAM Identity Center. Se você decidir alterar a fonte de identidade do IAM Identity Center de qualquer outra fonte para o Active Directory ou

alterá-la do Active Directory para qualquer outra fonte, o diretório deverá residir (pertencer à) conta de membro do administrador delegado do IAM Identity Center, se houver; caso contrário, deverá estar na conta de gerenciamento.

- Crie atribuições de usuário somente na conta de gerenciamento — O administrador delegado não pode alterar os conjuntos de permissões provisionados na conta de gerenciamento. No entanto, administradores delegados podem adicionar, editar e excluir grupos e exercícios em grupo.

Pré-requisitos

Antes de registrar uma conta-administrador delegado, você deve primeiro implantar o seguinte ambiente:

- AWS Organizations deve estar habilitado e configurado com pelo menos uma conta de membro, além da sua conta de gerenciamento padrão.
- Se sua fonte de identidade estiver definida como Active Directory, o atributo Sincronização configurável no AD do IAM Identity Center deverá estar habilitado.

Registre uma conta-membro

Para configurar a administração delegada, você deve primeiro registrar uma conta de membro em sua organização como administrador delegado. Os usuários dessa conta de membro que tenham permissões suficientes terão acesso administrativo ao IAM Identity Center. Depois que uma conta de membro for registrada com sucesso para a administração delegada, ela é chamada de conta de administrador delegado. Para saber mais sobre as tarefas que a conta de administrador delegado pode realizar, consulte Conta da AWS tipos.

O IAM Identity Center suporta o registro de apenas uma conta de membro como administrador delegado por vez. Você só pode registrar uma conta de membro enquanto estiver conectado com as credenciais da conta de gerenciamento.

Use o procedimento a seguir para conceder acesso administrativo ao IAM Identity Center registrando uma conta de membro específica em sua AWS organização como administrador delegado.

> **Important**
>
> Essa operação delega o acesso administrativo do IAM Identity Center aos usuários administradores dessa conta membro. Todos os usuários que têm permissões suficientes

para essa conta de administrador delegado podem realizar todas as tarefas administrativas do IAM Identity Center a partir da conta, exceto:

- Habilitar o IAM Identity Center
- Excluir configurações do IAM Identify Center
- Gerenciamento de conjuntos de permissões provisionados na conta de gerenciamento
- Registro ou cancelamento de registro de contas de outros membros como administradores delegados
- Ativar ou desativar o acesso do usuário na conta de gerenciamento

O administrador delegado pode editar a associação ao grupo.

Como registrar uma conta-membro

1. Faça login no AWS Management Console usando as credenciais de sua conta de gerenciamento em AWS Organizations. As credenciais da conta de gerenciamento são necessárias para executar a RegisterDelegatedAdministratorAPI.
2. Selecione a região em que o IAM Identity Center esteja ativado e, em seguida, abra o console do IAM Identity Center.
3. Escolha Configurações e, em seguida, selecione a guia Gerenciamento.
4. Na seção Administrador delegado do , selecione Cancelar conta.
5. Na página Registrar administrador delegado, selecione o Conta da AWS que você deseja registrar e, em seguida, escolha Registrar conta.

Cancelar o registro de uma conta-membro

Você só pode cancelar o registro de uma conta de membro enquanto estiver conectado com as credenciais da conta de gerenciamento.

Use o procedimento a seguir para remover o acesso administrativo do IAM Identity Center cancelando o registro de uma conta membro em sua AWS organização que havia sido designada anteriormente como administrador delegado.

> **Important**
>
> Ao cancelar o registro de uma conta, você efetivamente remove a capacidade de todos os usuários administradores gerenciarem o IAM Identity Center dessa conta. Como resultado, eles não podem mais administrar as identidades, o gerenciamento de acesso, a autenticação ou o acesso ao aplicativo do IAM Identity Center a partir dessa conta. Essa operação não afetará nenhuma permissão ou atribuição configurada no IAM Identity Center e, portanto, não terá impacto sobre seus usuários finais, pois eles continuarão a ter acesso aos seus aplicativos e Contas da AWS de dentro do portal de AWS acesso.

Como cancelar o registro de uma conta-membro

1. Faça login no AWS Management Console usando as credenciais de sua conta de gerenciamento em AWS Organizations. As credenciais da conta de gerenciamento são necessárias para executar a DeregisterDelegatedAdministratorAPI.
2. Selecione a região em que o IAM Identity Center esteja ativado e, em seguida, abra o console do IAM Identity Center.
3. Escolha Configurações e, em seguida, selecione a guia Gerenciamento.
4. Na seção Administrador delegado, selecione Cancelar conta.
5. Na caixa de diálogo Cancelar o registro da conta, analise as implicações de segurança e insira o nome da conta do membro para confirmar que você entendeu.
6. Escolha Cancelar o registro da conta.

Veja qual conta de membro foi registrada como administrador delegado

Use o procedimento a seguir para descobrir qual conta membro em sua AWS Organizations foi configurada como administradora delegada do IAM Identity Center.

Como visualizar sua conta-membro registrada

1. Abra o console do IAM Identity Center.
2. Escolha Configurações.
3. Na seção Detalhes, localize o nome da conta registrada em Administrador delegado. Você também pode localizar essas informações selecionando a guia Gerenciamento e visualizando-as na seção Administrador delegado.

Acesso elevado temporário

Todo acesso ao seu Conta da AWS envolve algum nível de privilégio. Operações sensíveis, como alterar a configuração de um recurso de alto valor, por exemplo, um ambiente de produção, exigem tratamento especial devido ao escopo e ao impacto potencial. O acesso temporário elevado (também conhecido como just-in-time acesso) é uma forma de solicitar, aprovar e rastrear o uso de uma permissão para realizar uma tarefa específica durante um período especificado. O acesso temporário elevado complementa outras formas de controle de acesso, como conjuntos de permissões e autenticação multifatorial.

AWS IAM Identity Center fornece as seguintes opções para gerenciamento temporário de acesso elevado em diferentes ambientes comerciais e técnicos:

- Soluções gerenciadas e suportadas pelo fornecedor — AWS validou as integrações do IAM Identity Center de ofertas selecionadas de parceiros e avaliou suas capacidades em relação a um conjunto comum de requisitos do cliente. Escolha a solução que melhor se alinha ao seu cenário e siga as orientações do provedor para habilitar o recurso com o IAM Identity Center.
- Autogerenciado e autossustentável — Essa opção fornece um ponto de partida se você estiver interessado em acessar AWS apenas temporariamente e puder implantar, personalizar e manter o recurso sozinho. Para obter mais informações, consulte Gerenciamento temporário de acesso elevado (TEAM).

Parceiros AWS de segurança validados para acesso temporário elevado

AWS Os parceiros de segurança usam abordagens diferentes para lidar com um conjunto comum de requisitos de acesso temporário elevado. Recomendamos que você analise cuidadosamente cada solução de parceiro para poder escolher a que melhor atenda às suas necessidades e preferências, incluindo sua empresa, a arquitetura do seu ambiente de nuvem e seu orçamento.

> **Note**
>
> Para recuperação de desastres, recomendamos que você configure o acesso de emergência ao AWS Management Console antes que ocorra uma interrupção.

AWS A Identity validou os recursos e a integração com o IAM Identity Center para as seguintes just-in-time ofertas dos parceiros de AWS segurança:

- CyberArk Secure Cloud Access— Parte dissoCyberArk Identity Security Platform, essa oferta fornece acesso elevado sob demanda a AWS ambientes multinuvem. As aprovações são tratadas por meio da integração com o ITSM ou ChatOps com ferramentas. Todas as sessões podem ser gravadas para fins de auditoria e conformidade.
- Tenable (previously Ermetic)— A Tenable plataforma inclui o provisionamento de acesso just-in-time privilegiado para operações administrativas em AWS ambientes multinuvem. Os registros de sessão de todos os ambientes de nuvem, inclusive registros de acesso AWS CloudTrail estão disponíveis em uma única interface para análise e auditoria. O recurso se integra a ferramentas corporativas e de desenvolvedores, como Slack e Microsoft Teams.
- OktaSolicitações de acesso — Parte da governança de Okta identidade, permite que você configure um fluxo de trabalho de solicitação de just-in-time acesso usando Okta como provedor de identidade externo (IdP) do IAM Identity Center e seus conjuntos de permissões do IAM Identity Center.

Essa lista será atualizada para AWS validar os recursos de soluções adicionais de parceiros e a integração dessas soluções com o IAM Identity Center.

> **Note**
>
> Se você estiver usando políticas baseadas em recursos, Amazon Elastic Kubernetes Service (Amazon EKS AWS Key Management Service) ou (Referenciando conjuntos de permissões em políticas de recursos, Amazon EKS e AWS KMS)AWS KMS, consulte antes de escolher sua solução. just-in-time

Capacidades temporárias de acesso elevado avaliadas para validação de AWS parceiros

AWS A Identity validou que os recursos de acesso temporário elevado oferecidos por CyberArk Secure Cloud Access, Tenable, e as solicitações de Okta acesso atendem aos seguintes requisitos comuns do cliente:

- Os usuários podem solicitar acesso a um conjunto de permissões por um período de tempo especificado pelo usuário, especificando a AWS conta, o conjunto de permissões, o período e o motivo.
- Os usuários podem receber o status de aprovação da solicitação.

- Os usuários não podem invocar uma sessão com um determinado escopo, a menos que haja uma solicitação aprovada com o mesmo escopo e eles invocem a sessão durante o período aprovado.
- Há uma forma de especificar quem pode aprovar solicitações.
- Os aprovadores não podem aprovar suas próprias solicitações.
- Os aprovadores têm uma lista de solicitações pendentes, aprovadas e rejeitadas e podem exportá-la para auditores.
- Os aprovadores podem aprovar e rejeitar solicitações pendentes.
- Os aprovadores podem adicionar uma nota explicando sua decisão.
- Os aprovadores podem revogar uma solicitação aprovada, impedindo o uso futuro do acesso elevado.

> **Note**
>
> Se um usuário estiver conectado com acesso elevado quando uma solicitação aprovada for revogada, a sessão permanecerá ativa por até uma hora após a revogação da aprovação. Para obter mais informações sobre sessões de autenticação, consulte Autenticação.

- As ações e aprovações do usuário estão disponíveis para auditoria.

Acesso com login único a Contas da AWS

Você pode atribuir aos usuários em seu diretório conectado permissões à conta de gerenciamento ou contas de membros em sua organização AWS Organizations com base em funções de trabalho comuns. Ou você pode usar permissões personalizadas para atender aos seus requisitos de segurança específicos. Por exemplo, você pode conceder amplas permissões ao Amazon RDS em contas de desenvolvimento, mas limita essas permissões em contas de produção. O IAM Identity Center configura automaticamente todas as permissões de usuário necessárias em seu Contas da AWS .

> **Note**
>
> Talvez seja necessário conceder permissões aos usuários ou grupos para operar na conta AWS Organizations de gerenciamento. Por ser uma conta altamente privilegiada, restrições de segurança adicionais exigem que você tenha a FullAccess política do IAM ou permissões

equivalentes antes de poder configurá-la. Essas restrições de segurança adicionais não são necessárias para nenhuma das contas dos membros em sua AWS organização.

Atribuir acesso de usuário a Contas da AWS

Use o procedimento a seguir para atribuir acesso logon único a usuários e grupos em seu diretório conectado e usar conjuntos de permissões para determinar o nível de acesso.

Para verificar o acesso existente de usuários e grupos, consulteExibir exercícios de usuários e grupos.

> **Note**
>
> Para simplificar a administração de permissões de acesso, é recomendável atribuir acesso diretamente a grupos, em vez de a usuários específicos. Com grupos, você pode conceder ou negar permissões para grupos de usuários, em vez de ter de aplicar essas permissões a cada indivíduo. Se um usuário for transferido para uma organização diferente, basta mover esse usuário para um grupo diferente para que recebam automaticamente as permissões necessárias para a nova organização.

Para atribuir acesso de usuário ou grupo ao Contas da AWS

1. Abra o console do IAM Identity Center.

   > **Note**
   >
   > Antes de passar para a etapa seguinte, confirme se o console do IAM Identity Center está usando uma das regiões em que seu diretório do AWS Managed Microsoft AD está localizado.

2. No painel de navegação, em Permissões de várias contas, escolha Contas da AWS.
3. Na página Contas da AWS, aparece uma lista de visualização em árvore da sua organização. Marque a caixa de seleção ao lado de uma ou mais Contas da AWS às quais deseja atribuir acesso de logon único.

> **Note**
>
> Você pode selecionar até 10 por Contas da AWS vez por conjunto de permissões ao atribuir acesso de login único a usuários e grupos. Para atribuir mais de 10 Contas da AWS ao mesmo conjunto de usuários e grupos, repita esse procedimento conforme necessário para as contas adicionais. Quando solicitado, selecione os mesmos usuários, grupos e conjunto de permissões.

4. Escolha Atribuir usuários ou grupos.
5. Na Etapa 1: Selecionar usuários e grupos, na página Atribuir usuários e grupos a "***AWS-account-name***", faça o seguinte:
   1. Na guia Usuários, selecione um ou mais usuários aos quais conceder acesso de login único.

      Para filtrar os resultados, comece a digitar o nome do usuário desejado na caixa de pesquisa.
   2. Na guia Grupos, selecione um ou mais grupos aos quais conceder acesso de login único.

      Para filtrar os resultados, comece a digitar o nome do grupo que deseja na caixa de pesquisa.
   3. Para exibir os usuários e grupos selecionados, escolha o triângulo lateral ao lado de Usuários e grupos selecionados.
   4. Depois de confirmar que os usuários e grupos corretos foram selecionados, escolha Avançar.
6. Na Etapa 2: Selecionar conjuntos de permissões, na página Atribuir conjuntos de permissões a "***AWS-account-name***", faça o seguinte:
   1. Selecione um ou mais conjuntos de permissões. Se necessário, você pode criar e selecionar novos conjuntos de permissões.
      - Para selecionar um ou mais conjuntos de permissões existentes, em Conjuntos de permissões, selecione os conjuntos de permissões que você deseja aplicar aos usuários e grupos selecionados na etapa anterior.
      - Para criar um ou mais novos conjuntos de permissões, escolha Criar conjunto de permissões e siga as etapas em Criar um conjunto de permissões. Depois de criar os conjuntos de permissões que você deseja aplicar, no console do IAM Identity Center, retorne a Contas da AWS e siga as instruções até chegar à Etapa 2: Selecionar conjuntos de permissões. Ao chegar a essa etapa, selecione os novos conjuntos de permissões que você criou e vá para a próxima etapa desse procedimento.

2. Depois de confirmar que os conjuntos de permissões corretos foram selecionados, escolha Avançar.

7. Na Etapa 3: Revisar e enviar, na página Revisar e enviar exercícios para "***AWS-account-name***", faça o seguinte:

   1. Analise os usuários, grupos e conjuntos de permissões selecionados.
   2. Depois de confirmar que os usuários, grupos e conjuntos de permissões corretos foram selecionados, escolha Enviar.

   > **Important**
   >
   > O processo de atribuição de usuário e grupo pode demorar alguns minutos para ser concluído. Mantenha a página aberta até que o processo seja concluído com êxito.

   > **Note**
   >
   > Talvez seja necessário conceder permissões aos usuários ou grupos para operar na conta AWS Organizations de gerenciamento. Por ser uma conta altamente privilegiada, restrições de segurança adicionais exigem que você tenha a FullAccess política do IAM ou permissões equivalentes antes de poder configurá-la. Essas restrições de segurança adicionais não são necessárias para nenhuma das contas dos membros em sua AWS organização.

Remover o acesso de usuários e grupos

Use esse procedimento para remover o acesso de login único a um Conta da AWS ou mais usuários e grupos em seu diretório conectado.

Para remover o acesso de usuários e grupos a um Conta da AWS

1. Abra o console do IAM Identity Center.
2. No painel de navegação, em Permissões de várias contas, escolha Contas da AWS.
3. Na página Contas da AWS, aparece uma lista de visualização em árvore da sua organização. Selecione o nome do Conta da AWS que contém os usuários e grupos dos quais você deseja remover o acesso de login único.

4. Na página Visão geral do Conta da AWS, em Usuários e grupos atribuídos, selecione o nome de um ou mais usuários ou grupos e escolha Remover acesso.
5. Na caixa de diálogo Remover acesso, confirme se os nomes dos usuários ou grupos estão corretos e escolha Remover acesso.

Revogar sessões de função ativas do IAM criadas por conjuntos de permissões

Veja a seguir um procedimento geral para revogar uma sessão ativa de conjunto de permissões para um usuário do IAM Identity Center. O procedimento pressupõe que você queira remover todo o acesso de um usuário que tenha credenciais comprometidas ou de um agente mal-intencionado que esteja no sistema. O pré-requisito é ter seguido as orientações em. Prepare-se para revogar uma sessão de função ativa do IAM criada por um conjunto de permissões Presumimos que a política de negar tudo esteja presente em uma política de controle de serviços (SCP).

> **Note**
>
> AWS recomenda que você crie automação para lidar com todas as etapas, exceto as operações somente do console.

1. Obtenha o ID de usuário da pessoa cujo acesso você deve revogar. Você pode usar as APIs do repositório de identidades para encontrar o usuário pelo nome de usuário.
2. Atualize a política de negação para adicionar o ID do usuário da etapa 1 em sua política de controle de serviço (SCP). Depois de concluir essa etapa, o usuário alvo perde o acesso e não consegue realizar ações com nenhuma função afetada pela política.
3. Remova todas as atribuições do conjunto de permissões para o usuário. Se o acesso for atribuído por meio de associações a grupos, remova o usuário de todos os grupos e de todas as atribuições diretas do conjunto de permissões. Essa etapa impede que o usuário assuma qualquer função adicional do IAM. Se um usuário tiver uma sessão ativa do portal de AWS acesso e você desabilitar o usuário, ele poderá continuar assumindo novas funções até que você remova o acesso.
4. Se você usar um provedor de identidade (IdP) ou o Microsoft Active Directory como fonte de identidade, desative o usuário na fonte de identidade. A desativação do usuário impede a criação de sessões adicionais do portal de AWS acesso. Use sua documentação do IdP ou

da API do Microsoft Active Directory para saber como automatizar essa etapa. Se você estiver usando o diretório do IAM Identity Center como fonte de identidade, ainda não desabilite o acesso do usuário. Você desativará o acesso do usuário na etapa 6.

5. No console do IAM Identity Center, encontre o usuário e exclua sua sessão ativa.

   a. Selecione Usuários.

   b. Escolha o usuário cuja sessão ativa você deseja excluir.

   c. Na página de detalhes do usuário, escolha a guia Sessões ativas.

   d. Marque as caixas de seleção ao lado das sessões que você deseja excluir e escolha Excluir sessão.

   Isso garante que a sessão do portal de AWS acesso do usuário seja interrompida em aproximadamente 60 minutos. Saiba mais sobre a duração da sessão.

6. No console do IAM Identity Center, desative o acesso do usuário.

   a. Selecione Usuários.

   b. Escolha o usuário cujo acesso você deseja desativar.

   c. Na página de detalhes do usuário, expanda Informações gerais e escolha o botão Desativar acesso do usuário para evitar mais logins do usuário.

7. Mantenha a política de negação em vigor por pelo menos 12 horas. Caso contrário, o usuário com uma sessão de função do IAM ativa terá ações restauradas com a função do IAM. Se você esperar 12 horas, as sessões ativas expirarão e o usuário não poderá acessar a função do IAM novamente.

> **Important**
>
> Se você desabilitar o acesso de um usuário antes de interromper a sessão do usuário (você concluiu a etapa 6 sem concluir a etapa 5), não poderá mais interromper a sessão do usuário por meio do console do IAM Identity Center. Se você desativar inadvertidamente o acesso do usuário antes de interromper a sessão do usuário, poderá reativá-lo, interromper a sessão e desativar o acesso novamente.

Agora você pode alterar as credenciais do usuário se a senha tiver sido comprometida e restaurar suas atribuições.

Delegar quem pode atribuir acesso de logon único a usuários e grupos na conta de gerenciamento

Atribuir acesso de logon único à conta mestre usando o console do IAM Identity Center é uma ação privilegiada. Por padrão, somente um usuário Usuário raiz da conta da AWS ou um usuário que tenha as políticas AWSSSOMasterAccountAdministratorIAMFullAccess AWS gerenciadas anexadas pode atribuir acesso de login único à conta de gerenciamento. As IAMFullAccesspolíticas AWSSSOMasterAccountAdministratore gerenciam o acesso de login único à conta de gerenciamento em uma AWS Organizations organização.

Use as etapas a seguir para delegar permissões para gerenciar o acesso SSO aos usuário e grupos em seu diretório.

Para conceder permissões para gerenciar o acesso SSO ao usuários e grupos em seu diretório

1. Faça login no console do como um usuário raiz da conta mestre ou com outro usuário do IAM Identity Center que tenha permissões de administrador do para a conta mestre.
2. Siga as etapas Criar um conjunto de permissões para criar um conjunto de permissões e faça o seguinte:

    1. Na página Criar novo conjunto de permissões, marque a caixa de seleção Criar um conjunto de permissões personalizado e escolha Avançar: Detalhes.
    2. Na página Criar novo conjunto de permissões, especifique um nome para o conjunto de permissões personalizado e, opcionalmente, uma descrição. Se necessário, modifique a duração da sessão e especifique um URL de estado de retransmissão.

        > **Note**
        >
        > Para o URL do estado de retransmissão, você deve especificar um URL que esteja no AWS Management Console. Por exemplo: .
        > **`https://console.aws.amazon.com/ec2/`**
        > Para ter mais informações, consulte Definir estado de retransmissão.

    3. Em Quais políticas você deseja incluir no seu conjunto de permissões? , marque a caixa de seleção Anexar políticas AWS gerenciadas.
    4. Na lista de políticas do IAM, escolha as políticas AWSSSOMasterAccountAdministratore as IAMFullAccess AWS gerenciadas. Essa política concede permissões a qualquer usuário e grupos que receberem acesso a esse conjunto de permissões definido no futuro.

5. Escolha Próximo: etiquetas.
6. Em Adicionar tags (opcional), especifique valores de Chave e Valor (opcional), e escolha Avançar: Revisão. Para obter mais informações sobre tags, consulte Marcando atributos AWS IAM Identity Center.
7. Verifique suas seleções e, em seguida, escolha Create function.

3. Siga as etapas em Atribuir acesso de usuário a Contas da AWS para atribuir os usuários e grupos apropriados ao conjunto de permissões que você acabou de criar.
4. Comunique o seguinte aos usuários atribuídos: Quando eles entrarem no portal de AWS acesso e escolherem a guia Contas, eles devem escolher o nome de função apropriado para serem autenticados com as permissões que você acabou de delegar.

Conjuntos de permissões

Um conjunto de permissões é um modelo que você cria e mantém que define uma coleção de uma ou mais políticas do IAM. Os conjuntos de permissões simplificam a atribuição de Conta da AWS acesso para usuários e grupos em sua organização. Por exemplo, você pode criar um conjunto de permissões de administrador de banco de dados que inclui políticas para administrar os serviços AWS RDS, DynamoDB e Aurora e usar esse único conjunto de permissões para conceder acesso a uma lista de Contas da AWS destinos em sua organização para seus administradores de banco de dados.AWS

O IAM Identity Center atribui acesso a um usuário ou grupo em um ou mais Contas da AWS com conjuntos de permissões. Quando você atribui um conjunto de permissões, o IAM Identity Center cria perfis do IAM correspondentes controlados pelo IAM Identity Center em cada conta e anexa as políticas especificadas no conjunto de permissões para esses perfis. O IAM Identity Center gerencia a função e permite que os usuários autorizados que você definiu assumam a função, usando o portal do usuário ou a AWS CLI do IAM Identity Center. Conforme você modificar o conjunto de permissões, o IAM Identity Center garantirá que as políticas e perfis do IAM correspondentes sejam devidamente atualizados.

Você pode adicionar políticas gerenciadas pela AWS, políticas gerenciadas pelo cliente, políticas em linha e políticas gerenciadas pela AWS para funções de trabalho aos seus conjuntos de permissões. Você também pode atribuir uma política gerenciada da AWS da ou uma política gerenciada pelo cliente como limite de permissões.

Para criar um conjunto de permissões, consulte Criar, gerenciar e excluir conjuntos de permissões.

Tópicos

Permissões predefinidas

Você pode criar um conjunto de permissões predefinido com políticas AWS gerenciadas.

Ao criar um conjunto de permissões com permissões predefinidas, você escolhe uma política em uma lista de políticas AWS gerenciadas. Dentro das políticas disponíveis, você pode escolher entre Políticas de permissão comuns e Políticas de funções de trabalho.

Políticas de permissão comuns

Escolha entre uma lista de políticas AWS gerenciadas que possibilitam o acesso total aos recursos Conta da AWS. Você pode adicionar uma das seguintes políticas:

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

Políticas de função de trabalho

Escolha em uma lista de políticas AWS gerenciadas que possibilitam o acesso a recursos em sua empresa Conta da AWS que possam ser relevantes para um cargo em sua organização. Você pode adicionar uma das seguintes políticas:

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser

- SystemAdministrator

Para obter descrições detalhadas das políticas de permissão comuns e políticas de função de trabalho disponíveis, consulte Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do AWS Identity and Access Management .

Para obter instruções sobre como criar um conjunto de permissões, consulte Criar, gerenciar e excluir conjuntos de permissões.

Permissões personalizadas

Você pode criar um conjunto de permissões com permissões personalizadas, combinando qualquer uma das políticas AWS gerenciadas e gerenciadas pelo cliente que você tem no AWS Identity and Access Management (IAM) com políticas em linha. Você também pode incluir um limite de permissões, definindo o máximo possível de permissões que outras políticas podem conceder aos usuários do seu conjunto de permissões.

Para obter instruções sobre como criar um conjunto de permissões, consulte Criar, gerenciar e excluir conjuntos de permissões.

Tipos de política que você pode anexar ao seu conjunto de permissões

Tópicos

- Políticas em linha
- AWS políticas gerenciadas
- Políticas gerenciadas pelo cliente
- Limites de permissões

Políticas em linha

Você pode anexar uma política em linha a um conjunto de permissões. Uma política em linha é um bloco de texto formatado como uma política do IAM que você adiciona diretamente ao seu conjunto de permissões. Você pode colar em uma política ou gerar uma nova com a ferramenta de criação de políticas no console do IAM Identity Center ao criar um novo conjunto de permissões. Você também pode criar políticas do IAM com o Gerador de Políticas da AWS.

Quando você implanta um conjunto de permissões com uma política embutida, o IAM Identity Center cria uma política do IAM no local em Contas da AWS que você atribui seu conjunto de permissões.

O IAM Identity Center cria a política quando você atribui o conjunto de permissões à conta. Em seguida, a política é anexada à função do IAM Conta da AWS que seu usuário assume.

Quando você cria uma política em linha e atribui seu conjunto de permissões, o IAM Identity Center configura as políticas em sua conta Contas da AWS para você. Ao criar seu conjunto de permissões comPolíticas gerenciadas pelo cliente, você Contas da AWS mesmo deve criar as políticas antes de atribuir o conjunto de permissões.

AWS políticas gerenciadas

Você pode anexar políticas AWS gerenciadas ao seu conjunto de permissões. AWS políticas gerenciadas são políticas do IAM que AWS mantém. Por outro lado, Políticas gerenciadas pelo cliente são as políticas do IAM em sua conta que você cria e mantém. AWS políticas gerenciadas tratam de casos de uso de privilégios mínimos comuns em seu Conta da AWS. Você pode atribuir uma política AWS gerenciada como permissões para a função que o IAM Identity Center cria ou como um limite de permissões.

AWS mantém políticas AWS gerenciadas para funções de trabalho que atribuem permissões de acesso específicas ao trabalho aos seus AWS recursos. Você pode adicionar uma política de função de trabalho ao optar por usar permissões predefinidas com seu conjunto de permissões. Ao escolher Permissões personalizadas, você pode adicionar mais de uma política de função de trabalho.

Você Conta da AWS também contém um grande número de políticas AWS gerenciadas de IAM para aplicações específicas Serviços da AWS e combinações de Serviços da AWS. Ao criar um conjunto de permissões com permissões personalizadas, você pode escolher entre várias políticas AWS gerenciadas adicionais para atribuir ao seu conjunto de permissões.

AWS preenche cada um Conta da AWS com políticas AWS gerenciadas. Para implantar um conjunto de permissões com políticas AWS gerenciadas, você não precisa primeiro criar uma política no seu Contas da AWS. Ao criar seu conjunto de permissões comPolíticas gerenciadas pelo cliente, você Contas da AWS mesmo deve criar as políticas antes de atribuir o conjunto de permissões.

Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

Políticas gerenciadas pelo cliente

Você pode anexar políticas gerenciadas pelo cliente ao seu conjunto de permissões. Políticas gerenciadas pelo cliente são políticas do IAM em sua conta que você cria e mantém. Por outro lado, AWS políticas gerenciadas são as políticas do IAM em sua conta que são AWS mantidas. Você pode

atribuir uma política gerenciada pelo cliente como permissões para o perfil que o IAM Identity Center cria ou como um limite de permissões.

Ao criar um conjunto de permissões com uma política gerenciada pelo cliente, você deve criar uma política do IAM com o mesmo nome e caminho em cada uma em Conta da AWS que o IAM Identity Center atribui seu conjunto de permissões. Se você estiver especificando um caminho personalizado, certifique-se de especificar o mesmo caminho em cada Conta da AWS. Para obter mais informações, consulte Nome e caminhos amigáveis no Guia do usuário do IAM. O IAM Identity Center associa a política do IAM ao perfil do IAM que ele cria na sua Conta da AWS. Como prática recomendada, aplique as mesmas permissões à política em cada conta à qual você atribui o conjunto de permissões. Para ter mais informações, consulte Use políticas do IAM nos conjuntos de permissões.

Para obter mais informações, consulte Políticas gerenciadas pelo cliente no Guia do usuário do IAM.

Limites de permissões

Você pode anexar um limite de permissões ao seu conjunto de permissões. Um limite de permissões é uma política de IAM AWS gerenciada ou gerenciada pelo cliente que define o máximo de permissões que uma política baseada em identidade pode conceder a um diretor do IAM. Quando você aplica um limite de permissões, seu Políticas em linha, Políticas gerenciadas pelo cliente e AWS políticas gerenciadas não podem conceder nenhuma permissão que exceda as permissões que seu limite de permissões concede. Um limite de permissões não concede nenhuma permissão, mas faz com que o IAM ignore todas as permissões além do limite.

Ao criar um conjunto de permissões com uma política gerenciada pelo cliente como limite de permissões, você deve criar uma política do IAM com o mesmo nome em cada Conta da AWS em que o IAM Identity Center atribui seu conjunto de permissões. O IAM Identity Center anexa a política do IAM como um limite de permissões ao perfil do IAM que ele cria em sua Conta da AWS .

Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

Criar, gerenciar e excluir conjuntos de permissões

Os conjuntos de permissões definem o nível de acesso que os usuários e grupos têm a uma Conta da AWS. Os conjuntos de permissões são armazenados no IAM Identity Center e podem ser provisionados para um ou mais Contas da AWS. Você pode atribuir mais de um conjunto de

permissões a um usuário. Para obter mais informações sobre conjuntos de permissões e como eles são usados no IAM Identify Center, consulteConjuntos de permissões.

Ao criar conjuntos de permissões, tenha em mente as seguintes considerações:

- Começar com um conjunto de permissões predefinido

  Com um conjunto de permissões predefinido, que usa permissões predefinidas, você escolhe uma única política AWS gerenciada em uma lista de políticas disponíveis. Cada política concede um nível específico de acesso a AWS serviços e recursos ou permissões para uma função de trabalho comum. Para obter informações sobre cada uma dessas políticas, consulte políticas gerenciadas pela AWS para funções de trabalho. Depois de coletar os dados de uso, você pode refinar o conjunto de permissões para torná-lo mais restritivo.
- Limitar a duração da sessão de gerenciamento a períodos de trabalho razoáveis

  Quando os usuários se federam Conta da AWS e usam o AWS Management Console ou a Interface de Linha de AWS Comando (AWS CLI), o IAM Identity Center usa a configuração de duração da sessão no conjunto de permissões para controlar a duração da sessão. Quando a sessão do usuário atinge a duração da sessão, ele é desconectado do console e solicitado a fazer login novamente. Como prática de segurança, recomendamos que você não defina um tempo de duração da sessão maior do que o necessário para desempenhar a função. Por padrão, o valor de Duração da sessão é uma hora. Você pode especificar um valor máximo de 12 horas. Para ter mais informações, consulte Definir duração da sessão.
- Limitar a duração da sessão do portal de usuários da força de trabalho

  Os usuários da força de trabalho usam sessões do portal para escolher perfis e acessar aplicações. Por padrão, o valor da duração máxima da sessão, que determina o período de tempo em que um usuário da força de trabalho pode entrar no portal de AWS acesso antes de precisar se autenticar novamente, é de oito horas. Você pode especificar um valor máximo de 90 dias. Para ter mais informações, consulte Configure a duração da sessão do portal de AWS acesso e dos aplicativos integrados do IAM Identity Center.
- Usar o perfil que fornece permissões de privilégio mínimo

  Cada conjunto de permissões que você cria e atribui ao seu usuário aparece como uma função disponível no portal de AWS acesso. Ao entrar no portal como esse usuário, escolha a função que corresponde ao conjunto de permissões mais restritivo que você pode utilizar para realizar tarefas na conta, em vez `AdministratorAccess` de. Teste os conjuntos de permissões para verificar se eles fornecem o acesso necessário antes de enviar o convite ao usuário.

> **Note**
>
> Como alternativa, você pode usar o AWS CloudFormation para criar e atribuir conjuntos de permissões e atribuir usuários a esses conjuntos de permissões.

Tópicos

Criar um conjunto de permissões

Use esse procedimento para criar um conjunto de permissões predefinido que usa uma única política gerenciada AWS ou um conjunto de permissões personalizado que usa até 10 políticas gerenciadas AWS ou gerenciadas pelo cliente e uma política em linha. Você pode solicitar um ajuste no número máximo de 10 políticas no console Service Quotas para IAM.

Você pode criar um conjunto de permissões no console do IAM Identity Center.

Para criar um conjunto de permissões

1. Abra o console do IAM Identity Center.
2. Em Permissões de várias contas, escolha Conjuntos de permissões.
3. Escolha Create permission set (Criar conjunto de permissões).
4. Na página Selecionar tipo de conjunto de permissões, em Tipo de conjunto de permissões, selecione um tipo de conjunto de permissões.
5. Escolha uma ou mais políticas que você deseja usar para o conjunto de permissões, com base no tipo de conjunto de permissões:

   - Conjunto de permissões predefinido

     1. Em Política para conjunto de permissões predefinido, selecione uma das políticas de função de trabalho do IAM ou políticas de permissão comuns na lista e escolha Avançar. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas

gerenciadas pela AWS para funções de trabalho no AWS Identity and Access Management Guia do usuário do IAM.

2. Vá para a Etapa 6 para concluir a página Especificar detalhes do conjunto de permissões.

- Conjunto de permissões personalizado

1. Escolha Próximo.
2. Na página Especificar políticas e limites de permissão, escolha os tipos de políticas do IAM que você deseja aplicar ao seu novo conjunto de permissões. Por padrão, você pode adicionar qualquer combinação de até 10 políticas AWS gerenciadas e políticas gerenciadas pelo cliente ao seu conjunto de permissões. Essa cota é definida pelo IAM. Para aumentá-la, solicite um aumento nas políticas gerenciadas de cotas do IAM anexadas a um perfil do IAM no console do Service Quotas em cada Conta da AWS na qual você deseja atribuir o conjunto de permissões.
   - Expanda as políticas AWS gerenciadas para adicionar políticas do IAM que AWS criam e mantêm. Para ter mais informações, consulte AWS políticas gerenciadas.
     a. Pesquise e escolha as políticas AWS gerenciadas que você deseja aplicar aos seus usuários no conjunto de permissões.
     b. Se você quiser adicionar outro tipo de política, escolha seu contêiner e faça sua seleção. Escolha Avançar quando tiver escolhido todas as políticas que deseja aplicar. Vá para a Etapa 6 para concluir a página Especificar detalhes do conjunto de permissões.
   - Expanda as políticas gerenciadas pelo cliente para adicionar políticas do IAM que você cria e mantém. Para ter mais informações, consulte Políticas gerenciadas pelo cliente.
     a. Escolha Anexar políticas e insira o nome de uma política que você deseja adicionar ao seu conjunto de permissões. Em cada conta à qual você deseja atribuir o conjunto de permissões, crie uma política com o nome inserido. Como prática recomendada, atribua as mesmas permissões à política em cada conta.
     b. Escolha Anexar mais para adicionar outra política.
     c. Se você quiser adicionar outro tipo de política, escolha seu contêiner e faça sua seleção. Escolha Avançar quando tiver escolhido todas as políticas que deseja aplicar. Vá para a Etapa 6 para concluir a página Especificar detalhes do conjunto de permissões.
   - Expanda a política embutida para adicionar um texto de política personalizado formatado em JSON. As políticas em linha não correspondem aos recursos existentes do IAM. Para criar uma política em linha, insira o idioma personalizado da política no formulário

fornecido. O IAM Identity Center adiciona a política aos recursos do IAM que ele cria em suas contas de membros. Para ter mais informações, consulte Políticas em linha.

a. Adicione as ações e os recursos desejados no editor interativo à sua política em linha. Declarações adicionais podem ser adicionadas com Adicionar nova declaração.

b. Se você quiser adicionar outro tipo de política, escolha seu contêiner e faça sua seleção. Escolha Avançar quando tiver escolhido todas as políticas que deseja aplicar. Vá para a Etapa 6 para concluir a página Especificar detalhes do conjunto de permissões.

- Expanda o limite de permissões para adicionar uma AWS política de IAM gerenciada ou gerenciada pelo cliente como as permissões máximas que suas outras políticas no conjunto de permissões podem atribuir. Para ter mais informações, consulte Limites de permissões.

  a. Escolha Usar um limite de permissões para controlar as permissões máximas.

  b. Escolha a política AWS gerenciada para definir uma política do IAM que AWS seja criada e mantida como seu limite de permissões. Escolha Políticas gerenciadas pelo cliente para definir uma política do IAM que você cria e mantém como limite de permissões.

  c. Se você quiser adicionar outro tipo de política, escolha seu contêiner e faça sua seleção. Escolha Avançar quando tiver escolhido todas as políticas que deseja aplicar. Vá para a Etapa 6 para concluir a página Especificar detalhes do conjunto de permissões.

6. Na página Specify permission set details (Especificar detalhes do conjunto de permissões), faça o seguinte:

   1. Em Nome do conjunto de permissões, digite um nome para identificar esse conjunto de permissões no IAM Identity Center. O nome que você especifica para esse conjunto de permissões aparece no portal de AWS acesso como uma função disponível. Os usuários entram no portal de AWS acesso, escolhem uma e Conta da AWS, em seguida, escolhem a função.
   2. (Opcional) Você pode também digitar uma descrição. A descrição aparece somente no console do IAM Identity Center, não no portal de AWS acesso.
   3. (Opcional) Especifique o valor da duração da sessão. Esse valor determina o período de tempo em que um usuário pode estar conectado antes que o console saia da sessão. Para ter mais informações, consulte Definir duração da sessão.

4. (Opcional) Especifique o valor para o Relay state.(estado de retransmissão). Esse valor é usado no processo de federação para redirecionar usuários dentro da conta. Para ter mais informações, consulte Definir estado de retransmissão.

   > **Note**
   >
   > O URL do estado de retransmissão deve estar dentro do AWS Management Console. Por exemplo: .
   > **`https://console.aws.amazon.com/ec2/`**

5. Expanda Tags (opcional), escolha Adicionar tag e especifique valores para Chave e Valor (opcional).

   Para obter mais informações sobre tags, consulte Marcando atributos AWS IAM Identity Center.

6. Escolha Próximo.

7. Na página Revisar e criar, revise as seleções que você fez e escolha Criar.

8. Por padrão, quando você cria um conjunto de permissões, o conjunto de permissões não é provisionado (usado em nenhum Contas da AWS). Para provisionar um conjunto de permissões em um Conta da AWS, você deve atribuir acesso ao IAM Identity Center aos usuários e grupos na conta e, em seguida, aplicar o conjunto de permissões a esses usuários e grupos. Para ter mais informações, consulte Acesso com login único a Contas da AWS.

Delegar a administração do conjunto de permissões

O IAM Identity Center permite delegar o gerenciamento de conjuntos de permissões e atribuições em contas criando políticas do IAM que fazem referência aos nomes do recursos da Amazon (ARNs) dos recursos do IAM Identity Center. Por exemplo, você pode criar políticas que permitam que diferentes administradores gerenciem atribuições em contas específicas para conjuntos de permissões com tags específicas.

Você pode usar um dos métodos a seguir para criar esses tipos de políticas.

- (Recomendado) Crie conjuntos de permissões no IAM Identity Center, cada um com uma política diferente, e atribua os conjuntos de permissões a usuários ou grupos diferentes. Isso permite que você gerencie permissões administrativas para usuários que fazem login usando a fonte de identidade do IAM Identity Center escolhida.

- Crie políticas personalizadas no IAM e, em seguida, anexe-as às funções do IAM que seus administradores assumem. Para obter informações sobre funções, consulte Funções do IAM para obter as permissões administrativas atribuídas ao IAM Identity Center.

> **Important**
>
> Os ARNs de recursos do IAM Identify Center são sensíveis a caracteres maiúsculos e minúsculos.

O exemplo a seguir mostra o caso adequado para referenciar o conjunto de permissões e os tipos de recursos da conta do IAM Identity Center.

Tipos de recursos	ARN	Chaves de contexto
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	`aws:ResourceTag/${TagKey}`
Conta	`arn:${Partition}:sso:::account/${AccountId}`	Não aplicável

Use políticas do IAM nos conjuntos de permissões

Em Criar um conjunto de permissões, você aprendeu a adicionar políticas, inclusive políticas gerenciadas pelo cliente e limites de permissões, a um conjunto de permissões. Quando você adiciona políticas e permissões gerenciadas pelo cliente a um conjunto de permissões, o IAM Identity Center não cria uma política em nenhum Contas da AWS. Em vez disso, você deve criar essas políticas com antecedência em cada conta à qual deseja atribuir seu conjunto de permissões e combiná-las com as especificações de nome e caminho do seu conjunto de permissões. Quando você atribui um conjunto de permissões a um Conta da AWS em sua organização, o IAM Identity Center cria uma função AWS Identity and Access Management (IAM) e anexa suas políticas do IAM a essa função.

> **Note**
>
> Antes de atribuir seu conjunto de permissões às políticas do IAM, você deve preparar sua conta de membro. O nome de uma política do IAM em sua conta de membro deve ser compatível com maiúsculas e minúsculas com o nome da política em sua conta de gerenciamento. O IAM Identity Center não consegue atribuir o conjunto de permissões se a política não existir em sua conta de membro.
> As permissões concedidas pela política não precisam ser uma correspondência exata entre as contas.

Como atribuir uma política do IAM a um conjunto de permissões

1. Crie uma política do IAM em cada um dos Contas da AWS locais em que você deseja atribuir o conjunto de permissões.
2. Atribua permissões à política do IAM;. Você pode atribuir permissões diferentes em contas diferentes. Para uma experiência consistente, configure e mantenha permissões idênticas em cada política. Você pode usar recursos de automação, como AWS CloudFormation StackSets criar cópias de uma política do IAM com o mesmo nome e permissões em cada conta membro. Para obter mais informações sobre CloudFormation StackSets, consulte Trabalhando com AWS CloudFormation StackSets no Guia AWS CloudFormation do usuário.
3. Crie um conjunto de permissões em sua conta de gerenciamento e adicione sua política do IAM em Políticas gerenciadas pelo cliente ou Limite de permissões. Para obter mais detalhes sobre como criar um conjunto de permissões, consulte Criar um conjunto de permissões.
4. Adicione quaisquer políticas em linha, políticas AWS gerenciadas ou políticas do IAM que você tenha preparado.
5. Crie e atribua seu conjunto de permissões.

Excluir conjuntos de permissões

Se você quiser revogar uma sessão ativa do conjunto de permissões, consulteRevogar sessões de função ativas do IAM criadas por conjuntos de permissões.

