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

Público-alvo

O serviço Identity and Access Management (IAM) destina-se a administradores, incluindo:

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

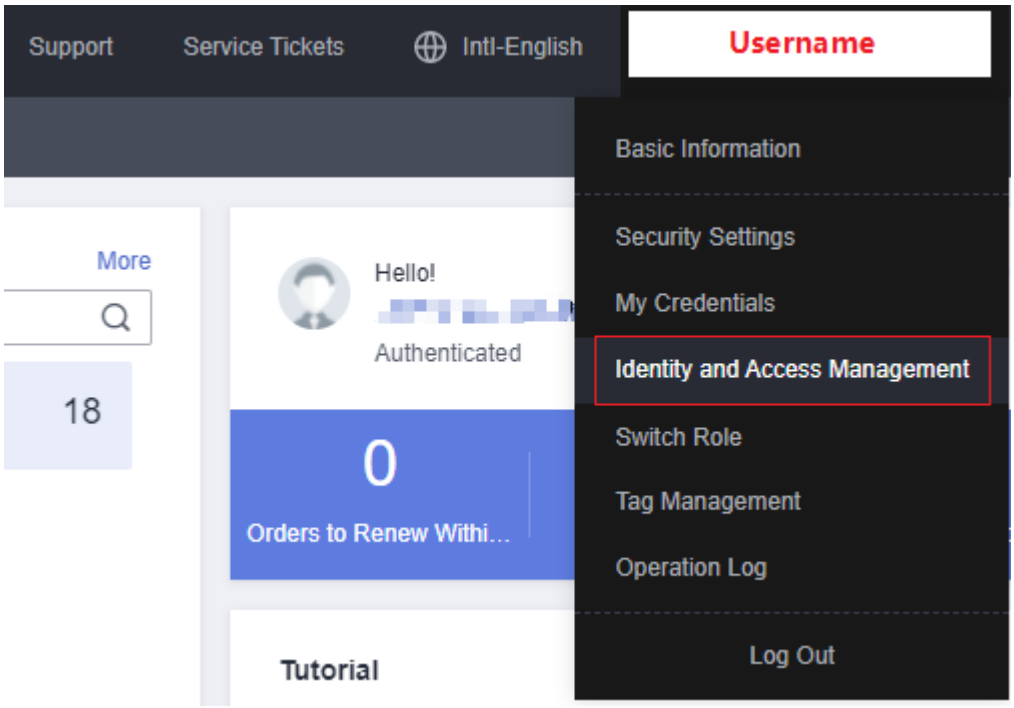
Se você quiser exibir, auditar e rastrear os registros das principais operações realizadas no IAM, ative o Cloud Trace Service (CTS). Para obter detalhes, consulte **12.1 Habilitação do CTS**.

Acesso do console do IAM

Passo 1 Faça login na HUAWEI CLOUD e clique em **Console** no canto superior direito.

Figura 1-1 Acesso do console

Passo 2 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.



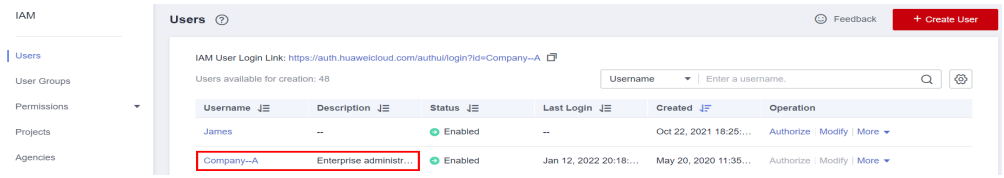
----Fim

Conta

Uma conta é criada depois de você se registrar com sucesso na HUAWEI CLOUD. Sua conta tem permissões de acesso totais dos seus recursos e efetuar pagamentos para uso desses recursos. Você não pode modificar ou excluir sua conta no IAM, mas pode fazê-lo em Minha Conta.

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

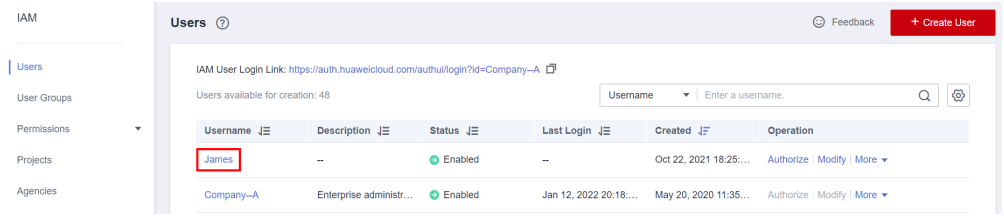
Figura 1-2 Usuário do IAM correspondente à conta



Usuário do IAM

Você e outros administradores podem criar usuários no IAM e atribuir permissões para recursos específicos. Conforme mostrado na figura a seguir, **James** é um usuário do IAM criado por um administrador. Os usuários do IAM podem fazer login na HUAWEI CLOUD usando seu nome de conta, nome de usuário e senha e, em seguida, usar recursos com base nas permissões atribuídas. Os usuários do IAM não possuem recursos e não podem fazer pagamentos.

Figura 1-3 Usuário do IAM criado pelo administrador

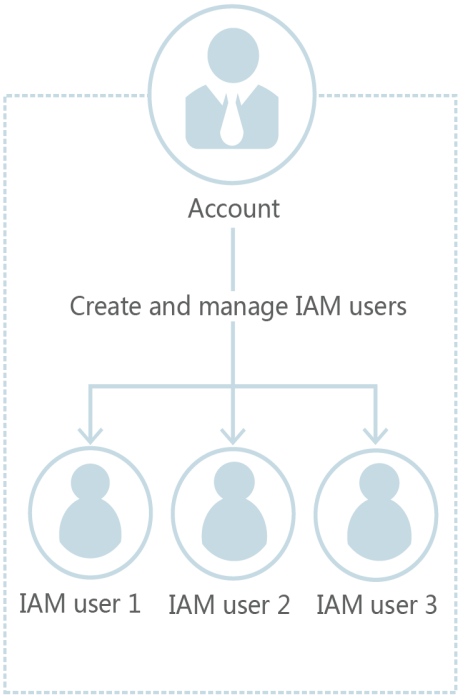


Relação entre uma conta e seus usuários do IAM

Uma conta e seus usuários do IAM compartilham uma relação pai-filho. A conta é proprietária dos recursos e faz pagamentos dos recursos usados pelos usuários do IAM. Ele tem permissões completas para esses recursos.

Os usuários do IAM são criados pelo administrador da conta, e têm apenas as permissões concedidas pelo administrador. O administrador pode modificar ou cancelar as permissões dos usuários do IAM em qualquer momento. As taxas geradas pelo uso de recursos pelos usuários do IAM são pagas pela conta.

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

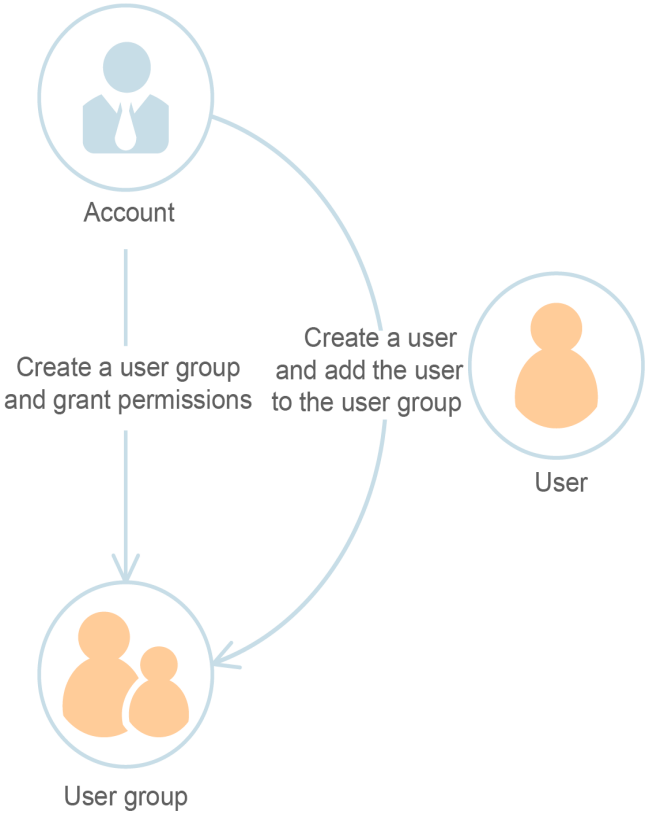


Grupo de usuários

Você pode usar grupos de usuários para atribuir permissões a usuários do IAM. Depois de um usuário do IAM ser 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 na nuvem. Os usuários desse grupo podem executar operações em todos os recursos, incluindo, mas não limitado a, criar grupos de usuários e usuários, modificar permissões e gerenciar recursos.

Figura 1-5 Grupo de usuários



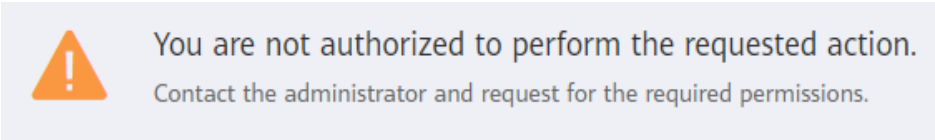
Permissão

O IAM fornece permissões comuns de serviços diferentes, como permissões de administrador e somente leitura, que você pode atribuir aos usuários. Por padrão, os novos usuários do IAM não têm permissões. Para atribuir permissões a novos usuários, 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 pertencem e 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 a escolha ideal para autorização refinada e controle de acesso seguro.
- Políticas: um tipo de mecanismo de autorização refinado que define as permissões necessárias para executar operações em recursos de nuvem específicos sob certas condições. Esse mecanismo permite uma autorização baseada em política mais flexível com base em um princípio do privilégio mínimo (PoLP). Por exemplo, você pode conceder aos usuários do (ECS Elastic Cloud Server) somente as permissões necessárias para gerenciar um determinado tipo de recursos ECS.

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

Figura 1-6 Sem permissões



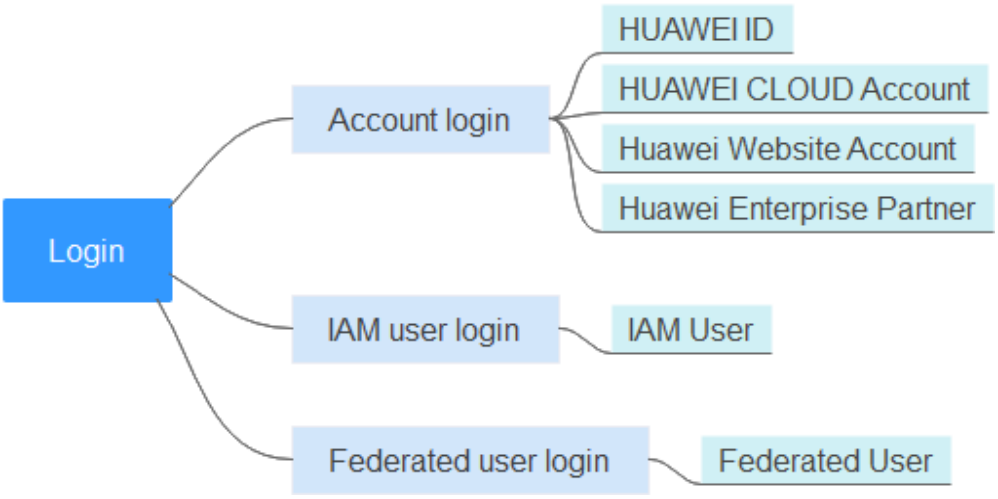
2 Faça login na HUAWEI CLOUD

Você pode fazer login na HUAWEI CLOUD usando qualquer um dos seguintes métodos (consulte **Figura 2-1**):

- **Login da conta**: Faça login com a conta que foi criada quando você usa a HUAWEI CLOUD pela primeira vez. Sua conta tem permissões de acesso total dos seus recursos na nuvem e efetuar pagamentos para uso desses recursos. Se fizer login na HUAWEI CLOUD utilizando uma conta, faça o seguinte:
  - **HUAWEI ID**: Seu HUAWEI ID é uma identidade única que você pode usar para acessar todos os serviços da Huawei. É **diferente de uma conta HUAWEI CLOUD**. Certifique-se de que você já registrou um HUAWEI ID. Se você não tiver um HUAWEI ID, crie um e use-o para habilitar os serviços da HUAWEI CLOUD. Para obter detalhes, consulte **Registro de um HUAWEI ID e habilitação dos serviços da HUAWEI CLOUD**.
  - **Digitalize o código QR para fazer login**: Se você fez login na aplicação HUAWEI CLOUD com uma conta ou como um usuário do IAM, você pode digitalizar o código QR na página de login para fazer login na HUAWEI CLOUD sem inserir as informações da conta novamente.
  - **Conta da HUAWEI CLOUD**: Utilize a sua conta da HUAWEI CLOUD para fazer login. Se esta for a primeira vez que você usa a HUAWEI CLOUD, **registre um HUAWEI ID e habilite os serviços da HUAWEI CLOUD**.
  - **Outras contas**: Ao fazer login usando **uma conta do site da Huawei** ou **uma conta de parceiro empresarial da Huawei** pela primeira vez, associe essas contas a uma conta existente ou uma nova da HUAWEI CLOUD. No próximo login, você pode fazer login diretamente usando a conta do site da Huawei ou a conta de parceiro empresarial da Huawei. Alternativamente, você pode usar a conta da HUAWEI CLOUD para fazer login.
- **Login do usuário do IAM**: 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** compartilham um relacionamento pai-filho. Os usuários do IAM só podem usar serviços de nuvem específicos com base nas permissões atribuídas.
  - **Digitalize o código QR para fazer login**: Se você fez login na aplicação HUAWEI CLOUD com uma conta ou como um usuário do IAM, você pode digitalizar o código QR na aplicação para fazer login na HUAWEI CLOUD.
- **Login de usuário federado**: Os usuários federados são registrados com um provedor de identidade empresarial criado pelo **administrador** no IAM.

– **Usuário federado**: Você pode fazer login 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 login no seu sistema de gerenciamento corporativo.

Figura 2-1 Fazer login na HUAWEI CLOUD usando diferentes contas



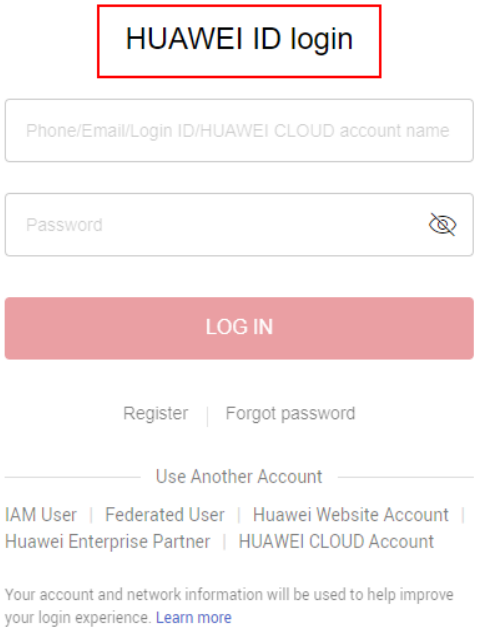
Fazer login usando um HUAWEI ID

Seu HUAWEI ID é uma identidade única que você pode usar para acessar todos os serviços da Huawei. Você pode registrar e gerenciar um HUAWEI ID no **site do HUAWEI ID**. Você pode também **registrar um HUAWEI ID e usá-lo para habilitar os serviços da HUAWEI CLOUD** na HUAWEI CLOUD. Ao fazer login no console da HUAWEI CLOUD usando um HUAWEI ID, você pode inserir um número de celular, endereço de e-mail, ID de login ou nome de conta da HUAWEI CLOUD.

Para fazer login usando um HUAWEI ID, faça o seguinte:

Passo 1 Na página de fazer login, insira o seu número de celular, endereço de e-mail, ID de login ou nome de conta da HUAWEI CLOUD, insira a senha e clique em **LOG IN**.

Figura 2-2 Fazer login usando um HUAWEI ID



NOTA

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

Passo 2 Selecione a conta que você deseja usar para fazer login.

Se o número de celular ou endereço de e-mail que você inseriu tiver sido usado para registrar um HUAWEI ID e uma conta da HUAWEI CLOUD, selecione uma conta para fazer login.

- Selecione o HUAWEI ID desejado e clique em **OK**. Então, acesse **Passo 3**.
- Selecione a conta da HUAWEI CLOUD e clique em **OK**. O login foi bem-sucedido.

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

Se você já associou um número de celular e um endereço de e-mail ao seu HUAWEI ID, você pode escolher verificação pelo número de celular ou 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 habilitar os serviços da HUAWEI CLOUD para o HUAWEI ID, para que possa utilizar o HUAWEI ID para fazer login na HUAWEI CLOUD. Depois de clicar neste botão, acesse **Passo 6**.
- **Use Another HUAWEI CLOUD Account**: Clique neste botão para fazer login usando outra conta da HUAWEI CLOUD. Depois de clicar neste botão, acesse **Passo 1**.

