



Manual do usuário

Centro de Identidade do AWS IAM



Centro de Identidade do AWS IAM: Manual do usuário

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

O que é o IAM Identity Center?	1
Por que usar o IAM Identity Center?	1
Renomeação do IAM Identity Center	3
Os namespaces legados permanecem os mesmos	3
Introdução	4
Pré-requisitos e considerações sobre o IAM Identity Center	6
Escolha de uma Região da AWS	7
Uso do IAM Identity Center apenas para aplicações	14
Perfis do IAM criados pelo IAM Identity Center	14
Centro de identidade do IAM e AWS Organizations	15
Instâncias do IAM Identity Center	16
Conta da AWS tipos que podem habilitar o IAM Identity Center	17
Instâncias de organização do IAM Identity Center	19
Instâncias de conta do Centro de Identidade do IAM	20
Excluir sua instância do IAM Identity Center	25
Habilitar o IAM Identity Center	27
Para habilitar uma instância do IAM Identity Center	28
Confirmar as fontes de identidades	31
Atualizar firewalls e gateways	33
Considerações sobre a inclusão de domínios e endpoints de URL na lista de permissões	35
Tutoriais sobre fonte de identidades	37
Active Directory	38
CyberArk	40
Pré-requisitos	41
Considerações SCIM	42
Etapa 1: Habilitar provisionamento no IAM Identity Center	43
Etapa 2: Configure o provisionamento no CyberArk	43
(Opcional) Etapa 3: Configure os atributos do usuário CyberArk para controle de acesso (ABAC) no IAM Identity Center	44
(Opcional) Passar atributos para controle de acesso	45
Google Workspace	46
Considerações	47
Etapa 1: Google Workspace: configurar a aplicação SAML	48

Etapa 2: IAM Identity Center e Google Workspace: alterar a fonte de identidades do IAM Identity Center e configurar o Google Workspace como um provedor de identidades SAML	48
Etapa 3: Google Workspace: habilitar as aplicações	50
Etapa 4: IAM Identity Center: configurar o provisionamento automático do IAM Identity Center	51
Etapa 5: Google Workspace: configurar o provisionamento automático	51
Passagem de atributos para controle de acesso: opcional	53
Atribuir acesso a Contas da AWS	54
Próximas etapas	57
Solução de problemas	57
JumpCloud	58
Pré-requisitos	59
Considerações SCIM	60
Etapa 1: Habilitar provisionamento no IAM Identity Center	60
Etapa 2: Configure o provisionamento no JumpCloud	61
(Opcional) Etapa 3: configure atributos do usuário no JumpCloud para controle de acesso no IAM Identity Center	62
(Opcional) Passar atributos para controle de acesso	63
Microsoft Entra ID	63
Pré-requisitos	64
Considerações	64
Etapa 1: preparar o locatário da Microsoft	66
Etapa 2: Prepare sua AWS conta	68
Etapa 3: configurar e testar a conexão SAML	71
Etapa 4: configurar e testar a sincronização SCIM	75
Etapa 5: configurar ABAC: opcional	79
Atribuir acesso a Contas da AWS	80
Microsoft Entra IDconfiguração para acesso a regiões adicionais	83
Solução de problemas	83
Okta	86
Considerações	87
Etapa 1: Okta: obter os metadados SAML da sua conta da Okta	88
Etapa 2: IAM Identity Center: configurar o Okta como fonte de identidades para o IAM Identity Center	89
Etapa 3: IAM Identity Center e Okta: provisionar usuários do Okta	90

Etapa 4: Okta: sincronizar os usuários do Okta com o IAM Identity Center	92
Passagem de atributos para controle de acesso: opcional	93
Atribuir acesso a Contas da AWS	94
Oktaconfiguração para acesso a regiões adicionais	96
Próximas etapas	97
Solução de problemas	97
OneLogin	99
Pré-requisitos	100
Etapa 1: Habilitar provisionamento no IAM Identity Center	101
Etapa 2: Configure o provisionamento no OneLogin	102
(Opcional) Etapa 3: configure atributos do usuário no OneLogin para controle de acesso no IAM Identity Center	103
(Opcional) Passar atributos para controle de acesso	104
Solução de problemas	104
Ping Identity	105
PingFederate	106
PingOne	113
Diretório do Identity Center	120
Vídeos de tutorial	126
Configurar a força de trabalho	127
Usuários, grupos e provisionamento	127
Exclusividade do nome de usuário e endereço de e-mail	127
Groups (Grupos)	128
Provisionamento de usuários e grupos	128
Desprovisionamento de usuários e grupos	128
Gerencie sua fonte de identidade	129
Considerações para alterar sua fonte de identidade	130
Alterar sua fonte de identidades	135
Atributos de usuário e grupo no IAM Identity Center	137
Provedores de identidades externos	138
Diretório Microsoft AD	157
Gerenciar usuários no diretório do Identity Center	178
Provisionamento quando os usuários estão no Centro de Identidade do IAM	178
Alterando sua origem de identidade	179
Adicionar usuários	179
Adicionar grupos	182

Adicionar usuários a grupos	183
Apagar grupos	184
Excluir usuários	185
Remover usuários de grupos	187
Editar propriedades do usuário	188
Acesso da força de trabalho	190
Como entender as sessões de autenticação	190
Tipos de sessões de autenticação	191
Formas de encerrar sessões de usuário final	192
O que acontece com o acesso do usuário quando você encerra uma sessão	193
Logout único	197
Práticas recomendadas para o gerenciamento de uma sessão	197
Configurar duração da sessão	198
Sessões interativas do usuário	198
Sessões de usuário em segundo plano	199
Sessões estendidas para Kiro	201
Encerrar sessões ativas para usuários da força de trabalho	202
Considerações sobre fontes de identidade, a AWS CLI e AWS SDKs	203
Desabilitar o acesso do usuário	207
Negar acesso do usuário	208
Como gerenciar o acesso para usuários do diretório do Identity Center	210
Gerenciamento de senhas	210
MFA	210
Como configurar senhas de usuário	211
Autenticação multifator	214
Acesso à aplicação	228
AWS aplicativos gerenciados	229
Controle de acesso a aplicações	229
Compartilhamento de informações de identidade	230
Restringindo o uso de aplicativos AWS gerenciados	231
Aplicações que você pode usar com o IAM Identity Center	232
Configurando o IAM Identity Center para testar aplicativos AWS gerenciados	238
Visualização e alteração dos detalhes da aplicação	244
Desabilitando um aplicativo AWS gerenciado	245
Como habilitar sessões de console com identidade avançada	246
Aplicações gerenciadas pelo cliente	249

Aplicativos SAML 2.0 e OAuth 2.0	250
Configuração de aplicação SAML 2.0	255
Propagação de identidades confiáveis	259
Benefícios da propagação de identidade confiável	259
Como habilitar a propagação de identidade confiável	259
Como funciona a propagação de identidade confiável	260
Pré-requisitos e considerações	262
Casos de uso	264
Serviços de autorização	291
Configurando seu próprio aplicativo OAuth 2.0	302
Configurar aplicações gerenciadas pelo cliente	302
Especificar aplicações confiáveis	307
Emissor de tokens confiáveis	308
Alternar certificados	323
Considerações antes de fazer a rotação de um certificado	324
Fazer a rotação de um certificado do IAM Identity Center	324
Indicadores do status de expiração do certificado	327
Compreender as propriedades da aplicação	327
URL de início da aplicação	327
Estado de retransmissão	328
Duração da sessão	329
Atribuir acesso de usuário às aplicações	329
Remover o acesso dos usuários a aplicações	330
Mapear atributos	331
Conta da AWS acesso	332
Conta da AWS tipos	332
Atribuindo acesso Conta da AWS	335
Experiência do usuário final	335
Imposição e limite de acesso	336
Delegar e impor o acesso	336
Limitar o acesso ao repositório de identidades das contas dos membros	337
Administradores delegados	338
Práticas recomendadas	339
Pré-requisitos	344
Registre uma conta-membro	344
Cancelar o registro de uma conta-membro	345

Visualizar contas de administrador delegado	346
Acesso elevado temporário	347
Acesso com login único a Contas da AWS	348
Atribuir acesso de usuário ou grupo a Contas da AWS	348
Remover o acesso de usuários e grupos a um Conta da AWS	351
Revogar sessão ativa de um conjunto de permissões	352
Delegar quem pode atribuir acesso com autenticação única	354
Conjuntos de permissões	356
Criar um conjunto de permissões que aplica permissões de privilégio mínimo	356
Permissões predefinidas	358
Permissões personalizadas	359
Criar, gerenciar e excluir conjuntos de permissões	362
Configurar propriedades do conjunto de permissões	376
Referenciação de conjuntos de permissões	383
Recomendações para evitar interrupções no acesso	385
Exemplos de políticas personalizadas	386
Controle de acesso por atributo	387
Benefícios	388
Lista de verificação: Configurando o ABAC AWS usando o IAM Identity Center	389
Atributos para controle de acesso	391
Perfis vinculados ao serviço	399
AWS portal de acesso	400
Introdução ao portal de AWS acesso	400
Configurar o portal de AWS acesso	401
O que você pode configurar	401
Ativando o portal de AWS acesso	401
Personalizando a URL do portal de AWS acesso	402
Confirme se os usuários podem entrar no portal de AWS acesso	403
Use o portal de AWS acesso	404
Como usar o portal de AWS acesso	405
Entrando no portal de AWS acesso	405
Redefinindo sua senha de usuário	408
AWS CLI e acesso ao AWS SDK	409
Criação de links de atalho	415
Registro de um dispositivo para MFA	417
Como encerrar a sessão ativa	420

Usando o IAM Identity Center em várias Regiões da AWS	422
Benefícios do suporte multirregional	422
Pré-requisitos e considerações	422
Escolhendo uma região adicional	423
Replique o IAM Identity Center para uma região adicional	424
Etapa 1: criar uma chave de réplica	424
Etapa 2: Adicionar a região	425
Etapa 3: atualizar a configuração do IdP externo	426
Etapa 4: Confirme as listas de permissões do firewall e do gateway	426
Etapa 5: fornecer informações aos seus usuários	426
A região muda além da adição da primeira região	427
Quais dados são replicados?	427
Acesso à força de trabalho por meio de uma região adicional	428
Sessões de usuário em várias Regiões da AWS	429
AWS acesse os endpoints do portal nos terminais primário e adicional Regiões da AWS	429
Endpoints ACS no primário e adicional Regiões da AWS	431
Usando aplicativos AWS gerenciados sem vários ACS URLs	432
Failover para uma região adicional para acesso Conta da AWS	433
Conta da AWS resiliência de acesso sem vários ACS URLs	434
Implantação e gerenciamento de aplicativos em várias Regiões da AWS	435
Implantação e gerenciamento de aplicativos AWS gerenciados em várias Regiões da AWS	435
Implantação e gerenciamento de aplicativos gerenciados pelo cliente em várias AWS regiões	437
Remover uma região do IAM Identity Center	437
Etapa 1: Atualizar a configuração do IdP externo	437
Etapa 2: remover a região	437
Etapa 3: excluir a chave de réplica	439
Serviço APIs suportado em adicionais Regiões da AWS	439
CloudTrail eventos nas regiões primárias e adicionais	440
Casos de uso do IAM Identity Center nas regiões primária e adicional	440
Design de resiliência e comportamento regional	443
Projetado para garantir disponibilidade	444
Configure o acesso de emergência ao Console de gerenciamento da AWS	444
Resumo da configuração de acesso de emergência	445
Como projetar suas funções operacionais críticas	446

Como planejar seu modelo de acesso	447
Como criar um mapeamento emergencial de funções, contas e grupos	448
Como criar sua configuração de acesso de emergência	449
Tarefas preparatórias de emergência	450
Processo de failover de emergência	450
Retorno às operações normais	451
Configuração única de um aplicativo de federação direta do IAM no Okta	451
Configuração única de um aplicativo de federação direta do IAM com ADFS	455
Segurança	462
Gerenciamento de identidade e acesso para o IAM Identity Center	463
Autenticação	463
Controle de acesso	463
Visão geral do gerenciamento de acesso	464
Exemplos de políticas baseadas em identidade	468
Exemplo de política baseada em recursos	476
AWS políticas gerenciadas	479
Uso de perfis vinculados ao serviço	501
Console do IAM Identity Center e autorização de API	509
Ações de API após novembro de 2023	509
Ações de API após outubro de 2020	510
AWS STS chaves de condição para o IAM Identity Center	512
UserId	513
IdentityStoreArn	514
ApplicationArn	514
CredentialId	515
InstanceArn	515
Registro em log e monitoramento	515
Registro de chamadas da API do IAM Identity Center com AWS CloudTrail	516
Registro em log do SCIM do IAM Identity Center SCIM com o AWS CloudTrail	556
Amazon EventBridge	563
Como registrar em log de erros de sincronização configurável do AD	563
Validação de conformidade	566
Padrões de conformidade compatíveis	567
Resiliência	568
Segurança da infraestrutura	569
Proteção de dados	570

Criptografia em trânsito	570
Privacidade de dados	571
Retenção de dados	571
Criptografia em repouso	571
Contexto de criptografia do IAM Identity Center	573
Usar o contexto de criptografia para controlar o acesso à chave gerenciada pelo cliente	574
Como monitorar chaves de criptografia para o IAM Identity Center	574
AWS armazenamento, criptografia e exclusão dos atributos de identidade do IAM Identity Center em aplicativos gerenciados	574
Como implementar chaves KMS gerenciadas pelo cliente	575
Declarações de chave KMS e de política do IAM de linha de base	585
Declarações de política de chave KMS avançadas	607
Marcar recursos	617
Restrições de tags	618
Gerenciar tags com o console	618
AWS CLI exemplos	619
Atribuir tags	619
Visualizar tags	620
Remover tags	620
Aplicar tags ao criar um conjunto de permissões	620
Ações da API	621
Integração da AWS CLI com o IAM Identity Center	622
Como integrar a AWS CLI com o IAM Identity Center	622
Considerações sobre acesso privado	623
Cotas	624
Cotas de aplicativos	624
Conta da AWS cotas	625
Cotas do Active Directory	626
IAM Identity Center Identity Store	626
Limites de controle do IAM Identity Center	627
Cotas de solicitação de serviço do OIDC	628
Cotas adicionais	629
Solução de problemas	631
Problemas ao criar uma instância de conta do IAM Identity Center	631
Você recebe um erro quando tenta visualizar a lista de aplicações de nuvem pré-configuradas para trabalhar com o IAM Identity Center	631

Problemas relacionados ao conteúdo das asserções SAML criadas pelo IAM Identity Center ..	633
Usuários específicos não conseguem sincronizar com o IAM Identity Center a partir de um provedor SCIM externo	633
Erro de usuário ou grupo duplicado ao provisionar usuários ou grupos com um provedor de identidades externo	635
Os usuários não podem fazer login quando o nome de usuário está no formato UPN	636
Recebo o erro “Não é possível realizar a operação no perfil protegido” ao modificar um perfil do IAM	636
Os usuários do diretório não podem redefinir suas senhas	637
Meu usuário é referenciado em um conjunto de permissões, mas não consegue acessar as contas ou aplicativos atribuídos	637
Não consigo configurar corretamente minha aplicação do catálogo de aplicações	638
Erro “Ocorreu um erro inesperado” quando um usuário tenta fazer login usando um provedor de identidades externo	638
Erro “Falha na ativação dos atributos do controle de acesso”	640
Recebo a mensagem “Navegador não suportado” quando tento registrar um dispositivo para MFA	640
O grupo “Usuários do domínio” do Active Directory não é sincronizado corretamente com o IAM Identity Center	640
Erro de credenciais de MFA inválidas	640
Recebo a mensagem “Ocorreu um erro inesperado” quando tento me registrar ou entrar usando um aplicativo autenticador	641
Eu recebo uma mensagem de erro “Não é você, somos nós” ao tentar fazer login no IAM Identity Center	641
Meus usuários não estão recebendo e-mails do IAM Identity Center	642
Erro: você não pode delete/modify/remove/assign acessar os conjuntos de permissões provisionados na conta de gerenciamento	642
Erro: token de sessão não encontrado ou inválido	642
Membros do grupo de domínios confiáveis não sincronizam com o IAM Identity Center	642
Solucione problemas de chaves gerenciadas pelo cliente em Centro de Identidade do AWS IAM	643
Acesso negado: problema de permissão decriptografia do KMS	643
AWS falhas de login de aplicativos gerenciados com uma chave KMS gerenciada pelo cliente ativada no IAM Identity Center	644
AWS falha de atribuição de and/or usuário na instalação do aplicativo gerenciado com uma chave KMS gerenciada pelo cliente ativada no IAM Identity Center	644

Problema de permissões do KMS: configuração da chave gerenciada pelo cliente com Centro de Identidade do AWS IAM	644
AWS falhas de login no portal de acesso com uma chave KMS gerenciada pelo cliente ativada no IAM Identity Center	645
Solucionar problemas de configuração multirregional em Centro de Identidade do AWS IAM ...	645
A região para a qual eu quero replicar minha instância do IAM Identity Center não está disponível no console do IAM Identity Center	645
AWS falhas de login de aplicativos gerenciados em uma região adicional	646
Histórico do documento	647
AWS Glossário	658
.....	dclix

O que é o IAM Identity Center?

Centro de Identidade do AWS IAM é a AWS solução para conectar os usuários da sua força de trabalho a aplicativos AWS gerenciados, como o Kiro e o Amazon Quick, além de outros AWS recursos. Você pode conectar o seu provedor de identidades existente e sincronizar os usuários e grupos do seu diretório, ou criar e gerenciar os usuários diretamente no IAM Identity Center. Depois, você pode usar o IAM Identity Center para ambas ou uma das seguintes alternativas:

- Acesso dos usuário a aplicações
- Acesso do usuário ao Contas da AWS

Já está usando o IAM para acessar Contas da AWS?

Você não precisa fazer nenhuma alteração em seus Conta da AWS fluxos de trabalho atuais para usar o IAM Identity Center para acessar aplicativos AWS gerenciados. Se você estiver usando a [federação com o IAM](#) para Conta da AWS acessar, seus usuários podem continuar Contas da AWS acessando da mesma forma que sempre fizeram, e você pode continuar usando seus fluxos de trabalho existentes para gerenciar esse acesso.

Por que usar o IAM Identity Center?

O IAM Identity Center agiliza e simplifica o acesso dos usuários da força de trabalho aos aplicativos ou Contas da AWS, ou ambos, por meio dos seguintes recursos principais.

Integração com aplicativos AWS gerenciados

[AWS aplicativos gerenciados](#), como o Kiro, e Amazon Redshift integrados ao IAM Identity Center. O IAM Identity Center fornece aplicativos AWS gerenciados com uma visão comum de usuários e grupos.

Propagação de identidades confiáveis entre aplicações

Com a propagação de identidade confiável, aplicativos AWS gerenciados como o Amazon Quick podem compartilhar com segurança a identidade de um usuário com outros aplicativos AWS gerenciados, como Amazon Redshift, por exemplo, autorizar o acesso a AWS recursos com base na identidade do usuário. Você pode auditar mais facilmente a atividade do usuário porque os CloudTrail eventos são registrados com base no usuário e nas ações que o usuário iniciou.

Isso facilita saber quem acessou o quê. Para obter informações sobre casos de uso compatíveis, incluindo diretrizes de end-to-end configuração, consulte [Casos de uso de propagação de identidades confiáveis](#).

Um local único para atribuir permissões a várias Contas da AWS

Com permissões multicontas, o IAM Identity Center fornece um local único para você atribuir permissões a grupos de usuários em várias Contas da AWS. 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 seu acesso a informações específicas Contas da AWS.

Esse atributo opcional só está disponível para [instâncias de organização](#) do IAM Identity Center.

Um ponto de federação único para simplificar o acesso dos usuários à AWS

Ao fornecer um ponto de federação, o IAM Identity Center reduz o esforço administrativo necessário para usar vários aplicativos AWS gerenciados Contas da AWS e. Com o IAM Identity Center, você só precisa federar uma vez e tem apenas um certificado para gerenciar ao usar um provedor de identidades [SAML 2.0](#). O IAM Identity Center fornece aos aplicativos AWS gerenciados uma visão comum de usuários e grupos para casos de uso confiáveis de propagação de identidade ou quando os usuários compartilham o acesso aos AWS recursos com outras pessoas.

Para obter informações sobre como configurar os provedores de identidades mais usados para operarem com o IAM Identity Center, consulte [Tutoriais sobre fontes de identidade do IAM Identity Center](#). Se você não tiver um provedor de identidades, poderá [criar e gerenciar usuários diretamente no IAM Identity Center](#).

Dois tipos de instância

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 a partir do qual você pode gerenciar o acesso do usuário. AWS

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 obter mais informações, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

Acesso a um portal amigável na Web para os usuários

O portal de AWS acesso é um portal da web fácil de usar que fornece aos usuários acesso contínuo a todos os aplicativos atribuídos ou a Contas da AWS ambos.

Acesso e aplicativos em Contas da AWS várias regiões

Quando você replica sua instância do IAM Identity Center para regiões adicionais, sua força de trabalho pode acessar seus aplicativos atribuídos Contas da AWS por meio de todas as regiões habilitadas e implantar aplicativos AWS gerenciados em cada região habilitada.

Renomeação do IAM Identity Center

Em 26 de julho de 2022, o AWS Single Sign-On foi renomeado para. Centro de Identidade do AWS IAM

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 `AWSIIdentitySync`
- [Endpoints de serviço](#) contendo `sso` e `identitystore`
- Recursos [CloudFormation](#) contendo prefixos `AWS::SSO`
- [Função vinculada ao serviço](#) contendo `AWSServiceRoleForSSO`
- Console URLs contendo `sso` e `singlesignon`
- Documentação URLs contendo `singlesignon`

Conceitos básicos do Centro de Identidade do IAM

Veja a seguir como você pode começar a usar o IAM Identity Center.

1. Habilitar o IAM Identity Center

Ao [habilitar o IAM Identity Center](#), você escolhe entre dois tipos de instâncias do IAM Identity Center. Esses tipos são: [instâncias da organização](#) (recomendadas) e [instâncias da conta](#). Para saber mais sobre os diferentes recursos desses tipos de instância, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

Note

Depois que o IAM Identity Center estiver habilitado, você poderá fazer login e abrir o [console do IAM Identity Center](#) fazendo o seguinte:

- Instância da organização - Faça login AWS usando credenciais com permissões administrativas na conta de gerenciamento.
- Instância da conta - Faça login AWS usando credenciais com permissões administrativas no local em Conta da AWS que o IAM Identity Center está ativado.

2. Conecte a fonte de identidade ao IAM Identity Center

No console do IAM Identity Center, confirme a fonte de identidade que você deseja usar. Consulte o seguinte para obter as fontes de identidade:

- Provedor de identidade externo — Se você tiver um provedor de identidade existente para gerenciar os usuários da força de trabalho, poderá conectá-lo ao IAM Identity Center. Para obter mais informações sobre como configurar os provedores de identidades mais usados para operarem com o IAM Identity Center, consulte [Tutoriais sobre fontes de identidade do IAM Identity Center](#).
- Active Directory — Se você estiver usando o Active Directory para gerenciar os usuários da força de trabalho, poderá conectá-lo ao IAM Identity Center. Para obter mais informações, consulte [Usar o Active Directory como uma fonte de identidades](#).
- IAM Identity Center — Como alternativa, você pode [criar e gerenciar usuários e grupos diretamente no IAM Identity Center](#).

 Note

Atualmente, você deve usar um provedor de identidade externo como fonte de identidade para aproveitar uma configuração multirregional com seu IAM Identity Center. Para obter mais informações sobre os benefícios dessa configuração, consulte [Usando o IAM Identity Center em várias Regiões da AWS](#).

3. Configurar o acesso do usuário a Contas da AWS (somente instância da organização)

Se você estiver usando uma instância organizacional do IAM Identity Center, você pode [atribuir acesso a usuários ou grupos Contas da AWS](#), usando [conjuntos de permissões](#) para conceder aos usuários acesso Contas da AWS e recursos.

4. Configurar o acesso do usuário a aplicações

Com o IAM Identity Center, você pode conceder aos usuários acesso a dois tipos de aplicações:

a. [AWS aplicativos gerenciados](#)

- Você pode usar o IAM Identity Center com aplicativos AWS gerenciados como Amazon Q Business e Amazon Redshift. AWS CLI Para obter mais informações, consulte [AWS aplicativos gerenciados](#) e [Integração da AWS CLI com o IAM Identity Center](#).

b. [Aplicações gerenciadas pelo cliente](#)

- Você pode integrar qualquer um dos seguintes tipos de aplicações gerenciadas pelo cliente com o IAM Identity Center:
 - [Aplicações listadas no catálogo do IAM Identity Center](#)
 - [Aplicações personalizadas](#)
- Depois de configurar a aplicação, você pode [atribuir o acesso à aplicação aos usuários](#).

5. Forneça aos usuários instruções de login para o portal de acesso do AWS

O portal de AWS acesso é um portal da web que fornece aos usuários acesso contínuo a todos os aplicativos atribuídos ou Contas da AWS a ambos. Novos usuários no IAM Identity Center devem ativar suas credenciais de usuário antes de poderem entrar no portal de AWS acesso.

Para obter 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. Para saber mais sobre o processo de login no portal de AWS acesso, consulte [Entrando no portal de AWS acesso](#).

Pré-requisitos e considerações sobre o IAM Identity Center

Você pode usar o IAM Identity Center para acessar somente aplicativos AWS gerenciados, Contas da AWS somente ou ambos. Se você estiver usando a federação do IAM para gerenciar o acesso Contas da AWS, você pode continuar fazendo isso enquanto usa o IAM Identity Center para acesso ao aplicativo.

Antes de habilitar o IAM Identity Center, considere o seguinte:

- AWS Região

Primeiro, você ativa o IAM Identity Center em uma única região [compatível](#) para cada instância do IAM Identity Center. Se você quiser usar o IAM Identity Center para acesso único às contas AWS, a região deverá estar acessível a todos os usuários da organização. Se você planeja usar o IAM Identity Center para acessar aplicativos, saiba que alguns aplicativos AWS gerenciados, como o Amazon SageMaker AI, podem operar somente nas regiões que oferecem suporte. Além disso, a maioria dos aplicativos AWS gerenciados exige que o IAM Identity Center esteja disponível na mesma região do aplicativo. Isso pode ser feito colocando-os na mesma região ou, quando houver suporte, replicando a instância do IAM Identity Center na região de implantação desejada de um AWS aplicativo gerenciado. Para obter mais informações, consulte [Considerações para escolher um Região da AWS](#).

- Acesso somente à aplicação

Você pode usar o IAM Identity Center somente para acesso do usuário a aplicativos como o Kiro, usando seu provedor de identidade existente. Para obter mais informações, consulte [Uso do IAM Identity Center para acesso dos usuário apenas a aplicações](#).

 Note

O acesso aos recursos da aplicação é gerenciado independentemente pelo proprietário da aplicação.

- Cotas para perfis do IAM

O IAM Identity Center cria perfis do IAM para dar aos usuários permissões para contabilizar os recursos. Para obter mais informações, consulte [Perfis do IAM criados pelo IAM Identity Center](#).

- 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. 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. Para obter mais informações, consulte [Centro de identidade do IAM e AWS Organizations](#).

As interfaces web do IAM Identity Center, incluindo o portal de acesso e o console do IAM Identity Center, devem ser acessadas por humanos por meio de navegadores da web compatíveis. Os navegadores compatíveis incluem as três versões mais recentes do Microsoft Edge, Mozilla Firefox, Google Chrome e Apple Safari. O acesso a esses endpoints usando caminhos não baseados em navegador não é suportado. Para acesso programático aos serviços do IAM Identity Center, recomendamos usar a documentação APIs disponível nos guias de referência da API IAM Identity Center e Identity Store.

Considerações para escolher um Região da AWS

Você pode ativar o IAM Identity Center em um único suporte Região da AWS de sua escolha e ele está disponível para usuários em todo o mundo. Essa disponibilidade global facilita a configuração do acesso do usuário a vários Contas da AWS aplicativos. A seguir, estão as principais considerações para escolher uma Região da AWS.

- **Localização geográfica dos seus usuários** — 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 o Amazon AI. SageMaker
- **Regiões de aceitação (regiões que estão desativadas por padrão)** — Uma região de aceitação é Região da AWS aquela que está desativada por padrão. Você deve habilitar a região opcional para usá-la. Para obter mais informações, consulte [Como gerenciar o IAM Identity Center em uma região de aceitação](#).
- **Replicação do IAM Identity Center para regiões adicionais** — Se você planeja replicar o IAM Identity Center para outras regiões Regiões da AWS, você deve escolher uma região ativada por padrão. Para obter mais informações, consulte [Usando o IAM Identity Center em várias Regiões da AWS](#).
- **Escolha de regiões de implantação para aplicativos AWS AWS gerenciados** — os Regiões da AWS aplicativos gerenciados podem operar somente onde estão disponíveis. Muitos aplicativos AWS gerenciados também podem operar somente em uma região na qual o IAM Identity Center está habilitado ou replicado (região primária ou adicional). Para confirmar se sua instância do

IAM Identity Center oferece suporte à replicação para regiões adicionais, consulte [Usando o IAM Identity Center em várias Regiões da AWS](#). Se a replicação não for uma opção, considere habilitar o IAM Identity Center na região em que você planeja usar aplicativos AWS gerenciados.

- Soberania digital: os regulamentos ou as políticas da empresa sobre soberania digital podem exigir o uso de uma determinada Região da AWS. Consulte o departamento jurídico da sua empresa.
- Fonte de identidade — Se você estiver usando [AWS Managed Microsoft AD](#) seu diretório autogerenciado no Active [Directory \(AD\)](#) como fonte de identidade, sua região de origem deverá corresponder à Região da AWS na qual você habilitou o IAM Identity Center.
- E-mails entre regiões com o Amazon Simple Email Service — Em algumas regiões, o IAM Identity Center pode chamar o [Amazon Simple Email Service \(Amazon SES\)](#) em outra região para enviar e-mails. Nessas chamadas entre regiões, o IAM Identity Center envia determinados atributos de usuário para a outra região. Para obter mais informações, consulte [E-mails entre regiões com o Amazon SES](#).
- AWS Control Tower— Se você estiver habilitando uma instância organizacional do IAM Identity Center a partir de AWS Control Tower, a instância será criada na mesma região da AWS Control Tower landing zone.

Tópicos

- [Armazenamento de dados e operações da região do IAM Identity Center](#)
- [Trocando Regiões da AWS](#)
- [Desativando e Região da AWS onde o IAM Identity Center está ativado](#)

Armazenamento de dados e operações da região do IAM Identity Center

Saiba como o IAM Identity Center lida com o armazenamento e as operações de dados entre as Regiões da AWS.

Entender como o IAM Identity Center armazena dados

Quando você ativa o IAM Identity Center, todos os dados que você configura no IAM Identity Center são armazenados na região em que você os habilitou. 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. Se você replicar sua instância do IAM Identity Center para regiões adicionais, o

IAM Identity Center replica automaticamente usuários, grupos, conjuntos de permissões e suas atribuições, além de outros metadados e configurações para essas regiões.

E-mails entre regiões com o Amazon SES

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.

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
ap-east-1	Ásia-Pacífico (Hong Kong)	ap-northeast-2	Ásia-Pacífico (Seul)
ap-east-2	Ásia-Pacífico (Taipei)	ap-northeast-1	Ásia-Pacífico (Tóquio)
ap-south-2	Ásia-Pacífico (Hyderabad)	ap-south-1	Ásia-Pacífico (Mumbai)
ap-southeast-4	Ásia-Pacífico (Melbourne)	ap-southeast-2	Ásia-Pacífico (Sydney)
ap-southeast-5	Ásia-Pacífico (Malásia)	ap-southeast-1	Ásia-Pacífico (Singapura)
ap-southeast-6	Ásia-Pacífico (Nova Zelândia)	ap-southeast-2	Ásia-Pacífico (Sydney)
ap-southeast-7	Ásia-Pacífico (Tailândia)	ap-northeast-3	Ásia-Pacífico (Osaka)

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
ca-west-1	Oeste do Canadá (Calgary)	ca-central-1	Canadá (Central)
eu-south-2	Europa (Espanha)	eu-west-3	Europa (Paris)
eu-central-2	Europa (Zurique)	eu-central-1	Europa (Frankfurt)
mx-central-1	México (Centro)	us-east-2	Leste dos EUA (Ohio)
me-central-1	Oriente Médio (Emirados Árabes Unidos)	eu-central-1	Europa (Frankfurt)
us-gov-east-1	AWS GovCloud (Leste dos EUA)	us-gov-west-1	AWS GovCloud (Oeste dos EUA)

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

Gerenciamento do IAM Identity Center em uma região de adesão opcional (região desabilitada por padrão)

A maioria Regiões da AWS está habilitada para operações em todos os AWS serviços por padrão, mas você deve habilitar as seguintes [regiões opcionais](#) se quiser usar o IAM Identity Center:

- Africa (Cape Town)

- Ásia Pacífico (Hong Kong)
- Ásia-Pacífico (Taipei)
- Ásia-Pacífico (Hyderabad)
- Ásia-Pacífico (Jacarta)
- Ásia-Pacífico (Melbourne)
- Ásia-Pacífico (Malásia)
- Ásia-Pacífico (Nova Zelândia)
- Ásia-Pacífico (Tailândia)
- Oeste do Canadá (Calgary)
- Europa (Milão)
- Europa (Espanha)
- Europa (Zurique)
- Israel (Tel Aviv)
- México (Centro)
- Oriente Médio (Bahrein)
- Oriente Médio (Emirados Árabes Unidos)

Se você implantar o IAM Identity Center em uma região de aceitação, deverá habilitar essa região em todas as contas em que desejar gerenciar o acesso ao IAM Identity Center. Todas as contas precisam dessa configuração, independentemente de você criar ou não recursos nessa região. Você pode habilitar uma região para as contas atuais da organização e deve repetir essa ação quando adicionar novas contas. Para obter instruções, consulte [Habilitar ou desabilitar uma região na organização](#) no Guia do Usuário do AWS Organizations . Para não precisar repetir essas etapas adicionais, você pode optar por implantar o IAM Identity Center em uma [Região habilitada por padrão](#).

 Note

Sua conta de AWS membro deve estar na mesma região da região de inscrição em que sua instância do IAM Identity Center está localizada, para que você possa acessar a conta do AWS membro a partir do portal de AWS acesso.

Metadados armazenados nas regiões de aceitação

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
- Amazon Resource Names (ARNs) das funções do IAM que o IAM Identity Center cria na conta do membro

Regiões da AWS que estão habilitados por padrão

As seguintes regiões estão habilitadas por padrão e você pode habilitar o IAM Identity Center nessas regiões.

- 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)
- Ásia-Pacífico (Osaka)

Trocando Regiões da AWS

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. Para obter mais informações, consulte [Considerações para escolher um Região da AWS](#).

Você pode alterar a região do IAM Identity Center somente ao [excluir a instância atual do IAM Identity Center](#) e criar uma instância em outra região. Se você já habilitou uma aplicação gerenciada pela AWS com a instância existente do IAM Identity Center, desabilite a aplicação antes de excluir o IAM Identity Center. Para obter instruções sobre como desativar aplicativos AWS gerenciados, consulte [Desabilitando um aplicativo AWS gerenciado](#).

Note

Se você está pensando em mudar sua região do IAM Identity Center para permitir a implantação de um aplicativo AWS gerenciado em outra região, considere replicar sua instância do IAM Identity Center para essa região. Para obter mais informações, consulte [Usando o IAM Identity Center em várias Regiões da AWS](#).

Considerações sobre a configuração na nova região

Você deverá recriar usuários, grupos, conjuntos de permissões, aplicações e atribuições na nova instância do IAM Identity Center. Você pode usar a conta do IAM Identity Center e a atribuição do aplicativo [APIs](#) para obter um instantâneo da sua configuração e, em seguida, usar esse instantâneo para reconstruir sua configuração em uma nova região. Mudar para uma região diferente também altera a URL do [portal de AWS acesso](#), que fornece aos usuários acesso de login único a seus aplicativos Contas da AWS e aplicativos. Pode ser necessário também recriar algumas configurações do IAM Identity Center por meio do Management Console da nova instância.

Desativando e Região da AWS onde o IAM Identity Center está ativado

Se você desabilitar um Região da AWS no qual o IAM Identity Center está instalado, o IAM Identity Center também será desativado. Após o IAM Identity Center ser desabilitado em uma região, os usuários dessa região não terão acesso de login único às Contas da AWS e aplicações.

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, 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.

Uso do IAM Identity Center para acesso dos usuário apenas a aplicações

Você pode usar o IAM Identity Center para acesso do usuário a aplicativos como o Kiro ou ambos. Contas da AWS Você pode conectar o seu provedor de identidades existente e sincronizar usuários e grupos do seu diretório, ou [criar e gerenciar os usuários diretamente no IAM Identity Center](#). Para obter informações sobre como conectar seu provedor de identidades existente ao IAM Identity Center, consulte os [Tutoriais sobre fontes de identidade do IAM Identity Center](#).

Já está usando o IAM para acessar Contas da AWS?

Você não precisa fazer nenhuma alteração em seus Conta da AWS fluxos de trabalho atuais para usar o IAM Identity Center para acessar aplicativos AWS gerenciados. Se você estiver usando a [federação com o IAM](#) para Conta da AWS acessar, seus usuários podem continuar Contas da AWS acessando da mesma forma que sempre fizeram, e você pode continuar usando seus fluxos de trabalho existentes para gerenciar esse acesso.

Perfis do IAM criados pelo IAM Identity Center

Quando você atribui um usuário a uma AWS conta, o IAM Identity Center cria funções do IAM para dar aos usuários permissões sobre 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.

A replicação da instância do IAM Identity Center para regiões adicionais não afeta as funções existentes do IAM e não cria novas funções do IAM.

 Note

Os conjuntos de permissões não são usados para conceder permissões às aplicações.

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 IAM Identity Center 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 da AWS adicionais que você convida para sua organização são contas-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 obter mais informações, consulte [Instâncias de organização 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 [Habilitar todos os recursos em sua organização](#) no Manual do usuário do AWS Organizations .

Para habilitar uma instância organizacional do IAM Identity Center, você deve entrar no Console de gerenciamento da AWS 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). Para obter mais informações, consulte [Criação e gerenciamento de uma AWS organização](#) no Guia AWS Organizations do usuário.

Ao fazer login com credenciais administrativas de uma conta AWS Organizations membro, você pode habilitar uma instância de conta do IAM Identity Center. As instâncias da conta têm recursos limitados e estão vinculadas a uma única AWS conta.

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.

- Instância de organização (recomendada)

Uma instância do IAM Identity Center que você ativa na conta AWS Organizations de gerenciamento. As instâncias da organização suportam todos os recursos do IAM Identity Center. Recomendamos que você implante uma instância de organização em vez de instâncias de conta para minimizar o número de pontos de gerenciamento.

- Instância de conta

Uma instância do IAM Identity Center vinculada a uma única Conta da AWS e visível somente na Conta da AWS AWS região em que está ativada. Use uma instância de conta para cenários mais simples e de conta única. Você pode habilitar uma instância de conta em:

- E Conta da AWS isso não é gerenciado por AWS Organizations
- Uma conta de membro em AWS Organizations

Conta da AWS tipos que podem habilitar o IAM Identity Center

Para habilitar o IAM Identity Center, faça login no Console de gerenciamento da AWS 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. Você pode associar somente uma instância do IAM Identity Center a uma instância autônoma Conta da AWS e usar essa instância para atribuições de aplicativos dentro dessa instância autônoma. Conta da AWS

Use a tabela a seguir para comparar os recursos fornecidos pelo tipo de instância:

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

Recurso	Instância na conta AWS Organizations de gerenciamento (recomendado)	Instância em uma conta-membro	Instância em uma instância autônoma Conta da AWS	
AWS portal de acesso para acesso com login único aos seus aplicativos AWS gerenciados	 S	 S	 Sim	
OAuth Aplicativos 2.0 (OIDC) gerenciados pelo cliente	 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	
Aplicações SAML 2.0 gerenciadas pelo cliente	 S	 N	 Não	
O administrador delegado pode gerenciar a instância	 S	 N	 Não	
Criptografia em repouso usando uma chave KMS gerenciada pelo cliente	 S	 N	 Não	

Recurso	Instância na conta AWS Organizations de gerenciamento (recomendado)	Instância em uma conta-membro	Instância em uma instância autônoma Conta da AWS
Replicando o IAM Identity Center para regiões adicionais		S 	N 

Para obter mais informações sobre aplicativos AWS gerenciados e o IAM Identity Center, consulte [AWS aplicativos gerenciados que você pode usar com o IAM Identity Center](#).

Tópicos

- [Instâncias de organização do IAM Identity Center](#)
- [Instâncias de conta do Centro de Identidade do IAM](#)
- [Excluir sua instância do IAM Identity Center](#)

Instâncias de organização do IAM Identity Center

Ao habilitar 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.

Para habilitar uma instância de organização do IAM Identity Center, consulte [Para habilitar uma instância do IAM Identity Center](#).

Quando usar uma instância de organização

Uma instância de organização é o principal método para habilitar o IAM Identity Center e, usualmente, uma instância de 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, a atribuição de acesso a aplicativos gerenciados pelo cliente e a replicação em várias regiões.
- Redução do número de pontos de gerenciamento: uma instância de organização tem um único ponto de gerenciamento, a conta gerencial. Recomendamos que você habilite uma instância de organização, em vez de uma instância de conta, para reduzir o número de pontos de gerenciamento.
- Controle central da 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).

Para obter instruções sobre como habilitar uma instância de organização do IAM Identity Center, consulte [Para habilitar uma instância do IAM Identity Center](#).

Instâncias de conta do Centro de Identidade do IAM

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 a partir de uma das seguintes opções: uma conta de membro AWS Organizations ou uma conta autônoma Conta da AWS que não seja gerenciada por AWS Organizations.

Para obter instruções sobre como habilitar uma instância de conta do IAM Identity Center, consulte [Para habilitar uma instância do IAM Identity Center](#) e escolha a aba Conta.

Quando usar uma instância de conta

Na maioria dos casos, uma [instância da organização](#) é recomendada. Use instâncias de conta somente 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 de organização do IAM Identity Center, mas deseja implantar uma aplicação gerenciada pela AWS compatível em um conjunto isolado de usuários que são distintos dos usuários da instância da sua organização.
- Você não controla a AWS organização na qual opera. Por exemplo, um terceiro controla a AWS organização que gerencia sua Contas da AWS.

Important

Se você planeja usar o IAM Identity Center para oferecer suporte a aplicações em várias contas, use uma instância de organização. As instâncias de conta não oferecem suporte a esse caso de uso.

AWS aplicativos gerenciados que oferecem suporte a instâncias de contas

Veja [AWS aplicativos gerenciados que você pode usar com o IAM Identity Center](#) 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.

Restrições de disponibilidade para contas-membro

Para implantar instâncias de conta do IAM Identity Center nas contas dos AWS Organizations membros, uma das seguintes condições deve ser verdadeira:

- Não há nenhuma instância de organização do IAM Identity Center em sua organização da .
- Há uma instância de organização do IAM Identity Center na organização e o administrador da instância permite a criação de instâncias de conta do IAM Identity Center (para instâncias organizacionais criadas após 15 de novembro de 2023).
- Há uma instância de organização do IAM Identity Center em sua organização da e o administrador da instância habilitou manualmente a criação de instâncias de conta pelas contas-membro da organização (para instâncias de organização criadas após 15 de novembro de 2023). Para instruções, consulte [Permitir a criação de instâncias de conta em contas de membros](#).

Depois que uma das condições anteriores for atendida, todas as seguintes condições devem ser verdadeiras:

- O administrador não criou uma [política de controle de serviços](#) que impede a criação de instâncias de conta.
- Você não tem uma instância do IAM Identity Center nessa mesma conta, não importando a Região da AWS.
- Você está trabalhando em um Região da AWS local onde o IAM Identity Center está disponível. Para obter mais informações sobre regiões, consulte [Armazenamento de dados e operações da região do IAM Identity Center](#).

Considerações sobre instâncias de conta

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

- As instâncias de conta não são compatíveis com conjuntos de permissões e, portanto, não são compatíveis com o acesso a Contas da AWS.
- Você não pode converter uma instância de conta em uma instância de organização.
- Somente [aplicações gerenciadas pela AWS](#) são compatíveis com instâncias de conta.
- 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.

Permitir a criação de instâncias de conta em contas de membros

Se você habilitou o IAM Identity Center antes de 15 de novembro de 2023, você tem uma [instância de organização](#) do IAM Identity Center com a capacidade de contas de membros criarem instâncias de conta desabilitada por padrão. Você pode escolher se as contas-membros podem criar instâncias de conta habilitando o atributo de instância de conta no console do IAM Identity Center.

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

Important

Habilitar instâncias de conta do IAM Identity Center para contas-membro é uma operação única. Isso significa que a operação não pode ser revertida. Uma vez habilitada, você pode limitar a criação de instâncias de conta criando uma política de controle de serviços (SCP). Para obter instruções, consulte [Control account instance creation with Service Control Policies](#).

1. Abra o [console do IAM Identity Center](#).
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.

Use as Políticas de controle de serviço para controlar a criação de instâncias de conta

A capacidade das contas de membros criarem instâncias de conta depende de quando você habilitou o IAM Identity Center:

- Antes de novembro de 2023 — Você deve [permitir a criação de instâncias de conta nas contas de membros](#), uma ação que não pode ser revertida.
- Depois de 15 de novembro de 2023, as contas de membros podem criar instâncias de conta por padrão.

Em ambos os casos, você pode usar Service Control Policies (SCPs) para:

- Impedir que todas as contas de membros criem instâncias de conta.
- Permitir que somente contas de membros específicas criem instâncias de conta.

Evitar instâncias de conta

Use o procedimento a seguir para gerar um SCP que impede a criação de instâncias de conta do IAM Identity Center.

1. Abra o [console do IAM Identity Center](#).
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 direcionado ao [AWS Organizations console](#) para criar o SCP ou anexá-lo como uma declaração a um SCP existente. SCPs 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.

Limitar instâncias de conta

Em vez de impedir a criação de todas as instâncias da conta, essa política nega qualquer tentativa de criar uma instância de conta do IAM Identity Center para todos, Contas da AWS exceto aqueles explicitamente listados no **"<ALLOWED-ACCOUNT-ID>"** espaço reservado.

Example: negue a política para limitar a criação de instâncias da conta

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyMemberAccountInstances",
      "Effect": "Deny",
      "Action": "sso:CreateInstance",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
        }
      }
    }
  ]
}
```

```
    ]
  }
```

- Substitua ["<ALLOWED-ACCOUNT-ID>"] pelas Conta da AWS IDs reais que você deseja permitir para criar uma instância de conta do IAM Identity Center.
- Você pode listar várias contas permitidas IDs no formato de matriz: ["**111122223333**", "**444455556666**"].
- Anexe essa política ao SCP da organização para impor o controle centralizado sobre a criação da instância de conta do IAM Identity Center.

Para obter instruções sobre como anexar uma SCP, consulte [Attaching and detaching service control policies](#) no AWS Organizations User Guide.

Excluir sua instância do IAM Identity Center

Quando uma instância do IAM Identity Center é excluída, todos os dados dessa instância são excluídos e não podem ser recuperados. A tabela a seguir descreve quais dados são excluídos com base no tipo de diretório que está configurado no IAM Identity Center.

Quais dados são excluídos	Diretório conectado - AWS Managed Microsoft AD, AD Connector ou provedor de identidade e externo	Armazenamento de identidades do IAM Identity Center	
Todos os conjuntos de permissões para os quais você configurou Contas da AWS			S Sim
Todas as aplicações que você configurou no IAM Identity Center			S Sim

Quais dados são excluídos	Diretório conectado - AWS Managed Microsoft AD, AD Connector ou provedor de identidade e externo	Armazenamento de identidades do IAM Identity Center	
Todas as atribuições de usuário para as quais você configurou Contas da AWS e aplicativos		S 	Sim
Todos os usuários e grupos no diretório ou armazenamento	N/D		Sim

Se você replicou sua instância do IAM Identity Center para regiões adicionais, você deve remover essas regiões antes de excluir a instância.

Use os procedimentos a seguir para excluir sua instância do IAM Identity Center.

Para excluir sua instância 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 caixa de seleção para confirmar que você entende que os dados serão excluídos. Digite sua instância do IAM Identity Center na caixa de texto e escolha Confirmar.

Habilitar o IAM Identity Center

Ao ativar o IAM Identity Center, você escolhe um tipo de Centro de Identidade do AWS IAM instância para habilitar. Uma instância de um serviço é uma implantação única de um serviço em seu AWS ambiente. Há dois tipos de instâncias disponíveis para o IAM Identity Center: instâncias de organização e instâncias de conta. Os tipos de instância disponíveis para você habilitar dependem do tipo de conta na qual você fez login.

A lista a seguir identifica o tipo de instâncias do IAM Identity Center que você pode habilitar para cada tipo de Conta da AWS:

- 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. Você pode replicar esse tipo de instância para regiões adicionais para aumentar a resiliência do acesso à conta e flexibilidade na escolha das regiões de implantação de AWS aplicativos.
- 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. Você pode associar somente uma instância do IAM Identity Center a uma instância autônoma Conta da AWS e usar essa instância para atribuições de aplicativos dentro dessa instância autônoma. Conta da AWS

Important

A conta gerencial da organização pode controlar se [as contas de membro da organização podem criar instâncias de conta do IAM Identity Center](#) usando uma Política de Controle de Serviços.

Se você usa uma conta de nível gratuito, a criação de uma AWS organização atualiza automaticamente sua conta para um plano pago com pay-as-you-go preços. Seus créditos de nível gratuito expiram imediatamente. Para obter mais informações, consulte [Nível gratuito da AWS FAQs](#).

Para obter uma comparação dos diferentes recursos fornecidos pelos diferentes tipos de instância, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

Antes de habilitar o IAM Identity Center, recomendamos que você revise [Pré-requisitos e considerações sobre o IAM Identity Center](#).

Para habilitar uma instância do IAM Identity Center

Escolha a aba para o tipo de instância do IAM Identity Center que você deseja habilitar, seja uma instância de organização ou conta:

Organization (recommended)

1. Realize um dos procedimentos a seguir para fazer login no Console de gerenciamento da AWS.
 - 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, insira a senha.
 - Já está usando AWS com uma conta independente Conta da AWS (credenciais do IAM) — Faça login usando suas credenciais do IAM com permissões administrativas.
 - Já está usando AWS Organizations (credenciais do IAM) — Faça login usando as credenciais da sua conta de gerenciamento.
2. Abra o [console do IAM Identity Center](#).
3. (Opcional) Se você quiser usar uma chave KMS gerenciada pelo cliente para criptografia em repouso em vez da chave AWS gerenciada padrão, configure a chave gerenciada pelo cliente na seção Chave para criptografar dados do IAM Identity Center em repouso. Para obter mais informações, consulte [Implementando chaves KMS gerenciadas pelo cliente em Centro de Identidade do AWS IAM](#).

Important

Execute essa etapa somente se você tiver configurado as permissões necessárias para o uso da chave KMS gerenciada pelo cliente. Sem as permissões adequadas, essa etapa pode falhar ou interromper a administração e os aplicativos AWS gerenciados do IAM Identity Center.

4. Em Habilitar o IAM Identity Center, escolha Habilitar.

5. Na página **Habilitar o IAM Identity Center com AWS Organizations**, revise as informações e selecione **Habilitar** para concluir o processo.

 Note

AWS Organizations pode ter o IAM Identity Center ativado somente em uma única AWS região. Depois de habilitar o IAM Identity Center, se você precisar alterar a região em que o IAM Identity Center está habilitado, [exclua](#) a instância atual e crie uma instância na outra região.

Depois de habilitar a instância de organização, recomendamos que você execute as seguintes etapas para concluir a configuração do ambiente:

- Confirme se você está usando a fonte de identidade de escolha. Se já tiver uma fonte de identidades atribuída, você poderá continuar a usá-la. Para obter mais informações, consulte [Confirmar as fontes de identidades do IAM Identity Center](#).
- Registre uma conta de membro como administrador delegado. Para obter mais informações, consulte [Administradores delegados](#).
- O IAM Identity Center fornece um portal de acesso aos AWS recursos. Se você filtrar o acesso a AWS domínios específicos ou endpoints de URL usando uma solução de filtragem de conteúdo da Web, como firewalls de próxima geração (NGFW) ou Secure Web Gateways (SWG), consulte. [Atualize firewalls e gateways para permitir o acesso ao Portal de acesso da AWS](#)

Account

1. Realize um dos procedimentos a seguir para fazer login no Console de gerenciamento da AWS.
 - 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, insira a senha.
 - Já está usando AWS (credenciais do IAM) — Faça login usando suas credenciais do IAM com permissões administrativas.
 - Já está usando AWS Organizations (credenciais do IAM) — Faça login usando as credenciais administrativas da sua conta de membro.

2. Abra o [console do IAM Identity Center](#).
3. Se você é novo AWS ou tem um autônomo Conta da AWS, em Ativar o IAM Identity Center, escolha Habilitar.

Você vê a página Habilitar o IAM Identity Center com AWS Organizations. Esta etapa não é exigida, mas é recomendada.

Selecione o link habilitar uma instância de conta do IAM Identity Center.

4. Se você for administrador de uma conta AWS Organizations membro, em Habilitar uma instância de conta do IAM Identity Center, selecione Habilitar uma instância de conta.
5. Na página Habilitar uma instância de conta do IAM Identity Center, revise as informações e, opcionalmente, adicione as tags que você deseja associar a essa instância de conta. Em seguida, selecione Habilitar para concluir o processo.

 Note

Se sua AWS conta for membro de uma organização, pode haver restrições à sua capacidade de habilitar uma instância de conta do IAM Identity Center.

- Se a organização habilitou o IAM Identity Center antes de 15 de novembro de 2023, a capacidade de contas-membros criarem instâncias de conta está desabilitada por padrão e deve ser habilitada pela conta gerencial da organização.
- Se a organização habilitou o IAM Identity Center após 15 de novembro de 2023, a capacidade das contas de membro criarem instâncias de conta está habilitada por padrão. No entanto, as políticas de controle de serviço podem ser usadas para impedir a criação de instâncias de conta do IAM Identity Center dentro de uma organização.

Para obter mais informações, consulte [the section called “Permitir a criação de instâncias de conta em contas de membros”](#) e [the section called “SCPs para criação de instância de conta”](#).

Confirmar as fontes de identidades do 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 a escolha. Se já tiver uma fonte de identidades atribuída, você poderá continuar a usá-la.

Se você já estiver gerenciando usuários e grupos no Active Directory ou em um IdP externo, recomendamos que considere conectar essa fonte de identidade quando habilitar o IAM Identity Center e escolher a fonte de identidade. Isso deve ser feito antes de você criar qualquer usuário e grupo no diretório padrão do Centro de Identidade 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 obter mais informações, consulte [Considerações para alterar sua fonte de identidade](#).

Para confirmar sua fonte de identidade

1. Abra o [console do IAM Identity Center](#).
2. Na página Painel, abaixo da seção Etapas de configuração recomendadas, escolha Confirmar sua fonte de identidades. 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

Ao habilitar o IAM Identity Center pela primeira vez, ele é configurado automaticamente com um diretório do IAM Identity Center como sua fonte de identidade padrão. Se você ainda não estiver usando outro provedor de identidade externo, pode começar a criar seus usuários e grupos e atribuir o nível de acesso deles aos seus Contas da AWS aplicativos. 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 Directory Service ou em seu diretório autogerenciado em Active 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 obter mais informações, consulte [Diretório Microsoft AD](#).

Note

O IAM Identity Center não oferece suporte ao Simple AD SAMBA4 baseado como fonte de identidade.

Provedores de identidade externos

Para provedores de identidade externos (IdPs), como Okta ou Microsoft 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 a configurações da fonte de identidades, consulte [Tutoriais sobre fontes de identidade do IAM Identity Center](#).

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 IAM Identity Center não é compatível com o uso de MFA por provedores de identidade externos. Para obter mais informações, consulte [Solicite aos usuários o MFA](#).

 Note

Se você planeja replicar o IAM Identity Center para regiões adicionais, precisará configurar um provedor de identidade externo. Para obter mais detalhes, incluindo os pré-requisitos, consulte. [Usando o IAM Identity Center em várias Regiões da AWS](#)

Atualize firewalls e gateways para permitir o acesso ao Portal de acesso da AWS

O portal de AWS acesso fornece aos usuários 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 iniciar rapidamente vários aplicativos simplesmente escolhendo o ícone Conta da AWS ou aplicativo no portal.

 Note

AWS os aplicativos gerenciados se integram ao IAM Identity Center e o usam para serviços de autenticação e diretório, mas podem não usar o portal de AWS acesso para acesso ao aplicativo.

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 incluir na lista de permissões os domínios e endpoints de URL associados ao portal de acesso. AWS

A lista a seguir fornece os domínios de pilha dupla IPv4 e os endpoints de URL para adicionar às suas listas de permissões da solução de filtragem de conteúdo da web.

IPv4 lista de permissões

- *[Directory ID or alias].awsapps.com*
- *[Identity Center instance ID].[Region].portal.amazonaws.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].prod.pr.panorama.console.api.aws/panoramamaroute`
- `[Region].signin.aws`
- `[Region].signin.aws.amazon.com`
- `signin.aws.amazon.com`
- `*.cloudfront.net`
- `opfcaptcha-prod.s3.amazonaws.com`

Lista de permissões de pilha dupla

- `[Identity Center instance ID].portal.[Region].app.aws`
- `*.aws.dev`
- `*.awsstatic.com`
- `*.console.aws.a2z.com`
- `oidc.[Region].api.aws`
- `sso.[Region].api.aws`
- `portal.sso.[Region].api.aws`
- `[Region].sso.signin.aws`
- `[Region].signin.aws.amazon.com`
- `signin.aws.amazon.com`
- `*.cloudfront.net`
- `cdn.us-east-1.threat-mitigation.aws.amazon.com`
- `us-east-1.threat-mitigation.aws.amazon.com`
- `amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com`

Lista de permissões combinada (IPv4 + Dual-stack com compatibilidade com versões anteriores)

- `[Directory ID or alias].awsapps.com`

- `[Identity Center instance ID].[Region].portal.amazonaws.com`
- `[Identity Centers instance ID].portal.[Region].app.aws`
- `*.aws.dev`
- `*.awsstatic.com`
- `*.console.aws.a2z.com`
- `oidc.[Region].amazonaws.com`
- `oidc.[Region].api.aws`
- `*.sso.amazonaws.com`
- `*.sso.[Region].amazonaws.com`
- `sso.[Region].api.aws`
- `*.sso-portal.[Region].amazonaws.com`
- `portal.sso.[Region].api.aws`
- `[Region].prod.pr.panorama.console.api.aws/panoramamaroute`
- `[Region].signin.aws`
- `[Region].sso.signin.aws`
- `[Region].signin.aws.amazon.com`
- `signin.aws.amazon.com`
- `*.cloudfront.net`
- `opfcaptcha-prod.s3.amazonaws.com`
- `cdn.us-east-1.threat-mitigation.aws.amazon.com`
- `us-east-1.threat-mitigation.aws.amazon.com`
- `amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com`

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

Além dos requisitos da lista de permissões para o portal de AWS acesso, os outros serviços e aplicativos que você usa podem exigir a lista de permissões de domínios.

- Para acessar Contas da AWS o console do Console de gerenciamento da AWS 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

Console de gerenciamento da AWS obter uma lista de Console de gerenciamento da AWS domínios.

- Para acessar aplicativos AWS gerenciados do seu portal de AWS acesso, você deve permitir seus respectivos domínios. Consulte a documentação do respectivo serviço para obter orientação.
- Se você usa software externo, como externo IdPs (por exemplo, Okta e Microsoft Entra ID), precisará incluir seus domínios nas suas listas de permissões.

Tutoriais sobre fontes de identidade do IAM Identity Center

Você pode conectar sua fonte de identidade existente em sua conta AWS Organizations de gerenciamento a [uma instância organizacional do IAM Identity Center](#). Se você não tiver um provedor de identidades existente, poderá criar e gerenciar usuários diretamente no diretório padrão do IAM Identity Center. Você só pode ter uma fonte de identidade por organização.

Os tutoriais desta seção descrevem como configurar uma instância organizacional do IAM Identity Center com uma fonte de identidade comumente usada, criar um usuário administrativo e, se você estiver usando o IAM Identity Center para gerenciar o acesso Contas da AWS, criar e configurar conjuntos de permissões. Se você estiver usando o IAM Identity Center apenas para acessar aplicações, não precisará usar conjuntos de permissões.

Esses tutoriais não descrevem como configurar instâncias de conta do IAM Identity Center. Você pode usar instâncias de conta para atribuir usuários e grupos a aplicações, mas não pode usar esse tipo de instância para gerenciar o acesso dos usuários a Contas da AWS. Para obter mais informações, consulte [Instâncias de conta do Centro de Identidade do IAM](#).

Note

Antes de iniciar qualquer um desses tutoriais, habilite o IAM Identity Center. Para obter mais informações, consulte [Habilitar o IAM Identity Center](#).

Tópicos

- [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](#)
- [Vídeos de tutorial](#)

Usar o Active Directory como uma fonte de identidades

Se você estiver gerenciando usuários em seu AWS Managed Microsoft AD diretório usando Directory Service ou em seu diretório autogerenciado no Active Directory (AD), você pode alterar sua fonte de identidade 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 Identity Center ajudará você 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 AWS Managed Microsoft AD, deverá habilitar o IAM Identity Center no mesmo Região da AWS local em que seu AWS Managed Microsoft AD diretório está configurado. O IAM Identity Center armazena os dados de atribuição na mesma região do diretório. Para administrar o IAM Identity Center, talvez seja necessário mudar para a região em que o IAM Identity Center está 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 Service 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 planeja habilitar um 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.

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

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 Service habilite o MFA no IAM Identity Center.

AWS Managed Microsoft AD

1. Revise as orientações em [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 [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

Após conectar seu diretório ao IAM Identity Center, você pode especificar um usuário ao qual deseja conceder permissões administrativas e, em seguida, sincronizar esse usuário do seu diretório com o IAM Identity Center.

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 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 [Crie 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. Para

obter mais informações, consulte [Uso de federação de identidades SAML e SCIM com provedores de identidade externos](#).

 Note

CyberArk atualmente não oferece suporte ao SAML Multiple Assertion Consumer Service (ACS) URLs no aplicativo. Centro de Identidade do AWS IAM Esse recurso SAML é necessário para aproveitar totalmente o [suporte multirregional](#) no IAM Identity Center. Se você planeja replicar o IAM Identity Center para regiões adicionais, saiba que o uso de uma única URL do ACS pode afetar a experiência do usuário nessas regiões adicionais. Sua região principal continuará funcionando normalmente. Recomendamos que você trabalhe com seu fornecedor de IdP para ativar esse recurso. Para obter mais informações sobre a experiência do usuário em regiões adicionais com um único URL ACS, consulte [the section called “Usando aplicativos AWS gerenciados sem vários ACS URLs”](#) e [the section called “Conta da AWS resiliência de acesso sem vários ACS URLs”](#).

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](#)
- [Considerações SCIM](#)
- [Etapa 1: Habilitar provisionamento no IAM Identity Center](#)
- [Etapa 2: Configure o provisionamento no CyberArk](#)
- [\(Opcional\) Etapa 3: Configure os atributos do usuário CyberArk para controle de acesso \(ABAC\) no IAM Identity Center](#)
- [\(Opcional\) Passar atributos para controle de acesso](#)

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 de Provisionamento automático de entrada, copie o endpoint e o token de acesso SCIM. Você precisará colá-los posteriormente ao configurar o provisionamento no IdP.
 - a. Endpoint SCIM - Por exemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Token de acesso: escolha Mostrar token para copiar o valor.

Warning

Esse é a única vez que você pode obter o endpoint e o token de acesso SCIM. Certifique-se de copiar esses valores antes de prosseguir. Você inserirá esses valores para configurar provisionamento automático em seu IdP mais adiante neste tutorial.

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.
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,

you create a set of permissions in the IAM Identity Center to manage access based on the attributes of which you passed from CyberArk.

Before starting this procedure, you must first enable the attribute [Attributes for access control](#). For more information about how to do this, consult [Enable and configure attributes for access control](#).

To configure attributes of the user in CyberArk for access control in the IAM Identity Center

1. Open the IAM Identity Center application of CyberArk that you installed as part of the configuration of SAML for CyberArk (Applications > Application Web).
2. Access the option Response SAML.
3. In Attributes, add the relevant attributes to the table following the logic below:
 - a. The name of the attribute is the name of the original attribute of CyberArk.
 - b. The value of the attribute is the name of the attribute sent in the SAML declaration for the IAM Identity Center.
4. Choose Save.

(Optional) Pass attributes for access control

Optionally, you can use the attribute [Attributes for access control](#) in the IAM Identity Center to pass an element `Attribute` with the attribute `Name` defined as `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. This element allows you to pass attributes as session tags in the SAML declaration. For more information about session tags, consult [Pass session tags AWS STS](#) in the IAM user guide.

To pass attributes as session tags, include the element `AttributeValue` that specifies the value of the tag. For example, to pass the key-value pair of tag `CostCenter = blue`, use the attribute as follows.

```
<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 Google Workspace no IAM Identity Center para dar a eles acesso aos AWS recursos. Você pode conseguir essa integração alterando sua fonte de identidades do IAM Identity Center, da fonte de identidades padrão do IAM Identity Center para o Google Workspace.

Note

Google Workspace atualmente não oferece suporte ao SAML Multiple Assertion Consumer Service (ACS) URLs no aplicativo. Centro de Identidade do AWS IAM Esse recurso SAML é necessário para aproveitar totalmente o [suporte multirregional](#) no IAM Identity Center. Se você planeja replicar o IAM Identity Center para regiões adicionais, saiba que o uso de uma única URL do ACS pode afetar a experiência do usuário nessas regiões adicionais. Sua região principal continuará funcionando normalmente. Recomendamos que você trabalhe com seu fornecedor de IdP para ativar esse recurso. Para obter mais informações sobre a experiência do usuário em regiões adicionais com um único URL ACS, consulte [the section called “Usando aplicativos AWS gerenciados sem vários ACS URLs”](#) e [the section called “Conta da AWS resiliência de acesso sem vários ACS URLs”](#)

As informações do usuário do Google Workspace são sincronizadas no IAM Identity Center usando o protocolo [System for Cross-domain Identity Management \(SCIM\) 2.0](#). Para obter mais informações, consulte [Uso de federação de identidades SAML e SCIM com provedores de identidade externos](#).

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 identidade e conectá-lo ao 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. Estruturas de diretórios, como grupos e unidades organizacionais, não estão incluídas neste tutorial. Depois de concluir este tutorial, seus usuários poderão acessar o portal de AWS acesso com suas Google Workspace credenciais.

Note

Para se cadastrar e fazer um teste gratuito do Google Workspace, visite [Google Workspace](#) no site do Google's.

Se você ainda não habilitou o IAM Identity Center, consulte [Habilitar o IAM Identity Center](#).

Considerações

- Antes de configurar o provisionamento SCIM entre o Google Workspace e o IAM Identity Center, é recomendável que você revise as [Considerações sobre o uso do provisionamento automático](#).
- Atualmente, a sincronização automática SCIM do Google Workspace está limitada ao provisionamento de usuários. O aprovisionamento automático de grupos não é possível no momento. Os grupos podem ser criados manualmente com o comando [create-group](#) do AWS CLI Identity Store ou a API AWS Identity and Access Management (IAM). [CreateGroup](#) Como alternativa, você pode usar [ssosync](#) para sincronizar os usuários e grupos do Google Workspace 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. Haverá falha na sincronização de usuários com vários valores. 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 já houver algum usuário no diretório do Identity Center com o mesmo nome de usuário e e-mail, ele será substituído e sincronizado usando o SCIM do Google Workspace.
- Há considerações adicionais ao alterar a fonte de identidades. Para obter mais informações, consulte [the section called “Mudar do IAM Identity Center para um IdP externo”](#).

Etapa 1: Google Workspace: configurar a aplicação SAML

1. Faça login no console do administrador do Google usando uma conta com privilégios de superadministrador.
2. No painel de navegação esquerdo do console do administrador do Google, expanda Aplicações e escolha Aplicações Web e móveis.
3. Na lista suspensa Adicionar aplicação, selecione Pesquisar aplicações.
4. Na caixa de pesquisa, insira Amazon Web Services e selecione a aplicação Amazon Web Services (SAML) na lista.
5. Na página Detalhes do provedor de identidades do Google - Amazon Web Services, você pode fazer uma das seguintes alternativas:
 - a. Baixe os metadados do IdP.
 - b. Copie o URL do SSO, o URL do ID da entidade e as informações de certificado.

Você precisará do arquivo XML ou das informações de URL da etapa 2.

6. Antes de passar para a próxima etapa no console de administração do Google, deixe essa página aberta e vá para o console do IAM Identity Center.

Etapa 2: IAM Identity Center e Google Workspace: alterar a fonte de identidades do IAM Identity Center e configurar o Google Workspace como um provedor de identidades SAML

1. Faça login no [console do IAM Identity Center](#) usando um perfil com permissões de administrador.
2. Escolha Configurações no painel de navegação à esquerda.

3. Na página Configurações, escolha Ações e depois Alterar fonte de identidades.
 - Se ainda não habilitou o IAM Identity Center, consulte [Habilitar o IAM Identity Center](#) para obter mais informações. Depois de habilitar e acessar o IAM Identity Center pela primeira vez, você chegará ao painel onde poderá selecionar Escolher a fonte de identidades.
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 essa página e a página Google Workspace na etapa 1, você precisará fazer o seguinte:
 - Na seção Metadados do provedor de identidades do console do IAM Identity Center, você precisará fazer uma das seguintes alternativas:
 - i. Faça o upload dos metadados SAML do Google como os metadados SAML do IdP no console do IAM Identity Center.
 - ii. Copie e cole o URL do SSO do Google no campo URL de login do IdP, o URL do emissor do Google no campo URL do emissor do IdP e carregue o certificado do Google como o certificado do IdP.
6. Depois de fornecer os metadados do Google na seção Metadados do provedor de identidades do console do IAM Identity Center, copie o URL do Assertion Consumer Service (ACS) do IAM Identity Center e o URL do emissor do IAM Identity Center. Você precisará fornecê-los URLs no Google Admin Console na próxima etapa.
7. Deixe a página aberta no console do IAM Identity Center e volte para o console do administrador do Google. Você deve estar na página Amazon Web Services: detalhes do provedor de serviços. Selecione Continuar.
8. Na página Detalhes do provedor de serviços, insira os valores URL do ACS e ID da entidade. Você copiou esses valores na etapa anterior e eles podem ser encontrados no console do IAM Identity Center.
 - Cole o URL do Assertion Consumer Service (ACS) do IAM Identity Center no campo URL do ACS
 - Cole o URL do emissor do IAM Identity Center no campo ID da entidade.
9. Na página Detalhes do provedor de serviços, preencha os campos em ID do nome como se segue:
 - 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 do Google Directory:
 - Para o atributo da aplicação `https://aws.amazon.com/SAML/Attributes/RoleSessionName`, selecione o campo Informações básicas, e-mail principal dos Atributos do Google Directory.
 - Para o atributo da aplicação do `https://aws.amazon.com/SAML/Attributes/Role`, selecione quaisquer atributos do Google Directory. Um atributo do Google Directory poderia 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 insira ACEITAR no espaço fornecido. Escolha Alterar origem de identidade.

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

Etapa 3: Google Workspace: habilitar as aplicações

1. Retorne ao GoogleAdmin Console e ao seu Centro de Identidade do AWS IAM aplicativo, que podem ser encontrados em Aplicativos e Aplicativos Web e Móveis.
2. No painel Acesso de usuários, ao lado de Acesso dos usuários, escolha a seta para baixo para expandir Acesso dos usuários para 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 de privilégio mínimo, recomendamos que, após concluir este tutorial, você altere o Status do serviço para DESATIVADO para todos. O serviço deve ser habilitado apenas para os usuários que precisam acessar o AWS. 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 vai inserir esses valores para configurar o provisionamento no Google Workspace.
 - a. Endpoint SCIM - Por exemplo,
 - IPv4 `https://scim.Region.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - Pilha dupla `https://scim.Region.api.aws/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. Token de acesso: escolha Mostrar token para copiar o valor.

Warning

Esse é a única vez que você pode obter o endpoint e o token de acesso 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 vai configurar o provisionamento automático do Google Workspace.

Etapa 5: Google Workspace: configurar o provisionamento automático

1. Volte ao console de administrador do Google e à aplicação Centro de Identidade do AWS IAM que podem ser encontrados em Aplicações e Aplicações Web e móveis. Na seção Provisionamento automático, escolha Configurar provisionamento automático.

2. No procedimento anterior, você copiou o valor de 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 de Endpoint SCIM no console do IAM Identity Center. Cole esse valor no campo URL do endpoint 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 do provisionamento, você pode escolher um grupo com o seu diretório do Google Workspace para fornecer acesso à aplicação Amazon Web Services. Pule esta etapa e selecione Continuar.
5. Na seção Desprovisionamento, você pode escolher como responder aos 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
 - após 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 no diretório do Google Workspace.

 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.

Passagem de atributos para controle de acesso: opcional

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.

Atribuir acesso a Contas da AWS

As etapas a seguir são necessárias apenas para conceder acesso Contas da AWS somente a. Essas etapas não são necessárias para conceder acesso aos AWS aplicativos.

Note

Para concluir essa etapa, você precisará de uma instância de organização do IAM Identity Center. Para obter mais informações, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

Etapa 1: IAM Identity Center: conceder aos usuários do Google Workspace acesso a contas

1. Volte para o 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. 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 SCIM do Google Workspace só é compatível com o provisionamento de usuários. O aprovisionamento automático de grupos não é possível no momento. Você não pode criar grupos para os usuários do Google Workspace usando o Console de gerenciamento da AWS. Depois de provisionar usuários, você pode criar grupos usando o comando [create-group](#) do AWS CLI Identity Store ou a API IAM. [CreateGroup](#)

Etapa 2 Google Workspace: confirmar o acesso Google Workspace dos usuários aos AWS recursos

1. Faça login no Google usando uma conta de usuário de teste. Para saber como adicionar usuários ao Google Workspace, consulte a [documentação do Google Workspace](#).
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. A aplicação Amazon Web Services é exibida.
4. Escolha a aplicação Amazon Web Services. Você está conectado ao portal de AWS acesso 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.
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 Console de gerenciamento da AWS.
7. O usuário fez login no console.

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 [CreateGroup](#) para 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.

Solução de problemas

Para solucionar problemas gerais de SCIM e SAML com o Google Workspace, consulte as seguintes seções:

- [Usuários específicos não conseguem sincronizar com o IAM Identity Center a partir de um provedor SCIM externo](#)

- [Problemas relacionados ao conteúdo das asserções SAML criadas pelo IAM Identity Center](#)
- [Erro de usuário ou grupo duplicado ao provisionar usuários ou grupos com um provedor de identidades externo](#)
- Para solução de problemas do Google Workspace, consulte a [documentação da Google Workspace](#).

Os recursos a seguir podem ajudá-lo a solucionar problemas enquanto você trabalha com AWS:

- [AWS re:Post](#)- Encontre FAQs e vincule outros recursos para ajudá-lo a solucionar problemas.
- [AWS Support](#): obter suporte técnico

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 [Security Assertion Markup Language \(SAML\)](#) 2.0. Para obter mais informações, consulte [Uso de federação de identidades SAML e SCIM com provedores de identidade externos](#).

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](#)
- [Considerações SCIM](#)
- [Etapa 1: Habilitar provisionamento no IAM Identity Center](#)
- [Etapa 2: Configure o provisionamento no JumpCloud](#)
- [\(Opcional\) Etapa 3: configure atributos do usuário no JumpCloud para controle de acesso no IAM Identity Center](#)
- [\(Opcional\) Passar atributos para controle de acesso](#)

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](#).
- Se você replicou o IAM Identity Center para regiões adicionais, você deve atualizar a configuração do seu provedor de identidade para permitir o acesso a aplicativos AWS gerenciados e a Contas da AWS partir dessas regiões. Consulte mais detalhes em [the section called “Etapa 3: atualizar a configuração do IdP externo”](#). Consulte a JumpCloud documentação para obter detalhes adicionais.
- 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 conector de login AWS único 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.

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 de Provisionamento automático de entrada, copie o endpoint e o token de acesso SCIM. Você precisará colá-los posteriormente ao configurar o provisionamento no IdP.
 - a. Endpoint SCIM - Por exemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Token de acesso: escolha Mostrar token para copiar o valor.

 Warning

Esse é a única vez que você pode obter o endpoint e o token de acesso SCIM. Certifique-se de copiar esses valores antes de prosseguir. Você inserirá esses valores para configurar provisionamento automático em seu IdP mais adiante neste tutorial.

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.
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 JumpCloud caso você opte por configurar atributos para o IAM Identity Center gerenciar o acesso aos seus AWS recursos. 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

Centro de Identidade do AWS IAM oferece suporte à integração com a [Security Assertion Markup Language \(SAML\) 2.0](#), bem como ao [provisionamento automático](#) (sincronização) de informações de usuários e grupos Microsoft Entra ID (anteriormente 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](#). Para obter mais informações, consulte [Uso de federação de identidades SAML e SCIM com provedores de identidade externos](#).

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 [Guia de início rápido: configurar um locatário](#) na documentação da Microsoft.
- Uma conta Centro de Identidade do AWS IAM ativada. Para obter mais informações, consulte [O que é o Centro de Identidade do IAM?](#) no Guia do usuário do Centro de Identidade do AWS IAM .

Considerações

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.

Provisionamento automático

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 em políticas de permissão que determinam quem em sua fonte de identidade pode acessar seus AWS recursos. 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. Ou então, você pode usar a [Sincronização do AD configurável do IAM Identity Center](#) para integrar grupos do Active Directory com o IAM Identity Center.