Antes de excluir um conjunto de permissões do IAM Identity Center, você deve removê-lo de todas as Contas da AWS que usam o conjunto de permissões. Para verificar o acesso existente de usuários e grupos, consulteExibir exercícios de usuários e grupos.

Para remover um conjunto de permissões de um Conta da AWS

1. Abra o console do IAM Identity Center.
2. Em Permissões de várias contas, escolha Contas da AWS.
3. Na página Contas da AWS, aparece uma lista de visualização em árvore da sua organização. Selecione o nome Conta da AWS do qual você deseja remover o conjunto de permissões.
4. Na página Visão geral do Conta da AWS, escolha a guia Conjuntos de permissões.
5. Marque a caixa de seleção ao lado dos usuários que deseja remover e escolha Remove (Remover).
6. Na caixa de diálogo Remover conjunto de permissões, confirme se o conjunto de permissões correto está selecionado, digite **`Delete`** para confirmar a remoção e escolha Remover acesso.

Use o procedimento a seguir para excluir um ou mais conjuntos de permissões para que eles não possam mais ser usados por ninguém Conta da AWS na organização.

> **Note**
>
> Todos os usuários e grupos aos quais foi atribuído esse conjunto de permissões, independentemente de quem o Conta da AWS esteja usando, não poderão mais fazer login. Para verificar o acesso existente de usuários e grupos, consulteExibir exercícios de usuários e grupos.

Para excluir um conjunto de permissões de um Conta da AWS

1. Abra o console do IAM Identity Center.
2. Em Permissões de várias contas, escolha Conjuntos de permissões.
3. Selecione o conjunto de permissões que você deseja excluir e, em seguida, Excluir.
4. Na caixa de diálogo Excluir conjunto de permissões, digite o nome do conjunto de permissões para confirmar a exclusão e escolha Excluir. O nome diferencia maiúsculas e minúsculas.

Configurar propriedades do conjunto de permissões

No IAM Identity Center, você pode personalizar a experiência do usuário configurando as seguintes propriedades no conjunto de permissões.

Tópicos

Definir duração da sessão

Para cada conjunto de permissões, você pode especificar uma duração de sessão de modo a controlar quanto tempo um usuário pode ficar conectado a uma conta da Conta da AWS. Quando a duração especificada expirar, AWS o usuário sai da sessão.

Quando você cria um novo conjunto de permissões, a duração da sessão é definida como 1 hora (em segundos) por padrão. A duração mínima da sessão é de 1 hora e pode ser definida, no máximo, para 12 horas. O IAM Identity Center cria automaticamente funções do IAM em cada conta atribuída para cada conjunto de permissões e configura essas funções com uma duração máxima de sessão de 12 horas.

Quando os usuários se federam em seus Conta da AWS consoles ou quando o AWS Command Line Interface (AWS CLI) é usado, o IAM Identity Center usa a configuração de duração da sessão no conjunto de permissões para controlar a duração da sessão. Por padrão, as funções do IAM geradas pelo IAM Identity Center para conjuntos de permissões só podem ser assumidas pelos próprios usuários do IAM Identity Center, o que garante que a duração da sessão especificada no conjunto de permissões do IAM Identity Center seja aplicada.

> **Important**
>
> Como melhor prática de segurança, recomendamos que você não defina um tempo de duração da sessão maior do que o necessário para executar a função.

Após a criação de um conjunto de permissões, você poderá atualizá-lo posteriormente para aplicar uma nova duração de sessão. Use o procedimento a seguir para modificar o tamanho da duração da sessão para um determinado conjunto de permissões.

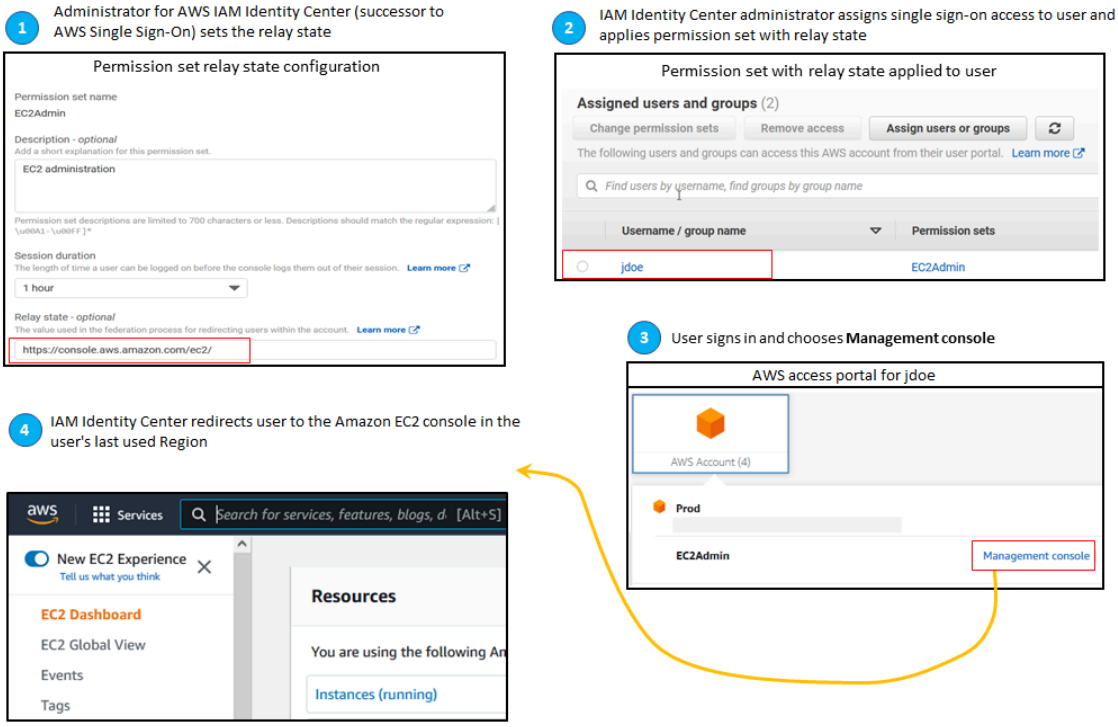
Como definir a duração da sessão

1. Abra o console do IAM Identity Center.

2. Em Permissões de várias contas, escolha Conjuntos de permissões.
3. Escolha o nome do conjunto de permissões para o qual deseja alterar a duração da sessão.
4. Na página de detalhes do conjunto de permissões, à direita do título da seção Configurações gerais, escolha Editar.
5. Na página Editar configurações gerais do conjunto de permissões, escolha um novo valor para a duração da sessão.
6. Se o conjunto de permissões for provisionado em alguma Contas da AWS, os nomes das contas aparecerão abaixo Contas da AWS para reprovisionamento automático. Depois que o valor da duração da sessão do conjunto de permissões for atualizado, todos os Contas da AWS que usam o conjunto de permissões serão reprovisionados. Isso significa que o novo valor dessa configuração é aplicado a todos Contas da AWS que usam o conjunto de permissões.
7. Escolha Salvar alterações.
8. Na parte superior da página Contas da AWS, uma notificação é exibida.
   - Se o conjunto de permissões for provisionado em uma ou mais Contas da AWS, a notificação confirma que as Contas da AWS foram reprovisionadas com êxito e que o conjunto de permissões atualizado foi aplicado às contas.
   - Se o conjunto de permissões não estiver provisionado em um Conta da AWS, a notificação confirma que as configurações do conjunto de permissões foram atualizadas.

Definir estado de retransmissão

Por padrão, quando um usuário entra no portal de AWS acesso, escolhe uma conta e, em seguida, escolhe a função AWS criada a partir do conjunto de permissões atribuído, o IAM Identity Center redireciona o navegador do usuário para o. AWS Management Console Você pode alterar esse comportamento configurando o estado de retransmissão para um URL diferente do console. A configuração do estado de retransmissão permite que você forneça ao usuário acesso rápido ao console mais apropriado para sua função. Por exemplo, você pode definir o estado de retransmissão para o URL do console do Amazon EC2 (**`https://console.aws.amazon.com/ec2/`**), redirecionando o usuário para esse console quando ele escolher a função de administrador do Amazon EC2. Durante o redirecionamento para o URL padrão ou URL do estado de retransmissão, o IAM Identity Center direciona o navegador do usuário para o endpoint do console na última vez em que o usuário Região da AWS usou. Por exemplo, se um usuário encerrou sua última sessão de console na região da Europa (Estocolmo) (eu-north-1), o usuário será redirecionado para o console do Amazon EC2 nessa região.



Para configurar o IAM Identity Center e fazer com que ele redirecione o usuário para um console em uma Região da AWS específica, inclua a especificação da região como parte do URL. Por exemplo, para redirecionar o usuário para o console do Amazon EC2 na região Leste dos EUA (Ohio) (us-east-2), especifique o URL do console do Amazon EC2 nessa região (**`https://us-east-2.console.aws.amazon.com/ec2/`**). Se você habilitou o IAM Identify Center na região Oeste dos EUA (Oregon) (us-west-2) e quiser direcionar o usuário para essa região, especifique. **`https://us-west-2.console.aws.amazon.com`**

Use o procedimento a seguir para configurar o URL do estado de retransmissão de um conjunto de permissões.

Para configurar o estado de retransmissão

1. Abra o console do IAM Identity Center.
2. Em Permissões de várias contas, escolha Conjuntos de permissões.
3. Escolha o nome do conjunto de permissões para o qual deseja definir o novo URL do estado de retransmissão.
4. Na página de detalhes do conjunto de permissões, à direita do título da seção Configurações gerais, escolha Editar.

5. Na página Editar configurações gerais do conjunto de permissões, em Estado de retransmissão, digite uma URL do console para qualquer um dos AWS serviços. Por exemplo: .

   `https://console.aws.amazon.com/ec2/`

   > **Note**
   >
   > O URL do estado de retransmissão deve estar dentro do AWS Management Console.

6. Se o conjunto de permissões for provisionado em alguma Contas da AWS, os nomes das contas aparecerão abaixo Contas da AWS para reprovisionamento automático. Depois que a URL do estado de retransmissão do conjunto de permissões for atualizada, todos os Contas da AWS que usam o conjunto de permissões serão reprovisionados. Isso significa que o novo valor dessa configuração é aplicado a todos Contas da AWS que usam o conjunto de permissões.
7. Escolha Salvar alterações.
8. Na parte superior da página da Organização AWS , uma notificação é exibida.

   - Se o conjunto de permissões for provisionado em uma ou mais Contas da AWS, a notificação confirma que as Contas da AWS foram reprovisionadas com êxito e que o conjunto de permissões atualizado foi aplicado às contas.
   - Se o conjunto de permissões não estiver provisionado em um Conta da AWS, a notificação confirma que as configurações do conjunto de permissões foram atualizadas.

> **Note**
>
> Você pode automatizar esse processo usando a AWS API, um AWS SDK ou o AWS Command Line Interface()AWS CLI. Para obter mais informações, consulte:
>
> - As ações `CreatePermissionSet` ou `UpdatePermissionSet` na referência de API do IAM Identity Center
> - Os comandos `create-permission-set` ou `update-permission-set` na seção sso-admin da Referência de Comandos AWS CLI .

Use uma política de negação para revogar as permissões ativas do usuário

Talvez seja necessário revogar o acesso de um usuário do IAM Identity Center Contas da AWS enquanto o usuário estiver usando ativamente um conjunto de permissões. Você pode remover a capacidade deles de usar suas sessões ativas de função do IAM implementando uma política de negação para um usuário não especificado com antecedência e, quando necessário, você pode atualizar a política de negação para especificar o usuário cujo acesso você deseja bloquear. Este tópico explica como criar uma política de negação e considerações sobre como implantá-la.

Prepare-se para revogar uma sessão de função ativa do IAM criada por um conjunto de permissões

Você pode impedir que o usuário execute ações com uma função do IAM que está usando ativamente aplicando uma política de negação de tudo para um usuário específico por meio do uso de uma Política de Controle de Serviços. Você também pode impedir que um usuário use qualquer conjunto de permissões até que você altere sua senha, o que remove o mau uso ativo de credenciais roubadas. Se você precisar negar o acesso amplamente e impedir que um usuário entre novamente em um conjunto de permissões ou acesse outros conjuntos de permissões, você também pode remover todo o acesso do usuário, interromper a sessão ativa do portal de AWS acesso e desativar o login do usuário. Consulte Revogar sessões de função ativas do IAM criadas por conjuntos de permissões para saber como usar a política de negação em conjunto com ações adicionais para uma revogação de acesso mais ampla.

Política de negação

Você pode usar uma política de negação com uma condição que corresponda à do usuário `UserID` do repositório de identidades do IAM Identity Center para evitar outras ações de uma função do IAM que o usuário está usando ativamente. O uso dessa política evita o impacto em outros usuários que possam estar usando o mesmo conjunto de permissões quando você implanta a política Negar. Essa política usa a ID de usuário do espaço reservado *`Add user ID here`*,, para `"identitystore:userId"` que você atualize com a ID de usuário à qual deseja revogar o acesso.

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

```
            "Condition": {
                "StringEquals": {
                    "identitystore:userId": "Add user ID here"
                }
            }
        }
    ]
}
```

Embora você possa usar outra chave de condição“`aws:userId`”, como, “`identitystore:userId`” é certa porque é um valor globalmente exclusivo associado a uma pessoa. O uso “`aws:userId`” na condição pode ser afetado pela forma como os atributos do usuário são sincronizados a partir de sua fonte de identidades e pode ser alterado se o nome de usuário ou endereço de e-mail do usuário forem alterados.

No console do IAM Identity Center, você pode encontrar um usuário `identitystore:userId` navegando até Usuários, pesquisando o usuário pelo nome, expandindo a seção Informações gerais e copiando o ID do usuário. Também é conveniente interromper a sessão do portal de AWS acesso de um usuário e desativar seu acesso de login na mesma seção ao pesquisar a ID do usuário. Você pode automatizar o processo para criar uma política de negação obtendo o ID de usuário do usuário consultando as APIs do repositório de identidades.

Implantando a política de negação

Você pode usar uma ID de usuário de espaço reservado que não seja válida, por exemplo*`Add user ID here`*, para implantar a política de negação com antecedência usando uma Política de Controle de Serviços (SCP) que você anexa aos Contas da AWS usuários que possam ter acesso. Essa é a abordagem recomendada por sua facilidade e velocidade de impacto. Ao revogar o acesso de um usuário com a política Negar, você editará a política para substituir a ID de usuário do espaço reservado pela ID de usuário da pessoa cujo acesso você deseja revogar. Isso impede que o usuário realize qualquer ação com qualquer permissão definida em todas as contas às quais você anexa ao SCP. Ele bloqueia as ações do usuário mesmo que ele use sua sessão ativa do portal de AWS acesso para navegar até contas diferentes e assumir funções diferentes. Com o acesso do usuário totalmente bloqueado pelo SCP, você pode então desativar sua capacidade de entrar, revogar suas atribuições e interromper a sessão do portal de AWS acesso, se necessário.

Como alternativa ao uso de SCPs, você também pode incluir a política Deny na política embutida de conjuntos de permissões e nas políticas gerenciadas pelo cliente que são usadas pelos conjuntos de permissões que o usuário pode acessar.

Se você precisar revogar o acesso de mais de uma pessoa, poderá usar uma lista de valores no bloco de condições, como:

```
        "Condition": {
                "StringEquals": {
                    "identitystore:userId": [" user1 userId", "user2 userId"...]
                    }
    }
```

> **Important**
>
> Independentemente do (s) método (s) usado (s), você deve tomar qualquer outra ação corretiva e manter a ID do usuário na política por pelo menos 12 horas. Após esse período, todas as funções assumidas pelo usuário expiram e você pode então remover o ID de usuário da política de negação.

Referenciando conjuntos de permissões em políticas de recursos, Amazon EKS e AWS KMS

Quando você atribui um conjunto de permissões a uma AWS conta, o IAM Identity Center cria uma função com um nome que começa com`AWSReservedSSO_`.

O nome completo e o Nome de recurso da Amazon (ARN) da função usam o seguinte formato:

Nome	ARN
`AWSReservedSSO_` *`permission-set-name_unique-suffix`*	`arn:aws:iam::` *`aws-account-ID`*`:role/aws-reserved/sso.amazonaws.com/` *`aws-region`* `/AWSReservedSSO_` *`permission-set-name_unique-suffix`*

Por exemplo, se você criar um conjunto de permissões que conceda acesso à AWS conta aos administradores do banco de dados, uma função correspondente será criada com o seguinte nome e ARN:

Nome	ARN
`AWSReservedSSO_DatabaseAdministrator_1234567890abcdef`	`arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef`

Se você excluir todas as atribuições desse conjunto de permissões na AWS conta, a função correspondente criada pelo IAM Identity Center também será excluída. Se você fizer uma nova atribuição ao mesmo conjunto de permissões posteriormente, o IAM Identity Center criará uma nova função para o conjunto de permissões. O nome e o ARN da nova função incluem um sufixo diferente e exclusivo. Neste exemplo, o sufixo exclusivo é abcdef0123456789.

Nome	ARN
`AWSReservedSSO_DatabaseAdministrator_` **`abcdef0123456789`**	`arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_` **`abcdef0123456789`**

A alteração do sufixo no novo nome e no ARN da função fará com que todas as políticas que façam referência ao nome e ao ARN originais out-of-date sejam, o que interrompe o acesso de indivíduos que usam o conjunto de permissões correspondente. Por exemplo, uma alteração no ARN da função interromperá o acesso dos usuários do conjunto de permissões se o ARN original for referenciado nas seguintes configurações:

- No arquivo do `aws-auth ConfigMap` para o Amazon Elastic Kubernetes Service (Amazon EKS)
- Em uma política baseada em recursos para uma chave AWS Key Management Service (AWS KMS). Essa política também é referenciada como política de chave.

Embora você possa atualizar as políticas baseadas em recursos para a maioria dos AWS serviços para fazer referência a um novo ARN para uma função que corresponda a um conjunto de permissões, você deve ter uma função de backup criada no IAM para o Amazon EKS e se AWS

KMS o ARN mudar. Para o Amazon EKS, a função de backup do IAM deve existir no `aws-auth ConfigMap`. No AWS KMS, ele deve existir em suas principais políticas. Se você não tiver uma função do IAM de backup em nenhum dos casos, entre em contato com AWS Support.

Recomendações para evitar interrupções no acesso

Para evitar interrupções no acesso devido a alterações no ARN de uma função que corresponda a um conjunto de permissões, recomendamos que você faça o seguinte.

- Mantenha pelo menos uma atribuição de conjunto de permissões.

  Mantenha essa atribuição nas AWS contas que contêm as funções às quais você faz referência `aws-auth ConfigMap` para o Amazon EKS, as principais políticas ou as políticas baseadas em AWS KMS recursos para outras. Serviços da AWS

  Por exemplo, se você criar um conjunto de `EKSAccess` permissões e referenciar o ARN da função correspondente a partir da AWS conta`111122223333`, atribua permanentemente um grupo administrativo ao conjunto de permissões dessa conta. Como a atribuição é permanente, o IAM Identity Center não excluirá a função correspondente, o que elimina o risco de renomeação. O grupo administrativo sempre terá acesso sem o risco de escalação de privilégios.
- Para Amazon EKS e AWS KMS: Inclua uma função criada no IAM.

  Se você fizer referência a ARNs de função para conjuntos de permissões em um `aws-auth ConfigMap` no cluster do Amazon EKS ou em políticas de chaves para chaves AWS KMS , recomendamos que você também inclua pelo menos uma função criada no IAM. A função deve permitir que você acesse o cluster do Amazon EKS ou gerencie a política de AWS KMS chaves. O conjunto de permissões deve ser capaz de assumir essa função. Dessa forma, se o ARN da função de um conjunto de permissões mudar, você poderá atualizar a referência ao ARN na política de chave ou. `aws-auth ConfigMap` AWS KMS A próxima seção fornece um exemplo de como você pode criar uma política de confiança para uma função criada no IAM. A função só pode ser assumida por um conjunto de permissões `AdministratorAccess`.

Exemplos de políticas personalizadas

Veja a seguir um exemplo de uma política de confiança personalizada que fornece um conjunto de `AdministratorAccess` permissões com acesso a uma função criada no IAM. Os principais elementos dessa política incluem:

- O elemento principal dessa política de confiança especifica o principal AWS da conta. Nessa política, os diretores da AWS conta `111122223333` com `sts:AssumeRole` permissões podem assumir a função criada no IAM.
- O `Condition element` dessa política de confiança especifica requisitos adicionais para elementos principais que podem assumir a função criada no IAM. Nessa política, o conjunto de permissões com o seguinte ARN do perfil pode assumir a função.

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/
AWSReservedSSO_AdministratorAccess_*"
```

> **Note**
>
> O elemento `Condition` inclui o operador de condição `ArnLike` e usa um caractere curinga no final do ARN do perfil do conjunto de permissões, em vez de um sufixo exclusivo. Isso significa que a política permite que o conjunto de permissões assuma a função criada no IAM, mesmo que o ARN da função do conjunto de permissões mude.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/aws-reserved/
sso.amazonaws.com/eu-west-2/AWSReservedSSO_AdministratorAccess_*"
        }
      }
    }
  ]
}
```

Incluir uma função que você cria no IAM em tal política fornecerá acesso emergencial aos seus clusters do Amazon EKS ou a outros AWS recursos se um conjunto de permissões ou todas as

atribuições ao conjunto de permissões forem excluídas e recriadas acidentalmente. AWS KMS keys

Controle de acesso baseado em atributos

O controle de acesso baseado em atributo (Attribute-based access control, ABAC) é uma estratégia de autorização que define permissões com base em atributos. Você pode usar o IAM Identity Center para gerenciar o acesso aos seus AWS recursos em vários Contas da AWS atributos de usuário provenientes de qualquer fonte de identidade do IAM Identity Center. Em AWS, esses atributos são chamados de tags. Usar atributos de usuário como tags AWS ajuda a simplificar o processo de criação de permissões refinadas AWS e garante que sua força de trabalho tenha acesso somente aos AWS recursos com tags correspondentes.

Por exemplo, você pode atribuir aos desenvolvedores Bob e Sally, que são de duas equipes diferentes, o mesmo conjunto de permissões no IAM Identity Center e, em seguida, selecionar o atributo do nome da equipe para controle de acesso. Quando Bob e Sally fazem login Contas da AWS, o IAM Identity Center envia o atributo de nome da equipe na AWS sessão para que Bob e Sally possam acessar os recursos do AWS projeto somente se o atributo do nome da equipe corresponder à tag do nome da equipe no recurso do projeto. Caso Bob se mude para a equipe de Sally futuramente, você poderá modificar o acesso dele simplesmente atualizando o atributo do nome da equipe no diretório corporativo. Na próxima vez que Bob fizer login, ele terá acesso automático aos recursos do projeto de sua nova equipe sem exigir nenhuma atualização de permissões no AWS.

Essa abordagem também ajuda a reduzir o número de permissões distintas que você precisa criar e gerenciar no IAM Identity Center, pois os usuários associados aos mesmos conjuntos de permissões agora podem ter permissões exclusivas com base em seus atributos. Você pode usar esses atributos de usuário nos conjuntos de permissões e nas políticas baseadas em recursos do IAM Identity Center para implementar o ABAC em AWS recursos e simplificar o gerenciamento de permissões em grande escala.

Benefícios

Veja a seguir outros benefícios de usar o ABAC no IAM Identify Center.

- O ABAC exige menos conjuntos de permissões — como não é necessário criar políticas diferentes para funções de trabalho diferentes, você cria menos conjuntos de permissões. Isso reduz a complexidade do gerenciamento de permissões.

- Usando o ABAC, as equipes podem mudar e crescer rapidamente — as permissões para novos recursos são concedidas automaticamente com base nos atributos quando os recursos são devidamente marcados na criação.
- Use atributos de funcionários do seu diretório corporativo com o ABAC — Você pode usar atributos de funcionários existentes de qualquer fonte de identidade configurada no IAM Identity Center para tomar decisões de controle de acesso no AWS.
- Rastreie quem está acessando os recursos — Os administradores de segurança podem determinar facilmente a identidade de uma sessão revisando os atributos do usuário AWS CloudTrail para rastrear a atividade do usuário em. AWS

Para obter informações sobre como configurar o ABAC usando o console do IAM Identify Center, consulteAtributos para controle de acesso. Para obter informações sobre como habilitar e configurar o ABAC usando as APIs do IAM Identity Center, consulte CreateInstanceAccessControlAttributeConfigurationo Guia de referência da API do IAM Identity Center.

Tópicos

- Lista de verificação: Configurando o ABAC AWS usando o IAM Identity Center
- Atributos para controle de acesso

Lista de verificação: Configurando o ABAC AWS usando o IAM Identity Center

Essa lista de verificação inclui as tarefas de configuração necessárias para preparar seus recursos AWS e configurar o IAM Identity Center para acesso ao ABAC. Conclua as tarefas nesta lista de verificação em ordem. Quando um link de referência levar você a um tópico, retorne a esse tópico para poder continuar com as tarefas restantes nesta lista de verificação.

Etapa	Tarefa	Referência
1	Veja como adicionar tags a todos os seus AWS recursos. Para implementar o ABAC no IAM Identity Center, primeiro você precisará adicionar tags a todos os seus recursos AWS para os quais deseja implement ar o ABAC.	• Recursos de marcação AWS

Etapa	Tarefa	Referência
2	Analise como configurar sua fonte de identidade no IAM Identity Center com as identidades e atributos de usuário associados em seu repositório de identidades. O IAM Identity Center permite que você use atributos de usuário de qualquer fonte de identidade do IAM Identity Center compatível para ABAC em AWS.	• Gerencie sua fonte de identidade
3	Com base nos critérios a seguir, determine quais atributos você deseja usar para tomar decisões de controle de acesso AWS e envie-os para o IAM Identity Center.	• Conceitos básicos
	• Se você estiver usando um provedor de identidad e externo (IdP), decida se deseja usar atributos passados do IdP ou selecionar atributos do IAM Identity Center.	• Escolher atributos ao usar um provedor de identidad e externo como origem de identidade
	• Se você escolher fazer com que seu IdP envie atributos, configure seu IdP para transmitir os atributos nas asserções do SAML. Consulte as `Optional` seções do tutorial para seu IdP específic o.	• Tutoriais de introdução
	• Se você usar um IdP como fonte de identidade e optar por selecionar atributos no IAM Identity Center, investigue como configurar o SCIM para que os valores de atributos venham do seu IdP. Se você não puder usar o SCIM com seu IdP, adicione os usuários e seus atributos usando a página de usuário do console do IAM Identity Center.	• Provisionamento automático • Atributos de provedor de identidade externo compatíveis

Etapa	Tarefa	Referência
	• Se você usa o Active Directory ou o IAM Identity Center como sua fonte de identidade, ou usa um IdP e opta por selecionar atributos no IAM Identity Center, revise os atributos disponíveis que você pode configurar. Em seguida, siga imediatamente até a etapa 4 para começar a configurar seus atributos ABAC usando o console do IAM Identity Center.	• Escolha de atributos ao usar o IAM Identity Center como sua origem de identidade • Escolha de atributos ao usar AWS Managed Microsoft AD como origem de identidade • Mapeamentos padrão
4	Selecione os atributos a serem usados para o ABAC usando a página Atributos para controle de acesso no console do IAM Identity Center. Nessa página, você pode selecionar atributos para controle de acesso na fonte de identidade que você configurou na etapa 2. Depois que suas identidades e seus atributos estiverem no IAM Identity Center, você deverá criar pares de valores-chave (mapeamentos) que serão passados para você Contas da AWS para uso em decisões de controle de acesso.	• Habilite e configure atributos para controle de acesso
5	Crie políticas de permissões personalizadas em seu conjunto de permissões e use atributos de controle de acesso para criar regras ABAC para que os usuários só possam acessar recursos com tags correspondentes. Os atributos do usuário que você configurou na etapa 4 são usados como tags no AWS nas decisões de controle de acesso. Você pode consultar os atributos de controle de acesso na política de permissões usando a condição `aws:PrincipalTag/key` .	• Criar políticas de permissão para ABAC no IAM Identify Center
6	Em seus vários Contas da AWS, atribua usuários aos conjuntos de permissões que você criou na etapa 5. Isso garante que, ao se federarem em suas contas e acessarem AWS recursos, eles só tenham acesso com base nas tags correspondentes.	• Atribuir acesso de usuário a Contas da AWS

Depois de concluir essas etapas, os usuários que se federarem Conta da AWS usando o login único terão acesso aos AWS recursos com base nos atributos correspondentes.

Atributos para controle de acesso

Atributos para controle de acesso é o nome da página no console do IAM Identity Center em que você seleciona os atributos do usuário que deseja usar nas políticas para controlar o acesso aos recursos. Você pode atribuir usuários às cargas de trabalho AWS com base nos atributos existentes na fonte de identidade dos usuários.

Por exemplo, suponha que você deseje atribuir acesso aos buckets do S3 com base nos nomes de departamento. Na página Atributos para controle de acesso, selecione o atributo de usuário do Departamento para uso com controle de acesso por atributo (ABAC). No conjunto de permissões do IAM Identity Center, você então escreve uma política que conceda acesso aos usuários somente quando o atributo Departamento corresponder à tag de departamento que você atribuiu aos seus buckets do S3. O IAM Identity Center passa o atributo de departamento do usuário para a conta que está sendo acessada. O atributo é então usado para determinar o acesso com base na política. Para ter mais informações sobre o ABAC, consulte Controle de acesso baseado em atributos.

Conceitos básicos

A forma como você começa a configurar atributos para controle de acesso depende da origem de identidade que você está usando. Independentemente da origem de identidade escolhida, depois de selecionar seus atributos, você precisa criar ou editar políticas de conjunto de permissões. Essas políticas devem conceder às identidades dos usuários acesso aos recursos AWS .

Escolha de atributos ao usar o IAM Identity Center como sua origem de identidade

Ao configurar o IAM Identity Center como origem de identidade, primeiro você adiciona usuários e configura seus atributos. Em seguida, navegue até a página Atributos para controle de acesso e selecione os atributos que você deseja usar nas políticas. Por fim, navegue até a página Contas da AWS para criar ou editar conjuntos de permissões para usar os atributos do ABAC.

Escolha de atributos ao usar AWS Managed Microsoft AD como origem de identidade

Ao configurar o IAM Identity Center AWS Managed Microsoft AD como sua fonte de identidade, primeiro mapeie um conjunto de atributos do Active Directory para os atributos do usuário no IAM Identity Center. Em seguida, navegue até a página Atributos para controle de acesso. Em seguida, escolha quais atributos usar em sua configuração ABAC com base no conjunto existente de atributos

de SSO mapeados do Active Directory. Por fim, crie regras ABAC usando os atributos de controle de acesso nos conjuntos de permissões para conceder às identidades dos usuários acesso aos recursos AWS . Para obter uma lista dos mapeamentos padrão dos atributos do usuário no IAM Identity Center para os atributos do usuário em seu AWS Managed Microsoft AD diretório, consulte. Mapeamentos padrão

Escolher atributos ao usar um provedor de identidade externo como origem de identidade

Quando você configura o IAM Identity Center com um provedor de identidade externo (IdP) como sua origem de identidade, há duas maneiras de usar atributos para o ABAC.

- Você pode configurar seu IdP para enviar os atributos por meio de asserções do SAML. Nesse caso, o IAM Identity Center passa o nome e o valor do atributo do IdP para avaliação da política.

  > **Note**
  >
  > Os atributos nas asserções do SAML não estarão visíveis para você na página Atributos para controle de acesso. Você precisará conhecer esses atributos com antecedência e adicioná-los às regras de controle de acesso ao criar políticas. Se você decidir confiar em seus atributos externos IdPs , esses atributos sempre serão transmitidos quando os usuários se federarem Contas da AWS. Em cenários em que os mesmos atributos estão chegando ao IAM Identity Center por meio de SAML e SCIM, o valor dos atributos SAML tem precedência nas decisões de controle de acesso.

- Você pode configurar quais atributos usar na página Atributos para controle de acesso no console do IAM Identity Center. Os valores de atributos escolhidos aqui substituem os valores de qualquer atributo correspondente proveniente de um IdP por meio de uma declaração. Dependendo se você estiver usando o SCIM, considere o seguinte:
  - Se estiver usando o SCIM, o IdP sincroniza automaticamente os valores dos atributos no IAM Identity Center. Atributos adicionais necessários para o controle de acesso podem não estar presentes na lista de atributos do SCIM. Nesse caso, considere colaborar com o administrador de TI em seu IdP para enviar esses atributos ao IAM Identity Center por meio de declarações SAML usando o prefixo `https://aws.amazon.com/SAML/Attributes/AccessControl:` necessário. Para obter informações sobre como configurar atributos de usuário para controle de acesso em seu IdP para envio por meio de asserções SAML, consulte para Tutoriais de introdução seu IdP.
  - Se você não estiver usando o SCIM, deverá adicionar manualmente os usuários e definir seus atributos, como se estivesse usando o IAM Identity Center como origem de identidade. Em

seguida, navegue até a página Atributos para controle de acesso e escolha os atributos que você deseja usar nas políticas.

Para obter uma lista completa de atributos compatíveis entre atributos de usuário no IAM Identity Center e atributos de usuário externos IdPs, consulteAtributos de provedor de identidade externo compatíveis.

Para começar a usar o ABAC no IAM Identify Center, consulte os tópicos a seguir.

Tópicos

- Habilite e configure atributos para controle de acesso
- Criar políticas de permissão para ABAC no IAM Identify Center

Habilite e configure atributos para controle de acesso

Para usar o ABAC em todos os casos, você deve primeiro habilitar o ABAC usando o console do IAM Identity Center ou a API do IAM Identity Center. Se você escolher usar o IAM Identity Center para selecionar atributos, use a página Atributos para controle de acesso no console do IAM Identity Center ou a API do IAM Identity Center. Se você usa o provedor de identidade externo (IdP) como origem de identidade e opta por enviar atributos por meio das asserções do SAML, configure seu IdP para passar os atributos. Se uma asserção SAML passar qualquer um desses atributos, o IAM Identity Center substituirá o valor do atributo pelo valor encontrado no armazenamento de identidades do IAM Identity Center. Somente atributos configurados no IAM Identity Center serão enviados para tomar decisões de controle de acesso quando os usuários se federarem em suas contas.

> **Note**
>
> Você não pode visualizar atributos configurados e enviados por um IdP externo na página Atributos para controle de acesso no console do IAM Identity Center. Se você estiver transmitindo atributos de controle de acesso nas asserções do SAML do seu IdP externo, esses atributos serão enviados diretamente para o Conta da AWS quando os usuários se federarem. Os atributos não estarão disponíveis no IAM Identity Center para mapeamento.

Desabilitar atributos para controle de acesso

Use o seguinte procedimento para ativar o recurso de controle de atributos de acesso (ABAC) usando o console do IAM Identity Center.

> **Note**
>
> Se você tem conjuntos de permissões existentes e planeja habilitar o ABAC em sua instância do IAM Identity Center, restrições de segurança adicionais exigem que você primeiro tenha a política `iam:UpdateAssumeRolePolicy`. Essas restrições de segurança adicionais não são obrigatórias se você não tiver nenhum conjunto de permissões criado em sua conta.

Atributos para controle de acesso

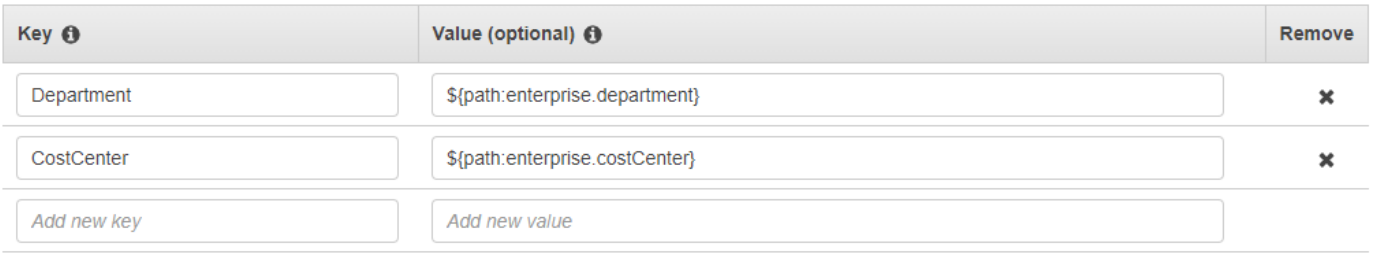
1. Abra o console do IAM Identity Center.
2. Escolha Configurações.
3. Na página de Configurações, localize a caixa Atributos para informações de controle de acesso e escolha Habilitar. Continue com o próximo procedimento para configurá-lo.

Selecione seus atributos

Use o procedimento a seguir para configurar atributos para sua configuração de ABAC.

Para selecionar seus atributos usando o console do IAM Identity Center

1. Abra o console do IAM Identity Center.
2. Escolha Configurações.
3. Na página Configurações, escolha a guia Atributos para controle de acesso e, em seguida, escolha Gerenciar atributos.
4. Na página Atributos para controle de acesso, escolha Adicionar atributo e insira os detalhes da chave e do valor. É aqui que você mapeará o atributo proveniente da sua origem de identidade para um atributo que o IAM Identity Center passa como uma tag de sessão.



A chave representa o nome que você está dando ao atributo para uso em políticas. Pode ser qualquer nome arbitrário, mas você precisa especificar esse nome exato nas políticas que você cria para controle de acesso. Por exemplo, digamos que você esteja usando Okta (um IdP externo) como sua fonte de identidade e precise transmitir os dados do centro de custos da sua organização como tags de sessão. Em Chave, você inseriria um nome com a mesma correspondência, CostCentercomo o nome da sua chave. É importante observar que, seja qual for o nome que você escolher aqui, ele também deve ter o mesmo nome em seu Chave da condição aws:PrincipalTag (ou seja, `"ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"`).

> **Note**
>
> Use um atributo de valor único para sua chave, por exemplo, **`Manager`**. O IAM Identity Center não oferece suporte a atributos de vários valores para ABAC, por exemplo, **`Manager, IT Systems`**.

O valor representa o conteúdo do atributo proveniente da sua fonte de identidade configurada. Aqui você pode inserir qualquer valor da tabela de origem de identidade apropriada listada em Mapeamentos de atributos para diretório AWS Managed Microsoft AD. Por exemplo, usando o contexto fornecido no exemplo mencionado acima, você analisaria a lista de atributos de IdP suportados e determinaria que a correspondência mais próxima de um atributo suportado seria **`${path:enterprise.costCenter}`** e, em seguida, iria inseri-la no campo Valor. Consulte a captura de tela fornecida acima para referência. Observe que você não pode usar valores de atributos externos do IdP fora dessa lista para o ABAC, a menos que use a opção de transmitir atributos por meio da asserção SAML.

5. Escolha Salvar alterações.

Agora que você configurou o mapeamento de seus atributos de controle de acesso, você precisa concluir o processo de configuração do ABAC. Para fazer isso, crie suas regras ABAC e adicione-

as aos seus conjuntos de permissões e/ou políticas baseadas em recursos. Isso é necessário para que você possa conceder acesso aos recursos AWS às identidades dos usuários. Para ter mais informações, consulte Criar políticas de permissão para ABAC no IAM Identify Center.

Desabilitar atributos para controle de acesso

Use o procedimento a seguir para desativar o recurso ABAC e excluir todos os mapeamentos de atributos que foram configurados.

Para desabilitar atributos para controle de acesso

1. Abra o console do IAM Identity Center.
2. Escolha Configurações.
3. Na página de Configurações, escolha a guia Atributos para controle de acesso e, em seguida, escolha Desativar.
4. Na caixa de diálogo Desabilitar atributos para controle de acesso, revise as informações e, quando estiver pronto, insira EXCLUIR e escolha Confirmar.

> **Important**
>
> Essa etapa exclui todos os atributos que foram configurados. Depois de excluídos, quaisquer atributos recebidos de uma origem de identidade e quaisquer atributos personalizados que você tenha configurado anteriormente não serão transmitidos.

Criar políticas de permissão para ABAC no IAM Identify Center

Você pode criar políticas de permissões que determinam quem pode acessar seus recursos da AWS com base nos valores de atributo configurados. Quando você habilita o ABAC e especifica atributos, o IAM Identity Center passa para o IAM o valor do atributo do usuário autenticado para uso na avaliação de políticas.