Passo 6 (Opcional) Se o número de celular ou endereço de e-mail que você inseriu tiver sido usado para registrar contas da HUAWEI CLOUD, selecione uma conta e associe-a ao seu HUAWEI ID.

NOTA

Depois de associar uma conta da HUAWEI CLOUD ao seu HUAWEI ID, você pode usar o HUAWEI ID para acessar a HUAWEI CLOUD, o HUAWEI Developers, o Vmall e outros serviços da Huawei.

- Associação de uma conta da HUAWEI CLOUD ao seu HUAWEI ID
  a. Selecione a conta da HUAWEI CLOUD e clique em **Next**.
  b. Insira a senha da conta da HUAWEI CLOUD e clique em **Next**.
  c. Confirme as informações do HUAWEI ID e clique em **OK**.
  d. Clique em **OK**. A página incial da HUAWEI CLOUD é exibida.

  NOTA

  - Depois de executar as etapas anteriores, sua conta da HUAWEI CLOUD é associada ao seu HUAWEI ID e se torna inválido. Você precisa usar o HUAWEI ID para o próximo login.
  - Se a atualização falhar, consulte "O que posso fazer se a atualização para um HUAWEI ID falhar?" nas *Perguntas frequentes do IAM*.
- Habilitação dos serviços da HUAWEI CLOUD

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

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

Agora você pode usar o HUAWEI ID para fazer login na HUAWEI CLOUD.

----Fim

Digitalização do código QR para fazer login

A aplicação HUAWEI CLOUD é um cliente móvel da HUAWEI CLOUD. Com a aplicação HUAWEI CLOUD, você pode gerenciar seus recursos da HUAWEI CLOUD no seu celular. Se você fez login na aplicação HUAWEI CLOUD usando uma conta ou como um usuário do IAM, você pode digitalizar o código QR na página de login para fazer login na HUAWEI CLOUD sem inserir informações da conta novamente.

NOTA

A aplicação HUAWEI CLOUD não suporta o login usando uma conta do site internacional da HUAWEI CLOUD. Portanto, você não pode digitalizar o código QR para fazer login.

Para fazer login digitalizando um código QR, faça o seguinte:

Passo 1 Na página de login da HUAWEI CLOUD, clique em **Scan to Log In** no canto superior direito.

Figura 2-3 Digitalização do código QR para fazer login

Passo 2 Use a aplicação HUAWEI CLOUD para digitalizar o código QR para fazer login na HUAWEI CLOUD.

----Fim

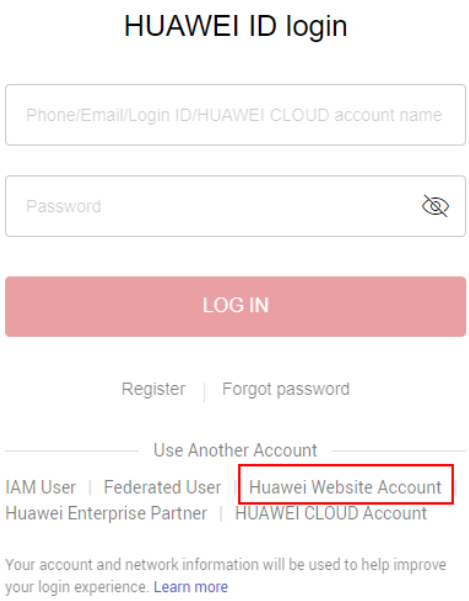
Fazer login usando outras contas

Se você já tem uma **conta do site da Huawei** ou uma **conta de parceiro empresarial da Huawei**, poderá usá-las para fazer login na HUAWEI CLOUD sem memorizar credenciais adicionais.

O procedimento a seguir descreve como usar uma conta do site oficial da Huawei para fazer login na HUAWEI CLOUD.

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

Figura 2-4 Fazer Login usando uma conta do site da Huawei



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

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

Da próxima vez que você fizer login no console da HUAWEI CLOUD, poderá usar o nome ou número de celular definido em **Passo 2** para a conta da HUAWEI CLOUD.

----Fim

Fazer login usando uma conta da HUAWEI CLOUD

Se tiver uma conta da HUAWEI CLOUD, pode usá-la para fazer login 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 login no console da HUAWEI CLOUD, você pode escolher fazer login por conta/e-mail ou por número de celular.

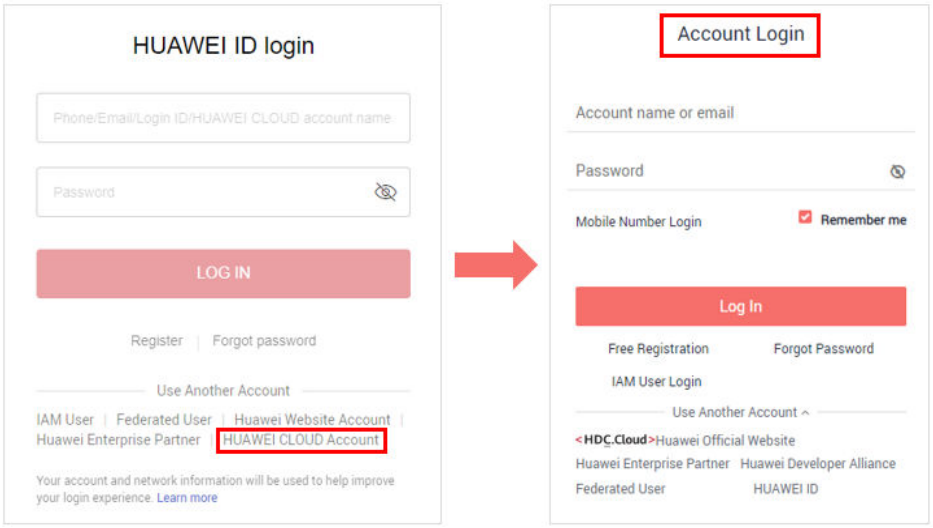
NOTA

Se a sua conta HUAWEI CLOUD tiver sido atualizada para um HUAWEI ID, use o HUAWEI ID para fazer login. Para obter detalhes, consulte **Fazer login usando um HUAWEI ID**.

Para fazer login usando uma conta da HUAWEI CLOUD, faça o seguinte:

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

Figura 2-5 Fazer login 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 associado à conta.

  NOTA

  Os nomes das contas não diferenciam maiúsculas e minúsculas.

- **Password**: A senha de login da conta. Se você esqueceu sua senha de login, **redefina-a** na página de login.
- **Mobile number**: Se você esqueceu o nome da conta, clique em **Mobile Number Login** e insira o número de celular associado e a senha de login para fazer login.

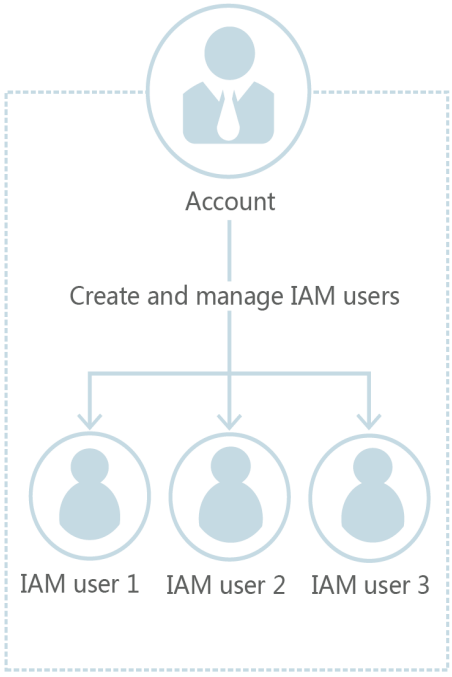
----Fim

Fazer login 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 (senha e chaves de acesso) e usa recursos de nuvem com base nas permissões atribuídas. Os usuários do IAM não possuem recursos e não podem fazer pagamentos.

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

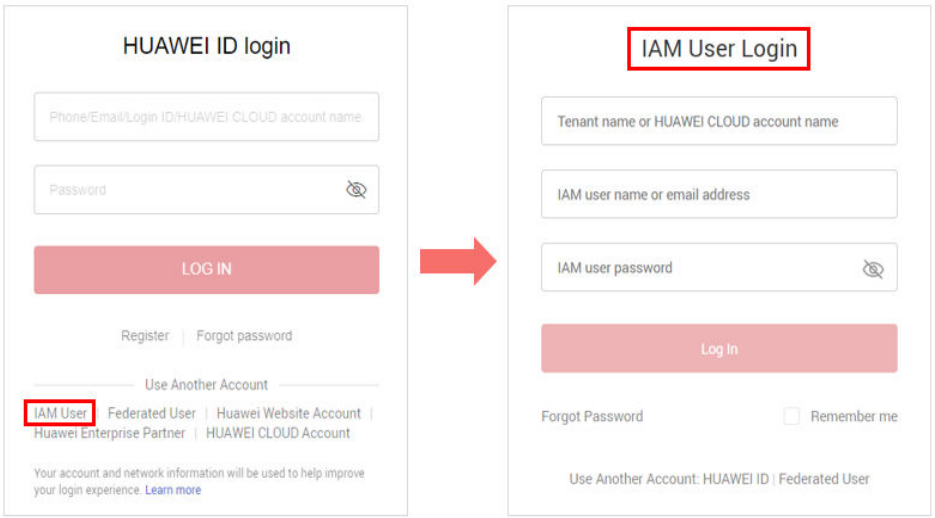
Figura 2-6 Conta e usuários do IAM



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

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

Figura 2-7 Fazer login 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, ou seja, a **conta** da HUAWEI CLOUD. 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 senha do **administrador**.

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

Passo 2 Clique em **Log In**.

----Fim

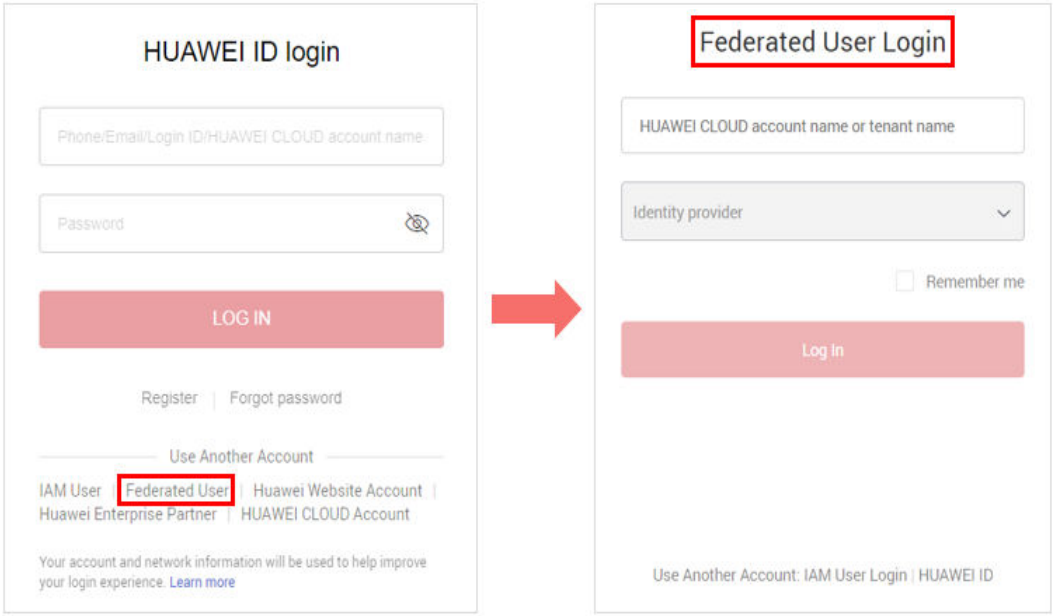
Fazer login como um usuário federado

Os usuários federados são criados em um sistema de gerenciamento empresarial. Depois de o administrador da conta **criar um provedor de identidade** no console do IAM, os usuários federados podem fazer login na HUAWEI CLOUD e usar os serviços em nuvem com base nas permissões atribuídas. Para obter mais detalhes, consulte **9.1 Introdução**.

Você pode fazer login na HUAWEI CLOUD como um usuário federado se tiver obtido o nome do provedor de identidade, a conta da HUAWEI CLOUD usada para criar o provedor de identidade e o nome de usuário e a senha para fazer login no seu sistema de gerenciamento empresarial.

Passo 1 Na página de fazer login da HUAWEI CLOUD, clique em **Federated User**, insira o nome da conta e selecione um provedor de identidade.

Figura 2-8 Fazer login como um usuário federado



- **HUAWEI CLOUD account name or tenant name**: O nome da conta da HUAWEI CLOUD 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 login do sistema de gerenciamento empresarial é exibida.

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

Passo 4 Clique no botão de login.

----Fim

3 Usuários do IAM

3.1 Criação de um usuário do IAM

Se você é um **administrador** e comprou 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 concedendo a eles as permissões necessárias para realizar operações em recursos específicos. Você não precisa compartilhar a senha da sua conta.

Por padrão, **os novos usuários do IAM não têm permissões**. Você pode 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 realizar 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 na nuvem. Os usuários desse grupo podem executar operações em todos os recursos, incluindo, mas não limitado a, criar grupos de usuários e usuários, modificar permissões e gerenciar recursos.

NOTA

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

Procedimento

Passo 1 Faça login 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 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 de cada vez.

Tabela 3-1 Detalhes do usuário

Parâmetro	Descrição
Nome do usuário	Esse parâmetro é definido pelo usuário e não pode ser igual ao de qualquer outra conta ou usuário do IAM conta .
Endereço de e-mail	Esse parâmetro é definido pelo usuário e não pode ser igual ao de qualquer outra conta ou usuário do IAM conta . Ele pode ser usado para autenticar o usuário do IAM e redefinir a senha.
Número de celular	Esse parâmetro é definido pelo usuário e não pode ser igual ao de qualquer outra conta ou usuário do IAM da conta. Ele pode ser usado para autenticar o usuário do IAM e redefinir a senha.
ID de identidade externa	Se você quiser configurar a **Autenticação de identidade federada baseada em SAML** para um usuário do IAM, o **ID de identidade externa** com o máximo 128 caracteres é obrigatório.

Passo 4 Selecione **Access Type**.

Tabela 3-2 Tipos de acesso

Tipo de acesso	Descrição
Acesso programático	Permite que os usuários acessem serviços de nuvem usando ferramentas de desenvolvimento, como APIs, CLI e SDKs.
Acesso ao console de gerenciamento	Permite que os usuários acessem serviços de nuvem por meio do console de gerenciamento. Uma senha é obrigatória para fazer o login.

Passo 5 Especifique **Credential Type**.

Tabela 3-3 Tipos de credencial

Tipo de credencial		Descrição
Chave de acesso		Depois de criar o usuário, você pode fazer o download da **chave de acesso (AK/SK)** gerada para o usuário. **Cada usuário pode ter no máximo duas chaves de acesso.**
Senha	Definir agora	Defina uma senha para o usuário e determine se deve exigir que o usuário redefina a senha no primeiro login. Se você for o usuário, selecione esta opção e defina uma senha para fazer login. Você não precisa selecionar **Require password reset at first login**.
	Gerado automaticamente	O sistema gera automaticamente uma senha de login para o usuário. Depois de o usuário ser criado, você pode fazer o download do arquivo de senha de EXCEL e fornecer a senha para o usuário. O usuário pode então usar essa senha para fazer login. **Essa opção está disponível somente quando você cria um único usuário.**
	Definida pelo usuário	Uma URL de login único será enviada ao usuário. O usuário pode clicar no link para fazer login no console e definir uma senha. Se você não usar o usuário do IAM, selecione essa opção e insira o endereço de e-mail e o número de celular do usuário do IAM. O usuário pode então definir uma senha clicando na URL de login único enviada por e-mail. A URL de login é válida por **sete dias**.

Tabela 3-4 Configurações recomendadas

Acesso ao console de gerenciamento	Acesso programático	Tipo de credencial	Tipo de acesso recomendado	Tipo de credencial recomendado
√	×	Não há nenhuma exigência especial.	Acesso ao console de gerenciamento	Senha
×	√	Não há nenhuma exigência especial.	Acesso programático	Chave de acesso
×	√	**Uma senha é necessária como uma credecial do acesso programático** (exigida por algumas APIs).	Acesso programático	Senha

Acesso ao console de gerenciamento	Acesso programático	Tipo de credencial	Tipo de acesso recomendado	Tipo de credencial recomendado
√	×	**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 Cloud Data Migration (CDM).	Acesso programático e acesso ao console de gerenciamento	Senha e chave

Passo 6 Configurar a proteção de login. Esse parâmetro só estará disponível quando você selecionou **Management console access** para **Access Type**.

- **Enable (Recommend)**: O usuário precisa inserir um código de verificação além do nome do usuário e senha durante o login. Habilitar esta função para a segurança da conta.

