IAM

Guia do usuário

Edição 01

Data 03-04-2023

HUAWEI TECHNOLOGIES CO., LTD.

Marcas registadas e permissões


e outras marcas registadas da Huawei são marcas registadas da Huawei Technologies Co., Ltd. Todos as outras marcas registadas e os nomes registados mencionados neste documento são propriedade dos seus respectivos detentores.

Aviso

Os produtos, serviços e funcionalidades adquiridos são estipulados pelo contrato feito entre a Huawei e o cliente. Todos ou parte dos produtos, serviços e funcionalidades descritos neste documento pode não estar dentro do âmbito de aquisição ou do âmbito de uso. Salvo especificação em contrário no contrato, todas as declarações, informações e recomendações neste documento são fornecidas "TAL COMO ESTÁ" sem garantias, ou representações de qualquer tipo, seja expressa ou implícita.

As informações contidas neste documento estão sujeitas a alterações sem aviso prévio. Foram feitos todos os esforços na preparação deste documento para assegurar a exatidão do conteúdo, mas todas as declarações, informações e recomendações contidas neste documento não constituem uma garantia de qualquer tipo, expressa ou implícita.

Huawei Technologies Co., Ltd.

Endereço: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Site: https://www.huawei.com

Email: support@huawei.com

Índice

1 Antes de começar

Audiência pretendida

O serviço Identity and Access Management (IAM) é destinado a administradores, incluindo:

- Administrador da conta (com permissões completas para todos os serviços, incluindo o IAM)
- Usuários do IAM adicionados ao grupo de **admin** (com permissões completas para todos os serviços, incluindo o IAM)
- Usuários do IAM atribuídos à função **Security Administrator** (com permissões para acessar o IAM)

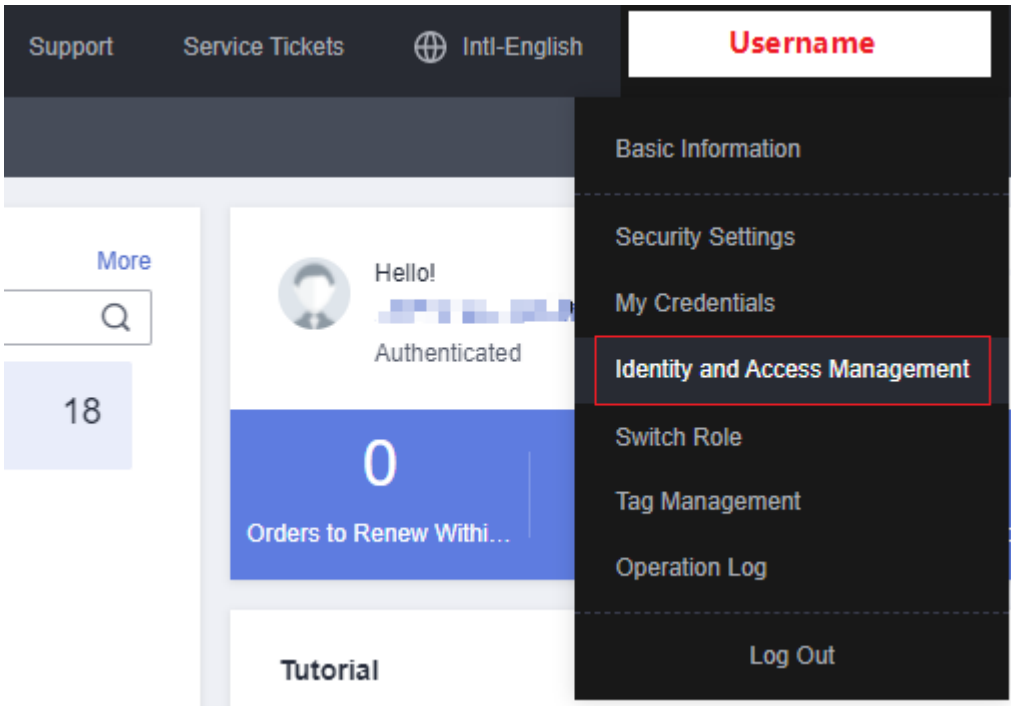
Se você quiser visualizar, auditar e rastrear os registros das principais operações realizadas no IAM, ative o Cloud Trace Service (CTS). Para mais detalhes, consulte **12.1 Ativação de CTS**.

Acessar o console do IAM

Passo 1 Faça logon na Huawei Cloud e clique em **Console** no canto superior direito.

Figura 1-1 Acessar o console

Passo 2 No console de gerenciamento, passe o mouse sobre o nome de usuário no canto superior direito e escolha **Identity and Access Management** na lista suspensa.



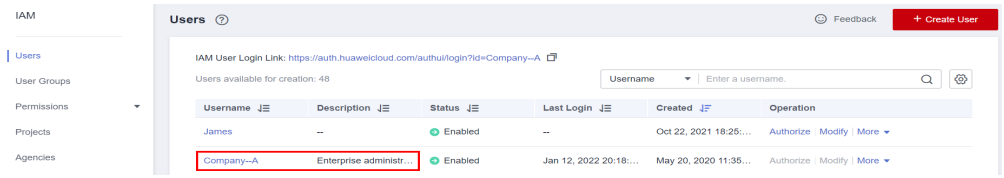
----Fim

Conta

Uma conta é criada depois que você se registra com sucesso na Huawei Cloud. Sua conta possui recursos e paga pelo uso desses recursos. Ela tem permissões de acesso total aos seus recursos. Você não pode modificar ou excluir sua conta no IAM, mas você pode fazer isso em Minha conta.

Depois de fazer logon na sua conta, você verá um usuário marcado como **Enterprise administrator** na página **Users** do console do IAM.

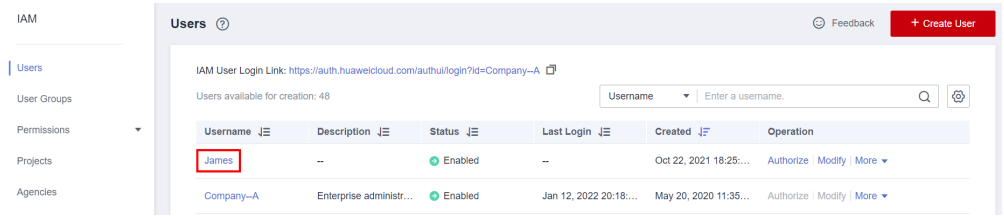
Figura 1-2 Usuário do IAM correspondente à conta



Usuário do IAM

Você pode criar usuários no IAM como administrador e atribuir permissões para recursos específicos. Conforme mostrado na figura a seguir, **James** é um usuário do IAM criado pelo administrador. Os usuários do IAM podem fazer logon na Huawei Cloud usando seu nome de conta, nomes de usuário e senhas e, em seguida, usar recursos com base nas permissões atribuídas. Os usuários do IAM não possuem recursos e não podem fazer pagamentos. Você usa sua conta para pagar as contas deles.

Figura 1-3 Usuário do IAM criado pelo administrador

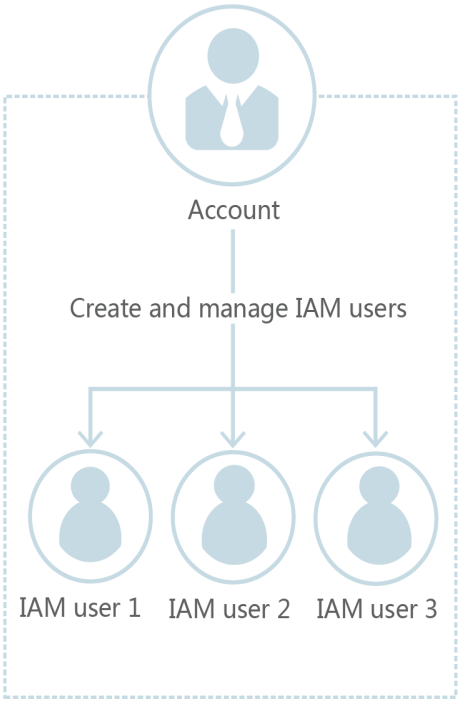


Relação entre uma conta e seus usuários do IAM

Uma conta e seus usuários do IAM têm um relacionamento pai-filho. A conta é proprietária dos recursos e faz pagamentos pelos recursos usados pelos usuários do IAM. Ela tem permissões completas para esses recursos.

Os usuários do IAM são criados pelo administrador da conta e só têm as permissões concedidas pelo administrador. O administrador pode modificar ou revogar as permissões dos usuários do IAM a qualquer momento. Os recursos usados pelos usuários do IAM na sua conta são cobrados na sua conta. Os usuários do IAM não precisam fazer pagamentos por conta própria.

Figura 1-4 Relação entre uma conta e seus usuários do IAM

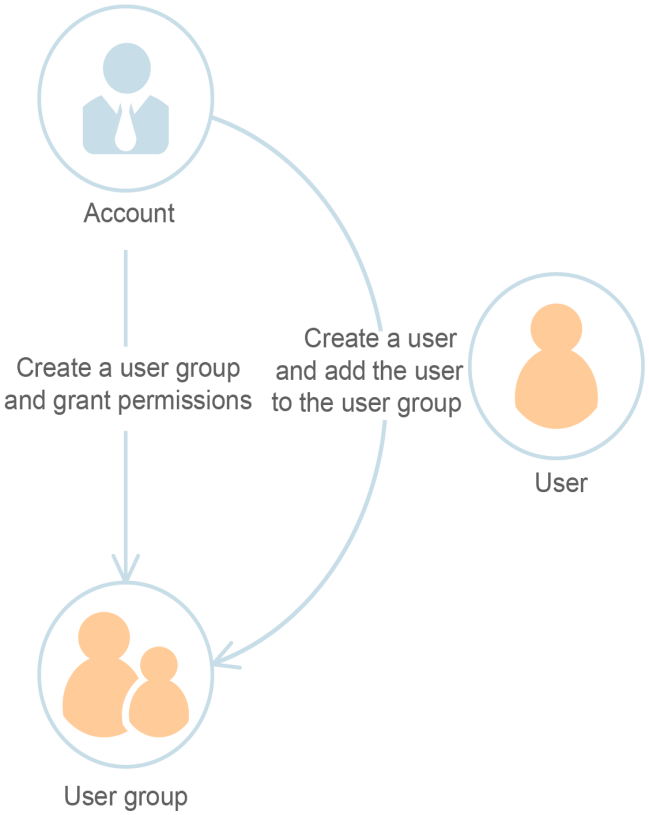


Grupo de usuários

Você pode usar grupos de usuários para atribuir permissões a usuários do IAM. Depois que um usuário do IAM é adicionado a um grupo de usuários, o usuário tem as permissões do grupo e pode executar operações em serviços de nuvem conforme especificado pelas permissões. Se um usuário for adicionado a vários grupos de usuários, o usuário herdará as permissões atribuídas a todos esses grupos.

O grupo de usuários padrão **admin** tem todas as permissões necessárias para usar todos os recursos da nuvem. Os usuários desse grupo podem executar operações em todos os recursos, incluindo, entre outros, a criação de grupos de usuários e usuários, a modificação de permissões e o gerenciamento de recursos.

Figura 1-5 Grupo de usuários



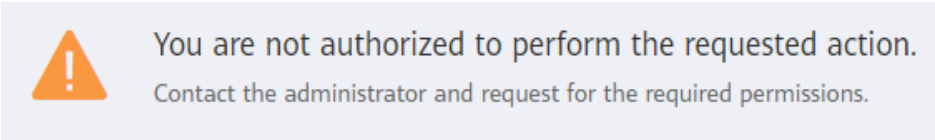
Permissão

O IAM fornece permissões comuns para diferentes serviços, como permissões de administrador e somente leitura. Novos usuários do IAM não têm permissões atribuídas por padrão. O administrador deve adicioná-los a um ou mais grupos e anexar políticas de permissões ou funções a esses grupos para que os usuários do IAM possam herdar permissões dos grupos. Os usuários do IAM também podem atribuir permissões a si mesmos. Em seguida, os usuários do IAM podem executar operações específicas em serviços de nuvem.

- Funções: um tipo de mecanismo de autorização de alta granularidade que define permissões de nível de serviço com base nas responsabilidades do usuário. Há apenas um número limitado de funções para conceder permissões aos usuários. Ao usar funções para conceder permissões, você também precisa atribuir funções de dependência. As funções não são uma escolha adequada para autorização refinada e controle de acesso seguro.
- Políticas: um tipo de mecanismo de autorização refinado que define as permissões necessárias para realizar operações em recursos de nuvem específicos sob determinadas condições. Esse mecanismo permite uma autorização mais flexível baseada em políticas com base em um princípio de privilégio mínimo (PoLP). Por exemplo, você pode conceder aos usuários do Elastic Cloud Server (ECS) apenas as permissões necessárias para gerenciar um determinado tipo de recursos do ECS.

Quando um usuário do IAM que recebeu apenas permissões de ECS acessa outros serviços, uma mensagem semelhante à seguinte será exibida.

Figura 1-6 Sem permissões

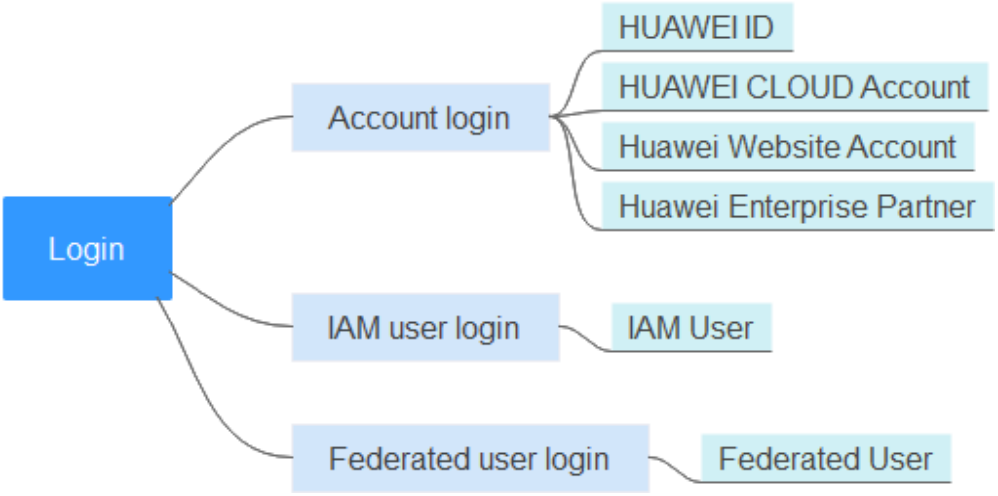


2 Fazer logon na Huawei Cloud

Você pode fazer logon na Huawei Cloud usando qualquer um dos seguintes métodos (consulte **Figura 2-1**):

- **Account login**: faça logon com a conta que foi criada quando você usa a Huawei Cloud. Sua conta tem permissões de acesso total para seus recursos e faz pagamentos pelo uso desses recursos. Para fazer logon na Huawei Cloud usando uma conta, faça o seguinte:
  - **HUAWEI ID**: uma HUAWEI ID é uma identidade unificada que você pode usar para acessar todos os serviços da Huawei. É **diferente de uma conta da Huawei Cloud**. Certifique-se de que você já registrou uma HUAWEI ID. Se você não tiver uma HUAWEI ID, crie uma e use-a para ativar os serviços da Huawei Cloud. Para obter detalhes, consulte **Registro de uma HUAWEI ID e ativação dos serviços da Huawei Cloud**.
  - **Conta da Huawei Cloud**: use sua conta da Huawei Cloud para fazer logon. Se esta é a primeira vez que você usa a Huawei Cloud, **registre uma HUAWEI ID e ative os serviços da Huawei Cloud**.
  - **Outras contas**: ao fazer logon usando uma **Huawei website account** ou **Huawei enterprise partner account** pela primeira vez, vincule essas contas a uma conta da Huawei Cloud existente ou nova. No próximo logon, você pode fazer logon diretamente usando a conta do site da Huawei ou a conta de parceiro empresarial da Huawei. Como alternativa, você pode usar a conta da Huawei Cloud para fazer logon.
- **IAM user login**: os usuários do IAM são criados por um **administrador** para usar serviços de nuvem específicos.
  - **Usuário do IAM**: **uma conta e os usuários do IAM** têm um relacionamento pai-filho. Os usuários do IAM só podem usar serviços de nuvem específicos com base nas permissões atribuídas.
- **Federated user login**: os usuários federados são registrados em um IdP empresarial criado pelo **administrador** no IAM.
  - **Usuário federado**: você pode fazer logon na Huawei Cloud como um usuário federado se tiver obtido o nome do provedor de identidade, a conta da Huawei Cloud usada para criar esse provedor de identidade e o nome de usuário e a senha para fazer logon no seu sistema de gerenciamento empresarial.

Figura 2-1 Fazer logon na Huawei Cloud



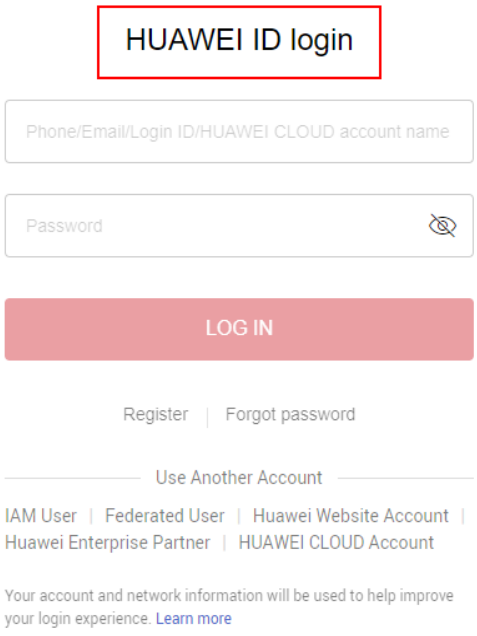
Fazer logon usando uma HUAWEI ID

uma HUAWEI ID é uma identidade unificada que você pode usar para acessar todos os serviços da Huawei. Você pode registrar e gerenciar uma HUAWEI ID no **site da HUAWEI ID**. Você também pode **registrar uma HUAWEI ID e usá-la para ativar os serviços da Huawei Cloud** na Huawei Cloud. Ao fazer logon no console da Huawei Cloud usando uma HUAWEI ID, você pode inserir um número de celular, endereço de e-mail, ID de logon ou nome de conta da Huawei Cloud.

Para fazer logon usando uma HUAWEI ID, faça o seguinte:

Passo 1 Na página de logon, digite seu número de celular, endereço de e-mail, ID de logon ou nome da conta da Huawei Cloud, digite a senha e clique em **LOG IN**.

Figura 2-2 Fazer logon usando uma HUAWEI ID



NOTA

- Você pode inserir uma conta da Huawei Cloud ou uma HUAWEI ID que tenha sido usada para ativar os serviços da Huawei Cloud.
- Se você inserir uma HUAWEI ID cujo número de celular ou endereço de e-mail tenha sido usado para ativar os serviços da Huawei Cloud, vá para **Passo 2**.
- Se você inserir uma HUAWEI ID cujo número de celular ou endereço de e-mail não tenha sido usado para ativar os serviços da Huawei Cloud, acesse **Passo 3**.

Passo 2 Selecione a conta que você deseja usar para logon.

Se o número de celular ou endereço de e-mail que você inseriu tiver sido usado para registrar uma HUAWEI ID e uma conta da Huawei Cloud, selecione uma conta para logon.

- Selecione a HUAWEI ID e clique em **OK**. Então, vá para **Passo 3**.
- Selecione a conta da Huawei Cloud e clique em **OK**. O logon foi bem-sucedido.

Passo 3 Clique em **Get code**, insira o código de verificação e clique em **OK**.

Se você já tiver vinculado um número de celular e um endereço de e-mail à sua HUAWEI ID, poderá escolher a verificação do número de celular ou do endereço de e-mail.

Passo 4 Na caixa de diálogo **Trust this browser?**, clique em **TRUST**.

Passo 5 Na caixa de diálogo exibida, clique em **Enable HUAWEI CLOUD Services** ou **Use Another HUAWEI CLOUD Account**.

- **Enable HUAWEI CLOUD Services**: clique neste botão para ativar os serviços da Huawei Cloud para a HUAWEI ID, para que possa usar a HUAWEI ID para fazer logon na Huawei Cloud. Depois de clicar neste botão, vá para **Passo 6**.
- **Use Another HUAWEI CLOUD Account**: clique neste botão para fazer logon usando outra conta da Huawei Cloud. Depois de clicar neste botão, vá para **Passo 1**.

Passo 6 (Opcional) Se o número de celular ou endereço de e-mail inserido tiver sido usado para registrar contas da Huawei Cloud, selecione uma conta e vincule-a à sua HUAWEI ID.

NOTA

Depois de vincular uma conta da Huawei Cloud à sua HUAWEI ID, você poderá usar a HUAWEI ID para acessar Huawei Cloud, HUAWEI Developers, VMALL e outros serviços da Huawei.

- Vincular uma conta da Huawei Cloud à sua HUAWEI ID
  a. Selecione uma conta da Huawei Cloud e clique em **Next**.
  b. Digite a senha da conta da Huawei Cloud e clique em **Next**.
  c. Confirme as informações da HUAWEI ID e clique em **OK**.
  d. Clique em **OK**. A página inicial da Huawei Cloud é exibida.

  NOTA

  - Depois de executar as etapas anteriores, a sua conta da Huawei Cloud é vinculada à sua HUAWEI ID e torna-se inválida. Você precisa usar a HUAWEI ID para o próximo logon.
  - Se a atualização falhar, consulte "O que posso fazer se a atualização para uma HUAWEI ID falhar?" nas *Perguntas frequentes do IAM*.
- Ativar os serviços da Huawei Cloud

  Clique em **Skip This Step and Enable HUAWEI CLOUD Services** e vá para **Passo 7**.

Passo 7 Na página **Enable HUAWEI CLOUD Services**, leia os contratos de serviço, confirme que os aceita e clique em **Enable**.

Agora você pode usar a HUAWEI ID para fazer logon na Huawei Cloud.

----Fim

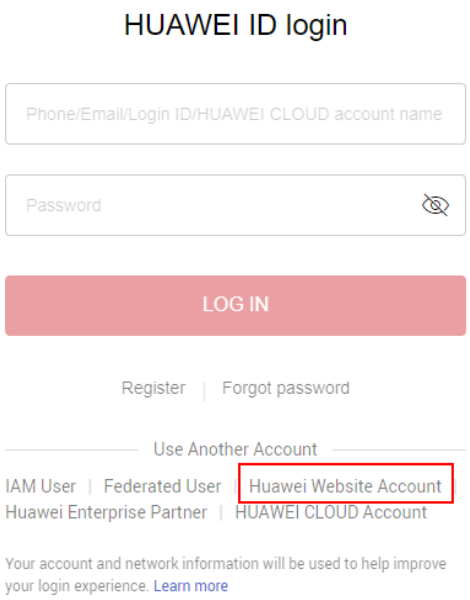
Fazer logon usando outras contas

Se você já tiver uma **conta do site da Huawei** ou uma **conta de parceiro empresarial da Huawei**, poderá usá-las para fazer logon na Huawei Cloud sem memorizar credenciais adicionais.

O procedimento a seguir descreve como usar uma conta do site oficial da Huawei para fazer logon na Huawei Cloud.

Passo 1 Na página de logon, clique em **Huawei Website Account**, conforme mostrado na figura a seguir.

Figura 2-3 Fazer logon usando uma conta do site da Huawei



Passo 2 Faça logon usando sua conta do site da Huawei.

- Se este for o primeiro logon, você será solicitado a vincular sua conta do site da Huawei a uma conta existente ou nova da Huawei Cloud. Para criar uma nova conta da Huawei Cloud, digite o nome da conta, o número do celular e o código de verificação. Clique em **Create and Bind**.
- Se este não for o primeiro logon, você pode fazer logon diretamente usando sua conta do site da Huawei.

Na próxima vez que fizer logon no console da Huawei Cloud, você poderá usar o nome ou o número de celular definido em **Passo 2** para a conta da Huawei Cloud.

----Fim

Fazer logon usando uma conta da Huawei Cloud

Se você tiver uma conta da Huawei Cloud, poderá usá-la para fazer logon na Huawei Cloud. A conta possui os recursos que você compra, faz pagamentos pelo uso desses recursos e tem permissões de acesso total para eles. Você pode usar a conta para redefinir senhas de usuário e atribuir permissões. Ao usar a conta para fazer logon no console da Huawei Cloud, você pode escolher logon de conta/e-mail ou logon de número de celular.

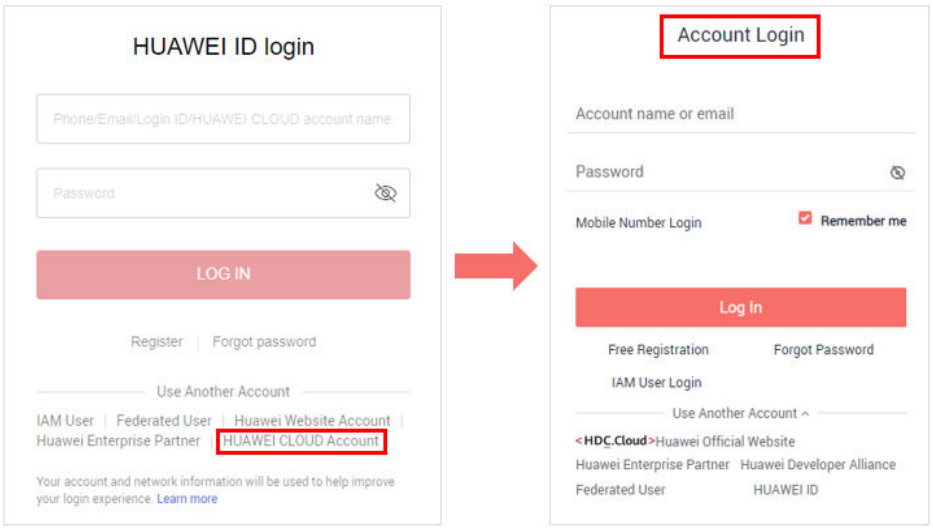
NOTA

Se a sua conta da Huawei Cloud tiver sido atualizada para uma HUAWEI ID, use a HUAWEI ID para fazer logon. Para obter detalhes, consulte **Fazer logon usando uma HUAWEI ID**.

Para fazer logon usando uma conta da Huawei Cloud, faça o seguinte:

Passo 1 Na página de logon, clique em **HUAWEI CLOUD Account**.

Figura 2-4 Fazer logon usando uma conta da Huawei Cloud



Passo 2 Insira as informações da sua conta e clique em **Log In**.

- **Account name or email**: o nome da conta ou o endereço de e-mail vinculado à conta.

  NOTA

  Os nomes das contas não diferenciam maiúsculas de minúsculas.

- **Password**: a senha de logon da conta. Se você esqueceu sua senha de login, **redefina-a** na página de logon.
- **Mobile Number Login**: se você esqueceu o nome da conta, clique em **Mobile Number Login** e digite o número de celular vinculado e a senha de logon para fazer logon.

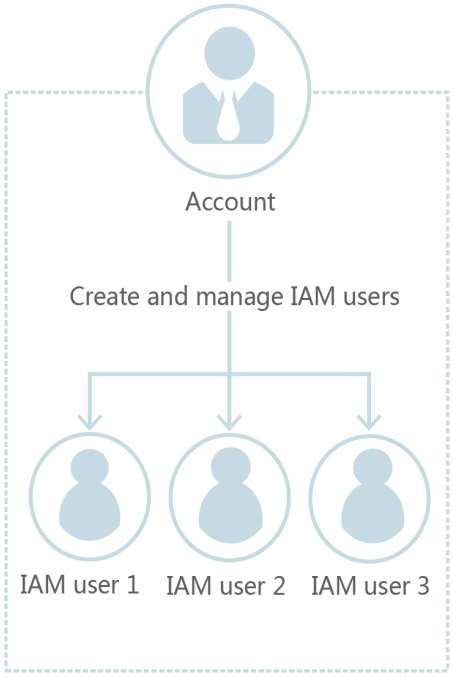
----Fim

Fazer logon como um usuário do IAM

Os usuários do IAM podem ser criados usando sua conta da Huawei Cloud ou por um **administrador**. Cada usuário do IAM tem suas próprias credenciais de identidade (senhas ou chaves de acesso) e usa recursos em nuvem com base nas permissões atribuídas. Os usuários do IAM não podem fazer pagamentos por conta própria. Você pode usar sua conta para pagar pelos recursos que eles usam.

Sua conta e os usuários do IAM têm uma relação pai-filho.

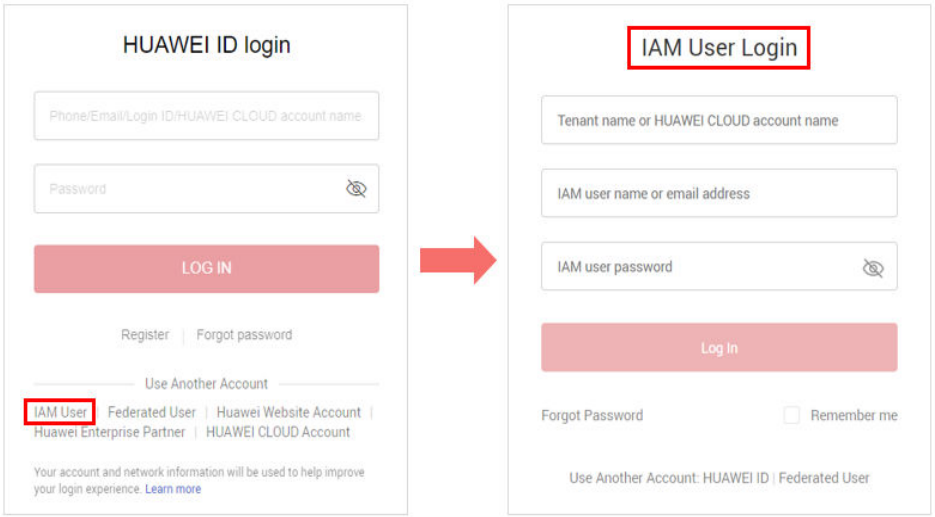
Figura 2-5 Conta e usuários do IAM



Para fazer logon como um usuário do IAM, faça o seguinte:

Passo 1 Clique em **IAM User** na página de logon e insira o nome da conta, o nome de usuário do IAM ou o endereço de e-mail e a senha.

Figura 2-6 Fazer logon como um usuário do IAM



- **Tenant name or HUAWEI CLOUD account name**: o nome da conta que foi usada para criar o usuário do IAM. Você pode obter o nome da conta do **administrador**.

- **IAM user name or email address**: o nome de usuário ou endereço de e-mail do **usuário do IAM**. Você pode obter o nome de usuário e a senha do **administrador**.
- **IAM user password**: a senha do usuário do IAM (não a senha da conta).

Passo 2 Clique em **Log In**.

----Fim

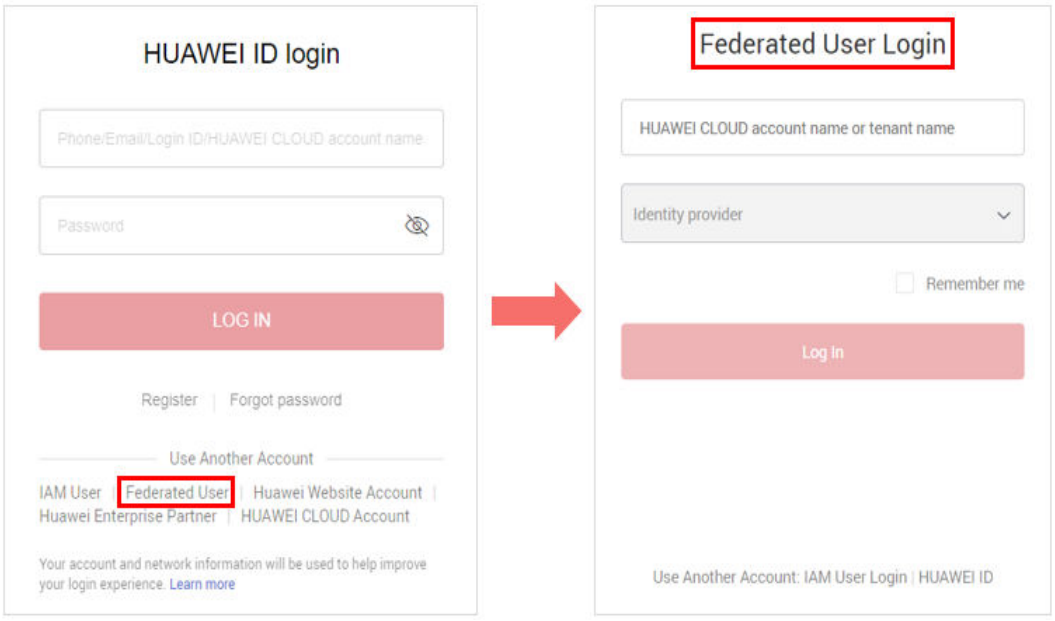
Fazer logon como um usuário federado

Os usuários federados são criados em um sistema de gerenciamento empresarial. Depois que o administrador da conta **cria uma entidade IdP** no console do IAM, os usuários federados podem fazer logon na Huawei Cloud e usar os serviços de nuvem com base nas permissões atribuídas. Para mais detalhes, consulte **9.1 Introdução**.

Você pode fazer logon na Huawei Cloud como um usuário federado se tiver obtido o nome do seu IdP, a conta da Huawei Cloud usada para criar o IdP e o nome de usuário e a senha para fazer logon no seu sistema de gerenciamento empresarial.

Passo 1 Na página de logon da Huawei Cloud, clique em **Federated User**, digite o nome da conta e selecione um provedor de identidade.

Figura 2-7 Fazer logon como um usuário federado



- **HUAWEI CLOUD account name or tenant name**: o nome da conta da Huawei Cloud que é usada para criar o provedor de identidade. Você pode obter o nome da conta do **administrador**.
- **Identity provider**: o nome do provedor de identidade criado pelo **administrador**. Você pode obter o nome do provedor de identidade do **administrador**.

Passo 2 Clique em **Log In**. A página de logon do sistema de gerenciamento empresarial é exibida.

Passo 3 Digite seu nome de usuário e senha para acessar o sistema de gerenciamento empresarial.

Passo 4 Clique no botão de logon.

----Fim

3 Usuários do IAM

3.1 Criação de um usuário do IAM

Se você for um **administrador** e tiver comprado vários recursos na Huawei Cloud, como Elastic Cloud Servers (ECSs), discos Elastic Volume Service (EVS) e Bare Metal Servers (BMSs), você pode criar usuários do IAM e conceder a eles as permissões necessárias para executar operações em recursos específicos. Dessa forma, você não precisa compartilhar a senha da sua conta.

Novos usuários do IAM não têm permissões atribuídas por padrão. É possível atribuir permissões a novos usuários ou adicioná-los a um ou mais grupos e conceder permissões a esses grupos, consultando **Atribuição de permissões a um grupo de usuários**, para que os usuários possam herdar as permissões dos grupos. Os usuários então podem executar operações específicas em serviços de nuvem, conforme especificado pelas permissões.

O grupo de usuários padrão **admin** tem todas as permissões necessárias para usar todos os recursos da nuvem. Os usuários desse grupo podem executar operações em todos os recursos, incluindo, entre outros, a criação de grupos de usuários e usuários, a modificação de permissões e o gerenciamento de recursos.

NOTA

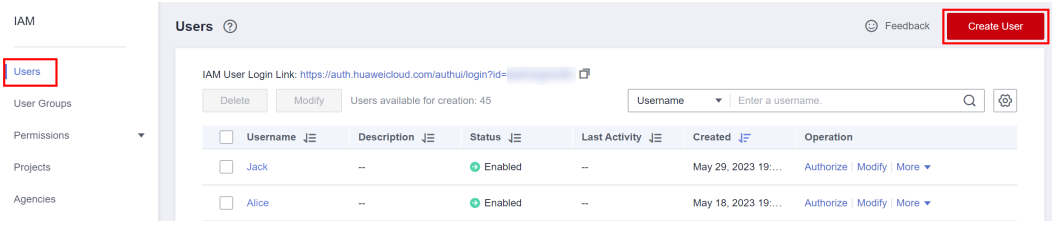
Se você excluir um usuário e depois criar um novo usuário com o mesmo nome, precisará conceder as permissões necessárias ao novo usuário novamente.

Procedimento

Passo 1 Faça logon no **console do IAM** como administrador.

Passo 2 Escolha **Users** no painel de navegação esquerdo e clique em **Create User** no canto superior direito.

Figura 3-1 Criação de um usuário do IAM



Passo 3 Especifique as informações do usuário na página **Create User**. Para criar mais usuários, clique em **Add User**. Você pode adicionar um máximo de 10 usuários por vez.

Figura 3-2 Especificar detalhes do usuário

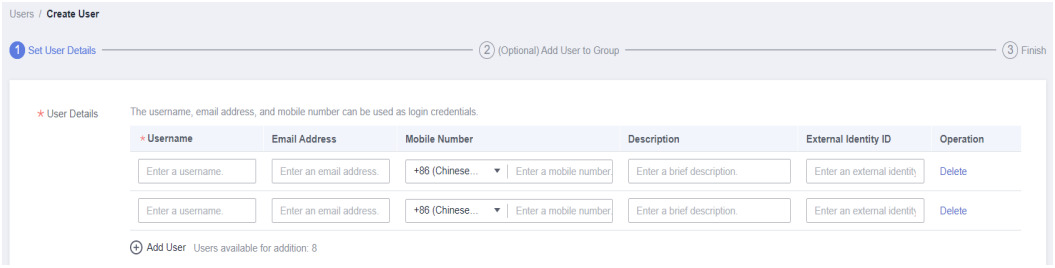


Tabela 3-1 Detalhes do usuário

Parâmetro	Descrição
Username	Esse parâmetro é definido pelo usuário e não pode ser o mesmo que o de qualquer outra conta ou de qualquer usuário do IAM na conta.
Email Address	Esse parâmetro é definido pelo usuário e não pode ser o mesmo que o de qualquer outra conta ou de qualquer usuário do IAM na conta. Ele pode ser usado para autenticar o usuário do IAM e redefinir a senha.
Mobile Number	Esse parâmetro é definido pelo usuário e não pode ser o mesmo que o de qualquer outra conta ou de qualquer usuário do IAM na conta. Ele pode ser usado para autenticar o usuário do IAM e redefinir a senha.
External Identity ID	Identidade de um usuário empresarial no SSO de usuário do IAM. O valor contém no máximo 128 caracteres. Esse parâmetro deve ser especificado se você quiser configurar a **federação de identidade via SAML** para um usuário do IAM.

Passo 4 Especifique o **Access Type**.

Figura 3-3 Selecionar tipos de acesso

Tabela 3-2 Tipos de acesso

Tipo de acesso	Descrição
Programmatic access	Permite que os usuários acessem serviços de nuvem usando ferramentas de desenvolvimento, como APIs, CLI e SDKs.
Management console access	Permite que os usuários acessem serviços de nuvem por meio do console de gerenciamento. Uma senha é obrigatória para o logon.

Passo 5 Especifique o **Credential Type**.

Figura 3-4 Selecionar tipos de credencial

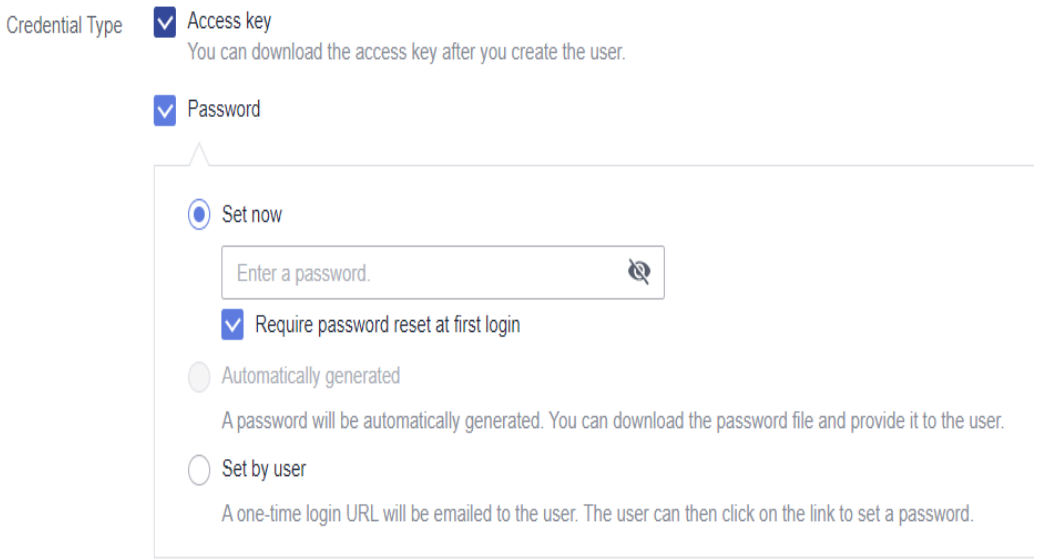


Tabela 3-3 Tipos de credenciais

Tipo de credencial	Descrição
Access key	Depois de criar o usuário, você pode baixar a **chave de acesso (AK/SK)** gerada para o usuário. **Cada usuário pode ter no máximo duas chaves de acesso.**

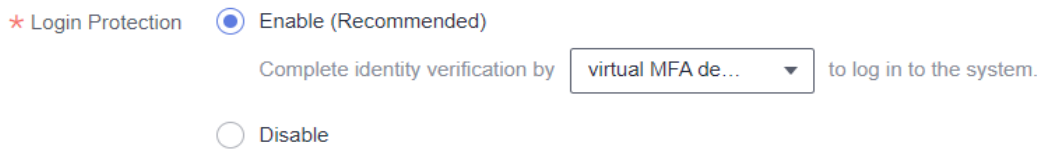
Tipo de credencial		Descrição
Password	Set now	Defina uma senha para o usuário e determine se deve exigir que o usuário redefina a senha no primeiro logon. Se você for usar o usuário do IAM sozinho, é recomendável selecionar essa opção, inserir uma senha e desmarcar **Require password reset at first login**.
	Automatically generated	O sistema gera automaticamente uma senha de logon para o usuário. Depois que o usuário é criado, você pode baixar o arquivo de senha EXCEL e fornecer a senha para o usuário. O usuário pode então usar essa senha para logon. **Essa opção está disponível somente quando você cria um único usuário.**
	Set by user	Um URL de logon único será enviado por e-mail ao usuário. O usuário pode clicar no link para fazer logon no console e definir uma senha. Se você não usar o usuário do IAM sozinho, selecione essa opção e digite o endereço de e-mail e o número do celular do usuário do IAM. O usuário pode então definir uma senha clicando no URL de logon único enviado por e-mail. O URL de logon é válido por **seven days**.

Tabela 3-4 Configurações recomendadas

Management Console Access	Programmatic Access	Tipo de credencial	Tipo de acesso recomendado	Tipo de credencial recomendado
Selecione	Desmarque	Não há requisitos especiais.	Management console access	Senha
Desmarque	Selecione	Não há requisitos especiais.	Programmatic access	Chave de acesso
Desmarque	Selecione	**Uma senha é necessária como uma credencial para acesso programático** (exigida por algumas APIs).	Programmatic access	Senha
Selecione	Selecione	**A chave de acesso (inserida pelo usuário do IAM) precisa ser verificada no console.** Por exemplo, o usuário precisa executar a verificação da chave de acesso antes de criar um trabalho de migração de dados no console do Cloud Data Migration (CDM).	Programmatic access e management console access	Senha e chave de acesso

Passo 6 Configure a proteção de logon. Esse parâmetro está disponível somente quando você selecionou **Management console access** para **Access Type**.

Figura 3-5 Ativação da proteção de logon

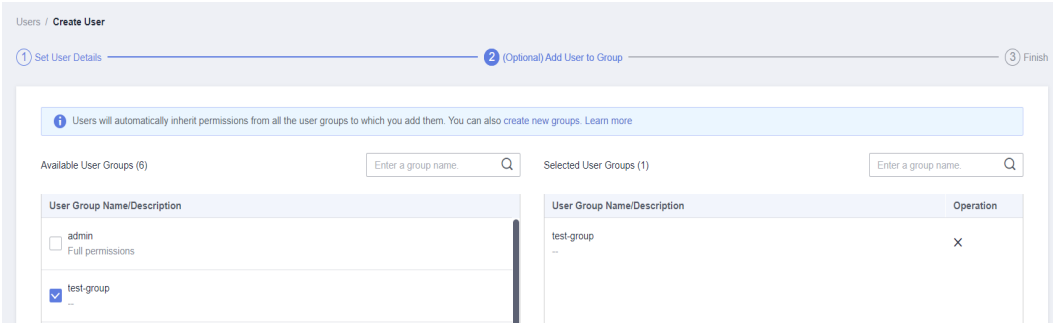


- **Enable (Recommend for account security)**: o usuário precisa inserir um código de verificação além do nome de usuário e senha para logon.

  Você pode escolher a verificação de logon baseada em SMS, e-mail ou MFA virtual.
- **Disable**: o usuário não precisa inserir um código de verificação para fazer logon. Se você quiser ativar a proteção de logon após a criação do usuário, consulte **Proteção de logon**.

Passo 7 Clique em **Next**. Selecione os grupos de usuários para adicionar o usuário. O usuário herdará as permissões atribuídas aos grupos de usuários.

Figura 3-6 Adição do usuário a grupos de usuários



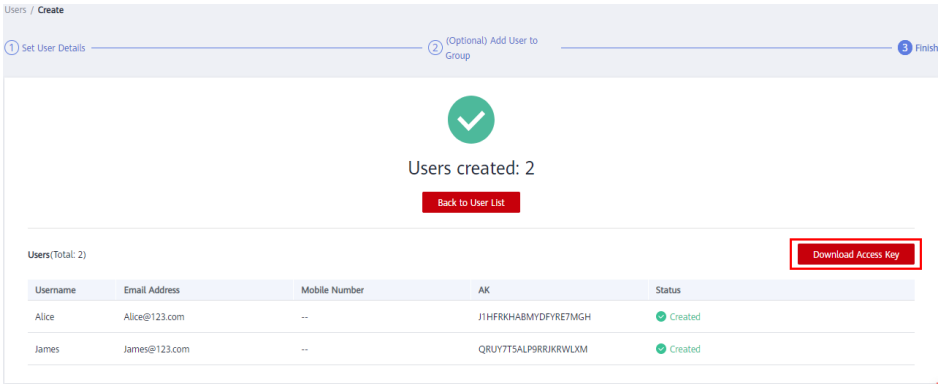
NOTA

- Você também pode criar um novo grupo e adicionar o usuário a esse grupo.
- Se você quiser que o usuário seja um administrador, adicione-o ao grupo padrão **admin**.
- Você pode adicionar um usuário a um máximo de 10 grupos de usuários.

Passo 8 Clique em **Create**.

- Se você selecionou **Access key** para **Credential Type** em **Passo 5**, você pode baixar a chave de acesso na página **Finish**.
- Se você selecionou **Password** > **Automatically generated** para **Credential Type** em **Passo 5**, poderá fazer o download do arquivo de senha na página **Finish**.

Figura 3-7 Usuários criados com sucesso



----Fim

Operações relacionadas

- Os usuários do IAM criados sem serem adicionados a nenhum grupo não têm permissões. O administrador pode atribuir permissões a esses usuários do IAM no console do IAM. Os usuários do IAM também podem atribuir permissões a si mesmos. Em seguida, os usuários podem usar recursos de nuvem com base nas permissões atribuídas. Para mais detalhes, consulte **3.2 Atribuição de permissões a um usuário do IAM**.
- As contas e os usuários do IAM usam métodos diferentes para fazer logon. Para obter detalhes sobre o logon de usuário do IAM, consulte **3.3 Fazer logon como um usuário do IAM**.

3.2 Atribuição de permissões a um usuário do IAM

Os usuários do IAM criados sem serem adicionados a nenhum grupo não têm permissões. O administrador pode atribuir permissões a esses usuários do IAM no console do IAM. Os usuários do IAM também podem atribuir permissões a si mesmos. Após a autorização, os usuários podem usar os recursos da nuvem em sua conta, conforme especificado por suas permissões.

Restrições

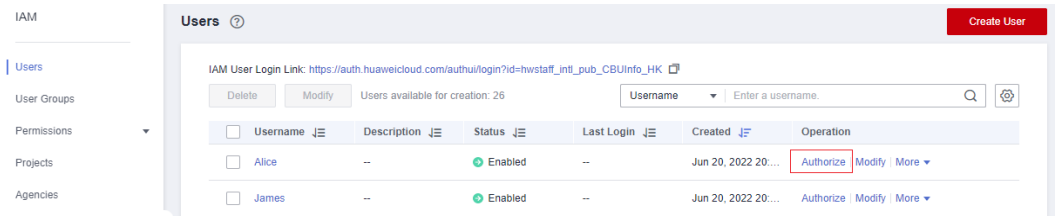
Um máximo de 500 permissões (incluindo permissões definidas pelo sistema e políticas personalizadas) podem ser atribuídas a cada usuário do IAM para projetos empresariais.

Procedimento

Passo 1 Faça logon no **console do IAM** como administrador.

Passo 2 Na lista de usuários, clique em **Authorize** na linha que contém o usuário de destino.

Figura 3-8 Autorizar um usuário do IAM

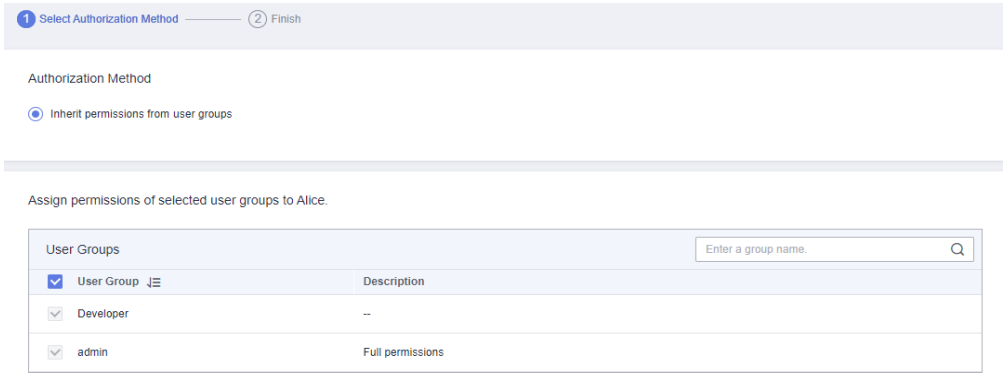


Passo 3 Na página **Authorize User**, selecione um modo de autorização e permissões.

- **Inherit permissions from user groups**: adicionar o usuário do IAM a determinados grupos para herdar suas permissões.

  Se você selecionar essa opção, selecione os grupos de usuários aos quais o usuário pertencerá.

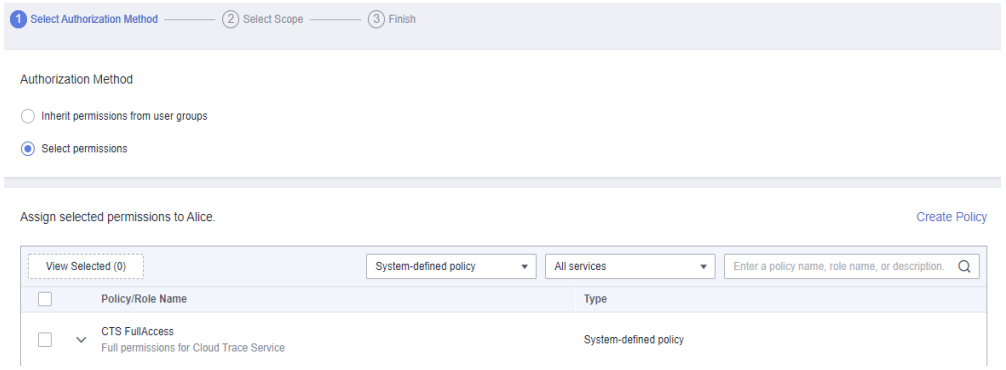
  Figura 3-9 Função Enterprise Project não ativada

- **Select permissions**: atribuir permissões específicas diretamente ao usuário do IAM. Você pode atribuir permissões diretamente aos usuários do IAM somente quando o Enterprise Project estiver ativado. Para ativar o Enterprise Project, consulte **Ativação da função Enterprise Project**.

  Se você selecionar essa opção, selecione permissões, clique em **Next** no canto inferior direito e vá para **Passo 4**.

  Figura 3-10 Função Enterprise Project ativada

NOTA

- Se você adicionar um usuário do IAM ao grupo padrão **admin**, o usuário se tornará um administrador e poderá executar todas as operações em todos os serviços de nuvem.
- Se você adicionar um usuário a vários grupos de usuários, o usuário herdará as permissões atribuídas a esses grupos.
- **Para obter detalhes sobre as permissões definidas pelo sistema de todos os serviços de nuvem suportados pelo IAM, consulte Permissões definidas pelo sistema.**
- Se você tiver ativado o gerenciamento empresarial, não será possível criar subprojetos no IAM.

Passo 4 Na página **Select Scope**, selecione os projetos empresariais que o usuário do IAM pode acessar. Você não precisa executar esta etapa se tiver selecionado **Inherit permissions from user groups**.

Passo 5 Clique em **OK**.

Você pode acessar a página **Permissions** > **Authorization** e visualizar ou modificar as permissões do usuário do IAM.