Chave da condição aws:PrincipalTag

Você pode usar atributos de controle de acesso em seus conjuntos de permissões usando a chave de condição `aws:PrincipalTag` para criar regras de controle de acesso. Por exemplo, na política de confiança a seguir, você pode marcar todos os recursos da sua organização com seus respectivos centros de custo. Você também pode usar um único conjunto de permissões que conceda aos desenvolvedores acesso aos recursos do centro de custos. Agora, sempre que os

desenvolvedores se federarem na conta usando o login único e seu atributo de centro de custos, eles só têm acesso aos recursos em seus respectivos centros de custo. À medida que a equipe adiciona mais desenvolvedores e recursos ao projeto, você só precisa marcar os recursos com o centro de custos correto. Em seguida, você passa as informações do centro de custos na AWS sessão quando os desenvolvedores se Contas da AWS federam. Como resultado, à medida que a organização adiciona novos recursos e desenvolvedores ao centro de custos, os desenvolvedores podem gerenciar recursos alinhados a seus centros de custo sem precisar de nenhuma atualização de permissão.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"
                }
            }
        }
    ]
}
```

Para obter mais informações, consulte aws:PrincipalTag e EC2: Iniciar ou interromper instâncias com base na correspondência das tags principal e de recurso no Guia do usuário do IAM.

Se as políticas contiverem atributos inválidos em suas condições, a condição da política falhará e o acesso será negado. Para ter mais informações, consulte Erro “Ocorreu um erro inesperado” quando um usuário tenta fazer login usando um provedor de identidades externo.

Provedor de identidade do IAM;

Quando você adiciona acesso de login único a um Conta da AWS, o IAM Identity Center cria um provedor de identidade do IAM em cada um. Conta da AWS Os provedores de identidade do IAM ajudam a manter sua Conta da AWS segura, pois você não precisa distribuir ou incorporar credenciais de segurança de longo prazo, como chaves de acesso, na sua aplicação.

Reparar o provedor de identidade do IAM

Se você excluir ou modificar acidentalmente seu provedor de identidade, deverá reaplicar manualmente suas atribuições de usuário e grupo. Reaplicar suas atribuições de usuário e grupo recria o provedor de identidade. Para obter mais informações, consulte:

- Gerencie o acesso ao Contas da AWS
- Gerenciar o acesso a aplicações

Perfis vinculados ao serviço

Service-linked roles (funções vinculadas a serviços) são permissões predefinidas do IAM que autorizam o IAM Identity Center a determinar e impor quais usuários têm acesso SSO a contas específicas da Contas da AWS na respectiva organização da AWS Organizations. O serviço habilita essa funcionalidade provisionando uma função vinculada ao serviço em cada Conta da AWS uma de sua organização. O serviço então permite que outros AWS serviços, como o IAM Identity Center, aproveitem essas funções para realizar tarefas relacionadas ao serviço. Para obter mais informações, consulte AWS Organizations e funções vinculadas ao serviço.

Quando você ativa o IAM Identity Center, ele cria uma função vinculada ao serviço em todas as contas da organização em AWS Organizations. O IAM Identity Center também cria a mesma função vinculada ao serviço em todas as contas que são adicionadas posteriormente à sua organização. Essa função permite que o IAM Identify Center acesse os recursos de cada conta em seu nome. Para ter mais informações, consulte Gerencie o acesso ao Contas da AWS.

As funções vinculadas ao serviço que são criadas em cada uma Conta da AWS são nomeadas. `AWSServiceRoleForSSO` Para ter mais informações, consulte As funções vinculadas ao serviço do IAM Identity Center permanecem..

Gerenciar o acesso a aplicações

Com AWS IAM Identity Center, você pode controlar quem pode ter acesso com login único aos seus aplicativos. Os usuários obtêm facilmente acesso a essas aplicações depois que usam suas credenciais de diretório para fazer login.

O IAM Identity Center comunica-se com segurança com essas aplicações por meio de uma relação de confiança entre o IAM Identity Center e o provedor de serviços da aplicação. Essa confiança pode ser criada de maneiras diferentes, dependendo do tipo de aplicação.

O IAM Identity Center oferece suporte a dois tipos de aplicativos: aplicativos AWS gerenciados e aplicativos gerenciados pelo cliente. AWS os aplicativos gerenciados são configurados diretamente dos consoles de aplicativos relevantes ou por meio das APIs do aplicativo. As aplicações gerenciadas pelo cliente devem ser adicionadas ao IAM Identity Center e configuradas com os metadados apropriados tanto para o IAM Identity Center quanto para o provedor de serviços.

Depois de configurar as aplicações para que funcionem com o IAM Identity Center, você pode gerenciar quais usuários ou grupos têm acesso a elas. Por padrão, nenhum usuário é atribuído às aplicações.

Você também pode conceder aos seus funcionários acesso AWS Management Console ao formulário específico Conta da AWS em sua organização. Para ter mais informações, consulte Gerencie o acesso ao Contas da AWS.

Tópicos

AWS aplicativos gerenciados

AWS os aplicativos gerenciados se integram ao IAM Identity Center e podem usá-lo para serviços de autenticação e diretório.

A integração de aplicativos AWS gerenciados com o IAM Identity Center oferece um caminho mais fácil para atribuir acesso ao usuário, sem a necessidade de configurar uma federação separada ou sincronização de usuários e grupos para cada aplicativo. Você pode conectar a fonte de identidade que deseja usar para autenticação uma vez e receber uma visão única das atribuições de usuários e grupos. Os administradores dos aplicativos que permitem a propagação confiável de identidades podem definir e auditar o acesso aos recursos do aplicativo com base na associação de um usuário ou grupo de usuários, sem a necessidade de mapeá-los para funções do IAM.

AWS os aplicativos gerenciados fornecem uma interface de usuário administrativa que você pode usar para gerenciar o acesso aos recursos do aplicativo. Por exemplo, QuickSight os administradores podem designar usuários para acessar painéis com base na associação ao grupo. A maioria dos aplicativos AWS gerenciados também fornece uma AWS Management Console experiência que permite atribuir usuários ao aplicativo. A experiência do console para essas aplicações pode integrar ambas as funções, para combinar os recursos de atribuição de usuários com a capacidade de gerenciar o acesso aos recursos das aplicações.

AWS os aplicativos gerenciados integrados ao IAM Identity Center incluem:

AWS aplicativos gerenciados que se integram ao IAM Identity Center

AWS aplicativo gerenciado	Integrado com a instância organizacional do IAM Identity Center	Integrado com instâncias de conta do IAM Identity Center	Permite a propagação de identidade confiável por meio do IAM Identity Center
Amazon Athena SQL	S	S	Sim
Amazon CodeCatalyst	S	S	Não

AWS aplicativo gerenciado	Integrado com a instância organizacional do IAM Identity Center	Integrado com instâncias de conta do IAM Identity Center	Permite a propagação de identidade confiável por meio do IAM Identity Center
Notebooks Amazon EMR	 S	 N	 Não
Amazon EMR no Amazon EC2	 S	 S	 Sim
Amazon EMR Studio	 S	 S	 Sim
Amazon Kendra	 S	 N	 Não
Amazon Managed Grafana	 S	 N	 Não
Amazon Monitron	 S	 N	 Não
Amazon Nimble Studio	 S	 N	 Não

AWS aplicativo gerenciado	Integrado com a instância organizacional do IAM Identity Center	Integrado com instâncias de conta do IAM Identity Center	Permite a propagação de identidade confiável por meio do IAM Identity Center
Amazon Pinpoint	 S	 N	 Não
Amazon Q Business	 S	 S	 Não
Amazon Q Developer	 S	 S *	 Não
Amazon QuickSight	 S	 S	 Sim
Amazon Redshift	 S	 S	 Sim
Concessões de acesso ao Amazon S3	 S	 S	 Sim
SageMaker Estúdio Amazon	 S	 N	 Não

AWS aplicativo gerenciado	Integrado com a instância organizacional do IAM Identity Center	Integrado com instâncias de conta do IAM Identity Center	Permite a propagação de identidade confiável por meio do IAM Identity Center
Amazon WorkSpaces Web	 S	 N	 Não
AWS CLI	 S	 N	 Não
AWS Deadline Cloud	 S	 S	 Não
AWS IoT Events	 S	 N	 Não
AWS IoT Fleet Hub	 S	 N	 Não
AWS IoT SiteWise	 S	 N	 Não
AWS Lake Formation	 S	 S	 Sim

AWS aplicativo gerenciado	Integrado com a instância organizacional do IAM Identity Center	Integrado com instâncias de conta do IAM Identity Center	Permite a propagação de identidade confiável por meio do IAM Identity Center
Cadeia de Suprimentos AWS	 S	 N	 Não
AWS Systems Manager	 S	 N	 Não
Acesso Verificado pela AWS	 S	 N	 Não

* As instâncias de conta do IAM Identity Center são suportadas, a menos que seus usuários precisem acessar o Amazon Q no AWS console.

Tópicos

- Controlar o acesso
- Coordenar tarefas administrativas
- Configurar o IAM Identity Center para compartilhar informações de identidade
- Considerações sobre o compartilhamento de informações de identidade no Contas da AWS
- Habilitando sessões de console com reconhecimento de identidade
- Restringindo o uso de aplicativos AWS gerenciados
- Visualizar detalhes sobre uma aplicação gerenciada pela AWS
- Desabilitando um aplicativo AWS gerenciado

Controlar o acesso

O acesso aos aplicativos AWS gerenciados é controlado de duas maneiras:

- Entrada inicial na aplicação: o IAM Identity Center gerencia isso por meio de atribuições à aplicação. Por padrão, as atribuições são necessárias para aplicativos AWS gerenciados.
- Acesso aos recursos da aplicação: a aplicação gerencia isso por meio de atribuições dos recursos independentes que ela controla.

Coordenar tarefas administrativas

Se você for administrador da aplicação, poderá escolher se deseja exigir atribuições a uma aplicação. Se as atribuições forem necessárias, quando os usuários entrarem no portal de AWS acesso, somente os usuários atribuídos ao aplicativo diretamente ou por meio de uma atribuição em grupo poderão visualizar o mosaico do aplicativo. Como alternativa, se atribuições não forem exigidas, você poderá permitir que todos os usuários do IAM Identity Center façam login na aplicação. Nesse caso, o aplicativo gerencia o acesso aos recursos e o mosaico do aplicativo fica visível para todos os usuários que visitam o portal de AWS acesso.

Se você for administrador do IAM Identity Center, poderá usar o console do IAM Identity Center para remover atribuições aos aplicativos AWS gerenciados. Antes de remover as atribuições, recomendamos que você coordene com o administrador da aplicação. Você também deverá coordenar com o administrador da aplicação se planejar modificar a configuração que determina se as atribuições são exigidas ou automatizar as atribuições da aplicação.

Configurar o IAM Identity Center para compartilhar informações de identidade

Para habilitar esse recurso, o IAM Identity Center fornece um repositório de identidades que contém os atributos dos usuários e dos grupos, exceto as credenciais de login. Você pode usar qualquer um dos métodos a seguir para manter os usuários e grupos em seu armazenamento de identidades do IAM Identity Center atualizados:

- Use o armazenamento de identidades do IAM Identity Center como fonte de identidade principal. Se você escolher esse método, gerencie seus usuários, suas credenciais de login e grupos a partir do console do IAM Identity Center ou AWS Command Line Interface ().AWS CLI Para ter mais informações, consulte Gerencie identidades no IAM Identity Center.

- Configure o provisionamento (sincronização) de usuários e grupos provenientes de uma das seguintes fontes de identidade para seu armazenamento de identidades do IAM Identity Center:
  - Active Directory: para obter mais informações, consulte Conectar-se a um diretório Microsoft AD.
  - Provedor de identidades externo: para obter mais informações, consulte Conecte-se a um provedor de identidades externo.

  Se você escolher esse método de provisionamento, continuará gerenciando os usuários e grupos na fonte de identidades, e essas alterações serão sincronizadas com o repositório de identidades do IAM Identity Center.

Seja qual for a fonte de identidade escolhida, o IAM Identity Center pode compartilhar as informações do usuário e do grupo com aplicativos AWS gerenciados. Assim, você pode conectar uma fonte de identidades ao IAM Identity Center uma vez e depois compartilhar as informações de identidade com várias aplicações na Nuvem AWS. Isso elimina a necessidade de configurar a federação e o provisionamento de identidades com cada aplicação separadamente. Esse atributo de compartilhamento também facilita o acesso dos usuários de sua força de trabalho a muitas aplicações em diferentes Contas da AWS.

Considerações sobre o compartilhamento de informações de identidade no Contas da AWS

O IAM Identity Center é compatível com os atributos mais usados em todos as aplicações. Esses atributos incluem nome e sobrenome, número de telefone, endereço de e-mail, endereço e idioma preferido. Considere cuidadosamente quais aplicações e quais contas podem usar essas informações de identificação pessoal.

Você pode controlar o acesso a essas informações de duas maneiras. Você pode optar por ativar o acesso somente na conta AWS Organizations de gerenciamento ou em todas as contas em AWS Organizations. Ou pode usar políticas de controle de serviços (SCPs) para controlar quais aplicações podem acessar as informações em quais contas do AWS Organizations. Por exemplo, se você ativar o acesso somente na conta AWS Organizations de gerenciamento, os aplicativos nas contas dos membros não terão acesso às informações. No entanto, se você habilitar o acesso em todas as contas, poderá usar SCPs para proibir o acesso de todas as aplicações, exceto aquelas que você deseja permitir.

Habilitando sessões de console com reconhecimento de identidade

Uma sessão com reconhecimento de identidade para o console aprimora a sessão do AWS console do usuário, fornecendo algum contexto adicional para personalizar a experiência do usuário. Atualmente, esse recurso é suportado por usuários do Amazon Q no AWS console.

Você pode habilitar sessões de console com reconhecimento de identidade sem fazer nenhuma alteração nos padrões de acesso existentes ou na federação no AWS console hoje. Se seus usuários fizerem login no AWS console com o IAM (por exemplo, se fizerem login como usuários do IAM ou por meio de acesso federado com o IAM), eles poderão continuar usando esses métodos. Se seus usuários entrarem no portal de AWS acesso, eles poderão continuar usando suas credenciais de usuário do IAM Identity Center.

Tópicos

Pré-requisitos e considerações

Antes de habilitar as sessões de console com reconhecimento de identidade, analise os seguintes pré-requisitos e considerações:

- Você deve habilitar sessões de console com reconhecimento de identidade para usuários que precisam de acesso ao Amazon Q no AWS console.
- Atualmente, as sessões de console com reconhecimento de identidade só são suportadas para uso com o Amazon Q no AWS console.
- As sessões de console com reconhecimento de identidade exigem uma instância organizacional do IAM Identity Center.
- A integração com o Amazon Q não é suportada se você habilitar o IAM Identity Center em um opt-in Região da AWS.
- Depois de ativar as sessões de console com reconhecimento de identidade, você não poderá desativar esse recurso.
- Para habilitar sessões de console com reconhecimento de identidade, você deve ter as seguintes permissões:
  - `sso:CreateApplication`

- `sso:GetSharedSsoConfiguration`
- `sso:ListApplications`
- `sso:PutApplicationAssignmentConfiguration`
- `sso:PutApplicationAuthenticationMethod`
- `sso:PutApplicationGrant`
- `sso:PutApplicationAccessScope`
- `signin:CreateTrustedIdentityPropagationApplicationForConsole`
- `signin:ListTrustedIdentityPropagationApplicationForConsole`
-

- Para permitir que seus usuários usem sessões de console com reconhecimento de identidade, você deve conceder a eles a `sts:setContext` permissão em uma política baseada em identidade. Para obter informações, consulte Conceder permissões aos usuários para usar sessões de console com reconhecimento de identidade.

Como habilitar identity-aware-console sessões

Você pode habilitar sessões de console com reconhecimento de identidade no console Amazon Q ou no console do IAM Identity Center.

Habilite sessões de console com reconhecimento de identidade no console Amazon Q

Antes de habilitar sessões de console com reconhecimento de identidade, você deve ter uma instância organizacional do IAM Identity Center com uma fonte de identidade conectada. Se você já configurou o IAM Identity Center, vá para a etapa 3.

1. Abra o console do Centro de Identidade do IAM. Escolha Habilitar e crie uma instância organizacional do IAM Identity Center. Para mais informações, consulte Habilitando AWS IAM Identity Center.
2. Conecte sua fonte de identidade ao IAM Identity Center e provisione usuários ao IAM Identity Center. Você pode escolher o diretório padrão do IAM Identity Center como sua fonte de identidade ou usar outro provedor de identidade. Para ter mais informações, consulte Tutoriais de introdução.
3. Depois de concluir a configuração do IAM Identity Center, abra o console do Amazon Q e siga as etapas em Assinaturas no Amazon Q Developer User Guide. Certifique-se de ativar as sessões de console com reconhecimento de identidade.

> **Note**
>
> Se você não tiver permissões suficientes para habilitar sessões de console com reconhecimento de identidade, talvez seja necessário pedir a um administrador do IAM Identity Center que execute essa tarefa para você no console do IAM Identity Center. Para obter mais informações, consulte o próximo procedimento.

Habilite sessões de console com reconhecimento de identidade no console do IAM Identity Center

Se você for administrador do IAM Identity Center, outro administrador pode solicitar que você habilite sessões de console com reconhecimento de identidade no console do IAM Identity Center.

1. Abra o console do Centro de Identidade do IAM.
2. No painel de navegação, selecione Configurações.
3. Em Habilitar sessões com reconhecimento de identidade, escolha Ativar.
4. Na segunda mensagem, escolha Ativar.
5. Depois que você terminar de ativar as sessões de console com reconhecimento de identidade, uma mensagem de confirmação será exibida na parte superior da página Configurações.
6. Na seção Detalhes, o status das sessões com reconhecimento de identidade é Ativado.

Como funcionam as sessões de console com reconhecimento de identidade

Com sessões de console com reconhecimento de identidade, os usuários do Amazon Q no AWS console podem fazer login AWS, abrir o site AWS Management Console ou outro AWS site, escolher o ícone do Amazon Q e iniciar um bate-papo ou usar outros recursos compatíveis. Para obter mais informações, consulte o Guia do usuário do Amazon Q Developer.

O IAM Identity Center aprimora a sessão atual do console do usuário para incluir o ID do usuário ativo do IAM Identity Center e o ID da sessão do IAM Identity Center.

As sessões de console com reconhecimento de identidade incluem os três valores a seguir:

- ID do usuário do repositório de identidades (loja de identidades: UserId) - Esse valor é usado para identificar exclusivamente um usuário na fonte de identidade conectada ao IAM Identity Center.

- Diretório de armazenamento de identidades ARN (loja de identidades: IdentityStoreArn) - Esse valor é o ARN do repositório de identidades conectado ao IAM Identity Center e onde você pode pesquisar atributos. `identitystore:UserId`
- ID da sessão do IAM Identity Center - Esse valor indica se a sessão do IAM Identity Center do usuário ainda é válida.

Os valores são os mesmos, mas obtidos de maneiras diferentes e adicionados em diferentes pontos do processo, dependendo de como o usuário faz login:

- Centro de identidade do IAM (portal de AWS acesso): nesse caso, os valores de ID de usuário e ARN do repositório de identidades do usuário já são fornecidos na sessão ativa do IAM Identity Center. O IAM Identity Center aprimora a sessão atual adicionando somente o ID da sessão.
- Outros métodos de login: se o usuário fizer login AWS como usuário do IAM, com uma função do IAM ou como usuário federado com o IAM, nenhum desses valores será fornecido. O IAM Identity Center aprimora a sessão atual adicionando o ID do usuário do repositório de identidades, o ARN do diretório do repositório de identidades e o ID da sessão.

Restringindo o uso de aplicativos AWS gerenciados

Quando você ativa o IAM Identity Center pela primeira vez, AWS permite o uso automático de aplicativos AWS gerenciados em todas as contas do AWS Organizations. Para restringir aplicações, você deve implementar SCPs. Você pode usar SCPs para bloquear o acesso às informações de usuários e grupos do IAM Identity Center e para impedir que a aplicação seja iniciada, exceto nas contas designadas.

Visualizar detalhes sobre uma aplicação gerenciada pela AWS

Depois de conectar um aplicativo AWS gerenciado ao IAM Identity Center usando o console ou as APIs do aplicativo, o aplicativo é registrado no IAM Identity Center. Depois que uma aplicação é registrada no IAM Identity Center, você pode visualizar informações detalhadas sobre ela no console do IAM Identity Center.

Para visualizar informações sobre um aplicativo AWS gerenciado no console do IAM Identity Center

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Escolha a guia Aplicações gerenciadas pela AWS .

4. Na lista de aplicações, escolha o nome da aplicação sobre a qual você deseja visualizar informações detalhadas.
5. As informações sobre a aplicação incluem se as atribuições de usuários e grupos são exigidas e, se for o caso, os usuários e os grupos atribuídos e as aplicações confiáveis para a propagação de identidades. Para obter mais informações sobre a propagação de identidades confiáveis, consulte Trusted identity propagation across applications.

Desabilitando um aplicativo AWS gerenciado

Para impedir que os usuários se autentiquem em um aplicativo AWS gerenciado, você pode desativar o aplicativo no console do IAM Identity Center.

> **Warning**
>
> Desabilitar uma aplicação exclui todas as permissões de usuários dessa aplicação, a desconecta do IAM Identity Center e a torna inacessível. Se você for um administrador do IAM Identity Center, recomendamos que coordene com o administrador da aplicação antes de realizar essa tarefa.

Para desativar um aplicativo AWS gerenciado

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Na página Aplicações, em AWS Aplicações gerenciadas pela , escolha a aplicação que você deseja desabilitar.
4. Com a aplicação selecionada, escolha Ações e depois escolha Desabilitar.
5. Na caixa de diálogo Suspender aplicação, escolha Suspender.
6. Na lista Aplicações gerenciadas pela AWS , o status da aplicação aparece como Inativo.

Aplicações gerenciadas pelo cliente

Com o IAM Identity Center, você pode criar ou conectar usuários da força de trabalho e gerenciar centralmente seu acesso em todos os aplicativos Contas da AWS . O IAM Identity Center atua como um serviço central de identidades e oferece diferentes maneiras de autenticar usuários. Se você já

usar um provedor de identidades (IdP), o IAM Identity Center poderá se integrar ao seu IdP para que você possa provisionar usuários e grupos para o IAM Identity Center e usar o IdP para autenticação.

Se você usar aplicações gerenciadas pelo cliente compatíveis com o SAML 2.0, poderá federar seu IdP no IAM Identity Center por meio do SAML 2.0 e usar o IAM Identity Center para gerenciar o acesso dos usuários a essas aplicações. O IAM Identity Center fornece um catálogo das aplicações mais usadas que são compatíveis com o SAML 2.0, o Salesforce e o Microsoft 365. Esse catálogo está disponível no console do IAM Identity Center. Você também pode configurar seus próprios aplicativos SAML 2.0.

> **Note**
>
> Se você tem aplicativos gerenciados pelo cliente que oferecem suporte ao OAuth 2.0 e seus usuários precisam acessar esses aplicativos aos AWS serviços, você pode usar a propagação de identidade confiável. Com a propagação de identidade confiável, um usuário pode entrar em um aplicativo e esse aplicativo pode transmitir a identidade dos usuários em solicitações para acessar dados em AWS serviços. Para ter mais informações, consulte Usar a propagação de identidades confiáveis com aplicações gerenciadas pelo cliente.

Tópicos

SAML 2.0 e OAuth 2.0

O IAM Identity Center permite que você forneça aos usuários acesso de logon único às aplicações SAML 2.0 ou OAuth 2.0. Os tópicos a seguir fornecem uma visão geral de alto nível do SAML 2.0 e do OAuth 2.0.

Tópicos

SAML 2.0

O SAML 2.0 é um padrão do setor usado para a troca segura de asserções SAML que transmitem informações sobre um usuário entre uma autoridade SAML (chamada de provedor de identidades ou IdP) e um consumidor SAML 2.0 (denominado provedor de serviços ou SP). O IAM Identity Center usa essas informações para fornecer acesso federado de login único para os usuários autorizados a usar aplicativos no AWS portal de acesso.

OAuth 2.0

O OAuth 2.0 é um protocolo que permite que aplicações acessem e compartilhem dados do usuário com segurança sem compartilhar senhas. Esse recurso oferece uma maneira segura e padronizada para os usuários permitirem que as aplicações acessem seus recursos. O acesso é facilitado por diferentes fluxos de concessão do OAuth 2.0.

O IAM Identity Center permite que aplicativos executados em clientes públicos recuperem credenciais temporárias de acesso Contas da AWS e serviços de forma programática em nome de seus usuários. Os clientes públicos geralmente são desktops, laptops ou outros dispositivos móveis usados para executar aplicativos localmente. Exemplos de AWS aplicativos executados em clientes públicos incluem o AWS Command Line Interface (AWS CLI) e os kits AWS Toolkit de desenvolvimento AWS de software (SDKs). Para permitir que esses aplicativos obtenham credenciais, o IAM Identity Center oferece suporte a partes dos seguintes fluxos do OAuth 2.0:

- Concessão de código de autorização com chave de prova para troca de código (PKCE) (RFC 6749 e RFC 7636)
- Concessão de autorização de dispositivo (RFC 8628)

> **Note**
>
> Esses tipos de subsídios só podem ser usados com Serviços da AWS esse recurso. Esses serviços podem não oferecer suporte a esse tipo de subsídio em sua totalidade Regiões da AWS. Consulte a documentação relevante Serviços da AWS para diferenças regionais.

O OpenID Connect (OIDC) é um protocolo de autenticação baseado no OAuth 2.0 Framework. O OIDC especifica como usar o OAuth 2.0 para autenticação. Por meio das APIs do serviço OIDC do IAM Identity Center, um aplicativo registra um cliente OAuth 2.0 e usa um desses fluxos para obter um token de acesso que fornece permissões às APIs protegidas do IAM Identity Center.

Um aplicativo especifica os escopos de acesso para declarar o usuário pretendido da API. Depois que você, como administrador do IAM Identity Center, configurar sua fonte de identidade, os usuários finais do aplicativo devem concluir um processo de login, caso ainda não tenham feito isso. Seus usuários finais devem então fornecer seu consentimento para permitir que o aplicativo faça chamadas de API. Essas chamadas de API são feitas usando as permissões dos usuários. Em resposta, o IAM Identity Center retorna um token de acesso ao aplicativo que contém os escopos de acesso com os quais os usuários consentiram.

Usando um fluxo de concessão do OAuth 2.0

Os fluxos de concessão do OAuth 2.0 só estão disponíveis por meio de aplicativos AWS gerenciados que oferecem suporte aos fluxos. Para usar um fluxo do OAuth 2.0, sua instância do IAM Identity Center e todos os aplicativos AWS gerenciados compatíveis que você usa devem ser implantados em um único. Região da AWS Consulte a documentação de cada um AWS service (Serviço da AWS) para determinar a disponibilidade regional dos aplicativos AWS gerenciados e a instância do IAM Identity Center que você deseja usar.

Para usar um aplicativo que usa um fluxo OAuth 2.0, o usuário final deve inserir a URL em que o aplicativo se conectará e se registrará na sua instância do IAM Identity Center. Dependendo do aplicativo, como administrador, você deve fornecer aos usuários a URL do portal de AWS acesso ou a URL do emissor da sua instância do IAM Identity Center. Você pode encontrar essas duas configurações na página de configurações do console do IAM Identity Center. Para obter informações adicionais sobre a configuração de um aplicativo cliente, consulte a documentação desse aplicativo.

A experiência do usuário final ao entrar em um aplicativo e fornecer consentimento depende se o aplicativo usa o Concessão de código de autorização com PKCE ouConcessão de autorização de dispositivo.

Concessão de código de autorização com PKCE

Esse fluxo é usado por aplicativos executados em um dispositivo que tem um navegador.

1. Uma janela do navegador é aberta.
2. Se o usuário não tiver se autenticado, o navegador o redirecionará para concluir a autenticação do usuário.
3. Após a autenticação, o usuário recebe uma tela de consentimento que exibe as seguintes informações:

- O nome do aplicativo
- Os escopos de acesso que o aplicativo está solicitando consentimento para usar

4. O usuário pode cancelar o processo de consentimento ou dar seu consentimento e o aplicativo prossegue com o acesso com base nas permissões do usuário.

Concessão de autorização de dispositivo

Esse fluxo pode ser usado por aplicativos executados em um dispositivo com ou sem um navegador. Quando o aplicativo inicia o fluxo, ele apresenta uma URL e um código de usuário que o usuário deve verificar posteriormente no fluxo. O código do usuário é necessário porque o aplicativo que inicia o fluxo pode estar sendo executado em um dispositivo diferente daquele no qual o usuário fornece consentimento. O código garante que o usuário concorde com o fluxo iniciado no outro dispositivo.

1. Quando o fluxo é iniciado a partir de um dispositivo com um navegador, uma janela do navegador é aberta. Quando o fluxo é iniciado em um dispositivo sem um navegador, o usuário deve abrir um navegador em um dispositivo diferente e acessar a URL que o aplicativo apresentou.
2. Em ambos os casos, se o usuário não tiver se autenticado, o navegador o redirecionará para concluir a autenticação do usuário.
3. Após a autenticação, o usuário recebe uma tela de consentimento que exibe as seguintes informações:
   - O nome do aplicativo
   - Os escopos de acesso que o aplicativo está solicitando consentimento para usar
   - O código do usuário que o aplicativo apresentou ao usuário
4. O usuário pode cancelar o processo de consentimento ou dar seu consentimento e o aplicativo prossegue com o acesso com base nas permissões do usuário.

Escopos de acesso

Um escopo define o acesso a um serviço para um serviço que pode ser acessado por meio de um fluxo do OAuth 2.0. Os escopos são uma forma de o serviço, também chamado de servidor de recursos, agrupar permissões relacionadas às ações e aos recursos do serviço e especificam as operações granulares que os clientes do OAuth 2.0 podem solicitar. Quando um cliente OAuth 2.0 se registra no serviço OIDC do IAM Identity Center, o cliente especifica os escopos para declarar suas ações pretendidas, para as quais o usuário deve fornecer consentimento.

Os clientes do OAuth 2.0 usam `scope` valores conforme definido na seção 3.3 do OAuth 2.0 (RFC 6749) para especificar quais permissões estão sendo solicitadas para um token de acesso. Os clientes podem especificar no máximo 25 escopos ao solicitar um token de acesso. Quando um usuário fornece consentimento durante uma concessão de código de autorização com PKCE ou fluxo de concessão de autorização de dispositivo, o IAM Identity Center codifica os escopos no token de acesso que ele retorna.

AWS adiciona escopos ao IAM Identity Center para obter suporte Serviços da AWS. A tabela a seguir lista os escopos que o serviço IAM Identity Center OIDC suporta quando você registra um cliente público.

Escopos de acesso compatíveis com o serviço IAM Identity Center OIDC ao registrar um cliente público

Escopo	Descrição	Serviços com suporte de
`sso:account:access`	Acesse contas gerenciadas e conjuntos de permissões do IAM Identity Center.	IAM Identity Center
`codewhisperer:analysis`	Habilite o acesso à análise de código do Amazon Q Developer.	ID do builder AWS e o IAM Identity Center
`codewhisperer:completions`	Habilite o acesso às sugestões de código em linha do Amazon Q.	ID do builder AWS e o IAM Identity Center
`codewhisperer:conversations`	Habilite o acesso ao Amazon Q chat.	ID do builder AWS e o IAM Identity Center
`codewhisperer:taskassist`	Habilite o acesso ao Amazon Q Developer Agent para desenvolvimento de software.	ID do builder AWS e o IAM Identity Center
`codewhisperer:transformations`	Habilite o acesso ao Amazon Q Developer Agent para transformação de código.	ID do builder AWS e o IAM Identity Center

Escopo	Descrição	Serviços com suporte de
`codecatalyst:read_write`	Leia e grave em seus CodeCatalyst recursos da Amazon, permitindo acesso a todos os seus recursos existentes.	ID do builder AWS e o IAM Identity Center

Configurar aplicações SAML 2.0 gerenciadas pelo cliente

Se você usar aplicações gerenciadas pelo cliente compatíveis com o SAML 2.0, poderá federar seu IdP no IAM Identity Center por meio do SAML 2.0 e usar o IAM Identity Center para gerenciar o acesso dos usuários a essas aplicações. Você pode selecionar uma aplicação SAML 2.0 em um catálogo das aplicações mais usadas no console do IAM Identity Center ou configurar sua própria aplicação SAML 2.0.

> **Note**
>
> Se você tem aplicativos gerenciados pelo cliente que oferecem suporte ao OAuth 2.0 e seus usuários precisam acessar esses aplicativos aos AWS serviços, você pode usar a propagação de identidade confiável. Com a propagação de identidade confiável, um usuário pode entrar em um aplicativo e esse aplicativo pode transmitir a identidade dos usuários em solicitações para acessar dados em AWS serviços. Para ter mais informações, consulte Usar a propagação de identidades confiáveis com aplicações gerenciadas pelo cliente.

Tópicos

- Catálogo de aplicações do IAM Identity Center
- Configurar sua própria aplicação SAML 2.0

Catálogo de aplicações do IAM Identity Center

Você pode usar o catálogo de aplicações no console do IAM Identity Center para adicionar muitas aplicações SAML 2.0 usadas comumente que funcionam com o IAM Identity Center. Os exemplos incluem o Salesforce, o Box e o Office 365.

A maioria das aplicações fornece instruções detalhadas sobre como configurar a confiança entre o IAM Identity Center e o provedor de serviços da aplicação. Essas informações ficam disponíveis

na página de configuração da aplicação depois que você a seleciona no catálogo. Depois de configurar a aplicação, você pode atribuir aos usuários ou grupos do IAM Identity Center acesso a ela, conforme necessário.

Tópicos

- Configurar uma aplicação do catálogo de aplicações

Configurar uma aplicação do catálogo de aplicações

Use este procedimento para configurar uma relação de confiança SAML 2.0 entre o IAM Identity Center e o provedor de serviços da aplicação.

Antes de começar este procedimento, é útil ter o arquivo de troca de metadados do provedor do serviço para poder configurar a confiança de modo mais eficiente. Mesmo se não tiver esse arquivo, você poderá usar este procedimento para configurar manualmente a confiança.

Para adicionar e configurar uma aplicação do catálogo de aplicações

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Escolha a guia Gerenciada pelo cliente.
4. Escolha Adicionar aplicação.
5. Na página Selecionar tipo de aplicação, em Preferências de configuração, escolha Quero selecionar uma aplicação do catálogo.
6. Em Catálogo de aplicações, comece a digitar, na caixa de pesquisa, o nome da aplicação que você deseja adicionar.
7. Escolha o nome da aplicação na lista quando ele aparecer nos resultados da pesquisa e depois escolha Avançar.
8. Na página Configurar aplicação, os campos Nome de exibição e Descrição já estão preenchidos com os detalhes relevantes da aplicação. Você pode editar essas informações.
9. Em Metadados do IAM Identity Center, faça o seguinte:

    a. Ao lado do Arquivo de metadados de SAML do IAM Identity Center, escolha Download para fazer download dos metadados do provedor de identidades.

    b. Ao lado de Certificado do IAM Identity Center, escolha Fazer download do certificado para baixar o certificado do provedor de identidades.

> **Note**
>
> Você precisará desses arquivos mais tarde ao configurar a aplicação no site do provedor de serviços. Siga as instruções desse provedor.

10. (Opcional) Em Propriedades da aplicação, você pode especificar URL de início da aplicação, Estado de retransmissão e Duração da sessão. Para ter mais informações, consulte Configurar as propriedades da aplicação no console do IAM Identity Center.
11. Em Metadados da aplicação, faça o seguinte:
    a. Se você tiver um arquivo de metadados, escolha Carregar o arquivo de metadados SAML da aplicação. Em seguida, selecione Escolher arquivo para encontrar e selecionar o arquivo de metadados.
    b. Se você não tiver um arquivo de metadados, escolha Digitar manualmente os valores dos metadados e forneça os valores de URL do ACS da aplicação e Público do SAML da aplicação.
12. Selecione Enviar. Você é direcionado para a página de detalhes da aplicação que acabou de adicionar.

Configurar sua própria aplicação SAML 2.0

Você pode configurar suas próprias aplicações que permitem a federação de identidades usando o SAML 2.0 e adicioná-las ao IAM Identity Center. A maioria das etapas para configurar suas próprias aplicações SAML 2.0 é igual à configuração de uma aplicação SAML 2.0 do catálogo de aplicações no console do IAM Identity Center. Porém, você também deve fornecer mapeamentos adicionais dos atributos SAML para suas próprias aplicações SAML 2.0. Esses mapeamentos informam ao IAM Identity Center como preencher corretamente a asserção SAML 2.0 para a aplicação. Você pode fornecer esse mapeamento de atributos SAML adicional quando configurar a aplicação pela primeira vez. Você também pode fornecer os mapeamentos dos atributos SAML 2.0 na página de detalhes da aplicação no IAM Identity Center.

Use o procedimento a seguir para configurar uma relação de confiança SAML 2.0 entre o IAM Identity Center e o provedor de serviços da sua aplicação SAML 2.0. Antes de iniciar este procedimento, verifique se você tem o certificado e os arquivos de troca de metadados do provedor de serviços, para que possa terminar de configurar a confiança.

Para configurar sua própria aplicação SAML 2.0

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Escolha a guia Gerenciada pelo cliente.
4. Escolha Adicionar aplicação.
5. Na página Selecionar tipo de aplicação, em Preferências de configuração, escolha Eu tenho uma aplicação que quero configurar.
6. Em Tipo de aplicação, escolha SAML 2.0.
7. Escolha Próximo.
8. Na página Configurar aplicação, em Configurar aplicação, insira um nome de exibição para a aplicação, como **`MyApp`**. Insira uma Descrição.
9. Em Metadados do IAM Identity Center, faça o seguinte:
   a. Ao lado do Arquivo de metadados de SAML do IAM Identity Center, escolha Download para fazer download dos metadados do provedor de identidades.
   b. Em Certificado do IAM Identity Center, escolha Baixar para baixar o certificado do provedor de identidades.

   > **Note**
   >
   > Você precisará desses arquivos mais tarde ao configurar a aplicação personalizada no site do provedor de serviços.

10. (Opcional) Em Propriedades da aplicação, você também pode especificar URL de início da aplicação, Estado de retransmissão e Duração da sessão. Para ter mais informações, consulte Configurar as propriedades da aplicação no console do IAM Identity Center.
11. Em Metadados da aplicação, escolha Digite manualmente seus valores de metadados. Em seguida, forneça os valores de URL do ACS da aplicação e Público do SAML da aplicação.
12. Selecione Enviar. Você é direcionado para a página de detalhes da aplicação que acabou de adicionar.

Trusted identity propagation across applications

A propagação confiável de identidade permite que AWS os serviços façam o seguinte:

- Autorize o acesso aos AWS recursos com base no contexto de identidade do usuário.
- Compartilhe com segurança o contexto de identidade do usuário com outros AWS serviços.

Esses recursos permitem que o acesso do usuário seja mais facilmente definido, concedido e registrado.

Com a propagação de identidade confiável, um usuário pode entrar em um aplicativo e esse aplicativo pode transmitir o contexto de identidade dos usuários em solicitações para acessar dados em AWS serviços. Como o acesso é gerenciado com base na identidade do usuário, os usuários não precisam usar as credenciais de usuário local do banco de dados nem assumir um perfil do IAM para acessar os dados.

Tópicos

Visão geral da propagação de identidades confiáveis

Com a propagação de identidade confiável, o acesso do usuário aos AWS recursos pode ser mais facilmente definido, concedido e registrado. A propagação de identidades confiáveis é baseada na Estrutura de autorização OAuth 2.0, o que permite que as aplicações acessem e compartilhem dados de usuário em segurança sem compartilhar senhas. O OAuth 2.0 fornece acesso delegado seguro aos recursos das aplicações. O acesso é delegado porque o administrador do recurso aprova ou delega a aplicação na qual o usuário faz login para acessar a outra aplicação.

Para evitar o compartilhamento de senhas de usuários, a propagação de identidades confiáveis usa tokens. Os tokens fornecem uma forma padrão de um aplicativo confiável afirmar quem é o usuário e quais solicitações são permitidas entre dois aplicativos. AWS aplicativos gerenciados que se integram à propagação confiável de identidade obtêm tokens diretamente do IAM Identity Center. O IAM Identity Center também oferece uma opção para que as aplicações troquem tokens de identidade e tokens de acesso provenientes de um servidor externo de autorização OAuth 2.0. Isso

possibilita que um aplicativo se autentique e obtenha tokens externos AWS, troque o token por um token do IAM Identity Center e use o novo token para fazer solicitações aos AWS serviços. Para ter mais informações, consulte Usar aplicações com um emissor de tokens confiáveis.

O processo do OAuth 2.0 começa quando um usuário faz login em uma aplicação. A aplicação na qual o usuário faz login inicia uma solicitação de acesso aos recursos da outra aplicação. A aplicação iniciadora (solicitante) pode acessar a aplicação recebedora em nome do usuário solicitando um token do servidor de autorização. O servidor de autorização retorna o token e a aplicação iniciadora passa esse token, com uma solicitação de acesso, para a aplicação recebedora.

Casos de uso confiável de propagação de identidade

Como administrador do IAM Identity Center, você pode ser solicitado a ajudar a configurar a propagação de identidade confiável entre os seguintes aplicativos iniciais que oferecem suporte a esse recurso e os serviços conectados AWS . As seções a seguir fornecem mais informações sobre os casos de uso específicos suportados por aplicativos que podem iniciar a propagação de identidade confiável.

Tópicos

- Amazon EMR
- Amazon QuickSight
- Editor de Consultas do Amazon Redshift v2
- Aplicativos de inteligência de negócios de terceiros
- Aplicativos desenvolvidos sob medida

Amazon EMR

Você pode usar o Amazon EMR como aplicativo inicial para os seguintes casos de uso confiável de propagação de identidade.

Descrição	Outros AWS serviços usados	Saiba mais
Execute análises interativas com o Apache Spark no Amazon EMR em clusters do Amazon EC2 por meio do Amazon EMR Studio.	Amazon EMR no Amazon EC2 autorizado por meio de Amazon S3 AWS Lake Formation	• Integre o Amazon EMR com o IAM Identity Center no Guia de gerenciamento do Amazon EMR.

Descrição	Outros AWS serviços usados	Saiba mais
Aplique o controle de acesso com base nas identidades da força de trabalho e nos atributos associados do AWS Glue Catalog até. AWS Lake Formation	Access Grants, Amazon S3, AWS Service Catalog **Note** • Requer acesso por meio do Amazon EMR Studio. • Somente controle de acesso em nível de mesa. • Não há suporte para Apache Hive, PrestoSQL/ Trino e EMR Serverless.	• Subsídios de acesso ao Amazon S3 e identidades de diretórios corporativos no Guia do usuário do Amazon Simple Storage Service. • Conexão AWS Lake Formation com o IAM Identity Center no Guia do AWS Lake Formation desenvolvedor • Use suas identidades corporativas para análises com o Amazon EMR e o IAM Identity Center no blog de big AWS data

Descrição	Outros AWS serviços usados	Saiba mais
Execute análises ad hoc com o Trino no Athena por meio do Amazon EMR Studio. Aplique o controle de acesso com base nas identidades da força de trabalho e nos atributos associados do AWS Glue Catalog até. AWS Lake Formation Acesso seguro a uma localização de bucket de resultados de consulta do Athena no Amazon S3 usando Amazon S3 Access Grants.	Athena autorizada por meio do Amazon S3 AWS Lake Formation Access Grants **Note** Requer acesso por meio do Amazon EMR Studio. O acesso direto do Amazon Athena console não é suportado.	• Integre o Amazon EMR com o IAM Identity Center no Guia de gerenciamento do Amazon EMR. • O uso do IAM Identity Center habilitou grupos de trabalho do Athena no Guia do usuário do Amazon Athena. • Subsídios de acesso ao Amazon S3 e identidades de diretórios corporativos no Guia do usuário do Amazon Simple Storage Service. • Conexão AWS Lake Formation com o IAM Identity Center no Guia do AWS Lake Formation desenvolvedor. • Traga sua identidade de força de trabalho para o Amazon EMR Studio e o Athena no AWS blog de Big Data.

Amazon QuickSight

Você pode usar a Amazon QuickSight como aplicativo inicial para os seguintes casos de uso confiável de propagação de identidade.

Descrição	Outros AWS serviços usados	Saiba mais
QuickSight Os usuários da Amazon podem consultar	Amazon Redshift	• Conecte o Redshift ao IAM Identity Center para oferecer

Descrição	Outros AWS serviços usados	Saiba mais
dados do Amazon Redshift. O acesso aos dados é concedido no Amazon Redshift por um administrador do Amazon Redshift.		aos usuários uma experiênc ia de login único no Guia de gerenciamento do Amazon Redshift. • Conecte o Amazon Redshift ao IAM Identity Center por meio da Amazon QuickSight no Guia de gerenciamento do Amazon Redshift.
QuickSight Os usuários da Amazon podem consultar o Amazon Redshift Spectrum para dados estruturados no Amazon S3, com acesso autorizado AWS Lake Formation por um administr ador.	Amazon Redshift Spectrum, dados estruturados do Amazon S3 *Por meio do Amazon Redshift Spectrum autorizado por AWS Lake Formation	• Conecte o Redshift ao IAM Identity Center para oferecer aos usuários uma experiênc ia de login único no Guia de gerenciamento do Amazon Redshift. • Conecte o Amazon Redshift ao IAM Identity Center por meio da Amazon QuickSight no Guia de gerenciamento do Amazon Redshift. • Conexão AWS Lake Formation com o IAM Identity Center no Guia do AWS Lake Formation desenvolvedor. • Simplifique o gerenciamento de acesso com o Amazon Redshift e AWS Lake Formation para usuários em um provedor de identidade externo no blog de AWS big data.

Descrição	Outros AWS serviços usados	Saiba mais
QuickSight Os usuários da Amazon podem consultar compartilhamentos de dados do Amazon Redshift para dados estruturados no Amazon S3, com acesso autorizado por um administrador. AWS Lake Formation	Compartilhamentos de dados do Amazon Redshift, dados estruturados do Amazon S3 *Por meio do Amazon Redshift autorizado por AWS Lake Formation	• Conecte o Amazon Redshift ao IAM Identity Center por meio da Amazon QuickSight no Guia de gerenciamento do Amazon Redshift. • Conexão AWS Lake Formation com o IAM Identity Center no Guia do AWS Lake Formation desenvolvedor. • Simplifique o gerenciamento de acesso com o Amazon Redshift e AWS Lake Formation para usuários em um provedor de identidade externo no blog de AWS big data.

Editor de Consultas do Amazon Redshift v2

Você pode usar o editor de consultas v2 do Amazon Redshift como aplicativo inicial para os seguintes casos de uso confiável de propagação de identidade.

Descrição	Outros AWS serviços usados	Saiba mais
Os usuários do editor de consultas v2 do Amazon Redshift podem consultar dados do Amazon Redshift. O acesso aos dados é concedido no Amazon Redshift por um administrador do Amazon Redshift.	Amazon Redshift	• Conecte o Redshift ao IAM Identity Center para oferecer aos usuários uma experiênc ia de login único no Guia de gerenciamento do Amazon Redshift. • Conecte-se a um banco de dados do Amazon Redshift

Descrição	Outros AWS serviços usados	Saiba mais
		no Guia de Gerenciamento do Amazon Redshift. • Integre-se Okta com o Amazon Redshift Query Editor V2 usando o AWS IAM Identity Center Single Sign-On sem interrupções no blog de Big Data.AWS
Os usuários do editor de consultas Amazon Redshift v2 podem consultar tabelas externas do Amazon Redshift Spectrum para dados estrutura dos no Amazon S3, com acesso autorizado por um administrador. AWS Lake Formation	Amazon Redshift Spectrum, dados estruturados do Amazon S3 *Por meio do Amazon Redshift Spectrum autorizado por AWS Lake Formation	• Conecte o Redshift ao IAM Identity Center para oferecer aos usuários uma experiênc ia de login único no Guia de gerenciamento do Amazon Redshift. • Conecte-se a um banco de dados do Amazon Redshift no Guia de Gerenciamento do Amazon Redshift. • Conexão AWS Lake Formation com o IAM Identity Center no Guia do AWS Lake Formation desenvolvedor.
Os usuários do editor de consultas v2 do Amazon Redshift podem consultar compartil hamentos de dados do Amazon Redshift com acesso autorizado por um administrador. AWS Lake Formation	compartilhamentos de dados do Amazon Redshift, AWS Lake Formation	• Conecte-se a um banco de dados do Amazon Redshift no Guia de Gerenciamento do Amazon Redshift. • Conexão AWS Lake Formation com o IAM Identity Center no Guia do AWS Lake Formation desenvolvedor.

Aplicativos de inteligência de negócios de terceiros

Você pode usar um aplicativo de business intelligence de terceiros, como o Tableau, como aplicativo inicial para casos de uso específicos de propagação de identidade confiável. Aplicativos modificados de inteligência comercial de terceiros podem transmitir ao driver do Amazon Redshift a identidade de um usuário por meio de tokens de identidade ou tokens de acesso do OAuth, para consultar dados no Amazon Redshift, com acesso autorizado por um administrador do Amazon Redshift.

Aplicativos desenvolvidos sob medida

Você pode usar seus próprios aplicativos desenvolvidos sob medida como um aplicativo inicial para os seguintes casos de uso confiável de propagação de identidade.

Descrição	Outros AWS serviços usados	Saiba mais
Crie um aplicativo que autentiqu e os usuários por meio de um servidor de autorização OAuth AWS IAM Identity Center e, em seguida, use o IAM para obter uma credencial de função do IAM com identidade aprimorada. Essa credencial é usada para solicitar acesso a dados não estrutura dos no Amazon S3, com acesso autorizado por um administrador do Amazon S3 Access Grants.	AWS IAM Identity Center, Dados não estruturados do Amazon S3 *Autorizado por meio do Amazon S3 Access Grants	• Subsídios de acesso ao Amazon S3 e identidades de diretórios corporativos no Guia do usuário do Amazon Simple Storage Service. • Como desenvolver um aplicativ o de dados voltado para o usuário com o IAM Identity Center e o Amazon S3 Access Grants (Parte 1) e (Parte 2) AWS no Storage Blog.
Crie um aplicativo personalizado que interaja com o Amazon Q Business para responder às perguntas dos usuários com base no seu próprio conteúdo e nas permissões do usuário.	Centro de identidad e do IAM, Amazon Q Business	• Habilite e configure uma instância do IAM Identity Center no Amazon Q Business User Guide. • Como usar aplicativos AWS gerenciados com o IAM Identity Center: habilite o Amazon Q sem migrar os fluxos de

Descrição	Outros AWS serviços usados	Saiba mais
		federação do IAM existentes no blog AWS de segurança.

Configurar a propagação de identidades confiáveis

A propagação de identidade confiável oferece suporte a diferentes maneiras de os aplicativos se autenticarem para que possam transmitir a identidade de um usuário aos AWS serviços. A configuração da propagação de identidades confiáveis varia de acordo com os tipos de aplicação e a forma como elas fazem a autenticação.

> **Note**
>
> Você deve configurar um emissor de token confiável se tiver aplicativos gerenciados pelo cliente que solicitam acesso aos aplicativos AWS gerenciados, mas não usam AWS APIs para se conectar.

Tópicos

- Pré-requisitos e considerações
- Usando propagação de identidade confiável com aplicativos AWS gerenciados
- Usar a propagação de identidades confiáveis com aplicações gerenciadas pelo cliente

Pré-requisitos e considerações

Antes de configurar a propagação de identidades confiáveis, revise os seguintes pré-requisitos e considerações.

Tópicos

- Pré-requisitos
- Considerações adicionais

Pré-requisitos

Para usar a propagação de identidades confiáveis, confirme que seu ambiente atende aos pré-requisitos a seguir.

- Implantação do IAM Identity Center com usuários e grupos provisionados

  Para usar a propagação de identidades confiáveis, você deve habilitar o IAM Identity Center e provisionar usuários e grupos. Para mais informações, consulte Introdução às tarefas comuns do IAM Identity Center.

  Instância da organização recomendada — Recomendamos que você use uma instância organizacional do IAM Identity Center que você habilite na conta de gerenciamento do AWS Organizations. Se você planeja usar a propagação de identidade confiável para permitir que os usuários acessem AWS serviços e recursos relacionados de forma diferente Contas da AWS dentro da mesma organização, você pode delegar a administração da sua instância do IAM Identity Center a uma conta membro.

  Se você planeja usar uma única instância de conta do IAM Identity Center, todos os AWS serviços e recursos que você deseja que os usuários acessem por meio de propagação de identidade confiável devem residir na mesma conta independente Conta da AWS ou na mesma conta membro na organização em que você habilitou o IAM Identity Center. Para ter mais informações, consulte Instâncias de conta do IAM Identity Center.
- Para aplicativos AWS gerenciados; conexão com o IAM Identity Center

  Para usar a propagação de identidade confiável, os aplicativos AWS gerenciados devem se integrar ao IAM Identity Center.

Considerações adicionais

Tenha em mente as seguintes considerações adicionais para usar a propagação de identidades confiáveis.

- Não modifique a configuração Exigir atribuições para aplicativos AWS gerenciados

  AWS os aplicativos gerenciados têm uma configuração de configuração padrão que determina se as atribuições são necessárias para usuários e grupos. Recomendamos que você não modifique essa configuração. Mesmo que você tenha configurado permissões refinadas que permitam que o

usuário acesse recursos específicos, modificar a configuração Exigir atribuições pode resultar em comportamento inesperado, incluindo a interrupção do acesso do usuário a esses recursos.

- Permissões de várias contas (conjuntos de permissões) não exigidas

  A propagação de identidades confiáveis não exige que você configure permissões de várias contas (conjuntos de permissões). Você pode habilitar o IAM Identity Center e usá-lo somente para a propagação de identidades confiáveis.

Usando propagação de identidade confiável com aplicativos AWS gerenciados

A propagação de identidade confiável permite que um aplicativo AWS gerenciado solicite acesso aos dados nos AWS serviços em nome de um usuário. O gerenciamento de acesso aos dados é baseado na identidade do usuário, portanto, os administradores podem conceder acesso com base no usuário e nas associações a grupo existentes dos usuários. A identidade do usuário, as ações realizadas em seu nome e outros eventos são registrados em registros e CloudTrail eventos específicos do serviço.

A propagação de identidades confiáveis é baseada no padrão OAuth 2.0. Para usar esse recurso, os aplicativos AWS gerenciados devem se integrar ao IAM Identity Center. AWS os serviços de análise podem fornecer interfaces baseadas em drivers que permitem que um aplicativo compatível use a propagação de identidade confiável. Por exemplo, os drivers JDBC, ODBC e Python permitem que ferramentas de consulta compatíveis usem a propagação de identidades confiáveis sem que você precise realizar etapas adicionais de configuração.

Tópicos

- Configure aplicativos AWS gerenciados para propagação confiável de identidade
- Fluxos de solicitação de propagação de identidade confiáveis para aplicativos AWS gerenciados
- Depois que uma aplicação obtém um token
- Sessões de perfil do IAM aprimoradas com identidade
- Tipos de sessões de perfil do IAM aprimoradas com identidade
- Processo de configuração e fluxo de solicitações para aplicativos AWS gerenciados

Configure aplicativos AWS gerenciados para propagação confiável de identidade

AWS os serviços que oferecem suporte à propagação de identidade confiável fornecem uma interface de usuário administrativa e APIs que você pode usar para configurar esse recurso. Nenhuma configuração é necessária no IAM Identity Center para esses serviços.

A seguir está o processo de alto nível para configurar um AWS serviço de propagação de identidade confiável. As etapas específicas variam de acordo com a interface administrativa e as APIs fornecidas pela aplicação.

1. Use o console da aplicação ou APIs para conectar a aplicação à instância do IAM Identity Center

   Use o console do aplicativo AWS gerenciado ou as APIs do aplicativo para conectar o aplicativo à sua instância do IAM Identity Center. Quando você usa o console da aplicação, a interface do usuário administrativa inclui um widget que simplifica o processo de configuração e conexão.
2. Usar o console da aplicação ou APIs para configurar o acesso do usuário aos recursos da aplicação

   Conclua esta etapa para autorizar quais recursos ou dados um usuário pode acessar. O acesso é baseado na identidade ou na associação a grupo do usuário. O modelo de autorização varia de acordo com a solicitação.

   > **Important**
   >
   > Você deve concluir essa etapa para permitir que os usuários acessem os recursos do serviço da AWS . Caso contrário, os usuários não poderão acessar os recursos, mesmo que a aplicação solicitante esteja autorizada a solicitar acesso ao serviço.

Fluxos de solicitação de propagação de identidade confiáveis para aplicativos AWS gerenciados

Todos os fluxos confiáveis de propagação de identidade para aplicativos AWS gerenciados devem começar com um aplicativo que obtém um token do IAM Identity Center. Esse token é obrigatório porque contém uma referência a um usuário conhecido pelo IAM Identity Center e às aplicações registradas no IAM Identity Center.

As seções a seguir descrevem as maneiras pelas quais um aplicativo AWS gerenciado pode obter um token do IAM Identity Center para iniciar a propagação de identidade confiável.

Tópicos

- Autenticação do IAM Identity Center na Web
- Solicitações de autenticação iniciadas pelo usuário no console

Autenticação do IAM Identity Center na Web

Para esse fluxo, o aplicativo AWS gerenciado fornece uma experiência de login único baseada na web usando o IAM Identity Center para autenticação.

Quando um usuário abre um aplicativo AWS gerenciado, um fluxo de login único que usa o IAM Identity Center é acionado. Se não houver uma sessão ativa para o usuário no IAM Identity Center, uma página de login será apresentada a ele com base na fonte de identidades que você especificou, e o IAM Identity Center criará uma sessão para o usuário.

O IAM Identity Center fornece ao aplicativo AWS gerenciado um token que inclui a identidade do usuário e uma lista de públicos (Auds) e escopos relacionados que o aplicativo está registrado para usar. A aplicação pode então usar o token para fazer solicitações a outros serviços da AWS recebedores.

Solicitações de autenticação iniciadas pelo usuário no console

Para esse fluxo, o aplicativo AWS gerenciado fornece uma experiência de console que os usuários iniciam.

Nesse caso, o aplicativo AWS gerenciado é inserido no AWS Management Console após assumir uma função. Para que a aplicação obtenha um token, o usuário deve iniciar um processo para acionar a aplicação para autenticar o usuário. Isso inicia a autenticação usando o IAM Identity Center, o que redirecionará o usuário para a fonte de identidades que você configurou.

Depois que uma aplicação obtém um token

Depois que uma aplicação solicitante obtém um token do IAM Identity Center, ela o atualiza periodicamente e ele pode ser usado durante toda a sessão do usuário. Durante esse tempo, a aplicação pode:

- Obter mais informações sobre o token para determinar quem é o usuário e quais escopos a aplicação pode usar com outras aplicações recebedoras gerenciadas pela AWS .
- Passe o token em chamadas para outros aplicativos AWS gerenciados de recebimento que suportem o uso de tokens.
- Obtenha sessões de função do IAM com identidade aprimorada que ele possa usar para fazer solicitações a outros aplicativos AWS gerenciados que usam o AWS Signature versão 4.

Uma sessão de perfil do IAM aprimorada com identidade é uma sessão de perfil do IAM que contém a identidade propagada do usuário armazenada em um token criado pelo IAM Identity Center.

Sessões de perfil do IAM aprimoradas com identidade

AWS Security Token Service Isso permite que um aplicativo obtenha uma sessão de função do IAM com identidade aprimorada. AWS aplicativos gerenciados que oferecem suporte ao contexto do usuário em uma sessão de função podem usar as informações de identidade para autorizar o acesso com base no usuário que está na sessão de função. Esse novo contexto permite que os aplicativos façam solicitações a aplicativos AWS gerenciados que oferecem suporte à propagação de identidade confiável por meio de solicitações de API AWS Signature Version 4.

Quando um aplicativo AWS gerenciado usa uma sessão de função do IAM com identidade aprimorada para acessar um recurso, CloudTrail registra a identidade do usuário (ID do usuário), a sessão inicial e a ação tomada.

Quando uma aplicação faz uma solicitação usando uma sessão de perfil do IAM aprimorada com identidade para uma aplicação recebedora, ela adiciona contexto à sessão para que a aplicação recebedora possa autorizar o acesso com base na identidade ou associação a grupo do usuário ou no perfil do IAM. O recebimento de aplicações compatíveis com a propagação de identidades confiáveis retornará um erro se a aplicação recebedora ou o recurso solicitado não estiverem configurados para autorizar o acesso com base na identidade ou na associação a grupo do usuário.

Para evitar esse problema, faça uma das seguintes alternativas:

- Verifique se a aplicação recebedora está conectada ao IAM Identity Center.
- Use o console da aplicação recebedora ou as APIs da aplicação para configurá-la para autorizar o acesso aos recursos com base na identidade ou na associação a grupo do usuário. Os requisitos de configuração para isso variam de acordo com a aplicação.

Para obter mais informações, consulte a documentação da aplicação recebedora gerenciada pela AWS .

Tipos de sessões de perfil do IAM aprimoradas com identidade

Um aplicativo obtém uma sessão de função do IAM com identidade aprimorada fazendo uma solicitação à AWS STS `AssumeRole` API e transmitindo uma declaração de contexto

no `ProvidedContexts` parâmetro da solicitação. `AssumeRole` A asserção do contexto é obtida da declaração `idToken` que está disponível na resposta da solicitação de `SSO OIDC` `CreateTokenWithIAM`.

AWS STS pode criar dois tipos diferentes de sessões de função do IAM com identidade aprimorada, dependendo da afirmação de contexto fornecida à solicitação: `AssumeRole`

- Sessões que registram apenas a identidade do usuário em CloudTrail.
- Sessões que permitem a autorização com base na identidade propagada do usuário e a CloudTrail registram em.

Para obter uma sessão de função do IAM com identidade aprimorada AWS STS que forneça apenas informações de auditoria registradas em uma CloudTrail trilha, forneça o valor da `sts:audit_context` declaração à solicitação. `AssumeRole` Para obter uma sessão que também permita que o AWS serviço de recebimento autorize o usuário do IAM Identity Center a realizar uma ação, forneça o valor da `sts:identity_context` declaração à `AssumeRole` solicitação. Você só pode fornecer um único contexto.

Sessões de perfil do IAM aprimoradas com identidade criadas com o **`sts:audit_context`**

Quando uma solicitação é feita a um AWS serviço usando uma sessão de função do IAM com identidade aprimorada criada com`sts:audit_context`, o IAM Identity Center do usuário `userId` é conectado ao elemento CloudTrail . `OnBehalfOf`