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

Passo 7 Clique em **Next**. Selecione o grupo de usuários ao qual o usuário será adicionado e adicione o usuário ao grupo de usuários. O usuário terá as permissões atribuídas ao grupo de usuários.

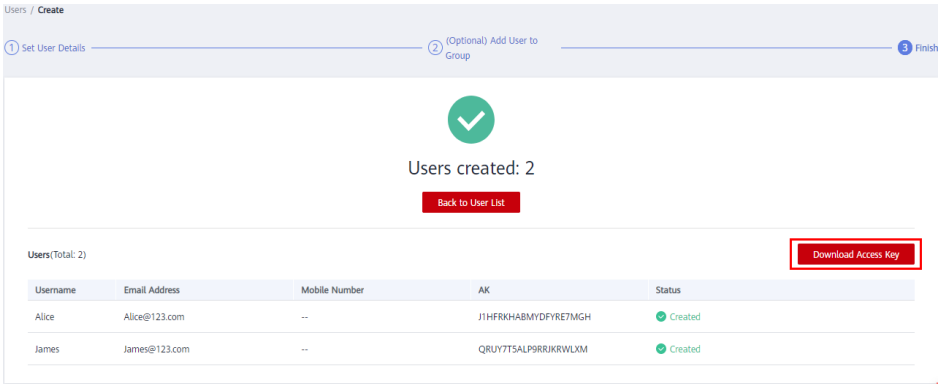
NOTA

- Você também pode criar um novo grupo e adicionar o usuário a esse grupo.
- Se o usuário for um administrador, adicione o usuário 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 **5**, você pode fazer o download da chave de acesso na página **Finish**.
- Se você selecionou **Password** > **Automatically generated** para **Credential Type** em **Passo 4**, você pode fazer o download do arquivo de senha na página **Finish**.

Figura 3-1 Usuários criados com êxito



----Fim

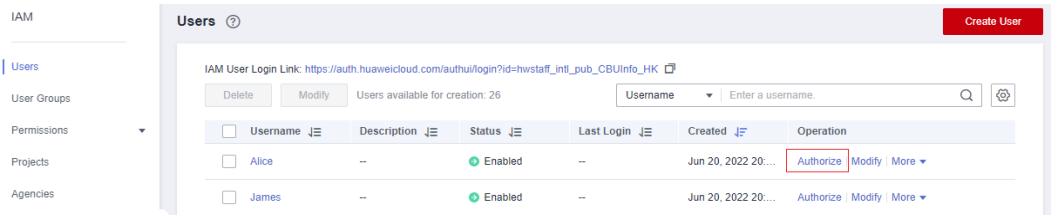
3.2 Atribuição de permissões a um usuário do IAM

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

Procedimento

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

Figura 3-2 Atualização de um usuário do IAM

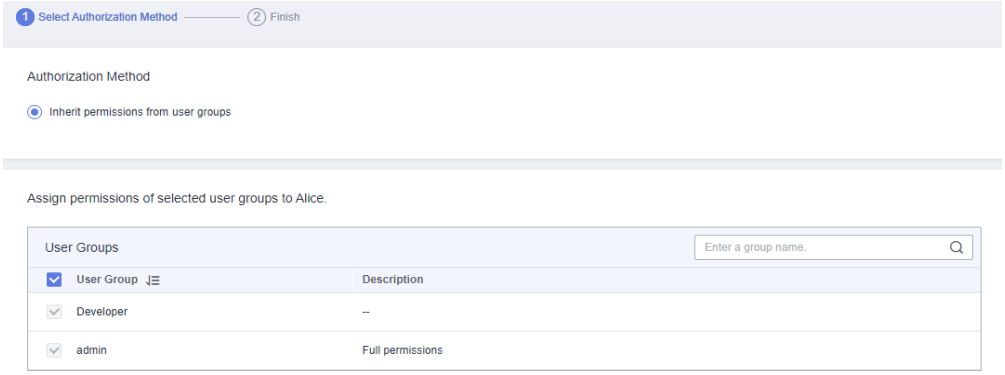


Passo 2 Na página **Authorize User**, selecione um modo de autorização e permissões.

- **Inherit permissions from user groups**: adicione 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.

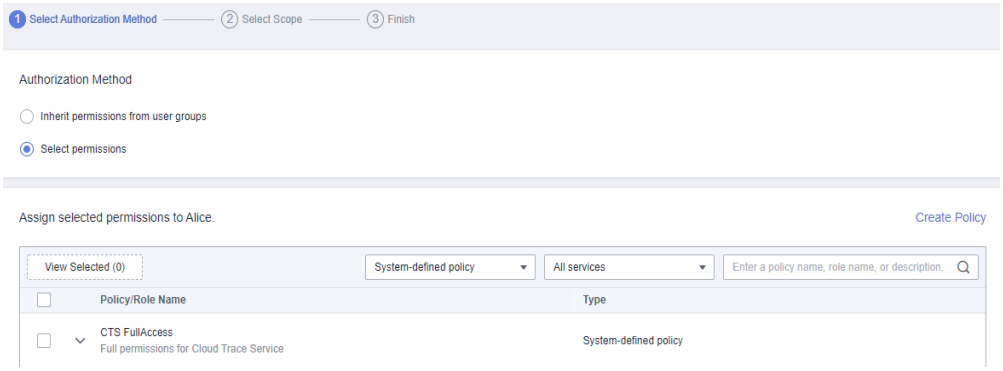
Figura 3-3 Função do projeto empresarial não ativada



- **Permissões selecionadas**: Atribua permissões específicas diretamente ao usuário do IAM. Essa opção estará disponível somente quando você tiver ativado a função de projeto empresarial. Para obter as informações sobre como habilitar a função de projeto empresarial, consulte **Habilitação da função do projeto empresarial**.

  Se você selecionar essa opção, selecione permissões, clique em **Next** no canto inferior direito e acesse **Passo 3**.

Figura 3-4 Função do projeto empresarial ativada



NOTA

- Se você adicionar um usuário do IAM ao grupo **admin** padrão, 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 todas as permissões que foram atribuídas a esses grupos.
- **Para obter detalhes sobre as permissões do sistema de todos os serviços de nuvem suportados pelo IAM, consulte Permissões do sistema.**
- Se você ativou o Gerenciamento empresarial, não poderá criar projetos no IAM.

Passo 3 Na página **Select Scope**, selecione os projetos corporativos que o usuário do IAM pode acessar. Você não precisa executar esse passo se tiver selecionado **Inherit permissions from user groups**.

Passo 4 Clique em **OK**.

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

----Fim

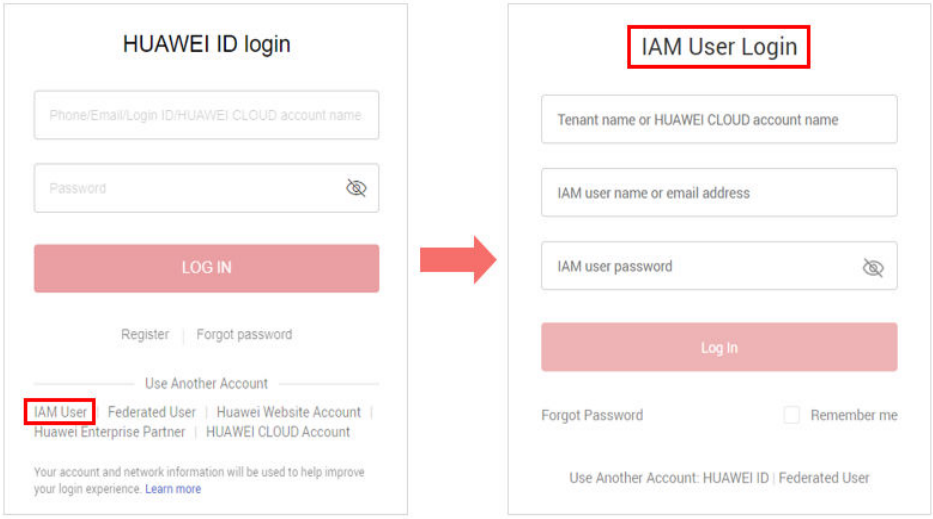
3.3 Fazer login como um usuário do IAM

Você pode fazer login na HUAWEI CLOUD como um usuário do IAM clicando em **IAM User** na página de login ou usando o link de login do usuário do IAM.

Método 1: Fazer login clicando em usuário do IAM

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

Figura 3-5 Fazer login 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, ou seja, a **conta** da HUAWEI CLOUD. 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 senha do **administrador**.
- **IAM user password**: A senha do usuário do IAM (não é 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 de usuários a ou remoção de usuários de um grupo de usuários**).
- Se você foi adicionado ao administrador de grupo **admin** padrão, você tem permissões de administrador e pode executar todas as operações em todos os serviços de nuvem.

----Fim

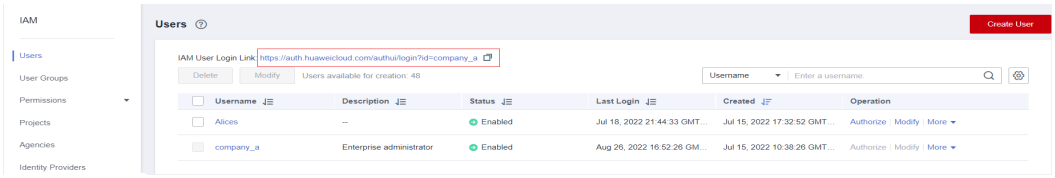
Método 2: Fazer login usando o link de fazer login do usuário do IAM

Você pode obter o link de login do usuário do IAM do administrador e, em seguida, efetuar login usando esse link. Quando você visita o link, o sistema exibe a página de login e

preenche automaticamente o nome da conta. Você só precisa inserir seu nome de usuário e senha.

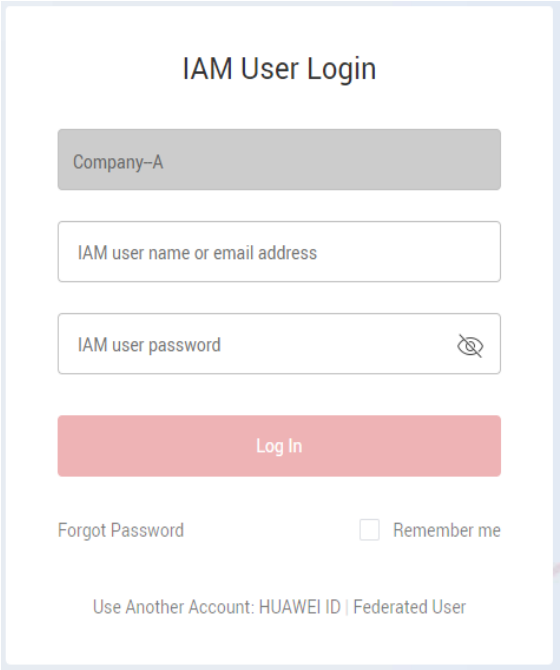
Passo 1 Obtenha o link de login do usuário do IAM do administrador.

Figura 3-6 Link de login 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 e a senha do IAM e clique em **Log In**.

Figura 3-7 Fazer login usando o link de fazer login do usuário do IAM

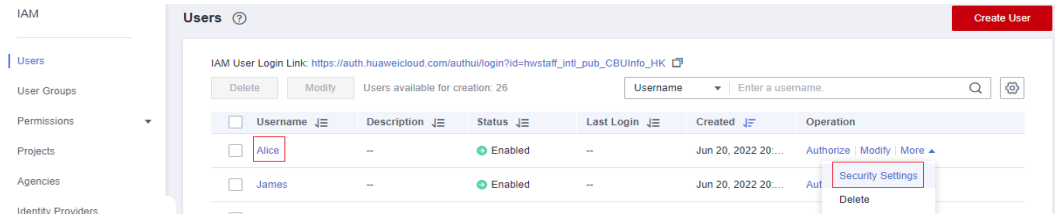


----Fim

3.4 Exibição ou modificação das informações do usuário do IAM

Como um 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 exibir ou excluir as permissões atribuídas. Para exibir ou modificar informações do usuário, clique em **Security Settings** na linha que contém o usuário do IAM.

Figura 3-8 Acesse a página de configurações de segurança do usuário do IAM

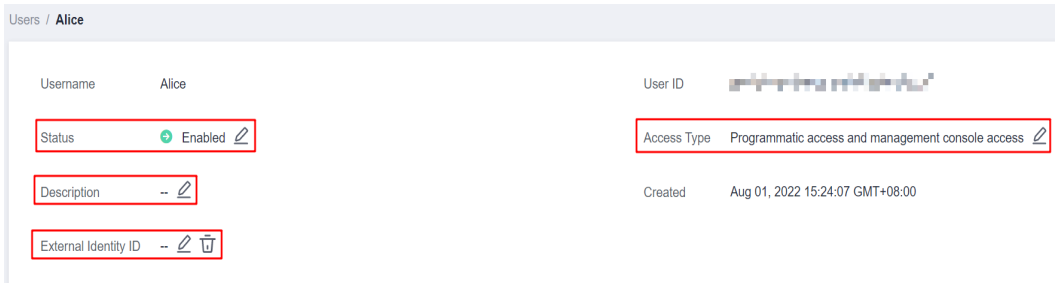


Para ajustar as colunas do item exibidas na lista, clique em  . As colunas **Username** e **Operation** são exibidas por padrão, e a coluna **Status** não pode ser removida. Você também pode selecionar **Description**, **Last Login**, **Created**, **Access Type**, **Virtual MFA Status**, **Password Age**, e **Access Key (Status, Age, and AK)**, e **External Identity ID**.

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 3-9 Modificação do status, do tipo de acesso, da descrição e do ID de identidade externo de um usuário do IAM



- **Status**: Novos usuários do IAM são ativados por padrão. Você pode definir **Status** como **Disabled** para desabilitar um usuário do IAM. Um usuário com deficiência deixa de fazer login na HUAWEI CLOUD por meio do console de gerenciamento ou do acesso programático.
- **Access Type**: Você pode alterar os tipos de acesso de cada 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 os 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** quando usar determinados serviços no console, como a criação de um trabalho de migração de dados no console do CDM (Cloud Data Migration), 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 ambos **Programmatic access** e **Management console access**, desmarque **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 no login federado usando SSO.

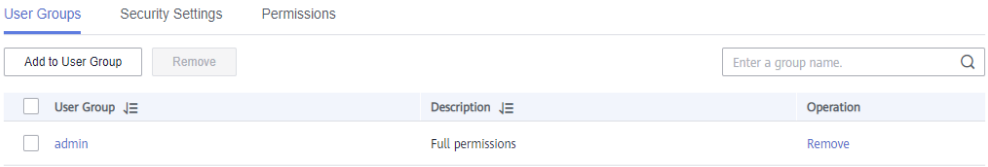
Grupos de usuários

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 Exibição ou modificação das informações do grupo de usuários**.

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

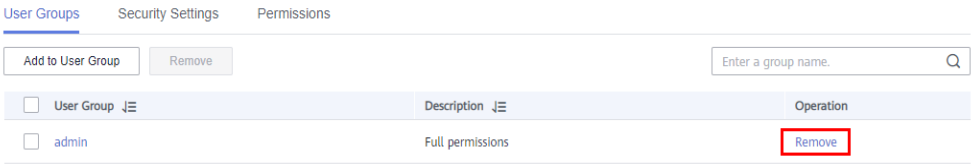
- Clique em **Add to User Groups** e selecione um ou mais grupos aos quais o usuário pertencerá. O usuário então herda as permissões desses grupos.

Figura 3-10 Adição do usuário a grupos de usuários



- Clique em **Remove** à direita do grupo de usuários e clique em **Yes**. O usuário deixa de ter as permissões atribuídas ao grupo.

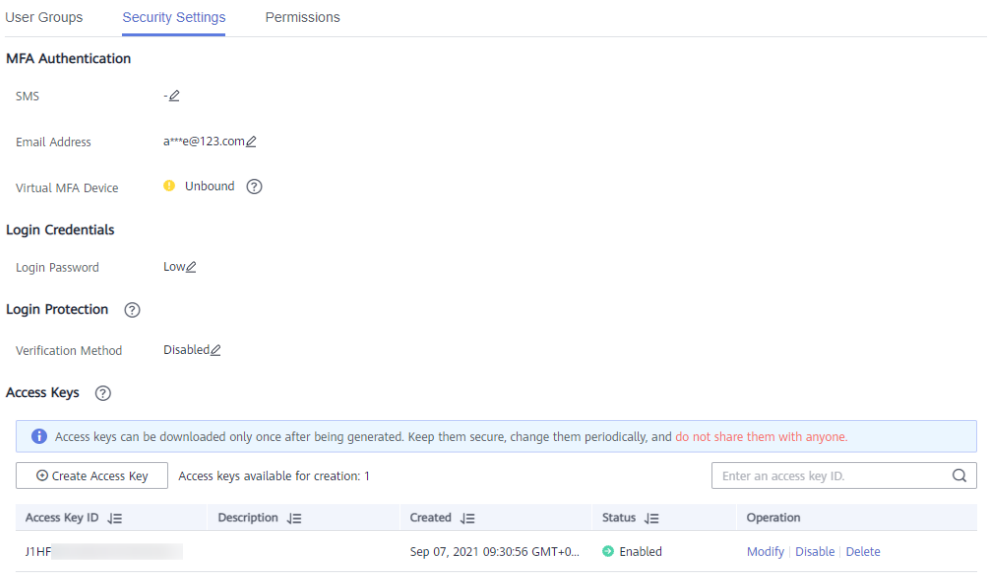
Figura 3-11 Remoção do usuário de um grupo de usuários



Configurações de segurança

Como um administrador, você pode modificar o dispositivo MFA, a credencial de login, a proteção de login 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 MFA virtual, consulte **8.1 Visão geral das configurações de segurança**.