----Fim

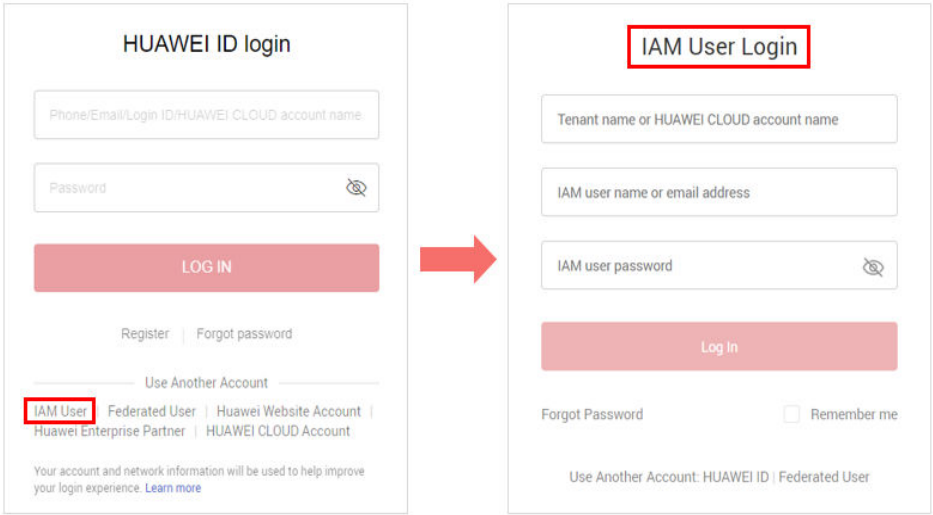
3.3 Fazer logon como um usuário do IAM

Para efetuar logon como um usuário do IAM, você pode escolher **IAM User** na página de logon ou obter o link de logon do usuário do IAM do administrador.

Método 1: efetuar logon clicando em usuário do IAM

Passo 1 Clique em **IAM User** na página de logon e insira o nome da conta, o nome de usuário do IAM ou o endereço de e-mail e a senha.

Figura 3-11 Fazer logon como um usuário do IAM



- **Tenant name or HUAWEI CLOUD account name**: o nome da conta que foi usada para criar o usuário do IAM. Você pode obter o nome da conta do **administrador**.
- **IAM user name or email address**: o nome de usuário ou endereço de e-mail do **usuário do IAM**. Você pode obter o nome de usuário e a senha do **administrador**.

- **IAM user password**: a senha do usuário do IAM (não a senha da conta).

Passo 2 Clique em **Log In**.

NOTA

- Se você não foi adicionado a nenhum grupo, você não tem permissões para acessar nenhum serviço de nuvem. Nesse caso, entre em contato com o administrador e solicite as permissões necessárias (consulte **4.1 Criação de um grupo de usuários e atribuição de permissões** e **4.2 Adição ou remoção de usuários de um grupo de usuários**).
- Se você tiver sido adicionado ao grupo padrão **admin**, terá permissões de administrador e poderá executar todas as operações em todos os serviços de nuvem.

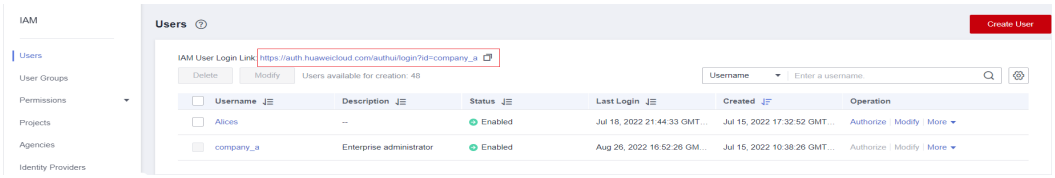
----Fim

Método : fazer logon usando o link de logon de usuário do IAM

Você pode obter o link de logon do usuário do IAM do administrador e, em seguida, efetuar logon usando esse link. Quando você acessa o link, o sistema exibe a página de logon e preenche automaticamente o nome da conta. Você só precisa inserir seu nome de usuário e senha.

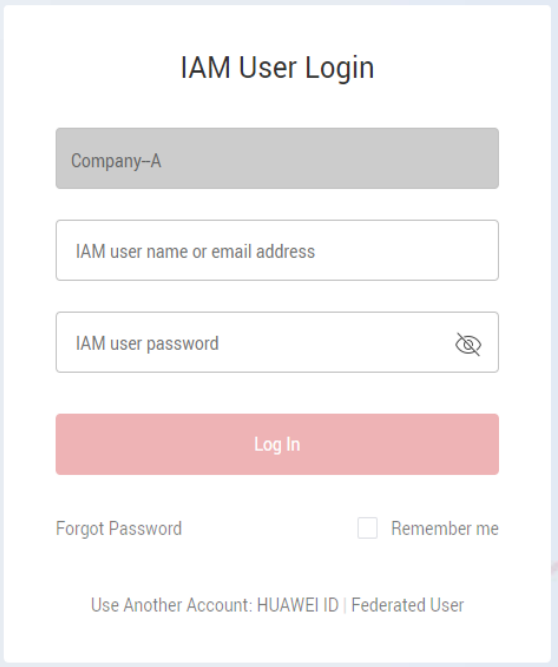
Passo 1 Obtenha o link de logon do usuário do IAM do administrador, que pode copiar o link de logon do **console do IAM**.

Figura 3-12 Link de logon do usuário do IAM



Passo 2 Cole o link na barra de endereços de um navegador, pressione **Enter**, insira o nome de usuário/endereço de e-mail do IAM e a senha e clique em **Log In**.

Figura 3-13 Fazer logon usando o link de logon do usuário do IAM

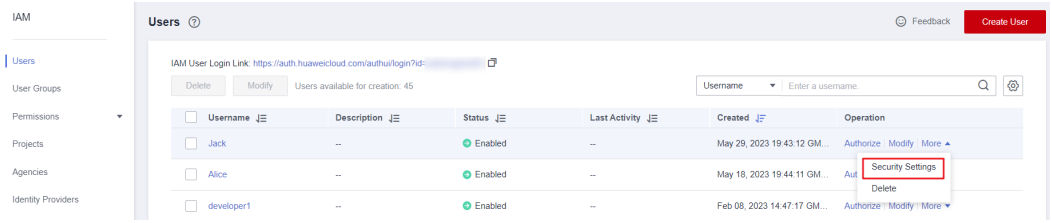


----Fim

3.4 Visualização ou modificação das informações do usuário do IAM

Como administrador, você pode modificar as informações básicas sobre um usuário do IAM, alterar as configurações de segurança do usuário e dos grupos aos quais o usuário pertence e visualizar ou excluir as permissões atribuídas. Para visualizar ou modificar informações do usuário, clique em **Security Settings** na linha que contém o usuário do IAM.

Figura 3-14 Acessar a página de configurações de segurança do usuário do IAM



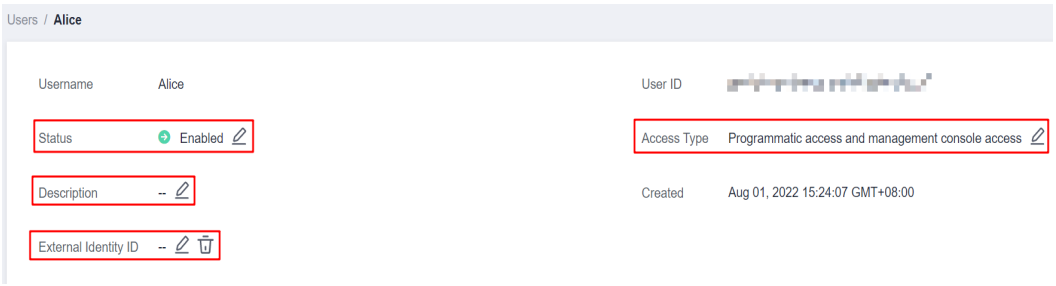
Para ajustar as colunas de itens exibidas na lista, clique em  . As colunas **Username**, **Status** e **Operation** são exibidas por padrão. Você também pode selecionar **Description**, **Last Activity**, **Created**, **Access Type**, **Login Authentication**, **Virtual MFA Status**, **Password Age**, **Access Key (Status, Age, and AK)** e **External Identity ID**.

Se você fizer logon no console ou obter um token mais de uma vez em um período de 5 minutos, a coluna **Last Activity** exibirá apenas o primeiro horário de logon.

Informações básicas

Você pode visualizar as informações básicas de cada usuário do IAM. O nome de usuário, ID de usuário e hora de criação não podem ser modificados.

Figura 3-15 Modificar o status, o tipo de acesso, a descrição e o ID de identidade externa de um usuário do IAM



- **Status**: novos usuários do IAM são ativados por padrão. Você pode definir **Status** como **Disabled** para desativar um usuário do IAM. Um usuário desativado não é mais capaz de fazer logon na Huawei Cloud por meio do console de gerenciamento ou acesso programático. Os usuários do IAM também podem modificar seus status.
- **Access Type**: você pode alterar o tipo de acesso do usuário do IAM.

  NOTA

  - Preste atenção ao seguinte ao definir o tipo de acesso de um usuário do IAM:
    - Se o usuário **acessar os serviços de nuvem somente usando o console de gerenciamento**, especifique o tipo de acesso como **Management console access** e o tipo de credencial como **Password**.
    - Se o usuário **acessar serviços de nuvem somente por meio de chamadas programáticas**, especifique o tipo de acesso como **Programmatic access** e o tipo de credencial como **Access key**.
    - Se o usuário **precisar usar uma senha como credencial para acesso programático** a determinadas APIs, especifique o tipo de acesso como **Programmatic access** e o tipo de credencial como **Password**.
    - Se o usuário precisar **executar a verificação da chave de acesso** ao usar determinados serviços no console, como a criação de um trabalho de migração de dados no console do Cloud Data Migration (CDM), especifique o tipo de acesso como **Programmatic access** e **Management console access** e o tipo de credencial como **Access Key** e **Password**.
  - Se o tipo de acesso do usuário for **Programmatic access** ou **Programmatic access** e **Management console access**, desmarcar **Programmatic access** restringirá o acesso do usuário aos serviços de nuvem. Tenha cuidado ao realizar esta operação.
- **Description**: você pode modificar a descrição do usuário do IAM.
- **External Identity ID**: identifica um usuário empresarial em logon federado usando SSO.

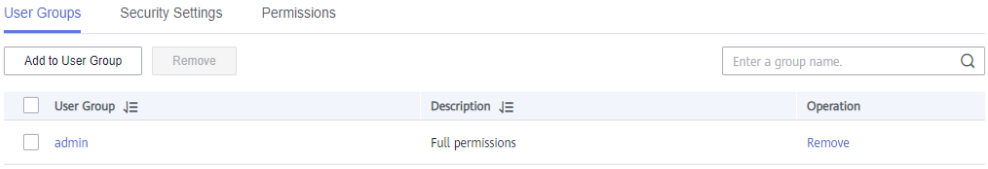
Grupos de usuários

Um usuário do IAM herda permissões dos grupos aos quais o usuário pertence. Você pode alterar as permissões atribuídas a um usuário do IAM alterando os grupos aos quais o usuário pertence. Para modificar as permissões de um grupo de usuários, consulte **4.4 Visualização ou modificação das informações do grupo de usuários**.

Sua conta pertence ao grupo padrão **admin**, que não pode ser alterado.

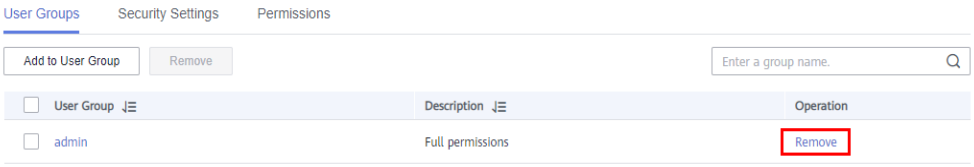
- Clique em **Add to User Group** e selecione um ou mais grupos aos quais o usuário pertencerá. O usuário então herda as permissões desses grupos.

  Figura 3-16 Adição do usuário a um grupo de usuários

- Clique em **Remove** à direita de um grupo de usuários e clique em **Yes**. O usuário não tem mais as permissões atribuídas ao grupo.

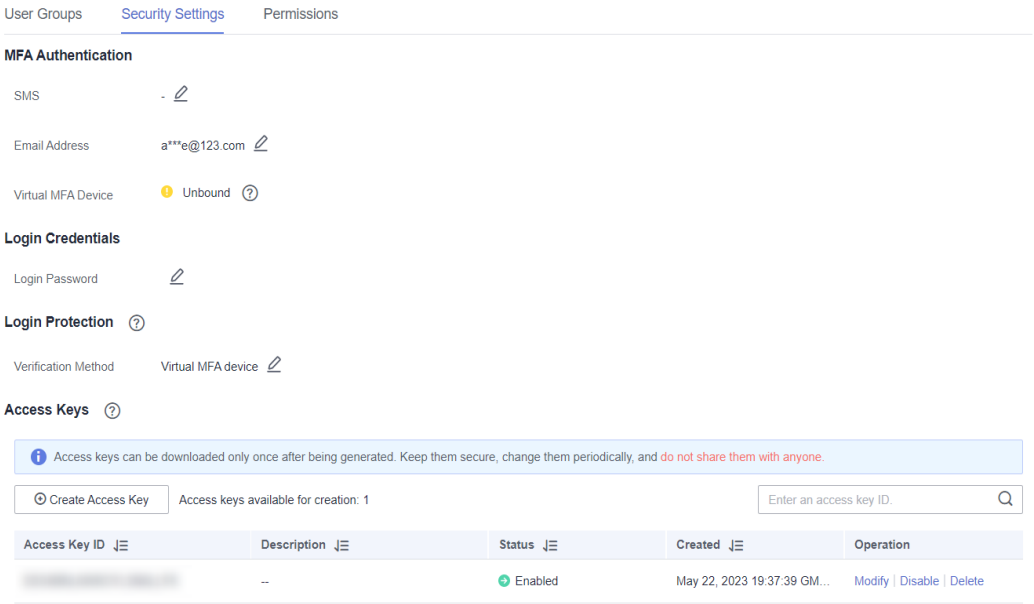
  Figura 3-17 Remover o usuário de um grupo de usuários

Configurações de segurança

Como administrador, você pode modificar o dispositivo de MFA, a credencial de logon, a proteção de logon e as chaves de acesso de um usuário do IAM nesta página. Se você for um usuário do IAM e precisar alterar seu número de celular, endereço de e-mail ou dispositivo de MFA virtual, consulte **8.1 Visão geral das configurações de segurança**.

Figura 3-18 Configurações de segurança do usuário do IAM



- **MFA Authentication**: você pode alterar as configurações de autenticação multifator (MFA) de um usuário do IAM na página **Security Settings**.

  - Altere ou exclua o número de celular ou o endereço de e-mail do usuário.

    NOTA

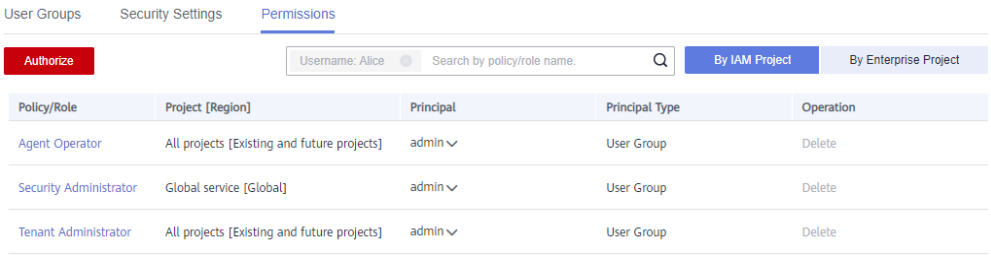
    O número de celular e o endereço de e-mail do usuário do IAM não podem ser iguais aos da sua conta ou de outros usuários do IAM.
  - Remova o dispositivo de MFA virtual do usuário. Para obter mais informações sobre autenticação MFA e dispositivo de MFA virtual, consulte **11 Autenticação MFA e dispositivo MFA virtual**.
- **Login Credentials**: você pode alterar a senha de logon do usuário do IAM. Para obter mais informações, consulte **3.6 Alteração da senha de logon de um usuário do IAM**. Você também pode excluir a senha de logon do usuário. Isso desativará seu acesso à Huawei Cloud. Tenha cuidado ao realizar esta operação.
- **Login Protection**: você pode alterar o método de verificação de logon do usuário do IAM. Três métodos de verificação estão disponíveis: dispositivo de MFA virtual, SMS e e-mail.

  Esta opção está desativada por padrão. Se você ativar essa opção, o usuário precisará inserir um código de verificação além do nome de usuário e senha ao fazer logon no console.
- **Access Keys**: você pode gerenciar as chaves de acesso do usuário do IAM. Para obter mais informações, consulte **3.7 Gerenciamento de chaves de acesso para um usuário do IAM**.

Permissões

Você pode exibir ou excluir permissões de usuários do IAM. Para modificar permissões de usuários do IAM, consulte **Grupos de usuários**.

Figura 3-19 Permissões atribuídas a um usuário do IAM



Para ver todos os registos de autorização na sua conta, consulte **5.5 Registros de autorização**.

NOTA

A exclusão das permissões de um usuário do IAM excluirá as permissões atribuídas ao grupo ao qual o usuário pertence. Todos os usuários do grupo não terão mais as permissões. Tenha cuidado ao realizar esta operação.

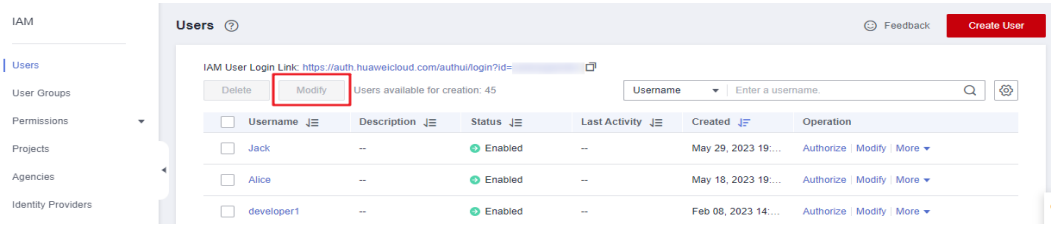
Modificar informações do usuário do IAM em lote

O IAM permite que você modifique em lote o status, o tipo de acesso, o método de verificação, a senha de logon, o número de celular e o endereço de e-mail dos usuários do IAM. Veja a seguir como modificar em lote o status dos usuários do IAM. Os métodos de modificação de outras informações sobre os usuários são semelhantes a esse método.

Passo 1 Faça logon no **console do IAM**. No painel de navegação, escolha **Users**.

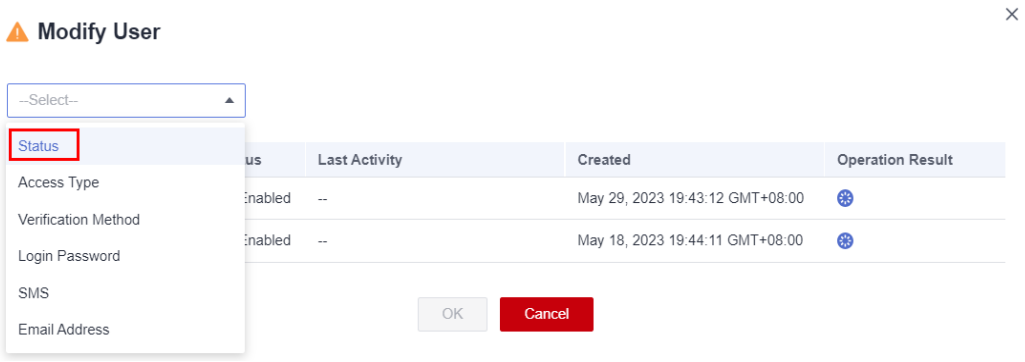
Passo 2 Na lista de usuários, selecione os usuários cujas informações você deseja modificar e clique em **Modify** acima da lista de usuários.

Figura 3-20 Modificação de informações do usuário



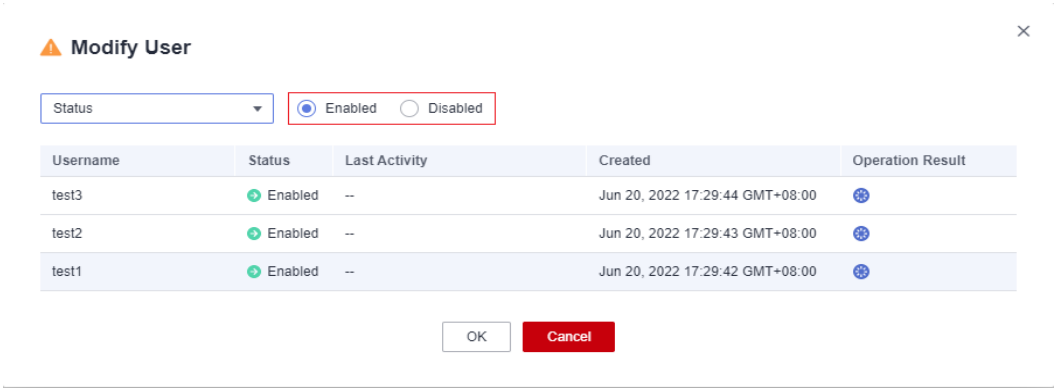
Passo 3 Selecione o atributo que deseja modificar. Neste exemplo, selecione **Status** na lista suspensa.

Figura 3-21 Selecionar o atributo de status



Passo 4 Selecione o status de destino a ser configurado para os usuários do IAM selecionados.

Figura 3-22 Selecionar o status de destino



NOTA

Certifique-se de que este usuário não esteja mais em uso. Desativar um usuário ativo pode afetar os serviços.

Passo 5 Clique em **OK**.

Passo 6 Na caixa de diálogo exibida, clique em **OK** para confirmar a alteração.

----Fim

3.5 Exclusão de um usuário do IAM

CUIDADO

Depois que um usuário do IAM for excluído, ele não poderá mais fazer logon e seu nome de usuário, senha, chaves de acesso e autorizações serão apagados e não poderão ser recuperados.

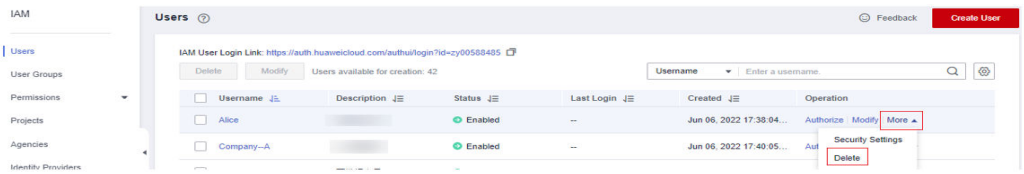
- Certifique-se de que os usuários a serem excluídos não são mais necessários. Se você não tiver certeza, desative-os em vez de excluí-los para que possam ser ativados se ocorrer alguma falha no serviço. Para desativar um usuário individual do IAM, consulte **Informações básicas**. Para desativar vários usuários do IAM ao mesmo tempo, consulte **Modificar informações do usuário do IAM em lote**.
- Para remover um usuário do IAM de um grupo de usuários, consulte **4.2 Adição ou remoção de usuários de um grupo de usuários**.
- Os usuários do IAM podem se excluir.

Exclusão de um usuário do IAM

Passo 1 Faça logon no **console do IAM**. No painel de navegação, escolha **Users**.

Passo 2 Escolha **More** > **Delete** na linha que contém o usuário do IAM que você deseja excluir e clique em **Yes**.

Figura 3-23 Exclusão de um usuário do IAM



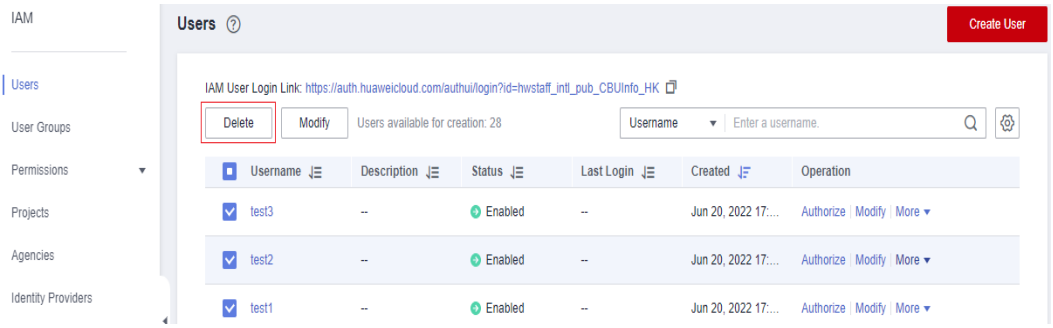
----Fim

Exclusão de usuários do IAM em lote

Passo 1 Faça logon no **console do IAM**. No painel de navegação, escolha **Users**.

Passo 2 Na lista de usuários, selecione os usuários a serem excluídos e clique em **Delete** acima da lista de usuários.

Figura 3-24 Exclusão em lote de usuários do IAM



Passo 3 Na caixa de diálogo exibida, clique em **Yes**.

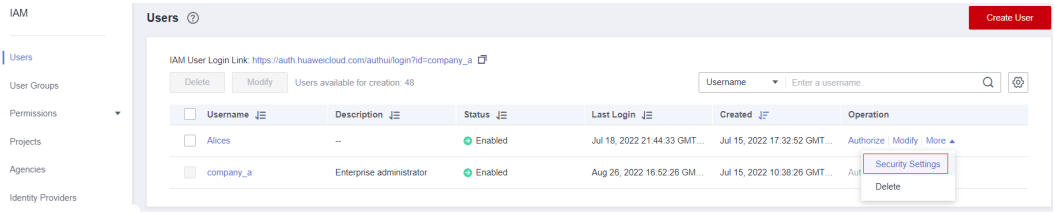
----Fim

3.6 Alteração da senha de logon de um usuário do IAM

Como administrador, você pode redefinir a senha de um usuário do IAM se o usuário tiver esquecido a senha e nenhum endereço de e-mail ou número de celular tiver sido vinculado ao usuário.

Para redefinir a senha de logon de um usuário do IAM, clique em **Security Settings** na linha que contém o usuário, clique em ao lado de **Login Password** na área **Login Credentials** e selecione um tipo de senha.

Figura 3-25 Alteração da senha de um usuário do IAM



NOTA

- Você pode redefinir a senha de um usuário do IAM na página **Security Settings**.
- A senha do usuário do IAM gerada automaticamente para sua conta não pode ser alterada na guia **Security Settings**. Para alterar a senha, acesse a página **Basic Information** de Minha conta.
- Os usuários do IAM podem alterar suas senhas na guia **Informações básicas**. Se você quiser alterar a senha da sua conta, consulte **Como alterar minha senha?**

- **Set by user**: um URL de logon único será enviado por e-mail ao usuário. O usuário pode então clicar no link para definir uma senha.
- **Automatically generated**: uma senha será gerada automaticamente e depois enviada ao usuário por e-mail.
- **Set now**: você define uma nova senha e envia a nova senha para o usuário.

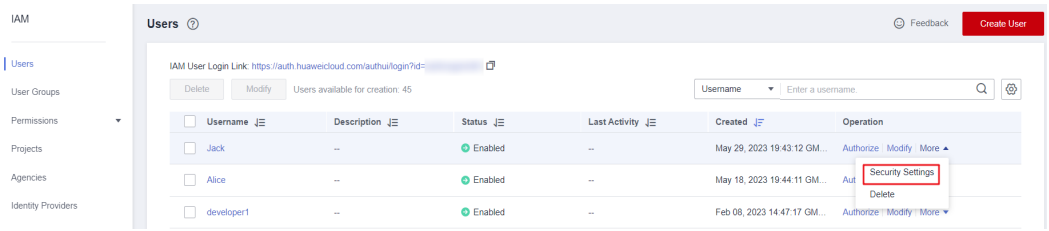
3.7 Gerenciamento de chaves de acesso para um usuário do IAM

Uma chave de acesso consiste em um par de ID de chave de acesso (AK) e chave de acesso secreta (SK). Você pode usar uma chave de acesso para acessar a Huawei Cloud usando ferramentas de desenvolvimento, incluindo APIs, CLI e SDKs. As chaves de acesso não podem ser usadas para fazer logon no console. O AK é um identificador exclusivo usado em conjunto com a SK para assinar solicitações criptograficamente, garantindo que as solicitações sejam secretas, completas e corretas.

Como administrador, você pode gerenciar chaves de acesso para usuários do IAM que esqueceram suas chaves de acesso e não têm acesso ao console.

Escolha **More** > **Security Settings** na linha que contém o usuário do IAM e, em seguida, crie ou exclua chaves de acesso na área **Access Keys**.

Figura 3-26 Gerenciamento de chaves de acesso para um usuário do IAM



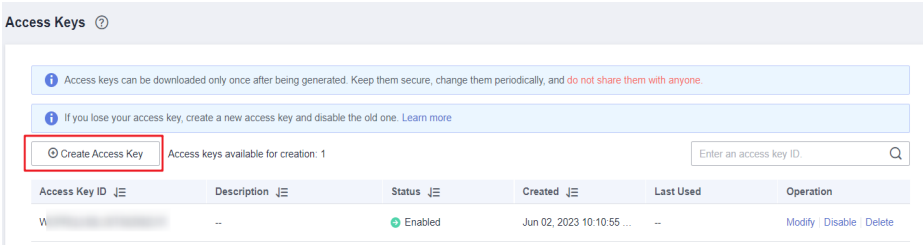
NOTA

- Os usuários federados só podem criar credenciais de acesso temporárias (AKs/SKs e tokens de segurança temporários). Para obter detalhes, consulte **Chave de acesso temporária (para usuários federados)**.
- Se um usuário estiver autorizado a usar o console, ele poderá **gerenciar chaves de acesso** na página **My Credentials**.
- As chaves de acesso são credenciais de identidade usadas para chamar APIs. O administrador da conta e os usuários do IAM só podem usar suas próprias chaves de acesso para chamar APIs.
- Se uma chave de acesso for usada mais de uma vez em um período de 15 minutos, a coluna **Last Used** na área **Access Keys** exibirá apenas o horário do primeiro uso.

- Criar uma chave de acesso

  a. Clique em **Create Access Key**.

  Figura 3-27 Criar uma chave de acesso

> **NOTA**
>
> Cada usuário tem no máximo duas chaves de acesso, e as chaves de acesso são permanentemente válidas. Para fins de segurança, altere as chaves de acesso dos usuários do IAM periodicamente.

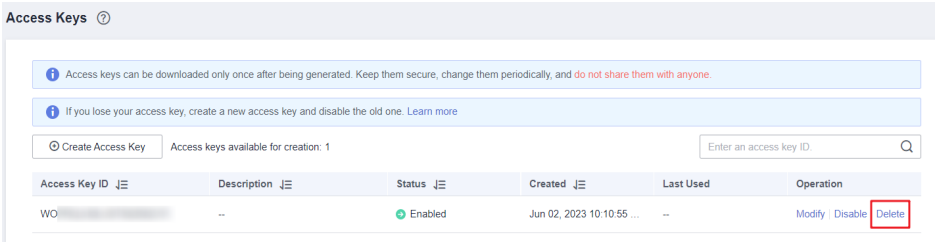
b. (Opcional) Se a proteção de operação estiver ativada, você precisará inserir um código de verificação ou uma senha.

c. Clique em **OK**. Uma chave de acesso é gerada automaticamente. Baixe a chave de acesso e forneça-a ao usuário.

- Excluir uma chave de acesso

a. Na lista de chaves de acesso, clique em **Delete** na linha que contém a chave de acesso a ser excluída.

Figura 3-28 Excluir uma chave de acesso



b. (Opcional) Se a proteção de operação estiver ativada, você precisará inserir um código de verificação ou uma senha.

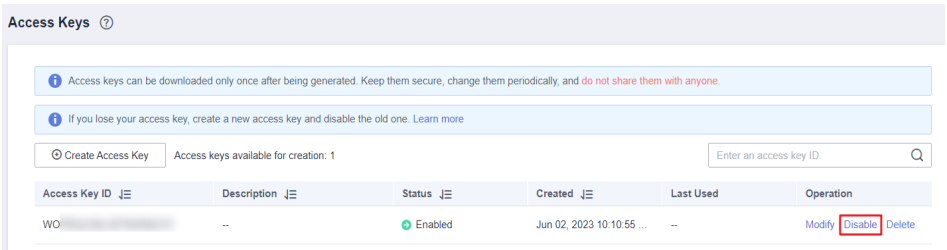
c. Clique em **Yes**.

- Ativar/desativar uma chave de acesso

Novas chaves de acesso são ativadas por padrão. Para desativar uma chave de acesso, execute as seguintes etapas:

a. Na lista de chaves de acesso, clique em **Disable** na linha que contém a chave de acesso que você deseja desativar.

Figura 3-29 Desativar uma chave de acesso



b. (Opcional) Se a proteção de operação estiver ativada, você precisará inserir um código de verificação ou uma senha e clicar em **Yes**.

O método de ativação de uma chave de acesso é semelhante ao de desativação de uma chave de acesso.

4 Grupos de usuários e autorização

4.1 Criação de um grupo de usuários e atribuição de permissões

Como administrador, você pode criar grupos de usuários e conceder permissões a eles anexando políticas ou funções. Os usuários que você adiciona aos grupos de usuários herdam permissões das políticas ou funções. Os usuários do IAM podem atribuir permissões a si mesmos. O IAM fornece permissões gerais (como permissões de administrador ou somente leitura) para cada serviço de nuvem, que você pode atribuir a grupos de usuários. Os usuários nos grupos podem então usar serviços de nuvem com base nas permissões atribuídas. Para mais detalhes, consulte **3.2 Atribuição de permissões a um usuário do IAM**. **Para obter detalhes sobre as permissões definidas pelo sistema de todos os serviços de nuvem, consulte Permissões definidas pelo sistema**.

Pré-requisitos

Antes de criar um grupo de usuários, saiba mais sobre o seguinte:

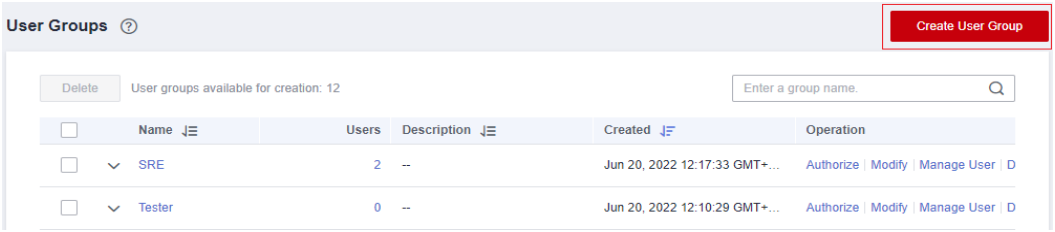
- Entenda os **conceitos básicos** de permissões.
- Conheça as **permissões definidas pelo sistema** fornecidas pelo IAM.

Criação de um grupo de usuários

Passo 1 Faça logon no **console do IAM** como administrador.

Passo 2 No console do IAM, escolha **User Groups** no painel de navegação e clique em **Create User Group** no canto superior direito.

Figura 4-1 Criação de um grupo de usuários



Passo 3 Na página exibida, insira um nome de grupo de usuários.

Passo 4 Clique em **OK**.

NOTA

Você pode criar um máximo de 20 grupos de usuários. Para criar mais grupos de usuários, aumente a cota referindo-se a **Como aumentar minha cota?**

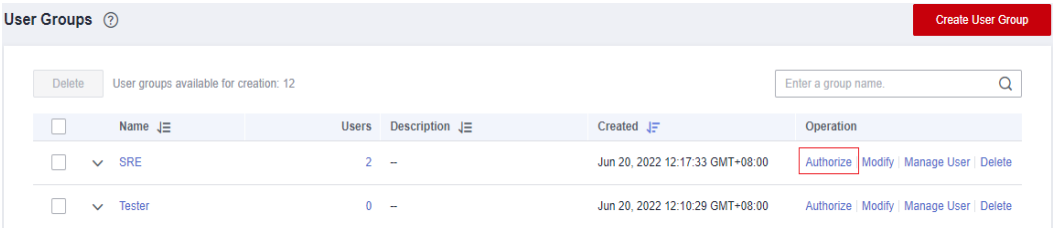
----Fim

Atribuição de permissões a um grupo de usuários

Para atribuir permissões a um grupo de usuários, faça o seguinte. Para revogar permissões de um grupo de usuários, consulte **4.5 Revogação de permissões de um grupo de usuários**.

Passo 1 Na lista de grupos de usuários, clique em **Authorize** na linha que contém o grupo de usuários criado.

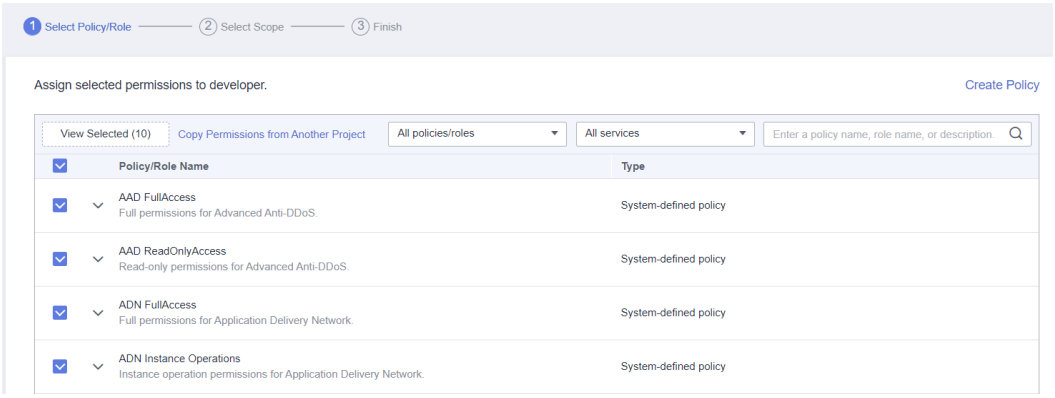
Figura 4-2 Acessar a página de autorização do grupo de usuários



Passo 2 Na página **Authorize User Group**, selecione as permissões a serem atribuídas ao grupo de usuários e clique em **Next**.

Se as políticas definidas pelo sistema não atenderem aos seus requisitos, clique em **Create Policy** no canto superior direito para criar políticas personalizadas. Você pode usá-las para complementar as políticas definidas pelo sistema para um controle refinado das permissões. Para mais detalhes, consulte **5.6.1 Criação de uma política personalizada**.

Figura 4-3 Seleção de permissões



Passo 3 Especifique o escopo. O sistema recomenda automaticamente um escopo de autorização para as permissões selecionadas. **Tabela 4-1** descreve todos os escopos de autorização fornecidos pelo IAM.

Tabela 4-1 Escopos de autorização

Escopo	Descrição
All resources	Os usuários do IAM poderão usar todos os recursos, incluindo aqueles em projetos empresariais, projetos da região específica e serviços globais em sua conta com base nas permissões atribuídas.
Enterprise projects	Os usuários do IAM podem usar os recursos nos projetos empresariais selecionados com base nas permissões atribuídas. Essa opção está disponível somente quando o Enterprise Project está ativado. Para obter detalhes sobre projetos empresariais, consulte **O que é o Enterprise Project Management Service?**. Para ativar Enterprise Project, consulte **Ativação da função Enterprise Project**.
Region-specific projects	Os usuários do IAM podem usar os recursos nos projetos da região específica selecionados com base nas permissões atribuídas. Se você selecionou permissões de serviço global e especificou o escopo como **Region-specific projects**, as permissões de serviço global serão aplicadas a todos os recursos por padrão. As permissões selecionadas para serviços no nível do projeto serão aplicadas aos projetos da região específica que você selecionar. **NOTA** Projetos da região específica em Dedicated Cloud não são suportados.
Global services	Os usuários do IAM podem usar serviços globais com base nas permissões atribuídas. Os serviços globais são implementados sem regiões físicas especificadas. Os usuários do IAM não precisam especificar uma região ao acessar esses serviços, como Object Storage Service (OBS) e Content Delivery Network (CDN). Se você selecionou permissões de serviço no nível do projeto e especificou o escopo como **Global services**, as permissões de serviço no nível do projeto serão aplicadas a todos os recursos por padrão. As permissões selecionadas para serviços globais ainda serão aplicadas aos serviços globais selecionados.

Passo 4 Clique em **OK**.

----Fim

Tabela 4-2 lista as permissões comuns. Para obter a lista completa de permissões específicas do serviço, consulte **Permissões definidas pelo sistema**.

NOTA

- Se você adicionar um usuário a vários grupos, o usuário herdará todas as permissões que foram atribuídas a esses grupos.
- Para obter mais informações sobre gerenciamento de permissões, consulte **Atribuição de permissões ao pessoal de O&M**, **4.6 Atribuição de funções de dependência** e **5.6.3 Casos de uso de políticas personalizadas**.

Tabela 4-2 Permissões comuns

Categoria	Nome da política/ função	Descrição	Escopo de autorização
Administração geral	FullAccess	Permissões completas para serviços que suportam controle de acesso baseado em políticas.	Todos
Gerenciamento de recursos	Tenant Administrator	Permissões de administrador para todos os serviços, exceto o IAM.	Todos
Visualização de recursos	Tenant Guest	Permissões somente leitura para todos os recursos.	Todos
Gerenciamento de usuários do IAM	Security Administrator	Permissões de administrador para o IAM.	Global services
Gerenciamento de contabilidade	BSS Administrator	Permissões de administrador para a Central de cobrança, incluindo o gerenciamento de faturas, pedidos, contratos e renovações, além da visualização de faturas. **NOTA** Essa função depende da função **BSS Administrator** para entrar em vigor.	Region-specific projects
O&M de computação	ECS FullAccess	Permissões de administrador para o ECS.	Region-specific projects

Categoria	Nome da política/ função	Descrição	Escopo de autorização
	CCE FullAccess	Permissões de administrador para o Cloud Container Engine (CCE).	Region-specific projects
	CCI FullAccess	Permissões de administrador para Cloud Container Instance (CCI).	Region-specific projects
	BMS FullAccess	Permissões de administrador para Bare Metal Server (BMS).	Region-specific projects
	IMS FullAccess	Permissões de administrador para Image Management Service (IMS).	Region-specific projects
	AutoScaling FullAccess	Permissões de administrador para Auto Scaling (AS).	Region-specific projects
O&M de rede	VPC FullAccess	Permissões de administrador para Virtual Private Cloud (VPC).	Region-specific projects
	ELB FullAccess	Permissões de administrador para Elastic Load Balance (ELB).	Region-specific projects
O&M do banco de dados	RDS FullAccess	Permissões de administrador para Relational Database Service (RDS).	Region-specific projects
	DDS FullAccess	Permissões de administrador para Document Database Service (DDS).	Region-specific projects
	DDM FullAccess	Permissões de administrador para Distributed Database Middleware (DDM).	Region-specific projects
O&M de segurança	Anti-DDoS Administrator	Permissões de administrador para Anti-DDoS.	Region-specific projects
	AAD Administrator	Permissões de administrador para Advanced Anti-DDoS (AAD).	Region-specific projects

Categoria	Nome da política/ função	Descrição	Escopo de autorização
	WAF Administrator	Permissões de administrador para Web Application Firewall (WAF).	Region-specific projects
	VSS Administrator	Permissões de administrador para Vulnerability Scan Service (VSS).	Region-specific projects
	CGS Administrator	Permissões de administrador para Container Guard Service (CGS).	Region-specific projects
	KMS Administrator	Permissões de administrador para Key Management Service (KMS), que foi renomeado para Data Encryption Workshop (DEW).	Region-specific projects
	DBSS System Administrator	Permissões de administrador para Database Security Service (DBSS).	Region-specific projects
	SES Administrator	Permissões de administrador para Security Expert Service (SES).	Region-specific projects
	SC Administrator	Permissões de administrador para SSL Certificate Manager (SCM).	Region-specific projects

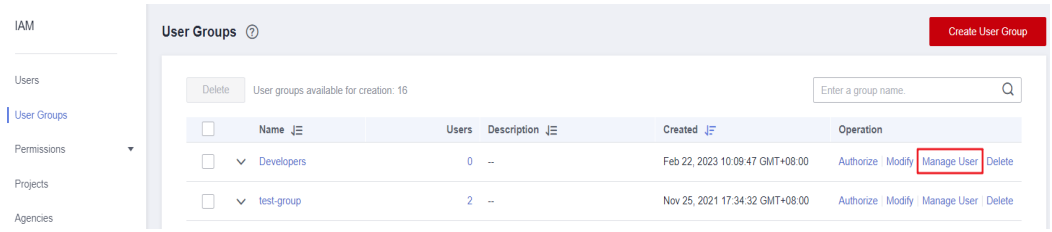
4.2 Adição ou remoção de usuários de um grupo de usuários

Um usuário herda permissões dos grupos aos quais o usuário pertence. Para alterar as permissões de um usuário, adicione o usuário a um novo grupo ou remova o usuário de um grupo existente.

Adição de usuários a um grupo de usuários

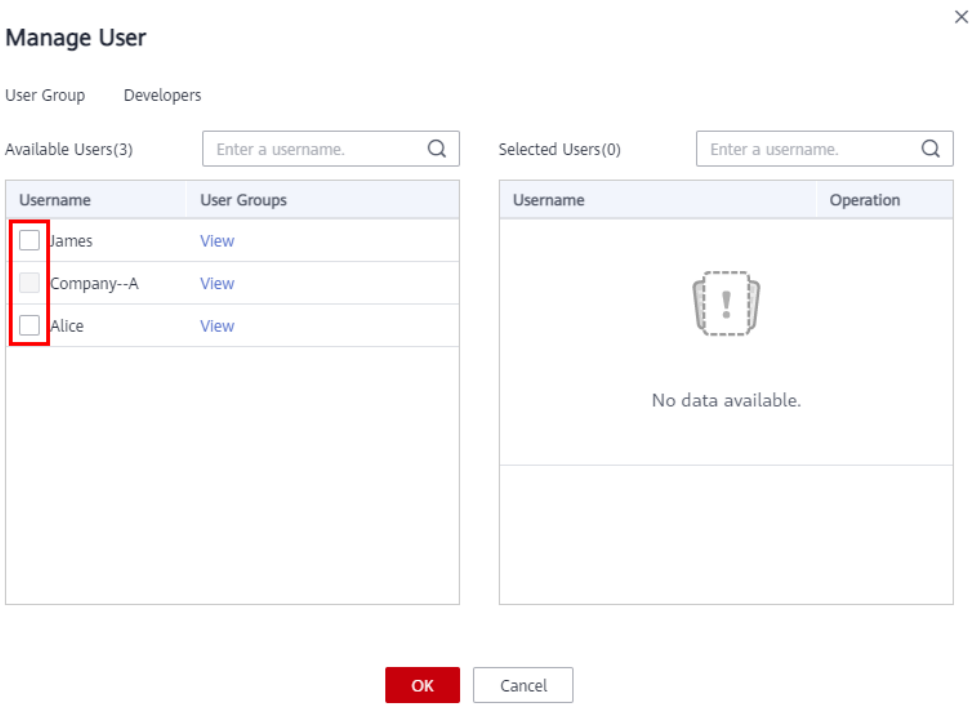
Passo 1 Na lista de grupos de usuários, clique em **Manage User** na linha que contém o grupo de usuários de destino.

Figura 4-4 Gerenciamento de usuários



Passo 2 Na caixa de diálogo **Manage User**, selecione os nomes de usuário a serem adicionados.

Figura 4-5 Selecionar usuários



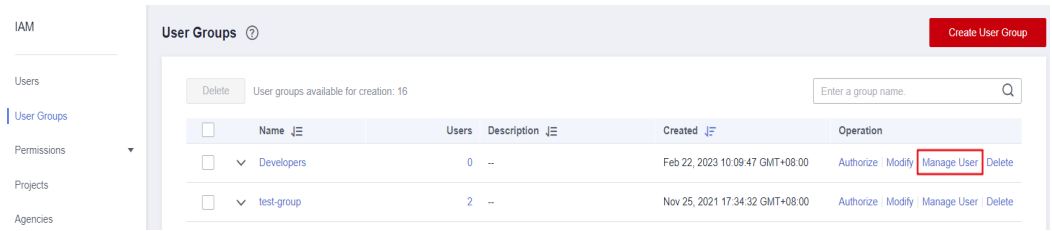
Passo 3 Clique em **OK**.

----Fim

Remoção de usuários de um grupo de usuários

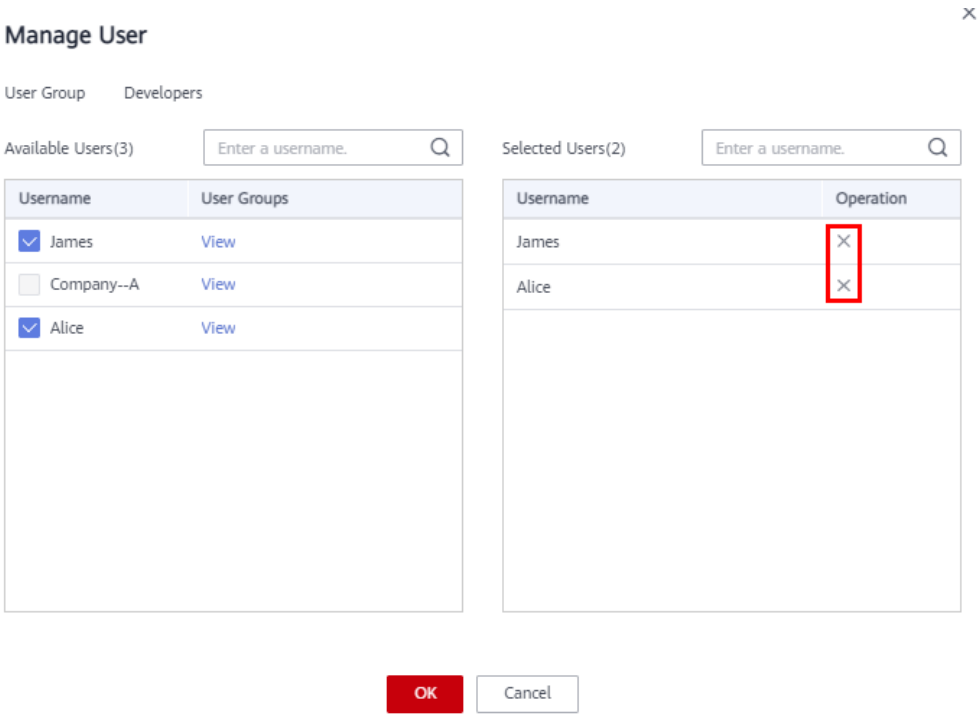
Passo 1 Na lista de grupos de usuários, clique em **Manage User** na linha que contém o grupo de usuários de destino.

Figura 4-6 Gerenciamento de usuários



Passo 2 Na área **Selected Users**, localize o usuário a ser removido e clique em ×. Em seguida, clique em **OK**.

Figura 4-7 Remoção de usuários de um grupo de usuários



----Fim

4.3 Exclusão de grupos de usuários

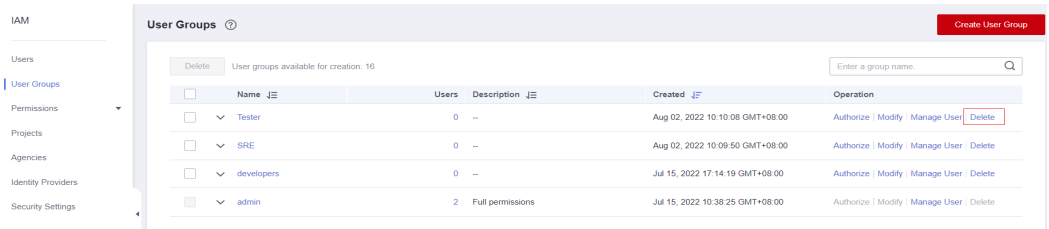
Procedimento

Para excluir um grupo de usuários, faça o seguinte:

Passo 1 Faça logon no **console do IAM**. No painel de navegação, escolha **User Groups**.

Passo 2 Na lista de grupos de usuários, clique em **Delete** na linha que contém o grupo de usuários a ser excluído.

Figura 4-8 Exclusão de um grupo de usuários



Passo 3 Na caixa de diálogo exibida, clique em **Yes**.

----Fim

Exclusão em lote de grupos de usuários

Para excluir vários grupos de usuários ao mesmo tempo, faça o seguinte:

Passo 1 Faça logon no **console do IAM**. No painel de navegação, escolha **User Groups**.

Passo 2 Na lista de grupos de usuários, selecione os grupos de usuários a serem excluídos e clique em **Delete** acima da lista.

Figura 4-9 Exclusão em lote de grupos de usuários

Passo 3 Na caixa de diálogo exibida, clique em **Yes**.