```
"userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLE:MyRole",
      "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
      "accountId": "111111111111",
      "accessKeyId": "ASIAEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAEXAMPLE",
            "arn": "arn:aws:iam::111111111111:role/MyRole",
            "accountId": "111111111111",
            "userName": "MyRole"
        },
        "attributes": {
            "creationDate": "2023-12-12T13:55:22Z",
```

```
            "mfaAuthenticated": "false"
        }
    },
    "onBehalfOf": {
        "userId": "11111111-1111-1111-1111-1111111111",
        "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/
d-111111111"
    }
}
```

> **Note**
>
> Essas sessões não podem ser usadas para autorizar o usuário do Identity Center. Elas continuam podendo ser usadas para autorizar o perfil do IAM.

Para obter esse tipo de sessão de função AWS STS, forneça o valor do `sts:audit_context` campo para a `AssumeRole` solicitação no parâmetro de `ProvidedContexts` solicitação. Use `arn:aws:iam::aws:contextProvider/IdentityStore` como valor de `ProviderArn`.

Sessões de perfil do IAM aprimoradas com identidade criadas com o **`sts:identity_context`**

Quando um usuário faz uma solicitação a um AWS serviço usando uma sessão de função do IAM com identidade aprimorada criada com`sts:identity_context`, a Central de Identidade do IAM do usuário `userId` é conectada ao CloudTrail `onBehalfOf` elemento da mesma forma que uma sessão criada com. `sts:audit_context`

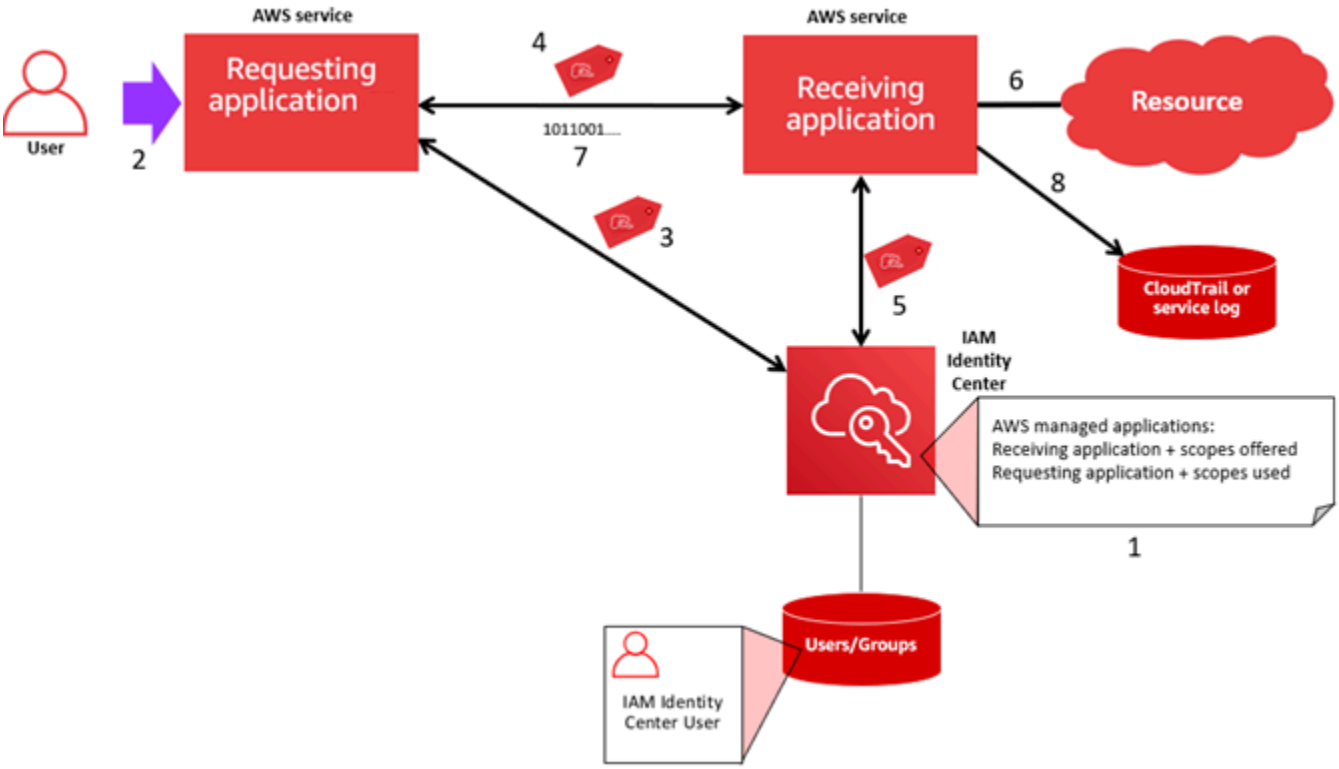
Além de registrar o usuário do `userId` IAM Identity Center CloudTrail, esse tipo de sessão também é usado por APIs compatíveis para autorizar ações com base na identidade propagada do usuário. Para ver uma lista de ações do IAM para as APIs compatíveis, consulte a política `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gerenciada. Essa política AWS gerenciada é fornecida como uma política de sessão quando uma sessão de função do IAM com identidade aprimorada é criada com. `sts:identity_context` A política impede que você use a sessão de função com AWS serviços sem suporte.

Para obter esse tipo de sessão de função AWS STS, forneça o valor do `sts:identity_context` campo para a `AssumeRole` solicitação no parâmetro de `ProvidedContexts` solicitação. Use `arn:aws:iam::aws:contextProvider/IdentityStore` como valor de `ProviderArn`.

Processo de configuração e fluxo de solicitações para aplicativos AWS gerenciados

Esta seção descreve o processo de configuração e o fluxo de solicitação para aplicações gerenciadas pela AWS que usam a propagação de identidades confiáveis e fornecem uma experiência de logon único na Web.

O diagrama a seguir fornece uma visão geral desse processo.



As etapas a seguir fornecem informações adicionais sobre esse processo.

1. Use o console do aplicativo AWS gerenciado ou as APIs do aplicativo para fazer o seguinte:
   a. Conecte a aplicação à instância do IAM Identity Center.
   b. Configure permissões para autorizar quais recursos da aplicação um usuário pode acessar.
2. O fluxo de solicitações começa quando um usuário abre um aplicativo AWS gerenciado que pode solicitar acesso aos recursos (um aplicativo solicitante).
3. Para obter um token para acessar o aplicativo AWS gerenciado receptor, o aplicativo AWS gerenciado solicitante inicia uma solicitação de login no IAM Identity Center.

   Se o usuário não tiver feito login, o IAM Identity Center acionará um fluxo de autenticação do usuário para a fonte de identidades que você especificou. Isso cria uma nova sessão do portal de AWS acesso para o usuário com a duração que você configurou no IAM Identity Center. Em

seguida, o IAM Identity Center gera um token associado à sessão, e o aplicativo pode operar pelo restante da sessão do portal de AWS acesso do usuário. Se o usuário sair da aplicação ou se você excluir a sessão do usuário, ela será encerrada automaticamente em duas horas.

4. O aplicativo AWS gerenciado inicia uma solicitação para o aplicativo receptor e fornece seu token.
5. A aplicação recebedora faz chamadas para o IAM Identity Center para obter a identidade do usuário e os escopos que estão codificados no token. A aplicação recebedora também pode fazer solicitações para obter os atributos do usuário ou as associações a grupos do usuário no diretório do Identity Center.
6. A aplicação recebedora usa sua configuração de autorização para determinar se o usuário está autorizado a acessar o recurso da aplicação solicitado.
7. Se o usuário estiver autorizado a acessar o recurso da aplicação solicitado, a aplicação recebedora responderá à solicitação.
8. A identidade do usuário, as ações realizadas em seu nome e outros eventos registrados nos logs e eventos do AWS CloudTrail da aplicação recebedora. O modo específico como essas informações são registradas varia de acordo com a aplicação.

Usar a propagação de identidades confiáveis com aplicações gerenciadas pelo cliente

A propagação confiável de identidade permite que um aplicativo gerenciado pelo cliente solicite acesso aos dados nos AWS serviços em nome de um usuário. O gerenciamento de acesso aos dados é baseado na identidade do usuário, portanto, os administradores podem conceder acesso com base no usuário e nas associações a grupo existentes dos usuários. A identidade do usuário, as ações realizadas em seu nome e outros eventos são registrados em registros e CloudTrail eventos específicos do serviço.

Com a propagação de identidade confiável, um usuário pode entrar em um aplicativo gerenciado pelo cliente e esse aplicativo pode transmitir a identidade do usuário em solicitações para acessar dados em AWS serviços.

> **Important**
>
> Para acessar um AWS serviço, os aplicativos gerenciados pelo cliente devem obter um token de um emissor de token confiável, externo ao IAM Identity Center. Um emissor de tokens confiáveis é um servidor de autorização OAuth 2.0 que cria tokens assinados. Esses tokens autorizam aplicativos que iniciam solicitações de acesso a AWS serviços (recebimento de

aplicativos). Para ter mais informações, consulte Usar aplicações com um emissor de tokens confiáveis.

Tópicos

- Configurar aplicações OAuth 2.0 gerenciadas pelo cliente para a propagação de identidades confiáveis
- Especificar aplicações confiáveis

Configurar aplicações OAuth 2.0 gerenciadas pelo cliente para a propagação de identidades confiáveis

Para configurar uma aplicação OAuth 2.0 gerenciada pelo cliente para a propagação de identidades confiáveis, você deve primeiro adicioná-la ao IAM Identity Center. Use o procedimento a seguir para adicionar a aplicação ao IAM Identity Center.

Tópicos

- Etapa 1: selecionar o tipo de aplicação
- Etapa 2: especificar detalhes da aplicação
- Etapa 3: especificar as configurações de autenticação
- Etapa 4: especificar as credenciais da aplicação
- Etapa 5: revisar e configurar

Etapa 1: selecionar o tipo de aplicação

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Escolha a guia Gerenciada pelo cliente.
4. Escolha Adicionar aplicação.
5. Na página Selecionar tipo de aplicação, em Preferências de configuração, escolha Eu tenho uma aplicação que quero configurar.
6. Em Tipo de aplicação, escolha OAuth 2.0.
7. Escolha Avançar para prosseguir para a próxima página, Etapa 2: especificar detalhes da aplicação.

Etapa 2: especificar detalhes da aplicação

1. Na página Especificar detalhes do aplicativo, em Nome e descrição do aplicativo, insira um nome de exibição para o aplicativo, como**`MyApp`**. Insira uma Descrição.
2. Em Método de atribuição de usuário e grupo, escolha uma das seguintes opções:

   - Exigir atribuições: permita apenas que usuários e grupos do IAM Identity Center atribuídos a essa aplicação a acessem.

     Visibilidade do bloco do aplicativo — Somente usuários atribuídos ao aplicativo diretamente ou por meio de uma atribuição em grupo podem visualizar o quadro do aplicativo no portal de AWS acesso, desde que a visibilidade do aplicativo no portal de AWS acesso esteja definida como Visível.
   - Não exigir atribuições: permita que todos os usuários e grupos autorizados do IAM Identity Center acessem essa aplicação.

     Visibilidade do bloco da aplicação: o bloco da aplicação é visível para todos os usuários que fazem login no Portal de acesso do AWS , a menos que Visibilidade da aplicação no Portal de acesso do AWS esteja definida como Não visível.
3. Em Portal de acesso do AWS , insira o URL no qual os usuários podem acessar a aplicação e especifique se o bloco da aplicação ficará visível ou não no Portal de acesso do AWS . Se você escolher Não visível, nem mesmo os usuários atribuídos poderão visualizar o bloco da aplicação.
4. Expanda Tags (opcional), escolha Adicionar nova tag e especifique valores de Chave e Valor (opcional).

   Para obter mais informações sobre tags, consulte Marcando atributos AWS IAM Identity Center.
5. Escolha Avançar e prossiga para a próxima página, Etapa 3: especificar as configurações de autenticação.

Etapa 3: especificar as configurações de autenticação

Para adicionar uma aplicação gerenciada pelo cliente compatível com o OAuth 2.0 ao IAM Identity Center, você deve especificar um emissor de tokens confiáveis. Um emissor de tokens confiáveis é um servidor de autorização OAuth 2.0 que cria tokens assinados. Esses tokens autorizam aplicativos que iniciam solicitações (solicitando aplicativos) para acessar aplicativos AWS gerenciados (recebimento de aplicativos).

1. Na página Especificar configurações de autenticação, em Emissores de token confiáveis, faça uma das seguintes alternativas:

   - Para usar um emissor de tokens confiáveis existente:

     Marque a caixa de seleção ao lado do nome do emissor de tokens confiáveis que você deseja excluir.

   - Para adicionar um novo emissor de tokens confiáveis:

     1. Escolha Criar emissor de tokens confiáveis.
     2. Uma nova guia de navegador é aberta. Siga as etapas de 5 a 8 em Como adicionar um emissor de tokens confiáveis ao console do IAM Identity Center.
     3. Depois de concluir essas etapas, volte à janela do navegador que você está usando para a configuração da aplicação e selecione o emissor de tokens confiáveis que acabou de adicionar.
     4. Na lista de emissores de tokens confiáveis, marque a caixa de seleção ao lado do nome do emissor de tokens confiáveis que você acabou de adicionar.

        Depois de selecionar um emissor de tokens confiáveis, a seção Configurar os emissores de tokens confiáveis selecionados é exibida.

2. Em Configurar os emissores de token confiáveis selecionados, insira a declaração Aud. A declaração Aud identifica o público-alvo (destinatários) do token gerado pelo emissor de tokens confiáveis. Para ter mais informações, consulte Declaração de Aud.
3. Para evitar que os usuários precisem ser autenticados novamente quando estiverem usando essa aplicação, selecione Atualizar automaticamente a autenticação do usuário para a sessão ativa da aplicação. Quando selecionada, essa opção atualiza o token de acesso da sessão a cada 60 minutos, até que a sessão expire ou o usuário encerre a sessão.
4. Escolha Avançar e prossiga para a próxima página, Etapa 4: especificar as credenciais da aplicação.

Etapa 4: especificar as credenciais da aplicação

Conclua as etapas deste procedimento para especificar as credenciais que a aplicação usa para realizar ações de troca de tokens com aplicações confiáveis. Essas credenciais são usadas em uma política baseada no recurso. A política exige que você especifique uma entidade principal que tenha permissões para fazer as ações nela especificadas. Você deve especificar uma entidade principal, mesmo que as aplicações confiáveis estejam na mesma Conta da AWS.

> **Note**
>
> Ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para a realização de 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.

Essa política exige a ação `sso-oauth:CreateTokenWithIAM`.

1. Na página Especificar credenciais da aplicação, escolha uma das seguintes opções:
   - Para especificar rapidamente um ou mais perfis do IAM:
     1. Selecione Inserir um ou mais perfis do IAM.
     2. Em Inserir perfis do IAM, especifique o nome do recurso da Amazon (ARN) de um perfil do IAM existente. Para especificar o ARN, use a sintaxe a seguir. A parte da região do ARN está em branco porque os recursos do IAM são globais.

        ```
        arn:aws:iam::account:role/role-name-with-path
        ```

        Para obter mais informações, consulte Cross-account access using resource-based policies e IAM ARNs no AWS Identity and Access Management User Guide.
   - Para editar manualmente a política (necessária se você especificar informações não AWS credenciais):
     1. Selecione Editar a política da aplicação.
     2. Modifique a política digitando ou colando texto na caixa de texto JSON.
     3. Resolva todos os avisos de segurança, erros ou avisos gerais gerados durante a validação de política. Para obter mais informações, consulte Validating IAM policies no AWS Identity and Access Management User Guide.
2. Escolha Avançar e prossiga para a próxima página, Etapa 5: revisar e configurar.

Etapa 5: revisar e configurar

1. Na página Revisar e configurar, revise as escolhas feitas. Para fazer alterações, escolha a seção de configuração desejada, escolha Editar e faça as alterações necessárias.
2. Quando terminar, escolha Adicionar aplicação.

3. A aplicação que você adicionou aparece na lista Aplicações gerenciadas pelo cliente.
4. Depois de configurar seu aplicativo gerenciado pelo cliente no IAM Identity Center, você deve especificar um ou mais AWS serviços, ou aplicativos confiáveis, para propagação de identidade. Isso permite que os usuários façam login na aplicação gerenciada pelo cliente e acessem os dados na aplicação confiável.

   Para ter mais informações, consulte Especificar aplicações confiáveis .

Especificar aplicações confiáveis

Depois de configurar seu aplicativo gerenciado pelo cliente, você deve especificar um ou mais AWS serviços confiáveis, ou aplicativos confiáveis, para propagação de identidade. Especifique um AWS serviço que tenha dados que os usuários dos aplicativos gerenciados pelo cliente precisam acessar. Quando os usuários fizerem login na aplicação gerenciada pelo cliente, ela passará a identidade dos usuários para a aplicação confiável.

Use o procedimento a seguir para selecionar um serviço e especificar as aplicações individuais confiáveis para esse serviço.

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Escolha a guia Gerenciada pelo cliente.
4. Na lista Aplicações gerenciadas pelo cliente, selecione a aplicação OAuth 2.0 para a qual você deseja iniciar solicitações de acesso. Essa é a aplicação na qual seus usuários fazem login.
5. Na página Detalhes, em Aplicações confiáveis para a propagação de identidades, escolha Especificar aplicações confiáveis.
6. Em Tipo de configuração, selecione Aplicações individuais e especificar acesso e escolha Avançar.
7. Na página Selecionar serviço, escolha o serviço da AWS que tem aplicações nos quais a aplicação gerenciada pelo cliente pode confiar para a propagação de identidades e depois escolha Avançar.

   O serviço que você seleciona define as aplicações confiáveis. Você selecionará as aplicações na próxima etapa.
8. Na página Selecionar aplicações, escolha Aplicações individuais, marque a caixa de seleção de cada aplicação que pode receber solicitações de acesso e escolha Avançar.

9. Na página Configurar acesso, em Método de configuração, escolha uma das seguintes opções:
    - Selecionar acesso por aplicação: selecione essa opção para configurar diferentes níveis de acesso para cada aplicação. Escolha a aplicação para a qual você deseja configurar o nível de acesso e depois escolha Editar acesso. Em Nível de acesso a ser aplicado, altere os níveis de acesso conforme necessário e escolha Salvar alterações.
    - Aplicar o mesmo nível de acesso a todos as aplicações: selecione essa opção se você não precisar configurar níveis de acesso por aplicação.
10. Escolha Próximo.
11. Na página Revisar configuração, revise as escolhas que fez. Para fazer alterações, escolha a seção de configuração desejada, escolha Editar acesso e faça as alterações necessárias.
12. Quando terminar, escolha Confiar nas aplicações.

Usar aplicações com um emissor de tokens confiáveis

Os emissores de tokens confiáveis permitem que você use a propagação de identidade confiável com aplicativos que se autenticam fora do. AWS Com emissores de tokens confiáveis, você pode autorizar essas aplicações a fazer solicitações em nome dos usuários para acessar aplicações gerenciadas pela AWS .

Os tópicos a seguir descrevem como os emissores de tokens confiáveis funcionam além de fornecer orientação sobre configuração.

Tópicos

Visão geral do emissor de tokens confiáveis

A propagação de identidade confiável fornece um mecanismo que permite que aplicativos que se autenticam externamente AWS façam solicitações em nome de seus usuários com o uso de um emissor de token confiável. Um emissor de tokens confiáveis é um servidor de autorização OAuth 2.0 que cria tokens assinados. Esses tokens autorizam aplicativos que iniciam solicitações (solicitando

aplicativos) de acesso a AWS serviços (recebimento de aplicativos). As aplicações solicitantes iniciam solicitações de acesso em nome dos usuários que o emissor de tokens confiáveis autentica. Os usuários são conhecidos tanto pelo emissor de tokens confiáveis quanto pelo IAM Identity Center.

AWS os serviços que recebem solicitações gerenciam autorizações refinadas para seus recursos com base em seus usuários e membros de grupos, conforme representado no diretório do Identity Center. AWS os serviços não podem usar diretamente os tokens do emissor externo do token.

Para resolver isso, o IAM Identity Center oferece uma maneira para a aplicação solicitante, ou um driver da AWS usado pela aplicação solicitante, trocar o token emitido pelo emissor de tokens confiáveis por um token gerado pelo IAM Identity Center. O token gerado pelo IAM Identity Center referencia o usuário correspondente do IAM Identity Center. A aplicação solicitante, ou o driver, usa o novo token para iniciar uma solicitação à aplicação recebedora. Como o novo token referencia o usuário correspondente no IAM Identity Center, a aplicação recebedora pode autorizar o acesso solicitado com base no usuário ou na sua associação a um grupo, conforme representado no IAM Identity Center.

> **Important**
>
> Escolher um servidor de autorização OAuth 2.0 para adicionar como um emissor de tokens confiáveis é uma decisão de segurança que requer consideração cuidadosa. Escolha somente emissores de token confiáveis em que você confia para realizar as seguintes tarefas:
>
> - Autenticar o usuário especificado no token.
> - Autorizar o acesso desse usuário à aplicação recebedora.
> - Gerar um token que o IAM Identity Center possa trocar por um token criado pelo IAM Identity Center.

Pré-requisitos e considerações para emissores de tokens confiáveis

Antes de configurar um emissor de tokens confiáveis, revise os seguintes pré-requisitos e considerações.

- Configuração de emissor de tokens confiáveis

  Você deve configurar um servidor de autorização OAuth 2.0 (o emissor confiável do token). Embora o emissor de token confiável seja normalmente o provedor de identidade que você usa

como fonte de identidade para o IAM Identity Center, ele não precisa ser. Para obter informações sobre como configurar o emissor de token confiável, consulte a documentação do provedor de identidade relevante.

> **Note**
>
> Você pode configurar até 10 emissores de tokens confiáveis para usar com o IAM Identity Center, desde que mapeie a identidade de cada usuário no emissor de tokens confiáveis para um usuário correspondente no IAM Identity Center.

- O servidor de autorização OAuth 2.0 (o emissor de tokens confiáveis) que cria o token deve ter um endpoint de descoberta OpenID Connect (OIDC) que o IAM Identity Center possa usar para obter chaves públicas para verificar as assinaturas do token. Para ter mais informações, consulte URL do endpoint de descoberta do OIDC (URL do emissor).
- Tokens emitidos pelo emissor de token confiável

  Os tokens do emissor confiável do token devem atender aos seguintes requisitos:

  - O token deve ser assinado e estar no formato JSON Web Token (JWT) usando o algoritmo RS256.
  - O token deve conter as seguintes afirmações:
    - Emissor (iss) — A entidade que emitiu o token. Esse valor deve corresponder ao valor configurado no endpoint de descoberta do OIDC (URL do emissor) no emissor de token confiável.
    - Assunto (sub) — O usuário autenticado.
    - Audiência (aud) — O destinatário pretendido do token. Esse é o AWS serviço que será acessado depois que o token for trocado por um token do IAM Identity Center. Para ter mais informações, consulte Declaração de Aud.
    - Tempo de expiração (exp) — O tempo após o qual o token expira.
    -
  - O token pode ser um token de identidade ou um token de acesso.
  - O token deve ter um atributo que possa ser mapeado exclusivamente para um usuário do IAM Identity Center.
- Declarações opcionais

O IAM Identity Center é compatível com todas as declarações opcionais definidas na RFC 7523. Para obter mais informações, consulte a Seção 3: formato JWT e requisitos de processamento dessa RFC.

Por exemplo, o token pode conter uma declaração JTI (JWT ID). Essa declaração, quando presente, impede que tokens com Lo mesmo JTI sejam reutilizados para trocas de tokens. Para obter mais informações sobre a declaração, consulte Detalhes da declaração JTI.

- Configuração do IAM Identity Center para funcionar com um emissor de tokens confiáveis

  Você também deve habilitar o IAM Identity Center, configurar a fonte de identidades para o IAM Identity Center e provisionar os usuários que correspondem aos usuários no diretório do emissor de tokens confiáveis.

  Para isso, faça uma das seguintes alternativas:

  - Sincronize os usuários com o IAM Identity Center usando o protocolo System for Cross-domain Identity Management (SCIM) v2.0.
  - Crie os usuários diretamente no IAM Identity Center.

  > **Note**
  >
  > Os emissores de tokens confiáveis não serão compatíveis se você usar o Serviço de Domínios do Active Directory como fonte de identidades.

Detalhes da declaração JTI

Se o IAM Identity Center receber uma solicitação para trocar um token que o IAM Identity Center já trocou, a solicitação falhará. Para detectar e evitar a reutilização de um token em trocas de tokens, você pode incluir uma declaração JTI. O IAM Identity Center protege contra a repetição de tokens com base nas declarações neles contidas.

Nem todos os servidores de autorização OAuth 2.0 adicionam uma declaração JTI aos tokens. Alguns servidores de autorização OAuth 2.0 adicionam uma declaração JTI aos tokens. Os servidores de autorização OAuth 2.0 compatíveis com o uso de uma declaração JTI podem adicionar essa declaração somente aos tokens de identidade, somente aos tokens de acesso ou a ambos. Para obter mais informações, consulte a documentação do servidor de autorização OAuth 2.0.

Para obter informações sobre a criação de aplicações que trocam tokens, consulte a documentação da API do IAM Identity Center. Para obter informações sobre como configurar uma aplicação gerenciada pelo cliente para obter e trocar os tokens corretos, consulte a documentação da aplicação.

Configurações de emissor de tokens confiáveis

As seções a seguir descrevem as configurações necessárias para configurar e usar um emissor de tokens confiáveis.

Tópicos

URL do endpoint de descoberta do OIDC (URL do emissor)

Ao adicionar um emissor de tokens confiáveis ao console do IAM Identity Center, é necessário especificar o URL do endpoint de descoberta OIDC. Esse URL é comumente referenciado por seu URL relativo, `/.well-known/openid-configuration`. No console do IAM Identity Center, esse URL é chamado de URL do emissor.

> **Note**
>
> Você deve colar a URL do endpoint de descoberta até o fim e para o final. `.well-known/openid-configuration` Se `.well-known/openid-configuration` for incluída na URL, a configuração do emissor de token confiável não funcionará. Como o IAM Identity Center não valida esse URL, se o URL não for formado corretamente, a configuração do emissor de token confiável falhará sem notificação.

O IAM Identity Center usa esse URL para obter informações adicionais sobre o emissor de tokens confiáveis. Por exemplo, o IAM Identity Center usa esse URL para obter as informações necessárias para verificar os tokens gerados pelo emissor de tokens confiáveis. Quando adicionar um emissor de tokens confiáveis ao IAM Identity Center, você deve especificar esse URL. Para encontrar o URL, consulte a documentação do provedor de servidor de autorização OAuth 2.0 que você usa para gerar tokens para sua aplicação ou entre em contato diretamente com o provedor para obter ajuda.

Mapeamento de atributos

Os mapeamentos de atributos permitem que o IAM Identity Center faça a correspondência entre o usuário declarado em um token emitido por um emissor de tokens confiáveis e um único usuário no IAM Identity Center. Você deve especificar o mapeamento de atributos quando adicionar o emissor de tokens confiáveis ao IAM Identity Center. Esse mapeamento de atributos é usado em uma declaração no token gerado pelo emissor de tokens confiáveis. O valor na declaração é usado para pesquisar no IAM Identity Center. A pesquisa usa o atributo especificado para recuperar um único usuário no IAM Identity Center, que será usado como usuário no AWS. A declaração que você escolher deve ser mapeada para um único atributo em uma lista fixa de atributos disponíveis no repositório de identidades do IAM Identity Center. Você pode escolher um dos seguintes atributos do repositório de identidades do IAM Identity Center: nome de usuário, e-mail e ID externo. O valor do atributo que você especifica no IAM Identity Center deve ser exclusivo para cada usuário.

Declaração de Aud

Uma declaração aud identifica o público (destinatários) ao qual um token se destina. Quando a aplicação que solicita acesso é autenticada por um provedor de identidades que não está federado ao IAM Identity Center, esse provedor de identidades deve ser configurado como um emissor de tokens confiáveis. A aplicação que recebe a solicitação de acesso (a aplicação recebedora) deve trocar o token gerado pelo emissor de tokens confiáveis por um token gerado pelo IAM Identity Center.

Para obter informações sobre como obter os valores da declaração aud para a aplicação recebedora como registrados no emissor de tokens confiáveis, consulte a documentação do emissor de tokens confiáveis ou entre em contato com o administrador do emissor de tokens confiáveis para obter ajuda.

Configurar um emissor de tokens confiáveis

Para permitir a propagação de identidades confiáveis para uma aplicação que faz a autenticação fora do IAM Identity Center, um ou mais administradores devem configurar um emissor de tokens confiáveis. Um emissor de tokens confiáveis é um servidor de autorização OAuth 2.0 que emite tokens para aplicações que iniciam solicitações (aplicações solicitantes). Os tokens autorizam esses aplicativos a iniciar solicitações em nome de seus usuários para um aplicativo receptor (um AWS serviço).

Tópicos

- Tarefas para configurar um emissor de tokens confiáveis
- Como adicionar um emissor de tokens confiáveis ao console do IAM Identity Center
- Como visualizar ou editar as configurações do emissor de tokens confiáveis no console do IAM Identity Center
- Processo de configuração e fluxo de solicitação para aplicações que usam um emissor de tokens confiáveis

Coordenar perfis e responsabilidades administrativas

Em alguns casos, um único administrador pode realizar todas as tarefas necessárias para configurar um emissor de tokens confiáveis. Se vários administradores realizarem essas tarefas, será necessária uma coordenação estreita. A tabela a seguir descreve como vários administradores podem se coordenar para configurar um emissor de token confiável e configurar o AWS serviço para usá-lo.

> **Note**
>
> O aplicativo pode ser qualquer AWS serviço integrado ao IAM Identity Center e que ofereça suporte à propagação de identidade confiável.

Para ter mais informações, consulte Tarefas para configurar um emissor de tokens confiáveis.

Função	Executa essas tarefas	Coordena com
Administrador do IAM Identity Center	Adiciona o IdP externo como um emissor de tokens confiáveis ao console do IAM Identity Center. Ajuda a configurar o mapeamento correto dos atributos entre o IAM Identity Center e o IdP externo. Notifica o administrador do AWS serviço quando o emissor de token confiável é adicionado ao console do IAM Identity Center.	Administrador do IdP (emissor de tokens confiáveis) externo AWS administrador do serviço

Função	Executa essas tarefas	Coordena com
Administrador do IdP (emissor de tokens confiáveis) externo	Configura o IdP externo para emitir tokens. Ajuda a configurar o mapeamento correto dos atributos entre o IAM Identity Center e o IdP externo. Fornece o nome do público (declaração Aud) ao administrador do serviço da AWS .	Administrador do IAM Identity Center AWS administrador do serviço
AWS administrador do serviço	Verifica o console AWS de serviço em busca do emissor de token confiável. O emissor de tokens confiáveis ficará visível no console do serviço da AWS depois que o administrador do IAM Identity Center o adicionar ao console do IAM Identity Center. Configura o AWS serviço para usar o emissor de token confiável.	Administrador do IAM Identity Center Administrador do IdP (emissor de tokens confiáveis) externo

Tarefas para configurar um emissor de tokens confiáveis

Para configurar um emissor de tokens confiáveis, um administrador do IAM Identity Center, o administrador do IdP (emissor de tokens confiáveis) externo e o administrador da aplicação devem realizar as tarefas a seguir.

> **Note**
>
> O aplicativo pode ser qualquer AWS serviço integrado ao IAM Identity Center e que ofereça suporte à propagação de identidade confiável.

1. Adicionar o emissor de tokens confiáveis ao IAM Identity Center: o administrador do IAM Identity Center adiciona o emissor de tokens confiáveis usando o console do IAM Identity Center ou APIs. Essa configuração requer a especificação do seguinte:

   - O nome do emissor de tokens confiáveis
   - O URL do endpoint de descoberta OIDC (no console do IAM Identity Center, esse URL é chamado de URL do emissor).
   - Mapeamento de atributos para pesquisa de usuários. Esse mapeamento de atributos é usado em uma declaração no token que é gerado pelo emissor de tokens confiáveis. O valor na declaração é usado para pesquisar no IAM Identity Center. A pesquisa usa o atributo especificado para recuperar um único usuário do IAM Identity Center.

2. Conectar o AWS serviço ao IAM Identity Center — O administrador do AWS serviço deve conectar o aplicativo ao IAM Identity Center usando o console do aplicativo ou das APIs do aplicativo.

   Depois que o emissor de token confiável é adicionado ao console do IAM Identity Center, ele também fica visível no console de AWS serviço e está disponível para seleção pelo administrador do AWS serviço.

3. Configurar o uso da troca de tokens — No console de AWS serviço, o administrador do AWS serviço configura o AWS serviço para aceitar tokens emitidos pelo emissor confiável do token. Esses tokens são trocados por tokens gerados pelo IAM Identity Center. Isso requer a especificação do nome do emissor de token confiável da Etapa 1 e o valor da solicitação de Aud que corresponde ao AWS serviço.

   O emissor de tokens confiáveis coloca o valor da declaração Aud no token que ele emite para indicar que o token se destina a ser usado pelo serviço da AWS . Para obter esse valor, entre em contato com o administrador do emissor de tokens confiáveis.

Como adicionar um emissor de tokens confiáveis ao console do IAM Identity Center

Em uma organização que tem vários administradores, essa tarefa é realizada por um administrador do IAM Identity Center. Se você for o administrador do IAM Identity Center, deverá escolher qual IdP externo usar como emissor de tokens confiáveis.

Para adicionar um emissor de tokens confiáveis ao console do IAM Identity Center

1. Abra o console do Centro de Identidade do IAM.

2. Escolha Configurações.
3. Na página Configurações, escolha a guia Autenticação.
4. Em Emissores de token confiáveis, escolha Criar emissor de tokens confiáveis.
5. Na página Configurar um IdP externo para emitir tokens confiáveis, em Detalhes do emissor de tokens confiáveis, faça o seguinte:

   - Para URL do emissor, especifique a URL de descoberta do OIDC do IdP externo que emitirá tokens para propagação de identidade confiável. Você deve especificar a URL do endpoint de descoberta até o fim e até o fim. `.well-known/openid-configuration` O administrador do IdP externo pode fornecer esse URL.

     > **Note**
     >
     > Observação Esse URL deve corresponder ao URL na declaração do Emissor (iss) em tokens emitidos para propagação de identidade confiável.

   - Em Nome do emissor de tokens confiáveis, insira um nome para identificar esse emissor de tokens confiáveis no IAM Identity Center e no console da aplicação.
6. Em Mapear atributos, faça o seguinte:

   - Em Atributo do provedor de identidades, selecione um atributo na lista para mapear para um atributo no repositório de identidades do IAM Identity Center.
   - Em Atributo do IAM Identity Center, selecione o atributo correspondente para o mapeamento de atributos.
7. Em Tags (opcional), escolha Adicionar nova tag e especifique um valor para Chave e, opcionalmente, para Valor.

   Para obter mais informações sobre tags, consulte Marcando atributos AWS IAM Identity Center.
8. Escolha Criar emissor de tokens confiáveis.
9. Depois de concluir a criação do emissor de tokens confiáveis, entre em contato com o administrador da aplicação para informar o nome do emissor de tokens confiáveis, para que ele possa confirmar que o emissor de tokens confiáveis está visível no console aplicável.
10. O administrador da aplicação deve selecionar esse emissor de tokens confiáveis no console aplicável para permitir o acesso do usuário à aplicação a partir das aplicações configuradas para a propagação de identidades confiáveis.

Como visualizar ou editar as configurações do emissor de tokens confiáveis no console do IAM Identity Center

Depois de adicionar um emissor de tokens confiáveis ao console do IAM Identity Center, você pode visualizar e editar as configurações relevantes.

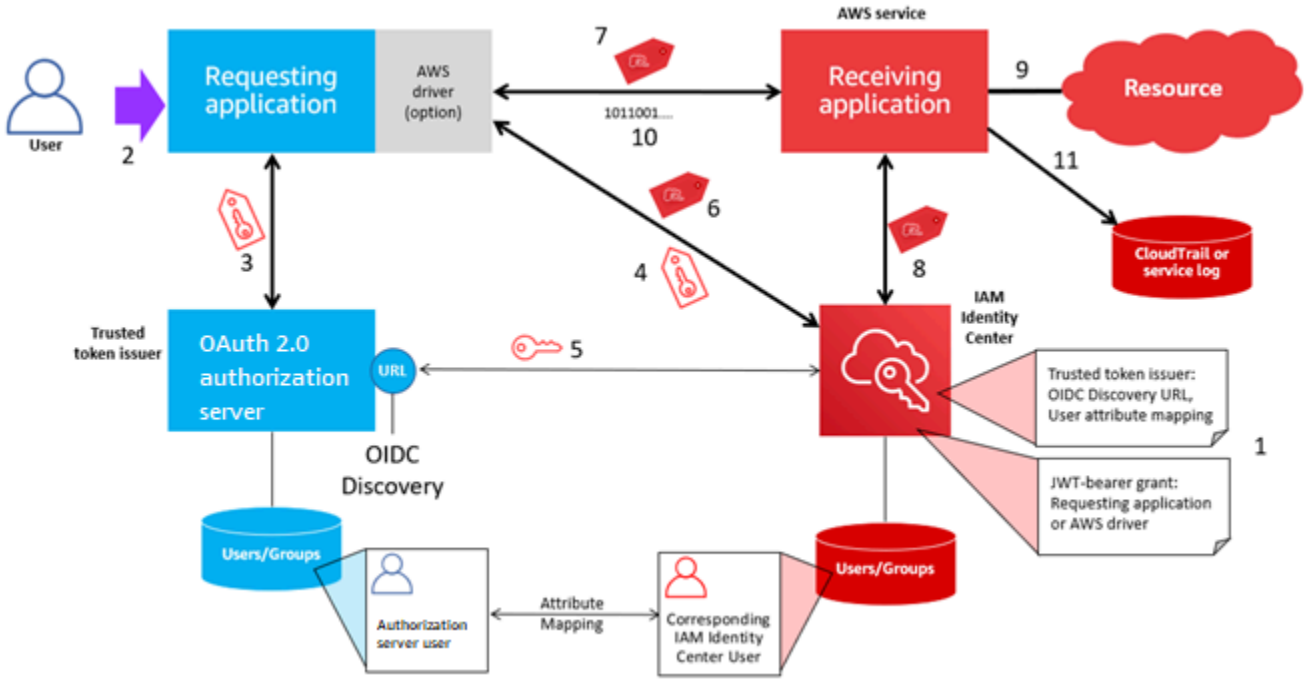