Figura 3-12 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 o número de celular ou o endereço de e-mail do usuário.

    NOTA

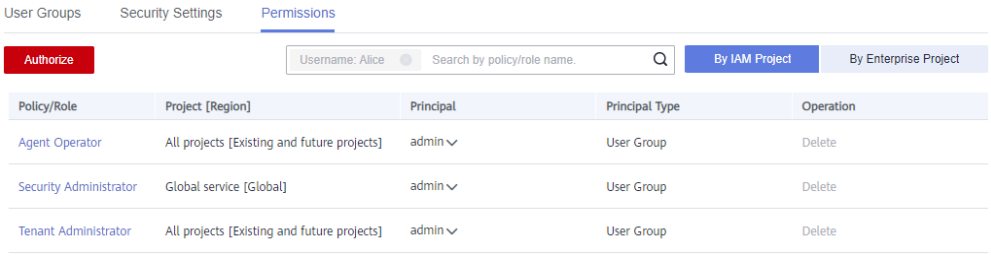
    O número de celular e o endereço de e-mail do usuário do IAM não podem ser iguais aos da sua conta ou de outros usuários do IAM.
  - Remova o dispositivo MFA do usuário. Para obter mais informações sobre autenticação de MFA e dispositivo MFA virtual, consulte **11 Autenticação MFA e dispositivo MFA virtual**.
- **Login Credentials**: Você pode alterar as senhas do login do usuário do IAM. Para obter mais informações, consulte **3.6 Alteração da senha de login de um usuário do IAM**.
- **Login Protection**: Você pode alterar os médotos de verificação do login do usuário do IAM. Três métodos de verificação estão disponíveis: dispositivo MFA virtual, SMS e e-mail.

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

Permissões

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

Figura 3-13 Permissões atribuídas a um usuário do IAM



Para exibir todos os registros de autorização sob sua conta, consulte **5.5 Registros de autorização**.

NOTA

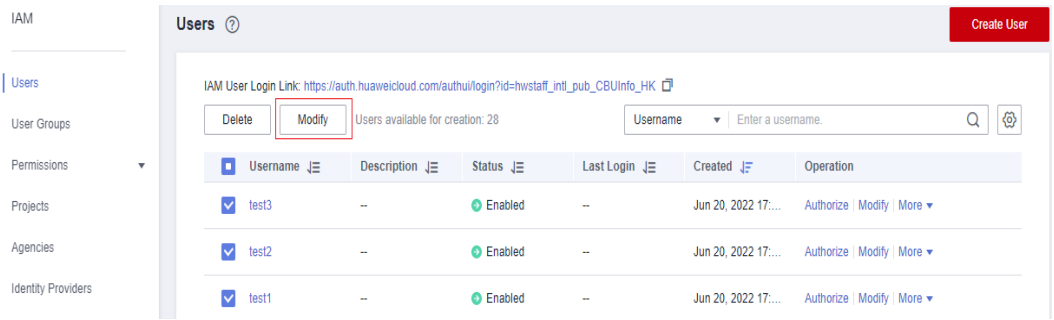
A exclusão das permissões de um usuário do IAM excluirá as permissões atribuídas ao grupo ao qual o usuário pertence. Todos os usuários do grupo deixarão de ter as permissões. Tenha cuidado ao realizar esta operação.

Modificação em lote das informações do usuário do IAM

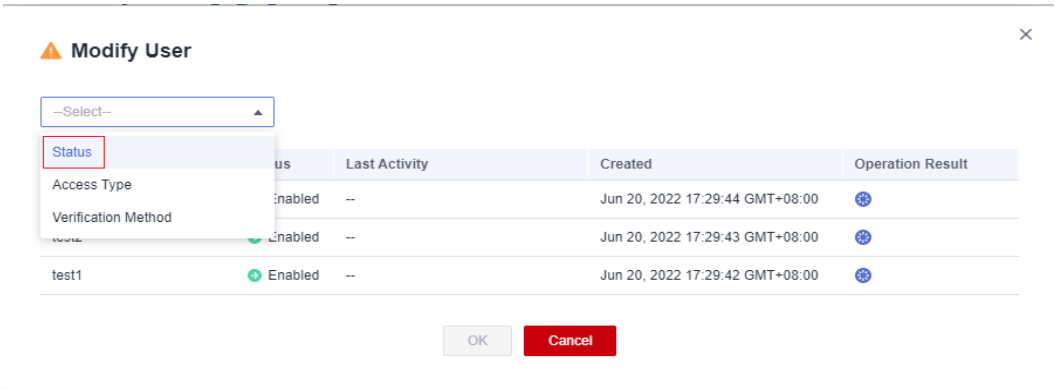
O IAM permite que você modifique em lote o status, o tipo de acesso e o método de verificação dos usuários do IAM. Em seguinda, descrevemos como modificar em lote o status dos usuários do IAM. Os métodos de modificar outras informações sobre os usuários são semelhantes a esse método.

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

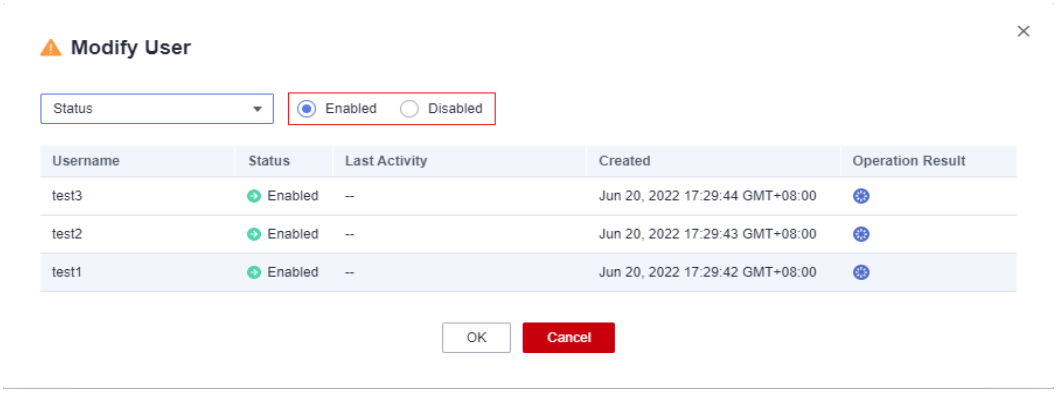
Passo 2 Na lista de usuários, selecione os usuários cujas informações você deseja modificar e clique em **Modify** acima da lista de usuários.



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



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



NOTA

Certifique-se de que esse usuário deixa de ser usado. Desabilitar 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 de um usuário do IAM ser excluído, ele não poderá mais fazer login e seu nome de usuário, senha, chaves de acesso e autorizações serão eliminados e não poderão ser recuperados.

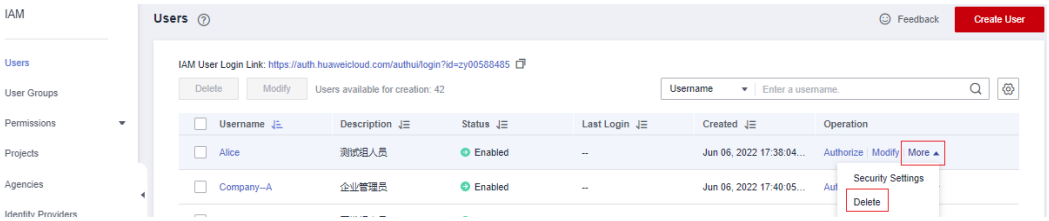
- Certifique-se de que os usuários a serem excluídos não são mais necessários. Se você não tiver certeza, desabilite-os em vez de excluí-los para que eles possam ser habilitados se ocorrer alguma falha de serviço. Para desabilitar um usuário individual do IAM, consulte **Informações básicas**. Para desabilitar vários usuários do IAM de uma vez, consulte **Modificação em lote das informações do usuário do IAM**.
- Para remover um usuário do IAM de um grupo de usuários, consulte **4.2 Adição de usuários a ou remoção de usuários de um grupo de usuários**.

Exclusão de um usuário do IAM

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

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

Figura 3-14 Exclusão de um usuário do IAM



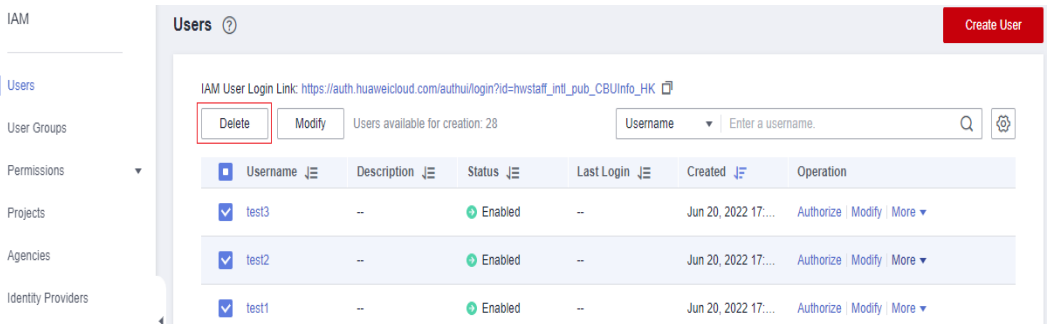
----Fim

Exclusão de usuários do IAM em lote

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

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

Figura 3-15 Exclusão de usuários do IAM em lote



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

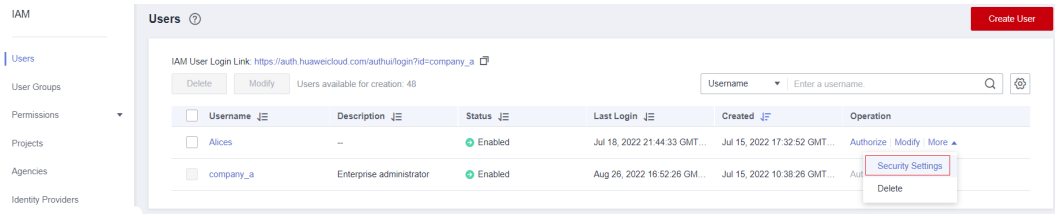
----Fim

3.6 Alteração da senha de login de um usuário do IAM

Como um 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 login 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 3-16 Alteração da senha do 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 página de guia **Security Settings**. Para alterar a senha, acesse a página **Basic Information** da Minha conta.
- Os usuários do IAM podem alterar suas senhas na página de guia **Basic Information**. Se você quiser alterar a senha da sua conta, consulte **Como faço para alterar minha senha?**

- **Set by user**: Uma URL de login único será enviada ao usuário. O usuário pode clicar no link para definir uma senha.
- **Automatically generated**: Uma senha será gerada automaticamente e, em seguida, enviada ao usuário por e-mail.
- **Set now**: Você define uma nova senha e envia a nova senha para o usuário.

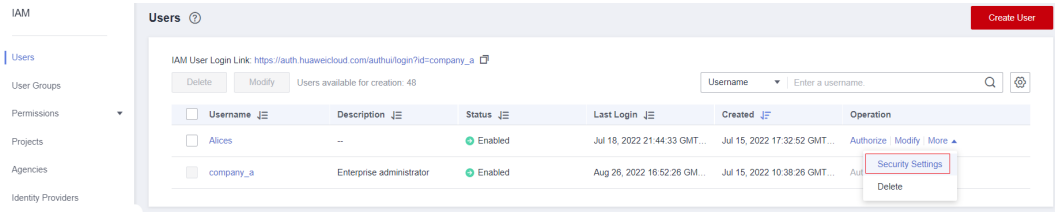
3.7 Gerenciamento das chaves de acesso de um usuário do IAM

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 teclas de acesso não podem ser usadas para fazer login no console. A AK é um identifidor exclusivo usada em conjunto com a SK para assinar solicitações criptograficamente, garantindo que as solicitações sejam secretas, completas e corretas.

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

Clique em **Security Settings** na linha que contém o usuário do IAM e crie ou exclua chaves de acesso.

Figura 3-17 Gerenciamento das chaves de acesso de um usuário do IAM



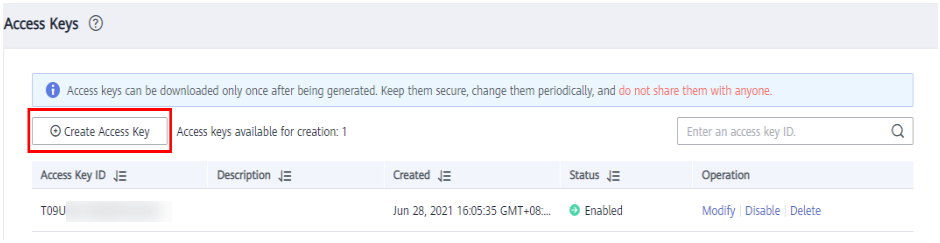
NOTA

- Se um usuário estiver autorizado a usar o console, ele poderá gerenciar **gerenciar chaves de acesso** na página **My Credentials**.
- As chaves de acesso são credenciais de identidade usadas para chamar as APIs. O administrador da conta e os usuários do IAM só podem usar suas próprias chaves de acesso para chamar as APIs.

- Criação de uma chave de acesso

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

  Figura 3-18 Criação de uma chave de acesso

  NOTA

  Cada usuário tem o máximo de 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.

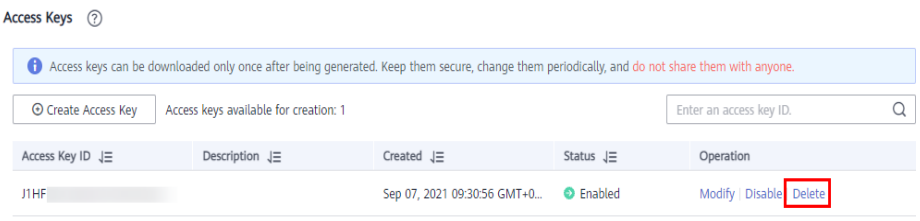
  b. (Opcional) Se a proteção de operação estiver ativada, você precisará inserir um código de verificação ou uma senha.

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

- Exclusão de 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 3-19 Exclusão de uma chave de acesso

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

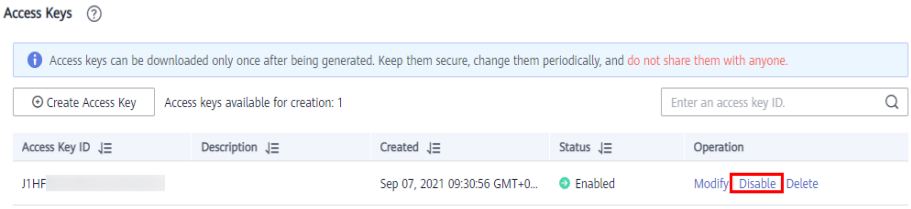
  c. Clique em **Yes**.

- Habilitação/Desabalitação de uma chave de acesso

  Novas chaves de acesso são ativadas por padrão. Para desabilitar uma chave de acesso, execute os seguintes passos:

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

Figura 3-20 Desabalitação de uma chave de acesso



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

O método de habilitar uma chave de acesso é semelhante ao de desabilitar uma chave de acesso.

4 Grupos de usuários e autorização

4.1 Criação de um grupo de usuários e atribuição de permissões

Como um 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. 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 os serviços de nuvem com base nas permissões atribuídas. Para obter detalhes, consulte **3.2 Atribuição de permissões a um usuário do IAM**. **Para obter detalhes sobre as permissões do sistema de todos os serviços de nuvem, consulte Permissões do sistema**.