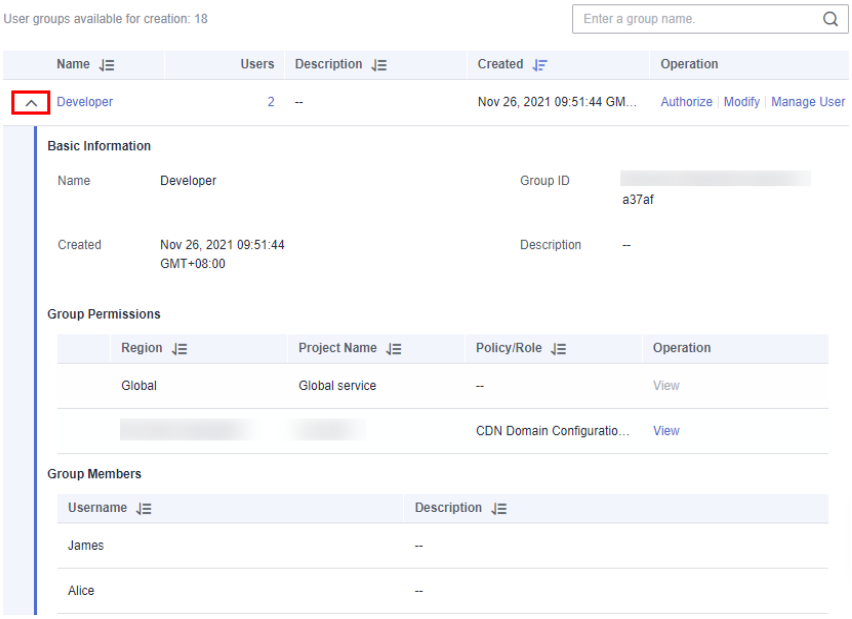
----Fim

4.4 Visualização ou modificação das informações do grupo de usuários

Visualização de informações do grupo de usuários

Na lista de grupos de usuários, clique em ao lado de um grupo de usuários para exibir suas informações básicas, permissões atribuídas e usuários gerenciados.

Figura 4-10 Exibir informações do grupo de usuários



Modificar permissões de grupo de usuários

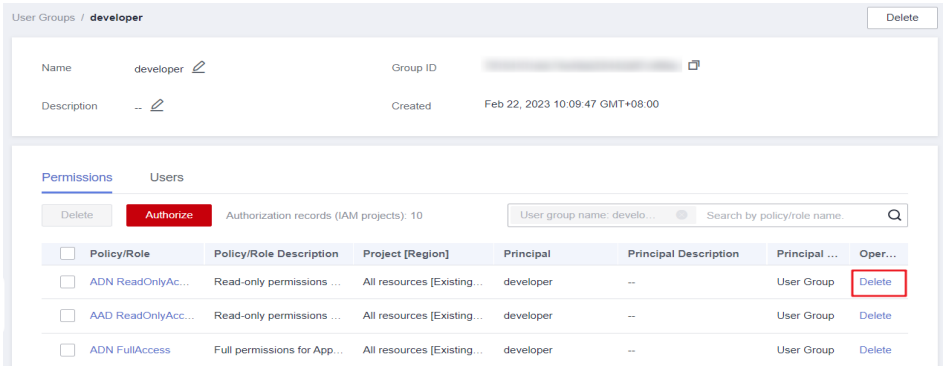
Visualize ou modifique permissões de grupos de usuários.

NOTA

- Modificar as permissões de um grupo de usuários afeta as permissões de todos os usuários no grupo de usuários. Tenha cuidado ao realizar esta operação.
- As permissões do grupo de usuários padrão **admin** não podem ser modificadas.

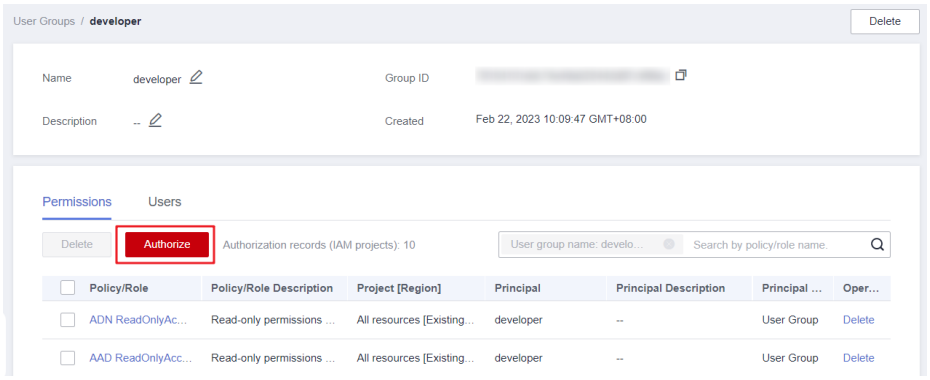
1. Clique no nome de um grupo de usuários (por exemplo, **Developers**) para acessar a página de detalhes e exibir as permissões do grupo na guia **Permissions**.
2. Clique em **Delete** na linha que contém a função ou política que você deseja excluir.

Figura 4-11 Excluir uma permissão atribuída



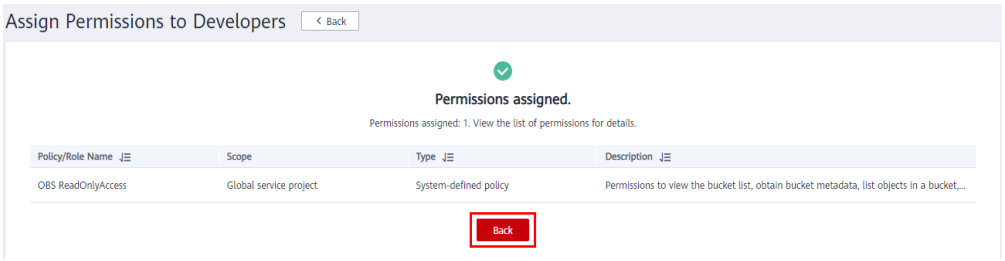
3. Clique em **Yes**.
4. Na guia **Permissions**, clique em **Authorize**.

Figura 4-12 Atribuição de permissões a um grupo de usuários



5. Selecione as permissões desejadas e um escopo e clique em **OK**.
6. Volte para a guia **Permissions** para exibir as permissões de grupo modificadas.

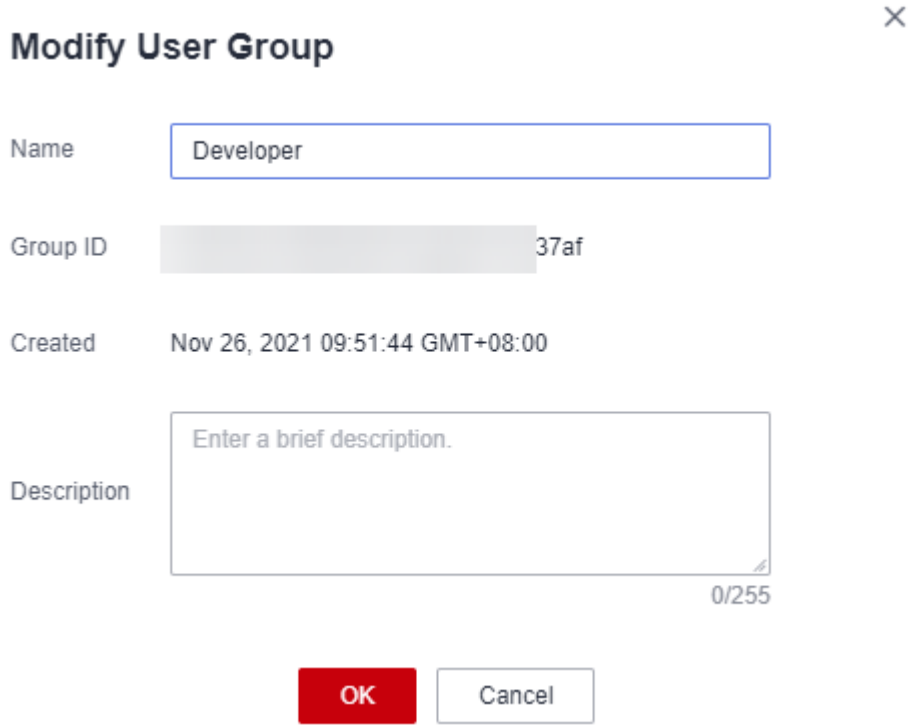
Figura 4-13 Voltar para a guia Permissions



Modificar o nome e a descrição de um grupo de usuários

Na lista de grupos de usuários, clique em **Modify** na linha que contém o grupo de usuários cujo nome e descrição você deseja modificar e modifique o nome e a descrição.

Figura 4-14 Modificar o nome e a descrição do grupo de usuários



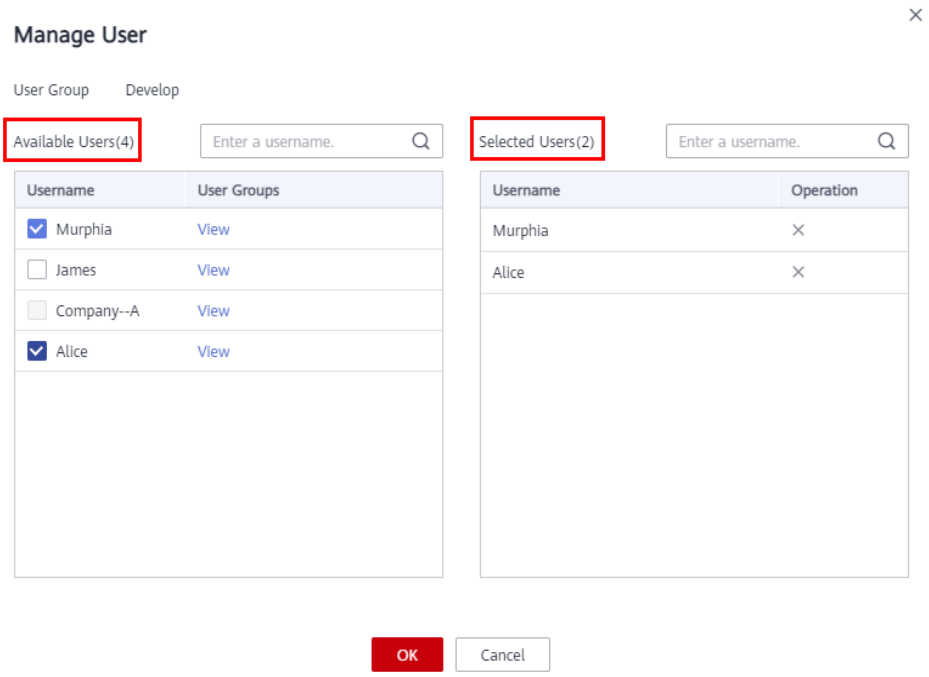
NOTA

Se um nome de grupo de usuários tiver sido configurado nas regras de conversão de identidade de um provedor de identidade, a modificação do nome do grupo de usuários fará com que as regras de conversão de identidade falhem. Tenha cuidado ao realizar esta operação.

Gerenciamento de usuários

Passo 1 Na lista de grupos de usuários, clique em **Manage User** na linha que contém o grupo de usuários que você deseja modificar.

Figura 4-15 Gerenciar usuários no grupo



Passo 2 Na área **Available Users**, selecione os usuários que você deseja adicionar ao grupo de usuários.

Passo 3 Na área **Selected Users**, remova os usuários do grupo de usuários.

----Fim

NOTA

Para o grupo padrão **admin**, você só pode gerenciar seus usuários e não pode modificar sua descrição ou permissões.

4.5 Revogação de permissões de um grupo de usuários

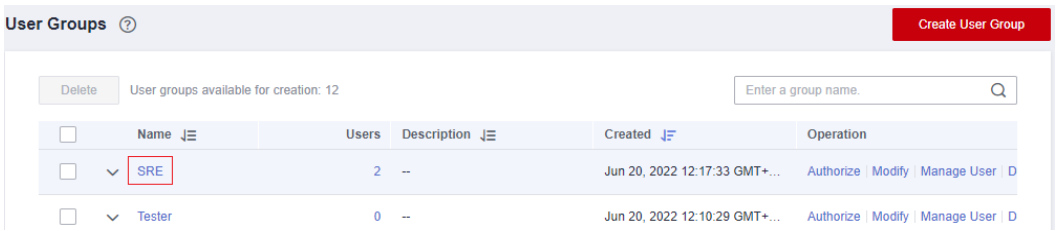
Procedimento

Para revogar uma política ou função anexada a um grupo de usuários, faça o seguinte:

Passo 1 Faça logon no **console do IAM**. No painel de navegação, escolha **User Groups**.

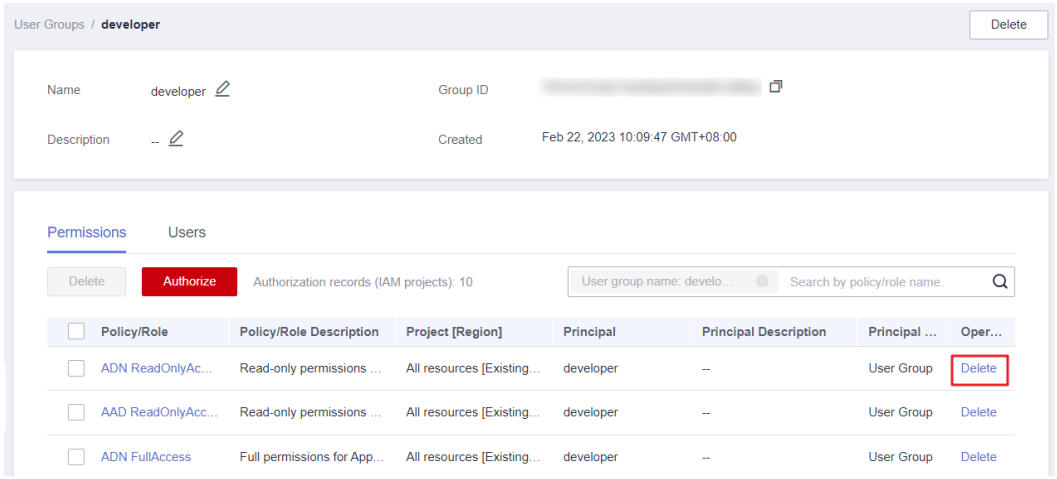
Passo 2 Clique no nome do grupo de usuários para acessar a página de detalhes do grupo.

Figura 4-16 Clicar em um nome de grupo de usuários



Passo 3 Na guia **Permissions**, clique em **Delete** na linha que contém a função ou política que você deseja excluir.

Figura 4-17 Revogação de permissões



Passo 4 Na caixa de diálogo exibida, clique em **Yes**.

----Fim

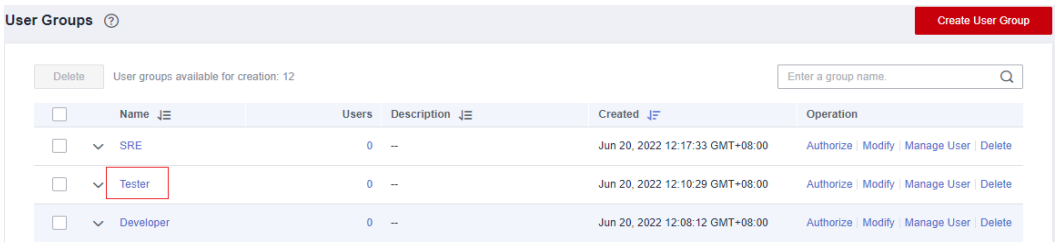
Revogar permissões em lote de um grupo de usuários

Para revogar várias políticas ou funções anexadas a um grupo de usuários, faça o seguinte:

Passo 1 Faça logon no **console do IAM**. No painel de navegação, escolha **User Groups**.

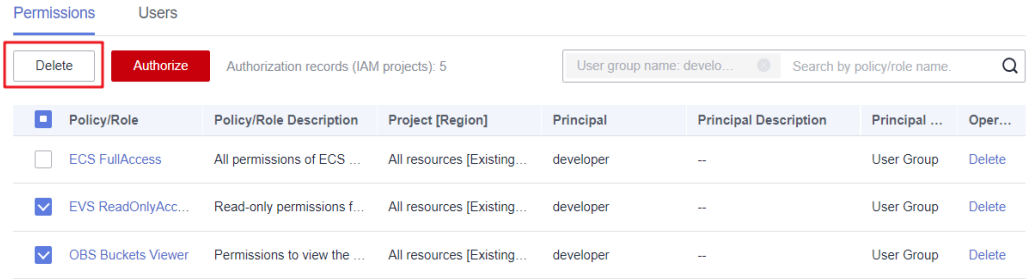
Passo 2 Clique no nome do grupo de usuários para acessar a página de detalhes do grupo.

Figura 4-18 Visualizar um grupo de usuários



Passo 3 Na página **Permissions**, selecione as funções ou políticas que deseja excluir e clique em **Delete** acima da lista.

Figura 4-19 Revogação de permissões em lote



Passo 4 Na caixa de diálogo exibida, clique em **Yes**.

----Fim

4.6 Atribuição de funções de dependência

Os serviços da Huawei Cloud interagem entre si. As funções de alguns serviços entram em vigor apenas se forem atribuídas juntamente com as funções de outros serviços.

Procedimento

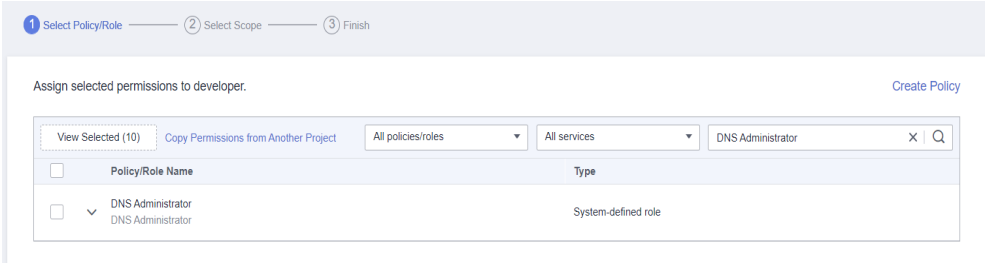
Passo 1 Faça logon no **console do IAM** como administrador.

Passo 2 Na lista de grupos de usuários, clique em **Authorize** na linha que contém o grupo de usuários criado.

Passo 3 Na página exibida, pesquise uma função na caixa de pesquisa no canto superior direito.

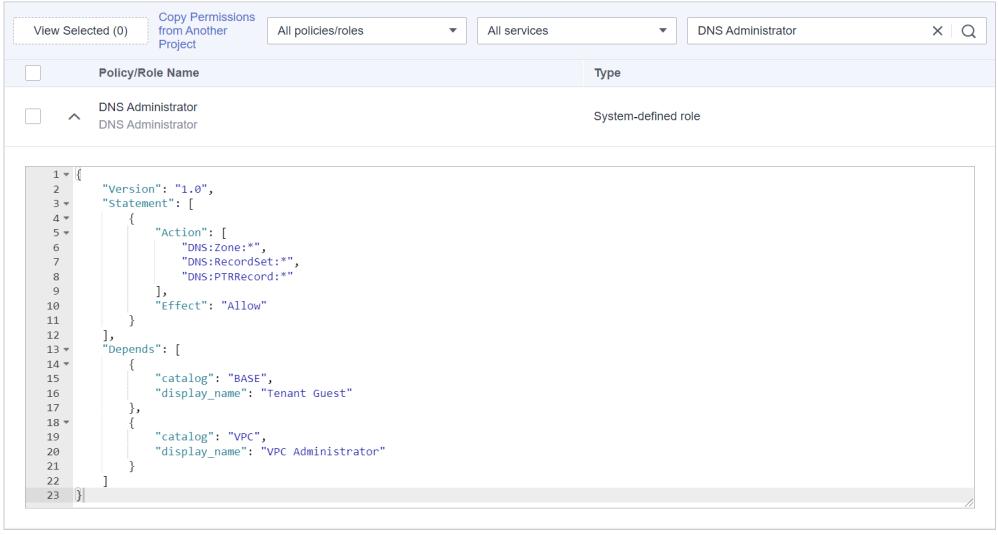
Passo 4 Selecione a função de destino. O sistema seleciona automaticamente as funções de dependência.

Figura 4-20 Selecionar uma função



Passo 5 Clique em ao lado da função para exibir as dependências.

Figura 4-21 Exibir dependências



Por exemplo, a função **DNS Administrator** contém o parâmetro **Depends** que especifica as funções de dependência. Quando você atribui a função **DNS Administrator** a um grupo de

usuários, também precisa atribuir as funções **Tenant Guest** e **VPC Administrator** ao grupo para o mesmo projeto.

Passo 6 Clique em **OK**.

----Fim

5 Gerenciamento de permissões

5.1 Conceitos básicos

Permissão

Por padrão, os usuários do IAM não têm permissões. Para atribuir permissões a usuários do IAM, adicione-os a um ou mais grupos e anexe políticas ou funções a esses grupos. Em seguida, os usuários herdam permissões dos grupos aos quais os usuários pertencem e podem executar operações específicas em serviços de nuvem.

Tipo de permissão

Você pode conceder permissões aos usuários usando funções e políticas.

- Funções: um tipo de mecanismo de autorização de alta granularidade que define permissões de nível de serviço com base nas responsabilidades do usuário. O IAM fornece um número limitado de funções para o gerenciamento de permissões. Ao usar funções para conceder permissões, você também precisa atribuir funções de dependência. As funções não são uma escolha adequada para autorização refinada e controle de acesso seguro.
- Políticas: um tipo de mecanismo de autorização refinado que define as permissões necessárias para realizar operações em recursos de nuvem específicos sob determinadas condições. Esse mecanismo permite uma autorização mais flexível baseada em políticas e um controle de acesso seguro. Por exemplo, você pode conceder aos usuários do ECS somente as permissões necessárias para gerenciar um determinado tipo de recursos do ECS.

  O IAM oferece suporte a **políticas definidas pelo sistema** e **políticas personalizadas**.

Política definida pelo sistema

Uma política definida pelo sistema define as ações comuns de um serviço de nuvem. Políticas definidas pelo sistema podem ser usadas para atribuir permissões a grupos de usuários e elas não podem ser modificadas. **Para obter detalhes sobre as políticas definidas pelo sistema de todos os serviços de nuvem, consulte Permissões de sistema**.

Se não houver políticas definidas pelo sistema para um serviço específico, isso indicará que o IAM não oferece suporte a esse serviço. Você pode **enviar um tíquete de serviço** e solicitar o gerenciamento de permissões no IAM.

Política personalizada

Você pode criar políticas personalizadas usando as ações suportadas pelos serviços de nuvem para complementar políticas definidas pelo sistema para um controle de acesso mais refinado. Você pode criar políticas personalizadas no editor visual ou na visualização JSON.

5.2 Funções

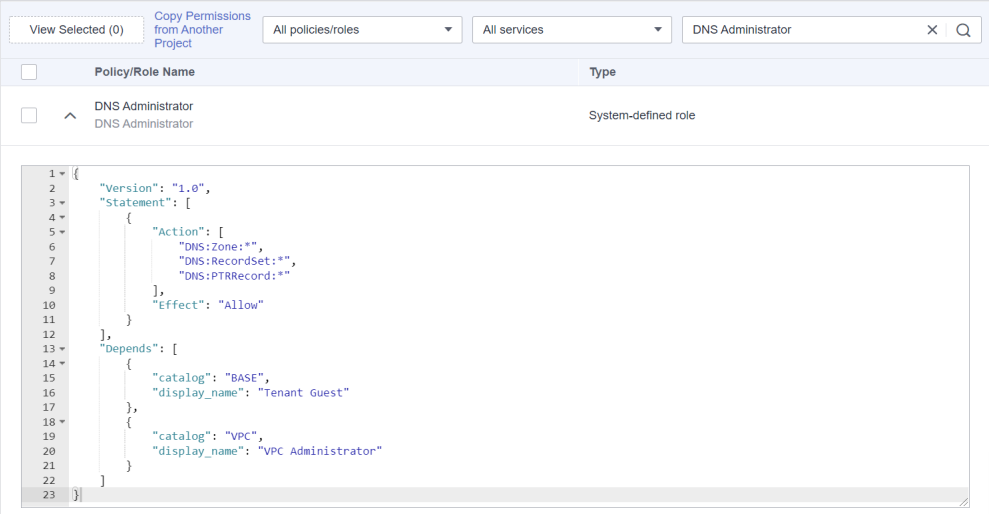
As funções são um tipo de mecanismo de autorização de alta granularidade que define permissões no nível do serviço com base nas responsabilidades do usuário. O IAM fornece um número limitado de funções para o gerenciamento de permissões.

Os serviços da Huawei Cloud interagem entre si. As funções de alguns serviços entram em vigor apenas se forem atribuídas juntamente com as funções de outros serviços. Para obter mais informações, consulte **4.6 Atribuição de funções de dependência**.

Conteúdo da função

Ao usar funções para atribuir permissões, você pode selecionar uma função e clicar em para exibir os detalhes da função. Esta seção usa a função **DNS Administrator** como um exemplo para descrever o conteúdo da função.

Figura 5-1 Conteúdo da função DNS Administrator




```
{
    "Version": "1.0",
```



```
    "Statement": [
        {
            "Action": [
                "DNS:Zone:*",
                "DNS:RecordSet:*",
                "DNS:PTRRecord:*"
            ],
            "Effect": "Allow"
        }
    ],
    "Depends": [
        {
            "catalog": "BASE",
            "display_name": "Tenant Guest"
        },
        {
            "catalog": "VPC",
            "display_name": "VPC Administrator"
        }
    ]
}
```

Descrição do parâmetro

Tabela 5-1 Descrição do parâmetro

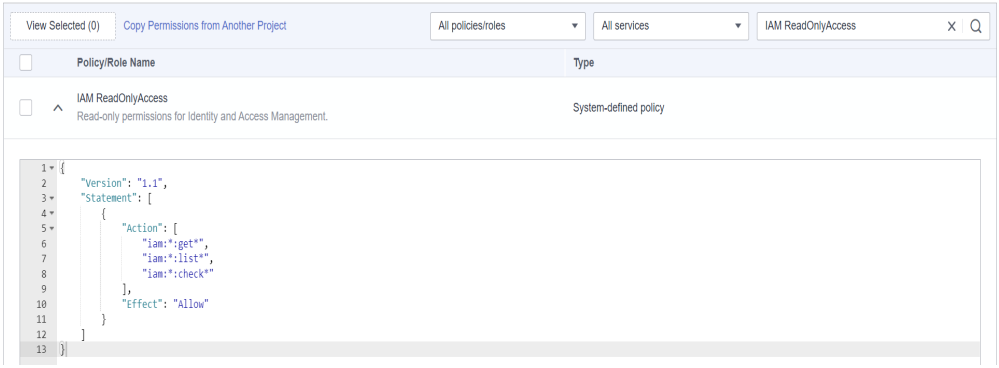
Parâmetro		Descrição	Valor
Version		Versão da função.	**1.0**: indica o controle de acesso baseado em função.
Statement	Action	Operações a serem realizadas no serviço.	Formato: "*Service name*:*Resource type*:*Operation*". **DNS:Zone:***: permissões para executar todas as operações em zonas de Domain Name Service (DNS).
	Effect	Determina se permitir ou negar as operações definidas na ação.	● Allow ● Deny **NOTA** Se uma função conceder os efeitos Allow e Deny para a mesma ação, o Deny terá precedência.
Depends	catalog	Nome do serviço ao qual pertence uma função de dependência.	Nome do serviço. Exemplo: **BASE** e **VPC**.
	display_name	Nome da função de dependência.	Nome da função. **NOTA** Quando você atribui a função **DNS Administrator** a um grupo de usuários, também precisa atribuir as funções **Tenant Guest** e **VPC Administrator** ao grupo para o mesmo projeto. Para obter mais informações sobre dependências, consulte **Permissões do sistema**.

5.3 Políticas

5.3.1 Conteúdo da política

Ao atribuir permissões a um grupo de usuários, você pode clicar em à esquerda do nome de uma política para exibir seus detalhes. Esta seção usa a política definida pelo sistema **IAM ReadOnlyAccess** como exemplo.

Figura 5-2 Conteúdo da política IAM ReadOnlyAccess




```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "iam:*:get*",
                "iam:*:list*",
                "iam:*:check*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

5.3.2 Sintaxe da política

O seguinte usa uma política personalizada para o OBS como um exemplo para descrever a sintaxe.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:bucket:ListAllMyBuckets",
                "obs:bucket:HeadBucket",
                "obs:bucket:ListBucket",
                "obs:bucket:GetBucketLocation"
            ],
            "Condition": {
                "StringEndWithIfExists": {
                    "g:UserName": [
                        "specialCharacter"
```

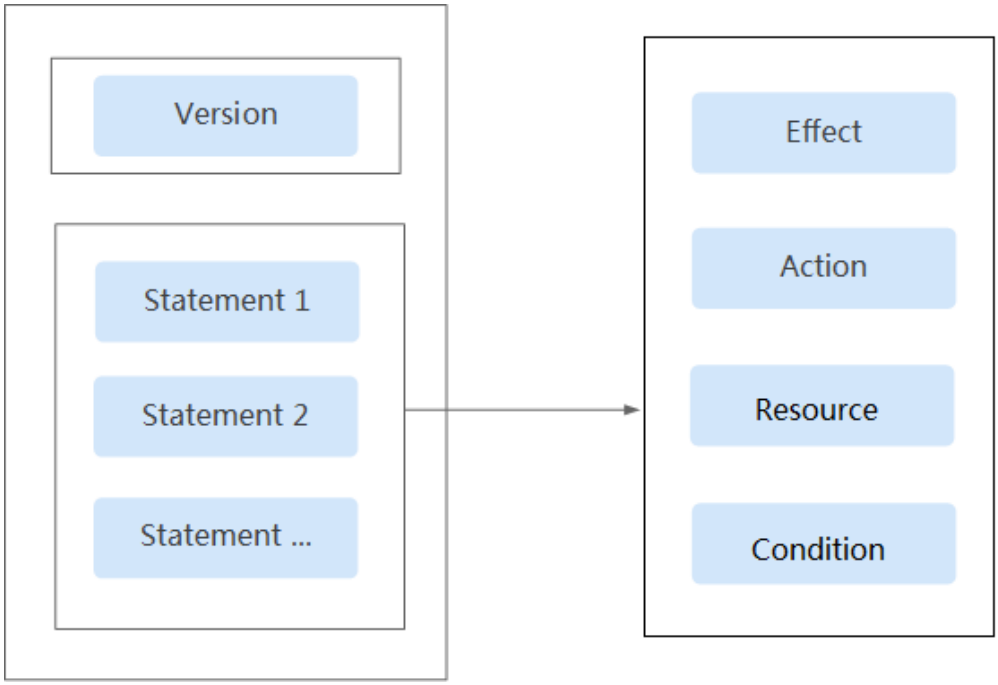


```
                    ]
                },
                "Bool": {
                    "g:MFAPresent": [
                        "true"
                    ]
                }
            },
            "Resource": [
                "obs:*:*:bucket:*"
            ]
        }
    ]
}
```

Estrutura da política

Uma política consiste em uma versão e uma ou mais instruções (indicando ações diferentes).

Figura 5-3 Estrutura da política



Parâmetros de política

Os parâmetros de política incluem **Version** e **Statement**, que são descritos na tabela a seguir. Você pode criar políticas personalizadas especificando os parâmetros. Para mais detalhes, consulte **5.6.3 Casos de uso de políticas personalizadas**.

Tabela 5-2 Parâmetros de política

Parâmetro	Descrição	Valor
Version	Versão da política.	**1.1**: indica o controle de acesso baseado em políticas.

Parâmetro		Descrição	Valor
Statement	Effect	Determina se permitir ou negar as operações definidas na ação.	● Allow ● Deny **NOTA** Se uma ação tiver efeitos Allow e Deny, o efeito Deny terá precedência.
	Action	Operações a serem realizadas no serviço.	Formato: "*Service name*:*Resource type*:*Operation*". Caracteres curinga (*) são suportados, indicando todas as opções. Exemplo: **obs:bucket:ListAllMybuckets**: permissões para listar todos os buckets do OBS. Veja todas as ações do serviço em sua *Referência de API*, por exemplo, veja **Ações suportadas de OBS**.
	Condition	Determina quando uma política entra em vigor. Uma condição consiste em uma **chave de condição** e um **operador**.	Formato: "*Condition operator*:{*Condition key*:[*Value 1*,*Value 2*]}" Se você definir várias condições, a política terá efeito somente quando todas as condições forem atendidas. Exemplo: **StringEndWithIfExists":{"g:UserName":["specialCharacter"]}**: a instrução é válida para usuários cujos nomes terminam com **specialCharacter**.
	Resource	Recursos nos quais a política entra em vigor.	Formato: *Service name*:*Region*:*Account ID*:*Resource type*:*Resource path*. Caracteres curinga (*) são suportados. Para obter detalhes sobre serviços de nuvem que suportam autorização em nível de recurso e tipos de recursos suportados, consulte **Serviços de nuvem que suportam a autorização em nível de recurso usando o IAM**. Exemplo: ● **obs:*:*:bucket:***: todos os buckets do OBS. ● **obs:*:*:object:my-bucket/my-object/***: todos os objetos no diretório **my-object** do bucket **my-bucket**.

- **Chave de condição**

  Uma chave de condição é uma chave no elemento **Condition** de uma instrução. Existem chaves de condição globais e de nível de serviço.

  – As chaves de condição global (começando com **g:**) se aplicam a todas as operações. O IAM fornece **common global condition keys** e **special global condition keys**.

    ■ Chaves de condição global comuns: os serviços de nuvem não precisam fornecer informações de identidade do usuário. Em vez disso, o IAM abstrai automaticamente as informações do usuário e autentica os usuários. Para mais detalhes, consulte **Tabela 5-3**.

    ■ Chaves de condição global especiais: o IAM obtém informações de condição dos serviços de nuvem para autenticação. Apenas determinados serviços de nuvem suportam chaves de condição global especiais.

  – Chaves de condição de nível de serviço (começando com uma abreviação de nome de serviço, por exemplo, **obs:**) aplicam-se apenas a operações no serviço especificado. Para obter detalhes, consulte o guia do usuário do serviço de nuvem correspondente, por exemplo, consulte **Condições de solicitação de OBS**.

Tabela 5-3 Chaves de condição global comuns

Chave de condição global	Tipo	Descrição
g:CurrentTime	Time	Hora em que uma solicitação de autenticação é recebida. A hora está no formato ISO 8601, por exemplo, **2012-11-11T23:59:59Z**. (**Veja um exemplo de política que usa essa chave de condição**)
g:DomainName	String	Nome da conta do solicitante. (**Veja um exemplo de política que usa essa chave de condição**)
g:MFAPresent	Boolean	Se deseja obter um token por meio da autenticação MFA. (**Veja um exemplo de política que usa essa chave de condição**)
g:MFAAge	Number	Período de validade de um token obtido por meio da autenticação MFA. Esta condição deve ser usada em conjunto com **g:MFAPresent**. (**Veja um exemplo de política que usa essa chave de condição**)
g:ProjectName	String	Nome do projeto. (**Veja um exemplo de política que usa essa chave de condição**)
g:ServiceName	String	Nome do serviço. (**Veja um exemplo de política que usa essa chave de condição**)
g:UserId	String	ID do usuário do IAM. (**Veja um exemplo de política que usa essa chave de condição**)
g:UserName	String	Nome de usuário do IAM. (**Veja um exemplo de política que usa essa chave de condição**)

Tabela 5-4 Chaves de condição global especiais

Chave de condição global	Tipo	Descrição
g:SourceIp	IP Address	Endereço IP do usuário que envia uma solicitação.
g:SourceVpc	String	ID de VPC do usuário que envia uma solicitação.
g:SourceVpce	String	ID do ponto de extremidade da VPC do usuário que está enviando uma solicitação.
g:TagKeys	String	Chave de tag de recurso.
g:ResourceTag/{TagKey}	String	Valor da chave da tag de recurso.

a. **g:CurrentTime**

Exemplo: a política a seguir concede permissão para criar funções personalizadas no IAM de 1º de março de 2023, 08:00 GMT+08:00 a 30 de março de 2023, 08:00 GMT+08:00. O valor da chave de condição **g:CurrentTime** está no formato UTC.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        "DateGreaterThan": {
                                "g:CurrentTime":
["2023-03-01T00:00:00Z"]
                        },
                        "DateLessThan": {
                                "g:CurrentTime":
["2023-03-30T00:00:00Z"]
                        }
                }
        }]
}
```

b. **g: DomainName**

Exemplo: a política a seguir só permite que o usuário **zhangsan** crie funções personalizadas no IAM.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        "StringEquals": {
                                "g:DomainName": ["zhangsan"]
                        }
                }
        }]
}
```

c. **g:MFAPresent**

Exemplo: a política a seguir permite que os usuários que obtêm credenciais usando a MFA criem funções personalizadas no IAM.


```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        "Bool": {
                                "g:MFAPresent": ["true"]
                        }
                }
        }]
}
```

d. **g:MFAAge**

Exemplo: a política a seguir permite que os usuários que obtêm credenciais usando a MFA com o período válido maior que 900s criem funções personalizadas no IAM.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        " NumberGreaterThanEquals ": {
                                "g:MFAAge": ["900"]
                        }
                }
        }]
}
```

e. **g:ProjectName**

Exemplo: a política a seguir permite que os usuários que obtêm credenciais em **CN North-Beijing** criem funções personalizadas no IAM.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        " StringEquals ": {
                                "g: ProjectName ": ["cn-north-4"]
                        }
                }
        }]
}
```

f. **g: ServiceName**

Exemplo: a política a seguir permite que os usuários acessem todos os serviços, exceto o IAM. O valor dessa chave de condição corresponde ao **Service Name** na solicitação de autenticação.

```
{
        "Version": "1.1",
        "Statement": [{
                "Action": [
                        "*:*:*"
                ],
                "Effect": "Allow",
                "Condition": {
                        "StringNotEqualsIgnoreCase": {
                                "g:ServiceName": [
                                        "iam"
                                ]
                        }
                }
        }]
}
```


g. **g: UserId**

Exemplo: a política a seguir só permite o usuário cujo ID é **xxxxxxxxxxx…** para criar funções personalizadas no IAM.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        "StringEquals": {
                                "g: UserId ": ["xxxxxxxxxxx…"]
                        }
                }
        }]
}
```

h. **g: UserName**

Exemplo: a política a seguir só permite que o usuário **lisi** crie funções personalizadas no IAM.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        "StringEquals": {
                                "g: UserName ": ["lisi"]
                        }
                }
        }]
}
```

– Chaves de condição multivalorada

i. ForAllValues: testa se o valor de cada membro do conjunto de solicitações é um subconjunto do conjunto de chaves de condição. A condição retorna true se cada valor de chave na solicitação corresponder a pelo menos um valor na política.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ims:images:share"
            ],
            "Condition": {
                "ForAllValues:StringEquals": {
                    "ims:TargetOrgPaths": [
                        "orgPath1",
                        "orgPath2",
                        "orgPath3"
                    ]
                }
            }
        }
    ]
}
```

Esta política mostra como usar o qualificador ForAllValues com o operador de condição StringEquals. A condição determina se o compartilhamento deve ser permitido com as contas de membros no caminho de organização orgPath1, orgPath2 ou orgPath3.

Suponha que um usuário faça uma solicitação para compartilhar o IMS com as contas de membros nos caminhos de organização orgPath1 e orgPath3. A

solicitação é permitida porque os atributos solicitados pelo usuário correspondem todos aos valores especificados na política.

Se a solicitação do usuário incluir orgPath1, orgPath2, orgPath3 e orgPath4, a solicitação falhará porque orgPath4 não está incluído no operador de condição.

ii. ForAnyValue: testa se pelo menos um membro do conjunto de valores de solicitação corresponde a pelo menos um membro do conjunto de valores de chave de condição. A condição retornará true se qualquer um dos valores de chave na solicitação corresponder a qualquer um dos valores de condição na política. Para nenhuma chave correspondente ou um conjunto de dados nulo, a condição retorna false.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ims:images:share"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "ims:TargetOrgPaths": [
                        "orgPath1",
                        "orgPath2",
                        "orgPath3"
                    ]
                }
            }
        }
    ]
}
```

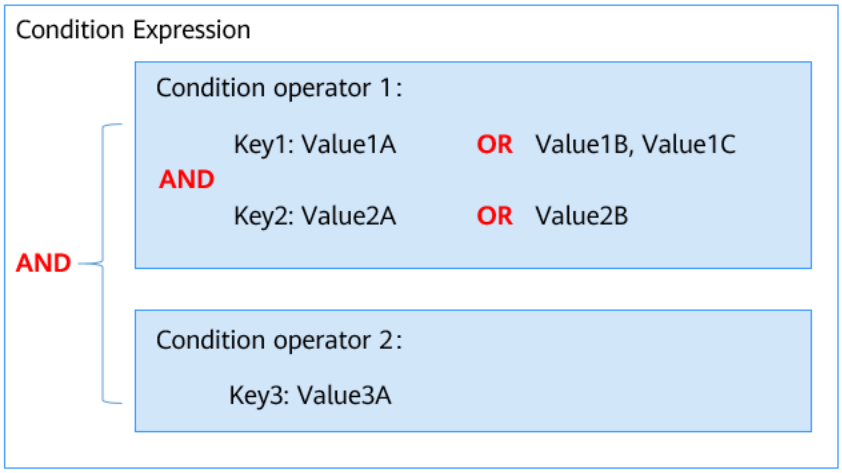
Esta política mostra como usar o qualificador ForAnyValue com o operador de condição StringEquals. A condição determina se o compartilhamento deve ser permitido com as contas de membros no caminho de organização orgPath1, orgPath2 ou orgPath3.

Suponha que um usuário faça uma solicitação para compartilhar o IMS com as contas de membros no caminho da organização orgPath1 ou orgPath4. A solicitação é permitida porque os atributos solicitados pelo usuário correspondem todos aos valores especificados na política.

Se o usuário iniciar uma solicitação para compartilhar o IMS com as contas de membros no caminho da organização orgPath4 ou orgPath5, a solicitação falhará porque orgPath4 e orgPath5 não estão incluídos no operador de condição.

Operadores de condição

Figura 5-4 Operadores de condição



a. Se um único operador de condição incluir vários valores para uma chave, esse operador de condição será avaliado usando um OR lógico. A condição retornará **true** se qualquer um dos valores de chave na solicitação corresponder a qualquer um dos valores de condição na política.

AVISO

Para operadores de condição de correspondência negada (como StringNotEquals), o valor da solicitação não pode corresponder a nenhum dos valores de condição com base nos operadores de condição.

b. Se a política tiver vários operadores de condição ou várias chaves anexadas a um único operador de condição, as condições serão avaliadas usando um AND lógico.

- **Operador**

  Um operador, uma chave de condição e um valor de condição juntos constituem uma instrução de condição completa. Uma política só entra em vigor quando suas condições de solicitação são atendidas. O sufixo **IfExists** do operador indica que uma política entra em vigor se um valor de solicitação estiver vazio ou atender à condição especificada. Por exemplo, se o operador **StringEqualsIfExists** for selecionado para uma política, a política entrará em vigor se o valor da solicitação estiver vazio ou igual ao valor da condição especificada. Os operadores são operadores de cadeia de caracteres. Eles não diferenciam maiúsculas de minúsculas, a menos que especificado de outra forma.

  – Operadores de condição de cadeia de caracteres

  Tabela 5-5 Operadores de condição de cadeia de caracteres

Tipo	Operador	Descrição
String	StringEquals	Correspondência exata, distinção entre maiúsculas e minúsculas
	StringNotEquals	Correspondência negada, distinção entre maiúsculas e minúsculas

Tipo	Operador	Descrição
	StringEqualsIgnoreCase	Correspondência exata
	StringNotEqualsIgnore-Case	Correspondência negada
	StringMatch	Correspondência com distinção entre maiúsculas e minúsculas. Os valores são expressões regulares que suportam apenas curingas de correspondência de vários caracteres (*) e curingas de correspondência de um único caractere (?).
	StringNotMatch	Correspondência negada com distinção entre maiúsculas e minúsculas. Os valores são expressões regulares que suportam apenas curingas de correspondência de vários caracteres (*) e curingas de correspondência de um único caractere (?).

Por exemplo, a instrução a seguir contém um elemento de condição que usa "g:DomainName" para especificar que o principal cujo nome de domínio é "ZhangSan" pode obter o conteúdo e os metadados do objeto.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:GetObject"
            ],
            "Condition": {
                "StringEquals": {
                    "g:DomainName": [
                        "ZhangSan"
                    ]
                }
            }
        }
    ]
}
```

– Operadores de condição numérica

Tabela 5-6 Operadores de condição numérica

Tipo	Operador	Descrição
Number	NumberEquals	Correspondência
	NumberNotEquals	Correspondência negada
	NumberLessThan	Correspondência "menor que"

Tipo	Operador	Descrição
	NumberLessThanEquals	Correspondência "menor que ou igual a"
	NumberGreaterThan	Correspondência "maior que"
	NumberGreaterThanEquals	Correspondência "maior que ou igual a"

Por exemplo, a instrução a seguir contém um elemento de condição que usa o operador de condição "NumericLessThanEquals" com a chave "obs:max-keys" para especificar que o solicitante pode listar até 10 objetos em "example_bucket" de cada vez.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:bucket:ListBucket"
            ],
            "Resource": [
                "OBS:*:*:bucket:example_bucket"
            ],
            "Condition": {
                "NumberLessThanEquals": {
                    "obs:max-keys": [
                        "10"
                    ]
                }
            }
        }
    ]
}
```

– Operadores de condição de data

Tabela 5-7 Operadores de condição de data

Tipo	Operador	Descrição
Date	DateLessThan	Correspondência antes de uma data e hora específicas
	DateLessThanEquals	Correspondência em ou antes de uma data e hora específicas
	DateGreaterThan	Correspondência após uma data e hora específicas
	DateGreaterThanEquals	Correspondência em ou após uma data e hora específicas

Por exemplo, a instrução a seguir contém um elemento de condição que usa o operador de condição "DateLessThan" com a chave "g:CurrentTime" para especificar que o solicitante só pode criar buckets antes de 1º de agosto de 2022.


```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:bucket:CreateBucket"
            ],
            "Condition": {
                "DateLessThan": {
                    "g:CurrentTime": [
                        "2022-08-01T00:00:00Z"
                    ]
                }
            }
        }
    ]
}
```

– Operadores de condição Bool

Tabela 5-8 Operadores de condição Bool

Tipo	Operador	Descrição
Bool	Bool	As condições Boolean permitem que você construa elementos de condição que restringem o acesso com base na comparação de uma chave com "true" ou "false".

Por exemplo, essa política baseada em identidade usa o operador de condição Bool com a chave "g:MFAPresent" para permitir que apenas solicitantes com MFA ativada possam modificar as chaves de acesso permanentes especificadas.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:credentials:updateCredential"
            ],
            "Condition": {
                "Bool": {
                    "g:MFAPresent": [
                        "true"
                    ]
                }
            }
        }
    ]
}
```

– Operadores de condição Null

Tabela 5-9 Operadores de condição Null

Tipo	Operador	Descrição
Null	Null	Use um operador de condição Null para verificar se uma chave de condição está ausente no momento da autorização. Na instrução de política, use "true" (a chave não existe ou é nula) ou "false" (a chave existe e seu valor não é nulo).

Por exemplo, você pode usar esse operador de condição para especificar que somente solicitações de criação de buckets de VPCs sejam permitidas.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                " obs:bucket:CreateBucket"
            ],
            "Condition": {
                "Null": {
                    "obs:SourceVpc": [
                        "false"
                    ]
                }
            }
        }
    ]
}
```

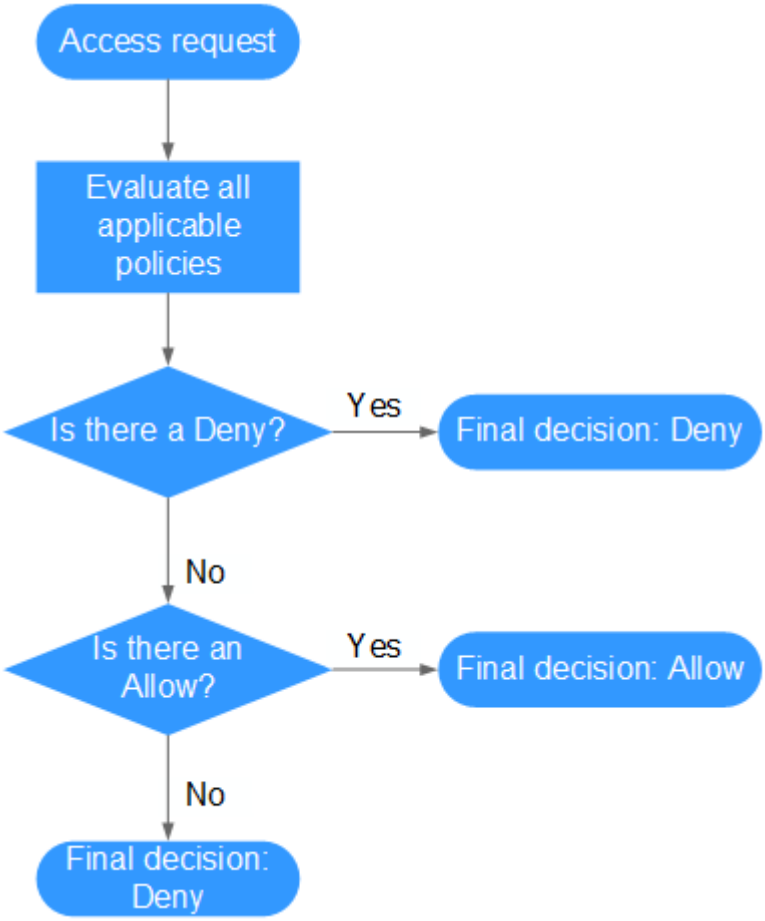
– Sufixo do operador IfExists

  Você pode adicionar "IfExists" ao final de qualquer nome de operador de condição, exceto "Null condition", por exemplo, StringEqualsIfExists. Se a chave de política estiver presente no contexto da solicitação, processe a chave conforme especificado na política. Se a chave não estiver presente, avalie o elemento de condição como true.

5.3.3 Processo de autenticação

Quando um usuário inicia uma solicitação de acesso, o sistema autentica a solicitação com base nas ações nas políticas que foram anexadas ao grupo ao qual o usuário pertence. O diagrama a seguir mostra um processo de autenticação.

Figura 5-5 Processo de autenticação



1. Um usuário inicia uma solicitação de acesso.
2. O sistema procura um Deny entre as ações aplicáveis das políticas das quais o usuário obtém permissões. Se o sistema encontrar uma Deny explícita aplicável, a decisão Deny será retornada, e a autenticação se encerrará.
3. Se nenhuma Deny for encontrada aplicável, o sistema procurará uma Allow que se aplique à solicitação. Se o sistema encontrar um Allow aplicável, ele retornará uma decisão de Allow e a autenticação terminará.
4. Se nenhuma Allow for encontrada aplicável, o sistema retorna uma decisão de Deny, e a autenticação se encerrará.

5.4 Alterações nos nomes de política definidos pelo sistema

Todas as políticas definidas pelo sistema (anteriormente chamadas de "políticas refinadas") foram renomeadas e os novos nomes entram em vigor a partir de 6 de fevereiro de 2020, às 22:30:00 GMT+08:00. Essa alteração não afeta seus serviços. As políticas definidas pelo sistema originais são Versão 1.0 e as novas políticas definidas pelo sistema são Versão 1.1. O IAM é compatível com ambas as versões.