Se você pretende editar as configurações do emissor de tokens confiáveis, lembre-se de que isso pode fazer com que os usuários percam o acesso a qualquer aplicação configurada para usar o emissor de tokens confiáveis. Para evitar interromper o acesso dos usuários, recomendamos que você coordene com os administradores de todas as aplicações configuradas para que usem o emissor de tokens confiáveis antes de editar as configurações.

Para visualizar ou editar as configurações do emissor de tokens confiáveis no console do IAM Identity Center

1. Abra o console do Centro de Identidade do IAM.
2. Escolha Configurações.
3. Na página Configurações, escolha a guia Autenticação.
4. Em Emissores de tokens confiáveis, selecione o emissor de tokens confiáveis que você deseja visualizar ou editar.
5. Escolha Ações e, em seguida, escolha Editar.
6. Na página Editar emissor de tokens confiáveis, visualize ou edite as configurações conforme necessário. Você pode editar o nome do emissor de tokens confiáveis os mapeamentos de atributos e as tags.
7. Escolha Salvar alterações.
8. Na caixa de diálogo Editar emissor de tokens confiáveis, você será solicitado a confirmar se deseja fazer alterações. Selecione a opção Confirmar.

Processo de configuração e fluxo de solicitação para aplicações que usam um emissor de tokens confiáveis

Esta seção descreve o processo de configuração e o fluxo de solicitação para aplicações que usam um emissor de tokens confiáveis para a propagação de identidades confiáveis. O diagrama a seguir fornece uma visão geral desse processo.



As etapas a seguir fornecem informações adicionais sobre esse processo.

1. Configure o IAM Identity Center e o aplicativo AWS gerenciado de recebimento para usar um emissor de token confiável. Para mais informações, consulte Tarefas para configurar um emissor de tokens confiáveis.
2. O fluxo de solicitação começa quando um usuário abre a aplicação solicitante.
3. O aplicativo solicitante solicita um token do emissor confiável do token para iniciar solicitações ao aplicativo gerenciado receptor AWS . Se o usuário ainda não tiver sido autenticado, esse processo acionará um fluxo de autenticação. O token contém as seguintes informações:
   - O assunto (Sub) do usuário.
   - O atributo que o IAM Identity Center usa para pesquisar o usuário correspondente no IAM Identity Center.
   - Uma declaração de público (Aud) que contém um valor que o emissor de tokens confiáveis associa à aplicação gerenciada pela AWS recebedora. Se outras declarações estiverem presentes, elas não serão usadas pelo IAM Identity Center.
4. O aplicativo solicitante, ou o AWS driver que ele usa, passa o token para o IAM Identity Center e solicita que o token seja trocado por um token gerado pelo IAM Identity Center. Se você usa um AWS driver, talvez seja necessário configurá-lo para esse caso de uso. Para obter mais informações, consulte a documentação do aplicativo AWS gerenciado relevante.

5. O IAM Identity Center usa o endpoint de descoberta OIDC para obter a chave pública que pode ser usada para verificar a autenticidade do token. Em seguida, o IAM Identity Center faz o seguinte:
   - Verifica o token.
   - Pesquisa o diretório do Identity Center. Para fazer isso, o IAM Identity Center usa o atributo mapeado especificado no token.
   - Verifica se o usuário está autorizado a acessar a aplicação recebedora. Se o aplicativo AWS gerenciado estiver configurado para exigir atribuições a usuários e grupos, o usuário deverá ter uma atribuição direta ou baseada em grupo ao aplicativo; caso contrário, a solicitação será negada. Se a aplicação gerenciada pela AWS estiver configurada para não exigir atribuições de usuários e grupos, o processamento continuará.

     > **Note**
     >
     > AWS os serviços têm uma configuração de configuração padrão que determina se as atribuições são necessárias para usuários e grupos. Recomendamos que você não modifique a configuração Exigir atribuições para essas aplicações se planejar usá-las com a propagação de identidades confiáveis. Mesmo que você tenha configurado permissões refinadas que permitam que o usuário acesse recursos específicos da aplicação, modificar a configuração Exigir atribuições pode resultar em um comportamento inesperado, incluindo interrupção do acesso do usuário a esses recursos.

   - Verifica se o aplicativo solicitante está configurado para usar escopos válidos para o aplicativo gerenciado receptor AWS .
6. Se as etapas de verificação anteriores forem bem-sucedidas, o IAM Identity Center criará um novo token. O novo token é um token opaco (criptografado) que inclui a identidade do usuário correspondente no IAM Identity Center, o público (Aud) do aplicativo AWS gerenciado receptor e os escopos que o aplicativo solicitante pode usar ao fazer solicitações ao aplicativo gerenciado receptor AWS .
7. A aplicação solicitante, ou o driver que ela usa, inicia uma solicitação de recurso para a aplicação recebedora e passa o token que o IAM Identity Center gerou para a aplicação recebedora.
8. A aplicação recebedora faz chamadas para o IAM Identity Center para obter a identidade do usuário e os escopos que estão codificados no token. Ela também pode fazer solicitações para obter os atributos do usuário ou das associações a grupos do usuário no diretório do Identity Center.

9. A aplicação recebedora usa sua configuração de autorização para definir se o usuário está autorizado a acessar o recurso da aplicação solicitado.
10. Se o usuário estiver autorizado a acessar o recurso da aplicação solicitado, a aplicação recebedora responderá à solicitação.
11. A identidade do usuário, as ações realizadas em seu nome e outros eventos registrados nos registros e CloudTrail eventos do aplicativo receptor. O modo específico como essas informações são registradas varia de acordo com a aplicação.

Gerenciar certificados do IAM Identity Center

O IAM Identity Center usa certificados para configurar uma relação de confiança SAML entre o IAM Identity Center e o provedor de serviços da aplicação. Quando você adiciona uma aplicação no IAM Identity Center, um certificado do IAM Identity Center é criado automaticamente para uso com essa aplicação durante o processo de configuração. Por padrão, esse certificado do IAM Identity Center gerado automaticamente é válido por um período de cinco anos.

Como administrador do IAM Identity Center, você ocasionalmente precisará substituir certificados antigos por novos para um determinada aplicação. Por exemplo, você talvez precise substituir um certificado quando a data de expiração do certificado está se aproximando. O processo de substituição de um certificado antigo por um mais novo é chamado de rotação de certificados.

Tópicos

- Considerações antes de fazer a rotação de um certificado
- Fazer a rotação de um certificado do IAM Identity Center
- Indicadores do status de expiração do certificado

Considerações antes de fazer a rotação de um certificado

Antes de iniciar o processo de rotação de um certificado no IAM Identity Center, considere o seguinte:

- O processo de rotação da certificação exige que você restabeleça a confiança entre o IAM Identity Center e o provedor de serviços. Para restabelecer a confiança, use os procedimentos fornecidos em Fazer a rotação de um certificado do IAM Identity Center.

- A atualização do certificado com o provedor de serviços pode causar uma interrupção temporária do serviço para seus usuários até que a confiança seja restabelecida com sucesso. Planeje essa operação com cuidado fora do horário de pico, se possível.

Fazer a rotação de um certificado do IAM Identity Center

A rotação de um certificado do IAM Identity Center é um processo de várias etapas que envolve o seguinte:

- Gerar um novo certificado
- Adicionar o novo certificado ao site do provedor de serviços
- Configurar o novo certificado como ativo
- Excluir o certificado inativo

Use todos os procedimentos a seguir na seguinte ordem para concluir o processo de rotação de certificados para um determinada aplicação.

Etapa 1: gerar um novo certificado.

Os novos certificados do IAM Identity Center que você gera podem ser configurados para usar as seguintes propriedades:

- Período de validade: especifica o tempo alocado (em meses) antes que um novo certificado do IAM Identity Center expire.
- Tamanho da chave: determina o número de bits que uma chave deve usar com seu algoritmo criptográfico. Você pode definir esse valor como RSA de 1024 bits ou RSA de 2048 bits. Para obter informações gerais sobre como os tamanhos das chaves funcionam na criptografia, consulte Tamanho da chave.
- Algoritmo: especifica o algoritmo que o IAM Identity Center usa ao assinar a asserção/resposta do SAML. Você pode definir esse valor como SHA-1 ou SHA-256. AWS recomenda usar SHA-256 quando possível, a menos que seu provedor de serviços exija SHA-1. Para obter informações gerais sobre como os algoritmos de criptografia funcionam, consulte Criptografia de chave pública.

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Na lista de aplicações, escolha a aplicação para o qual deseja gerar um novo certificado.

4. Na página de detalhes da aplicação, selecione a guia Configuração. Em Metadados do IAM Identity Center, escolha Gerenciar certificado. Se você não tiver uma guia Configuração ou se a configuração não estiver disponível, não será necessário fazer o rodízio de certificados para essa aplicação.
5. Na página Certificado do IAM Identity Center, escolha Gerar novo certificado.
6. Na caixa de diálogo Gerar novo certificado do IAM Identity Center, especifique os valores apropriados para Período de validade, Algoritmo e Tamanho da chave. Em seguida, escolha Gerar.

Etapa 2: atualize o site do provedor de serviços.

Use o procedimento a seguir para restabelecer a confiança com o provedor de serviços da aplicação.

> **Important**
>
> Quando você carrega o novo certificado para o provedor de serviços, talvez seus usuários não consigam se autenticar. Para corrigir essa situação, defina o novo certificado como ativo conforme descrito na próxima etapa.

1. No console do IAM Identity Center, escolha a aplicação para o qual você acabou de gerar um novo certificado.
2. Na página de detalhes da aplicação, escolha Editar configuração.
3. Escolha Ver instruções e siga as instruções do site do seu provedor de serviços de aplicações específico para adicionar o certificado recém-gerado.

Etapa 3: defina o novo certificado como ativo.

Uma aplicação pode ter até dois certificados atribuídos a ela. O IAM Identity Center usará a certificação que está definida como ativa para assinar todas as asserções SAML.

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Na lista de aplicações, escolha sua aplicação.
4. Na página de detalhes da aplicação, selecione a guia Configuração. Em Metadados do IAM Identity Center, escolha Gerenciar certificado.

5. Na página do certificado do IAM Identity Center, selecione o certificado que você deseja definir como ativo, escolha Ações e, em seguida, escolha Definir como ativo.
6. Na caixa de diálogo Definir o certificado selecionado como ativo, confirme que você entende que definir um certificado como ativo pode exigir que você restabeleça a confiança e escolha Tornar ativo.

Etapa 4: excluir o certificado antigo.

Use o procedimento a seguir para concluir o processo de rotação do certificado para sua inscrição. Você só pode excluir um certificado que esteja em um estado inativo.

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Na lista de aplicações, escolha sua aplicação.
4. Na página de detalhes da aplicação, selecione a aba Configuração. Em Metadados do IAM Identity Center, escolha Gerenciar certificado.
5. Na página do certificado do IAM Identity Center, selecione o certificado que deseja excluir. Escolha Ações e, em seguida, escolha Excluir.
6. Na caixa de diálogo Excluir certificado, escolha Excluir.

Indicadores do status de expiração do certificado

Enquanto estiver na página Aplicações, nas propriedades de uma aplicação, você poderá observar ícones coloridos indicadores de status. Esses ícones aparecem na coluna Expira em ao lado de cada certificado na lista. A seguir, descrevemos os critérios que o IAM Identity Center usa para determinar qual ícone é exibido para cada certificado.

- Vermelho – Indica que um certificado está expirado no momento.
- Amarelo: indica que um certificado expirará em 90 dias ou menos.
- Verde – Indica que um certificado está atualmente válido e permanecerá válido por pelo menos mais 90 dias.

Para verificar o status atual de um certificado

1. Abra o console do IAM Identity Center.

2. Selecione Aplicações.
3. Na lista de aplicações, revise o status dos certificados na lista, conforme indicado na coluna Expira em.

Configurar as propriedades da aplicação no console do IAM Identity Center

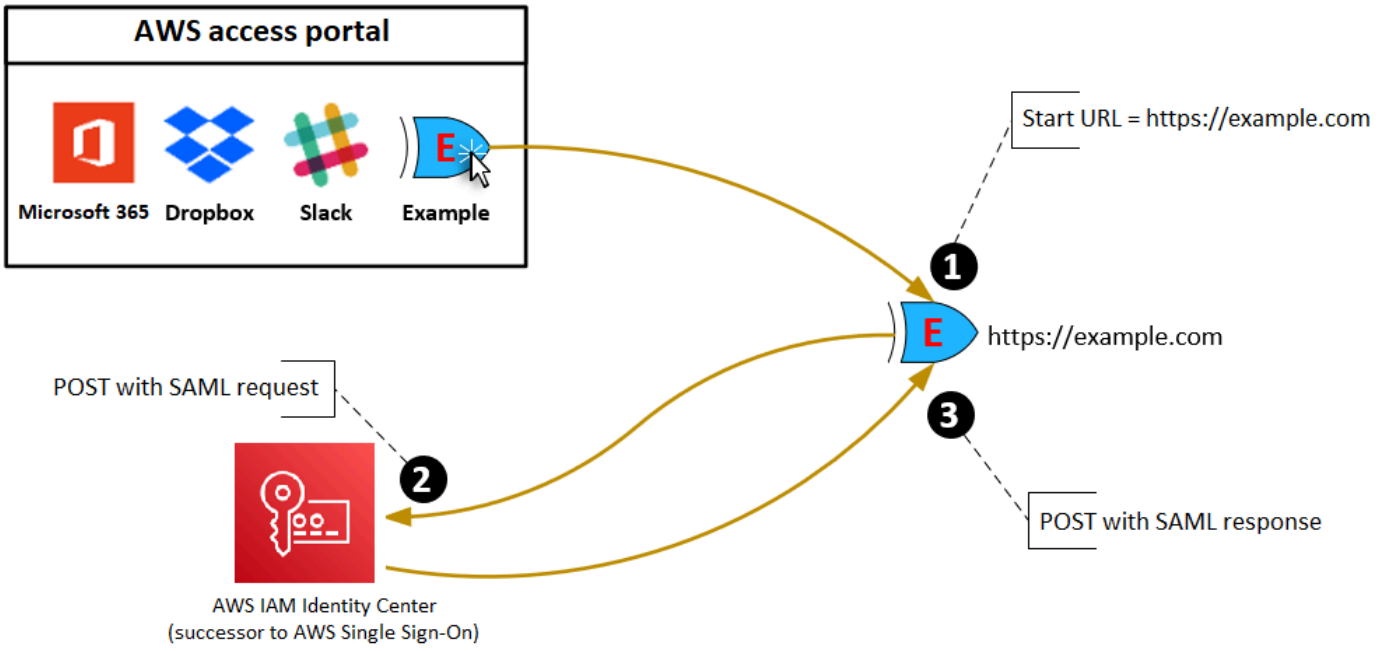
No IAM Identity Center, você pode personalizar a experiência do usuário configurando o URL de início da aplicação, o estado de retransmissão e a duração da sessão.

URL de início da aplicação

Você usa um URL de início da aplicação para iniciar o processo de federação com sua aplicação. O uso típico é para uma aplicação que só permite vínculo iniciado pelo provedor de serviços (SP).

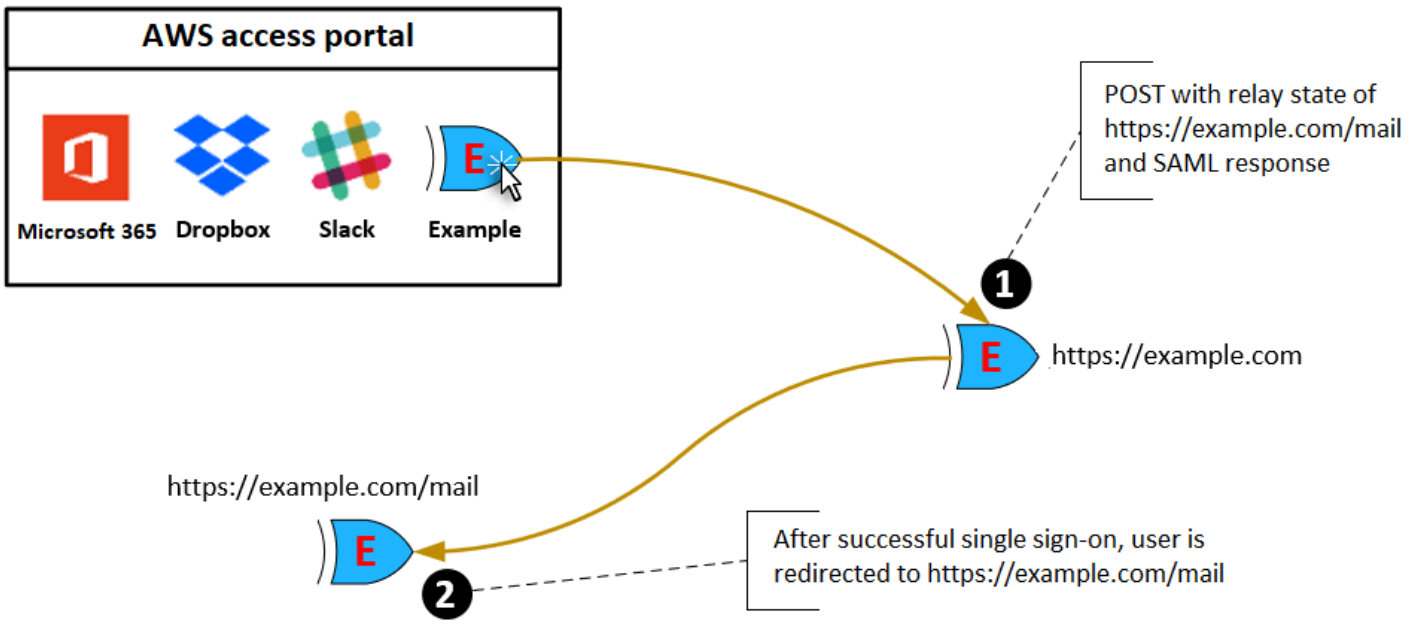
As etapas e o diagrama a seguir ilustram o fluxo de trabalho de autenticação de URL de início da aplicação quando um usuário escolhe uma aplicação no portal de acesso do AWS :

1. O navegador do usuário redireciona a solicitação de autenticação usando o valor do URL de início de aplicação (neste caso, https://example.com).
2. A aplicação envia um `HTML POST` com `SAMLRequest` para o IAM Identity Center.
3. O IAM Identity Center então envia um `HTML POST` com uma `SAMLResponse` de volta para a aplicação.



Estado de retransmissão

Durante o processo de autenticação de federação, o estado de retransmissão redireciona os usuários dentro da aplicação. Para o SAML 2.0, esse valor é passado, não modificado, para a aplicação. Depois que as propriedades da aplicação são configuradas, o IAM Identity Center envia o valor do estado de retransmissão juntamente com uma resposta SAML para a aplicação.



Duração da sessão

A duração da sessão é o período de tempo durante o qual as sessões dos usuários da aplicação permanecem válidas. Para o SAML 2.0, isso é usado para definir a data de `SessionNotOnOrAfter` do elemento `saml2:AuthNStatement` da asserção SAML.

A duração da sessão pode ser interpretada pelas aplicações de uma das seguintes maneiras:

- As aplicações podem usá-la para determinar o tempo máximo permitido para a sessão do usuário. As aplicações podem gerar uma sessão de usuário com uma duração menor. Isso pode acontecer quando a aplicação permite apenas sessões de usuário com duração menor que a duração da sessão configurada.
- As aplicações podem usá-la como a duração exata e podem impedir que os administradores configurem o valor. Isso pode acontecer quando a aplicação permite apenas um tamanho de sessão específico.

Para obter mais informações sobre como a duração da sessão é usada, consulte a documentação a sua aplicação específica.

Atribuir acesso de usuário às aplicações no console do IAM Identity Center

Você pode atribuir aos usuários acesso de logon único a aplicações SAML 2.0 do catálogo de aplicações ou a aplicações SAML 2.0 personalizadas.

Considerações sobre exercícios em grupo:

- Atribua acesso diretamente aos grupos. Para ajudar a simplificar a administração de permissões de acesso, é recomendável atribuir acesso diretamente a grupos, em vez de a usuários específicos. Com grupos, você pode conceder ou negar permissões para grupos de usuários, em vez de ter de aplicar essas permissões a cada indivíduo. Se um usuário se mudar para uma organização diferente, basta mover esse usuário para um grupo diferente. Em seguida, o usuário recebe automaticamente as permissões necessárias para a nova organização.
- Grupos aninhados não são compatíveis. Ao atribuir acesso de usuário às aplicações, o IAM Identity Center não oferece suporte à adição de usuários a grupos aninhados. Se um usuário for adicionado a um grupo aninhado, ele poderá receber a mensagem “Você não tem nenhuma

aplicação" durante o login. As atribuições devem ser feitas em relação ao grupo imediato do qual o usuário é membro.

Para atribuir acesso de usuário ou grupo a aplicações

> **Important**
>
> Para aplicativos AWS gerenciados, você deve adicionar usuários diretamente dos consoles de aplicativos relevantes ou por meio das APIs.

1. Abra o console do Centro de Identidade do IAM.

   > **Note**
   >
   > Se você gerencia usuários em AWS Managed Microsoft AD, certifique-se de que o console do IAM Identity Center esteja usando a AWS região em que seu AWS Managed Microsoft AD diretório está localizado antes de dar a próxima etapa.

2. Selecione Aplicações.
3. Na lista de aplicações, escolha o nome da aplicação à qual deseja atribuir acesso.
4. Na página de detalhes da aplicação, na seção Usuários atribuídos, selecione Atribuir usuários.
5. Na caixa de diálogo Atribuir usuários, digite um nome de usuário ou grupo. Você também pode pesquisar usuários e grupos. Você pode especificar vários usuários ou grupos selecionando as contas aplicáveis à medida que elas aparecem nos resultados da pesquisa.
6. Escolha Atribuir usuários.

Remover o acesso do usuário no console do IAM Identity Center

Use esse procedimento para remover o acesso do usuário às aplicações SAML 2.0 do catálogo de aplicações ou às aplicações SAML 2.0 personalizadas.

Para remover acesso do usuário de uma aplicação

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.

3. Na lista de aplicações, escolha a aplicação da qual você deseja remover o acesso de usuário.
4. Na página de detalhes da aplicação, na guia Usuários atribuídos, selecione o usuário ou grupo que você deseja remover e, em seguida, escolha o botão Remover acesso.
5. Na caixa de diálogo Remove access (Remover acesso), confirme o nome do usuário ou do grupo. Em seguida, escolha Remove access (Remover acesso).

Mapear atributos em sua aplicação para atributos do IAM Identity Center

Alguns provedores de serviço personalizados exigem asserções do SAML para transmitir dados adicionais sobre logins de usuário. Nesse caso, use o procedimento a seguir para especificar como os atributos de usuário de suas aplicações devem ser mapeados para atributos correspondentes no IAM Identity Center.

Para mapear atributos da aplicação para atributos no IAM Identity Center

1. Abra o console do IAM Identity Center.
2. Selecione Aplicações.
3. Na lista de aplicações, escolha a aplicação na qual deseja mapear atributos.
4. Na página de detalhes da aplicação, escolha Ações e depois escolha Editar mapeamento de atributos.
5. Escolha Adicionar novo mapeamento de atributo.
6. Na primeira caixa de texto, digite o atributo da aplicação.
7. Na segunda caixa de texto, digite o atributo no IAM Identity Center que você deseja mapear para o atributo da aplicação. Por exemplo, você pode mapear o atributo **`Username`** da aplicação para o atributo **`email`** do usuário do IAM Identity Center. Para ver a lista de atributos de usuário permitidos no IAM Identity Center, consulte a tabela em Mapeamentos de atributos para diretório AWS Managed Microsoft AD.
8. Na terceira coluna da tabela, escolha o formato apropriado para o atributo no menu.
9. Escolha Salvar alterações.

Design de resiliência e comportamento regional

O serviço IAM Identity Center é totalmente gerenciado e usa serviços duráveis AWS e de alta disponibilidade, como o Amazon S3 e o Amazon EC2. Para garantir a disponibilidade no caso de uma interrupção na zona de disponibilidade, o IAM Identity Center opera em várias zonas de disponibilidade. Para obter informações sobre os objetivos de projeto de disponibilidade do IAM Identity Center, consulte Appendix A: Designed-For Availability for Select AWS Services no Reliability Pillar Guide.

Você ativa o IAM Identity Center na sua conta AWS Organizations de gerenciamento. Isso é necessário para que o IAM Identity Center possa provisionar, desprovisionar e atualizar funções em todos os seus Contas da AWS. Quando você ativa o IAM Identity Center, ele é implantado no Região da AWS que está atualmente selecionado. Se você quiser implantar em uma Região da AWS específica, altere a seleção da região antes de ativar o IAM Identity Center.

> **Note**
>
> O IAM Identity Center controla o acesso a seus conjuntos de permissões e aplicativos somente de sua região principal. Recomendamos que você considere os riscos associados ao controle de acesso quando o IAM Identity Center opera em uma única região.

Embora o IAM Identity Center determine o acesso da região na qual você ativa o serviço, Contas da AWS são globais. Isso significa que, depois que os usuários fazem login no IAM Identity Center, eles podem operar em qualquer região quando acessam Contas da AWS por meio do IAM Identity Center. A maioria dos aplicativos AWS gerenciados, como a Amazon SageMaker, no entanto, deve ser instalada na mesma região do IAM Identity Center para que os usuários se autentiquem e atribuam acesso a esses aplicativos. Para obter informações sobre restrições regionais ao usar um aplicativo com o IAM Identity Center, consulte a documentação do aplicativo.

Você também pode usar o IAM Identity Center para autenticar e autorizar o acesso a aplicativos baseados em SAML que podem ser acessados por meio de uma URL pública, independentemente da plataforma ou da nuvem na qual o aplicativo foi criado.

Não recomendamos o uso do Instâncias de conta do IAM Identity Center como meio de implementar resiliência, pois ele cria um segundo ponto de controle isolado que não é conectado à instância da organização.

Configure o acesso de emergência ao AWS Management Console

O IAM Identity Center é construído a partir de uma infraestrutura AWS altamente disponível e usa uma arquitetura de zona de disponibilidade para eliminar pontos únicos de falha. Para obter uma camada extra de proteção no caso improvável de uma central de identidade do IAM ou Região da AWS interrupção, recomendamos que você defina uma configuração que possa ser usada para fornecer acesso temporário aoAWS Management Console.

Conteúdo

Visão geral

O AWS permite:

- Conectar seu IdP de terceiros ao IAM Identity Center.
- Conectar seu IdP de terceiros ao Contas da AWS individual usando a federação baseada em SAML 2.0.

Se você usa o IAM Identity Center, pode usar esses recursos para criar a configuração de acesso de emergência descrita nas seções a seguir. Essa configuração permite que você use o IAM Identity Center como mecanismo de acesso Conta da AWS. Se o IAM Identity Center for interrompido, seus usuários de operações de emergência poderão fazer login no AWS Management Console por meio de federação direta, usando as mesmas credenciais que usam para acessar suas contas. Essa

configuração funciona quando o IAM Identity Center não está disponível, mas o plano de dados do IAM e seu provedor de identidades (IdP) externo estão disponíveis.

> **Important**
>
> Recomendamos que você implante essa configuração antes que ocorra uma interrupção, pois você não poderá criar a configuração se seu acesso para criar as os perfis do IAM necessários também for interrompido. Além disso, teste essa configuração periodicamente para garantir que sua equipe entenda o que fazer se o IAM Identity Center for interrompido.

Resumo da configuração de acesso de emergência

Execute as tarefas a seguir para configurar o acesso de emergência.

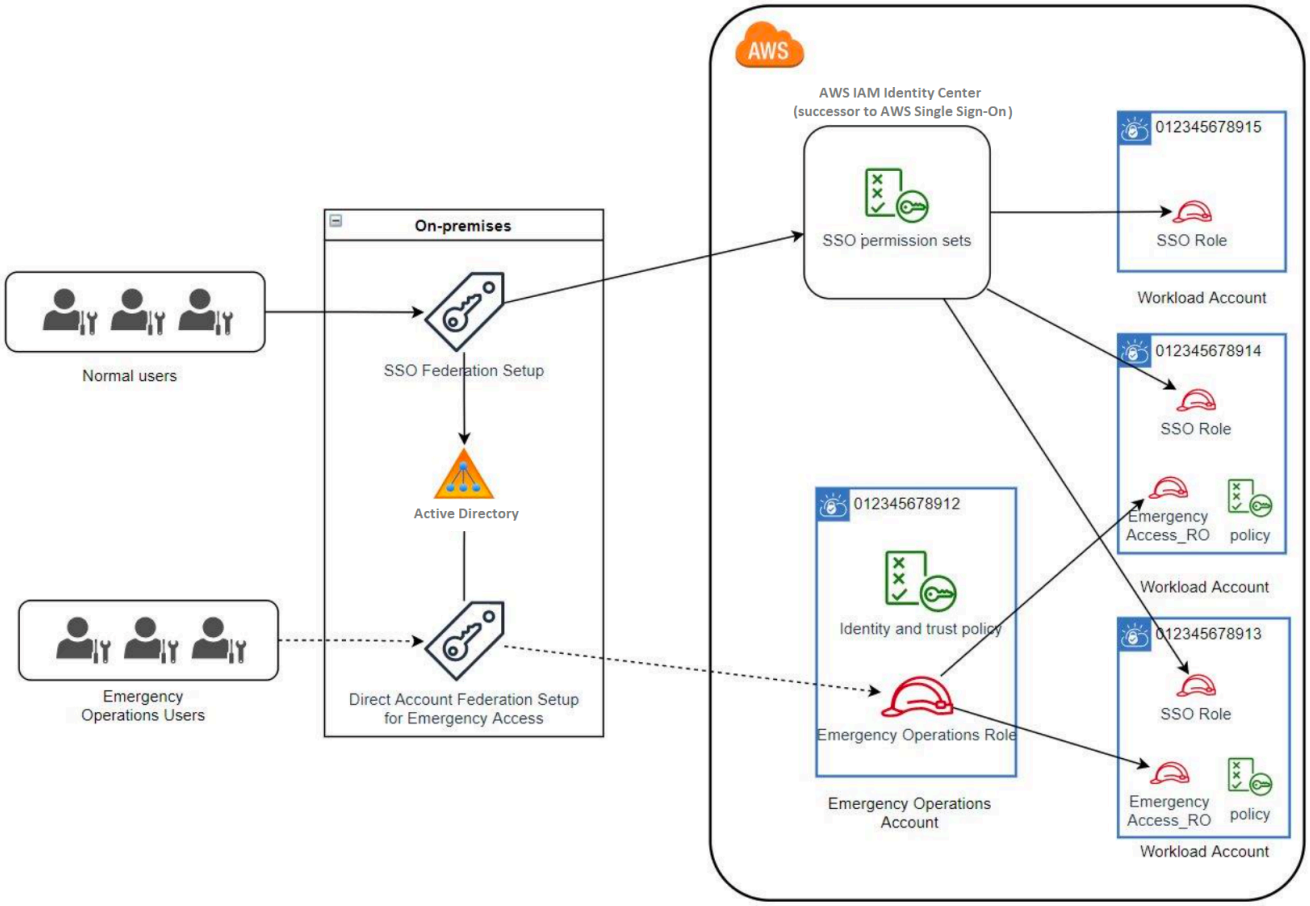
1. Crie uma conta de operações de emergência em sua organização em AWS Organizations.
2. Conecte seu IdP à conta de operações de emergência usando a federação baseada em SAML 2.0.
3. Na conta de operações de emergência, crie uma função para a federação de provedores de identidade de terceiros. Além disso, crie uma função de operações de emergência em cada uma das suas contas de workload, com as permissões necessárias.
4. Delegue acesso às suas contas de workload para o perfil do IAM que você criou na conta de operações de emergência. Para autorizar o acesso à sua conta de operações de emergência, crie um grupo de operações de emergência em seu IdP, sem membros.
5. Permita que o grupo de operações de emergência em seu IdP use a função de operações de emergência criando uma regra em seu IdP que permita o acesso federado do SAML 2.0 ao AWS Management Console.

Durante as operações normais, ninguém tem acesso à conta de operações de emergência porque o grupo de operações de emergência em seu IdP não tem membros. No caso de uma interrupção do IAM Identity Center, use seu IdP para adicionar usuários confiáveis ao grupo de operações de emergência em seu IdP. Esses usuários podem então entrar no seu IdP, navegar até o AWS Management Console e assumir o perfil de operações de emergência na conta de operações de emergência. A partir daí, esses usuários podem alternar perfis para a função de acesso de emergência em suas contas de workload, onde precisam realizar trabalhos operacionais.

Como projetar suas funções operacionais críticas

Com esse design, você configura um único Conta da AWS no qual você federa por meio do IAM, para que os usuários possam assumir funções operacionais críticas. As funções de operações críticas têm uma política de confiança que permite que os usuários assumam uma função correspondente em suas contas de workload. As funções nas contas de workload fornecem as permissões que os usuários precisam para realizar trabalhos essenciais.

O diagrama a seguir oferece uma visão geral de um design.



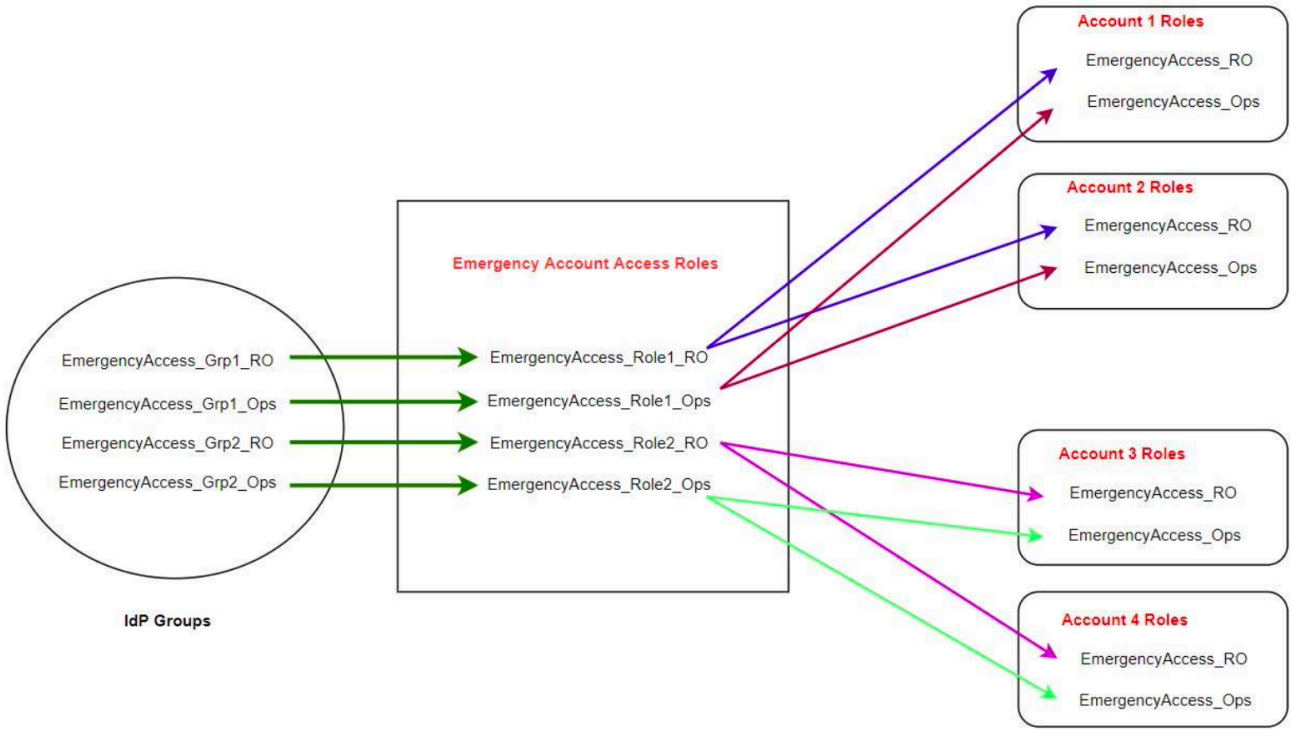
Como planejar seu modelo de acesso

Antes de configurar o acesso de emergência, crie um plano de como o modelo de acesso funcionará. Para criar esse plano, siga este processo.

1. Identifique Contas da AWS onde o acesso do operador de emergência é essencial durante uma interrupção no IAM Identity Center. Por exemplo, suas contas de produção provavelmente são essenciais, mas suas contas de desenvolvimento e teste podem não ser.
2. Para esse conjunto de contas, identifique as funções críticas específicas de que você precisa em suas contas. Em todas essas contas, seja consistente ao definir o que os perfis podem fazer. Isso simplifica o trabalho em sua conta de acesso de emergência, na qual você cria funções entre contas. Recomendamos que você comece com duas funções distintas nessas contas: Somente leitura (RO) e Operações (Ops). Se necessário, você pode criar mais funções e mapear essas funções para um grupo mais distinto de usuários de acesso de emergência em sua configuração.
3. Identifique e crie grupos de acesso de emergência em seu IdP. Os membros do grupo são os usuários aos quais você está delegando acesso às funções de acesso de emergência.
4. Defina quais funções esses grupos podem assumir na conta de acesso de emergência. Para fazer isso, defina regras em seu IdP que gerem declarações que listam quais funções o grupo pode acessar. Esses grupos podem então assumir suas funções de Somente Leitura ou Operações na conta de acesso de emergência. A partir dessas funções, eles podem assumir funções correspondentes em suas contas de workload.

Como criar um mapeamento emergencial de funções, contas e grupos

O diagrama a seguir mostra como mapear seus grupos de acesso de emergência para funções em sua conta de acesso de emergência. O diagrama também mostra as relações de confiança entre contas que permitem que as funções da conta de acesso de emergência acessem as funções correspondentes em suas contas de workload. Recomendamos que o design do seu plano de emergência use esses mapeamentos como ponto de partida.



Como criar sua configuração de acesso de emergência

Use a tabela de mapeamento a seguir para criar sua configuração de acesso de emergência. Essa tabela reflete um plano que inclui duas funções nas contas de workload: somente leitura (RO) e operações (operações), com políticas de confiança e políticas de permissões correspondentes. As políticas de confiança permitem que as funções da conta de acesso de emergência acessem as funções individuais da conta de workload. As funções individuais da conta de workload também têm políticas de permissões sobre o que a função pode fazer na conta. As políticas de permissões podem ser políticas gereciadas por AWS ou políticas gerenciadas pelo cliente.

Conta	Perfis a sertem criados	Política de confiança	Política de permissões
Conta 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
Conta 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator

Conta	Perfis a sertem criados	Política de confiança	Política de permissões
Conta 2	Emergency Access_RO	Emergency Access_Role2_RO	arn:aws:iam: :aws:policy/ ReadOnlyAccess
Conta 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:policy/job-function/ SystemAdministrator
Conta-acesso de emergência	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO Emergency Access_Role2_Ops	IdP	AssumeRole para recurso de função na conta

Nesse plano de mapeamento, a conta de acesso de emergência contém dois perfis somente para leitura e dois perfis de operações. Esses perfis confiam em seu IdP para autenticar e autorizar seus grupos selecionados a acessar os perfis transmitindo os nomes dos perfis nas afirmações. Há perfis correspondentes somente para leitura e operações na Conta 1 e na Conta 2 da workload. Para a Conta de workload 1, o `EmergencyAccess_RO` perfil confia no `EmergencyAccess_Role1_RO` perfil que reside na conta de acesso de emergência. A tabela especifica padrões de confiança semelhantes entre os perfis somente para leitura e operações da conta de workload e os perfis de acesso de emergência correspondentes.

Tarefas preparatórias de emergência

Para preparar sua configuração de acesso de emergência, recomendamos realizar as seguintes tarefas antes que uma emergência ocorra.

1. Configure um aplicativo direto de federação do IAM em seu IdP. Para ter mais informações, consulte Configuração única de um aplicativo de federação direta do IAM no Okta.

2. Crie uma conexão IdP na conta de acesso de emergência que possa ser acessada durante o evento.
3. Crie funções de acesso de emergência nas contas de acesso de emergência, conforme descrito na tabela de mapeamento acima.
4. Crie funções de operações temporárias com políticas de confiança e permissão em cada uma das contas de workload.
5. Crie grupos de operações temporárias em seu IdP. Os nomes dos grupos dependerão dos nomes das funções de operações temporárias.
6. Teste a federação direta do IAM.
7. Desative o aplicativo de federação de IdP em seu IdP para evitar o uso regular.

Processo de failover de emergência

Quando uma instância do IAM Identity Center não está disponível e você determina que precisa fornecer acesso de emergência ao Console de Gerenciamento AWS, recomendamos o seguinte processo de failover.

1. O administrador do IdP ativa o aplicativo direto de federação do IAM em seu IdP.
2. Os usuários solicitam acesso ao grupo de operações temporárias por meio de seu mecanismo existente, como uma solicitação por e-mail, canal do Slack ou outra forma de comunicação.
3. Os usuários que você adiciona aos seus grupos de acesso de emergência entram no IdP, selecionam a conta de acesso de emergência e escolhem uma função para usar na conta de acesso de emergência. A partir desses perfis, eles podem assumir funções em contas de workload correspondentes que tenham confiança entre contas com p perfil de conta de emergência.

Retorno às operações normais

Verifique o AWS Health Dashboardpara confirmar quando a integridade do serviço IAM Identity Center foi restaurada. Para retornar às operações normais, execute as etapas a seguir.

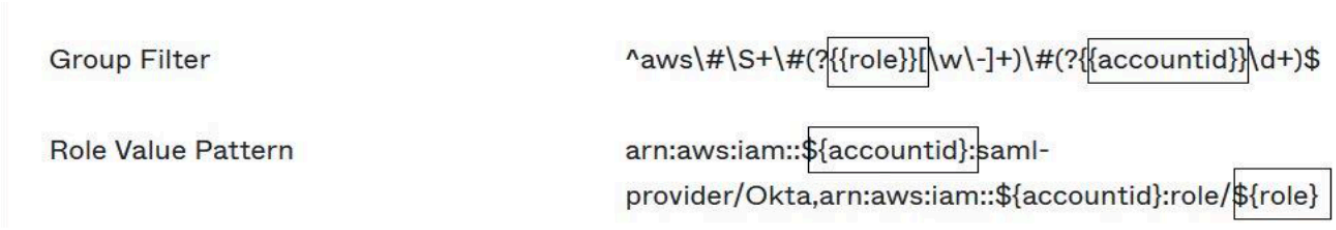
1. Depois que o ícone de status do serviço IAM Identity Center indicar que o serviço está íntegro, faça login no IAM Identity Center.

2. Se você conseguir entrar no IAM Identity Center com sucesso, comunique aos usuários de acesso de emergência que o IAM Identity Center está disponível. Instrua esses usuários a se desconectarem e usarem o portal de acesso AWS para entrar novamente no IAM Identity Center.
3. Depois que todos os usuários de acesso de emergência se desconectarem, no IdP, desative o aplicativo de federação de IdP. Recomendamos que essa tarefa seja executada após o horário de trabalho.
4. Remova todos os usuários do grupo de acesso de emergência no IdP.

Sua infraestrutura de perfil de acesso de emergência permanece em vigor como um plano de acesso de backup, mas agora está desativada.

Configuração única de um aplicativo de federação direta do IAM no Okta

1. Uma conta da Okta com a qual você possa fazer login como usuário com permissões administrativas.
2. No Okta Admin Console, em Applications, escolha Applications,
3. Escolha Browse App Catalog. Pesquise e escolha AWS Account Federation. Escolha Add integration.
4. Configure a federação direta do IAM AWS seguindo as etapas em How to Configure SAML 2.0 for de AWS Account Federation.
5. Na guia Sign-On Options, selecione SAML 2.0 e insira as configurações de Group Filter e Role Value Pattern. O nome do grupo para o diretório do usuário depende do filtro que você configura.



Na figura acima, a `role` variável é para o perfil de operações de emergência em sua conta de acesso de emergência. Por exemplo, se você criar o perfil `EmergencyAccess_Role1_R0` (conforme descrito na tabela de mapeamento) em Conta da AWS`123456789012`, e se a configuração do filtro de grupo estiver configurada conforme mostrado na figura acima, o nome do seu grupo deverá ser `aws#EmergencyAccess_Role1_R0#123456789012`.

6. Em seu diretório (por exemplo, seu diretório no Active Directory), crie o grupo de acesso de emergência e especifique um nome para o diretório (por exemplo, `aws#EmergencyAccess_Role1_R0#123456789012`). Atribua seus usuários a esse grupo usando seu mecanismo de provisionamento existente.
7. Na conta de acesso de emergência, configure uma política de confiança personalizada que forneça as permissões necessárias para que o perfil de acesso de emergência seja assumido durante uma interrupção. Veja a seguir um exemplo de declaração de uma política de confiança personalizada anexada ao `EmergencyAccess_Role1_R0` perfil. Para ver uma ilustração, consulte a conta de emergência no diagrama em Como criar um mapeamento emergencial de funções, contas e grupos.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
         "Effect":"Allow",
         "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
         },
         "Action":[
            "sts:AssumeRoleWithSAML",
            "sts:SetSourceIdentity",
            "sts:TagSession"
         ],
         "Condition":{
            "StringEquals":{
               "SAML:aud":"https:~/~/signin.aws.amazon.com/saml"
            }
         }
      }
   ]
}
```