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 dos Grupos A, B, C
5. Grupo L com uma regra para incluir membros do Grupos 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.

Etapa 1: preparar o locatário da Microsoft

Nesta etapa, você explicará como instalar e configurar seu aplicativo Centro de Identidade do AWS IAM corporativo e atribuir acesso a um usuário de Microsoft Entra ID teste recém-criado.

Step 1.1 >

Etapa 1.1: Configurar o aplicativo Centro de Identidade do AWS IAM corporativo no Microsoft Entra ID

Neste procedimento, você instala o aplicativo Centro de Identidade do AWS IAM corporativo em Microsoft Entra ID. Posteriormente, você precisará desse aplicativo para configurar sua conexão SAML com 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 **Centro de Identidade do AWS IAM** na caixa de pesquisa.
4. Selecione Centro de Identidade do AWS IAM nos resultados.
5. Escolha 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@*example.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: Teste a experiência de Nikki antes de atribuir suas permissões a Centro de Identidade do AWS IAM

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 a página de login do [portal Minha conta](#) e insira o endereço de e-mail completo de Nikki. Por exemplo, NikkiWolf@*example.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 o prompt 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 Centro de Identidade do AWS IAM 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 Centro de Identidade do AWS IAM.

1. No console do [Centro de administração do Microsoft Entra](#), navegue até Identidade > Aplicações > Aplicações empresariais e escolha Centro de Identidade do AWS IAM 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 e NikkiWolf, em seguida, escolha Selecionar.
6. Na página Adicionar tarefa, escolha Atribuir. NikkiWolf agora aparece na lista de usuários atribuídos ao Centro de Identidade do AWS IAM aplicativo.

Etapa 2: Prepare sua AWS conta

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 RegionalAdmin permissões no IAM Identity Center

Esse conjunto de permissões será usado para conceder à Nikki as permissões de AWS conta necessárias para gerenciar regiões na página Conta no Console de gerenciamento da AWS. 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 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 ser RegionalAdmin exibido na lista de conjuntos de permissões.

Step 2.2 >

Etapa 2.2: Criar um NikkiWolf usuário 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 IAM Identity Center](#).
2. Escolha Usuários, depois Adicionar usuário e forneça as seguintes informações:
 - a. Para nome de usuário e endereço de e-mail — insira o mesmo **NikkiWolf@*yourcompanydomain.extension*** que você usou ao criar seu Microsoft Entra ID usuário. Por exemplo, NikkiWolf@*example.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 RegionalAdmin permissões em IAM Identity Center

Aqui você localiza a região Conta da AWS na qual Nikki administrará as regiões e, em seguida, atribuirá as permissões necessárias para que ela acesse com sucesso o portal de AWS acesso.

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*) na qual você deseja conceder à Nikki acesso para gerenciar regiões e, em seguida, 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.
- 5.

Example

<caption>On the Selecionar conjuntos de permissões page, choose the RegionalAdmin permission set created in Step 2.1, and then choose Próximo.</caption>

6. Na página Revisar e enviar, revise as seleções e escolha Enviar.

Etapa 3: configurar e testar a conexão SAML

Nesta etapa, você configura sua conexão SAML usando o aplicativo Centro de Identidade do AWS IAM corporativo 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 de alteração da fonte de identidade no console do IAM Identity Center e recuperará o arquivo de metadados e o URL de login AWS específico que você precisará inserir ao configurar a conexão na próxima etapa. Microsoft Entra ID

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 identidade externo, em Metadados do provedor de serviços, escolha Padrão IPv4 ou Dual-stack. Você pode baixar o arquivo de metadados do provedor de serviços depois de concluir a alteração da fonte de identidade.
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 vá para a próxima etapa (**Step 3.2**) para configurar a aplicação Centro de Identidade do AWS IAM corporativa em Microsoft Entra ID. Posteriormente, você retornará a essa página para concluir o processo.

Step 3.2 >

Etapa 3.2: Configurar o aplicativo Centro de Identidade do AWS IAM corporativo 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 login 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 Centro de Identidade do AWS IAM.
2. No painel esquerdo, selecione 2. Configurar autorização única.
3. Na página Configurar autenticação única com SAML, escolha SAML. Na página 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 do Identificador e do URL de Resposta (URL do Assertion Consumer Service) agora apontam para os endpoints em AWS
 - Identificador - Esse é o URL do emissor do IAM Identity Center. O mesmo valor se aplica independentemente de você usar endpoints IPv4 -only ou dual-stack.
 - URL de resposta (URL do Assertion Consumer Service) - Os valores aqui incluem endpoints IPv4 somente e de pilha dupla de todas as regiões habilitadas do seu IAM Identity Center. Você pode usar o URL do ACS da região primária como padrão para que os usuários sejam redirecionados para a região primária ao iniciarem o aplicativo Amazon Web Services a partir de. Microsoft Entra ID Para obter mais informações sobre o ACS URLs, consulte [Endpoints ACS no primário e adicional Regiões da AWS](#).
 - (Opcional) Se você replicou o IAM Identity Center para regiões adicionais, você também pode criar um aplicativo de favoritos Microsoft Entra ID para o portal de AWS acesso em cada região adicional. Isso permite que seus usuários acessem o portal de AWS acesso em regiões adicionais a partir de Microsoft Entra ID. Certifique-se de conceder aos seus usuários permissões para acessar os aplicativos de favoritos em Microsoft Entra ID. Consulte a [Microsoft Entra ID documentação](#) para obter mais detalhes. Se você planeja replicar o IAM Identity Center para outras regiões posteriormente, visite [Microsoft Entra ID configuração para acesso a regiões adicionais](#) para obter orientação sobre como habilitar o acesso às regiões adicionais após essa configuração inicial.
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 login único com Centro de Identidade do AWS IAM, escolha Não, vou testar mais tarde. Você fará essa verificação em uma etapa posterior.
7. Na página Configurar login único com SAML, na seção Certificados SAML, ao lado de XML dos metadados da federação, escolha Baixar para salvar o arquivo de metadados no 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 Centro de Identidade do AWS IAM

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 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 de autenticado, você selecionará o Centro de Identidade do AWS IAM aplicativo que redirecionará Nikki para o AWS portal de acesso.

1. Vá até página de login do [portal Minha conta](#) e insira o endereço de e-mail completo de Nikki. Por exemplo, **NikkiWolf@example.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 Centro de Identidade do AWS IAM. Deve ser solicitado que você faça uma autenticação adicional.

5. Na página de login da Microsoft, escolha suas NikkiWolf credenciais. Se a autenticação for solicitada pela segunda vez, escolha suas NikkiWolf credenciais novamente. Isso deve redirecioná-lo automaticamente para o portal de AWS acesso.

 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 sua Contas da AWS tela.

 Tip

Se a página estiver vazia e sem Contas da AWS exibição, confirme se Nikki foi atribuída com sucesso ao conjunto de RegionalAdminpermissões (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 deve ter apenas privilégios de administrador suficientes para gerenciar regiões na página Contas.

1. No portal de AWS acesso, escolha a guia Contas para exibir a lista de contas. Os nomes das contas IDs, contas e endereços de e-mail associados a todas as 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. Em seguida, RegionalAdmin escolha Console de gerenciamento para assumir a função que você definiu no conjunto de RegionalAdminpermissões. Isso redirecionará você para a página inicial do Console de gerenciamento da AWS .
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@*example.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,

- IPv4: `https://scim.aws-region.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
- Pilha dupla: `https://scim.aws-region.api.aws/1111111111-2222-3333-4444-555555555555/scim/v2`

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

 Warning

Esse é a única vez que você pode obter o endpoint e o token de acesso SCIM. Certifique-se de copiar esses valores antes de prosseguir.

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 seu usuário de RichRoe teste instalado e habilitou o SCIM no IAM Identity Center, você pode continuar com a configuração das configurações de sincronização do SCIM em. Microsoft Entra ID

1. No console do [Centro de administração do Microsoft Entra](#), navegue até Identidade > Aplicações > Aplicações empresariais e escolha Centro de Identidade do AWS IAM.
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 4.2**. 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 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 e RichRoe, em seguida, 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 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 seu RichRoeusuário exibido. Observe que na coluna Criado por, o valor está definido como SCIM.
3. Escolha RichRoe, em Perfil, verificar se os atributos a seguir foram copiados deMicrosoft 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 RichRoeao conjunto de **RegionalAdmin** permissões usado anteriormente para conceder a Nikki as permissões para gerenciar regiões (consulte **Step 2.3**) e depois testar seu nível de acesso usando **Step 3.5**.

Parabéns!

Você configurou com êxito uma conexão SAML entre a Microsoft AWS e verificou que o provisionamento automático está funcionando para manter tudo sincronizado. Agora

you can apply what you learned to configure your production environment with more ease.

Etapa 5: configurar ABAC: opcional

Now that you configured SAML and SCIM successfully, you can opt to configure access control by attribute (ABAC). ABAC is an authorization strategy that defines permissions based on attributes.

With Microsoft Entra ID, you can use either of the two methods below to configure ABAC for use with IAM Identity Center.

Configure user attributes in Microsoft Entra ID for access control in IAM Identity Center

Configurar atributos do usuário no Microsoft Entra ID para controle de acesso no IAM Identity Center

In the procedure below, you will determine which Microsoft Entra ID attributes should be used by IAM Identity Center to manage access to your AWS resources. After you define them, Microsoft Entra ID will send these attributes to IAM Identity Center via SAML assertions. Next, you will need to access [Create a set of permissions](#) in IAM Identity Center to manage access based on the attributes you passed from Microsoft Entra ID.

Before starting this procedure, you must first enable the attribute [Attributes for access control](#). For more information about how to do this, consult [Enable and configure attributes for access control](#).

1. In the console of [Microsoft Entra admin center](#), navigate to Identity > Applications > Enterprise applications and choose Centro de Identidade do AWS IAM.
2. Choose Logon único.
3. In the Attributes and declarations section, choose Edit.
4. In the Attributes and declarations page, do the following:
 - a. Choose Add new claim.
 - b. In Name, enter `AccessControl:Attribute`. Replace `Attribute` with the name of the attribute you expect in IAM Identity Center. For example, `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.

Configure ABAC using IAM Identity Center

Configurar 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 `Department=billing`, use o seguinte atributo:

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

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

Atribuir acesso a Contas da AWS

As etapas a seguir são necessárias apenas para conceder acesso Contas da AWS somente a. Essas etapas não são necessárias para conceder acesso aos AWS aplicativos.

 Note

Para concluir essa etapa, você precisará de uma instância de organização do IAM Identity Center. Para obter mais informações, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

Etapa 1: IAM Identity Center: conceder aos usuários do Microsoft Entra ID acesso a contas

1. Volte para o 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. 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.

Etapa 2 Microsoft Entra ID: confirmar o acesso Microsoft Entra ID dos usuários aos AWS recursos

1. Volte ao console Microsoft Entra ID e navegue até a aplicação de login baseada em SAML do IAM Identity Center.
 2. Selecione Usuários e grupos e selecione Adicionar usuários ou grupos. Você adicionará o usuário que criou neste tutorial na Etapa 4 à aplicação Microsoft Entra ID. Ao adicionar o usuário, você permitirá que ele faça login na AWS. Procure o usuário que você criou na Etapa 4. Se você seguiu esta etapa, seria **RichardRoe**.
- Para uma demonstração, consulte [Federar a instância existente do IAM Identity Center com o Microsoft Entra ID](#)

Microsoft Entra ID configuração para acesso a regiões adicionais do IAM Identity Center - opcional

Se você replicou o IAM Identity Center para regiões adicionais, você deve atualizar a configuração do seu provedor de identidade para permitir o acesso aos aplicativos AWS gerenciados e Contas da AWS por meio das regiões adicionais. As etapas abaixo orientam você pelo procedimento. Para obter mais detalhes sobre esse tópico, incluindo os pré-requisitos, consulte [Usando o IAM Identity Center em várias Regiões da AWS](#)

1. Recupere o ACS URLs para as regiões adicionais do console do IAM Identity Center, conforme descrito em [Endpoints ACS no primário e adicional Regiões da AWS](#)
2. No console do [Centro de administração do Microsoft Entra](#), navegue até Identidade > Aplicações > Aplicações empresariais e escolha Centro de Identidade do AWS IAM.
3. No painel esquerdo, selecione 2. Configurar autorização única.
4. Na página Configuração básica do SAML, na seção URL de resposta (URL do Assertion Consumer Service), escolha Adicionar URL de resposta para cada URL ACS adicional da região. Você pode manter o URL do ACS da região primária como padrão para que os usuários continuem sendo redirecionados para a região primária ao iniciarem o Centro de Identidade do AWS IAM aplicativo. Microsoft Entra ID
5. Quando terminar de adicionar o ACS URLs, salve o Centro de Identidade do AWS IAM aplicativo.
6. Você pode criar um aplicativo de favoritos Microsoft Entra ID para o portal de AWS acesso em cada região adicional. Isso permite que seus usuários acessem o portal de AWS acesso em regiões adicionais a partir de Microsoft Entra ID. Certifique-se de conceder aos seus usuários permissões para acessar os aplicativos de favoritos em Microsoft Entra ID. Consulte a [Microsoft Entra ID documentação](#) para obter mais detalhes.
7. Verifique se você pode entrar no portal de AWS acesso em cada região adicional. Navegue até o [portal de AWS acesso URLs](#) ou inicie os aplicativos de Microsoft Entra ID favoritos em.

Solução de problemas

Para solucionar problemas gerais de SCIM e SAML com o Microsoft Entra ID, consulte as seguintes seções:

- [Problemas de sincronização com o Microsoft Entra ID e o IAM Identity Center](#)

- [Usuários específicos não conseguem sincronizar com o IAM Identity Center a partir de um provedor SCIM externo](#)
- [Problemas relacionados ao conteúdo das asserções SAML criadas pelo IAM Identity Center](#)
- [Erro de usuário ou grupo duplicado ao provisionar usuários ou grupos com um provedor de identidades externo](#)
- [Recursos adicionais do](#)

Problemas de sincronização com o Microsoft Entra ID e o IAM Identity Center

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 AWS CloudTrail o evento falhou. Isso pode ser feito pesquisando no console do Histórico de Eventos ou CloudTrail usando o seguinte filtro:

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

O erro no CloudTrail evento 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 é revisar os atributos do usuário no Microsoft Entra ID, garantindo que nenhum deles 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](#).

Sincronização da conta de convidado do Microsoft Entra ID

Se você quiser sincronizar os usuários convidados do Microsoft Entra ID com o IAM Identity Center, consulte o procedimento a seguir.

O e-mail dos usuários convidados do Microsoft Entra ID é diferente do de outros usuários do Microsoft Entra ID. Essa diferença causa problemas ao tentar sincronizar usuários convidados do Microsoft Entra ID com o IAM Identity Center. Por exemplo, veja o seguinte endereço de e-mail de um usuário convidado:

`exampleuser_domain.com#EXT#@domain.onmicrosoft.com.`

O IAM Identity Center não espera que o endereço de e-mail contenha o `#EXT#@domain` formato.

1. Faça login no console do [Centro de administração do Microsoft Entra](#), navegue até Identidade > Aplicativos > Aplicativos empresariais e escolha Centro de Identidade do AWS IAM
2. Navegue até a guia Autenticação única no painel esquerdo.
3. Selecione Editar, que aparece ao lado de Atributos e declarações do usuário.
4. Selecione Identificador exclusivo do usuário (ID do nome) após Declarações obrigatórias.
5. Você criará duas condições de declaração para usuários e usuários convidados do Microsoft Entra ID:
 - a. Para usuários do Microsoft Entra ID, crie um tipo de usuário para membros com o atributo de origem definido como `user.userprincipalname`.
 - b. Para usuários convidados do Microsoft Entra ID, crie um tipo de usuário para convidados externos com o atributo de origem definido como `user.mail`.
 - c. Selecione Salvar e tente fazer login novamente como usuário convidado do Microsoft Entra ID.

Recursos adicionais do

- Para obter dicas de solução de problemas em geral, consulte [Solução de problemas do IAM Identity Center](#).
- Para solução de problemas do Microsoft Entra ID, consulte a [documentação da Microsoft](#).
- Para saber mais sobre a federação entre várias Contas da AWS, consulte [Protegendo Contas da AWS com Azure Active Directory Federation](#).

Os recursos a seguir podem ajudá-lo a solucionar problemas enquanto você trabalha com AWS:

- [AWS re:Post](#)- Encontre FAQs e vincule outros recursos para ajudá-lo a solucionar problemas.
- [AWS Support](#): obter suporte técnico

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

Você pode provisionar ou sincronizar informações de usuários e grupos do Okta para o IAM Identity Center automaticamente usando o protocolo [System for Cross-domain Identity Management \(SCIM\) 2.0](#). Para obter mais informações, consulte [Uso de federação de identidades SAML e SCIM com provedores de identidade externos](#).

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 compara os atributos de usuário esperados entre o IAM Identity Center e a sua conta da 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 à aplicação 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.

- Importar usuários — Os usuários podem ser importados do IAM Identity Center para Okta o.

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.

Os seguintes recursos são compatíveis ao se conectar Okta ao IAM Identity Center por meio do SAML:

- Login SAML iniciado pelo IdP — Os usuários fazem login por meio do Okta portal e obtêm acesso ao IAM Identity Center.
- Login SAML iniciado pelo SP — Os usuários acessam o portal de AWS acesso, que os redireciona para entrar pelo portal. Okta

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.

Se você ainda não habilitou o IAM Identity Center, consulte [Habilitar o IAM Identity Center](#).

Considerações

- Antes de configurar o provisionamento SCIM entre o Okta e o IAM Identity Center, é recomendável que você revise as [Considerações sobre o uso do provisionamento automático](#).
- 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. Haverá falha na sincronização de usuários com vários valores. 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.

- Ao usar o Okta com o IAM Identity Center, IAM Identity Center geralmente é configurado como uma aplicação no Okta. Isso permite que você configure várias instâncias do IAM Identity Center como várias aplicações, permitindo acesso a várias organizações da AWS em uma única instância do Okta.
- 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.
- Se você replicou o IAM Identity Center para regiões adicionais, você deve atualizar a configuração do seu provedor de identidade para permitir o acesso a aplicativos AWS gerenciados e Contas da AWS por meio de regiões adicionais. Para obter mais detalhes, incluindo os pré-requisitos, consulte [Usando o IAM Identity Center em várias Regiões da AWS](#). As etapas específicas do Okta são descritas em [Oktaconfiguração para acesso a regiões adicionais](#)

Etapa 1: Okta: obter os metadados SAML da sua conta da 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 Centro de Identidade do AWS IAM, 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, pois você continuará usando esse console em etapas posteriores.

Etapa 2: IAM Identity Center: 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, copie os seguintes itens em um arquivo de texto para facilitar o acesso:
 - URL do IAM Identity Center Assertion Consumer Service (ACS) — Você pode escolher entre ACS IPv4 somente e ACS de pilha dupla. URLs Além disso, se sua instância do IAM Identity Center estiver habilitada em várias regiões, cada região adicional terá seu próprio IPv4 ACS de pilha dupla e somente. URLs Para obter mais informações sobre o ACS URLs, consulte [Endpoints ACS no primário e adicional Regiões da AWS](#).
 - URL do emissor do IAM Identity Center

Você vai precisar desses valores mais adiante neste tutorial.

- b. Em Metadados do provedor de identidades, em Metadados do IdP SAML, selecione Escolher arquivo e selecione o arquivo metadata.xml que você criou no procedimento 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 Okta admin dashboard e selecione a guia Entrar do Centro de Identidade do AWS IAM aplicativo e, em seguida, selecione Editar.
9. Em Configurações avançadas de login, insira o seguinte:
 - Para o URL do ACS, insira os valores que você copiou para o URL do IAM Identity Center Assertion Consumer Service (ACS). Você pode usar o URL do ACS da região primária como

padrão para que os usuários sejam redirecionados para a região primária ao iniciarem o aplicativo Amazon Web Services a partir de. Okta

- (Opcional) Se você replicou o IAM Identity Center para regiões adicionais, você também pode criar um aplicativo de favoritos Okta para o portal de AWS acesso em cada região adicional. Isso permite que seus usuários acessem o portal de AWS acesso em regiões adicionais a partir de Okta. Certifique-se de conceder aos seus usuários permissões para acessar os aplicativos de favoritos em Okta. Consulte a [Okta documentação](#) para obter mais detalhes. Se você planeja replicar o IAM Identity Center para outras regiões posteriormente, visite [Okta configuração para acesso a regiões adicionais](#) para obter orientação sobre como habilitar o acesso às regiões adicionais após essa configuração inicial.
- Em URL do emissor, insira o valor que você copiou para URL do emissor do IAM Identity Center
- Em Formato de nome de usuário da aplicação, selecione uma das opções do menu.

Certifique-se de que o valor escolhido seja exclusivo de 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 o Okta admin dashboard aberto e volte para o console do IAM Identity Center para o realizar a próxima etapa.

Etapa 3: IAM Identity Center e Okta: 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:
 - a. Endpoint SCIM - O formato do endpoint depende da sua configuração:
 - IPv4: `https://scim.us-east-2.amazonaws.com/scim/v21111111111-2222-3333-4444-555555555555`

- Pilha dupla: `https://scim.us-east-2.api.aws/ /scim/v2`
`1111111111-2222-3333-4444-5555555555`

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

 Warning

Esse é a única vez que você pode obter o endpoint e o token de acesso SCIM. Certifique-se de copiar esses valores antes de prosseguir. Você inserirá esses valores para configurar o provisionamento automático no Okta mais adiante neste tutorial.

3. Escolha Fechar.
4. Volte para o Okta admin dashboard e navegue até a aplicação IAM Identity Center.
5. Na página Aplicação do IAM Identity Center, escolha a guia Provisionamento e, no painel de navegação esquerdo, em Configurações, escolha Integração.
6. Escolha Editar e marque a caixa de seleção ao lado de Habilitar integração de API para habilitar o provisionamento automático.
7. Configure Okta com os valores de provisionamento do SCIM Centro de Identidade do AWS IAM que você copiou anteriormente nesta etapa:
 - a. No campo URL da base, insira o valor do Endpoint SCIM.
 - 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 Centro de Identidade do AWS IAM foi verificado com sucesso! é exibida.
9. Escolha Salvar. Você é levado para a seção Configurações, com a opção Integração selecionada.
10. Em Configurações, escolha Para aplicação e marque a caixa de seleção Habilitar para cada um dos atributos de Provisionamento para aplicação que você deseja habilitar. 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: Okta: 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 provisionamento provisionam os usuários que são membros do grupo. Conclua as etapas a seguir para sincronizar grupos e usuários com Centro de Identidade do AWS IAM.

1. Na página Aplicação do IAM Identity Center do Okta, 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 você deseja sincronizar com o 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. Para adicionar usuários individuais do Okta ao IAM Identity Center, use as seguintes etapas:

- a. Na página Atribuições, escolha Atribuir e, em seguida, escolha Atribuir a pessoas.
- b. 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 Centro de Identidade do AWS IAM aplicativo, na página Aplicativos do Okta 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.

5. 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.

Passagem de atributos para controle de acesso: opcional

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.

Atribuir acesso a Contas da AWS

As etapas a seguir são necessárias apenas para conceder acesso Contas da AWS somente a. Essas etapas não são necessárias para conceder acesso aos AWS aplicativos.

Note

Para concluir essa etapa, você precisará de uma instância de organização do IAM Identity Center. Para obter mais informações, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

Etapa 1: IAM Identity Center: 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. 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 sub-etapas da 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, é exibida 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. Na 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 reprovionada e que o conjunto de permissões atualizado foi aplicado. Quando o usuário fizer login, ele terá a opção de escolher a `AdministratorAccess` função.

Etapa 2Okta: confirmar o acesso Okta dos usuários aos AWS recursos

1. Faça login usando uma conta de teste no Okta dashboard.
2. Em Minhas aplicações, selecione o ícone do Centro de Identidade do AWS IAM.

3. Você deve 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 o acesso tanto ao acesso programático Console de gerenciamento da AWS quanto ao acesso programático. Selecione Console de gerenciamento para abrir o Console de gerenciamento da AWS.
6. O usuário faz login no Console de gerenciamento da AWS.

Você também pode usar o portal de AWS acesso. Isso redireciona você para entrar pelo Okta portal antes de levá-lo ao portal de AWS acesso. Esse caminho segue o fluxo de login do SAML iniciado pelo SP.

Oktaconfiguração para acesso a regiões adicionais do IAM Identity Center - opcional

Se você replicou o IAM Identity Center para regiões adicionais, você deve atualizar a configuração do seu provedor de identidade para permitir o acesso aos aplicativos AWS gerenciados e Contas da AWS por meio das regiões adicionais. As etapas abaixo orientam você pelo procedimento. Para obter mais detalhes sobre esse tópico, incluindo os pré-requisitos, consulte. [Usando o IAM Identity Center em vários Regiões da AWS](#)

1. Recupere o ACS URLs para as regiões adicionais do console do IAM Identity Center, conforme descrito em. [Endpoints ACS no primário e adicional Regiões da AWS](#)
2. No painel de navegação do painel de Okta administração, escolha Aplicativos e, em seguida, Aplicativos novamente na lista expandida.
3. Escolha o aplicativo do Centro de Identidade do AWS IAM.
4. Escolha a guia Fazer login.
5. Em Configurações avançadas de login e Outro SSO solicitável URLs, escolha Adicionar outro para o URL do ACS de cada região adicional e cole o URL do ACS no campo de texto.
6. Quando terminar de adicionar o ACS URLs, salve o Centro de Identidade do AWS IAMaplicativo.
7. Você pode criar um aplicativo de favoritos Okta para o portal de AWS acesso em cada região adicional. Isso permite que seus usuários acessem o portal de AWS acesso em regiões

adicionais a partir de Okta. Certifique-se de conceder aos seus usuários permissões para acessar os aplicativos de favoritos em Okta. Consulte a [Okta documentação](#) para obter mais detalhes.

8. Verifique se você pode entrar no portal de AWS acesso em cada região adicional. Navegue até o [portal de AWS acesso URLs](#) ou inicie os aplicativos de Okta favoritos em.

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, veja [Atribuir acesso de usuário ou grupo a Contas da AWS](#).
- Conceder acesso a aplicações na nuvem, consulte [Atribuir acesso de usuário às aplicações no console do IAM Identity Center](#).
- Configure as permissões de acordo com as funções, consulte [Criar um conjunto de permissões](#).

Solução de problemas

Para solucionar problemas gerais de SCIM e SAML com o Okta, consulte as seguintes seções:

- [Reprovisionamento de usuários e grupos excluídos do IAM Identity Center](#)
- [Erro de provisionamento automático no Okta](#)
- [Usuários específicos não conseguem sincronizar com o IAM Identity Center a partir de um provedor SCIM externo](#)
- [Problemas relacionados ao conteúdo das asserções SAML criadas pelo IAM Identity Center](#)
- [Erro de usuário ou grupo duplicado ao provisionar usuários ou grupos com um provedor de identidades externo](#)
- [Recursos adicionais do](#)

Reprovisionamento de usuários e grupos excluídos do IAM Identity Center

- Você poderia receber a seguinte mensagem de erro no console do Okta se estivesse tentando alterar um usuário ou grupo do Okta que já foi sincronizado e depois excluído do IAM Identity Center:

- Centro de Identidade do AWS IAM Falha no envio automático do perfil do usuário *Jane Doe* para o aplicativo: Erro ao tentar enviar a atualização do perfil para *jane_doe@example.com*: Nenhum usuário retornou para o usuário *xxxxx-xxxxxx-xxxxx-xxxxxxx*
- O grupo vinculado está ausente em Centro de Identidade do AWS IAM. Altere o grupo vinculado para retomar o envio automático de associações ao grupo.
- Você também poderia receber a seguinte mensagem de erro nos logs de sistemas do Okta para usuários ou grupos do IAM Identity Center sincronizados e excluídos:
 - Erro Okta: eventfailed application.provision.user.push_profile: Nenhum usuário retornou para o usuário *xxxxx-xxxxxx-xxxxx-xxxxxxx*
 - Erro Okta: application.provision.group_push.mapping.update.or.delete.failed.with.error: o grupo vinculado está ausente. Centro de Identidade do AWS IAM Altere o grupo vinculado para retomar o envio automático de associações ao grupo.

Warning

Usuários e grupos devem ser excluídos do Okta em vez do IAM Identity Center se você tiver sincronizado o Okta com o IAM Identity Center usando SCIM.

Solução de problemas de usuários excluídos do IAM Identity Center

Para resolver esse problema de usuários excluídos do IAM Identity Center, os usuários devem ser excluídos do Okta. Se necessário, esses usuários também deveriam ser recriados no Okta. Quando o usuário for recriado no Okta, ele também será reprovisionado no IAM Identity Center por SCIM. Para ter mais informações sobre a exclusão de um usuário, consulte a [documentação do Okta](#).

Note

Se você precisar remover o acesso de um usuário do Okta ao IAM Identity Center, primeiro remova-o do envio automático de grupo e depois do grupo de atribuição no Okta. Isso garante que o usuário seja removido da sua associação ao grupo correspondente no IAM Identity Center. Para obter mais informações sobre solução de problemas de envio automático de grupo, consulte a [documentação do Okta](#).

Solução de problemas de grupos do IAM Identity Center excluídos

Para resolver esse problema de grupos do IAM Identity Center excluídos, os usuários devem ser excluídos do Okta. Se necessário, esses grupos também precisariam ser recriados no Okta usando o envio automático de grupo. Quando o usuário for recriado no Okta, ele também será reprovisionado no IAM Identity Center por SCIM. Para ter mais informações sobre a exclusão de um grupo, consulte a [documentação do Okta](#).

Erro de provisionamento automático no Okta

Se você recebeu um a seguinte mensagem de erro no Okta:

Falha no provisionamento automático da usuária Jane Doe para o aplicativo: usuário correspondente Centro de Identidade do AWS IAM não encontrado

Consulte a [documentação do Okta](#) para obter mais informações.

Recursos adicionais do

- Para obter dicas de solução de problemas em geral, consulte [Solução de problemas do IAM Identity Center](#).

Os recursos a seguir podem ajudá-lo a solucionar problemas enquanto você trabalha com AWS:

- [AWS re:Post](#)- Encontre FAQs e vincule outros recursos para ajudá-lo a solucionar problemas.
- [AWS Support](#): obter suporte técnico

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. Para obter mais informações, consulte [Uso de federação de identidades SAML e SCIM com provedores de identidade externos](#).

Note

OneLogin atualmente não oferece suporte ao SAML Multiple Assertion Consumer Service (ACS) URLs no aplicativo. Centro de Identidade do AWS IAM Esse recurso SAML é necessário para aproveitar totalmente o [suporte multirregional](#) no IAM Identity Center. Se

Se você planeja replicar o IAM Identity Center para regiões adicionais, saiba que o uso de uma única URL do ACS pode afetar a experiência do usuário nessas regiões adicionais. Sua região principal continuará funcionando normalmente. Recomendamos que você trabalhe com seu fornecedor de IdP para ativar esse recurso. Para obter mais informações sobre a experiência do usuário em regiões adicionais com um único URL ACS, consulte [the section called “Usando aplicativos AWS gerenciados sem vários ACS URLs”](#) e [the section called “Conta da AWS resiliência de acesso sem vários ACS URLs”](#).

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](#)
- [Etapa 1: Habilitar provisionamento no IAM Identity Center](#)
- [Etapa 2: Configure o provisionamento no OneLogin](#)
- [\(Opcional\) Etapa 3: configure atributos do usuário no OneLogin para controle de acesso no IAM Identity Center](#)
- [\(Opcional\) Passar atributos para controle de acesso](#)
- [Solução de problemas](#)

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 de Provisionamento automático de entrada, copie o endpoint e o token de acesso SCIM. Você precisará colá-los posteriormente ao configurar o provisionamento no IdP.
 - a. Endpoint SCIM - Por exemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Token de acesso: escolha Mostrar token para copiar o valor.

Warning

Esse é a única vez que você pode obter o endpoint e o token de acesso SCIM. Certifique-se de copiar esses valores antes de prosseguir. Você inserirá esses valores para configurar provisionamento automático em seu IdP mais adiante neste tutorial.

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 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 escolha Configuração no painel de navegação.
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. 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. No painel de navegação, escolha Provisioning (Provisionamento).
6. Marque as caixas de seleção Ativar provisionamento, Criar usuário, Excluir usuário e Atualizar usuário e, em seguida, escolha Salvar.
7. No painel de navegação, escolha Users.
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, and/or 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 OneLogin se você optar por configurar atributos que usará no IAM Identity Center para gerenciar o acesso aos seus AWS recursos. 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 user/group sincronização

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](#)

- [PingOne](#)

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. Para obter mais informações, consulte [Uso de federação de identidades SAML e SCIM com provedores de identidade externos](#).

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](#)
- [Considerações](#)
- [Etapa 1: Habilitar provisionamento no IAM Identity Center](#)
- [Etapa 2: Configure o provisionamento no PingFederate](#)
- [\(Opcional\) Etapa 3: configurar os atributos do usuário em PingFederate para controle de acesso no IAM Identity Center](#)
- [\(Opcional\) Passar atributos para controle de acesso](#)

- [Solução de problemas](#)

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 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.
- Se você replicou o IAM Identity Center para regiões adicionais, você deve atualizar a configuração do seu provedor de identidade para permitir o acesso a aplicativos AWS gerenciados e a Contas da AWS partir dessas regiões. Consulte mais detalhes em [the section called “Etapa 3: atualizar a configuração do IdP externo”](#). Consulte a PingFederate documentação para obter detalhes adicionais.

Considerações

A seguir estão considerações importantes sobre o PingFederate 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 de Provisionamento automático de entrada, copie o endpoint e o token de acesso SCIM. Você precisará colá-los posteriormente ao configurar o provisionamento no IdP.
 - a. Endpoint SCIM - Por exemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Token de acesso: escolha Mostrar token para copiar o valor.

Warning

Esse é a única vez que você pode obter o endpoint e o token de acesso SCIM. Certifique-se de copiar esses valores antes de prosseguir. Você inserirá esses valores para configurar provisionamento automático em seu IdP mais adiante neste tutorial.

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. 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 **AWSIAMIdentityCenterchannel1**) 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 PingFederate para controle de acesso no IAM Identity Center

Esse é um procedimento opcional PingFederate se você optar por configurar atributos que usará no IAM Identity Center para gerenciar o acesso aos seus AWS recursos. 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.

Solução de problemas

Para solucionar problemas gerais de SCIM e SAML com o PingFederate, consulte as seguintes seções:

- [Usuários específicos não conseguem sincronizar com o IAM Identity Center a partir de um provedor SCIM externo](#)
- [Problemas relacionados ao conteúdo das asserções SAML criadas pelo IAM Identity Center](#)
- [Erro de usuário ou grupo duplicado ao provisionar usuários ou grupos com um provedor de identidades externo](#)
- Para obter mais informações sobre o PingFederate, consulte a [documentação do PingFederate](#).

Os recursos a seguir podem ajudá-lo a solucionar problemas enquanto você trabalha com AWS:

- [AWS re:Post](#)- Encontre FAQs e vincule outros recursos para ajudá-lo a solucionar problemas.
- [AWS Support](#): obter suporte técnico

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.

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](#)
- [Considerações](#)
- [Etapa 1: Habilitar provisionamento no IAM Identity Center](#)
- [Etapa 2: Configure o provisionamento no PingOne](#)
- [\(Opcional\) Etapa 3: configure atributos do usuário no PingOne para controle de acesso no IAM Identity Center](#)
- [\(Opcional\) Passar atributos para controle de acesso](#)
- [Solução de problemas](#)

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,

you will use it to configure a SAML connection from your PingOne instance with the IAM Identity Center. Use the “download” and “import” metadata in both ends to exchange SAML metadata between PingOne and the IAM Identity Center. For more instructions on how to configure this connection, consult the PingOne documentation.

- If you replicated the IAM Identity Center for additional regions, you must update the configuration of your identity provider to allow access to AWS applications managed and AWS accounts from these regions. Consult more details in [the section called “Etapa 3: atualizar a configuração do IdP externo”](#). Consult the PingOne documentation for more details.

Considerações

The following are important considerations about PingOne that can affect the way you implement provisioning with the IAM Identity Center.

- The PingOne does not support group provisioning through SCIM. Contact Ping for the most recent information about group support in SCIM in PingOne.
- Users can continue to be provisioned in PingOne after the provisioning in the administrative portal of PingOne. If you need to stop provisioning immediately, exclude the SCIM token bearer and/or [Provisionar usuários e grupos de um provedor de identidades externo usando o SCIM](#) deactivate it in the IAM Identity Center.
- If an attribute is removed from a user in the data store configured in PingOne, this attribute will not be removed from the corresponding user in the IAM Identity Center. This is a known limitation in the implementation of the PingOne provider. If an attribute is modified, the change will be synchronized with the IAM Identity Center.
- The following are important observations about your SAML configuration in PingOne:
 - The IAM Identity Center is compatible only as emailaddress in the NameId format. This means that you must choose a user attribute that is exclusive in your directory in PingOne, not null and formatted as email/UPN (for example, user@domain.com) for its mapping to SAML_SUBJECT in PingOne E-mail (commercial) is a reasonable value to use in test configurations with the integrated directory of PingOne.
 - Users in PingOne with an email address containing a + character cannot log in to the IAM Identity Center, presenting errors such as 'SAML_215' or 'Invalid input'. To correct this, in PingOne, choose the Advanced option for the mapping to SAML_SUBJECT in Attribute Mappings. Next, define the Name ID Format.

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 de Provisionamento automático de entrada, copie o endpoint e o token de acesso SCIM. Você precisará colá-los posteriormente ao configurar o provisionamento no IdP.
 - a. Endpoint SCIM - Por exemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Token de acesso: escolha Mostrar token para copiar o valor.

Warning

Esse é a única vez que você pode obter o endpoint e o token de acesso SCIM. Certifique-se de copiar esses valores antes de prosseguir. Você inserirá esses valores para configurar provisionamento automático em seu IdP mais adiante neste tutorial.

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. 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](#) no 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 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 para o IAM Identity Center 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.

Solução de problemas

Para solucionar problemas gerais de SCIM e SAML com o PingOne, consulte as seguintes seções:

- [Usuários específicos não conseguem sincronizar com o IAM Identity Center a partir de um provedor SCIM externo](#)
- [Problemas relacionados ao conteúdo das asserções SAML criadas pelo IAM Identity Center](#)
- [Erro de usuário ou grupo duplicado ao provisionar usuários ou grupos com um provedor de identidades externo](#)
- Para obter mais informações sobre o PingOne, consulte a [documentação do PingOne](#).

Os recursos a seguir podem ajudá-lo a solucionar problemas enquanto você trabalha com AWS:

- [AWS re:Post](#)- Encontre FAQs e vincule outros recursos para ajudá-lo a solucionar problemas.
- [AWS Support](#): obter suporte técnico

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 fonte de identidade padrão, portanto não é necessário escolher uma fonte de identidades. Se a organização usar outro provedor de identidades, como o Microsoft Active Directory, o Microsoft Entra ID ou o Okta, considere a opção de integrar essa fonte de identidades com o IAM Identity Center em vez de usar a configuração padrão.

Objetivo

Neste tutorial, você usará o diretório padrão como fonte de identidade e uma instância de organização do IAM Identity Center para configurar e testar um usuário-administrativo. Esse usuário administrativo cria e gerencia usuários e grupos e concede AWS acesso com conjuntos de permissões. Nas próximas etapas, você criará o seguinte:

- Um usuário administrativo chamado *Nikki Wolf*
- Um grupo chamado *Admin team*
- 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. Como alternativa, se você quiser conceder acesso à aplicação aos usuários, siga a [etapa 1](#) do procedimento e [configure o acesso à aplicação](#).

Pré-requisitos

Os seguintes pré-requisitos são necessários para concluir este tutorial:

- [Habilitar o IAM Identity Center](#) e ter uma [instância de organização do IAM Identity Center](#)
 - Se você tiver uma [instância de conta](#) do IAM Identity Center, poderá criar usuários e grupos, além de conceder a eles acesso às aplicações. Para obter mais informações, consulte [Acesso à aplicação](#).
- Faça login Console de gerenciamento da AWS e acesse o console do IAM Identity Center como:

- 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, insira a senha.
- Já está usando AWS (credenciais do IAM) — Faça login usando suas credenciais do IAM com permissões administrativas.
 - Para obter mais ajuda para fazer login no Console de gerenciamento da AWS, consulte o [Início de Sessão da AWS Guia](#).
- Você pode configurar a autenticação multifator para os usuários do IAM Identity Center. Para obter mais informações, consulte [Configurar MFA no IAM Identity Center](#).

Etapa 1: adicionar um usuário

1. Abra o [console do IAM Identity Center](#).
2. No painel de navegação do IAM Identity Center, escolha Usuários e selecione Adicionar usuário.
3. Na página Especificar 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. Seus usuários devem se lembrar do nome de usuário para entrar no portal de AWS acesso 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 e-mail da Amazon Web Services, com a linha de assunto Convite para ingressar no IAM Identity Center. 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.
4. Escolha Próximo. A página Adicionar usuário a grupos é exibida. Vamos criar um grupo ao qual atribuir permissões administrativas em vez de concedê-las diretamente *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 *Admin team*.
 - b. Escolha Criar grupo.
 - c. Feche a guia Grupos do navegador para retornar à guia Adicionar usuário do navegador
5. Na área Grupos, selecione o botão Atualizar. O *Admin team* grupo aparece na lista.

Marque a caixa de seleção ao lado de *Admin team*, em seguida, escolha Avançar.

6. 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 ao *Admin team* grupo para que ele *Nikki* tenha acesso aos recursos.

Etapa 2: adicionar permissões administrativas

Important

Siga essas etapas somente se você habilitou uma [instância de organização do IAM Identity Center](#).

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 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. Para a Etapa 1: Selecione usuários e grupos, escolha o *Admin team* grupo que você criou. 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 do conjunto de permissões e escolha Avançar.

- c. Na página Etapa 3: revisar e enviar exercícios, confirme se o *Admin team* grupo 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 *Nikki's* acesso 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 sua organização, ele pode entrar 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 *Nikki's* as credenciais para fazer login e configurar a senha. Ao adicionar o usuário *Nikki Wolf* na Etapa 1, você optou por *Nikki* receber 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 *Nikki's* do usuário e a URL do portal de AWS acesso que eles usarão para entrar na organização. Registre essas informações para uso futuro.

Você é direcionado para a página de inscrição de novos usuários, onde pode definir a *Nikki's* senha e [registrar o dispositivo de MFA](#).

2. Depois de definir *Nikki's* a senha, você será direcionado para a página de login. Digite *nikkiw* e escolha Avançar, depois digite *Nikki's* a senha e escolha Entrar.
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, Perfil ou Chaves 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 o AWS SDK. Inclui as informações para usar credenciais de curto prazo que são atualizadas automaticamente ou chaves de acesso de curto prazo. Para obter mais informações, consulte [Obter credenciais de usuário do IAM Identity Center para o ou AWS CLI AWS SDKs](#).

4. Escolha o link Perfil 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.

Vídeos de tutorial

Como recurso adicional, você pode usar esses tutoriais em vídeo para saber mais sobre como configurar provedores de identidades externos:

- [Migração entre provedores de identidade externos em Centro de Identidade do AWS IAM](#)
- [Federando sua Centro de Identidade do AWS IAM instância existente com Microsoft Entra ID](#)

Configurar a força de trabalho no IAM Identity Center

O IAM Identity Center é a AWS solução para conectar os usuários da sua força de trabalho a aplicativos AWS gerenciados, como o Kiro e o Amazon Quick, além de outros AWS recursos. Você pode conectar o seu provedor de identidades existente e sincronizar os usuários e grupos do seu diretório, ou criar e gerenciar os usuários diretamente no IAM Identity Center.

Já está usando o IAM para acessar Contas da AWS?

Você não precisa fazer nenhuma alteração em seus Conta da AWS fluxos de trabalho atuais para usar o IAM Identity Center para acessar aplicativos AWS gerenciados. Se você estiver usando a [federação com o IAM](#) para Conta da AWS acessar, seus usuários podem continuar Contas da AWS acessando da mesma forma que sempre fizeram, e você pode continuar usando seus fluxos de trabalho existentes para gerenciar esse acesso.

Escolha a abordagem que melhor se adequa à estratégia de gerenciamento de identidade e à infraestrutura existente da organização.

Tópicos

- [Usuários, grupos e provisionamento no IAM Identity Center](#)
- [Gerencie sua fonte de identidade](#)
- [Gerenciar usuários no diretório do Identity Center](#)

Usuários, grupos e provisionamento no IAM Identity Center

O IAM Identity Center permite que você controle quem pode fazer login e quais recursos pode acessar. Um usuário deve ser provisionado para fazer login. Em seguida, você pode atribuir acesso somente a usuários ou grupos provisionados. Saiba mais sobre usuários, grupos e provisionamento no IAM Identity Center.

Exclusividade do nome de usuário e endereço de e-mail

O IAM Identity Center exige que cada usuário tenha um nome de usuário exclusivo. O nome de usuário é o identificador principal do usuário. O nome do usuário não precisa corresponder ao endereço de e-mail do usuário. O IAM Identity Center exige que todos os nomes de usuário e endereços de e-mail dos usuários não sejam NULL e sejam exclusivos.

Groups (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 grupos aninhados (um grupo dentro de outro). Os grupos são úteis ao atribuir acesso 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.

Provisionamento de usuários e grupos

O provisionamento é o processo de disponibilizar informações de usuários e grupos para uso pelo IAM Identity Center e aplicativos gerenciados ou aplicativos AWS gerenciados pelo cliente. Você pode criar usuários e grupos diretamente no IAM Identity Center ou conectar a fonte de identidade ao IAM Identity Center. Com o IAM Identity Center, você pode atribuir acesso às Contas da AWS e aplicações conectadas aos usuários e grupos.

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](#).

Desprovisionamento de usuários e grupos

O desprovisionamento é o processo de remover informações de usuários e grupos do IAM Identity Center.

Se estiver usando o Active Directory ou outro provedor de identidades externo com o IAM Identity Center, você deve remover os usuários e grupos dessas fontes de identidade em vez do IAM Identity Center. A exclusão de usuários e grupos do IAM Identity Center não os removerá completamente se a fonte de identidade for o Active Directory ou outro provedor de identidades externo.

Se você precisar desprovisionar usuários ou grupos do IAM Identity Center, primeiro [remova todas as atribuições de conjuntos de permissões](#) ou aplicações para os usuários ou grupos que deseja desprovisionar. Caso contrário, você terá conjuntos de permissões e atribuições de aplicações não atribuídas no IAM Identity Center.

Gerencie sua fonte de identidade

Sua fonte de identidade no IAM Identity Center define onde seus usuários e grupos são gerenciados. 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 ou ambos.

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

- [Provedor de identidades externo](#): escolha essa opção se quiser gerenciar usuários em um provedor de identidades (IdP) externo, como Okta ou Microsoft Entra ID.
- [Seu Active Directory local ou AWS gerenciado](#) — Escolha essa opção se quiser conectar seu Active Directory (AD).
- [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 a fonte de identidade padrão, a menos que você escolha outra fonte de identidades. Com o diretório do Identity Center, você cria seus usuários e grupos e atribui o nível de acesso deles aos seus Contas da AWS aplicativos.

Note

O IAM Identity Center não oferece suporte ao Simple AD SAMBA4 baseado como fonte de identidade.

Tópicos

- [Considerações para alterar sua fonte de identidade](#)
- [Alterar sua fonte de identidades](#)
- [Atributos de usuário e grupo compatíveis com o IAM Identity Center compatíveis](#)
- [Provedores de identidades externos](#)
- [Diretório Microsoft AD](#)

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 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.

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.

Como alternar entre o diretório do IAM Identity Center e 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.

Important

Ao alterar o tipo de fonte de identidade no IAM Identity Center para ou do Active Directory, esteja ciente de que o ID do Identity Store mudará. Isso pode ter as seguintes implicações:

- Sua URL padrão do portal de AWS acesso mudará. Você precisará comunicar o novo URL à força de trabalho e atualizar os favoritos, as listas de permissões do gateway ou do firewall e as configurações em que esse URL é referenciado. Recomendamos que você realize essa alteração em uma janela de manutenção programada para minimizar a interrupção para os usuários.
- Se você estiver usando uma chave KMS gerenciada pelo cliente para criptografia em repouso no IAM Identity Center e tiver configurado a política de chave KMS com o contexto de criptografia, saiba que o contexto de criptografia do Identity Store mudará. Por exemplo, no ARN do Identity Store “arn:aws:identitystore: :123456789012:identitystore/d-922763e9b3”, “d-922763e9b3” é o ID do Identity Store. Para evitar a interrupção do serviço durante essa transição, modifique temporariamente a política de chave KMS para usar um padrão curinga: “arn:aws:identitystore: :123456789012:identitystore/*”.

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. Porém, 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 você use a opção [Criar, Atualizar e Excluir APIs 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 que as usam. 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.
- **Se os usuários forem excluídos ou desativados no console do IAM Identity Center usando o Identity Store APIs**, os usuários com sessões ativas poderão continuar acessando aplicativos e contas integrados. Para obter informações sobre duração da sessão e comportamento do usuário na autenticação, consulte [Como entender as sessões de autenticação no IAM Identity Center](#).

Para obter informações sobre a forma como o IAM Identity Center provisiona usuários e grupos, consulte [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 continuam funcionando, desde que o

novo IdP envie as afirmações corretas (por exemplo, nome SAML). IDs Essas asserções devem corresponder aos nomes de usuário e grupos do IAM Identity Center.

- Sem sincronização de saída: o IAM Identity Center não é compatível com sincronização de saída, portanto, o IdP externo não será atualizado automaticamente com as alterações feitas em usuários e grupos no IAM Identity Center.
- Provisionamento SCIM: se você estiver usando provisionamento SCIM, as alterações de usuários e grupos do provedor de identidades só serão refletidas no IAM Identity Center depois que o provedor de identidades enviar essas alterações para o IAM Identity Center. Consulte [Considerações sobre o uso do provisionamento automático](#).
- Reversão: você pode reverter sua fonte de identidades para usar o IAM Identity Center a qualquer momento. Consulte [Mudar de um IdP externo para o IAM Identity Center](#).
- As sessões de usuário existentes são revogadas quando a duração da sessão expira: depois que você altera sua fonte de identidades para um provedor de identidades externo, as sessões de usuário ativas persistem pelo restante da duração máxima da sessão configurada no console. Por exemplo, se a duração da sessão do portal de AWS acesso for definida como oito horas e você tiver alterado a fonte de identidade na quarta hora, as sessões de usuário ativas persistirão por mais quatro horas. Para revogar sessões de usuário, consulte [the section called “Encerrar sessões ativas para usuários da força de trabalho”](#).

Se os usuários forem excluídos ou desativados no console do IAM Identity Center usando o Identity Store APIs, os usuários com sessões ativas poderão continuar acessando aplicativos e contas integrados. Para obter informações sobre duração da sessão e comportamento do usuário na autenticação, consulte [Como entender as sessões de autenticação no IAM Identity Center](#).

Note

Você não pode revogar sessões de usuário do console do IAM Identity Center depois que excluir o usuário.

Para obter informações sobre a forma como o IAM Identity Center provisiona usuários e grupos, consulte [Provedores de identidades externos](#).

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.
- As sessões de usuário existentes são revogadas quando a duração da sessão expira: depois que você altera sua fonte de identidades para o IAM Identity Center, as sessões de usuário ativas persistem pelo restante da duração máxima da sessão configurada no console. Por exemplo, se a duração da sessão do portal de AWS acesso for de oito horas e você tiver alterado a fonte de identidade na quarta hora, as sessões de usuário ativas continuarão sendo executadas por mais quatro horas. Para revogar sessões de usuário, consulte [the section called “Encerrar sessões ativas para usuários da força de trabalho”](#).

Se os usuários forem excluídos ou desativados no console do IAM Identity Center usando o Identity Store APIs, os usuários com sessões ativas poderão continuar acessando aplicativos e contas integrados. Para obter informações sobre duração da sessão e comportamento do usuário na autenticação, consulte [Como entender as sessões de autenticação no IAM Identity Center](#).

 Note

Você não poderá revogar sessões de usuário do console do IAM Identity Center depois que excluir o usuário.

- Suporte multirregional — Se você tiver replicado o IAM Identity Center para regiões adicionais ou planeja fazer isso, você deve usar um provedor de identidade externo como fonte de identidade. Para obter mais informações, incluindo outros pré-requisitos, consulte [Usando o IAM Identity Center em várias Regiões da AWS](#)

Para obter informações sobre a forma como o IAM Identity Center provisiona usuários e grupos, consulte [Gerenciar usuários no diretório do Identity Center](#).

Mudar de um IdP externo para outro IdP externo

Se você já estiver usando um IdP externo como fonte de identidade 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 do usuário, as atribuições de grupo e as associações de

grupos continuam funcionando, desde que o novo IdP envie as afirmações corretas (por exemplo, nome SAML). IDs

Essas afirmações devem corresponder aos nomes de usuário no IAM Identity Center quando seus usuários se autenticam por meio do novo IdP externo.

- **Provisionamento SCIM:** se você for usar SCIM para fazer provisionamento para o IAM Identity Center, recomendamos que 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 habilitado.
- **As sessões de usuário existentes são revogadas quando a duração da sessão expira:** depois que você altera sua fonte de identidades para outro provedor de identidades externo, as sessões de usuário ativas persistem pelo restante da duração máxima da sessão configurada no console. Por exemplo, se a duração da sessão do portal de AWS acesso for de oito horas e você tiver alterado a fonte de identidade na quarta hora, as sessões de usuário ativas persistirão por mais quatro horas. Para revogar sessões de usuário, consulte [the section called “Encerrar sessões ativas para usuários da força de trabalho”](#).

Se os usuários forem excluídos ou desativados no console do IAM Identity Center usando o Identity Store APIs, os usuários com sessões ativas poderão continuar acessando aplicativos e contas integrados. Para obter informações sobre duração da sessão e comportamento do usuário na autenticação, consulte [Como entender as sessões de autenticação no IAM Identity Center](#).

Note

Você não pode revogar sessões de usuário do console do IAM Identity Center depois que excluir o usuário.

Para obter informações sobre a forma como o IAM Identity Center provisiona usuários e grupos, consulte [Provedores de identidades externos](#).

Alternar entre o Active Directory e um IdP externo

Se você alternar 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.
- Se os usuários forem excluídos ou desativados no console do IAM Identity Center usando o Identity Store APIs, os usuários com sessões ativas poderão continuar acessando aplicativos e contas integrados. Para obter informações sobre duração da sessão e comportamento do usuário na autenticação, consulte [Como entender as sessões de autenticação no IAM Identity Center](#).
- Suporte multirregional — Se você tiver replicado o IAM Identity Center para regiões adicionais ou planeja fazer isso, você deve usar um provedor de identidade externo como fonte de identidade. Para obter mais informações, incluindo outros pré-requisitos, consulte [Usando o IAM Identity Center em várias Regiões da AWS](#)

Para obter informações sobre a forma como o IAM Identity Center provisiona usuários e grupos, consulte [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](#). Para concluir esse procedimento, você precisará de uma instância de organização do IAM Identity Center. Para obter mais informações, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

Warning

Dependendo da implantação atual, essa alteração remove qualquer atribuição de usuário e grupo que você configurou no IAM Identity Center. Essa alteração também removerá as funções do IAM do conjunto de permissões do seu Contas da AWS. Como resultado, talvez seja necessário atualizar suas políticas de recursos e garantir que isso não interrompa seu acesso às AWS KMS chaves e aos clusters do Amazon EKS. Para saber mais, consulte

Referenciando conjuntos de permissões em políticas de recursos, mapas de configuração do Amazon EKS Cluster e AWS KMS políticas principais.

Quando isso ocorrer, todos os usuários e grupos, incluindo o usuário administrativo no IAM Identity Center, perderão o acesso de login único a seus aplicativos Contas da AWS .

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.

Note

Se você replicou o IAM Identity Center para regiões adicionais, não poderá alterar o tipo de fonte de identidade. Você só pode substituir o IdP externo atual por outro. Para alterar o tipo de fonte de identidade, primeiro você precisará remover todas as regiões adicionais. Para obter mais informações, consulte [Usando o IAM Identity Center em várias Regiões da AWS](#).

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.

Atributos de usuário e grupo compatíveis com o IAM Identity Center compatíveis

Este guia fornece uma referência para o suporte de atributos do SCIM no IAM Identity Center. Ele lista quais atributos do usuário e do grupo da especificação SCIM são compatíveis com o repositório de identidades do IAM Identity Center e identifica atributos e subatributos específicos que não são compatíveis com o IAM Identity Center.

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 é compatível com os atributos mais usados por meio da entrada manual e do provisionamento automático do SCIM.

- [Para obter informações sobre a especificação System for Cross-Domain Identity Management \(SCIM\), consulte <https://tools.ietf.org/html/rfc7642>](#).
- Para obter informações sobre provisionamento manual e automático, consulte [Provisionamento quando os usuários vêm de um IdP externo](#).
- Para obter informações sobre mapeamento de atributos, consulte [Mapeamento de atributos entre o IAM Identity Center e o diretório de provedores de identidades externos](#).

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 próximas seções descrevem quais atributos não são compatíveis com o IAM Identity Center.

Objetos do usuário não compatíveis

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'

Objetos do grupo não compatíveis

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

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

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

Provedores de identidades externos

Com o IAM Identity Center, você pode conectar suas identidades de força de trabalho existentes de provedores de identidade externos (IdPs) por meio dos protocolos Security Assertion Markup Language (SAML) 2.0 e System for Cross-Domain Identity Management (SCIM). Isso permite que seus usuários façam login no portal de acesso da AWS 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.

Se você estiver usando um diretório autogerenciado no Active Directory ou em um AWS Managed Microsoft AD, consulte [Diretório Microsoft AD](#).

 Note

O protocolo SAML não fornece uma forma de consultar o IdP para saber mais 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 [Provisionar usuários e grupos de um provedor de identidades externo usando o SCIM](#) para usuários e grupos ou usar o [Provisionamento manual](#). Independentemente de como você provisiona usuários, o IAM Identity Center redireciona a interface da Console de gerenciamento da AWS 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](#).

Tópicos

- [Como se conectar a um provedor de identidades externo](#)
- [Como alterar metadados de um provedor de identidades externo no IAM Identity Center](#)
- [Uso de federação de identidades SAML e SCIM com provedores de identidade externos](#)
- [Perfil do SCIM e implementação SAML 2.0](#)

Como se conectar a um provedor de identidades externo

Existem diferentes pré-requisitos, considerações e procedimentos de provisionamento para o suporte externo. IdPs Há step-by-step tutoriais disponíveis para vários: IdPs

- [CyberArk](#)
- [Google Workspace](#)
- [JumpCloud](#)
- [Microsoft Entra ID](#)
- [Okta](#)
- [OneLogin](#)
- [Ping Identity](#)

Para obter mais informações sobre as considerações externas suportadas pelo IdPs IAM Identity Center, consulte [Uso de federação de identidades SAML e SCIM com provedores de identidade externos](#).

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 Settings.
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.

Note

O arquivo de metadados SAML que você baixa contém tanto o serviço de consumidor de asserção IPv4 (ACS) somente quanto o dual-stack. URLs Além

disso, se sua Central de Identidade do IAM for replicada para regiões adicionais, o arquivo de metadados conterá ACS URLs para cada região adicional. Se o seu IdP externo tiver um limite no número de ACS URLs, você precisará remover o ACS desnecessário. URLs Por exemplo, se sua organização adotou totalmente os endpoints de pilha dupla e não usa mais aqueles IPv4 somente, você pode remover os últimos. Uma abordagem alternativa é não usar o arquivo de metadados, mas copiar e colar o ACS URLs no IdP 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 de chave pública x509 que é necessário e 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 as atribuições 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.

Como alterar metadados de um provedor de identidades externo no IAM Identity Center

É possível alterar os metadados do seu provedor de identidades externo que você forneceu anteriormente ao IAM Identity Center. Essas mudanças afetam a capacidade dos usuários de fazer login e acessar AWS recursos por meio do IAM Identity Center. O procedimento a seguir descreve como atualizar os metadados do IdP externo armazenados no IAM Identity Center. Para concluir esse procedimento, você precisará de uma instância de organização do IAM Identity Center. Para obter mais informações, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

Para alterar os metadados de 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. Selecione Ações e depois escolha Gerenciar autenticação.
4. Na seção Metadados do provedor de identidades, escolha Editar metadados do IdP. Você pode fazer as alterações no URL de login do IdP e/ou no URL do emissor do seu IdP externo nesta página. Escolha Salvar alterações quando tiver feito todas as alterações necessárias.

Uso de 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 addr-spec RFC 2822 \(https://tools.ietf.org/html/rfc2822\) compatível com addr-spec \(/rfc2822 #section-3.4.1\). name@domain.com https://tools.ietf.org/html](https://tools.ietf.org/html/rfc2822)
 - 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.
 - O IAM Identity Center não é compatível com a assinatura de solicitações de autenticação SAML enviadas para o exterior IdPs.

- O IdP precisa oferecer suporte a vários serviços ao consumidor de asserção (ACS) URLs se você planeja replicar o IAM Identity Center para regiões adicionais e aproveitar totalmente os benefícios de um IAM Identity Center multirregional. Para obter mais informações, consulte [Usando o IAM Identity Center em várias Regiões da AWS](#). Usar um único URL do ACS pode afetar a experiência do usuário em outras regiões. Sua região principal continuará funcionando normalmente. Para obter mais informações sobre a experiência do usuário em regiões adicionais com um único URL ACS, consulte [the section called “Usando aplicativos AWS gerenciados sem vários ACS URLs”](#) e [the section called “Conta da AWS resiliência de acesso sem vários ACS URLs”](#)
- SCIM
 - [A implementação do IAM Identity Center SCIM é baseada no SCIM RFCs 7642 \(<https://tools.ietf.org/html/rfc7642>\), 7643 \(\[/rfc7643\]\(https://tools.ietf.org/html/rfc7643\)\) e 7644 \(<https://tools.ietf.org/html/rfc7644>\) e nos requisitos de interoperabilidade estabelecidos no rascunho de março de <https://tools.ietf.org/html2020> do Basic SCIM Profile 1.0 \(#rfc .section.4\). FastFed \[https://openid.net/specs/fastfed-scim-1_0-02.html\]\(https://openid.net/specs/fastfed-scim-1_0-02.html\)](#) 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 ExternalId PDirectory do evento Login
- Registros específicos do IdP, registros and/or de depuração
- [Solução de problemas do IAM Identity Center](#)

Note

Alguns IdPs, como os do [Tutoriais sobre fontes de identidade do IAM Identity Center](#), 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 outros and/or endpoints de abordagem de federação 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 Console de gerenciamento da AWS de terceiros Microsoft 365, como, e. Concur Salesforce

Porém, o protocolo SAML não oferece um modo de consultar o IdP para obter informações 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, consulte [Provisionar usuários e grupos de um provedor de identidades externo usando o SCIM](#). 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

- [Provisionar usuários e grupos de um provedor de identidades externo usando o SCIM](#)
- [Fazer rodízio de certificados SAML 2.0](#)

Provisionar usuários e grupos de um provedor de identidades externo usando o SCIM

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](#)
- [Como monitorar a expiração do token de acesso](#)
- [Gerar um token de acesso](#)
- [Habilitar provisionamento automático](#)
- [Excluir um token de acesso](#)
- [Desabilitar provisionamento automático](#)
- [Fazer rodízio de um token de acesso](#)
- [Auditar e reconciliar recursos provisionados automaticamente](#)
- [Provisionamento manual](#)

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 os [Tutoriais sobre fontes de identidade do IAM Identity Center](#) aplicáveis 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 de usuários é gerenciado pelo provedor de identidades e pode variar de acordo com sua implementação. Consulte seu provedor de identidades para obter detalhes sobre desprovisionamento de usuários.
- Depois de configurar o provisionamento automático com o SCIM para o IdP, você não pode mais adicionar ou editar usuários no console do IAM Identity Center. Se precisar adicionar ou modificar um usuário, você deve fazer isso no IdP externo ou da fonte de identidade.

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.

Gerar um 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 obter mais informações, consulte [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.

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 os [Tutoriais sobre fontes de identidade do IAM Identity Center](#) para o 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 de Provisionamento automático de entrada, copie o endpoint e o token de acesso SCIM. Você precisará colá-los posteriormente ao configurar o provisionamento no IdP.
 - a. Endpoint SCIM - Por exemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Token de acesso: escolha Mostrar token para copiar o valor.

 Warning

Esse é a única vez que você pode obter o endpoint e o token de acesso SCIM. Certifique-se de copiar esses valores antes de prosseguir. Você inserirá esses valores para configurar provisionamento automático em seu IdP mais adiante neste tutorial.

5. Escolha Fechar.

Depois de concluir este procedimento, você deve configurar o provisionamento automático em seu IdP. Para obter mais informações, consulte os [Tutoriais sobre fontes de identidade do IAM Identity Center](#) para o seu IdP.

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.

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 obter mais informações, consulte [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.

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 [Gerar um 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 [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.

Auditar e reconciliar recursos provisionados automaticamente

O SCIM permite que você provisione automaticamente usuários, grupos e associações de grupos da fonte de identidade para o IAM Identity Center. Este guia ajuda você a verificar e reconciliar esses recursos para manter uma sincronização precisa.

Por que auditar os recursos?

A auditoria regular ajuda a garantir que os controles de acesso permaneçam precisos e que seu provedor de identidade (IdP) permaneça devidamente sincronizado com o IAM Identity Center. Isso é particularmente importante para a conformidade de segurança e o gerenciamento de acesso.

Recursos que podem ser auditados:

- Usuários
- Groups (Grupos)
- Associações de grupo

Você pode usar os [comandos do AWS Identity Store API ou da CLI](#) para conduzir a auditoria e a reconciliação. Os exemplos a seguir usam comandos AWS CLI . Para alternativas de API, consulte as [operações correspondentes](#) na referência da API do Identity Store.

Como auditar recursos

Aqui estão alguns exemplos de como auditar esses recursos usando AWS CLI comandos.

Antes de começar, verifique se você tem:

- Acesso de administrador ao IAM Identity Center.
- AWS CLI instalado e configurado. Para obter informações, consulte o Guia do usuário da interface da linha de comando da [AWS](#) .

- Permissões do IAM exigidas para comandos do Identity Store.

Etapa 1: listar os recursos atuais

Você pode visualizar seus recursos atuais usando AWS CLI o.

Note

Ao usar o AWS CLI, a paginação é processada automaticamente, a menos que você especifique. `--no-paginate` Se você estiver chamando a API diretamente (por exemplo, com um SDK ou um script personalizado), manipule o `NextToken` na resposta. Isso garante que você recupere todos os resultados em várias páginas.

Example para usuários

```
aws identitystore list-users \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

Example para grupos

```
aws identitystore list-groups \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

Example para associações de grupo

```
aws identitystore list-group-memberships \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-id GROUP_ID
```

Etapa 2: comparar a fonte de identidade

Compare os recursos listados com a fonte de identidade para identificar quaisquer discrepâncias, como:

- Recursos ausentes que devem ser provisionados no IAM Identity Center.

- Recursos extras que devem ser removidos do IAM Identity Center.

Example para usuários

```
# Create missing users
aws identitystore create-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-name USERNAME \
  --display-name DISPLAY_NAME \
  --name GivenName=FIRST_NAME,FamilyName=LAST_NAME \
  --emails Value=EMAIL,Primary=true

# Delete extra users
aws identitystore delete-user \
  --identity-store-id IDENTITY_STORE_ID \
  --user-id USER_ID
```

Example para grupos

```
# Create missing groups
aws identitystore create-group \
  --identity-store-id IDENTITY_STORE_ID \
  [group attributes]

# Delete extra groups
aws identitystore delete-group \
  --identity-store-id IDENTITY_STORE_ID \
  --group-id GROUP_ID
```

Example para associações de grupo

```
# Add missing members
aws identitystore create-group-membership \
  --identity-store-id IDENTITY_STORE_ID \
  --group-id GROUP_ID \
  --member-id '{"UserId": "USER_ID"}'

# Remove extra members
aws identitystore delete-group-membership \
  --identity-store-id IDENTITY_STORE_ID \
  --membership-id MEMBERSHIP_ID
```

Considerações

- Os comandos estão sujeitos a [cotas de serviço e controle de utilização de API](#).
- Quando você encontrar muitas diferenças durante a reconciliação, faça pequenas alterações graduais no AWS Identity Store. Isso ajuda a evitar erros que afetam vários usuários.
- A sincronização do SCIM pode substituir as alterações manuais. Verifique as configurações de IdP para entender esse comportamento.

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 obter 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 obter mais informações, consulte [Groups \(Grupos\)](#).

Fazer rodízio de 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

- [Alternar um certificado SAML 2.0](#)
- [Indicadores de status de expiração do certificado](#)

Alternar 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 rotatividade 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

A página Gerenciar certificados SAML 2.0 exibe ícones indicadores de status coloridos na coluna Expira em ao lado de cada certificado da 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 expirou.
- Amarelo: indica que um certificado expira em 90 dias ou menos.
- Verde: indica que um certificado é 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.

Diretório Microsoft AD

Com Centro de Identidade do AWS IAM, 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 AWS aplicativos ou ambos.

AWS Directory Service ajuda você a configurar e executar um AWS Managed Microsoft AD diretório autônomo hospedado no Nuvem AWS. Você também pode usar 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 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 Directory Service resida AWS Managed Microsoft AD em sua AWS Organizations conta de gerenciamento.
- O IAM Identity Center não é compatível SAMBA 4-based Simple AD como diretório conectado.
- O IAM Identity Center não pode sincronizar entidades de segurança estrangeiras (FSPs). Se um grupo AWS Managed Microsoft AD contiver membros de um domínio confiável como FSPs, esses membros não serão sincronizados.

Para uma demonstração do processo de uso do Active Directory como fonte de identidade para o IAM Identity Center, assista ao seguinte vídeo YouTube:

[Usando o Active Directory como fonte de identidade para Centro de Identidade do AWS IAM | Amazon Web Services](#)

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, deverá habilitar o IAM Identity Center no mesmo Região da AWS local em que seu AWS Managed Microsoft AD diretório está configurado. O IAM Identity Center armazena os dados de atribuição na mesma região do diretório. Para administrar o IAM Identity Center, talvez seja necessário mudar para a região em que o IAM Identity Center está 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 Service 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 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.

Note

O IAM Identity Center não oferece suporte ao Simple AD SAMBA4 baseado como fonte de identidade.

AWS Managed Microsoft AD

1. Revise as orientações em [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 [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](#).

IdP externo

1. Revise as orientações em [Provedores de identidades externos](#).
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

Após conectar o Active Directory ao IAM Identity Center, você pode especificar um usuário ao qual deseja conceder permissões administrativas e, em seguida, sincronizar esse usuário do diretório com o IAM Identity Center.

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 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, 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 [Crie um conjunto de permissões](#).

Provisioning when users come from Active Directory.

O IAM Identity Center usa a conexão fornecida pelo 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](#)
- [Mapeamento de atributos entre o IAM Identity Center e o diretório de provedores de identidades externos](#)
- [Sincronização configurável no AD do IAM Identity Center](#)

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 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. 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.

Centro de Identidade do AWS IAM 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 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.

Note

Para usar AWS aplicativos, como o IAM Identity Center, para ler usuários do Directory Service diretório de domínios confiáveis, as Directory Service contas exigem permissões para o `userAccountControl` atributo dos usuários confiáveis. Sem permissões de leitura para esse atributo, as aplicações da AWS não conseguem determinar se a conta está habilitada ou desabilitada.

O acesso de leitura a esse atributo é fornecido por padrão quando uma relação de confiança é criada. Se você negar o acesso a esse atributo (não recomendado), impedirá que aplicações como o Identity Center consigam ler os usuários confiáveis. A solução é permitir especificamente o acesso de leitura ao `userAccountControl` atributo nas contas de AWS serviço na OU AWS reservada (prefixada com `AWS_`).

- 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 Guia de administração AWS Directory Service . As seguintes considerações devem ser observadas ao usar o AD Connector:

- 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 Directory Service para o Microsoft Active Directory.

 Note

O IAM Identity Center não funciona com diretórios Simple AD SAMBA4 baseados.

Mapeamento de atributos entre o IAM Identity Center e o diretório de provedores de identidades externos

Os mapeamentos de atributos são usados para mapear os tipos de atributos que existem no IAM Identity Center com atributos semelhantes em uma fonte de identidades externa, como o Google Workspace, o Microsoft Active Directory (AD) e o Okta. O IAM Identity Center recupera atributos de usuário da fonte de identidades e os mapeia para os atributos de usuário do IAM Identity Center.

Se o IAM Identity Center estiver sincronizado para usar um provedor de identidades (IdP) externo como Google Workspace, Okta ou Ping como fonte de identidade, você precisará mapear os atributos no IdP.

O IAM Identity Center preenche previamente um conjunto de atributos para você na aba Mapeamentos de atributo encontrada na página de configuração. O IAM Identity Center usa esses atributos de usuário para preencher as asserções SAML (como atributos SAML) que são enviadas à aplicação. Esses atributos de usuário, por sua vez, são recuperados da fonte de identidades. Cada aplicação determina a lista de atributos SAML 2.0 necessários para que o login único tenha sucesso. Para obter 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 atributos da página de configuração do Active Directory se você estiver usando o Active Directory como fonte de identidade. Para obter mais informações, consulte [Como mapear atributos de usuário entre o IAM Identity Center e o diretório Microsoft AD](#).