Pré-requisitos

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

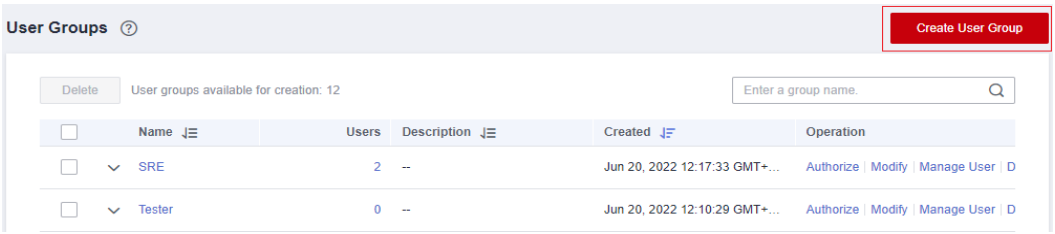
- Entenda os **conceitos básicos** de permissões.
- **Conheça Permissões do sistema fornecidas pelo IAM.**

Criação de um grupo de usuários

Passo 1 Faça login no console do IAM como um 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 o máximo de 20 grupos de usuários. Para criar mais grupos de usuários, aumente a cota consultando **Como faço para aumentar minha cota?**

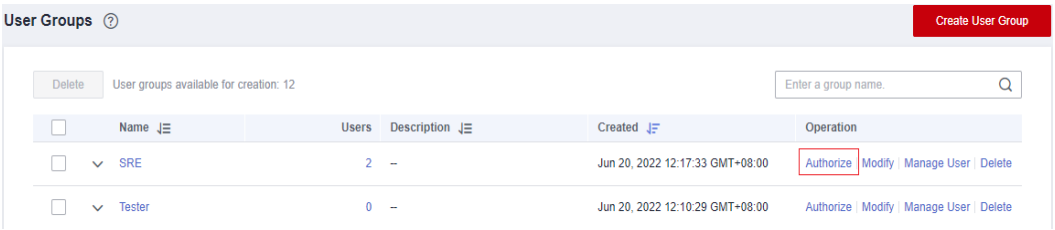
----Fim

Atribuição de permissões a um grupo de usuários

Para atribuir permissões a um grupo de usuários, faça o seguinte:

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

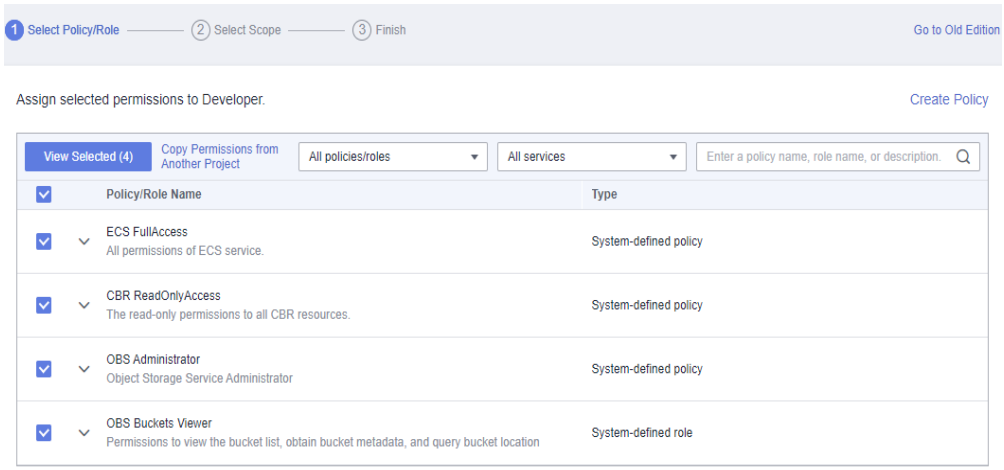
Figura 4-2 Ir para a página de autorização do grupo de usuários



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-los para complementar políticas definidas pelo sistema para controle de permissões refinado. Para obter detalhes, consulte **5.6.1 Criação de um política personalizada**.

Figura 4-3 Seleção de permissões



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

Tabela 4-1 Escopos da autorização

Escopo	Descrição
Todos os recursos	Os usuários do IAM podem usar os recursos em todos os projetos específicos da região e o projeto de serviço global em sua conta, conforme especificado pelas permissões.
Projetos empresariais	Os usuários do IAM podem usar os recursos nos projetos empresariais que selecionou, conforme especificado pelas permissões. **Essa opção está disponível somente quando a função do projeto empresarial estiver ativada.** Para obter detalhes sobre projetos empresariais, consulte **O que é o Serviço de gerenciamento de projetos empresariais?**. Para habilitar a função de projeto empresarial, consulte **Habilitação da função do projeto empresarial**.
Projetos específicos da região	Os usuários do IAM podem usar os recursos nos projetos empresariais da região que selecionou, conforme especificado pelas permissões. Se algumas das permissões selecionadas pertencerem a serviços globais, o sistema definirá automaticamente o escopo de autorização dessas permissões como **Todos os recursos**. As permissões selecionadas para serviços de nível de projeto serão aplicadas aos projetos específicos da região que você selecionar.

Escopo	Descrição
Serviços globais	Os usuários do IAM podem usar serviços globais conforme especificado pelas permissões. Serviços globais são implantados 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 algumas das permissões selecionadas pertencerem a serviços de nível de projeto, o sistema definirá automaticamente o escopo de autorização dessas permissões como **Todos os recursos**. As permissões selecionadas para serviços globais serão aplicadas aos serviços globais.

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 do sistema**.

NOTA

- Se você adicionar um usuário a vários grupos, o usuário herdará todas as permissões que foram atribuídas aos grupos.
- Para obter mais informações sobre gerenciamento de permissões, consulte **Atribuição das permissões a 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 da 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 serviços.	Todos
Gerenciamento de usuários do IAM	Security Administrator	Permissões de administrador para o IAM.	Serviços globais

Categoria	Nome da política/ função	Descrição	Escopo da autorização
Gerenciamento de contabilidade	BSS Administrator	Permissões de administrador do centro de faturamento, incluindo o gerenciamento de faturas, pedidos, contratos e renovações e a exibição de faturas. **NOTA** Essa função depende da função **BSS Administrator** para entrar em vigor.	Projetos específicos da região
Computação de O&M	ECS FullAccess	Permissões de administrador para ECS.	Projetos específicos da região
	CCE FullAccess	Permissões de administrador para Cloud Container Engine (CCE).	Projetos específicos da região
	CCI FullAccess	Permissões de administrador para Cloud Container Instance (CCI).	Projetos específicos da região
	BMS FullAccess	Permissões de administrador para Bare Metal Server (BMS).	Projetos específicos da região
	IMS FullAccess	Permissões de administrador para Image Management Service (IMS).	Projetos específicos da região
	AutoScaling FullAccess	Permissões de administrador para Auto Scaling (AS).	Projetos específicos da região
O&M de rede	VPC FullAccess	Permissões de administrador para Virtual Private Cloud (VPC).	Projetos específicos da região
	ELB FullAccess	Permissões de administrador para Elastic Load Balance (ELB).	Projetos específicos da região
O&M de banco de dados	RDS FullAccess	Permissões de administrador para Relational Database Service (RDS).	Projetos específicos da região
	DDS FullAccess	Permissões de administrador para Document Database Service (DDS).	Projetos específicos da região

Categoria	Nome da política/ função	Descrição	Escopo da autorização
	DDM FullAccess	Permissões de administrador para Distributed Database Middleware (DDM).	Projetos específicos da região
O&M de Segurança	Anti-DDoS Administrator	Permissões de administrador para Anti-DDoS.	Projetos específicos da região
	CAD Administrator	Permissões de administrador para Advanced Anti-DDoS (AAD).	Projetos específicos da região
	WAF Administrator	Permissões de administrador para Web Application Firewall (WAF).	Projetos específicos da região
	VSS Administrator	Permissões de administrador para Vulnerability Scan Service (VSS).	Projetos específicos da região
	CGS Administrator	Permissões de administrador para Container Guard Service (CGS).	Projetos específicos da região
	KMS Administrator	Permissões de administrador para Key Management Service (KMS), que foi renomeado Data Encryption Workshop (DEW).	Projetos específicos da região
	DBSS System Administrator	Permissões de administrador para Database Security Service (DBSS).	Projetos específicos da região
	SES Administrator	Permissões de administrador para Security Expert Service (SES).	Projetos específicos da região
	SC Administrator	Permissões de administrador para SSL Certificate Manager (SCM).	Projetos específicos da região

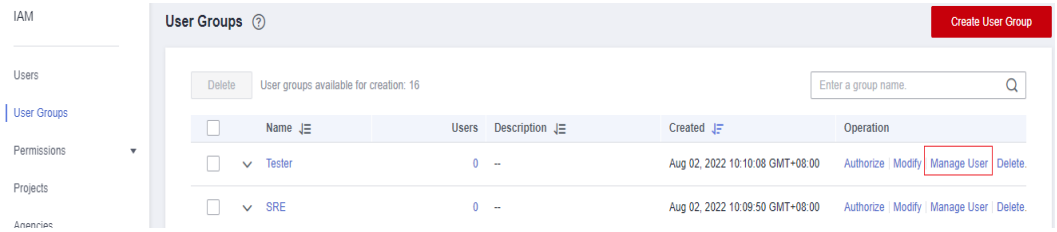
4.2 Adição de usuários a ou remoção de usuários de um grupo de usuários

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 dos usuários a um grupo de usuários

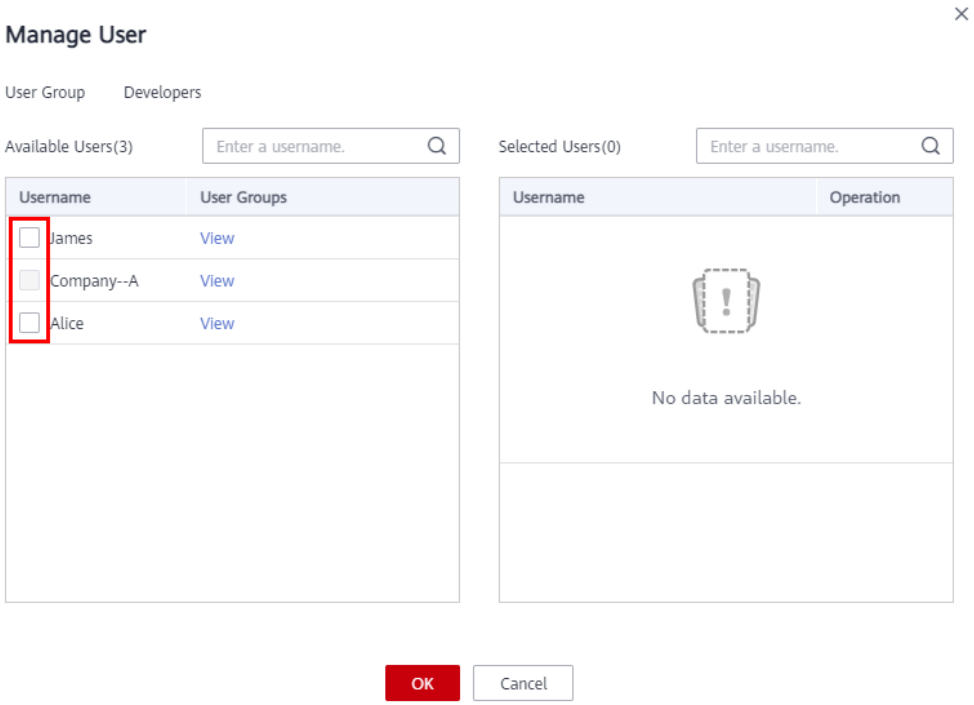
Passo 1 Na lista de grupos de usuários, clique em **Manage User** na linha que contém o grupo de usuários alvo, por exemplo, **Developers**.

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



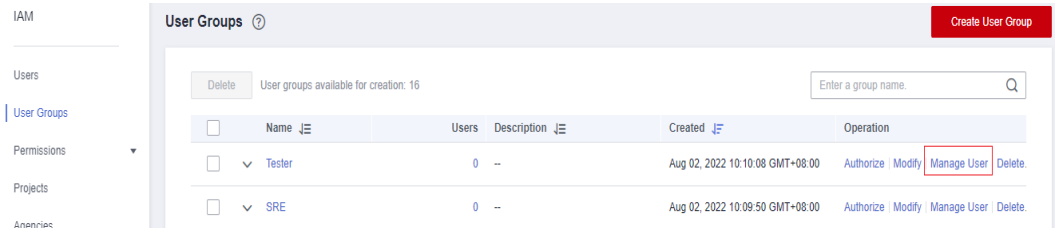
Passo 3 Clique em **OK**.

----Fim

Remoção dos usuários de um grupo de usuários

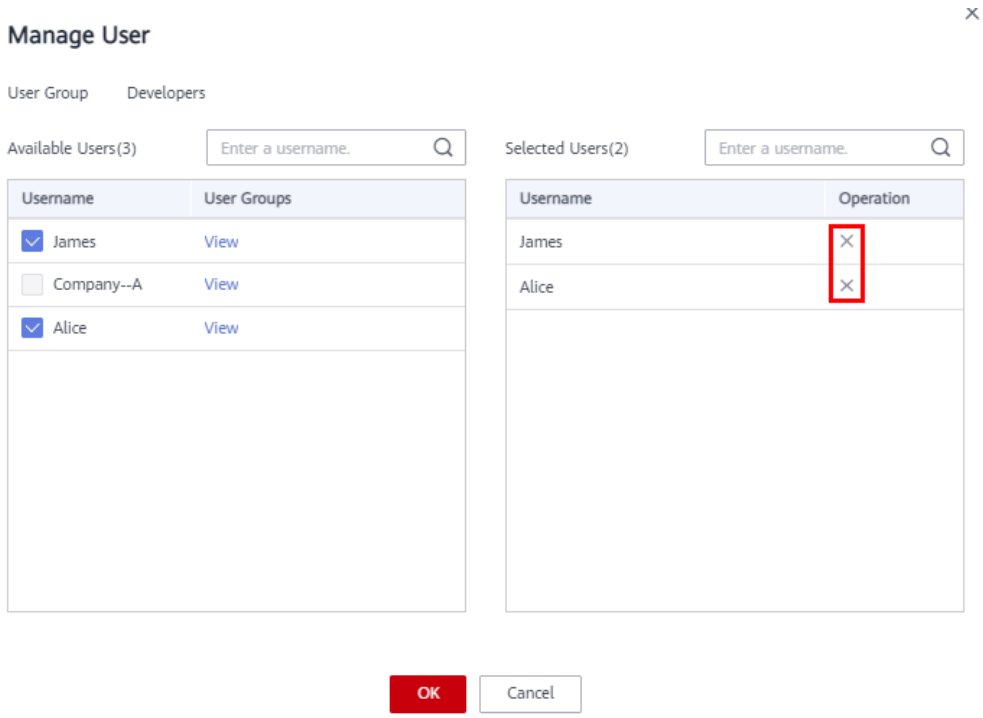
Passo 1 Na lista de grupos de usuários, clique em **Manage User** na linha que contém o grupo de usuários alvo, por exemplo, **Developers**.

Figura 4-6 Gerenciamento de usuários



Passo 2 Na área **Selected Users**, clique no ícone **x** à direita dos nomes de usuário a serem removidos e clique em **OK**.

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



----Fim

4.3 Exclusão de um grupo de usuários

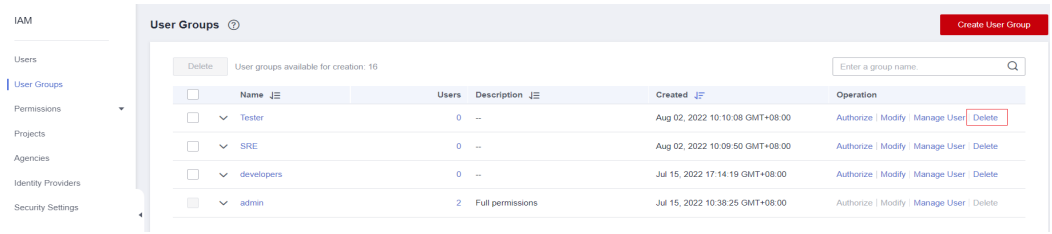
Procedimento

Para excluir um grupo de usuários, faça o seguinte:

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

Passo 2 Na lista do grupo 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**.