8. Veja a seguir um exemplo de declaração de uma política de confiança personalizada anexada ao perfil `EmergencyAccess_Role1_R0`. Para ver uma ilustração, consulte a conta de emergência no diagrama em Como criar um mapeamento emergencial de funções, contas e grupos.

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

```
      {
         "Effect":"Allow",
         "Action":"sts:AssumeRole",
         "Resource":[
            "arn:aws:iam::<account 1>:role/EmergencyAccess_RO",
            "arn:aws:iam::<account 2>:role/EmergencyAccess_RO"
         ]
      }
   ]
}
```

9. Nas contas de workload, configure uma política de confiança personalizada. Veja a seguir um exemplo de declaração de uma política de confiança personalizada anexada ao perfil `EmergencyAccess_RO`. Neste exemplo, a conta `123456789012` é a conta de acesso de emergência. Para ver uma ilustração, consulte a conta de workload no diagrama abaixo [Como criar um mapeamento emergencial de funções, contas e grupos].

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

> **Note**
>
> A maioria IdPs permite que você mantenha a integração de aplicativos desativada até que seja necessária. Recomendamos que você mantenha o aplicativo de federação direta do IAM desativado em seu IdP até que seja necessário para acesso de emergência.

Segurança em AWS IAM Identity Center

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

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos compliance programs AWS. Para saber mais sobre os programas de conformidade aplicáveis AWS IAM Identity Center, consulte AWS Serviços no escopo por programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o IAM Identity Center. Os tópicos a seguir mostram como configurar o IAM Identity Center para atender aos seus objetivos de segurança e de conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do IAM Identity Center.

Tópicos

Gerenciamento de identidade e acesso para o IAM Identity Center

O acesso ao IAM Identity Center requer credenciais que AWS possam ser usadas para autenticar suas solicitações. Essas credenciais devem ter permissões para acessar AWS recursos, como um aplicativo AWS gerenciado.

A autenticação no portal de AWS acesso é controlada pelo diretório que você conectou ao IAM Identity Center. No entanto, a autorização para os Contas da AWS que estão disponíveis para os usuários de dentro do portal de AWS acesso é determinada por dois fatores:

1. A quem foi atribuído acesso às pessoas Contas da AWS no console do IAM Identity Center. Para ter mais informações, consulte Acesso com login único a Contas da AWS.
2. Que nível de permissão foi concedido aos usuários finais no console do IAM Identity Center para lhes conceder acesso apropriado a Contas da AWS. Para ter mais informações, consulte Criar, gerenciar e excluir conjuntos de permissões.

As seções a seguir explicam como você, como administrador, pode controlar o acesso ao console do IAM Identity Center ou delegar acesso administrativo para day-to-day tarefas do console do IAM Identity Center.

- Autenticação
- Controle de acesso

Autenticação

Saiba como acessar AWS usando identidades do IAM.

Controle de acesso

Você pode ter credenciais válidas para autenticar suas solicitações, mas, a menos que tenha permissões, não poderá criar nem acessar os recursos do IAM Identity Center. Por exemplo, você deve ter permissões para criar um diretório conectado do IAM Identity Center.

As seções a seguir descrevem como gerenciar permissões para o IAM Identity Center. Recomendamos que você leia a visão geral primeiro.

- Visão geral do gerenciamento de permissões de acesso aos seus recursos do IAM Identity Center

- Exemplos de políticas baseadas em identidade para o IAM Identity Center
- As funções vinculadas ao serviço do IAM Identity Center permanecem.

Visão geral do gerenciamento de permissões de acesso aos seus recursos do IAM Identity Center

Cada AWS recurso é de propriedade de um Conta da AWS, e as permissões para criar ou acessar os recursos são regidas por políticas de permissões. Um administrador de conta pode anexar políticas de permissões a identidades do IAM (ou seja, usuários, grupos e perfis). Alguns serviços (como o AWS Lambda) também oferecem suporte à anexação de políticas de permissões aos recursos.

> **Note**
>
> Um administrador da conta (ou usuário administrador) é um usuário com privilégios de administrador. Para obter mais informações, consulte Melhores práticas do IAM no IAM User Guide.

Tópicos

- Recursos e operações do IAM Identity Center
- Informações sobre propriedade de recursos
- Gerenciamento de acesso aos recursos
- Especificar elementos da política: ações, efeitos, recursos e entidades principais
- Especificar condições em uma política

Recursos e operações do IAM Identity Center

No IAM Identity Center, os recursos principais são instâncias, perfis e conjuntos de permissões e aplicativos.

Informações sobre propriedade de recursos

O proprietário de um recurso é Conta da AWS aquele que criou um recurso. Ou seja, o proprietário Conta da AWS do recurso é a entidade principal (a conta, um usuário ou uma função do IAM) que autentica a solicitação que cria o recurso. Os seguintes exemplos mostram como isso funciona:

- Se Usuário raiz da conta da AWS criar um recurso do IAM Identity Center, como uma instância de aplicativo ou um conjunto de permissões, você Conta da AWS é o proprietário desse recurso.
- Se você criar um usuário em sua AWS conta e conceder a esse usuário permissões para criar recursos do IAM Identity Center, o usuário poderá então criar recursos do IAM Identity Center. No entanto, sua AWS conta, à qual o usuário pertence, possui os recursos.
- Se você criar uma função do IAM em sua AWS conta com permissões para criar recursos do IAM Identity Center, qualquer pessoa que possa assumir a função poderá criar recursos do IAM Identity Center. Sua Conta da AWS, à qual pertence o perfil, é proprietária dos recursos do IAM Identity Center.

Gerenciamento de acesso aos recursos

A política de permissões descreve quem tem acesso a quê. A seção a seguir explica as opções disponíveis para a criação de políticas de permissões.

> **Note**
>
> Esta seção discute o uso do IAM no contexto do IAM Identity Center. Não são fornecidas informações detalhadas sobre o serviço IAM. Para ver a documentação completa do IAM, consulte What is IAM? no IAM User Guide. Para obter informações sobre a sintaxe e as descrições da política do IAM, consulte a IAM policy reference AWS no IAM User Guide.

As políticas anexadas a uma identidade do IAM são chamadas de políticas baseadas em identidade (políticas do IAM). As políticas anexadas a um recurso são chamadas de políticas baseadas em recursos. O IAM Identity Center oferece suporte apenas às políticas baseadas em identidade (políticas do IAM).

Tópicos

- Políticas baseadas em identidade (políticas do IAM)
- Políticas baseadas em atributos

Políticas baseadas em identidade (políticas do IAM)

Você pode adicionar permissões a identidades do IAM. Por exemplo, você pode fazer o seguinte:

- Anexe uma política de permissões a um usuário ou grupo em seu Conta da AWS — Um administrador da conta pode usar uma política de permissões associada a um usuário específico para conceder permissões para que esse usuário adicione um recurso do IAM Identity Center, como um novo aplicativo.
- Anexar uma política de permissões a uma função: você pode anexar uma política de permissões baseada em identidade a um perfil do IAM para conceder permissões entre contas.

  Para obter mais informações sobre o uso do IAM para delegar permissões, consulte Access management no IAM User Guide.

A seguinte política de permissões concede permissões a um usuário para executar todas as ações que começam com `List`. Essas ações mostram informações sobre um recurso do IAM Identity Center, como uma instância de aplicativo ou conjunto de permissões. Observe que o caractere curinga (*) no elemento `Resource` indica que as ações são permitidas para todos os recursos do IAM Identity Center pertencentes à conta.

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

Para obter mais informações sobre o uso de políticas baseadas em identidade com o IAM Identity Center, consulte Exemplos de políticas baseadas em identidade para o IAM Identity Center. Para obter mais informações sobre usuários, grupos, funções e permissões, consulte Identities (users, groups, and roles) no Guia do usuário do IAM.

Políticas baseadas em atributos

Outros serviços, como o Amazon S3, também aceitam políticas de permissões baseadas em recurso. Por exemplo: você pode anexar uma política a um bucket do S3 para gerenciar permissões de acesso a esse bucket. O IAM Identity Center não é compatível com Políticas baseadas em recursos.

Especificar elementos da política: ações, efeitos, recursos e entidades principais

Para cada recurso do IAM Identity Center (consulte Recursos e operações do IAM Identity Center), o serviço define um conjunto de operações da API. Para conceder permissões a essas operações da API, o IAM Identity Center define um conjunto de ações que podem ser especificadas em uma política. Observe que a execução de uma operação de API pode exigir permissões para mais de uma ação.

Estes são os elementos de política básicos:

- Recurso: em uma política, você usa um nome do recurso da Amazon (ARN) para identificar o recurso a que a política se aplica.
- Ação: você usa palavras-chave de ação para identificar operações de recursos que deseja permitir ou negar. Por exemplo, a permissão `sso:DescribePermissionsPolicies` permite que o usuário execute a operação `DescribePermissionsPolicies` do IAM Identity Center.
- Efeito: você especifica o efeito quando o usuário solicita a ação específica, que pode ser permitir ou negar. Se você não conceder (permitir) explicitamente acesso a um recurso, o acesso estará implicitamente negado. Você também pode negar explicitamente o acesso a um recurso, para ter certeza de que um usuário não consiga acessá-lo, mesmo que uma política diferente conceda acesso.
- Entidade principal: em políticas baseadas em identidade (políticas do IAM), o usuário ao qual a política é anexada é a entidade principal implícita. Para as políticas baseadas em recursos, você especifica quais usuários, contas, serviços ou outras entidades deseja que recebam permissões (isso se aplica somente a políticas baseadas em recursos). O IAM Identity Center não é compatível com Políticas baseadas em recursos.

Para saber mais sobre a sintaxe e as descrições da política do IAM, consulte IAM policy reference AWS no IAM User Guide.

Especificar condições em uma política

Ao conceder permissões, você pode usar a linguagem de política de acesso para especificar as condições que devem ser atendidas para que uma política entre em vigor. Por exemplo, é recomendável aplicar uma política somente após uma data específica. Para obter mais informações sobre como especificar condições em uma linguagem de política, consulte Condition no Guia do usuário do IAM.

Para expressar condições, você usa chaves de condição predefinidas. Não existem chaves de condição específicas do IAM Identity Center. No entanto, existem chaves de AWS condição que você pode usar conforme apropriado. Para obter uma lista completa das AWS chaves, consulte Chaves de condição globais disponíveis no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para o IAM Identity Center

Este tópico fornece exemplos de políticas do IAM que você pode criar para conceder aos usuários e perfis permissões para administrar o IAM Identity Center.

> **Important**
>
> Recomendamos analisar primeiro os tópicos introdutórios que explicam os conceitos básicos e as opções disponíveis para gerenciar o acesso aos recursos do seu IAM Identity Center. Para ter mais informações, consulte Visão geral do gerenciamento de permissões de acesso aos seus recursos do IAM Identity Center.

As seções neste tópico abrangem o seguinte:

- Exemplos de políticas personalizadas
- Permissões necessárias para usar o console do IAM Identity Center

Exemplos de políticas personalizadas

Esta seção fornece exemplos de casos de uso comuns que exigem uma política do IAM personalizada. Esses exemplos de políticas são políticas baseadas em identidade, que não especificam o elemento da entidade principal. Isso ocorre porque, com uma política baseada em identidade, não se especifica a entidade principal que obtém as permissões. Em vez disso, você anexa a política à entidade entidade principal. Quando você anexa uma política de permissão baseada em identidade a um perfil do IAM, a entidade principal identificada na política de confiança do perfil obtém as permissões. Você pode criar políticas baseadas em identidade no IAM e anexá-las a usuários, grupos e/ou funções. Você também pode aplicar essas políticas aos usuários do IAM Identity Center ao criar um conjunto de permissões no IAM Identity Center.

> **Note**
>
> Use esses exemplos ao criar políticas para seu ambiente e certifique-se de testar casos de teste positivos (“acesso concedido”) e negativos (“acesso negado”) antes de implantar essas políticas em seu ambiente de produção. Para obter mais informações sobre como testar políticas do IAM, consulte Testing IAM policies with the IAM policy simulator no Guia do usuário do IAM.

Tópicos

Exemplo 1: permitir que um usuário visualize o IAM Identity Center

A política de permissões a seguir concede permissões somente de leitura a um usuário para que ele possa visualizar todas as configurações e informações de diretório configuradas no IAM Identity Center.

> **Note**
>
> Esta política é fornecida apenas para fins de exemplo. Em um ambiente de produção, recomendamos que você use a política `ViewOnlyAccess` AWS gerenciada para o IAM Identity Center.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ds:DescribeDirectories",
                "ds:DescribeTrusts",
                "iam:ListPolicies",
```

```
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListAccountsForParent",
                "organizations:ListOrganizationalUnitsForParent",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListPermissionSets",
                "sso:DescribePermissionSet",
                "sso:GetInlinePolicyForPermissionSet",
                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo 2: permitir que um usuário gerencie permissões Contas da AWS no IAM Identity Center

A política de permissões a seguir concede permissões para permitir que um usuário crie, gerencie e implemente conjuntos de permissões para o seu Contas da AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeleteInlinePolicyFromPermissionSet",
                "sso:DeletePermissionSet",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:ProvisionPermissionSet",
```

```
                "sso:PutInlinePolicyToPermissionSet",
                "sso:UpdatePermissionSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMListPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:ListPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AccessToSSOProvisionedRoles",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetSAMLProvider"
            ],
            "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
        }
    ]
}
```

> **Note**
>
> As permissões adicionais listadas nas `"Sid": "IAMListPermissions"` `"Sid": "AccessToSSOProvisiondRoles"` seções e são necessárias somente para permitir que o usuário crie atribuições na conta AWS Organizations de gerenciamento. Em certos casos, também pode ser necessário adicionar itens `iam:UpdateSAMLProvider` a essas seções.

Exemplo 3: permitir que um usuário gerencie aplicativos no IAM Identity Center

A política de permissões a seguir concede permissões para permitir que um usuário visualize e configure aplicativos no IAM Identity Center, incluindo aplicativos SaaS pré-integrados do catálogo do IAM Identity Center.

> **Note**
>
> A operação `sso:AssociateProfile` usada no exemplo de política a seguir é necessária para o gerenciamento das atribuições de usuários e grupos aos aplicativos. Também permite que um usuário atribua usuários e grupos Contas da AWS usando os conjuntos de permissões existentes. Se um usuário precisar gerenciar o Conta da AWS acesso no IAM Identity Center e exigir as permissões necessárias para gerenciar os conjuntos de permissões, consulteExemplo 2: permitir que um usuário gerencie permissões Contas da AWS no IAM Identity Center.

Em outubro de 2020, muitas dessas operações estavam disponíveis somente por meio do console AWS . Esse exemplo de política inclui ações de “leitura”, como listar, obter e pesquisar, que são relevantes para a operação sem erros do console nesse caso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:ImportApplicationInstanceServiceProviderMetadata",
                "sso:DeleteApplicationInstance",
```

```
                "sso:DeleteProfile",
                "sso:DisassociateProfile",
                "sso:GetApplicationTemplate",
                "sso:UpdateApplicationInstanceServiceProviderConfiguration",
                "sso:UpdateApplicationInstanceDisplayData",
                "sso:DeleteManagedApplicationInstance",
                "sso:UpdateApplicationInstanceStatus",
                "sso:GetManagedApplicationInstance",
                "sso:UpdateManagedApplicationInstanceStatus",
                "sso:CreateManagedApplicationInstance",
                "sso:UpdateApplicationInstanceSecurityConfiguration",
                "sso:UpdateApplicationInstanceResponseConfiguration",
                "sso:GetApplicationInstance",
                "sso:CreateApplicationInstanceCertificate",
                "sso:UpdateApplicationInstanceResponseSchemaConfiguration",
                "sso:UpdateApplicationInstanceActiveCertificate",
                "sso:DeleteApplicationInstanceCertificate",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationTemplates",
                "sso:ListApplications",
                "sso:ListApplicationInstances",
                "sso:ListDirectoryAssociations",
                "sso:ListProfiles",
                "sso:ListProfileAssociations",
                "sso:ListInstances",
                "sso:GetProfile",
                "sso:GetSSOStatus",
                "sso:GetSsoConfiguration",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeUsers",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo 4: permitir que um usuário gerencie usuários e grupos no seu diretório do Identity Center

A seguinte política de permissões concede permissões para permitir que um usuário crie, visualize, modifique e exclua usuários e grupos no IAM Identity Center.

Em alguns casos, as modificações diretas nos usuários e grupos no IAM Identity Center são restritas. Por exemplo, quando o Active Directory, ou um provedor de identidade externo com o provisionamento automático ativado, é selecionado como fonte de identidade.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso-directory:ListGroupsForUser",
                "sso-directory:DisableUser",
                "sso-directory:EnableUser",
                "sso-directory:SearchGroups",
                "sso-directory:DeleteGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:DescribeDirectory",
                "sso-directory:UpdateUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:SearchUsers",
                "sso:ListDirectoryAssociations",
                "sso-directory:RemoveMemberFromGroup",
                "sso-directory:DeleteUser",
                "sso-directory:DescribeUsers",
                "sso-directory:UpdateGroup",
                "sso-directory:CreateGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

Permissões necessárias para usar o console do IAM Identity Center

Para que um usuário trabalhe com o console do IAM Identity Center sem erros, são necessárias permissões adicionais. Se você criar uma política do IAM que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para os usuários com essa política. O exemplo a seguir lista o conjunto de permissões que podem ser necessárias para garantir uma operação sem erros no console do IAM Identity Center.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DescribeAccountAssignmentCreationStatus",
                "sso:DescribeAccountAssignmentDeletionStatus",
                "sso:DescribePermissionSet",
                "sso:DescribePermissionSetProvisioningStatus",
                "sso:DescribePermissionsPolicies",
                "sso:DescribeRegisteredRegions",
                "sso:GetApplicationInstance",
                "sso:GetApplicationTemplate",
                "sso:GetInlinePolicyForPermissionSet",
                "sso:GetManagedApplicationInstance",
                "sso:GetMfaDeviceManagementForDirectory",
                "sso:GetPermissionSet",
                "sso:GetPermissionsPolicy",
                "sso:GetProfile",
                "sso:GetSharedSsoConfiguration",
                "sso:GetSsoConfiguration",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:ListAccountAssignmentCreationStatus",
                "sso:ListAccountAssignmentDeletionStatus",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationInstances",
                "sso:ListApplications",
                "sso:ListApplicationTemplates",
                "sso:ListDirectoryAssociations",
                "sso:ListInstances",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetProvisioningStatus",
                "sso:ListPermissionSets",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListProfileAssociations",
                "sso:ListProfiles",
                "sso:ListTagsForResource",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeGroups",
```

```
                "sso-directory:DescribeUsers",
                "sso-directory:ListGroupsForUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS políticas gerenciadas para o IAM Identity Center

É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre as políticas gerenciadas da AWS , consulte Políticas gerenciadas da AWS no IAM User Guide.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos atributos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e perfis) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo atributo for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de funções de trabalho, consulte managed policies for job functions AWS para funções de trabalho no IAM User Guide.

Novas ações que permitem listar e excluir sessões de usuário estão disponíveis no novo namespace`identitystore-auth`. Quaisquer permissões adicionais para ações nesse namespace serão atualizadas nesta página. Ao criar suas políticas personalizadas do IAM, evite usar * depois de `identitystore-auth`, pois isso se aplica a todas as ações que existem no namespace hoje ou no futuro.

AWS política gerenciada: AWSSSOMasterAccountAdministrator

A política `AWSSSOMasterAccountAdministrator` fornece as ações administrativas necessárias às entidades principais A política é destinada a diretores que desempenham a função de AWS IAM Identity Center administrador. Com o tempo, a lista de ações fornecidas será atualizada para corresponder à funcionalidade existente do IAM Identity Center e às ações que são necessárias como administrador.

É possível anexar a política `AWSSSOMasterAccountAdministrator` a suas identidades do IAM. Ao anexar a `AWSSSOMasterAccountAdministrator` política a uma identidade, você concede AWS IAM Identity Center permissões administrativas. Os diretores com essa política podem acessar o IAM Identity Center na conta de AWS Organizations gerenciamento e em todas as contas dos membros. Essa entidade principal pode gerenciar totalmente todas as operações do IAM Identity Center, incluindo a capacidade de criar uma instância do IAM Identity Center, usuários, conjuntos de permissões e atribuições. O diretor também pode instanciar essas atribuições em todas as contas dos membros da AWS organização e estabelecer conexões entre os diretórios AWS Directory Service gerenciados e o IAM Identity Center. À medida que novos atributos administrativos forem lançados, o administrador da conta receberá essas permissões automaticamente.

Agrupamentos de permissões

Esta política é agrupada em declarações com base no conjunto de permissões fornecidas.

- `AWSSSOMasterAccountAdministrator`— Permite que o IAM Identity Center transmita o perfil de serviço chamado `AWSServiceRoleforSSO` para o IAM Identity Center para que ele possa posteriormente assumir o perfil e realizar ações em seu nome. Isso é necessário quando a pessoa ou o aplicativo tenta ativar o IAM Identity Center. Para ter mais informações, consulte Gerencie o acesso ao Contas da AWS.
- `AWSSSOMemberAccountAdministrator`— Permite que o IAM Identity Center execute ações do administrador da conta em um AWS ambiente com várias contas. Para ter mais informações, consulte AWS política gerenciada: AWSSSOMemberAccountAdministrator.
- `AWSSSOManageDelegatedAdministrator`— Permite que o IAM Identity Center registre e cancele o registro de um administrador delegado para sua organização.

Para ver as permissões dessa política, consulte AWSSSOMasterAccountAdministratorem Referência de política AWS gerenciada.

Informações adicionais sobre essa política.

Quando o IAM Identity Center é ativado pela primeira vez, o serviço IAM Identity Center cria uma função vinculada ao serviço na conta AWS Organizations de gerenciamento (antiga conta principal) para que o IAM Identity Center possa gerenciar os recursos em sua conta. As ações necessárias são `iam:CreateServiceLinkedRole` e `iam:PassRole`, que são mostradas nos trechos a seguir.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "AWSSSOCreateSLR",
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "sso.amazonaws.com"
            }
         }
      },
      {
         "Sid":"AWSSSOMasterAccountAdministrator",
         "Effect":"Allow",
         "Action":"iam:PassRole",
         "Resource":"arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition":{
             "StringLike":{
               "iam:PassedToService":"sso.amazonaws.com"
             }
         }
      },
   ]
}
```

AWS política gerenciada: AWSSSOMemberAccountAdministrator

A política `AWSSSOMemberAccountAdministrator` fornece as ações administrativas necessárias às entidades principais A política é destinada a entidades principais que desempenham a função de administrador de um IAM Identity Center. Com o tempo, a lista de ações fornecidas será atualizada

para corresponder à funcionalidade existente do IAM Identity Center e às ações que são necessárias como administrador.

É possível anexar a política `AWSSSOMemberAccountAdministrator` a suas identidades do IAM. Ao anexar a `AWSSSOMemberAccountAdministrator` política a uma identidade, você concede AWS IAM Identity Center permissões administrativas. Os diretores com essa política podem acessar o IAM Identity Center na conta de AWS Organizations gerenciamento e em todas as contas dos membros. Essa entidade principal pode gerenciar totalmente todas as operações do IAM Identity Center, incluindo a capacidade de criar usuários, conjuntos de permissões e atribuições. O diretor também pode instanciar essas atribuições em todas as contas dos membros da AWS organização e estabelecer conexões entre os diretórios AWS Directory Service gerenciados e o IAM Identity Center. À medida que novos atributos administrativos forem lançados, o administrador da conta receberá essas permissões automaticamente.

Para ver as permissões dessa política, consulte AWSSSOMemberAccountAdministratorem Referência de política AWS gerenciada.

Informações adicionais sobre essa política.

Os administradores do IAM Identity Center gerenciam usuários, grupos e senhas em seu repositório de diretórios do Identity Center (diretório sso). A função de administrador da conta inclui permissões para as seguintes ações:

- `"sso:*"`
- `"sso-directory:*"`

Os administradores do IAM Identity Center precisam de permissões limitadas para as seguintes AWS Directory Service ações para realizar tarefas diárias.

- `"ds:DescribeTrusts"`
- `"ds:UnauthorizeApplication"`
- `"ds:DescribeDirectories"`
- `"ds:AuthorizeApplication"`
- `“ds:CreateAlias”`

Essas permissões permitem que os administradores do IAM Identity Center identifiquem os diretórios existentes e gerenciem aplicativos para que possam ser configurados para uso com o IAM Identity

Center. Para obter mais informações sobre cada uma dessas ações, consulte Permissões AWS Directory Service da API: referência de ações, recursos e condições.

O IAM Identity Center usa políticas do IAM para conceder permissões aos usuários do IAM Identity Center. Os administradores do IAM Identity Center criam conjuntos de permissões e anexam políticas a eles. O administrador do IAM Identity Center deve ter as permissões para listar as políticas existentes para poder escolher quais políticas usar com o conjunto de permissões que está criando ou atualizando. Para definir permissões seguras e funcionais, o administrador do IAM Identity Center deve ter permissões para executar a validação da política do IAM Access Analyzer.

- `"iam:ListPolicies"`
- `"access-analyzer:ValidatePolicy"`

Os administradores do IAM Identity Center precisam de acesso limitado às seguintes AWS Organizations ações para realizar tarefas diárias:

- `"organizations:EnableAWSServiceAccess"`
- `"organizations:ListRoots"`
- `"organizations:ListAccounts"`
- `"organizations:ListOrganizationalUnitsForParent"`
- `"organizations:ListAccountsForParent"`
- `"organizations:DescribeOrganization"`
- `"organizations:ListChildren"`
- `"organizations:DescribeAccount"`
- `"organizations:ListParents"`
- `"organizations:ListDelegatedAdministrators"`
- `"organizations:RegisterDelegatedAdministrator"`
- `"organizations:DeregisterDelegatedAdministrator"`

Essas permissões permitem que os administradores do IAM Identity Center trabalhem com os recursos da organização (contas) para tarefas administrativas básicas do IAM Identity Center, como as seguintes:

- Identificar a conta de gerenciamento que pertence à organização
- Identificar as contas dos membros que pertencem à organização

- Habilitando AWS o acesso ao serviço para contas
- Configurar um administrador delegado

Para obter mais informações sobre como usar um administrador delegado com o IAM Identity Center, consulteAdministradores delegados. Para obter mais informações sobre como essas permissões são usadas com AWS Organizations, consulte Usando AWS Organizations com outros AWS serviços.

AWS política gerenciada: AWSSSODirectoryAdministrator

É possível anexar a política `AWSSSODirectoryAdministrator` a suas identidades do IAM.

Essa política concede permissões administrativas aos usuários e grupos do IAM Identity Center. Os diretores com essa política anexada podem fazer qualquer atualização nos usuários e grupos do IAM Identity Center.

Para ver as permissões dessa política, consulte AWSSSODirectoryAdministratorem Referência de política AWS gerenciada.

AWS política gerenciada: AWSSSOReadOnly

É possível anexar a política `AWSSSOReadOnly` a suas identidades do IAM.

Esta política concede permissões de acesso somente para leitura que permitem que usuários visualizem informações no IAM Identity Center. Os diretores com essa política anexada não podem visualizar diretamente os usuários ou grupos do IAM Identity Center. Os diretores com essa política anexada não podem fazer nenhuma atualização no IAM Identity Center. Por exemplo, diretores com essas permissões podem visualizar as configurações do IAM Identity Center, mas não podem alterar nenhum dos valores da configuração.

Para ver as permissões dessa política, consulte AWSSSOReadOnlyem Referência de política AWS gerenciada.

AWS política gerenciada: AWSSSODirectoryReadOnly

É possível anexar a política `AWSSSODirectoryReadOnly` a suas identidades do IAM.

Essa política concede permissões somente para leitura que permitem que os usuários visualizem usuários e grupos no IAM Identity Center. Os diretores com essa política anexada não podem visualizar as atribuições, os conjuntos de permissões, os aplicativos ou as configurações do IAM Identity Center. Os diretores com essa política anexada não podem fazer nenhuma atualização no IAM Identity Center. Por exemplo, diretores com essas permissões podem visualizar os usuários do

IAM Identity Center, mas não podem alterar nenhum atributo do usuário nem atribuir dispositivos de MFA.

Para ver as permissões dessa política, consulte AWSSSODirectoryReadOnlyem Referência de política AWS gerenciada.

AWS política gerenciada: AWSIdentitySyncFullAccess

É possível anexar a política `AWSIdentitySyncFullAccess` a suas identidades do IAM.

As entidades principais com esta política anexada têm permissões de acesso total para criar e excluir perfis de sincronização, associar ou atualizar um perfil de sincronização a um destino de sincronização, criar, listar e excluir filtros de sincronização e iniciar ou interromper a sincronização.

Detalhes da permissão

Para ver as permissões dessa política, consulte AWSIdentitySyncFullAccessem Referência de política AWS gerenciada.

AWS política gerenciada: AWSIdentitySyncReadOnlyAccess

É possível anexar a política `AWSIdentitySyncReadOnlyAccess` a suas identidades do IAM.

Essa política concede permissões somente para leitura que permitem que os usuários visualizem informações sobre o perfil de sincronização de identidade, filtros e configurações de destino.
As entidades principais com essa política anexada não podem fazer nenhuma atualização nas configurações de sincronização. Por exemplo, entidades principais com essas permissões podem visualizar as configurações de sincronização de identidade, mas não podem alterar nenhum valor do perfil ou do filtro.

Para ver as permissões dessa política, consulte AWSIdentitySyncReadOnlyAccessem Referência de política AWS gerenciada.

AWS política gerenciada: AWSSSOServiceRolePolicy

É possível anexar a política `AWSSSOServiceRolePolicy` a suas identidades do IAM.

Essa política é anexada a uma função vinculada ao serviço que permite que o IAM Identity Center delegue e imponha quais usuários têm acesso de login único a um login específico. Contas da AWS AWS Organizations Quando você ativa o IAM, uma função vinculada ao serviço é criada em toda a sua Contas da AWS organização. O IAM Identity Center também cria a mesma função vinculada ao serviço em todas as contas que são adicionadas posteriormente à sua organização.

Essa função permite que o IAM Identify Center acesse os recursos de cada conta em seu nome. As funções vinculadas ao serviço que são criadas em cada uma Conta da AWS são nomeadas. `AWSServiceRoleForSSO` Para ter mais informações, consulte As funções vinculadas ao serviço do IAM Identity Center permanecem..

AWS política gerenciada: AWSIAMIdentityCenterAllowListForIdentityContext

Ao assumir uma função com o contexto de identidade do IAM Identity Center, AWS Security Token Service (AWS STS) anexa automaticamente a `AWSIAMIdentityCenterAllowListForIdentityContext` política à função.

Essa política fornece a lista das ações permitidas quando você usa a propagação de identidades confiáveis com perfis que são assumidos com o contexto de identidades do IAM Identity Center. Todas as outras ações são chamadas com esse contexto são bloqueadas. O contexto de identidades é passado como `ProvidedContext`.

Para ver as permissões dessa política, consulte AWSIAMIdentityCenterAllowListForIdentityContextem Referência de política AWS gerenciada.

Atualizações do IAM Identity Center para políticas AWS gerenciadas

A tabela a seguir descreve as atualizações nas políticas AWS gerenciadas do IAM Identity Center desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed de RSS na página de Histórico do documento IAM Identity Center.

Alteração	Descrição	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora inclui`elasticmapreduce:AddJobFlowSteps` ,, `elasticmapreduce:DescribeCluster` `elasticmapreduce:CancelSteps` `elasticmapreduce:DescribeStep` , e `elasticmapreduce:ListSteps` ações para apoiar a	17 de maio de 2024

Alteração	Descrição	Data
	propagação de identidade confiável no Amazon EMR.	