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}
```

```
${path:addresses[type eq "work"].formatted}
```

```
${path:phoneNumbers[type eq "work"].value}
```

```
${path:userType}
```

```
${path:title}
```

```
${path:locale}
```

Atributos compatíveis em seu IdP

`${path:timezone}`

`${path:enterprise.employeeNumber}`

`${path:enterprise.costCenter}`

`${path:enterprise.organization}`

`${path:enterprise.division}`

`${path:enterprise.department}`

`${path:enterprise.manager.value}`

Mapeamento padrão entre o IAM Identity Center e o Microsoft AD

A tabela a seguir lista os mapeamentos padrão dos atributos de usuário no IAM Identity Center para os atributos de usuário no seu diretório Microsoft AD. O IAM Identity Center só é compatível com a lista de atributos na coluna User attribute in IAM Identity Center.

Atributo de usuário no IAM Identity Center	Mapeia para este atributo no Active Directory
displayname	<code>\${displayname}</code>
emails[?primary].value *	<code>\${mail}</code>
externalid	<code>\${objectguid}</code>
name.givenname	<code>\${givenname}</code>
name.familyname	<code>\${sn}</code>
name.middlename	<code>\${initials}</code>
sid	<code>\${objectsid}</code>
username	<code>\${userprincipalname}</code>

* O atributo de e-mail no IAM Identity Center deve ser exclusivo dentro do diretório.

Atributo de grupo no IAM Identity Center	Mapeia para este atributo no Active Directory
externalid	\${objectguid}
description	\${description}
displayname	\${samaccountname}@{associateddomain}

Considerações

- Se você não tiver nenhuma atribuição para os usuários e grupos no IAM Identity Center ao habilitar a sincronização configurável do AD, os mapeamentos padrão na tabela anterior serão usados. Para obter informações sobre como personalizar esses mapeamentos, consulte [Configure mapeamentos de atributos para sua sincronização](#).
- 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 valor windowsUpn como o valor padrão para "nome de usuário". Se você quiser alterar o mapeamento de atributos do mapeamento atual para "nome de usuário", confirme se os fluxos do IAM Identity Center com dependência de "nome de usuário" continuarão funcionando como esperado, antes de fazer a alteração.

Atributos do Microsoft AD do IAM Identity Center compatíveis

A tabela a seguir fornece a lista completa de atributos de diretório do Microsoft AD compatíveis e que podem ser mapeados para atributos de usuário no IAM Identity Center.

Atributos compatíveis em seu diretório do Microsoft AD
\${samaccountname}
\${description}

Atributos compatíveis em seu diretório do Microsoft AD

`${objectguid}`

`${objectsid}`

`${givenname}`

`${sn}`

`${initials}`

`${mail}`

`${userprincipalname}`

`${displayname}`

`${distinguishedname}`

`${proxyaddresses[?type == "SMTP"].value}`

`${proxyaddresses[?type == "smtp"].value}`

`${useraccountcontrol}`

`${associateddomain}`

Considerações

- Você pode especificar qualquer combinação de atributos de diretório do Microsoft AD compatíveis para mapear para um único atributo no IAM Identity Center.

Atributos do IAM Identity Center compatíveis com Microsoft AD

A tabela a seguir lista todos os atributos do IAM Identity Center que são compatíveis e que podem ser mapeados para atributos de usuário no seu diretório Microsoft AD. 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 IAM Identity Center compatíveis com Active Directory

`${user:AD_GUID}`

`${user:AD_SID}`

`${user:email}`

`${user:familyName}`

`${user:givenName}`

`${user:middleName}`

`${user:name}`

`${user:preferredUsername}`

`${user:subject}`

Como mapear atributos de usuário entre o IAM Identity Center e o diretório Microsoft AD

Você pode usar o procedimento a seguir para especificar como os atributos de usuário no IAM Identity Center devem ser mapeados para atributos correspondentes no 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 `${mail}`.
5. Escolha Salvar alterações.

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.

- 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.

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 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 obter 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 obter mais informações, consulte [Adicione usuários e grupos ao escopo de sincronização](#).

- Fazendo atribuições para grupos aninhados no Active Directory

Grupos que são membros de outros grupos são chamados de grupos aninhados (ou grupos secundários).

- Sincronização do AD configurável: usar a sincronização do AD configurável para fazer atribuições a um grupo do Active Directory que contém grupos aninhados pode aumentar o escopo dos usuários que têm acesso a aplicações ou Contas da AWS. Nesse caso, a atribuição é aplicada a todos os usuários, incluindo os usuários 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 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](#).

Tópicos

- [Como funciona a sincronização configurável do AD](#)
- [Configure mapeamentos de atributos para sua sincronização](#)
- [Configuração de sincronização entre o Active Directory e o IAM Identity Center](#)
- [Adicione usuários e grupos ao escopo de sincronização](#)
- [Remova usuários e grupos ao escopo de sincronização](#)
- [Interromper e retomar a sincronização](#)
- [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. Para saber mais sobre os pré-requisitos, consulte [Pré-requisitos e considerações](#)

Criação

Depois de conectar seu diretório autogerenciado no Active Directory ou seu AWS Managed Microsoft AD diretório gerenciado pelo 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 de grupos aninhados ou grupos secundários) também são gravados no repositório de identidades.

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, por padrão, sincroniza dados do Active Directory a cada hora em um ciclo de sincronização. A sincronização de dados com o IAM Identity Center pode levar de 30 minutos a 2 horas, dependendo do tamanho do 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 levar um ciclo de sincronização para uma atualização de atributos 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 mapeamentos de atributos para sua sincronização

Para obter mais informações sobre atributos disponíveis, consulte [Mapeamento de atributos entre o IAM Identity Center e o diretório de provedores de identidades externos](#).

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 grupo, os atributos do IAM Identity Center identity store e os atributos de grupo do Active Directory não podem ser alterados.

6. Escolha Salvar alterações. Isso o levará de volta à página Manage Sync.

Configuração de sincronização entre o Active Directory e o IAM Identity Center

Se você estiver sincronizando os usuários e grupos do Active Directory para o IAM Identity Center pela primeira vez, siga as etapas. Como alternativa, você pode seguir as etapas descritas em [Alterar sua fonte de identidades](#) para alterar a fonte de identidade do IAM Identity Center para Active Directory.

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

Note

Ao adicionar grupos ao seu escopo de sincronização, sincronize grupos diretamente do domínio local confiável em vez de grupos no AWS Managed Microsoft AD domínio. Os grupos sincronizados diretamente do domínio confiável contêm objetos de usuário reais que o IAM Identity Center pode acessar e sincronizar com êxito.

Adicione usuários e grupos do Active Directory ao IAM Identity Center seguindo estas etapas.

Como adicionar usuários

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 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. Se o usuário que você especificou não aparecer 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. Se o grupo que você especificou não aparecer 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 Remove .

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. Selecione a guia Grupos.

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 Remove .

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.

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 IAMIdentityCenterAllUsersAndGroups.
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.

Gerenciar usuários no diretório do 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 obter 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 Directory Service. Para obter mais informações, consulte considerações para [Como alternar entre o diretório do IAM Identity Center e 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 ao diretório do Identity Center](#)
- [Adicionar grupos ao diretório do Centro de Identidade do IAM](#)
- [Adicionar usuários a grupos](#)
- [Excluir grupos do IAM Identity Center](#)
- [Excluir usuários do IAM Identity Center](#)
- [Remover usuários de grupos](#)
- [Editar as propriedades do usuário no IAM Identity Center](#)

Adicionar usuários ao diretório do Identity Center

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 diretório do Identity Center. Como alternativa, você pode chamar a operação AWS da API [CreateUser](#) para adicionar usuários.

Console

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. Enviar um e-mail para este usuário com instruções de configuração de senha — Essa opção envia automaticamente ao usuário um e-mail endereçado do Amazon Web Services, com a linha de assunto Convite para ingressar no Centro de Identidade do AWS IAM. O e-mail convida, em nome da sua empresa, o usuário a acessar o portal de acesso AWS do IAM Identity Center e registra uma senha. O convite enviado por e-mail expirará em sete dias. Se isso acontecer, você poderá reenviar o e-mail escolhendo Redefinir senha e depois Enviar um e-mail ao usuário com instruções para redefinição da senha. Antes que o usuário aceite o convite, você verá o link Enviar verificação por e-mail, que serve para verificar o endereço de e-mail do usuário. Porém, essa etapa é opcional e desaparecerá depois que o usuário aceitar o convite e registrar uma senha.

 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 [E-mails entre regiões com o Amazon SES](#).

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. O usuário precisará verificar seu endereço de e-mail. Você pode iniciar o processo escolhendo Enviar link de verificação por e-mail. O link de verificação de e-mail expirará em sete dias. Se isso acontecer, você pode reenviar o link de verificação por e-mail escolhendo Redefinir senha e depois Gerar uma senha de uso único e compartilhar a senha com o usuário.

- 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 obter mais informações, consulte [Provisionar usuários e grupos de um provedor de identidades externo usando o SCIM](#).
- 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.

AWS CLI

Para adicionar um usuário

O comando `create-user` a seguir cria um novo usuário no diretório do Identity Center.

```
aws identitystore create-user \  
  --identity-store-id d-1234567890 \  
  --user-name johndoe \  
  --name "GivenName=John,FamilyName=Doe" \  
  --display-name "John Doe" \  
  --emails "Type=work,Value=johndoe@example.com"
```

Saída:

```
{
  "UserId": "1234567890-abcdef",
  "IdentityStoreId": "d-1234567890"
}
```

Note

Ao criar usuários com o comando `create-user` da CLI ou a operação da API [CreateUser](#), os usuários não têm senhas. Você pode atualizar as configurações no IAM Identity Center para enviar a esses usuários um e-mail de verificação após a primeira tentativa de login para que eles possam configurar uma senha. Se você não habilitar essa configuração, deverá gerar uma senha de uso único e compartilhá-la com o usuário. Para obter mais informações, consulte [Enviar uma senha de uso único por e-mail para os usuários criados com a API ou CLI](#).

Adicionar grupos ao diretório do Centro de Identidade do IAM

Use o procedimento a seguir para adicionar grupos ao diretório do Identity Center. Como alternativa, você pode chamar a operação AWS da API [CreateGroup](#) para adicionar grupos.

Console

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.

AWS CLI

Para adicionar um grupo

O comando `create-group` a seguir cria um novo grupo no diretório do Identity Center.

```
aws identitystore create-group \  
  --identity-store-id d-1234567890 \  
  --display-name "Developers" \  
  --description "Group that contains all developers"
```

Saída:

```
{  
  "GroupId": "1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p",  
  "IdentityStoreId": "d-1234567890"  
}
```

Depois de adicionar esse grupo ao diretório do Identity Center, você pode atribuir acesso de login único ao grupo. Para obter mais informações, consulte [Atribuir acesso de usuário ou grupo a Contas da AWS](#).

Adicionar usuários a grupos

Use o procedimento a seguir para adicionar usuários como membros de um grupo que você criou anteriormente no diretório do Identity Center. Como alternativa, você pode chamar a operação da AWS API [CreateGroupMembership](#) para adicionar um usuário como membro de um grupo.

Console

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**.

AWS CLI

Para adicionar um usuário como membro de um grupo

O comando `create-group-membership` a seguir adiciona um usuário a um grupo no diretório do Identity Center.

```
aws identitystore create-group-membership \
  --identity-store-id d-1234567890 \
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
  --member-id UserId=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Saída:

```
{
  "MembershipId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
  "IdentityStoreId": "d-1234567890"
}
```

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 diretório do Identity Center.

Important

As instruções nesta página aplicam-se a [Centro de Identidade do AWS IAM](#). 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 .

Console

Para excluir um grupo

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.

AWS CLI

Para excluir um grupo

O comando `delete-group` a seguir exclui o grupo especificado do diretório do Identity Center.

```
aws identitystore delete-group \  
  --identity-store-id d-1234567890 \  
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

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. Depois de excluir um usuário, você não pode desfazer essa ação. Use o procedimento a seguir para excluir um usuário do diretório do 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 obter mais informações, consulte [Como entender as sessões de autenticação no IAM Identity Center](#).

 Important

As instruções nesta página aplicam-se a [Centro de Identidade do AWS IAM](#). 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 .

Console

Para excluir um usuário

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.

AWS CLI

Para excluir um usuário

O comando `delete-user` a seguir exclui um usuário do diretório do Identity Center.

```
aws identitystore delete-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Remover usuários de grupos

Use o procedimento a seguir para remover membros de um grupo. Como alternativa, você pode chamar a operação AWS da API [DeleteGroupMembership](#) para remover um usuário de um grupo.

Console

Para remover um usuário de um grupo

1. Abra o [console do IAM Identity Center](#).
2. Selecione Grupos.
3. Escolha o grupo que deseja atualizar.
4. Na página de detalhes do grupo, em Usuários neste grupo, escolha os usuários a serem removidos.
5. Escolha Remover usuários do grupo.
6. Na caixa de diálogo Remover usuários, escolha Remover usuários do grupo para confirmar que deseja remover o acesso dos usuários à conta e aplicações atribuídas ao grupo.

AWS CLI

Para remover um usuário de um grupo

O comando `delete-group-membership` a seguir remove a associação de um grupo.

```
aws identitystore delete-group-membership  
  --identity-store-id d-1234567890 \  
  --membership-id a1b2c3d4-5678-90ab-cdef-EXAMPLE33333
```

Editar as propriedades do usuário no IAM Identity Center

Use o procedimento a seguir para editar as propriedades de um usuário no diretório do Identity Center. Como alternativa, você pode chamar a operação da AWS API [UpdateUser](#) para atualizar as propriedades do usuário.

Console

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.

AWS CLI

Para editar as propriedades do usuário no IAM Identity Center

O comando `update-user` a seguir atualiza o apelido do usuário.

```
aws identitystore update-user \
```

```
--identity-store-id d-1234567890 \  
--user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--operations '{"AttributePath":"nickName","AttributeValue":"Johnny"}'
```

Configurar o acesso da força de trabalho aos recursos AWS

Configure como os usuários da sua força de trabalho autenticam e acessam AWS recursos por meio do IAM Identity Center. Esta seção aborda os seguintes componentes que controlam o acesso dos usuários da força de trabalho ao ambiente da AWS :

- **Sessões de autenticação** — Entenda como o IAM Identity Center gerencia diferentes tipos de sessões de usuário, desde sessões interativas do portal até sessões de aplicação em segundo plano, e como interagem.
- **Gerenciamento de acesso de usuários** — Configure a duração das sessões, desabilite contas de usuário e implemente bloqueios de acesso em toda a organização para manter a segurança e a conformidade.
- **Gerenciamento de senhas** — Para usuários criados no diretório do Identity Center, defina requisitos de senha, gerencie a configuração de credenciais do usuário e as redefinições de senha.
- **Autenticação multifatorial** — Para usuários criados no diretório do Identity Center, aprimore a segurança com o MFA usando aplicações autenticadoras, chaves de segurança ou autenticadores integrados para proteger os logins dos usuários.

Tópicos

- [Como entender as sessões de autenticação no IAM Identity Center](#)
- [Configurar a duração da sessão no IAM Identity Center](#)
- [Desative o acesso do usuário Contas da AWS e os aplicativos no IAM Identity Center](#)
- [Negar acesso do usuário com Políticas de controle de serviço](#)
- [Como gerenciar o acesso para usuários do diretório do Identity Center](#)

Como entender as sessões de autenticação no IAM Identity Center

Quando um usuário faz login no [portal de acesso do AWS](#), o IAM Identity Center cria uma sessão de autenticação que representa a identidade verificada do usuário.

Depois de autenticado, o usuário pode acessar todos os [aplicativos atribuídos Contas da AWS e AWS gerenciados pelo cliente](#) que os administradores lhes concederam permissão para usar, sem logins adicionais.

Tipos de sessões de autenticação

Sessões interativas do usuário

Depois que um usuário faz login no portal de AWS acesso, o IAM Identity Center cria uma sessão interativa com o usuário. Essa sessão representa o estado autenticado do usuário no IAM Identity Center e serve como base para a criação de outros tipos de sessão. As sessões interativas do usuário podem ter a duração configurada no IAM Identity Center, que pode ser de até 90 dias.

As sessões interativas do usuário são o principal mecanismo de autenticação. Elas terminam quando o usuário sai ou quando um administrador encerra a sessão. A duração dessas sessões deve ser cuidadosamente configurada com base nos requisitos de segurança da organização.

Para obter informações sobre como configurar a duração da sessão interativa do usuário, consulte [the section called “Configurar duração da sessão”](#).

Sessões de aplicação

As sessões de aplicativos são as conexões autenticadas entre usuários e aplicativos AWS gerenciados (como o Kiro ou o Amazon Quick) que o IAM Identity Center estabelece por meio de login único.

Por padrão, as sessões de aplicação têm vida útil de uma hora, mas são atualizadas automaticamente, desde que a sessão interativa do usuário subjacente permaneça válida. Esse mecanismo de atualização fornece uma experiência perfeita para os usuários, mantendo os controles de segurança. Quando uma sessão interativa do usuário termina, seja por meio da saída do usuário ou da ação do administrador, as sessões de aplicação terminam na próxima tentativa de atualização, normalmente em 30 minutos.

Sessões de usuário em segundo plano

Sessões de usuários em segundo plano são sessões de duração prolongada projetadas para aplicações que precisam executar processos por horas ou dias sem interrupção. Atualmente, esse tipo de sessão se aplica principalmente ao [Amazon SageMaker Studio](#), onde cientistas de dados podem executar trabalhos de treinamento de aprendizado de máquina que levam muitas horas para serem concluídos.

Para obter informações sobre como configurar a duração da sessão do usuário em segundo plano, consulte [Sessões de usuários em segundo plano](#).

Sessões de Kiro

Você pode estender as sessões do Kiro para permitir que os desenvolvedores que usam o Kiro in mantenham IDEs a autenticação por até 90 dias. Esse atributo reduz as interrupções de login enquanto você trabalha no código.

Essas sessões são independentes de outros tipos de sessão e não afetam as sessões interativas do usuário ou outras aplicações gerenciadas pela AWS . Dependendo de quando você habilitou o IAM Identity Center, esse atributo pode ser habilitado por padrão.

Para obter informações sobre como configurar sessões estendidas do Kiro, consulte. [???](#)

Sessões de perfil do IAM criadas pelo IAM Identity Center

O IAM Identity Center cria um tipo diferente de sessão quando os usuários acessam o Console de gerenciamento da AWS ou AWS CLI. Nesses casos, o IAM Identity Center usa a sessão de login para obter uma sessão do IAM assumindo um perfil do IAM especificado no conjunto de permissões do usuário.

Important

Diferentemente das sessões de aplicação, as sessões de perfil do IAM operam independentemente depois de estabelecidas. Elas persistem pela duração configurada no conjunto de permissões, que pode ser de até 12 horas, independentemente do status da sessão de login original. Esse comportamento garante que operações de CLI de longa duração ou sessões de console não sejam encerradas inesperadamente.

Formas de encerrar sessões de usuário final no IAM Identity Center

Iniciadas pelo usuário

Quando um usuário sai do portal de AWS acesso, a sessão de login termina, impedindo que o usuário acesse novos recursos.

As sessões de aplicação existentes, no entanto, não terminam instantaneamente. Em vez disso, eles terminarão em aproximadamente 30 minutos, quando tentarem a próxima atualização e descobrirem que a sessão de login não é mais válida. As sessões de perfil do IAM existentes continuam até expirarem com base na configuração do conjunto de permissões, o que pode ocorrer até 12 horas depois.

Iniciadas pelo administrador

Qualquer pessoa com permissões administrativas do IAM Identity Center na organização, geralmente administradores de TI ou equipes de segurança, pode [encerrar a sessão de um usuário](#). Essa ação funciona da mesma forma como se os usuários saíssem por conta própria, permitindo que os administradores exijam que os usuários façam login novamente quando necessário. Esse recurso é útil quando as políticas de segurança mudam ou quando atividades suspeitas são detectadas.

Quando um administrador do IAM Identity Center [exclui um usuário](#) ou [desabilita o acesso de um usuário](#), o usuário perde o acesso ao portal de acesso do AWS e é impedido de entrar novamente para iniciar uma nova sessão de aplicação ou perfil do IAM. Em 30 minutos, o usuário perderá acesso às sessões de aplicação existentes. Todas as sessões de perfil do IAM existentes continuarão com base na duração da sessão configurada no conjunto de permissões do IAM Identity Center. A duração máxima da sessão pode ser de 12 horas.

O que acontece com o acesso do usuário quando você encerra uma sessão

Essa referência fornece informações detalhadas sobre como as sessões do IAM Identity Center se comportam quando ações administrativas são tomadas. As tabelas nesta seção mostram a duração e os efeitos das ações de gerenciamento de usuários e das alterações de permissão no acesso ao portal de AWS acesso, aos aplicativos e às Conta da AWS sessões.

Gerenciamento de usuários

Esta tabela resume como as alterações no gerenciamento de usuários afetam o acesso a AWS recursos, sessões de aplicativos e sessões de AWS contas.

Ação	O usuário perde o acesso ao IAM Identity Center	O usuário não pode criar novas sessões de aplicação	O usuário não pode acessar as sessões de aplicação existentes	O usuário perde o acesso às Conta da AWS sessões existentes
Acesso do usuário desabilitado	Com efeito imediato	Com efeito imediato	Dentro de 30 minutos	Dentro de 12 horas ou menos. A duração depende do

Ação	O usuário perde o acesso ao IAM Identity Center	O usuário não pode criar novas sessões de aplicação	O usuário não pode acessar as sessões de aplicação existentes	O usuário perde o acesso às Conta da AWS sessões existentes
				tempo de expiração da sessão de perfil do IAM configurado para o conjunto de permissões.
Usuário excluído	Com efeito imediato	Com efeito imediato	Dentro de 30 minutos	Dentro de 12 horas ou menos. A duração depende do tempo de expiração da sessão de perfil do IAM configurado para o conjunto de permissões.
Sessão de usuário revogada	O usuário deve fazer login novamente para recuperar o acesso	Com efeito imediato	Dentro de 30 minutos	Dentro de 12 horas ou menos. A duração depende do tempo de expiração da sessão de perfil do IAM configurado para o conjunto de permissões.

Ação	O usuário perde o acesso ao IAM Identity Center	O usuário não pode criar novas sessões de aplicação	O usuário não pode acessar as sessões de aplicação existentes	O usuário perde o acesso às Conta da AWS sessões existentes
O usuário desconecta	O usuário deve fazer login novamente para recuperar o acesso	Com efeito imediato	Dentro de 30 minutos	Dentro de 12 horas ou menos. A duração depende do tempo de expiração da sessão de perfil do IAM configurado para o conjunto de permissões.

Associação a grupos

Esta tabela resume como as alterações nas permissões do usuário e nas associações de grupos afetam o acesso aos AWS recursos, às sessões do aplicativo e às sessões AWS da conta.

Ação	O usuário perde o acesso ao IAM Identity Center	O usuário não pode criar novas sessões de aplicação	O usuário não pode acessar as sessões de aplicação existentes	O usuário perde o acesso às Conta da AWS sessões existentes
Aplicativo ou Conta da AWS acesso removido do usuário	Não — o usuário pode continuar acessando o IAM Identity Center	Com efeito imediato	Dentro de 1 hora	Dentro de 12 horas ou menos. A duração depende do tempo de expiração da sessão de

Ação	O usuário perde o acesso ao IAM Identity Center	O usuário não pode criar novas sessões de aplicação	O usuário não pode acessar as sessões de aplicação existentes	O usuário perde o acesso às Conta da AWS sessões existentes
				perfil do IAM configurado para o conjunto de permissões.
Usuário removido do grupo que tinha uma aplicação ou Conta da AWS atribuída	Não — o usuário pode continuar acessando o IAM Identity Center	Dentro de 1 hora	Dentro de 2 horas	Dentro de 12 horas ou menos. A duração depende do tempo de expiração da sessão de perfil do IAM configurado para o conjunto de permissões.
Aplicativo ou Conta da AWS acesso removido do grupo	Não — o usuário pode continuar acessando o IAM Identity Center	Com efeito imediato	Dentro de 1 hora	Dentro de 12 horas ou menos. A duração depende do tempo de expiração da sessão de perfil do IAM configurado para o conjunto de permissões.

 Note

O portal de AWS acesso e AWS CLI refletirá as permissões de usuário atualizadas dentro de 1 hora após você adicionar ou remover um usuário desse grupo.

Noções básicas sobre diferenças de horário

- Com efeito imediato — Ações que exigem reautenticação imediata.
- Dentro de 30 minutos a 2 horas — As sessões de aplicação precisam de tempo para verificar com o IAM Identity Center e descobrir quaisquer alterações.
- Dentro de 12 horas ou menos — As sessões de perfil do IAM operam independentemente e só terminam quando a duração configurada expirar.

Logout único

O IAM Identity Center não é compatível com o SAML Single Logout (um protocolo que desconecta automaticamente os usuários de todas as aplicações conectadas quando eles fazem logout) iniciado por um provedor de identidade que atua como a [fonte de identidade](#). Além disso, ele não envia o SAML Single Logout para [aplicações SAML 2.0](#) que usam o IAM Identity Center como provedor de identidade.

Práticas recomendadas para o gerenciamento de uma sessão

O gerenciamento eficaz de sessão requer configuração e monitoramento cuidadosos. As organizações devem configurar as durações das sessões de acordo com os requisitos de segurança, geralmente usando durações mais curtas para aplicações e ambientes confidenciais.

A implementação de processos para encerrar as sessões quando os usuários mudam de cargo ou saem da organização é essencial para manter os limites de segurança. A análise regular das sessões ativas deve ser incorporada às práticas de monitoramento de segurança para detectar comportamentos anômalos que possam indicar problemas de segurança, como padrões de acesso incomuns, horários ou locais de login inesperados ou acesso a recursos fora das funções normais da tarefa.

Configurar a duração da sessão no IAM Identity Center

Você pode configurar a duração da sessão para os usuários da sua força de trabalho quando eles usam o Portal de acesso da AWS e os aplicativos que funcionam com o IAM Identity Center, incluindo o Kiro. O IAM Identity Center fornece os seguintes tipos de sessão: sessões interativas com o usuário, sessões em segundo plano do usuário e sessões estendidas para o Kiro.

Tópicos

- [Sessões interativas do usuário](#)
- [Sessões de usuário em segundo plano](#)
- [Sessões estendidas para Kiro](#)
- [Visualizar e encerrar sessões ativas para os usuários da força de trabalho](#)
- [Considerações sobre a duração da sessão para usar fontes de identidade, a AWS CLI e AWS SDKs](#)

Sessões interativas do usuário

As sessões interativas do usuário são sessões vinculadas ao login do usuário no portal de acesso ou ao AWS acesso aos aplicativos [AWS gerenciados](#). A duração da sessão de autenticação nos aplicativos Portal de acesso da AWS e é o tempo máximo em que um usuário pode se conectar sem se autenticar novamente. Se você encerrar uma sessão ativa do portal de AWS acesso, isso também encerrará todas as sessões desses aplicativos gerenciados.

Por padrão, a duração da sessão interativa do usuário é de 8 horas. Você pode especificar uma duração diferente, de um mínimo de 15 minutos a um máximo de 90 dias. Os valores de duração personalizados devem ser inseridos em minutos e estar entre 15 minutos e 129.600 minutos (90 dias). Para obter mais informações, consulte [Como entender as sessões de autenticação no IAM Identity Center](#).

Para considerações sobre como as fontes de identidade do IAM Identity Center podem afetar a duração da sessão interativa do usuário, consulte [the section called “Considerações sobre fontes de identidade, a AWS CLI e AWS SDKs”](#).

Para configurar a duração de uma sessão interativa do usuário

1. Abra o console do IAM Identity Center.

2. Escolha Configurações.
3. Na página Configurações, escolha a guia Autenticação.
4. Em Autenticação, ao lado de Duração da sessão, escolha Configurar. A caixa de diálogo Configurar duração da sessão é exibida.
5. Na caixa de diálogo Configurar duração da sessão, em Sessões interativas do usuário, escolha a duração máxima da sessão para os usuários selecionando a seta suspensa. Escolha a duração da sessão e escolha Salvar.

 Note

As alterações na duração da sessão se aplicam somente às novas sessões. As sessões atuais mantêm a duração original.

6. Você retornará à aba Autenticação. Uma mensagem de notificação verde aparece acima da aba indicando que as configurações da sessão foram atualizadas com sucesso.

Sessões de usuário em segundo plano

As sessões em segundo plano do usuário permitem que um usuário inicie um trabalho de longa duração em um aplicativo AWS gerenciado, como o [Amazon SageMaker Studio](#), sem que o usuário precise permanecer conectado enquanto o trabalho é executado. A tarefa é executada imediatamente e usa o recurso de [propagação de identidade confiável](#) do IAM Identity Center para garantir que as permissões do usuário sejam mantidas enquanto a tarefa é executada em segundo plano. O trabalho pode continuar em execução mesmo que o usuário desligue o computador, a sessão de login do IAM Identity Center expire ou o usuário saia do AWS portal de acesso. Esse recurso permite que cientistas de dados, engenheiros de machine learning e outros iniciem fluxos de trabalho de analytics e machine learning executados em segundo plano sem o envolvimento ativo do usuário.

As sessões em segundo plano do usuário são habilitadas por padrão para aplicativos AWS gerenciados compatíveis, como o Amazon SageMaker Studio. Para usar esse recurso, no entanto, você deve habilitar a propagação de identidade confiável no Amazon SageMaker Studio ao criar ou atualizar um domínio. Para obter mais informações, consulte [Habilitar a propagação de identidade confiável em seu domínio Amazon SageMaker AI](#).

A duração padrão das sessões de usuários em segundo plano é de 7 dias. Você pode especificar uma duração diferente, de um mínimo de 15 minutos a um máximo de 90 dias. Os valores de

duração personalizados devem ser inseridos em minutos e estar entre 15 minutos e 129.600 minutos (90 dias).

Lembre-se dos seguintes fatores para as sessões de usuários em segundo plano:

- Uma sessão em segundo plano do usuário só pode ser criada quando um usuário inicia manualmente um trabalho no Amazon SageMaker Studio. Esse recurso não é compatível com fluxos de trabalho automatizados e programados.
- Para obter uma lista de AWS regiões que oferecem suporte a sessões em segundo plano do usuário, consulte [AWS Regiões suportadas](#).
- Você pode ver as sessões em segundo plano do usuário em CloudTrail. Para obter informações, consulte [Como identificar dos detalhes da sessão de usuário em segundo plano](#).
- Você também pode encerrar sessões ativas para um usuário na organização. Para obter informações, consulte [Encerrar sessões ativas para os usuários da força de trabalho](#).

Para configurar a duração de uma sessão de usuário em segundo plano

1. Abra o console do IAM Identity Center.
2. Escolha Configurações.
3. Na página Configurações, escolha a guia Autenticação.
4. Em Autenticação, ao lado de Duração da sessão, escolha Configurar. A caixa de diálogo Configurar duração da sessão é exibida.
5. Na caixa de diálogo Configurar duração da sessão, se a caixa de seleção Habilitar sessões de usuários em segundo plano ainda não estiver marcada, selecione-a. Desmarque a caixa de seleção para desabilitar as sessões de usuários em segundo plano.

 Note

As sessões atuais não serão afetadas se você desabilitar as sessões de usuários em segundo plano.

6. Em Sessões de usuários em segundo plano, escolha a duração máxima da sessão selecionando a seta suspensa. Escolha a duração da sessão e escolha Salvar.

Note

As alterações na duração da sessão se aplicam somente às novas sessões. As sessões atuais mantêm a duração original.

7. Você retornará à aba Autenticação. Uma mensagem de notificação verde aparece acima da aba indicando que as configurações da sessão foram atualizadas com sucesso.

Note

Uma aplicação gerenciada pelo cliente não pode criar uma sessão de usuário em segundo plano.

Sessões estendidas para Kiro

Se seus desenvolvedores usam o Kiro como parte de um ambiente de desenvolvimento integrado (IDE), você pode definir a duração da sessão do Kiro para 90 dias. Dependendo de quando você ativou o IAM Identity Center, a duração estendida da sessão do Kiro pode estar ativada por padrão. Essa sessão estendida não afeta a duração da sessão do portal de AWS acesso ou de outros aplicativos AWS gerenciados.

Para considerações sobre como as fontes de identidade do IAM Identity Center podem afetar a duração estendida da sessão, consulte [the section called “Considerações sobre fontes de identidade, a AWS CLI e AWS SDKs”](#).

Note

O Kiro pode ser acessado a partir de consoles configurados como comerciais Regiões da AWS que são ativados por padrão. Se sua instância do IAM Identity Center estiver localizada em uma região onde o Kiro não está acessível no momento, habilitar a duração estendida da sessão de 90 dias não substituirá a configuração padrão. Isso significa que a duração da sessão permanecerá inalterada, independentemente de você habilitar ou não a duração da sessão estendida de 90 dias. Para obter informações, [AWS Regiões suportadas pelo Kiro](#).

Para estender uma sessão para Kiro

1. Abra o console do IAM Identity Center.
2. Escolha Configurações.
3. Na página Configurações, escolha a guia Autenticação.
4. Em Autenticação, ao lado de Duração da sessão, escolha Configurar. A caixa de diálogo Configurar duração da sessão é exibida.
5. Na caixa de diálogo Configurar duração da sessão, marque a caixa de seleção Habilitar sessões estendidas para o Kiro. Desmarque a caixa de seleção para desativar as sessões estendidas do Kiro.
6. Escolha Salvar para voltar para a página Configurações.

Visualizar e encerrar sessões ativas para os usuários da força de trabalho

O administrador do IAM Identity Center pode ver a lista das sessões ativas dos usuários da força de trabalho e, se exigido, encerrar uma ou mais sessões para um usuário. Por exemplo, talvez seja necessário encerrar as sessões de um usuário quando:

- O usuário não precisa mais das sessões.
- O usuário não deve manter o estado de autenticação atual. Isso pode ocorrer quando alguém sai da empresa ou quando as permissões são alteradas.

Você pode visualizar e encerrar essas sessões usando o console do IAM Identity Center. Seus usuários também podem visualizar e encerrar suas próprias sessões usando o portal de AWS acesso. Para obter informações sobre como os usuários da força de trabalho podem visualizar e encerrar as sessões sem a ajuda de um administrador, consulte [Como visualizar e encerrar a sessão ativa](#).

Note

Encerrar uma sessão ativa para um usuário do IAM Identity Center não encerra nenhuma sessão ativa da função do IAM no Console de gerenciamento da AWS ou AWS CLI. Para obter mais informações, consulte [Como entender as sessões de autenticação no IAM Identity Center](#).

Para encerrar uma sessão ativa para um usuário da força de trabalho (console do IAM Identity Center)

1. Abra o console do IAM Identity Center.
2. Selecione Usuários.
3. Na página Usuários, escolha o nome 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 desse usuário.
5. Pesquisar sessões de usuários em segundo plano (opcional)

Para pesquisar sessões pelo nome do recurso da Amazon (ARN) da tarefa que está usando a sessão, na lista Tipo de sessão, escolha Sessões de usuários em segundo plano e insira o ARN da tarefa na caixa de pesquisa.

 Note

Você só pode encerrar as sessões ativas que estão carregadas. Se um usuário tiver muitas sessões, escolha Carregar mais sessões ativas para exibir sessões adicionais.

6. Marque a caixa de seleção ao lado de cada sessão que você deseja encerrar e escolha Encerrar sessões.
7. É exibida uma caixa de diálogo que confirma que você está excluindo sessões ativas para esse usuário. Revise as informações e, se quiser continuar, digite `confirm` e escolha Encerrar sessões.
8. Você é levado de volta à página do usuário. Uma mensagem de notificação verde será exibida indicando que as sessões selecionadas foram encerradas com sucesso.

Considerações sobre a duração da sessão para usar fontes de identidade, a AWS CLI e AWS SDKs

A seguir estão algumas considerações para configurar a duração da sessão se você usar o Microsoft Active Directory (AD) ou um provedor de identidade externo (IdP) como fonte de identidade, ou os AWS Command Line Interface Kits de Desenvolvimento de AWS Software (SDKs) ou outras ferramentas de desenvolvimento para acessar serviços de forma AWS programática. AWS

Microsoft Active Directory, sessões interativas com o usuário e sessões estendidas para Kiro

Se você usa o Microsoft Active Directory (AD) como fonte de identidade e configura a duração da sessão para sessões interativas com o usuário ou sessões estendidas para o Kiro, lembre-se das seguintes considerações.

Note

Essas considerações não se aplicam às sessões de usuários em segundo plano.

Independentemente de você usar AWS Managed Microsoft AD ou configurar o AD Connector AWS Directory Service, a vida útil máxima dos tíquetes Kerberos de usuário definidos no Microsoft AD pode afetar por quanto tempo as sessões interativas do usuário e as sessões estendidas do Kiro são válidas. Para obter mais informações sobre essa configuração, consulte [Vida útil máxima do ticket de usuário](#) no site da Microsoft.

- **AWS Managed Microsoft AD:** Se você usa o AWS Managed Microsoft AD configure in AWS Directory Service, a vida útil máxima dos tíquetes Kerberos do usuário é fixada em 10 horas. Portanto, a duração da sessão interativa do usuário é definida como a menor que a configuração do IAM Identity Center e 10 horas. Por exemplo, se você definir a duração da sessão interativa do usuário para 12 horas, seus usuários deverão se autenticar novamente no portal de AWS acesso após 10 horas. O mesmo limite de 10 horas se aplica às sessões prolongadas do Kiro.
- **AD Connector:** Se você usa o AD Connector configurado em AWS Directory Service, a vida útil máxima dos tíquetes Kerberos do usuário é definida no Microsoft AD por trás do AD Connector. O valor padrão é 10 horas e tem o mesmo efeito nas sessões interativas do usuário e nas sessões estendidas que as de AWS Managed Microsoft AD. Embora esse limite possa ser configurado no Microsoft AD, recomendamos que você trabalhe com seu administrador de TI para considerar os riscos, especialmente porque essa configuração pode afetar a duração da sessão de outros aplicativos cliente do Microsoft AD.

Provedores de identidade externos, sessões interativas com o usuário e sessões estendidas para Kiro

Se você usa um provedor de identidade externo (IdP) e configura a duração da sessão para sessões interativas com o usuário ou sessões estendidas para o Kiro, lembre-se das seguintes considerações.

Note

Essas considerações não se aplicam às sessões de usuários em segundo plano.

O IAM Identity Center usa o atributo `SessionNotOnOrAfter` das asserções 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 (interativa com o usuário) e de uma sessão estendida 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. Da mesma forma, se você definir uma sessão estendida de 90 dias para o Kiro, seus usuários do Kiro precisarão se autenticar novamente após 90 dias.
- Se `SessionNotOnOrAfter` for passado em uma declaração SAML, o valor da duração da sessão será definido como a menor duração da sessão do portal de AWS acesso (interativa com o usuário) ou a duração da sessão estendida 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. Da mesma forma, se você definir uma sessão estendida de 90 dias para o Kiro, seus usuários do Kiro precisarão se autenticar novamente no Kiro após 18 horas.
- Se a duração da sessão do IdP for maior do que a definida no IAM Identity Center, os usuários poderão iniciar uma nova sessão do IAM Identity Center sem reinserir suas credenciais, com base em sua sessão de login ainda válida no IdP.

AWS CLI e sessões de SDK

Se você estiver usando a AWS CLI 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 acesso e os AWS aplicativos gerenciados. AWS SDKs AWS

- 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 AWS configuração 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 do 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

Note

Para casos de uso de acesso à conta, 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 em 20 horas, enquanto a duração do conjunto de permissões estiver definida em 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 SDKs que oferecem suporte ao gerenciamento de sessões do IAM Identity Center

A seguir estão as versões mínimas do 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: 1.18.0 credentials/v1.13.0, config/v
JS V2	2.1253.0
JS V3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

Desative o acesso do usuário Contas da AWS e os aplicativos 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. A desativação do acesso do usuário impede que eles entrem no portal de AWS acesso e eles não terão mais acesso aos aplicativos atribuídos Contas da AWS e aos aplicativos. Use desabilitar o acesso do usuário para remover temporariamente o acesso quando precisar restaurar o acesso posteriormente.

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 obter mais informações, consulte [Como entender as sessões de autenticação no IAM Identity Center](#).

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 [Centro de Identidade do AWS IAM](#). 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 desabilitar, na seção Informações gerais, escolha Desabilitar o acesso do usuário.
5. Na caixa de diálogo Desabilitar acesso do usuário, escolha Desabilitar acesso do usuário.

Negar acesso do usuário com Políticas de controle de serviço

Para negar imediatamente o acesso para fazer chamadas de API autorizadas quando o acesso de um usuário do IAM Identity Center for desabilitado ou o usuário for excluído, você pode:

1. [Adicionar ou atualizar](#) a [política embutida](#) dos conjuntos de permissões atribuídos ao usuário adicionando um efeito Deny explícito para todas as ações em todos os recursos.
2. Especifique a chave de condição `aws:userid` ou `identitystore:userid`

Como alternativa, você pode usar uma [Política de controle de serviço](#) para negar o acesso do usuário a todas as contas membros da organização.

Example Exemplo de SCP para negar acesso

Essa política de negação bloqueia todas AWS as ações de um usuário específico, independentemente de outras permissões que ele possa ter recebido em outro lugar. Essa política substitui todas as políticas Allow.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "aws:UserId": "*:deleteduser@domain.com"
        }
      }
    }
  ]
}
```

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "identitystore:UserId": "DELETEDUSER_ID"
        }
      }
    }
  ]
}
```

```
}  
  }  
    ]  
      }
```

Como gerenciar o acesso para usuários do diretório do Identity Center

Saiba mais como gerenciar senhas e autenticação multifator (MFA) para usuários no diretório do IAM Identity Center. Esses atributos de segurança ajudam a proteger as contas dos usuários.

Note

Esses atributos não se aplicam a usuários do Active Directory ou usuários de provedores de identidade externos.

Os administradores podem gerenciar senhas e MFA por meio do console do IAM Identity Center. Esses atributos de segurança funcionam somente com o diretório integrado do Identity Center.

Gerenciamento de senhas

O gerenciamento de senhas inclui os seguintes recursos:

- Redefinir senhas com instruções por e-mail
- Gerar senhas de uso único
- Configurar verificação automática de e-mail para usuários criados pela API

AWS impõe requisitos fixos de segurança, incluindo regras de complexidade e restrições de reutilização de senhas.

MFA

A MFA é habilitada por padrão e oferece suporte a até oito dispositivos por usuário.

Os tipos de dispositivos compatíveis incluem:

- Aplicativos de autenticador
- Chaves de segurança
- Autenticadores biométricos integrados

Os administradores podem registrar e gerenciar dispositivos de MFA para usuários.

Tópicos

- [Como configurar senhas de usuário](#)
- [MFA para usuários do diretório do Identity Center](#)

Como configurar senhas de usuário

Para usuários criados no diretório do Identity Center, os administradores podem gerenciar políticas de senha, lidar com usuários sem senhas iniciais e redefinir senhas quando necessário. Esses atributos de gerenciamento de senhas se aplicam somente aos usuários no diretório integrado do Identity Center. Se você estiver usando o Active Directory ou um provedor de identidade externo, deverá gerenciar senhas nesses sistemas.

Opções de gerenciamento de senhas

- Requisitos de senha — Requisitos de segurança que os usuários devem atender ao definir ou alterar senhas. Isso inclui regras de complexidade e restrições de reutilização.
- Configuração de senha única — Configure a verificação de e-mail para usuários criados por meio de API ou CLI que não têm senhas iniciais. Você também pode gerar senhas temporárias para acesso imediato.
- Redefinições de senha — Redefina as senhas para usuários que estão bloqueados ou precisam de novas credenciais. Você pode enviar instruções de redefinição por e-mail ou gerar senhas de uso único.

Tópicos

- [Requisitos de senha ao gerenciar identidade no IAM Identity Center](#)
- [Enviar uma senha de uso único por e-mail para os usuários criados com a API ou CLI](#)
- [Redefinir a senha de usuário do IAM Identity Center para um usuário final](#)

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 outra fonte de identidades, não o IAM Identity Center, para autenticação, como o [Active Directory](#) ou um [provedor de identidades externo](#), as políticas de senha para os usuários serão 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 de comprimento.
- A senha deve conter pelo menos um caractere de cada uma das quatro seguintes categorias:
 - 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.

Enviar uma senha de uso único por e-mail para os usuários criados com a API ou CLI

Quando você cria usuários com a operação da API [CreateUser](#) ou o comando da CLI `create-user`, eles não têm senhas. Você poderá atualizar as configurações no IAM Identity Center para enviar a esses usuários um e-mail de verificação após a primeira tentativa de login, se tiver especificado um e-mail para o usuário quando ele foi criado. Depois de receber o e-mail de verificação, o usuário deve definir uma senha para fazer login.

Se você não habilitar essa configuração, deverá [gerar uma senha de uso único](#) e compartilhá-la com os usuários que você criar usando a API `CreateUser` ou o comando da CLI `create-user`.

Para enviar a senha de uso único para os usuários criados com o comando CreateUser da API ou **create-user** da CLI

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. Na caixa de diálogo Configurar autenticação padrão, marque a caixa de seleção Enviar e-mail OTP. Depois, escolha Salvar. O status é atualizado de Desabilitado para Habilitado.

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 a própria senha do IAM Identity Center, consulte [Redefinindo sua senha de usuário do portal de AWS acesso](#).

Redefinir a senha de um usuário final do IAM Identity Center

Important

As instruções nesta página aplicam-se a [Centro de Identidade do AWS IAM](#). 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.

MFA para usuários do diretório do Identity Center

 Important

Atualmente, o MFA no IAM Identity Center não é compatível com [provedores de identidade externos](#).

O IAM Identity Center é pré-configurado com a autenticação multifator (MFA) ativada por padrão para que todos os usuários precisem fazer login com a MFA além do nome de usuário e a senha. Isso garante que os usuários devam entrar no portal de AWS acesso usando os dois fatores a seguir:

- 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 AWS recursos, 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](#).

Tópicos

- [Tipos de MFA disponíveis para o IAM Identity Center](#)
- [Configurar MFA no IAM Identity Center](#)
- [Registrar um dispositivo de MFA para os usuários](#)
- [Renomeação e exclusão de dispositivos de MFA no IAM Identity Center](#)

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.

- [FIDO2 autenticadores](#), incluindo autenticadores e chaves de segurança integrados
- [Aplicativos de autenticação virtual](#)
- Sua própria [RADIUS MFA](#) implementação conectada por AWS Managed Microsoft AD

Um usuário pode ter até oito dispositivos de MFA, que incluem até duas aplicações autenticadoras virtuais e seis autenticadores FIDO, registrados em uma Conta da AWS. Você também pode definir as configurações de MFA para exigir MFA sempre que eles tentarem fazer login em um novo dispositivo ou navegador, ou ao fazer login de um endereço IP desconhecido. Para obter mais informações sobre como configurar o MFA para seus usuários, consulte [Escolher tipos de MFA para autenticação de usuário](#) e [Configurar a imposição de dispositivos de MFA](#).

FIDO2 autenticadores

[FIDO2](#) é um padrão que inclui CTAP2 [WebAuthn](#) e se baseia 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.

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 Feitian, YubiKeys 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. Duas aplicações autenticadoras podem ser registradas 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 do setor que fornece gerenciamento de autenticação, autorização e contabilidade para que os usuários possam se conectar aos serviços de rede. Directory Service inclui um cliente RADIUS que se conecta ao servidor RADIUS no qual você implementou sua solução de 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 AWS deseja a autenticação nativa 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 Directory Service com os quais funcionam, como o Amazon RDS for SQL Server.

Se seu MFA estiver desativado no console do IAM Identity Center e você tiver configurado o RADIUS MFA com Directory Service, o RADIUS MFA controla o login no portal de acesso. AWS Isso significa que o IAM Identity Center retornará à configuração RADIUS MFA se o MFA estiver desativado.

Configurar MFA no IAM Identity Center

Você pode configurar os recursos de autenticação multifator (MFA) no IAM Identity Center quando sua fonte de identidade está configurada com o repositório de identidades do IAM Identity Center ou o AWS Managed Microsoft AD AD Connector. Atualmente, o MFA no IAM Identity Center não é compatível com [provedores de identidade externos](#).

A seguir estão as recomendações gerais de MFA, dependendo das configurações do IAM Identity Center e das preferências organizacionais.

- 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 Exigir que eles forneçam uma senha de uso único enviada por e-mail 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 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](#).
- O YouTube vídeo a seguir fornece uma visão geral do MFA e do IAM Identity Center:

[IAM Identity Center: padrões de autenticação multifatorial para novas instâncias](#)

Tópicos

- [Solicite aos usuários o MFA](#)
- [Escolher tipos de MFA para autenticação de usuário](#)
- [Configurar a imposição de dispositivos de MFA](#)
- [Permita que os usuários registrem seus próprios dispositivos de MFA](#)

Solicite aos usuários o MFA

Você pode usar as etapas a seguir para determinar com que frequência os usuários da força de trabalho são solicitados a usar a autenticação multifator (MFA) sempre que tentam entrar no portal de acesso. AWS Antes de começar, recomendamos que você entenda o [Tipos de MFA disponíveis para o IAM Identity Center](#).

 Important

As instruções da presente seção aplicam-se a [Centro de Identidade do AWS IAM](#). 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 Guide AWS Identity and Access Management .

 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 configurar 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:

- Toda vez que eles fazem login (sempre ativo)

Nesse modo (a configuração padrão), o IAM Identity Center exige que os usuários com um dispositivo de MFA registrado sejam avisados sempre que fizerem login. Essa é a configuração mais segura e garante que suas políticas organizacionais ou de conformidade sejam aplicadas, exigindo que o MFA seja usado sempre que eles 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.

- Somente quando o contexto de login muda (sensível ao contexto)

Nesse modo, o IAM Identity Center oferece aos usuários a opção de confiar nos 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, mas é menos seguro do que a opção sempre ativa. Os usuários só receberão uma solicitação de MFA se o contexto de login mudar.

- Nunca (desativado)

Nesse modo, todos os usuários entrarão somente com seu nome de usuário e senha padrão. Escolher esta opção desabilita a MFA do IAM Identity Center e não é recomendada.

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

Note

Se você já estiver usando o RADIUS MFA 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 Salvar alterações.

Related Topics

- [Escolher tipos de MFA para autenticação de usuário](#)
- [Configurar a imposição de dispositivos de MFA](#)
- [Permita que os usuários registrem seus próprios dispositivos de MFA](#)

Escolher tipos de MFA para autenticação de usuário

Use o procedimento a seguir para escolher os tipos de dispositivos com os quais seus usuários podem se autenticar quando solicitados a autenticação multifator (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 e chaves de segurança integrados
 - Aplicativos de autenticador
6. Escolha Salvar alterações.

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 obter mais informações sobre MFA no IAM, consulte [Código da autenticação multifator no IAM da 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 AWS ambientes da sua organização com a 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 AWS acesso. 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

Os administradores do IAM Identity Center podem permitir que os 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 Salvar alterações.

 Note

Depois de configurar o autorregistro para seus usuários, talvez você queira enviar a eles um link para o procedimento [Registro de um dispositivo para MFA](#). Este tópico fornece instruções sobre como configurar os próprios dispositivos MFA.

Registrar um dispositivo de MFA para os usuários

Os administradores do IAM Identity Center podem configurar um novo dispositivo de MFA para o acesso de um usuário específico no console do IAM Identity Center. Você deve ter acesso físico ao dispositivo de 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, depois, use o app para digitalizar o código de QR. Por exemplo, você pode escolher o ícone de câmera ou escolher uma opção

semelhante a Digitalizar código. 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 (time-based one-time passwords, TOTP) expiram após um curto período. Caso isso ocorra, você pode resincronizar 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

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 .

Renomeação e exclusão de dispositivos de MFA no IAM Identity Center

Os administradores do IAM Identity Center podem usar os procedimentos a seguir para 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.

Configurar o acesso a aplicações

Com Centro de Identidade do AWS IAM, 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 do aplicativo APIs. 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 Console de gerenciamento da AWS ao formulário específico Conta da AWS em sua organização. Para obter mais informações, consulte [Configurar o acesso a Contas da AWS](#).

Tópicos

- [AWS aplicativos gerenciados](#)
- [Aplicações gerenciadas pelo cliente](#)
- [Visão geral da propagação de identidades confiáveis](#)
- [Configurando seu próprio aplicativo OAuth 2.0](#)
- [Fazer o rodízio de certificados do IAM Identity Center](#)
- [Compreender as propriedades da aplicação no console do IAM Identity Center](#)
- [Atribuir acesso de usuário às aplicações no console do IAM Identity Center](#)
- [Remover o acesso dos usuários a aplicações SAML 2.0](#)
- [Mapear atributos em sua aplicação para atributos do IAM Identity Center](#)

AWS aplicativos gerenciados

Centro de Identidade do AWS IAM agiliza e simplifica a tarefa de conectar os usuários da sua força de trabalho a aplicativos AWS gerenciados, como o Kiro e o Amazon Quick. Com o IAM Identity Center, você pode conectar seu provedor de identidades existente uma vez e sincronizar usuários e grupos do seu diretório, ou criar e gerenciar os usuários diretamente no IAM Identity Center. Fornecendo um único ponto de federação, o IAM Identity Center elimina a necessidade de configurar a federação ou a sincronização de usuários e grupos para cada aplicação, e reduz seu esforço administrativo. Você também tem uma [visão comum das tarefas dos usuários e grupos](#).

Para obter uma tabela de AWS aplicativos que funcionam com o IAM Identity Center, consulte [AWS aplicativos gerenciados que você pode usar com o IAM Identity Center](#).

Controle do acesso a aplicativos AWS gerenciados

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. O administrador da aplicação pode escolher se deseja exigir atribuições a uma aplicação.

Se forem necessárias atribuições, quando os usuários fizerem login no portal de acesso Portal de acesso da AWS, apenas os usuários atribuídos à aplicação diretamente ou por meio de uma atribuição de grupo poderão visualizar o bloco da aplicação.

Se atribuições não forem necessárias, você poderá permitir que todos os usuários do IAM Identity Center façam login na aplicação. Nesse caso, a aplicação gerencia o acesso aos recursos, e o bloco da aplicação fica visível para todos os usuários que visitam o portal de acesso Portal de acesso da AWS.

Important

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.

- Acesso aos recursos da aplicação

A aplicação gerencia isso por meio de atribuições de recursos independentes que ela controla.

AWS os aplicativos gerenciados fornecem uma interface de usuário administrativa que você pode usar para gerenciar o acesso aos recursos do aplicativo. Por exemplo, os administradores do Quick podem designar usuários para acessar painéis com base na associação ao grupo. A maioria dos aplicativos AWS gerenciados também fornece uma Console de gerenciamento da AWS 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.

Compartilhamento de informações de identidade

Considerações sobre o compartilhamento de informações de identidade no Contas da AWS

O IAM Identity Center é compatível com os atributos mais usados em todas 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 uma dessas duas maneiras:

- Você pode optar por ativar o acesso somente na conta AWS Organizations de gerenciamento ou em todas as contas em AWS Organizations.
- Como alternativa, você pode usar políticas de controle de serviço (SCPs) para controlar quais aplicativos podem acessar as informações em quais contas estão 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 ativar o acesso em todas as contas, poderá usar SCPs para proibir o acesso de todos os aplicativos, exceto aqueles que você deseja permitir.

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.

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 (CLI). Para obter mais informações, consulte [Gerenciar usuários no diretório do 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 [Diretório Microsoft AD](#).
 - Provedor de identidades externo: para obter mais informações, consulte [Provedores de identidades externos](#).

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.

Restringindo o uso de aplicativos AWS gerenciados

Quando você habilita o IAM Identity Center pela primeira vez, ele se torna disponível como uma fonte de identidade para aplicações gerenciadas pela AWS em todas as suas contas no AWS

Organizations. Para restringir os aplicativos, você deve implementar políticas de controle de serviço (SCPs). SCPs são um recurso AWS Organizations que você pode usar para controlar centralmente o máximo de permissões que as identidades (usuários e funções) em sua organização podem ter. Você pode usar SCPs para bloquear o acesso às informações de usuários e grupos do IAM Identity Center e impedir que o aplicativo seja iniciado, exceto nas contas designadas. Para obter mais informações, consulte [Políticas de controle de serviço \(SCPs\)](#) no Guia AWS Organizations do usuário.

O exemplo de SCP a seguir bloqueia o acesso às informações de usuário e grupo do IAM Identity Center e impede que a aplicação seja iniciado, exceto em contas designadas (111111111111 e 222222222222):

```
{
  "Sid": "DenyIdCExceptInDesignatedAWSAccounts",
  "Effect": "Deny",
  "Action": [
    "identitystore:*",
    "sso:*",
    "sso-directory:*",
    "sso-oauth:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": [
        "111111111111",
        "222222222222"
      ]
    }
  }
}
```

AWS aplicativos gerenciados que você pode usar com o IAM Identity Center

O IAM Identity Center permite que você conecte a fonte de identidade existente ou crie usuários uma vez. Isso permite que os administradores de aplicativos gerenciem o acesso aos seguintes aplicativos AWS gerenciados sem federação separada ou sincronização de usuários e grupos.

Todos os aplicativos AWS gerenciados na tabela a seguir se integram às [instâncias organizacionais do IAM Identity Center](#). A tabela também fornece informações sobre o seguinte para um aplicativo AWS gerenciado compatível:

- Se a aplicação também se integra a uma instância de conta do IAM Identity Center
- Se a aplicação pode habilitar a propagação de identidade confiável por meio do IAM Identity Center
- Se a aplicação é compatível com o IAM Identity Center configurado com uma chave KMS gerenciada pelo cliente
- Se o aplicativo oferece suporte à implantação em regiões adicionais do IAM Identity Center

Note

Os aplicativos que oferecem suporte à implantação em regiões adicionais do IAM Identity Center também oferecem suporte ao IAM Identity Center configurado com uma chave KMS gerenciada pelo cliente. Cada aplicativo AWS gerenciado listado aqui oferece suporte à implantação na região principal. Para obter mais informações, consulte [the section called “Implantação e gerenciamento de aplicativos AWS gerenciados em várias Regiões da AWS”](#).

AWS aplicativos gerenciados que se integram ao IAM Identity Center

AWS aplicativo gerenciado	Integradas com uma instância de conta do IAM Identity Center	Permite a propagação de identidades confiáveis por meio do IAM Identity Center	Compatível com o IAM Identity Center configurado com uma chave KMS gerenciada pelo cliente	Oferece suporte à implantação em regiões adicionais do IAM Identity Center
SQL do Amazon Athena	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
Amazon CodeCatalyst	Sim	Não	Sim	Não

AWS aplicativo gerenciado	Integradas com uma instância de conta do IAM Identity Center	Permite a propagação de identidades confiáveis por meio do IAM Identity Center	Compatível com o IAM Identity Center configurado com uma chave KMS gerenciada pelo cliente	Oferece suporte à implantação em regiões adicionais do IAM Identity Center
Amazon DataZone	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
Recursos do Amazon EKS	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
Amazon EMR no EC2	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
Amazon EMR no EKS	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
Amazon EMR Sem Servidor	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
Amazon EMR Studio	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
Amazon Kendra	Não	Não	Sim	Não
Amazon Managed Grafana	Não	Não	Sim	Não
Amazon Monitron	Não	Nº	Nº	Nº
OpenSearch Serviço Amazon	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não

AWS aplicativo gerenciado	Integrada s com uma instância de conta do IAM Identity Center	Permite a propagação de identidade es confiáveis s por meio do IAM Identity Center	Compatível com o IAM Identity Center configura do com uma chave KMS gerenciada pelo cliente	Oferece suporte à implantação em regiões adicionais do IAM Identity Center
OpenSearch Serviço Amazon Serverless Service	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
Amazon Q Business	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
Amazon Quick	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
banco de dados de origem	Sim ²	Yes (Sim)	Yes (Sim)	Yes (Sim)
Amazon S3 Access Grants	Yes (Sim)	Yes (Sim)	Yes (Sim)	Yes (Sim)
SageMaker Estúdio Amazon	Não	Yes (Sim)	Yes (Sim)	Não
Amazon SageMaker Unified Studio	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
Amazon WorkMail	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
Amazon WorkSpaces	Sim	Não	Sim	Não
Amazon WorkSpaces Secure Browser	Não	Não	Sim	Não

AWS aplicativo gerenciado	Integrada s com uma instância de conta do IAM Identity Center	Permite a propagação de identidade es confiáveis s por meio do IAM Identity Center	Compatível com o IAM Identity Center configura do com uma chave KMS gerenciada pelo cliente	Oferece suporte à implantação em regiões adicionais do IAM Identity Center
AWS App Studio	Sim	Não	Nº	Não
AWS Deadline Cloud	Sim	Não	Yes (Sim)	Yes (Sim)
AWS Glue	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
AWS IoT Events	Nº	Nº	Nº	Nº
AWS IoT SiteWise	Nº	Nº	Nº	Não
AWS Lake Formation	Yes (Sim)	Yes (Sim)	Yes (Sim)	Yes (Sim)
AWS re:Post Privado	Yes (Sim)	Não	Sim	Não
Cadeia de Suprimentos AWS	Sim	Não	Sim	Não
AWS Systems Manager	Nº	Não	Sim	Sim - Desktop remoto do Fleet Manager

AWS aplicativo gerenciado	Integradas com uma instância de conta do IAM Identity Center	Permite a propagação de identidades confiáveis por meio do IAM Identity Center	Compatível com o IAM Identity Center configurado com uma chave KMS gerenciada pelo cliente	Oferece suporte à implantação em regiões adicionais do IAM Identity Center
AWS Transfer Family aplicativos da web	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não
AWS Transformação	Sim	Não	Sim	Não
Acesso Verificado pela AWS	Nº	Não	Sim	Não
Kiro	Sim ¹	Yes (Sim)	Yes (Sim)	Não
Aprovação Multilateral	Não	Yes (Sim)	Yes (Sim)	Não
OpenSearch user interface (Dashboards)	Yes (Sim)	Yes (Sim)	Yes (Sim)	Não

¹ Para o Kiro, as instâncias de conta do IAM Identity Center são suportadas, a menos que seus usuários precisem acessar o conjunto completo de recursos do Kiro nos AWS sites. Para obter mais informações, consulte [Configurando o Kiro](#) no Guia do usuário do Kiro.

² Para o Amazon Redshift, as instâncias de conta do IAM Identity Center são suportadas, exceto para aplicativos como o Query Editor v2, que exigem conjuntos de permissões, que não são compatíveis com instâncias de conta.

 Note

Alguns AWS serviços, como o Amazon Connect, não AWS Client VPN estão listados nesta tabela, embora você possa usá-los com o IAM Identity Center. Isso ocorre porque eles se integram ao IAM Identity Center usando exclusivamente SAML e, portanto, são categorizados como aplicativos [gerenciados pelo cliente](#).

Início rápido: configuração do IAM Identity Center para testar aplicativos AWS gerenciados

Se seu administrador ainda não tiver fornecido acesso ao IAM Identity Center, você pode usar as etapas deste tópico para configurar o IAM Identity Center para testar aplicativos AWS gerenciados. Você aprenderá como habilitar o IAM Identity Center, criar um usuário diretamente no IAM Identity Center e atribuir esse usuário a um aplicativo AWS gerenciado.

Este tópico fornece etapas de início rápido sobre como habilitar o IAM Identity Center de uma das seguintes formas:

- Com AWS Organizations — Se você escolher essa opção, uma instância organizacional do IAM Identity Center será criada.
- Somente no seu caso específico Conta da AWS — Se você escolher essa opção, uma instância de conta do IAM Identity Center será criada.

Para obter informações sobre esses tipos de instâncias, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

Pré-requisitos

Antes de habilitar o IAM Identity Center, confirme o seguinte:

- Você tem um Conta da AWS — Se você não tiver um Conta da AWS, consulte [Introdução a um Conta da AWS](#) no Guia de referência de gerenciamento de AWS contas.
- O aplicativo AWS gerenciado funciona com o IAM Identity Center — revise a lista [AWS aplicativos gerenciados que você pode usar com o IAM Identity Center](#) para confirmar se o aplicativo AWS gerenciado que você deseja testar funciona com o IAM Identity Center.

- Você analisou as considerações regionais — Certifique-se de que o aplicativo AWS gerenciado que você deseja testar seja compatível com o local em Região da AWS que você habilita o IAM Identity Center. Para obter mais informações, consulte a documentação da aplicação gerenciada pela AWS .

 Note

Você deve implantar seu aplicativo AWS gerenciado na mesma região em que planeja ativar o IAM Identity Center.

Configurar uma instância organizacional do IAM Identity Center para testar aplicativos AWS gerenciados

 Note

Este tópico descreve como habilitar o IAM Identity Center com AWS Organizations, que é a forma recomendada de habilitar o IAM Identity Center.

Confirmar as permissões

Para habilitar o IAM Identity Center com AWS Organizations, você deve entrar no AWS Management Console usando uma das seguintes opções:

- Um usuário com permissões administrativas na Conta da AWS em que o IAM Identity Center será habilitado com o AWS Organizations.
- O usuário-raiz (não recomendado, a menos que não existam outros usuários administrativos).

 Important

O usuário root tem acesso a todos os AWS serviços e recursos da conta. Como prática recomendada de segurança, a menos que você não tenha outras credenciais, não use as credenciais raiz da sua conta para acessar AWS recursos. Estas credenciais fornecem acesso ilimitado à conta e são difíceis de revogar.

Etapa 1. Ative o IAM Identity Center com AWS Organizations

1. Realize um dos procedimentos a seguir para fazer login no Console de gerenciamento da AWS.
 - 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, insira a senha.
 - Já está usando AWS com uma conta independente Conta da AWS (credenciais do IAM) — Faça login usando suas credenciais do IAM com permissões administrativas.
2. Na página inicial do AWS Management Console, selecione o serviço IAM Identity Center ou navegue até o [console do IAM Identity Center](#).
3. Escolha Ativar e habilite o IAM Identity Center com AWS Organizations. Ao fazer isso, você está criando uma [instância de organização](#) do IAM Identity Center.

Etapa 2. Criar um usuário administrativo no IAM Identity Center

Esse procedimento descreve como criar um usuário diretamente no diretório do Identity Center incorporado. Esse diretório não está conectado a outro diretório que o administrador possa usar para gerenciar usuários da força de trabalho. Depois de criar o usuário no IAM Identity Center, você especificará novas credenciais para esse usuário. Ao entrar como esse usuário para testar seu aplicativo AWS gerenciado, você entrará com as novas credenciais, não com as credenciais existentes que você usa para acessar os recursos corporativos.

Note

Recomendamos que você use esse método apenas para criar usuários para fins de teste.

1. No painel de navegação do console do IAM Identity Center, selecione Usuários e Adicionar usuário.
2. Siga as orientações no console para adicionar o usuário. Mantenha selecionado Enviar um e-mail para este usuário com instruções de configuração de senha e certifique-se de especificar um endereço de e-mail ao qual você tenha acesso.
3. No painel de navegação, escolha Contas da AWS, marque a caixa de seleção ao lado da sua conta e escolha Atribuir usuários ou grupos.
4. Escolha a aba Usuários, marque a caixa de seleção ao lado do usuário que você acabou de adicionar e escolha Avançar.

5. Escolha Criar conjunto de permissões e siga as orientações no console para criar o conjunto de permissões predefinido do AdministratorAccess.
6. Quando terminar, o novo conjunto de permissões será exibido na lista. Feche a aba Conjuntos de permissões na janela do navegador, retorne à aba Atribuir usuários e grupos e escolha o ícone de atualização ao lado de Criar conjunto de permissões.
7. Na aba do navegador Atribuir usuários e grupos, o novo conjunto de permissões aparece na lista. Marque a caixa de seleção ao lado do nome do conjunto de permissões, escolha Avançar e, em seguida, escolha Enviar.
8. Faça logout do Console da .

Etapa 3. Entre no portal de AWS acesso como usuário administrativo

O portal de AWS acesso é um portal da web que fornece ao usuário que você criou acesso ao console AWS de gerenciamento. Antes de fazer login no portal de acesso da AWS , você deve aceitar o convite para entrar no IAM Identity Center e ativar as credenciais de usuário.

1. Verifique seu e-mail para ver a linha de assunto Convite para participar do IAM Identity Center da AWS .
2. Escolha Aceitar convite e siga as orientações na página de inscrição para definir uma nova senha, fazer login e registrar um dispositivo de MFA para o usuário.
3. Depois de registrar seu dispositivo de MFA, o portal de AWS acesso é aberto.
4. No portal de AWS acesso, selecione seu Conta da AWS e escolha AdministratorAccess. O sistema redireciona você para o AWS Management Console.

Etapa 4: Configurar o aplicativo AWS gerenciado para usar o IAM Identity Center

1. Enquanto estiver conectado ao AWS Management Console, abra o console do aplicativo AWS gerenciado que você planeja usar.
2. Siga as orientações no console para configurar o aplicativo AWS gerenciado para usar o IAM Identity Center. Durante esse processo, você pode atribuir o usuário criado à aplicação.

Configurar uma instância de conta do IAM Identity Center para testar aplicativos AWS gerenciados

Note

Uma instância de conta do IAM Identity Center limita a implantação a uma única organização Conta da AWS. Você deve habilitar essa instância da Região da AWS mesma forma que o AWS aplicativo que você deseja testar.

Confirme o aplicativo

Todos os aplicativos AWS gerenciados que funcionam com o IAM Identity Center podem ser usados com instâncias organizacionais do IAM Identity Center. No entanto, somente algumas dessas aplicações podem ser usadas com instâncias de conta do IAM Identity Center. Revise a lista do [AWS aplicativos gerenciados que você pode usar com o IAM Identity Center](#).

Etapa 1. Habilitar uma instância de conta do IAM Identity Center

1. Realize um dos procedimentos a seguir para fazer login no Console de gerenciamento da AWS.
 - 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, insira a senha.
 - Já está usando AWS com uma conta independente Conta da AWS (credenciais do IAM) — Faça login usando suas credenciais do IAM com permissões administrativas.
2. Na página inicial do AWS Management Console, selecione o serviço IAM Identity Center ou navegue até o [console do IAM Identity Center](#).
3. Escolha Habilitar.
4. Na página Habilitar o IAM Identity Center com AWS Organizations, escolha habilitar uma instância de conta do IAM Identity Center.
5. Na página Habilitar instância de conta do IAM Identity Center, revise as informações e, opcionalmente, adicione as tags que você deseja associar a essa instância de conta. Em seguida, selecione Permitir.

Etapa 2. Criar um usuário no IAM Identity Center

Esse procedimento descreve como criar um usuário diretamente no diretório do Identity Center incorporado. Esse diretório não está conectado a outro diretório que o administrador possa usar para gerenciar usuários da força de trabalho. Depois de criar o usuário no IAM Identity Center, você especificará novas credenciais para esse usuário. Ao entrar como esse usuário para testar seu aplicativo AWS gerenciado, você entrará com as novas credenciais. As novas credenciais não permitirão que você acesse outros recursos corporativos.

Note

Recomendamos que você use esse método apenas para criar usuários para fins de teste.

1. No painel de navegação do console do IAM Identity Center, selecione Usuários e Adicionar usuário.
2. Siga as orientações no console para adicionar o usuário. Mantenha selecionado Enviar um e-mail para este usuário com instruções de configuração de senha e certifique-se de especificar um endereço de e-mail ao qual você tenha acesso.
3. Faça logout do Console da .

Etapa 3. Faça login no portal de AWS acesso como usuário do IAM Identity Center

O portal de AWS acesso é um portal da web que fornece ao usuário que você criou acesso ao console AWS de gerenciamento. Antes de fazer login no portal de acesso da AWS , você deve aceitar o convite para entrar no IAM Identity Center e ativar as credenciais de usuário.

1. Verifique seu e-mail para ver a linha de assunto Convite para participar do IAM Identity Center da AWS .
2. Escolha Aceitar convite e siga as orientações na página de inscrição para definir uma nova senha, fazer login e registrar um dispositivo de MFA para o usuário.
3. Depois de registrar seu dispositivo de MFA, o portal de AWS acesso é aberto. Quando os aplicações estiverem disponíveis para você, você as encontrará na aba Aplicativos.

 Note

AWS aplicativos que oferecem suporte a instâncias de conta permitem que os usuários façam login nos aplicativos sem exigir permissões adicionais. Portanto, a aba Contas permanecerá vazia.

Etapa 4: Configurar o aplicativo AWS gerenciado para usar o IAM Identity Center

1. Enquanto estiver conectado ao AWS Management Console, abra o console do aplicativo AWS gerenciado que você planeja usar.
2. Siga as orientações no console para configurar o aplicativo AWS gerenciado para usar o IAM Identity Center. Durante esse processo, você pode atribuir o usuário criado à aplicação.

Visualizando e alterando detalhes sobre um aplicativo AWS gerenciado

Depois de conectar um aplicativo AWS gerenciado ao IAM Identity Center usando o console ou APIs para o aplicativo, o aplicativo é registrado no IAM Identity Center. Depois que uma aplicação é registrada no IAM Identity Center, você pode visualizar e alterar detalhes sobre ela no console do IAM Identity Center.

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 [Visão geral da propagação de identidades confiáveis](#).

Para visualizar e alterar 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 Gerenciada pela AWS .
4. Escolha o link da aplicação gerenciada que você deseja abrir e visualizar.
5. Se você quiser alterar as informações sobre um aplicativo AWS gerenciado, escolha Ação e, em seguida, escolha Editar detalhes.

6. Você pode alterar o nome de exibição e a descrição da aplicação, bem como o método de atribuição de usuários e grupos.
 - a. Para alterar o nome de exibição, insira o nome desejado no campo Nome de exibição e escolha Salvar alterações.
 - b. Para alterar a descrição, insira a descrição desejada no campo Descrição e escolha Salvar alterações.
 - c. Para alterar o método de atribuição de usuários e grupos, faça a alteração desejada e escolha Salvar alterações. Para obter mais informações, consulte [the section called “Usuários, grupos e provisionamento”](#).

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.

Para desativar um aplicativo AWS gerenciado

1. Abra o [console do IAM Identity Center](#).
2. Selecione Aplicações.
3. Na página Aplicações, em Aplicações gerenciadas pela AWS , escolha a aplicação que você deseja desabilitar.
4. Com a aplicação selecionada, escolha Ações e depois escolha Desabilitar.
5. Na caixa de diálogo Desabilitar aplicação, escolha Desabilitar.
6. Na lista Aplicações gerenciadas pela AWS , o status da aplicação aparece como Inativo.

Note

Se um aplicativo AWS gerenciado estiver desativado, você poderá restaurar a capacidade dos usuários de se autenticarem no aplicativo escolhendo Ações e, em seguida, Habilitar.

Como habilitar sessões de console com identidade avançada

Uma sessão com identidade aprimorada 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 compatível com usuários do Kiro Pro do [Kiro em AWS aplicativos e sites](#).

Você pode habilitar sessões de console com identidade aprimorada sem fazer nenhuma alteração nos padrões de acesso existentes ou na federação no AWS console. 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](#)
- [Como habilitar identity-enhanced-console sessões](#)
- [Como as sessões de console com identidade avançada funcionam](#)

Pré-requisitos e considerações

Antes de habilitar sessões de console com identidade avançada, revise os seguintes pré-requisitos e considerações:

- Se seus usuários acessarem o Kiro em AWS aplicativos e sites por meio de uma assinatura do Kiro Pro, você deverá ativar as sessões de console com identidade aprimorada.

Note

Os usuários do Kiro podem acessar o Kiro sem sessões com identidade aprimorada, mas não terão acesso às suas assinaturas do Kiro Pro.

- As sessões de console com identidade avançada exigem uma [instância de organização](#) do IAM Identity Center.
- A integração com o Kiro não é suportada se você habilitar o IAM Identity Center em um Região da AWS opt-in.
- Para habilitar sessões de console com identidade avançada, você deve ter as seguintes permissões:

- `sso:CreateApplication`
- `sso:GetSharedSsoConfiguration`
- `sso:ListApplications`
- `sso:PutApplicationAssignmentConfiguration`
- `sso:PutApplicationAuthenticationMethod`
- `sso:PutApplicationGrant`
- `sso:PutApplicationAccessScope`
- `signin:CreateTrustedIdentityPropagationApplicationForConsole`
- `signin:ListTrustedIdentityPropagationApplicationsForConsole`
- Para permitir que seus usuários usem sessões de console com identidade avançada, você deve conceder a eles a permissão de `sts:setContext` em uma política baseada em identidade. Para obter informações, consulte [Como conceder permissões para o uso de sessões de console com identidade avançada](#).

Como habilitar identity-enhanced-console sessões

Você pode habilitar sessões de console com identidade aprimorada no console Kiro ou no console do IAM Identity Center.

Habilite sessões de console com identidade aprimorada no console Kiro

Antes de habilitar sessões de console com identidade avançada, você deve ter uma instância de organização do IAM Identity Center com uma fonte de identidade conectada. Se você já configurou o IAM Identity Center, pule para a etapa 3.

1. Abra o console do IAM Identity Center. Escolha Habilitar e crie uma instância de organização do IAM Identity Center. Para mais informações, consulte [Habilitar o IAM Identity Center](#).
2. Conecte sua fonte de identidades ao IAM Identity Center e provisione usuários para o IAM Identity Center. Você pode conectar a fonte de identidade existente ao IAM Identity Center ou usar o diretório do Identity Center se ainda não estiver usando outra fonte de identidades. Para obter mais informações, consulte [Tutoriais sobre fontes de identidade do IAM Identity Center](#).
3. Depois de concluir a configuração do IAM Identity Center, abra o console do Kiro e siga as etapas em [Assinaturas no Guia](#) do usuário do Kiro. Certifique-se de habilitar sessões de console de identidade avançada.

 Note

Se você não tiver permissões suficientes para habilitar sessões de console com identidade avançada, talvez seja necessário pedir a um administrador do IAM Identity Center que faça essa tarefa para você no console do IAM Identity Center. Para obter mais informações, consulte o próximo procedimento.

Habilitar sessões de console com identidade avançada no console do IAM Identity Center

Outro administrador pode pedir ao administrador do IAM Identity Center para habilitar sessões de console de identidade avançada, no console do IAM Identity Center.

1. Abra o console do IAM Identity Center.
2. No painel de navegação, selecione Configurações.
3. Em Habilitar sessões com identidade avançada, escolha Habilitar.
4. Na segunda mensagem, escolha Habilitar.
5. Depois de habilitar sessões de console com identidade avançada, uma mensagem de confirmação é exibida na parte superior da página Configurações.
6. Na seção Detalhes, o status de Sessões com identidade avançada é Habilitado.

Como as sessões de console com identidade avançada funcionam

O IAM Identity Center aprimora a sessão atual de 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 identidade avançada incluem estes três valores:

- ID do usuário do repositório de identidades ([loja de identidades: UserId](#)): esse valor é usado para identificar exclusivamente um usuário na fonte de identidades conectada ao IAM Identity Center.
- ARN do diretório do repositório de identidades ([loja de identidades: IdentityStoreArn](#)): esse valor é o ARN do repositório de identidades conectada ao IAM Identity Center e é onde você pode pesquisar atributos do `identitystore:UserId`.
- ID de 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 são 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 apenas o ID da sessão.
- Outros métodos de login: se o usuário fizer login na AWS como usuário do IAM, com um perfil 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.

Aplicações gerenciadas pelo cliente

O IAM Identity Center atua como um serviço central de identidades para os usuários e grupos da sua força de trabalho. 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. Com uma única conexão, o IAM Identity Center representa seu IdP na frente de vários Serviços da AWS e permite que seus aplicativos OAuth 2.0 solicitem acesso aos dados nesses serviços em nome de seus usuários. Você também pode usar o IAM Identity Center para atribuir aos usuários acesso às aplicações [SAML 2.0](#). Isso inclui AWS serviços como o Amazon Connect e AWS Client VPN, que se integram ao IAM Identity Center usando exclusivamente SAML e, portanto, são classificados como aplicativos gerenciados pelo cliente.

- Se seu aplicativo for compatível com JSON Web Tokens (JWTs), você poderá usar o recurso confiável de propagação de identidade do IAM Identity Center para permitir que seu aplicativo solicite acesso aos dados Serviços da AWS em nome de seus usuários. A propagação de identidade confiável é baseada na Estrutura de Autorização OAuth 2.0 e inclui uma opção para os aplicativos trocarem tokens de identidade provenientes de um servidor de autorização OAuth 2.0 externo por tokens emitidos pelo IAM Identity Center e reconhecidos pelo Serviços da AWS. Para obter mais informações, consulte [Casos de uso de propagação de identidades confiáveis](#).
- Se a aplicação for compatível com SAML 2.0, você poderá conectá-la a uma [instância de organização do IAM Identity Center](#). Você pode usar o IAM Identity Center para atribuir acesso à aplicação SAML 2.0.

 Note

Ao integrar aplicativos gerenciados pelo cliente com uma instância do IAM Identity Center que usa uma [chave KMS gerenciada pelo cliente](#), verifique se o aplicativo invoca o serviço IAM Identity Center APIs para confirmar se o aplicativo precisa de permissões de chave KMS. Siga as orientações para conceder permissões de chave KMS para fluxos de trabalho personalizados nas políticas [básicas](#) de chaves KMS do IAM Identity Center.

Tópicos

- [Acesso de login único aos aplicativos SAML 2.0 e 2.0 OAuth](#)
- [Configurar aplicações SAML 2.0 gerenciadas pelo cliente](#)

Acesso de login único aos aplicativos SAML 2.0 e 2.0 OAuth

O IAM Identity Center permite que você forneça aos usuários acesso de login único aos aplicativos SAML 2.0 ou OAuth 2.0. Os tópicos a seguir fornecem uma visão geral de alto nível do SAML 2.0 e OAuth 2.0.

Tópicos

- [SAML 2.0](#)
- [OAuth 2.0](#)

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.

 Note

O IAM Identity Center não oferece suporte à validação de assinaturas de solicitações de autenticação SAML recebidas de aplicações SAML.