Tabela 5-10 Nomes originais e atuais de políticas definidas pelo sistema

Serviço	Original	Atual
AOM	AOM Admin	AOM FullAccess
	AOM Viewer	AOM ReadOnlyAccess
APM	APM Admin	APM FullAccess
	APM Viewer	APM ReadOnlyAccess
Auto Scaling	AutoScaling Admin	AutoScaling FullAccess
	AutoScaling Viewer	AutoScaling ReadOnlyAccess
BMS	BMS Admin	BMS FullAccess
	BMS User	BMS CommonOperations
	BMS Viewer	BMS ReadOnlyAccess
BSS	EnterpriseProject_BSS_Administrator	EnterpriseProject BSS FullAccess
CBR	CBR Admin	CBR FullAccess
	CBR User	CBR BackupsAndVaults-FullAccess
	CBR Viewer	CBR ReadOnlyAccess
CCE	CCE Admin	CCE FullAccess
	CCE Viewer	CCE ReadOnlyAccess
CCI	CCI Admin	CCI FullAccess
	CCI Viewer	CCI ReadOnlyAccess
CDM	CDM Admin	CDM FullAccess
	CDM Operator	CDM FullAccessExceptUpdateEIP
	CDM Viewer	CDM ReadOnlyAccess
	CDM User	CDM CommonOperations
CDN	CDN Domain Configuration Operator	CDN DomainConfigureAccess
	CDN Domain Viewer	CDN DomainReadOnlyAccess
	CDN Logs Viewer	CDN LogsReadOnlyAccess
	CDN Refresh And Preheat Operator	CDN RefreshAndPreheatAccess

Serviço	Original	Atual
	CDN Statistics Viewer	CDN StatisticsReadOnlyAccess
CES	CES Admin	CES FullAccess
	CES Viewer	CES ReadOnlyAccess
CS	CS Admin	CS FullAccess
	CS Viewer	CS ReadOnlyAccess
	CS User	CS CommonOperations
CSE	CSE Admin	CSE FullAccess
	CSE Viewer	CSE ReadOnlyAccess
DCS	DCS Admin	DCS FullAccess
	DCS Viewer	DCS ReadOnlyAccess
	DCS User	DCS UseAccess
DDM	DDM Admin	DDM FullAccess
	DDM Viewer	DDM ReadOnlyAccess
	DDM User	DDM CommonOperations
DDS	DDS Admin	DDS FullAccess
	DDS DBA	DDS ManageAccess
	DDS Viewer	DDS ReadOnlyAccess
DLF	DLF Admin	DLF FullAccess
	DLF Developer	DLF Development
	DLF Operator	DLF OperationAndMaintenanceAccess
	DLF Viewer	DLF ReadOnlyAccess
DMS	DMS Admin	DMS FullAccess
	DMS Viewer	DMS ReadOnlyAccess
	DMS User	DMS UseAccess
DNS	DNS Admin	DNS FullAccess
	DNS Viewer	DNS ReadOnlyAccess
DSS	DSS Admin	DSS FullAccess
	DSS Viewer	DSS ReadOnlyAccess
DWS	DWS Admin	DWS FullAccess

Serviço	Original	Atual
	DWS Viewer	DWS ReadOnlyAccess
ECS	ECS Admin	ECS FullAccess
	ECS Viewer	ECS ReadOnlyAccess
	ECS User	ECS CommonOperations
ELB	ELB Admin	ELB FullAccess
	ELB Viewer	ELB ReadOnlyAccess
EPS	EPS Admin	EPS FullAccess
	EPS Viewer	EPS ReadOnlyAccess
EVS	EVS Admin	EVS FullAccess
	EVS Viewer	EVS ReadOnlyAccess
GES	GES Admin	GES FullAccess
	GES Viewer	GES ReadOnlyAccess
	GES User	GES Development
ICITY	iCity Admin	iCity FullAccess
	iCity Viewer	iCity ReadOnlyAccess
IMS	IMS Admin	IMS FullAccess
	IMS Viewer	IMS ReadOnlyAccess
Image Recognition	Image Recognition User	Image Recognition FullAccess
KMS	DEW Keypair Admin	DEW KeypairFullAccess
	DEW Keypair Viewer	DEW KeypairReadOnlyAccess
	KMS CMK Admin	KMS CMKFullAccess
LTS	LTS Admin	LTS FullAccess
	LTS Viewer	LTS ReadOnlyAccess
MRS	MRS Admin	MRS FullAccess
	MRS Viewer	MRS ReadOnlyAccess
	MRS User	MRS CommonOperations
ModelArts	ModelArts Admin	ModelArts FullAccess
	ModelArts User	ModelArts CommonOperations

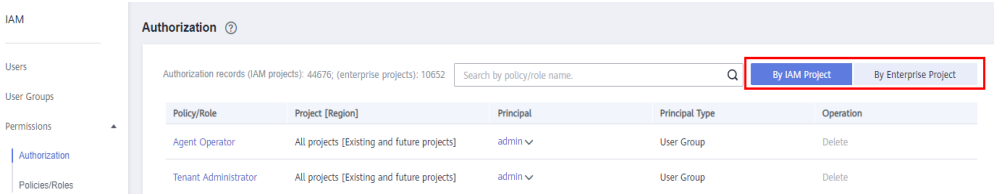
Serviço	Original	Atual
Moderation	Moderation User	Moderation FullAccess
NAT	NAT Admin	NAT FullAccess
	NAT Viewer	NAT ReadOnlyAccess
OBS	OBS Operator	OBS OperateAccess
	OBS Viewer	OBS ReadOnlyAccess
RDS	RDS Admin	RDS FullAccess
	RDS DBA	RDS ManageAccess
	RDS Viewer	RDS ReadOnlyAccess
RES	RES Admin	RES FullAccess
	RES Viewer	RES ReadOnlyAccess
ROMA Connect	ROMA Admin	ROMA FullAccess
	ROMA Viewer	ROMA ReadOnlyAccess
SCM	SCM Admin	SCM FullAccess
	SCM Viewer	SCM ReadOnlyAccess
	SCM Viewer	SCM ReadOnlyAccess
SFS	SFS Admin	SFS FullAccess
	SFS Viewer	SFS ReadOnlyAccess
SFS Turbo	SFS Turbo Administrator	SFS Turbo FullAccess
	SFS Turbo Viewer	SFS Turbo ReadOnlyAccess
ServiceStage	ServiceStage Admin	ServiceStage FullAccess
	ServiceStage Developer	ServiceStage Development
	ServiceStage Viewer	ServiceStage ReadOnlyAccess
VPC	VPC Admin	VPC FullAccess
	VPC Viewer	VPC ReadOnlyAccess

5.5 Registros de autorização

Você pode exibir todos os registros de autorização em sua conta na página **Permissions** > **Authorization**. Você pode filtrar registros por nome de política/função, nome de usuário, nome de grupo de usuários, nome da agência, projeto do IAM, projeto empresarial (se ativado) e tipo de entidade (usuário, grupo de usuários ou agência).

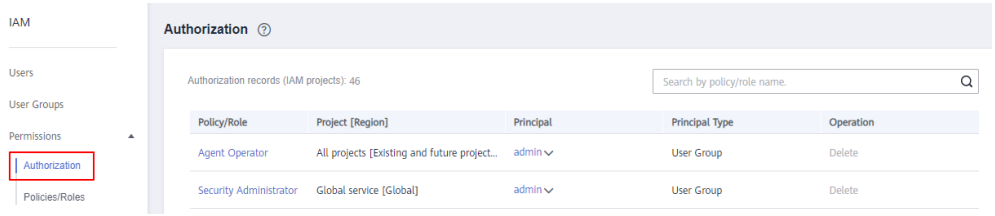
- Função Enterprise Project ativada: exibir registros de autorização por IAM ou projeto empresarial.

Figura 5-6 Função Enterprise Project ativada



- Função Enterprise Project não ativada: exibir registros de autorização por projeto do IAM. Para ativar Enterprise Project, consulte **Ativação da função Enterprise Project**.

Figura 5-7 Função Enterprise Project não ativada



Visualização de registros de autorização por projeto do IAM

Ao visualizar registros de autorização por projeto do IAM, selecione as seguintes condições de filtro:

- **Policy/Role name**:

  Para exibir os registros de autorização de uma política ou função, selecione **Policy/Role name** e digite um nome. Para obter detalhes sobre as permissões de todos os serviços de nuvem, consulte **Permissões definidas pelo sistema**.

- **Username/User group name/Agency name**:

  Para exibir as permissões de projeto do IAM atribuídas a um usuário, grupo de usuários ou agência específicos do IAM, selecione **Username**, **User group name** ou **Agency name** e insira um nome.

  NOTA

  Para autorização baseada em projeto do IAM, você atribui permissões por grupo de usuários. Se você consultar os registros de autorização de um usuário específico, os registros de autorização do grupo ao qual o usuário pertence serão exibidos.

- **IAM project**: o escopo de aplicação das permissões. Se você quiser exibir registros de autorização de um projeto do IAM, selecione **IAM project** e qualquer uma das seguintes opções:
  - **Global services**: exibir registros de autorização de todos os serviços globais.
  - **All resources**: exibir registros de autorização de todos os projetos, ou seja, os serviços globais e todos os projetos da região específica (incluindo projetos criados posteriormente).
  - **Region-specific projects**: exibir registros de autorização de um projeto ou subprojeto padrão (como ap-southeast-1).

- **Principal type**: o tipo de objetos que são autorizados. Existem três tipos de entidades: usuário, grupo de usuários e agência. Na visualização de projeto do IAM, você pode filtrar registros por grupo de usuários ou agência. Se você selecionar **User**, nenhum registro será exibido.
- **Enterprise projects**: o nome de um projeto empresarial. Se você selecionar **Enterprise project** e inserir um nome de projeto empresarial, a **visualização do projeto empresarial** será exibida.

Visualização de registros de autorização por projeto empresarial

Ao visualizar registros de autorização por projeto empresarial, selecione as seguintes condições de filtro:

- **Policy/Role name**:

  Para exibir os registros de autorização de uma política ou função, selecione **Policy/Role name** e digite um nome. Para obter detalhes sobre as permissões de serviço de nuvem suportadas por projetos empresariais, consulte **Permissões de serviço de nuvem**.
- **Username/User group name/Agency name**:

  Para exibir as permissões de projeto empresarial atribuídas a um usuário ou grupo de usuários do IAM específico, selecione **Username** ou **User group name** e digite um nome.

  NOTA

  - Para autorização baseada em projeto empresarial, você atribui permissões por usuário. Se você consultar os registros de autorização de um usuário específico, os registros de autorização do usuário e do grupo de usuários ao qual o usuário pertence serão exibidos.
- **Enterprise project**: o nome de um projeto empresarial, ou seja, o escopo da aplicação de permissões. Para exibir os registros de autorização de um projeto empresarial específico, selecione **Enterprise project** e insira um nome de projeto empresarial.
- **Principal type**: o tipo de objetos que são autorizados. Existem três tipos de entidades: usuário, grupo de usuários e agência.
- **IAM project**: o nome de um projeto ou região do IAM. Se você selecionar **IAM project** e inserir um nome de projeto, a **visualização do projeto do IAM** será exibida.

5.6 Políticas personalizadas

5.6.1 Criação de uma política personalizada

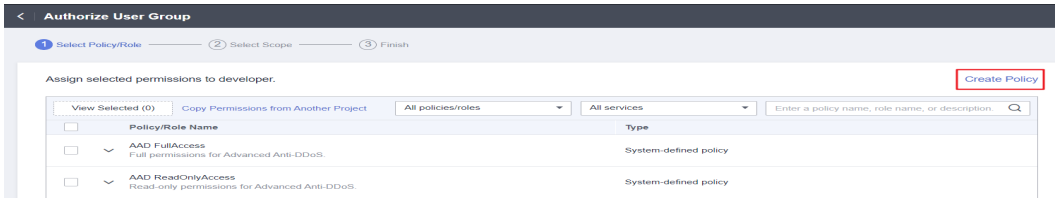
Você pode criar políticas personalizadas para complementar políticas definidas pelo sistema e implementar um controle de acesso mais refinado.

Você pode criar políticas personalizadas de uma das seguintes maneiras:

- Editor visual: selecione serviços de nuvem, ações, recursos e condições de solicitação. Isso não requer conhecimento de sintaxe de política.
- JSON: crie uma política JSON ou edite uma existente.

Esta seção descreve como criar políticas personalizadas na página **Permissions** > **Policies/Roles**. Você também pode criar políticas personalizadas durante a autorização (consulte **Figura 5-8**).

Figura 5-8 Criar uma política durante a autorização

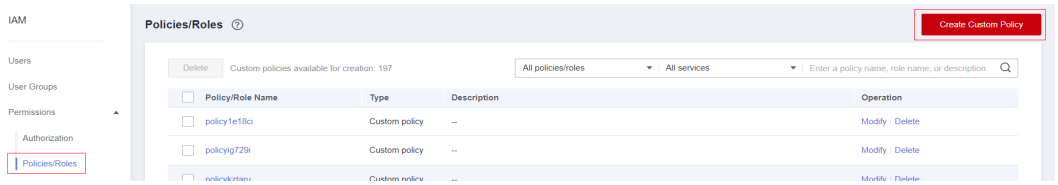


Criação de uma política personalizada no editor visual

Passo 1 Faça logon no **console do IAM**.

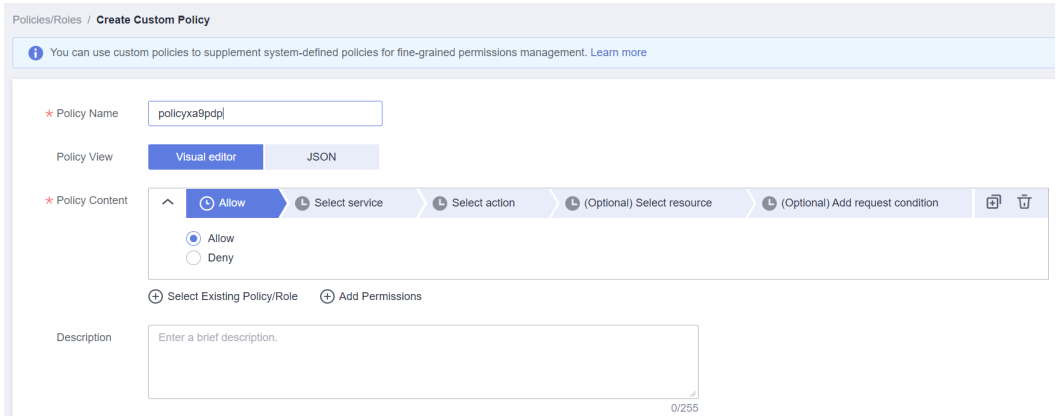
Passo 2 No console do IAM, escolha **Permissions** > **Policies/Roles** no painel de navegação e clique em **Create Custom Policy** no canto superior direito.

Figura 5-9 Criar uma política personalizada



Passo 3 Insira um nome de política.

Figura 5-10 Inserir um nome de política



Passo 4 Selecione **Visual editor** para **Policy View**.

Passo 5 Defina o conteúdo da política.

1. Selecione **Allow** ou **Deny**.
2. Selecione um serviço de nuvem.

NOTA

- Apenas um serviço de nuvem pode ser selecionado para cada bloco de permissão. Para configurar permissões para vários serviços de nuvem, clique em **Add Permissions** ou alterne para a visualização JSON (consulte **Criação de uma política personalizada na visualização JSON**).
- Uma política personalizada pode conter permissões para serviços globais ou de nível de projeto. Para definir as permissões necessárias para acessar serviços globais e de nível de projeto, coloque as permissões em duas políticas personalizadas separadas para autorização refinada.

3. Selecione ações.
4. (Opcional) Selecione todos os recursos ou selecione recursos específicos especificando seus caminhos.

   Para obter detalhes sobre serviços de nuvem que suportam autorização de nível de recurso, consulte **5.6.4 Serviços de nuvem que suportam a autorização em nível de recurso usando o IAM**.

   Tabela 5-11 Tipo de recurso

Parâmetro	Descrição
Specific	Permissões para recursos específicos. Por exemplo, para definir permissões para buckets cujos nomes começam com **TestBucket**, especifique o caminho do recurso do bucket como **OBS:*:*:bucket:TestBucket***. **NOTA** – Especificar recursos do bucket Formato: "OBS:*:*:bucket:*Bucket name*". Para recursos do bucket, o IAM gera automaticamente o prefixo do caminho do recurso: **obs:*:*:bucket:**. Para o caminho de um bucket específico, adicione o *bucket name* ao final. Você também pode usar um caractere curinga (*) para indicar qualquer bucket. Por exemplo, **obs:*:*:bucket:*** indica qualquer bucket do OBS. – Especificar recursos de objeto Formato: "OBS:*:*:object:*Bucket name/object name*". Para recursos de objeto, o IAM gera automaticamente o prefixo do caminho do recurso: **obs:*:*:object:**. Para o caminho de um objeto específico, adicione o *bucket name/object name* ao final do caminho do recurso. Você também pode usar um caractere curinga (*) para indicar qualquer objeto em um bucket. Por exemplo, **obs:*:*:object:my-bucket/my-object/*** indica qualquer objeto no diretório **my-object** do bucket **my-bucket**.
All	Permissões para todos os recursos.

5. (Opcional) Adicione condições de solicitação especificando chaves de condição, operadores e valores.

Tabela 5-12 Parâmetros de condição

Nome	Descrição
Condition Key	Uma chave no elemento **Condition** de uma instrução. Existem chaves de condição globais e específicas do serviço. **As chaves de condição global** (começando com **g:**) estão disponíveis para operações de todos os serviços, enquanto as chaves de condição específicas do serviço (começando com um nome de abreviação de serviço, como **obs:**) estão disponíveis apenas para operações do serviço correspondente. Para obter detalhes, consulte o guia de usuário do serviço de nuvem correspondente, por exemplo, consulte **Condições de solicitação de OBS**.
Operator	Usado em conjunto com uma chave de condição e um valor de condição para formar uma instrução de condição completa.
Value	Usado em conjunto com uma chave de condição e um operador que requer uma palavra-chave, para formar uma instrução de condição completa.

Figura 5-11 Adição de uma condição de solicitação

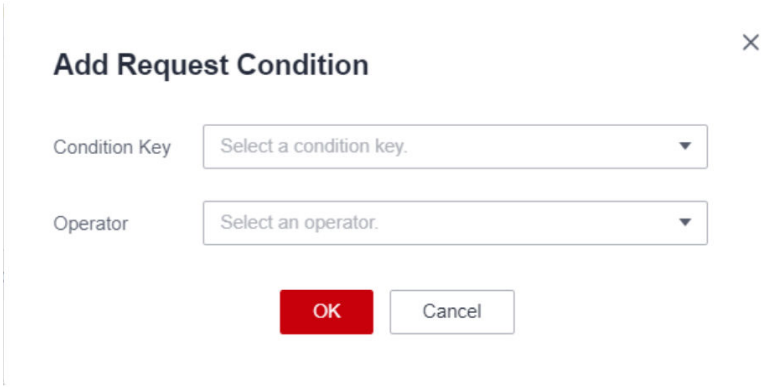


Tabela 5-13 Chaves de condição global

Chave de condição global	Tipo	Descrição
g:CurrentTime	Time	Hora em que uma solicitação de autenticação é recebida. A hora está no formato ISO 8601, por exemplo, **2012-11-11T23:59:59Z**.
g:DomainName	String	Nome da conta.
g:MFAPresent	Boolean	Se deseja obter um token por meio da autenticação MFA.

Chave de condição global	Tipo	Descrição
g:MFAAge	Number	Período de validade de um token obtido por meio da autenticação MFA. Esta condição deve ser usada em conjunto com **g:MFAPresent**.
g:ProjectName	String	Nome do projeto.
g:ServiceName	String	Nome do serviço.
g:UserId	String	ID do usuário do IAM.
g:UserName	String	Nome de usuário do IAM.

Passo 6 (Opcional) Alterne para a visualização JSON e modifique o conteúdo da política no formato JSON.

NOTA

Se o conteúdo da política modificado estiver incorreto, verifique e modifique o conteúdo novamente ou clique em **Reset** para cancelar as modificações.

Passo 7 (Opcional) Para adicionar outro bloco de permissão para a política, clique em **Add Permissions**. Como alternativa, clique no ícone de adição (+) à direita de um bloco de permissões existente para clonar suas permissões.

Passo 8 (Opcional) Insira uma breve descrição para a política.

Passo 9 Clique em **OK**.

Passo 10 Anexe a política a um grupo de usuários. Os usuários do grupo herdam as permissões definidas nessa política.

NOTA

Você pode anexar políticas personalizadas a um grupo de usuários da mesma maneira que você anexa políticas definidas pelo sistema. Para mais detalhes, consulte **4.1 Criação de um grupo de usuários e atribuição de permissões**.

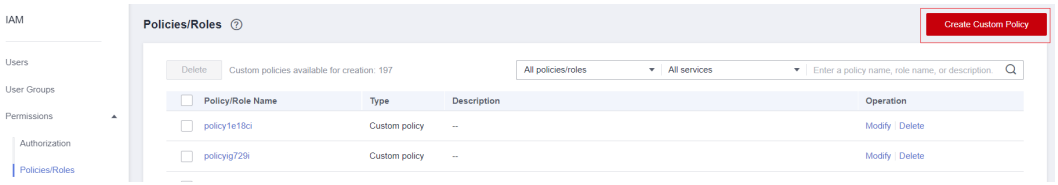
----Fim

Criação de uma política personalizada na visualização JSON

Passo 1 Faça logon no **console do IAM**.

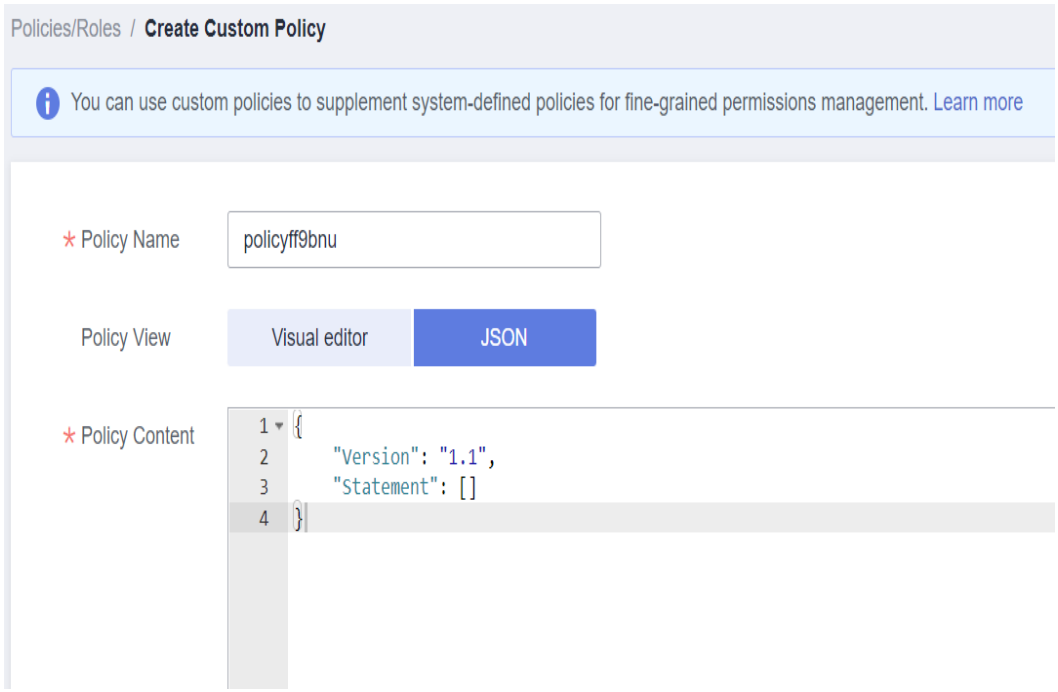
Passo 2 No console do IAM, escolha **Permissions** > **Policies/Roles** no painel de navegação e clique em **Create Custom Policy** no canto superior direito.

Figura 5-12 Criar uma política personalizada



Passo 3 Insira um nome de política.

Figura 5-13 Inserir um nome de política



Passo 4 Selecione **JSON** para **Policy View**.

Passo 5 (Opcional) Clique em **Select Existing Policy/Role** e selecione uma política/função para usá-la como modelo, por exemplo, selecione **EVS FullAccess**.

NOTA

Se você selecionar várias políticas, todas elas devem ter o mesmo escopo, ou seja, **Global services** ou **Project-level services**. Para definir as permissões necessárias para acessar serviços globais e de nível de projeto, coloque as permissões em duas políticas personalizadas separadas para autorização refinada.

Passo 6 Clique em **OK**.

Passo 7 Modifique a instrução no modelo.

- **Effect**: defina-o como **Allow** ou **Deny**.
- **Action**: insira as ações listadas na tabela de ações da API (consulte **Figura 5-14**) do serviço EVS, por exemplo, **evs:volumes:create**.

Figura 5-14 Ações da API

Permission	API	Action
Listing IAM Users	GET /v3/users	iam:users:listUsers

NOTA

- A versão de cada política personalizada é fixada em **1.1**.
- Para obter detalhes sobre as ações de API suportadas por cada serviço, consulte **Permissões definidas pelo sistema**.

Passo 8 (Opcional) Insira uma breve descrição para a política.

Passo 9 Clique em **OK**. Se a lista de políticas for exibida, a política será criada com sucesso. Se uma mensagem indicando o conteúdo incorreto da política for exibida, modifique a política.

Passo 10 Anexe a política a um grupo de usuários. Os usuários do grupo herdam as permissões definidas nessa política.

NOTA

Você pode anexar políticas personalizadas a um grupo de usuários da mesma maneira que você anexa políticas definidas pelo sistema. Para mais detalhes, consulte **4.1 Criação de um grupo de usuários e atribuição de permissões**.

----Fim

5.6.2 Modificação ou exclusão de uma política personalizada

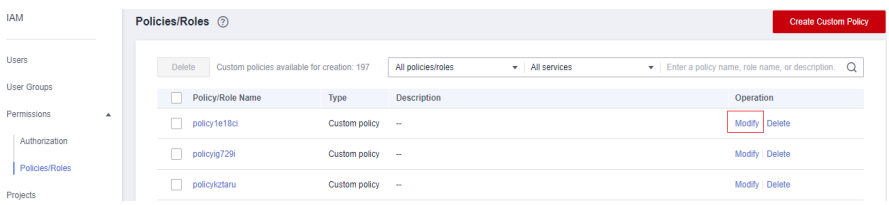
Você pode modificar ou excluir políticas personalizadas.

Modificar uma política personalizada

Modifique o nome, a descrição ou o conteúdo de uma política personalizada.

1. No painel de navegação esquerdo do **console do IAM**, escolha **Permissions** > **Policies/Roles**.
2. Localize a política personalizada que deseja modificar e clique em **Modify** na coluna **Operation** ou clique no nome da política personalizada para acessar a página de detalhes da política.

Figura 5-15 Modificar o conteúdo da política



3. Modifique o nome ou a descrição da política conforme necessário.
4. Modifique o conteúdo da política seguindo as instruções fornecidas em **Criação de uma política personalizada no editor visual**, conforme necessário.

5. Clique em **OK** para salvar as modificações.

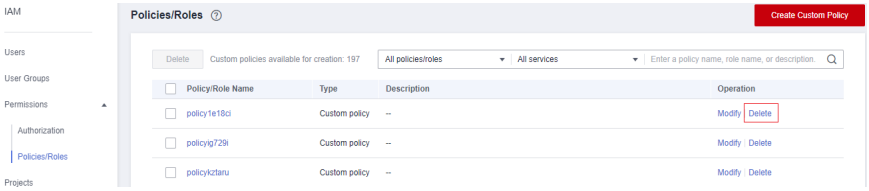
Excluir uma política personalizada

NOTA

Somente políticas personalizadas que não estejam anexadas a nenhum grupo de usuários ou agências podem ser excluídas. Se uma política personalizada tiver sido anexada a determinados grupos de usuários ou agências, desanexe a política e, em seguida, exclua-a.

1. No painel de navegação esquerdo do **console do IAM**, escolha **Permissions** > **Policies/Roles**.
2. Na linha que contém a política personalizada que você deseja excluir, clique em **Delete**.

Figura 5-16 Excluir uma política personalizada



3. Clique em **Yes**.

5.6.3 Casos de uso de políticas personalizadas

Uso de uma política personalizada junto com políticas definidas pelo sistema com permissão completa

Se quiser atribuir permissões completas a um usuário, mas não permitir que ele acesse um serviço específico, como o Cloud Trace Service (CTS), crie uma política personalizada para negar acesso ao CTS e anexe essa política personalizada junto com a política **FullAccess** ao usuário. Como uma negação explícita em qualquer política substitui qualquer permissão, o usuário pode executar operações em todos os serviços, exceto CTS.

Exemplo de política que nega acesso apenas ao CTS:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                    "cts:*:*"
            ]
        }
    ]
}
```

NOTA

- **Action**: operações a serem realizadas. Cada ação deve ser definida no formato "*Service name*:*Resource type*:*Operation*".

  Por exemplo, **cts:*:*** refere-se a permissões para executar todas as operações em todos os tipos de recursos de CTS.
- **Effect**: determina se deve negar ou permitir a operação.

Uso de uma política personalizada junto com uma política definida pelo sistema

- Se você quiser atribuir permissões completas a um usuário, mas não permitir que ele crie BMSs, crie uma política personalizada negando a ação **bms:servers:create** e anexe essa política personalizada junto com a política **BMS FullAccess** ao usuário. Como uma negação explícita em qualquer política substitui qualquer permissão, o usuário pode executar todas as operações no BMS, exceto a criação de BMSs.

  Exemplo de política que nega a criação de BMS:

  ```
  {
      "Version": "1.1",
      "Statement": [
          {
              "Effect": "Deny",
              "Action": [
                      "bms:servers:create"
              ]
          }
      ]
  }
  ```

- Se você deseja atribuir permissões somente leitura do OBS a todos os usuários, mas impedir que determinados usuários visualizem recursos específicos, por exemplo, proibir usuários cujos nomes começam com **TestUser** de visualizar buckets cujos nomes começam com **TestBucket**, crie uma política personalizada negando tais operações e anexe esta política personalizada junto com a política OBS ReadOnlyAccess para esses usuários. Como uma negação explícita em qualquer política substitui qualquer permissão, certos usuários não podem ver buckets cujos nomes começam com **TestBucket**.

  Exemplo de política que nega aos usuários cujos nomes começam com **TestUser** a visualização de buckets cujos nomes começam com **TestBucket**:

  ```
  {
          "Version": "1.1",
          "Statement": [
                  {
                          "Effect": "Deny",
                          "Action": [
                                  "obs:bucket:ListAllMybuckets",
                                  "obs:bucket:HeadBucket",
                                  "obs:bucket:ListBucket",
                                  "obs:bucket:GetBucketLocation"
                          ],
                          "Resource": [
                              "obs:*:*:bucket:TestBucket*"
                          ],
                          "Condition": {
                              "StringStartWith": {
                                  "g:UserName": [
                                      "TestUser"
                      ]
                  }
              }
                  }
          ]
  }
  ```

  NOTA

  Atualmente, apenas alguns serviços de nuvem (como o OBS) suportam autorização baseada em recursos. Para serviços que não suportam esta função, não é possível criar políticas personalizadas que contenham tipos de recursos.

Uso de apenas uma política personalizada

Você pode criar uma política personalizada e anexar apenas a política personalizada ao grupo ao qual o usuário pertence.

- A seguir está um exemplo de política que permite acesso apenas ao ECS, EVS, VPC, ELB e Application Operations Management (AOM).

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow"
                        "Action": [
                                "ecs:*:*",
                                "evs:*:*",
                                "vpc:*:*",
                                "elb:*:*",
                                "aom:*:*"
                        ]
                }
        ]
}
```

- Veja a seguir um exemplo de política que permite que apenas usuários do IAM cujos nomes começam com **TestUser** excluam todos os objetos no diretório **my-object** do bucket **my-bucket**.

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                            "obs:object:DeleteObject"
                        ],
                        "Resource": [
                            "obs:*:*:object:my-bucket/my-object/*"
                        ],
                        "Condition": {
                            "StringStartWith": {
                                "g:UserName": [
                                    "TestUser"
                    ]
                }
        ]
}
```

- Veja a seguir um exemplo de política que permite acesso a todos os serviços, exceto ECS, EVS, VPC, ELB, AOM e APM.

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "*:*:*"
                        ]
                },
                {
                        "Action": [
                                "ecs:*:*",
                "evs:*:*",
                "vpc:*:*",
                "elb:*:*",
                "aom:*:*",
                "apm:*:*"
                        ],
                        "Effect": "Deny"
                }
```



```
            ]
}
```

5.6.4 Serviços de nuvem que suportam a autorização em nível de recurso usando o IAM

Se você deseja conceder permissões a um usuário do IAM para recursos específicos, **crie uma política personalizada** que contenha permissões para os recursos e anexe a política ao usuário. O usuário então só tem as permissões para os recursos especificados. Por exemplo, para conceder a um usuário do IAM permissões para buckets cujos nomes começam com **TestBucket**, crie uma política personalizada, especifique o caminho do recurso como **OBS:*:*:bucket:TestBucket*** e anexe a política ao usuário.

A tabela a seguir lista os serviços de nuvem que suportam autorização em nível de recurso e os tipos de recursos suportados.

Tabela 5-14 Serviços de nuvem que suportam autorização em nível de recurso e os tipos de recursos suportados

Serviço	Tipo de recurso	Nome do recurso
Elastic Cloud Server (ECS)	instance	ECS
Elastic Volume Service (EVS)	volume	Disco do EVS
Object Storage Service (OBS)	bucket	Bucket
	object	Objeto
Virtual Private Cloud (VPC)	publicip	EIP
Software Repository for Container (SWR)	chart	Gráfico
	repository	Repositório
	instance	Instância
Intelligent EdgeFabric (IEF)	product	Produto
	node	Nó de borda
	group	Grupo de nós de borda
	deployment	Implementação
	batchjob	Trabalho em lote
	application	Modelo de aplicação
	appVersion	Versão do modelo de aplicação
	IEFInstance	Instância do IEF
	cluster	Cluster
Data Lake Insight (DLI)	queue	Fila de DLI

Serviço	Tipo de recurso	Nome do recurso
	database	Banco de dados de DLI
	table	Tabela de DLI
	column	Coluna de DLI
	datasourceauth	Informações de autenticação de segurança de DLI
	jobs	Trabalho de DLI
	resource	Pacote de recursos
	elasticresourcepool	Pool de recursos elástico
	group	Grupo de pacotes de recursos
Graph Engine Service (GES)	graphName	Nome do gráfico de GES
	backupName	Nome do backup de GES
	metadataName	Nome dos metadados
FunctionGraph	function	Função
	trigger	Disparador
Distributed Message Service (DMS)	rabbitmq	Instância do RabbitMQ
	kafka	Instância de Kafka
Distributed Cache Service (DCS)	instance	Instância
Document Database Service (DDS)	instanceName	Nome da instância
Resource Formation Service (RFS)	stack	Pilha
Data Encryption Workshop (DEW)	KeyId	ID da chave
GaussDB(DWS)	cluster	Cluster
Cloud Bastion Host (CBH)	instanceId	ID da instância
ROMA Connect	graph	Fluxograma de serviço

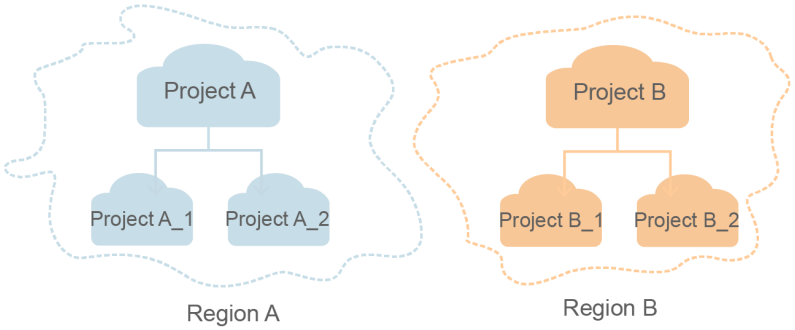
6 Projetos

Os projetos são usados para isolar recursos (incluindo recursos de computação, armazenamento e rede) entre as regiões físicas. Um projeto é fornecido para cada região por padrão, e as permissões são atribuídas com base em projetos.

Para um controle de acesso mais refinado, crie subprojetos em um projeto e compre recursos nos subprojetos. Em seguida, forneça aos usuários permissões para acessar recursos em subprojetos específicos.

Projetos do IAM são diferentes de projetos empresariais. Para obter detalhes sobre suas diferenças, consulte **Quais são as diferenças entre os projetos de IAM e os projetos empresariais?**

Figura 6-1 Isolamento do projeto



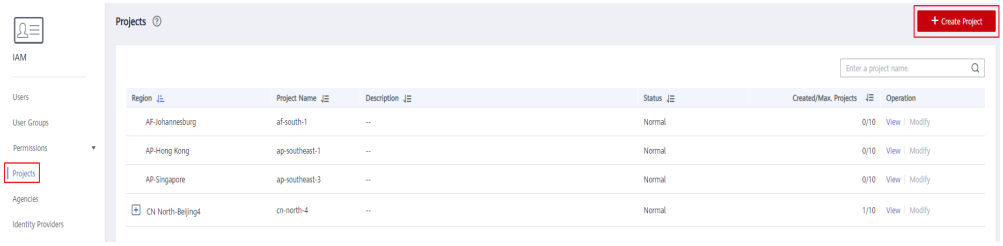
NOTA

- Os recursos não podem ser transferidos entre projetos do IAM.
- Não é possível criar projetos no IAM depois de ativar a função Enterprise Project.

Criar um projeto

Passo 1 No painel de navegação esquerdo no **console do IAM**, escolha **Projects** e clique em **Create Project**.

Figura 6-2 Criar um projeto



Passo 2 Selecione uma região na qual você deseja criar um subprojeto.

Passo 3 Insira o nome de um projeto.

NOTA

- O nome do projeto estará no formato. "*Name of the default project for the selected region_Custom project name*". O nome dos projetos padrão não pode ser modificado.
- O nome do projeto só pode conter letras, dígitos, hifens (-) e sublinhados (_). O comprimento total do nome do projeto não pode exceder 64 caracteres.

Passo 4 (Opcional) Insira uma descrição para o projeto.

Passo 5 Clique em **OK**.

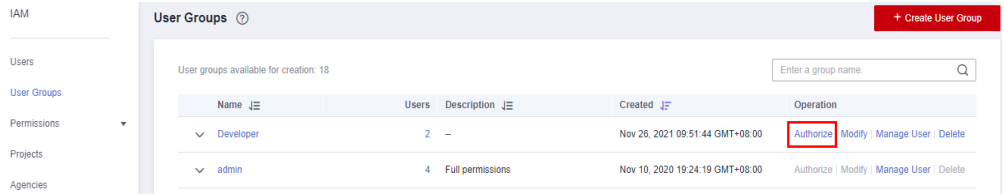
----Fim

Conceder permissões a um grupo de usuários para um projeto

Você pode atribuir permissões com base em projetos para controlar o acesso a recursos em projetos específicos.

Passo 1 Na lista de grupos de usuários, clique em **Authorize** na linha que contém o grupo de usuários de destino.

Figura 6-3 Gerenciamento de permissões



Passo 2 Na página **Authorize User Group**, selecione as políticas ou funções a serem anexadas ao grupo de usuários e clique em **Next**.

Passo 3 Especifique o escopo da autorização. Se você selecionar **Region-specific projects**, selecione um ou mais projetos.

Passo 4 Clique em **OK**.

NOTA

Para obter mais informações sobre autorização de grupo de usuários, consulte **4.1 Criação de um grupo de usuários e atribuição de permissões**.

----Fim

Mudar de regiões ou projetos

Para serviços no nível do projeto, mude para uma região ou projeto no qual você tenha sido autorizado a acessar serviços de nuvem. Não é necessário alternar regiões ou projetos para serviços globais.

Passo 1 Faça logon no console de gerenciamento da Huawei Cloud.

Passo 2 Vá para uma página de serviço de nuvem no nível do projeto. Clique na caixa de listagem suspensa no canto superior esquerdo da página e selecione uma região.

----Fim

7 Agências

7.1 Delegação de conta

7.1.1 Delegação de acesso a recursos para outra conta

A função de agência permite delegar outra conta para implementar O&M em seus recursos com base nas permissões atribuídas.

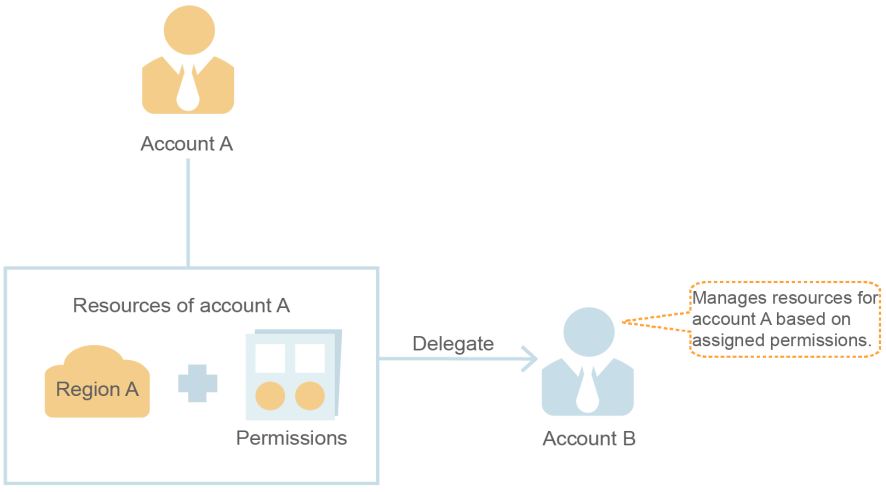
NOTA

Você pode delegar acesso a recursos somente para contas. As contas podem, então, delegar acesso a usuários do IAM sob elas.

Segue-se o procedimento para delegar o acesso a recursos a outra conta. A conta A é a parte delegante e a conta B é a parte delegada.

Passo 1 A conta A cria uma agência no IAM para delegar acesso a recursos à conta B.

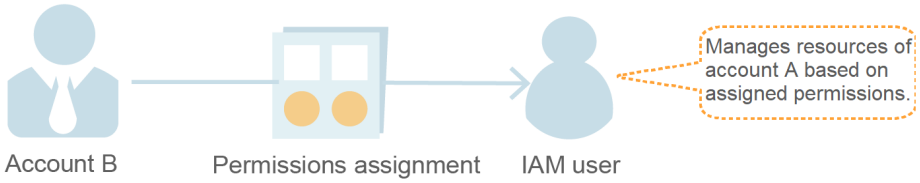
Figura 7-1 (Conta A) Criação de uma agência



Passo 2 (Opcional) Conta B atribui permissões a um usuário do IAM para gerenciar recursos específicos da conta A.

1. Crie um grupo de usuários e conceda a ele as permissões necessárias para gerenciar os recursos da conta A.
2. Crie um usuário e adicione o usuário ao grupo de usuários.

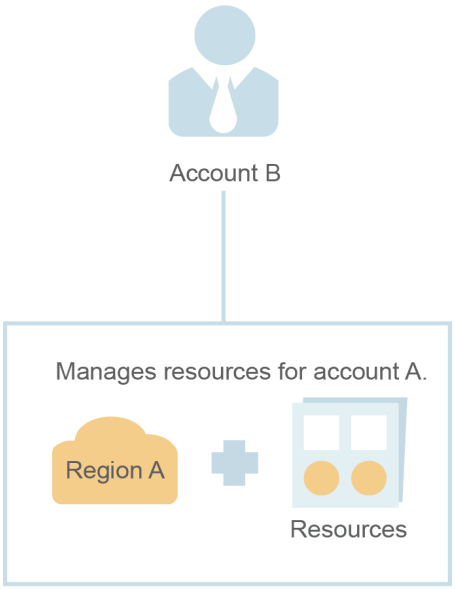
Figura 7-2 (Conta B) Autorizar um usuário do IAM para gerenciar recursos delegados



Passo 3 A conta B ou o usuário autorizado gerencia os recursos da conta A.

1. Use a conta B para fazer logon e alternar a função para a conta A.
2. Alterne para a região A e gerencie os recursos da conta A nessa região.

Figura 7-3 (Conta B) Alternar a função



----Fim

7.1.2 Criação de uma agência (por uma parte delegante)

Ao criar uma agência, você pode compartilhar seus recursos com outra conta ou delegar um indivíduo ou equipe para gerenciar seus recursos. Você não precisa compartilhar suas credenciais de segurança (a senha ou as chaves de acesso) com a parte delegada. Em vez disso, a parte delegada pode fazer logon com suas próprias credenciais de conta e, em seguida, alternar a função para sua conta e gerenciar seus recursos.

Pré-requisitos

Antes de criar uma agência, conclua as seguintes operações:

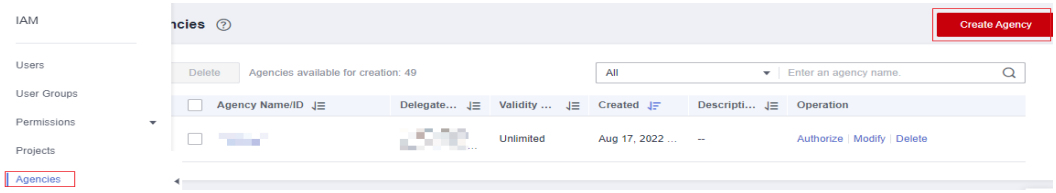
- Entenda os **conceitos básicos** de permissões.
- Determine as **permissões definidas pelo sistema** a serem atribuídas à agência e verifique se as permissões têm dependências. Para obter mais detalhes, consulte **Atribuição de funções de dependência**.

Procedimento

Passo 1 Faça logon no **console do IAM**.

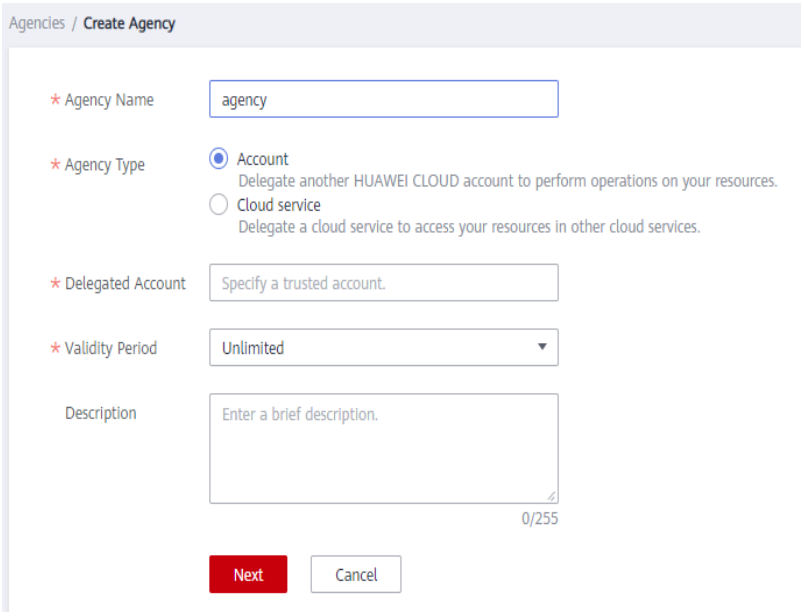
Passo 2 No console do IAM, escolha **Agencies** no painel de navegação esquerdo e clique em **Create Agency** no canto superior direito.

Figura 7-4 Criar uma agência



Passo 3 Insira um nome de agência.

Figura 7-5 Configurar o nome da agência



Passo 4 Especifique o tipo de agência como **Account** e insira o nome de uma conta delegada.

NOTA

- **Account**: compartilhe recursos com outra conta ou delegue um indivíduo ou equipe para gerenciar seus recursos. A conta delegada só pode ser uma conta, em vez de um usuário do IAM ou um usuário federado.
- **Cloud service**: delegue um serviço específico para acessar outros serviços. Para obter mais informações, consulte **7.2 Agência de serviços de nuvem**.

Passo 5 Defina o período de validade e insira uma descrição para a agência.

Passo 6 Clique em **Next**.

Passo 7 Selecione as políticas ou funções a serem anexadas à agência, clique em **Next** e selecione o escopo de autorização.

NOTA

- A atribuição de permissões a uma agência é semelhante à atribuição de permissões a um grupo de usuários. As duas operações diferem apenas no número de permissões disponíveis. Para obter detalhes sobre como atribuir permissões a um grupo de usuários, consulte **Atribuição de permissões a um grupo de usuários**.
- Você pode atribuir a função **Security Administrator** à agência, mas não recomendamos que você faça isso. Para fins de segurança da conta, conceda apenas as permissões necessárias à agência com base no princípio do privilégio mínimo (PoLP).

Passo 8 Clique em **OK**.

NOTA

Depois de criar uma agência, forneça o nome de sua conta, o nome da agência, o ID da agência e as permissões da agência para a parte delegada. A parte delegada pode então alternar a função para sua conta e gerenciar recursos específicos com base nas permissões atribuídas.

----Fim

7.1.3 (Opcional) Atribuição de permissões a um usuário do IAM (por uma parte delegada)

Quando uma relação de confiança é estabelecida entre sua conta e outra conta, você se torna uma parte delegada. Por padrão, somente sua conta e os membros do grupo **admin** podem gerenciar recursos para a parte delegante. Para autorizar os usuários do IAM a gerenciar esses recursos, atribua permissões aos usuários.

Você pode autorizar um usuário do IAM a gerenciar recursos para todas as partes delegantes ou autorizar o usuário a gerenciar recursos para uma parte delegante específica.

Pré-requisitos

- Uma relação de confiança foi estabelecida entre sua conta e outra conta.
- Você obteve o nome da conta delegante e o nome e ID da agência criada.

Procedimento

Passo 1 Crie um grupo de usuários e conceda permissões a ele.

1. Na página **User Groups**, clique em **Create User Group**.
2. Insira um nome de grupo de usuários.

3. Clique em **OK**.
4. Na linha que contém o grupo de usuários, clique em **Authorize**.
5. Crie uma política personalizada.