Alteração	Descrição	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora incluiqapps:CreateQApp ,,,qapps:PredictProblemStatementFromConversation ,,qapps:PredictQAppFromProblemStatement ,qapps:CopyQApp ,qapps:GetQApp ,qapps:ListQApps ,qapps:UpdateQApp ,,qapps:DeleteQApp ,qapps:AssociateQAppWithUser ,qapps:DisassociateQAppFromUser ,qapps:ImportDocumentToQApp ,qapps:ImportDocumentToQAppSession ,,qapps:CreateLibraryItem , qapps:GetLibraryItem qapps:UpdateLibraryItem qapps:CreateLibraryItemReview qapps:ListLibraryItems qapps:CreateSubscriptionToken qapps:StartQAppSession , e qapps:StopQAppSession ações para oferecer suporte a sessões de console com reconheci	30 de abril de 2024

Alteração	Descrição	Data
	mento de identidade para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	
AWSSSOMasterAccountAdministrator	Essa política agora inclui as `signin:ListTrustedIdentityPropagationApplicationsForConsole` ações `signin:CreateTrustedIdentityPropagationApplicationForConsole` e para oferecer suporte a sessões de console com reconhecimento de identidade para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	26 de abril de 2024
AWSSSOMemberAccountAdministrator	Essa política agora inclui as `signin:ListTrustedIdentityPropagationApplicationsForConsole` ações `signin:CreateTrustedIdentityPropagationApplicationForConsole` e para oferecer suporte a sessões de console com reconhecimento de identidade para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	26 de abril de 2024

Alteração	Descrição	Data
AWSSSOReadOnly	Essa política agora inclui a `signin:ListTrustedIdentityPropagationApplicationsForConsole` ação para oferecer suporte a sessões de console com reconhecimento de identidade para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	26 de abril de 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora inclui a `qbusiness:PutFeedback` ação para oferecer suporte a sessões de console com reconhecimento de identidade para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	26 de abril de 2024

Alteração	Descrição	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora incluiq:StartConversation ,,,,q:SendMessage , q:ListConversations q:GetConversation q:StartTroubleshootingAnalysis q:GetTroubleshootingResults q:StartTroubleshootingResolutionExplanation , e q:UpdateTroubleshootingCommandResult ações para oferecer suporte a sessões de console com reconhecimento de identidade para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	24 de abril de 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora inclui a sts:SetContext ação para oferecer suporte a sessões de console com reconhecimento de identidade para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	19 de abril de 2024

Alteração	Descrição	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora inclui as `qbusiness:DeleteConversation` ações`qbusiness:Chat` ,, `qbusiness:ChatSync` `qbusiness:ListConversations` `qbusiness:ListMessages` , e para oferecer suporte a sessões de console com reconhecimento de identidade para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	11 de abril de 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política também inclui as ações `s3:GetAccessGrantsInstanceForPrefix` e `s3:GetDataAccess` .	26 de novembro de 2023
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política fornece a lista das ações permitidas quando você usa a propagação de identidades confiáveis com perfis que são assumidos com o contexto de identidades do IAM Identity Center.	15 de novembro de 2023
AWSSSODirectoryReadOnly	Essa política agora inclui o novo namespace `identitystore-auth` com novas permissões para permitir que os usuários listem e obtenham sessões.	21 de fevereiro de 2023

Alteração	Descrição	Data
AWSSSOServiceRolePolicy	Essa política agora permite que a ação `UpdateSAMLProvider` seja tomada na conta de gerenciamento.	20 de outubro de 2022
AWSSSOMasterAccountAdministrator	Essa política agora inclui o novo namespace `identitystore-auth` com novas permissões para permitir que os usuários listem e obtenham sessões.	20 de outubro de 2022
AWSSSOMemberAccountAdministrator	Essa política agora inclui o novo namespace `identitystore-auth` com novas permissões para permitir que os usuários listem e obtenham sessões.	20 de outubro de 2022
AWSSSODirectoryAdministrator	Essa política agora inclui o novo namespace `identitystore-auth` com novas permissões para permitir que os usuários listem e obtenham sessões.	20 de outubro de 2022

Alteração	Descrição	Data
AWSSSOMasterAccountAdministrator	Essa política agora inclui novas permissões para fazer chamadas ListDelegatedAdministrators_ AWS Organizations. Essa política agora também inclui um subconjunto de permissões AWSSSOManageDelegatedAdministrator que inclui permissões para chamar RegisterDelegatedAdministrator e DeregisterDelegatedAdministrator.	16 de agosto de 2022
AWSSSOMemberAccountAdministrator	Essa política agora inclui novas permissões para fazer chamadas ListDelegatedAdministrators_ AWS Organizations. Essa política agora também inclui um subconjunto de permissões AWSSSOManageDelegatedAdministrator que inclui permissões para chamar RegisterDelegatedAdministrator e DeregisterDelegatedAdministrator.	16 de agosto de 2022
AWSSSOReadOnly	Essa política agora inclui novas permissões para fazer chamadas ListDelegatedAdministrators AWS Organizations.	11 de agosto de 2022

Alteração	Descrição	Data
AWSSSOServiceRolePolicy	Essa política agora inclui novas permissões para chamar DeleteRolePermissionsBoundary e PutRolePermisionsBoundary.	14 de julho de 2022
AWSSSOServiceRolePolicy	Essa política agora inclui novas permissões para chamar ListAWSServiceAccessForOrganization and ListDelegatedAdministrators em AWS Organizations.	11 de maio de 2022
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	O IAM Access Analyzer adicionou uma nova ação para permitir que a entidade principal use as verificações de política para validação.	28 de abril de 2022
AWSSSOMasterAccountAdministrator	Essa política agora permite todas as ações do serviço IAM Identity Center Identity Store. Para obter informações sobre as ações disponíveis no serviço IAM Identity Center Identity Store, consulte a Referência da API IAM Identity Center Identity Store.	29 de março de 2022

Alteração	Descrição	Data
AWSSSOMemberAccountAdministrator	Essa política agora permite todas as ações do serviço IAM Identity Center Identity Store.	29 de março de 2022
AWSSSODirectoryAdministrator	Essa política agora permite todas as ações do serviço IAM Identity Center Identity Store.	29 de março de 2022
AWSSSODirectoryReadOnly	Essa política agora concede acesso às ações de leitura do serviço IAM Identity Center Identity Store. Esse acesso é necessário para recuperar informações de usuários e grupos do serviço IAM Identity Center Identity Store.	29 de março de 2022
AWSIdentitySyncFullAccess	Esta política permite acesso total às permissões de sincronização de identidade.	3 de março de 2022
AWSIdentitySyncReadOnlyAccess	Esta política concede permissões de acesso somente leitura que permitem que uma entidade principal visualize as configurações de sincronização de identidade.	3 de março de 2022
AWSSSOReadOnly	Esta política concede permissões de acesso somente leitura que permitem que uma entidade principal visualize as configurações de sincronização do IAM Identity Center.	4 de agosto de 2021

Alteração	Descrição	Data
O IAM Identity Center começou a monitorar as alterações	O IAM Identity Center começou a monitorar as mudanças nas políticas AWS gerenciadas.	4 de agosto de 2021

As funções vinculadas ao serviço do IAM Identity Center permanecem.

AWS IAM Identity Center usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). A função vinculada ao serviço é um tipo exclusivo de perfil do IAM vinculada diretamente ao IAM Identity Center. Ele é predefinido pelo IAM Identity Center e inclui todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome. Para ter mais informações, consulte Perfis vinculados ao serviço.

Um perfil vinculado ao serviço facilita a configuração do IAM Identity Center porque você não precisa adicionar as permissões necessárias manualmente. O IAM Identity Center define as permissões de seu perfil vinculado a serviço e, exceto se definido de outra forma, somente o IAM Identity Center pode assumir sua função. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham Sim na coluna Função vinculada a serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

As funções vinculadas ao serviço do IAM Identity Center permanecem.

O IAM Identity Center usa a função vinculada ao serviço nomeada AWSServiceRoleForSSOpara conceder permissões ao IAM Identity Center para gerenciar AWS recursos, incluindo funções, políticas e SAML IdP em seu nome.

A função AWSServiceRoleForSSO vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `IAM Identity Center`

A política de permissões AWSServiceRoleForSSO de função vinculada ao serviço permite que o IAM Identity Center conclua o seguinte em funções no caminho “/aws-reserved/sso.amazonaws.com/” e com o prefixo do nome “_”: AWSReservedSSO

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam:DeleteRole`
- `iam:DeleteRolePermissionsBoundary`
- `iam:DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:ListRolePolicies`
- `iam:PutRolePolicy`
- `iam:PutRolePermissionsBoundary`
- `iam:ListAttachedRolePolicies`

A política de permissões AWSServiceRoleForSSO de função vinculada ao serviço permite que o IAM Identity Center conclua o seguinte em provedores de SAML com o prefixo de nome “_”: AWSSSO

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam:DeleteSAMLProvider`

A política de permissões AWSServiceRoleForSSO de funções vinculadas ao serviço permite que o IAM Identity Center conclua o seguinte em todas as organizações:

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

A política de permissões AWSServiceRoleForSSO de função vinculada ao serviço permite que o IAM Identity Center conclua o seguinte em todas as funções do IAM (*):

- `iam:listRoles`

A política de permissões de função AWSServiceRoleForSSO vinculada ao serviço permite que o IAM Identity Center conclua o seguinte em “arn:aws:iam: :*:role/ /sso.amazonaws.com/”: aws-service-role AWSServiceRoleForSSO

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

A política de permissões da função permite que o IAM Identity Center execute as seguintes ações em recursos:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"IAMRoleProvisioningActions",
         "Effect":"Allow",
         "Action":[
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam:DeleteRolePermissionsBoundary",
            "iam:PutRolePermissionsBoundary",
            "iam:PutRolePolicy",
            "iam:UpdateRole",
            "iam:UpdateRoleDescription",
            "iam:UpdateAssumeRolePolicy"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ],
         "Condition":{
            "StringNotEquals":{
               "aws:PrincipalOrgMasterAccountId":"${aws:PrincipalAccount}"
            }
         }
      },
      {
```

```
         "Sid":"IAMRoleReadActions",
         "Effect":"Allow",
         "Action":[
            "iam:GetRole",
            "iam:ListRoles"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"IAMRoleCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:ListRolePolicies",
            "iam:ListAttachedRolePolicies"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ]
      },
      {
         "Sid":"IAMSLRCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus",
            "iam:DeleteRole",
            "iam:GetRole"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO"
         ]
      },
      {
        "Sid": "IAMSAMLProviderCreationAction",
        "Effect": "Allow",
        "Action": [
          "iam:CreateSAMLProvider"
      ],
```

```
      "Resource": [
         "arn:aws:iam::*:saml-provider/AWSSSO_*"
       ],
      "Condition": {
         "StringNotEquals": {
            "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
          }
        }
      },
      {
        "Sid": "IAMSAMLProviderUpdateAction",
        "Effect": "Allow",
        "Action": [
          "iam:UpdateSAMLProvider"
        ],
        "Resource": [
           "arn:aws:iam::*:saml-provider/AWSSSO_*"
        ]
      },
      {
         "Sid":"IAMSAMLProviderCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteSAMLProvider",
            "iam:GetSAMLProvider"
         ],
         "Resource":[
            "arn:aws:iam::*:saml-provider/AWSSSO_*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "organizations:DescribeAccount",
            "organizations:DescribeOrganization",
            "organizations:ListAccounts",
            "organizations:ListAWSServiceAccessForOrganization",
            "organizations:ListDelegatedAdministrators"
         ],
         "Resource":[
            "*"
         ]
      },
      {
```

```
            "Sid":"AllowUnauthAppForDirectory",
            "Effect":"Allow",
            "Action":[
               "ds:UnauthorizeApplication"
            ],
            "Resource":[
               "*"
            ]
         },
         {
            "Sid":"AllowDescribeForDirectory",
            "Effect":"Allow",
            "Action":[
               "ds:DescribeDirectories",
               "ds:DescribeTrusts"
            ],
            "Resource":[
               "*"
            ]
         },
         {
            "Sid":"AllowDescribeAndListOperationsOnIdentitySource",
            "Effect":"Allow",
            "Action":[
               "identitystore:DescribeUser",
               "identitystore:DescribeGroup",
               "identitystore:ListGroups",
               "identitystore:ListUsers"
            ],
            "Resource":[
               "*"
            ]
         }
      ]
}
```

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para obter mais informações, consulte Service-linked role permissions no IAM User Guide.

Criar um perfil vinculado ao serviço para o IAM Identity Center

Não é necessário criar manualmente uma função vinculada a serviço. Depois de ativado, o IAM Identity Center cria uma função vinculada ao serviço em todas as contas da organização em Organizations AWS . O IAM Identity Center também cria a mesma função vinculada ao serviço em todas as contas que são adicionadas posteriormente à sua organização. Essa função permite que o IAM Identify Center acesse os recursos de cada conta em seu nome.

Observações

- Se você estiver conectado à conta AWS Organizations de gerenciamento, ela usará sua função atualmente conectada e não a função vinculada ao serviço. Isso evita a escalada de privilégios.
- Quando o IAM Identity Center executa qualquer operação do IAM na conta AWS Organizations de gerenciamento, todas as operações acontecem usando as credenciais do diretor do IAM. Isso permite que os logins CloudTrail forneçam visibilidade de quem fez todas as alterações de privilégios na conta de gerenciamento.

Important

Se você estava usando o serviço IAM Identity Center antes de 7 de dezembro de 2017, quando ele começou a oferecer suporte a funções vinculadas ao serviço, o IAM Identity Center criou a AWSServiceRoleForSSO função em sua conta. Para saber mais, consulte A New Role Appeared in My IAM Account.

Se você excluir essa função vinculada a serviço e depois precisar criá-la novamente, poderá usar esse mesmo processo para recriar a função em sua conta.

Criar um perfil vinculado ao serviço para o IAM Identity Center

O IAM Identity Center não permite que você edite a função AWSServiceRoleForSSO vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para ter mais informações, consulte Editing a service-linked role no IAM User Guide.

Criar um perfil vinculado ao serviço para o IAM Identity Center

Você não precisa excluir manualmente a AWSServiceRoleForSSO função. Quando um Conta da AWS é removido de uma AWS organização, o IAM Identity Center limpa automaticamente os recursos e exclui a função vinculada ao serviço. Conta da AWS

Também é possível usar o console do IAM, a CLI do IAM; ou a API do IAM para excluir manualmente a função vinculada ao serviço. Para isso, primeiro você deve limpar manualmente os recursos de sua função vinculada ao serviço e depois excluí-la manualmente.

> **Note**
>
> Se o serviço IAM Identity Center estiver usando a função quando você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir os recursos do IAM Identity Center usados pelo AWSServiceRoleForSSO

1. Remover o acesso de usuários e grupos para todos os usuários e grupos que têm acesso a Conta da AWS.
2. Excluir conjuntos de permissões que você associou a Conta da AWS.

Como excluir manualmente a função vinculada a serviço usando o IAM

Use o console do IAM, a CLI do IAM ou a API do IAM para excluir a função vinculada ao AWSServiceRoleForSSO serviço. Para obter mais informações, consulte Deleting a Service-Linked Role no IAM User Guide.

Console do IAM Identity Center e autorização de API

As APIs existentes no console do IAM Identity Center são compatíveis com autorização dupla, o que permite que você continue a usar as operações de API existentes quando novas APIs estiverem disponíveis. Se você tiver instâncias do IAM Identity Center existentes que foram criadas antes de 15 de novembro de 2023 e depois de 15 de outubro de 2020, poderá usar a tabela a seguir para determinar quais operações de API agora são mapeadas para as operações de API mais novas que foram lançadas após essa data.

Tópicos

- Ações de API após novembro de 2023
- Ações de API após outubro de 2020

Ações de API após novembro de 2023

As instâncias do IAM Identity Center criadas antes de 15 de novembro de 2023 honram as antigas e as novas ações de API, desde que não haja negação explícita de nenhuma das ações. As instâncias criadas após 15 de novembro de 2023 usam as ações de API mais novas para obter autorização no console do IAM Identity Center.

Nome da operação do console em uso antes de 15 de novembro de 2023	Ações de API usadas após 15 de novembro de 2023
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance | CreateApplicationInstance	CreateApplication
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod
DeleteApplicationInstance | DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments

Nome da operação do console em uso antes de 15 de novembro de 2023	Ações de API usadas após 15 de novembro de 2023
UpdateApplicationInstanceDisplayData | UpdateApplicationInstanceStatus | UpdateManagedApplicationInstanceStatus	UpdateApplication

Ações de API após outubro de 2020

As instâncias do IAM Identity Center criadas antes de 15 de outubro de 2020 honram as antigas e as novas ações de API, desde que não haja negação explícita de nenhuma das ações. As instâncias criadas após 15 de outubro de 2020 usam as ações de API mais novas para autorização no console do IAM Identity Center.

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AssociateProfile	AssociateProfile	CreateAccountAssignment
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWsAccount	DeleteApplicationInstance | DeleteTrust	DeleteAccountAssignment
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances | GetApplicationInstance	ListAccountsForProvisionedPermissionSet
ListAWSAccountProfiles	ListProfiles | GetProfile	ListPermissionSetsProvisionedToAccount
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance | CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile | CreateProfile | UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust | CreateTrust | UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS STS chaves de contexto de condição para o IAM Identity Center

Quando um diretor faz uma solicitação AWS, AWS reúne as informações da solicitação em um contexto de solicitação, que é usado para avaliar e autorizar a solicitação. É possível usar o elemento `Condition` de uma política JSON para comparar chaves no contexto da solicitação com os valores de chave especificados em sua política. As informações da solicitação são fornecidas por fontes diferentes, incluindo o principal que faz a solicitação, o recurso, a solicitação contra a qual ela é feita e os metadados sobre a solicitação em si. As chaves de condição específicas do serviço são definidas para uso com um serviço individual AWS .

O IAM Identity Center inclui um provedor de AWS STS contexto que permite que aplicativos AWS gerenciados e aplicativos de terceiros adicionem valores às chaves de condição definidas pelo IAM Identity Center. Essas chaves estão incluídas nas funções do IAM. Os valores-chave são definidos quando um aplicativo passa um token para AWS STS o. O aplicativo obtém o token para o qual ele passa AWS STS de uma das seguintes formas:

- Durante a autenticação com o IAM Identity Center.
- Após a troca do token com um emissor de token confiável para propagação de identidade confiável. Nesse caso, o aplicativo obtém um token de um emissor de token confiável e troca esse token por um token do IAM Identity Center.

Essas chaves são normalmente usadas por aplicativos que se integram à propagação de identidade confiável. Em alguns casos, quando os valores das chaves estão presentes, você pode usar essas chaves nas políticas do IAM que você cria para permitir ou negar permissões.

Por exemplo, talvez você queira fornecer acesso condicional a um recurso com base no valor do`UserId`. Esse valor indica qual usuário do IAM Identity Center está usando a função. O exemplo é semelhante ao uso`SourceId`. Diferentemente`SourceId`, no entanto, o valor de `UserId` representa um usuário específico e verificado do repositório de identidades. Esse valor está presente

no token que o aplicativo obtém e para AWS STS o qual passa. Não é uma string de uso geral que pode conter valores arbitrários.

Tópicos

loja de identidades: UserId

Essa chave de contexto é `UserId` do usuário do IAM Identity Center que é o assunto da declaração de contexto emitida pelo IAM Identity Center. A afirmação do contexto é passada para AWS STS. Você pode usar essa chave para comparar o `UserId` usuário do IAM Identity Center em nome de quem a solicitação é feita com o identificador do usuário que você especifica na política.

- Disponibilidade — Essa chave é incluída no contexto da solicitação após a definição de uma declaração de contexto emitida pelo IAM Identity Center, quando uma função é assumida usando qualquer AWS STS `assume-role` comando na operação da AWS CLI AWS STS `AssumeRole` API.
- Tipo de dados: string
- Tipo de valor: valor único

loja de identidades: IdentityStoreArn

Essa chave de contexto é o ARN do repositório de identidades anexado à instância do IAM Identity Center que emitiu a declaração de contexto. É também o repositório de identidades no qual você pode pesquisar atributos`identitystore:UserID`. Você pode usar essa chave nas políticas para determinar se ela `identitystore:UserID` vem de um ARN de armazenamento de identidades esperado.

- Disponibilidade — Essa chave é incluída no contexto da solicitação após a definição de uma declaração de contexto emitida pelo IAM Identity Center, quando uma função é assumida usando qualquer AWS STS `assume-role` comando na operação da AWS CLI AWS STS `AssumeRole` API.

- Tipo de dados — Arn, String
- Tipo de valor: valor único

centro de identidade: ApplicationArn

Essa chave de contexto é o ARN do aplicativo para o qual o IAM Identity Center emitiu uma declaração de contexto. Você pode usar essa chave nas políticas para determinar se `identitycenter:ApplicationArn` vem de um aplicativo esperado. O uso dessa chave pode ajudar a impedir que uma função do IAM seja acessada por um aplicativo inesperado.

- Disponibilidade — Essa chave está incluída no contexto da solicitação de uma operação de AWS STS `AssumeRole` API. O contexto da solicitação inclui uma declaração de contexto emitida pelo IAM Identity Center.
- Tipo de dados — Arn, String
- Tipo de valor: valor único

centro de identidade: CredentialId

Essa chave de contexto é uma ID aleatória para a credencial da função com identidade aprimorada e é usada somente para registro. Como esse valor de chave é imprevisível, recomendamos que você não o use para afirmações de contexto em políticas.

- Disponibilidade — Essa chave está incluída no contexto da solicitação de uma operação de AWS STS `AssumeRole` API. O contexto da solicitação inclui uma declaração de contexto emitida pelo IAM Identity Center.
- Tipo de dados: string
- Tipo de valor: valor único

centro de identidade: InstanceArn

Essa chave de contexto é o ARN da instância do IAM Identity Center que emitiu a declaração de contexto para o. `identitystore:UserID` Você pode usar essa chave para determinar se a declaração de contexto `identitystore:UserID` e veio do ARN de uma instância esperada do IAM Identity Center.

- Disponibilidade — Essa chave está incluída no contexto da solicitação de uma operação de AWS STS `AssumeRole` API. O contexto da solicitação inclui uma declaração de contexto emitida pelo IAM Identity Center.
- Tipo de dados — Arn, String
- Tipo de valor: valor único

Registro e monitoramento no IAM Identity Center

Como uma prática recomendada, você deve monitorar a sua organização para garantir que as alterações sejam registradas. Isso ajuda você a garantir que qualquer alteração inesperada possa ser investigada e que alterações indesejadas possam ser revertidas. AWS IAM Identity Center atualmente oferece suporte a dois AWS serviços que ajudam você a monitorar sua organização e a atividade que acontece dentro dela.

Tópicos

- Registro de chamadas da API do IAM Identity Center com AWS CloudTrail
- Amazon EventBridge
- Registro de sincronização do AD e erros configuráveis de sincronização do AD

Registro de chamadas da API do IAM Identity Center com AWS CloudTrail

AWS IAM Identity Center é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no IAM Identity Center. CloudTrail captura chamadas de API para o IAM Identity Center como eventos. As chamadas capturadas incluem as chamadas do console do IAM Identity Center e as chamadas de código para as operações da API do IAM Identity Center. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o IAM Identity Center. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao IAM Identity Center, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Tópicos

- Informações do IAM Identity Center em CloudTrail

- Noções básicas sobre registros de arquivo de log do IAM Identity Center
- Noções básicas sobre eventos de login do IAM Identity Center

Informações do IAM Identity Center em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no IAM Identity Center, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos do IAM Identity Center, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS . A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para mais informações, consulte:

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

Quando o CloudTrail registro está ativado em seu Conta da AWS, as chamadas de API feitas para as ações do IAM Identity Center são rastreadas em arquivos de log. Os registros do IAM Identity Center são gravados junto com outros registros AWS de serviço em um arquivo de log. CloudTrail determina quando criar e gravar em um novo arquivo com base no período e no tamanho do arquivo.

As seguintes CloudTrail operações do IAM Identity Center são suportadas:

Operações da API do console	Operações públicas de API
`AssociateDirectory`	`AttachManagedPolicyToPermissionSet`

Operações da API do console	Operações públicas de API
AssociateProfile	CreateAccountAssignment
BatchDeleteSession	CreateInstanceAccessControlAttributeConfiguration
BatchGetSession	CreatePermissionSet
CreateApplicationInstance	DeleteAccountAssignment
CreateApplicationInstanceCertificate	DeleteInlinePolicyFromPermissionSet
CreatePermissionSet	DeleteInstanceAccessControlAttributeConfiguration
CreateProfile	DeletePermissionSet
DeleteApplicationInstance	DescribeAccountAssignmentCreationStatus
DeleteApplicationInstanceCertificate	DescribeAccountAssignmentDeletionStatus
DeletePermissionsPolicy	DescribeInstanceAccessControlAttributeConfiguration
DeletePermissionSet	DescribePermissionSet
DeleteProfile	DescribePermissionSetProvisioningStatus
DescribePermissionsPolicies	DetachManagedPolicyFromPermissionSet
DisassociateDirectory	GetInlinePolicyForPermissionSet
DisassociateProfile	ListAccountAssignmentCreationStatus

Operações da API do console	Operações públicas de API
GetApplicationInstance	ListAccountAssignmentDeletionStatus
GetApplicationTemplate	ListAccountAssignments
GetMfaDeviceManagementForDirectory	ListAccountsForProvisionedPermissionSet
GetPermissionSet	ListInstances
GetSSOStatus	ListManagedPoliciesInPermissionSet
ImportApplicationInstanceServiceProviderMetadata	ListPermissionSetProvisioningStatus
ListApplicationInstances	ListPermissionSets
ListApplicationInstanceCertificates	ListPermissionSetsProvisionedToAccount
ListApplicationTemplates	ListTagsForResource
ListDirectoryAssociations	ProvisionPermissionSet
ListPermissionSets	PutInlinePolicyToPermissionSet
ListProfileAssociations	TagResource
ListProfiles	UntagResource
ListSessions	UpdateInstanceAccessControlAttributeConfiguration
PutMfaDeviceManagementForDirectory	UpdatePermissionSet
PutPermissionsPolicy	

Operações da API do console	Operações públicas de API
StartSSO	
UpdateApplicationInstanceActiveCertificate	
UpdateApplicationInstanceDisplayData	
UpdateApplicationInstanceServiceProviderConfiguration	
UpdateApplicationInstanceStatus	
UpdateApplicationInstanceResponseConfiguration	
UpdateApplicationInstanceResponseSchemaConfiguration	
UpdateApplicationInstanceSecurityConfiguration	
UpdateDirectoryAssociation	
UpdateProfile	

Para obter mais informações sobre as operações de API pública do IAM Identity Center, consulte o IAM Identity Center API Reference Guide.

As seguintes CloudTrail operações do IAM Identity Center Identity Store são suportadas:

- AddMemberToGroup
- CompleteVirtualMfaDeviceRegistration
- CompleteWebAuthnDeviceRegistration
- CreateAlias
- CreateExternalIdPConfigurationForDirectory

- CreateGroup
- CreateUser
- DeleteExternalIdPConfigurationForDirectory
- DeleteGroup
- DeleteMfaDeviceForUser
- DeleteUser
- DescribeDirectory
- DescribeGroups
- DescribeUsers
- DisableExternalIdPConfigurationForDirectory
- DisableUser
- EnableExternalIdPConfigurationForDirectory
- EnableUser
- GetAWSSPConfigurationForDirectory
- ListExternalIdPConfigurationsForDirectory
- ListGroupsForUser
- ListMembersInGroup
- ListMfaDevicesForUser
- PutMfaDeviceManagementForDirectory
- RemoveMemberFromGroup
- SearchGroups
- SearchUsers
- StartVirtualMfaDeviceRegistration
- StartWebAuthnDeviceRegistration
- UpdateExternalIdPConfigurationForDirectory
- UpdateGroup
- UpdateMfaDeviceForUser
- UpdatePassword
- UpdateUser
- VerifyEmail

As seguintes CloudTrail ações do IAM Identity Center OIDC são suportadas:

- `CreateToken`
- `RegisterClient`
- `StartDeviceAuthorization`

As seguintes CloudTrail ações do IAM Identity Center Portal são suportadas:

- `Authenticate`
- `Federate`
- `ListApplications`
- `ListProfilesForApplication`
- `ListAccounts`
- `ListAccountRoles`
- `GetRoleCredentials`
- `Logout`

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

- Se a solicitação foi feita com as credenciais do usuário root ou do usuário AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o elemento CloudTrail userIdentity.

Noções básicas sobre registros de arquivo de log do IAM Identity Center

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante.

CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro para um administrador (samadams@example.com) que ocorreu no console do IAM Identity Center:


```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDAJAIENLMexample",
            "arn":"arn:aws:iam::08966example:user/samadams",
            "accountId":"08966example",
            "accessKeyId":"AKIAIIJM2K4example",
            "userName":"samadams"
         },
         "eventTime":"2017-11-29T22:39:43Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"DescribePermissionsPolicies",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":{
            "permissionSetId":"ps-79a0dde74b95ed05"
         },
         "responseElements":null,
         "requestID":"319ac6a1-d556-11e7-a34f-69a333106015",
         "eventID":"a93a952b-13dd-4ae5-a156-d3ad6220b071",
         "readOnly":true,
         "resources":[

         ],
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```


O exemplo a seguir mostra uma entrada de CloudTrail registro para uma ação do usuário final (bobsmith@example.com) que ocorreu no portal de AWS acesso:

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"Unknown",
            "principalId":"example.com//
S-1-5-21-1122334455-3652759393-4233131409-1126",
            "accountId":"08966example",
            "userName":"bobsmith@example.com"
         },
         "eventTime":"2017-11-29T18:48:28Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"ListApplications",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":null,
         "responseElements":null,
         "requestID":"de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
         "eventID":"e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro para uma ação do usuário final (bobsmith@example.com) que ocorreu no IAM Identity Center OIDC:

```
{
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "Unknown",
        "principalId": "example.com//S-1-5-21-1122334455-3652759393-4233131409-1126",
        "accountId": "08966example",
        "userName": "bobsmith@example.com"
      },
      "eventTime": "2020-06-16T01:31:15Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "CreateToken",
      "awsRegion": "us-east-1",
```

```
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": {
        "clientId": "clientid1234example",
        "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "grantType": "urn:ietf:params:oauth:grant-type:device_code",
        "deviceCode": "devicecode1234example"
      },
      "responseElements": {
        "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "tokenType": "Bearer",
        "expiresIn": 28800,
        "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
      "readOnly": false,
      "resources": [
        {
          "accountId": "08966example",
          "type": "IdentityStoreId",
          "ARN": "d-1234example"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "08966example"
}
```


Noções básicas sobre eventos de login do IAM Identity Center

AWS CloudTrail registra eventos de login bem-sucedidos e malsucedidos para todas as AWS IAM Identity Center fontes de identidade. As identidades originadas pelo SSO nativo e pelo Active Directory (AD Connector e AWS Managed Microsoft AD) incluirão eventos de login adicionais que serão capturados sempre que um usuário for solicitado a resolver um desafio ou fator específico de credencial, bem como o status dessa solicitação de verificação de credencial específica. Somente após o usuário concluir todos os desafios de credenciais necessários, o usuário será conectado, o que resultará no registro de um evento `UserAuthentication`.

A tabela a seguir captura cada um dos nomes dos CloudTrail eventos de login do IAM Identity Center, sua finalidade e aplicabilidade a diferentes fontes de identidade.

Nome do evento	Objetivo do evento	Aplicabilidade da fonte de identidade
`CredentialChallenge`	Usado para notificar que o IAM Identity Center solicitou que o usuário resolvesse um desafio de credencial específico e especifica o `CredentialType` que era necessário (por exemplo, SENHA ou TOTP).	Usuários nativos do IAM Identity Center, AD Connector e AWS Managed Microsoft AD
`CredentialVerification`	Usado para notificar que o usuário tentou resolver uma solicitação `CredentialChallenge` específica e especifica se essa credencial foi bem-sucedida ou falhou.	Usuários nativos do IAM Identity Center, AD Connector e AWS Managed Microsoft AD
`UserAuthentication`	Usado para notificar que todos os requisitos de autenticação com os quais o usuário foi desafiado foram concluídos com êxito e que o usuário foi conectado com sucesso. Se os usuários não conseguirem concluir com êxito os desafios de credenciais exigidos, nenhum *`UserAuthentication`* evento será registrado.	Todas as fontes de identidade

A tabela a seguir captura outros campos úteis de dados de eventos contidos em eventos de login CloudTrail específicos.

Nome do evento	Objetivo do evento	Aplicabilidade do evento de login	Exemplos de valores
`AuthWorkflowID`	Usado para correlacionar todos os eventos emitidos em uma sequência de login inteira. Para cada login de usuário, vários eventos podem ser emitidos pelo IAM Identity Center.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	“AuthWorkflowIdentificação”: “9de74b32-8362-4a01-a524-de21df59fd83"
`CredentialType`	Usado para especificar a credencial ou o fator que foi contestado. Os eventos `UserAuthentication` incluirão todos os valores `CredentialType` que foram verificados com sucesso na sequência de login do usuário.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	CredentialType“: “PASSWORD” ou ""“: CredentialType “PASSWORD, TOTP” (os valores possíveis incluem: PASSWORD, TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP)
`DeviceEnrollmentRequired`	Usado para especificar que o usuário precisou registrar um dispositivo de MFA durante o login e que o usuário concluiu essa solicitação com êxito.	`UserAuthentication`	“DeviceEnrollmentRequired“: “verdadeiro”

Nome do evento	Objetivo do evento	Aplicabilidade do evento de login	Exemplos de valores
`LoginTo`	Usado para especificar o local de redirecionamento após uma sequência de login bem-sucedida.	`UserAuthentication`	“LoginTo“:" https://mydirectory.awsapps.com/start/...”

Exemplos de eventos para cenários de login do IAM Identity Center

Os exemplos a seguir mostram a sequência esperada de CloudTrail eventos para diferentes cenários de login.

Tópicos

- Login bem-sucedido ao se autenticar apenas com uma senha
- Login bem-sucedido ao se autenticar com um provedor de identidade externo
- Login bem-sucedido ao se autenticar com uma senha e um aplicativo autenticador TOTP
- É necessário fazer login bem-sucedido ao autenticar com uma senha e um registro forçado de MFA
- Login bem-sucedido ao se autenticar apenas com uma senha

Login bem-sucedido ao se autenticar apenas com uma senha

A sequência de eventos a seguir captura um exemplo de login bem-sucedido somente com senha.

CredentialChallenge (Senha)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
```

```
   },
   "eventTime":"2020-12-07T20:33:58Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
   "eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

Bem sucedido CredentialVerification (Senha)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
```

```
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"c49640f6-0c8a-43d3-a6e0-900e3bb188d4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

Bem-sucedido UserAuthentication (somente senha)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
```

```
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


Login bem-sucedido ao se autenticar com um provedor de identidade externo

A sequência de eventos a seguir captura um exemplo de login bem-sucedido quando autenticado por meio do protocolo SAML usando um provedor de identidade externo.

Sucesso UserAuthentication (provedor de identidade externo)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":""
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
```

```
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"EXTERNAL_IDP"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


Login bem-sucedido ao se autenticar com uma senha e um aplicativo autenticador TOTP

A sequência de eventos a seguir captura um exemplo em que a autenticação multifatorial foi necessária durante o login e o usuário fez login com sucesso usando uma senha e um aplicativo autenticador TOTP.

CredentialChallenge (Senha)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:13Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
```

```
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"e454ea66-1027-4d00-9912-09c0589649e1",
   "eventID":"d89cc0b5-a23a-4b88-843a-89329aeaef2e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


Bem sucedido CredentialVerification (Senha)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
```

```
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"4533fd49-6669-4d0b-b272-a0b2139309a8",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

CredentialChallenge (PARA TP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"29202f08-f240-40cc-b789-c0cea8a27847",
   "readOnly":false,
```

```
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

Sucesso CredentialVerification (TOTP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"e889ff1d-fcaf-454f-805d-7132cf2362a4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
```

```
   }
}
```

Sucesso UserAuthentication (Senha + TOTP)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFfO01O8qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMlui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD,TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"7a8c8725-db2f-488d-a43e-788dc6c73a4a",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
```

```
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

É necessário fazer login bem-sucedido ao autenticar com uma senha e um registro forçado de MFA

A sequência de eventos a seguir captura um exemplo de login com senha bem-sucedido, mas o usuário precisou e concluiu com êxito o registro de um dispositivo de MFA antes de concluir o login.

CredentialChallenge (Senha)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:02Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"321f4b13-42b5-4005-a0f7-826cad26d159",
   "eventID":"8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
```

```
   }
}
```

Bem sucedido CredentialVerification (Senha)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
   "eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

Sucesso UserAuthentication (senha + registro de MFA obrigatório)

```
{
```

```
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:14Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNnQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHYz52rgR28sYAKN1oEk2G07czrwzXvE9HLlN2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY EgU3fhOL3QWvWiquYnDPMyPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi5OYI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD",
      "DeviceEnrollmentRequired":"true"
   },
   "requestID":"74d24604-a365-4237-8c4a-350795494b92",
   "eventID":"a15bf257-7f37-46c0-b67c-fea5fa6166be",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

Login bem-sucedido ao se autenticar apenas com uma senha

A sequência de eventos a seguir captura um exemplo de login somente com senha que falhou.

CredentialChallenge (Senha)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:15Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
   "eventID":"d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


Falha CredentialVerification (senha)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:21Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"04528c82-a678-4a1f-a56d-ea2c6445a72a",
   "eventID":"9160fe06-fc2a-474f-9b78-000ee067a09d",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Failure"
   }
}
```


Amazon EventBridge

O IAM Identity Center pode trabalhar com EventBridge a Amazon para gerar eventos quando ações especificadas pelo administrador ocorrem em uma organização. Por exemplo, devido à confidencialidade dessas ações, a maioria dos administradores desejarão ser avisados sempre que alguém criar uma nova conta na organização ou quando um administrador de uma conta membro tentar deixar a organização. Você pode configurar EventBridge regras que buscam essas ações e,

em seguida, enviam os eventos gerados para destinos definidos pelo administrador. Os alvos podem ser um tópico do Amazon SNS que envia e-mails ou mensagens de texto a seus assinantes. Você também pode criar uma AWS Lambda função que registre os detalhes da ação para sua análise posterior.

Para saber mais sobre EventBridge, inclusive como configurá-lo e habilitá-lo, consulte o Guia EventBridge do usuário da Amazon.

Registro de sincronização do AD e erros configuráveis de sincronização do AD

Você pode ativar o registro na sincronização do Active Directory (AD) e nas configurações configuráveis de sincronização do AD para receber registros com informações sobre erros que podem ocorrer durante o processo de sincronização. Com esses registros, você pode monitorar se há algum problema com a sincronização do AD e a sincronização configurável do AD e agir, se aplicável. Você pode enviar seus registros para um grupo de CloudWatch logs do Amazon Logs, um bucket do Amazon Simple Storage Service (Amazon S3) ou um Amazon Data Firehose com entrega entre contas compatível com buckets e Firehose do Amazon S3.

Para obter mais informações sobre limitações, permissões e registros vendidos, consulte Habilitando o registro em. Serviços da AWS

> **Note**
>
> Você é cobrado pelo registro. Para obter mais informações, consulte Vended Logs na página de CloudWatch preços da Amazon.

Para habilitar a sincronização do AD e os registros de erros configuráveis do AD Sync

1. Faça login no console do IAM Identity Center.
2. Escolha Configurações.
3. Na página Configurações, escolha a guia Fonte de identidade, escolha Ações e, em seguida, escolha Gerenciar registros.
4. Escolha Adicionar entrega de registros e um dos seguintes tipos de destino.
    a. Escolha To Amazon CloudWatch Logs. Em seguida, escolha ou insira o grupo de registros de destino.

b. Escolha Para Amazon S3. Em seguida, escolha ou insira o bucket de destino.

c. Escolha To Firehose. Em seguida, escolha ou insira o fluxo de entrega de destino.

5. Selecione Enviar.

Para desativar a sincronização do AD e os registros de erros configuráveis do AD Sync

1. Faça login no console do IAM Identity Center.
2. Escolha Configurações.
3. Na página Configurações, escolha a guia Fonte de identidade, escolha Ações e, em seguida, escolha Gerenciar registros.
4. Escolha Remover para o destino que você deseja remover.
5. Selecione Enviar.

Sincronização do AD e campos de registro de erros configuráveis do AD Sync

Consulte a lista a seguir para ver os possíveis campos de registro de erros.

`sync_profile_name`

O nome do perfil de sincronização.

`error_code`

O código de erro que representa o tipo de erro que ocorreu.

`error_message`

Uma mensagem que contém informações detalhadas sobre o erro que ocorreu.

`sync_source`

A fonte de sincronização é de onde as entidades estão sendo sincronizadas. Para o IAM Identity Center, esse é um Active Directory (AD) gerenciado por AWS Directory Service. A fonte de sincronização contém o domínio e o ARN do diretório afetado.

`sync_target`

O destino de sincronização é o destino em que as entidades estão sendo salvas. Para o IAM Identity Center, esse é um repositório de identidades. O destino de sincronização contém o ARN afetado do Identity Store.

`source_entity_id`

Um identificador exclusivo para a entidade que está causando o erro. Para o IAM Identity Center, esse é o SID da entidade.

`source_entity_type`

O tipo de entidade que está causando o erro. O valor pode ser `USER` ou `GROUP`.

`eventTimestamp`

O carimbo de data e hora em que o erro ocorreu.

Sincronização do AD e exemplos de registros de erros configuráveis do AD Sync

Exemplo 1: Um registro de erros para uma senha expirada para um diretório do AD

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "InvalidDirectoryCredentials",
        "error_message": "The password for your AD directory has expired. Please reset
 the password to allow Identity Sync to access the directory."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:123456789:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "eventTimestamp": "1683355579981"
}
```

Exemplo 2: Um registro de erros para um usuário com um nome de usuário não exclusivo

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "ConflictError",
        "error_message": "The source entity has a username conflict with the sync
 target. Please verify that the source identity has a unique username in the target."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:111122223333:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
```

```
    "sync_target": {
        "arn": "arn:aws:identitystore::111122223333:identitystore/d-123456"
    },
    "source_entity_id": "SID-1234",
    "source_entity_type": "USER",
    "eventTimestamp": "1683355579981"
}
```

Validação de conformidade do IAM Identity Center

Auditores terceirizados avaliam a segurança e a conformidade Serviços da AWS AWS IAM Identity Center como parte de vários programas de AWS conformidade.

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

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

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

  > **Note**
  >
  > Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.

- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Padrões de conformidade compatíveis

O IAM Identity Center submeteu-se à auditoria dos padrões a seguir e está qualificado para uso como parte de soluções para as quais você precisa obter certificação de conformidade.

AWS expandiu seu programa de conformidade com a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) para incluir o IAM Identity Center como um serviço qualificado pela HIPAA.

AWS oferece um whitepaper focado na HIPAA para clientes que desejam saber mais sobre como podem ser usados Serviços da AWS para processar e armazenar informações de saúde. Para obter mais informações, consulte HIPAA compliance.

O Information Security Registered Assessors Program (IRAP) permite que os clientes do governo australiano validem se os controles apropriados estão em vigor e determinem o modelo de responsabilidade correto para o cumprimento dos requisitos do Manual de Segurança da Informação (ISM) do governo australiano produzido pelo Australian Cyber Security Centre (ACSC). Para obter mais informações, consulte IRAP Resources.

O IAM Identity Center tem um Atestado de Conformidade com o Padrão de Segurança de Dados (DSS) da Indústria de Cartões de Pagamento (PCI) versão 3.2 no Nível 1 de Provedor de Serviços.

Clientes que usam AWS produtos e serviços para armazenar, processar ou transmitir dados do titular do cartão podem usar as seguintes fontes de identidade no IAM Identity Center para gerenciar sua própria certificação de conformidade com o PCI DSS:

- Active Directory
- Provedores de identidade externos

Atualmente, a fonte de identidade do IAM Identity Center não está em conformidade com o PCI DSS.

	Para obter mais informações sobre o PCI DSS, incluindo como solicitar uma cópia do PCI AWS Compliance Package, consulte PCI DSS nível 1.
	Os relatórios de Controle do sistema e da organização (System and Organization Control, SOC) são relatórios de exames de terceiros independentes que demonstram como o IAM Identity Center obtém os principais controles e objetivos de conformidade. Esses relatórios têm como finalidade ajudar você e os auditores a entenderem como os controles oferecem suporte às operações e à conformidade. Existem três tipos de relatórios do SOC: • AWS Relatório SOC 1 - Baixe com Artifact AWS • AWS SOC 2: Relatório de segurança, disponibilidade e confidencialidade - Baixe com Artifact AWS • AWS SOC 3: Relatório de segurança, disponibilidade e confidencialidade O IAM Identity Center está no escopo dos AWS relatórios SOC 1, SOC 2 e SOC 3. Para obter mais informações, consulte Conformidade com o SOC.

Resiliência no IAM Identity Center

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As Zonas de Disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte infraestrutura AWS global.

Para saber mais sobre AWS IAM Identity Center resiliência, consulteDesign de resiliência e comportamento regional.

Segurança da infraestrutura no IAM Identity Center

Como serviço gerenciado, AWS IAM Identity Center é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o IAM Identity Center pela rede. Os clientes devem ser compatíveis com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, são compatíveis com esses modos.

Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Marcando atributos AWS IAM Identity Center

Uma tag é um rótulo de atributo personalizado que você adiciona a um recurso da AWS para facilitar a identificação, organização e pesquisa de recursos. Cada tag tem duas partes:

- Uma chave de tag (por exemplo `CostCenter`, `Environment` ou `Project`). As chaves de tag podem ter até 128 caracteres e diferenciam minúsculas de maiúsculas.
- Um valor de tag (por exemplo, `111122223333` ou `Production`). Os valores de tag podem ter até 256 caracteres e, como as chaves de tag, diferenciam minúsculas de maiúsculas. É possível definir o valor de uma tag em uma string vazia, mas não configurar o valor de um tag como nula. Omitir o valor da tag é o mesmo que usar uma string vazia.

As tags ajudam a identificar e organizar os recursos da AWS. Muitos serviços da AWS oferecem suporte à marcação para que você possa atribuir a mesma tag a recursos de diferentes serviços para indicar que os recursos estão relacionados. Por exemplo, você pode atribuir a mesma tag a um conjunto específico de permissões na instância do IAM Identity Center. Para obter mais informações sobre estratégias de marcação, consulte Tagging AWS Resources no Referência geral da AWSGuide e Tagging Best Practices.