OAuth 2.0

OAuth 2.0 é um protocolo que permite que os aplicativos 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 subsídios 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. Clientes públicos geralmente são desktops, laptops ou outros dispositivos móveis usados para executar aplicações localmente. Exemplos de AWS aplicativos executados em clientes públicos incluem o AWS Command Line Interface (AWS CLI) e AWS Toolkit os kits de desenvolvimento de AWS software (SDKs). Para permitir que esses aplicativos obtenham credenciais, o IAM Identity Center oferece suporte a partes dos seguintes fluxos OAuth 2.0:

- Concessão de código de autorização com Proof Key for Code Exchange (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 ser compatíveis com esse tipo de concessão em todas as Regiões da AWS. Consulte a documentação relevante Serviços da AWS para diferenças regionais.

O OpenID Connect (OIDC) é um protocolo de autenticação baseado no 2.0 Framework. OAuth O OIDC especifica como usar OAuth 2.0 para autenticação. Por meio do [serviço OIDC do IAM Identity Center APIs](#), um aplicativo registra um cliente OAuth 2.0 e usa um desses fluxos para obter um token de acesso que fornece permissões para o IAM Identity Center protegido. APIs Uma aplicação especifica os [escopos de acesso](#) para declarar seu usuário pretendido da API. Depois que você, como administrador do IAM Identity Center, configurar sua fonte de identidades, os usuários finais da aplicação deverão concluir um processo de login, se ainda não o fizeram. Os usuários finais deverão então fornecer seu consentimento para permitir que a aplicação 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 à aplicação que contém os escopos de acesso nos quais os usuários consentiram.

Usando um fluxo de concessão OAuth 2.0

OAuth Os fluxos de concessão 2.0 só estão disponíveis por meio de aplicativos AWS gerenciados que oferecem suporte aos fluxos. Para usar um fluxo OAuth 2.0, sua instância do IAM Identity Center e todos os aplicativos AWS gerenciados compatíveis que você usa devem ser implantados em um única 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 da aplicação, como administrador, você deve fornecer aos usuários o URL do portal de acesso AWS ou o URL do emissor da sua instância do IAM Identity Center. Você pode encontrar essas duas configurações na página Configurações do [console do IAM Identity Center](#). Para obter informações adicionais sobre a configuração de uma aplicação cliente, consulte a documentação da aplicação.

A experiência do usuário final ao fazer login em uma aplicação e fornecer consentimento depende do uso de [Concessão de código de autorização com PKCE](#) ou [Concessão de autorização de dispositivo](#) pela aplicação.

Concessão de código de autorização com PKCE

Esse fluxo é usado pelas aplicações executadas em um dispositivo que tem navegador.

1. Uma janela do navegador se abre.
2. Se o usuário ainda não foi autenticado, o navegador o redirecionará para a autenticação de usuário.
3. Após a autenticação, é apresentada ao usuário uma tela de consentimento que exibe as seguintes informações:
 - O nome da aplicação
 - Os escopos de acesso que a aplicação está solicitando consentimento para usar
4. O usuário pode cancelar o processo de consentimento ou dar seu consentimento, e a aplicação prossegue com o acesso segundo as permissões do usuário.

Concessão de autorização de dispositivo

Esse fluxo pode ser usado por aplicações executadas em um dispositivo com ou sem navegador. Quando a aplicação inicia o fluxo, apresenta um URL e um código de usuário que o usuário deverá

verificar mais adiante no fluxo. O código do usuário é necessário porque a aplicação que inicia o fluxo pode estar sendo executada em um dispositivo que não é o mesmo no qual o usuário fornece consentimento. O código garante que o usuário esteja consentindo o fluxo iniciado no outro dispositivo.

Note

Se você tiver clientes usando o `device.sso.region.amazonaws.com`, deverá atualizar o fluxo de autorização para usar a chave de prova para troca de código (PKCE). Para obter mais informações, consulte [Como configurar a autenticação do IAM Identity Center com a AWS CLI](#) no Guia do Usuário do AWS Command Line Interface .

1. Quando o fluxo é iniciado em um dispositivo com navegador, uma janela do navegador é aberta. Quando o fluxo é iniciado em um dispositivo sem navegador, o usuário deve abrir um navegador em um outro dispositivo e acessar o URL que a aplicação apresentou.
2. Em ambos os casos, se o usuário ainda não foi autenticado, o navegador o redirecionará para fazer a autenticação de usuário.
3. Após a autenticação, é apresentada ao usuário uma tela de consentimento que exibe as seguintes informações:
 - O nome da aplicação
 - Os escopos de acesso que a aplicação está solicitando consentimento para usar
 - O código do usuário que a aplicação apresentou ao usuário
4. O usuário pode cancelar o processo de consentimento ou dar seu consentimento, e a aplicação prossegue com o acesso segundo as permissões do usuário.

Escopos de acesso

Um escopo define o acesso a um serviço que pode ser acessado por meio de um fluxo 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 OAuth os clientes 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.

OAuth Os clientes 2.0 usam scope valores conforme definido na [seção 3.3 de OAuth 2.0 \(RFC 6749\)](#) para especificar quais permissões estão sendo solicitadas para um token de acesso. Os clientes podem especificar até 25 escopos ao solicitar um token de acesso. Quando um usuário fornece consentimento durante uma concessão de código de autorização com PKCE ou um 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 compatíveis com o serviço OIDC do IAM Identity Center quando você registra um cliente público.

Escopos de acesso compatíveis com o serviço IAM Identity Center OIDC ao registrar um cliente público

Escopo	Description	Serviços com suporte de
<code>sso:account:access</code>	Acesse contas gerenciadas e conjuntos de permissões do IAM Identity Center.	Centro de Identidade do IAM
<code>codewhisperer:analysis</code>	Habilite o acesso à análise de código do Kiro.	ID do builder AWS e o IAM Identity Center
<code>codewhisperer:completions</code>	Habilite o acesso às sugestões de código em linha do Kiro.	ID do builder AWS e o IAM Identity Center
<code>codewhisperer:conversations</code>	Habilite o acesso ao chat do Kiro.	ID do builder AWS e o IAM Identity Center
<code>codewhisperer:taskassist</code>	Habilite o acesso ao Kiro Agent para desenvolvimento de software.	ID do builder AWS e o IAM Identity Center
<code>codewhisperer:transformations</code>	Habilite o acesso ao Kiro Agent para transformação de código.	ID do builder AWS e o IAM Identity Center

Escopo	Description	Serviços com suporte de
<code>codecatalyst:read_write</code>	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
<code>verified_access:application:connect</code>	Habilitar Acesso Verificado pela AWS	Acesso Verificado pela AWS
<code>redshift:connect</code>	Conectar-se ao Amazon Redshift	banco de dados de origem
<code>datazone:domain:access</code>	Acesse sua função DataZone de execução de domínio	Amazon DataZone
<code>nosqlworkbench:datamodeladviser</code>	Criar e ler modelos de dados	NoSQL Workbench
<code>transform:read_write</code>	Habilite o acesso ao AWS Transform Agent para transformação de código	AWS Transformação

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 à OAuth versão 2.0 e seus usuários precisam acessar esses aplicativos Serviços da AWS, você pode usar a propagação de identidade confiável. Com a propagação de identidade confiável, um usuário

pode fazer login em uma aplicação e essa aplicação pode transmitir a identidade do usuário nas solicitações para acessar dados nos Serviços da AWS.

Tópicos

- [Configurar uma aplicação do catálogo de aplicações do IAM Identity Center](#)
- [Configurar sua própria aplicação SAML 2.0](#)

Configurar uma aplicação do 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.

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 obter mais informações, consulte [Compreender 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 seus valores de metadados e, em seguida, forneça os valores de URL do ACS da aplicação e do público de 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 obter mais informações, consulte [Compreender 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.

Visão geral da propagação de identidades confiáveis

A propagação de identidade confiável é um atributo do IAM Identity Center que permite que os administradores de Serviços da AWS concedam permissões com base em atributos do usuário, como associações a grupos. Com a propagação de identidade confiável, o contexto de identidade é adicionado a uma função do IAM para identificar o usuário que está solicitando acesso aos AWS recursos. Esse contexto é propagado para outros Serviços da AWS.

O contexto de identidade compreende informações que são Serviços da AWS usadas para tomar decisões de autorização ao receber solicitações de acesso. Essas informações incluem metadados que identificam o solicitante (por exemplo, um usuário do IAM Identity Center), o acesso AWS service (Serviço da AWS) ao qual o acesso é solicitado (por exemplo, Amazon Redshift) e o escopo do acesso (por exemplo, acesso somente para leitura). O destinatário AWS service (Serviço da AWS) usa esse contexto e todas as permissões atribuídas ao usuário para autorizar o acesso aos seus recursos.

Benefícios da propagação de identidade confiável

A propagação confiável de identidades permite que os administradores concedam permissões Serviços da AWS a recursos, como dados, usando as identidades corporativas de sua força de trabalho. Além disso, eles podem auditar quem acessou quais dados examinando os registros de serviço ou AWS CloudTrail. Outros administradores do AWS service (Serviço da AWS) podem solicitar ao administrador do IAM Identity Center para habilitar a propagação de identidade confiável.

Como habilitar a propagação de identidade confiável

O processo de habilitar a propagação de identidade confiável envolve as duas etapas a seguir:

1. Ative o IAM Identity Center e conecte sua fonte existente de identidades ao IAM Identity Center — Você continuará gerenciando suas identidades de força de trabalho em sua fonte

de identidades existente; conectá-la ao IAM Identity Center cria uma referência à sua força de trabalho que todos Serviços da AWS em seu caso de uso podem compartilhar. Também está disponível para os proprietários de dados usarem em casos de uso futuros.

2. Conecte o Serviços da AWS em seu caso de uso ao IAM Identity Center — O administrador de cada AWS service (Serviço da AWS) caso de uso de propagação de identidade confiável segue as orientações na respectiva documentação do serviço para conectar o serviço ao IAM Identity Center.

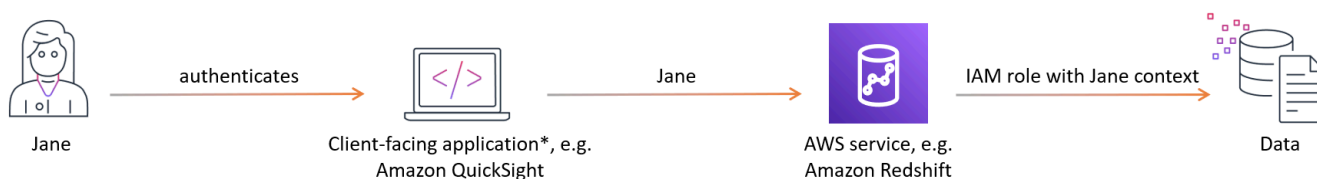
Note

Se p caso de uso envolver uma aplicação desenvolvida por terceiros ou pelo cliente, você habilita a propagação de identidade confiável configurando uma relação de confiança entre o provedor de identidade que autentica os usuários da aplicação e o IAM Identity Center. Isso permite que a aplicação aproveite o fluxo de propagação de identidade confiável descrito anteriormente.

Para obter mais informações, consulte [Usar aplicações com um emissor de tokens confiáveis](#).

Como funciona a propagação de identidade confiável

O diagrama a seguir mostra o fluxo de trabalho de alto nível para a propagação de identidade confiável:



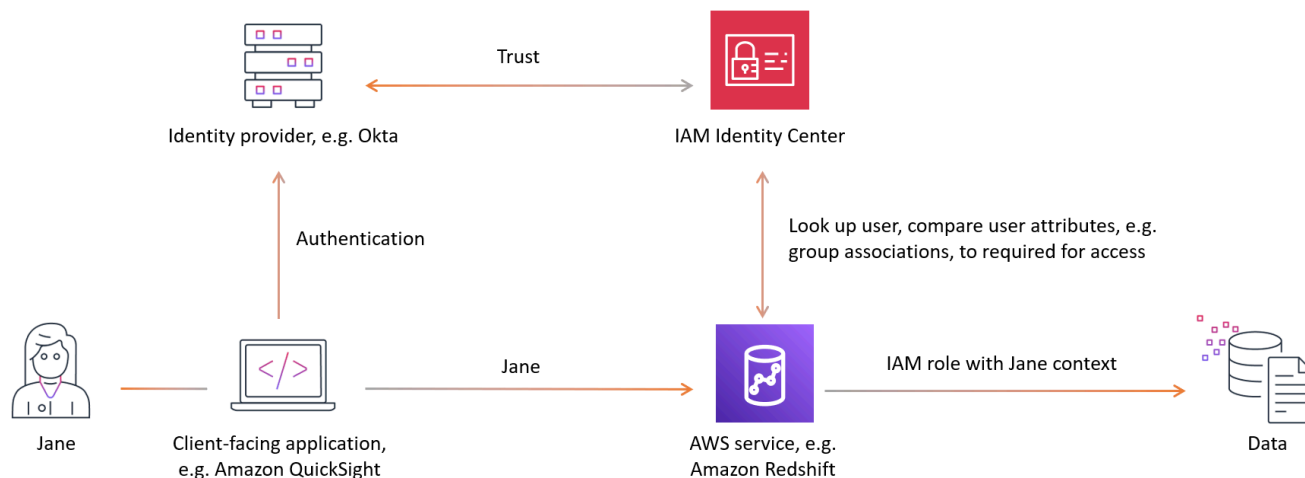
1. Os usuários se autenticam com um aplicativo voltado para o cliente, por exemplo, o Quick.
2. O aplicativo voltado para o cliente solicita acesso para usar e consultar dados e inclui informações sobre o usuário. AWS service (Serviço da AWS)

Note

Alguns casos de uso confiável de propagação de identidade envolvem ferramentas que interagem com o Serviços da AWS uso de drivers de serviço. Você pode descobrir se isso se aplica ao caso de uso na [orientação do caso de uso](#).

3. Ele AWS service (Serviço da AWS) verifica a identidade do usuário com o IAM Identity Center e compara os atributos do usuário, como suas associações de grupo, com aqueles necessários para acesso. O AWS service (Serviço da AWS) autoriza o acesso, desde que o usuário ou seu grupo tenha as permissões necessárias.
4. Serviços da AWS podem registrar o identificador do usuário em seus registros de serviço. AWS CloudTrail Consulte a documentação do serviço para obter mais detalhes.

A imagem a seguir fornece uma visão geral das etapas descritas anteriormente no fluxo de trabalho de propagação de identidade confiável:



Tópicos

- [Pré-requisitos e considerações](#)
- [Casos de uso de propagação de identidades confiáveis](#)
- [Serviços de autorização](#)

Pré-requisitos e considerações

Antes de configurar a propagação de identidades confiáveis, revise os seguintes pré-requisitos e considerações.

Tópicos

- [Pré-requisitos](#)
- [Considerações](#)
- [Considerações sobre aplicações gerenciadas pelo cliente](#)

Pré-requisitos

Para usar a propagação de identidade confiável, confirme que o ambiente atende aos pré-requisitos a seguir:

- Habilitar e provisionar o IAM Identity Center
 - Para usar a propagação de identidade confiável, você deve habilitar o IAM Identity Center no mesmo Região da AWS local em que os AWS aplicativos e serviços que seus usuários acessarão estão habilitados. Para mais informações, consulte [Habilitar o IAM Identity Center](#).
 - Instância de organização recomendada do IAM Identity Center: recomendamos que você use uma [instância de organização](#) do IAM Identity Center habilitada na conta gerencial do AWS Organizations. Você pode [delegar a administração](#) de uma instância de organização do IAM Identity Center a uma conta de membro. Se você escolher uma [instância de conta](#) do IAM Identity Center, todos os Serviços da AWS que você deseja que os usuários acessem com propagação de identidade confiável devem residir na mesma Conta da AWS em que você habilitou o IAM Identity Center. Para obter mais informações, consulte [Instâncias de conta do Centro de Identidade do IAM](#).
 - Conecte o provedor de identidade existente ao IAM Identity Center e provisione os usuários e grupos no IAM Identity Center. Para obter mais informações, consulte [Tutoriais sobre fontes de identidade do IAM Identity Center](#).
- Conecte os aplicativos e serviços AWS gerenciados em seu caso de uso confiável de propagação de identidade ao IAM Identity Center. Para usar a propagação de identidade confiável, os aplicativos AWS gerenciados devem estar conectados ao IAM Identity Center.

Considerações

Ao configurar e usar a propagação de identidade confiável, leve em consideração o seguinte:

- Instâncias de organização versus de conta do IAM Identity Center
 - Uma [instância de organização](#) do IAM Identity Center lhe dará o máximo de controle e flexibilidade para expandir os casos de uso para vários Contas da AWS, usuários e Serviços da AWS. Se você não conseguir usar uma instância de organização, o caso de uso pode ser compatível com instâncias de conta do IAM Identity Center. Para saber mais sobre quais Serviços da AWS no caso de uso são compatíveis com instâncias de conta do IAM Identity Center, consulte [AWS aplicativos gerenciados que você pode usar com o IAM Identity Center](#).
- 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.

Considerações sobre aplicações gerenciadas pelo cliente

Sua força de trabalho pode se beneficiar da propagação confiável de identidade, mesmo que seus usuários interajam com aplicativos voltados para o cliente que não são gerenciados, por exemplo AWSTableau, por seus aplicativos desenvolvidos sob medida. Os usuários dessas@aplicações podem não estar provisionados no IAM Identity Center. Para permitir o reconhecimento e a autorização fáceis do acesso do usuário aos AWS recursos, o IAM Identity Center permite que você configure uma relação confiável entre o provedor de identidade que autentica seus usuários e o IAM Identity Center. Para obter mais informações, consulte [Usar aplicações com um emissor de tokens confiáveis](#).

Além disso, configurar a propagação de identidade confiável para a aplicação exigirá:

- Seu aplicativo deve usar a estrutura OAuth 2.0 para autenticação. A propagação de identidade confiável não é compatível com integrações do SAML 2.0.
- A aplicação deve ser reconhecida pelo IAM Identity Center. Siga as orientações específicas para o [caso de uso](#).

Casos de uso de propagação de identidades confiáveis

Pode ser solicitado ao administrador do IAM Identity Center que ajude a configurar a propagação de identidade confiável das aplicações voltadas para os Serviços da AWS. Para apoiar essa solicitação, serão necessárias as seguintes informações:

- Com qual aplicação voltada para o cliente os usuários interagirão?
- Quais Serviços da AWS são usados para consultar os dados e autorizar o acesso aos dados?
- O que AWS service (Serviço da AWS) autoriza o acesso aos dados?

A função em permitir casos de uso de propagação de identidade confiável que não envolvam aplicações de terceiros ou aplicações desenvolvidas sob medida é:

1. [Ative o IAM Identity Center.](#)
2. [Conecte a fonte atual de identidades ao IAM Identity Center.](#)

As etapas restantes da configuração de identidade confiável para esses casos de uso são executadas nos aplicativos conectados Serviços da AWS e. Os administradores dos aplicativos conectados Serviços da AWS ou dos aplicativos devem consultar os respectivos guias do usuário para obter uma orientação abrangente e específica do serviço.

Função em permitir casos de uso de propagação de identidade confiáveis que envolvam aplicações de terceiros ou aplicações desenvolvidas sob medida inclui as etapas [Habilitar o IAM Identity Center](#) e a [conexão da fonte de identidades](#), bem como:

1. Como configurar a conexão do provedor de identidade (IdP) com a aplicação de terceiros ou desenvolvida de forma personalizada.
2. Como permitir que o IAM Identity Center reconheça a aplicação de terceiros ou desenvolvida de forma personalizada.
3. Como configurar o IdP como um emissor de tokens confiáveis no IAM Identity Center Para obter mais informações, consulte [Usar aplicações com um emissor de tokens confiáveis](#).

Os administradores dos aplicativos conectados Serviços da AWS devem consultar os respectivos guias do usuário para obter uma orientação abrangente e específica do serviço.

Casos de uso de analytics, data lakehouse e machine learning

Você pode habilitar casos de uso de propagação confiável com os seguintes serviços de analytics e machine learning:

- Amazon Redshift — Para obter orientação, consulte [Propagação de identidade confiável com o Amazon Redshift](#).
- Amazon EMR — Para obter orientação, consulte [Propagação de identidade confiável com o Amazon EMR](#).
- Amazon Athena — Para obter orientação, consulte [Propagação de identidade confiável com o Amazon Athena](#).
- SageMaker Studio - Para obter orientação, consulte [Propagação de identidade confiável com o Amazon Studio SageMaker](#).

Casos de uso adicionais

Você pode habilitar o IAM Identity Center e a propagação de identidade confiável com estes Serviços da AWS adicionais:

- Amazon Q Business — Para obter orientação, consulte:
 - [Fluxo de trabalho administrativo para aplicações que usam o IAM Identity Center](#).
 - [Como configurar uma aplicação do Amazon Q Business usando o IAM Identity Center](#).
 - [Configure o Amazon Q Business com a propagação de identidade confiável do IAM Identity Center](#).
- Amazon OpenSearch Service — para obter orientação, consulte:
 - [Suporte confiável de propagação de identidade do IAM Identity Center para Amazon OpenSearch Service](#).
 - [Interface de OpenSearch usuário centralizada \(painéis\) com o Amazon OpenSearch Service](#).
- AWS Transfer Family — Para obter orientações, consulte:
 - [Aplicativos Transfer Family da web](#).

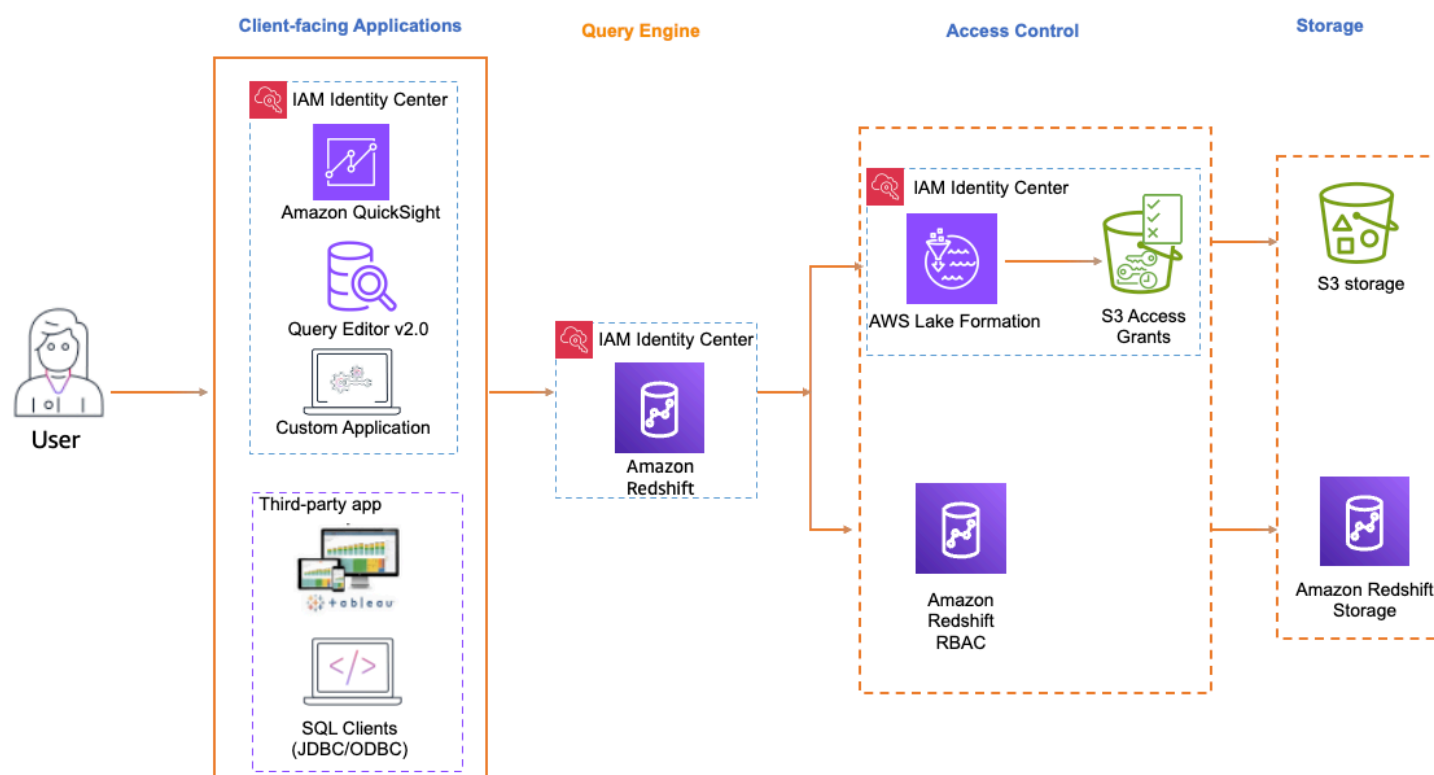
Tópicos

- [Propagação de identidade confiável com o Amazon Redshift](#)
- [Propagação de identidade confiável com o Amazon EMR](#)

- [Propagação de identidade confiável com o Amazon Athena](#)
- [Propagação de identidade confiável com o Amazon Studio SageMaker](#)

Propagação de identidade confiável com o Amazon Redshift

As etapas para permitir a propagação de identidade confiável dependem de seus usuários interagirem com aplicativos AWS gerenciados ou aplicativos gerenciados pelo cliente. O diagrama a seguir mostra uma configuração confiável de propagação de identidade para aplicativos voltados ao cliente — AWS gerenciados ou externos AWS — que consultam dados do Amazon Redshift com controle de acesso fornecido pelo Amazon Redshift ou por serviços de autorização, como o Amazon S3. AWS Lake Formation Access Grants



Quando a propagação de identidade confiável para o Amazon Redshift está habilitada, os administradores do Redshift podem configurar o Redshift para criar perfis automaticamente para o IAM Identity Center como provedor de identidade, mapear perfis do Redshift para grupos no IAM Identity Center e usar o controle de acesso baseado em perfis do Redshift para conceder acesso.

Aplicações voltadas para o cliente compatíveis

AWS aplicativos gerenciados

Os seguintes aplicativos AWS gerenciados voltados para o cliente oferecem suporte à propagação confiável de identidade para o Amazon Redshift:

- [Query Editor V2 do Amazon Redshift](#)
- [Rápido](#)

 Note

Se você estiver usando o Amazon Redshift Spectrum para acessar bancos de dados ou tabelas externas no AWS Glue Data Catalog, pense em [configurar o Lake Formation](#) e o [Amazon S3 Access Grants](#) para fornecer controle de acesso refinado.

Aplicações gerenciadas pelo cliente

As seguintes aplicações gerenciadas pelo cliente oferecem suporte à propagação de identidade confiável para o Amazon Redshift:

- Tableau incluindo Tableau Desktop, Tableau Server e Tableau Prep
 - Para permitir a propagação de identidade confiável para usuários do Tableau, consulte [Integrar Tableau e Okta com o Amazon Redshift usando o IAM Identity Center](#) no Blog de big data da AWS .
- Clientes SQL (DBEaver e DBVisualizer)
 - Para habilitar a propagação de identidade confiável para usuários de Clientes SQL (DBEaver e DBVisualizer), consulte [Integrar o Provedor de Identidades \(IdP\) com o Editor de Consultas V2 do Amazon Redshift e o Cliente SQL usando o IAM Identity Center para logon único contínuo](#) no Blog de big data da AWS .

Como configurar a propagação de identidade confiável com o Editor de Consultas V2 do Amazon Redshift

O procedimento a seguir explica como obter uma propagação de identidade confiável do Editor de Consultas V2 do Amazon Redshift para o Amazon Redshift.

Pré-requisitos

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

1. [Ative o IAM Identity Center](#). A [instância de organização](#) é recomendada. Para obter mais informações, consulte [Pré-requisitos e considerações](#).
2. [Provisione os usuários e grupos da fonte de identidades no IAM Identity Center](#).

A habilitação da propagação de identidade confiável inclui tarefas executadas por um administrador do IAM Identity Center no console do IAM Identity Center e tarefas executadas por um administrador do Amazon Redshift no console do Amazon Redshift.

Tarefas executadas pelo administrador do IAM Identity Center

As seguintes tarefas precisavam ser concluídas pelo administrador do IAM Identity Center:

1. Crie um [perfil do IAM](#) na conta em que existe o cluster do Amazon Redshift ou a instância Serverless com a seguinte política de permissão. Para obter mais informações, consulte [Criação do Perfil do IAM](#).
- Os exemplos de políticas a seguir incluem as permissões necessárias para concluir este tutorial. Para usar essa política, substitua *italicized placeholder text* a política do exemplo por suas próprias informações. Para obter instruções adicionais, consulte [Criar uma política](#) ou [Editar uma política](#).

Política de permissão:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRedshiftApplication",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    },
    {
```

```

        "Sid": "AllowIDCPPermissions",
        "Effect": "Allow",
        "Action": [
            "sso:DescribeApplication",
            "sso:DescribeInstance"
        ],
        "Resource": [
            "arn:aws:sso::instance/Your-IAM-Identity-Center-Instance-ID",
            "arn:aws:sso::111122223333:application/Your-IAM-Identity-Center-Instance-ID/*"
        ]
    }
}

```

Política de confiança:

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift-serverless.amazonaws.com",
          "redshift.amazonaws.com"
        ]
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}

```

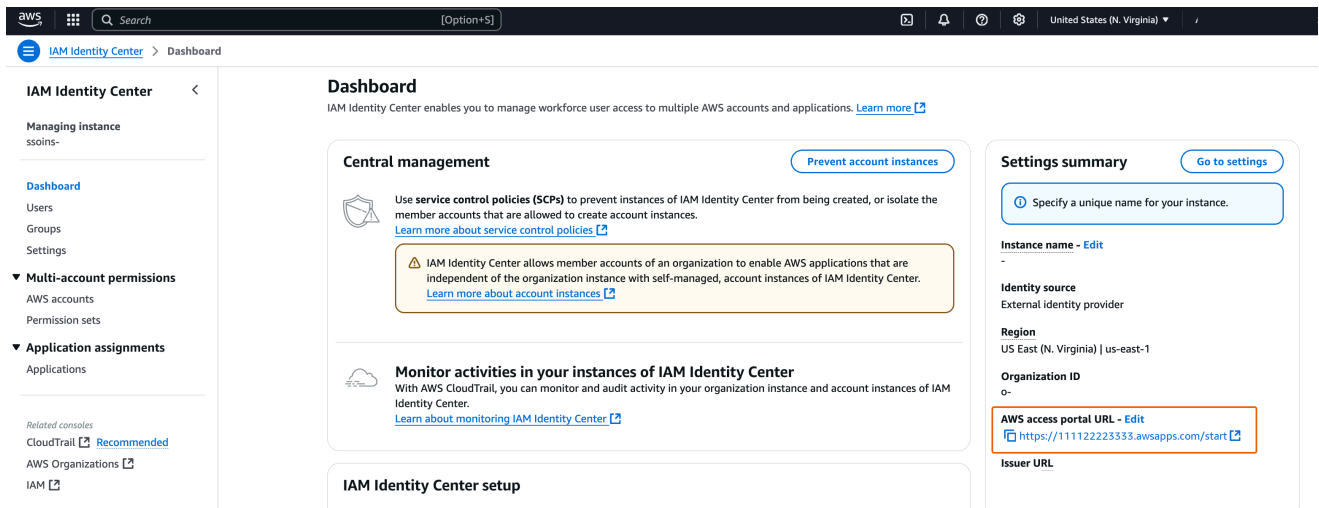
2. Crie um conjunto de permissões na conta gerencial do AWS Organizations em que o IAM Identity Center está habilitado. Você o usará na próxima etapa para permitir que usuários federados acessem o Editor de Consultas V2 do Redshift.
 - a. Acesse o console do IAM Identity Center e, em Permissões de várias contas, escolha Conjuntos de permissões.
 - b. Escolha Create permission set (Criar conjunto de permissões).
 - c. Escolha Conjunto de permissões personalizado e, em seguida, escolha Avançar.
 - d. Em Políticas gerenciadas pela AWS , escolha **AmazonRedshiftQueryEditorV2ReadSharing**.
 - e. Em Política embutida, adicione a seguinte política:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    }
  ]
}
```

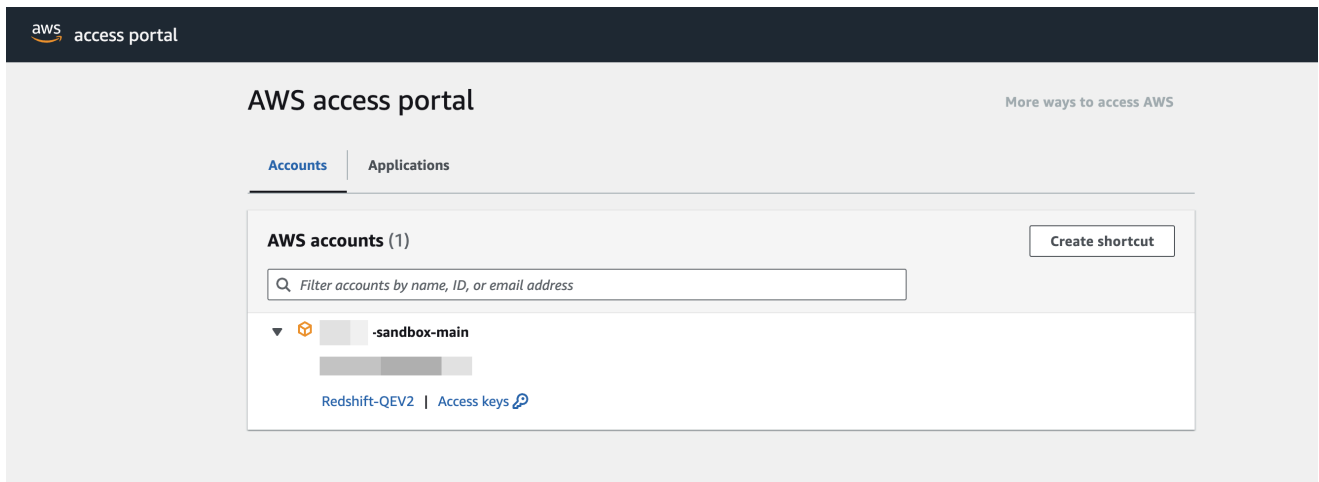
- f. Selecione Avançar e forneça um nome para o nome do conjunto de permissões. Por exemplo, **Redshift-Query-Editor-V2**
- g. Em Estado de retransmissão — opcional, defina o estado de retransmissão padrão para o URL do Editor de Consultas V2, usando o formato: `https://your-region.console.aws.amazon.com/sqlworkbench/home`.
- h. Revise as configurações e escolha Criar.

- i. Navegue até o painel do IAM Identity Center e copie o URL do portal de acesso do AWS da seção Resumo da configuração.



- j. Abra uma nova janela de navegador anônimo e cole o URL.

Isso o levará ao seu portal de AWS acesso, garantindo que você esteja fazendo login com um usuário do IAM Identity Center.



Para obter mais informações sobre o conjunto de permissões, consulte [Gerencie Contas da AWS com conjuntos de permissões](#).

3. Permita que usuários federados acessem o Editor de Consultas V2 do Redshift.
 - a. Na conta AWS Organizations de gerenciamento, abra o console do IAM Identity Center.
 - b. No painel de navegação, em Permissões de várias contas, escolha Contas da AWS.
 - c. Na Contas da AWS página, selecione o Conta da AWS que você deseja atribuir acesso.
 - d. Escolha Atribuir usuários ou grupos.

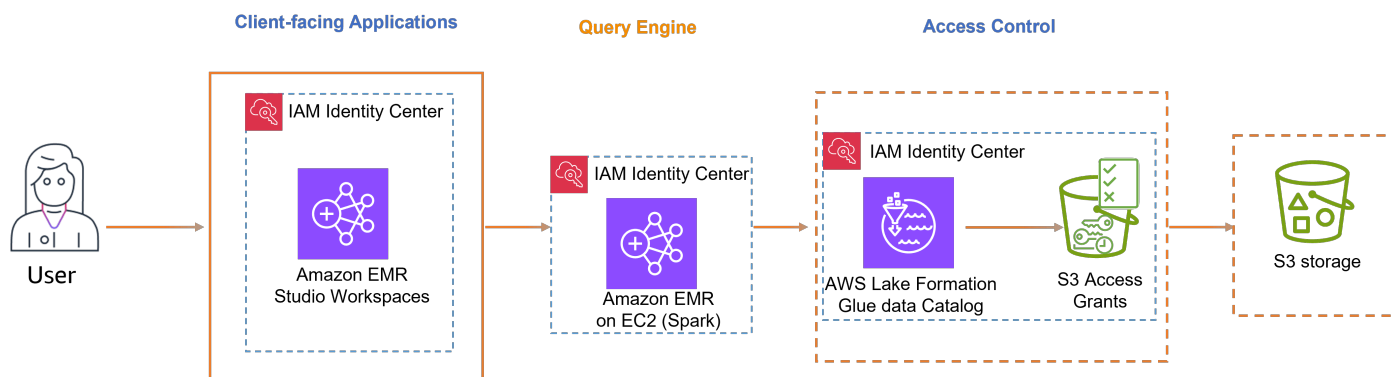
- e. Na página Atribuir usuários e grupos, escolha os usuários e/ou grupos para os quais deseja criar o conjunto de permissões. Em seguida, escolha Próximo.
- f. Na página Atribuir conjuntos de permissões, escolha o conjunto de permissões que você criou na etapa anterior. Em seguida, escolha Próximo.
- g. Na página Revisar e enviar atribuições, revise as seleções e escolha Enviar.

Tarefas executadas por um administrador do Amazon Redshift

A habilitação da propagação de identidade confiável para o Amazon Redshift exige que um administrador de cluster do Amazon Redshift ou administrador do Amazon Redshift sem servidor execute várias tarefas no console do Amazon Redshift. Para obter mais informações, consulte [Integrar o provedor de identidades \(IdP\) com o Editor de Consultas V2 do Amazon Redshift e o cliente SQL usando o IAM Identity Center para um login único direto](#) no Blog de big data da AWS .

Propagação de identidade confiável com o Amazon EMR

O diagrama a seguir mostra uma configuração confiável de propagação de identidade para o Amazon EMR Studio usando o Amazon EMR no Amazon EC2 com controle de acesso fornecido pelo Amazon S3. AWS Lake Formation Access Grants



Aplicações voltadas para o cliente compatíveis

- Amazon EMR Studio

Para habilitar a propagação de identidade confiável, siga estas etapas:

- [Configure o Amazon EMR Studio](#) como aplicação voltada para o cliente para o cluster do Amazon EMR.
- Configure o [Cluster do Amazon EMR no Amazon EC2 com Apache Spark](#).

- Recomendado: [AWS Lake Formation](#) e o [Amazon S3 Access Grants](#) para fornecer controle de acesso refinado AWS Glue Data Catalog e locais de dados subjacentes no S3.

Como configurar a propagação de identidade confiável com o Amazon EMR Studio

O procedimento a seguir orienta você na configuração do Amazon EMR Studio para a propagação confiável de identidade em consultas em grupos de trabalho do Amazon Athena ou clusters do Amazon EMR que executam o Apache Spark.

Pré-requisitos

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

1. [Ative o IAM Identity Center](#). A [instância de organização](#) é recomendada. Para obter mais informações, consulte [Pré-requisitos e considerações](#).
2. [Provisione os usuários e grupos da fonte de identidades no IAM Identity Center](#).

Para concluir a configuração da propagação de identidade confiável do Amazon EMR Studio, o administrador do EMR Studio deve executar as seguintes etapas.

Etapas 1. Criar os perfis do IAM exigidos para o EMR Studio

Nesta etapa, o administrador do Amazon EMR Studio cria um perfil de serviço do IAM e um perfil de usuário do IAM para o EMR Studio.

1. [Crie um perfil de serviço do EMR Studio](#) — O EMR Studio assume esse perfil do IAM para gerenciar com segurança espaços de trabalho e notebooks, conectar-se a clusters e lidar com interações de dados.
 - a. Navegue até o console do IAM (<https://console.aws.amazon.com/iam/>) e crie uma função do IAM.
 - b. Selecione AWS service (Serviço da AWS) como entidade confiável e, em seguida, escolha Amazon EMR. Anexe as políticas a seguir para definir as permissões e a relação de confiança do perfil.

Para usar essas políticas, substitua a política *italicized placeholder text* no exemplo por suas próprias informações. Para obter instruções adicionais, consulte [Criar uma política](#) ou [Editar uma política](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectActions",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
      }
    },
    {
      "Sid": "BucketActions",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetEncryptionConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
      }
    }
  ]
}
```

Para obter uma referência de todas as permissões de perfil de serviço, consulte [Permissões de perfil de serviço do EMR Studio](#).

2. [Crie um perfil de usuário do EMR Studio para autenticação do IAM Identity Center](#) — o EMR Studio assume esse perfil quando um usuário faz login pelo IAM Identity Center para gerenciar espaços de trabalho, clusters do EMR, tarefas e repositórios git. Esse perfil é usado para iniciar o fluxo de trabalho de propagação de identidade confiável.

 Note

A função de usuário do EMR Studio não precisa incluir permissões para acessar as localizações das tabelas no Amazon S3 no Catálogo. AWS Glue AWS Lake Formation as permissões e as localizações registradas dos lagos serão usadas para receber permissões temporárias.

O exemplo de política a seguir pode ser usado em um perfil que permite que um usuário do EMR Studio use grupos de trabalho do Athena para executar consultas.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDefaultEC2SecurityGroupsCreationInVPCWithEMRTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-
policies": "true"
        }
      }
    }
  ]
}
```

```

    },
    {
      "Sid": "AllowAddingEMRTagsDuringDefaultSecurityGroupCreation",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*:*:security-group/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true",
          "ec2:CreateAction": "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid": "AllowSecretManagerListSecrets",
      "Action": [
        "secretsmanager:ListSecrets"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Sid": "AllowSecretCreationWithEMRTagsAndEMRStudioPrefix",
      "Effect": "Allow",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true"
        }
      }
    },
    {
      "Sid": "AllowAddingTagsOnSecretsWithEMRStudioPrefix",
      "Effect": "Allow",
      "Action": "secretsmanager:TagResource",
      "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*"
    },
    {
      "Sid": "AllowPassingServiceRoleForWorkspaceCreation",

```

```

        "Action": "iam:PassRole",
        "Resource": [
            "arn:aws:iam::111122223333:role/service-
role/AmazonEMRStudio_ServiceRole_Name"
        ],
        "Effect": "Allow"
    },
    {
        "Sid": "AllowS3ListAndLocationPermissions",
        "Action": [
            "s3:ListAllMyBuckets",
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws:s3:::*",
        "Effect": "Allow"
    },
    {
        "Sid": "AllowS3ReadOnlyAccessToLogs",
        "Action": [
            "s3:GetObject"
        ],
        "Resource": [
            "arn:aws:s3:::aws-logs-Your-AWS-Account-ID-Region/
elasticmapreduce/*"
        ],
        "Effect": "Allow"
    },
    {
        "Sid": "AllowAthenaQueryExecutions",
        "Effect": "Allow",
        "Action": [
            "athena:StartQueryExecution",
            "athena:GetQueryExecution",
            "athena:GetQueryResults",
            "athena:StopQueryExecution",
            "athena:ListQueryExecutions",
            "athena:GetQueryResultsStream",
            "athena:ListWorkGroups",
            "athena:GetWorkGroup",
            "athena:CreatePreparedStatement",
            "athena:GetPreparedStatement",
            "athena>DeletePreparedStatement"
        ],
    },

```

```

        "Resource": "*"
    },
    {
        "Sid": "AllowGlueSchemaManipulations",
        "Effect": "Allow",
        "Action": [
            "glue:GetDatabase",
            "glue:GetDatabases",
            "glue:GetTable",
            "glue:GetTables",
            "glue:GetPartition",
            "glue:GetPartitions"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowQueryEditorToAccessWorkGroup",
        "Effect": "Allow",
        "Action": "athena:GetWorkGroup",
        "Resource": "arn:aws:athena:*:111122223333:workgroup*"
    },
    {
        "Sid": "AllowConfigurationForWorkspaceCollaboration",
        "Action": [
            "elasticmapreduce:UpdateEditor",
            "elasticmapreduce:PutWorkspaceAccess",
            "elasticmapreduce>DeleteWorkspaceAccess",
            "elasticmapreduce:ListWorkspaceAccessIdentities"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Condition": {
            "StringEquals": {
                "elasticmapreduce:ResourceTag/creatorUserId":
"${aws:userId}"
            }
        }
    },
    {
        "Sid": "DescribeNetwork",
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeVpcs",
            "ec2:DescribeSubnets",

```

```
        "ec2:DescribeSecurityGroups"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ListIAMRoles",
      "Effect": "Allow",
      "Action": [
        "iam:ListRoles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AssumeRole",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "*"
    }
  ]
}
```

A política de confiança a seguir permite que o EMR Studio assuma o perfil:

 Note

Permissões adicionais são necessárias para aproveitar os EMR Studio Workspaces e os EMR Notebooks. Consulte [Criar políticas de permissões para usuários do EMR Studio](#) para obter mais informações.

Você pode encontrar essas informações nos seguintes links:

- [Defina permissões personalizadas do IAM com políticas gerenciadas pelo cliente](#)
- [Permissões de função de serviço do EMR Studio](#)

Etapa 2. Criar e configurar o EMR Studio

Nesta etapa, você criará um Amazon EMR Studio no console do EMR Studio e usará os perfis do IAM que você criou em [Etapa 1. Criar os perfis do IAM exigidos para o EMR Studio](#).

1. Navegue até o console do EMR Studio, selecione Criar Studio e a opção Configuração personalizada. Você pode criar um bucket S3 ou novo usar um existente. Você pode marcar a caixa Criptografar arquivos do espaço de trabalho com as próprias chaves KMS. Para obter mais informações, consulte [AWS Key Management Service](#).

The screenshot shows the 'Create a Studio' page in the AWS EMR Studio console. The page is divided into several sections:

- Setup options:** Three radio buttons are visible: 'Interactive workloads', 'Batch jobs', and 'Custom'. The 'Custom' option is selected.
- Studio settings:**
 - Studio name:** A text input field containing 'Studio_1'.
 - Description - optional:** A text area with the placeholder 'Describe the Studio'.
- S3 location for Workspace storage:**
 - Text: 'Specify an Amazon S3 location where Workspace work will be saved.'
 - Two radio buttons: 'Create new bucket' (selected) and 'Select existing location'.
 - Text: 'We'll create a new bucket and use the location s3://aws-emr-studio-225989353012-us-east-1/1735848818523.'
 - ☐ **Encrypt Workspace files with your own AWS KMS key**
EMR Studio automatically uses the S3 location's encryption configuration. Choose this option if you want to override the S3 location's encryption configuration with your own AWS KMS key. This key information will not be editable past Studio creation.

2. Em Perfil de serviço para permitir que o Studio acesse os recursos, selecione um perfil de serviço criado em [Etapa 1. Criar os perfis do IAM exigidos para o EMR Studio](#) no menu.
3. Escolha IAM Identity Center em Autenticação. Selecione o perfil de usuário criado em [Etapa 1. Criar os perfis do IAM exigidos para o EMR Studio](#).

Service role to let Studio access your AWS resources

AmazonEMRStudio_

[View permission details](#)

Authentication [Info](#)

Authentication
Choose an authentication method for your Studio.

☐ AWS Identity and Access Management (IAM)
Authenticate with single sign-on using IAM identity federation or IAM credentials.

☒ **IAM Identity Center (AWS Single Sign-On)**
Authenticate with single sign-on using IAM Identity Center (recommended to centrally manage access permissions for multiple AWS accounts).

User role
Each Studio will have a default set of user roles. You can further refine user permissions once you have created a Studio. To create an additional set of permission use [AWS IAM](#).

emrstudio-userrole-idc

[Create IAM role](#)

Connect EMR Studio to IAM Identity Center
instance of IAM Identity Center
Manage access to EMR Studio by assigning users and groups from your Identity Center directory.

[arn:aws:sso::instance/ssoins-](#)

4. Marque a caixa **Propagação de identidade confiável**. Escolha **Somente usuários e grupos** atribuídos na seção **Acesso à aplicação**, o que permitirá que você conceda somente usuários e grupos autorizados a acessar este studio.
5. (Opcional) — Você pode configurar a VPC e a sub-rede se estiver usando este Studio com clusters do EMR.

Trusted identity propagation [Info](#)
Control and log the access that a user has across connected applications.

☒ **Enable trusted identity propagation**
When users make requests to applications that are connected through Identity Center, share their user identity information from EMR Studio. This setting applies for the lifetime of the Studio. You can't turn it off later.

The following features aren't supported from a Studio with trusted identity propagation: creating EMR on EC2 clusters without a template, using EMR Serverless applications, launching EMR on EKS clusters, using a runtime role, and enabling SQL Explorer or Workspace collaboration.

Application access [Info](#)
Choose who can access your application
Specify whether only assigned users and groups can access your application.

☒ **Only assigned users and groups**
Only the users and groups that you specify from your Identity Center directory can access this application.

☐ All users and groups
Any user or group from your IAM Identity Center directory can access this application.

Networking and security - optional

VPC [Info](#)
Select a VPC for your Studio to use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag the VPC with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).

Select a VPC

Subnets [Info](#)
Select the subnets that your Studio can use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag each subnet with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).

6. Revise todos os detalhes e selecione **Criar Studio**.
7. Depois de configurar um cluster do WorkGroup Athena ou do EMR, faça login na URL do Studio para:
 - a. Executar consultas do Athena com o Editor de Consultas.

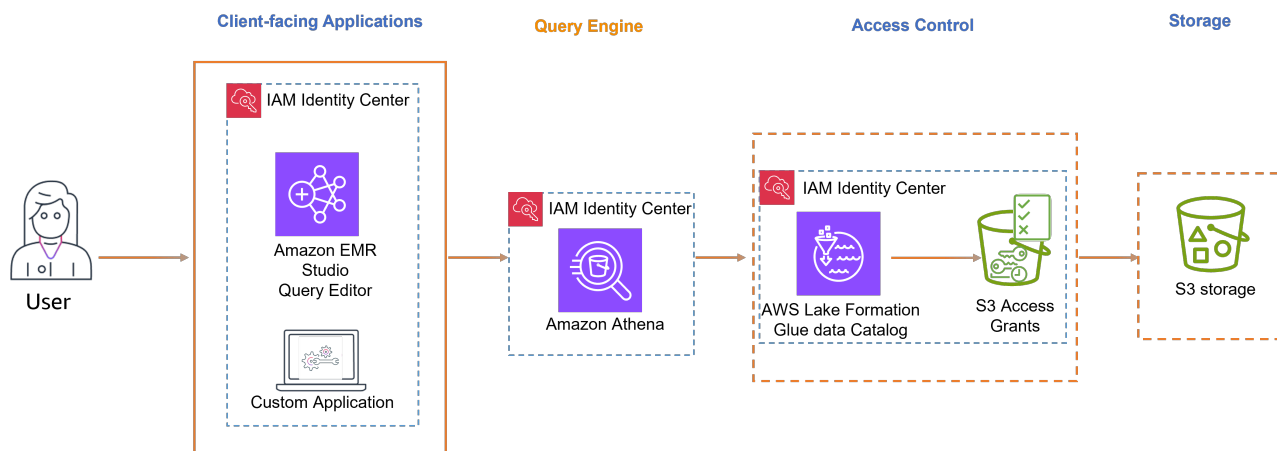
- b. Execute as tarefas do Spark no espaço de trabalho usando o caderno Jupyter.

Propagação de identidade confiável com o Amazon Athena

As etapas para permitir a propagação de identidade confiável dependem de seus usuários interagirem com aplicativos AWS gerenciados ou aplicativos gerenciados pelo cliente. O diagrama a seguir mostra uma configuração confiável de propagação de identidade para aplicativos voltados ao cliente — AWS gerenciados ou externos AWS — que usam o Amazon Athena para consultar dados do Amazon S3 com controle de acesso fornecido pelo Amazon S3. AWS Lake Formation Access Grants

Note

- Propagação de identidade confiável com o Amazon Athena requer o uso do Trino.
- Os clientes Apache Spark e SQL conectados ao Amazon Athena por meio de drivers ODBC e JDBC não são compatíveis.



AWS aplicativos gerenciados

O seguinte aplicativo AWS gerenciado voltado para o cliente oferece suporte à propagação confiável de identidade com o Athena:

- Amazon EMR Studio

Para habilitar a propagação de identidade confiável, siga estas etapas:

- [Configure o Amazon EMR Studio](#) como aplicação voltada para o cliente para o Athena. O Editor de Consultas no EMR Studio é necessário para executar as consultas do Athena quando a propagação de identidade confiável está habilitada.
- [Configure o Athena Workgroup](#).
- [Configure AWS Lake Formation](#) para ativar o controle de acesso refinado para AWS Glue tabelas com base no usuário ou grupo no IAM Identity Center.
- [Configure o Amazon S3 Access Grants](#) para permitir o acesso temporário aos locais de dados subjacentes no S3.

 Note

Tanto o Lake Formation quanto o Amazon S3 Access Grants são necessários para o controle de acesso AWS Glue Data Catalog e para os resultados da consulta do Athena no Amazon S3.

Aplicações gerenciadas pelo cliente

Para habilitar a propagação de identidade confiável para usuários de aplicativos desenvolvidos sob medida, consulte [Access Serviços da AWS programaticamente usando propagação de identidade confiável](#) no Blog de Segurança.AWS

Como configurar a propagação de identidade confiável com grupos de trabalho do Amazon Athena

A procedimento a seguir explica como configurar grupos de trabalho do Amazon Athena para propagação de identidade confiável.

Pré-requisitos

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

1. [Ative o IAM Identity Center](#). A [instância de organização](#) é recomendada. Para obter mais informações, consulte [Pré-requisitos e considerações](#).
2. [Provisione os usuários e grupos da fonte de identidades no IAM Identity Center](#).
3. Essa configuração requer o [Amazon EMR Studio](#) e a [Concessão de Acesso do Amazon S3. AWS Lake Formation](#)

Como configurar a propagação de identidade confiável com o Athena

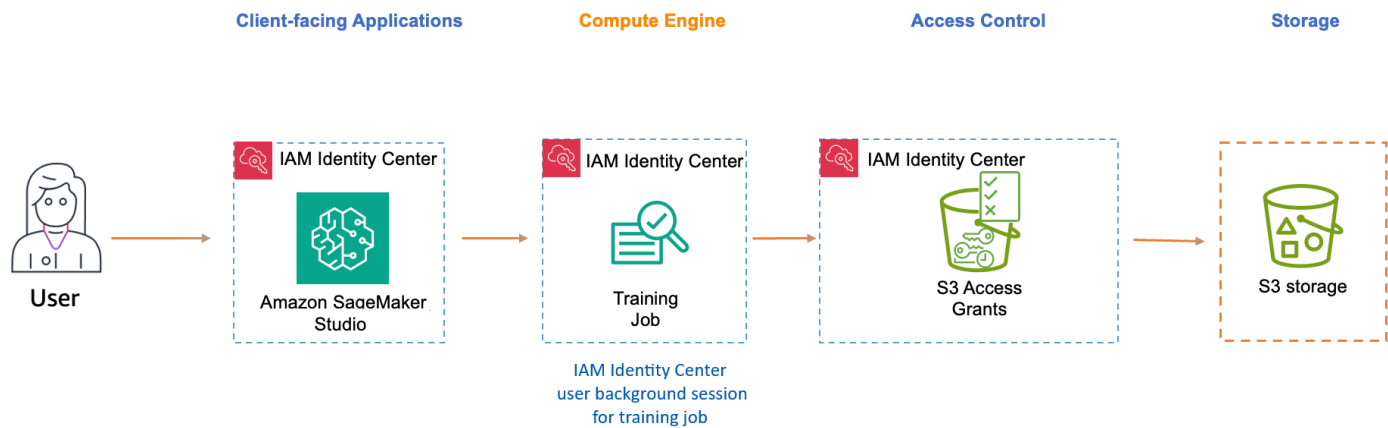
Para configurar a propagação de identidade confiável com o Athena, o administrador do Athena deve:

1. Analise [Considerações e limitações do uso de grupos de trabalho do Athena habilitados para o IAM Identity Center](#).
2. [Crie um grupo de trabalho do Athena habilitado para o IAM Identity Center](#).

Propagação de identidade confiável com o Amazon Studio SageMaker

[O Amazon SageMaker Studio](#) se integra ao IAM Identity Center e oferece suporte a [sessões em segundo plano de usuários](#) e propagação confiável de identidade. As sessões em segundo plano do usuário permitem que um usuário inicie um trabalho de longa duração no SageMaker Studio, sem que o usuário precise permanecer conectado enquanto o trabalho é executado. A tarefa é executada imediatamente e em segundo plano, usando as permissões do usuário que iniciou a tarefa. O trabalho pode continuar em execução mesmo que o usuário desligue o computador, a sessão de login do IAM Identity Center expire ou o usuário saia do AWS portal de acesso. A duração padrão da sessão para as sessões de usuários em segundo plano é de 7 dias, mas você pode especificar uma duração máxima de 90 dias. A propagação de identidade confiável permite que seja fornecido acesso refinado a recursos da AWS como buckets do Amazon S3 com base na identidade do usuário ou na associação ao grupo.

O diagrama a seguir mostra uma configuração confiável de propagação de identidade para o SageMaker Studio, com acesso aos dados armazenados em um bucket do Amazon S3. As sessões em segundo plano do usuário estão habilitadas para o IAM Identity Center, o que permite que o trabalho de treinamento do SageMaker Studio seja executado em segundo plano. O controle de acesso aos dados de treinamento é fornecido pelo Amazon S3 Access Grants.



AWS aplicativo gerenciado

O seguinte aplicativo AWS gerenciado voltado para o cliente oferece suporte à propagação confiável de identidade:

- [SageMaker Estúdio Amazon](#)

Para habilitar a propagação de identidade confiável e as sessões de usuários em segundo plano, siga estas etapas:

- [Configure o SageMaker Studio como o aplicativo voltado para o cliente.](#)
- [Configure o Amazon S3 Access Grants](#) para permitir o acesso temporário aos locais de dados subjacentes no Amazon S3.

Configurando a propagação de identidade confiável com o Studio SageMaker

O procedimento a seguir orienta você na configuração do SageMaker Studio para propagação confiável de identidade e sessões em segundo plano do usuário.

Pré-requisitos

Antes de começar este tutorial, você precisará concluir as seguintes tarefas:

1. [Ative o IAM Identity Center.](#) É exigida uma instância de organização. Para obter mais informações, consulte [Pré-requisitos e considerações.](#)
2. [Provisione os usuários e grupos da fonte de identidades no IAM Identity Center.](#)

3. [Confirme se as sessões de usuários em segundo plano estão habilitadas](#) no console do IAM Identity Center. Por padrão, as sessões de usuários em segundo plano estão habilitadas e a duração da sessão é definida como 7 dias. Você pode alterar essa duração.

Para configurar a propagação de identidade confiável do SageMaker Studio, o administrador do SageMaker Studio deve executar as etapas a seguir.

Etapa 1: Habilitar a propagação de identidade confiável em um domínio do SageMaker Studio novo ou existente

SageMaker O Studio usa domínios para organizar perfis de usuário, aplicativos e seus recursos associados. Para habilitar a propagação de identidade confiável, você deve criar um domínio do SageMaker Studio ou modificar um domínio existente conforme descrito no procedimento a seguir.

1. Abra o console do SageMaker AI, navegue até Domínios e siga um dos procedimentos a seguir.
 - Crie um novo domínio do SageMaker Studio usando a [Configuração para organizações](#).

Escolha Configurar para organizações e, em seguida, faça o seguinte:

- Escolha AWS Identity Center como método de autenticação.
- Marque a caixa de seleção Habilitar propagação de identidade confiável para todos os usuários neste domínio.
- Modifique um domínio do SageMaker Studio existente.
 - Selecione um domínio existente que use o IAM Identity Center para autenticação.

 Important

A propagação de identidade confiável só é suportada em domínios do SageMaker Studio que usam o IAM Identity Center para autenticação. Se o domínio usar o IAM para autenticação, você não poderá alterar o método de autenticação e, portanto, não poderá habilitar a propagação de identidade confiável.

- [Editar configurações de domínio](#) Edite as configurações de Autenticação e permissões para permitir a propagação de identidade confiável.
2. Vá para a [Etapa 2: configurar o perfil de execução de domínio padrão](#). Essa função é necessária para que os usuários de um domínio do SageMaker Studio acessem outros AWS serviços, como o Amazon S3.

Etapa 2: configure o perfil de execução do domínio padrão e a política de confiança do perfil

Uma função de execução de domínio é uma [função do IAM](#) que um domínio do SageMaker Studio assume em nome de todos os usuários no domínio. As permissões que você atribui a essa função determinam quais ações o SageMaker Studio pode realizar.

1. Para criar ou selecionar um perfil de execução de domínio, execute uma das seguintes ações:
 - Crie ou selecione um perfil usando a [Configuração para organizações](#).
 - Abra o console de SageMaker IA e siga as orientações do console na Etapa 2: Configurar funções e atividades de ML para criar uma nova função de execução de domínio ou selecionar uma função existente.
 - Conclua o restante das etapas de configuração para criar seu domínio do SageMaker Studio.
 - Crie um perfil de execução manualmente.
 - Abra o console do IAM e [crie o perfil de execução](#).
2. [Atualize a política de confiança](#) anexada ao perfil de execução do domínio para que ela inclua as duas ações a seguir: [sts:AssumeRole](#) e [sts:SetContext](#). Para obter informações sobre como encontrar a função de execução do seu domínio SageMaker Studio, consulte [Obter função de execução do domínio](#).

Uma política de confiança especifica a identidade que pode assumir um perfil. Essa política é necessária para permitir que o serviço SageMaker Studio assuma a função de execução do domínio. Adicione essas duas ações para que elas apareçam da seguinte forma na política.

```
{

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

  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "sagemaker.amazonaws.com"
        ]
      },
      "Action": [
```



```

        "sts:AssumeRole",
        "sts:SetContext"
    ]
}

```

Etapa 3: verificar as permissões exigidas da Concessão de Acesso do Amazon S3 para o perfil de execução do domínio

Para usar o Amazon S3 Access Grants, você deve ter uma política de permissões anexada (como uma política embutida ou uma política gerenciada pelo cliente) à sua função de execução de domínio do SageMaker Studio que contenha as seguintes permissões.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
    }
  ]
}

```

Se você não tiver uma política que contenha essas permissões, siga as instruções em [Adicionar e remover permissões de identidade do IAM](#) no Guia do usuário do AWS Identity and Access Management .

Etapa 4: atribuir grupos e usuários ao domínio

Atribua grupos e usuários ao domínio do SageMaker Studio seguindo as etapas em [Adicionar grupos e usuários](#).

Etapa 5: configurar a Concessão de Acesso do Amazon S3

Para configurar a Concessão de Acesso do Amazon S3, siga as etapas em [Como configurar Concessão de Acesso do Amazon S3 para propagação de identidade confiável por meio do IAM Identity Center](#). Use as step-by-step instruções para concluir as seguintes tarefas:

1. Crie instâncias de Concessão de Acesso do Amazon S3.
2. Registre um local nessa instância.
3. Crie subsídios para permitir que usuários ou grupos específicos do IAM Identity Center acessem locais ou subconjuntos designados do Amazon S3 (por exemplo, prefixos específicos) dentro desses locais.

Etapa 6: enviar um trabalho de SageMaker treinamento e visualizar os detalhes da sessão em segundo plano do usuário

No SageMaker Studio, lance um novo notebook Jupyter e envie um trabalho de treinamento. Enquanto a tarefa estiver em execução, conclua as etapas a seguir para visualizar as informações da sessão e verificar se o contexto da sessão de usuário em segundo plano está ativo.

1. Abra o console do IAM Identity Center.
2. Selecione Usuários.
3. Na página Usuários, escolha o nome 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 desse usuário.
5. Para pesquisar sessões pelo nome do recurso da Amazon (ARN) da tarefa que está usando a sessão, na lista Tipo de sessão, escolha Sessões de usuários em segundo plano e insira o ARN da tarefa na caixa de pesquisa.

Veja a seguir um exemplo de como uma tarefa de treinamento usando uma sessão de usuário em segundo plano aparece na aba Sessões ativas para um usuário.

Profile
Groups (0)
AWS accounts
Applications
MFA devices (1)
Active sessions (5)

Active sessions (5)
End sessions

You can end any of the active sessions in this list. The list shows all active sessions initiated by wei_zhang [Learn more](#)

Session type
All

< 1 >

☐	Client	Session type	Used by	IP address
☐	-	User background se...	arn:aws:sagemaker:us-west-2:777788889999:training-job/trustedidprop-trjob-12345a6b	-

Etapa 7: Exibir os CloudTrail registros para verificar a propagação de identidade confiável no CloudTrail

Quando a propagação de identidade confiável está ativada, as ações aparecem nos registros de CloudTrail eventos abaixo do `onBehalfOf` elemento. O `userId` reflete a ID do usuário do IAM Identity Center que iniciou a tarefa de treinamento. O CloudTrail evento a seguir captura o processo de propagação de identidade confiável.

```

      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AR0A123456789EXAMPLE:SageMaker",
        "arn": "arn:aws:sts::111122223333:assumed-role/SageMaker-
ExecutionRole-20250728T125817/SageMaker",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AR0A123456789EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/service-role/SageMaker-
ExecutionRole-20250728T125817",
            "accountId": "111122223333",
            "userName": "SageMaker-ExecutionRole-20250728T125817"
          },
          "attributes": {
            "creationDate": "2025-07-29T17:17:10Z",
            "mfaAuthenticated": "false"
          }
        },
        "onBehalfOf": {
          "userId": "2801d3e0-f0e1-707f-54e8-f558b19f0a10",

```

```
"identityStoreArn": "arn:aws:identitystore::777788889999:identitystore/d-1234567890"
  }
},
```

Considerações sobre runtime

Se um administrador definir trabalhos `MaxRuntimeInSeconds` de treinamento ou processamento de longa duração que sejam inferiores à duração da sessão em segundo plano do usuário, o SageMaker Studio executará o trabalho pelo mínimo de uma `MaxRuntimeInSeconds` ou da duração da sessão em segundo plano do usuário.

Para obter mais informações sobre `MaxRuntimeInSeconds`, consulte a orientação para o `CreateTrainingJob` [StoppingCondition](#) parâmetro na Amazon SageMaker API Reference.

Serviços de autorização

Em todos os [casos de uso de analytics e data lakehouse](#), você pode obter controles de acesso refinados usando:

- AWS Lake Formation - para obter orientação, consulte [Configuração AWS Lake Formation com o IAM Identity Center](#).
- Amazon S3 Access Grants — Para obter orientação, consulte. [Como configurar a Concessão de Acesso do Amazon S3 com o IAM Identity Center](#)

Configuração AWS Lake Formation com o IAM Identity Center

[AWS Lake Formation](#) é um serviço gerenciado que simplifica a criação e o gerenciamento de data lakes na AWS. Ele automatiza a coleta, catalogação e segurança de dados, fornecendo um repositório centralizado para armazenar e analisar diversos tipos de dados. O Lake Formation oferece controles de acesso refinados e se integra a vários serviços de AWS análise, permitindo que as organizações configurem, protejam e obtenham insights de seus data lakes com eficiência.

Siga estas etapas para permitir que o Lake Formation conceda permissões de dados com base na identidade do usuário usando o IAM Identity Center e a propagação de identidade confiável.

Pré-requisitos

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

- [Ative o IAM Identity Center](#). A [instância de organização](#) é recomendada. Para obter mais informações, consulte [Pré-requisitos e considerações](#).

Etapas para configurar a propagação de identidade confiável

1. Integre o IAM Identity Center ao AWS Lake Formation seguindo as orientações em [Como conectar o Lake Formation ao IAM Identity Center](#).

 Important

Se você não tiver tabelas AWS Glue Data Catalog, deverá criá-las para usar o AWS Lake Formation para conceder acesso aos usuários e grupos do IAM Identity Center. Consulte [Como criar objetos no AWS Glue Data Catalog](#) para obter mais informações.

2. Registre os locais de data lake.

[Registre os locais do S3](#) em que os dados das tabelas Glue são armazenados. Ao fazer isso, o Lake Formation provisionará acesso temporário aos locais necessários do S3 quando as tabelas forem consultadas, eliminando a necessidade de incluir permissões do S3 na função de serviço (por exemplo, a função de serviço Athena configurada no). WorkGroup

- a. Navegue até os locais do Data Lake na seção Administração no painel de navegação do AWS Lake Formation console. Selecione Registrar local.

Isso permitirá que o Lake Formation provisione credenciais temporárias do IAM com as permissões necessárias para acessar os locais de dados do S3.

Register location

Amazon S3 location
Register an Amazon S3 path as the storage location for your data lake.

Amazon S3 path
Choose an Amazon S3 path for your data lake.

Review location permissions - strongly recommended
Registering the selected location may result in your users gaining access to data already at that location. Before registering a location, we recommend that you review existing location permissions on resources in that location.

IAM role
To add or update data, Lake Formation needs read/write access to the chosen Amazon S3 path. Choose a role that you know has permission to do this, or choose the `AWSServiceRoleForLakeFormationDataAccess` service-linked role. When you register the first Amazon S3 path, the service-linked role and a new inline policy are created on your behalf. Lake Formation adds the first path to the inline policy and attaches it to the service-linked role. When you register subsequent paths, Lake Formation adds the path to the existing policy.

☐ **Enable Data Catalog Federation**
Checking this box will allow Lake Formation to assume a role to access tables in a federated database.

Permission mode
Select the permission mode you want to use to manage access.

☒ **Hybrid access mode**
Lake Formation permissions can co-exist with IAM permission policies for AWS Glue and S3 actions to manage access.
[Learn more](#)

☐ **Lake Formation**
Only Lake Formation permissions are enforced.

- b. Insira o caminho S3 dos locais de dados das tabelas AWS Glue no campo Caminho do Amazon S3.
- c. Na seção Perfil do IAM, não selecione o perfil vinculado ao serviço se quiser usá-lo com a propagação de identidade confiável. Crie um perfil separado com as seguintes permissões.

Para usar essas políticas, substitua a política *italicized placeholder text* no exemplo por suas próprias informações. Para obter instruções adicionais, consulte [Criar uma política](#) ou [Editar uma política](#). A política de permissão deve conceder acesso ao local do S3 especificado no caminho:

- i. Política de permissão:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
```

```

        "arn:aws:s3:::Your-S3-Bucket/*"
    ],
    },
    {
        "Sid":
        "LakeFormationDataAccessPermissionsForS3ListBucket",
        "Effect": "Allow",
        "Action": [
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::Your-S3-Bucket"
        ]
    },
    {
        "Sid": "LakeFormationDataAccessServiceRolePolicy",
        "Effect": "Allow",
        "Action": [
            "s3:ListAllMyBuckets"
        ],
        "Resource": [
            "arn:aws:s3:::*"
        ]
    }
}

```

- ii. Relação de confiança: deve incluir `sts:SectContext`, exigido para a propagação de identidade confiável.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "lakeformation.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",

```

```
    "sts:SetContext"  
  ]  
}  
]
```

Note

O perfil do IAM criado pelo assistente é um perfil vinculado ao serviço e não inclui `sts:SetContext`.

- d. Depois de criar o perfil do IAM, selecione Registrar local.

Propagação de identidade confiável com Lake Formation em todo o lado Contas da AWS

AWS Lake Formation suporta o uso [AWS Resource Access Manager \(RAM\)](#) para compartilhar tabelas Contas da AWS e funciona com propagação de identidade confiável quando a conta do concedente e a conta do beneficiário estão na mesma Região da AWS, na mesma e compartilham a mesma AWS Organizations instância organizacional do IAM Identity Center. Consulte [Compartilhamento de dados entre contas no Lake Formation](#) para obter mais informações.

Como configurar a Concessão de Acesso do Amazon S3 com o IAM Identity Center

O [Amazon S3 Access Grants](#) oferece a flexibilidade de conceder controle de acesso refinado baseado em identidade aos locais do S3. Você pode usar o Amazon S3 Access Grants para conceder acesso ao bucket do Amazon S3 diretamente aos usuários e grupos corporativos. Siga estas etapas para habilitar o S3 Access Grants com o IAM Identity Center e obter uma propagação de identidade confiável.

Pré-requisitos

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

- [Ative o IAM Identity Center](#). A [instância de organização](#) é recomendada. Para obter mais informações, consulte [Pré-requisitos e considerações](#).

Como configurar a Concessão de acesso do S3 para propagação de identidade confiável por meio do IAM Identity Center

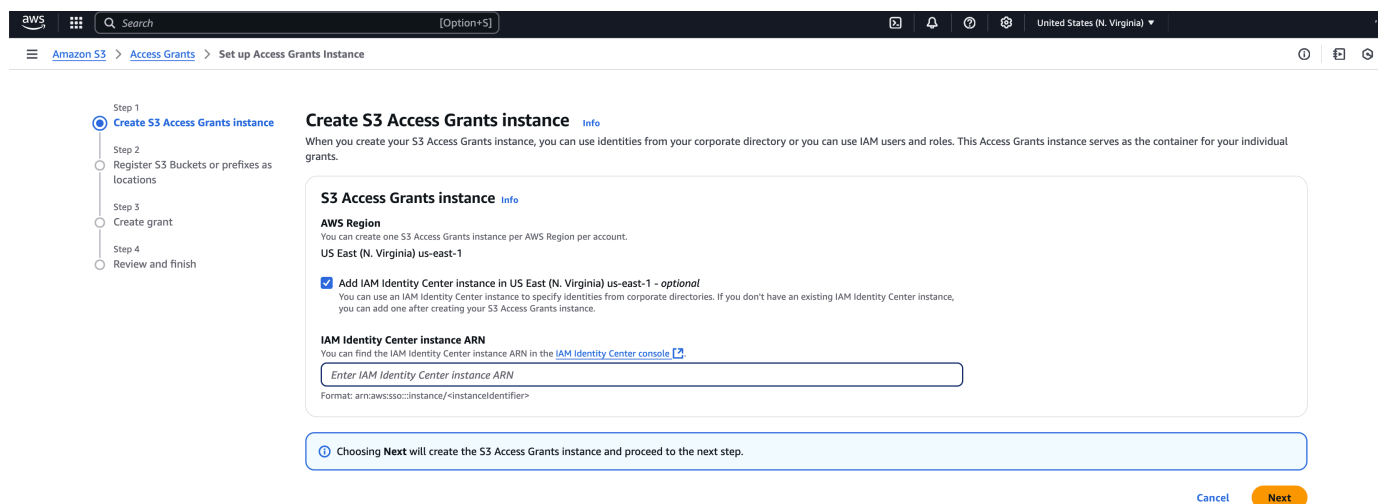
Se você já tiver uma instância do Amazon S3 Access Grants com um local registrado, siga estas etapas:

1. [Associe a instância do IAM Identity Center.](#)
2. [Crie uma concessão](#)

Se você ainda não criou uma Amazon S3 Access Grants, siga estas etapas:

1. [Crie uma Access Grants instância S3](#) - Você pode criar uma Access Grants instância S3 por Região da AWS. Ao criar a instância de S3 Access Grants, certifique-se de marcar a caixa Adicionar instância do IAM Identity Center e fornecer o ARN da instância do IAM Identity Center. Escolha Próximo.

A imagem a seguir mostra a página Criar instância de S3 Access Grants no console do Amazon S3 Access Grants:



2. Registre um local - Depois de criar e [criar uma Access Grants instância do Amazon S3](#) Região da AWS em sua conta, você [registra um local do S3 nessa](#) instância. Um local do S3 Access Grants mapeia a região padrão do S3 (S3://), um bucket ou um prefixo a um perfil do (IAM). O S3 Access Grants assume esse perfil do Amazon S3 para distribuir credenciais temporárias ao beneficiário que está acessando esse local específico. Primeiro, é necessário registrar pelo menos um local na instância do S3 Access Grants para poder criar uma concessão de acesso.

Para Escopo do local, especifique `s3://`, o que inclui todos os buckets nessa região. Esse é o escopo de local recomendado para a maioria dos casos de uso. Se você tiver um caso de uso de gerenciamento de acesso avançado, poderá definir o escopo do local para um bucket `s3://bucket` ou prefixo específico dentro de um bucket `s3://bucket/prefix-with-path`. Para obter mais informações, consulte [Registrar um local](#) no Guia do usuário do Amazon Simple Storage Service.

 Note

Certifique-se de que as localizações S3 das AWS Glue tabelas às quais você deseja conceder acesso estejam incluídas nesse caminho.

O procedimento exige que você configure um perfil do IAM para o local. Esse perfil deve incluir permissões para acessar o escopo do local. Você pode usar o assistente do console do S3 para criar o perfil. Você precisará especificar o ARN da instância do S3 Access Grants nas políticas desse perfil do IAM. O valor padrão do ARN da instância do S3 Access Grants é `arn:aws:s3:Your-Region:Your-AWS-Account-ID:access-grants/default`.