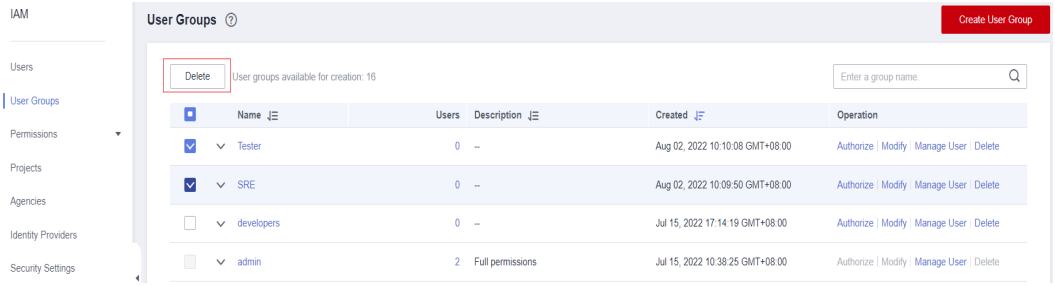
----Fim

Exclusão dos grupos de usuários em lote

Para excluir vários grupos de usuários de uma vez, faça o seguinte:

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

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



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

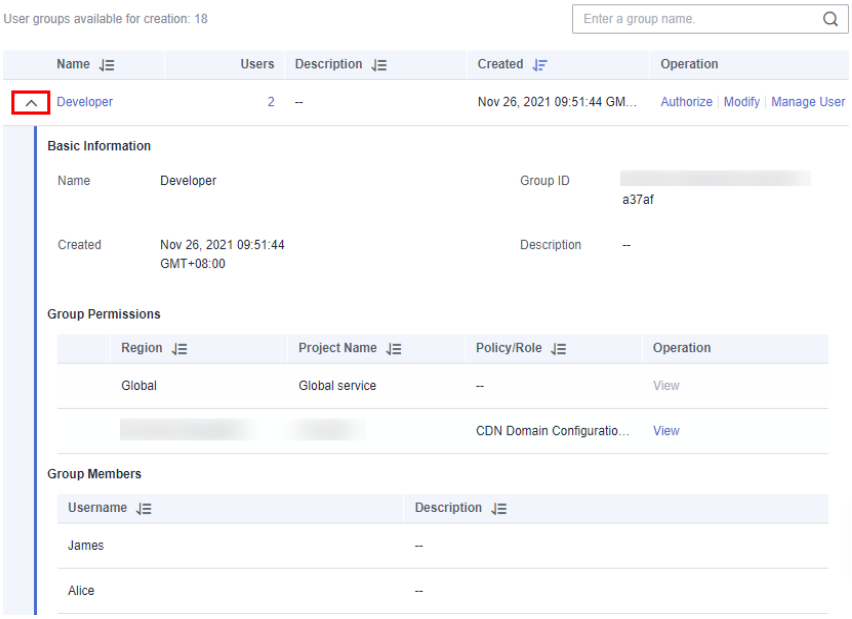
----Fim

4.4 Exibição ou modificação das informações do grupo de usuários

Exibição das 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 4-9 Exibição das informações do grupo de usuários



Modificação de permissões do grupo de usuários

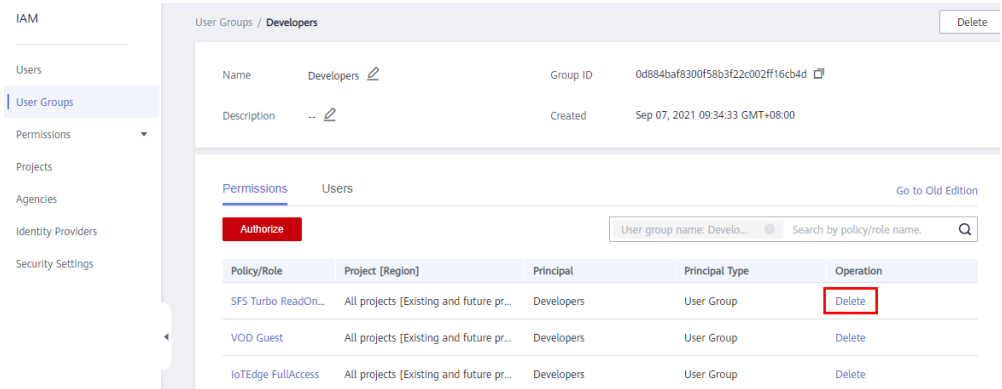
Exibir ou modificar as informações do grupo de usuários.

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 **admin** padrão não podem ser modificadas.

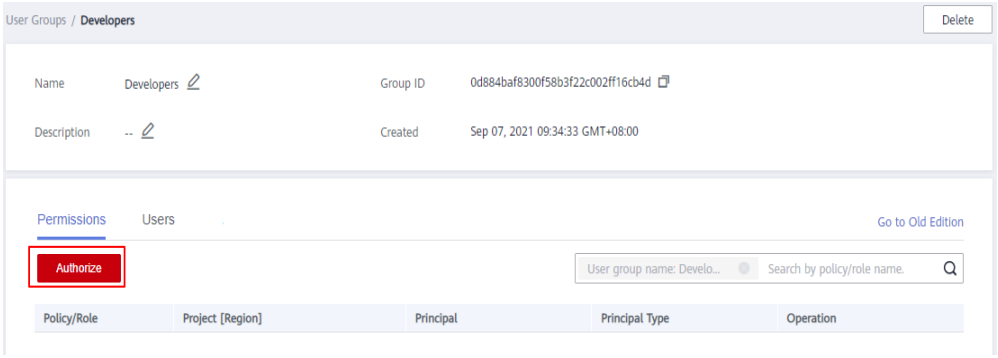
1. Clique no nome de um grupo de usuários (por exemplo, **Developers**) para acessar a página de detalhes e exibir as permissões do grupo na página da guia **Permissions**.
2. Clique em **Delete** na linha que contém a função ou política que você deseja excluir.

Figura 4-10 Exclusão de uma permissão atribuída



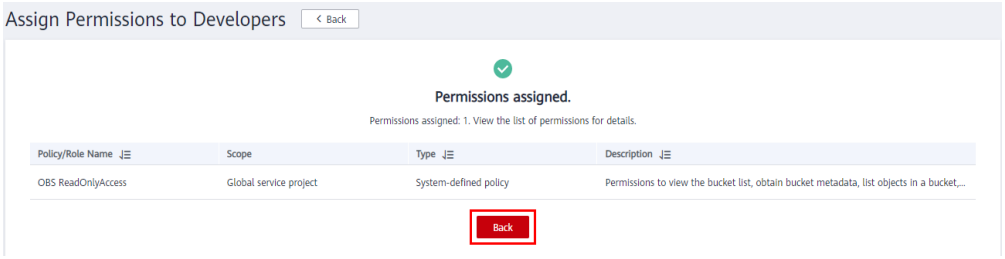
3. Clique em **Yes**.
4. Na página de guia **Permissions**, clique em **Authorize**.

Figura 4-11 Atribuição de permissões a um grupo de usuários



5. Selecione as permissões desejadas e um escopo e clique em **OK**.
6. Clique em **Back**. Em seguida, exiba as permissões do grupo na página da guia **Permissions**.

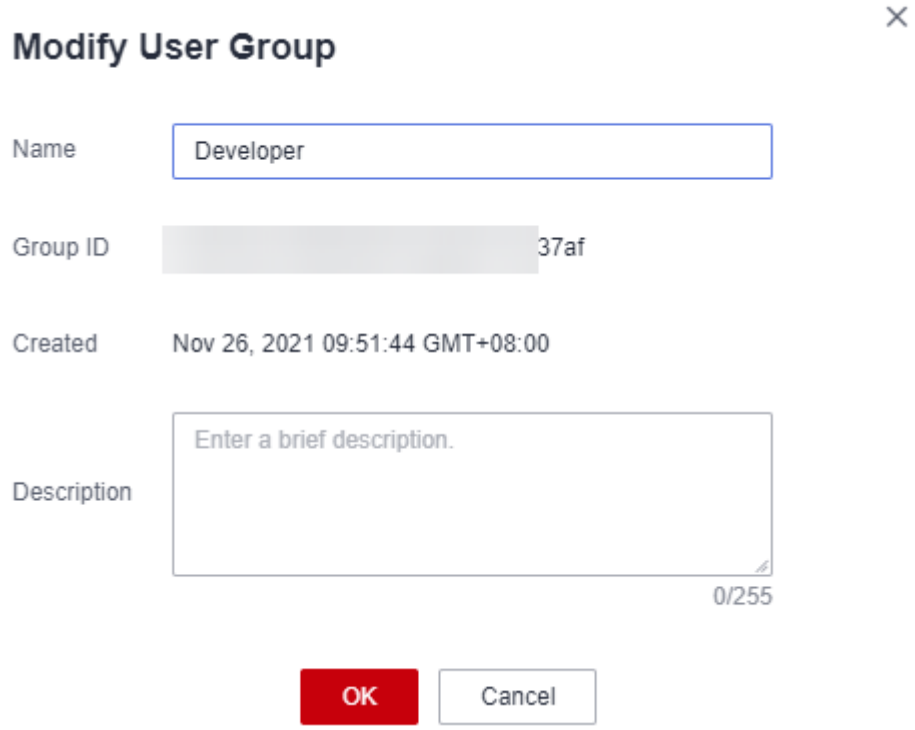
Figura 4-12 Clique em Back



Modificação da descrição e do nome 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 4-13 Modificação da descrição e do nome de um grupo de usuários



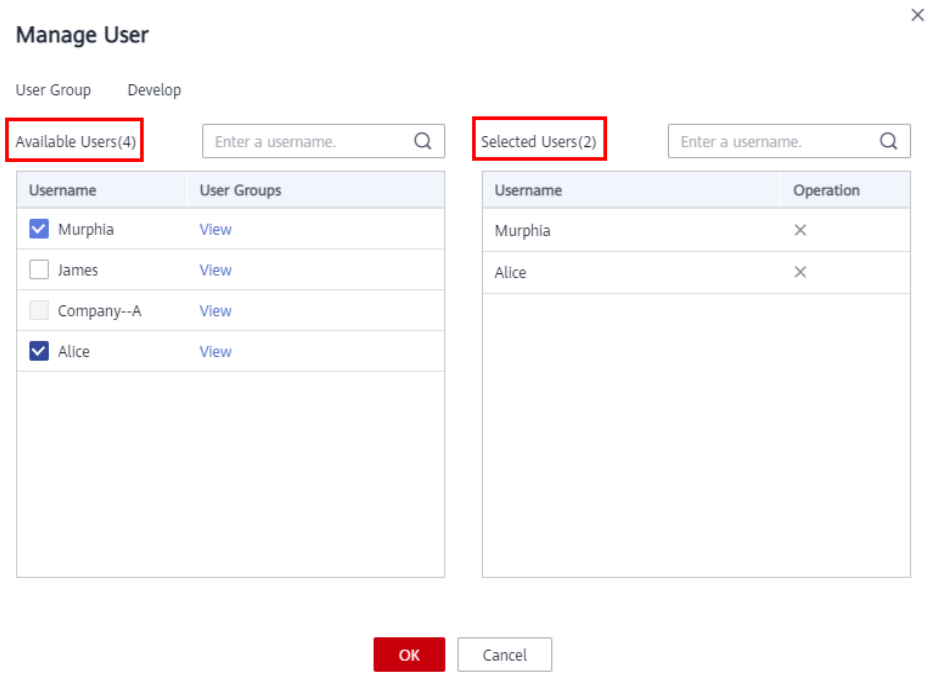
NOTA

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 contendo o grupo de usuários que você deseja modificar.

Figura 4-14 Gerenciamento de 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 usuários do grupo de usuários.

----Fim

NOTA

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

4.5 Revogação de permissões de um grupo de usuários

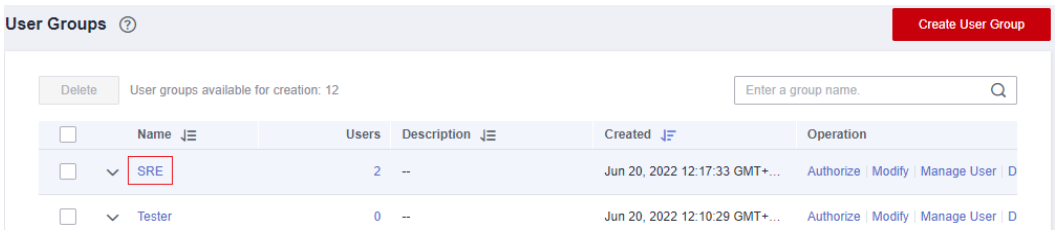
Procedimento

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

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

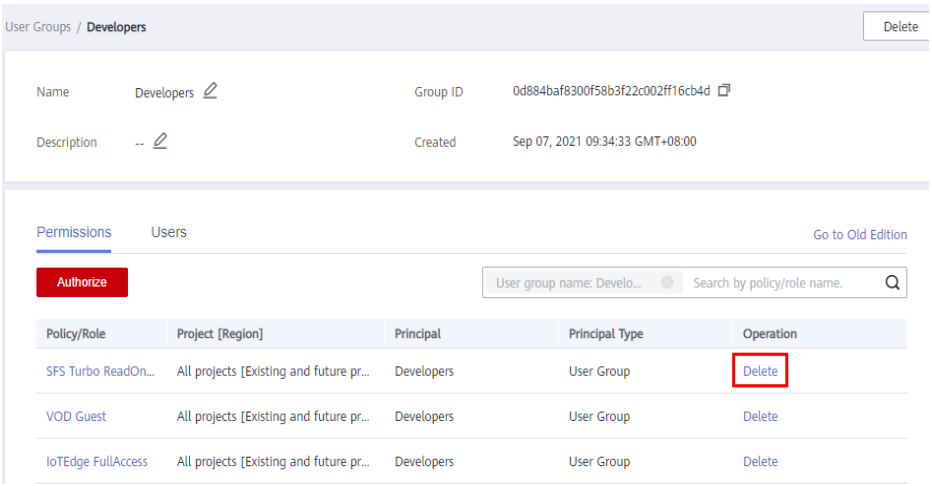
Passo 2 Clique no nome do grupo de usuários para acessar a página de detalhes do grupo.

Figura 4-15 Clique do nome do grupo de usuários



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

Figura 4-16 Revogação de permissões



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

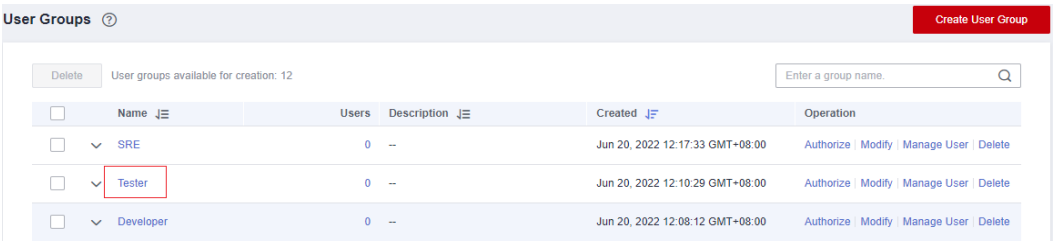
----Fim

Revogação de permissões em lote de um grupo de usuários

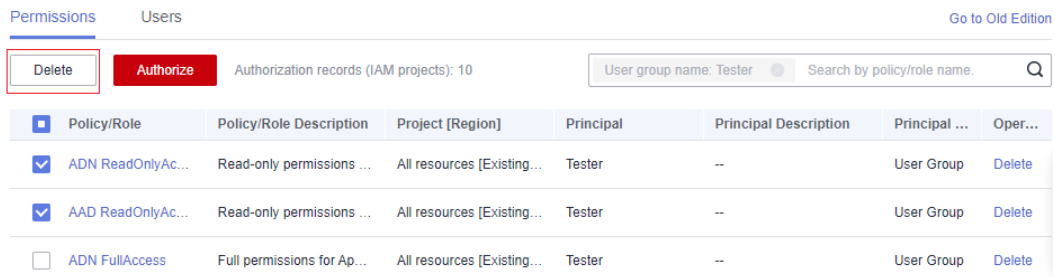
Para revogar várias políticas ou funções anexadas a um grupo de usuários, faça o seguinte:

Passo 1 Faça login 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.



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



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

----Fim

4.6 Atribuição de funções de dependência

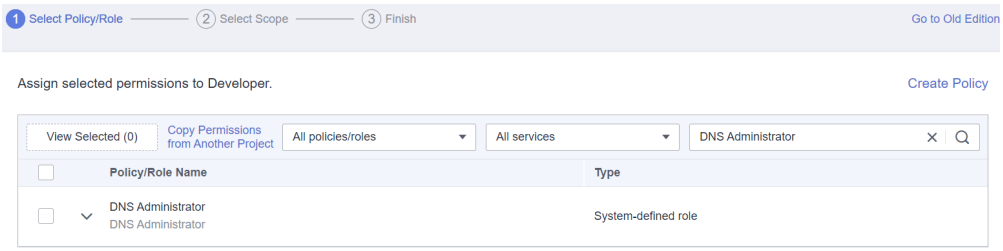
Os serviços da HUAWEI CLOUD interagem entre si. As funções de alguns serviços só entram em vigor se forem atribuídas juntamente com as funções de outros serviços.

Procedimento

Passo 1 Ao atribuir permissões a usuários ou grupos de usuários, pesquise uma função na caixa de pesquisa.

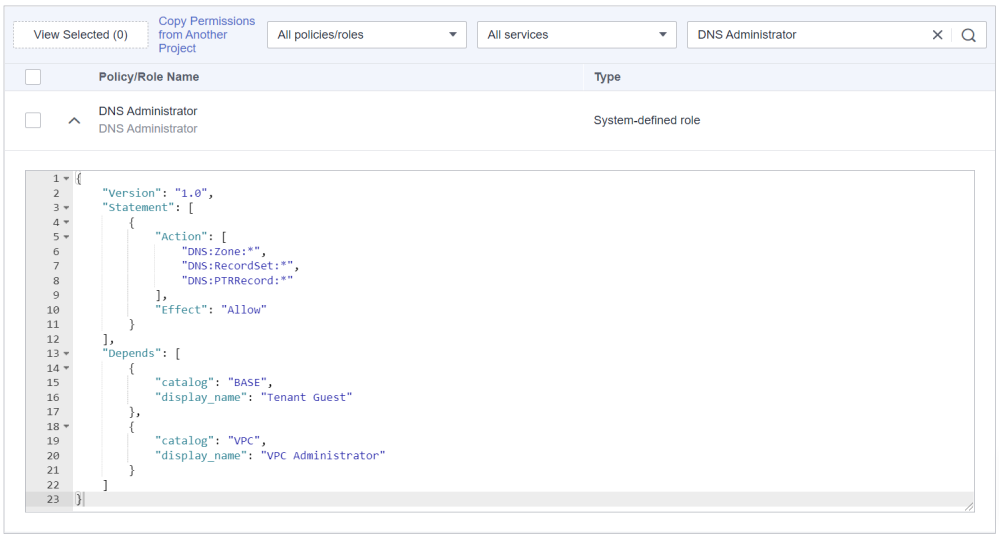
Passo 2 Selecione a função de destino. O sistema seleciona automaticamente as funções de dependência.