Além de identificar, organizar e rastrear seus AWS recursos com tags, você pode usar tags nas políticas do IAM para ajudar a controlar quem pode visualizar e interagir com seus recursos. Para obter informações sobre como usar tags para limitar o acesso aos seus recursos, consulte Controlling access to AWS resources using tags no Guia do usuário do IAM. Por exemplo, você pode permitir que um usuário atualize um conjunto de permissões do IAM Identity Center, mas somente se o conjunto de permissões do IAM Identity Center tiver uma tag `owner` com o valor do nome desse usuário.

Atualmente, você pode aplicar tags somente a conjuntos de permissões. Você não pode aplicar tags às funções correspondentes que o IAM Identity Center cria em Contas da AWS. Você pode usar o console IAM Identity Center, AWS CLI ou as APIs do IAM Identity Center para adicionar, editar ou excluir tags para um conjunto de permissões.

As seções a seguir fornecem mais informações sobre tags para o IAM Identity Center.

Restrições de tags

As restrições básicas a seguir se aplicam a tags nos recursos do IAM Identity Center:

- O número máximo de tags que você pode atribuir a um recurso é 50.
- O comprimento máximo da chave é 128 caracteres Unicode.
- O número máximo de tags que você pode atribuir a um recurso é 50.
- Os caracteres válidos para uma chave de tag e um valor são:

  a-z, A-Z, 0-9, espaço e os seguintes caracteres: _ . : / = + - e @
- As chaves e os valores diferenciam letras maiúsculas de minúsculas.
- Não use `aws:` como um prefixo para chaves, pois ele é reservado para uso da AWS

Gerencie tags usando o console do IAM Identity Center

Você pode usar o console do IAM Identity Center para adicionar, editar e remover as tags associadas à instância ou ao conjuntos de permissões.

Para gerenciar tags para conjuntos de permissões para um console do IAM Identity Center

1. Abra o console IAM Identity Center.
2. Escolha Permission sets.
3. Escolha o nome do conjunto de permissões que tem as tags que você deseja gerenciar.
4. Na guia Permissions, em Tags, faça o seguinte e prossiga para a próxima etapa:

   a. Se as tags já estiverem atribuídas para esse conjunto de permissões, escolha Edit tags.

   b. Se nenhuma tag for atribuída a esse conjunto de permissões, escolha Add tags.
5. Para cada nova tag, digite os valores nas colunas Key e Valor (opcional). Ao concluir, escolha Save changes.

Para remover uma tag, escolha o X na coluna Remove ao lado da tag que você deseja remover.

Para gerenciar tags para uma instância do IAM Identity Center

1. Abra o console do Centro de Identidade do IAM.
2. Escolha Configurações.
3. Escolha a guia Tags.
4. Para cada nova tag, digite os valores nos campos Chave e Valor (opcional). Quando terminar, escolha o botão Adicionar nova tag.

Para remover uma tag, escolha o botão Remover ao lado da tag que você deseja remover.

Exemplos do AWS CLI

O AWS CLI fornece comandos que podem ser usados para gerenciar as tags que você atribui ao seu conjunto de permissões.

Atribuir tags

Use os comandos a seguir para atribuir tags ao seu conjunto de permissões.

Example Comando **`tag-resource`** para um conjunto de permissões

Atribuir tags a um conjunto de permissões usando `tag-resource` dentro do conjunto de comandos `sso`:

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test
```

Esse comando inclui os seguintes parâmetros:

- `instance-arn`— O nome do recurso da Amazon (ARN) da instância do IAM Identity Center sob o qual a operação será executada.
- `resource-arn`— O ARN do recurso com as tags a serem listadas.
- `tags` – Os pares de chave/valor das tags.

Para atribuir várias tags ao mesmo tempo, você deve especificá-las em uma lista separada por vírgulas:

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

Visualizar tags

Use os comandos a seguir para visualizar as tags que você atribuiu ao seu conjunto de permissões.

Example Comando **`list-tags-for-resource`** para um conjunto de permissões

Visualize as tags atribuídas a um conjunto de permissões usando `list-tags-for-resource` no conjunto de comandos`sso`:

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

Remover tags

Use os comandos a seguir para atribuir tags ao seu conjunto de permissões.

Example Comando **`untag-resource`** para um conjunto de permissões

Remover tags de um conjunto de permissões usando `untag-resource` dentro do conjunto de comandos `sso`:

```
$ aws sso-admin untag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tag-keys Stage CostCenter Owner
```

Para o parâmetro `--tag-keys`, especifique uma ou mais chaves de tag e não inclua os valores das tags.

Aplicar tags ao criar um conjunto de permissões

Use os comandos a seguir para atribuir tags no momento de criar seu conjunto de permissões.

Example Comando **`create-permission-set`** com etiquetas

Quando você cria um grupo de usuários utilizando o comando `create-permission-set`, pode especificar tags com o parâmetro `--tags`:

```
$ aws sso-admin create-permission-set \
> --instance-arn sso-instance-arn \
> --name permission=set-name \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

Gerencie tags usando o console do IAM Identity Center

Você pode usar as seguintes ações na API do IAM Identity Center para gerenciar as tags do seu conjunto de permissões.

Ações de API para tags de instância do IAM Identity Center

Use as ações de API a seguir para atribuir, visualizar e remover tags de um grupo de permissões ou de uma instância do IAM Identity Center.

- TagResource
- ListTagsForResource
- UntagResource
- CreatePermissionSet
- CreateInstance

Integração da CLI AWS com o IAM Identity Center

AWSA integração da interface de linha de comando (Command Line Interface - CLI) versão 2 com o IAM Identity Center simplifica o processo de login. Os desenvolvedores podem fazer login diretamente na AWS CLI usando as mesmas credenciais do Active Directory ou do IAM Identity Center que normalmente usam para entrar no IAM Identity Center e acessar suas contas e funções atribuídas. Por exemplo, depois que um administrador configura o IAM Identity Center para usar o Active Directory para autenticação, um desenvolvedor pode fazer login na AWS CLI diretamente usando suas credenciais do Active Directory.

AWSA integração da CLI com o IAM Identity Center oferece os seguintes benefícios:

- As empresas podem permitir que seus desenvolvedores façam login usando credenciais do IAM Identity Center ou do Active Directory conectando o IAM Identity Center ao Active Directory usando a AWS Directory Service.
- Os desenvolvedores podem fazer login a partir da CLI para um acesso mais rápido.
- Os desenvolvedores podem listar e alternar entre contas e funções às quais atribuíram acesso.
- Os desenvolvedores podem gerar e salvar perfis de função nomeados na configuração da CLI automaticamente e referenciá-los na CLI para executar comandos nas contas e funções desejadas.
- A CLI gerencia automaticamente as credenciais de curto prazo para que os desenvolvedores possam começar e permanecer na CLI com segurança, sem interrupção, e executar scripts de longa execução.

Como integrar a CLI da AWS com o IAM Identity Center

Para usar a integração da CLI da AWS com o IAM Identity Center, você precisa baixar, instalar e configurar a versão 2 da AWS Command Line Interface. Para obter etapas detalhadas sobre como fazer o download e integrar a AWS CLI ao IAM Identity Center, consulte Como configurar a CLI da AWS para usar o IAM Identity Center no Guia do usuário da AWS Command Line Interface.

AWS IAM Identity Center Disponibilidade da região

O IAM Identity Center está disponível em vários idiomas comumente usados Regiões da AWS. Essa disponibilidade facilita a configuração do acesso do usuário a vários aplicativos Contas da AWS e aplicativos comerciais. Quando seus usuários entram no portal de AWS acesso, eles podem selecionar o Conta da AWS para o qual têm permissões e, em seguida, acessar AWS Management Console o. Para ver uma lista completa dos recursos compatíveis com o Regiões da AWS IAM Identity Center, consulte os endpoints e cotas do IAM Identity Center.

Dados de região do IAM Identity Center

Quando você habilita o IAM Identity Center pela primeira vez, todos os dados que você configura no IAM Identity Center são armazenados na região em que você os configurou. Esses dados incluem configurações de diretório, conjuntos de permissões, instâncias do aplicativo e atribuições de usuários aos Conta da AWS aplicativos. Se você estiver usando o armazenamento de identidades do IAM Identity Center, todos os usuários e grupos que você cria no IAM Identity Center também são armazenados na mesma região. Recomendamos que você instale o IAM Identity Center em uma região que você pretende manter disponível para os usuários, não em uma região que talvez seja necessário desabilitar.

AWS Organizations suporta apenas um Região da AWS de cada vez. Para habilitar o IAM Identity Center em uma região diferente, você deve primeiro excluir sua configuração atual do IAM Identity Center. Alternar para uma região diferente também altera a URL do portal de AWS acesso, e você deve reconfigurar todos os conjuntos de permissões e atribuições.

Chamadas entre regiões

O IAM Identity Center usa o Amazon Simple Email Service (Amazon SES) para enviar e-mails aos usuários finais quando eles tentam fazer login com uma senha de uso único (OTP) como segundo fator de autenticação. Esses e-mails também são enviados para determinados eventos de gerenciamento de identidade e credenciais, como quando o usuário é convidado a configurar uma senha inicial, verificar um endereço de e-mail e redefinir sua senha. O Amazon SES está disponível em um subconjunto do suporte do Regiões da AWS IAM Identity Center.

O IAM Identity Center chama os endpoints locais do Amazon SES quando o Amazon SES está disponível localmente em uma Região da AWS. Quando o Amazon SES não está disponível

localmente, o IAM Identity Center chama os endpoints do Amazon SES em uma Região da AWS diferente, conforme indicado na tabela a seguir.

Os códigos de região do Amazon SES estão listados na tabela a seguir.

Código da região do IAM Identity Center	Nome da região do IAM Identity Center	Código de região do Amazon SES	Nome de região do Amazon SES
us-gov-east-1	AWS GovCloud (Leste dos EUA)	us-gov-west-1	AWS GovCloud (Oeste dos EUA)
ap-east-1	Ásia-Pacífico (Hong Kong)	ap-northeast-2	Ásia-Pacífico (Seul)
ap-southeast-4	Ásia-Pacífico (Melbourne)	ap-southeast-2	Ásia-Pacífico (Sydney)
ap-south-2	Ásia-Pacífico (Hyderabad)	ap-south-1	Ásia-Pacífico (Mumbai)
eu-central-2	Europa (Zurique)	eu-central-1	Europa (Frankfurt)
eu-south-2	Europa (Espanha)	eu-west-3	Europa (Paris)
me-central-1	Oriente Médio (Emirados Árabes Unidos)	eu-central-1	Europa (Frankfurt)

Nessas chamadas entre regiões, o IAM Identity Center pode enviar os seguintes atributos de usuário:

- Endereço de e-mail
- Nome
- Sobrenome
- Conta em AWS Organizations
- AWS URL do portal de acesso
- Nome de usuário
- ID de diretório

- ID de usuário

Gerenciando o IAM Identity Center em uma região opcional (região que está desativada por padrão)

A maioria Regiões da AWS está habilitada para operações em todos os AWS serviços por padrão. Essas regiões são automaticamente habilitadas para uso com o IAM Identity Center. As seguintes Regiões da AWS são regiões opcionais e você deve habilitá-las:

- Africa (Cape Town)
- Ásia-Pacífico (Hong Kong)
- Ásia-Pacífico (Jacarta)
- Ásia-Pacífico (Melbourne)
- Ásia-Pacífico (Hyderabad)
- Europa (Milão)
- Europa (Zurique)
- Europa (Espanha)
- Israel (Tel Aviv)
- Oriente Médio (Barém)
- Oriente Médio (Emirados Árabes Unidos)

Quando você ativa o IAM Identity Center para uma conta de gerenciamento em um opt-in Região da AWS, os seguintes metadados do IAM Identity Center para qualquer conta membro são armazenados na região.

- ID da conta
- Nome da conta
- E-mail da conta
- Nomes de recursos da Amazon (ARNs) dos perfis do IAM que o IAM Identity Center cria na conta do membro

Se você desabilitar uma região na qual o IAM Identity Center está instalado, o IAM Identity Center também será desabilitado. Depois que o IAM Identity Center for desativado em uma região, os

usuários dessa região não terão acesso de login único Contas da AWS e aplicativos. AWS retém os dados na configuração do IAM Identity Center por pelo menos 10 dias. Se você reabilitar o IAM Identity Center dentro desse período, os dados de configuração do IAM Identity Center ainda estarão disponíveis na região.

Para reativar o IAM Identity Center no opt-in Regiões da AWS, você deve reativar a região. Como o IAM Identity Center precisa reprocessar todos os eventos pausados novamente, a reabilitação do IAM Identity Center pode levar algum tempo.

> **Note**
>
> O IAM Identity Center pode gerenciar o acesso somente aos Contas da AWS que estão habilitados para uso em um Região da AWS. Para gerenciar o acesso em todas as contas da sua organização, habilite o IAM Identity Center na conta de gerenciamento em uma Região da AWS que seja ativada automaticamente para uso com o IAM Identity Center.

Para obter mais informações sobre como ativar e desativar Regiões da AWS, consulte Gerenciando Regiões da AWS na Referência AWS Geral.

Exclua a configuração do IAM Identity Center

Quando uma configuração do IAM Identity Center é excluída, todos os dados nessa configuração são excluídos e não podem ser recuperados. A tabela a seguir descreve quais dados são excluídos com base no tipo de diretório atualmente configurado no IAM Identity Center.

Quais dados são excluídos	Diretório conectado (AWS Managed Microsoft AD ou AD Connector)	Armazenamento de identidades do IAM Identity Center
Todos os conjuntos de permissões para os quais você configurou Contas da AWS	✓	✓

Quais dados são excluídos	Diretório conectado (AWS Managed Microsoft AD ou AD Connector)	Armazenamento de identidades do IAM Identity Center
Todas as aplicações que você configurou no IAM Identity Center	✓	✓
Todas as atribuições de usuário para as quais você configurou Contas da AWS e aplicativos	✓	✓
Todos os usuários e grupos no diretório ou armazenamento	N/D	✓

Use o procedimento a seguir quando precisar excluir a configuração atual do IAM Identity Center.

Para excluir a configuração do IAM Identity Center

1. Abra o console do IAM Identity Center.
2. No painel de navegação à esquerda, escolha Configurações.
3. Na página Configurações, escolha a aba Gerenciar.
4. Na seção Excluir configuração do IAM Identity Center, escolha Excluir.
5. Na caixa de diálogo Excluir configuração do IAM Identity Center, marque cada uma das caixas de seleção para confirmar que você entende que seus dados serão excluídos. Digite sua instância do IAM Identity Center na caixa de texto e escolha Confirmar.

AWS IAM Identity Center cotas

As tabelas a seguir descrevem as cotas no IAM Identity Center. As solicitações de aumento de cota devem vir de uma conta administrativa ou de administrador delegado. Para aumentar uma cota, consulte solicitação de aumento de cota.

> **Note**
>
> Recomendamos usar a AWS CLI e as APIs se você tiver mais de 50.000 usuários, 10.000 grupos ou 500 conjuntos de permissões. Para obter mais informações sobre a CLI, consulte Integração da CLI AWS com o IAM Identity Center. Para obter mais informações sobre APIs, consulte Welcome to the IAM Identity Center API Reference.

Cotas de aplicativos

Recurso	Cota padrão	Pode ser aumentada
Tamanho do arquivo de certificados SAML do provedor de serviços (no formato PEM)	2 KB	Não
Limite de asserção do SAML	50.000 caracteres	Não
Limite de tamanho de arquivo do certificado IdP carregado no IAM Identity Center	2.500 caracteres (UTF-8)	Não
Escopos de acesso por aplicação	25	Não

Conta da AWS cotas

Recurso	Cota padrão	Pode ser aumentada
Número de conjuntos de permissões permitidos no IAM Identify Center	2000	Sim
Número de conjuntos de permissões provisionados permitidos por Conta da AWS	250	Sim
Número de políticas em linha por conjunto de permissões	1	Não
Número de políticas AWS gerenciadas e gerenciadas pelo cliente por conjunto de permissões	20 [1]	Não
Tamanho máximo de política em linha por conjunto de permissões	32.768 bytes O tamanho máximo de caracteres sem espaço em branco na política em linha por conjunto de permissões é de 10.240 bytes.	Não
Número de funções do IAM (conjuntos de permissões) no Conta da AWS que podem ser atualizadas por vez	1	Não

[1]AWS Identity and Access Management (IAM) define uma cota de 10 políticas gerenciadas por função. Para aproveitar essa cota, solicite um aumento nas políticas gerenciadas de cotas do IAM anexadas a uma função do IAM no console do Service Quotas para Conta da AWS cada local em que você deseja implantar o conjunto de permissões.

> **Note**
>
> Conjuntos de permissõessão provisionados Contas da AWS como funções do IAM ou usam funções existentes do IAM e Contas da AWS, portanto, seguem as cotas do IAM. Para obter mais informações sobre cotas associadas às funções do IAM, consulte Cotas do IAM e STS.

Cotas do Active Directory

Recurso	Cota padrão	Pode ser aumentada
Número de diretórios conectados que você pode ter por vez	1	Não

IAM Identity Center Identity Store

Recurso	Cota padrão	Pode ser aumentada
Número de usuários com suporte no IAM Identify Center	100000	Sim
Número de grupos aceitos no IAM Identify Center	100000	Não
Número de grupos exclusivos que podem ser usados para avaliar as permissões de um usuário	1000	Não

Limites de controle do IAM Identity Center

Recurso	Cota padrão
APIs do IAM Identity Center	As APIs do IAM Identity Center têm um controle coletivo de no máximo 20 transaçõe s por segundo (TPS). CreateAccountAssig nmentTem uma taxa máxima de 10 chamadas assíncronas pendentes. Essas cotas não podem ser alteradas.

Cotas adicionais

Recurso	Cota padrão	Pode ser aumentada
Número total de aplicativos Contas da AWS ou aplicativos que podem ser configurados*	3000	Sim
Número total de Instâncias do IAM Identity Center por conta	1	Não
Número total de emissores de tokens confiáveis	10	Não

* Até 3000 Contas da AWS aplicativos (total combinado) são suportados. Por exemplo, você pode configurar 2750 contas e 250 aplicativos, resultando em um total de 3.000 contas e aplicativos.

Solução de problemas do IAM Identity Center

Os tópicos a seguir podem ajudar você a solucionar alguns problemas comuns que podem ser encontrados ao configurar ou usar o IAM Identity Center.

Problemas ao criar uma instância de conta do IAM Identity Center

Várias restrições podem se aplicar à criação de uma instância de conta do IAM Identity Center. Se você não conseguir criar uma instância de conta por meio do console do IAM Identity Center ou da experiência de configuração de um aplicativo AWS gerenciado compatível, verifique os seguintes casos de uso:

- Marque outra Regiões da AWS Conta da AWS na qual você está tentando criar a instância da conta. O limite é de uma instância do IAM Identity Center por Conta da AWS. Para habilitar o aplicativo, alterne para a Região da AWS com a instância do IAM Identity Center ou mude para uma conta sem uma instância do IAM Identity Center.
- Se sua organização habilitou o IAM Identity Center antes de 14 de setembro de 2023, talvez seu administrador precise optar pela criação da instância da conta. Peça ao administrador para permitir a criação de instâncias de conta usando o console do IAM Identity Center na conta de gerenciamento.
- O administrador pode ter criado uma política de controle de serviços para limitar a criação de instâncias de conta do IAM Identity Center. Peça ao administrador para adicionar sua conta à lista de permissões.

Você recebe um erro quando tenta visualizar a lista de aplicações de nuvem pré-configuradas para trabalhar com o IAM Identity Center

O erro a seguir ocorre quando você tem uma política que permite `sso:ListApplications`, mas não outras APIs do IAM Identity Center. Atualize a política para resolver esse erro.

A permissão de `ListApplications` autoriza várias APIs:

- A API `ListApplications`.

- Uma API interna semelhante à API `ListApplicationProviders` usada no console do IAM Identity Center.

Para ajudar a resolver duplicações, a API interna agora também autoriza o uso da ação `ListApplicationProviders`. Para permitir a API `ListApplications` pública, mas negar a API interna, a política deve incluir uma instrução negando a ação `ListApplicationProviders`:

```
      "Statement": [
    {
         "Effect": "Deny",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
]
```

Para permitir a API interna, mas negar `ListApplications`, a política precisa permitir somente `ListApplicationProviders`. A API `ListApplications` é negada se não for explicitamente permitida.

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

Quando suas políticas forem atualizadas, entre em contato AWS Support para remover essa medida proativa.

Problemas relacionados ao conteúdo das asserções SAML criadas pelo IAM Identity Center

O IAM Identity Center fornece uma experiência de depuração baseada na web para as asserções SAML criadas e enviadas pelo IAM Identity Center, incluindo atributos dentro dessas asserções, ao acessar aplicativos SAML a partir do Contas da AWS portal de acesso. AWS Para ver os detalhes de uma asserção SAML que o IAM Identity Center gera, use as etapas a seguir.

1. Faça login no portal de AWS acesso.
2. Enquanto estiver conectado ao portal, mantenha pressionada a tecla Shift e, em seguida, escolha o bloco de aplicativos e solte a tecla Shift.
3. Examine as informações na página intitulada You are now in administrator mode (Agora você está no modo de administrador). Para manter essas informações para futura referência, escolha Copiar XML e cole o conteúdo em outro lugar.
4. Escolha Enviar para <application> para continuar. Essa opção envia a asserção ao provedor de serviços.

> **Note**
>
> Algumas configurações de navegador e sistemas operacionais podem não ser compatível com esse procedimento. Esse procedimento foi testado no Windows 10 usando os navegadores Firefox, Chrome e Edge.

Usuários específicos não conseguem sincronizar com o IAM Identity Center a partir de um provedor SCIM externo

Se a sincronização do SCIM for bem-sucedida para um subconjunto de usuários configurados em seu IdP para provisionamento no IAM Identity Center, mas falhar para outros, você poderá ver um erro semelhante a `'Request is unparsable, syntactically incorrect, or violates schema'` do seu provedor de identidades. Você também pode ver mensagens detalhadas de falha de provisionamento em. AWS CloudTrail

Esse problema geralmente indica que o usuário em seu IdP está configurado de uma forma que o IAM Identity Center não é compatível. Detalhes completos da implementação de SCIM

do IAM Identity Center, incluindo as especificações de parâmetros e operações obrigatórios, opcionais e proibidos para objetos de usuário, podem ser encontrados no Guia do desenvolvedor de implementação de SCIM do IAM Identity Center. O Guia do desenvolvedor de SCIM deve ser considerado confiável para obter informações sobre os requisitos do SCIM. No entanto, a seguir estão alguns motivos comuns para esse erro:

1. O objeto de usuário no IdP não tem o primeiro nome (dado), sobrenome (nome de família) e/ou nome de exibição.

   - Solução: adicione um nome (determinado), sobrenome (família) e nome de exibição para o objeto do usuário. Além disso, certifique-se de que os mapeamentos de provisionamento do SCIM para objetos de usuário em seu IdP estejam configurados para enviar valores não vazios para todos esses atributos.

2. Mais de um valor para um único atributo está sendo enviado para o usuário (também conhecido como “atributos de vários valores”). Por exemplo, o usuário pode ter um número de telefone comercial e residencial especificado no IdP, ou vários e-mails ou endereços físicos, e seu IdP está configurado para tentar sincronizar vários ou todos os valores desse atributo.

   - Opções de solução:

     i. Atualize seus mapeamentos de provisionamento SCIM para objetos de usuário em seu IdP para enviar somente um único valor para um determinado atributo. Por exemplo, configure um mapeamento que envie somente o número de telefone comercial de cada usuário.

     ii. Se os atributos adicionais puderem ser removidos com segurança do objeto do usuário no IdP, você poderá remover os valores adicionais, deixando um ou zero valores definidos para esse atributo para o usuário.

     iii. Se o atributo não for necessário para nenhuma ação em AWS, remova o mapeamento desse atributo dos mapeamentos de provisionamento do SCIM para objetos de usuário em seu IdP.

3. Seu IdP está tentando combinar os usuários no destino (o IAM Identity Center, nesse caso) com base em vários atributos. Como os nomes de usuário têm garantia de exclusividade em uma determinada instância do IAM Identity Center, você só precisa especificar o `username` como atributo usado para fazer a correspondência.

   - Solução: verifique se a configuração do SCIM no seu IdP está usando apenas um único atributo para correspondência com os usuários no IAM Identity Center. Por exemplo,

mapear `username` ou `userPrincipalName` no IdP para o atributo `userName` no SCIM para provisionamento no IAM Identity Center será correto e suficiente para a maioria das implementações.

Os usuários não podem fazer login quando o nome de usuário está no formato UPN

Talvez os usuários não consigam entrar no portal de AWS acesso com base no formato que usam para inserir seu nome de usuário na página de login. Na maioria das vezes, os usuários podem entrar no portal do usuário usando seu nome de usuário simples, seu nome de login de nível inferior (DOMÍNIO\UserName) ou seu nome de login UPN (). `UserName@Corp.Example.com` A exceção é quando o IAM Identity Center está usando um diretório conectado que foi habilitado com o MFA e o modo de verificação foi definido como Sensível ao contexto ou Sempre ativo. Nesse cenário, os usuários devem entrar com seu nome de login de nível inferior (DOMÍNIO\). UserName Para ter mais informações, consulte Autenticação multifator para usuários do Identity Center. Para obter informações gerais sobre os formatos de nome de usuário usados para entrar no Active Directory, consulte Formatos de nome de usuário no site de documentação da Microsoft.

Recebo o erro “Não é possível realizar a operação no perfil protegido” ao modificar um perfil do IAM

Ao analisar as funções do IAM em uma conta, você pode notar que os nomes das funções começam com 'AWSReservedSSO_'. Esses são os perfis que o serviço do IAM Identity Center criou na conta e vieram da atribuição de um conjunto de permissões à conta. A tentativa de modificar essas funções no console do IAM resultará no seguinte erro:

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -
 this role is only modifiable by AWS'
```

Essas funções só podem ser modificadas no console do administrador do IAM Identity Center, que está na conta de gerenciamento do AWS Organizations. Depois de modificadas, você pode transferir as alterações para as contas da AWS às quais elas estão atribuídas.

Os usuários do diretório não podem redefinir suas senhas

Quando um usuário do diretório redefine sua senha usando a opção Esqueceu a senha? opção durante o login no portal de AWS acesso, sua nova senha deve seguir a política de senha padrão, conforme descrito em. Requisitos de senha ao gerenciar identidade no IAM Identity Center

Se um usuário digitar uma senha que esteja de acordo com a política e receber o erro`We couldn't update your password`, verifique se a falha AWS CloudTrail foi registrada. Isso pode ser feito pesquisando no console do Histórico de Eventos ou CloudTrail usando o seguinte filtro:

```
"UpdatePassword"
```

Se a mensagem indicar o seguinte, talvez seja necessário entrar em contato com o suporte:

```
"errorCode": "InternalFailure",
      "errorMessage": "An unknown error occurred“
```

Outra causa possível desse problema está na convenção de nomenclatura que foi aplicada ao valor do nome de usuário. As convenções de nomenclatura devem seguir padrões específicos, como 'Surname.givenName'. No entanto, alguns nomes de usuário podem ser muito longos ou conter caracteres especiais, o que pode fazer com que os caracteres sejam eliminados na chamada da API, resultando em um erro. Talvez você queira tentar redefinir a senha com um usuário de teste da mesma maneira para verificar se esse é o caso.

Se o problema persistir, entre em contato com o AWS Support Center.

Meu usuário é referenciado em um conjunto de permissões, mas não consegue acessar as contas ou aplicativos atribuídos

Esse problema pode ocorrer se você estiver usando o Sistema de gerenciamento de identidade entre domínios (SCIM) para provisionamento automático com um provedor de identidades externo. Especificamente, quando um usuário ou o grupo do qual o usuário era membro é excluído e recriado usando o mesmo nome de usuário (para usuários) ou nome (para grupos) no provedor de identidades, um novo identificador interno exclusivo é criado para o novo usuário ou grupo no IAM Identity Center. No entanto, o IAM Identity Center ainda tem uma referência ao identificador antigo em seu banco de dados de permissões, de forma que o nome do usuário ou grupo ainda aparece na

interface do usuário, mas o acesso falha. Isso ocorre porque o ID de usuário ou grupo subjacente ao qual a interface do usuário se refere não existe mais.

Para restaurar o Conta da AWS acesso nesse caso, você pode remover o acesso do usuário ou grupo antigo do Conta da AWS(s) em que ele foi originalmente atribuído e, em seguida, reatribuir o acesso ao usuário ou grupo. Isso atualiza o conjunto de permissões com o identificador correto para o novo usuário ou grupo. Da mesma forma, para restaurar o acesso ao aplicativo, você pode remover o acesso do usuário ou grupo da lista de usuários atribuídos para esse aplicativo e, em seguida, adicionar o usuário ou grupo novamente.

Você também pode verificar se a falha AWS CloudTrail foi registrada pesquisando seus CloudTrail registros em busca de eventos de sincronização do SCIM que façam referência ao nome do usuário ou grupo em questão.

Não consigo configurar corretamente minha aplicação do catálogo de aplicações

Se você adicionou uma aplicação do catálogo de aplicações no IAM Identity Center, observe que cada provedor de serviços fornece sua própria documentação detalhada. Você pode acessar essas informações na guia Configuração da aplicação no console do IAM Identity Center.

Se o problema estiver relacionado com a configuração de confiança entre sua aplicação e o IAM Identity Center, lembre-se de examinar as etapas de solução de problemas no manual de instruções.

Erro “Ocorreu um erro inesperado” quando um usuário tenta fazer login usando um provedor de identidades externo

Esse erro pode ocorrer por vários motivos, mas um motivo comum é a incompatibilidade entre as informações do usuário transportadas na solicitação do SAML e as informações do usuário no IAM Identity Center.

Para que um usuário do IAM Identity Center faça login com sucesso ao usar um IdP externo como fonte de identidade, o seguinte deve ser verdadeiro:

- O formato de nameID do SAML (configurado em seu provedor de identidades) deve ser 'e-mail'
- O valor de nameID deve ser uma sequência formatada corretamente (RFC2822) (user@domain.com)

- O valor de nameID deve corresponder exatamente ao nome de usuário de um usuário existente no IAM Identity Center (não importa se o endereço de e-mail no IAM Identity Center corresponde ou não – a correspondência de entrada é baseada no nome de usuário)
- A implementação do IAM Identity Center da federação SAML 2.0 aceita apenas 1 asserção na resposta do SAML entre o provedor de identidades e o IAM Identity Center. Ele não oferece suporte a asserções do SAML criptografadas.
- As declarações a seguir se aplicam se Atributos para controle de acesso estiverem ativados em sua conta do IAM Identity Center:
  - O número de atributos mapeados na solicitação do SAML deve ser 50 ou menos.
  - A solicitação do SAML não deve conter atributos de vários valores.
  - A solicitação do SAML não deve conter vários atributos com o mesmo nome.
  - O atributo não deve conter XML estruturado como o valor.
  - O formato do nome deve ser um formato especificado pelo SAML, não um formato genérico.

> **Note**
>
> O IAM Identity Center não realiza a criação “just in time” de usuários ou grupos para novos usuários ou grupos por meio da federação SAML. Isso significa que o usuário deve ser pré-criado no IAM Identity Center, manualmente ou por meio de provisionamento automático, para fazer login no IAM Identity Center.

Esse erro também pode ocorrer quando o endpoint do Assertion Consumer Service (ACS) configurado no seu provedor de identidades não corresponde ao URL do ACS fornecido pela sua instância do IAM Identity Center. Certifique-se de que esses dois valores fazem uma correspondência exata.

Além disso, você pode solucionar ainda mais as falhas de login do provedor de identidade externo acessando AWS CloudTrail e filtrando o nome do evento P. ExternalId DirectoryLogin

Erro “Falha na ativação dos atributos do controle de acesso”

Esse erro pode ocorrer se o usuário que habilita o ABAC não tiver as permissões `iam:UpdateAssumeRolePolicy` necessárias para habilitar Atributos para controle de acesso.

Recebo a mensagem “Navegador não suportado” quando tento registrar um dispositivo para MFA

WebAuthn atualmente é compatível com os navegadores Google Chrome, Mozilla Firefox, Microsoft Edge e Apple Safari, bem como nas plataformas Windows 10 e Android. Alguns componentes do WebAuthn suporte podem ser variados, como o suporte ao autenticador de plataforma nos navegadores macOS e iOS. Se os usuários tentarem registrar WebAuthn dispositivos em um navegador ou plataforma incompatível, eles verão certas opções acinzentadas que não são suportadas ou receberão uma mensagem de erro informando que todos os métodos compatíveis não são suportados. Nesses casos, consulte FIDO2: Web Authentication (WebAuthn) para obter mais informações sobre o suporte a navegadores/plataformas. Para obter mais informações sobre o WebAuthn IAM Identity Center, consulteAutenticadores FIDO2.

O grupo “Usuários do domínio” do Active Directory não é sincronizado corretamente com o IAM Identity Center

O grupo Usuários do domínio do Active Directory é o “grupo primário” padrão para objetos de usuário do AD. Os grupos primários do Active Directory e suas associações não podem ser lidos pelo IAM Identity Center. Ao atribuir acesso aos recursos ou aplicações do IAM Identity Center, use grupos que não sejam o grupo de usuários do domínio (ou outros grupos atribuídos como grupos primários) para que a associação ao grupo seja refletida adequadamente no armazenamento de identidades do IAM Identity Center.

Erro de credenciais de MFA inválidas

Esse erro pode ocorrer quando um usuário tenta entrar no IAM Identity Center usando uma conta de um provedor de identidades externo (por exemplo, Okta ouMicrosoft Entra ID) antes que sua conta seja totalmente provisionada para o IAM Identity Center usando o protocolo do SCIM. Depois que a conta do usuário for provisionada para o IAM Identity Center, esse problema deve ser resolvido. Confirme se a conta foi provisionada para o IAM Identity Center. Caso contrário, verifique os registros de provisionamento no provedor de identidades externo.

Recebo a mensagem “Ocorreu um erro inesperado” quando tento me registrar ou entrar usando um aplicativo autenticador

Os sistemas de senha de uso único com marcação temporal (TOTP), como os usados pelo IAM Identity Center em combinação com aplicativos autenticadores baseados em código, dependem da sincronização de hora entre o cliente e o servidor. Certifique-se de que o dispositivo em que seu aplicativo autenticador está instalado esteja sincronizado corretamente com uma fonte de hora confiável ou defina manualmente a hora em seu dispositivo para corresponder a uma fonte confiável, como NIST (https://www.time.gov/) ou outros equivalentes locais/regionais.

Eu recebo um erro “Não é você, somos nós” ao tentar entrar no IAM Identity Center

Esse erro indica que há um problema de configuração com sua instância do IAM Identity Center ou com o provedor de identidade externo (IdP) que o IAM Identity Center está usando como fonte de identidade. Recomendamos que você verifique o seguinte:

- Verifique as configurações de data e hora no dispositivo que você está usando para fazer login. Recomendamos que você defina a data e a hora a serem definidas automaticamente. Se isso não estiver disponível, recomendamos sincronizar sua data e hora com um servidor conhecido do Network Time Protocol (NTP).
- Verifique se o certificado do IdP carregado no IAM Identity Center é o mesmo fornecido pelo seu IdP. Você pode verificar o certificado no console do IAM Identity Center navegando até Configurações. Na guia Fonte de identidade, escolha Ação e, em seguida, escolha Gerenciar autenticação. Se os certificados do IdP e do IAM Identity Center não corresponderem, importe um novo certificado para o IAM Identity Center.
- Certifique-se de que o formato NameID no arquivo de metadados do seu provedor de identidade seja o seguinte:
  - `urn:oasis:name:tc:SAML:1.1:nameid-format:emailAddress`
- Se você estiver usando o AD Connector AWS Directory Service como seu provedor de identidade, verifique se as credenciais da conta de serviço estão corretas e não expiraram. Consulte Atualizar as credenciais da conta de serviço do AD Connector em AWS Directory Service para obter mais informações.

Meus usuários não estão recebendo e-mails do IAM Identity Center

Todos os e-mails enviados pelo serviço IAM Identity Center virão do endereço `no-reply@signin.aws` ou `no-reply@login.awsapps.com`. Seu sistema de e-mail deve estar configurado para aceitar e-mails desses endereços de e-mail do remetente e não os trate como lixo eletrônico ou spam.

Erro: você não pode excluir/modificar/remover/atribuir acesso aos conjuntos de permissões provisionados na conta de gerenciamento

Essa mensagem indica que o Administradores delegados recurso foi ativado e que a operação que você tentou anteriormente só pode ser executada com êxito por alguém que tenha permissões da conta de gerenciamento AWS Organizations. Para resolver esse problema, entre como um usuário que tenha essas permissões e tente executar a tarefa novamente ou atribua essa tarefa a alguém que tenha as permissões corretas. Para ter mais informações, consulte Registre uma conta-membro.

Erro: token de sessão não encontrado ou inválido

Esse erro pode ocorrer quando um cliente, como um navegador da Web AWS Toolkit AWS CLI, ou tenta usar uma sessão revogada ou invalidada no lado do servidor. Para corrigir esse problema, retorne ao aplicativo ou site do cliente e tente novamente, incluindo fazer login novamente, se solicitado. Às vezes, isso pode exigir que você também cancele solicitações pendentes, como uma tentativa de conexão pendente de AWS Toolkit dentro do seu IDE.

Histórico do documento

A tabela a seguir descreve adições importantes à AWS IAM Identity Center documentação. Também atualizamos a documentação com frequência para abordar os comentários enviados por você.

- Última atualização importante da documentação: 23 de setembro de 2019

Alteração	Descrição	Data
Atualizações da política AWS gerenciada	Permissões atualizadas para a política `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gerenciada.	17 de maio de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política `AWSIAMIdentityCenterAllowListForIdentityContext` AWS gerenciada.	30 de abril de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política `AWSSSOMasterAccountAdministrator` AWS gerenciada.	26 de abril de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política `AWSSSOMemberAccountAdministrator` AWS gerenciada.	26 de abril de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política `AWSSSOReadOnly` AWS gerenciada.	26 de abril de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política `AWSIAMIde`	26 de abril de 2024

	`ntityCenterAllowLi stForIdentityConte xt` AWS gerenciada.	
Atualizações da política AWS gerenciada	Permissões atualizadas para a política `AWSIAMIde ntityCenterAllowLi stForIdentityConte xt` AWS gerenciada.	24 de abril de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política `AWSIAMIde ntityCenterAllowLi stForIdentityConte xt` AWS gerenciada.	19 de abril de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política `AWSIAMIde ntityCenterAllowLi stForIdentityConte xt` AWS gerenciada.	11 de abril de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política `AWSIAMIde ntityCenterAllowLi stForIdentityConte xt` AWS gerenciada.	26 de novembro de 2023
Novo tópico de política AWS gerenciada	Detalhes adicionados para a política `AWSIAMIde ntityCenterAllowLi stForIdentityConte xt` AWS gerenciada.	15 de novembro de 2023
Orientação aprimorada para começar a usar o IAM Identity Center	Novo conteúdo adicionado para começar a usar o IAM Identity Center e criar um usuário administrativo	23 de setembro de 2022

Usuários e grupos atualizados na Referência da API do Identity Center	Essa atualização inclui referências às novas APIs de criação, atualização e exclusão no Guia de referência da API do Identity Center.	31 de agosto de 2022
AWS Login único (AWS SSO) renomeado para IAM Identity Center AWS	AWS introduz. AWS IAM Identity Center O IAM Identity Center expande os recursos do AWS Identity and Access Management (IAM) para ajudá-lo a gerenciar centralmente a conta e o acesso aos aplicativos para os usuários da sua força de trabalho. Os atributos do IAM Identity Center incluem atribuições de aplicativos, permissões para várias contas e um portal de acesso AWS .	26 de julho de 2022
Suporte para limites de permissões e políticas gerenciadas pelo cliente em conjuntos de permissões	Conteúdo adicionado para usar políticas AWS gerenciadas e gerenciadas pelo cliente AWS Identity and Access Management (IAM) com conjuntos de permissões.	14 de julho de 2022
Support para AWS regiões ativadas manualmente	Conteúdo adicionado para usar o IAM Identity Center em regiões ativadas manualmente.	15 de junho de 2022
Atualizações para políticas AWS gerenciadas	Permissões atualizadas para a política `AWSSSOServiceRolePolicy` AWS gerenciada.	11 de maio de 2022

Suporte para administração delegada	Conteúdo adicionado para o atributo de administração delegada.	11 de maio de 2022
Atualizações para políticas AWS gerenciadas	Permissões atualizadas para o `AWSSSOMasterAccountAdministrator`, `AWSSSOMemberAccountAdministrator`, e políticas `AWSSSOReadOnly` AWS gerenciadas.	28 de abril de 2022
Suporte para sincronização configurável do AD	Conteúdo adicionado para o atributo configurável de sincronização do AD.	14 de abril de 2022
Novo tópico de política AWS gerenciada	Detalhes adicionados para a política `AWSSSOMasterAccountAdministrator` AWS gerenciada.	4 de agosto de 2021
Atualizações para cotas	Ajustes nas tabelas de cotas.	21 de dezembro de 2020
Novos exemplos de políticas	Foram adicionados novos exemplos de políticas gerenciadas pelo cliente e atualizações à seção de permissões necessárias.	21 de dezembro de 2020
Suporte para controle de acesso por atributo (ABAC)	Conteúdo adicionado para o atributo ABAC.	24 de novembro de 2020
Suporte para inscrição forçada no MFA	Atualizações para exigir que os usuários inscrevam um dispositivo de MFA no login.	23 de novembro de 2020

Support for WebAuthn	Conteúdo adicionado para o novo atributo WebAuthn.	20 de novembro de 2020
Suporte para Ping Identity	Conteúdo adicionado para integração com produtos Ping Identity como um provedor de identidade externo compatível.	26 de outubro de 2020
Support for OneLogin	Conteúdo adicionado para integração com OneLogin como um provedor de identidade externo compatível.	31 de julho de 2020
Suporte para Okta	Conteúdo adicionado para integração com Okta como um provedor de identidade externo compatível.	28 de maio de 2020
Suporte para provedores de identidade externos	Alterou as referências do diretório para a fonte de identidade, adicionou conteúdo para oferecer suporte a provedores de identidade externos.	26 de novembro de 2019
Novas configurações de MFA	Removeu o tópico de verificação em duas etapas e adicionou um novo tópico de MFA em seu lugar.	24 de outubro de 2019
Nova configuração para adicionar a verificação em duas etapas	Foi adicionado conteúdo sobre como ativar a verificação em duas etapas para os usuários.	16 de janeiro de 2019
Support para duração da sessão em AWS contas	Conteúdo adicionado sobre como definir a duração da sessão para uma AWS conta.	30 de outubro de 2018

Nova opção para usar o diretório do Identity Center	Adição de conteúdo para escolha de um diretório do Identity Center ou conexão com um diretório existente no Active Directory.	17 de outubro de 2018
Suporte ao estado do relé e à duração da sessão nos aplicativos	Adicionado conteúdo sobre o estado de retransmissão e a duração de sessão das aplicações.	10 de outubro de 2018
Compatibilidade adicional com novas aplicações	Adicionados 4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvaInSync, Egnyte, Engagedly, Expensify, Freshdesk, IdeaScale, Igloo, Jitbit, Kudos, LiquidFiles, Lucidchart, PurelyHR, Samanage, ScreenSteps, Sli.do, SmartSheet, Syncplicity, TalentLMS, Trello, UserVoice, Zoho, OpsGenie, DigiCert, WeekDone, ProdPad, e UserEcho ao catálogo de aplicativos.	3 de agosto de 2018
Suporte para acesso de várias contas a contas de gerenciamento	Adição de conteúdo sobre como delegar acesso a usuários em múltiplas contas em uma conta de gerenciamento.	9 de julho de 2018
Compatibilidade com novas aplicações	Adicionados DocuSign, Keeper Security, e SugarCRM ao catálogo de aplicativos.	16 de março de 2018

Obter credenciais temporárias para acesso à CLI	Foram adicionadas informaçõ es sobre como obter credencia is temporárias para executar AWS CLI comandos.	22 de fevereiro de 2018
Novo guia	Esta é a primeira versão do Guia do usuário do IAM Identity Center.	7 de dezembro de 2017

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.