O exemplo de política de permissões a seguir concede permissões ao Amazon S3 para o perfil do IAM que você criou. E a política de confiança de exemplo a seguir permite que a entidade principal de serviço do S3 Access Grants assumo o perfil do IAM.

a. Política de permissão

Para usar essas políticas, substitua a política *italicized placeholder text* no exemplo por suas próprias informações. Para obter instruções adicionais, consulte [Criar uma política](#) ou [Editar uma política](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
      "Effect": "Allow",
      "Action": [
```

```

        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
    ],
    "Resource": [
        "arn:aws:s3:::*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "111122223333"
        },
        "ArnEquals": {
            "s3:AccessGrantsInstanceArn": [
                "arn:aws:s3:::access-grants/instance-id"
            ]
        }
    }
},
{
    "Sid": "ObjectLevelWritePermissions",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:AbortMultipartUpload"
    ],
    "Resource": [
        "arn:aws:s3:::*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "111122223333"
        },
        "ArnEquals": {
            "s3:AccessGrantsInstanceArn": [
                "arn:aws:s3:::access-grants/instance-id"
            ]
        }
    }
}

```

```

    },
    {
      "Sid": "BucketLevelReadPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "111122223333"
        },
        "ArnEquals": {
          "s3:AccessGrantsInstanceArn": [
            "arn:aws:s3:::access-grants/instance-id"
          ]
        }
      }
    },
    {
      "Sid": "OptionalKMSPermissionsForSSEEncryption",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}

```

b. Política de confiança

Na política de confiança do perfil do IAM, dê à entidade principal do serviço Concessão de Acesso do S3 (`access-grants.s3.amazonaws.com`) acesso ao perfil do IAM que você criou. Para fazer isso, você pode criar um arquivo JSON que contém as instruções a seguir. Para adicionar a política de confiança à sua conta, consulte [Criar uma função usando políticas de confiança personalizadas](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "aws:SourceArn": "Your-Custom-Access-Grants-Location-ARN"
        }
      }
    },
    {
      "Sid": "Stmt1234567891012",
      "Effect": "Allow",
      "Action": "sts:SetContext",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333",
          "aws:SourceArn": "Your-Custom-Access-Grants-Location-ARN"
        },
        "ForAllValues:ArnEquals": {
          "sts:RequestContextProviders":
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
        }
      }
    }
  ]
}
```

Criar uma Concessão de Acesso do Amazon S3

Se você tiver uma instância do Amazon S3 Access Grants com um local registrado e tiver associado a instância do IAM Identity Center a ela, poderá [criar uma concessão](#). Na página Criar concessão do console do S3, conclua o seguinte:

Criar uma concessão

1. Selecione o local criado na etapa anterior. Você pode reduzir o escopo da concessão adicionando um subprefixo. O subprefixo pode ser um bucket, bucket/prefix ou um objeto no bucket. Para obter mais informações, acesse [Subprefixo](#) no Guia do usuário do Amazon Simple Storage Service.
2. Em Permissões e acesso, selecione Ler e/ou Gravar de acordo com as necessidades.
3. Em Tipo de concedente, escolha Identidade de diretório no IAM Identity Center.
4. Forneça o ID de usuário ou grupo do IAM Identity Center. Você pode encontrar o usuário e o grupo IDs no console do IAM Identity Center [nas seções Usuário e Grupo](#). Escolha Próximo.
5. Na página Revisar e concluir, revise as configurações do S3 Access Grant e selecione Criar concessão.

A imagem a seguir mostra a página Criar concessão no console do Amazon S3 Access Grants:

The screenshot shows the 'Create Grant' page in the AWS S3 Access Grants console. The page is titled 'Create Grant' and includes a breadcrumb trail: 'Amazon S3 > Access Grants > US East (N. Virginia) us-east-1: default > Create Grant'. The main content area is divided into several sections:

- Grant scope:** This section explains that the grant scope is a combination of the location and the subprefix. It includes a 'Location' field with a value of 's3://' and a 'Subprefix - optional' field with a value of 'bucket-name/prefix/'. There are buttons for 'Browse locations' and 'Register location'. A note states: 'Don't include any part of the grant already specified in the location. Format for bucket: <bucket>/* Format for prefix: <bucket>/<prefix>-with-path/* Format for object: <bucket>/<prefix>-with-path/<object>'.
- Grant scope:** This section includes a checkbox for 'The grant scope is an object' which is currently unchecked.
- Permissions and access:** This section includes a warning: 'The S3 console can't be used to access the data specified in the grant scope. To access the data, the grantee must do so through the AWS CLI, the application, or other AWS services.' Below this, there are checkboxes for 'Read' (checked) and 'Write' (unchecked).
- Grantee type:** This section includes a radio button for 'Directory identity from IAM Identity Center' (selected) and a radio button for 'IAM principal'.
- Directory identity type:** This section includes radio buttons for 'User' and 'Group' (selected).
- IAM Identity Center group ID:** This section includes a text input field for 'Enter group ID'.

Configurando seu próprio aplicativo OAuth 2.0

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 fazer login em uma aplicação gerenciada pelo cliente e essa aplicação pode transmitir a identidade do usuário em solicitações para acessar dados nos Serviços da AWS.

Important

Para acessar um AWS service (Serviço da AWS), os aplicativos gerenciados pelo cliente devem obter um token de um emissor de token confiável, externo ao IAM Identity Center. Um emissor de token confiável é um servidor de autorização OAuth 2.0 que cria tokens assinados. Esses tokens autorizam aplicativos que iniciam solicitações de acesso Serviços da AWS (recebimento de aplicativos). Para obter mais informações, consulte [Usar aplicações com um emissor de tokens confiáveis](#).

Tópicos

- [Configure aplicativos OAuth 2.0 gerenciados pelo cliente para propagação confiável de identidade](#)
- [Especificar aplicações confiáveis](#)
- [Usar aplicações com um emissor de tokens confiáveis](#)

Configure aplicativos OAuth 2.0 gerenciados pelo cliente para propagação confiável de identidade

Para configurar um aplicativo OAuth 2.0 gerenciado pelo cliente para propagação confiável de identidade, você deve primeiro adicioná-lo 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 aplicativo, 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 da aplicação, em Nome e descrição da aplicação, insira um Nome de exibição para a aplicação, 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 do aplicativo — O bloco do aplicativo é visível para todos os usuários que entram no portal de AWS acesso, a menos que a visibilidade do aplicativo no portal de AWS acesso esteja definida como Não visível.

3. Em portal de AWS acesso, insira a URL na qual os usuários podem acessar o aplicativo e especifique se o mosaico do aplicativo ficará visível ou não no portal de AWS acesso. 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 [Recursos de marcação Centro de Identidade do AWS IAM](#).

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 um aplicativo gerenciado pelo cliente que suporte OAuth 2.0 ao IAM Identity Center, você deve especificar um emissor de token confiável. Um emissor de token confiável é um servidor de autorização OAuth 2.0 que cria tokens assinados. Esses tokens autorizam as aplicações que iniciam as solicitações (aplicações solicitantes) a acessar as aplicações gerenciadas pela AWS (aplicações receptoras).

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 obter mais informações, consulte [Declaração de Aud](#).
3. Para evitar que os usuários precisem ser autenticados novamente quando estiverem usando essa aplicação, selecione Habilitar concessão de tokens de atualização. 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 recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo.

Essa política exige a ação de API [CreateTokenWithIAM](#). Para obter mais informações sobre essa política e um exemplo que você pode adaptar conforme exigido ao ambiente, consulte [Exemplo de política baseada em recursos para o IAM Identity Center](#).

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 [Acesso entre contas usando políticas baseadas em recursos](#) e [IAM ARNs no Guia do usuário.AWS Identity and Access Management](#)

- 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 Serviços da AWS 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 obter 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 de aplicativos gerenciados pelo cliente, selecione o aplicativo OAuth 2.0 que 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 todas 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 esses aplicativos a fazer solicitações em nome de seus usuários para acessar aplicativos AWS gerenciados.

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](#)
- [Pré-requisitos e considerações para emissores de tokens confiáveis](#)
- [Detalhes da declaração JTI](#)
- [Configurações de emissor de tokens confiáveis](#)
- [Configurar um emissor de tokens confiáveis](#)
- [Sessões de perfil do IAM aprimoradas com identidade](#)

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 token confiável é um servidor de autorização OAuth 2.0 que cria tokens assinados. Esses tokens autorizam aplicativos que iniciam solicitações (solicitando aplicativos) para acesso Serviços da AWS (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.

Serviços da AWS 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. Serviços da AWS não pode usar os tokens diretamente 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 receptora. Como o novo token referencia o usuário correspondente no IAM Identity Center, a aplicação receptora 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 token confiável é uma decisão de segurança que requer uma análise 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 receptora.
- 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 tokens confiáveis seja normalmente o provedor de identidades que você usa como fonte de identidades para o IAM Identity Center, não precisa ser. Para obter informações

sobre como configurar o emissor de tokens confiáveis, consulte a documentação do provedor de identidades 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 confiável do token) que cria o token deve ter um endpoint de descoberta do [OpenID Connect \(OIDC\)](#) que o IAM Identity Center possa usar para obter chaves públicas para verificar as assinaturas do token. Para obter mais informações, consulte [URL do endpoint de descoberta OIDC \(URL do emissor\)](#).
- Tokens emitidos pelo emissor de tokens confiáveis

Os tokens do emissor de tokens confiáveis devem atender aos seguintes requisitos:

- O token deve ser assinado e estar no formato [JSON Web Token \(JWT\)](#) usando o RS256 algoritmo.
- O token deve conter as seguintes declarações:
 - [Emissor](#) (iss): a entidade que emitiu o token. Esse valor deve corresponder ao valor configurado no endpoint de descoberta OIDC (URL do emissor) no emissor de tokens confiáveis.
 - [Assunto](#) (sub): o usuário autenticado.
 - [Público](#) (aud): o destinatário pretendido do token. Esse é o AWS service (Serviço da AWS) que será acessado após o token ser trocado por um token do IAM Identity Center. Para obter mais informações, consulte [Declaração de Aud](#).
 - [Tempo de validade](#) (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.

 Note

Não há suporte para o uso de uma chave JWTs de Microsoft Entra ID assinatura personalizada para from. Para usar tokens do Microsoft Entra ID com um emissor de token confiável, você não pode usar uma chave de assinatura personalizada.

- 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.

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 reivindicação de JTI aos tokens. Alguns servidores de autorização OAuth 2.0 podem não permitir que você adicione uma JTI como uma declaração personalizada. OAuth Os servidores de autorização 2.0 que suportam o uso de uma declaração de 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 seu 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 OIDC \(URL do emissor\)](#)
- [Mapeamento de atributos](#)
- [Declaração de Aud](#)

URL do endpoint de descoberta 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 o URL do endpoint de descoberta até e sem `.well-known/openid-configuration`. Se `.well-known/openid-configuration` for incluída no URL, a configuração do emissor de tokens confiáveis não funcionará. Como o IAM Identity Center não valida esse URL, se o URL não estiver formado corretamente, a configuração do emissor de tokens confiáveis falhará sem notificação.

O URL do endpoint de descoberta OIDC só deve ser acessível pelas portas 80 e 443.

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 a URL, consulte a documentação do provedor de servidor de autorização OAuth 2.0 que você usa para gerar tokens para seu aplicativo ou entre em contato diretamente com o provedor para obter assistência.

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 token confiável é um servidor de autorização OAuth 2.0 que emite tokens para aplicativos que iniciam solicitações (solicitando aplicativos). Os tokens autorizam esses aplicativos a iniciar solicitações em nome de seus usuários para um aplicativo receptor (an AWS service (Serviço da AWS)).

Tópicos

- [Coordenar perfis e responsabilidades administrativas](#)
- [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 obter mais informações, consulte [Tarefas para configurar um emissor de tokens confiáveis](#).

Perfil	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.	Administrador do IdP (emissor de tokens confiáveis) externo
	Ajuda a configurar o mapeamento correto dos atributos entre o IAM Identity Center e o IdP externo.	AWS administrador do serviço
	Notifica o administrador do AWS serviço quando o emissor de token	

Perfil	Executa essas tarefas	Coordena com
	confiável é adicionado ao console do IAM Identity Center.	
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. Fornecer 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 confiável do token ficará visível no console de AWS serviço 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. Adicione o emissor de token confiável ao IAM Identity Center — O administrador do IAM Identity Center [adiciona o emissor de token confiável usando o console do IAM Identity Center](#) ou. [APIs](#)
Essa configuração requer a especificação do seguinte:
 - Um nome de 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). O endpoint de descoberta só deve ser acessível pelas portas 80 e 443.
 - 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 do aplicativo APIs.

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 confiável do token coloca o valor da reivindicação Aud no token que ele emite para indicar que o token se destina ao uso pelo AWS serviço. 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 IAM Identity Center](#).
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:

- Em URL do emissor, especifique o [URL de descoberta OIDC](#) do IdP externo que emitirá tokens para a propagação de identidade confiável. Você deve especificar o URL do endpoint de descoberta até e sem `.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 identidades confiáveis.

- 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 [Recursos de marcação Centro de Identidade do AWS IAM](#).

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.

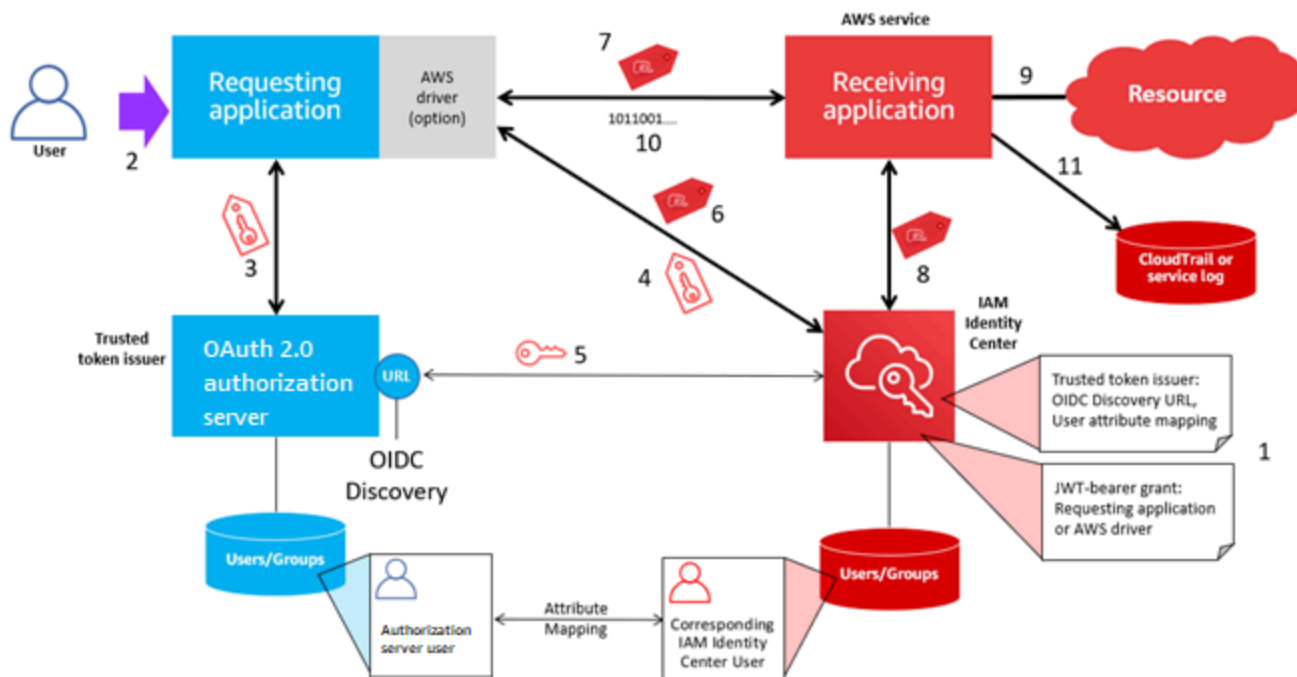
Se você pretende editar as configurações do emissor de tokens confiáveis, lembre-se de que isso pode fazer com que os usuários percam o acesso a qualquer aplicação configurada para usar o emissor de tokens confiáveis. Para evitar interromper o acesso dos usuários, recomendamos que você coordene com os 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 IAM Identity Center](#).
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, será solicitado que você confirme se deseja fazer alterações. Escolha 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 receptora. 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 usar um driver da AWS, 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 receptora. 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 o aplicativo AWS gerenciado estiver configurado 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 receptora e passa o token que o IAM Identity Center gerou para a aplicação receptora.
8. A aplicação receptora 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 receptora 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 receptora responderá à solicitação.
11. A identidade do usuário, as ações realizadas em seu nome e outros eventos são registrados nos registros e CloudTrail eventos do aplicativo receptor. O modo específico como essas informações são registradas varia de acordo com a aplicação.

Sessões de perfil do IAM aprimoradas com identidade

O [AWS Security Token Service](#) (STS) permite que uma aplicação obtenha uma sessão de perfil do IAM de identidade avançada. As sessões de função aprimorada com identidade têm um contexto de identidade adicional que carrega um identificador de usuário para AWS service (Serviço da AWS) aquele que ela chama. Serviços da AWS pode pesquisar as associações de grupo e os atributos do usuário no IAM Identity Center e usá-los para autorizar o acesso do usuário aos recursos.

AWS os aplicativos obtêm sessões de função aprimoradas com identidade fazendo solicitações à ação da AWS STS [AssumeRole](#) API e transmitindo uma declaração de contexto com o identificador do usuário (userId) no `ProvidedContexts` parâmetro da solicitação para `AssumeRole`. A declaração de contexto é obtida da reivindicação `idToken` recebida em resposta a uma solicitação a SSO OIDC para [CreateTokenWithIAM](#). Quando um AWS aplicativo usa uma sessão de função com identidade aprimorada para acessar um recurso, CloudTrail registra `userId` a sessão inicial e a ação realizada. Para obter mais informações, consulte [Registro em log de sessão de perfil do IAM aprimorado com identidade](#).

Tópicos

- [Tipos de sessões de perfil do IAM aprimoradas com identidade](#)
- [Registro em log de sessão de perfil do IAM aprimorado com identidade](#)

Tipos de sessões de perfil do IAM aprimoradas com identidade

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 As aplicações que obtiveram tokens de ID do IAM Identity Center podem adicionar `sts:identity_context` (recomendado) ou `sts:audit_context` (compatível em versões anteriores) às sessões de perfil do IAM. Uma sessão de perfil do IAM de identidade avançada só pode ter uma dessas asserções de contexto, não ambas.

Sessões de perfil do IAM aprimoradas com identidade criadas com o **`sts:identity_context`**

Quando uma sessão de perfil de identidade avançada contém `sts:identity_context`, o AWS service (Serviço da AWS) chamado determina se a autorização do recurso é baseada no usuário representado na sessão de perfil ou se é baseada no perfil. O Serviços da AWS que oferece suporte à autorização baseada no usuário fornece ao administrador da aplicação controles para atribuir acesso ao usuário ou aos grupos dos quais o usuário é membro.

Serviços da AWS que não oferecem suporte à autorização baseada no usuário, desconsidere o. `sts:identity_context` CloudTrail registra o UserID do usuário do IAM Identity Center com todas as ações realizadas pela função. Para obter mais informações, consulte [Registro em log de sessão de perfil do IAM aprimorado com identidade](#).

Para obter esse tipo de sessão de função com identidade aprimorada AWS STS, os aplicativos fornecem o valor do `sts:identity_context` campo na [AssumeRole](#) solicitação usando o parâmetro de `ProvidedContexts` solicitação. Use `arn:aws:iam::aws:contextProvider/IdentityCenter` como valor de `ProviderArn`.

Para obter mais informações sobre como a autorização se comporta, consulte a documentação do recebimento. AWS service (Serviço da AWS)

Sessões de perfil do IAM aprimoradas com identidade criadas com o **`sts:audit_context`**

No passado, `sts:audit_context` era usado para permitir registrar Serviços da AWS a identidade do usuário sem usá-la para tomar uma decisão de autorização. Serviços da AWS agora são capazes de usar um único contexto - `sts:identity_context` - para conseguir isso, bem como para tomar decisões de autorização. Recomendamos usar `sts:identity_context` em todas as novas implantações de propagação de identidade confiável.

Registro em log de sessão de perfil do IAM aprimorado com identidade

Quando uma solicitação é feita para AWS service (Serviço da AWS) usar uma sessão de função do IAM com identidade aprimorada, o IAM Identity Center do usuário `userId` é conectado ao elemento CloudTrail `onBehalfOf`. A forma como os eventos são registrados CloudTrail varia de acordo com o AWS service (Serviço da AWS). Nem todos os Serviços da AWS registram em log o elemento `onBehalfOf`.

Veja a seguir um exemplo de como uma solicitação feita a uma AWS service (Serviço da AWS) sessão de função com identidade aprimorada é registrada. CloudTrail

```
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROEXAMPLE:MyRole",
  "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
  "accountId": "111111111111",
  "accessKeyId": "ASIAEXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROEXAMPLE",
      "arn": "arn:aws:iam::111111111111:role/MyRole",
      "accountId": "111111111111",
      "userName": "MyRole"
    },
    "attributes": {
      "creationDate": "2023-12-12T13:55:22Z",
      "mfaAuthenticated": "false"
    }
  },
  "onBehalfOf": {
    "userId": "11111111-1111-1111-1111-111111111111",
    "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/d-1111111111"
  }
}
```

Fazer o rodízio de 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 uma 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.

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 uma 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 aba Configuração ou se a configuração não estiver disponível, não será necessário alternar o certificado 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: atualizar 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: definir 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

No console do IAM Identity Center, a página Aplicações exibe ícones indicadores de status nas propriedades de cada aplicação. Esses ícones são exibidos na coluna Expira em ao lado de cada certificado na lista. A seguir está a descrição dos critérios que o IAM Identity Center usa para determinar qual ícone será 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 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.

Compreender 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.

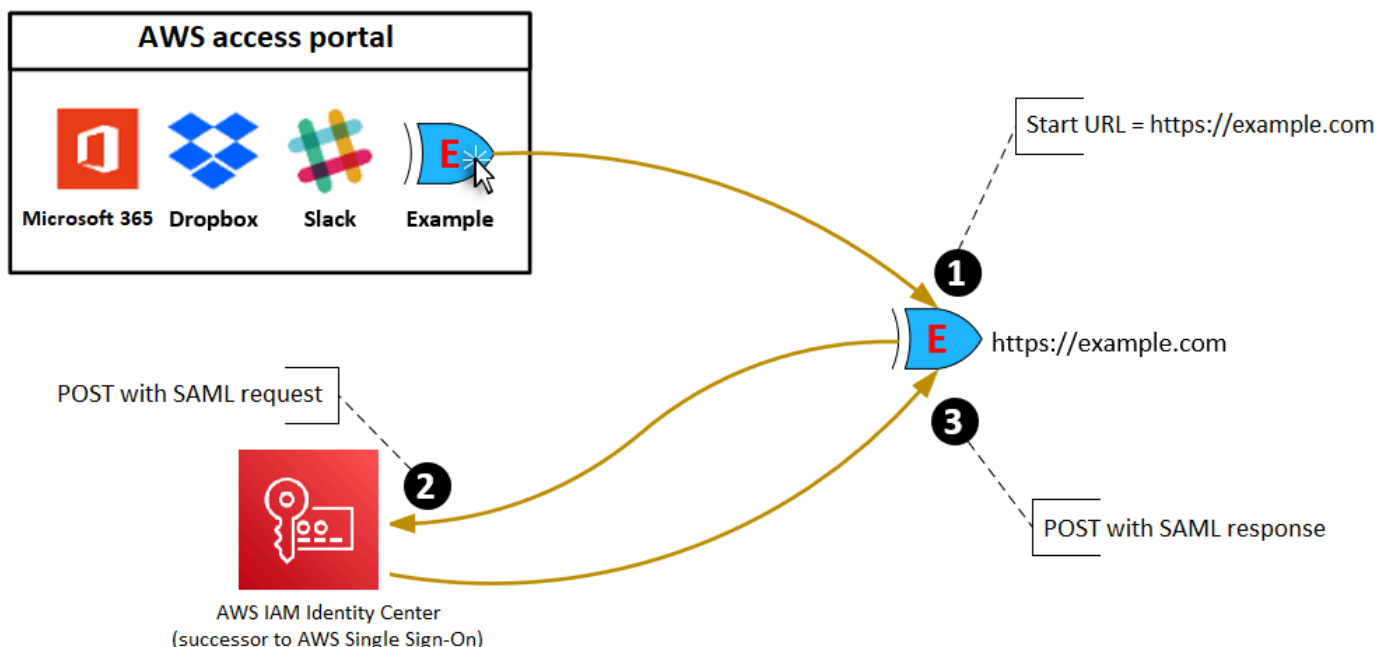
URL de início da aplicação

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 :

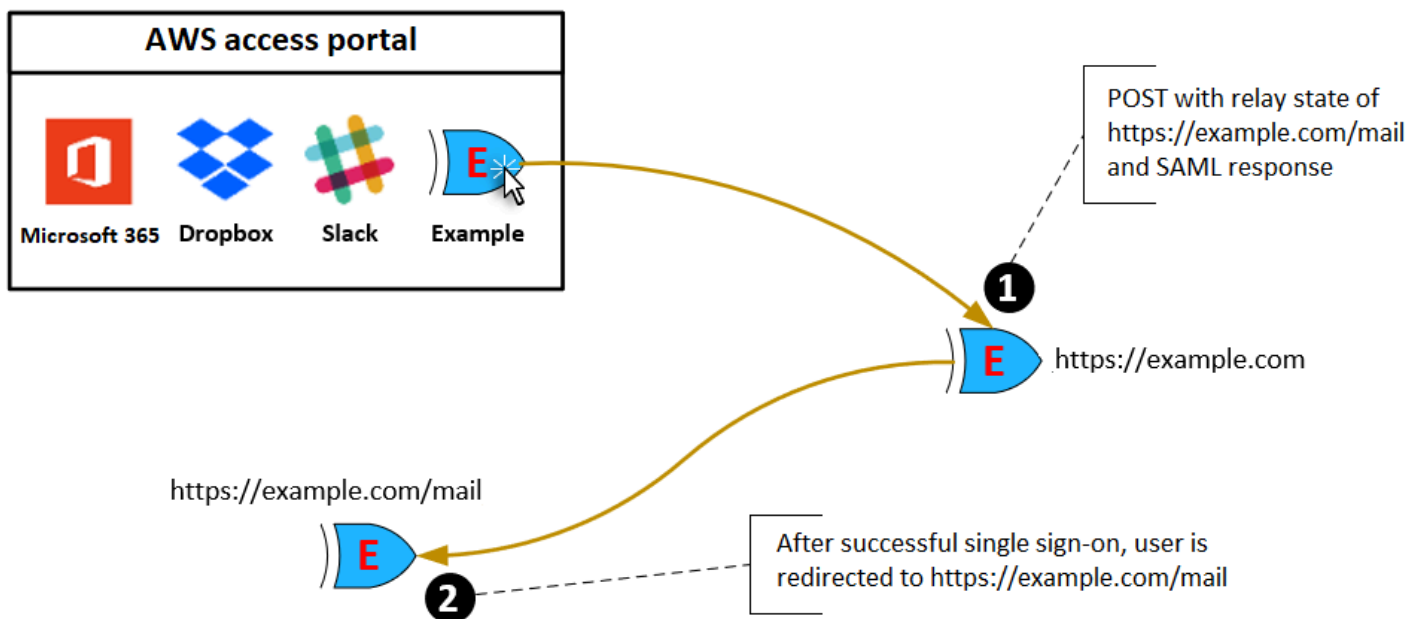
1. O navegador do usuário redireciona a solicitação de autenticação usando o valor da URL inicial do aplicativo (nesse caso `https://example.com`).
2. A aplicação envia um HTML POST com SAMLRequest para o IAM Identity Center.

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 login 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 do APIs.

1. Abra o [console do IAM Identity Center](#).

 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, insira um nome de exibição de usuário ou grupo. 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 dos usuários a aplicações SAML 2.0

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 obter mais informações sobre sessões de autenticação e durações, consulte [Como entender as sessões de autenticação no IAM Identity Center](#).

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 [Mapeamento de atributos entre o IAM Identity Center e o diretório de provedores de identidades externos](#).
8. Na terceira coluna da tabela, escolha o formato apropriado para o atributo no menu.
9. Escolha Salvar alterações.

Configurar o acesso a Contas da AWS

Centro de Identidade do AWS IAM 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 usando uma [instância organizacional](#) do IAM Identity Center. As [instâncias de conta](#) do IAM Identity Center não são compatíveis com acesso a contas.

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 obter 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 delegada	conta gerencial
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 delegada	conta gerencial
Adicionar, editar ou excluir usuários ou grupos	 Não		 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)
Criar, editar ou excluir aplicações gerenciadas pelo cliente	 No (Não)	 Yes (Sim)	 Yes (Sim)
Crie, edite ou exclua aplicativos AWS gerenciados	 Yes (Sim)	 Yes (Sim)	 Yes (Sim)

Tarefas administrativas do IAM Identity Center	Conta-membro	Conta de administrador delegada	conta gerencial
Configure o MFA	 No (Não)	 Yes (Sim)	 Yes (Sim)
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)	 Sim
Habilitar o IAM Identity Center	 Não	 No (Não)	 Sim
Exclua a configuração do IAM Identity Center	 Não	 No (Não)	 Sim
Ative ou desative o acesso do usuário na conta de gerenciamento	 Não	 No (Não)	 Sim

Tarefas administrativas do IAM Identity Center	Conta-membro	Conta de administrador delegada	conta gerencial
Registre ou cancele o registro de uma conta-membro como administrador delegado	 Não	 No (Não)	 Sim

*Consulte as melhores práticas para administração delegada em relação às atribuições de usuários e grupos à conta gerencial.

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 login único aos aplicativos. Para mais informações, consulte [Configurar 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 [Console de gerenciamento da AWS](#), 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 Console de gerenciamento da AWS ou recuperar as credenciais temporárias para acessar os AWS serviços de forma programática.

Para abrir Console de gerenciamento da AWS 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_styles` ao conjunto de `PowerUser` permissões, a função será exibida no portal de AWS acesso como `PowerUser/john_styles`. Os usuários com vários conjuntos de permissões escolhem qual função deve ser usada. Os usuários podem escolher seu perfil para acessar o Console de gerenciamento da AWS.
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 [Configurando e usando o portal de AWS acesso](#) e [Obter credenciais de usuário do IAM Identity Center para o ou AWS CLI 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 (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 [Compreender os perfis vinculados ao serviço do IAM Identity Center](#) 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 Centro de Identidade do AWS IAM 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

Para garantir que seus aplicativos AWS gerenciados funcionem bem com seu IAM Identity Center, você deve evitar aplicar esse SCP ao Contas da AWS local onde você implantou esses aplicativos. Além disso, se você usa administração delegada, evite aplicar esse SCP à conta de administração delegada. Para obter mais informações, consulte [Práticas recomendadas](#).

Para obter mais informações, consulte [Políticas de controle de serviço \(SCPs\)](#) no Guia AWS Organizations do usuário.

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 AWS Organizations, consulte [Configurar o acesso a 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](#)
- [Pré-requisitos](#)
- [Registre uma conta-membro](#)
- [Cancelar o registro de uma conta-membro](#)
- [Veja qual conta de membro foi registrada como administrador delegado](#)

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. Você também pode considerar o uso de [acesso elevado temporário](#) para conceder esse acesso somente quando necessário.
- Conjuntos de permissões dedicados para a conta gerencial — Use conjuntos de permissões dedicados para a conta gerencial. Por motivos de segurança, um conjunto de permissões usado para acessar a conta gerencial só pode ser modificado por um administrador do IAM Identity Center da conta gerencial. O administrador delegado não pode alterar conjuntos de permissões provisionados na conta gerencial.
- Atribua somente usuários (não grupos) aos conjuntos de permissões na conta de gerenciamento — Como a conta de gerenciamento tem privilégios especiais, você deve ter cuidado ao atribuir acesso a essa conta no console ou (AWS Command Line Interface CLI). Se você atribuir grupos a conjuntos de permissões com acesso à conta de gerenciamento, qualquer pessoa com permissão para modificar as associações nesses grupos poderá usar add/remove to/from esses grupos e, assim, afetar quem tem acesso à conta de gerenciamento. É qualquer administrador de grupo com controle sobre a fonte de identidade, incluindo o administrador do provedor de identidade (IdP), o administrador do Microsoft Active Directory Domain Service (AD DS) ou o administrador do IAM Identity Center. Portanto, você deve atribuir usuários diretamente aos conjuntos de permissões que concedem acesso à conta gerencial e evitar grupos. Se você usa grupos para gerenciar o acesso à conta gerencial, certifique-se de que os controles adequados estejam em vigor no IdP para limitar quem tem a capacidade de modificar esses grupos, e garanta que as alterações nesses grupos (ou alterações nas credenciais dos usuários na conta gerencial) sejam registradas e revisadas conforme necessário.
- 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 origem para o Active Directory, ou alterá-la do Active Directory para qualquer outra origem, o diretório deverá residir na conta de membro administrador delegado do IAM Identity Center. Se quiser que o Active Directory esteja

na conta gerencial, você deve realizar a configuração na conta gerencial, pois o administrador delegado não terá as permissões necessárias para concluí-la.

Limite as ações de armazenamento de identidades do IAM Identity Center na conta de administração delegada com fontes de identidade externas

Se você usa uma fonte de identidade externa, como um IdP ou Directory Service, deve implementar políticas que limitem as ações do repositório de identidades que um administrador do IAM Identity Center pode realizar na conta de administração delegada. As operações de gravação e exclusão devem ser cuidadosamente consideradas. Geralmente, a fonte de identidade externa é a fonte confiável para usuários e os atributos e para associações a grupos. Se você modificá-los usando o repositório de identidades APIs ou o console, suas alterações serão substituídas durante os ciclos normais de sincronização. É melhor deixar essas operações sob o controle exclusivo da fonte de identidade confiável. Isso também protege contra um administrador do IAM Identity Center que modifique as associações de grupo para conceder acesso a um conjunto de permissões ou aplicativo atribuído a um grupo, em vez de deixar o controle da associação de grupo para o administrador do IdP. Você também deve controlar quem pode criar tokens de portador SCIM a partir da conta de administração delegada, pois isso pode permitir que um administrador de conta de membro modifique grupos e usuários por meio de um cliente SCIM.

Pode haver momentos em que as operações de gravação ou exclusão sejam apropriadas na conta de administrador delegado. Por exemplo, você pode criar um grupo sem adicionar membros e, em seguida, fazer atribuições a um conjunto de permissões sem precisar esperar que o administrador do IdP crie o grupo. Ninguém terá acesso a essa tarefa até que o administrador do IdP provisione o grupo e o processo de sincronização do IdP estabeleça os membros do grupo. Também pode ser apropriado excluir um usuário ou grupo para impedir o login ou a autorização durante um período em que você não consegue esperar que o processo de sincronização do IdP remova o acesso do usuário ou do grupo. No entanto, o uso indevido dessa permissão pode atrapalhar os usuários. Você deve usar o princípio de privilégio mínimo ao atribuir permissões de armazenamento de identidades. Você pode controlar quais ações de armazenamento de identidades são permitidas pelos administradores de conta de administração delegada usando uma política de controle de serviços (SCP).

O exemplo de SCP abaixo impede a atribuição de usuários a grupos por meio da API Identity Store e da Console de gerenciamento da AWS, o que é recomendado quando sua fonte de identidade é externa. Isso não afeta a sincronização do usuário de Directory Service ou para um IdP externo (via SCIM).

 Note

É possível que, embora você use uma fonte de identidade externa, sua organização dependa, total ou parcialmente, do Identity Store APIs para o provisionamento de usuários e grupos. Portanto, antes de ativar esse SCP, você deve confirmar que o processo de provisionamento de usuários não usa essa operação da API do Identity Store. Além disso, consulte a próxima seção para obter informações sobre como limitar o gerenciamento de associações de grupos a grupos específicos.

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

Se você quiser evitar a adição de usuários apenas a grupos que concedem acesso à conta gerencial, você pode referenciar esses grupos específicos usando o ARN do grupo no seguinte formato: `arn:${Partition}:identitystore:::group/${GroupId}`. Esse e outros tipos de recursos disponíveis no Identity Store estão documentados em [Tipos de recursos definidos pelo AWS Identity Store](#) na Referência de Autorização de Serviço. Você também pode considerar a inclusão de um Identity Store adicional APIs no SCP. Para obter mais informações, consulte [Ações](#) na Referência da API do Identity Store.

Ao adicionar a seguinte declaração de política ao SCP, você pode impedir a criação de tokens portadores do SCIM pelo administrador delegado. Você pode aplicar isso para ambas as fontes de identidade externas.

 Note

Se o administrador delegado precisar configurar o provisionamento de usuários com o SCIM ou realizar a rotação periódica do token portador do SCIM, você precisará permitir temporariamente o acesso a essa API para permitir que o administrador delegado conclua essas tarefas.

```
{ "Effect": "Deny",
  "Action": ["sso-directory:CreateBearerToken"],
  "Resource": [ "*" ]
}
```

Limite as ações de armazenamento de identidades do IAM Identity Center na conta de administração delegada para usuários gerenciados localmente

Se você criar seus usuários e grupos diretamente no IAM Identity Center, em vez de usar um IdP externo ou Directory Service, você deve tomar precauções sobre quem pode criar usuários, redefinir senhas e controlar a associação ao grupo. Essas ações dão ao administrador grandes poderes sobre quem pode fazer login e obter acesso por meio da participação em grupos. Essas políticas são melhor implementadas como políticas em linha dentro dos conjuntos de permissões que você usa para os administradores do IAM Identity Center, em vez de como SCPs. O exemplo de política em linha a seguir tem dois objetivos. Em primeiro lugar, impede a adição de usuários a grupos específicos. Você pode usar isso para impedir que administradores delegados adicionem usuários aos grupos que concedem acesso à conta gerencial. Em segundo lugar, impede a emissão de tokens portadores do SCIM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Deny",
      "Action": ["identitystore:CreateGroupMembership"],
      "Resource": [ arn:${Partition}:identitystore:::group/${GroupId1},
                    arn:${Partition}:identitystore:::group/${GroupId2}
                  ]
    },
    { "Effect": "Deny",
      "Action": ["sso-directory:CreateBearerToken"],
      "Resource": [ "*" ] }
  ]
}
```

Separe o gerenciamento de configurações do IAM Identity Center do gerenciamento PermissionSet

Separe as tarefas administrativas, incluindo modificação da fonte de identidade externa, gerenciamento de tokens SCIM e configuração do tempo limite da sessão, das tarefas para criar, modificar e atribuir conjuntos de permissões criando conjuntos de permissões de administrador distintos de sua conta gerencial.

Limitar a emissão de tokens portadores do SCIM

Os tokens portadores do SCIM permitem que uma fonte de identidade externa provisione usuários, grupos e associações de grupos por meio do protocolo SCIM quando a fonte de identidade do IAM Identity Center é um IdP externo, como Okta ou Entra ID. Você pode configurar o seguinte SCP para impedir a criação de tokens portadores do SCIM por administradores delegados. Se o administrador delegado precisar configurar o provisionamento de usuários com o SCIM ou realizar a rotação periódica do token portador do SCIM, você precisará permitir temporariamente o acesso a essa API para permitir que o administrador delegado conclua essas tarefas.

```
{ "Effect": "Deny",  
  "Action": ["sso-directory:CreateBearerToken"],  
  "Resource": [ "*" ]  
}
```

Use tags de conjunto de permissões e listas de contas para delegar a administração de contas específicas

Você pode criar conjuntos de permissões que você atribui aos administradores do IAM Identity Center para delegar quem pode criar conjuntos de permissões e quem pode atribuir quais conjuntos de permissões em quais contas. Isso é feito marcando conjuntos de permissões e usando condições de política nos conjuntos de permissões que você atribui aos administradores. Por exemplo, você pode criar conjuntos de permissões que permitem que um usuário crie conjuntos de permissões, desde que sejam marcados de uma determinada forma. Você também pode criar políticas que permitem que um administrador atribua conjuntos de permissões que tenham uma tag específica em contas específicas. Isso pode ajudar você a delegar o gerenciamento de contas sem dar a um administrador os privilégios para modificar acesso e privilégios referentes à conta de administração delegada. Por exemplo, ao marcar os conjuntos de permissões que você usa somente na conta de administração delegada, você pode especificar uma política que conceda somente a determinadas

peçoas as permissões para modificar conjuntos de permissões e atribuições que afetam a conta de administração delegada. Você também pode conceder permissões a outras pessoas para gerenciar uma lista de contas fora da conta de administração delegada. Para saber mais, consulte [Delegar o gerenciamento do conjunto de permissões e a atribuição de contas no Centro de Identidade do AWS IAM](#) no Blog de segurança da AWS .

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 Identity 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 Console de gerenciamento da AWS 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 Console de gerenciamento da AWS 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 Settings.
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 para Contas da AWS

Todo acesso ao seu Conta da AWS envolve algum nível de privilégio. Operações sensíveis, como alterar a configuração de 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.

Note

Para garantir a continuidade dos negócios, recomendamos [configurar o acesso de emergência ao Console de gerenciamento da AWS](#).

Para atender a uma variedade de necessidades dos clientes, Centro de Identidade do AWS IAM integra-se às soluções dos parceiros de competência em AWS segurança. AWS valida que essas soluções atendem a um conjunto comum de requisitos temporários de acesso elevado. Recomendamos que você analise cuidadosamente cada solução de parceiro para que possa escolher aquela que melhor se adapta às suas necessidades e preferências exclusivas, incluindo o negócio, a arquitetura do ambiente de nuvem e o orçamento.

As soluções validadas incluem a [Apono Access Management Platform](#), [CyberArk Secure Cloud Access](#), [Okta Access Requests](#) e [Tenable](#) (anteriormente Ermetic).

Os parceiros podem indicar soluções usando o aplicativo AWS Security Competency no Partner Center. Para obter mais informações, consulte [Parceiros do AWS Security Competency](#).

Note

Se você estiver usando o Amazon Elastic AWS Key Management Service Kubernetes Service baseado em recursos [ou consulte Conjuntos de permissões de referência em políticas de recursos, mapas de AWS KMS configuração de cluster do Amazon EKS e políticas](#) de chaves antes de escolher sua solução. just-in-time

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 política de [IAMFullacesso](#) 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.

Tópicos

- [Atribuir acesso de usuário ou grupo a Contas da AWS](#)
- [Remover o acesso de usuários e grupos a um Conta da AWS](#)
- [Revogar sessões ativas de perfil do IAM criadas por conjuntos de permissões](#)
- [Delegar quem pode atribuir acesso de login único a usuários e grupos na conta de gerenciamento](#)

Atribuir acesso de usuário ou grupo a Contas da AWS

Use o procedimento a seguir para atribuir acesso login único a usuários e grupos em seu diretório conectado e usar conjuntos de permissões para determinar o nível de acesso.

Para verificar o acesso dos usuários e grupos existentes, consulte [Visualizar e alterar um conjunto de permissões](#).

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, 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.

 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. Para a 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. Para a 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 [Crie 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. Para a 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.

Considerações

- 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 política de [IAMFullacesso](#) 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.

8. 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 IAM Identity Center, 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.

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 [fazer login no portal de acesso da AWS](#) ou usar os comandos [AWS Command Line Interface \(AWS CLI\)](#).

Remover o acesso de usuários e grupos a um Conta da AWS

Use esse procedimento para remover o acesso de login único a um Conta da AWS ou mais usuários e grupos em seu diretório conectado. Você também pode usar a [delete-account-assignment](#) AWS CLI.

 Note

Quando precisar desprovisionar usuários ou grupos do IAM Identity Center, primeiro [remova todas as atribuições de conjuntos de permissões de](#) os usuários e grupos antes de excluir os usuários e grupos.

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 ativas de perfil do IAM criadas por conjuntos de permissões

O procedimento a seguir é o procedimento genérico para revogação de uma sessão ativa de um conjunto de permissões do IAM Identity Center. O procedimento pressupõe que você queira remover todo o acesso de um usuário cujas credenciais foram comprometidas ou de um agente mal-intencionado que está no sistema. O pré-requisito é ter seguido as orientações em [Preparar-se para revogar sessões ativas de perfil do IAM criadas por conjuntos de permissões](#). Presumimos que a política de negação total 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 do usuário cujo acesso você deve revogar. Você pode usar o repositório de identidades APIs para encontrar o usuário pelo nome de usuário.
2. Atualize a política de negação para adicionar o ID do usuário da etapa 1 na sua política de controle de serviços (SCP). Após essa etapa ser concluída, o usuário-alvo perde o acesso e não consegue realizar ações com nenhum perfil afetado pela política.
3. Remova todas as atribuições de conjunto de permissões do usuário. Se o acesso foi 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 evita que o usuário assuma qualquer outro perfil 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 identidades (IdP) ou o Microsoft Active Directory como fonte de identidades, desabilite o usuário na fonte de identidades. Desabilitar o usuário impede a criação de sessões adicionais no portal de acesso AWS . Use a documentação do seu IdP ou das APIs do Microsoft Active Directory para saber como automatizar essa etapa. Se você estiver usando o diretório do IAM Identity Center como fonte de identidade, não desabilite o acesso do usuário ainda. Você desabilitará 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 selecione Excluir sessão.

Depois de excluir uma sessão de usuário, o usuário perderá imediatamente o acesso ao portal de AWS acesso. Saiba mais sobre a [duração da sessão](#).

6. No console do IAM Identity Center, desabilite o acesso do usuário.
 - a. Selecione Usuários.
 - b. Escolha o usuário que deseja desabilitar.
 - c. Na página de detalhes do usuário, expanda Informações gerais e escolha o botão Desabilitar o acesso do usuário para evitar que usuário faça outros logins.
7. Mantenha a política de negação em vigor por pelo menos 12 horas. Caso contrário, as ações do usuário com uma sessão de perfil do IAM ativa serão restauradas com perfil do IAM. Se você

esperar 12 horas, as sessões ativas expirarão e o usuário não poderá voltar acessar o perfil do IAM.

 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 usando o console do IAM Identity Center. Se você desabilitar inadvertidamente o acesso do usuário antes de interromper a sessão do usuário, poderá reativá-lo, interromper a sessão e, em seguida, desabilitar novamente seu acesso.

Agora você poderá alterar as credenciais do usuário se a senha dele 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 `IAMFullAccess` políticas `AWSSSOMasterAccountAdministratore` gerenciam o acesso de login único à conta de gerenciamento em uma AWS Organizations organização.

Como alternativa, você pode usar AWS CLI para criar, anexar políticas e atribuir conjuntos de permissões. A seguir, são listados os comandos para cada etapa:

- Para criar um conjunto de permissões: [create-permission-set](#)
- Para anexar AWS Managed Policy a um conjunto de permissões: [attach-managed-policy-to-permission-set](#)
- Para anexar a política gerenciada pelo cliente a um conjunto de permissões: [attach-customer-managed-policy-to-permission-set](#)
- Para atribuir um conjunto de permissões a um diretor: [create-account-assignment](#)

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 [Crie 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 Console de gerenciamento da AWS. Por exemplo:

<https://console.aws.amazon.com/ec2/>

Para obter mais informações, consulte [Defina o estado do relé para acesso rápido ao Console de gerenciamento da AWS](#).

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 AWSSSOMasterAccountAdministrators e 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: tags.
 6. Em Adicionar tags (opcional), especifique valores de Chave e Valor (opcional), e escolha Avançar: Revisão. Para obter mais informações sobre tags, consulte [Recursos de marcação Centro de Identidade do AWS IAM](#).
 7. Verifique suas seleções e, em seguida, escolha Create function.
3. Siga as etapas em [Atribuir acesso de usuário ou grupo a Contas da AWS](#) para atribuir os usuários e grupos apropriados ao conjunto de permissões que você acabou de criar.

4. Comunique aos usuários designados o seguinte: quando eles fizerem login no portal de acesso AWS e selecionarem a guia Contas, deverão escolher o nome do perfil apropriado para serem autenticados com as permissões que você acabou de delegar.

Gerencie Contas da AWS com 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 do 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 tarefa](#) aos conjuntos de permissões. Você também pode atribuir uma política gerenciada da AWS ou uma política gerenciada pelo cliente como [limite de permissões](#).

Para criar um conjunto de permissões, consulte [Criar, gerenciar e excluir conjuntos de permissões](#).

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 mudar para permissões de privilégio mínimo, você pode executar o IAM Access Analyzer para monitorar os principais com AWS políticas gerenciadas. Depois de saber 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 apenas 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. Diferentemente do conjunto de permissões administrativas, que usa as permissões de `AdministratorAccess`, o conjunto de permissões de `PowerUserAccess` 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 obter mais informações, consulte [Defina a duração da sessão para Contas da AWS](#).

- Você também pode configurar a duração da sessão do portal de AWS acesso para controlar o período 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 obter mais informações, consulte [Configurar a duração da sessão no 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 acesso de usuário ou grupo a Contas da AWS](#).

Tópicos

- [Permissões predefinidas para políticas AWS gerenciadas](#)
- [Permissões personalizadas para políticas AWS gerenciadas e gerenciadas pelo cliente](#)
- [Criar, gerenciar e excluir conjuntos de permissões](#)
- [Configurar propriedades do conjunto de permissões](#)

Permissões predefinidas para políticas AWS gerenciadas

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 para políticas AWS gerenciadas e gerenciadas pelo cliente

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 com [Políticas 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 com [Políticas 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 obter mais informações, consulte [Use políticas do IAM nos conjuntos de permissões](#).

Note

Quando uma política gerenciada pelo cliente é anexada a um conjunto de permissões, o nome da política não diferencia maiúsculas de minúsculas.

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, o [Políticas em linha](#), [Políticas gerenciadas pelo cliente](#) e [AWS políticas gerenciadas](#) não podem conceder nenhuma permissão que exceda as permissões que o 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 Identity Center, consulte [Gerencie Contas da AWS com conjuntos de permissões](#).

Note

Você pode pesquisar e classificar conjuntos de permissões por nome no console do IAM Identity Center.

Ao criar conjuntos de permissões, tenha em mente as seguintes considerações:

- Instância de organização

Para usar conjuntos de permissões, você precisará usar uma instância de organização do IAM Identity Center. Para obter mais informações, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

- 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 a Console de gerenciamento da AWS 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 melhor prática de segurança, recomendamos que você não defina um tempo de duração da sessão maior do que o necessário para executar a função. Por padrão, o valor de Duração da sessão é uma hora. Você pode especificar um valor máximo de 12 horas. Para obter mais informações, consulte [Defina a duração da sessão para Contas da AWS](#).

- 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 obter mais informações, consulte [Configurar a duração da sessão no 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

- [Crie um conjunto de permissões](#)
- [Visualizar e alterar um conjunto de permissões](#)
- [Delegar a administração do conjunto de permissões](#)
- [Use políticas do IAM nos conjuntos de permissões](#)
- [Remover conjuntos de permissões no IAM Identity Center](#)
- [Excluir conjuntos de permissões no IAM Identity Center](#)

Crie 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.

 Note

Para usar conjuntos de permissões, você precisará usar uma instância de organização do IAM Identity Center. Para obter mais informações, consulte [Instâncias de organização e de conta 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 predefinidas, selecione uma das políticas de funções do IAM ou políticas de permissões comuns na lista, depois escolha Avançar. Para obter mais informações, consulte [Políticas gerenciadas pela AWS](#) ou [Políticas gerenciadas pela AWS para funções de trabalho](#) no Guia do usuário do AWS Identity and Access Management .
 2. Vá para a etapa 6 para preencher a página Especificar detalhes do conjunto de permissões.
 - Conjunto de permissões personalizado
 1. Escolha Próximo.
 2. Na página Especificar políticas e limite de permissões, 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 obter 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 preencher 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 obter 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 preencher a página Especificar detalhes do conjunto de permissões.
 - Expanda Política em linha para adicionar texto personalizado de política em formato 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 obter mais informações, consulte [Políticas em linha](#).
 - a. Adicione as ações e os recursos desejados no editor interativo à sua política em linha. Instruções adicionais podem ser adicionadas com Adicionar nova instrução.
 - 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 preencher 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 obter 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 preencher a página Especificar detalhes do conjunto de permissões.
6. Na página Specify permission set details (Especificação de 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.

 Note

Os nomes de conjuntos de permissões devem ser exclusivos na instância do IAM Identity Center.

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 obter mais informações, consulte [Defina a duração da sessão para Contas da AWS](#).
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 obter mais informações, consulte [Defina o estado do relé para acesso rápido ao Console de gerenciamento da AWS](#).

 Note

O URL do estado de retransmissão deve estar dentro do Console de gerenciamento da AWS. 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 [Recursos de marcação Centro de Identidade do AWS IAM](#).

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 nenhuma 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 obter mais informações, consulte [Atribuir acesso de usuário ou grupo a Contas da AWS](#).

Visualizar e alterar um conjunto de permissões

Você pode usar conjuntos de permissões para conceder acesso a Contas da AWS. Você pode visualizar e alterar um conjunto de permissões com o Centro de Identidade do AWS IAM console. Você pode pesquisar e classificar conjuntos de permissões por nome no console do IAM Identity Center. Para obter mais informações sobre conjuntos de permissões e como eles são usados no IAM Identity Center, consulte [the section called “Conjuntos de permissões”](#).

Os conjuntos de permissões não são exigidos para gerenciar o acesso do usuário aos aplicações.

Note

Para usar conjuntos de permissões, você precisará usar uma instância de organização do IAM Identity Center. Para obter mais informações, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

Visualizar atribuições do conjunto de permissões

Use esse procedimento para visualizar um conjunto de permissões aplicadas no console do Centro de Identidade do AWS IAM .

All Contas da AWS where a permission set is provisioned

Para visualizar todas as atribuições de um conjunto de permissões, use o seguinte procedimento:

1. Faça login no Console de gerenciamento da AWS e abra o Centro de Identidade do AWS IAM console em <https://console.aws.amazon.com/singlesignon/>.
2. Em Permissões multicontas, escolha Conjuntos de permissões.
3. Na página Conjuntos de permissões, selecione o conjunto de permissões que você deseja visualizar.
4. Uma vez na página de conjuntos de permissões selecionados, na aba Contas, você pode ver as contas em que o conjunto de permissões é usado. Você pode selecionar a conta para ver como o conjunto de permissões é provisionado na conta. Você pode [excluir](#), editar e anexar políticas ao conjunto de permissões.

All permission sets for an Conta da AWS

Para visualizar todas as atribuições de um conjunto de permissões, use o seguinte procedimento:

1. Faça login no Console de gerenciamento da AWS e abra o Centro de Identidade do AWS IAM console em <https://console.aws.amazon.com/singlesignon/>.
2. Em Permissões de várias contas, escolha Contas da AWS. Selecione a conta para a qual deseja visualizar os conjuntos de permissões provisionados.
3. Uma vez na Conta da AWS página selecionada, na guia Conjuntos de permissões, você pode ver os diferentes conjuntos de permissões atribuídos aos selecionados Conta da AWS. Você pode selecionar o hiperlink do conjunto de permissões para saber mais sobre o conjunto de permissões.

All applied permission sets to users and groups

Para visualizar todos os conjuntos de permissões atribuídos a usuários ou grupos, use o seguinte procedimento:

1. Faça login no Console de gerenciamento da AWS e abra o Centro de Identidade do AWS IAM console em <https://console.aws.amazon.com/singlesignon/>.
2. Selecione Usuários ou Grupos em Painel para ver os usuários ou grupos do IAM Identity Center.
 - a. Na página Usuários, selecione o usuário para o qual você deseja ver os conjuntos de permissões aplicados. Em seguida, selecione a aba Contas da AWS e a seção Conta da AWS abaixo de acesso à conta AWS . Você poderá ver os conjuntos de permissões aplicados e Conta da AWS para o usuário selecionado.
 - b. Na página Grupos, selecione o grupo que você deseja ver os conjuntos de permissões aplicados. Em seguida, selecione a aba Contas da AWS e a seção Conta da AWS abaixo de acesso a Conta da AWS . Você poderá ver os conjuntos de permissões aplicados e Conta da AWS do grupo selecionado.

Alterar um conjunto de permissões

Use esse procedimento para alterar um [conjunto de permissões](#) com o console do IAM Identity Center. Você pode adicionar ou remover conjuntos de permissões de usuários ou grupos.

1. Faça login no Console de gerenciamento da AWS e abra o Centro de Identidade do AWS IAM console em <https://console.aws.amazon.com/singlesignon/>.
2. Em Permissões de várias contas, escolha Contas da AWS.

3. Na página Conta da AWS, aparece uma lista de visualização em árvore da sua organização. Selecione o nome da Conta da AWS cujo conjunto de permissões você deseja alterar.
4. Na página Visão geral da Conta da AWS, em Usuários e grupos atribuídos, selecione o nome de usuário ou o nome do grupo do conjunto de permissões que você deseja alterar. Em seguida, escolha Alterar conjuntos de permissões.
5. Faça as alterações desejadas no conjunto de permissões e escolha Salvar alterações.
6. Navegue até a guia Conjuntos de permissões, selecione o conjunto de permissões alterado recentemente e escolha Atualizar.
7. Na página Atualizar permissões, escolha Atualizar.

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 [Amazon Resource Names \(ARNs\) 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.

Note

Para usar conjuntos de permissões, você precisará usar uma instância de organização do IAM Identity Center. Para obter mais informações, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

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

ARNs Os recursos do IAM Identity Center diferenciam maiúsculas de minúsculas.

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 [Crie 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 nenhuma 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 uma 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.

Considerações

- Para usar conjuntos de permissões, você precisará usar uma instância de organização do IAM Identity Center. Para obter mais informações, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

- 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-membro deve ser igual ao 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.

 Note

Quando uma política gerenciada pelo cliente é anexada a um conjunto de permissões, o nome da política não diferencia maiúsculas de minúsculas.

- As permissões concedidas pela política não precisam ser uma correspondência exata entre as contas.

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 [Crie 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.

Remover conjuntos de permissões no IAM Identity Center

Você pode remover um conjunto de permissões de usuários e grupos do IAM Identity Center no console do IAM Identity Center. Você também pode remover um conjunto de permissões de uma Conta da AWS. Para obter mais informações sobre conjuntos de permissões e como eles são usados no IAM Identify Center, consulte [Gerencie Contas da AWS com conjuntos de permissões](#).

Note

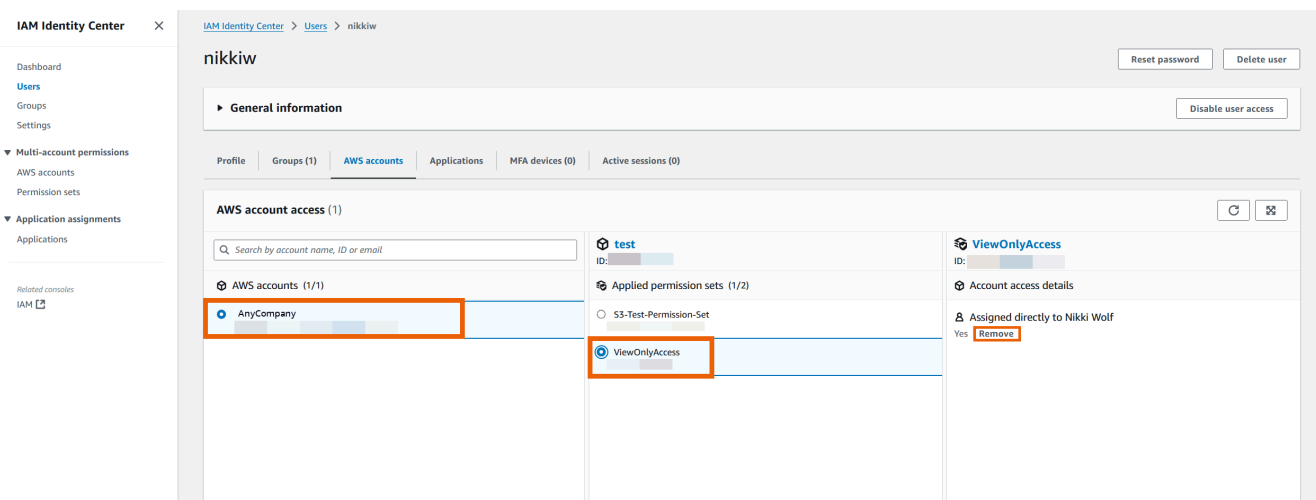
Para usar conjuntos de permissões, você precisará usar uma instância de organização do IAM Identity Center. Para obter mais informações, consulte [Instâncias de organização e de conta do IAM Identity Center](#).

Remove permission set from a user

Remover um conjunto de permissões de um usuário

Use esse procedimento para remover um conjunto de permissões de um usuário com o console do IAM Identity Center.

1. Faça login no Console de gerenciamento da AWS e abra o Centro de Identidade do AWS IAM console em <https://console.aws.amazon.com/singlesignon/>.
2. Em IAM Identity Center, selecione Usuários.
3. Selecione o nome do usuário do qual você deseja remover um conjunto de permissões.
4. Na página Detalhes do usuário, selecione a aba Contas da AWS. Em Acesso à Conta da AWS, selecione a Conta da AWS.
5. No painel direito, as permissões aplicadas para o usuário selecionado são exibidas. Selecione o conjunto de permissões que deseja remover. Em Detalhes de acesso à conta, selecione Remover.
6. Uma caixa de diálogo aparece perguntando se você deseja remover esse conjunto de permissões. Selecione Remover.

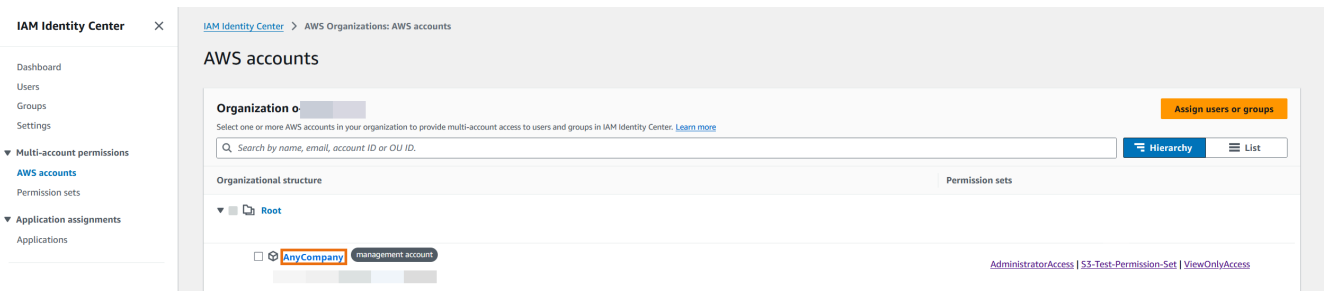


Remove permission set from a group

Remover conjunto de permissões de um grupo

Use esse procedimento para remover um conjunto de permissões de um grupo com o console do IAM Identity Center.

1. Faça login no Console de gerenciamento da AWS e abra o Centro de Identidade do AWS IAM console em <https://console.aws.amazon.com/singlesignon/>.
2. Em Permissões de várias contas, escolha Contas da AWS. Selecione o link para a conta gerencial.



3. Na aba Usuários e grupos atribuídos, selecione o grupo do qual você deseja remover o conjunto de permissões e, em seguida, selecione Alterar conjunto de permissões.
4. Na página Alterar conjuntos de permissões, limpe o conjunto de permissões que você deseja remover e selecione Salvar alterações.

Remove permission set from an Conta da AWS

Use esse procedimento para remover um conjunto de permissões da Conta da AWS com o console do IAM Identity Center.

1. Faça login no Console de gerenciamento da AWS e abra o Centro de Identidade do AWS IAM console em <https://console.aws.amazon.com/singlesignon/>.
2. Em Permissões de várias contas, escolha Contas da AWS. Selecione o nome do Conta da AWS do qual você deseja remover o conjunto de permissões.
3. Na página Visão geral da Conta da AWS, escolha a aba Conjuntos de permissões. Selecione o conjunto de permissões que deseja remover. Em seguida, selecione Remover.
4. 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.

Excluir conjuntos de permissões no IAM Identity Center

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 dos usuários e grupos existentes, consulte [Visualizar e alterar um conjunto de permissões](#).

Considerações

- Para usar conjuntos de permissões, você precisará usar uma instância de organização do IAM Identity Center. Para obter mais informações, consulte [Instâncias de organização e de conta do IAM Identity Center](#).
- Se você quiser revogar uma sessão de conjunto de permissões ativa, consulte [the section called “Encerrar sessões ativas para usuários da força de trabalho”](#).
- Você deve remover conjuntos de permissões e atribuições de aplicações dos usuários ou grupos que deseja excluir antes de excluí-los. Caso contrário, você terá conjuntos de permissões e aplicações não atribuídos e não utilizados no IAM Identity Center.

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.

Important

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 dos usuários e grupos existentes, consulte [Visualizar e alterar um conjunto de permissões](#).

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, os administradores podem fazer as seguintes tarefas de configuração e gerenciamento para controlar o acesso do usuário e a duração da sessão.

Tarefa	Saiba mais
Os administradores podem definir a duração máxima das sessões do usuário ao acessar AWS recursos por meio do IAM Identity Center.	Defina a duração da sessão para Contas da AWS
Os administradores podem personalizar a página inicial que os usuários veem após a autenticação bem-sucedida por meio do IAM Identity Center.	Defina o estado do relé para acesso rápido ao Console de gerenciamento da AWS
Garanta que os usuários não tenham mais acesso aos AWS recursos quando suas permissões forem revogadas.	Use uma política de negação para revogar as permissões ativas do usuário

Defina a duração da sessão para Contas da AWS

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.

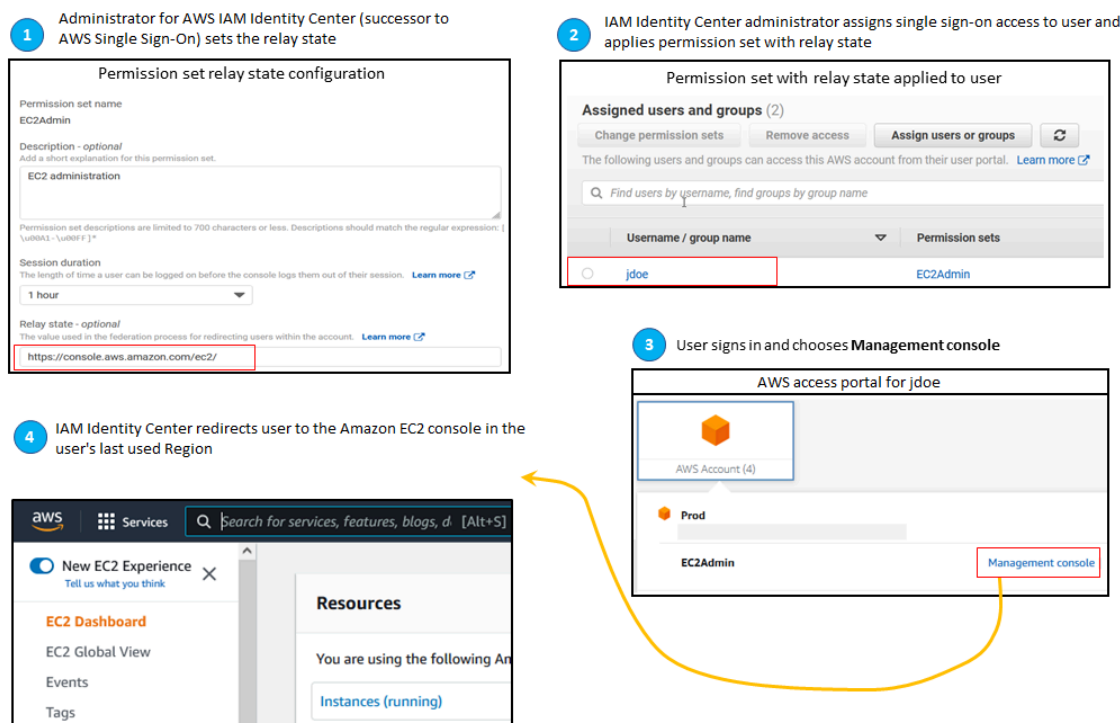
Como definir a duração da sessão

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.

Defina o estado do relé para acesso rápido ao Console de gerenciamento da AWS

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 Console de gerenciamento da AWS. 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 Identity 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>**

Configurar o estado de retransmissão

Use o procedimento a seguir para configurar o URL do estado de retransmissão de um conjunto de permissões.

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 Console de gerenciamento da AWS.

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 uma 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 sua capacidade de usar suas sessões de perfil do IAM ativas implementando uma política de negação para um usuário não especificado com antecedência e, quando necessário, atualizar a política de negação para especificar o usuário cujo acesso você deseja bloquear. Este tópico explica como criar uma política de negação e faz considerações sobre como implantar a política.

Preparar-se para revogar sessões ativas de perfil do IAM criadas por conjuntos de permissões

Você pode impedir que o usuário realize ações com um perfil do IAM que ele está usando ativamente, aplicando uma política de negação total para um usuário específico por meio de uma política de controle de serviços. Você também pode impedir que um usuário use qualquer conjunto de permissões até que você altere a senha, o que remove um malfeitor que esteja usando ativamente 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 acesso AWS e desabilitar o login do usuário. Consulte [the section called “Encerrar sessões ativas para usuários da força de trabalho”](#) para saber como usar a política de negação em conjunto com outras ações para fazer uma revogação de acesso mais ampla.

Política de negação

Você pode usar uma política de negação com uma condição que corresponda ao `UserId` do usuário do repositório de identidades do IAM Identity Center para impedir outras ações de um perfil do IAM que o usuário esteja usando ativamente. O uso dessa política evita o impacto em outros usuários que possam estar usando o mesmo conjunto de permissões quando você implantar a política de negação. Essa política usa o ID de usuário do espaço reservado, *Add user ID here*, para o `"identitystore:userId"` que você atualizará com o ID de usuário cujo acesso você deseja revogar.

JSON

```
{
  "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, como `"aws:userId"`, `"identitystore:userId"` é garantido porque é um valor globalmente exclusivo que é associado a uma pessoa. O modo como os atributos do usuário são sincronizados a partir da fonte de identidades pode afetar o uso de `"aws:userId"` na condição e poderá 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 o `identitystore:userId` de um usuário 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 a ID de usuário do usuário consultando o repositório de identidades. APIs

Implantação da política de negação

Você pode usar uma ID de usuário de espaço reservado que não seja válida *Add user ID here*, como 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 efeito rápido. Quando revogar o acesso de um usuário com a política de negação, você editará a política para substituir o ID de usuário do espaço reservado pelo ID de usuário da pessoa cujo acesso você deseja revogar. Isso impede que o usuário faça qualquer ação com qualquer permissão definida em todas as contas a que você anexar a SCP. Ela bloqueia as ações do usuário mesmo que ele use sua sessão ativa do portal de acesso AWS para navegar para outras contas e assumir outros perfis. 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 SCPs, você também pode incluir a política Negar 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 dos métodos usados, você deve tomar qualquer outra medida corretiva e manter o ID do usuário na política por, pelo, menos 12 horas. Após esse período, todos os perfis assumidos pelo usuário expiram e você poderá então remover o ID de usuário da política de negação.

Referenciando conjuntos de permissões em políticas de recursos, mapas de configuração do Amazon EKS Cluster e AWS KMS políticas principais

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
<code>AWSReservedSSO_ <i>permission-set-name</i> <i>e-unique-suffix</i></code>	<code>arn:aws:iam:: <i>aws-account-ID</i>:role/aws-reserved/sso.amazonaws.com/ <i>aws-region</i> /AWSReservedSSO_ <i>permission-set-name</i> <i>e-unique-suffix</i></code>

Se sua fonte de identidade no IAM Identity Center estiver hospedada em `us-east-1`, não há nenhuma *aws-region* no ARN. O nome completo e o ARN do perfil usam o seguinte formato:

Nome	ARN
<code>AWSReservedSSO_ <i>permission-set-name</i> <i>e-unique-suffix</i></code>	<code>arn:aws:iam:: <i>aws-account-ID</i> :role/aws-reserved/sso.amazonaws.com/AWSReservedSSO_ <i>permission-set-name</i> <i>e-unique-suffix</i></code>

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
<code>AWSReservedSSO_DatabaseAdministrator_1234567890abcdef</code>	<code>arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/</code>

Nome	ARN
	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 `aws-auth ConfigMap` para clusters do Amazon Elastic Kubernetes Service (Amazon EKS) quando você usa o `aws-auth ConfigMap` para acesso a cluster.
- Em uma política baseada em recursos para uma chave AWS Key Management Service (AWS KMS). Essa política também é referenciada como política de chave.

Note

Recomendamos que você use as [entradas de acesso ao Amazon EKS](#) para gerenciar o acesso aos clusters do Amazon EKS. Isso permite que você use as permissões do IAM para

gerenciar as entidades principais que têm acesso a um cluster do Amazon EKS. Usando as entradas de acesso ao Amazon EKS, você pode usar uma entidade principal do IAM com permissões do Amazon EKS para recuperar o acesso a um cluster sem entrar em contato com o Suporte.

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`. Pois AWS KMS, ele deve existir em suas principais políticas. Se você não tiver uma função de backup do IAM com permissões para atualizar a política `aws-auth ConfigMap` ou a política de AWS KMS chaves, entre em contato Suporte para recuperar o acesso a esses recursos.

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 conta111122223333, 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 escalção de privilégios.

- Para clusters do Amazon EKS que usam **aws-auth ConfigMap** e AWS KMS: Incluem uma função criada no IAM.

Se você referenciar uma função ARNs para conjuntos de permissões em um `aws-auth ConfigMap` cluster do Amazon EKS ou em políticas de AWS KMS chaves para chaves, 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

A seguir há um exemplo de uma política de confiança personalizada que fornece um conjunto de permissões `AdministratorAccess` 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 assumira um perfil criado no IAM, mesmo que o ARN do perfil do conjunto de permissões seja alterado.

JSON

```
{  
  "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 por atributo

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 várias 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 Identity Center.

- O ABAC exige menos conjuntos de permissões — Uma vez que não é necessário criar políticas diferentes para funções de tarefa 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 Identity Center, consulte [Atributos para controle de acesso](#). Para obter informações sobre como habilitar e configurar o ABAC usando o IAM Identity Center APIs, consulte o Guia [CreateInstanceAccessControlAttributeConfiguration](#) 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 implementar o ABAC.	• Recursos de marcação AWS
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.	• Introdução
	• Se você estiver usando um provedor de identidade 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 identidade 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	• Tutoriais sobre fontes de identidade do IAM Identity Center

Etapa	Tarefa	Referência
	seções Optional do tutorial para seu IdP específico. • 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. • 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.	• Provisionar usuários e grupos de um provedor de identidades externo usando o SCIM • Atributos de provedor de identidade externo compatíveis • Escolha de atributos ao usar o IAM Identity Center como sua origem de identidade • Escolha de atributos ao usar AWS Managed Microsoft AD como fonte de identidade • Mapeamento padrão entre o IAM Identity Center e o Microsoft AD
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

Etapa	Tarefa	Referência
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 <code>aws:PrincipalTag/key</code> .	• Criar políticas de permissão para ABAC no IAM Identity 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 ou grupo 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 por atributo](#).

Introdução

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 fonte 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.

[Mapeamento padrão entre o IAM Identity Center e o Microsoft AD](#)

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 SCIM 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 enviar por meio de asserções SAML, consulte os [Tutoriais sobre fontes de identidade do IAM Identity Center](#) para o 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, consulte [Atributos de provedor de identidade externo compatíveis](#).

Para começar a usar o ABAC no IAM Identity Center, consulte os tópicos a seguir.

Tópicos

- [Habilite e configure atributos para controle de acesso](#)
- [Criar políticas de permissão para ABAC no IAM Identity Center](#)

Habilite e configure atributos para controle de acesso

Para usar o controle de acesso por atributo (ABAC), você deve primeiro habilitá-lo na página Configurações do console do IAM Identity Center ou na [API do IAM Identity Center](#). Independentemente da fonte de identidade, você sempre pode configurar os atributos do usuário do

Identity Store para uso no ABAC. No console, você pode fazer isso navegando até a aba Atributos para controle de acesso na página Configurações. Se você usa o provedor de identidades (IdP) externo como fonte de identidade, também tem a opção de receber atributos do IdP externo nas asserções do SAML. Nesse caso, você precisa configurar o IdP externo para enviar os atributos desejados. Se um atributo de uma declaração SAML também for definido como um atributo ABAC no IAM Identity Center, o IAM Identity Center enviará o valor do Identity Store como uma [tag de sessão](#) ao fazer login em uma Conta da AWS.

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.

Tópicos

- [Desabilitar atributos para controle de acesso](#)
- [Selecionar atributos para controle de acesso](#)
- [Desabilitar atributos para controle de acesso](#)

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. Se sua instância do IAM Identity Center foi criada antes de dezembro de 2020 e você planeja habilitar o ABAC nela, você deve ter a `iam:UpdateAssumeRolePolicy` política associada

à função administrativa do IAM Identity Center, independentemente de ter conjuntos de permissões criados 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.

Selecionar atributos para controle de acesso

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.

Key ⓘ	Value (optional) ⓘ	Remove
Department	<code>\${path.enterprise.department}</code>	✕
CostCenter	<code>\${path.enterprise.costCenter}</code>	✕
Add new key	Add new value	

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, CostCenter como 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 [Mapeamento de atributos entre o IAM Identity Center e o diretório de provedores de identidades externos](#). 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 às políticas baseadas em and/or recursos de seus conjuntos de permissões. Isso é necessário para que você possa conceder acesso aos recursos AWS às identidades dos usuários. Para obter mais informações, consulte [Criar políticas de permissão para ABAC no IAM Identity 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 Settings.

3. Na página Configurações, escolha a guia Atributos para controle de acesso e, em seguida, escolha Gerenciar atributos.
4. Na página Gerenciar atributos para controle de acesso, escolha Desabilitar.
5. Na janela de diálogo Desabilitar atributos para controle de acesso, revise as informações e, quando estiver com tudo pronto, insira **DISABLE** e escolha Confirmar.

 Important

Essa etapa exclui todos os atributos e interrompe o uso de atributos para controle de acesso durante a federação para as Contas da AWS, independentemente de algum atributo estar presente nas asserções SAML de um provedor externo de fonte de identidade.

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 a seguir, você pode marcar todos os recursos da organização com os 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.

JSON

```
{
  "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 obter mais informações, consulte [Erro “Ocorreu um erro inesperado” quando um usuário tenta fazer login usando um provedor de identidades externo](#).

Compreender os perfis vinculados ao serviço do IAM Identity Center

[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 Identity Center acesse os recursos de cada conta em seu nome. Para obter mais informações, consulte [Configurar o acesso a Contas da AWS](#).

As funções vinculadas ao serviço que são criadas em cada uma Conta da AWS são nomeadas. `AWSServiceRoleForSSO` Para obter mais informações, consulte [As funções vinculadas ao serviço do IAM Identity Center permanecem..](#)

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 realiza 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 logs CloudTrail forneçam visibilidade de quem fez todas as alterações de privilégios na conta de gerenciamento.

Configurando e usando o portal de AWS acesso

O portal de AWS acesso conecta sua força de trabalho aos Contas da AWS aplicativos em nuvem por meio do IAM Identity Center. Os administradores configuram o portal e gerenciam o acesso do usuário, enquanto os usuários finais fazem login uma vez para acessar diretamente todos os recursos autorizados.