Figura 4-17 Seleção de uma função



Passo 3 Clique em ao lado da função para exibir as dependências.

Figura 4-18 Exibição de dependências



Por exemplo, a função **DNS Administrator** contém o parâmetro **Depends** que especifica as funções de dependência. Quando você atribui o **DNS Administrator** a um grupo de usuários, também precisa atribuir as funções de **Tenant Guest** e **VPC Administrator** ao grupo do mesmo projeto.

Passo 4 Clique em **OK**.

----Fim

5 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 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 a escolha ideal para autorização refinada e controle de acesso seguro.
- Políticas: um tipo de mecanismo de autorização refinado que define as permissões necessárias para executar operações em recursos de nuvem específicos sob certas condições. Esse mecanismo permite uma autorização baseada em política mais flexível e o controle de acesso seguro. Por exemplo, você pode conceder aos usuários ECS somente as permissões necessárias para gerenciar um determinado tipo de recursos ECS.

  O IAM suporta **system-defined policies** e **custom policies**.

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 não podem ser modificadas. **Para obter detalhes sobre as políticas pelo sistema de todos os serviços de nuvem, consulte Permissões do 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 ticket do 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

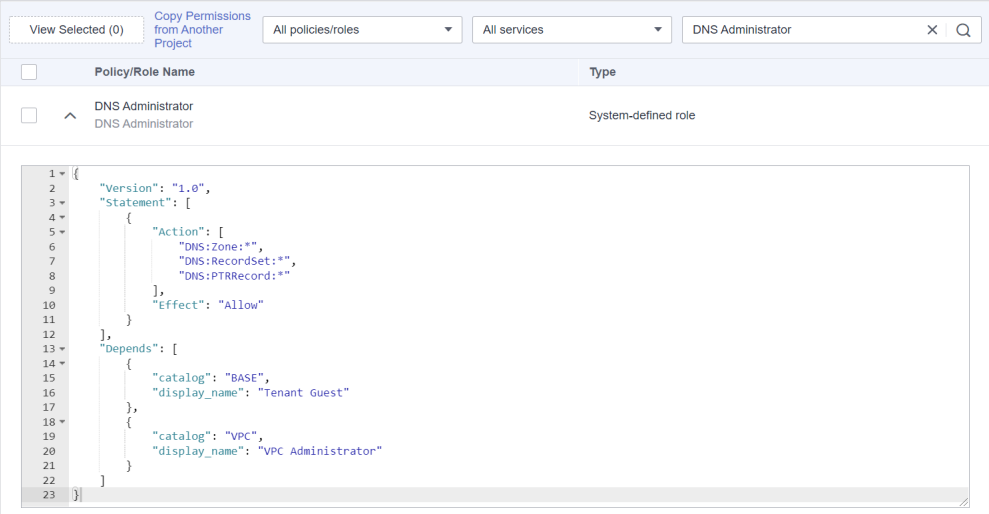
Funções são um tipo de mecanismo de autorização de alta granularidade que define permissões de nível de serviço com base nas responsabilidades do usuário. O IAM fornece um número limitado de funções para o gerenciamento de permissões.

Serviços da HUAWEI CLOUD interagem entre si. As funções de alguns serviços só entram em vigor 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 de **DNS Administrator** como um exemplo para descrever o conteúdo da função.

Figura 5-1 Conteúdo da função de administrator DNS




```
{
    "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

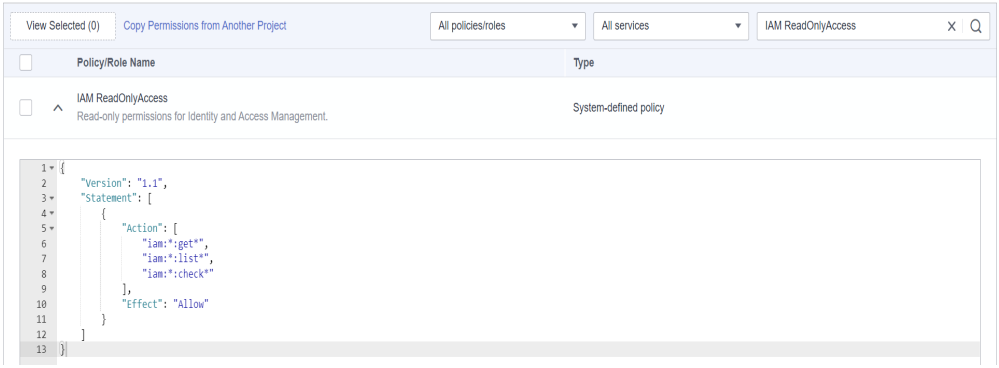
Parâmetro		Descrição	Valor
Version		Versão da função.	**1.0**: indica controle de acesso baseado em função.
Statement	Action	Operações a serem realizadas no serviço.	Formato: "*Service name*:*Resource type*:*Operation*". **DNS:Zone:***: Permissões para executar todas as operações em zonas do DNS (Domain Name Service).
	Effect	Determina se permitir ou negar as operações definidas em action.	● Allow ● Deny **NOTA** Se as funções usadas para conceder permissões a um usuário contiverem Allow e Deny para a mesma action, a Deny terá proriodade.
Depends	catalog	Nome do serviço ao qual uma função de dependência pertence.	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 de **Tenant Guest** e **VPC Administrator** ao grupo do 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 ⌄ no lado esquerdo 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 de IAM ReadOnlyAccess




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

5.3.2 Sintaxe da política

O seguinte utiliza 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": [
                        "specialCharactor"
```

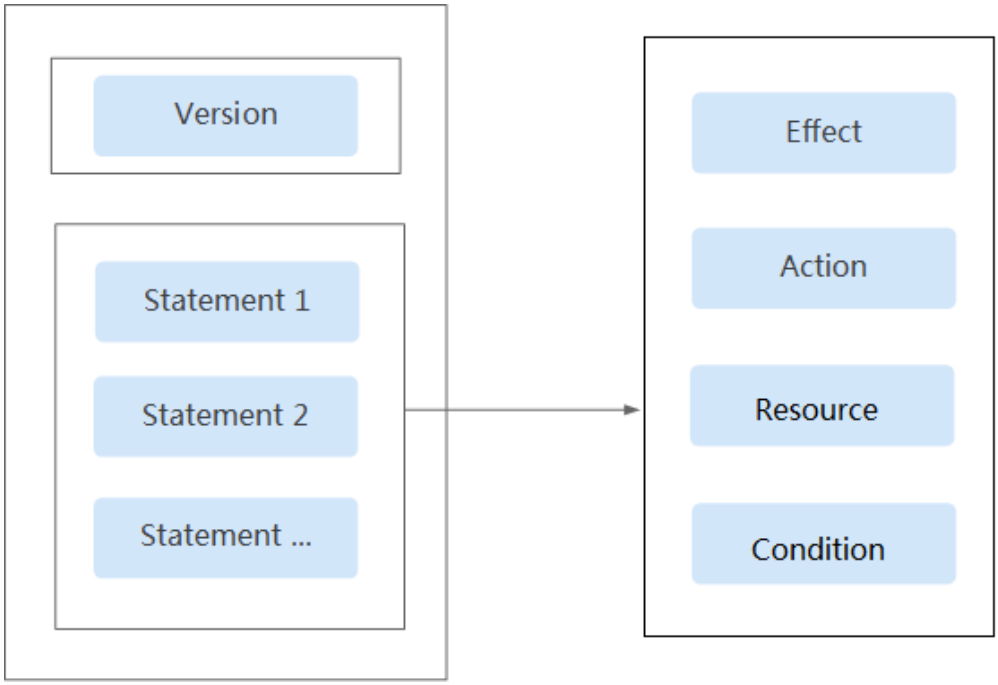


```
                    ]
                },
                "Bool": {
                    "g:MFAPresent": [
                        "true"
                    ]
                }
            },
            "Resource": [
                "obs:*:*:bucket:*"
            ]
        }
    ]
}
```

Estrutura da política

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

Figura 5-3 Estrutura da política



Parâmetros da política

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

Tabela 5-2 Parâmetros da política

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

Parâmetro		Descrição	Valor
Statement	Effect	Determina se permitir ou negar as operações definidas em action.	● Allow ● Deny **NOTA** Se as políticas usadas para conceder permissões a um usuário contiverem Allow e Deny para a mesma action, a Deny terá proriodade.
	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, consulte **Ações suportadas do 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 entrará em vigor somente quando todas as condições forem atendidas. Exemplo: **StringEndWithIfExists": {"g:UserName": ["specialCharactor"]}**: A declaração é válida para usuários cujos nomes terminam com **specialCharactor**.
	Resource	Recursos sobre os quais a política entra em vigor.	Formato: *Service name*:*Region*:*Account ID*:*Resource type*:*Resource path*. Caracteres curinga (*) são suportados. Exemplo: ● **obs:*:*:bucket:***: Todos os buckets 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 **chaves de condição globais communs** e **chaves de condição globais especiais**.
  - Chaves de condição globais communs: 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 obter detalhes, consulte **Common global condition keys**.
  - Chaves de condição globais especiais: O IAM obtém informações de condição dos serviços em nuvem para autenticação.

– As 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 do OBS**.

Tabela 5-3 Chaves de condição globais communs

Chave de condição global	Tipo	Descrição
g:CurrentTime	Tempo	Hora em que uma solicitação de autenticação é recebida. O tempo é expresso no formato definido pelo ISO 8601, por exemplo, **2012-11-11T23:59:59Z**.
g:DomainName	String	Nome da conta.
g:MFAPresent	Boolean	Indica se deseja obter um token por meio da autenticação MFA.
g:MFAAge	Número	Período de validade de um token obtido através 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.

- **Operador**

  Um operador (consulte **Operadores**), uma chave de condição e um valor de condição para formar uma declaração 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 um valor de solicitação estiver vazio ou igual ao valor da condição especificada.

Tabela 5-4 Operadores (Os operadores de string não diferenciam maiúsculas e minúsculas, a menos que especificado de outra forma.)

Operador	Tipo	Descrição
StringEquals	String	(Diferencia maiúsculas e minúsculas) O valor da solicitação é o mesmo que o valor da condição.
StringNotEquals	String	(Diferencia maiúsculas e minúsculas) O valor da solicitação é diferente do valor da condição.
StringEqualsIgnoreCase	String	O valor da solicitação é o mesmo que o valor da condição.
StringNotEqualsIgnoreCase	String	O valor da solicitação é diferente do valor da condição.
StringLike	String	O valor da solicitação contém o valor da condição.
StringNotLike	String	O valor da solicitação não contém o valor da condição.
StringStartWith	String	O valor da solicitação começa com o valor da condição.
StringEndWith	String	O valor da solicitação termina com o valor da condição.
StringNotStartWith	String	O valor da solicitação não começa com o valor da condição.
StringNotEndWith	String	O valor da solicitação não termina com o valor da condição.
StringEqualsAnyOf	String	(Diferencia maiúsculas e minúsculas) O valor da solicitação é o mesmo que qualquer um dos valores da condição configurados.
StringNotEqualsAnyOf	String	(Diferencia maiúsculas e minúsculas) O valor da solicitação é diferente de todos os valores de condição configurados.
StringEqualsIgnoreCaseAnyOf	String	O valor da solicitação é o mesmo que qualquer um dos valores da condição configurados.
StringNotEqualsIgnoreCaseAnyOf	String	O valor da solicitação é diferente de todos os valores de condição configurados.
StringLikeAnyOf	String	O valor da solicitação contém qualquer um dos valores da condição configurados.
StringNotLikeAnyOf	String	O valor da solicitação não contém qualquer um dos valores da condição configurados.
StringStartWithAnyOf	String	O valor da solicitação começa com qualquer um dos valores da condição configurados.

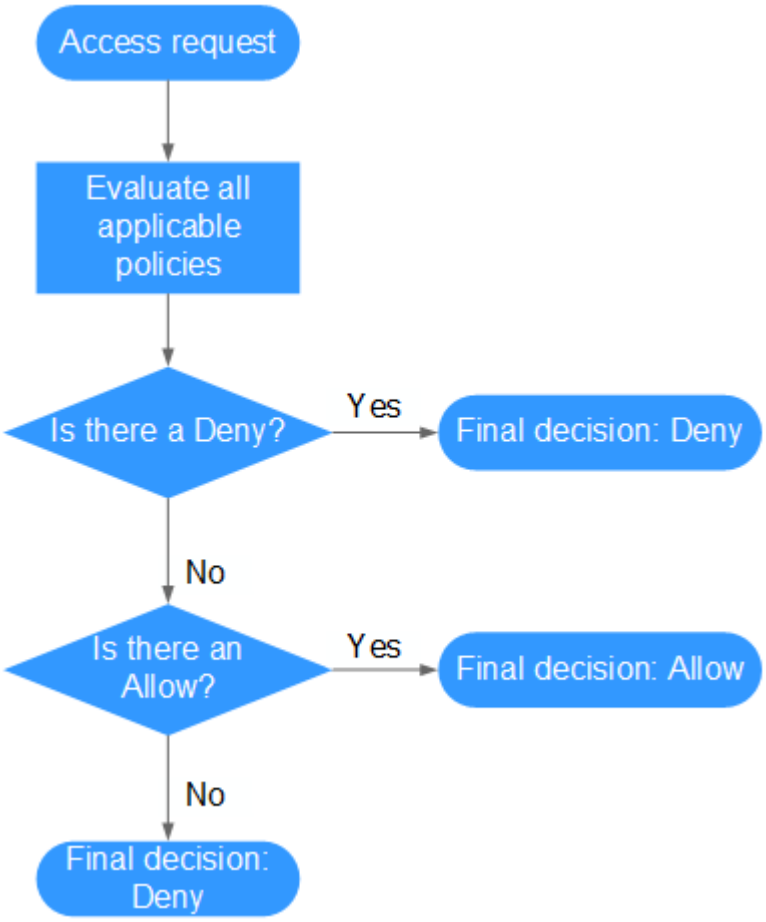
Operador	Tipo	Descrição
StringEndWithAnyOf	String	O valor da solicitação termina com qualquer um dos valores da condição configurados.
StringNotStartWithAnyOf	String	O valor da solicitação não começa com qualquer um dos valores da condição configurados.
StringNotEndWithAnyOf	String	O valor da solicitação não termina com qualquer um dos valores da condição configurados.
NumberEquals	Número	O valor da solicitação é igual ao valor da condição.
NumberNotEquals	Número	O valor da solicitação não é igual ao valor da condição.
NumberLessThan	Número	O valor da solicitação é menor que o valor da condição.
NumberLessThanEquals	Número	O valor da solicitação é menor que ou igual ao valor da condição.
NumberGreaterThan	Número	O valor da solicitação é maior que o valor da condição.
NumberGreaterThanEquals	Número	O valor da solicitação é maior que ou igual ao valor da condição.
NumberEqualsAnyOf	Número	O valor da solicitação é igual a qualquer um dos valores da condição configurados.
NumberNotEqualsAnyOf	Número	O valor da solicitação não é igual a qualquer um dos valores da condição configurados.
DateLessThan	Tempo	O valor da solicitação é anterior ao valor da condição.
DateLessThanEquals	Tempo	O valor da solicitação é anterior ou igual ao valor da condição.
DateGreaterThan	Tempo	O valor da solicitação é posterior ao valor da condição.
DateGreaterThanEquals	Tempo	O valor da solicitação é posterior ou igual ao valor da condição.
Bool	Boolean	O valor da solicitação é igual ao valor da condição.
IpAddress	Endereço IP	O valor da solicitação está dentro do intervalo de endereços IP definido no valor da condição.
NotIpAddress	Endereço IP	O valor da solicitação está fora do intervalo de endereços IP definido no valor da condição.
IsNullOrEmpty	Nulo	O valor da solicitação é null ou uma string vazia.

Operador	Tipo	Descrição
IsNull	Nulo	O valor da solicitação é null.
IsNotNull	Nulo	O valor da solicitação não é null.