   NOTA

   Esta etapa é usada para criar uma política contendo as permissões necessárias para gerenciar recursos de uma agência específica. Se você quiser autorizar um usuário do IAM a gerenciar recursos para todas as agências, acesse **Passo 1.6**.

   a. Na página **Select Policy/Role**, clique em **Create Policy** no canto superior direito da lista de permissões.
   b. Insira um nome de política.
   c. Selecione **JSON** para **Policy View**.
   d. Na área **Policy Content**, insira o seguinte conteúdo:

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Action": [
                                "iam:agencies:assume"
                        ],
                        "Resource": {
                                "uri": [
                                        "/iam/agencies/
b36b1258b5dc41a4aa8255508xxx..."
                                ]
                        },
                        "Effect": "Allow"
                }
        ]
}
```

   NOTA

   - Substitua *b36b1258b5dc41a4aa8255508xxx...* pelo ID da agência obtido de uma parte delegante. Não faça nenhuma outra alteração.
   - Para obter mais informações sobre permissões, consulte **5 Gerenciamento de permissões**.

   e. Clique em **Next**.
6. Selecione a política criada na etapa anterior ou a função **Agent Operator** e clique em **Next**.
   – Política personalizada: permite que um usuário gerencie recursos somente para uma agência identificada por um ID específico.
   – Função **Agent Operator**: permite que um usuário gerencie recursos para todas as agências.
7. Especifique o escopo da autorização.
8. Clique em **OK**.

Passo 2 Crie um usuário do IAM e adicione o usuário ao grupo de usuários.

1. Na página **Users**, clique em **Create User**.
2. Na página **Create User**, digite um nome de usuário.
3. Selecione **Management console access** para **Access Type** e, em seguida, selecione **Set by user** para **Credential Type**.
4. Ative a proteção de logon e clique em **Next**.

5. Selecione o grupo de usuários criado em **Passo 1** e clique em **Create**.

   NOTA

   Após a conclusão da autorização, o usuário do IAM pode alternar para a conta da parte delegante e gerenciar recursos específicos na conta.

----Fim

Operações relacionadas

A conta delegada ou os usuários autorizados do IAM podem **mudar suas funções** para a conta delegante para visualizar e usar seus recursos.

7.1.4 Troca de funções (por uma parte delegada)

Quando uma conta estabelece uma relação de confiança com sua conta, você se torna uma parte delegada. Os usuários do IAM que recebem permissões de agência podem alternar para a conta de delegação e gerenciar recursos na conta com base nas permissões concedidas.

Pré-requisitos

- Uma relação de confiança foi estabelecida entre sua conta e outra conta.
- Você obteve o nome da conta de delegação e o nome da agência.

Procedimento

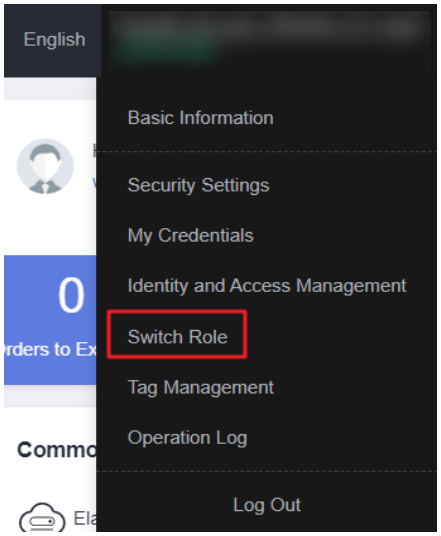
Passo 1 Faça logon no console da Huawei Cloud usando sua conta ou faça logon como o usuário do IAM criado em **Passo 2**.

NOTA

O usuário do IAM criado em **Passo 2** pode alternar funções para gerenciar recursos para a parte delegante.

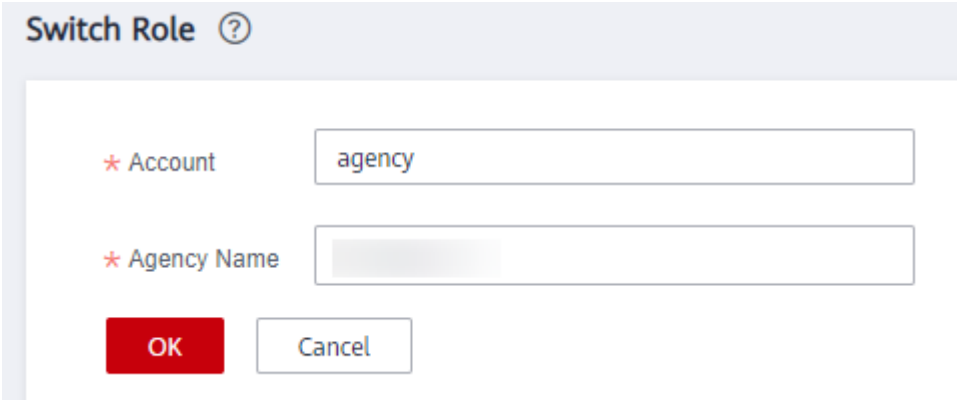
Passo 2 Passe o ponteiro do mouse sobre o nome de usuário no canto superior direito e escolha **Switch Role**.

Figura 7-6 Alternar a função



Passo 3 Na página **Switch Role**, digite o nome da conta da parte delegante.

Figura 7-7 Inserir o nome da conta e o nome da agência da parte delegante



NOTA

Depois que você inserir o nome da conta, as agências criadas nessa conta serão exibidas automaticamente após você clicar na caixa de texto do nome da agência. Selecione um autorizado na lista suspensa.

Passo 4 Clique em **OK** para alternar para a conta de delegação.

----Fim

Procedimento de acompanhamento

Para retornar à sua própria conta, passe o ponteiro do mouse sobre o nome de usuário no canto superior direito, escolha **Switch Role** e selecione sua conta.

7.2 Agência de serviços de nuvem

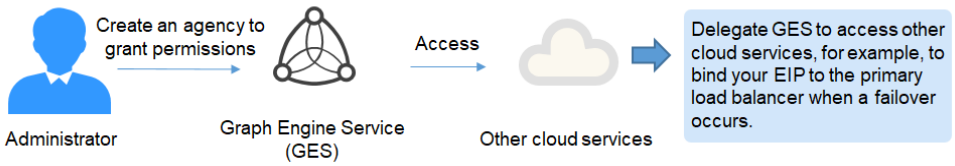
Os serviços da Huawei Cloud interagem entre si e alguns serviços de nuvem dependem de outros serviços. Para delegar um serviço de nuvem para acessar outros serviços e executar O&M de recursos, crie uma agência para o serviço.

O IAM fornece dois métodos para criar uma agência de serviços de nuvem:

1. **Criação de uma agência de serviços de nuvem no console do IAM**

   Por exemplo, crie uma agência para o Graph Engine Service (GES) e conceda a ela permissões para vincular seu EIP ao balanceador de carga primário se ocorrer um failover.

Figura 7-8 Agência de serviços de nuvem



2. Criação automática de uma agência de serviços de nuvem para usar determinados recursos

   A seguir, o Scalable File Service (SFS) é um exemplo para descrever o procedimento para criar automaticamente uma agência de serviços de nuvem:

   a. Vá para o console do SFS.

   b. Na página **Create File System**, ative a criptografia de dados estática.

   c. Uma caixa de diálogo é exibida solicitando que você confirme a criação de uma agência do SFS. Depois de clicar em **OK**, o sistema cria automaticamente uma agência do SFS com permissões **KMS CMKFullAccess** para o projeto atual. Com a agência, o SFS pode obter chaves de KMS para criptografar ou descriptografar sistemas de arquivos.

   d. Você pode visualizar a agência na lista de agências no console do IAM.

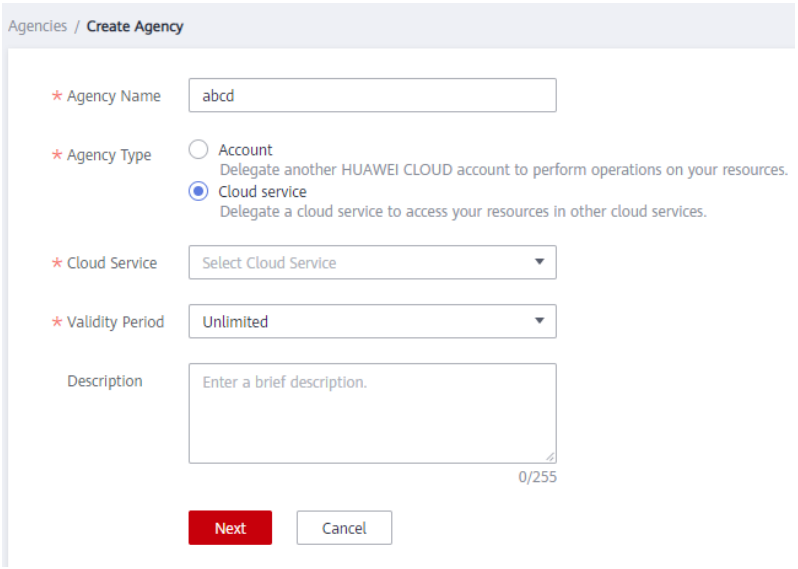
Criação de uma agência de serviços de nuvem no console do IAM

Passo 1 Faça logon no **console do IAM**.

Passo 2 No console do IAM, escolha **Agencies** no painel de navegação e clique em **Create Agency**.

Passo 3 Insira um nome de agência.

Figura 7-9 Nome da agência de serviço de nuvem



Passo 4 Selecione o tipo de agência **Cloud service** e, em seguida, selecione um serviço.

Passo 5 Selecione um período de validade.

Passo 6 (Opcional) Digite uma descrição para a agência para facilitar a identificação.

Passo 7 Clique em **Next**.

Passo 8 Selecione as permissões a serem atribuídas à agência, clique em **Next** e especifique o escopo da autorização.

Passo 9 Clique em **OK**.

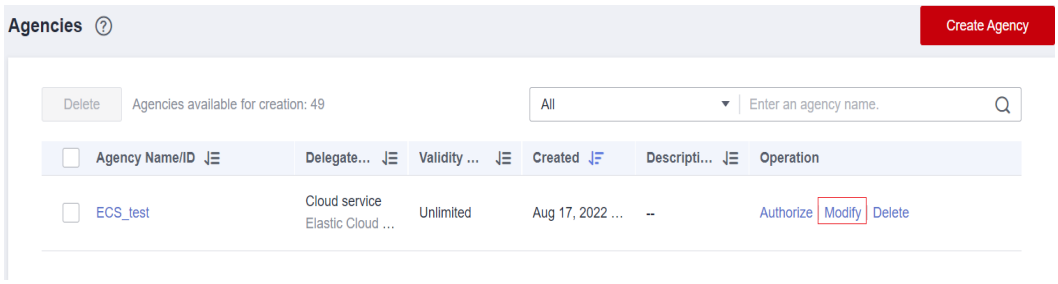
----Fim

7.3 Exclusão ou modificação de agências

Modificação de uma agência

Para modificar as permissões, o período de validade e a descrição de uma agência, clique em **Modify** na linha que contém a agência que você deseja modificar.

Figura 7-10 Modificação de uma agência



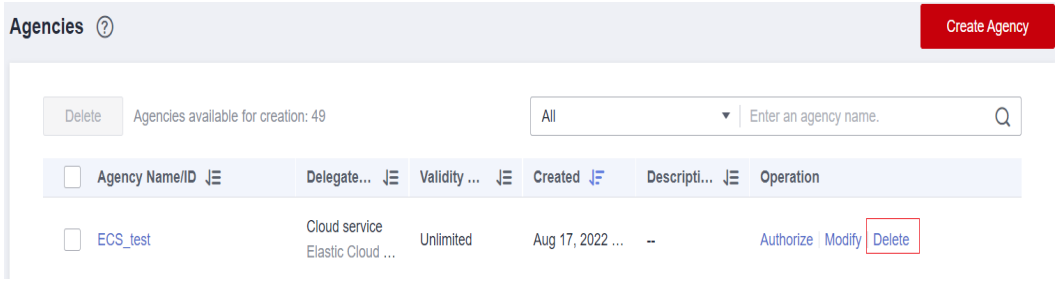
NOTA

- Você pode alterar o serviço de nuvem, o período de validade, a descrição e as permissões das agências de serviço de nuvem, mas não pode alterar o nome e o tipo da agência.
- A modificação das permissões das agências de serviços de nuvem pode afetar o uso de determinadas funções dos serviços de nuvem. Tenha cuidado ao realizar esta operação.

Exclusão de uma agência

Para excluir uma agência, clique em **Delete** na linha que contém a agência a ser excluída e clique em **Yes**.

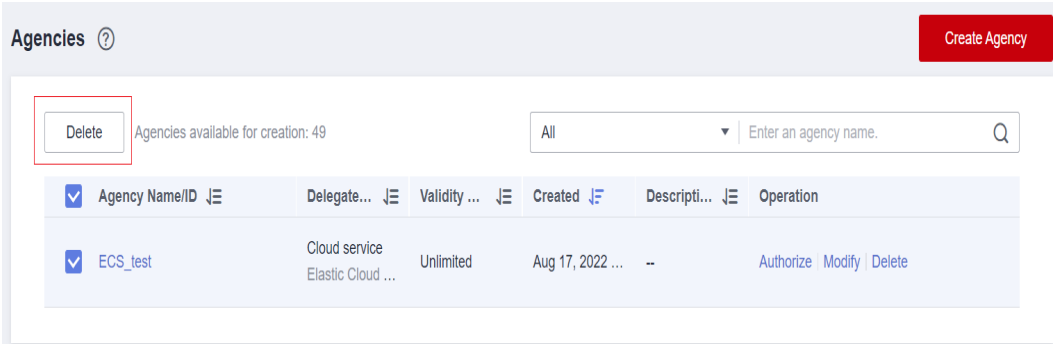
Figura 7-11 Exclusão de uma agência



Exclusão de agências em lote

Para excluir várias agências, selecione as agências a serem excluídas na lista e clique em **Delete** acima da lista.

Figura 7-12 Exclusão de agências em lote



NOTA

Depois de excluir uma agência, todas as permissões concedidas às contas delegadas serão revogadas.

8 Configurações de segurança

8.1 Visão geral das configurações de segurança

Você pode definir as configurações da conta, a proteção de operação crítica, a política de autenticação de logon, a política de senha e a lista de controle de acesso (ACL) na página **Security Settings**. Para obter detalhes, consulte **8.2 Informações básicas**, **8.3 Proteção de operações críticas**, **8.4 Política de autenticação de logon**, **8.5 Política de senha** e **8.6 ACL**. Este capítulo descreve como acessar a página **Security Settings** e quem é o público-alvo.

Público-alvo

Tabela 8-1 lista o público-alvo de diferentes funções fornecidas na página **Security Settings** e suas permissões de acesso para as funções.

Tabela 8-1 Público-alvo

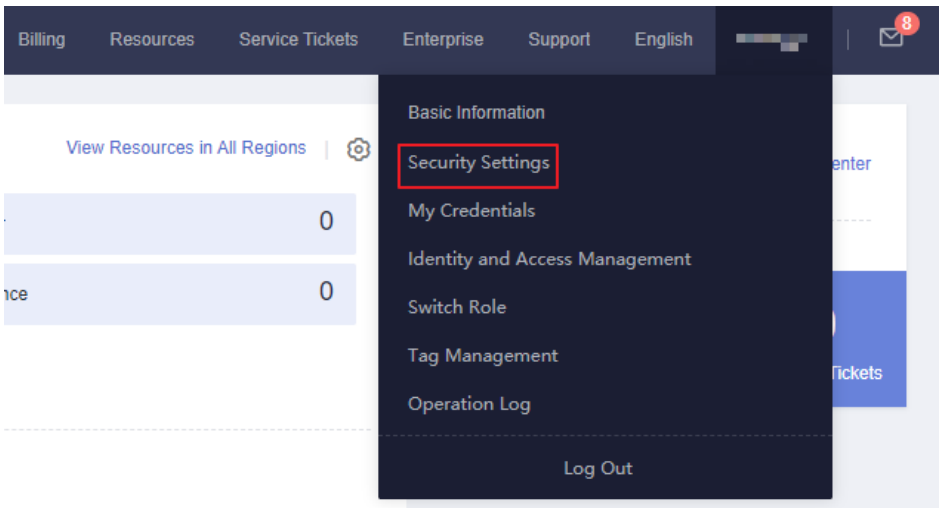
Função	Público-alvo
Informação básica	• Usuários do IAM: acesso completo • Conta: para alterar as informações básicas, consulte **Gerenciamento de informações básicas**.
Operações críticas	• **Administrador**: acesso completo • Usuários do IAM: sem acesso

Função	Público-alvo
Política de autenticação de logon	● **Administrador**: acesso completo ● Usuários do IAM: acesso somente leitura
Política de senha	● **Administrador**: acesso completo ● Usuários do IAM: acesso somente leitura
ACL	● **Administrador**: acesso completo ● Usuários do IAM: sem acesso

Acesso à página Security Settings

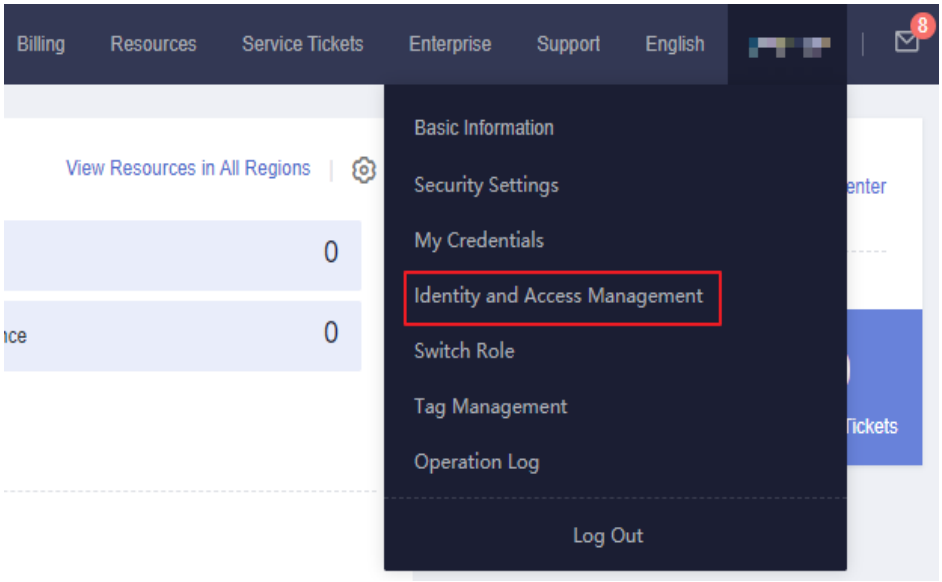
- Você e todos os usuários do IAM criados usando sua conta podem acessar a página **Security Settings** no console de gerenciamento.
  a. Faça logon na Huawei Cloud e clique em **Console** no canto superior direito.
  b. No console de gerenciamento, passe o ponteiro do mouse sobre o nome de usuário no canto superior direito e escolha **Security Settings** na lista suspensa.

  Figura 8-1 Acessar a página de configurações de segurança



- Como **administrador**, você também pode acessar a página **Security Settings** no console do IAM.
  a. Faça logon na Huawei Cloud e clique em **Console** no canto superior direito.
  b. No console de gerenciamento, passe o ponteiro do mouse sobre o nome de usuário no canto superior direito e escolha **Identity and Access Management** na lista suspensa.

Figura 8-2 Acesso ao serviço IAM



c. No console do IAM, escolha **Security Settings** no painel de navegação esquerdo.

8.2 Informações básicas

Como administrador de conta, você e seus usuários do IAM podem gerenciar informações básicas nesta página. Você também pode alterar sua senha de logon, número de celular e endereço de e-mail consultando **Gerenciamento de informações da HUAWEI ID**.

NOTA

- Um número de celular ou endereço de e-mail só pode ser vinculado a uma conta ou usuário do IAM.
- Apenas um número de celular, endereço de e-mail e dispositivo de MFA virtual podem ser vinculados a uma conta ou um usuário do IAM.

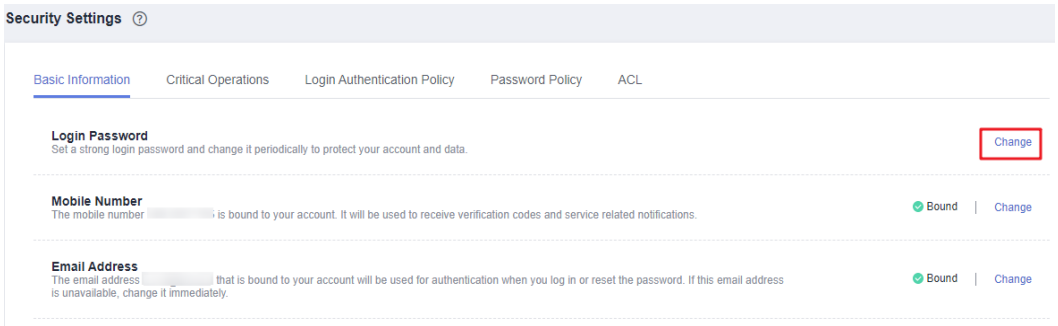
Alteração da senha de logon, do número de celular ou do endereço de e-mail

Os métodos para alterar a senha de logon, o número de celular e o endereço de e-mail são semelhantes. Para alterar a senha de logon, faça o seguinte:

Passo 1 Vá para a página **Configurações de segurança**.

Passo 2 Clique na guia **Basic Information** e clique em **Change** na linha **Login Password**.

Figura 8-3 Alterar a senha de logon



Passo 3 (Opcional) Selecione a verificação do endereço de e-mail ou do número de celular e digite o código de verificação.

NOTA

Se nem o endereço de e-mail nem o número de celular estiverem vinculados, nenhuma verificação será necessária.

Passo 4 Digite a senha anterior e a nova senha e digite a nova senha novamente.

NOTA

- A senha não pode ser o nome de usuário ou o nome de usuário escrito ao contrário. Por exemplo, se o nome de usuário for **A12345**, a senha não poderá ser **A12345**, **a12345**, **54321A** ou **54321a**.
- Para evitar a quebra de senha, o administrador pode configurar a política de senha para definir requisitos de senha, como o comprimento mínimo da senha. Para mais detalhes, consulte **8.5 Política de senha**.

Passo 5 Clique em **OK**.

----Fim

8.3 Proteção de operações críticas

Somente um **administrador** pode configurar a proteção de operação crítica, e os usuários do IAM só podem visualizar as configurações. Se um usuário do IAM precisar modificar as configurações, ele poderá solicitar que o administrador execute a modificação ou conceda as permissões necessárias.

NOTA

Usuários federados não precisam verificar sua identidade ao executar operações críticas.

Dispositivo de MFA virtual

Um dispositivo de MFA gera códigos de verificação de 6 dígitos em conformidade com o TOTP (Algoritmo de senha de uso único baseado em tempo). Os dispositivos de MFA podem ser baseados em hardware ou software. Atualmente, apenas dispositivos de MFA virtuais baseados em software são suportados e são programas de aplicações executados em dispositivos inteligentes, como telefones celulares.

Esta seção descreve como vincular um dispositivo de MFA virtual, por exemplo, o aplicativo Huawei Cloud. Se você instalou outro aplicativo de MFA, adicione um usuário seguindo as instruções na tela. Para obter detalhes sobre como vincular ou remover um dispositivo de MFA virtual, consulte **11.2 Dispositivo de MFA virtual**.

O método para vincular um dispositivo de MFA virtual varia dependendo se sua **conta da Huawei Cloud** foi atualizada para uma **HUAWEI ID**.

NOTA

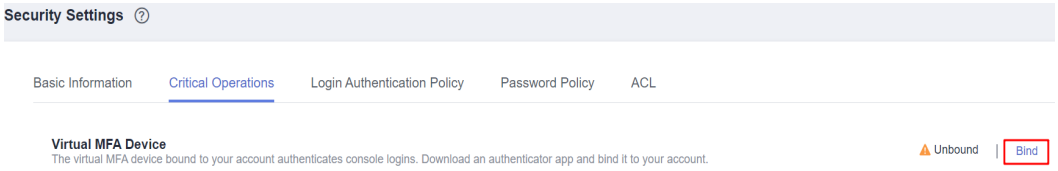
Antes de vincular um dispositivo de MFA virtual, verifique se você instalou um aplicativo de MFA (como um aplicativo Autenticador) em seu dispositivo móvel.

- **Conta da Huawei Cloud**

Passo 1 Vá para a página **Configurações de segurança**.

Passo 2 Clique na guia **Critical Operations** e clique em **Bind** na linha **Virtual MFA Device**.

Figura 8-4 Dispositivo de MFA virtual



Passo 3 Configure o aplicativo de MFA digitalizando o código QR ou inserindo manualmente a chave secreta.

Você pode vincular um dispositivo de MFA virtual à sua conta digitalizando o código QR ou inserindo a chave secreta.

- Digitalizar o código QR

  Abra o aplicativo de MFA em seu telefone celular e use-o para digitalizar o código QR exibido na página **Bind Virtual MFA Device**. Sua conta ou usuário IAM é então adicionado à aplicação.

- Inserir manualmente a chave secreta

  Abra o aplicativo de MFA no seu celular e digite a chave secreta.

  NOTA

  O usuário só pode ser adicionado manualmente usando senhas de uso único baseadas em tempo (TOTP). É aconselhável ativar a definição automática da hora no seu telefone celular.

Passo 4 Visualize os códigos de verificação no aplicativo de MFA. O código é atualizado automaticamente a cada 30 segundos.

Passo 5 Na página **Bind Virtual MFA Device**, insira dois códigos de verificação consecutivos e clique em **OK**.

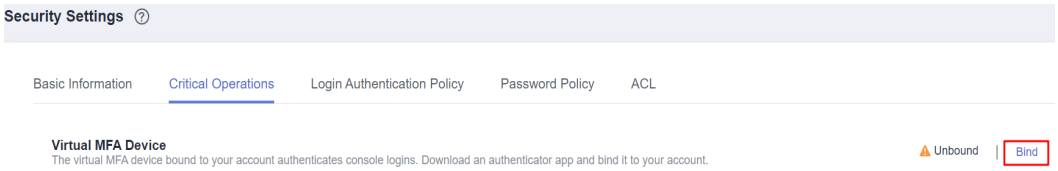
----Fim

- **HUAWEI ID**

Passo 1 Vá para a página **Configurações de segurança**.

Passo 2 Clique na guia **Critical Operations** e clique em **Bind** na linha **Virtual MFA Device**.

Figura 8-5 Vincular um dispositivo de MFA virtual



Passo 3 Na página **Account & security** da central de contas da HUAWEI ID, vincule um autenticador à sua HUAWEI ID conforme as instruções.

----Fim

Proteção de logon

Depois que a proteção de logon estiver ativada, você e os usuários do IAM criados usando sua conta precisarão inserir um código de verificação além do nome de usuário e senha durante o logon. Ative esta função para a segurança da conta.

Para a conta, apenas o administrador da conta pode ativar a proteção de logon para ela. Para usuários do IAM, o administrador da conta e outros administradores podem ativar esse recurso para os usuários.

- **(Administrador) Ativação da proteção de logon para um usuário do IAM**

  Para ativar a proteção de logon para um usuário do IAM, acesse a página **Users** e escolha **More** > **Security Settings** na linha que contém o usuário do IAM. Na área **Login Protection** na guia **Security Settings** exibida, clique em ao lado de **Verification Method** e selecione um método de verificação de SMS, e-mail ou dispositivo de MFA virtual.

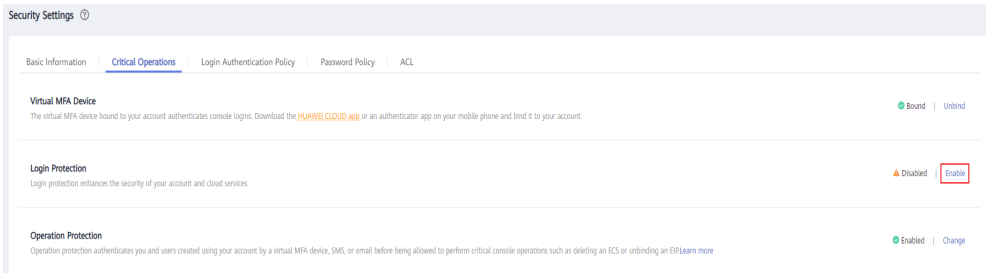
  NOTA

  Depois de ativar a proteção de logon, os usuários do IAM precisam executar a verificação de identidade quando acessarem a Huawei Cloud usando o console de gerenciamento. A configuração não se aplica se os usuários do IAM usarem acesso programático.

- **Ativação da proteção de logon para sua conta da Huawei Cloud**

  Se a sua conta da Huawei Cloud não tiver sido atualizada para uma HUAWEI ID, você poderá ativar a proteção de logon na página **Security Settings**. Vá para a página **Security Settings** e clique na guia **Critical Operations**. Clique em **Enable** ao lado de **Login Protection**, selecione um método de verificação, digite o código de verificação e clique em **OK**.

  Figura 8-6 Ativação da proteção de logon

- **Ativação da proteção de logon para sua HUAWEI ID**

  Se a sua conta da Huawei Cloud tiver sido atualizada para uma HUAWEI ID, ative a proteção de logon na central de contas da HUAWEI ID. Vá para a **central de contas da HUAWEI ID**, escolha **Account & security**, localize **Two-step verification** na área **Security verification**, clique em **ENABLE**, conclua a verificação e clique em **OK**.

  O sistema autentica sua identidade quando você faz logon com uma HUAWEI ID. Se você usar um novo terminal para fazer logon, você será autenticado com seu número de telefone de segurança no primeiro logon. Se a verificação em duas etapas não estiver ativada, clique em **Trust** para adicionar seu terminal à lista de confiança. Então você não precisará mais realizar a autenticação ao fazer logon usando este terminal na próxima vez.

Proteção da operação

- **Ativação da proteção da operação**

  Depois que a proteção de operação é ativada, você e os usuários do IAM criados usando sua conta precisam inserir um código de verificação ao executar uma **operação crítica**, como a exclusão de um ECS. Essa função está ativada por padrão. Para garantir a segurança do recurso, mantenha-a ativada.

  A verificação é válida por 15 minutos e você não precisa ser verificado novamente ao realizar operações críticas dentro do período de validade.

Passo 1 Vá para a página **Configurações de segurança**.

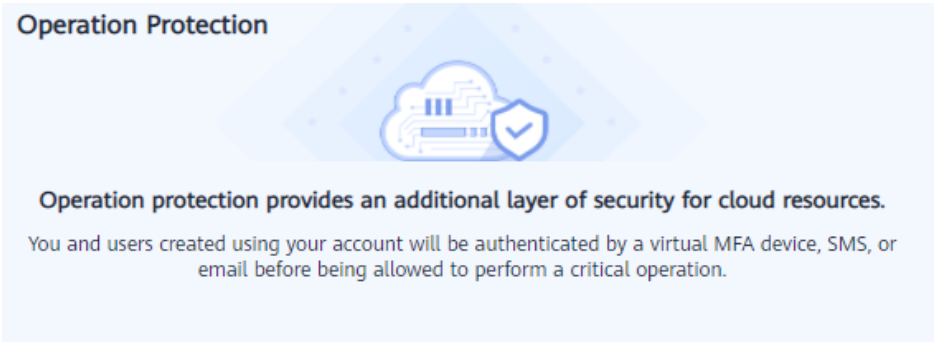
Passo 2 Na guia **Critical Operations**, localize a linha **Operation Protection** e clique em **Enable**.

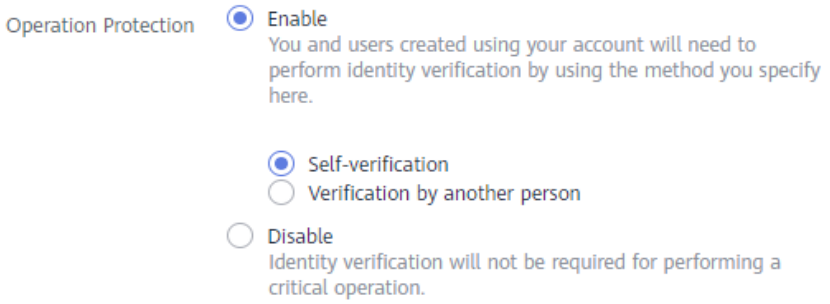
Figura 8-7 Ativar a proteção de operação

Passo 3 Selecione **Enable** e, em seguida, selecione **Self-verification** ou **Verification by another person**.

Se você selecionar **Verification by another person**, uma verificação de identidade será necessária para garantir que esse método de verificação esteja disponível.

Figura 8-8 Configuração da proteção da operação





- **Self-verification**: você ou os próprios usuários do IAM executam a verificação ao executar uma operação crítica.

- **Verification by another person**: a pessoa especificada conclui a verificação quando você ou os usuários do IAM executam uma operação crítica. Somente a verificação por SMS e e-mail é suportada.

Passo 4 Clique em **OK**.

----Fim

- **Desativação da proteção de operação**

Se a proteção da operação estiver desativada, você e os usuários do IAM criados usando sua conta não precisarão inserir um código de verificação ao executar uma **operação crítica**.

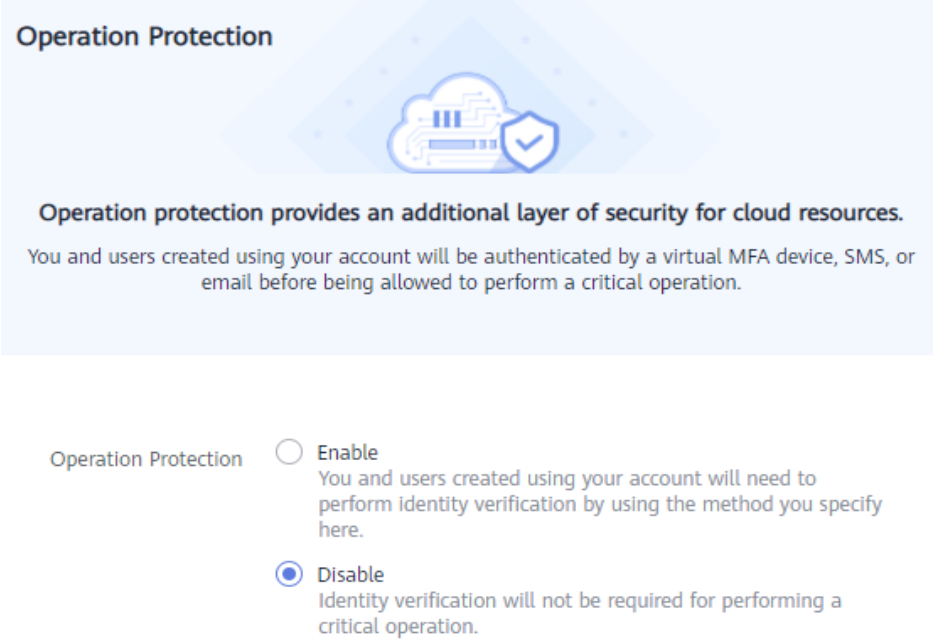
Passo 1 Vá para a página **Configurações de segurança**.

Passo 2 Na guia **Critical Operations**, localize a linha **Operation Protection** e clique em **Change**.

Figura 8-9 Desativação da proteção de operação

Passo 3 Selecione **Disable** e clique em **OK**.

Figura 8-10 Desativação da proteção de operação



Passo 4 Insira um código de verificação.

- **Self-verification**: o administrador que deseja desativar a proteção de operação conclui a verificação. SMS, e-mail e verificação de MFA virtual são suportados.
- **Verification by another person**: a pessoa especificada completa a verificação. Somente a verificação por SMS e e-mail é suportada.

Passo 5 Clique em **OK**.

----Fim

NOTA

- Cada serviço de nuvem define suas próprias operações críticas.
- Quando os usuários do IAM criados usando sua conta executam uma operação crítica, eles serão solicitados a escolher um método de verificação de e-mail, SMS e dispositivo de MFA virtual.
  - Se um usuário estiver vinculado apenas a um número de celular, apenas a verificação por SMS estará disponível.
  - Se um usuário estiver vinculado apenas a um endereço de e-mail, apenas a verificação de e-mail estará disponível.
  - Se um usuário não estiver vinculado a um endereço de e-mail, número de celular ou dispositivo de MFA virtual, o usuário precisará vincular pelo menos um deles antes que ele possa executar quaisquer operações críticas.
- Talvez você não consiga receber códigos de verificação por e-mail ou SMS devido a erros de comunicação. Nesse caso, é aconselhável usar um dispositivo de MFA virtual para verificação.
- Você pode alterar o número de celular ou endereço de e-mail em **Minha conta** e alterar o **dispositivo de MFA virtual** na página **Configurações de segurança** do console do IAM.
- Se a proteção de operação estiver ativada, os usuários do IAM precisarão inserir códigos de verificação ao executar uma operação crítica. Os códigos de verificação são enviados para o número de celular ou endereço de e-mail vinculado aos usuários do IAM.

Gerenciamento de chaves de acesso

- **Ativação do gerenciamento de chaves de acesso**

  Após a ativação do gerenciamento de chaves de acesso, somente o administrador pode criar, ativar, desativar ou excluir chaves de acesso de usuários do IAM. Esta função está desativada por padrão. Para garantir a segurança dos recursos, ative essa função.

  Para ativar o gerenciamento de chaves de acesso, clique na guia **Critical Operations** na página **Configurações de segurança** e clique em na linha **Access Key Management**.

- **Desativação do gerenciamento de chaves de acesso**

  Depois que o gerenciamento de chaves de acesso é desativado, todos os usuários do IAM podem criar, ativar, desativar ou excluir suas próprias chaves de acesso.

  Para ativar o gerenciamento de chaves de acesso, clique na guia **Critical Operations** na página **Configurações de segurança** e clique em na linha **Access Key Management**.

Autogerenciamento de informações

- **Ativação do autogerenciamento de informações**

  Por padrão, o autogerenciamento de informações é ativado, indicando que todos os usuários do IAM podem gerenciar suas próprias **informações básicas** (senha de logon, número de celular e endereço de e-mail). Determine se permitir que os usuários do IAM gerenciem suas próprias informações e quais informações eles podem modificar.

  Para ativar o autogerenciamento de informações, clique na guia **Critical Operations** na página **Configurações de segurança** e clique em **Enable** na linha **Information Self-Management**. Selecione **Enable**, selecione os tipos de informações que os usuários do IAM podem modificar e clique em **OK**.

- **Desativação do autogerenciamento de informações**

  Depois de desativar o autogerenciamento de informações, somente os administradores podem gerenciar suas próprias **informações básicas**. Se os usuários do IAM precisarem

modificar a senha de logon, o número de celular ou o endereço de e-mail, eles poderão entrar em contato com o administrador. Para mais detalhes, consulte **3.4 Visualização ou modificação das informações do usuário do IAM**.

Para desativar o autogerenciamento de informações, clique na guia **Critical Operations** na página **Configurações de segurança** e clique em **Change** na linha **Information Self-Management**. No painel exibido, selecione **Disable** e clique em **OK**.

Operações críticas

As tabelas a seguir listam as operações críticas definidas por cada serviço de nuvem.

Tabela 8-2 Operações críticas definidas pelos serviços de nuvem

Categoria de serviço	Serviço	Operação crítica
Computação	Elastic Cloud Server (ECS)	● Interromper, reiniciar ou excluir um ECS ● Redefinir a senha para fazer logon em um ECS ● Desanexar um disco ● Desvincular um EIP
	Bare Metal Server (BMS)	● Interromper ou reiniciar um BMS ● Redefinir a senha do BMS ● Desanexar um disco ● Desvincular um EIP
	Auto Scaling (AS)	Excluir um grupo de AS
Armazenamento	Object Storage Service (OBS)	● Excluir um bucket ● Criar, editar ou excluir uma política de bucket ● Configurar uma política de objetos ● Criar, editar ou excluir uma ACL de bucket ● Configurar o registro de acesso ● Configurar a validação de URL ● Criar ou editar um inventário de bucket
	Elastic Volume Service (EVS)	Excluir um disco de EVS
	Cloud Backup and Recovery (CBR)	● Excluir um cofre ● Excluir um backup ● Restaurar um backup ● Excluir uma política ● Desvincular um recurso ● Aceitar um backup
CDN e Intelligent Edge	Content Delivery Network (CDN)	Configurar a política de encerramento de serviço

Categoria de serviço	Serviço	Operação crítica
Containers	Cloud Container Engine (CCE)	Excluir um cluster
	Application Orchestration Service (AOS)	Excluir uma pilha
Rede	Domain Name Service (DNS)	● Modificar, desativar ou excluir um conjunto de registros ● Modificar ou excluir um registro PTR ● Excluir uma linha personalizada
	Virtual Private Cloud (VPC)	● Liberar ou desvincular um EIP ● Excluir uma conexão de emparelhamento de VPC ● Operações de grupo de segurança – Excluir uma regra de entrada ou de saída – Modificar uma regra de entrada ou de saída – Excluir regras de entrada ou de saída em lote
	Elastic Load Balance (ELB)	● Balanceadores de carga compartilhados – Excluir um balanceador de carga – Excluir um ouvinte – Excluir um certificado – Remover um servidor back-end – Desvincular um EIP – Desvincular um endereço IPv4 público ou privado ● Balanceadores de carga dedicados – Excluir um balanceador de carga – Excluir um ouvinte – Excluir um certificado – Remover um servidor back-end – Desvincular um EIP – Desvincular um endereço IPv4 público ou privado – Desvincular um endereço IPv6 – Remover da largura de banda compartilhada IPv6
	Elastic IP (EIP)	● Excluir uma largura de banda compartilhada ● Liberar ou desvincular um EIP ● Liberar ou desvincular EIPs em lote

Categoria de serviço	Serviço	Operação crítica
Rede	Virtual Private Network (VPN)	● Excluir uma conexão de VPN ● Cancelar a assinatura de um gateway de VPN anual/mensal
Segurança e conformidade	SSL Certificate Manager (SCM)	● Excluir um certificado ● Revogar um certificado
Gerenciamento e governança	Identity and Access Management (IAM)	● Desativar a proteção de operação ● Desativar a proteção de logon ● Alterar o número de celular ● Alterar o endereço de e-mail ● Alterar a senha de logon ● Alterar o método de autenticação de logon ● Excluir um usuário do IAM ● Desativar um usuário do IAM ● Excluir uma agência ● Excluir um grupo de usuários ● Excluir uma política ● Excluir permissões ● Criar uma chave de acesso ● Excluir uma chave de acesso ● Desativar uma chave de acesso ● Excluir um projeto ● Modificar o status do gerenciamento de chaves de acesso
Gerenciamento e governança	Cloud Trace Service (CTS)	Desativar um rastreador do sistema
Gerenciamento e governança	Log Tank Service (LTS)	● Excluir um fluxo de logs ou grupo de logs ● Desinstalar o ICAgent
Aplicação	Distributed Cache Service (DCS)	● Redefinir a senha de uma instância de DCS ● Excluir uma instância de DCS ● Limpar dados de instância do DCS
Nuvem dedicada	Dedicated Distributed Storage Service (DSS)	Excluir um disco

Categoria de serviço	Serviço	Operação crítica
Banco de dados	RDS for MySQL	● Redefinir a senha de administrador ● Excluir uma instância de banco de dados ● Excluir um backup de banco de dados ● Restaurar uma instância de banco de dados existente a partir de um arquivo de backup ● Restaurar uma instância de banco de dados existente para um ponto no tempo ● Alternar entre instâncias de banco de dados primárias e em espera ● Alterar a porta do banco de dados ● Excluir uma conta de banco de dados ● Excluir um banco de dados ● Alterar um endereço IP flutuante ● Desvincular um EIP ● Baixar um backup completo
Banco de dados	RDS for PostgreSQL	● Redefinir a senha de administrador ● Excluir uma instância de banco de dados ● Excluir um backup de banco de dados ● Alternar entre instâncias de banco de dados primárias e em espera ● Alterar a porta do banco de dados ● Alterar um endereço IP flutuante ● Desvincular um EIP ● Baixar um backup completo
Banco de dados	GaussDB(for MySQL)	● Excluir uma instância de BD ● Reiniciar uma instância de BD ● Reiniciar um nó ● Excluir uma réplica de leitura ● Desvincular um EIP ● Excluir um banco de dados ● Redefinir uma senha para uma conta de banco de dados ● Excluir uma conta de banco de dados ● Redefinir a senha de administrador ● Alterar um nome de domínio privado ● Alterar um endereço IP privado ● Restaurar dados para um ponto específico no tempo

Categoria de serviço	Serviço	Operação crítica
Banco de dados	Document Database Service (DDS)	● Redefinir a senha ● Reiniciar ou excluir uma instância de banco de dados ● Reiniciar um nó ● Alternar os nós primário e secundário de um conjunto de réplicas ● Excluir uma regra de grupo de segurança ● Ativar endereços IP de nós shard e config ● Restaurar a instância de banco de dados atual a partir de um backup ● Restaurar uma instância de banco de dados existente a partir de um backup ● Alterar uma instância anual/mensal para pagamento por uso
Inteligência empresarial	GaussDB(DWS)	● Dimensionar ou redimensionar um cluster ● Reinicializar um cluster ● Reparar um nó ● Redefinir a senha

Categoria de serviço	Serviço	Operação crítica
	MapReduce Service (MRS)	● Clusters – Excluir um cluster – Alterar um cluster de pagamento por uso para cobrança anual/mensal – Parar todos os componentes – Sincronizar configurações de cluster ● Nós – Interromper todas as funções – Isolar um host – Cancelar o isolamento de um host ● Componentes – Desativar um serviço – Reiniciar um serviço – Executar uma reinicialização contínua do serviço – Interromper uma instância de função – Reiniciar uma instância de função – Executar uma reinicialização contínua da instância – Recomissionar uma instância de função – Desativar uma instância de função – Salvar configurações de serviço ● Patches – Instalar um patch – Desinstalar um patch – Reverter um patch
Comunicações em nuvem	Message&SMS	● Excluir uma assinatura ● Excluir um modelo ● Obter um app_secret ● Vincular um número de celular ou um endereço de e-mail à sua conta da Huawei Cloud ● Configurar uma lista branca de endereços IP ● Renovar um pacote

Categoria de serviço	Serviço	Operação crítica
Desenvolvimento de software DevCloud	Project management (ProjectMan)	• Excluir um projeto • Excluir um membro do projeto • Modificar informações do membro • Modificar ou excluir permissões • Modificar informações básicas do projeto • Excluir um item de trabalho
Suporte ao usuário	Central de cobrança	• Pagar um pedido • Cancelar a assinatura de um pedido • Liberar recursos

8.4 Política de autenticação de logon

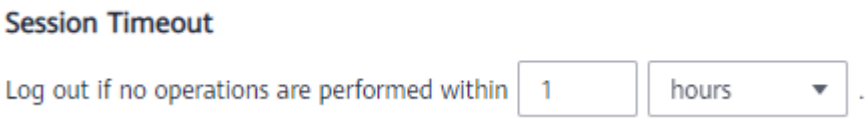
A guia **Login Authentication Policy** da página **Configurações de segurança** fornece as configurações **Tempo limite da sessão**, **Bloqueio de conta**, **Desativação de conta**, **Informações de logon recente** e **Informações personalizadas**. Essas configurações entram em vigor para sua conta e para os usuários do IAM criados usando a conta.

Somente o **administrador** pode configurar a política de autenticação de logon e os usuários do IAM podem visualizar apenas as configurações. Se um usuário do IAM precisar modificar as configurações, ele poderá solicitar que o administrador execute a modificação ou conceda as permissões necessárias.

Tempo limite da sessão

Defina o tempo limite de sessão que será aplicado se você ou os usuários criados usando sua conta não executarem nenhuma operação dentro de um período específico.

Figura 8-11 Tempo limite da sessão

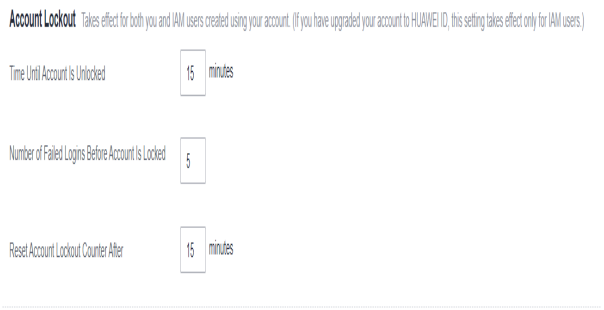


O tempo limite varia de 15 minutos a 24 horas, e o tempo limite padrão é de 1 hora.

Bloqueio de conta

Defina uma duração para bloquear os usuários se um número específico de tentativas de logon sem sucesso for atingido dentro de um determinado período. Você não pode desbloquear sua própria conta ou a conta de um usuário do IAM. Aguarde até que o tempo de bloqueio expire.

Figura 8-12 Bloqueio de conta



O administrador pode definir a duração do bloqueio de conta, o número máximo de tentativas de logon sem sucesso antes que a conta seja bloqueada e o tempo para redefinir o contador de bloqueio de conta.

- Duração do bloqueio: o valor varia de 15 a 30 minutos e o valor padrão é **15 minutes**.
- Número máximo de tentativas de logon sem sucesso: o valor varia de 3 a 10, e o valor padrão é **5**.
- Tempo para redefinir o contador de bloqueio de conta: o valor varia de 15 a 60 minutos e o valor padrão é **15 minutes**.

Desativação de conta

Defina um período de validade para desativar os usuários do IAM se eles não tiverem acessado a Huawei Cloud usando o console ou as APIs dentro de um determinado período.

Esta opção está desativada por padrão. O período de validade varia de 1 a 240 dias.

Se você ativar essa opção, a configuração entrará em vigor apenas para usuários do IAM criados usando sua conta. Se um usuário do IAM estiver desativado, ele poderá solicitar ao administrador que ative sua conta novamente.

Informações de logon recente

Configure se deseja que o sistema exiba as informações de logon anterior após o logon. Se informações de logon incorretas forem exibidas na página **Login Verification**, altere sua senha imediatamente.

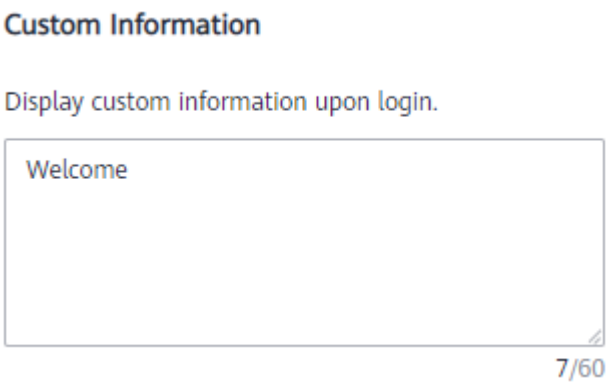
Esta opção está desativada por padrão e pode ser ativada pelo administrador.

Informações personalizadas

Defina as informações personalizadas que serão exibidas após o logon bem-sucedido. Por exemplo, insira a palavra **Welcome**.

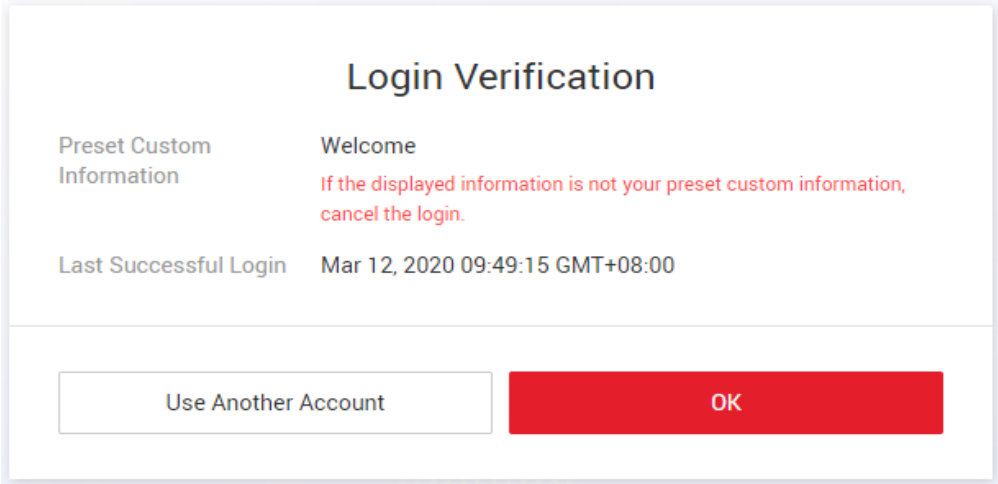
Esta opção está desativada por padrão e pode ser ativada pelo administrador.

Figura 8-13 Informações personalizadas



Você e todos os usuários do IAM criados usando sua conta verão as mesmas informações após o logon bem-sucedido.

Figura 8-14 Verificação de logon



8.5 Política de senha

A guia **Password Policy** da página **Configurações de segurança** fornece as configurações **Composição e reutilização de senhas**, **Expiração da senha** e **Idade mínima da senha**.

Somente o **administrador** pode configurar a política de senha e os usuários do IAM podem visualizar apenas as configurações. Se um usuário do IAM precisar modificar as configurações, ele poderá solicitar que o administrador execute a modificação ou conceda as permissões necessárias.

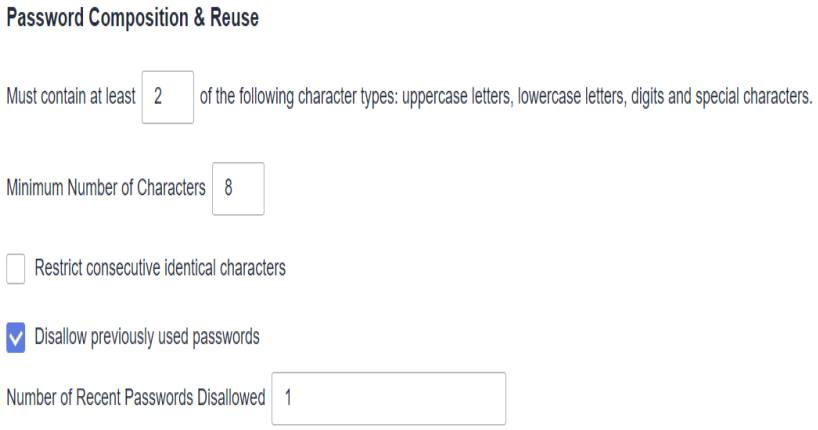
Você pode configurar a política de senha para garantir que os usuários do IAM criem senhas fortes e as alterem periodicamente. Na política de senha, você pode definir requisitos de senha, como o comprimento mínimo da senha, se deve permitir caracteres idênticos consecutivos em uma senha e se deve permitir senhas usadas anteriormente.

NOTA

Se a sua conta da Huawei Cloud já tiver sido atualizada para uma HUAWEI ID, a política de senha não entrará em vigor para o ID.

Composição e reutilização de senhas

Figura 8-15 Composição e reutilização de senhas



- Certifique-se de que a senha contém de 2 a 4 dos seguintes tipos de caracteres: letras maiúsculas, letras minúsculas, dígitos e caracteres especiais. Por padrão, a senha deve conter pelo menos dois desses tipos de caracteres.
- Defina o número mínimo de caracteres que uma senha deve conter. O valor padrão é 8 e o intervalo de valores é de 8 a 32.
- (Opcional) Ative a opção **Restrict consecutive identical characters** e defina o número máximo de vezes que um caractere pode estar consecutivamente presente em uma senha. Por exemplo, o valor **1** indica que caracteres idênticos consecutivos não são permitidos em uma senha.
- (Opcional) Ative a opção **Disallow previously used passwords** e defina o número de senhas usadas anteriormente que não são permitidas. Por exemplo, o valor **3** indica que o usuário não pode definir as últimas três senhas que o usuário usou anteriormente ao definir uma nova senha.

As alterações na política de senha entram em vigor na próxima vez que você ou seus usuários do IAM alterarem as senhas. A nova política de senha também se aplicará aos usuários do IAM criados posteriormente.

Expiração da senha

Defina um período de validade para as senhas para que os usuários precisem alterar suas senhas periodicamente. Os usuários serão solicitados a alterar suas senhas 15 dias antes da expiração da senha. Senhas expiradas não podem ser usadas para fazer logon na Huawei Cloud.

Esta opção está desativada por padrão. O período de validade varia de 1 a 180 dias.

As alterações entrarão em vigor imediatamente para sua conta e para todos os usuários do IAM em sua conta.

> **NOTA**
>
> Depois que a senha expirar, os usuários precisarão definir uma nova senha por meio do URL enviado por e-mail. A nova senha deve ser diferente da senha anterior.

Idade mínima da senha

Para evitar a perda de senha devido a alterações frequentes de senha, você pode definir um período mínimo após o qual os usuários podem fazer uma alteração de senha.

Esta opção está desativada por padrão. O período de validade varia de 0 a 1.440 minutos.

As alterações entrarão em vigor imediatamente para sua conta e para todos os usuários do IAM em sua conta.

8.6 ACL

A guia **ACL** da página **Configurações de segurança** fornece as configurações de **Intervalos de endereços IP**, **Blocos CIDR IPv4** e **Pontos de extremidade da VPC** para permitir o acesso do usuário somente de intervalos de endereços IP especificados, blocos CIDR IPv4 ou pontos de extremidade da VPC.

Somente o **administrador** pode configurar a ACL. Se um usuário do IAM precisar configurar a ACL, ele poderá solicitar que o administrador execute a configuração ou conceda as permissões necessárias.

Access type:

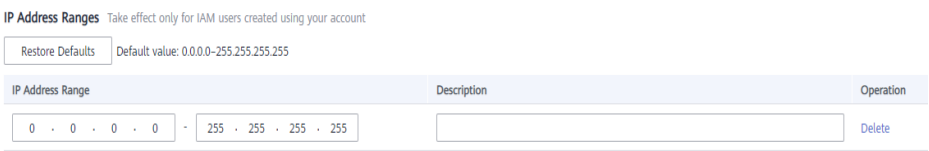
- **Console Access** (recomendado): a ACL entra em vigor apenas para usuários do IAM e usuários federados (iniciados pelo SP) que são criados usando sua conta e têm acesso ao console.
- **API Access**: a ACL controla o acesso à API dos usuários por meio do API Gateway e entra em vigor apenas para usuários do IAM e usuários federados duas horas após a conclusão da configuração.

NOTA

- Você pode configurar um máximo de 200 itens de controle de acesso.
- Se um usuário do IAM ou um usuário federado acessar a Huawei Cloud por meio de um servidor de proxy, defina os endereços IP, intervalos de endereços ou blocos CIDR permitidos com base no endereço IP do proxy. Se um usuário do IAM ou um usuário federado acessar a Huawei Cloud por meio de uma rede pública, defina com base no endereço IP público.

Intervalos de endereços IP

Figura 8-16 Intervalos de endereços IP



Especifique o endereço IP varia de 0.0.0.0 a 255.255.255.255 para permitir o acesso à Huawei Cloud. O valor padrão é **0.0.0.0–255.255.255.255**. Se esse parâmetro for deixado em branco ou o valor padrão for usado, os usuários do IAM poderão acessar o console da Huawei Cloud de qualquer lugar.

Blocos CIDR IPv4

Especifique blocos CIDR IPv4 para permitir o acesso à Huawei Cloud. Por exemplo, defina **IPv4 CIDR block** como **10.10.10.10/32**.

Pontos de extremidade da VPC

Especifique pontos de extremidade de VPC, como **0ccad098-b8f4-495a-9b10-613e2a5exxxx**, para permitir acesso baseado em API à Huawei Cloud. Se o controle de acesso não estiver configurado, você poderá acessar APIs de todos os pontos de extremidade da VPC por padrão.

NOTA

- O acesso do usuário será permitido se qualquer um dos **IP Address Ranges**, **IPv4 CIDR Blocks** e **VPC Endpoints** for atendido.
- Para restaurar **IP Address Ranges** para as configurações padrão (0.0.0.0–255.255.255.255) e limpar as configurações em **IPv4 CIDR Blocks** e **VPC Endpoints**, clique em **Restore Defaults**.

9 Provedores de identidade

9.1 Introdução

A Huawei Cloud fornece federação de identidade baseada em SAML (Security Assertion Markup Language) ou OpenID Connect. Essa função permite que os usuários em seu sistema de gerenciamento empresarial acessem a Huawei Cloud por meio de logon único (SSO).

Conceitos básicos

Tabela 9-1 Conceitos básicos

Conceito	Descrição
Provedor de identidade (IdP)	Um IdP coleta e armazena informações de identidade do usuário, como nomes de usuário e senhas, e autentica os usuários durante o logon. Para a federação de identidade entre uma empresa e a Huawei Cloud, o sistema de autenticação de identidade da empresa é um provedor de identidade e também é chamado de "IdP empresarial". Os IdPs de terceiros mais populares incluem os Serviços de Federação do Active Directory (AD FS) de Microsoft e o Shibboleth.

Conceito	Descrição
Provedor de serviços (SP)	Um provedor de serviços estabelece uma relação de confiança com um IdP e fornece serviços com base nas informações do usuário fornecidas pelo IdP. Para federação de identidade entre uma empresa e a Huawei Cloud, a Huawei Cloud é um provedor de serviços.
Federação de identidade	A federação de identidade é o processo de **estabelecer uma relação de confiança** entre um IdP e um SP para implementar o SSO.
Logon único (SSO)	O SSO permite que os usuários acessem um SP confiável após efetuar logon no IdP empresarial. Por exemplo, depois que uma relação de confiança é estabelecida entre um sistema de gerenciamento empresarial e a Huawei Cloud, os usuários no sistema de gerenciamento empresarial podem usar suas contas e senhas existentes para acessar a Huawei Cloud por meio do link de logon no sistema de gerenciamento empresarial. A Huawei Cloud oferece suporte a dois tipos de SSO: SSO de usuário virtual e SSO de usuário do IAM.
SAML 2.0	A SAML 2.0 é um protocolo baseado em XML que usa tokens de segurança contendo asserções para passar informações sobre um usuário final entre um IdP e um SP. É um padrão aberto ratificado pela Organização para o Avanço de Padrões de Informação Estruturada (OASIS) e está sendo usado por muitos IdPs. Para obter mais informações sobre esse padrão, consulte **Visão geral técnica de SAML 2.0**. A Huawei Cloud implementa a federação de identidade em conformidade com SAML 2.0. Para federar com sucesso seus usuários empresariais com a Huawei Cloud, certifique-se de que seu IdP empresarial seja compatível com este protocolo.
OpenID Connect	OpenID Connect é uma camada de identidade simples sobre o protocolo Open Authorization 2.0 (OAuth 2.0). O IAM implementa a federação de identidade em conformidade com OpenID Connect 1.0. Para federar com sucesso seus usuários empresariais com a Huawei Cloud, certifique-se de que seu IdP empresarial seja compatível com este protocolo. Para obter mais informações sobre OpenID Connect, consulte **Introdução ao OpenID Connect**.
OAuth 2.0	OAuth 2.0 é um protocolo de autorização aberto. A estrutura de autorização deste protocolo permite que aplicações de terceiros obtenham permissões de acesso.

Vantagens da federação de identidade

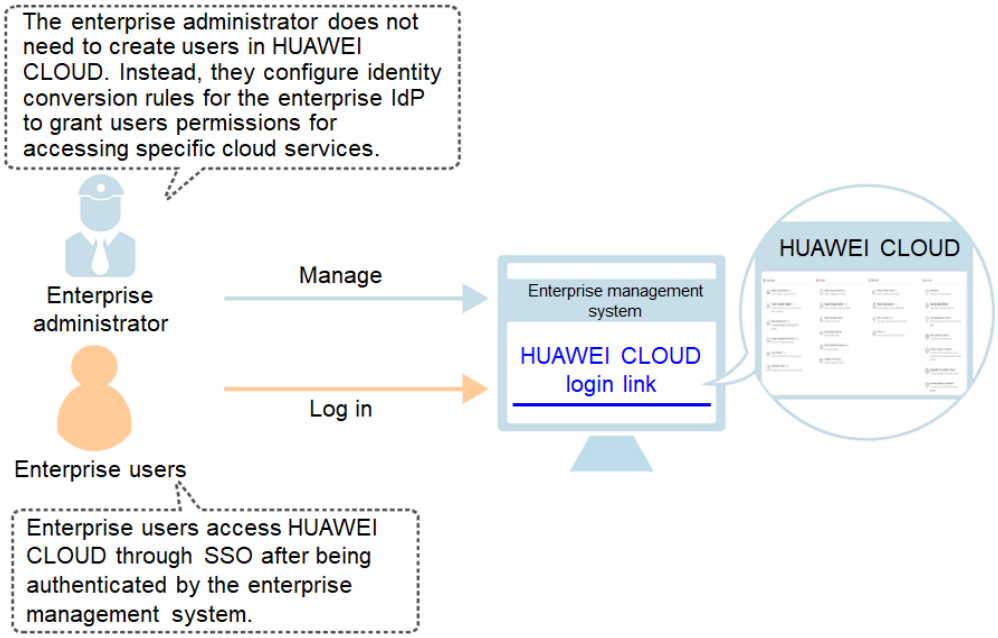
- Gerenciamento fácil de identidade

  Com um provedor de identidade, o administrador pode gerenciar as identidades da força de trabalho fora da Huawei Cloud e conceder a essas identidades externas da força de trabalho permissões para usar recursos na Huawei Cloud.

- Operações simplificadas

  Os usuários da força de trabalho podem usar suas contas existentes na empresa para acessar a Huawei Cloud por meio do SSO.

Figura 9-1 Vantagens da federação de identidade



Tipo de SSO

O IAM oferece suporte a dois tipos de SSO: SSO de usuário virtual e SSO de usuário do IAM. Para obter detalhes sobre como escolher um tipo de SSO, consulte **9.2 Cenários de aplicações de SSO de usuário virtual e SSO de usuário do IAM**.

- SSO de usuário virtual

  Depois que um usuário federado fizer logon na Huawei Cloud, o sistema cria automaticamente um usuário virtual e concede permissões de acesso ao usuário virtual com base nas regras de conversão de identidade configuradas.

- SSO de usuário do IAM

  Depois que um usuário federado faz logon na Huawei Cloud, o sistema mapeia automaticamente o **ID de identidade externa** para um usuário do IAM para que o usuário federado tenha as permissões do usuário do IAM mapeado.

Atualmente, o IAM oferece suporte a dois métodos de logon federados: SSO baseado em navegador (SSO da Web) e SSO via chamada de API.

- SSO da Web: os navegadores são usados como meio de comunicação. Esse tipo de autenticação permite que usuários comuns acessem a Huawei Cloud usando navegadores. Você pode iniciar o SSO da Web a partir do lado do IdP ou do SP.
  - SSO iniciado por IdP: **configure um link de logon no sistema de gerenciamento empresarial**. Os funcionários da sua empresa podem usar o link para fazer logon na Huawei Cloud a partir do sistema de gerenciamento empresarial.
  - SSO iniciado por SP: a Huawei Cloud fornece a entrada de **logon de usuário federado**. Os funcionários da sua empresa podem inserir uma conta da Huawei

Cloud e escolher o IdP da empresa na página de logon para acessar a Huawei Cloud.

- SSO via chamada de API: funcionários empresariais chamam APIs usando ferramentas de desenvolvimento (como OpenStack Client e ShibbolethECP Client) para acessar a Huawei Cloud.

Tabela 9-2 Logons federados

Tipo de SSO	Protocolos suportados	SSO da Web	Chamada de API	Iniciado pelo IdP	Iniciado pelo SP	Vários IdPs
Usuário virtual	SAML 2.0 e OpenID Connect	Compatível	Compatível	Compatível	Compatível	Compatível
Usuário do IAM	SAML 2.0	Compatível	Compatível	Compatível	Compatível	Não compatível

Este capítulo descreve como acessar a Huawei Cloud por meio do logon SSO da Web. Para obter detalhes sobre como acessar a Huawei Cloud chamando APIs, consulte **Gerenciamento de federação de identidade**.

Precauções

- Certifique-se de que seu servidor de IdP empresarial e a Huawei Cloud usem o Horário do Meridiano de Greenwich (GMT) no mesmo fuso horário.
- As informações de identidade (como endereço de e-mail ou número de celular) de usuários federados são armazenadas no IdP empresarial. Os usuários federados são mapeados para a Huawei Cloud como identidades virtuais, portanto, seu acesso à Huawei Cloud tem as seguintes restrições:
  - Os usuários federados não precisam executar uma verificação em duas etapas ao executar operações críticas, mesmo que a **proteção de operação crítica** (proteção de logon ou proteção de operação) esteja ativada.
  - Os usuários federados não podem criar chaves de acesso com validade ilimitada, mas podem obter credenciais de acesso temporárias (chaves de acesso e tokens de segurança) usando tokens de usuário ou agência. Para obter detalhes, consulte **Obtenção de uma chave de acesso temporária e de um token de segurança por meio de um token**.

    Se um usuário federado precisar de uma chave de acesso com validade ilimitada, ele poderá entrar em contato com o administrador da conta ou com um usuário do IAM para criar uma. Uma chave de acesso contém as permissões concedidas a um usuário, portanto, é recomendável que o usuário federado solicite que um usuário do IAM no mesmo grupo crie uma chave de acesso.

9.2 Cenários de aplicações de SSO de usuário virtual e SSO de usuário do IAM

O IAM oferece suporte a dois tipos de SSO: SSO de usuário virtual e SSO de usuário do IAM. Esta seção descreve os dois tipos de SSO e suas diferenças, ajudando você a escolher um tipo apropriado para o seu negócio.

SSO de usuário virtual

Depois que um usuário federado faz logon na Huawei Cloud, o sistema cria automaticamente um usuário virtual e atribui permissões ao usuário com base nas regras de conversão de identidade. O SSO de usuário virtual é recomendado se:

- Para reduzir os custos de gerenciamento, você não deseja criar e gerenciar usuários do IAM na plataforma de nuvem.
- Você deseja atribuir permissões para recursos de nuvem com base nos grupos de usuários ou atributos em seu IdP empresarial local. As alterações de permissão no IdP empresarial local podem ser sincronizadas com a plataforma de nuvem ajustando os grupos de usuários ou atributos localmente.
- Sua empresa tem filiais e pode exigir vários IdPs empresariais. Esses IdPs precisam acessar a mesma conta da Huawei Cloud. Você precisa configurar vários IdPs na Huawei Cloud para federação de identidade.

SSO de usuário do IAM

Depois que um usuário federado faz logon na Huawei Cloud, o sistema mapeia automaticamente o ID de identidade externa para um usuário do IAM para que o usuário federado tenha as permissões do usuário do IAM mapeado. O SSO de usuário do IAM é recomendado se:

- Os produtos de nuvem que você usa (como o **CodeArts**) não oferecem suporte ao SSO de usuário virtual.
- Você não precisa de SSO de usuário virtual e deseja simplificar a configuração de IdP.

Diferenças entre o SSO de usuário virtual e o SSO de usuário do IAM

As diferenças entre o SSO de usuário virtual e o SSO de usuário do IAM são descritas a seguir:

1. Conversão de identidade: o SSO de usuário virtual usa **regras de conversão de identidade**, enquanto o SSO de usuário do IAM usa IDs de identidade externa para conversão de identidade. Se o valor **IAM_SAML_Attributes_xUserId** de um ou mais usuários de IdP for o mesmo que o **ID de identidade externa** de um usuário do IAM, esses usuários de IdP serão mapeados para o usuário do IAM. Ao usar o SSO de usuário do IAM, certifique-se de ter definido **IAM_SAML_Attributes_xUserId** no IdP e **External Identity ID** no SP com o mesmo valor.

2. Identidade do usuário no IAM: no SSO de usuário virtual, o usuário do IdP não tem um usuário do IAM correspondente na lista de usuários do IAM. Depois que o usuário do IdP faz logon, o sistema cria automaticamente um usuário virtual para ele. No SSO de usuário do

IAM, o usuário do IdP tem um usuário do IAM mapeado por ID de identidade externa no console do IAM.

3. Atribuição de permissões no IAM: no SSO de usuário virtual, as permissões do usuário do IdP são definidas pela regra de conversão de identidade. No SSO de usuário do IAM, o usuário do IdP herda as permissões do grupo de usuários ao qual o usuário do IAM mapeado pertence.

9.3 SSO de usuário virtual via SAML

9.3.1 Visão geral do SSO de usuário virtual via SAML

Huawei Cloud suporta federação de identidade com Security Assertion Markup Language (SAML), que é um padrão aberto usado por muitos provedores de identidade (IdPs). Durante a federação de identidade, a Huawei Cloud funciona como um provedor de serviços (SP) e as empresas funcionam como IdPs. Esta seção descreve como configurar a federação de identidades e como funciona a federação de identidades.

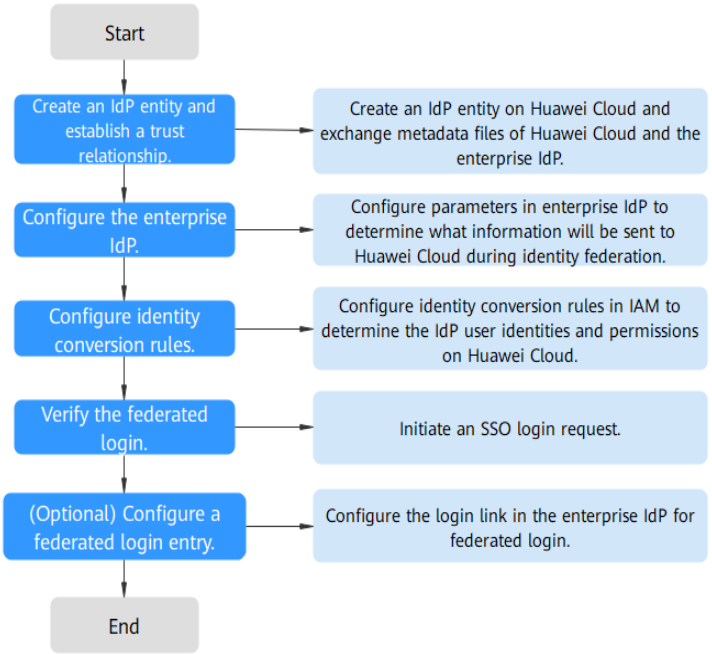
⚠ CUIDADO

Certifique-se de que o seu IdP empresarial ofereça suporte à SAML 2.0.

Configurar a federação de identidade

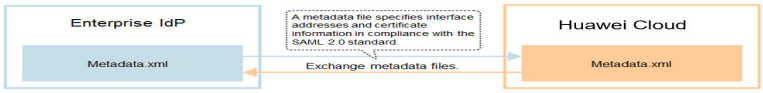
A seguir, descrevemos como configurar o seu IdP empresarial e a Huawei Cloud para que confiem um no outro.

Figura 9-2 Configuração de SSO de usuário virtual via SAML



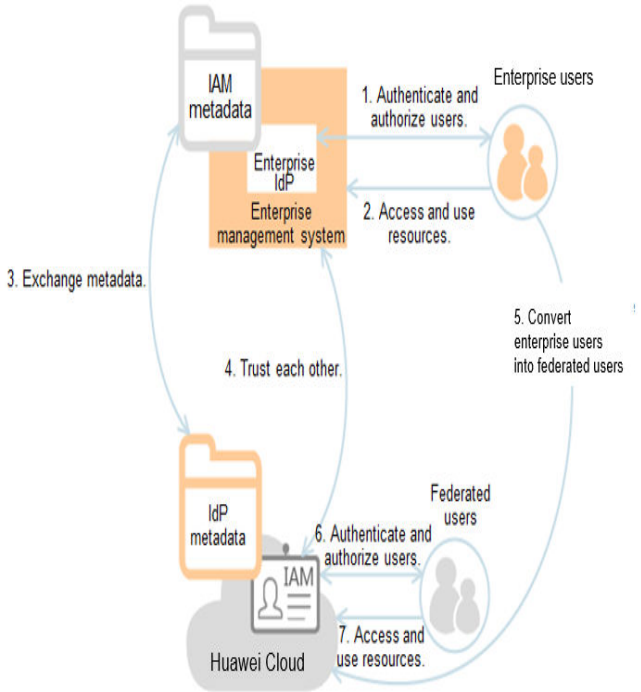
1. **Criar uma entidade IdP e estabelecer uma relação de confiança**: crie uma entidade IdP para sua empresa na Huawei Cloud. Em seguida, faça o upload do arquivo de metadados da Huawei Cloud para o IdP empresarial e faça o upload do arquivo de metadados do IdP empresarial para a Huawei Cloud.

   Figura 9-3 Troca de arquivos de metadados



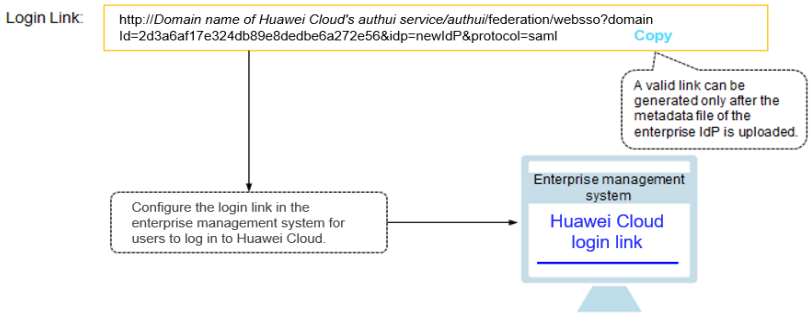
2. **Configurar o IdP empresarial**: configure parâmetros de IdP empresarial para determinar quais informações podem ser enviadas para a Huawei Cloud.
3. **Configurar regras de conversão de identidade**: configure regras de conversão de identidade para determinar as identidades e permissões de usuário de IdP na Huawei Cloud.

   Figura 9-4 Mapeamento de identidades externas para usuários virtuais



4. **Verificar o logon federado**: verifique se o usuário empresarial pode fazer logon na Huawei Cloud por meio de SSO.
5. **(Opcional) Configurar uma entrada de logon federada**: configure o link de logon (consulte **Figura 9-5**) no IdP empresarial para permitir que os usuários empresariais sejam redirecionados para a Huawei Cloud a partir do seu sistema de gerenciamento empresarial.

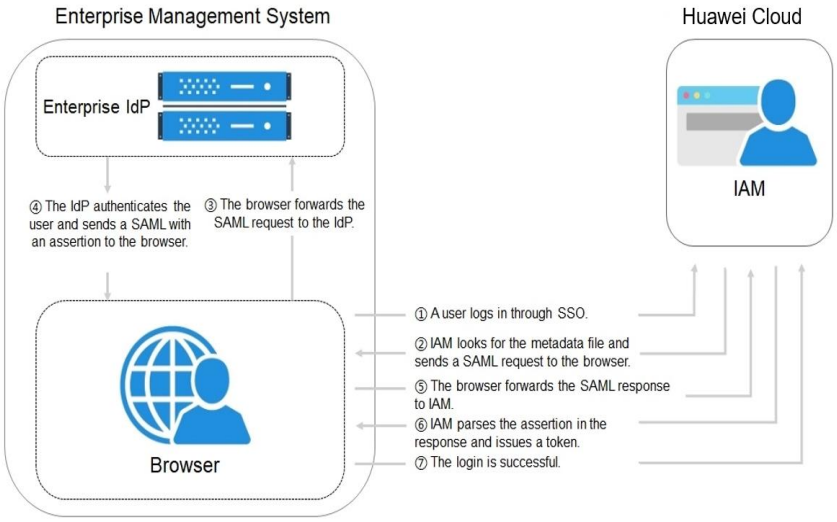
Figura 9-5 Modelo de logon do SSO



Como funciona a federação de identidade

Figura 9-6 mostra o processo de federação de identidade entre um sistema de gerenciamento empresarial e a Huawei Cloud.

Figura 9-6 Como funciona a federação de identidade



NOTA

Para visualizar solicitações e asserções interativas com uma experiência melhor, é recomendável usar o Google Chrome e instalar o SAML Message Decoder.

Como mostrado em **Figura 9-6**, o processo de federação de identidade é o seguinte:

1. Um usuário abre o link de logon gerado após a criação do IdP no navegador. O navegador envia uma solicitação de SSO para a Huawei Cloud.
2. A Huawei Cloud autentica o usuário no arquivo de metadados do IdP empresarial e constrói uma solicitação SAML para o navegador.
3. O navegador encaminha a solicitação SAML para o IdP empresarial.
4. O usuário insere seu nome de usuário e senha na página de logon. Depois que o IdP empresarial autentica a identidade do usuário, ele constrói uma asserção SAML contendo os detalhes do usuário e envia a asserção ao navegador como uma resposta SAML.

5. O navegador responde e encaminha a resposta SAML para a Huawei Cloud.
6. A Huawei Cloud analisa a asserção na resposta SAML, identifica o mapeamento do grupo de usuários do IAM para o usuário com base nas regras de conversão de identidade e emite um token para o usuário.
7. O logon do SSO foi bem-sucedido.

NOTA

A afirmação deve conter uma assinatura; caso contrário, o logon falhará.

9.3.2 Etapa 1: criar uma entidade IdP

Para estabelecer uma relação de confiança entre um IdP empresarial e a Huawei Cloud, carregue o arquivo de metadados da Huawei Cloud para o IdP empresarial e, em seguida, crie uma entidade IdP e carregue o arquivo de metadados do IdP empresarial no console do IAM.

Pré-requisitos

Você leu a documentação do IdP empresarial ou entendeu como usar o IdP empresarial. As configurações de diferentes IdPs empresariais são muito diferentes, portanto não são descritas neste documento. Para obter detalhes sobre como obter o arquivo de metadados do IdP empresarial e como carregar o arquivo de metadados da Huawei Cloud para o IdP empresarial, consulte a documentação de ajuda do IdP.

Estabelecer uma relação de confiança entre o IdP empresarial e a Huawei Cloud

O arquivo de metadados da Huawei Cloud precisa ser configurado no IdP empresarial para estabelecer uma relação de confiança entre os dois sistemas.

Passo 1 Baixe o arquivo de metadados da Huawei Cloud.

Visite **https://auth-intl.huaweicloud.com/authui/saml/metadata.xml** (O Google Chrome é recomendado). Faça o download do arquivo de metadados da Huawei Cloud e defina o nome do arquivo, por exemplo, **SP-metadata.xml**.

Passo 2 Faça upload do arquivo de metadados para o servidor de IdP empresarial. Para obter detalhes, consulte a documentação de ajuda do IdP empresarial.

Passo 3 Obtenha o arquivo de metadados do IdP empresarial. Para obter detalhes, consulte a documentação de ajuda do IdP empresarial.

----Fim

Criar uma entidade IdP na Huawei Cloud

Para criar uma entidade IdP no console do IAM, faça o seguinte:

Passo 1 Faça logon no **console do IAM**, escolha **Identity Providers** no painel de navegação e clique em **Create Identity Provider** no canto superior direito.

Passo 2 Especifique o nome, o protocolo, o tipo de SSO, o status e a descrição da entidade IdP.

Tabela 9-3 Parâmetros básicos de um IdP

Parâmetro	Descrição
Name	Nome do IdP, que deve ser exclusivo globalmente. Você é aconselhado a usar o nome de domínio.
Protocol	Protocolo de IdP. A Huawei Cloud oferece suporte aos protocolos SAML e OpenID Connect. Para obter detalhes sobre a federação de identidade baseada em OpenID Connect, consulte **9.5 SSO de usuário virtual via OpenID Connect**.
SSO Type	Tipo de IdP. Uma conta pode ter apenas um tipo de IdP. A seguir, descreve-se o tipo de usuário virtual. SSO do usuário virtual: depois que um usuário federado faz logon na Huawei Cloud, o sistema cria automaticamente um usuário virtual para o usuário federado. Uma conta pode ter vários IdPs do tipo de usuário virtual.
Status	Status do IdP. O valor padrão é **Enabled**.

Passo 3 Clique em **OK**.

----Fim

Configurar o arquivo de metadados do IdP empresarial na Huawei Cloud

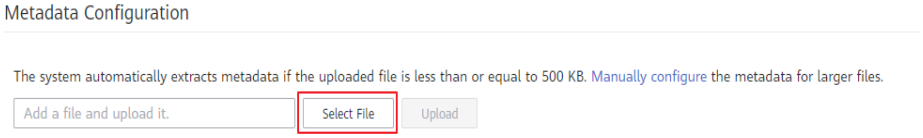
Para configurar o arquivo de metadados do IdP empresarial na Huawei Cloud, você pode fazer upload do arquivo de metadados ou editar manualmente os metadados no console do IAM. Para um arquivo de metadados maior que 500 KB, configure manualmente os metadados. Se os metadados tiverem sido alterados, carregue o arquivo de metadados mais recente ou edite os metadados existentes para garantir que os usuários federados possam fazer logon na Huawei Cloud com sucesso.

NOTA

Para obter detalhes sobre como obter o arquivo de metadados de um IdP empresarial, consulte a documentação de ajuda do IdP empresarial.

- **Carregar um arquivo de metadados.**
  a. Clique em **Modify** na linha que contém o IdP.
  b. Clique em **Select File** e selecione o arquivo de metadados do IdP empresarial.

  Figura 9-7 Carregar um arquivo de metadados

  c. Clique em **Upload**. Os metadados extraídos do arquivo carregado são exibidos. Clique em **OK**.
     - Se o arquivo de metadados carregado contiver vários IdPs, selecione o IdP que deseja usar na lista suspensa **Entity ID**.

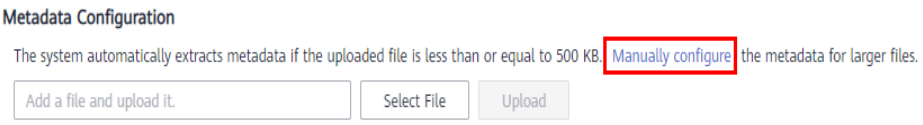
- Se uma mensagem for exibida indicando que nenhum ID de entidade foi especificado ou que o certificado de assinatura expirou, verifique o arquivo de metadados e carregue-o novamente ou configure os metadados manualmente.

d. Clique em **OK**.

- **Configurar metadados manualmente.**

a. Clique em **Manually configure**.

Figura 9-8 Configuração manual de metadados



b. Na caixa de diálogo **Configure Metadata**, defina os parâmetros de metadados, como **Entity ID**, **Signing Certificate** e **SingleSignOnService**.

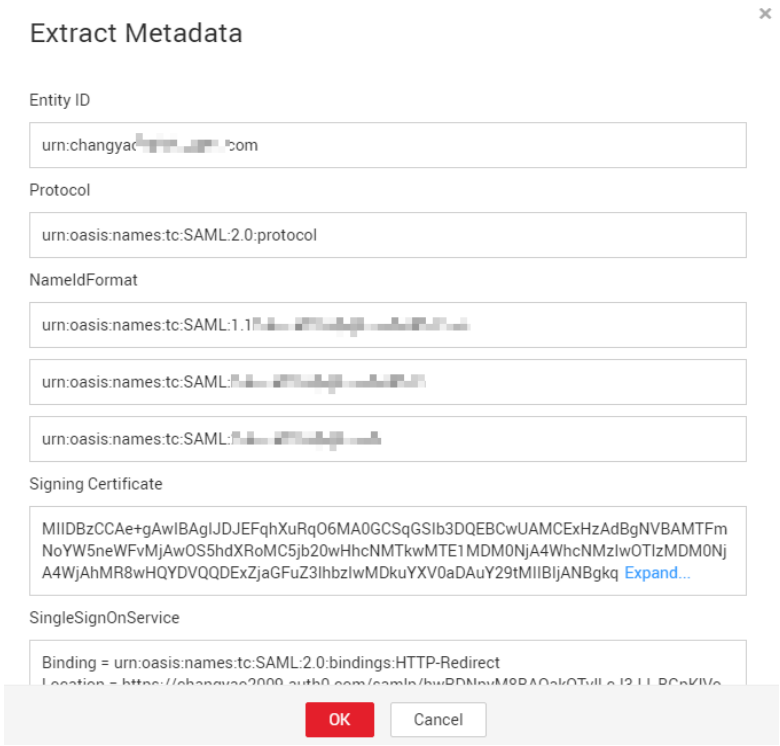
Parâmetro	Obrigatório	Descrição
Entity ID	Sim	O identificador exclusivo de um IdP. Digite o valor de **entityID** exibido no arquivo de metadados do IdP empresarial. Se o arquivo de metadados contiver vários IdPs, escolha aquele que você deseja usar.
Protocol	Sim	Protocolo usado para federação de identidade entre um IdP empresarial e SP. O protocolo é selecionado por padrão.
NameIdFormat	Não	Digite o valor de **NameIdFormat** exibido no arquivo de metadados do IdP. Especifica o formato de identificador de nome de usuário suportado pelo IdP, que é usado para comunicação entre o IdP e o usuário federado. Se você configurar vários valores, a Huawei Cloud usa o primeiro valor por padrão.

Parâmetro	Obrigatório	Descrição
Signing Certificate	Sim	Insira o valor de **<X509Certificate>** exibido no arquivo de metadados do IdP. Um certificado de assinatura é um certificado de chave pública usado para verificação de assinatura. Para fins de segurança, insira uma chave pública contendo pelo menos 2.048 bits. O certificado de assinatura é usado durante a federação de identidade para garantir que as afirmações sejam confiáveis e completas. Se você configurar vários valores, a Huawei Cloud usa o primeiro valor por padrão.
SingleSignOnService	Sim	Digite o valor de **SingleSignOnService** exibido no arquivo de metadados do IdP. Este parâmetro define como as solicitações SAML são enviadas durante o SSO. Ele deve suportar HTTP Redirect ou HTTP POST. Se você configurar vários valores, a Huawei Cloud usa o primeiro valor por padrão.
SingleLogoutService	Não	Digite o valor de **SingleLogoutService** exibido no arquivo de metadados do IdP. Este parâmetro indica o endereço para o qual os usuários federados serão redirecionados após encerrarem suas sessões. Ele deve suportar HTTP Redirect ou HTTP POST. Se você configurar vários valores, a Huawei Cloud usa o primeiro valor por padrão.

O exemplo a seguir mostra o arquivo de metadados de um IdP empresarial e os metadados configurados manualmente.

Figura 9-9 Arquivo de metadados de um IdP empresarial

Figura 9-10 Configuração manual de metadados



c. Clique em **OK**.

Operações relacionadas

- Visualizar informações de IdP: na lista de IdP, clique em **View** na linha que contém o IdP e exiba suas informações básicas, configuração de metadados e regras de conversão de identidade.

  NOTA

  Para modificar a configuração de um IdP, clique em **Modify** na parte inferior da página de detalhes.

- Modificar um IdP: na lista do IdP, clique em **Modify** na linha que contém o IdP e, em seguida, altere seu status ou modifique a descrição, os metadados ou as regras de conversão de identidade.
- Excluir um IdP: na lista do IdP, clique em **Delete** na linha que contém o IdP e clique em **Yes** na caixa de diálogo exibida.

Procedimento de acompanhamento

- Configurar o IdP empresarial: configure parâmetros de IdP empresarial para determinar quais informações podem ser enviadas para a Huawei Cloud.
- Configurar regras de conversão de identidade: na área **Identity Conversion Rules**, configure regras de conversão de identidade para estabelecer um mapeamento entre usuários empresariais e grupos de usuários do IAM. Desta forma, os usuários empresariais podem obter as permissões correspondentes na Huawei Cloud. Para mais detalhes, consulte **9.3.4 Etapa 3: configurar regras de conversão de identidade**.
- Verificar o logon federado: verifique se o usuário empresarial pode fazer logon na Huawei Cloud por meio de SSO. Para mais detalhes, consulte **9.3.5 Etapa 4: verificar o logon federado**.

9.3.3 Etapa 2: configurar o IdP empresarial

Você pode configurar parâmetros no IdP empresarial para determinar quais informações serão enviadas para a Huawei Cloud. A Huawei Cloud autentica a identidade federada e atribui permissões com base nas informações recebidas e nas regras de conversão de identidade.

Parâmetros comuns em um IdP empresarial

Tabela 9-4 Parâmetros comuns em um IdP empresarial

Parâmetro	Descrição	Cenário
IAM_SAML_Attributes_redirect_url	URL de destino para o qual o usuário federado será redirecionado	Durante o logon do SSO, o usuário federado será redirecionado para uma página na Huawei Cloud, por exemplo, a página inicial do Cloud Eye na região CN-Hong Kong.
IAM_SAML_Attributes_domain_id	ID da conta da Huawei Cloud a ser federado com o IdP empresarial	Esse parâmetro é obrigatório na federação iniciada por IdP empresarial.
IAM_SAML_Attributes_idp_id	Nome da entidade IdP criada na Huawei Cloud	Esse parâmetro é obrigatório na federação iniciada por IdP empresarial.

9.3.4 Etapa 3: configurar regras de conversão de identidade

Depois que um usuário de IdP empresarial faz logon na Huawei Cloud, a Huawei Cloud autentica a identidade e atribui permissões ao usuário com base nas regras de conversão de identidade. Você pode personalizar regras de conversão de identidade com base em seus requisitos de serviço. Se você não configurar regras de conversão de identidade, o nome de usuário do usuário federado na Huawei Cloud é **FederationUser** por padrão, e o usuário federado só pode acessar a Huawei Cloud por padrão.

Você pode configurar os seguintes parâmetros para usuários federados:

- Username: nomes de usuários de usuários federados na Huawei Cloud.

- User permissions: permissões atribuídas a usuários federados na Huawei Cloud. Você precisa mapear os usuários federados para grupos de usuários do IAM. Dessa forma, os usuários federados podem obter as permissões dos grupos de usuários para usar os recursos da Huawei Cloud. Certifique-se de que grupos de usuários foram criados. Para obter detalhes sobre como criar um grupo de usuários, consulte **4.1 Criação de um grupo de usuários e atribuição de permissões**.

NOTA

- As modificações nas regras de conversão de identidade entrarão em vigor na próxima vez que os usuários federados fizerem logon.
- Para modificar as permissões de um usuário, modifique as permissões do grupo de usuários ao qual o usuário pertence. Em seguida, reinicie o IdP empresarial para que as modificações tenham efeito.

Pré-requisitos

- O administrador empresarial criou uma conta na Huawei Cloud, criou grupos de usuários e atribuiu permissões ao grupo no IAM. Para mais detalhes, consulte **4.1 Criação de um grupo de usuários e atribuição de permissões**.
- Um IdP foi criado na Huawei Cloud. Para mais detalhes, consulte **9.3.2 Etapa 1: criar uma entidade IdP**.

Procedimento

Se você configurar regras de conversão de identidade clicando em **Create Rule**, o IAM converterá os parâmetros especificados para o formato JSON. Como alternativa, você pode clicar em **Edit Rule** para configurar regras diretamente no formato JSON. Para mais detalhes, consulte **9.6 Sintaxe das regras de conversão de identidade**.

- **Criar regras**
  a. Faça logon no **console do IAM** como administrador. No painel de navegação, escolha **Identity Providers**.
  b. Na lista de IdP, clique em **Modify** na linha que contém o IdP.
  c. Na área **Identity Conversion Rules**, clique em **Create Rule**. Em seguida, configure as regras na caixa de diálogo **Create Rule**.

Figura 9-11 Clicar em Create Rule

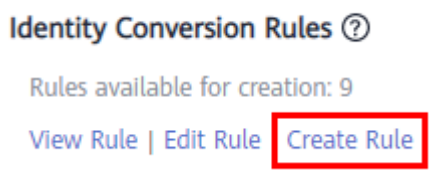


Figura 9-12 Criar regras

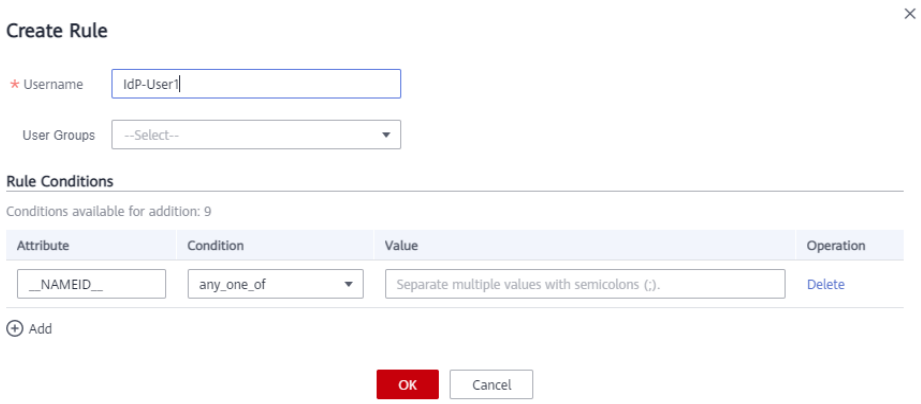


Tabela 9-5 Descrição do parâmetro

Parâmetro	Descrição	Observações
Username	Nome de usuário de usuários federados na Huawei Cloud.	Para distinguir os usuários federados dos usuários da Huawei Cloud, é recomendável definir o nome de usuário como **FederationUser-***IdP_XXX*. *IdP* indica um nome de IdP, por exemplo, AD FS ou Shibboleth. *XXX* indica um nome personalizado. **AVISO** ● O nome de usuário de cada usuário federado deve ser exclusivo no mesmo IdP. Os usuários federados com os mesmos nomes de usuário no mesmo IdP serão mapeados para o mesmo usuário do IAM na Huawei Cloud. ● O nome de usuário só pode conter letras, dígitos, espaços, hifens (-), sublinhados (_) e pontos (.). Ele não pode começar com um dígito e não pode conter os seguintes caracteres especiais: ", \", \\, \n, \r
User Groups	Grupos de usuários aos quais os usuários federados pertencem na Huawei Cloud.	Os usuários federados herdarão permissões dos grupos aos quais pertencem. Você pode selecionar um grupo de usuários que já foi criado.

Parâmetro	Descrição	Observações
Rule Conditions	Condições que um usuário federado deve atender para obter permissões dos grupos de usuários selecionados.	Os usuários federados que não atendem a essas condições não podem acessar a Huawei Cloud. Você pode criar no máximo 10 condições para uma regra de conversão de identidade. Os parâmetros **Attribute** e **Value** são usados para que o IdP empresarial transfira informações do usuário para a Huawei Cloud por meio de asserções SAML. O parâmetro **Condition** pode ser definido como **empty**, **any_one_of** ou **not_any_of**. Para obter detalhes sobre esses parâmetros, consulte **Sintaxe das regras de conversão de identidade**. **NOTA** ● Uma regra de conversão de identidade pode ter várias condições. Ela só entra em vigor se todas as condições forem atendidas. ● Um IdP pode ter várias regras de conversão de identidade. Se um usuário federado não atender a nenhuma das condições, o usuário será negado a acessar a Huawei Cloud.

Por exemplo, defina uma regra de conversão de identidade para administradores no sistema de gerenciamento empresarial.

- Nome de usuário: **FederationUser-IdP_admin**
- Grupo de usuários: **admin**
- Condição da regra: **_NAMEID_** (atributo), **any_one_of** (condição) e **000000001** (valor).

  Somente o usuário com ID 000000001 é mapeado para o usuário do IAM **FederationUser-IdP_admin** e herda permissões do grupo de usuários **admin**.

d. Na caixa de diálogo **Create Rule**, clique em **OK**.

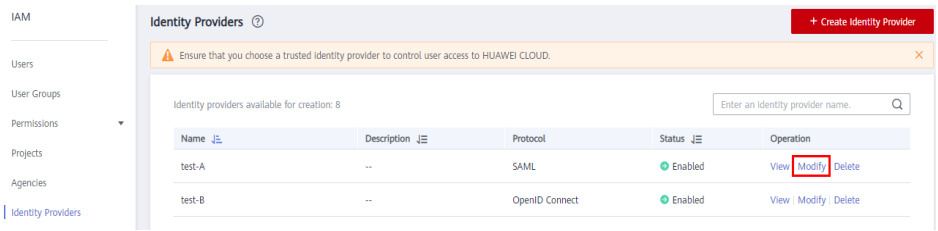
e. Na página **Modify Identity Provider**, clique em **OK**.

- **Editar regras**

a. Faça logon no **console do IAM** como administrador. No painel de navegação, escolha **Identity Providers**.

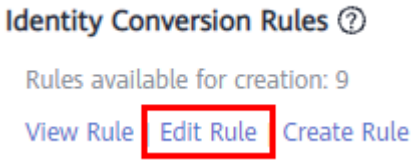
b. Na lista de IdP, clique em **Modify** na linha que contém o IdP.

Figura 9-13 Modificar um IdP



c. Na área **Identity Conversion Rules**, clique em **Edit Rule**.

Figura 9-14 Editar regras de conversão de identidade



d. Edite as regras de conversão de identidade no formato JSON. Para mais detalhes, consulte **9.6 Sintaxe das regras de conversão de identidade**.

e. Clique em **Validate** para verificar a sintaxe das regras.

f. Se a regra estiver correta, clique em **OK** na caixa de diálogo **Edit Rule** e clique em **OK** na página **Modify Identity Provider**.

Se for exibida uma mensagem indicando que o arquivo JSON está incompleto, modifique as instruções ou clique em **Cancel** para cancelar as modificações.

Operações relacionadas

Exibir regras de conversão de identidade: clique em **View Rule** na página **Modify Identity Provider**. As regras de conversão de identidade são exibidas no formato JSON. Para obter detalhes sobre o formato JSON, consulte **Sintaxe das regras de conversão de identidade**.

9.3.5 Etapa 4: verificar o logon federado

Verificar o logon federado

Os usuários federados podem iniciar um logon a partir do IdP ou SP.

- Iniciar um logon a partir de um IdP, por exemplo, Serviços de Federação do Active Directory (AD FS) de Microsoft ou Shibboleth.
- Iniciar um logon a partir do SP (HUAWEI CLOUD). Você pode obter o link de logon na página de detalhes do IdP no console do IAM.

O método de logon iniciado pelo IdP depende do IdP. Para obter detalhes, consulte a documentação de ajuda do IdP. Esta seção descreve como iniciar um logon a partir do SP.

Passo 1 Efetue logon como um usuário federado.

Na página **Identity Providers** do console do IAM, clique em **View** na linha que contém o IdP. Clique em para copiar o link de logon exibido na área **Basic Information**, abra o link usando um navegador e digite o nome de usuário e a senha usados no sistema de gerenciamento empresarial.

Passo 2 Verifique se o usuário federado tem as permissões atribuídas ao seu grupo de usuários.

----Fim

Redirecionamento para uma região ou serviço especificado

Você pode especificar a página de destino para a qual o usuário federado será redirecionado após o logon, por exemplo, a página inicial do Cloud Eye na região CN-Hong Kong.

- Configurar o link de logon no SP

  Combine o link de logon obtido no console com o URL especificado usando o formato **Login link&service=Specified URL**. Por exemplo, se o link de logon obtido for **https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml** e o URL especificado for **https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1**, o link de logon configurado no SP será **https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml&service=https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1**
- Configurar o link de logon no IdP

  Configure **IAM_SAML_Attributes_redirect_url** (o URL para o qual será redirecionado) na asserção SAML do IdP empresarial.

9.3.6 (Opcional) Etapa 5: configurar uma entrada de logon federado no IdP empresarial

Configure uma entrada de logon federada no IdP empresarial para que os usuários empresariais possam usar o link de logon para acessar a Huawei Cloud.

NOTA

Se nenhum link de logon tiver sido configurado em seu sistema de gerenciamento empresarial, os usuários federados em sua empresa poderão fazer logon na Huawei Cloud por meio da página de logon da Huawei Cloud. Para mais detalhes, consulte **Fazer logon como um usuário federado**.

Pré-requisitos

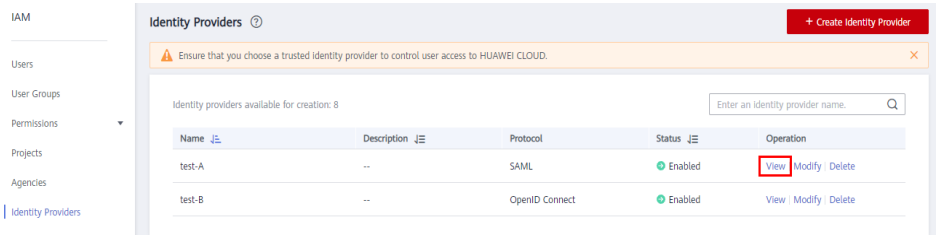
- Uma entidade de IdP foi criada na Huawei Cloud. Para obter detalhes sobre como criar uma entidade de IdP, consulte **9.3.2 Etapa 1: criar uma entidade IdP**.
- A entrada de logon para fazer logon na Huawei Cloud foi configurada no sistema de gerenciamento empresarial.

Procedimento

Passo 1 Faça logon no **console do IAM**. No painel de navegação, escolha **Identity Providers**.

Passo 2 Clique em **View** na linha que contém o IdP.

Figura 9-15 Visualização de detalhes do IdP



Passo 3 Copie o link de logon clicando em na linha **Login Link**.

Figura 9-16 Cópia do link de logon

Passo 4 Adicione a seguinte instrução ao arquivo de página do sistema de gerenciamento empresarial:

```
<a href="<Login link>"> Huawei Cloud login entry </a>
```

Passo 5 Faça logon no sistema de gerenciamento empresarial usando sua conta empresarial e clique no link de logon configurado para acessar a Huawei Cloud.

----Fim

9.4 SSO de usuário do IAM via SAML

9.4.1 Visão geral do SSO de usuário do IAM via SAML

Huawei Cloud suporta federação de identidade com Security Assertion Markup Language (SAML), que é um padrão aberto usado por muitos provedores de identidade (IdPs). Durante a federação de identidade, a Huawei Cloud funciona como um provedor de serviços (SP) e as empresas funcionam como IdPs. A federação baseada em SAML permite o logon único (SSO), para que os funcionários da sua empresa possam fazer logon na Huawei Cloud como usuários do IAM.

Esta seção descreve como configurar a federação de identidades e como funciona a federação de identidades.

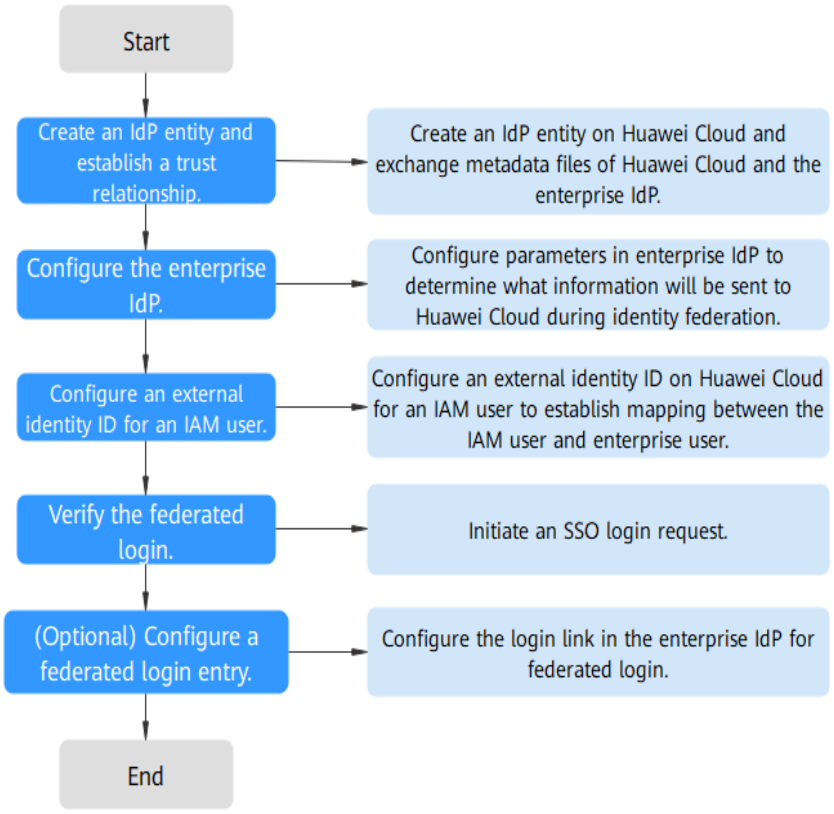
⚠ CUIDADO

Certifique-se de que o seu IdP empresarial ofereça suporte à SAML 2.0.

Configurar a federação de identidade

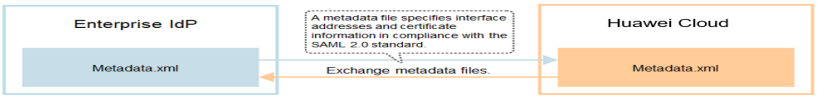
A seguir, descrevemos como configurar o seu IdP empresarial e a Huawei Cloud para que confiem um no outro.

Figura 9-17 Configuração do SSO do usuário do IAM via SAML



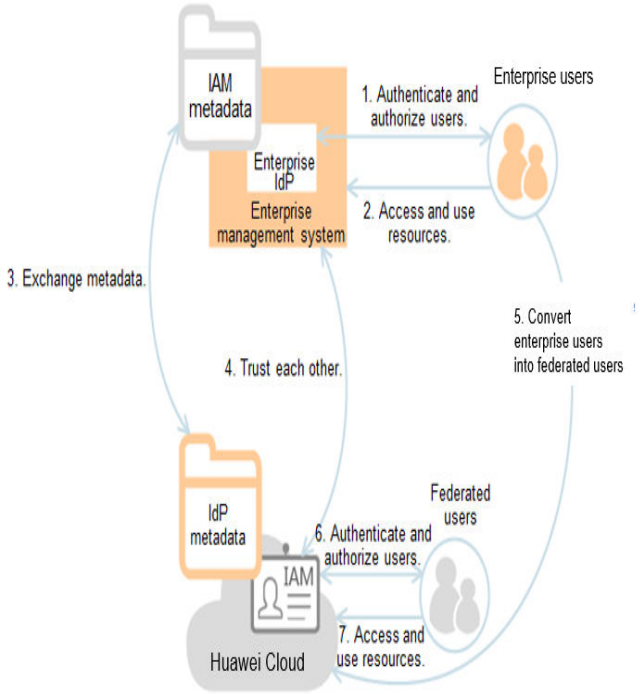
1. **Criar uma entidade IdP e estabelecer uma relação de confiança**: crie uma entidade IdP para sua empresa na Huawei Cloud. Em seguida, faça o upload do arquivo de metadados da Huawei Cloud para o IdP empresarial e faça o upload do arquivo de metadados do IdP empresarial para a Huawei Cloud.

   Figura 9-18 Troca de arquivos de metadados

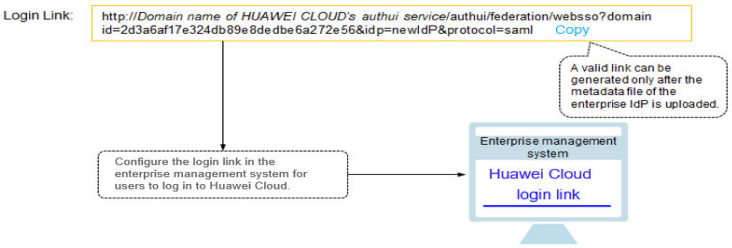
2. **Configurar o IdP empresarial**: configure parâmetros de IdP empresarial para determinar quais informações podem ser enviadas para a Huawei Cloud.
3. **Configurar um ID de identidade externa**: estabeleça um mapeamento entre um usuário do IAM e um usuário empresarial. Quando seu IdP empresarial estabelece acesso SSO à Huawei Cloud, o usuário empresarial pode fazer logon na Huawei Cloud como o usuário do IAM com o ID de identidade externa especificado. Por exemplo, se um usuário empresarial **IdP_Test_User** for mapeado para o usuário do IAM **Alice**, o usuário empresarial **IdP_Test_User** efetuará logon na Huawei Cloud como o usuário do IAM **Alice**.

Figura 9-19 Mapeamento de identidades externas para usuários do IAM



4. **Verificar o logon federado**: verifique se o usuário empresarial pode fazer logon na Huawei Cloud por meio de SSO.
5. **(Opcional) Configurar uma entrada de logon federada**: configure o link de logon (consulte **Figura 9-20**) no IdP empresarial para permitir que os usuários empresariais sejam redirecionados para a Huawei Cloud a partir do seu sistema de gerenciamento empresarial.

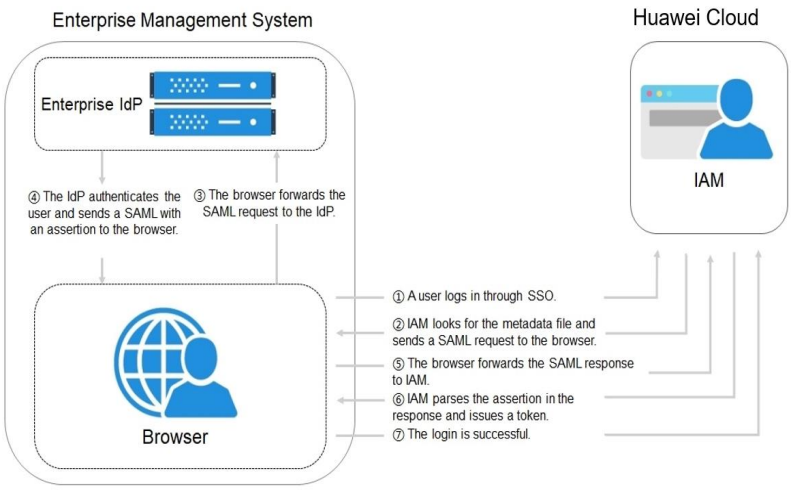
Figura 9-20 Modelo de logon do SSO



Como funciona a federação de identidade

Figura 9-21 mostra o processo de federação de identidade entre um sistema de gerenciamento empresarial e a Huawei Cloud.

Figura 9-21 Como funciona a federação de identidade



NOTA

Para visualizar solicitações e asserções interativas com uma experiência melhor, é recomendável usar o Google Chrome e instalar o SAML Message Decoder.

Como mostrado em **Figura 9-21**, o processo de federação de identidade é o seguinte:

1. Um usuário abre o link de logon gerado após a criação do IdP no navegador. O navegador envia uma solicitação de SSO para a Huawei Cloud.
2. A Huawei Cloud autentica o usuário no arquivo de metadados do IdP empresarial e constrói uma solicitação SAML para o navegador.
3. O navegador encaminha a solicitação SAML para o IdP empresarial.
4. O usuário insere seu nome de usuário e senha na página de logon. Depois que o IdP empresarial autentica a identidade do usuário, ele constrói uma asserção SAML contendo os detalhes do usuário e envia a asserção ao navegador como uma resposta SAML.
5. O navegador responde e encaminha a resposta SAML para a Huawei Cloud.
6. A Huawei Cloud analisa a asserção na resposta SAML, identifica o mapeamento do grupo de usuários do IAM para o usuário com base nas regras de conversão de identidade e emite um token para o usuário.
7. O logon do SSO foi bem-sucedido.

NOTA

A afirmação deve conter uma assinatura; caso contrário, o logon falhará.

9.4.2 Etapa 1: criar uma entidade IdP

Para estabelecer uma relação de confiança entre um IdP empresarial e a Huawei Cloud, carregue o arquivo de metadados da Huawei Cloud para o IdP empresarial e, em seguida, crie uma entidade IdP e carregue o arquivo de metadados do IdP empresarial no console do IAM.

Estabelecer uma relação de confiança entre o IdP empresarial e a Huawei Cloud

Configure o arquivo de metadados da Huawei Cloud no IdP empresarial para estabelecer uma confiança.

Passo 1 Baixe o arquivo de metadados da Huawei Cloud.

Visite **https://auth-intl.huaweicloud.com/authui/saml/metadata.xml** (O Google Chrome é recomendado). Faça o download do arquivo de metadados da Huawei Cloud e defina o nome do arquivo, por exemplo, **SP-metadata.xml**.

Passo 2 Faça upload do arquivo de metadados para o servidor de IdP empresarial. Para obter detalhes, consulte a documentação de ajuda do IdP empresarial.

Passo 3 Obtenha o arquivo de metadados do IdP empresarial. Para obter detalhes, consulte a documentação de ajuda do IdP empresarial.

----Fim

Criar uma entidade IdP na Huawei Cloud

Para criar uma entidade IdP no console do IAM, faça o seguinte:

Passo 1 Faça logon no **console do IAM**, escolha **Identity Providers** no painel de navegação e clique em **Create Identity Provider** no canto superior direito.

Passo 2 Especifique o nome, o protocolo, o tipo de SSO, o status e a descrição da entidade IdP.

Tabela 9-6 Parâmetros básicos de um IdP

Parâmetro	Descrição
Name	Nome do IdP, que deve ser exclusivo globalmente. Você é aconselhado a usar o nome de domínio.
Protocol	Protocolo de IdP. A Huawei Cloud oferece suporte aos protocolos SAML e OpenID Connect. Para obter detalhes sobre a federação de identidade baseada em OpenID Connect, consulte **9.5 SSO de usuário virtual via OpenID Connect**.
SSO Type	Tipo de IdP. Uma conta pode ter apenas um tipo de IdP. A seguir descreve-se o tipo de usuário do IAM. SSO de usuário do IAM: depois que um usuário federado faz logon na Huawei Cloud, o sistema mapeia automaticamente o **ID de identidade externa** para um usuário do IAM para que o usuário federado tenha as permissões do usuário do IAM mapeado. Uma conta pode ter apenas um IdP do tipo de usuário do IAM. Se você selecionar o SSO de usuário do IAM, verifique se criou um usuário do IAM e defina a ID de identidade externa. Para mais detalhes, consulte **3.1 Criação de um usuário do IAM**.
Status	Status do IdP. O valor padrão é **Enabled**.

Passo 3 Clique em **OK**.

----Fim

Configurar o arquivo de metadados do IdP empresarial na Huawei Cloud

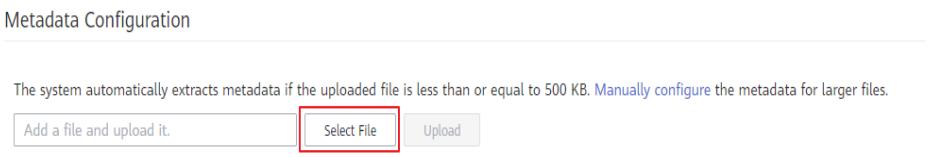
Você pode fazer upload do arquivo de metadados ou editar manualmente os metadados no console do IAM. Para um arquivo de metadados maior que 500 KB, configure manualmente

os metadados. Se os metadados tiverem sido alterados, carregue o arquivo de metadados mais recente ou edite os metadados existentes para garantir que os usuários federados possam fazer logon na Huawei Cloud com sucesso.

> **NOTA**
>
> Para obter detalhes sobre como obter o arquivo de metadados de um IdP empresarial, consulte a documentação de ajuda do IdP empresarial.

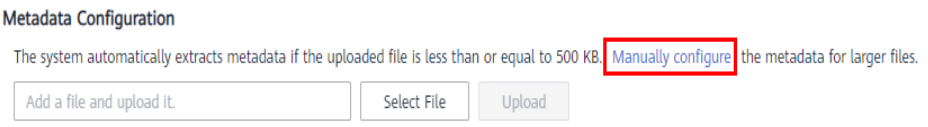
- **Carregar um arquivo de metadados.**
  a. Clique em **Modify** na linha que contém o IdP.
  b. Clique em **Select File** e selecione o arquivo de metadados do IdP empresarial.

  Figura 9-22 Carregar um arquivo de metadados

  c. Clique em **Upload**. Os metadados extraídos do arquivo carregado são exibidos. Clique em **OK**.
     - Se o arquivo de metadados carregado contiver vários IdPs, selecione o IdP que deseja usar na lista suspensa **Entity ID**.
     - Se uma mensagem for exibida indicando que nenhum ID de entidade foi especificado ou que o certificado de assinatura expirou, verifique o arquivo de metadados e carregue-o novamente ou configure os metadados manualmente.
  d. Clique em **OK** para salvar as configurações.
- **Configurar metadados manualmente.**
  a. Clique em **Manually configure**.

  Figura 9-23 Configuração manual de metadados

  b. Na caixa de diálogo **Configure Metadata**, defina os parâmetros de metadados, como **Entity ID**, **Signing Certificate** e **SingleSignOnService**.

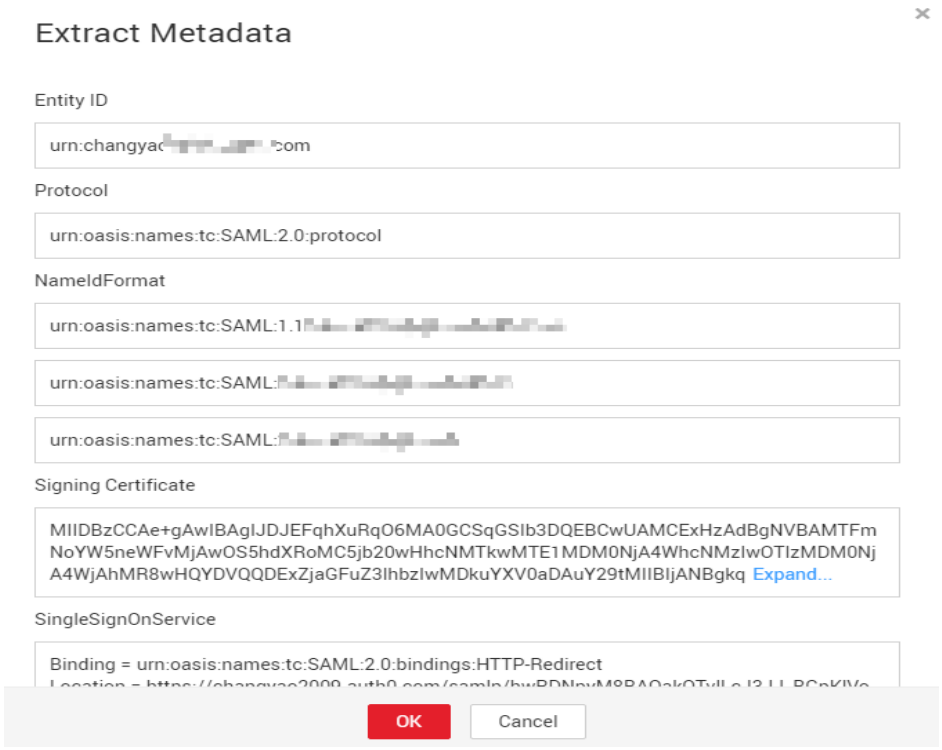
Parâmetro	Obrigatório	Descrição
Entity ID	Sim	O identificador exclusivo de um IdP. Digite o valor de **entityID** exibido no arquivo de metadados do IdP empresarial. Se o arquivo de metadados contiver vários IdPs, escolha aquele que você deseja usar.

Parâmetro	Obrigatório	Descrição
Protocol	Sim	Protocolo usado para federação de identidade entre um IdP empresarial e SP. O protocolo é selecionado por padrão.
NameIdFormat	Não	Digite o valor de **NameIdFormat** exibido no arquivo de metadados do IdP. Especifica o formato de identificador de nome de usuário suportado pelo IdP, que é usado para comunicação entre o IdP e o usuário federado. Se você configurar vários valores, a Huawei Cloud usa o primeiro valor por padrão.
Signing Certificate	Sim	Insira o valor de **<X509Certificate>** exibido no arquivo de metadados do IdP. Um certificado de assinatura é um certificado de chave pública usado para verificação de assinatura. Para fins de segurança, insira uma chave pública contendo pelo menos 2.048 bits. O certificado de assinatura é usado durante a federação de identidade para garantir que as afirmações sejam confiáveis e completas. Se você configurar vários valores, a Huawei Cloud usa o primeiro valor por padrão.
SingleSignOnService	Sim	Digite o valor de **SingleSignOnService** exibido no arquivo de metadados do IdP. Este parâmetro define como as solicitações SAML são enviadas durante o SSO. Ele deve suportar HTTP Redirect ou HTTP POST. Se você configurar vários valores, a Huawei Cloud usa o primeiro valor por padrão.
SingleLogoutService	Não	Digite o valor de **SingleLogoutService** exibido no arquivo de metadados do IdP. Este parâmetro indica o endereço para o qual os usuários federados serão redirecionados após encerrarem suas sessões. Ele deve suportar HTTP Redirect ou HTTP POST. Se você configurar vários valores, a Huawei Cloud usa o primeiro valor por padrão.

O exemplo a seguir mostra o arquivo de metadados de um IdP empresarial e os metadados configurados manualmente.

Figura 9-24 Arquivo de metadados de um IdP empresarial

Figura 9-25 Configuração manual de metadados



c. Clique em **OK** para salvar as configurações.

9.4.3 Etapa 2: configurar o IdP empresarial

Você pode configurar parâmetros no IdP empresarial para determinar quais informações serão enviadas para a Huawei Cloud. A Huawei Cloud autentica a identidade federada e atribui permissões com base nas informações recebidas.

NOTA

Se o tipo de SSO for usuário do IAM, o IdP empresarial deverá ter a asserção **IAM_SAML_Attributes_xUserId** configurada.

Parâmetros comuns em um IdP empresarial

Tabela 9-7 Parâmetros comuns em um IdP empresarial

Parâmetro	Descrição	Cenário
IAM_SAML_Attributes_xUserId	ID de um usuário de IdP empresarial (usuário federado)	Esse parâmetro é obrigatório quando o tipo de SSO é usuário do IAM. Cada usuário federado é mapeado para um usuário do IAM. O **IAM_SAML_Attributes_xUserId** do usuário federado é igual ao ID de identidade externa do usuário do IAM correspondente.
IAM_SAML_Attributes_redirect_url	URL de destino para o qual o usuário federado será redirecionado	Durante o logon do SSO, o usuário federado será redirecionado para uma página na Huawei Cloud , por exemplo, a página inicial do Cloud Eye na região CN-Hong Kong.
IAM_SAML_Attributes_domain_id	ID da conta da Huawei Cloud a ser federado com o IdP empresarial	Esse parâmetro é obrigatório na federação iniciada por IdP empresarial.
IAM_SAML_Attributes_idp_id	Nome da entidade IdP criada na Huawei Cloud	Esse parâmetro é obrigatório na federação iniciada por IdP empresarial.

9.4.4 Etapa 3: configurar um ID de identidade externa

Para o tipo de SSO de usuário do IAM, você deve configurar um ID de identidade externa para o usuário do IAM para o qual o usuário federado mapeia na Huawei Cloud. O ID de identidade externa deve ser igual ao valor **IAM_SAML_Attributes_xUserId** do usuário de IdP empresarial (usuário federado). Você pode criar um usuário do IAM e configurar um ID de identidade externa para ele ou alterar o ID de identidade externa de um usuário do IAM existente.

- **Criar um usuário do IAM e configurar um ID de identidade externa**
- **Alterar o ID de identidade externa de um usuário existente do IAM**

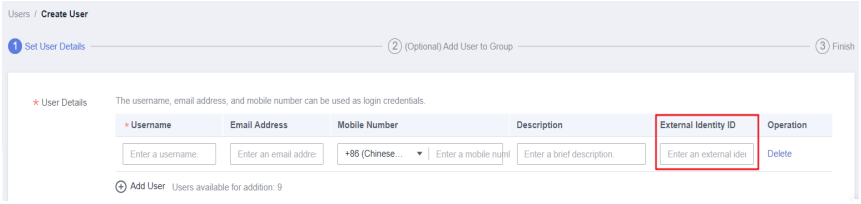
Criar um usuário do IAM e configurar um ID de identidade externa

Passo 1 Faça logon no console do IAM como um administrador.

Passo 2 No console do IAM, escolha **Users** no painel de navegação e clique em **Create User** no canto superior direito.

Passo 3 Na área **User Details**, configure um ID de identidade externa. Para obter detalhes sobre outras configurações, consulte **3.1 Criação de um usuário do IAM**.

Figura 9-26 Configurar um ID de identidade externa

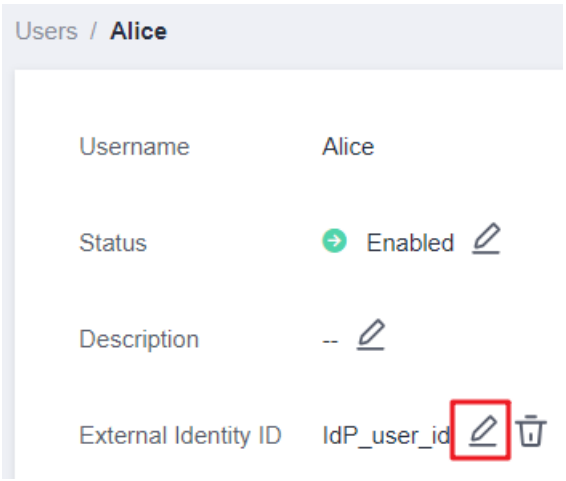


----Fim

Alterar o ID de identidade externa de um usuário existente do IAM

Na lista de usuários do IAM, clique em um nome de usuário ou escolha **More** > **Security Settings** na linha que contém o usuário e altere o ID de identidade externa.

Figura 9-27 Alteração do ID de identidade externa de um usuário do IAM existente



9.4.5 Etapa 4: verificar o logon federado

Verificar o logon federado

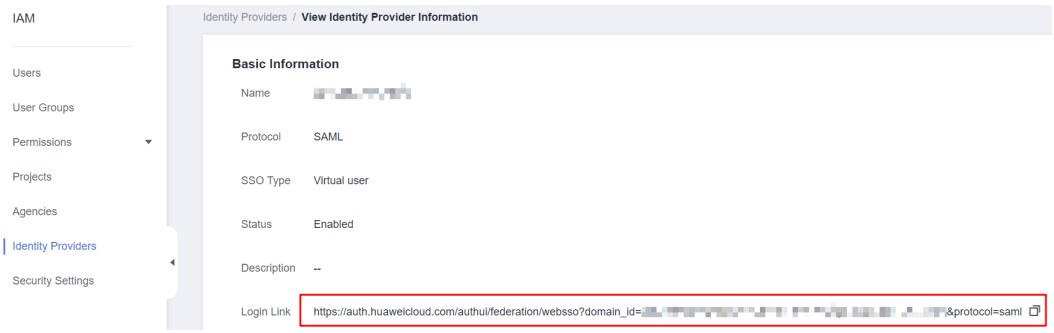
Os usuários federados podem iniciar um logon a partir do IdP ou SP.

- Iniciar um logon a partir de um IdP, por exemplo, Serviços de Federação do Active Directory (AD FS) de Microsoft ou Shibboleth.
- Iniciar um logon a partir do SP (HUAWEI CLOUD). Você pode obter o link de logon na página de detalhes do IdP no console do IAM.

O método de logon iniciado pelo IdP depende do IdP. Para obter detalhes, consulte a documentação de ajuda do IdP. Esta seção descreve como iniciar um logon a partir do SP.

Passo 1 Efetue logon como um usuário federado.

Na página **Identity Providers** do console do IAM, clique em **View** na linha que contém o IdP. Clique em para copiar o link de logon exibido na área **Basic Information**, abra o link usando um navegador e digite o nome de usuário e a senha usados no sistema de gerenciamento empresarial.



Passo 2 Verifique se o usuário federado está fazendo logon como um usuário do IAM.

----Fim

Redirecionamento para uma região ou serviço especificado

Você pode especificar a página de destino para a qual o usuário federado será redirecionado após o logon, por exemplo, a página inicial do Cloud Eye na região CN-Hong Kong.

- Configurar o link de logon no SP

  Combine o link de logon obtido no console com o URL especificado usando o formato **Login link&service=Specified URL**. Por exemplo, se o link de logon obtido for **https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml** e o URL especificado for **https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1**, o link de logon configurado no SP será **https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml&service=https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1**

- Configurar o link de logon no IdP

  Configure **IAM_SAML_Attributes_redirect_url** (o URL para o qual será redirecionado) na asserção SAML do IdP empresarial.

9.4.6 (Opcional) Etapa 5: configurar uma entrada de logon federado no IdP empresarial

Configure uma entrada de logon federada no IdP empresarial para que os usuários empresariais possam usar o link de logon para acessar a Huawei Cloud.

NOTA

Se você não quiser configurar a entrada de logon no seu sistema de gerenciamento empresarial, pule esta seção. A Huawei Cloud fornece uma entrada de logon para usuários federados. Para obter detalhes sobre o logon, consulte **Fazer logon como um usuário federado**.

Pré-requisitos

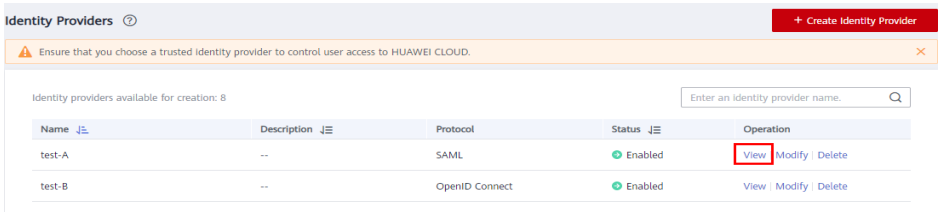
- Uma entidade IdP foi criada na Huawei Cloud, e o link de logon para o IdP está disponível. Para mais detalhes, consulte **9.4.2 Etapa 1: criar uma entidade IdP**.
- A entrada de logon para fazer logon na Huawei Cloud foi configurada no sistema de gerenciamento empresarial.

Procedimento

Passo 1 Faça logon no **console do IAM**. No painel de navegação, escolha **Identity Providers**.

Passo 2 Clique em **View** na linha que contém o IdP.

Figura 9-28 Visualização de detalhes do IdP



Passo 3 Copie o link de logon clicando em na linha **Login Link**.

Figura 9-29 Cópia do link de logon

Passo 4 Adicione a seguinte instrução ao arquivo de página do sistema de gerenciamento empresarial:

```
<a href="<Login link>"> Huawei Cloud login entry </a>
```

Passo 5 Faça logon no sistema de gerenciamento empresarial usando sua conta empresarial e clique no link de logon configurado para acessar a Huawei Cloud.

----Fim

9.5 SSO de usuário virtual via OpenID Connect

9.5.1 Visão geral do SSO de usuário virtual via OpenID Connect

Esta seção descreve como configurar a federação de identidades e como funciona a federação de identidades.

Configurar a federação de identidade

A seguir, descrevemos como configurar o seu IdP empresarial e a Huawei Cloud para que confiem um no outro.

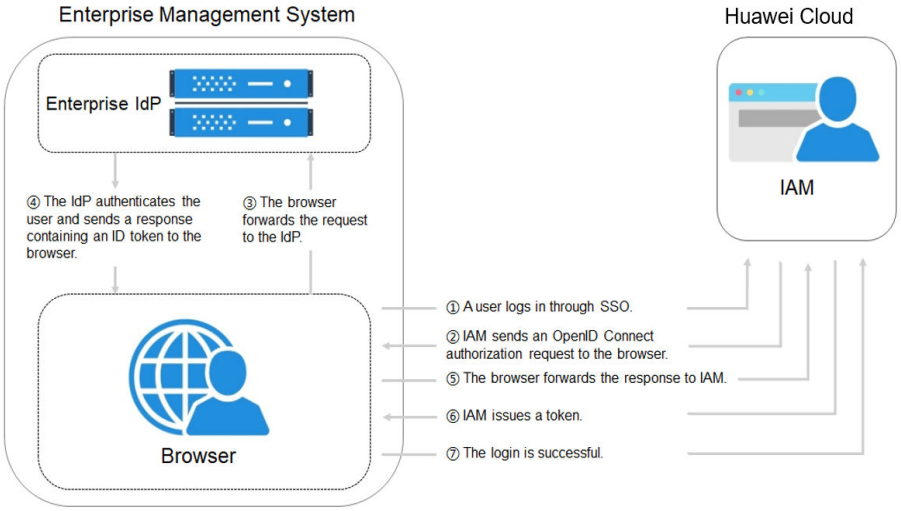
1. **Criar uma entidade IdP e estabelecer uma relação de confiança**: crie credenciais OAuth 2.0 no IdP empresarial. Na Huawei Cloud, crie uma entidade IdP e estabeleça uma relação de confiança entre os dois sistemas.

2. **Configurar regras de conversão de identidade**: configure regras de conversão de identidade na Huawei Cloud para mapear os usuários, grupos de usuários e permissões no IdP empresarial para a Huawei Cloud.
3. **Configurar uma entrada de logon federada**: configure o link de logon no IdP empresarial para permitir que os usuários empresariais sejam redirecionados para a Huawei Cloud a partir do seu sistema de gerenciamento empresarial.

Como funciona a federação de identidade

Figura 9-30 mostra o processo de federação de identidade entre um sistema de gerenciamento empresarial e a Huawei Cloud.

Figura 9-30 Como funciona a federação de identidade



O processo de federação de identidade é o seguinte:

1. Um usuário abre o link de logon obtido no console do IAM no navegador. O navegador envia uma solicitação de SSO para a Huawei Cloud.
2. A Huawei Cloud autentica o usuário em relação à configuração do IdP empresarial e constrói uma solicitação de OpenID Connect para o navegador.
3. O navegador encaminha a solicitação de OpenID Connect para o IdP empresarial.
4. O usuário insere seu nome de usuário e senha na página de logon exibida no IdP empresarial. Depois que o IdP empresarial autentica a identidade do usuário, ele constrói um token de ID contendo as informações do usuário e envia o token de ID para o navegador como uma resposta de autorização de OpenID Connect.
5. O navegador responde e encaminha a resposta de OpenID Connect para a Huawei Cloud.
6. A Huawei Cloud analisa o token de ID na resposta de OpenID Connect, identifica o mapeamento do grupo de usuários do IAM para o usuário com base nas regras de conversão de identidade e emite um token para o usuário.
7. O logon do SSO foi bem-sucedido.

9.5.2 Etapa 1: criar uma entidade IdP

Para estabelecer uma relação de confiança entre um IdP empresarial e a Huawei Cloud, defina os URLs de redirecionamento do usuário e crie credenciais OAuth 2.0 no IdP empresarial. No console do IAM, crie uma entidade IdP e configure as informações de autorização.

Pré-requisitos

- O administrador empresarial criou uma conta na Huawei Cloud, criou grupos de usuários e atribuiu-lhes permissões no IAM. Para mais detalhes, consulte **4.1 Criação de um grupo de usuários e atribuição de permissões**. Os grupos de usuários criados no IAM serão mapeados para usuários federados para que os usuários federados possam obter as permissões dos grupos de usuários para usar os recursos da Huawei Cloud.
- O administrador empresarial leu a documentação de ajuda do IdP empresarial ou entendeu como usar o IdP empresarial. As configurações de diferentes IdPs empresariais são muito diferentes, portanto não são descritas neste documento. Para obter detalhes sobre como obter credenciais OAuth 2.0 de um IdP empresarial, consulte a documentação de ajuda do IdP.

Criar credenciais OAuth 2.0 no IdP empresarial

Passo 1 Defina URIs de redirecionamento **https://auth.huaweicloud.com/authui/oidc/redirect** e **https://auth.huaweicloud.com/authui/oidc/post** no IdP empresarial para que os usuários possam ser redirecionados para o IdP de OpenID Connect na Huawei Cloud.

Passo 2 Obtenha as credenciais OAuth 2.0 do IdP empresarial.

----Fim

Criar uma entidade IdP na Huawei Cloud

Crie uma entidade IdP e configure as informações de autorização no IAM para estabelecer uma relação de confiança entre o IdP empresarial e o IAM.

Passo 1 Faça logon no **console do IAM**, escolha **Identity Providers** no painel de navegação e clique em **Create Identity Provider** no canto superior direito.

Passo 2 Digite um nome de IdP, selecione **OpenID Connect** e **Enabled** e clique em **OK**.

NOTA

O nome do IdP deve ser exclusivo na sua conta. Você é aconselhado a usar o nome de domínio.

----Fim

Configurar informações de autorização na Huawei Cloud

Passo 1 Clique em **Modify** na coluna **Operation** da linha que contém o IdP que você deseja modificar.

Passo 2 Selecione um tipo de acesso.

Tabela 9-8 Descrição do tipo de acesso

Tipo de acesso	Descrição
Programmatic access and management console access	● Programmatic access: os usuários federados podem usar ferramentas de desenvolvimento (incluindo APIs, CLI e SDKs) que suportam autenticação de chave para acessar a Huawei Cloud. ● Management console access: os usuários federados podem fazer logon na Huawei Cloud usando seus próprios nomes de usuário e senhas. Selecione esse tipo de acesso se quiser que os usuários acessem a Huawei Cloud por meio de SSO.
Programmatic access	Os usuários federados só podem usar ferramentas de desenvolvimento (incluindo APIs, CLI e SDKs) que suportem autenticação de chave para acessar a Huawei Cloud.

Passo 3 Especifique as informações de configuração.

Tabela 9-9 Informações de configuração

Parâmetro	Descrição
Identity Provider URL	URL do IdP de OpenID Connect. Defina-o como o valor de **issuer** em **Openid-configuration**. **NOTA** **Openid-configuration** indica um URL definido em OpenID Connect, contendo configurações de um IdP empresarial. O formato do URL é **https://***{base URL}***/.well-known/openid-configuration**, em que *base URL* é definido pelo IdP empresarial. Por exemplo, o **Openid-configuration** do Google é **https://accounts.google.com/.well-known/openid-configuration**.
Client ID	ID de um cliente registrado com o IdP de OpenID Connect. O ID do cliente é **uma credencial OAuth 2.0 criada no IdP empresarial**.
Authorization Endpoint	Ponto de extremidade de autorização do IdP de OpenID Connect. Defina-o como o valor de **authorization_endpoint** em **Openid-configuration**. Esse parâmetro só será necessário se você definir **Access Type** como **Programmatic access and management console access**.
Scopes	Escopos das solicitações de autorização. **openid** é selecionado por padrão. Esse parâmetro só será necessário se você definir **Access Type** como **Programmatic access and management console access**. Valores enumerados: ● openid ● email ● profile

Parâmetro	Descrição
Response Type	Tipo de resposta de solicitações de autorização. O valor padrão é **id_token**. Esse parâmetro só será necessário se você definir **Access Type** como **Programmatic access and management console access**.
Response Mode	Modo de resposta das solicitações de autorização. As opções incluem **form_post** e **fragment**. **form_post** é recomendado. ● **form_post**: se este modo estiver selecionado, defina o URL de redirecionamento para **https://auth.huaweicloud.com/authui/oidc/post** no IdP empresarial. ● **fragment**: se este modo estiver selecionado, defina o URL de redirecionamento para **https:/auth.huaweicloud.com/authui/oidc/redirect** no IdP empresarial. Esse parâmetro só será necessário se você definir **Access Type** como **Programmatic access and management console access**.
Signing Key	Chave pública usada para assinar o token de ID do IdP de OpenID Connect. Para fins de segurança da conta, altere a chave de assinatura periodicamente.

Passo 4 Clique em **OK**.

----Fim

Verificar o logon federado

Passo 1 Clique no link de logon exibido na página de detalhes do IdP e verifique se a página de logon do servidor de IdP empresarial é exibida.

1. Na página **Identity Providers**, clique em **Modify** na coluna **Operation** do provedor de identidade.
2. Copie o link de logon exibido na página **Modify Identity Provider** e visite o link usando um navegador.
3. Se a página de logon do IdP empresarial não for exibida, verifique as configurações do IdP e do servidor do IdP empresarial.

Passo 2 Digite o nome de usuário e a senha de um usuário que foi criado no sistema de gerenciamento empresarial.

- Se o logon for bem-sucedido, adicione o link de logon ao sistema de gerenciamento empresarial.
- Se o logon falhar, verifique o nome de usuário e a senha.

NOTA

Os usuários federados só podem acessar a Huawei Cloud por padrão. Para atribuir permissões a usuários federados, configure regras de conversão de identidade para o IdP. Para mais detalhes, consulte **9.5.3 Etapa 2: configurar regras de conversão de identidade**.

----Fim

Operações relacionadas

- Visualizar informações de IdP: na lista de IdP, clique em **View** na linha que contém o IdP e exiba suas informações básicas, configuração de metadados e regras de conversão de identidade.

  NOTA

  Para modificar a configuração de um IdP, clique em **Modify** na parte inferior da página de detalhes.

- Modificar um IdP: na lista do IdP, clique em **Modify** na linha que contém o IdP e, em seguida, altere seu status ou modifique a descrição, os metadados ou as regras de conversão de identidade.
- Excluir um IdP: na lista do IdP, clique em **Delete** na linha que contém o IdP e clique em **Yes** na caixa de diálogo exibida.

Procedimento de acompanhamento

- Configure regras de conversão de identidade para mapear usuários de IdP empresarial para grupos de usuários do IAM e atribua permissões aos usuários. Para mais detalhes, consulte **9.5.3 Etapa 2: configurar regras de conversão de identidade**.
- Configure o sistema de gerenciamento empresarial para permitir que os usuários acessem a Huawei Cloud por meio do SSO. Para mais detalhes, consulte **9.5.4 (Opcional) Etapa 3: configurar o link de logon no sistema de gerenciamento empresarial**.

9.5.3 Etapa 2: configurar regras de conversão de identidade

Os usuários federados são nomeados **FederationUser** por padrão na Huawei Cloud. Esses usuários só podem fazer logon na Huawei Cloud e não têm outras permissões. Você pode configurar regras de conversão de identidade no console do IAM para obter o seguinte:

- Exiba usuários empresariais com nomes diferentes na Huawei Cloud.
- Atribua permissões aos usuários empresariais para usar os recursos da Huawei Cloud mapeando esses usuários para grupos de usuários do IAM. Certifique-se de ter criado os grupos de usuários necessários. Para mais detalhes, consulte **4.1 Criação de um grupo de usuários e atribuição de permissões**.

NOTA

- As modificações nas regras de conversão de identidade entrarão em vigor na próxima vez que os usuários federados fizerem logon.
- Para modificar as permissões de um usuário, modifique as permissões do grupo de usuários ao qual o usuário pertence. Em seguida, reinicie o IdP empresarial para que as modificações tenham efeito.

Pré-requisitos

Uma entidade IdP foi criada e o link de logon do IdP está acessível. (Para obter detalhes sobre como criar e verificar uma entidade IdP, consulte **9.5.2 Etapa 1: criar uma entidade IdP**.)

Procedimento

Se você configurar regras de conversão de identidade clicando em **Create Rule**, o IAM converterá os parâmetros de regra para o formato JSON. Como alternativa, você pode clicar em **Edit Rule** para configurar regras no formato JSON. Para mais detalhes, consulte **9.6 Sintaxe das regras de conversão de identidade**.

- **Criar regras**
  a. Faça logon no **console do IAM** como administrador. No painel de navegação, escolha **Identity Providers**.
  b. Na lista de IdP, clique em **Modify** na linha que contém o IdP.
  c. Na área **Identity Conversion Rules**, clique em **Create Rule**. Em seguida, configure as regras na caixa de diálogo **Create Rule**.

Figura 9-31 Criar regras

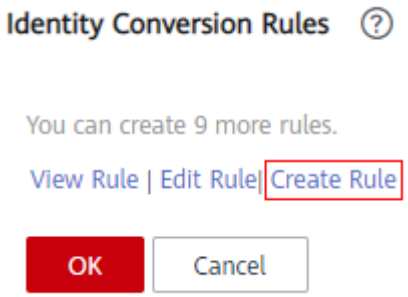


Figura 9-32 Definir parâmetros

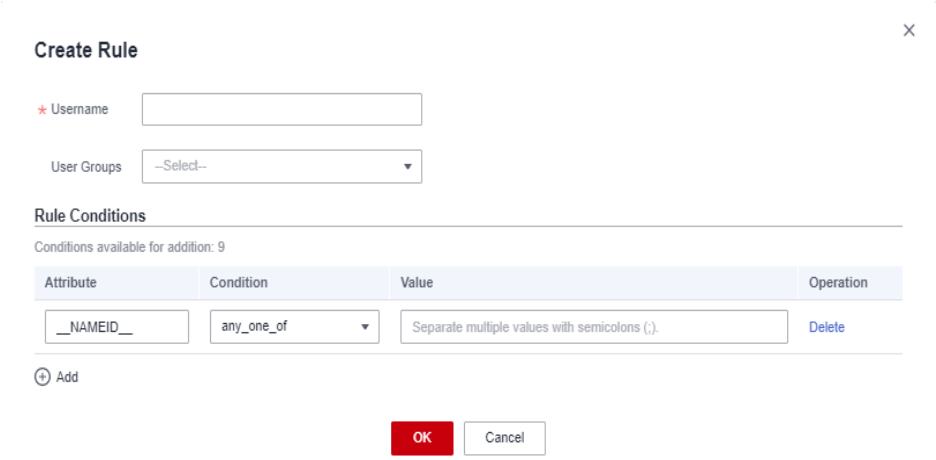


Tabela 9-10 Descrição do parâmetro

Parâmetro	Descrição	Observações
Username	Nome de usuário de usuários federados na Huawei Cloud.	Para distinguir os usuários federados dos usuários da Huawei Cloud, é recomendável definir o nome de usuário como **FederationUser-***IdP_XXX*. *IdP* indica um nome de IdP, por exemplo, AD FS ou Shibboleth. *XXX* indica um nome personalizado. **AVISO** ● O nome de usuário de cada usuário federado deve ser exclusivo no mesmo IdP. Os usuários federados com os mesmos nomes de usuário no mesmo IdP serão mapeados para o mesmo usuário do IAM na Huawei Cloud. ● O nome de usuário só pode conter letras, dígitos, espaços, hifens (-), sublinhados (_) e pontos (.). Ele não pode começar com um dígito e não pode conter os seguintes caracteres especiais: ", \", \\, \n, \r
User Groups	Grupos de usuários aos quais os usuários federados pertencem na Huawei Cloud.	Os usuários federados herdarão permissões de seus grupos de usuários. Você pode selecionar um grupo de usuários que já foi criado.
Rule Conditions	Condições que um usuário federado deve atender para obter permissões dos grupos de usuários selecionados.	Os usuários federados que não atendem a essas condições não podem acessar a Huawei Cloud. Você pode criar no máximo 10 condições para uma regra de conversão de identidade. **NOTA** ● Uma regra de conversão de identidade pode ter várias condições. Ela só entra em vigor se todas as condições forem atendidas. ● Um IdP pode ter várias regras de conversão de identidade. Se um usuário federado não atender a nenhuma das condições, o usuário será negado a acessar a Huawei Cloud.

Por exemplo, defina uma regra de conversão de identidade para administradores no sistema de gerenciamento empresarial.

- Nome de usuário: **FederationUser-IdP_admin**
- Grupo de usuários: **admin**
- Condição da regra: **_NAMEID_** (atributo), **any_one_of** (condição) e **000000001** (valor).

  Somente o usuário com ID 000000001 é mapeado para o usuário do IAM **FederationUser-IdP_admin** e herda permissões do grupo de usuários **admin**.

d. Na caixa de diálogo **Create Rule**, clique em **OK**.

e. Na página **Modify Identity Provider**, clique em **OK**.

- **Editar regras**

a. Faça logon no **console do IAM** como administrador. No painel de navegação, escolha **Identity Providers**.

b. Na lista de IdP, clique em **Modify** na linha que contém o IdP.

c. Na área **Identity Conversion Rules**, clique em **Edit Rule**.

d. Edite as regras de conversão de identidade no formato JSON. Para mais detalhes, consulte **9.6 Sintaxe das regras de conversão de identidade**.

e. Clique em **Validate** para verificar a sintaxe das regras.

f. Se a regra estiver correta, clique em **OK** na caixa de diálogo **Edit Rule** e clique em **OK** na página **Modify Identity Provider**.

Se for exibida uma mensagem indicando que o arquivo JSON está incompleto, modifique as instruções ou clique em **Cancel** para cancelar as modificações.

Verificar permissões de usuário federado

Depois de configurar as regras de conversão de identidade, verifique as permissões dos usuários federados.

Passo 1 Efetue logon como um usuário federado.

Na página **Identity Providers** do console do IAM, clique em **View** na linha que contém o IdP. Clique em para copiar o link de logon exibido na área **Basic Information**, abra o link usando um navegador e digite o nome de usuário e a senha usados no sistema de gerenciamento empresarial.

Passo 2 Verifique se o usuário federado tem as permissões atribuídas ao seu grupo de usuários.

Por exemplo, configure uma regra de conversão de identidade para mapear o usuário federado **ID1** para o grupo de usuários **admin** para que o **ID1** tenha permissões completas para todos os serviços de nuvem. No console de gerenciamento, selecione um serviço de nuvem e verifique se você pode acessar o serviço.

----Fim

Operações relacionadas

Exibir regras de conversão de identidade: clique em **View Rule** na página **Modify Identity Provider**. As regras de conversão de identidade são exibidas no formato JSON. Para obter detalhes sobre o formato JSON, consulte **Sintaxe das regras de conversão de identidade**.

9.5.4 (Opcional) Etapa 3: configurar o link de logon no sistema de gerenciamento empresarial

Configure uma entrada de logon federada no IdP empresarial para que os usuários empresariais possam usar o link de logon para acessar a Huawei Cloud.

NOTA

Se nenhum link de logon tiver sido configurado em seu sistema de gerenciamento empresarial, os usuários federados em sua empresa poderão fazer logon na Huawei Cloud por meio da página de logon da Huawei Cloud. Para mais detalhes, consulte **Fazer logon como um usuário federado**.

Pré-requisitos

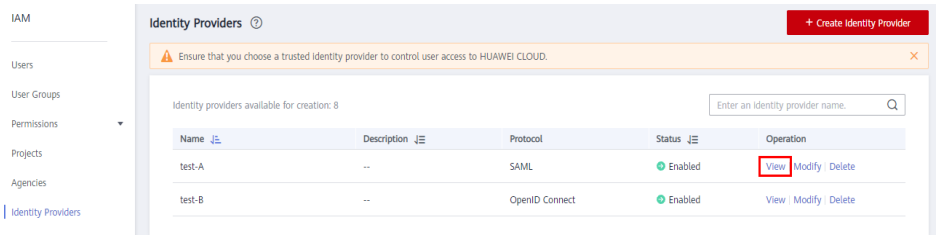
- Uma entidade de IdP foi criada na Huawei Cloud. Para obter detalhes sobre como criar uma entidade de IdP, consulte **9.3.2 Etapa 1: criar uma entidade IdP**.
- A entrada de logon para fazer logon na Huawei Cloud foi configurada no sistema de gerenciamento empresarial.

Procedimento

Passo 1 Faça logon no **console do IAM**. No painel de navegação, escolha **Identity Providers**.

Passo 2 Clique em **View** na linha que contém o IdP.

Figura 9-33 Visualização de detalhes do IdP



Passo 3 Copie o link de logon clicando em na linha **Login Link**.

Figura 9-34 Cópia do link de logon

Passo 4 Adicione a seguinte instrução ao arquivo de página do sistema de gerenciamento empresarial:

```
<a href="<Login link>"> Huawei Cloud login entry </a>
```

Passo 5 Faça logon no sistema de gerenciamento empresarial usando sua conta empresarial e clique no link de logon configurado para acessar a Huawei Cloud.

----Fim

9.6 Sintaxe das regras de conversão de identidade

Uma regra de conversão de identidade é um objeto JSON que pode ser modificado. O seguinte é um exemplo de objeto JSON:

```
[
        {
                "local": [
                        {
                                "<user> or <group> or <groups>"
```



```
                                }
                        ],
                        "remote": [
                                {
                                        "<condition>"
                                }
                        ]
                }
]
```

Descrição do parâmetro:

- **local**: informações de identidade de um usuário federado mapeado para o IAM. O valor desse campo pode conter espaços reservados, como **{0...n}**. Os atributos **{0}** e **{1}** representam o primeiro e o segundo atributos remotos das informações do usuário, respectivamente.
- **remote**: informações sobre um usuário federado do IdP. Esse campo é uma expressão que consiste em atributos e operadores de asserção. O valor deste campo é determinado pela asserção.
  - **condition**: condições para que a regra de conversão de identidade entre em vigor. Os três tipos de condições a seguir são suportados:
    - **empty**: a regra corresponde a todas as declarações que contêm o tipo de atributo. Essa condição não precisa ser especificada. O resultado da condição é o argumento que é passado como entrada.
    - **any_one_of**: a regra é correspondida somente se qualquer uma das cadeias de caracteres especificadas aparecer no tipo de atributo. O resultado da condição é Boolean, não o argumento que é passado como entrada.
    - **not_any_of**: a regra não é correspondida se qualquer uma das cadeias de caracteres especificadas aparecer no tipo de atributo. O resultado da condição é Boolean, não o argumento que é passado como entrada.

AVISO

As informações do usuário mapeadas para o IAM podem conter apenas letras, dígitos, espaços, hifens (-), sublinhados (_) e pontos (.) e não podem começar com um dígito.

Exemplos da condição empty

A condição **empty** retorna cadeias de caracteres para substituir os atributos locais **{0..n}**.

- No exemplo a seguir, o nome de usuário de um usuário federado será "o valor do primeiro atributo remoto+espaço+o valor do segundo atributo remoto" no IAM, ou seja, *FirstName LastName*. O grupo ao qual o usuário pertence é o valor do terceiro atributo remoto *Group*. Este atributo tem apenas um valor.

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0} {1}"
                    }
                },
                {
                    "group": {
                        "name": "{2}"
                    }
```



```
                }
            ],
            "remote": [
                {
                    "type": "FirstName"
                },
                {
                    "type": "LastName"
                },
                {
                    "type": "Group"
                }
            ]
        }
]
```

Se a seguinte asserção (simplificada para facilitar a compreensão) for recebida, o nome de usuário do usuário federado será **John Smith** e o usuário só pertencerá ao grupo **admin**.

```
{FirstName: John}
{LastName: Smith}
{Group: admin}
```

- Se um usuário federado pertencer a vários grupos de usuários no IAM, a regra de conversão de identidade poderá ser configurada da seguinte maneira:

  No exemplo a seguir, o nome de usuário de um usuário federado será "o valor do primeiro atributo remoto+espaço+o valor do segundo atributo remoto" no IAM, ou seja, *FirstName LastName*. Os grupos aos quais o usuário pertence são o valor do terceiro atributo remoto *Groups*.

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0} {1}"
                    }
                },
                {
                    "group":   {
                        "name": "{2}"
                    }
                }
            ],
            "remote": [
                {
                    "type": "FirstName"
                },
                {
                    "type": "LastName"
                },
                {
                    "type": "Groups"
                }
            ]
        }
]
```

  Se a asserção a seguir for recebida, o nome de usuário do usuário federado será **John Smith** e o usuário pertencerá aos grupos **admin** e **manager**.

```
{FirstName: John}
{LastName: Smith}
{Groups: [admin, manager]}
```


Exemplos das condições "any one of" e "not any of"

Ao contrário da condição **empty**, as condições **any one of** e **not any of** retornam valores Boolean. Esses valores não serão usados para substituir os atributos locais. No exemplo a seguir, apenas **{0}** será substituído pelo valor retornado da primeira condição **empty** no bloco **remote**. O valor do **group** é fixo como **admin**.

- O nome de usuário do usuário federado no IAM é o valor do primeiro atributo remoto, ou seja, *UserName*. O usuário federado pertence ao grupo **admin**. Essa regra entra em vigor somente para usuários que são membros do grupo **idp_admin** no IdP.

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
                {
                    "group": {
                        "name": "admin"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
                },
                {
                    "type": "Groups",
                    "any_one_of": [
                        "idp_admin"
                    ]
                }
            ]
        }
]
```

- Se um usuário federado pertencer a vários grupos de usuários no IAM, a regra de conversão de identidade poderá ser configurada da seguinte maneira:

  O nome de usuário do usuário federado no IAM é o valor do primeiro atributo remoto, ou seja, *UserName*. O usuário federado pertence aos grupos **admin** e **manager**. Essa regra entra em vigor somente para usuários que são membros do grupo **idp_admin** no IdP.

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
                {
                    "group": {
                           "name":"admin"
                    }
                },
                {
                    "group": {
                           "name":"manager"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
```



```
                },
                {
                    "type": "Groups",
                    "any_one_of": [
                        "idp_admin"
                    ]
                }
            ]
        }
]
```

– A asserção a seguir indica que o usuário federado John Smith é membro do grupo **idp_admin**. Portanto, o usuário pode acessar a Huawei Cloud.

```
{UserName: John Smith}
{Groups: [idp_user, idp_admin, idp_agency]}
```

– A asserção a seguir indica que o usuário federado John Smith não é membro do grupo **idp_admin**. Portanto, a regra não entra em vigor para o usuário e o usuário não pode acessar a Huawei Cloud.

```
{UserName: John Smith}
{Groups: [idp_user, idp_agency]}
```

Exemplo de condição contendo uma expressão regular

Você pode adicionar **"regex": true** a uma condição para calcular resultados usando uma expressão regular.

Esta regra entra em vigor para qualquer usuário cujo nome de usuário termine com **@mail.com**. O nome de usuário de cada usuário federado aplicável é *UserName* no IAM e o usuário pertence ao grupo **admin**.

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
                {
                    "group": {
                        "name": "admin"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
                },
                {
                    "type": "Groups",
                    "any_one_of": [
                        ".*@mail.com$"
                    ],
                    "regex": true
                }
            ]
        }
]
```

Exemplos de condições combinadas

Várias condições podem ser combinadas usando o operador lógico AND.

Essa regra entra em vigor somente para os usuários federados que não pertencem ao grupo de usuários **idp_user** ou **idp_agent** no IdP. O nome de usuário de cada usuário federado aplicável é *UserName* no IAM e o usuário pertence ao grupo **admin**.


```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
                {
                    "group": {
                        "name": "admin"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
                },
                {
                    "type": "Groups",
                    "not_any_of": [
                        "idp_user"
                    ]
                },
                {
                    "type": "Groups",
                    "not_any_of": [
                        "idp_agent"
                    ]
                }
            ]
        }
]
```

A regra anterior é equivalente à seguinte:

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
                {
                    "group": {
                        "name": "admin"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
                },
                {
                    "type": "Groups",
                    "not_any_of": [
                        "idp_user",
                        "idp_agent"
                    ]
                }
            ]
        }
]
```

Exemplos de regras combinadas

Se várias regras forem combinadas, os métodos para correspondência de nomes de usuários e grupos de usuários serão diferentes.

O nome de um usuário federado será o nome de usuário correspondente na primeira regra que entrar em vigor, e o usuário pertencerá a todos os grupos correspondentes em todas as regras que entrarem em vigor. Um usuário federado só pode fazer logon se pelo menos uma regra entrar em vigor para corresponder ao nome de usuário. Para facilitar a compreensão, as regras de nome de usuário e grupo de usuários podem ser configuradas separadamente.

No exemplo a seguir, as regras entram em vigor para usuários no grupo **idp_admin**. O nome de usuário de cada usuário federado aplicável é *UserName* no IAM e o usuário pertence ao grupo **admin**.

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}"
                }
            }
        ],
        "remote": [
            {
                "type": "UserName"
            }
        ]
    },
    {
        "local": [
            {
                "group": {
                    "name": "admin"
                }
            }
        ],
        "remote": [
            {
                "type": "Groups",
                "any_one_of": [
                    "idp_admin"
                ]
            }
        ]
    }
]
```

A asserção a seguir indica que o usuário John Smith é membro do grupo **idp_admin** no IdP e, portanto, atende às regras. O nome de usuário desse usuário será **John Smith** no IAM e o usuário pertencerá ao grupo **admin**.

```
{UserName: John Smith}
{Groups: [idp_user, idp_admin, idp_agency]}
```


10 Agente identificador personalizado

10.1 Ativação do acesso ao corretor de identidade personalizado com uma agência

Se o **IdP da sua empresa** não for compatível com SAML ou OpenID Connect, você poderá criar um corretor de identidade personalizado para permitir o acesso à Huawei Cloud. Você pode escrever e executar código para gerar um URL de logon. Os usuários da sua empresa podem usar o URL para fazer logon na Huawei Cloud. Os usuários serão autenticados pelo seu IdP empresarial.

NOTA

Se o seu IdP empresarial for compatível com SAML ou OpenID Connect, configure a **federação de identidade** para permitir que os usuários da sua empresa acessem a Huawei Cloud por meio do SSO.

Pré-requisitos

- Sua empresa tem um sistema de gerenciamento empresarial.
- Você registrou uma conta (por exemplo, **DomainA**) na Huawei Cloud como um administrador empresarial e criou um grupo de usuários (por exemplo, **GroupC**) e atribuiu a ele a função **Agent Operator**. (Para obter detalhes, consulte **Criação de um grupo de usuários e atribuição de permissões**.)

Procedimento

Passo 1 Use a conta **DomainA** para criar um usuário do IAM (por exemplo, **UserB**) e adicione o usuário ao **GroupC** seguindo as instruções em **Adição de usuários a um grupo de usuários**.

> **NOTA**
>
> Certifique-se de que o usuário do IAM possa **acessar programaticamente** os serviços da Huawei Cloud. Para obter detalhes sobre como alterar o tipo de acesso, consulte **3.4 Visualização ou modificação das informações do usuário do IAM**.

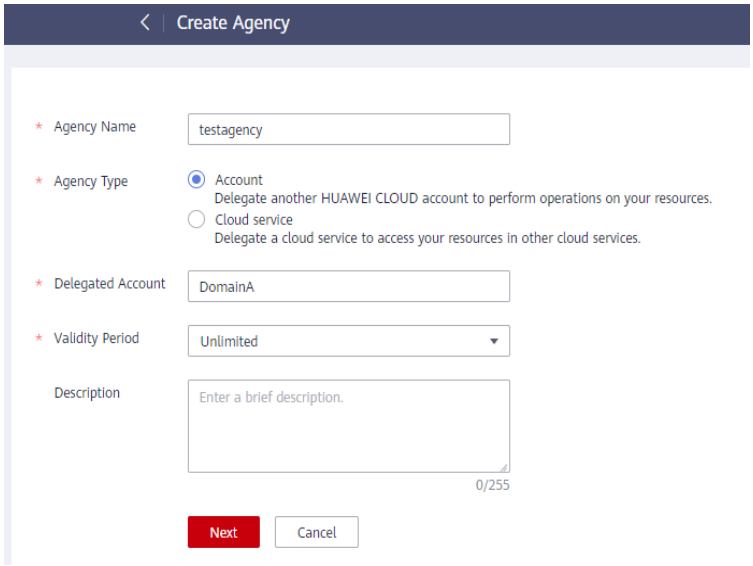
Passo 2 Configure a **chave de acesso** (recomendado) ou o nome de usuário e senha de **UserB** no arquivo de configuração do seu IdP empresarial para que o usuário possa obter um token para chamar APIs. Para segurança da conta, criptografe a senha e a chave de acesso antes de armazená-las.