O portal de AWS acesso fornece acesso de login único para:

- Contas da AWS na sua organização.
- AWS aplicativos gerenciados, como Amazon Quick e Kiro.
- Aplicações em nuvem como Office 365, Concur, Salesforce e outros.

Quando os usuários entram no portal, eles encontram Contas da AWS os aplicativos que estão autorizados a acessar sem login adicional.

Introdução ao portal de AWS acesso

Para administradores:

Você precisa de acesso administrativo à [instância da sua organização](#) ou [instância da conta](#) do IAM Identity Center para configurar o portal de AWS acesso e gerenciar o acesso do usuário.

1. Opcionalmente, personalize a URL do portal de AWS acesso.
2. Atribua acesso ao usuário Contas da AWS e aos aplicativos. AWS Os recursos atribuídos são exibidos no portal.

Para usuários finais:

Seu administrador deve ter concluído a configuração do portal de AWS acesso e fornecido a você a URL do portal e as credenciais de entrada.

1. Obtenha o URL do portal do administrador (normalmente, `https://your-company.awsapps.com/start`).
2. Faça login usando as credenciais fornecidas pelo administrador.

3. Acesse os recursos no portal.

Configurar o portal de AWS acesso

Como administrador, você pode personalizar o portal de AWS acesso para atender às necessidades da sua organização e garantir que os usuários possam acessar facilmente seus recursos autorizados.

O que você pode configurar

AWS ativação do portal de acesso: configure o acesso inicial do usuário ao portal de AWS acesso, incluindo ativação da credencial do usuário e processos de login pela primeira vez.

URL personalizada do portal de AWS acesso (opcional): Personalize a URL do portal de AWS acesso da sua organização do formato padrão (`d-xxxxxxxxx.awsapps.com/start`) para um subdomínio mais reconhecível (`.your-company.awsapps.com/start`).

Antes de começar

Certifique-se de ter acesso administrativo ao IAM Identity Center, verifique se o IAM Identity Center está configurado como uma [instância de organização](#) ou [instância de conta](#) e planeje o nome de subdomínio personalizado (essa é uma configuração única que não pode ser alterada posteriormente).

Depois de configurados, os usuários podem AWS acessar o portal de acesso usando a URL personalizada e seguir o processo de ativação que você estabeleceu para sua organização.

Tópicos

- [Ativando o portal de AWS acesso para usuários iniciantes do IAM Identity Center](#)
- [Personalizando a URL do portal de AWS acesso](#)
- [Confirme se os usuários podem entrar no portal de AWS acesso](#)

Ativando o portal de AWS acesso para usuários iniciantes do IAM Identity Center

Se esta é a primeira vez que você tenta entrar 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 seguintes métodos 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 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 conecta você automaticamente. Se isso não ocorrer, você poderá fazer login manualmente no portal de acesso da AWS usando as instruções fornecidas em [Entrando no portal de AWS acesso](#).

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-xxxxxxxxx.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 Centro de Identidade do AWS IAM console em <https://console.aws.amazon.com/singlesignon/>.
2. No console do IAM Identity Center, no painel de navegação, escolha Painel e localize a seção Resumo das configurações.
3. Escolha o botão Personalizar abaixo da URL do seu portal de AWS acesso.

 Note

Quando o botão Personalizar não é exibido, significa que o portal de acesso AWS 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 de subdomínio desejado e escolha Salvar.

Agora você pode entrar no AWS Console por meio do seu portal de AWS acesso com sua URL personalizada.

Confirme se os usuários podem entrar no portal de AWS acesso

As etapas a seguir são para que o administrador do IAM Identity Center confirme se o usuário do IAM Identity Center pode entrar no AWS portal de acesso e acessar Conta da AWS o.

Faça login no portal de AWS acesso

1. Realize um dos procedimentos a seguir para entrar no Console de gerenciamento da AWS.
 - 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, insira a 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 identidade, faça login usando as credenciais de usuário do Active Directory ou do IdP.
 - Se você estiver usando o diretório padrão do Identity Center como a fonte de identidade, faça o login usando o nome de usuário que você especificou ao criar o usuário e a nova senha que especificou para o usuário.
6. Na guia Contas, Conta da AWS localize sua e expanda-a.

7. Os perfis disponíveis para você são exibidos. Por exemplo, se você receber o conjunto de `AdministratorAccess` permissões 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.
8. 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 vir 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 ou grupo 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 no Console de gerenciamento da AWS e saia 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 puder 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.

Use o portal de AWS acesso

Você pode iniciar vários aplicativos escolhendo a guia Conta da AWS ou 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 essas Contas da AWS ou aplicativos. Isso também significa que você pode acessar todas essas contas ou aplicativos do portal de AWS acesso sem solicitações adicionais de login.

Como usar o portal de AWS acesso

Para usar o portal de AWS acesso:

1. Obtenha o URL do portal do administrador (normalmente tem a aparência de `https://your-company.awsapps.com/start`).
2. Faça login usando as credenciais fornecidas pelo administrador.
3. Escolha as contas e aplicações no portal que você deseja acessar.

O administrador controla o que você vê no portal com base no seu perfil e permissões. Entre em contato com o administrador ou helpdesk para solicitar acesso adicional nessas situações:

- Você não vê um aplicativo Conta da AWS ou que precisa acessar.
- O acesso que você tem a uma determinada conta ou aplicação não é o que você esperava.

Tópicos

- [Entrando no portal de AWS acesso](#)
- [Redefinindo sua senha de usuário do portal de AWS acesso](#)
- [Obter credenciais de usuário do IAM Identity Center para o ou AWS CLI AWS SDKs](#)
- [Criação de links de atalho para destinos Console de gerenciamento da AWS](#)
- [Registro de um dispositivo para MFA](#)
- [Como visualizar e encerrar a sessão ativa](#)

Entrando no portal de AWS acesso

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. A seguir, descrevemos como você pode entrar no portal de AWS acesso, dicas para entrar e como sair do portal de AWS acesso.

Pré-requisitos

O IAM Identity Center precisa estar habilitado para usar o portal de AWS acesso. Para obter mais informações, consulte [Habilitar o IAM Identity Center](#).

 Note

Depois de entrar, a duração padrão da sua sessão do portal de AWS acesso é de 8 horas. Lembre-se de que um administrador pode [alterar a duração](#) dessa sessão.

Faça login no portal de AWS acesso

Para entrar no portal de AWS acesso

1. Na janela do navegador, cole o URL de login que lhe foi fornecido e pressione Enter. O URL se parece com `d-xxxxxxxxxx.awsapps.com/start` ou `your_subdomain.awsapps.com/start`. É recomendável marcar esse link para o portal agora, para que possa acessá-lo rapidamente mais tarde.
2. Faça login usando as credenciais de login padrão da empresa.

 Note

Se o administrador lhe enviou uma senha de uso único (OTP) por e-mail e esta é a primeira vez que você faz login, insira essa senha. Depois de fazer login, você deve criar uma nova senha para futuros logins.

Se for solicitado um código de verificação, verifique seu e-mail, copie e cole o código na página de login.

 Note

Normalmente, os códigos de verificação são enviados por e-mail, mas o método de entrega pode variar. Para obter detalhes, consulte o administrador.

3. Uma vez conectado, você pode acessar qualquer Conta da AWS aplicativo exibido no portal.

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 seja necessário 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 atualizados 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 .

Redefinindo sua senha de usuário do portal de AWS acesso

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 [Console de gerenciamento da AWS](#), 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 AD](#) como sua fonte de identidade. Se o usuário estiver conectado a um provedor de identidades externo ou ao [AD Connector](#), as redefinições de senha de usuário deverão ser feitas no provedor de identidades externo ou no Active Directory conectado.

- Se a fonte de identidades for um diretório do IAM Identity Center, consulte [Requisitos de senha ao gerenciar identidade no IAM Identity Center](#).
- Se a fonte de identidades for uma AWS Managed Microsoft AD, consulte [Requisitos de senha ao redefinir uma senha no 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. 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 ou AWS CLI AWS SDKs

Você pode acessar AWS os serviços programaticamente usando o AWS Command Line Interface ou AWS Software Development Kits (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 o AWS SDKs para acessar AWS serviços de forma programática, seguir os procedimentos neste tópico também estabelecerá diretamente a autenticação para o. AWS SDKs Para obter informações sobre o AWS SDKs, consulte o [Guia de referência de ferramentas 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 sempre 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 Identity Center e criar um usuário do IAM Identity Center, consulte [Conceitos básicos do Centro de Identidade do IAM](#).
- 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 obter mais informações, consulte [Atribuir acesso de usuário ou grupo 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 Identity 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 obter mais informações, consulte [Defina a duração da sessão para Contas da AWS](#).

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 designado para qualquer 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 vir 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 obter mais informações, consulte [Atribuir acesso de usuário ou grupo 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 `PowerUserAccess` permissões da conta, a função aparecerá no portal de AWS acesso como `PowerUserAccess`.
4. Dependendo da sua opção ao lado do nome do perfil, escolha Chaves de acesso ou Linha de comando ou acesso programático.

5. Na caixa de diálogo Obter credenciais, escolha macOS e Linux, Windows PowerShell, 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 Conta da AWS específica. 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 opção ao lado do nome do perfil do IAM, escolha Chaves de acesso ou Linha de comando ou acesso programático.

Note

Se você não vir 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 obter mais informações, consulte [Atribuir acesso de usuário ou grupo a Contas da AWS](#).

3. Na caixa de diálogo Obter credenciais, escolha macOS e Linux, Windows PowerShell, 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, inclusive as configurações nos arquivos `credentials` e nos arquivos `config`. 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 [Arquivos de configuração e credenciais compartilhados no Guia](#) de referência de ferramentas 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 criar na 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 Console de gerenciamento da AWS

Os links de atalho criados no portal de AWS acesso levam os usuários do IAM Identity Center a um destino específico no Console de gerenciamento da AWS, com um conjunto de permissões específico e em um determinado Conta da AWS.

Os links de atalho poupam tempo a você e a seus colaboradores. Em vez de navegar até o URL de destino desejado Console de gerenciamento da AWS (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 de link de atalhos

Os links de atalho têm três opções de destino, listadas aqui por ordem de prioridade:

- (Opcional) Qualquer URL de destino no Console de gerenciamento da AWS 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 mais informações sobre a configuração de estado de retransmissão, consulte [Defina o estado do relé para acesso rápido ao Console de gerenciamento da AWS](#).
- Console de gerenciamento da AWS 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 planejar especificar um URL de destino (a primeira opção na lista anterior), você poderá 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 contas IDs e nomes correspondentes que você pode acessar. Você só pode escolher uma conta à qual tenha acesso.
- b. Opcionalmente, escolha um perfil do IAM na lista suspensa. Esses são os conjuntos de permissões atribuídos a você para a conta selecionada. Se você não escolher o perfil, será solicitado que os usuários selecionem um perfil atribuído 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 só funcionam com os conjuntos de permissões já atribuídos ao usuário. Se o usuário não tiver os conjuntos de permissões necessários atribuídos para conta e o URL de destino, o acesso será negado.

- c. Opcionalmente, insira a URL de destino do portal de AWS acesso. Se você não inserir 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, de acordo com a 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 suficientes.

Construindo links de Console de gerenciamento da AWS 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 no 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:

IPv4 ponto final:

`https://[your_subdomain].awsapps.com/start/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination]`

Endpoint de pilha dupla

`https://[identity_center_instance_id].portal.[region].app.aws/#/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 permissões de S3FullAccess e o leva à página inicial do console S3:

- IPv4 ponto final: `https://example.awsapps.com/start/#/console?
account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- Endpoint de pilha dupla: `https://ssoins-1234567890abcdef.portal.us-east-1.app.aws/#/console?
account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) IPv4 ponto final: `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`
- (AWS GovCloud (US) Region) Endpoint de pilha dupla: `https://ssoins-1234567890abcdef.portal.us-gov-west-1.app.aws/#/console?
account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`

Registro de um dispositivo para MFA

Para usuários no diretório do Identity Center, use o seguinte procedimento no portal de acesso do AWS para registrar o novo dispositivo para autenticação multifator (MFA).

Important

Atualmente, o MFA no IAM Identity Center não é compatível com [provedores de identidade externos](#).

Antes de começar

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](#).

Registrar o dispositivo

Para registrar o dispositivo para usar com MFA

1. Entre no seu portal de AWS acesso. Para obter 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 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, depois, use o app para digitalizar o código de QR. Por exemplo, você pode escolher o ícone de câmera ou escolher uma opção semelhante a Digitalizar código. 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 a aplicação 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.

Como visualizar e encerrar a sessão ativa

Você pode usar seu portal de AWS acesso para visualizar a lista de suas sessões ativas e, se necessário, encerrar uma ou mais sessões.

Encerre sua sessão ativa usando seu portal de AWS acesso

1. Entre no seu portal de AWS acesso. Para obter mais informações, consulte [Entrando no portal de AWS acesso](#).
2. Próximo do canto superior direito da página, escolha Segurança.
3. Na página Segurança, o número entre parênteses ao lado de Sessões ativas indica quantas sessões ativas você tem. Marque a caixa de seleção ao lado de cada sessão que você deseja encerrar e escolha Encerrar sessões.

 Tip

Para a sessão de usuário em segundo plano, você pode pesquisar sessões pelo nome do recurso da Amazon (ARN) da tarefa que está usando a sessão. Na lista Tipo de sessão, escolha Sessões de usuários em segundo plano e insira o ARN da tarefa na caixa de pesquisa.

Você só pode encerrar as sessões ativas que estão carregadas. Se você tiver muitas sessões, escolha Carregar mais sessões ativas para exibir sessões adicionais.

4. Marque a caixa de seleção ao lado de cada sessão que você deseja encerrar e escolha Encerrar sessões.
5. É exibida uma caixa de diálogo que confirma que você está encerrando sessões ativas. Revise as informações e, se quiser continuar, digite `confirm` e escolha Encerrar sessões.

6. Você retornará à lista de sessões ativas. Uma mensagem de notificação verde será exibida indicando que as sessões selecionadas foram encerradas com sucesso.

Usando o IAM Identity Center em várias Regiões da AWS

Este tópico explica como usar Centro de Identidade do AWS IAM em várias Regiões da AWS. Saiba como replicar sua instância para regiões adicionais, gerenciar o acesso e as sessões da força de trabalho, implantar aplicativos e manter o acesso à conta durante interrupções no serviço.

Ao habilitar uma instância organizacional do IAM Identity Center, você escolhe uma única Região da AWS (região primária). Você pode replicar essa instância para mais Regiões da AWS se ela atender a determinados pré-requisitos. O IAM Identity Center replica automaticamente identidades da força de trabalho, conjuntos de permissões, atribuições de usuários e grupos, sessões e outros metadados da região primária para as regiões adicionais escolhidas.

Benefícios do suporte multirregional

A replicação do IAM Identity Center para outras Regiões da AWS fornece dois benefícios principais:

- Maior resiliência de Conta da AWS acesso — Sua força de trabalho pode acessar seus Conta da AWS dados mesmo que a instância do IAM Identity Center sofra uma interrupção do serviço em sua região principal. Isso se aplica ao acesso com permissões provisionadas antes da interrupção.
- Maior flexibilidade na escolha de regiões de implantação para aplicativos AWS gerenciados — Você pode implantar aplicativos AWS gerenciados em suas regiões preferidas para atender aos requisitos de residência de dados de aplicativos e melhorar o desempenho por meio da proximidade com os usuários. Os aplicativos implantados em regiões adicionais acessam as identidades replicadas da força de trabalho localmente para obter desempenho e confiabilidade ideais.

Pré-requisitos e considerações

Antes de replicar sua instância do IAM Identity Center, certifique-se de que os seguintes requisitos sejam atendidos:

- Tipo de instância: sua instância do IAM Identity Center deve ser uma [instância da organização](#). O suporte multirregional não está disponível nas [instâncias da conta](#).
- Fonte de identidade - Sua instância do IAM Identity Center deve estar conectada a um provedor de identidade externo (IdP), como. [Okta](#) O suporte multirregional não está disponível para instâncias que usam o [Active Directory](#) ou o [diretório do Identity Center](#) como fonte de identidade.

- AWS Regiões - O suporte multirregional está disponível em [regiões comerciais habilitadas por padrão](#) em seu Conta da AWS. Atualmente, não há suporte para regiões opcionais.
- Tipo de chave KMS para criptografia em repouso — Sua instância do IAM Identity Center deve ser configurada com uma chave [KMS multirregional gerenciada pelo cliente](#). A chave KMS deve estar localizada na mesma AWS conta do IAM Identity Center. Para obter mais informações, consulte [Implementando chaves KMS gerenciadas pelo cliente em Centro de Identidade do AWS IAM](#).
- AWS compatibilidade de aplicativos gerenciados - Visite a tabela de aplicativos [the section called “Aplicações que você pode usar com o IAM Identity Center”](#) para confirmar os dois requisitos de aplicativos a seguir:
 - Todos os aplicativos AWS gerenciados que estão em uso pela sua organização devem oferecer suporte ao IAM Identity Center, configurado com uma chave KMS gerenciada pelo cliente.
 - Os aplicativos AWS gerenciados que você deseja implantar em regiões adicionais devem oferecer suporte a esse tipo de implantação.
- Compatibilidade com IdP externo - Para aproveitar totalmente o suporte multirregional, o IdP externo deve oferecer suporte ao serviço de consumidor de múltiplas declarações (ACS).
URLs Esse é um recurso SAML compatível com, por IdPs exemplo OktaMicrosoft Entra ID, PingFederate, PingOne, e. JumpCloud

Se você usa um IdP que não suporta vários ACS URLs, como Google Workspace, recomendamos que você trabalhe com seu fornecedor de IdP para habilitar esse recurso. Para opções que estão disponíveis sem vários ACS URLs, consulte [the section called “Usando aplicativos AWS gerenciados sem vários ACS URLs”](#) e [the section called “Conta da AWS resiliência de acesso sem vários ACS URLs”](#)

Escolhendo uma região adicional

Ao escolher uma região adicional entre as regiões comerciais ativadas por padrão, considere estes fatores:

- Requisitos de conformidade — Se você precisar executar aplicativos AWS gerenciados que acessam conjuntos de dados limitados a uma região específica por motivos de conformidade, escolha a região em que os conjuntos de dados residem.
- Otimização do desempenho — Se a residência dos dados não for um fator, selecione uma região mais próxima dos usuários do seu aplicativo para otimizar sua experiência.

- Suporte de aplicativos — Verifique se os AWS aplicativos necessários estão disponíveis na região escolhida.
- Conta da AWS resiliência de acesso — Para continuidade do acesso a Conta da AWS s, escolha uma região geograficamente distante da região primária da sua instância do IAM Identity Center.

 Note

O IAM Identity Center tem uma cota no número de Regiões da AWS. Para obter mais informações, consulte [the section called “Cotas adicionais”](#).

Replique o IAM Identity Center para uma região adicional

Se seu ambiente atender aos [pré-requisitos](#), como configurar o IAM Identity Center com uma chave KMS multirregional gerenciada pelo cliente, conclua as etapas a seguir para replicar sua instância do IAM Identity Center em uma região adicional. Sua região principal continua operando normalmente durante e após essas etapas.

Etapas 1: criar uma chave de réplica na região adicional

Antes de replicar o IAM Identity Center em uma região, você deve primeiro criar uma chave de réplica da chave KMS gerenciada pelo cliente nessa região e configurar a chave de réplica com as permissões necessárias para as operações do IAM Identity Center. Para obter instruções sobre como criar chaves de réplica em várias regiões, consulte [Criar chaves de réplica em várias regiões](#).

A abordagem recomendada para as permissões de chave do KMS é copiar a política de chaves da chave primária, o que concede as mesmas permissões já estabelecidas para o IAM Identity Center na região primária. Como alternativa, você pode definir políticas de chave específicas para cada região, embora essa abordagem aumente a complexidade do gerenciamento de permissões entre regiões e possa exigir coordenação adicional ao atualizar políticas no futuro.

 Note

AWS KMS não sincroniza sua política de chaves KMS entre as regiões de sua chave KMS multirregional. Para manter a política de chaves do KMS sincronizada entre as principais regiões do KMS, você precisará aplicar as alterações em cada região individualmente.

Etapa 2: adicionar a região no IAM Identity Center

Adicionar uma região ao IAM Identity Center aciona a replicação automática dos dados do IAM Identity Center para essa região. A replicação é assíncrona com consistência eventual. As guias a seguir fornecem instruções para fazer isso no Console de gerenciamento da AWS e. AWS CLI

Console

Para adicionar uma região

1. Abra o [console do IAM Identity Center](#).
2. No painel de navegação, selecione Configurações.
3. Escolha a guia Gerenciamento.
4. Na seção Regiões para o IAM Identity Center, escolha Adicionar região.
5. Na seção Regiões da AWS disponível para replicação, escolha sua preferência Região da AWS. Se a região não aparecer na lista, ela não estará disponível para replicação porque a chave KMS não foi replicada lá. Para obter mais informações, consulte [the section called “Como implementar chaves KMS gerenciadas pelo cliente”](#).
6. Selecione Adicionar região.
7. Na seção Regiões do IAM Identity Center, monitore o status da região. Use o botão Atualizar (seta circular) para verificar o status mais recente da região, conforme necessário. Depois que a replicação for concluída, vá para a Etapa 2.

AWS CLI

Para adicionar uma região

```
aws sso-admin add-region \
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
  --region-name eu-west-1
```

Para verificar o status atual da região

```
aws sso-admin describe-region \
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
  --region-name eu-west-1
```

Quando o status da Região for ATIVO, você poderá prosseguir para a Etapa 2.

A duração da replicação inicial para uma região adicional depende da quantidade de dados na sua instância do IAM Identity Center. Na maioria dos casos, as alterações incrementais subsequentes são replicadas em segundos.

Etapa 3: atualizar a configuração do IdP externo

Siga o tutorial do seu IdP externo [Tutoriais sobre fonte de identidades](#) para seguir as seguintes etapas:

Etapa 3.a: Adicionar o Assertion Consumer Service (ACS) URLs ao seu IdP externo

Essa etapa permite o login direto em cada região adicional e é necessária para permitir o login em aplicativos AWS gerenciados implantados nessas regiões e para Conta da AWS acesso a s por meio dessas regiões. Para saber onde encontrar o ACS URLs, consulte [Endpoints ACS no primário e adicional Regiões da AWS](#).

Etapa 3.b (opcional): Portal de acesso da AWS disponibilizar o no portal externo do IdP

Portal de acesso da AWS Disponibilize o na região adicional como um aplicativo de favoritos no portal externo do IdP. Os aplicativos de favoritos contêm apenas um link (URL) para o destino desejado e são semelhantes a um marcador do navegador. Você pode encontrá-las Portal de acesso da AWS URLs no console escolhendo Exibir tudo Portal de acesso da AWS URLs na seção Regiões do IAM Identity Center. Para obter mais informações, consulte [the section called “AWS acesse os endpoints do portal nos terminais primário e adicional Regiões da AWS”](#).

O IAM Identity Center é compatível com SAML SSO iniciado pelo IdP em cada região adicional, mas os externos IdPs normalmente oferecem suporte a isso com apenas uma única URL do ACS. Para continuidade, recomendamos manter o URL do ACS da região principal em uso para o SAML SSO iniciado pelo IdP e confiar nos aplicativos de favoritos e nos favoritos do navegador para acessar regiões adicionais.

Etapa 4: Confirme as listas de permissões do firewall e do gateway

[Revise suas listas de permissões de domínio em firewalls ou gateways e atualize-as com base nas listas de permissões documentadas](#).

Etapa 5: fornecer informações aos seus usuários

Forneça aos usuários informações sobre a nova configuração, incluindo o Portal de acesso da AWS URL na região adicional e como usar as regiões adicionais. Consulte as seções a seguir para obter detalhes relevantes:

- [the section called “Acesso à força de trabalho por meio de uma região adicional”](#)
- [the section called “Failover para uma região adicional para acesso Conta da AWS ”](#)
- [the section called “Implantação e gerenciamento de aplicativos em várias Regiões da AWS”](#)

A região muda além da adição da primeira região

Você pode adicionar e remover regiões adicionais. A região primária não pode ser removida a não ser excluindo toda a instância do IAM Identity Center. Para obter mais informações sobre como remover uma região, consulte [the section called “Remover uma região do IAM Identity Center”](#).

Você não pode promover uma região adicional para ser a principal ou rebaixar a região principal para ser adicional.

Quais dados são replicados?

O IAM Identity Center replica os seguintes dados:

Dados	Origem e destino da replicação
Identities da força de trabalho (usuários, grupos, associações a grupos)	Da região primária às regiões adicionais
Conjuntos de permissões e suas atribuições a usuários e grupos	Da região primária às regiões adicionais
Configuração (como configurações SAML de IdP externo)	Da região primária às regiões adicionais
Metadados de aplicativos e atribuições de aplicativos para usuários e grupos	Da região do centro de identidade do IAM conectada de um aplicativo às outras regiões habilitadas
Emissores de tokens confiáveis	Da região primária às regiões adicionais

Dados	Origem e destino da replicação
Sessões	Da região de origem da sessão para as outras regiões habilitadas

Note

O IAM Identity Center não replica dados armazenados em aplicativos AWS gerenciados. Além disso, isso não altera a abrangência regional da implantação de um aplicativo. Por exemplo, se sua instância do IAM Identity Center estiver no Leste dos EUA (Norte da Virgínia) e você tiver o Amazon Redshift implantado na mesma região, a replicação do IAM Identity Center para o Oeste dos EUA (Oregon) não afetará a região de implantação do Amazon Redshift e os dados que ele armazena.

Considerações:

- Identificadores globais de recursos nas regiões habilitadas - usuários, grupos, conjuntos de permissões e outros recursos têm os mesmos identificadores nas regiões habilitadas.
- A replicação não afeta as funções provisionadas do IAM — as funções existentes do IAM provisionadas a partir de atribuições de conjuntos de permissões são usadas durante o login da conta em qualquer região habilitada.

Acesso à força de trabalho por meio de uma região adicional

Esta seção explica como sua força de trabalho pode acessar os Portal de acesso da AWS, Conta da AWS e aplicativos quando você habilita o IAM Identity Center em várias regiões.

Portal de acesso da AWS Em uma região adicional exibe Conta da AWS os aplicativos aos quais sua força de trabalho tem acesso da mesma forma que na região primária. Sua força de trabalho pode entrar em uma região adicional por meio de um link direto para o endpoint do portal regional (por exemplo, <https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com>) ou por meio de um [aplicativo de favoritos](#) que você configurou no IdP externo. Portal de acesso da AWS

Você pode usar o Portal de acesso da AWS endpoint em uma região adicional para autorizar o AWS CLI acesso APIs como usuário do IAM Identity Center. Essa funcionalidade funciona da mesma

forma que na região principal. No entanto, as autorizações da CLI não são replicadas nas regiões habilitadas. Portanto, você precisa autorizar a CLI em cada região individualmente.

Sessões de usuário em várias Regiões da AWS

O IAM Identity Center replica as sessões do usuário da região de origem para as outras regiões habilitadas. A revogação e a saída da sessão em uma região também são replicadas para as outras regiões.

Revogação de sessão pelos administradores do IAM Identity Center

Os administradores do IAM Identity Center podem revogar sessões de usuários em outras regiões. Como as sessões são replicadas entre regiões, em condições normais, basta revogar uma sessão em uma única região e permitir que o IAM Identity Center replique a alteração nas outras regiões habilitadas. Se a região principal do IAM Identity Center tiver uma interrupção, os administradores poderão realizar essa operação em outras regiões.

Portal de acesso da AWS endpoints no primário e adicional Regiões da AWS

Se você precisar consultar o portal de AWS acesso URLs para as regiões habilitadas, siga estas etapas:

1. Abra o [console do IAM Identity Center](#).
2. No painel de navegação, selecione Configurações.
3. Escolha a guia Gerenciamento.
4. Na seção Regiões do IAM Identity Center, escolha Visualizar todo o portal de AWS acesso URLs.

A tabela a seguir especifica os Portal de acesso da AWS endpoints nas regiões primária e adicional de uma instância do IAM Identity Center.

Portal de acesso da AWS endpoint	Região principal	Região adicional	Padrão e exemplo de URL
Clássico IPv4 apenas ¹	Sim	Não	Pattern: <code>https://[Identity Store ID].awsapps.com/start</code>

Portal de acesso da AWS endpoint	Região principal	Região adicional	Padrão e exemplo de URL
			Exemplo: <code>https://d-12345678.awsapps.com/start</code>
Apenas 1 alias personalizado IPv4	Sim (opcional)	Não	Pattern: <code>https://[<i>custom alias</i>].awsapps.com/start</code> Exemplo: <code>https://mycompany.awsapps.com/start</code>
Alternativa: IPv4 apenas ²	Sim	Sim	Pattern: <code>https://[<i>Identity Center instance ID</i>].[<i>Region</i>].portal.amazonaws.com</code> Exemplo: <code>https://soins-111111h2222j33pp.eu-west-1.portal.amazonaws.com</code>
Dual-stack ²	Sim	Sim	Pattern: <code>https://[<i>Identity Center instance ID</i>].portal.[<i>Region</i>].app.aws</code> Exemplo: <code>https://soins-111111h2222j33pp.portal.eu-west-1.app.aws</code>

¹ Em regiões adicionais, o alias personalizado não é suportado e o domínio `awsapps.com` principal não está disponível.

² Os endpoints do portal, IPv4 somente alternativos e de pilha dupla, não têm o final na URL. /start

Endpoints do Assertion Consumer Service (ACS) nos terminais primários e adicionais Regiões da AWS

Se você precisar pesquisar o ACS URLs ou baixá-lo como parte dos metadados do SAML, siga estas etapas:

1. Abra o [console do IAM Identity Center](#).
2. No painel de navegação, selecione Configurações.
3. Escolha a guia Origem da identidade.
4. No menu suspenso Ações, escolha Gerenciar autenticação.
5. A seção Metadados do provedor de serviços exibe o URL Portal de acesso da AWS e o ACS para cada região habilitada. IPv4-only e dual-stack URLs são exibidos em guias separadas. Se o seu IdP suportar o upload de um arquivo de metadados SAML, você pode escolher Baixar arquivo de metadados para baixar o arquivo de metadados SAML com todos os ACS. URLs Se o seu IdP não suportar o upload de um arquivo de metadados ou se você preferir adicionar o ACS URLs individualmente, você poderá copiar o indivíduo URLs da tabela no console ou escolher Exibir URLs ACS e depois Copiar tudo. URLs Mantenha a URL do ACS que já está configurada para a região primária para garantir que o login único SAML iniciado pelo provedor de serviços a partir da região primária permaneça funcional.

A tabela a seguir especifica os endpoints do SAML Assertion Consumer Service (ACS) nas regiões primária e adicional de uma instância do IAM Identity Center:

Endpoint ACS	Região principal	Região adicional	Padrão e exemplo de URL
IPv4 somente	Sim	Sim	Pattern: <code>https://[Region].signin.aws/platform/saml/acs/ [Tenant ID]</code> Exemplo: <code>https://us-west-2.signin.aws/platform/saml/ac</code>

Endpoint ACS	Região principal	Região adicional	Padrão e exemplo de URL
			s/1111111111111111-aaee-fff f-dddd-1111111111
IPv4 Somente alternativa*	Sim	Não	Pattern: <code>https://[Region].signin.aws.amazon.com/platform/saml/acs/[Tenant ID]</code> Exemplo: <code>https://us-west-2.signin.aws.amazon.com/platform/saml/acs/1111111111111111-aaee-ffff-dddd-1111111111</code>
Pilha dupla	Sim	Sim	Pattern: <code>https://[Region].sso.signin.aws/platform/saml/acs/[Tenant ID]</code> Exemplo: <code>https://us-west-2.sso.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-1111111111</code>

* Para instâncias que foram habilitadas antes de fevereiro de 2026, mantenha esse endpoint porque o login único SAML iniciado pelo provedor de serviços na região primária o exige. O IAM Identity Center não usa esse endpoint para instâncias que foram habilitadas em fevereiro de 2026 ou mais tarde.

Usando aplicativos AWS gerenciados sem vários ACS URLs

Alguns provedores de identidade externos (IdPs) não oferecem suporte a vários serviços ao consumidor de asserção (ACS) URLs em seu aplicativo IAM Identity Center. Vários ACS URLs são um recurso SAML necessário para o login direto em uma região específica em um centro de identidade IAM multirregional.

Por exemplo, se você iniciar um aplicativo AWS gerenciado por meio de um link de aplicativo, o sistema acionará o login por meio da região do centro de identidade do IAM conectada ao aplicativo. No entanto, se o URL do ACS dessa região não estiver configurado no IdP externo, o login falhará.

Para resolver esse problema, trabalhe com seu fornecedor de IdP para habilitar o suporte para vários ACS. Enquanto isso, você ainda pode usar aplicativos AWS gerenciados em regiões adicionais. Primeiro, faça login na região cujo URL do ACS está configurado no IdP externo (a região primária por padrão). Depois de ter uma sessão ativa no IAM Identity Center, você pode iniciar o aplicativo a partir do portal de AWS acesso em qualquer região habilitada ou por meio de um link de aplicativo.

Failover para uma região adicional para acesso Conta da AWS

O tópico de Conta da AWS acesso por meio do IAM Identity Center é abordado extensivamente em [Conta da AWS acesso](#). Esta seção fornece detalhes adicionais relevantes para manter o Conta da AWS acesso entre várias Regiões da AWS no caso de uma interrupção do serviço na região principal.

Se sua instância do IAM Identity Center sofrer uma interrupção na região principal (por exemplo, o portal de AWS acesso na região primária não estiver disponível), sua força de trabalho poderá mudar para uma região adicional para continuar acessando aplicativos não Conta da AWS afetados. Para obter mais informações, consulte [the section called “Acesso à força de trabalho por meio de uma região adicional”](#).

Recomendamos que você comunique os Portal de acesso da AWS endpoints em regiões adicionais e a configuração do IdP externo (como aplicativos de favoritos para as regiões adicionais) à sua força de trabalho assim que concluir a configuração. [the section called “Replique o IAM Identity Center para uma região adicional”](#) Isso permitirá que eles estejam prontos para o failover para uma região adicional, se necessário.

Da mesma forma, recomendamos que AWS CLI os usuários criem [AWS CLI perfis](#) para regiões adicionais para cada um dos perfis que eles têm para a região principal. Em seguida, eles podem mudar para esse perfil se houver uma interrupção do serviço na região principal.

Note

A continuidade do acesso a Conta da AWS s também depende da integridade do seu IdP externo e das permissões, como atribuições de conjuntos de permissões e associações a

grupos, provisionadas e replicadas antes da interrupção do serviço. Recomendamos que sua organização também configure o acesso [AWS rápido para manter o AWS acesso a um pequeno grupo de usuários privilegiados quando o IdP externo tiver uma interrupção](#) no serviço. O [acesso de emergência](#) é uma opção semelhante que evita o uso de usuários do IAM, mas também depende do IdP externo.

Conta da AWS resiliência de acesso sem vários ACS URLs

Alguns provedores de identidade externos (IdPs) não oferecem suporte a vários serviços ao consumidor de asserção (ACS) URLs em seu aplicativo IAM Identity Center. Vários ACS URLs são um recurso SAML necessário para o login direto em uma região específica em um centro de identidade IAM multirregional.

Para permitir que seus usuários os acessem Contas da AWS por meio de várias regiões do IAM Identity Center, você deve configurar o respectivo ACS regional URLs no IdP externo. No entanto, se o IdP externo oferecer suporte apenas a uma única URL do ACS em seu aplicativo do IAM Identity Center, os usuários poderão fazer login diretamente em uma única região do IAM Identity Center.

Para resolver esse problema, trabalhe com seu fornecedor de IdP para habilitar o suporte para vários ACS. URLs Enquanto isso, você pode usar regiões adicionais como backup para acesso a. Contas da AWS

Se ocorrer uma interrupção do serviço do IAM Identity Center na região principal, você deverá atualizar o URL do ACS no IdP externo com o URL do ACS de uma região adicional. Após essa atualização, seus usuários podem acessar o portal de AWS acesso na região adicional usando o aplicativo IAM Identity Center existente no portal externo do IdP ou por meio de um link direto que você compartilha com eles.

Recomendamos que você teste essa configuração periodicamente para garantir que ela funcione quando necessário e comunique esse processo de failover à sua organização.

Note

Quando você usa uma região adicional para acessar Contas da AWS nessa configuração, seus usuários talvez não consigam acessar aplicativos AWS gerenciados conectados à região principal. Portanto, recomendamos isso apenas como uma medida temporária para manter o acesso Contas da AWS a.

Implantação e gerenciamento de aplicativos em várias AWS regiões

O tópico de acesso a aplicativos por meio do IAM Identity Center é abordado extensivamente em [Acesso à aplicação](#). Esta seção fornece detalhes adicionais relevantes para a implantação e o gerenciamento de aplicativos em várias Regiões da AWS.

Implantação e gerenciamento de aplicativos AWS gerenciados em vários Regiões da AWS

Com uma instância do IAM Identity Center de região única, você pode implantar aplicativos AWS gerenciados na mesma região da sua instância. Alguns aplicativos, como o Amazon Q Business, oferecem suporte a uma conexão entre regiões com o IAM Identity Center, o que permite sua implantação fora da região do IAM Identity Center, se o aplicativo de interesse estiver disponível lá. No entanto, chamadas entre regiões podem causar um desempenho mais lento do aplicativo, e a maioria dos aplicativos AWS gerenciados não oferece suporte a esse tipo de conexão.

Uma instância multirregional do IAM Identity Center permite que você implante aplicativos AWS gerenciados em qualquer região habilitada com uma conexão com o IAM Identity Center na mesma região (“conexão região-local”). A implantação na região principal é suportada por todos os aplicativos AWS gerenciados integrados. Para confirmar quais aplicativos AWS gerenciados oferecem suporte à implantação em regiões adicionais do IAM Identity Center, consulte a tabela de aplicativos em [the section called “Aplicações que você pode usar com o IAM Identity Center”](#). De qualquer forma, o aplicativo AWS gerenciado deve estar disponível na região em que você deseja implantá-lo.

Com uma conexão regional local com o IAM Identity Center, os aplicativos AWS gerenciados acessam as identidades da força de trabalho na mesma região para obter desempenho e confiabilidade ideais. Recomendamos escolher uma conexão região-local ao implantar um aplicativo AWS gerenciado sempre que os [pré-requisitos](#) forem atendidos.

Para implantar um aplicativo AWS gerenciado em uma região adicional do IAM Identity Center, inicie a implantação nessa região por meio do console do aplicativo ou da API da mesma forma que você implanta na região principal.

Considerações:

- Se você ainda não replicou seu IAM Identity Center para essa região, recomendamos que você faça isso primeiro para que a implantação do aplicativo possa ser concluída imediatamente.
- AWS aplicativos gerenciados, em muitos casos, estabelecerão automaticamente uma conexão região-local se você já tiver replicado o IAM Identity Center para a região.
- Se um aplicativo AWS gerenciado oferecer uma conexão entre regiões com o IAM Identity Center, recomendamos que você escolha uma conexão região-local, desde que os [pré-requisitos](#) sejam atendidos.
- Se o aplicativo não oferecer suporte à implantação em regiões adicionais, você poderá implantá-lo na região principal, desde que o aplicativo esteja disponível lá.

Important

Se sua instância do IAM Identity Center for multirregional, todos os aplicativos AWS gerenciados em uso pela sua organização devem oferecer suporte ao IAM Identity Center configurado com uma chave KMS gerenciada pelo cliente, independentemente da região de implantação do aplicativo. Confirme isso [the section called “Aplicações que você pode usar com o IAM Identity Center”](#) antes de implantar um aplicativo e antes de configurar uma chave KMS gerenciada pelo cliente em seu IAM Identity Center.

Região de gerenciamento de um aplicativo

Depois de implantar um aplicativo AWS gerenciado em uma região adicional do IAM Identity Center usando uma conexão região-local, você gerencia o aplicativo e suas atribuições para usuários e grupos na mesma região. O IAM Identity Center replica os metadados do aplicativo, incluindo atribuições a usuários e grupos em outras regiões habilitadas, para que sua força de trabalho possa lançar aplicativos de qualquer região habilitada.

Se seu aplicativo AWS gerenciado estiver usando uma conexão entre regiões com o IAM Identity Center, você pode gerenciar os detalhes do aplicativo, como nome e descrição, e as atribuições do aplicativo para usuários e grupos por meio do console do IAM Identity Center e da API na região conectada. Independentemente do tipo de conexão, você pode gerenciar o aplicativo por meio do console em sua região de implantação.

Propagação de identidades confiáveis

Você pode usar a propagação de identidade confiável com aplicativos AWS gerenciados que a suportam em qualquer região habilitada da sua instância do IAM Identity Center.

Todos os aplicativos que propagam o contexto de identidade entre si devem estar na mesma região.

A dependência de um aplicativo em sua região conectada do centro de identidade do IAM

Cada aplicativo AWS gerenciado se conecta a uma região específica do IAM Identity Center durante a implantação. O aplicativo então depende dessa região para o login do usuário, mesmo que sua Central de Identidade do IAM esteja habilitada em várias regiões. Se o seu IAM Identity Center estiver passando por uma interrupção nessa região, os usuários talvez não consigam acessar os aplicativos AWS gerenciados conectados à região.

Implantação e gerenciamento de aplicativos gerenciados pelo cliente em várias Regiões da AWS

O IAM Identity Center é compatível com SAML e [aplicativos gerenciados pelo OAuth2 cliente](#). Você pode optar por criá-los em qualquer região habilitada da sua instância do IAM Identity Center. Depois de criar um, você gerencia o aplicativo e suas atribuições para usuários e grupos na mesma região.

Remover uma região do IAM Identity Center

Para remover uma região adicional da sua instância do IAM Identity Center, siga estas etapas:

Etapa 1: Atualizar a configuração do IdP externo

Você pode optar por remover a URL do ACS dessa região do seu IdP externo ou mantê-la caso queira adicionar essa região novamente mais tarde. Recomendamos que você remova ou oculte o aplicativo de favoritos que você possa ter criado para o Portal de acesso da AWS nesta região.

Etapa 2: remover a região

Console

Para adicionar uma região

1. Abra o [console do IAM Identity Center](#).

2. No painel de navegação, selecione Configurações.
3. Escolha a guia Gerenciamento.
4. Na seção Regiões para o IAM Identity Center, escolha a região adicional que você deseja remover.
5. Escolha Remover .
6. Antes de confirmar a remoção escolhendo Remover região, preste atenção ao aviso sobre a possível perda de acesso aos aplicativos que foram criados nessa região do IAM Identity Center. Se você não tiver certeza se tem esses aplicativos, escolha Aplicativos no painel de navegação e confirme a região conectada na coluna Criado a partir de cada aplicativo AWS gerenciado e gerenciado pelo cliente.

 Note

Você pode continuar incorrendo em cobranças pelas implantações de aplicativos AWS gerenciados que ainda estão conectados à região removida, mesmo se você perder o acesso a esses aplicativos. Para evitar isso, você precisa remover essas implantações de aplicativos AWS gerenciados por meio do console do aplicativo ou da API antes de remover a região no IAM Identity Center. Se você já removeu a região do IAM Identity Center, pode restaurar o acesso aos aplicativos adicionando a região novamente.

7. Na seção Regiões do IAM Identity Center, monitore o status da região. Use o botão Atualizar (seta circular) para ver o status mais recente da região, conforme necessário. Depois que a região é removida, ela não aparece mais na lista de regiões.

AWS CLI

Para remover uma região

```
aws sso-admin remove-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Para verificar o status atual da região

```
aws sso-admin describe-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

```
--region-name eu-west-1
```

Quando a região for removida, vá para a Etapa 2.

Etapa 3: excluir a chave de réplica

Você pode optar por remover a chave de réplica dessa região para evitar cobranças de armazenamento do KMS. Para obter mais informações, consulte [Excluindo uma AWS KMS chave](#).

 Important

Certifique-se de excluir somente a chave de réplica nessa região específica. As outras regiões do IAM Identity Center continuam contando com a chave KMS nas outras regiões habilitadas para operações normais.

O serviço IAM Identity Center é APIs suportado em outras AWS regiões

solicitações de	Funcionalidade em regiões adicionais
API do Identity Center	Compatível: • read/write Operações de gerenciamento de aplicativos • Operações de leitura de instância Não compatível: • Qualquer operação de gravação que não seja relacionada ao aplicativo • Operações de leitura de conjunto de permissões e atribuição de conta
API do Identity Store	Operações de leitura
API OIDC	Todas as operações são suportadas

solicitações de	Funcionalidade em regiões adicionais
API do portal de acesso	Todas as operações são suportadas
API SCIM	Nenhuma operação é suportada

AWS CloudTrail eventos do IAM Identity Center na região primária e adicional

Em AWS CloudTrail, você pode auditar as ações que os usuários e administradores do IAM Identity Center realizam em todas as ações habilitadas Regiões da AWS da sua instância do IAM Identity Center. Os AWS CloudTrail eventos são emitidos e registrados na região onde a ação ocorre. Para obter mais informações, consulte [the section called “Registro em log e monitoramento”](#).

Disponibilidade dos casos de uso do IAM Identity Center nas regiões primária e adicional

Recurso	Disponibilidade regional
Diretório da força de trabalho com um portal do usuário	
Acesso do usuário ao portal Portal de acesso da AWS , incluindo login no portal e sessões globais (um login para todas as regiões)	Todas as regiões habilitadas
Exibição de todas as contas atribuídas	Todas as regiões habilitadas
Exibição de todos os aplicativos atribuídos (independentemente de onde os aplicativos foram criados)	Todas as regiões habilitadas
Leia o acesso a usuários, grupos e associações no AWS console ou via Identity Store APIs	Todas as regiões habilitadas
Revogar sessões de usuário	Todas as regiões habilitadas

Recurso	Disponibilidade regional
Sincronização automática de usuários e grupos de uma fonte de identidade externa, como IdP externo por meio da API SCIM ou da API Identity Store	Somente região primária
Configure o provisionamento automático de identidade com o SCIM	Somente região primária
Configurar SAML SSO com um IdP externo	Somente região primária - acesso de leitura pelo console em todas as regiões habilitadas
Create/update/delete operações em usuários, grupos e associações de grupos por meio do console ou do Identity Store APIs.	Região primária: disponível por meio da API Identity Store, mas bloqueada no console do IAM Identity Center quando a API SCIM é usada para provisionamento (exceto o acesso disable/enable do usuário e a exclusão do usuário, que estão sempre disponíveis). Regiões adicionais: indisponível
Acesso a várias contas	
Acesse contas atribuídas por meio dos Portal de acesso da AWS links AWS CLI, e de atalho	Todas as regiões habilitadas
Gerencie conjuntos de permissões de várias contas e suas atribuições no console e APIs (incluindo acesso elevado temporário)	Somente região primária
Acesso a aplicativos e AWS serviços	
Implemente aplicativos AWS gerenciados por meio do console de aplicativos e APIs	Todas as regiões habilitadas — sujeitas à disponibilidade regional dos aplicativos e ao suporte para implantação em regiões adicionais

Recurso	Disponibilidade regional
Crie aplicativos gerenciados pelo cliente por meio do console do Identity Center e APIs	Todas as regiões habilitadas
Gerencie metadados e atribuições do aplicativo no console e APIs	Região do Centro de Identidade IAM conectada ao aplicativo
Inicie aplicativos do Portal de acesso da AWS ou diretamente por meio de um link de aplicativo ou marcador	Todas as regiões habilitadas
SSO para instâncias do Amazon EC2	Todas as regiões habilitadas
Propagação de identidade confiável	
Criar um emissor de token confiável	Somente região primária
Propagação de identidade confiável com aplicativos AWS gerenciados	Todas as regiões habilitadas - os aplicativos que propagam o contexto de identidade entre si devem estar na mesma região
Outros recursos administrativos	
Todos os outros recursos administrativos, como gerenciamento de regiões, gerenciamento de chaves KMS, gerenciamento de instâncias e gerenciamento de sessões (exceto revogação de sessão)	Somente região primária - acesso de leitura disponível em todas as regiões habilitadas para alguns dados (excluindo atribuições de conjuntos de permissões)

Design de resiliência e comportamento regional

O serviço IAM Identity Center é totalmente gerenciado e usa AWS serviços duráveis 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. Você pode replicar sua instância do IAM Identity Center para regiões adicionais para manter o acesso à conta com permissões já provisionadas no caso de uma interrupção regional. Para obter mais informações, consulte [Usando o IAM Identity Center em várias Regiões da AWS](#).

Você ativa o IAM Identity Center na sua conta AWS Organizations de gerenciamento. Isso é necessário para que o IAM Identity Center provisione, cancele e atualize funções em todos os seus Contas da AWS. Quando você ativa o IAM Identity Center, ele é Região da AWS implantado na região atualmente selecionada, chamada de “região primária”. Se você quiser implantar em uma região específica Região da AWS, altere a seleção da região antes de ativar o IAM Identity Center, pois a região primária não pode ser alterada após a ativação do IAM Identity Center.

O IAM Identity Center oferece suporte à maioria das funções administrativas somente da região principal. Isso inclui a conexão com um provedor de identidade externo, a sincronização de usuários e grupos e a criação e atribuição de conjuntos de permissões a usuários e grupos. Por outro lado, o gerenciamento dos aplicativos e suas atribuições devem ocorrer na região do Centro de Identidades do IAM em que o aplicativo foi criado.

Note

Mesmo que sua Central de Identidade do IAM seja replicada para outras regiões, recomendamos que você configure o acesso [AWS rápido](#). Isso ajuda você a manter o AWS acesso de um pequeno grupo de usuários privilegiados durante eventos como uma interrupção do serviço no IdP externo. O [acesso de emergência](#) é outra opção que usa identidades de um IdP externo em vez de usuários do IAM; no entanto, ele não protege contra uma interrupção no IdP externo.

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 ao acessarem Contas da AWS por meio do IAM Identity Center. No entanto, a maioria dos aplicativos AWS gerenciados, como o Amazon SageMaker AI, deve ser instalada em uma região da sua instância do IAM Identity Center para que os usuários 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 e [the section called “Implantação e gerenciamento de aplicativos AWS gerenciados em várias Regiões da AWS”](#)

Você também pode usar o IAM Identity Center para autenticar e autorizar o acesso a aplicativos gerenciados pelo cliente baseados em SAML que podem ser acessados por meio de uma URL pública, independentemente da plataforma ou da nuvem na qual o aplicativo é criado.

Não recomendamos o uso [Instâncias de conta do Centro de Identidade do IAM](#) como meio de implementar resiliência porque eles não oferecem suporte ao acesso à AWS conta e porque criam um segundo ponto de controle isolado que não está conectado à instância da sua organização.

Projetado para garantir disponibilidade

A tabela a seguir fornece a disponibilidade que o IAM Identity Center foi projetado para alcançar em uma única AWS região. Esses valores não representam um contrato de nível de serviço nem uma garantia, e sim uma visão das metas de projeto. As porcentagens de disponibilidade referem-se ao acesso a dados ou funções, não à durabilidade (por exemplo, retenção de dados a longo prazo).

Componente do serviço	Meta de design de disponibilidade
Plano de dados (incluindo login)	99.95%
Ambiente de gerenciamento	99.90%

Configure o acesso de emergência ao Console de gerenciamento da AWS

O IAM Identity Center é construído a partir de uma AWS infraestrutura 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 ao Console de gerenciamento da AWS.

AWS permite que você:

- [Conectar seu IdP de terceiros ao IAM Identity Center](#).

- Conecte seu IdP de terceiros ao indivíduo Contas da AWS 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 Conta da AWS acesso. Se o IAM Identity Center for interrompido, seus usuários de operações de emergência poderão fazer login no Console de gerenciamento da AWS 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. [Se você preferir não depender do IdP externo, considere configurar AWS o acesso sem vidro](#)

 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 exigidos 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.

Tópicos

- [Resumo da configuração de acesso de emergência](#)
- [Como projetar suas funções operacionais críticas](#)
- [Como planejar seu modelo de acesso](#)
- [Como criar um mapeamento emergencial de funções, contas e grupos](#)
- [Como criar sua configuração de acesso de emergência](#)
- [Tarefas preparatórias de emergência](#)
- [Processo de failover de emergência](#)
- [Retorno às operações normais](#)
- [Configuração única de um aplicativo de federação direta do IAM no Okta](#)
- [Configuração única de um aplicativo de federação direta do IAM com ADFS](#)

Resumo da configuração de acesso de emergência

Execute as tarefas a seguir para configurar o acesso de emergência.

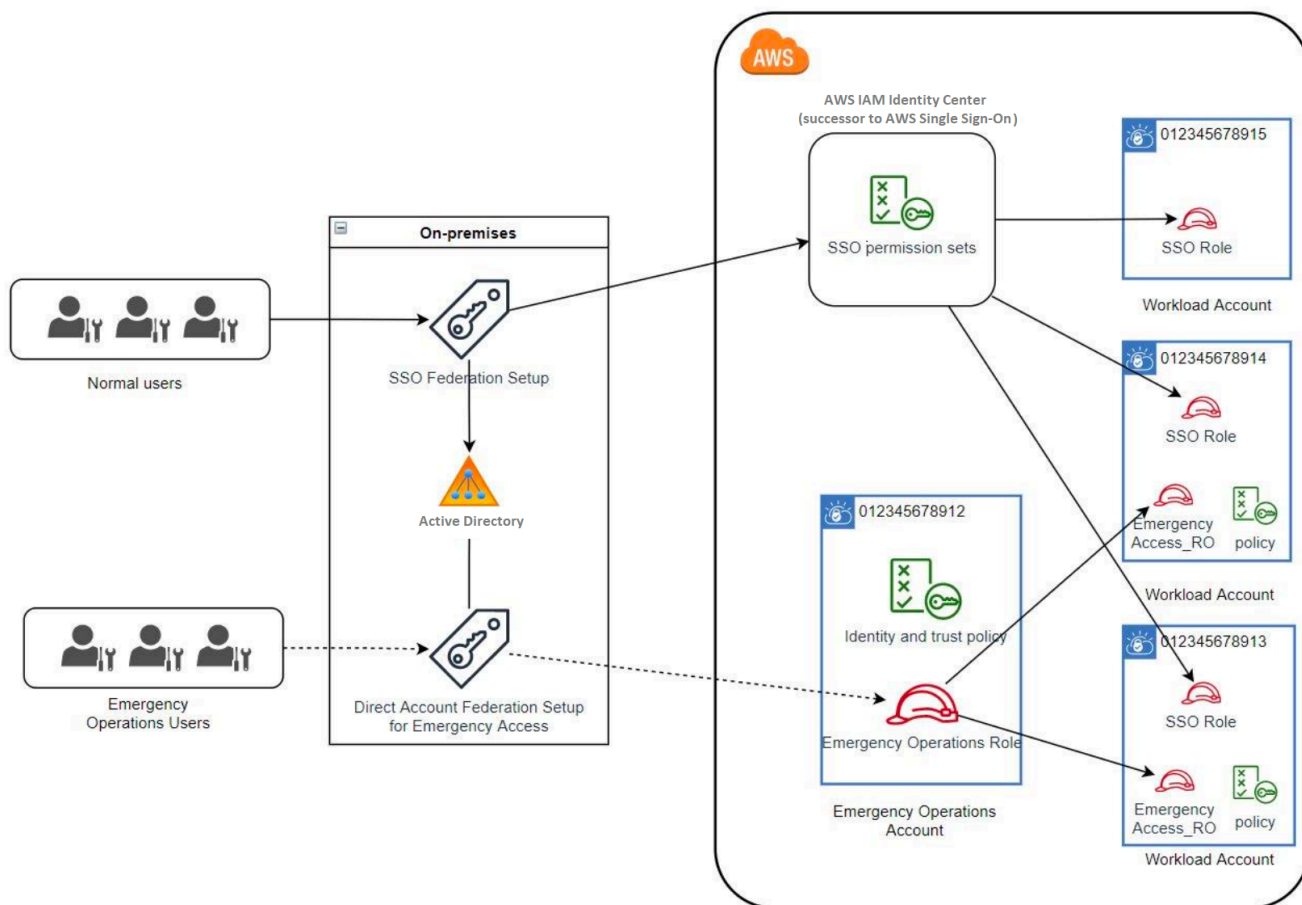
1. [Crie uma conta de operações de emergência em sua organização em AWS Organizations](#). Essa conta se tornará sua conta de operações emergenciais.
2. Conecte seu IdP à conta de operações de emergência usando a [federação baseada em SAML 2.0](#).
3. Na conta de operações de emergência, [crie uma função 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 Console de gerenciamento da AWS](#).

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 e assumir a Console de gerenciamento da AWS função 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

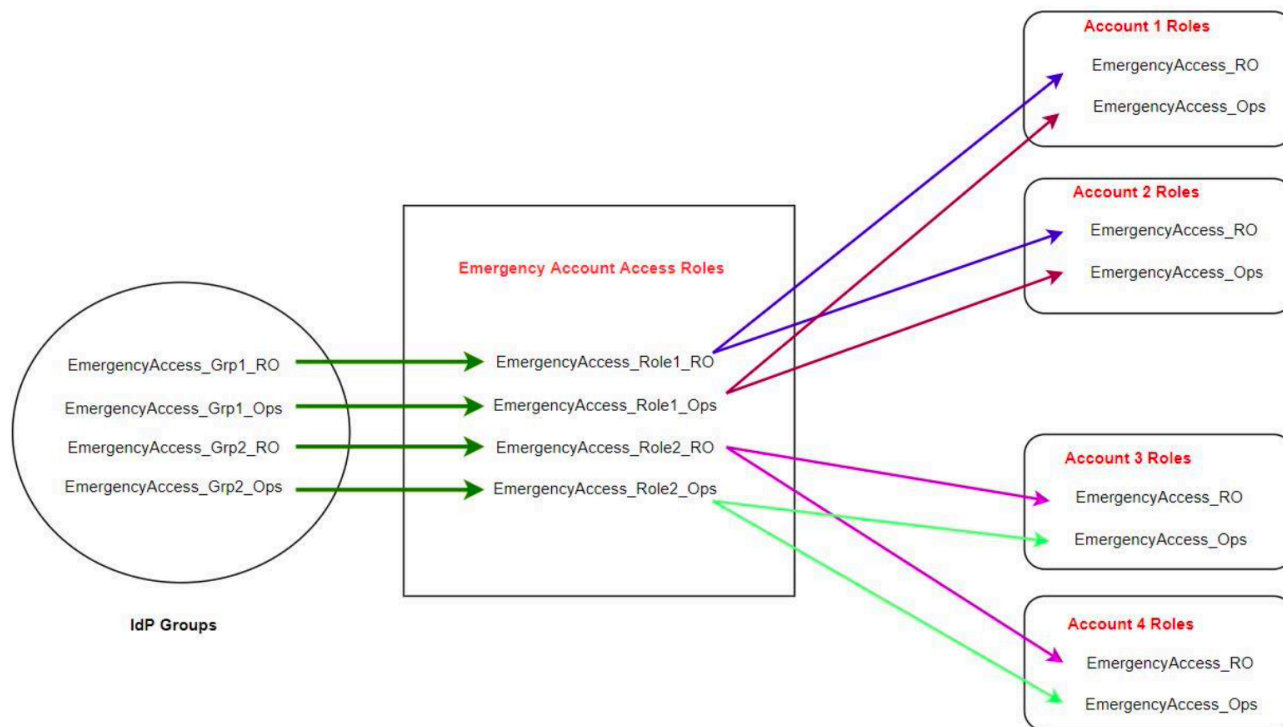
Antes de configurar o acesso de emergência, crie um plano de como o modelo de acesso funcionará. Para criar esse plano, siga este processo.

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 gerenciadas por AWS](#) ou [políticas gerenciadas pelo cliente](#).

Conta	Perfis a serem 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 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_R0 perfil confia no EmergencyAccess_Role1_R0 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. Se você estiver usando o Okta ou outro externo IdPs como fonte de identidade, consulte [Configuração única de um aplicativo de federação direta do IAM no Okta](#). Se você estiver usando o Active Directory como sua fonte de identidade, consulte [Configuração única de um aplicativo de federação direta do IAM com ADFS](#).
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 AWS Management Console, 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 o perfil de conta de emergência.

Retorno às operações normais

Verifique o [AWS Health Dashboard](#) para 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 AWS acesso 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 [Como configurar o SAML 2.0 para federação de AWS contas](#). Para lidar com cenários de falha regional, ao configurar o

endpoint de login, recomendamos que você habilite o endpoint não regional e vários endpoints regionais para todas as regiões em que você opera para melhorar a resiliência da federação. Ao configurar o URL do ACS para esse acesso de emergência, recomendamos que você use o endpoint regional de uma região diferente daquela em que seu IAM Identity Center está implantado. Consulte os [endpoints de login na](#) Referência AWS geral para obter a lista de endpoints regionais.

- 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.

Group Filter	<code>^aws\#\S+\#(?{{role}}[\w\-\+])\#(?{{accountid}}\d+)\\$</code>
Role Value Pattern	<code>arn:aws:iam::\${accountid}:saml-provider/Okta,arn:aws:iam::\${accountid}:role/\${role}</code>

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 a `EmergencyAccess_Role1_R0` função (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`.

- 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.
- 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](#). Substitua o exemplo de ARN do provedor SAML pelo correto que você criou na conta de acesso de emergência. Substitua os endpoints regionais no exemplo pelas regiões de sua escolha.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::123456789012:saml-provider/[SAML PROVIDER NAME]"
      },
      "Action": [
        "sts:AssumeRoleWithSAML",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "SAML:aud": [
            "https://signin.aws.amazon.com/saml",
            "https://us-west-2.signin.aws.amazon.com/saml",
            "https://us-west-1.signin.aws.amazon.com/saml",
            "https://us-east-2.signin.aws.amazon.com/saml"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::123456789012:saml-provider/Okta"
      },
      "Action": "sts:SetSourceIdentity"
    }
  ]
}
```

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](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
        "arn:aws:iam::111122223333:role/EmergencyAccess_R0",
        "arn:aws:iam::444455556666:role/EmergencyAccess_R0"
      ]
    }
  ]
}
```

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_R0. 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](#).

JSON

```
{
  "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.

Configuração única de um aplicativo de federação direta do IAM com ADFS

Este guia descreve o processo de configuração único para configurar a federação direta do IAM ADFS para permitir o acesso de emergência Contas da AWS quando o IAM Identity Center não estiver disponível.

Pré-requisitos

Se você planeja configurar ADFS com o Microsoft AD AWS gerenciado, recomendamos que primeiro [configure a replicação multirregional](#) e continue com as etapas a seguir na região adicional e não na região primária para fins de resiliência.

Planeje sua convenção de nomenclatura de grupos do Active Directory

Crie grupos do AD usando um padrão de nomenclatura específico que permite a correspondência automática entre nomes de grupos e funções AWS do IAM.

Formato de nomenclatura do grupo: AWS-<AccountNumber>-<RoleName>

Para ver uma ilustração, consulte a conta de emergência no diagrama em [Como criar um mapeamento emergencial de funções, contas e grupos](#). Quando um usuário é atribuído a esse grupo, ele recebe acesso à EmergencyAccess_Role1_R0 função na conta123456789012. Se um usuário estiver associado a vários grupos, ele verá uma lista das funções disponíveis Conta da AWS e poderá escolher qual função assumir.

AWS configuração

A configuração completa inclui configurações em uma conta de acesso de emergência e nas contas de carga de trabalho. Para obter uma ilustração da configuração geral, consulte [Como criar um mapeamento emergencial de funções, contas e grupos](#).

1. [Crie um provedor de identidade SAML](#)
2. [Crie funções de acesso de emergência](#)
3. [Configurar funções da conta de carga de trabalho](#)

Crie um provedor de identidade SAML

Na conta de acesso de emergência, crie um provedor de identidade SAML no IAM seguindo as etapas em [Criar um provedor de identidade SAML no IAM](#). Baixe os metadados necessários do seu ADFS servidor:

```
https://<yourADFSserverFQDN>/FederationMetadata/2007-06/  
FederationMetadata.xml
```

Crie funções de acesso de emergência

[Crie funções de acesso de emergência](#) na conta de emergência usando o SAML 2.0 Federation como o tipo de entidade confiável. Selecione o provedor SAML 2.0 que você criou na etapa anterior.

Considerações:

- Inclua todas as regiões em que você opera — selecione todas as regiões nas quais você tem cargas de trabalho ativas para garantir que a federação permaneça disponível durante uma interrupção regional.
- Configure pelo menos um endpoint regional adicional, mesmo se você operar em uma única região — por exemplo, se você opera somente em us-east-1, adicione us-west-2 como endpoint secundário. Você pode transferir seu IdP para o endpoint de login do us-west-2 SAML e ainda acessar seus us-east-1 recursos, mesmo sem nenhuma carga de trabalho. us-west-2
- Habilite o endpoint não regional e os endpoints regionais — Embora o endpoint não regional (<https://signin.aws.amazon.com/saml>) esteja altamente disponível, ele é hospedado em um único endpoint Região da AWS us-east-1, enquanto os endpoints regionais (<https://<region>.signin.aws.amazon.com/saml>) melhoram a resiliência reduzindo a dependência de um único endpoint global.

Configurar política de confiança

Consulte [Configuração única de um aplicativo de federação direta do IAM no Okta](#) para obter um exemplo de política de confiança com vários endpoints regionais de login. Substitua o exemplo de endpoints regionais e o provedor de SAML pelos seus ARNs .

Configurar políticas de permissões

Consulte [Configuração única de um aplicativo de federação direta do IAM no Okta](#) para obter um exemplo de política de permissões que você anexa às funções de acesso de emergência.

Configurar funções da conta de carga de trabalho

Para as funções da conta de carga de trabalho, configure uma política de confiança personalizada que permita que as funções de acesso de emergência na conta de acesso de emergência as assumam. Consulte [Configuração única de um aplicativo de federação direta do IAM no Okta](#) para obter um exemplo de política de confiança, em que a conta 123456789012 é a conta de acesso de emergência.

Configuração do Active Directory

As etapas a seguir descrevem como configurar o Active Directory e ADFS o acesso de emergência.

1. [Crie grupos](#)
2. [Crie um grupo confiável](#)
3. [Crie regras de reivindicação](#)

Crie grupos

Crie grupos de emergência no Active Directory de acordo com a convenção de nomenclatura descrita anteriormente (por exemplo, AWS-123456789012-EmergencyAccess_Role1_R0). Atribua usuários a esses grupos por meio de seus mecanismos de provisionamento existentes.

Crie um grupo confiável

ADFSa federação requer uma configuração de parte confiável. A parte confiável é AWS Security Token Service (AWS STS), que terceiriza a autenticação ADFS como provedor de identidade.

1. No console ADFS de gerenciamento, use o menu Ação e selecione Adicionar confiança de parte confiável. Selecione Reivindicações sensíveis ao adicionar uma parte confiável.
2. Para metadados de federação, insira a URL de metadados das informações de metadados do provedor de identidade no console do IAM. Por exemplo:

```
https://signin.aws.amazon.com/static/saml/SAMLSPXXXXXX/saml-metadata.xml
```

3. Defina o nome de exibição da parte confiável (por exemplo, Acesso àAWS conta) e escolha Avançar.
4. Selecione quem você deseja permitir o acesso AWS. Você pode selecionar grupos específicos e definir requisitos como o MFA.
5. Escolha Fechar na página Concluir para concluir o Assistente para Adicionar Parte Confiável. AWS agora está configurado como uma parte confiável.

Crie regras de reivindicação

ADFSusa a linguagem de regras de reivindicações para emitir e transformar reivindicações entre fornecedores de sinistros e partes confiáveis. Você precisa criar quatro regras de reivindicação:NameId,RoleSessionName, Obter grupos do AD e Funções para AWS acesso.

Clique com o botão direito do mouse na parte confiável e escolha Editar política de emissão de reivindicações. Escolha Adicionar regra para adicionar regras.

1NameId.

- a. Selecione Transformar uma reclamação recebida e escolha Avançar.
- b. Use as seguintes configurações:
 - Nome da regra de reivindicação: NameId
 - Tipo de reclamação recebida: Windows Account Name
 - Tipo de reclamação de saída: Name ID
 - Formato de ID de nome de saída: Persistent Identifier
 - Passe por todos os valores da reclamação: verificado
- c. Escolha OK.

2. RoleSessionName

- a. Escolha Add Rule.
- b. Na lista de modelos de regras de declaração, selecione Enviar atributos LDAP como declarações.
- c. Use as seguintes configurações:
 - Nome da regra de reivindicação: RoleSessionName
 - Armazenamento de atributos: Active Directory
 - Atributo LDAP: E-Mail-Addresses

- Tipo de reclamação de saída: `https://aws.amazon.com/SAML/Attributes/RoleSessionName`

d. Escolha OK.

3. Obtenha grupos do AD

a. Escolha Add Rule.

b. Na lista de modelos de regras de reivindicação, selecione Enviar reivindicações usando uma regra personalizada e escolha Avançar.

c. Em Nome da regra de reivindicaçãoGet AD Groups, insira e, em Regra personalizada, insira o seguinte:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> add(store = "Active Directory", types = ("http://temp/variable"), query =
";tokenGroups;{0}", param = c.Value);
```

Essa regra personalizada usa um script na linguagem da regra de declaração que recupera todos os grupos dos quais o usuário autenticado é membro e os coloca em uma declaração temporária chamada. `http://temp/variable`

Note

Certifique-se de que não haja espaços em branco no final para evitar resultados inesperados.

4. Atributos da função

a. Escolha Add Rule.

b. Na lista de modelos de regras de reivindicação, selecione Enviar reivindicações usando uma regra personalizada e escolha Avançar.

c. Em Nome da regra de reivindicaçãoRoles, insira e, em Regra personalizada, insira o seguinte:

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([\d]{12})"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =  
  RegExReplace(c.Value, "AWS-([\d]{12})-", "arn:aws:iam::$1:saml-provider/  
<ADFS>,arn:aws:iam::$1:role/"));
```

Essa regra personalizada usa expressões regulares para transformar cada uma das associações de grupo do formulário na função do IAM ARN e AWS-
<Account Number>-<Role Name> no formulário ARN do provedor de federação do IAM que espera. AWS

Note

No exemplo de linguagem de regras acima, ADFS representa o nome lógico dado ao provedor de identidade SAML na configuração do provedor de AWS identidade. Altere isso com base no nome lógico que você escolheu no console do IAM para seu provedor de identidade.

Testar a configuração

Teste se a solução funciona autenticando em `https://<yourADFSserverFQDN>/adfs/ls/IdpInitiatedSignOn.aspx`. Selecione o nome da parte confiável que você criou na lista suspensão dos sites.

Atualize o endpoint de asserção SAML padrão em ADFS

Important

Ao configurar a confiança de uma parte confiável ADFS, o endpoint SAML Assertion assume como padrão o `https://signin.aws.amazon.com/` qual não é um endpoint global e está localizado em `us-east-1`. Recomendamos que você modifique o endpoint padrão para um endpoint regional diferente de onde seu IAM Identity Center está configurado para resiliência. Por exemplo, se seu IAM Identity Center estiver implantado `us-east-1` e você também operar `us-west-2`, altere o endpoint de consumidor padrão do SAML Assertion para `https://us-west-2.signin.aws.amazon.com/saml`.

1. Escolha Propriedades na confiança da parte confiável e vá para a guia Monitoramento. Desmarque a caixa de seleção Atualizar automaticamente parte confiável.
2. Vá até a guia Endpoints, selecione seu endpoint de login preferido e escolha Editar.

3. Marque a caixa de seleção Definir o URL confiável como padrão. Escolha OK e Aplicar para que a configuração tenha efeito.

 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 Centro de Identidade do AWS IAM

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 [programas de conformidade da AWS](#). Para saber mais sobre os programas de conformidade aplicáveis Centro de Identidade do AWS IAM, 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](#)
- [Console do IAM Identity Center e autorização de API](#)
- [AWS STS chaves de contexto de condição para o IAM Identity Center](#)
- [Registro e monitoramento no IAM Identity Center](#)
- [Validação de conformidade do IAM Identity Center](#)
- [Resiliência no IAM Identity Center](#)
- [Segurança da infraestrutura no IAM Identity Center](#)

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 obter 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 obter 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 as solicitações, mas, a menos que tenha permissões, não poderá criar ou acessar o IAM Identity Center. Por exemplo, você deve ter permissões para criar um diretório conectado do IAM Identity Center.

Note

Se a instância do IAM Identity Center estiver configurada com uma chave KMS gerenciada pelo cliente, os administradores do IAM Identity Center e outros atores que precisam acessar

a chave KMS precisarão de permissões adicionais. Consulte [Implementando chaves KMS gerenciadas pelo cliente em Centro de Identidade do AWS IAM](#).

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](#)
- [Exemplo de política baseada em recursos 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 uma 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](#)
- [Gerenciar acesso aos recursos da](#)
- [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 do 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.

Gerenciar acesso aos recursos da

Uma política de permissões descreve quem tem acesso a quê. A seção a seguir explica as opções disponíveis para a criação de políticas de permissões.

Note

Esta seção discute o uso do IAM no contexto 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 recursos](#)

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.

JSON

```
{
  "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 recursos

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 Amazon Resource Name (ARN – Nome do recurso da Amazon) 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 obter 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 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, and/or grupos e 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](#)
- [Exemplo 2: permitir que um usuário gerencie permissões Contas da AWS no IAM Identity Center](#)
- [Exemplo 3: permitir que um usuário gerencie aplicativos no IAM Identity Center](#)
- [Exemplo 4: permitir que um usuário gerencie usuários e grupos no seu diretório do Identity Center](#)

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.

JSON

```
{
  "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:ListDelegatedAdministrators",
        "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.

JSON

```
{
  "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": "AccessToSSOProvisionedRoles" 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, consulte [Exemplo 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.

JSON

```
{
  "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.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:ListGroupForUser",
        "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 foi criada uma política do IAM que seja mais restritiva que as permissões mínimas exigidas, 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.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribeAccountAssignmentDeletionStatus",
        "sso:DescribePermissionSet",
        "sso:DescribePermissionSetProvisioningStatus",
        "sso:DescribeRegisteredRegions",
        "sso:GetApplicationInstance",
        "sso:GetApplicationTemplate",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetMfaDeviceManagementForDirectory",
        "sso:GetPermissionSet",
        "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": "*"
}
]
}

```

Exemplo de política baseada em recursos para o IAM Identity Center

Todo aplicativo que funciona com o IAM Identity Center e usa [OAuth 2.0](#) exige uma política baseada em recursos. O aplicativo pode ser gerenciado ou AWS gerenciado pelo cliente. A política baseada em recursos necessária, chamada de política de aplicativo (ou [ActorPolicy](#) na APIs), define quais [diretores do IAM](#) estão autorizados a chamar ações de API do método de autenticação do IAM, como. [CreateTokenWithIAM](#) O método de autenticação do IAM permite que um principal do IAM,

como uma função ou um AWS serviço do IAM, se autentique no serviço OIDC do IAM Identity Center apresentando as credenciais do IAM para solicitar ou gerenciar tokens de acesso no `/token?` ponto final `aws_iam=t`.

A política de aplicação rege as operações de emissão de tokens (`CreateTokenWithIAM`). A política também rege ações somente de permissão que são usadas somente por aplicativos AWS gerenciados para validar tokens (`IntrospectTokenWithIAM`) e revogar tokens (`RevokeTokenWithIAM`). Para uma aplicação gerenciada pelo cliente, você configura essa política especificando quais entidades principais do IAM estão autorizadas a chamar `CreateTokenWithIAM`. Quando uma entidade principal autorizada chama essa ação de API, ela recebe tokens de acesso e atualização para a aplicação.

Se você estiver usando o console do IAM Identity Center para configurar um aplicativo gerenciado pelo cliente para [propagação confiável de identidade](#), consulte a Etapa 4 em [Configurar aplicativos OAuth 2.0 gerenciados pelo cliente](#) para obter informações sobre como configurar a política do aplicativo. Para obter um exemplo de política, consulte [Exemplo de política: permitir que um perfil do IAM crie tokens de acesso e atualização](#) mais adiante neste tópico.

Requisitos de política

A política deve atender aos seguintes requisitos:

- A política deve incluir um elemento `Version` definido como "2012-10-17".
- A política deve incluir pelo menos um elemento `Statement`.
- Cada política `Statement` deve incluir os seguintes elementos: `Effect`, `Principal`, `Action` e `Resource`.

Elementos da política

A política deve incluir os seguintes elementos:

Versão

Especifica a versão do documento de política. Define a versão como 2012-10-17 (a versão mais recente).

Declaração

Contém a política `Statements`. A política deve conter pelo menos um `Statement`.

Cada política `Statement` consiste nos seguintes elementos:

Efeito

(Obrigatório) Determina se as permissões devem ser permitidas ou negadas na instrução de política. Os valores válidos são Allow ou Deny.

Entidade principal

(Obrigatório) A [entidade principal](#) é a identidade que recebe a especificação de permissões na instrução de política. Você pode especificar perfis do IAM ou entidades principais do serviço AWS.

Ação

(Exigido) As operações de API do serviço IAM Identity Center OIDC para permitir ou negar. As ações válidas incluem:

- `sso-oauth:CreateTokenWithIAM`: essa ação, que corresponde à operação da [CreateTokenWithIAM](#) API, concede permissão para criar e retornar tokens de acesso e atualização para aplicativos clientes autorizados que são autenticados usando qualquer entidade do IAM, como uma função de AWS serviço ou usuário. Esses tokens podem conter escopos definidos que especificam permissões como `read:profile` ou `write:data`.
- `sso-oauth:IntrospectTokenWithIAM` [somente permissão]: concede permissão para validar e recuperar informações sobre tokens de acesso OAuth 2.0 ativos e tokens de atualização, incluindo seus escopos e permissões associados. Essa permissão é usada somente por aplicativos AWS gerenciados e não está documentada na Referência da API OIDC do IAM Identity Center.
- `RevokeTokenWithIAM` [somente permissão]: concede permissão para revogar tokens de acesso OAuth 2.0 e atualizar tokens, invalidando-os antes da expiração normal. Essa permissão é usada somente por aplicativos AWS gerenciados e não está documentada na Referência da API OIDC do IAM Identity Center.

Recurso

(Exigido) Nessa política, o valor do elemento Resource é "*", que significa "esta aplicação".

Para obter mais informações sobre a sintaxe da AWS política, consulte [Referência de política AWS do IAM](#) no Guia do usuário do IAM.

Exemplo de política: permitir que um perfil do IAM crie tokens de acesso e atualização

A política de permissões a seguir concede permissões ao `ExampleAppClientRole`, um perfil do IAM assumido por um workload para criar e retornar tokens de acesso e atualização.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRoleToCreateTokens",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleAppClientRole"
      },
      "Action": "sso-oauth:CreateTokenWithIAM",
      "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 Guia do usuário do IAM.

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 recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso 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 Centro de Identidade do AWS IAM 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` às suas identidades do IAM. Ao anexar a `AWSSSOMasterAccountAdministrator` política a uma identidade, você concede Centro de Identidade do AWS IAM 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.

Essa política também inclui AWS Key Management Service as permissões necessárias para instâncias do IAM Identity Center que usam chaves gerenciadas pelo cliente para criptografia.

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 obter mais informações, consulte [Configurar o acesso a Contas da AWS](#).

- **AWSSSOMemberAccountAdministrator**— Permite que o IAM Identity Center execute ações do administrador da conta em um AWS ambiente com várias contas. Para obter mais informações, consulte [AWS política gerenciada: AWSSSOMember AccountAdministrator](#).
- **AWSSSOManageDelegatedAdministrator**— Permite que o IAM Identity Center registre e cancele o registro de um administrador delegado para sua organização.
- **AllowKMSKeyUseViaService** e **AllowKMSKeyDiscovery** — Permite AWS Key Management Service operações para chaves gerenciadas pelo cliente usadas pelas instâncias do IAM Identity Center.

Para ver as permissões dessa política, consulte [AWSSSOMasterAccountAdministrator](#) em 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 exigidas são `iam:CreateServiceLinkedRole` e `iam:PassRole`.

AWS política gerenciada: AWSSSOMember AccountAdministrator

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** às suas identidades do IAM. Ao anexar a **AWSSSOMemberAccountAdministrator** política a uma identidade, você concede Centro de Identidade do AWS IAM 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.

Essa política também inclui AWS Key Management Service as permissões necessárias para instâncias do IAM Identity Center que usam chaves gerenciadas pelo cliente para criptografia.

Para ver as permissões dessa política, consulte [AWSSSOMemberAccountAdministrator](#) em 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 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 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, consulte [Administradores 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: AWSSSODirectory Administrator

É possível anexar a política AWSSSODirectoryAdministrator às 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. Essa política também inclui AWS Key Management Service as permissões necessárias para instâncias do IAM Identity Center que usam chaves gerenciadas pelo cliente para criptografia.

Esta política inclui as seguintes permissões:

- Diretório do IAM Identity Center — Acesso administrativo completo às operações do diretório do IAM Identity Center.
- Identity Store — Acesso administrativo total às operações e autenticação do repositório de identidades.
- IAM Identity Center — Permissão para listar associações de diretórios.
- AWS Key Management Service — Permissões para descriptografar, descrever chaves e gerar chaves de dados para chaves gerenciadas pelo cliente usadas pelas instâncias do IAM Identity Center.

Para ver as permissões dessa política, consulte [AWSSSODirectoryAdministrador](#) na Referência de Política AWS Gerenciada.

AWS política gerenciada: AWSSSORRead somente

É possível anexar a política AWSSSORReadOnly às 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.

Essa política também inclui AWS Key Management Service as permissões necessárias para instâncias do IAM Identity Center que usam chaves gerenciadas pelo cliente para criptografia.

Para ver as permissões dessa política, consulte [AWSSSORReadSomente](#) na Referência de política AWS gerenciada.

AWS política gerenciada: AWSSSODirectoryReadOnly

É possível anexar a política `AWSSSODirectoryReadOnly` às 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, entidades principais com essas permissões podem visualizar os usuários do IAM Identity Center, mas não podem alterar nenhum atributo do usuário nem atribuir dispositivos de MFA.

Essa política também inclui AWS Key Management Service as permissões necessárias para instâncias do IAM Identity Center que usam chaves gerenciadas pelo cliente para criptografia.

Para ver as permissões dessa política, consulte [AWSSSODirectoryReadOnly](#) em Referência de política AWS gerenciada.

AWS política gerenciada: AWSIdentitySyncFullAccess

É possível anexar a política `AWSIdentitySyncFullAccess` às 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 [AWSIdentitySyncFullAccess](#) em Referência de política AWS gerenciada.

AWS política gerenciada: AWSIdentitySyncReadOnlyAccess

É possível anexar a política `AWSIdentitySyncReadOnlyAccess` às 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 [AWSIdentitySyncReadOnlyAccess](#) em Referência de política AWS gerenciada.

AWS política gerenciada: AWSSSOService RolePolicy

Você não pode anexar a política AWSSSOServiceRolePolicy às 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 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 Identity 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 obter mais informações, consulte [As funções vinculadas ao serviço do IAM Identity Center permanecem..](#)

AWS política gerenciada: AWSIAMIdentity CenterAllowListForIdentityContext

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 [AWSIAMIdentityCenterAllowListForIdentityContext](#) em Referência de política AWS gerenciada.

AWS política gerenciada: AWSIdentity CenterExternalManagementPolicy

É possível anexar a política AWSIdentityCenterExternalManagementPolicy às suas identidades do IAM.

Essa política fornece acesso para gerenciar usuários do IAM Identity Center a partir de um provedor externo.

Para ver as permissões dessa política, consulte [AWSIdentityCenterExternalManagementPolicy](#) em 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
AWSIdentityCenterExternalManagementPolicy	Política gerenciada atualizada para alterar o ARN do inquilino de provisionamento.	5 de dezembro de 2025
AWSIdentityCenterExternalManagementPolicy	Essa política fornece acesso para gerenciar usuários do IAM Identity Center a partir de um provedor externo.	21 de novembro de 2025
AWSSSOMasterAccountAdministrator , AWSSSOMemberAccountAdministrator , AWSSSOReadSomente , AWSSSODirectoryAdministrator , AWSSSODirectoryReadOnly	Políticas gerenciadas atualizadas para incluir AWS KMS as permissões necessárias para instâncias do IAM Identity Center que usam chaves gerenciadas pelo cliente para criptografia.	17 de setembro de 2025
AWSSSOServiceRolePolicy	Essa política agora inclui novas permissões para chamar <code>identity-sync:DeleteSyncProfile</code> .	11 de fevereiro de 2025
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora inclui as <code>qapps:ExportQAppSessionData</code> ações <code>qapps:ListQAppSessionData</code> e para oferecer suporte a sessões de console	2 de outubro de 2024

Alteração	Descrição	Data
	com identidade aprimorada para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	
AWSSSOMasterAccountAdministrator	O IAM Identity Center adicionou uma nova ação para conceder DeleteSyncProfile permissões para permitir que você use essa política para excluir perfis de sincronização. Essa ação está associada à DeleteInstance API.	26 de setembro de 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora inclui a s3:ListCallerAccessGrants ação para oferecer suporte a sessões de console com identidade aprimorada para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	4 de setembro de 2024

Alteração	Descrição	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora incluía <code>oss:APIAccessAll</code> , <code>es:ESHttpHead</code> <code>es:ESHttpPost</code> <code>es:ESHttpGet</code> <code>es:ESHttpPatch</code> <code>es:ESHttpDelete</code> , e <code>es:ESHttpPut</code> ações para oferecer suporte a sessões de console com identidade aprimorada para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	12 de julho de 2024

Alteração	Descrição	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora inclui <code>qapps:PredictQApp</code> , <code>qapps:ImportDocument</code> , <code>qapps:AssociateLibraryItemReview</code> , <code>qapps:DissociateLibraryItemReview</code> , <code>qapps:GetQAppSession</code> , <code>qapps:UpdateQAppSession</code> , <code>qapps:GetQAppSessionMetadata</code> , <code>qapps:UpdateQAppSessionMetadata</code> , e <code>qapps:TagResource</code> ações para oferecer suporte a sessões de console com identidade aprimorada para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	27 de junho de 2024

Alteração	Descrição	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora inclui as ações <code>elasticmapreduce:AddJobFlowSteps</code> , <code>elasticmapreduce:DescribeCluster</code> , <code>elasticmapreduce:CancelSteps</code> , <code>elasticmapreduce:DescribeStep</code> e <code>elasticmapreduce:ListSteps</code> para ser compatível com a propagação de identidades confiável no Amazon EMR.	17 de maio de 2024

Alteração	Descrição	Data
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	Essa política agora inclui <code>qapps:CreateQApp</code> , <code>qapps:PredictProblemStatementFromConversation</code> , <code>qapps:PredictQAppFromProblemStatement</code> , <code>qapps:CopyQApp</code> , <code>qapps:GetQApp</code> , <code>qapps:ListQApps</code> , <code>qapps:UpdateQApp</code> , <code>qapps:DeleteQApp</code> , <code>qapps:AssociateQAppWithUser</code> , <code>qapps:DisassociateQAppFromUser</code> , <code>qapps:ImportDocumentToQAppSession</code> , <code>qapps>CreateLibraryItem</code> , <code>qapps:GetLibraryItem</code> , <code>qapps:UpdateLibraryItem</code> , <code>qapps>CreateLibraryItemReview</code> , <code>qapps:ListLibraryItems</code> , <code>qapps>CreateSubscriptionToken</code> , <code>qapps:StartQAppSession</code> , e <code>qapps:StopQAppSession</code> ações para oferecer suporte a sessões de console com identidade	30 de abril de 2024

Alteração	Descrição	Data
	e aprimorada para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	
AWSSSOMasterAccountAdministrator	Essa política agora inclui as <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> ações <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> e para oferecer suporte a sessões de console com identidade e aprimorada para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	26 de abril de 2024
AWSSSOMemberAccountAdministrator	Essa política agora inclui as <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> ações <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> e para oferecer suporte a sessões de console com identidade e aprimorada para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	26 de abril de 2024

Alteração	Descrição	Data
AWSSSOReadSomente	Essa política agora inclui a <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> ação para oferecer suporte a sessões de console com identidade aprimorada para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	26 de abril de 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora inclui a <code>qbusiness:PutFeedback</code> ação para oferecer suporte a sessões de console com identidade aprimorada para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	26 de abril de 2024

Alteração	Descrição	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora inclui <code>StartConversation</code> , <code>SendMessage</code> , <code>ListConversations</code> , <code>GetConversation</code> , <code>StartTroubleshootingAnalysis</code> , <code>GetTroubleshootingResults</code> , <code>StartTroubleshootingResolutionExplanation</code> , e <code>UpdateTroubleshootingCommandResult</code> ações para oferecer suporte a sessões de console com identidade aprimorada para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	24 de abril de 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora inclui a <code>sts:SetContext</code> ação para oferecer suporte a sessões de console com identidade aprimorada para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	19 de abril de 2024

Alteração	Descrição	Data
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política agora inclui as <code>qbusiness:DeleteConversation</code> ações <code>qbusiness:Chat</code> , <code>qbusiness:ChatSync</code> <code>qbusiness:ListConversations</code> <code>qbusiness:ListMessages</code> , e para oferecer suporte a sessões de console com identidade e aprimorada para aplicativos AWS gerenciados que oferecem suporte a essas sessões.	11 de abril de 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Essa política também inclui as ações <code>s3:GetAccessGrantsInstanceForPrefix</code> e <code>s3:GetDataAccess</code> .	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 <code>identitystore-auth</code> 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 <code>identitystore-auth</code> 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 <code>identitystore-auth</code> 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 <code>identitystore-auth</code> com novas permissões para permitir que os usuários listem e obtenham sessões.	20 de outubro de 2022

Alteração	Descrição	Data
<u>AWSSSOMasterAccountAdministrator</u>	Essa política agora inclui novas permissões para fazer chamadas <u>ListDelegatedAdministrators</u> _ AWS Organizations. Essa política agora também inclui um subconjunto de permissões <u>AWSSSOManageDelegatedAdministrator</u> que inclui permissões para chamar <u>RegisterDelegatedAdministrator</u> e <u>DeregisterDelegatedAdministrator</u> .	16 de agosto de 2022
<u>AWSSSOMemberAccountAdministrator</u>	Essa política agora inclui novas permissões para fazer chamadas <u>ListDelegatedAdministrators</u> _ AWS Organizations. Essa política agora também inclui um subconjunto de permissões <u>AWSSSOManageDelegatedAdministrator</u> que inclui permissões para chamar <u>RegisterDelegatedAdministrator</u> e <u>DeregisterDelegatedAdministrator</u> .	16 de agosto de 2022
<u>AWSSSORReadSomente</u>	Essa política agora inclui novas permissões para fazer chamadas <u>ListDelegatedAdministrators</u> AWS Organizations.	11 de agosto de 2022

Alteração	Descrição	Data
AWSSSOServiceRolePolicy	Essa política agora inclui novas permissões para chamar DeleteRolePermissionsBoundary e PutRolePermissionsBoundary .	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 AWSSSORReadSomente	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
<u>AWSSSOMemberAccountAdministrator</u>	Essa política agora permite todas as ações do serviço IAM Identity Center Identity Store.	29 de março de 2022
<u>AWSSSODirectoryAdministrator</u>	Essa política agora permite todas as ações do serviço IAM Identity Center Identity Store.	29 de março de 2022
<u>AWSSSODirectoryReadOnly</u>	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
<u>AWSIdentitySyncFullAccess</u>	Esta política permite acesso total às permissões de sincronização de identidade.	3 de março de 2022
<u>AWSIdentitySyncReadOnlyAccess</u>	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
<u>AWSSSORReadSomente</u>	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.

Centro de Identidade do AWS IAM 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 obter mais informações, consulte [Compreender os perfis vinculados ao serviço do IAM Identity Center](#).

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 [Produtos da AWS compatíveis com o IAM](#) e procure por serviços que apresentam Sim na coluna Funções vinculadas ao serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

As funções vinculadas ao serviço do IAM Identity Center permanecem.

O IAM Identity Center usa a função vinculada ao serviço chamada `AWSServiceRoleForSSO` para conceder permissões ao IAM Identity Center para gerenciar AWS recursos, incluindo funções, políticas e SAML IdP em seu nome.

A função vinculada ao serviço `AWSServiceRoleForSSO` confia nos seguintes serviços para assumir a função:

- IAM Identity Center (prefixo de serviço: `sso`)

A política de permissões AWSSSOService RolePolicy 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 “SSO_”: AWSReserved

- 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 AWSSSOService RolePolicy 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 AWSSSOService RolePolicy 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 AWSSSOService RolePolicy 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 AWSSSOService RolePolicy de função vinculada ao serviço permite que o IAM Identity Center conclua o seguinte em “arn:aws:iam: *:”: role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO

- iam:GetServiceLinkedRoleDeletionStatus
- iam>DeleteServiceLinkedRole

A política de permissões de função AWSSSOService RolePolicy vinculada ao serviço permite que o IAM Identity Center conclua o seguinte em “arn:aws:identity-sync: *:*:profile/*”:

- identity-sync>DeleteSyncProfile

Para obter mais informações sobre atualizações na política de permissões AWSSSOService RolePolicy de funções vinculadas ao serviço, consulte [Atualizações do IAM Identity Center para políticas AWS gerenciadas](#)

JSON

```
{
  "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": [
        "*"
    ]
},
{

```

```
        "Sid": "AllowDeleteSyncProfile",
        "Effect": "Allow",
        "Action": [
            "identity-sync:DeleteSyncProfile"
        ],
        "Resource": [
            "arn:aws:identity-sync:*:*:profile/*"
        ]
    }
}
```

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado 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

Você não precisa 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 Identity 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 logs 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 função de AWSService RoleFor SSO 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 vinculada ao serviço AWSService RoleFor SSO. 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 função AWSService RoleFor SSO. 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 AWSService RoleFor SSO

1. [Remover o acesso de usuários e grupos a um Conta da AWS](#) para todos os usuários e grupos que têm acesso a Conta da AWS.

2. [Remover conjuntos de permissões no IAM Identity Center](#) que você associou a Conta da AWS.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM, a CLI do IAM ou a API do IAM para excluir a função vinculada ao serviço AWSService RoleFor SSO. Para obter mais informações, consulte [Deleting a Service-Linked Role](#) no IAM User Guide.

Console do IAM Identity Center e autorização de API

O console existente do IAM Identity Center APIs oferece suporte à autorização dupla, o que permite que você mantenha o uso das operações de API existentes quando as mais 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

Nome da operação do console em uso antes de 15 de novembro de 2023	Ações de API usadas após 15 de novembro de 2023
DeleteApplicationInstance DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments
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

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWSAccount	DeleteApplicationInstance DeleteTrust	DeleteAccountAssignment
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances GetApplicationInstance	ListAccountsForProvisionedPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
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
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 diferentes fontes, incluindo a entidade principal que faz a solicitação, o recurso em relação ao qual a solicitação 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 são incluídas nos [perfis 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 usando o IAM Identity Center.
- Após a troca de tokens com um [emissor de tokens confiáveis](#) para propagação de identidades confiáveis. Nesse caso, a aplicação obtém um token de um emissor de tokens confiáveis e troca esse token por um token do IAM Identity Center.

Essas chaves normalmente são usadas por aplicações integradas com a propagação de identidades confiáveis. Em alguns casos, quando existem valores de chave presentes, é possível usar essas chaves nas políticas do IAM que você cria para permitir ou negar permissões.

Por exemplo, pode ser que você queira fornecer acesso condicional a um recurso com base no valor de `UserId`. Esse valor indica qual usuário do IAM Identity Center está usando o perfil. O exemplo é semelhante a usar `SourceId`. Porém, diferentemente de `SourceId`, o valor de `UserId` representa um usuário específico, verificado no 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`](#)
- [loja de identidades: `IdentityStoreArn`](#)
- [centro de identidade: `ApplicationArn`](#)
- [centro de identidade: `CredentialId`](#)
- [centro de identidade: `InstanceArn`](#)

loja de identidades: `UserId`

Essa chave de contexto é o `UserId` do usuário do IAM Identity Center que é o assunto da asserção 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` do usuário do IAM Identity Center em nome do qual 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 asserção de contexto. É também o repositório de identidades no qual você pode pesquisar atributos para o `identitystore:UserID`. Você pode usar essa chave nas políticas para determinar se o `identitystore:UserID` vem de um ARN de repositório 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 da aplicação para a qual o IAM Identity Center emitiu uma asserção de contexto. Você pode usar essa chave em políticas para determinar se o `identitycenter:ApplicationArn` vem de uma aplicação esperada. Usar essa chave pode ajudar a evitar que um perfil do IAM seja acessado por uma aplicação inesperada.

- Disponibilidade — Essa chave está incluída no contexto da solicitação de uma operação de AWS STS `AssumeRole` API. O contexto da solicitação inclui uma asserção 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 um ID aleatório para a credencial de perfil com identidade aprimorada e é usada apenas para registro em log. Como esse valor de chave é imprevisível, recomendamos que ele não seja usado para asserções 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 asserção 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 asserção de contexto para o `identitystore:UserID`. Você pode usar essa chave para determinar se o `identitystore:UserID` e a asserção de contexto vieram de um ARN de instância do IAM Identity Center esperado.

- Disponibilidade — Essa chave está incluída no contexto da solicitação de uma operação de AWS STS AssumeRole API. O contexto da solicitação inclui uma asserção de contexto emitida pelo IAM Identity Center.
- Tipo de dados: [ARN](#), [string](#)
- Tipo de valor: valor único

Registro e monitoramento no IAM Identity Center

A prática recomendada é monitorar a organização para garantir que as alterações sejam registradas em log. O monitoramento ajuda a garantir que você possa investigar qualquer alteração inesperada e reverter alterações indesejadas. Atualmente, o IAM Identity Center oferece suporte a dois AWS serviços que ajudam você a monitorar sua organização e a atividade que acontece dentro dela: AWS CloudTrail e a Amazon EventBridge.

Tópicos

- [Registro de chamadas da API do IAM Identity Center com AWS CloudTrail](#)
- [Registrando chamadas da API SCIM do IAM Identity Center com AWS CloudTrail](#)

- [Conecte os componentes do aplicativo com a Amazon EventBridge](#)
- [Como registrar em log de erros de sincronização configurável do AD](#)

Registro de chamadas da API do IAM Identity Center com AWS CloudTrail

O Centro de Identidade do AWS IAM 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](#).

A tabela a seguir resume os CloudTrail eventos do IAM Identity Center, suas fontes de CloudTrail eventos e a correspondência APIs. Consulte as [referências da API do IAM Identity Center](#) para saber mais sobre APIs o.

Note

Há um grupo adicional de CloudTrail eventos, chamado de Sign-in, que é AWS emitido para login AWS como usuário do IAM Identity Center. Esses eventos não têm público correspondente e APIs, portanto, não estão listados nas referências da API.

CloudTrail eventos	Público APIs	Description	CloudTrail fontes de eventos
Centro de Identidade do IAM	Centro de Identidade do IAM	O IAM Identity Center APIs permite o gerenciamento de conjuntos de permissões, aplicativ	sso.amazonservices.com

CloudTrail eventos	Público APIs	Description	CloudTrail fontes de eventos
		os, emissores de tokens confiáveis, atribuições de contas e aplicativos, instâncias do IAM Identity Center e tags.	
Loja de identidades	Loja de identidades	O Identity Store APIs permite o gerenciamento do ciclo de vida dos usuários e grupos de sua força de trabalho e das associações de grupos de usuários. Além disso, oferecem suporte ao gerenciamento dos dispositivos de MFA dos usuários.	sso-directory.amazonaws.com, identitystore.amazonaws.com
OIDC	OIDC	O OIDC APIs oferece suporte à propagação confiável de identidade e aos kits de ferramentas de login AWS CLI e IDE como um usuário já autenticado do IAM Identity Center.	sso.amazonaws.com, sso-oauth.amazonaws.com

CloudTrail eventos	Público APIs	Description	CloudTrail fontes de eventos
AWS portal de acesso	AWS portal de acesso	O portal de AWS acesso APIs oferece suporte às operações do portal de AWS acesso e aos usuários que obtêm as credenciais da conta por meio do AWS CLI.	sso.amazonaws.com
SCIM	SCIM	O SCIM APIs suporta o provisionamento de usuários, grupos e associações de grupos por meio do protocolo SCIM. Consulte Registramos as chamadas da API SCIM do IAM Identity Center com AWS CloudTrail para obter mais informações.	identitystore-scim.amazonaws.com
Início de Sessão da AWS	Nenhuma API pública	AWS emite CloudTrail eventos de login para autenticação de usuários e fluxos de federação no IAM Identity Center.	signin.amazonaws.com

Tópicos

- [CloudTrail casos de uso do IAM Identity Center](#)
- [Informações do IAM Identity Center em CloudTrail](#)

CloudTrail casos de uso do IAM Identity Center

Os CloudTrail eventos que o IAM Identity Center emite podem ser valiosos para uma variedade de casos de uso. As organizações podem usar esses registros de eventos para monitorar e auditar o acesso e a atividade do usuário em seu AWS ambiente. Isso pode ajudar nos casos de uso de conformidade, pois os registros capturam detalhes sobre quem está acessando quais recursos e quando. Você também pode usar os CloudTrail dados para investigações de incidentes, permitindo que as equipes analisem as ações dos usuários e rastreiem comportamentos suspeitos. Além disso, o histórico de eventos pode apoiar os esforços de solução de problemas, fornecendo visibilidade das alterações feitas nas permissões e configurações do usuário ao longo do tempo.

As seções a seguir descrevem os casos de uso fundamentais que informam os fluxos de trabalho, como auditoria, investigação de incidentes e solução de problemas.

Identificação do usuário nos eventos iniciados pelo usuário CloudTrail do IAM Identity Center

O IAM Identity Center emite dois CloudTrail campos que permitem identificar o usuário do IAM Identity Center por trás dos CloudTrail eventos, como fazer login no IAM Identity Center ou usar o portal de AWS acesso AWS CLI, incluindo o gerenciamento de dispositivos de MFA:

- **userId** — O identificador de usuário exclusivo e imutável do Identity Store de uma instância do IAM Identity Center.
- **identityStoreArn** — O nome do recurso da Amazon (ARN) do Identity Store que contém o usuário.

Os **identityStoreArn** campos **userId** e são exibidos no **onBehalfOf** elemento aninhado dentro do [userIdentity](#) elemento, conforme mostrado no exemplo de registro de CloudTrail eventos a seguir. Esse log de eventos mostra esses dois campos em um evento em que o tipo de **userIdentity** é “IdentityCenterUser”. Você também pode encontrar esses campos em eventos para usuários autenticados do IAM Identity Center em que o tipo de **userIdentity** é “Unknown”. Os fluxos de trabalho devem aceitar os dois valores de tipo.

```
"userIdentity":{
  "type":"IdentityCenterUser",
  "accountId":"111122223333",
  "onBehalfOf": {
    "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
```



```
},  
  "credentialId" : "90e292de-5eb8-446e-9602-90f7c45044f7"  
}
```

Tip

Recomendamos que você use `userId` e `identityStoreArn` identifique o usuário por trás dos CloudTrail eventos do IAM Identity Center. Os campos `userName` e `principalId` abaixo do elemento `userIdentity` não estão mais disponíveis. Se os fluxos de trabalho, como auditoria ou resposta a incidentes, dependerem do acesso ao `username`, você terá duas opções:

- Recuperar o nome de usuário do diretório do IAM Identity Center, conforme explicado em [Nome de usuário em eventos de login CloudTrail](#).
- Obter o `UserName` que o IAM Identity Center emite sob o elemento `additionalEventData` em Sign-in. Essa opção não exige acesso ao diretório do IAM Identity Center. Para obter mais informações, consulte [Nome de usuário em eventos de login CloudTrail](#).

Para recuperar os detalhes de um usuário, incluindo o campo `username`, você consulta o Identity Store com o ID do usuário e o ID do Identity Store como parâmetros. Você pode realizar essa ação por meio da solicitação [DescribeUser](#) da API ou da CLI. O comando de CLI a seguir é um exemplo. Você pode omitir o parâmetro `region` se a instância do IAM Identity Center estiver na região padrão da CLI.

```
aws identitystore describe-user \  
--identity-store-id d-1234567890 \  
--user-id 544894e8-80c1-707f-60e3-3ba6510dfac1 \  
--region your-region-id
```

Para determinar o valor do Identity Store ID para o comando CLI no exemplo anterior, você pode extrair o ID do Identity Store do valor `identityStoreArn`. No ARN de exemplo `arn:aws:identitystore::111122223333:identitystore/d-1234567890`, o ID do Identity Store é `d-1234567890`. Como alternativa, você pode localizar o ID do Identity Store navegando até a aba Identity Store na seção Configurações do console do IAM Identity Center.

Se você estiver automatizando a pesquisa de usuários no diretório do IAM Identity Center, recomendamos que você estime a frequência das pesquisas de usuários e considere o [limite do controle de utilização do IAM Identity Center na API Identity Store](#). O armazenamento em cache dos atributos recuperados do usuário pode ajudar você a permanecer dentro do limite do controle de utilização.

Como correlacionar eventos de usuário na mesma sessão de usuário

O [AuthWorkflowID](#) campo emitido em eventos de login permite rastrear todos os CloudTrail eventos associados a uma sequência de login antes do início de uma sessão de usuário do IAM Identity Center.

Para ações do usuário dentro do portal de AWS acesso, o `credentialId` valor é definido como o ID da sessão do usuário do IAM Identity Center usada para solicitar a ação. Você pode usar esse valor para identificar CloudTrail eventos iniciados na mesma sessão de usuário autenticada do IAM Identity Center no portal de AWS acesso.

 Note

Você não pode usar `credentialId` para correlacionar eventos de login aos eventos subsequentes, como o uso do portal de acesso do AWS. O valor do campo `credentialId` emitido em eventos de login tem uso interno e recomendamos que você não confie nele. O valor do campo `credentialId` emitido para [eventos do portal de acesso do AWS](#) invocados com o OIDC é igual ao ID do token de acesso.

Identificação dos detalhes da sessão em segundo plano do usuário nos eventos iniciados pelo usuário CloudTrail do IAM Identity Center

O CloudTrail evento a seguir captura o processo de troca de tokens OAuth 2.0, no qual um token de acesso existente (`objectToken`) que representa a sessão interativa do usuário é trocado por um token de atualização (`requestedTokenType`). O token de atualização permite que tarefas de longa duração iniciadas por qualquer usuário continuem sendo executadas com as permissões do usuário, mesmo após o usuário sair.

Para [sessões em segundo plano de usuários do](#) IAM Identity Center, o CloudTrail evento inclui um elemento adicional chamado `resource` no `requestParameters` elemento. O `resource` parâmetro contém o nome do recurso da Amazon (ARN) da tarefa executada em segundo plano.

Esse elemento está presente somente nos registros de CloudTrail eventos e não está incluído nas respostas da API IAM do IAM Identity Center ou [CreateTokenWithdo](#) SDK.

```
{
  "clientId": "EXAMPLE-CLIENT-ID",
  "grantType": "urn:ietf:params:oauth:grant-type:token-exchange",
  "code": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "redirectUri": "https://example.com/callback",
  "assertion": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectTokenType": "urn:ietf:params:oauth:token-type:access_token",
  "requestedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
  "resource": "arn:aws:sagemaker:us-west-2:123456789012:training-job/my-job"
}
```

Como correlacionar usuários entre o IAM Identity Center e diretórios externos

O IAM Identity Center fornece dois atributos de usuário que você pode usar para correlacionar um usuário no diretório ao mesmo usuário em um diretório externo (por exemplo, Microsoft Active Directory e Okta Universal Directory).

- **externalId** — O identificador externo de um usuário do IAM Identity Center. Recomendamos que você mapeie esse identificador para um identificador de usuário imutável no diretório externo. Observe que o IAM Identity Center não emite esse valor em CloudTrail.
- **username** — Um valor fornecido pelo cliente com o qual os usuários geralmente fazem login. O valor pode mudar (por exemplo, com uma atualização do SCIM). Observe que, quando a fonte de identidade é Directory Service, o nome de usuário que o IAM Identity Center emite CloudTrail corresponde ao nome de usuário que você digitou para autenticar. O nome de usuário não precisa corresponder exatamente ao nome de usuário no diretório do IAM Identity Center.

Se você tiver acesso aos CloudTrail eventos, mas não ao diretório do IAM Identity Center, poderá usar o nome de usuário emitido sob o `additionalEventData` elemento no login. Para obter mais detalhes sobre o nome de usuário em `additionalEventData`, consulte [Nome de usuário em eventos de login CloudTrail](#).

O mapeamento desses dois atributos de usuário para os atributos de usuário correspondentes em um diretório externo é definido no IAM Identity Center quando a fonte de identidade é Directory Service. Para obter mais informações, consulte [Mapeamento de atributos entre o IAM Identity Center e o diretório de provedores de identidades externos](#). Externamente, IdPs esse provisionamento, os

usuários com SCIM têm seu próprio mapeamento. Mesmo se você usar o diretório do IAM Identity Center como fonte de identidade, você pode usar o atributo `externalId` para fazer referência cruzada de entidades principais de segurança ao diretório externo.

A seção a seguir explica como você pode pesquisar um usuário do IAM Identity Center considerando o `username` e o `externalId`.

Como visualizar um usuário do IAM Identity Center por nome de usuário e ID externo

Você pode recuperar atributos de usuário do diretório do IAM Identity Center para um nome de usuário conhecido, solicitando primeiro um `userId` correspondente usando a solicitação de API [GetUserId](#) e, em seguida, emitindo uma solicitação de API [DescribeUser](#) conforme mostrado no exemplo anterior. O exemplo a seguir demonstra como recuperar um `userId` do Identity Store para um nome de usuário específico. Você pode omitir o parâmetro `region` se a instância do IAM Identity Center estiver na região padrão com a CLI.

```
aws identitystore get-user-id \
  --identity-store d-9876543210 \
  --alternate-identifier '{
    "UniqueAttribute": {
      "AttributePath": "username",
      "AttributeValue": "anyuser@example.com"
    }
  }' \
  --region your-region-id
```

Da mesma forma, você pode usar o mesmo mecanismo quando souber o `externalId`. Atualize o caminho do atributo no exemplo anterior com o valor `externalId` e o valor do atributo com o `externalId` específico que está pesquisando.

Como visualizar o Identificador Seguro (SID) de um usuário no Microsoft Active Directory (AD) e no ExternalID

Em certos casos, o IAM Identity Center emite o SID de um usuário no `principalId` campo de CloudTrail eventos, como aqueles que o portal de AWS acesso e o APIs OIDC emitem. Esses casos estão sendo gradualmente descontinuados. Recomendamos que os fluxos de trabalho usem o atributo AD `objectguid` quando você precisar de um identificador de usuário exclusivo do AD. Você pode encontrar esse valor no atributo `externalId` no diretório do IAM Identity Center. No entanto, se seus fluxos de trabalho exigirem o uso de SID, recupere o valor do AD, pois ele não está disponível no IAM Identity Center. APIs

[Como correlacionar eventos de usuário na mesma sessão de usuário](#) descreve como você pode usar os campos `externalId` e `username` para correlacionar um usuário do IAM Identity Center a um usuário correspondente em um diretório externo. Por padrão, o IAM Identity Center mapeia `externalId` para o atributo `objectguid` no AD, e esse mapeamento é fixo. O IAM Identity Center permite aos administradores a flexibilidade de mapear `username` de forma diferente do mapeamento padrão para o `userprincipalname` no AD.

Você pode visualizar esses mapeamentos no console do IAM Identity Center. Navegue até a aba Fonte de identidade de Configurações e escolha Gerenciar sincronização no menu Ações. Na seção Gerenciar sincronização, escolha o botão Exibir mapeamentos de atributos.

Embora você possa usar qualquer identificador de usuário exclusivo do AD disponível no IAM Identity Center para pesquisar um usuário no AD, recomendamos usá-lo nas consultas `objectguid` porque é um identificador imutável. O exemplo a seguir mostra como consultar o Microsoft AD com o Powershell para recuperar um usuário usando o valor `objectguid` do usuário de `16809ecc-7225-4c20-ad98-30094aefdbca`. Uma resposta bem-sucedida a essa consulta inclui o SID do usuário.

```
Install-WindowsFeature -Name RSAT-AD-PowerShell
```

```
Get-ADUser `
-Filter {objectGUID -eq [GUID]::Parse("16809ecc-7225-4c20-ad98-30094aefdbca")} `
-Properties *
```

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](#).

Note

Para obter mais informações sobre como a identificação do usuário e o rastreamento das ações do usuário em CloudTrail eventos estão evoluindo, consulte [Alterações importantes nos CloudTrail eventos do IAM Identity Center](#) no blog AWS de segurança.

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 uma trilha é criada no console, a mesma 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 obter mais informações, consulte os seguintes tópicos no Guia do usuário do AWS CloudTrail :

- [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.

CloudTrail eventos para o IAM Identity Center compatível APIs

As seções a seguir fornecem informações sobre os CloudTrail eventos associados aos seguintes APIs que o IAM Identity Center suporta:

- [API do IAM Identity Center](#)
- [API do Identity Store](#)
- [API OIDC](#)
- [AWS API do portal de acesso](#)
- [API SCIM](#)

CloudTrail eventos das operações da API do IAM Identity Center

A lista a seguir contém os CloudTrail eventos que as operações públicas do IAM Identity Center emitem com a fonte do sso.amazonaws.com evento. Para obter mais informações sobre as

operações públicas da API do IAM Identity Center, consulte a [Referência de APIs do IAM Identity Center](#).

Você pode encontrar eventos adicionais CloudTrail para as operações de API do console do IAM Identity Center nas quais o console depende. Para obter mais informações sobre esses consoles APIs, consulte a [Referência de Autorização de Serviço](#).

- [AttachCustomerManagedPolicyReferenceToPermissionSet](#)
- [AttachManagedPolicyToPermissionSet](#)
- [CreateAccountAssignment](#)
- [CreateApplication](#)
- [CreateApplicationAssignment](#)
- [CreateInstance](#)
- [CreateInstanceAccessControlAttributeConfiguration](#)
- [CreatePermissionSet](#)
- [CreateTrustedTokenIssuer](#)
- [DeleteAccountAssignment](#)
- [DeleteApplication](#)
- [DeleteApplicationAccessScope](#)
- [DeleteApplicationAssignment](#)
- [DeleteApplicationAuthenticationMethod](#)
- [DeleteApplicationGrant](#)
-

[DeleteInlinePolicyFromPermissionSet](#)

-

[DeleteInstance](#)

-

[DeleteInstanceAccessControlAttributeConfiguration](#)

-

[DeletePermissionsBoundaryFromPermissionSet](#)

-

[DeletePermissionSet](#)

-

[DeleteTrustedTokenIssuer](#)

-

[DescribeAccountAssignmentCreationStatus](#)[S](#)

-

[DescribeAccountAssignmentDeletionStatus](#)

-

[DescribeApplication](#)

-

[DescribeApplicationAssignment](#)

-

[DescribeApplicationProvider](#)

-

[DescribeInstance](#)

-

[DescribeInstanceAccessControlAttributeConfiguration](#)

-

[DescribePermissionSet](#)

-

[DescribePermissionSetProvisioningStatus](#)

- [DescribeTrustedTokenIssuer](#)
- [DetachCustomerManagedPolicyReferenceFromPermissionSet](#)
- [DetachManagedPolicyFromPermissionSet](#)
- [GetApplicationAccessScope](#)
- [GetApplicationAssignmentConfiguration](#)
- [GetApplicationAuthenticationMethod](#)
- [GetApplicationGrant](#)
- [GetInlinePolicyForPermissionSet](#)
- [GetPermissionsBoundaryForPermissionSet](#)
- [ListAccountAssignmentCreationStatus](#)
- [ListAccountAssignmentDeletionStatus](#)
- [ListAccountAssignments](#)
- [ListAccountAssignmentsForPrincipal](#)
- [ListAccountsForProvisionedPermissionSet](#)
- [ListApplicationAccessScopes](#)
-

[ListApplicationAssignments](#)

-

[ListApplicationAssignmentsForPrincipal](#)

-

[ListApplicationAuthenticationMethods](#)

-

[ListApplicationGrants](#)

-

[ListApplicationProviders](#)

-

[ListApplications](#)

-

[ListCustomerManagedPolicyReferencesInPermissionSet](#)

-

[ListInstances](#)

-

[ListManagedPoliciesInPermissionSet](#)

-

[ListPermissionSetProvisioningStatus](#)

-

[ListPermissionSets](#)

-

[ListPermissionSetsProvisionedToAccount](#)

-

[ListTagsForResource](#)

-

[ListTrustedTokenIssuers](#)

-

[ProvisionPermissionSet](#)

-

[PutApplicationAccessScope](#)

- [PutApplicationAssignmentConfiguration](#)
- [PutApplicationAuthenticationMethod](#)
- [PutApplicationGrant](#)
- [PutInlinePolicyToPermissionSet](#)
- [PutPermissionsBoundaryToPermissionSet](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateApplication](#)
- [UpdateInstance](#)
- [UpdateInstanceAccessControlAttributeConfiguration](#)
- [UpdatePermissionSet](#)
- [UpdateTrustedTokenIssuer](#)

CloudTrail eventos das operações da API do Identity Store

A lista a seguir contém os CloudTrail eventos que as operações públicas do Identity Store emitem com a fonte do `identitystore.amazonaws.com` evento. Para obter mais informações sobre as operações de API do Identity Store, consulte a [Referência de API do Identity Store](#).

Você pode encontrar eventos adicionais CloudTrail para as operações de API do console do Identity Store com a fonte do `sso-directory.amazonaws.com` evento. Eles APIs oferecem suporte

ao console e AWS ao portal de acesso. Se você precisar detectar a ocorrência de uma operação específica, como adicionar membros a um grupo, recomendamos considerar as operações de API pública e de console. Para obter mais informações sobre esses consoles APIs, consulte a [Referência de Autorização de Serviço](#).

- [CreateGroup](#)
- [CreateGroupMembership](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteGroupMembership](#)
- [DeleteUser](#)
- [DescribeGroup](#)
- [DescribeGroupMembership](#)
- [DescribeUser](#)
- [GetGroupId](#)
- [GetGroupMembershipId](#)
- [GetUserId](#)
- [IsMemberInGroups](#)
- [ListGroupMemberships](#)
- [ListGroupMembershipsForMember](#)
- [ListGroups](#)
- [ListUsers](#)
- [UpdateGroup](#)
- [UpdateUser](#)

CloudTrail eventos das operações da API OIDC

A lista a seguir contém os CloudTrail eventos que as operações públicas do OIDC emitem. Para obter mais informações sobre as operações da API pública do OIDC, consulte a [Referência de API OIDC](#).

- [CreateToken](#) (origem de evento `sso.amazonaws.com`)
- [CreateTokenWithIAM](#) (origem de evento `sso-oauth.amazonaws.com`)

CloudTrail eventos das operações da API do portal de AWS acesso

A lista a seguir contém os CloudTrail eventos que as operações da API do portal de AWS acesso emitem com a fonte do sso.amazonaws.com evento. As operações de API consideradas indisponíveis na API pública oferecem suporte às operações do portal de AWS acesso. O uso do AWS CLI pode levar à emissão de CloudTrail eventos tanto das operações da API do portal de AWS acesso público quanto daquelas que não estão disponíveis na API pública. Para obter mais informações sobre as operações da API do portal de AWS acesso público, consulte a [Referência da API do portal de AWS acesso](#).

- Authenticate(Não disponível na API pública. Fornece login no portal de AWS acesso.)
- Federate(Não disponível na API pública. Fornece federação nas aplicações.)
- [ListAccountRoles](#)
- [ListAccounts](#)
- ListApplications(Não disponível na API pública. Fornece recursos atribuídos aos usuários para exibição no portal de AWS acesso.)
- ListProfilesForApplication(Não disponível na API pública. Fornece metadados do aplicativo para exibição no portal de AWS acesso.)
- [GetRoleCredentials](#)
- [Logout](#)

CloudTrail eventos das operações da API SCIM

Para obter informações sobre as operações públicas da API SCIM, consulte a [Referência de API do portal de acesso do AWS](#).

Informações de identidade em CloudTrail eventos do IAM Identity Center

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar o seguinte:

- 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.

- Indica se a solicitação foi feita por um usuário do IAM Identity Center. Nesse caso, os `identityStoreArn` campos `userId` e estão disponíveis nos CloudTrail eventos para identificar o usuário do IAM Identity Center que iniciou a solicitação. Para obter mais informações, consulte [Identificação do usuário nos eventos iniciados pelo usuário CloudTrail do IAM Identity Center](#).

Para obter mais informações, consulte [Elemento `userIdentity` do CloudTrail](#).

Note

Atualmente, o IAM Identity Center não emite CloudTrail eventos para login de usuários em aplicativos web AWS gerenciados (por exemplo, Amazon SageMaker AI Studio) com a API OIDC. Essas aplicações da web são um subconjunto do conjunto mais amplo de the section called “AWS aplicativos gerenciados”, que também inclui aplicações não web como Amazon Athena SQL e Concessão de Acesso do Amazon S3.

Entendendo CloudTrail os eventos do IAM Identity Center

Uma trilha é uma configuração que permite a entrega de eventos a um bucket do Amazon S3 especificado. 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 eventos não são um rastreamento de pilha ordenado das chamadas públicas da API, portanto, eles não aparecem em nenhuma ordem específica. Saiba mais sobre o [conteúdo de um CloudTrail registro](#) no Guia CloudTrail do usuário.

Este exemplo demonstra uma entrada de CloudTrail registro que captura uma `DescribePermissionsPolicies` ação realizada por um usuário do IAM (samadams) interagindo com o IAM Identity Center:

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJAIENLMexample",
        "arn": "arn:aws:iam::08966example:user/samadams",
        "accountId": "111122223333",
        "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": "111122223333"
    }
]
}

```

Este exemplo demonstra uma entrada de CloudTrail registro capturando uma ListApplications ação realizada por um usuário do IAM Identity Center no portal de AWS acesso:

```

{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IdentityCenterUser",
        "accountId": "111122223333",
        "onBehalfOf": {
          "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
          "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "credentialId": "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
      },
      "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": "111122223333"
    }
]
}

```

Este exemplo demonstra uma entrada de CloudTrail registro capturando uma `CreateToken` ação realizada por um usuário do IAM Identity Center autenticado com o serviço IAM Identity Center OIDC:

```

{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IdentityCenterUser",
        "accountId": "111122223333",
        "onBehalfOf": {
            "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
            "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "credentialId": "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
    },
    "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": "111122223333",
        "type": "IdentityStoreId",
        "ARN": "d-1234567890"
      }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }
}

```

Noções básicas sobre eventos de login do IAM Identity Center

AWS CloudTrail registra eventos de login bem-sucedidos e malsucedidos para todas as fontes de identidade do IAM Identity Center. As identidades originadas do IAM Identity Center e do Active Directory (AD Connector e AWS Managed Microsoft AD) incluem eventos de login adicionais que são capturados sempre que um usuário é solicitado a resolver um desafio ou fator de credencial específico, além do 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
<code>CredentialChallenge</code>	Usado para notificar que o IAM Identity Center solicitou que o usuário resolvesse um desafio de credencial específico	Usuários nativos do IAM Identity Center, AD Connector e AWS Managed Microsoft AD

Nome do evento	Objetivo do evento	Aplicabilidade da fonte de identidade
	o e especifica o <code>CredentialType</code> que era necessário (por exemplo, SENHA ou TOTP).	
<code>CredentialVerification</code>	Usado para notificar que o usuário tentou resolver uma solicitação <code>CredentialChallenge</code> específica e especifica se essa credencial foi bem-sucedida ou falhou.	Usuários nativos do IAM Identity Center, AD Connector e AWS Managed Microsoft AD
<code>UserAuthentication</code>	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 <code>UserAuthentication</code> evento será registrado.	Todas as fontes de identidade

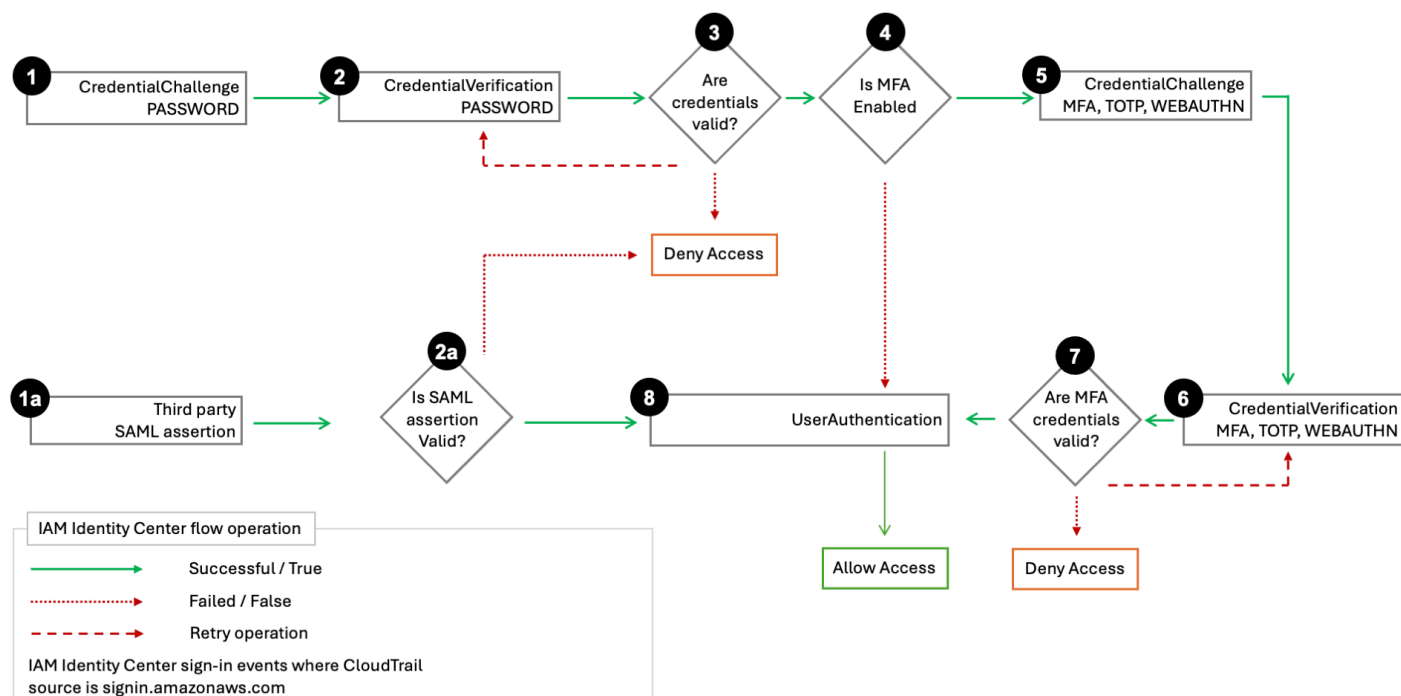
A tabela a seguir captura outros campos úteis de dados de eventos contidos em eventos de login CloudTrail específicos.

Campo	Objetivo do evento	Aplicabilidade do evento de login	Exemplos de valores
<code>AuthWorkflowID</code>	Usado para correlacionar todos os eventos emitidos em uma	<code>CredentialChallenge</code> , <code>Credential</code>	“AuthWorkflowIdentificação”: “9de74b32

Campo	Objetivo do evento	Aplicabilidade do evento de login	Exemplos de valores
	sequência de login inteira. Para cada login de usuário, vários eventos podem ser emitidos pelo IAM Identity Center.	lVerifica tion , UserAuthen tication	-8362-4a01-a524-de 21df59fd83"
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.	Credentia lChalleng e , Credentia lVerifica tion , UserAuthen tication	CredentialType": "PASSWORD" ou "": CredentialType "PASSWORD, TOTP" (os valores possíveis incluem: PASSWORD, TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP, EMAIL_OTP)
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.	UserAuthen tication	"DeviceEnrollmentRequired": "verdadeiro"
LoginTo	Usado para especificar o local de redirecionamento após uma sequência de login bem-sucedida.	UserAuthen tication	"LoginTo": "https:// mydirectory.awsapp s.com/start/....."

CloudTrail eventos nos fluxos de login do IAM Identity Center

O diagrama a seguir descreve o fluxo de login e os CloudTrail eventos que o Sign-in emite.



O diagrama mostra um fluxo de login com senha e um fluxo de login federado.

O fluxo de login com senha, que consiste nas etapas de 1 a 8, demonstra as etapas durante o processo de login com nome de usuário e senha. O IAM Identity Center define `userIdentity.additionalEventData.CredentialType` como "PASSWORD", e o IAM Identity Center passa pelo ciclo de desafio-resposta de credenciais, tentando novamente conforme necessário.

O número de etapas depende do tipo de [login e da presença da autenticação multifator \(MFA\)](#).

O processo inicial resulta em três ou cinco CloudTrail eventos com o `UserAuthentication` término da sequência para uma autenticação bem-sucedida. Tentativas malsucedidas de autenticação de senha resultam em CloudTrail eventos adicionais, pois o IAM Identity Center reemite `CredentialChallenge` a autenticação regular ou, se habilitada, a autenticação MFA.

O fluxo de login com senha também abrange o cenário em que um usuário do IAM Identity Center recém-criado com uma chamada de API `CreateUser` faz login com uma senha de uso único (OTP). O tipo de credencial nesse cenário é "EMAIL_OTP".

O fluxo de login federado, composto pelas etapas 1a, 2a e 8, demonstra as principais etapas durante o processo de autenticação federada, em que uma [declaração SAML é fornecida por um provedor de identidade](#), validada pelo IAM Identity Center e, se bem-sucedida, resulta em `UserAuthentication`. O IAM Identity Center não invoca a sequência de autenticação interna da MFA nas etapas 3 a 7 porque um provedor de identidade externo federado é responsável por toda a autenticação de credenciais do usuário.

Nome de usuário em eventos de login CloudTrail

O IAM Identity Center emite o campo `UserName` abaixo do elemento `additionalEventData` uma vez por login bem-sucedido de um usuário do IAM Identity Center. A lista a seguir descreve os dois eventos de login no escopo e as condições sob as quais esses eventos acontecem. Somente uma das condições pode ser verdadeira quando um usuário está fazendo login.

- `CredentialChallenge`
 - Quando `CredentialType` é "PASSWORD" — se aplica à autenticação por senha com Directory Service ou Diretório do Centro de Identidade do IAM.
 - Quando `CredentialType` é "EMAIL_OTP" — aplica-se somente Diretório do Centro de Identidade do IAM quando um usuário criado com uma chamada de `CreateUser` API tenta fazer login pela primeira vez, e o usuário recebe uma senha de uso único para entrar com essa senha uma vez.
- `UserAuthentication`
 - Quando `CredentialType` é "EXTERNAL_IDP" — aplica-se à autenticação com um IdP externo.

O valor de `UserName` para autenticações bem-sucedidas é o seguinte:

- Quando a fonte de identidade é um IdP externo, o valor é igual ao valor `nameID` na declaração de entrada do SAML. Esse valor é igual ao campo `UserName` no Diretório do Centro de Identidade do IAM.
- Quando a fonte de identidade é uma Diretório do Centro de Identidade do IAM, o valor emitido é igual ao `UserName` campo nesse diretório.
- Quando a fonte de identidade é a Directory Service, o valor emitido é igual ao nome de usuário que o usuário insere durante a autenticação. Por exemplo, um usuário que tem o nome de usuário `anyuser@company.com` pode se autenticar com `anyuseranyuser@company.com`, ou `ecompany.com/anyuser`, em cada caso, o valor inserido é emitido CloudTrail respectivamente.

Mascaramento de segurança de tentativas incorretas de nome de usuário

O `UserName` campo contém a string `HIDDEN_DUE_TO_SECURITY_REASONS` quando o evento gravado é uma falha de login no console causada pela entrada incorreta do nome de usuário. CloudTrail não registra o conteúdo nesse caso porque o texto pode conter informações confidenciais, conforme descrito nos exemplos a seguir:

- Um usuário digita acidentalmente uma senha no campo de nome do usuário.
- Um usuário digita acidentalmente o nome de uma conta de email pessoal, um identificador de login de um banco ou algum outro ID privado.

Tip

Recomendamos que você use `userId` e `identityStoreArn` identifique o usuário por trás dos CloudTrail eventos do IAM Identity Center. Se precisar usar o campo `userName`, você pode usar o `userName` abaixo do elemento `additionalEventData` que é emitido uma vez por login bem-sucedido.

Para obter informações adicionais sobre como você pode usar o campo `UserName`, consulte [Como correlacionar eventos de usuário na mesma sessão de usuário](#).

Exemplos de eventos para cenários de login do IAM Identity Center

Os exemplos a seguir ilustram as sequências de CloudTrail eventos típicas geradas durante vários cenários de AWS login. Esses exemplos servem como padrões de referência para ajudar você a interpretar os logs de autenticação, identificar problemas de segurança e verificar se as políticas de autenticação estão funcionando corretamente.

Tópicos

- [Login bem-sucedido ao se autenticar apenas com senha](#)
- [Login bem-sucedido ao se autenticar com um provedor de identidade externo](#)
- [Login bem-sucedido ao se autenticar com uma senha e uma aplicação autenticadora de senha de uso único com marcação temporal \(TOTP\)](#)
- [É necessário fazer login bem-sucedido ao autenticar com uma senha e um registro forçado de MFA](#)
- [Falha no login devido à autenticação de senha incorreta](#)

Login bem-sucedido ao se autenticar apenas com senha

A sequência de eventos a seguir captura um exemplo de login bem-sucedido somente com senha.

CredentialChallenge (Senha)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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",
    "UserName": "bobsmith@example.com",
    "CredentialType": "PASSWORD"
  },
  "requestID": "5be44ffb-6946-4f47-acaf-1adebd4afead",
  "eventID": "27ea7725-c1fd-4355-bdba-d0e628e0e604",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "serviceEventDetails": {
    "CredentialChallenge": "Success"
  }
}
```

```
}
```

Bem sucedido CredentialVerification (Senha)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSBsh1Ic50BAA6ftz73M6LsflWDlf0xvi02K3wet946lC30f_iWdilx-zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx-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": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSBsh1Ic50BAA6ftz73M6LsfLWD1f0xvi02K3wet946lC30f_iWdilx-zv__4pShf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx-east-1",
    "CredentialType": "EXTERNAL_IDP",
    "UserName": "bobsmith@example.com"
  },
  "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 uma aplicação autenticadora de senha de uso único com marcação temporal (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": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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",
  "UserName":"bobsmith@example.com"
},
"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":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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\u003dQV1BQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSXp0MDZ6auth_code\u003d11FirmCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIG1YUUVe31Nkzd7ihxKn6DMdnFf00108qc3RFRF00108qc3RFSx-pjBXXKG_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 demonstra uma autenticação de senha bem-sucedida em que o usuário precisou se registrar e concluir com sucesso a autenticação multifator (MFA) antes de finalizar o processo de login.

CredentialChallenge (Senha)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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",
  "UserName":"bobsmith@example.com"
},
"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":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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": "IdentityCenterUser",
        "arn": "",
        "accountId": "111122223333",
        "accessKeyId": "",
        "onBehalfOf": {
            "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
            "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
        },
        "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
    },
    "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_maUsZ7ABETjeQhyWfvIHyz52rgR28sYAKN1oEk2G07czrwzXvE9HL1N2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY_EgU3fh0L3QWvWiQuYnDPMYPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi50YI9QSc
\u003dd-9067230c03\u0026region\u003ddus-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"
    }
  }
}

```

Falha no login devido à autenticação de senha incorreta

A sequência de eventos a seguir demonstra uma tentativa de autenticação em que o usuário inseriu seu nome de usuário com sucesso, mas falhou na etapa de verificação da senha, resultando em um login malsucedido.

CredentialChallenge (Senha)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"Unknown",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
  },

```

```

"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",
  "UserName":"bobsmith@example.com"
},
"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",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":""
  },
  "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"
}
}
```

Registrando chamadas da API SCIM do IAM Identity Center com AWS CloudTrail

O [IAM Identity Center SCIM](#) é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou um AWS service (Serviço da AWS). CloudTrail captura chamadas de API para o SCIM como eventos. Usando as informações coletadas por CloudTrail, você pode determinar as informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. Para saber mais sobre isso CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#).

Note

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. No entanto, pode ser necessário fazer rodízio de tokens de acesso para ver os eventos do SCIM, caso o token tenha sido criado antes de setembro de 2024.

Para obter mais informações, consulte [Fazer rodízio de um token de acesso](#).

O SCIM suporta o registro das seguintes operações como eventos em: CloudTrail

- [CreateGroup](#)
- [CreateUser](#)

- [DeleteGroup](#)
- [DeleteUser](#)
- [GetGroup](#)
- [GetSchema](#)
- [GetUser](#)
- [ListGroups](#)
- [ListResourceTypes](#)
- [ListSchemas](#)
- [ListUsers](#)
- [PatchGroup](#)
- [PatchUser](#)
- [PutUser](#)
- [ServiceProviderConfig](#)

Exemplos de CloudTrail eventos

Os exemplos a seguir demonstram registros de CloudTrail eventos típicos gerados durante as operações do SCIM com o IAM Identity Center. Esses exemplos mostram a estrutura e o conteúdo dos eventos para operações bem-sucedidas e cenários de erro comuns, ajudando você a entender como interpretar os CloudTrail registros ao solucionar problemas de provisionamento do SCIM.

Operação **CreateUser** bem-sucedida

Este CloudTrail evento mostra uma CreateUser operação bem-sucedida realizada por meio da API SCIM. O evento captura os parâmetros da solicitação (com informações confidenciais mascaradas) e os elementos de resposta, incluindo o ID do usuário recém-criado. Esse tipo de evento é gerado quando um provedor de identidades provisiona com sucesso um novo usuário para o IAM Identity Center usando o protocolo SCIM.

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "WebIdentityUser",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
```

```

"eventTime": "xxxx",
"eventSource": "identitystore-scim.amazonaws.com",
"eventName": "CreateUser",
"awsRegion": "us-east-1",
"sourceIPAddress": "xx.xxx.xxx.xxx",
"userAgent": "Go-http-client/2.0",
"requestParameters": {
  "httpBody": {
    "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "schemas" : [
      "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "name": {
      "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "active": true,
    "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "tenantId": "xxxx"
},
"responseElements": {
  "meta" : {
    "created" : "Oct 10, 2024, 1:23:45 PM",
    "lastModified" : "Oct 10, 2024, 1:23:45 PM",
    "resourceType" : "User"
  },
  "displayName" : "HIDDEN_DUE_TO_SECURITY_REASONS",
  "schemas" : [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ],
  "name": {
    "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "active": true,
  "id" : "c4488478-a0e1-700e-3d75-96c6bb641596",
  "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
},
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,

```

```
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}
```

Falha na operação **PatchGroup**: ausência do atributo de caminho obrigatório

Esse CloudTrail evento mostra uma falha na PatchGroup operação que resultou em ValidationException uma mensagem de erro "Missing path in PATCH request". O erro ocorreu porque a operação PATCH exige um atributo de caminho para especificar qual atributo de grupo modificar, mas esse atributo estava ausente na solicitação.

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "Missing path in PATCH request",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REMOVE",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ],
      "schemas": [
        "HIDDEN_DUE_TO_SECURITY_REASONS"
      ]
    },
    "tenantId": "xxxx",
    "id": "xxxx"
  }
}
```



```

},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Falha na operação **CreateGroup**: o nome do grupo já existe

Esse CloudTrail evento mostra uma falha na CreateGroup operação que resultou em ConflictException uma mensagem de erro "Duplicate GroupDisplayName". Esse erro ocorre ao tentar criar um grupo com um nome de exibição que já existe no IAM Identity Center. O provedor de identidades deve usar um nome de grupo exclusivo ou atualizar o grupo existente em vez de criar um novo.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ConflictException",
  "errorMessage": "Duplicate GroupDisplayName",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
}

```

```

"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Falha na operação **PatchUser**: vários endereços de e-mail não compatíveis

Esse CloudTrail evento mostra uma falha na PatchUser operação que resultou em ValidationException uma mensagem de erro "List attribute emails exceeds allowed limit of 1". Esse erro ocorre ao tentar atribuir vários endereços de e-mail a um usuário, uma vez que o IAM Identity Center oferece suporte a apenas um endereço de e-mail por usuário. O provedor de identidade deve configurar o mapeamento SCIM para enviar somente um único endereço de e-mail para cada usuário.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "List attribute emails exceeds allowed limit of 1",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REPLACE",
          "path": "emails",

```

```

        "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
      }
    ],
    "schemas": [
      "HIDDEN_DUE_TO_SECURITY_REASONS"
    ]
  },
  "tenantId": "xxxx",
  "id": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Erros comuns de validação da API SCIM no IAM Identity Center

As mensagens de erro de validação a seguir geralmente aparecem em CloudTrail eventos ao usar a API SCIM com o IAM Identity Center. Esses erros de validação geralmente ocorrem durante as operações de provisionamento de usuários e grupos.

Para obter orientação detalhada sobre como resolver esses erros e configurar adequadamente o provisionamento do SCIM, consulte este [Artigo de AWS re:Post](#)

- E-mail de atributo de lista excede o limite permitido de 1
- Limite permitido de endereços de atributo de lista de 1
- 1 erros de validação detectados: o valor em '*name.familyName*' não satisfaz a restrição: o membro deve satisfazer o padrão de expressão regular: `[\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r ]+`
- 2 erros de validação detectados: o valor em 'name.familyName' não satisfaz a restrição: o comprimento do membro deve ser maior ou igual a 1; o valor em 'name.familyName' não satisfaz a restrição: o membro deve satisfazer o padrão de expressão regular: `[\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r ]+`

- 2 erros de validação detectados: o valor em 'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value' não satisfaz a restrição: o membro deve ter comprimento maior ou igual a 1; o valor em 'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value' não satisfaz a restrição: o membro deve satisfazer o padrão de expressão regular: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\ n\\ r] +"`,
- JSON inválido de RequestBody
- Formato de arquivo inválido

Conecte os componentes do aplicativo com a Amazon EventBridge

Você pode integrar o IAM Identity Center com EventBridge a [Amazon](#) para gerar eventos que iniciam notificações administrativas ou invocam fluxos de trabalho automatizados em resposta a ações específicas do IAM Identity Center registradas em eventos. CloudTrail

Por exemplo, você pode configurar [EventBridge regras](#) para detectar quando um usuário exclui um aplicativo ou quando o IAM Identity Center cria um novo grupo. [Dependendo do seu caso de uso, você pode rotear esses eventos para um tópico do Amazon SNS para notificar administradores ou invocar automação adicional usando Step AWS LambdaFunctions ou outros serviços compatíveis. EventBridge](#)

Como registrar em log de erros de sincronização configurável do AD

Você pode habilitar o registro em log nas configurações de sincronização do Active Directory (AD) configuráveis para receber logs com informações sobre erros que podem ocorrer durante o processo de sincronização. Com esses logs, você pode monitorar se há algum problema na sincronização do AD configurável e tomar as medidas aplicáveis. 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

O registro em log é cobrado. Para obter mais informações, consulte [Vended Logs](#) na página de [CloudWatch preços da Amazon](#).

Para habilitar logs de erros de sincronização do AD configurável

1. Faça login no [console do IAM Identity Center](#).
2. Escolha Configurações.
3. Na página Configurações, escolha a guia Fonte de identidades, escolha Ações e depois Gerenciar sincronização.
4. Escolha Adicionar entrega de logs e um dos seguintes tipos de destino.
 - a. Escolha To Amazon CloudWatch Logs. Depois, escolha ou insira o grupo de logs de destino.
 - b. Escolha Para o Amazon S3. Depois, escolha ou insira o bucket de destino.
 - c. Escolha Para o Firehose. Depois, escolha ou insira o fluxo de entrega de destino.
5. Selecione Enviar.

Para desabilitar logs de erros de sincronização do AD configurável

1. Faça login no [console do IAM Identity Center](#).
2. Escolha Configurações.
3. Na página Configurações, escolha a guia Fonte de identidades, escolha Ações e depois Gerenciar sincronização.
4. Escolha Remover para o destino que você deseja remover.
5. Selecione Enviar.

Campos dos logs de erros de sincronização do AD configurável

Veja na lista a seguir os possíveis campos de logs 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 origem da sincronização é de onde as entidades estão sendo sincronizadas. Para o IAM Identity Center, é um Active Directory (AD) gerenciado pelo Directory Service. A origem da sincronização contém o domínio e o ARN do diretório afetado.

sync_target

O destino da sincronização é o destino onde as entidades estão sendo salvas. Para o IAM Identity Center, é um repositório de identidades. O destino de sincronização contém o ARN do repositório de identidades afetado.

source_entity_id

Um identificador exclusivo da entidade que está causando o erro. Para o IAM Identity Center, 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 timestamp de quando ocorreu o erro.

Exemplos de logs de erros de sincronização do AD configurável

Exemplo 1: um log de erros de 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 log 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

Audidores terceirizados avaliam a segurança e a conformidade Serviços da AWS Centro de Identidade do AWS IAM 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 regulamentações aplicáveis. Para obter mais informações sobre sua responsabilidade de conformidade ao usar Serviços da AWS, consulte a [Documentação AWS de segurança](#).

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 data center tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte [infraestrutura AWS global](#).

Para saber mais sobre Centro de Identidade do AWS IAM resiliência, consulte [Design de resiliência e comportamento regional](#).

Segurança da infraestrutura no IAM Identity Center

Como serviço gerenciado, Centro de Identidade do AWS IAM 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 por meio da rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Proteção de dados no IAM Identity Center

O [modelo de responsabilidade AWS compartilhada](#) se aplica à proteção de dados no AWS IAM Identity Center. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa toda a AWS nuvem. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos AWS serviços que usa. Para obter mais informações sobre a privacidade de dados, consulte as [Perguntas frequentes sobre privacidade de dados](#). Para obter mais informações sobre a proteção de dados na Europa, consulte o artigo do blog [AWS Shared Responsibility Model and GDPR](#) no Blog de segurança da AWS .

É recomendável também que você proteja seus dados da seguinte maneira:

- Use a autenticação multifator (MFA) com o IAM Identity Center.
- Use o TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como [trabalhar com CloudTrail trilhas](#) no Guia AWS CloudTrail do usuário.
- Use soluções AWS de criptografia, juntamente com todos os controles de segurança padrão nos AWS serviços.

Recomendamos fortemente que você nunca insira informações confidenciais ou sensíveis, como os endereços de e-mail de clientes, em tags ou campos de texto livre, como um campo Nome. Isso inclui quando você trabalha com Centro de Identidade do AWS IAM ou outros AWS serviços usando o console, a API ou AWS SDKs. AWS CLI Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de diagnóstico.

Criptografia em trânsito

O IAM Identity Center protege os dados em trânsito, à medida que viajam de e para o serviço, criptografando automaticamente todos os dados entre redes usando o protocolo de criptografia Transport Layer Security (TLS) 1.2 ou TLS 1.3. As solicitações HTTPS diretas autenticadas com o IAM e enviadas para o IAM Identity Center APIs, a API Identity Store ou a API OIDC são assinadas usando o [algoritmo AWS Signature versão 4](#) para estabelecer uma conexão segura.

Privacidade de dados

Com o IAM Identity Center, você retém o controle dos dados da organização. Suas identidades de usuário e grupo armazenadas no IAM Identity Center são compartilhadas com outros AWS serviços, como [aplicativos AWS gerenciados](#), somente se você habilitá-las com o IAM Identity Center e se necessário para esses serviços.

Para obter informações adicionais, consulte as [Perguntas frequentes sobre privacidade de dados na AWS](#).

Retenção de dados

O IAM Identity Center armazena os dados, como identidades de usuários e grupos e metadados, até que você os exclua do serviço. Quando você exclui uma instância do IAM Identity Center, os dados que ela contém também são excluídos.

Criptografia em repouso

O IAM Identity Center fornece criptografia para proteger os dados em repouso do cliente usando os seguintes tipos de chaves:

- Chaves pertencentes à AWS (tipo de chave padrão) — O IAM Identity Center usa essas chaves por padrão para criptografar automaticamente seus dados. Você não pode visualizar, gerenciar, auditar seu uso ou usar chaves AWS próprias para outros fins. O IAM Identity Center gerencia totalmente o gerenciamento de chaves para manter os dados seguros, sem que você precise realizar qualquer ação. Para obter mais informações, consulte [Chaves de propriedade da AWS no Guia do desenvolvedor do AWS Key Management Service](#).
- Chaves gerenciadas pelo cliente — Nas instâncias de organização do IAM Identity Center, você pode escolher uma chave simétrica gerenciada pelo cliente para criptografia do resto dos dados de identidade da força de trabalho, como atributos de usuário e grupo. É possível criar, possuir e gerenciar essas chaves de criptografia. Como você tem controle total dessa camada de criptografia, você pode realizar tarefas como:
 - Estabelecer e manter políticas de chave para restringir o acesso à chave somente aos diretores do IAM que precisam de acesso, como o IAM Identity Center AWS Organizations e [AWS aplicativos gerenciados](#) a seus administradores.
 - Como estabelecer e manter políticas do IAM para acesso à chave, incluindo acesso entre contas
 - Habilitar e desabilitar políticas de chaves

- Alternar os materiais de criptografia de chave
- Como auditar o acesso aos dados que exigem chave de acesso
- Adicionar etiquetas
- Criar réplicas de chaves
- Chaves de agendamento para exclusão

Para saber como implementar uma chave KMS gerenciada pelo cliente no IAM Identity Center, consulte [Implementando chaves KMS gerenciadas pelo cliente em Centro de Identidade do AWS IAM](#). Para obter mais informações sobre chaves gerenciadas pelo cliente, consulte [Chave gerenciada pelo cliente](#) no Guia do desenvolvedor do AWS Key Management Service .

 Note

O IAM Identity Center habilita automaticamente a criptografia em repouso usando chaves KMS AWS próprias para proteger os dados do cliente sem nenhum custo. No entanto, AWS KMS cobranças se aplicam ao usar uma chave gerenciada pelo cliente. Para obter mais informações sobre preços, consulte [definição de preços da AWS Key Management Service](#).

Considerações sobre a implementação de chaves gerenciadas pelo cliente:

- Chaves dedicadas: recomendamos criar uma nova chave KMS dedicada gerenciada pelo cliente para cada instância do IAM Identity Center, em vez de reutilizar uma chave existente. Essa abordagem fornece uma separação mais clara das tarefas, simplifica o gerenciamento do controle de acesso e torna a auditoria de segurança mais simples. Ter uma chave dedicada também reduz o risco ao limitar o impacto das alterações de chave em uma única instância do IAM Identity Center.
- Uso do IAM Identity Center em várias Regiões da AWS: Se você planeja replicar sua instância do IAM Identity Center para outras Regiões da AWS, precisará usar uma chave KMS gerenciada pelo cliente para criptografia em repouso. O tipo de chave KMS de AWS propriedade padrão não é suportado em um IAM Identity Center multirregional. Para obter mais informações, consulte [Usando o IAM Identity Center em várias Regiões da AWS](#).

Note

O IAM Identity Center usa criptografia de [criptografia envelopada](#) dos dados de identidade da força de trabalho. A chave KMS cumpre a função de uma chave de empacotamento que criptografa a chave de dados que é realmente usada para criptografar os dados.

Para obter mais informações sobre o AWS KMS, consulte [O que é o AWS Key Management Service?](#)

Contexto de criptografia do IAM Identity Center

Um [contexto de criptografia](#) é um conjunto opcional de pares de valores-chave não secretos que contêm informações contextuais adicionais sobre os dados. AWS KMS usa o contexto de criptografia como dados autenticados adicionais para oferecer suporte à criptografia autenticada. Quando você inclui um contexto de criptografia em uma solicitação para criptografar dados, AWS KMS vincula o contexto de criptografia aos dados criptografados. Para descriptografar os dados, você inclui o mesmo contexto de criptografia na solicitação. Consulte o [Guia do desenvolvedor do AWS KMS](#) para obter mais informações sobre o contexto de criptografia.

O IAM Identity Center usa chaves de contexto de criptografia das seguintes: `aws:sso:instance-arn`, `aws:identitystore:identitystore-arn` e `tenant-key-id`. Por exemplo, o contexto de criptografia a seguir pode aparecer nas operações de AWS KMS API invocadas pela [API do IAM Identity Center](#).

```
"encryptionContext": {
  "tenant-key-id": "ssoins-1234567890abcdef",
  "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-1234567890abcdef"
}
```

O contexto de criptografia a seguir pode aparecer nas operações de AWS KMS API invocadas pela [API do Identity Store](#).