Passo 3 No painel de navegação do console do IAM, escolha **Agencies**. Em seguida, clique em **Create Agency** no canto superior direito.

Passo 4 Defina os parâmetros da agência.

Por exemplo, defina o nome da agência como **testagency**, o tipo de agência como **Account** e delegue conta como **DomainA**. Defina o período de validade e clique em **Next**.

Figura 10-1 Criar uma agência



Passo 5 Defina o escopo de autorização e selecione as permissões que deseja conceder à agência.

Passo 6 No IdP empresarial, crie um grupo de usuários chamado **testagency** (mesmo que o nome da agência criada em **Passo 4**), adicione usuários empresariais ao grupo e conceda aos usuários permissões para fazer logon na Huawei Cloud por meio de um corretor de identidade personalizado. Para obter detalhes, consulte a documentação do IdP empresarial.

Passo 7 Depois que um usuário empresarial fizer logon no sistema de gerenciamento empresarial, o usuário poderá acessar o corretor de identidade personalizado do IdP empresarial selecionando uma agência na lista de agências. O usuário pode obter a agência do administrador de segurança ou do usuário raiz. Para obter detalhes, consulte a documentação do sistema de gerenciamento empresarial.

> **NOTA**
>
> As agências do corretor de identidade devem existir na Huawei Cloud e ter os mesmos nomes que alguns grupos de usuários criados no IdP empresarial.

Passo 8 O corretor de identidade personalizado usa o token de **userB** para chamar a API **POST /v3.0/OS-CREDENTIAL/securitytokens** usada para obter um token de segurança temporário. Para obter detalhes, consulte **Obtenção de uma chave de acesso temporária e de um securityToken por meio de uma agência**.

NOTA

Ao obter um securityToken com uma agência, defina o parâmetro **session_user.name** no corpo da solicitação.

Passo 9 O corretor de identidade personalizado usa a chave de acesso temporária, o token de segurança e o nome de domínio global do IAM (iam.myhuaweicloud.com) para chamar a API **POST /v3.0/OS-AUTH/securitytoken/logintokens** para obter um loginToken. O valor de **X-Subject-LoginToken** no cabeçalho da resposta é um loginToken. Para obter detalhes, consulte **Obtenção de um loginToken**.

NOTA

- Para obter um loginToken chamando a API **POST /v3.0/OS-AUTH/securitytoken/logintokens**, use o nome de domínio global (iam.myhuaweicloud.com) do IAM.
- Um loginToken é emitido para um usuário fazer logon por meio de um corretor de identidade personalizado e contém informações de identidade e sessão sobre o usuário. Um loginToken é válido por 10 minutos por padrão. LoginTokens são necessários para autenticação quando os usuários fazem logon em um console de serviço usando o FederationProxyUrl.
- Você pode definir o período de validade de um loginToken chamando a API **POST /v3.0/OS-AUTH/securitytoken/logintokens**. O período de validade varia de 10 minutos a 12 horas. Se o valor que você especificou for maior que o período de validade restante do token de segurança temporário, será usado o período de validade restante do securityToken temporário.

Passo 10 O corretor de identidade personalizado gera um FederationProxyUrl e o retorna ao navegador por meio de **Location**. O FederationProxyUrl será no seguinte formato:

https://auth.huaweicloud.com/authui/federation/login?idp_login_url={enterprise_system_loginURL}&service={console_service_region_url}*&logintoken={logintoken}*

Exemplo:

*https://auth.huaweicloud.com/authui/federation/login?idp_login_url=https%3A%2F%2Fexample.com&service=https%3a%2f%2fconsole.huaweicloud.com%2fapm%2f%3fregion%3dcn-north-4%23%2fapm%2fatps%2ftopology&logintoken=******

Tabela 10-1 Descrição do parâmetro

Parâmetro	Descrição
idp_login_url	URL de logon do sistema de gerenciamento empresarial.
service	Endereço de acesso de um serviço da Huawei Cloud.
logintoken	LoginToken do corretor de identidade personalizado.

Os três parâmetros anteriores devem ser codificados usando URLEncode para garantir que eles possam ser identificados pelo navegador.

Para obter detalhes sobre como criar um FederationProxyUrl, veja o exemplo fornecido em **10.2 Criação de um FederationProxyUrl usando uma agência**.

NOTA

O FederationProxyUrl contém o loginToken que foi obtido do IAM e é codificado em porcentagem.

Passo 11 Se o loginToken for autenticado com sucesso, os usuários federados serão automaticamente redirecionados para o endereço de serviço da Huawei Cloud especificado no parâmetro **service**.

Se o loginToken não for autenticado, os usuários serão redirecionados para o endereço especificado em **idp_login_url**.

----Fim

10.2 Criação de um FederationProxyUrl usando uma agência

Esta seção fornece o código de exemplo usado para criar um FederationProxyUrl programaticamente usando uma agência para fazer logon nos serviços da Huawei Cloud.

Exemplo de código usando Java

O código de Java a seguir mostra como criar um FederationProxyUrl que dá aos usuários federados acesso direto ao console da Huawei Cloud.

```
import java.net.*;
import java.util.Collections;
import com.huaweicloud.sdk.core.auth.GlobalCredentials;
import com.huaweicloud.sdk.core.exception.ClientRequestException;
import com.huaweicloud.sdk.core.exception.ServerResponseException;
import com.huaweicloud.sdk.core.http.HttpConfig;
import com.huaweicloud.sdk.iam.v3.IamClient;
import com.huaweicloud.sdk.iam.v3.model.*;


// Use the global domain name to obtain a loginToken.
String endpoint = "https://iam.myhuaweicloud.com";

// Configure client attributes.
HttpConfig config = HttpConfig.getDefaultHttpConfig()
        .withIgnoreSSLVerification(true)
        .withProxyHost("proxy.huawei.com")
        .withProxyPort(8080);

// Use the domain ID (account ID), AK, and SK of userB to initialize the
specified IAM client "{Service}Client". For details about how to create userB,
see section "Creating an IAM User".
IamClient iamClient = IamClient.newBuilder().withCredential(new
GlobalCredentials()
        .withDomainId("domainId")
        .withAk("ak")
        .withSk("sk"))
        .withEndpoint(endpoint)
        .withHttpConfig(config)
        .build();

/*CreateTemporaryAccessKeyByAgency
Call the API used to obtain a temporary access key and security token with an
agency.
The default validity period of an access key and securityToken is 900 seconds,
that is, 15 minutes. The value ranges from 15 minutes to 24 hours. In this
example, the validity period is set to 3600 seconds, that is, 1 hour.
When you obtain a loginToken with a specified validity period, ensure that the
```



```
validity period of the loginToken is not greater than the remaining validity
period of the security token.
*/
IdentityAssumerole identityAssumerole = new IdentityAssumerole().

withAgencyName("testagency").withDomainId("0525e2c87exxxxxxx").withSessionUser(new
 AssumeroleSessionuser().withName("ExternalUser")).withDurationSeconds(3600);
AgencyAuth agencyAuth = new AgencyAuth().withIdentity(new
AgencyAuthIdentity().withAssumeRole(identityAssumerole).

withMethods(Collections.singletonList(AgencyAuthIdentity.MethodsEnum.fromValue("as
sume_role"))));
CreateTemporaryAccessKeyByAgencyRequestBody
createTemporaryAccessKeyByAgencyRequestBody = new
CreateTemporaryAccessKeyByAgencyRequestBody().withAuth(agencyAuth);
CreateTemporaryAccessKeyByAgencyResponse createTemporaryAccessKeyByAgencyResponse
= iamClient.createTemporaryAccessKeyByAgency(new
CreateTemporaryAccessKeyByAgencyRequest().withBody(createTemporaryAccessKeyByAgenc
yRequestBody));
Credential credential = createTemporaryAccessKeyByAgencyResponse.getCredential();

/*CreateLoginToken
Obtain a loginToken.
LoginTokens are issued to users to log in through custom identity brokers. Each
loginToken contains identity and session information of a user.
To log in to a cloud service console using a custom identity broker URL, call
this API to obtain a loginToken for authentication.
The default validity period of a loginToken is 600 seconds, that is, 10 minutes.
The value ranges from 10 minutes to 12 hours. In this example, the validity
period is set to 1800 seconds, that is, half an hour.
Ensure that the validity period of the loginToken is not greater than the
remaining validity period of the security token.
When obtaining a securityToken with an agency, set the session_user.name
parameter in the request body.
*/
CreateLoginTokenRequestBody createLoginTokenRequestBody = new
CreateLoginTokenRequestBody().
        withAuth(new LoginTokenAuth().withSecuritytoken(new
LoginTokenSecurityToken().
                withAccess(credential.getAccess()).
                withId(credential.getSecuritytoken()).
                withSecret(credential.getSecret()).withDurationSeconds(1800)));
CreateLoginTokenResponse createLoginTokenResponse =
iamClient.createLoginToken(new
CreateLoginTokenRequest().withBody(createLoginTokenRequestBody));
String loginToken = createLoginTokenResponse.getXSubjectLoginToken();

// Login URL of the custom identity broker
String authURL = "https://auth.huaweicloud.com/authui/federation/login";
// Login URL of an enterprise management system.
String enterpriseSystemLoginURL = "https://example.com/";
// Huawei Cloud service address to access.
String targetConsoleURL = "https://console.huaweicloud.com/iam/?region=cn-
north-4";

// Create a FederationProxyUrl and return it to the browser through Location.
String FederationProxyUrl = authURL + "?idp_login_url=" +
        URLEncoder.encode(enterpriseSystemLoginURL, "UTF-8") +
        "&service=" + URLEncoder.encode(targetConsoleURL, "UTF-8") +
        "&logintoken=" +URLEncoder.encode(loginToken, "UTF-8");
```

Exemplo de código usando Python

O código Python a seguir mostra como criar um FederationProxyUrl que dá aos usuários federados acesso direto ao console da Huawei Cloud.

```
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.http.http_config import HttpConfig
from huaweicloudsdkiam.v3 import *
```



```
import urllib


# Use the global domain name to obtain a loginToken.
endpoint = "https://iam.myhuaweicloud.com"

# Configure client attributes.
config = HttpConfig.get_default_config()
config.ignore_ssl_verification = True
config.proxy_protocol = "https"
config.proxy_host = "proxy.huawei.com"
config.proxy_port = 8080
credentials = GlobalCredentials(ak, sk, domain_id)

# Use the domain ID (account ID), AK, and SK of userB to initialize the specified
IAM client "{Service}Client". For details about how to create userB, see section
"Creating an IAM User".
client = IamClient().new_builder(IamClient) \
    .with_http_config(config) \
    .with_credentials(credentials) \
    .with_endpoint(endpoint) \
    .build()

# CreateTemporaryAccessKeyByAgency
# Call the API used to obtain a temporary access key and security token with an
agency.
# The default validity period of an access key and securityToken is 900 seconds,
that is, 15 minutes. The value ranges from 15 minutes to 24 hours. In this
example, the validity period is set to 3600 seconds, that is, 1 hour.
# When you obtain a loginToken with a specified validity period, ensure that the
validity period of the loginToken is not greater than the remaining validity
period of the security token.
# When obtaining a securityToken with an agency, set the session_user.name
parameter in the request body.
assume_role_session_user = AssumeroleSessionuser(name="ExternalUser")
identity_assume_role = IdentityAssumerole(agency_name="testagency",
                                          domain_id="0525e2c87exxxxxxx",
                      session_user=assume_role_session_user,
                      duration_seconds=3600)
identity_methods = ["assume_role"]
body = CreateTemporaryAccessKeyByAgencyRequestBody(
    AgencyAuth(AgencyAuthIdentity(methods=identity_methods,
assume_role=identity_assume_role)))
request = CreateTemporaryAccessKeyByAgencyRequest(body)
create_temporary_access_key_by_agency_response =
client.create_temporary_access_key_by_agency(request)
credential = create_temporary_access_key_by_agency_response.credential

# CreateLoginToken
# Obtain a loginToken.
# The default validity period of a loginToken is 600 seconds, that is, 10
minutes. The value ranges from 10 minutes to 12 hours. In this example, the
validity period is set to 1800 seconds, that is, half an hour.
# Ensure that the validity period of the loginToken is not greater than the
remaining validity period of the security token.
login_token_security_token = LoginTokenSecurityToken(access=credential.access,
secret=credential.secret,
                             id=credential.securitytoken, duration_seconds=1800)
body = CreateLoginTokenRequestBody(LoginTokenAuth(login_token_security_token))
request = CreateLoginTokenRequest(body)
create_login_token_response = client.create_login_token(request)
login_token = create_login_token_response.x_subject_login_token

# Obtain a custom identity broker URL.
auth_URL = "https://auth.huaweicloud.com/authui/federation/login"
# Login URL of an enterprise management system.
enterprise_system_login_URL = "https://example.com/"
# Huawei Cloud service address to access.
```



```
target_console_URL = "https://console.huaweicloud.com/iam/?region=cn-north-4"

# Create a FederationProxyUrl and return it to the browser through Location.
FederationProxyUrl = auth_URL + "?idp_login_url=" + urllib.parse.quote(
    enterprise_system_login_URL) + "&service=" + urllib.parse.quote(
    target_console_URL) + "&logintoken=" + urllib.parse.quote(login_token)
print(FederationProxyUrl)
```

10.3 Ativação do acesso ao corretor de identidade personalizado com um token

Se o IdP da sua empresa não for compatível com SAML ou OpenID Connect, você poderá criar um corretor de identidade personalizado para permitir o acesso à Huawei Cloud. Você pode escrever e executar código para gerar um URL de logon. Os usuários da sua empresa podem usar o URL para fazer logon na Huawei Cloud. Os usuários serão autenticados pelo seu IdP empresarial.

NOTA

Se o seu IdP empresarial for compatível com SAML ou OpenID Connect, configure a **federação de identidade** para permitir que os usuários da sua empresa acessem a Huawei Cloud por meio do SSO.

Pré-requisitos

- Sua empresa tem um sistema de gerenciamento empresarial.
- O administrador da empresa criou uma conta (por exemplo, **DomainA**) na Huawei Cloud.

Procedimento

Passo 1 Use a conta **DomainA** para criar um usuário do IAM (por exemplo, **UserB**) seguindo as instruções em **3.1 Criação de um usuário do IAM**.

Passo 2 (Opcional) Adicione **UserB** a um grupo de usuários (por exemplo, **GroupC**) e conceda permissões ao grupo de usuários seguindo as instruções em **4.1 Criação de um grupo de usuários e atribuição de permissões**.

Passo 3 Configure a **chave de acesso** (recomendado) ou o nome de usuário e a senha de **UserB** no arquivo de configuração do seu IdP empresarial para que o usuário possa obter um token de usuário. Para segurança da conta, criptografe a senha e a chave de acesso antes de armazená-las.

Passo 4 Efetue logon no sistema de gerenciamento empresarial, acesse o corretor de identidade personalizado selecionando um usuário comum na lista de usuários. Para obter detalhes, consulte a documentação do sistema de gerenciamento empresarial. Para este exemplo, selecione o usuário **UserB**.

NOTA

A lista de usuários do corretor personalizado é a mesma que a lista de usuários do IAM na sua conta da Huawei Cloud. Para alinhar esses usuários do IAM com as contas de usuário da sua empresa, configure as **chaves de acesso** dos usuários do IAM (recomendado) ou nomes de usuário e senhas no arquivo de configuração do IdP empresarial.

Passo 5 O corretor de identidade personalizado usa o token de **userB** para chamar a API **POST / v3.0/OS-CREDENTIAL/securitytokens** usada para obter uma chave de acesso temporária e

um token de segurança. Para obter detalhes, consulte **Obtenção de uma chave de acesso temporária e de um token de segurança por meio de um token**.

Passo 6 O corretor de identidade personalizado usa a chave de acesso temporária, o token de segurança e o nome de domínio global do IAM (iam.myhuaweicloud.com) para chamar a API **POST /v3.0/OS-AUTH/securitytoken/logintokens** para obter um loginToken. O valor de **X-Subject-LoginToken** no cabeçalho da resposta é um loginToken. Para obter detalhes, consulte **Obtenção de um token de logon**.

NOTA

- Para obter um loginToken chamando a API **POST /v3.0/OS-AUTH/securitytoken/logintokens**, use o nome de domínio global (iam.myhuaweicloud.com) do IAM.
- Um loginToken é emitido para um usuário fazer logon por meio de um corretor de identidade personalizado e contém informações de identidade e sessão sobre o usuário. Um loginToken é válido por 10 minutos por padrão.
- Você pode definir o período de validade de um loginToken chamando a API **POST /v3.0/OS-AUTH/securitytoken/logintokens**. O período de validade varia de 10 minutos a 12 horas. Se o valor que você especificou for maior que o período de validade restante do token de segurança temporário, será usado o período de validade restante do securityToken temporário.

Passo 7 O corretor de identidade personalizado gera um FederationProxyUrl e o retorna ao navegador por meio de **Location**.

```
https://auth.huaweicloud.com/authui/federation/login?
idp_login_url={enterprise_system_loginURL}&service={console_service_region_url}&lo
gintoken={logintoken}
```

Exemplo:

```
https://auth.huaweicloud.com/authui/federation/login?idp_login_url=https%3A%2F
%2Fexample.com&service=https%3a%2f%2fconsole.huaweicloud.com%2fapm%2f%3fregion
%3dcn-north-4%23%2fapm%2fatps%2ftopology&logintoken=******
```

Tabela 10-2 Descrição do parâmetro

Parâmetro	Descrição
idp_login_url	URL de logon do sistema de gerenciamento empresarial.
service	Endereço de acesso de um serviço da Huawei Cloud.
logintoken	LoginToken do corretor de identidade personalizado.

Para obter detalhes sobre como criar um FederationProxyUrl, veja o exemplo fornecido em **10.4 Criação de um FederationProxyUrl usando um token**.

NOTA

O FederationProxyUrl contém o loginToken obtido do IAM e o valor de cada parâmetro no FederationProxyUrl é codificado usando URLEncode.

Passo 8 Se o loginToken for autenticado com sucesso, você será automaticamente redirecionado para o endereço de serviço da Huawei Cloud especificado no parâmetro **service**.

Se o loginToken não for autenticado, você será redirecionado para o endereço especificado em **idp_login_url**.

----Fim

10.4 Criação de um FederationProxyUrl usando um token

Esta seção fornece o código de exemplo usado para criar um FederationProxyUrl programaticamente usando um token para fazer logon nos serviços da Huawei Cloud.

Exemplo de código usando Java

O código de Java a seguir mostra como criar um FederationProxyUrl que dá aos usuários federados acesso direto ao console da Huawei Cloud.

```
import java.net.URLEncoder;
import java.util.Collections;
import com.huaweicloud.sdk.core.auth.GlobalCredentials;
import com.huaweicloud.sdk.core.http.HttpConfig;
import com.huaweicloud.sdk.core.exception.*;
import com.huaweicloud.sdk.iam.v3.IamClient;
import com.huaweicloud.sdk.iam.v3.model.*;

// Use the global domain name to obtain a loginToken.
String endpoint = "https://iam.myhuaweicloud.com";

// Configure client attributes.
HttpConfig config = HttpConfig.getDefaultHttpConfig()
        .withIgnoreSSLVerification(true)
        .withProxyHost("proxy.huawei.com")
        .withProxyPort(8080);

// Use the domain ID (account ID), AK, and SK of userB to initialize the
specified IAM client "{Service}Client". For details about how to create userB,
see section "Creating an IAM User".
IamClient iamClient = IamClient.newBuilder().withCredential(new
GlobalCredentials()
        .withDomainId(domainId)
        .withAk(ak)
        .withSk(sk))
        .withEndpoint(endpoint)
        .withHttpConfig(config)
        .build();

/*CreateTemporaryAccessKeyByToken
Call the API used to obtain a temporary access key and security token with a
token.
The default validity period of an access key and security token is 900 seconds,
that is, 15 minutes. The value ranges from 15 minutes to 24 hours. In this
example, the validity period is set to 3600 seconds, that is, 1 hour.
When you obtain a loginToken with a specified validity period, ensure that the
validity period of the loginToken is not greater than the remaining validity
period of the securityToken.
*/
TokenAuthIdentity tokenAuthIdentity = new
TokenAuthIdentity().withMethods(Collections.singletonList(TokenAuthIdentity.Method
sEnum.fromValue("token"))).withToken(new
IdentityToken().withDurationSeconds(3600));
CreateTemporaryAccessKeyByTokenRequestBody
createTemporaryAccessKeyByTokenRequestBody = new
CreateTemporaryAccessKeyByTokenRequestBody().withAuth(new
TokenAuth().withIdentity(tokenAuthIdentity));
CreateTemporaryAccessKeyByTokenResponse createTemporaryAccessKeyByTokenResponse =
iamClient.createTemporaryAccessKeyByToken(new
CreateTemporaryAccessKeyByTokenRequest().withBody(createTemporaryAccessKeyByTokenR
equestBody));
Credential credential = createTemporaryAccessKeyByTokenResponse.getCredential();

/*CreateLoginToken
Obtain a loginToken.
```



```
LoginTokens are issued to users to log in through custom identity brokers. Each
loginToken contains identity and session information of a user.
To log in to a cloud service console using a custom identity broker URL, call
this API to obtain a loginToken for authentication.
The default validity period of a loginToken is 600 seconds, that is, 10 minutes.
The value ranges from 10 minutes to 12 hours. In this example, the validity
period is set to 1800 seconds, that is, half an hour.
Ensure that the validity period of the loginToken is not greater than the
remaining validity period of the security token.
*/
CreateLoginTokenRequestBody createLoginTokenRequestBody = new
CreateLoginTokenRequestBody().
        withAuth(new LoginTokenAuth().withSecuritytoken(new
LoginTokenSecurityToken().
                withAccess(credential.getAccess()).
                withId(credential.getSecuritytoken()).
                withSecret(credential.getSecret()).withDurationSeconds(1800)));
CreateLoginTokenResponse createLoginTokenResponse =
iamClient.createLoginToken(new
CreateLoginTokenRequest().withBody(createLoginTokenRequestBody));
String loginToken = createLoginTokenResponse.getXSubjectLoginToken();

// Obtain a custom identity broker URL.
String authURL = "https://auth.huaweicloud.com/authui/federation/login";
// Login URL of an enterprise management system.
String enterpriseSystemLoginURL = "https://example.com/";
// Huawei Cloud service address to access.
String targetConsoleURL = "https://console.huaweicloud.com/iam/?region=cn-
north-4";

// Create a FederationProxyUrl and return it to the browser through Location.
String FederationProxyUrl = authURL + "?idp_login_url=" +
        URLEncoder.encode(enterpriseSystemLoginURL, "UTF-8") +
        "&service=" + URLEncoder.encode(targetConsoleURL, "UTF-8") +
        "&logintoken=" +URLEncoder.encode(loginToken, "UTF-8");
```

Exemplo de código usando Python

O código Python a seguir mostra como criar um FederationProxyUrl que dá aos usuários federados acesso direto ao console da Huawei Cloud.

```
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.http.http_config import HttpConfig
from huaweicloudsdkiam.v3 import *

import urllib

# Use the global domain name to obtain a loginToken.
endpoint = "https://iam.myhuaweicloud.com"

# Configure client attributes.
config = HttpConfig.get_default_config()
config.ignore_ssl_verification = True
config.proxy_protocol = "https"
config.proxy_host = "proxy.huawei.com"
config.proxy_port = 8080
credentials = GlobalCredentials(ak, sk, domain_id)

# Use the domain ID (account ID), AK, and SK of userB to initialize the specified
IAM client "{Service}Client". For details about how to create userB, see section
"Creating an IAM User".
client = IamClient().new_builder(IamClient) \
    .with_http_config(config) \
    .with_credentials(credentials) \
    .with_endpoint(endpoint) \
    .build()

# CreateTemporaryAccessKeyByToken
# Call the API used to obtain a temporary access key and security token with a
```



```
token.
# The default validity period of an access key and securityToken is 900 seconds,
that is, 15 minutes. The value ranges from 15 minutes to 24 hours. In this
example, the validity period is set to 3600 seconds, that is, 1 hour.
# When you obtain a loginToken with a specified validity period, ensure that the
validity period of the loginToken is not greater than the remaining validity
period of the security token.
identity_methods = ["token"]
identity_token = IdentityToken(duration_seconds=3600)
body = CreateTemporaryAccessKeyByTokenRequestBody(
    TokenAuth(TokenAuthIdentity(methods=identity_methods, token=identity_token)))
request = CreateTemporaryAccessKeyByTokenRequest(body)
create_temporary_access_key_by_token_response =
client.create_temporary_access_key_by_token(request)
credential = create_temporary_access_key_by_token_response.credential

# CreateLoginToken
# Obtain a loginToken.
# LoginTokens are issued to users to log in through custom identity brokers. Each
loginToken contains identity and session information of a user.
# To log in to a cloud service console using a custom identity broker URL, call
this API to obtain a loginToken for authentication.
# The default validity period of a loginToken is 600 seconds, that is, 10
minutes. The value ranges from 10 minutes to 12 hours. In this example, the
validity period is set to 1800 seconds, that is, half an hour.
# Ensure that the validity period of the loginToken is not greater than the
remaining validity period of the security token.
login_token_security_token = LoginTokenSecurityToken(access=credential.access,
secret=credential.secret,
                            id=credential.securitytoken, duration_seconds=1800)
body = CreateLoginTokenRequestBody(LoginTokenAuth(login_token_security_token))
request = CreateLoginTokenRequest(body)
create_login_token_response = client.create_login_token(request)
login_token = create_login_token_response.x_subject_login_token


# Login URL of the custom identity broker
auth_URL = "https://auth.huaweicloud.com/authui/federation/login"
# Login URL of an enterprise management system.
enterprise_system_login_URL = "https://example.com/"
# Huawei Cloud service address to access.
target_console_URL = "https://console.huaweicloud.com/iam/?region=cn-north-4"

# Create a FederationProxyUrl and return it to the browser through Location.
FederationProxyUrl = auth_URL + "?idp_login_url=" + urllib.parse.quote(
    enterprise_system_login_URL) + "&service=" + urllib.parse.quote(
    target_console_URL) + "&logintoken=" + urllib.parse.quote(login_token)
print(FederationProxyUrl)
```


11 Autenticação MFA e dispositivo MFA virtual

11.1 Autenticação MFA

O que é a autenticação MFA?

A autenticação MFA fornece uma camada adicional de proteção além do nome de usuário e da senha. Se você ativar a autenticação MFA, os usuários precisarão digitar o nome de usuário e a senha, bem como um código de verificação, antes de poderem fazer logon no console.

A autenticação MFA também pode ser ativada para verificar a identidade de um usuário antes que o usuário tenha permissão para executar operações críticas.

Métodos de autenticação MFA

A autenticação MFA pode ser realizada por meio de SMS, e-mail e dispositivo de MFA virtual.

Cenários de aplicações

A autenticação MFA é adequada para proteção de logon e proteção de operação crítica. Se a autenticação MFA estiver ativada, a configuração entrará em vigor para o console de gerenciamento e para as APIs REST.

- Proteção de logon: quando você ou um IAM da sua conta faz logon no console, você e o usuário precisam inserir um código de verificação, além do nome de usuário e da senha.
- Proteção da operação: quando você ou um IAM sob sua conta tenta executar uma operação crítica, como excluir um recurso do ECS, você e o usuário precisam inserir um código de verificação para prosseguir.

Para obter mais informações sobre proteção de logon e proteção de operação crítica, consulte **8.3 Proteção de operações críticas**.

11.2 Dispositivo de MFA virtual

Esta seção descreve como **vincular** e **desvincular** um dispositivo de MFA virtual. Se o dispositivo de MFA virtual vinculado de um usuário do IAM for excluído ou o telefone celular no qual ele é executado não estiver disponível, você poderá **remover** o dispositivo de MFA virtual para o usuário do IAM.

O que é um dispositivo de MFA virtual?

Um dispositivo ou uma aplicação de MFA gera códigos de verificação de 6 dígitos em conformidade com o TOTP (Algoritmo de senha única baseado em tempo). Os dispositivos de MFA podem ser baseados em hardware ou software. Atualmente, os dispositivos de MFA virtuais baseados em software são suportados. Eles são programas de aplicações executados em dispositivos inteligentes, como telefones celulares.

Vincular um dispositivo de MFA virtual

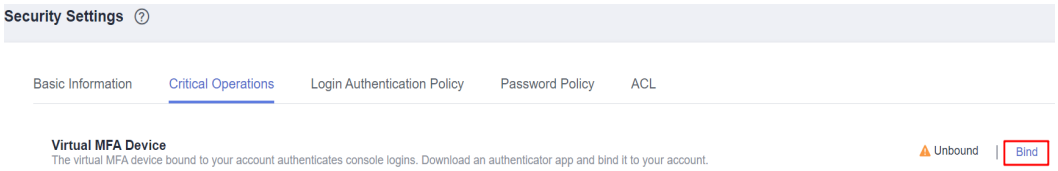
Antes de vincular um dispositivo de MFA virtual, instale primeiro um aplicativo autenticador (como o Google Authenticator ou o Microsoft Authenticator) em seu dispositivo móvel.

- **Conta da Huawei Cloud**

Passo 1 Vá para a página **Configurações de segurança**.

Passo 2 Clique na guia **Critical Operations** e clique em **Bind** na linha **Virtual MFA Device**.

Figura 11-1 Dispositivo de MFA virtual



Passo 3 Configure o aplicativo de MFA digitalizando o código QR ou inserindo manualmente a chave secreta.

Você pode vincular um dispositivo de MFA virtual à sua conta digitalizando o código QR ou inserindo a chave secreta.

- Digitalizar o código QR

  Abra o aplicativo de MFA em seu telefone celular e use-o para digitalizar o código QR exibido na página **Bind Virtual MFA Device**. Sua conta ou usuário IAM é então adicionado à aplicação.

- Inserir manualmente a chave secreta

  Abra o aplicativo de MFA no seu celular e digite a chave secreta.

  NOTA

  O usuário só pode ser adicionado manualmente usando senhas de uso único baseadas em tempo (TOTP). É aconselhável ativar a definição automática da hora no seu telefone celular.

Passo 4 Visualize os códigos de verificação no aplicativo de MFA. O código é atualizado automaticamente a cada 30 segundos.

Passo 5 Na página **Bind Virtual MFA Device**, insira dois códigos de verificação consecutivos e clique em **OK**.

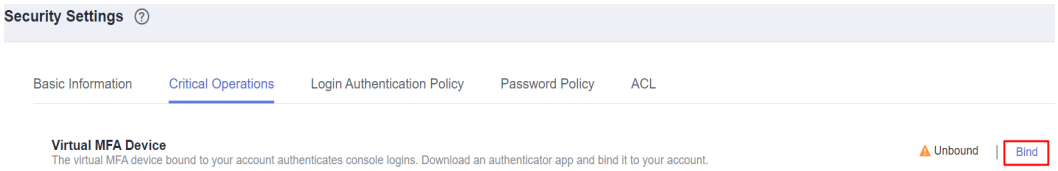
----Fim

- **HUAWEI ID**

Passo 1 Vá para a página **Configurações de segurança**.

Passo 2 Clique na guia **Critical Operations** e clique em **Bind** na linha **Virtual MFA Device**.

Figura 11-2 Vincular um dispositivo de MFA virtual



Passo 3 Na página **Account & security** da central de contas da HUAWEI ID, vincule um autenticador à sua HUAWEI ID conforme as instruções.

----Fim

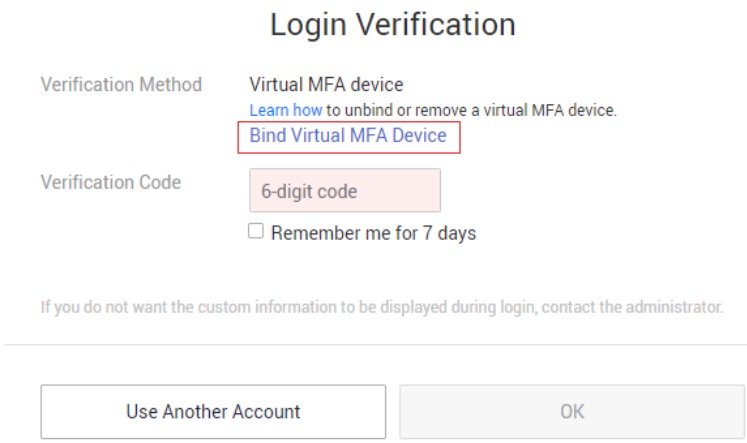
- **Usuário do IAM**

Os usuários do IAM podem vincular um dispositivo de MFA virtual no console do IAM. O procedimento é o mesmo que para **vincular um dispositivo de MFA virtual a uma conta da Huawei Cloud**.

Se o administrador tiver redefinido o dispositivo de MFA virtual de um usuário do IAM ou se o usuário do IAM fizer logon no sistema pela primeira vez e a proteção de logon tiver sido ativada com o dispositivo de MFA virtual como método de verificação, o usuário do IAM precisa vincular um dispositivo de MFA virtual novamente durante o logon. O procedimento é o seguinte:

Passo 1 Faça logon no console de gerenciamento como um usuário do IAM.

Passo 2 Na caixa de diálogo **Login Verification**, clique em **Bind Virtual MFA Device**.



Passo 3 No painel deslizante, siga as instruções para vincular um dispositivo de MFA virtual.

----Fim

Obter um código de verificação do MFA

Se a proteção de logon ou proteção de operação baseada em MFA virtual estiver ativada, você precisará inserir um código de verificação de MFA ao fazer logon no console ou executar uma operação crítica.

Abra a aplicação de MFA no seu dispositivo inteligente, veja o código de verificação exibido ao lado da sua conta e insira o código no console.

Desvincular um dispositivo de MFA virtual

Você pode desvincular o dispositivo de MFA virtual, desde que o telefone celular vinculado ao dispositivo de MFA virtual esteja disponível e o dispositivo de MFA virtual ainda esteja instalado em seu celular.

- Usuário do IAM: se o telefone celular de um usuário do IAM não estiver disponível ou se o dispositivo de MFA virtual tiver sido excluído de celular, solicite ao administrador que **remova o dispositivo de MFA virtual**.
- Conta: se o telefone celular vinculado à conta não estiver disponível ou se o dispositivo de MFA virtual tiver sido excluído do celular, entre em contato com o atendimento ao cliente para remover o dispositivo de MFA virtual.

Passo 1 Vá para a página **Configurações de segurança**.

Passo 2 Clique na guia **Critical Operations** e clique em **Unbind** na linha **Virtual MFA Device**.

NOTA

Se você atualizou sua conta da Huawei Cloud para uma HUAWEI ID, você será redirecionado para o site da HUAWEI ID. Vá para a página **Account center** > **Account and security** e clique em **Disassociate** na linha **Authenticator** na área **Security verification**.

Passo 3 Na página **Unbind Virtual MFA Device**, insira um código de verificação gerado pela aplicação de MFA.

Figura 11-3 Inserir um código de verificação de MFA virtual

Passo 4 Clique em **OK**.

----Fim

Remoção do dispositivo de MFA virtual

Conta: se o telefone celular vinculado à conta não estiver disponível ou se o dispositivo de MFA virtual tiver sido excluído do celular, entre em contato com o atendimento ao cliente para remover o dispositivo de MFA virtual.

Usuário do IAM: se o telefone celular de um usuário do IAM não estiver disponível ou se o dispositivo de MFA virtual tiver sido excluído do celular do usuário, entre em contato com o **administrador** para remover o dispositivo de MFA virtual. O administrador precisa executar as seguintes etapas:

Passo 1 Faça logon no console do IAM.

Passo 2 Na página **Users**, clique em **Security Settings** na linha que contém o usuário para o qual você deseja remover o dispositivo de MFA virtual vinculado.

Passo 3 Na página de guia **Security Settings**, clique em **Remove** na linha **Virtual MFA Device**.

Passo 4 Clique em **OK**.

----Fim

12 Exibição dos registros de operação do IAM

12.1 Ativação de CTS

O CTS registra as operações realizadas em recursos de nuvem em sua conta. Os logs de operações podem ser usados para realizar análises de segurança, rastrear alterações de recursos, realizar auditorias de conformidade e localizar falhas.

É recomendável que você ative o serviço CTS para registrar as principais operações do IAM, como criar e excluir usuários.

Procedimento

Passo 1 Faça logon no console de gerenciamento.

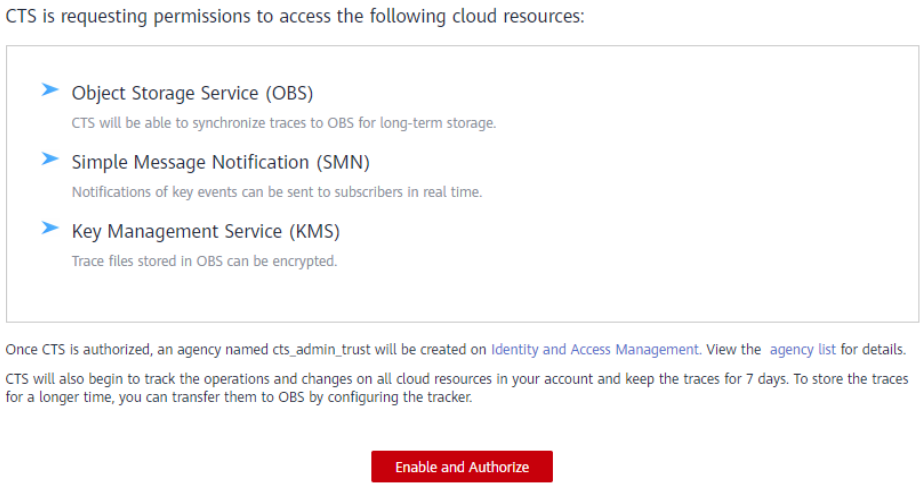
Passo 2 Se você fizer logon na Huawei Cloud usando uma conta, acesse **Passo 3**. Se você fizer logon como um usuário do IAM, solicite ao administrador que lhe conceda as seguintes permissões:

- Security Administrator
- CTS FullAccess

Para mais detalhes, consulte **3.2 Atribuição de permissões a um usuário do IAM**.

Passo 3 Escolha **Service List** > **Management & Governance** > **Cloud Trace Service**.

Figura 12-1 Ativação e autorização do CTS



Passo 4 Na página de autorização exibida, clique em **Enable and Authorize**.

NOTA

- Ao usar o CTS, você deve ter as permissões necessárias para operações relevantes, mas não precisa receber novamente a função **Security Administrator**.
- Depois de ativar o CTS, o sistema cria automaticamente dois rastreadores para registrar os traços de gerenciamento, ou seja, as operações (como criação, logon e exclusão) realizadas em todos os recursos da nuvem.
  - Na **current region**, um rastreador é criado para registrar os traços de gerenciamento de todos os serviços de nível de projeto implementados nessa região.
  - Na região **CN-Hong Kong**, um rastreador é criado para registrar os traços de gerenciamento de todos os serviços globais, como o IAM.

----Fim

O CTS registra todas as operações realizadas no IAM, como a criação de usuários e grupos de usuários. **Tabela 12-1** mostra as operações do IAM que podem ser gravadas pelo CTS.

Tabela 12-1 Operações do IAM que podem ser gravadas pelo CTS

Operação	Tipo de recurso	Nome de traços
Fazer logon	user	login
Falha no registro (falhas de logon da HUAWEI ID não incluídas)	user	loginFailed
Fazer logoff	user	logout
Fazer logon usando um código QR	user	scanQRCodeLogin

Operação	Tipo de recurso	Nome de traços
Falha no registro usando um código QR	user	scanQRCodeLoginFailed
Fazer logon via OpenID Connect	user	oidcLoginSuccess
Falha no registro via OpenID Connect	user	oidcLoginFailed
Fazer logon via SSO	user	iamUserSsoLoginSuccess
Falha no registro via SSO	user	iamUserSsoLoginFailed
Redefinir a senha	user	fpwdResetSuccess
Criar um usuário do IAM	user	createUser
Alterar o endereço de e-mail ou o número de celular	user	updateUser
Excluir um usuário	user	deleteUser
Alterar a senha	user	updateUserPwd
Definir uma senha para um usuário (pelo administrador)	user	updateUserPwd
Modificar a proteção de logon de um usuário do IAM	user	modifyLoginProtect
Alterar o número do celular usando um e-mail	user	changeMobileByEmail
Alterar a senha usando um e-mail	user	updateUserPwdByEmail
Logon inicial bem-sucedido como um usuário federado	user	tenantLoginBySamlSuccess

Operação	Tipo de recurso	Nome de traços
Logon bem-sucedido usando informações armazenadas em cache como um usuário federado	user	federationLoginNoPwdSuccess
Falha no logon usando informações armazenadas em cache como um usuário federado	user	federationLoginNoPwdFailed
Criar um grupo de usuários	userGroup	createGroup
Modificar um grupo de usuários	userGroup	updateGroup
Excluir um grupo de usuários	userGroup	deleteGroup
Adicionar usuários a um grupo de usuários	userGroup	addUserToGroup
Remover usuários de um grupo de usuários	userGroup	removeUserFromGroup
Desvincular um dispositivo de MFA virtual	MFA	UnBindMFA
Vincular um dispositivo de MFA virtual	MFA	BindMFA
Criar um projeto	project	createProject
Modificar um projeto	project	updateProject
Excluir um projeto	project	deleteProject
Criar uma agência	agency	createAgency
Modificar uma agência	agency	updateAgency
Excluir uma agência	agency	deleteAgency

Operação	Tipo de recurso	Nome de traços
Mudar de agência	agency	switchRole
Atribuir todas as permissões de projeto a uma agência	agency	updateAgencyInheritedGrants
Revogar todas as permissões de projeto de uma agência	agency	deleteAgencyInheritedGrants
Atribuir permissões de serviço global a uma agência	agency	updateAgencyAssignsByRole
Atribuir permissões de serviço global a uma agência (API)	roleAgencyDomain	assignRoleToAgencyOnDomain
Atualizar permissões de agência	agency	updateAgencyAssignsByRole
Registrar um provedor de identidade	identityProvider	createIdentityProvider
Modificar um provedor de identidade	identityProvider	updateIdentityProvider
Excluir um provedor de identidade	identityProvider	deleteIdentityProvider
Atualizar uma regra de conversão de identidade	identityProvider	updateMapping
Atualizar os metadados do provedor de identidade	identityProvider	metadataConfiguration
Editar manualmente os metadados de um IdP predefinido	identityProvider	metadataConfiguration

Operação	Tipo de recurso	Nome de traços
Registrar um mapeamento	mapping	createMapping
Atualizar um mapeamento	mapping	updateMapping
Excluir um mapeamento	mapping	deleteMapping
Registrar um protocolo	identityProvider	createProtocol
Atualizar um protocolo	identityProvider	updateProtocol
Excluir um protocolo	identityProvider	deleteProtocol
Revogar permissões de serviço global de uma agência	roleAgencyDomain	unassignRoleToAgencyOnDomain
Atribuir permissões de projeto a uma agência	roleAgencyProject	assignRoleToAgencyOnProject
Revogar permissões de projeto de uma agência	roleAgencyProject	unassignRoleToAgencyOnProject
Modificar política de autenticação de logon	SecurityPolicy	modifySecurityPolicy
Modificar a política de senha	SecurityPolicy	modifySecurityPolicy
Modificar a ACL	SecurityPolicy	modifySecurityPolicy
Modificar política de autenticação de logon	loginpolicy	securitypolicy
Modificar a política de senha	passwordpolicy	securitypolicy
Modificar a ACL	acl	securitypolicy
Criar uma conta	domain	createDomain
Atualizar uma conta	domain	updateDomain

Operação	Tipo de recurso	Nome de traços
Excluir uma conta	domain	deleteDomain
Falha no registro via OpenID Connect	domain	oidcLoginFailed
Criar uma política personalizada	Policy	createRole
Modificar uma política personalizada	Policy	updateRole
Excluir uma política personalizada	Policy	deleteRole
Atribuir permissões de serviço globais a um grupo de usuários (API)	assignment	createAssignment
Atribuir permissões de serviço globais a um grupo de usuários	group	updateGroupAssignsByRole
Revogar permissões de serviço globais de um grupo de usuários	assignment	deleteAssignment
Criar uma AK/SK permanente	credential	createCredential
Atualizar uma chave de acesso permanente (AK/SK)	credential	updateCredential
Excluir uma chave de acesso permanente (AK/SK)	credential	deleteCredential
Desativar ou ativar uma chave de acesso (AK/SK)	credential	updateCredential

Operação	Tipo de recurso	Nome de traços
Atribuir permissões a usuários ou projetos empresariais	assignment	grantRoleToUserOnEnterpriseProject
Revogar permissões de usuários ou projetos empresariais	enterpriseProject	revokeRoleFromUserOnEnterpriseProject
Atualizar permissões de grupo de usuários para projetos empresariais	enterpriseProject	updateRoleFromGroupOnEnterpriseProject
Criar um grupo de usuários	group	createGroup
Excluir um grupo de usuários	group	deleteGroup

13 Cotas

O que é uma cota?

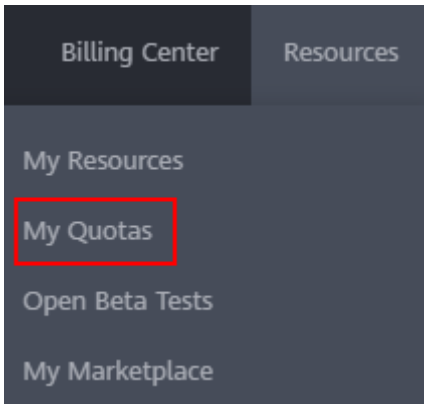
Uma cota é um limite na quantidade ou capacidade de um determinado tipo de recursos de serviço que um usuário pode usar, por exemplo, o número máximo de usuários do IAM ou grupos de usuários que você pode criar.

Se a cota de recursos atual não puder atender aos seus requisitos de serviço, você poderá solicitar uma cota mais alta.

Como visualizar minhas cotas?

1. Faça logon no console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione uma região e um projeto.
3. No canto superior direito da página, escolha **Resources** > **My Quotas**.
   A página **Quota** é exibida.

   Figura 13-1 Minhas cotas

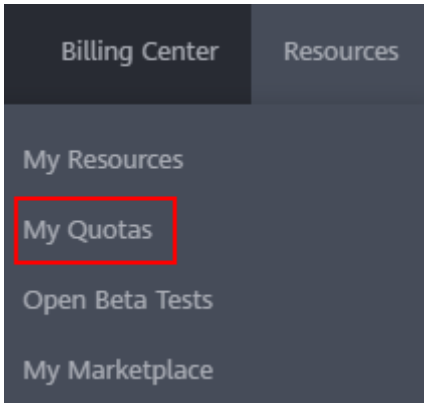
4. Clique em (o ícone **My Quotas**) no canto superior direito.
   A página **Quotas** é exibida.
5. Clique em (o ícone **My Quotas**) no canto superior direito.
   A página **Quotas** é exibida.

6. Na página **Quotas**, visualize as cotas usadas e totais de cada tipo de recurso.
   Se a cota não puder atender aos seus requisitos de serviço, aumente a cota.

Como aumentar minha cota?

1. Faça logon no console de gerenciamento.
2. No canto superior direito da página, escolha **Resources** > **My Quotas**.
   A página **Quotas** é exibida.

   Figura 13-2 Minhas cotas



3. Clique em **Increase Quota**.
4. Na página **Create Service Ticket**, defina os parâmetros.
   Na área **Problem Description**, insira a cota necessária e o motivo do ajuste da cota.
5. Leia os contratos e confirme que concorda com eles e, em seguida, clique em **Submit**.

14 Histórico de alterações

Tabela 14-1 Histórico de alterações

Lançado em	Descrição
17/06/2022	Este é o 25º lançamento oficial. Suporte a operações em lote, incluindo modificação em lote de informações sobre usuários do IAM, exclusão em lote de usuários, grupos de usuários e agências, e revogação em lote de permissões.
30/11/2021	Esta edição é o 24º lançamento oficial, que incorpora as seguintes alterações: Atualização de seções sobre autorização e políticas personalizadas com base em alterações na função de autorização.
01/11/2021	Esta edição é o 23º lançamento oficial, que incorpora as seguintes alterações: Atualização de **2 Fazer logon na Huawei Cloud** com base no novo recurso de logon da HUAWEI ID.
02/09/2021	Esta edição é o 22º lançamento oficial, que incorpora as seguintes alterações: ● Adição da seção **5.5 Registros de autorização**. ● Adição da seção **Permissões**. ● Modificação da seção **4.4 Visualização ou modificação das informações do grupo de usuários**.
16/08/2021	Esta edição é o 21º lançamento oficial, que incorpora a seguinte alteração: Adição da seção **Autogerenciamento de informações**.
22/04/2021	Esta edição é o 20º lançamento oficial, que incorpora a seguinte alteração: Adição da seção **13 Cotas**.

Lançado em	Descrição
16/04/2021	Esta edição é o 19º lançamento oficial, que incorpora a seguinte alteração: Adição da seção **Fazer logon como um usuário federado**.
27/03/2021	Esta edição é o 18º lançamento oficial, que incorpora a seguinte alteração: Atualização de **2 Fazer logon na Huawei Cloud** com base no novo recurso de logon da HUAWEI ID.
24/03/2021	Esta edição é o 17º lançamento oficial, que incorpora a seguinte alteração: Adição da seção **5.6.4 Serviços de nuvem que suportam a autorização em nível de recurso usando o IAM**.
30/12/2020	Esta edição é o 16º lançamento oficial, que incorpora as seguintes alterações: Atualização do documento com base em alterações na página de logon, na função de configurações de segurança e nas cadeias da interface do usuário.
26/11/2020	Esta edição é o 15º lançamento oficial, que incorpora a seguinte alteração: Modificação de seção **8 Configurações de segurança** com base nas alterações do console.
05/11/2020	Esta edição é o 14º lançamento oficial, que incorpora as seguintes alterações: ● Ajuste da estrutura de **9 Provedores de identidade**. ● Adição da seção **9.5.1 Visão geral do SSO de usuário virtual via OpenID Connect**.
26/10/2020	Esta edição é o 13º lançamento oficial, que incorpora a seguinte alteração: Atualização das capturas de tela da página de logon com base na alteração do método de logon.
11/09/2020	Esta edição é o 12º lançamento oficial, que incorpora a seguinte alteração: Modificação de seção **3 Usuários do IAM** com base nas alterações do console.
18/08/2020	Esta edição é o 11º lançamento oficial, que incorpora a seguinte alteração: Adição da seção **2 Fazer logon na Huawei Cloud**.

Lançado em	Descrição
20/04/2020	Esta edição é o 10º lançamento oficial, que incorpora as seguintes alterações: Adição de descrições sobre a remoção de usuários em **4.2 Adição ou remoção de usuários de um grupo de usuários**. Adição da seção **4.5 Revogação de permissões de um grupo de usuários**.
30/03/2020	Esta edição é o 9º lançamento oficial, que incorpora a seguinte alteração: Exclusão de descrições do teste beta aberto para controle de acesso baseado em políticas. Esta função está atualmente em uso comercial.
10/02/2020	Esta edição é o 8º lançamento oficial, que incorpora as seguintes alterações: Adição da seção **5.4 Alterações nos nomes de política definidos pelo sistema**. Modificação de seção **4.1 Criação de um grupo de usuários e atribuição de permissões** com base nas alterações de nome da política.
20/01/2020	Esta edição é o 7º lançamento oficial, que incorpora as seguintes alterações: Modificação das seguintes seções com base nas alterações do console: **4 Grupos de usuários e autorização** e **5 Gerenciamento de permissões**
20/11/2019	Esta edição é o 6º lançamento oficial, que incorpora as seguintes alterações: Adição de **Pontos de extremidade da VPC** em **8.6 ACL**. Adição de **Ativação/desativação de uma chave de acesso** em **3.7 Gerenciamento de chaves de acesso para um usuário do IAM**.
15/10/2019	Esta edição é o 5º lançamento oficial, que incorpora as seguintes alterações: Adição da seção **5.6.2 Modificação ou exclusão de uma política personalizada**. Adição de descrições sobre a criação de políticas personalizadas no editor visual em **5.6.1 Criação de uma política personalizada**. Adição de descrições sobre a sintaxe para políticas usadas para atribuir permissões de nível de recurso e condição em **5.3 Políticas** e **5.6.3 Casos de uso de políticas personalizadas**.

Lançado em	Descrição
29/09/2019	Esta edição é o 4º lançamento oficial, que incorpora a seguinte alteração: Adição da seção **10 Agente identificador personalizado**.
11/06/2019	Esta edição é o 3º lançamento oficial, que incorpora a seguinte alteração: Otimização de capítulos **1 Antes de começar**, **3 Usuários do IAM**, **4 Grupos de usuários e autorização**, **5 Gerenciamento de permissões**, **6 Projetos**, **8 Configurações de segurança** e **12 Exibição dos registros de operação do IAM**.
13/02/2018	Esta edição é o 2º lançamento oficial, que incorpora a seguinte alteração: Adição de uma tabela que descreve os tipos de agência em **7 Agências**.
30/12/2017	Esta edição é o 1º lançamento oficial.