```
"encryptionContext": {
  "tenant-key-id": "12345678-1234-1234-1234-123456789012",
  "aws:identitystore:identitystore-arn":
    "arn:aws:identitystore::123456789012:identitystore/d-1234567890"
}
```

Usar o contexto de criptografia para controlar o acesso à chave gerenciada pelo cliente

Você pode usar o contexto de criptografia nas políticas de chave e políticas do IAM como condições para controlar o acesso à sua chave simétrica gerenciada pelo cliente. Alguns dos modelos de política de chave do [Declarações de política de chave KMS avançadas](#) incluem essas condições para garantir que a chave seja usada somente com uma instância específica do IAM Identity Center.

Como monitorar chaves de criptografia para o IAM Identity Center

Ao usar uma chave KMS gerenciada pelo cliente com sua instância do IAM Identity Center, você pode usar [AWS CloudTrail](#) o [Amazon CloudWatch Logs para rastrear as solicitações para as](#) quais o IAM Identity Center envia. AWS KMS As operações da API KMS que o IAM Identity Center chama estão listadas em [Etapa 2: preparar as declarações de política de chave KMS](#). CloudTrail os eventos dessas operações de API contêm o contexto de criptografia, que permite monitorar as operações de AWS KMS API chamadas pela instância do IAM Identity Center para acessar dados criptografados pela chave gerenciada pelo cliente.

Exemplo de contexto de criptografia em um CloudTrail evento de uma operação de AWS KMS API:

```
{
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "encryptionContext": {
      "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-xxxxxxxxxxxxxxxx",
      "tenant-key-id": "ssoins-xxxxxxxxxxxxxxxx"
    }
  }
}
```

AWS armazenamento, criptografia e exclusão dos atributos de identidade do IAM Identity Center em aplicativos gerenciados

Alguns aplicativos AWS gerenciados com os quais você implanta Centro de Identidade do AWS IAM, como AWS Systems Manager e Amazon CodeCatalyst, armazenam atributos específicos de usuários e grupos do IAM Identity Center em seu próprio armazenamento de dados. A criptografia em repouso com uma chave KMS gerenciada pelo cliente no IAM Identity Center não se estende aos atributos de usuário e grupo do IAM Identity Center armazenados em aplicativos AWS gerenciados.

AWS os aplicativos gerenciados oferecem suporte a diferentes métodos de criptografia para os dados que eles armazenam. Por fim, quando você exclui atributos de usuário e grupo no IAM Identity Center, esses aplicativos AWS gerenciados podem continuar armazenando essas informações após sua exclusão no IAM Identity Center. Consulte o guia do usuário de seus aplicativos AWS gerenciados para ver a criptografia e a segurança dos dados armazenados nos aplicativos.

Implementando chaves KMS gerenciadas pelo cliente em Centro de Identidade do AWS IAM

As chaves gerenciadas pelo cliente são AWS chaves do Serviço de Gerenciamento de Chaves que você cria, possui e gerencia. Para implementar uma chave KMS gerenciada pelo cliente para criptografia em repouso no AWS IAM Identity Center, siga estas etapas:

Important

Alguns aplicativos AWS gerenciados não podem ser usados com o AWS IAM Identity Center configurado com uma chave KMS gerenciada pelo cliente. Consulte [AWS aplicativos gerenciados que você pode usar com o IAM Identity Center](#).

1. [Etapa 1: identificar casos de uso para a organização](#) — Para definir as permissões corretas para o uso da chave KMS, você precisa identificar os casos de uso relevantes na organização. As permissões da chave KMS consistem em declarações de política de chave KMS e políticas baseadas em identidade que trabalham juntas para permitir que as entidades principais apropriadas do IAM usem a chave KMS para casos de uso específicos.
2. [Etapa 2: preparar as declarações de política de chave KMS](#) — Escolha modelos de declaração de política de chave KMS pertinentes com base nos casos de uso identificados na Etapa 1 e preencha os identificadores obrigatórios e os nomes da entidade principal do IAM. Comece com as declarações de política de chave KMS de linha de base e, se as políticas de segurança exigirem, refine-as conforme descrito nas declarações de política de chaves avançadas do KMS.
3. [Etapa 3: criar uma chave KMS gerenciada pelo cliente](#)— Crie uma chave KMS no AWS KMS que atenda aos requisitos do IAM Identity Center e adicione as declarações de política de chaves do KMS preparadas na Etapa 2 à política de chaves do KMS.
4. [Etapa 4: configurar políticas do IAM para o uso entre contas da chave KMS](#) — Escolha modelos de declaração de política do IAM pertinentes com base nos casos de uso identificados na Etapa 1 e prepare-os para uso preenchendo a chave ARN. Em seguida, permita que as entidades principais do IAM de cada caso de uso específico usem a chave KMS em todas as contas,

adicionando as declarações de política do IAM preparadas às políticas do IAM das entidades principais.

5. [Etapa 5: configurar a chave KMS no IAM Identity Center](#) — Habilite a chave KMS gerenciada pelo cliente na instância do IAM Identity Center para usá-la para criptografia em repouso.

Etapa 1: identificar casos de uso para a organização

Antes de criar e configurar a chave KMS gerenciada pelo cliente, identifique os casos de uso e prepare as permissões exigidas da chave KMS. Consulte o [Guia do desenvolvedor do AWS KMS](#) para obter mais informações sobre a política de chave KMS.

Os diretores do IAM que chamam o serviço IAM Identity Center APIs exigem permissões. Por exemplo, um administrador delegado pode ser autorizado a usá-los APIs por meio de uma política de conjunto de permissões. Quando o IAM Identity Center é configurado com uma chave gerenciada pelo cliente, os diretores do IAM também devem ter permissões para usar a API KMS por meio do serviço IAM Identity Center. APIs Você define essas permissões da API de KMS em dois lugares: na política de chave KMS e nas políticas do IAM associadas às entidades principais do IAM.

As permissões da chave KMS consistem em:

1. Declarações de política de chave KMS que você especifica na chave KMS durante a criação em [Etapa 3: criar uma chave KMS gerenciada pelo cliente](#).
2. Declarações de política do IAM para entidade principais do IAM que você especifica em [Etapa 4: configurar políticas do IAM para o uso entre contas da chave KMS](#) depois de criar a chave KMS.

A tabela a seguir especifica os casos de uso relevantes e as entidades principais do IAM que precisam de permissões para usar a chave KMS.

Caso de uso	Entidades principais do IAM que precisam de permissões para usar a chave KMS	Obrigatório/opcional
Uso do AWS IAM Identity Center	- Administradores do AWS IAM Identity Center - Serviço do IAM Identity Center e serviço do Identity Store associado	Obrigatório

Caso de uso	Entidades principais do IAM que precisam de permissões para usar a chave KMS	Obrigatório/ opcional
Uso de aplicativos AWS gerenciados com o IAM Identity Center	- Administradores de aplicativos AWS gerenciados - AWS aplicativos gerenciados Funções de serviço que os aplicativos AWS gerenciados assumem para chamar o serviço IAM Identity Center APIs	Opcional
Uso de AWS Control Tower na instância do AWS IAM Identity Center que ele habilitou	AWS Control Tower administradores	Opcional
SSO para instâncias do Amazon EC2 AWS com o IAM Identity Center	Diretores do IAM autorizados a realizar SSO para instâncias do Amazon EC2	Opcional
Qualquer outro caso de uso que faça chamadas para o serviço IAM Identity Center APIs com diretores do IAM, como aplicativos gerenciados pelo cliente, fluxos de trabalho de provisionamento de conjuntos de permissões ou funções AWS Lambda	Princípios do IAM usados por esses fluxos de trabalho para chamar o serviço IAM Identity Center APIs	Opcional

 Note

Vários diretores do IAM listados na tabela exigem permissões da API AWS KMS. No entanto, para proteger seus dados de usuários e grupos no IAM Identity Center, somente os serviços IAM Identity Center e Identity Store chamam diretamente a API AWS KMS.

Etapa 2: preparar as declarações de política de chave KMS

Depois de identificar os casos de uso relevantes para a organização, você pode preparar as declarações de política de chave KMS correspondentes.

1. Escolha as declarações de política de chave KMS que correspondam aos casos de uso da organização. Comece com os modelos de política de linha de base. Se você precisar de políticas mais específicas com base nos requisitos de segurança, poderá modificar as declarações de política usando os exemplos em [Declarações de política de chave KMS avançadas](#). Para obter orientação sobre essa decisão, consulte [Considerações sobre a escolha das declarações de política de chave KMS de linha de base em comparação com as avançadas](#). Além disso, cada seção de linha de base em [Declarações de chave KMS e de política do IAM de linha de base](#) inclui considerações relevantes.
2. Copie as políticas relevantes para um editor e insira os identificadores exigidos e os nomes das entidades principais do IAM nas declarações de política de chave KMS. Para obter ajuda para encontrar os valores dos identificadores referenciados, consulte [Onde encontrar os identificadores necessários](#).

A seguir estão os modelos de política de linha de base para cada caso de uso. Somente o primeiro conjunto de permissões do AWS IAM Identity Center é necessário para usar uma chave KMS. Recomendamos analisar as subseções aplicáveis para obter informações adicionais específicas do caso de uso.

- [Declarações da política de chave KMS de linha de base para uso do IAM Identity Center \(obrigatório\)](#)
- [Chave básica do KMS e declarações de política do IAM para uso de AWS aplicativos gerenciados](#)
- [Declaração chave básica do KMS para uso de AWS Control Tower](#)
- [Chave básica do KMS e declarações de política do IAM para uso do IAM Identity Center em instâncias do Amazon EC2](#)
- [Chave KMS de linha de base e declarações de política do IAM para uso de fluxos de trabalho personalizados com o IAM Identity Center](#)

Important

Tenha cuidado ao modificar as políticas de chave KMS para chaves já em uso pelo IAM Identity Center. Embora o IAM Identity Center valide as permissões de criptografia e descryptografia quando você configura inicialmente uma chave KMS, ele não pode verificar

alterações de política subsequentes. A remoção inadvertida das permissões necessárias pode interromper a operação normal do IAM Identity Center. Para obter orientação sobre como solucionar erros comuns relacionados às chaves gerenciadas pelo cliente no IAM Identity Center, consulte [Solucione problemas de chaves gerenciadas pelo cliente em Centro de Identidade do AWS IAM](#).

Note

O IAM Identity Center e o Identity Store associado exigem permissões de nível de serviço para usar a chave KMS gerenciada pelo cliente. Esse requisito se estende aos aplicativos AWS gerenciados que chamam o serviço IAM Identity Center APIs usando credenciais de serviço. Para outros casos de uso em que o serviço IAM Identity Center APIs é chamado com [sessões de acesso direto](#), somente o principal do IAM iniciante (como um administrador) precisa de permissões de chave KMS. Notavelmente, os usuários finais que usam o portal de AWS acesso e os aplicativos AWS gerenciados não precisam de permissões diretas da chave KMS, pois elas são concedidas por meio dos respectivos serviços.

Etapa 3: criar uma chave KMS gerenciada pelo cliente

Você pode criar uma chave gerenciada pelo cliente usando o AWS Management Console ou o AWS KMS. APIs Ao criar a chave, adicione as declarações de política de chave KMS que você preparou na Etapa 2 à política de chave KMS. Para obter instruções detalhadas, incluindo orientações sobre a política de chave padrão do KMS, consulte o [Guia do desenvolvedor do AWS Key Management Service](#).

A chave deve atender aos seguintes requisitos:

- A chave KMS deve estar na mesma AWS região da instância do IAM Identity Center
- Você pode criar um cluster de região única ou multirregional. No entanto, se você planeja usar o IAM Identity Center em vários, Regiões da AWS você deve criar uma chave KMS multirregional. Você não pode converter uma chave KMS de região única em uma de várias regiões, portanto, recomendamos começar com uma chave KMS de várias regiões, a menos que você tenha requisitos específicos para usar uma chave KMS de região única.
- A chave KMS deve ser uma chave simétrica configurada para o uso de “criptografar e descriptografar”

- A chave KMS deve estar na mesma conta AWS Organizations de gerenciamento da instância organizacional do IAM Identity Center

 Note

Se você planeja replicar essa chave do KMS para regiões nas quais deseja replicar sua Central de Identidades do IAM, recomendamos que você primeiro conclua a configuração nesta seção e, em seguida, siga as orientações em [the section called “Replique o IAM Identity Center para uma região adicional”](#)

Etapa 4: configurar políticas do IAM para o uso entre contas da chave KMS

Qualquer diretor do IAM que usa o serviço IAM Identity Center APIs de outra AWS conta, como administradores delegados do IAM Identity Center, também precisa de uma declaração de política do IAM que permita o uso da chave KMS por meio deles. APIs

Para cada caso de uso identificado na etapa 1:

1. Localize os modelos de declaração de política do IAM pertinentes na chave KMS da linha de base e nas declarações de política do IAM.
2. Copie os modelos para um editor e preencha a chave ARN, que agora está disponível após a criação da chave KMS na etapa 3. Para obter ajuda para encontrar o valor ARN da chave, consulte [Onde encontrar os identificadores necessários](#).
3. No Console de gerenciamento da AWS, localize a política do IAM do principal do IAM que está associada ao caso de uso. O local da política varia de acordo com o caso de uso e como o acesso é concedido.
 - Para o acesso concedido diretamente no IAM, você pode localizar as entidades principais do IAM, como perfis do IAM no console do IAM.
 - Para acesso concedido pelo IAM Identity Center, você pode localizar o conjunto de permissões pertinente no console do IAM Identity Center.
4. Adicione as declarações de política do IAM específicas do caso de uso ao perfil do IAM e salve a alteração.

 Note

As políticas do IAM descritas aqui são políticas baseadas em identidade. Embora essas políticas possam ser anexadas a usuários, grupos e perfis do IAM, recomendamos o uso de perfis do IAM sempre que possível. Consulte o Guia do Usuário do IAM para obter mais informações sobre perfis do IAM versus usuários do IAM.

Configuração adicional em alguns aplicativos AWS gerenciados

Alguns aplicativos AWS gerenciados exigem que você configure uma função de serviço para permitir que os aplicativos usem o serviço IAM Identity Center APIs. Se sua organização usa aplicativos AWS gerenciados com o IAM Identity Center, conclua as etapas a seguir para cada aplicativo implantado:

1. Consulte o guia do usuário da aplicação para confirmar se as permissões foram atualizadas para incluir permissões relacionadas à chave KMS para uso da aplicação com o IAM Identity Center.
2. Nesse caso, atualize as permissões conforme as instruções no guia do usuário do @aplicação para evitar interrupções nas operações da aplicação.

 Note

Se você não tiver certeza se um aplicativo AWS gerenciado usa essas permissões, recomendamos que você verifique os guias do usuário de todos os aplicativos AWS gerenciados implantados. Você só precisa realizar essa configuração uma vez para cada aplicação que requer a configuração.

Etapas 5: configurar a chave KMS no IAM Identity Center

 Important

Antes de prosseguir com esta etapa:

- Verifique se seus aplicativos AWS gerenciados são compatíveis com as chaves KMS gerenciadas pelo cliente. Para obter uma lista de aplicações compatíveis, consulte [Aplicações gerenciadas pela AWS que você pode usar com o IAM Identity Center](#). Se você tiver aplicações incompatíveis, não continue.

- Configure as permissões necessárias para o uso da chave KMS. Sem as permissões adequadas, essa etapa pode falhar ou interromper a administração do IAM Identity Center, o uso de aplicações gerenciadas pela AWS e outros casos de uso que exigem permissões de chave KMS. Para obter mais informações, consulte [Etapa 1: identificar casos de uso para a organização](#).
- Certifique-se de que as permissões para aplicativos AWS gerenciados e aplicativos gerenciados pelo cliente que chamam o serviço IAM Identity Center APIs com funções do IAM também permitam o uso da chave KMS por meio do serviço APIs IAM Identity Center. Alguns aplicativos AWS gerenciados exigem que você configure permissões, como uma função de serviço, para o uso deles APIs. Consulte o Guia do usuário de cada aplicativo AWS gerenciado implantado para confirmar se você precisa adicionar permissões específicas da chave KMS.

Especificar uma chave KMS ao habilitar uma nova instância de organização do IAM Identity Center

Ao habilitar uma nova instância de organização do IAM Identity Center, você pode especificar uma chave KMS gerenciada pelo cliente durante a configuração. Isso garante que a instância use a chave para criptografia em repouso desde o início. Antes de começar, consulte [Considerações sobre chaves KMS gerenciadas pelo cliente e políticas avançadas de chaves KMS](#).

1. Na página Habilitar IAM Identity Center, expanda a seção Criptografia em repouso.
2. Escolha Manage Encryption (Gerenciar criptografia).
3. Escolha Chave gerenciada pelo cliente.
4. Em Chave KMS, realize um destes procedimentos:
 - a. Escolha Selecionar nas chaves KMS e selecione a chave que você criou na lista suspensa.
 - b. Escolha Inserir ARN da chave KMS e insira o ARN completo da chave.
5. Escolha Salvar.
6. Escolha Habilitar para concluir a configuração.

Para obter mais informações, consulte [Habilitar o IAM Identity Center](#).

Alterar a configuração de chaves para uma instância de organização existente do IAM Identity Center

Você pode alterar a chave KMS gerenciada pelo cliente para outra chave ou mudar para uma chave de propriedade da AWS a qualquer momento.

Console

Para alterar a configuração da chave KMS

1. Abra o console do IAM Identity Center em <https://console.aws.amazon.com/singlesignon/>.
2. No painel de navegação, selecione Configurações.
3. Selecione a guia Configurações adicionais.
4. Escolha Gerenciar criptografia.
5. Escolha uma das seguintes opções:
 - a. Chave gerenciada pelo cliente — Selecione uma chave gerenciada pelo cliente diferente na lista suspensa ou insira um novo ARN da chave.
 - b. AWS chave própria - Mude para a opção de criptografia padrão.
6. Escolha Salvar.

AWS CLI

Para alterar uma instância de organização existente do IAM Identity Center para usar a chave KMS gerenciada pelo cliente

```
aws sso-admin update-instance \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --encryption-configuration \  
    KeyType=CUSTOMER_MANAGED_KEY,KmsKeyArn=arn:aws:kms:us-  
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Para alterar uma instância de organização existente do IAM Identity Center para usar a chave de propriedade da AWS

```
aws sso-admin update-instance \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --encryption-configuration KeyType=AWS_OWNED_KMS_KEY
```

Considerações sobre chave gerenciada pelo cliente

- Atualizar a configuração da chave KMS para a operação do IAM Identity Center não tem efeito nas sessões ativas do usuário no IAM Identity Center. Você pode continuar usando o portal de

AWS acesso, o console do IAM Identity Center e o serviço IAM Identity Center APIs durante esse processo.

- Ao mudar para uma nova chave KMS, o IAM Identity Center valida que pode usar a chave com sucesso para criptografia e descriptografia. Se você cometeu um erro durante a configuração da política de chave ou da política do IAM, o console mostrará uma mensagem de erro explicativa e a chave KMS anterior permanecerá em uso.
- A rotação anual padrão de chaves KMS ocorrerá automaticamente. Você pode consultar o [Guia do desenvolvedor do AWS KMS](#) para obter informações sobre tópicos como [rotação de chaves](#), [monitoramento de chaves AWS KMS](#) e [controle do acesso à exclusão de chaves](#).

Important

Se a chave KMS gerenciada pelo cliente em uso pela instância do IAM Identity Center for excluída, desabilitada ou tornar-se inacessível devido a uma política de chave KMS incorreta, os usuários da força de trabalho e os administradores do IAM Identity Center não poderão usar o IAM Identity Center. A perda de acesso pode ser temporária (uma política de chave pode ser corrigida) ou permanente (uma chave excluída não pode ser restaurada), dependendo das circunstâncias. Recomendamos que você [restringa o acesso](#) a operações críticas, como excluir ou desativar a chave KMS. Além disso, recomendamos que sua organização configure [procedimentos de acesso AWS rápidos](#) para garantir que seus usuários privilegiados possam acessar AWS caso o IAM Identity Center esteja inacessível.

Onde encontrar os identificadores necessários

Ao configurar as permissões para a chave KMS gerenciada pelo cliente, você precisará de identificadores de recursos da AWS específicos para atender à política de chave e os modelos de declaração de política do IAM. Insira os identificadores exigidos (por exemplo, ID da organização) e os nomes das entidades principais do IAM nas declarações de política de chave KMS.

Abaixo está um guia para localizar esses identificadores no AWS Management Console.

IAM Identity Center: nome do recurso da Amazon (ARN) e ARN do Identity Store

Uma instância do IAM Identity Center é um AWS recurso com seu próprio ARN exclusivo, como `arn:aws:sso::instance/ssoins-1234567890abcdef`. O ARN segue o padrão documentado na seção de tipos de recursos do IAM Identity Center da Referência de autorização de serviço.

Cada instância do IAM Identity Center tem um Identity Store associado que armazena as identidades do usuário e do grupo. Um Identity Store tem um identificador exclusivo chamado Identity Store ID (por exemplo, d-123456789a). O ARN segue o padrão documentado na seção Tipos de recursos do Identity Store da [Referência de autorização de serviço](#).

Você pode encontrar os valores do ARN e do ID do Identity Store na página Configurações do IAM Identity Center. O ID do repositório de identidades está na aba Fonte de identidade.

AWS Organizations ID

Se você quiser especificar um ID da organização (por exemplo, o-exampleorg1) na política de chave, pode encontrar o valor na página Configurações dos consoles IAM Identity Center e Organizations. O ARN segue o padrão documentado na seção Tipos de recursos do Organizations da Referência de autorização de serviço.

ARN da chave KMS

Você pode encontrar o ARN de uma chave KMS no console. AWS KMS Escolha Chaves gerenciadas pelo cliente à esquerda, clique na chave cujo ARN você deseja pesquisar e você a verá na seção Configuração geral. O ARN segue o padrão documentado na seção de tipos de AWS KMS recursos da Referência de Autorização de Serviço.

Consulte o Guia do AWS Key Management Service desenvolvedor para obter mais informações sobre as principais políticas AWS KMS e a solução de problemas de AWS KMS permissões. Para obter mais informações sobre as políticas do IAM e a representação em JSON, consulte o Guia do usuário do IAM.

Declarações de chave KMS e de política do IAM de linha de base

A chave KMS de linha de base e as políticas baseadas em identidade fornecidas aqui servem como base para requisitos comuns. Também recomendamos que você revise se [Declarações de política de chave KMS avançadas](#) fornece controles de acesso mais granulares, como garantir que a chave KMS seja acessível somente para uma instância específica do IAM Identity Center ou aplicação gerenciada pela AWS. Antes de usar declarações avançadas de política de chave KMS, revise [Considerações sobre a escolha das declarações de política de chave KMS de linha de base em comparação com as avançadas](#).

As seções a seguir fornecem declarações de política de linha de base para cada caso de uso. Expanda as seções que correspondem aos seus casos de uso e copie as principais declarações de política do KMS. Em seguida, volte para [Etapa 2: preparar as declarações de política de chave KMS](#).

Declarações da política de chave KMS de linha de base para uso do IAM Identity Center (obrigatório)

Use o seguinte modelo de declaração de política de chave KMS em [Etapa 2: preparar as declarações de política de chave KMS](#) para permitir que os administradores do IAM Identity Center, do Identity Store associado e do IAM Identity Center usem a chave KMS.

- No elemento Principal das declarações de política do administrador, especifique os diretores das contas de administração do IAM Identity Center, que são a AWS conta de gerenciamento da AWS organização e a conta de administração delegada, usando o formato "arn:aws:iam: :111122223333:root".
- No PrincipalArn elemento, substitua o exemplo pelas ARNs funções do IAM dos administradores do IAM Identity Center.

Você pode especificar:

- ARN específico de perfil do IAM:

```
"arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/ap-southeast-2/AWSReservedSSO_permsetname_12345678"
```

- Padrão curinga (recomendado):

```
"arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/ap-southeast-2/AWSReservedSSO_permsetname_*"
```

O uso do curinga (*) evita a perda de acesso se o conjunto de permissões for excluído e recriado, pois o Identity Center gera novos identificadores exclusivos para conjuntos de permissões recriados. Para ver um exemplo de implementação, consulte [Exemplos de políticas personalizadas](#).

- No SourceAccount elemento, especifique o ID da conta do IAM Identity Center.
- O Identity Store tem a própria entidade principal de serviço, `identitystore.amazonaws.com`, que deve ter permissão para usar a chave KMS.
- Essas declarações de política permitem que suas instâncias do IAM Identity Center em uma AWS conta específica usem a chave KMS. Para restringir o acesso a uma instância específica do IAM Identity Center, consulte [Declarações de política de chave KMS avançadas](#). Você pode ter somente uma instância do IAM Identity Center para cada AWS conta.

Declarações de política de chave KMS

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:root",
        "arn:aws:iam::444455556666:root"
      ]
    },
    "Action": [
      "kms:Decrypt",
      "kms:Encrypt",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
      "ArnLike": {
        "aws:PrincipalArn": [
          "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
          "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_"
        ]
      }
    },
    "StringLike": {
      "kms:ViaService": "sso.*.amazonaws.com",
      "kms:EncryptionContext:aws:sso:instance-arn": "*"
    }
  }
],
{
  "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityStore",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:root",
      "arn:aws:iam::444455556666:root"
    ]
  },
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt",

```

```

    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
        "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
      ]
    }
  },
  "StringLike": {
    "kms:ViaService": "identitystore.*.amazonaws.com",
    "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
  }
},
{
  "Sid": "AllowIAMIdentityCenterAdminToDescribeTheKMSKey",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:root",
      "arn:aws:iam::444455556666:root"
    ]
  },
  "Action": "kms:DescribeKey",
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
        "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
      ]
    }
  }
},
{
  "Sid": "AllowIAMIdentityCenterToUseTheKMSKey",
  "Effect": "Allow",
  "Principal": {

```

```

    "Service": "sso.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:ReEncryptTo",
    "kms:ReEncryptFrom",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:sso:instance-arn": "*"
    },
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    }
  }
},
{
  "Sid": "AllowIdentityStoreToUseTheKMSKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "identitystore.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:ReEncryptTo",
    "kms:ReEncryptFrom",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    },
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    }
  }
},
{
  "Sid": "AllowIAMIdentityCenterAndIdentityStoreToDescribeKMSKey",
  "Effect": "Allow",
  "Principal": {

```

```

    "Service": [
      "identitystore.amazonaws.com",
      "sso.amazonaws.com"
    ],
    "Action": "kms:DescribeKey",
    "Resource": "*"
  }
]
}

```

Use o seguinte modelo de declaração de política do IAM em [the section called “Etapa 4: configurar políticas do IAM”](#) para permitir que os administradores do IAM Identity Center usem a chave KMS.

- Substitua o exemplo da chave ARN no elemento Resource pelo ARN real da chave KMS. Para obter ajuda para encontrar os valores dos identificadores referenciados, consulte [Onde encontrar os identificadores necessários](#).
- Essas declarações de política do IAM concedem acesso à chave KMS ao principal do IAM, mas não restringem qual AWS serviço pode fazer a solicitação. A política de chave KMS normalmente fornece essas restrições de serviço. No entanto, você pode adicionar contexto de criptografia a essa política do IAM para limitar o uso a uma instância específica do Identity Center. Para obter detalhes, consulte [Declarações de política de chave KMS avançadas](#).

Declarações de política do IAM exigidas para administradores delegados do IAM Identity Center

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "IAMPolicyToAllowIAMIdentityCenterAdminToUseKMSkey",
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:GenerateDataKeyWithoutPlaintext",
      "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  {
    "Sid": "IAMPolicyToAllowIAMIdentityCenterAdminToListKeyAliases",

```

```
"Effect": "Allow",
"Action": "kms:ListAliases",
"Resource": "*"
}
]
```

Chave básica do KMS e declarações de política do IAM para uso de AWS aplicativos gerenciados

 Note

Alguns aplicativos AWS gerenciados não podem ser usados com o IAM Identity Center configurado com uma chave KMS gerenciada pelo cliente. Para obter mais informações, consulte as [Aplicações gerenciadas pela AWS que funcionam com o IAM Identity Center](#).

Use o seguinte modelo de declaração de política de chaves do KMS [Etapa 2: preparar as declarações de política de chave KMS](#) para permitir que os aplicativos AWS gerenciados e seus administradores usem a chave KMS.

- Insira seu AWS Organizations ID no PrincipalOrg ID e SourceOrgId nas condições. Para obter ajuda para encontrar os valores dos identificadores referenciados, consulte [Onde encontrar os identificadores necessários](#).
- Essas declarações de política permitem que qualquer um dos seus aplicativos AWS gerenciados e quaisquer diretores do IAM (administradores de aplicativos) na AWS organização usem o kms: Decrypt usando o IAM Identity Center e o Identity Store. Para restringir essas declarações de política a aplicações gerenciadas pela AWS específicas, contas ou instâncias do IAM Identity Center, consulte [Declarações de política de chave KMS avançadas](#).

Você pode restringir o acesso a administradores de aplicações específicas substituindo o * pelas entidades principais específicas do IAM. Para se proteger contra alterações no nome do perfil do IAM quando os conjuntos de permissões são recriados, use a abordagem mostrada em [Exemplos de políticas personalizadas](#). Para obter mais informações, consulte [Considerações sobre a escolha das declarações de política de chave KMS de linha de base em comparação com as avançadas](#).

Declarações de política de chave KMS

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



```
"Statement": [  
  {  
    "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityCenter",  
    "Effect": "Allow",  
    "Principal": "*",  
    "Action": "kms:Decrypt",  
    "Resource": "*",  
    "Condition": {  
      "StringEquals": {  
        "aws:PrincipalOrgID": "o-a1b2c3d4e5"  
      },  
      "StringLike": {  
        "kms:ViaService": "sso.*.amazonaws.com",  
        "kms:EncryptionContext:aws:sso:instance-arn": ""  
      }  
    }  
  },  
  {  
    "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityStore",  
    "Effect": "Allow",  
    "Principal": "*",  
    "Action": "kms:Decrypt",  
    "Resource": "*",  
    "Condition": {  
      "StringEquals": {  
        "aws:PrincipalOrgID": "o-a1b2c3d4e5"  
      },  
      "StringLike": {  
        "kms:ViaService": "identitystore.*.amazonaws.com",  
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": ""  
      }  
    }  
  },  
  {  
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityCenter",  
    "Effect": "Allow",  
    "Principal": "*",  
    "Action": "kms:Decrypt",  
    "Resource": "*",  
    "Condition": {  
      "StringLike": {  
        "kms:ViaService": "sso.*.amazonaws.com",  
        "kms:EncryptionContext:aws:sso:instance-arn": ""  
      }  
    }  
  },  
]
```

```

    "Bool": {
      "aws:PrincipalIsAWSService": "true"
    },
    "StringEquals": {
      "aws:SourceOrgID": "o-a1b2c3d4e5"
    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
      }
    }
  }
]
}

```

Use o seguinte modelo de declaração de política do IAM [Etapa 4: configurar políticas do IAM para o uso entre contas da chave KMS](#) para permitir que administradores de aplicações gerenciadas pela AWS usem a chave KMS de uma conta de membro.

- Substitua o ARN de exemplo no elemento Resource pelo ARN real da chave KMS. Para obter ajuda para encontrar os valores dos identificadores referenciados, consulte [Onde encontrar os identificadores necessários](#).
- Alguns aplicativos AWS gerenciados exigem que você configure permissões para o serviço IAM Identity Center APIs. Antes de configurar uma chave gerenciada pelo cliente no IAM Identity Center, verifique se essas permissões também permitem o uso da chave KMS. Para requisitos

específicos de permissão da chave KMS, consulte a documentação de cada aplicação gerenciada pela AWS que você implantou.

Declarações de política do IAM necessárias para administradores de aplicativos AWS gerenciados:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid":
    "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }]
}
```

Declaração chave básica do KMS para uso de AWS Control Tower

Use os seguintes modelos de declaração de chave KMS [Etapa 2: preparar as declarações de política de chave KMS](#) para permitir que os administradores do AWS Control Tower usem a chave KMS.

- No elemento Principal, especifique os principais do IAM usados para acessar o serviço APIs do IAM Identity Center. Para obter mais informações sobre as entidades principais do IAM, consulte [Como especificar uma entidade principal](#) no Guia do usuário do IAM.
- Essas declarações de política permitem que os administradores do AWS Control Tower usem a chave KMS por meio de qualquer uma das suas instâncias do IAM Identity Center. No entanto, AWS o Control Tower restringe o acesso à instância organizacional do IAM Identity Center na mesma AWS organização. Por causa dessa restrição, não há nenhum benefício prático em restringir ainda mais a chave KMS a uma instância específica do IAM Identity Center, conforme descrito em. [Declarações de política de chave KMS avançadas](#)

- Para ajudar a se proteger contra alterações no nome da função do IAM quando os conjuntos de permissões são recriados, use a abordagem descrita no [Exemplos de políticas personalizadas](#).

Declaração de política de chaves do KMS:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowControlTowerAdminRoleToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/AWSControlTowerAdmin"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    },
    {
      "Sid": "AllowControlTowerAdminRoleToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/AWSControlTowerAdmin"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
      }
    }
  ]
}
```

AWS Control Tower não oferece suporte à administração delegada e, portanto, você não precisa configurar uma política do IAM para seus administradores.

Important

A declaração de política anterior abrange operações AWS Control Tower gerenciadas por serviços, como inscrição automática de contas, onde AWS Control Tower assume a função. `AWSControlTowerAdmin` No entanto, para operações iniciadas pelo cliente, como provisionar contas por meio do Account Factory ou ligar AWS Control Tower APIs diretamente, AWS Control Tower usa [sessões de acesso direto \(FAS\)](#) e opera sob a função IAM do próprio cliente. Isso significa que a função do IAM que você usa para iniciar essas operações também precisa de `kms:Decrypt` permissões na chave KMS gerenciada pelo cliente.

Adicione as seguintes declarações de política chave do KMS ao lado das `AWSControlTowerAdmin` declarações acima. *MyControlTowerRole* Substitua pelo ARN da função do IAM com a qual você usa para interagir AWS Control Tower, como uma função do conjunto de permissões do IAM Identity Center (por exemplo, `AWSReservedSSO_PermissionSetName_*`), uma função personalizada do IAM para automação ou qualquer outra função usada para chamar AWS Control Tower ou. AWS Service Catalog APIs

Declaração de política chave do KMS para operações iniciadas pelo cliente AWS Control Tower :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomerRoleToUseTheKMSKeyViaIdentityCenterForControlTower",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyControlTowerRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid": "AllowCustomerRoleToUseTheKMSKeyViaIdentityStoreForControlTower",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/MyControlTowerRole"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  }
]
}

```

Chave básica do KMS e declarações de política do IAM para uso do IAM Identity Center em instâncias do Amazon EC2

Use o seguinte modelo de declaração de política de chaves do KMS [Etapa 2: preparar as declarações de política de chave KMS](#) para permitir que usuários de login único (SSO) nas instâncias do Amazon EC2 usem a chave KMS em todas as contas.

- Especifique as entidades principais do IAM usadas para acessar o IAM Identity Center no campo Entidade principal. Para obter mais informações sobre as entidades principais do IAM, consulte [Como especificar uma entidade principal](#) no Guia do usuário do IAM.
- Essa declaração de política permite que qualquer uma das instâncias do IAM Identity Center use a chave KMS. Para restringir o acesso a uma instância específica do IAM Identity Center, consulte [Declarações de política de chave KMS avançadas](#).
- Para ajudar a se proteger contra alterações no nome do perfil do IAM quando os conjuntos de permissões são recriados, use a abordagem descrita no Exemplo de política de confiança personalizada.

Declaração de política de chaves do KMS

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowIAMIdentityCenterPermissionSetRoleToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_MyPermissionSet_1a2b3c4d5e6f7g8h"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowIAMIdentityCenterPermissionSetRoleToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_MyPermissionSet_1a2b3c4d5e6f7g8h"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  }
]
}

```

Use o seguinte modelo de declaração de política do IAM [Etapa 4: configurar políticas do IAM para o uso entre contas da chave KMS](#) para permitir que o SSO para instâncias do EC2 usem a chave KMS.

Anexe a declaração de política do IAM ao conjunto de permissões existente no IAM Identity Center que você está usando para permitir o acesso por SSO às instâncias do Amazon EC2. Para exemplos de políticas do IAM, consulte [Conexões do protocolo de desktop remoto](#) no Guia do usuário do AWS Systems Manager.

- Substitua o ARN de exemplo no elemento Resource pelo ARN real da chave KMS. Para obter ajuda para encontrar os valores dos identificadores referenciados, consulte [Onde encontrar os identificadores necessários](#).

Política do IAM do conjunto de permissões:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "IAMPolicyToAllowKMSKeyUseViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }]
}
```

Chave KMS de linha de base e declarações de política do IAM para uso de fluxos de trabalho personalizados com o IAM Identity Center

Use os seguintes modelos de declaração de política de chaves do KMS [Etapa 2: preparar as declarações de política de chave KMS](#) para permitir que fluxos de trabalho personalizados, como aplicativos gerenciados pelo cliente, na conta de AWS Organizations gerenciamento ou na conta de administração delegada usem a chave KMS. Observe que a federação do SAML em aplicativos gerenciados pelo cliente não exige permissões de chave KMS.

- No elemento Principal, especifique os principais do IAM usados para acessar o serviço APIs do IAM Identity Center. Para obter mais informações sobre as entidades principais do IAM, consulte [Como especificar uma entidade principal](#) no Guia do usuário do IAM.
- Essas declarações de política permitem que o fluxo de trabalho use a chave KMS em qualquer uma das instâncias do IAM Identity Center. Para restringir o acesso a uma instância específica do IAM Identity Center, consulte [Declarações de política de chave KMS avançadas](#).
- Para ajudar a se proteger contra alterações no nome da função do IAM quando os conjuntos de permissões são recriados, use a abordagem descrita no [Exemplos de políticas personalizadas](#).

Declaração de política de chaves do KMS:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyCustomWorkflowRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "*"
        }
      }
    },
    {
      "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyCustomWorkflowRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
        }
      }
    }
  ]
}
```

```

    }
  }
}
]
}

```

Use o seguinte modelo de declaração de política do IAM em [Etapa 4: configurar políticas do IAM para o uso entre contas da chave KMS](#) para permitir que a entidade principal do IAM associada ao fluxo de trabalho personalizado use a chave KMS em todas as contas. Adicione a declaração de política do IAM à entidade principal do IAM.

- Substitua o ARN de exemplo no elemento Resource pelo ARN real da chave KMS. Para obter ajuda para encontrar os valores dos identificadores referenciados, consulte [Onde encontrar os identificadores necessários](#).

Declaração de política do IAM (exigida somente para uso entre contas):

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowCustomWorkflowToUseTheKMSKeyViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "Condition": {
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      }
    }
  }]
}

```

Exemplos de declarações de política chave do KMS para casos de uso comuns

IAM Identity Center com administradores delegados e AWS aplicativos gerenciados

Esta seção contém exemplos de declarações de política de chaves do KMS que você pode usar para uma instância do IAM Identity Center que tenha administradores delegados e AWS aplicativos gerenciados.

Important

As declarações de política de chaves do KMS presumem que sua instância do IAM Identity Center não é usada em nenhum outro caso de uso que exija permissões de chave do KMS. Para confirmar, você pode analisar todos os [casos de uso](#). Além disso, para confirmar se seus aplicativos AWS gerenciados exigem configuração adicional, consulte [the section called “Configuração adicional em alguns aplicativos AWS gerenciados”](#)

Copie as declarações da política de chaves do KMS abaixo da tabela e adicione-as à sua política de chaves do KMS. Este exemplo usa os seguintes valores de exemplo:

- 111122223333- ID da conta da instância do IAM Identity Center
- 444455556666- ID da conta de administração delegada
- o-a1b2c3d4e5- ID AWS da organização
- `arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*`- Um padrão curinga da função IAM de um administrador do IAM Identity Center provisionado a partir do conjunto de permissões. *Admin* Essa função contém o código de região da região primária (us-east-1 neste exemplo).
- `arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*`- Um padrão curinga da função IAM de administrador delegado do IAM Identity Center provisionado a partir do conjunto de permissões. *DelegatedAdmin* Essa função contém o código de região da região primária (us-east-1 neste exemplo).

Se a função do IAM não foi gerada a partir de um conjunto de permissões, a função do IAM parecerá uma função normal, como `arn:aws:iam::111122223333:role/idcadmin`.

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:root",
        "arn:aws:iam::444455556666:root"
      ]
    },
    "Action": [
      "kms:Decrypt",
      "kms:Encrypt",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
      "ArnLike": {
        "aws:PrincipalArn": [
          "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_Admin_*",
          "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/AWSReservedSSO_DelegatedAdmin_*"
        ]
      }
    },
    "StringLike": {
      "kms:ViaService": "sso.*.amazonaws.com",
      "kms:EncryptionContext:aws:sso:instance-arn": "*"
    }
  }
],
{
  "Sid": "AllowIAMIdentityCenterAdminToUseTheKMSKeyViaIdentityStore",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:root",
      "arn:aws:iam::444455556666:root"
    ]
  },
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt",

```

```

    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
        "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
      ]
    }
  },
  "StringLike": {
    "kms:ViaService": "identitystore.*.amazonaws.com",
    "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
  }
},
{
  "Sid": "AllowIAMIdentityCenterAdminToDescribeTheKMSKey",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:root",
      "arn:aws:iam::444455556666:root"
    ]
  },
  "Action": "kms:DescribeKey",
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_Admin_*",
        "arn:aws:iam::444455556666:role/aws-reserved/sso.amazonaws.com/us-east-1/
AWSReservedSSO_DelegatedAdmin_*"
      ]
    }
  }
},
{
  "Sid": "AllowIAMIdentityCenterToUseTheKMSKey",
  "Effect": "Allow",
  "Principal": {

```

```

    "Service": "sso.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:ReEncryptTo",
    "kms:ReEncryptFrom",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:sso:instance-arn": "*"
    },
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    }
  }
},
{
  "Sid": "AllowIdentityStoreToUseTheKMSKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "identitystore.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:ReEncryptTo",
    "kms:ReEncryptFrom",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
    },
    "StringEquals": {
      "aws:SourceAccount": "111122223333"
    }
  }
},
{
  "Sid": "AllowIAMIdentityCenterAndIdentityStoreToDescribeKMSKey",
  "Effect": "Allow",
  "Principal": {

```

```

    "Service": [
      "identitystore.amazonaws.com",
      "sso.amazonaws.com"
    ],
    "Action": "kms:DescribeKey",
    "Resource": "*"
  },
  {
    "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-a1b2c3d4e5"
      },
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowAppAdminsInTheSameOrganizationToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-a1b2c3d4e5"
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      }
    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityCenter",
    "Effect": "Allow",

```

```

    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "*"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
      }
    }
  },
  {
    "Sid": "AllowManagedAppsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn": "*"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "o-a1b2c3d4e5"
      }
    }
  }
]
}

```

Declarações de política de chave KMS avançadas

Use declarações de política de chave KMS avançadas para implementar controles de acesso mais granulares para a chave KMS gerenciada pelo cliente. Essas políticas se baseiam em [Declarações de chave KMS e de política do IAM de linha de base](#) adicionando condições de contexto de

criptografia e restrições específicas do serviço. Antes de decidir se você deve usar declarações de política de chave KMS avançadas, analise as considerações pertinentes.

Como usar o contexto de criptografia para restringir o acesso

Você pode restringir o uso da chave KMS a uma instância específica do IAM Identity Center especificando uma condição de contexto de criptografia nas declarações de política de chave. As declarações políticas de chave de linha de base já incluem esse contexto com um valor genérico. Substitua o caractere curinga “*” por um ARN específico da instância do Identity Center e pelo ARN do Identity Store para garantir que a chave funcione somente com a instância pretendida. Você também pode adicionar as mesmas condições de contexto de criptografia à política do IAM configurada para o uso entre contas da chave KMS.

Identity Center

```
"StringEquals": {
  "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
}
```

Armazenamento de identidades

```
"StringEquals": {
  "kms:EncryptionContext:aws:identitystore:identitystore-arn":
  "arn:aws:identitystore:::111122223333:identitystore/d-1234567890"
}
```

Se precisar de ajuda para encontrar esses identificadores, consulte [Onde encontrar os identificadores necessários](#).

Note

Você pode usar uma chave KMS gerenciada pelo cliente somente com uma instância de organização do IAM Identity Center. A chave gerenciada pelo cliente deve estar localizada na conta de gerenciamento da AWS organização, o que ajuda a garantir que a chave seja usada com uma única instância do IAM Identity Center. No entanto, o mecanismo de contexto de criptografia fornece uma proteção técnica independente do uso de uma única

instância. Você também pode usar a chave de condição `aws:SourceArn` nas declarações de política de chave KMS destinadas às entidades principais de serviço do Identity Center e do Identity Store.

Considerações para implementar condições de contexto de criptografia

Antes de implementar as condições de contexto de criptografia, analise estes requisitos:

- **DescribeKey ação.** O contexto de criptografia não pode ser aplicado à ação `kms:DescribeKey`, que pode ser usada pelos administradores do IAM Identity Center. Ao configurar a política de chave KMS, exclua o contexto de criptografia dessa ação específica para garantir as operações adequadas da instância do IAM Identity Center.
- **Configuração da nova instância.** Se for habilitar uma nova instância do IAM Identity Center com uma chave KMS gerenciada pelo cliente, consulte [Considerações sobre chaves KMS gerenciadas pelo cliente e políticas avançadas de chaves KMS](#).
- **Alterações na fonte de identidade.** Ao alterar a fonte de identidade de ou para o Active Directory, o contexto de criptografia requer atenção especial. Consulte [Considerações para alterar sua fonte de identidade](#).

Modelos de políticas

Escolha entre esses modelos de política avançada com base nos requisitos de segurança. Equilibre os controles de acesso granulares com a sobrecarga administrativa que eles introduzem.

Tópicos abordados aqui:

- [Declarações de política do KMS para uso somente para leitura de uma instância específica do IAM Identity Center](#). Esta seção demonstra o uso do contexto de criptografia para acesso somente leitura ao IAM Identity Center.
- [Declarações de política chave do KMS refinadas para uso de aplicativos AWS gerenciados](#). Esta seção demonstra como refinar as políticas de chaves do KMS para aplicativos AWS gerenciados usando o contexto de criptografia e as informações do aplicativo, como o principal do serviço do aplicativo, o ARN do aplicativo e o ID da conta. AWS

Declarações de política do KMS para uso somente para leitura de uma instância específica do IAM Identity Center

Essa política permite que [auditores de segurança](#) e outros funcionários que precisam apenas de acesso de leitura ao IAM Identity Center usem a chave KMS.

Para usar essa política:

1. Substituir as amostras de entidades principais do IAM de administrador somente leitura pelas entidades principais do IAM de administrador reais
2. Substituir o exemplo de ARN da instância do IAM Identity Center pelo ARN da instância real
3. Substituir o exemplo do Identity Store ARN pelo ARN real do Identity Store
4. Se estiver usando a [administração delegada](#), consulte [Etapa 4: configurar políticas do IAM para o uso entre contas da chave KMS](#)

Se precisar de ajuda para encontrar os valores desses identificadores, consulte [Onde encontrar os identificadores necessários](#).

Depois de atualizar o modelo com os valores, volte a [Etapa 2: preparar as declarações de política de chave KMS](#) para preparar declarações adicionais de política de chave KMS, conforme necessário.

A ação kms:Decrypt sozinha não restringe o acesso às operações somente para leitura. A política do IAM deve impor o acesso somente de leitura no serviço IAM Identity Center. APIs

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToIdentityCenterAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid": "AllowReadOnlyAccessToIdentityStoreAPI",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
      }
    }
  }
]
}

```

Declarações de política chave do KMS refinadas para uso de aplicativos AWS gerenciados

Esses modelos de política fornecem um controle mais granular sobre quais aplicativos AWS gerenciados podem usar sua chave KMS.

Note

Alguns aplicativos AWS gerenciados não podem ser usados com o IAM Identity Center configurado com uma chave KMS gerenciada pelo cliente. Consulte [Aplicações gerenciadas pela AWS que você pode usar com o IAM Identity Center](#).

Eles [Chave básica do KMS e declarações de política do IAM para uso de AWS aplicativos gerenciados](#) permitem que qualquer aplicativo AWS gerenciado de qualquer conta na mesma AWS organização use a chave KMS. Use essas políticas refinadas para restringir o acesso por meio de:

- Entidade principal do serviço de aplicação
- Instância do aplicativo ARNs

- AWS account IDs
- Contexto de criptografia para instâncias específicas do IAM Identity Center

Note

Um principal de serviço é um identificador exclusivo para um AWS serviço, normalmente formatado como servicename.amazonaws.com (por exemplo, elasticmapreduce.amazonaws.com para Amazon EMR).

Restringir por conta

Esse modelo de declaração de política de chaves do KMS permite que um aplicativo AWS gerenciado em AWS contas específicas use a chave KMS usando uma instância específica do IAM Identity Center.

Para usar essa política:

1. Substituir a amostra da entidade principal de serviço pela entidade principal de serviço da aplicação real
2. Substitua a conta IDs de exemplo pela conta real em IDs que seus aplicativos AWS gerenciados são implantados
3. Substituir o exemplo do Identity Store ARN pelo ARN real do Identity Store
4. Substituir o exemplo de ARN da instância do IAM Identity Center pelo ARN da instância real

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```

        "aws:SourceAccount": [
            "111122223333",
            "444455556666"
        ]
    },
    "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso::instance/
ssoins-1234567890abcdef"
    },
    "Bool": {
        "aws:PrincipalIsAWSService": "true"
    }
}
},
{
    "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
        "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": [
                "111122223333",
                "444455556666"
            ]
        }
    },
    "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "Bool": {
        "aws:PrincipalIsAWSService": "true"
    }
}
}
]
}

```

Restringir por instância da aplicação

Esse modelo de declaração de política de chaves do KMS permite que uma instância específica do aplicativo AWS gerenciado use a chave KMS usando uma instância específica do IAM Identity Center.

Para usar essa política:

1. Substituir a amostra da entidade principal de serviço pela entidade principal de serviço da aplicação real
2. Substituir o ARN da aplicação de exemplo pelo ARN real da instância da aplicação
3. Substituir o exemplo do Identity Store ARN pelo ARN real do Identity Store
4. Substituir o exemplo de ARN da instância do IAM Identity Center pelo ARN da instância real

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-application"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/sssoins-1234567890abcdef"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    }
  ],
  {
```

```

    "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      }
    }
  }
]
}

```

Considerações sobre chaves KMS gerenciadas pelo cliente e políticas avançadas de chaves KMS

Ao implementar chaves KMS gerenciadas pelo cliente com o IAM Identity Center, considere esses fatores que afetam a configuração, a segurança e a manutenção contínua de a configuração de criptografia.

Considerações sobre a escolha das declarações de política de chave KMS de linha de base em comparação com as avançadas

Ao decidir se deve tornar as permissões da chave KMS mais específicas usando [Declarações de política de chave KMS avançadas](#), considere a sobrecarga de gerenciamento e as necessidades de segurança da organização. Declarações de política mais específicas fornecem um controle mais refinado sobre quem pode usar a chave e para quais propósitos; no entanto, elas exigem manutenção contínua à medida que a configuração do IAM Identity Center evolui. Por exemplo, se você restringir o uso da chave KMS a implantações específicas de aplicativos AWS gerenciados, precisará atualizar a política de chaves sempre que sua organização quiser implantar ou

desimplantar um aplicativo. Políticas menos restritivas reduzem a carga administrativa, mas podem conceder permissões mais amplas do que as necessárias para os requisitos de segurança.

Considerações para habilitar uma nova instância do IAM Identity Center com uma chave KMS gerenciada pelo cliente

As considerações aqui se aplicam se você estiver usando o contexto de criptografia conforme descrito em [Declarações de política de chave KMS avançadas](#) para restringir o uso da chave KMS a uma instância específica do IAM Identity Center.

Ao habilitar uma nova instância do IAM Identity Center com uma chave KMS gerenciada pelo cliente, o IAM Identity Center e o Identity Store ARNs não estarão disponíveis até a configuração. Você tem as seguintes opções:

- Use padrões ARN genéricos temporariamente e, em seguida, substitua por full ARNs depois que a instância for ativada. Lembre-se de alternar entre StringLike operadores StringEquals e conforme necessário.
 - Para o IAM Identity Center SPN: "arn:\${Partition}:sso:::instance/*".
 - Para o Identity Store SPN: "arn:\${Partition}:identitystore:::\${Account}:identitystore/*".
- Use "Purpose:KEY_CONFIGURATION" no ARN temporariamente. Isso funciona somente para habilitação de instâncias e deve ser substituído pelo ARN real para que a instância do IAM Identity Center funcione normalmente. A vantagem dessa abordagem é que você não pode esquecer de substituí-la depois que a instância estiver habilitada.
 - Para o IAM Identity Center SPN, use: "arn:\${Partition}:sso:::instance/purpose:KEY_CONFIGURATION"
 - Para o Identity Store SPN, use: "arn:\${Partition}:identitystore:::\${Account}:identitystore/purpose:KEY_CONFIGURATION"

 Important

Não aplique essa configuração a uma chave KMS já em uso em uma instância existente do IAM Identity Center, pois isso pode interromper as operações normais.

- Omita a condição do contexto de criptografia da política de chave KMS até que a instância seja habilitada.

Recursos de marcação Centro de Identidade do AWS IAM

Uma tag é um rótulo de atributo personalizado que você adiciona a um AWS recurso para facilitar a identificação, a organização e a pesquisa de recursos. Cada tag da 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. Você pode 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 você a identificar e organizar seus AWS recursos. Muitos AWS serviços oferecem suporte à marcação, então você pode atribuir a mesma tag a recursos de serviços diferentes 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 [AWS Recursos de marcação](#) no Referência geral da AWS Guia e Melhores práticas de [marcação](#).

Além de identificar, organizar e monitorar 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 saber mais sobre o uso de tags para controlar o acesso, consulte [Como controlar o acesso a AWS recursos usando 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.

Você só pode aplicar tags a conjuntos de permissões. Você não pode aplicar tags às funções correspondentes que o IAM Identity Center cria Contas da AWS. Você pode usar o console do IAM Identity Center AWS CLI ou o IAM Identity Center APIs 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.

Tópicos

- [Restrições de tags](#)
- [Gerencie tags usando o console do IAM Identity Center](#)

- [AWS CLI exemplos](#)
- [Gerencie tags usando o console do 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 aos 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 IAM Identity Center](#).
2. Escolha Settings.
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.

AWS CLI exemplos

AWS CLI Ele fornece comandos que você pode usar 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 comandosso:

```
$ 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

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 AWS CLI com o IAM Identity Center

AWS A integração da interface de linha de comando (CLI) versão 2 com o IAM Identity Center simplifica o processo de login. Os desenvolvedores podem fazer login diretamente no 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 AWS CLI diretamente usando suas credenciais do Active Directory.

AWS A 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 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 AWS CLI com o IAM Identity Center

Para usar a integração da AWS CLI com o IAM Identity Center, baixe, instale e configure a AWS Command Line Interface versão 2. Para obter etapas detalhadas sobre como fazer o download e integrá-lo AWS CLI ao IAM Identity Center, consulte Como [configurar a AWS CLI para usar o IAM Identity Center](#) no Guia AWS Command Line Interface do usuário.

Considerações sobre o acesso Console de gerenciamento da AWS privado

Se sua organização usa o recurso de acesso Console de gerenciamento da AWS privado, você deve considerar como seus usuários farão login no IAM Identity Center.

Uma política de VPC endpoint restringe o login no console de gerenciamento, o que impede que seus usuários se conectem aos quais não Contas da AWS estão autorizados a acessar. Para obter mais informações, consulte [Console de gerenciamento da AWS Private Access](#) no Console de gerenciamento da AWS Getting Started Guide.

Endpoints da VPC bloqueiam o login no IAM Identity Center

É importante observar que o uso de endpoints da VPC bloqueará o login no IAM Identity Center. Isso acontece quando um usuário já está conectado ao console de gerenciamento via endpoint da VPC. Para garantir que seus usuários possam continuar fazendo login no IAM Identity Center, eles devem usar o endpoint público para fazer login na AWS , em vez do endpoint da VPC.

Cotas e limites no IAM Identity Center

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 APIs administrar o IAM Identity Center 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 AWS CLI com o IAM Identity Center](#). Para obter mais informações sobre isso APIs, consulte [Bem-vindo à referência da API do IAM Identity Center](#).

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 baixado para o 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	3500	Sim
Número de conjuntos de permissões provisionados permitidos por Conta da AWS	500	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	25 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

¹AWS 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

[Gerencie Contas da AWS com conjuntos de permissões](#) são 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 Identity Center	200000	Sim
Número de grupos aceitos no IAM Identity Center	100000	Sim
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
Central de identidade do IAM APIs	O IAM Identity Center APIs tem um limite coletivo de 20 transações por segundo (TPS). Para leitura APIs, você pode abrir um caso de suporte para solicitar um aumento de limite. A API de CreateAccountAssignment gravação tem um limite de 15 chamadas assíncronas pendentes. Este limite não pode ser aumentado.
Loja de identidades APIs	O Identity Store APIs tem um limite de 20 transações por segundo (TPS) por API. Esse limite se aplica por instância do Identity Store. Você pode abrir um caso de suporte para solicitar um aumento de limite.
SCIM APIs	O SCIM APIs tem limites de aceleração de 25 transações por segundo (TPS) para gravação APIs e 40 TPS para leitura. APIs Esses limites se aplicam por instância do Identity Store. Você pode abrir um caso de suporte para solicitar um aumento de limite.

Se sua instância do IAM Identity Center estiver habilitada em várias Regiões da AWS, os limites de aceleração se aplicarão igualmente a cada região habilitada. Por exemplo, você teria o limite de aceleração de 20 TPS no Identity Store APIs em cada região habilitada. Para obter mais informações sobre quais operações de API estão disponíveis em outras regiões, consulte a [tabela](#) correspondente.

Cotas de solicitação de serviço do OIDC

Recurso	Valor padrão (solicitações por segundo)	Pode ser aumentada
Taxa de solicitação de um endereço remoto para registrar um OAuth cliente público Aplica-se a: RegisterClient	20	Sim
Taxa de solicitação de um cliente público registrado no serviço OIDC Aplica-se a: CreateToken , StartDeviceAuthorization	80	Sim
Taxa de solicitação de todos os clientes públicos registrados com a mesma instância do IAM Identity Center Aplica-se a: CreateToken	250	Sim
Taxa de solicitação de uma aplicação do IAM Identity Center registrada na instância do IAM Identity Center Aplica-se a: CreateTokenWithIAM	80	Sim
Taxa de geração de tokens de todas as aplicações do IAM Identity Center registradas com a mesma instância	10	Entre em contato com o AWS Support

Recurso	Valor padrão (solicitações por segundo)	Pode ser aumentada
do IAM Identity Center com concessão do JWT Bearer		
Aplica-se a: CreateTokenWithIAM		

Se sua instância do IAM Identity Center estiver ativada em várias Regiões da AWS, as taxas de solicitação acima se aplicarão igualmente a cada região habilitada. Por exemplo, se sua taxa de solicitação permitida para registrar um OAuth cliente público a partir de um endereço remoto for de 20 solicitações por segundo, essa taxa de transferência estará disponível em cada região habilitada. Para obter mais informações sobre quais operações de API estão disponíveis em outras regiões, consulte a [tabela](#) correspondente.

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
Número total de grupos que podem ser atribuídos a um conjunto de permissões por Conta da AWS aplicativo ou a um aplicativo	100	Não

Recurso	Cota padrão	Pode ser aumentada
Número total de Regiões da AWS habilitados para uma única instância do IAM Identity Center	3	Sim

* Por exemplo, você pode configurar 2750 contas e 250 aplicativos, resultando em um total de 3.000 contas e aplicativos.

** A operação da API [ProvisionPermissionSet](#) pode provisionar um conjunto de permissões usando a opção ALL_PROVISIONED_ACCOUNTS para, no máximo, 3500 Contas da AWS. Se precisar provisionar um conjunto de permissões para mais de 3500 Contas da AWS, pode usar a operação de API ProvisionPermissionSet com a opção AWS_ACCOUNT, que provisiona o conjunto de permissões em uma única Conta da AWS. Você pode fazer até três chamadas simultâneas para ProvisionPermissionSet.

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, pode ser necessária a adesão de seu administrador à criação de instâncias de 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 permitesso: `ListApplications`, mas não outro IAM Identity Center APIs. Atualize a política para resolver esse erro.

A `ListApplications` permissão autoriza vários 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": "sso:ListApplicationProviders",  
    "Resource": "*"  
  },  
  {  
    "Effect": "Allow",  
    "Action": "sso: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": "sso:ListApplicationProviders",  
    "Resource": "*"  
  }  
]
```

Quando suas políticas forem atualizadas, entre em contato Suporte 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 seu provedor de identidades (IdP) estiver configurado para provisionar usuários no IAM Identity Center usando sincronização SCIM, você pode experimentar falhas de sincronização durante o processo de provisionamento de usuários. Isso pode indicar que a configuração de usuário do IdP não é compatível com os requisitos do IAM Identity Center. Quando isso acontece, o IAM Identity Center SCIM APIs retornará mensagens de erro que fornecem informações sobre a causa raiz do problema. Você pode encontrar essas mensagens de erro nos logs ou na interface de usuário do IdP. Ou então, você pode encontrar informações mais detalhadas sobre as falhas de provisionamento nos [logs do AWS CloudTrail](#).

Para obter mais informações sobre as implementações do IAM Identity Center, incluindo as especificações de parâmetros e operações obrigatórias, opcionais e incompatíveis para objetos de usuário, consulte [IAM Identity Center SCIM Implementation Developer Guide](#) no SCIM Developer Guide

A seguir, alguns motivos comuns desse erro:

1. O objeto de usuário no IdP não tem um nome próprio (dado), um sobrenome (de família) e and/or um nome de exibição.

Mensagem de erro: “2 erros de validação detectados: o valor em *'name.givenName'* falhou em satisfazer a restrição: o membro deve satisfazer o padrão de expressão regular: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\ n\\ r] +`; O valor em *'name.givenName'* falhou em satisfazer a restrição: o membro deve ter comprimento maior ou igual a 1”

- 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.

Mensagem de erro: “O atributo da lista *emails* excede o limite permitido de 1”

- 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.

Erro de usuário ou grupo duplicado ao provisionar usuários ou grupos com um provedor de identidades externo

Se você tiver problemas de sincronização do IAM Identity Center ao provisionar usuários ou grupos em um provedor de identidades (IdP) externo, talvez os atributos atribuídos aos usuários ou grupos do IdP externo não sejam exclusivos. Você pode receber as seguintes mensagens de erro no IdP externo:

Recusou-se a criar um novo, recurso duplicado

Você pode experimentar esse problema nos seguintes cenários:

- Cenário 1
 - Você está usando atributos personalizados não exclusivos no IdP externo para atributos que devem ser exclusivos no IAM Identity Center. Ocorre falha na sincronização de usuários ou grupos existentes do IAM Identity Center com o IdP.
- Cenário 2
 - Você tenta criar usuários que têm atributos duplicados para atributos devem ser exclusivos no IAM Identity Center.
 - Por exemplo, você cria ou tem um usuário existente do IAM Identity Center com os seguintes atributos:
 - Nome de usuário: Maria da Silva
 - Endereço de e-mail principal: jane_doe@example.com
 - Em seguida, você tenta criar outro usuário no IdP externo com os seguintes atributos:
 - Nome de usuário: Ricardo da Silva

- Endereço de e-mail principal: jane_doe@example.com
- O IdP externo tenta criar e sincronizar o usuário no IAM Identity Center. Porém, essas ações não são bem-sucedidas porque os dois usuários têm valores duplicados para um endereço de e-mail principal que deve ser exclusivo.

O nome de usuário, o endereço de e-mail principal e o externalID devem ser exclusivos para que a sincronização de usuários do IdP externo com o IAM Identity Center seja bem-sucedida. Da mesma forma, o nome do grupo deve ser exclusivo para que a sincronização de grupos do IdP externo com o IAM Identity Center seja bem-sucedida.

A solução é revisar os atributos da sua fonte de identidades e garantir que sejam exclusivos.

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 obter mais informações, consulte [MFA para usuários do diretório 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 acesso da AWS a esse 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 NameID deve ser uma string 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 Login. ExternalId PDirectory

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 browser/platform suporte. Para obter mais informações sobre o WebAuthn IAM Identity Center, consulte [FIDO2 autenticadores](#).

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 ou Microsoft 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 horário confiável ou defina manualmente a hora em seu dispositivo para corresponder a uma fonte confiável, como NIST (<https://www.time.gov/>) ou outros equivalentes. local/regional

Eu recebo uma mensagem de erro “Não é você, somos nós” ao tentar fazer login no IAM Identity Center

Esse erro indica que há um problema de configuração em sua instância do IAM Identity Center ou no provedor de identidades (IdP) externo que o IAM Identity Center está usando como fonte de identidades. 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 ative a definição automática de data e hora. Se não estiver disponível, recomendamos sincronizar a data e hora com um servidor Network Time Protocol (NTP) conhecido.
- Verifique se o certificado do IdP carregado no IAM Identity Center é o mesmo que foi fornecido pelo provedor de identidades. Você pode verificar o certificado no console do IAM Identity Center navegando para Configurações. Na guia Fonte de identidades, escolha Ação e depois Gerenciar autenticação. Se os certificados do IdP e do IAM Identity Center não forem iguais, importe um novo certificado para o IAM Identity Center.
- Certifique-se de que o formato NameID no arquivo de metadados do provedor de identidades 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 [Update your AD Connector service account credentials in 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 ser configurado para aceitar e-mails desses endereços de e-mail remetentes e não tratá-los como lixo eletrônico ou spam.

Erro: você não pode delete/modify/remove/assign acessar os conjuntos de permissões provisionados na conta de gerenciamento

Essa mensagem indica que o atributo [Administradores delegados](#) foi habilitado e que a operação que você tentou realizar anteriormente só pode ser realizada com êxito por alguém que tenha as permissões da conta de gerenciamento do AWS Organizations. Para resolver esse problema, faça login como um usuário que tem essas permissões e tente executar a tarefa novamente, ou atribua essa tarefa a alguém que tenha as permissões corretas. Para obter 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, volte à aplicação ou ao site do cliente e tente novamente, inclusive fazendo 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.

Membros do grupo de domínios confiáveis não sincronizam com o IAM Identity Center

Se um grupo de segurança for sincronizado com sucesso com o IAM Identity Center, mas seus membros de um domínio local confiável não aparecerem no IAM Identity Center, isso pode ser causado pelo fato de o grupo residir AWS Managed Microsoft AD e conter Foreign Security Principal (FSPs) representando usuários de um domínio confiável.

Tente as seguintes etapas para solucionar os problemas:

- Sincronize grupos diretamente do domínio confiável: em vez de sincronizar um grupo AWS Managed Microsoft AD que contém membros de vários domínios, crie e sincronize o grupo

diretamente do domínio local confiável. Essa abordagem funciona porque o IAM Identity Center pode acessar objetos reais do usuário no domínio de origem.

- Verifique as permissões da conta de serviço: certifique-se de que a conta de serviço do IAM Identity Center tenha as permissões necessárias sobre objetos de usuário no domínio confiável: `ReadProperties` e a `ListContents` permissão.

Solucione problemas de chaves gerenciadas pelo cliente em Centro de Identidade do AWS IAM

Este tópico descreve erros comuns relacionados a chaves gerenciadas pelo cliente que você pode encontrar ao usar Centro de Identidade do AWS IAM e fornece etapas de solução de problemas para resolvê-los.

Acesso negado: problema de permissão de descriptografia do KMS

Erro: “O usuário xxxxxxxx não está autorizado a executar: kms: Descriptografar no recurso associado a esse texto cifrado porque nenhuma política baseada em identidade permite a ação Descriptografar”
kms:

O usuário ou entidade principal do IAM não tem a permissão `kms:Decrypt` exigida na política do IAM ou na política de chave KMS.

Solução de problemas com AWS CloudTrail:

1. Procure `kms.amazonaws.com` eventos em CloudTrail
2. Pesquise o nome do evento `Decrypt`
3. Revise os campos `errorCode` e `errorMessage`
4. Verifique `userIdentity` para confirmar qual entidade principal tentou a operação

Para resolver esse problema, conceda ao usuário ou à entidade principal do IAM as permissões de acesso `kms:Decrypt` na política do IAM e na política de chave KMS. Para obter mais informações, consulte [Implementando chaves KMS gerenciadas pelo cliente em Centro de Identidade do AWS IAM](#).

AWS falhas de login de aplicativos gerenciados com uma chave KMS gerenciada pelo cliente ativada no IAM Identity Center

Se nenhum usuário do Identity Center puder fazer login em aplicativos AWS gerenciados e você tiver uma chave KMS gerenciada pelo cliente ativada em sua instância do IAM Identity Center, verifique se a política de chaves do KMS concede aos aplicativos AWS gerenciados permissões para usar a chave KMS gerenciada pelo cliente. Para obter mais informações, consulte [Declarações de chave KMS e de política do IAM de linha de base](#).

AWS falha de atribuição de and/or usuário na instalação do aplicativo gerenciado com uma chave KMS gerenciada pelo cliente ativada no IAM Identity Center

Erro: “O usuário xxxxxxxx não está autorizado a executar: kms: Descriptografar no recurso associado a esse texto cifrado porque nenhuma política baseada em identidade permite a ação Descriptografar” kms:

O usuário ou entidade principal do IAM não tem a permissão kms :Decrypt exigida na política do IAM ou na política de chave KMS.

Solução de problemas com CloudTrail:

1. Pesquise o nome do evento Decrypt
2. Revise os campos errorCode e errorMessage
3. Verifique userIdentity para confirmar qual entidade principal tentou a operação

Para resolver esse problema, conceda ao usuário ou à entidade principal do IAM as permissões de acesso kms :Decrypt na política do IAM e na política de chave KMS. Para obter mais informações, consulte [Implementando chaves KMS gerenciadas pelo cliente em Centro de Identidade do AWS IAM](#).

Problema de permissões do KMS: configuração da chave gerenciada pelo cliente com Centro de Identidade do AWS IAM

O usuário ou entidade principal do IAM não tem uma ou mais permissões de KMS exigidas (kms:Decrypt, kms:Encrypt, kms:GenerateDataKey, kms:DescribeKey) ao habilitar a chave gerenciada pelo cliente.

Solução de problemas com CloudTrail:

1. Pesquise por eventos Decrypt, Encrypt, GenerateDataKey ou DescribeKey
2. Revise os campos errorCode e errorMessage
3. Verifique userIdentity para confirmar qual entidade principal tentou a operação

Para resolver esse problema, conceda todas as permissões exigidas do KMS ao usuário ou à entidade principal do IAM na política baseada em identidade ou política de chave KMS. Para obter mais informações, consulte [Implementando chaves KMS gerenciadas pelo cliente em Centro de Identidade do AWS IAM](#).

AWS falhas de login no portal de acesso com uma chave KMS gerenciada pelo cliente ativada no IAM Identity Center

Erro: “Código de ERRO: 0001 - o acesso ao IdentityCenter serviço está bloqueado. Entre em contato com seu IdentityCenter administrador para obter mais etapas.”

Se os usuários não conseguirem fazer login no portal de AWS acesso e você tiver uma chave KMS gerenciada pelo cliente ativada na sua instância do IAM Identity Center, verifique se a política de chaves do KMS concede as permissões necessárias ao Identity Center e ao Identity Store. Para obter mais informações, consulte [Declarações de chave KMS e de política do IAM de linha de base](#).

Solucionar problemas de configuração multirregional em Centro de Identidade do AWS IAM

Este tópico descreve erros comuns relacionados à configuração de várias regiões que você pode encontrar ao usar Centro de Identidade do AWS IAM e fornece etapas de solução de problemas para resolvê-los.

A região para a qual eu quero replicar minha instância do IAM Identity Center não está disponível no console do IAM Identity Center

Primeiro, você deve criar uma chave de réplica para sua chave KMS gerenciada pelo cliente na região para a qual você deseja replicar sua instância do IAM Identity Center. Depois que a chave de réplica for criada, você verá a região na lista de regiões disponíveis para replicações. Para obter mais informações, consulte [the section called “Etapa 1: criar uma chave de réplica”](#).

AWS falhas de login de aplicativos gerenciados em uma região adicional

Se nenhum usuário do IAM Identity Center puder fazer login em aplicativos AWS gerenciados em uma região adicional depois que você adicionou a região no IAM Identity Center, confirme se você configurou a URL adicional do Assertion Consumer Service (ACS) da região no provedor de identidade externo, conforme descrito em. [the section called “Etapa 3: atualizar a configuração do IdP externo”](#) Além disso, confirme se seus usuários têm conectividade com a região.

Histórico do documento

A tabela a seguir descreve adições importantes à Centro de Identidade do AWS IAM documentação. Também atualizamos a documentação com frequência para abordar os comentários enviados por você.

- Última atualização importante da documentação: 21 de outubro de 2025

Alteração	Descrição	Data
Suporte multirregional	Suporte multirregional adicionado, incluindo replicação para regiões adicionais, Conta da AWS acesso e uso de aplicativos AWS gerenciados em outras regiões.	2 de fevereiro de 2026
Política AWS gerenciada atualizada	Atualizou a política AWSIdentityCenterExternalManagementPolicy AWS gerenciada para alterar o ARN do provisionamento do inquilino.	5 de dezembro de 2025
Novo tópico de política AWS gerenciada	Detalhes adicionados para a política AWSIdentityCenterExternalManagementPolicy AWS gerenciada.	21 de novembro de 2025
Orientação sobre auditoria e reconciliação de provisionamento automático	Orientações adicionais para auditar e reconciliar usuários, grupos e associações de grupos provisionados automaticamente pelo SCIM	17 de outubro de 2025

usando o Identity Store e comandos. APIs AWS CLI

[Cotas de solicitação de serviço do OIDC](#)

Foram adicionadas cotas de solicitação de serviço do OIDC, incluindo limites de taxa para registro de OAuth clientes, criação de tokens e outras operações do OIDC.

13 de outubro de 2025

[Atualizações da política AWS gerenciada](#)

O IAM Identity Center atualizou as políticas gerenciadas `AWSSSOMasterAccountAdministrator`, `AWSSSOMemberAccountAdministrator`, `AWSSS0ReadOnly`, `AWSSS0DirectoryAdministrator`, e `AWSSS0DirectoryReadOnly` incluiu AWS KMS as permissões necessárias para instâncias do IAM Identity Center que usam chaves gerenciadas pelo cliente para criptografia.

17 de setembro de 2025

[Chaves gerenciadas pelo cliente para criptografia em repouso](#)

Foi adicionado suporte para chaves KMS gerenciadas pelo cliente para criptografar dados de identidade da força de trabalho em repouso.

17 de setembro de 2025

Exemplo de política baseada em recursos para permitir a criação de tokens	Foi adicionado um exemplo de política baseada em recursos que permite a criação de tokens para aplicações de clientes autorizados.	16 de setembro de 2025
Suporte para sessões de usuários em segundo plano	Conteúdo adicionado para sessões de usuários em segundo plano.	11 de agosto de 2025
Sessões de console com identidade avançada	Terminologia atualizada para sessões de console com identidade avançada (anteriormente conhecidas como sessões com reconhecimento de identidade).	12 de maio de 2025
Reorganização da introdução	Conteúdo de introdução reorganizado para melhorar a clareza e a experiência do usuário.	6 de maio de 2025
Descontinuação do IAM Identity Center AD Sync	Você não pode mais provisionar usuários do Active Directory com o IAM Identity Center AD Sync. Em vez disso, você pode usar o AD Sync configurável do IAM Identity Center.	17 de abril de 2025
Conteúdo atualizado para sessão autenticada	Atualize as durações das sessões do IAM Identity Center quando a sessão do usuário for excluída.	2 de abril de 2025

Atualizações da política AWS gerenciada	Permissões atualizadas para a política AWSSS0ServiceRolePolicy AWS gerenciada.	11 de fevereiro de 2025
Fluxo de trabalho de habilitação do IAM Identity Center aprimorado	Fluxo de trabalho atualizado para habilitar instâncias de organização e de conta do IAM Identity Center.	11 de fevereiro de 2025
Atualizações na habilitação do IAM Identity Center	Conteúdo e procedimentos atualizados para habilitar instâncias de organização e de conta do IAM Identity Center.	10 de outubro de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política AWSIAMIdentityCenterAllowListForIdentityContext AWS gerenciada.	2 de outubro de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política AWSSS0MasterAccountAdministrator AWS gerenciada.	26 de setembro de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política AWSIAMIdentityCenterAllowListForIdentityContext AWS gerenciada.	4 de setembro de 2024
Atualizações de "What is IAM Identity Center?" tópico	Atualizado o conteúdo que descreve os benefícios e os recursos do IAM Identity Center.	19 de agosto de 2024

Atualizações da política AWS gerenciada	Permissões atualizadas para a política AWSIAMIdentityCenterAllowListForIdentityContext AWS gerenciada.	12 de julho de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política AWSIAMIdentityCenterAllowListForIdentityContext AWS gerenciada.	27 de junho de 2024
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 AWSSSOSReadOnly AWS gerenciada.	26 de abril de 2024

Atualizações da política AWS gerenciada	Permissões atualizadas para a política AWSIAMIdentityCenterAllowListForIdentityContext AWS gerenciada.	26 de abril de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política AWSIAMIdentityCenterAllowListForIdentityContext AWS gerenciada.	24 de abril de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política AWSIAMIdentityCenterAllowListForIdentityContext AWS gerenciada.	19 de abril de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política AWSIAMIdentityCenterAllowListForIdentityContext AWS gerenciada.	11 de abril de 2024
Atualizações da política AWS gerenciada	Permissões atualizadas para a política AWSIAMIdentityCenterAllowListForIdentityContext AWS gerenciada.	26 de novembro de 2023
Novo tópico de política AWS gerenciada	Detalhes adicionados para a política AWSIAMIdentityCenterAllowListForIdentityContext AWS gerenciada.	15 de novembro de 2023

<u>Orientação aprimorada para começar a usar o IAM Identity Center</u>	Novo conteúdo adicionado para começar a usar o IAM Identity Center e criar um usuário administrativo	23 de setembro de 2022
<u>Usuários e grupos atualizados na Referência da API do Identity Center</u>	Essa atualização inclui referências ao novo Guia de referência da API Create, Update e Delete APIs no Identity Center API.	31 de agosto de 2022
<u>AWS Single Sign-On (AWS SSO) renomeado para IAM Identity Center AWS</u>	AWS introduz. Centro de Identidade do AWS IAM 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
<u>Suporte para limites de permissões e políticas gerenciadas pelo cliente em conjuntos de permissões</u>	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
<u>Support para AWS regiões ativadas manualmente</u>	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 AWSSS0ServiceRolePolicy 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 oAWSSS0MasterAccountAdministrator ,AWSSS0MemberAccountAdministrator , e políticas AWSSS0ReadOnly 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 AWSSS0MasterAccountAdministrator 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

<u>Suporte para inscrição forçada no MFA</u>	Atualizações para exigir que os usuários inscrevam um dispositivo de MFA no login.	23 de novembro de 2020
<u>Support for WebAuthn</u>	Conteúdo adicionado para o novo atributo WebAuthn.	20 de novembro de 2020
<u>Suporte para Ping Identity</u>	Conteúdo adicionado para integração com produtos Ping Identity como um provedor de identidade externo compatível.	26 de outubro de 2020
<u>Support for OneLogin</u>	Conteúdo adicionado para integração com OneLogin como um provedor de identidade externo compatível.	31 de julho de 2020
<u>Suporte para Okta</u>	Conteúdo adicionado para integração com Okta como um provedor de identidade externo compatível.	28 de maio de 2020
<u>Suporte para provedores de identidade externos</u>	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
<u>Novas configurações de MFA</u>	Removeu o tópico de verificação em duas etapas e adicionou um novo tópico de MFA em seu lugar.	24 de outubro de 2019
<u>Nova configuração para adicionar a verificação em duas etapas</u>	Foi adicionado conteúdo sobre como ativar a verificação em duas etapas para os usuários.	16 de janeiro de 2019

<u>Support para a duração da sessão em AWS contas</u>	Conteúdo adicionado sobre como definir a duração da sessão para uma AWS conta.	30 de outubro de 2018
<u>Nova opção para usar o diretório do Identity Center</u>	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
<u>Suporte ao estado do relé e à duração da sessão nos aplicativos</u>	Adicionado conteúdo sobre o estado de retransmissão e a duração de sessão das aplicações.	10 de outubro de 2018
<u>Compatibilidade adicional com novas aplicações</u>	Adicionados 4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvalnSync, 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
<u>Suporte para acesso de várias contas a contas de gerenciamento</u>	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 informações sobre como obter credenciais 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

AWS Glossário

Para obter a AWS terminologia mais recente, consulte o [AWS glossário](#) na Glossário da AWS Referência.

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.