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 5-4 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 Alteração dos nomes de política definidos pelo sistema

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

Tabela 5-5 Nomes de políticas originais e atuais definidos 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

Serviço	Original	Atual
	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
	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

Serviço	Original	Atual
	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
	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

Serviço	Original	Atual
	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
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

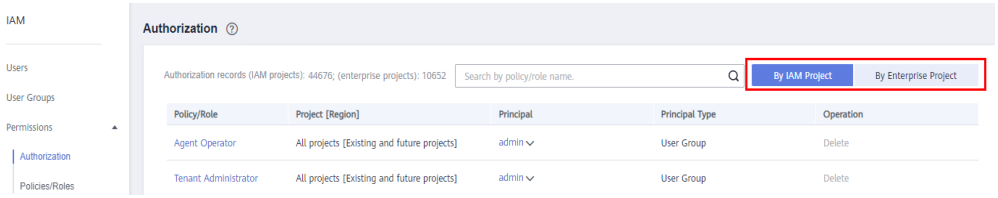
Serviço	Original	Atual
	VPC Viewer	VPC ReadOnlyAccess

5.5 Registros de autorização

Veja todos os registros de autorização sob sua conta na página **Permissions** > **Authorization**. Você pode filtrar registros por nome de política/função, projeto (região), principal e tipo principal (usuário, grupo de usuários e agência).

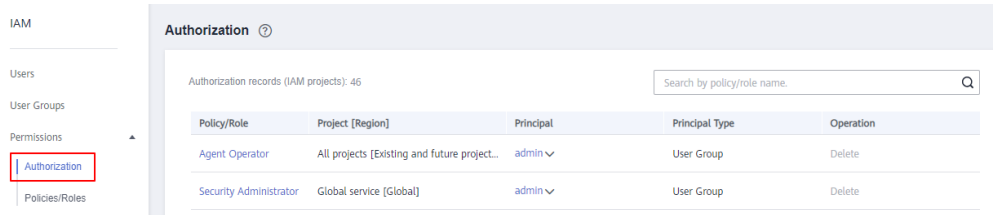
- Função do projeto empresarial habilitada: Exibir registros de autorização por IAM ou projeto empresarial.

  Figura 5-5 Função do projeto empresarial habilitada

- Função do projeto empresarial não habilitada: Exibir registros de autorização por projeto do IAM. Para habilitar a função do projeto empresarial, consulte **habilitação da função do projeto empresarial**.

  Figura 5-6 Função do projeto empresarial não habilitada

Exibir registros de autorização por projeto do IAM

Ao exibir 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 insira um nome. Para obter detalhes sobre as permissões de todos os serviços de nuvem, consulte **Permissões do Sistema**.

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

  Para exibir as permissões de projeto do IAM atribuídas a um usuário, grupo de usuários ou agência do IAM específico, 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 permissões da aplicação. Se você quiser exibir registros de autorização de um projeto do IAM, selecione **IAM project** e qualquer uma das seguintes opções:
  - **Global service**: Exibir registros de autorização de todos os serviços globais.
  - **All resources**: Exibir registros de autorização de todos os projetos, ou seja, o projeto de serviço global e todos os projetos específicos da região (incluindo projetos criados posteriormente).
  - Projeto específico da região: Exibir registros de autorização de um projeto ou subprojeto padrão (como eu-west-101)
- **Principal type**: O tipo de objetos que são autorizados. Existem três tipos principais: usuário, grupo de usuários e agência. Na visualização de projeto do IAM, filtre registros por grupo de usuários ou agência. Se você selecionar **User**, nenhum registro será exibido.
- **Enterprise project**: O nome de um projeto empresarial. Se você selecionar **Enterprise project** e inserir um nome de projeto da empresa, a **enterprise project view** será exibida.

Exibição de registros de autorização por projeto empresarial

Ao exibir 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 insira 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 insira um nome.

  NOTA

  - Para autorização baseada em projeto empresarial, você atribui permissões por usuários. 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 de permissões da aplicação. Para exibir os registros de autorização de um projeto da empresa específico, selecione **Enterprise project** e insira um nome de projeto empresarial.
- **Principal type**: O tipo de objetos que são autorizados. Existem três tipos principais: usuário, grupo de usuários e agência.
- **IAM project**: O nome de um projeto do IAM ou região. Se você selecionar **IAM project** e inserir um nome de projeto, a **IAM project view** será exibida.

5.6 Políticas personalizadas

5.6.1 Criação de um política personalizada

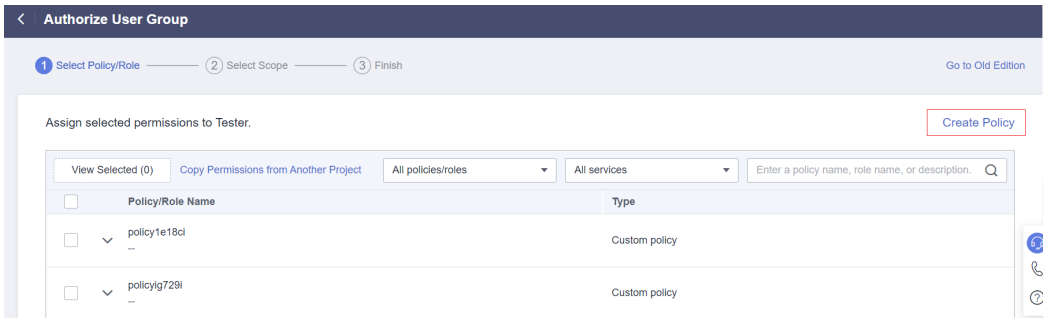
Você pode criar políticas personalizadas para complementar políticas definidas pelo sistema e implementar um controle de acesso mais refinado.

Você pode criar políticas personalizadas de uma das seguintes maneiras:

- Editor visual: Selecione um serviço de nuvem, especifique ações e recursos e adicione condições de solicitação. Você não precisa ter conhecimento da sintaxe JSON.
- JSON: Crie uma política no formato JSON a partir do zero ou com base em uma política existente.

Esta seção descreve como criar políticas personalizadas na página **Permissions** > **Policies/Roles**. Você também pode criar políticas personalizadas durante a autorização (consulte **Figura 5-7**) sem encerrar a operação atual.`

Figura 5-7 Criação de uma política durante a autorização

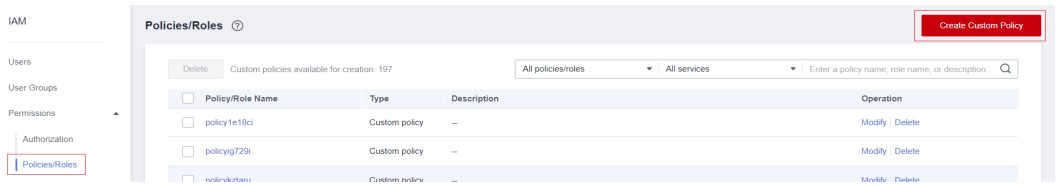


Criação de uma política personalizada no editor visual

Passo 1 Faça login no console do IAM.

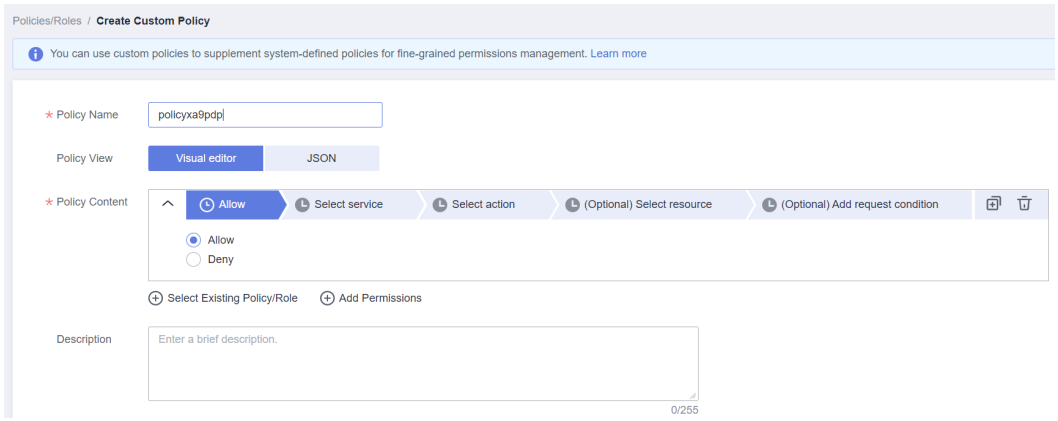
Passo 2 No console do IAM, escolha **Permissions** > **Policies/Roles** no painel de navegação e clique em **Create Custom Policy** no canto superior direito.

Figura 5-8 Criação de um política personalizada



Passo 3 Insira um nome de política.

Figura 5-9 Inserção de 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 separadas para autorização refinada.
3. Selecione as ações.
4. (Opcional) Selecione todos os recursos ou selecione recursos específicos especificando seus caminhos.

   Os serviços de nuvem que permitem autorização para recursos específicos incluem: Object Storage Service (OBS), Intelligent EdgeFabric (IEF), Data Lake Insight (DLI), Graph Engine Service (GES), FunctionGraph, Distributed Message Service (DMS), IoT Device Access (IoTDA), Key Management Service (KMS), Autonomous Driving Cloud Service (Octopus), and Data Warehouse Service (DWS). Para obter detalhes, consulte **5.6.4 Serviços de nuvem suportados pelo IAM**.

Tabela 5-6 Tipo de recurso

Parâmetro	Descrição
Específico	Permissões para recursos específicos. Por exemplo, para definir permissões para buckets cujos nomes começam com **TestBucket**, especificar o caminho do recurso do bucket como **OBS:*:*:bucket:TestBucket***. **NOTA** – Especificação de 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 OBS. – Especificação de recursos do objeto Formato: "OBS:*:*:object:*Bucket name or object name*". Para recursos do 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**.
Todos	Permissões para todos os recursos.

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

Tabela 5-7 Parâmetros de condição

Nome	Descrição
Chave de condição	Uma chave no elemento **Condition** de uma instrução. Existem chaves de condição globais e de nível de serviço. **As chaves de condição globais** (começando com **g:**) estão disponíveis para operações de todos os serviços, enquanto as chaves de condição de nível de 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 do usuário do serviço de nuvem correspondente, por exemplo, **OBS Request Conditions**.
Operador	Usado em conjunto com uma chave de condição e um valor de condição para formar uma declaração de condição completa.
Valor	Usado em conjunto com uma chave de condição e um operador que requer uma palavra-chave, para formar uma declaração de condição completa.

Figura 5-10 Adição de uma condição de solicitação

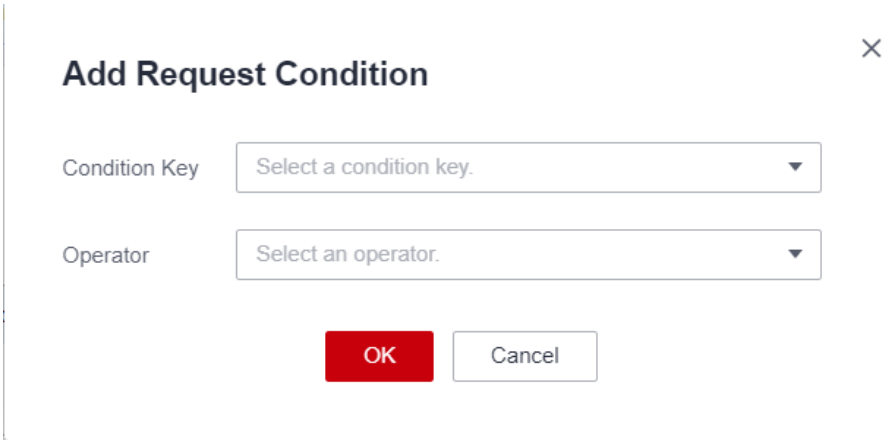


Tabela 5-8 Chaves de condição globais

Chave de condição global	Tipo	Descrição
g:CurrentTime	Tempo	Hora em que uma solicitação de autenticação é recebida. O tempo é expresso no formato definido pela 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.
g:MFAAge	Número	Período de validade de um token obtido através 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 modificada 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 permissão existente para clonar suas permissões.

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

Passo 9 Clique em **OK**.

Passo 10 Atribuição da política a um grupo de usuários. Em seguida, os utilizadores do grupo herdam as permissões definidas nesta política.

NOTA

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

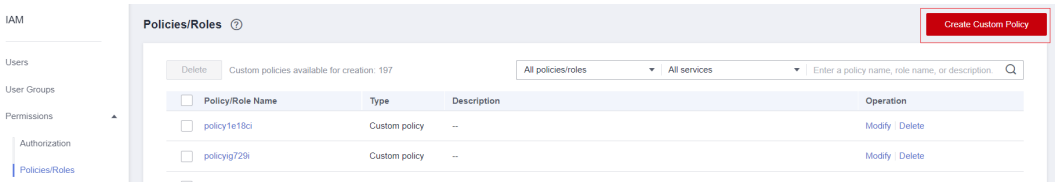
----Fim

Criação de uma política personalizada na visualização JSON

Passo 1 Faça login no console do IAM.

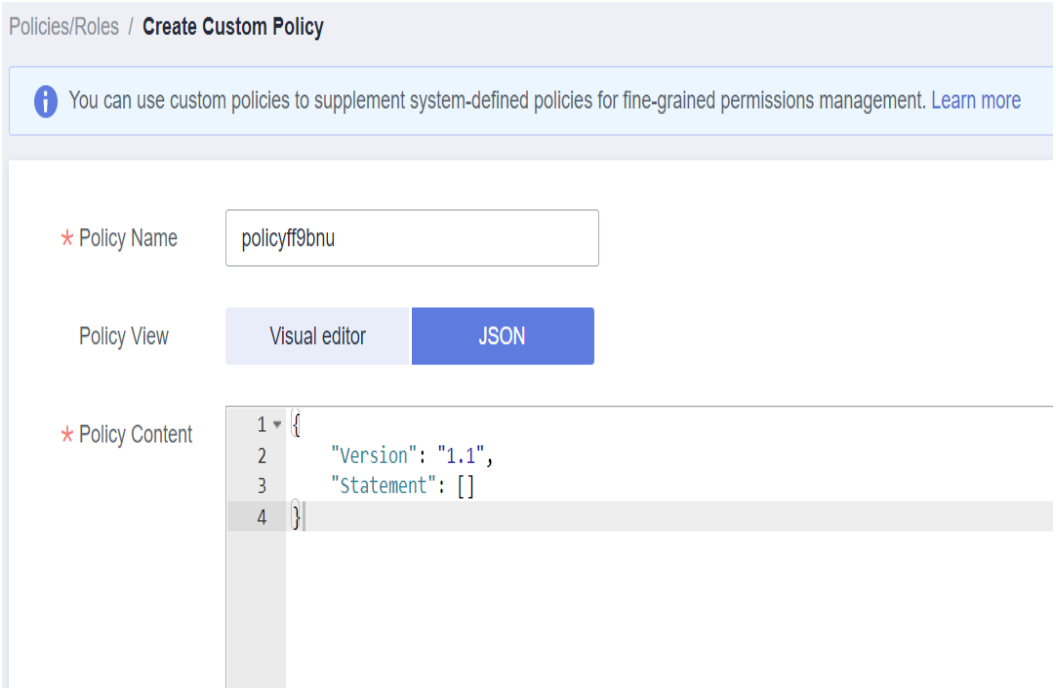
Passo 2 No console do IAM, escolha **Permissions** > **Policies/Roles** no painel de navegação e clique em **Create Custom Policy** no canto superior direito.

Figura 5-11 Criação de uma política personalizada



Passo 3 Insira um nome de política.

Figura 5-12 Inserção de 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 as 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**: Configure-o como **Allow** ou **Deny**.
- **Action**: Insira as ações listadas na tabela de ações da API (consulte **Figura 5-13**) do serviço EVS, por exemplo, **evs:volumes:create**.

Figura 5-13 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 do sistema**.

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

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

Passo 10 Atribuição da política a um grupo de usuários. Em seguida, os utilizadores do grupo herdam as permissões definidas nesta política.

NOTA

Você pode anexar políticas personalizadas a um grupo de usuários da mesma forma que você anexa políticas definidas pelo sistema. Para obter 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

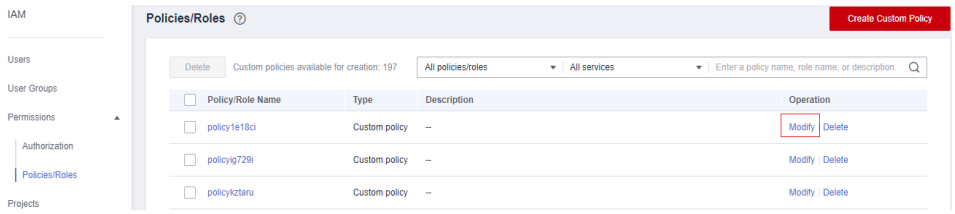
Você pode modificar ou excluir políticas personalizadas.

Modificanção de uma política personalizada

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

1. No painel de navegação 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 à página de detalhes da política.

Figura 5-14 Modificação do 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.

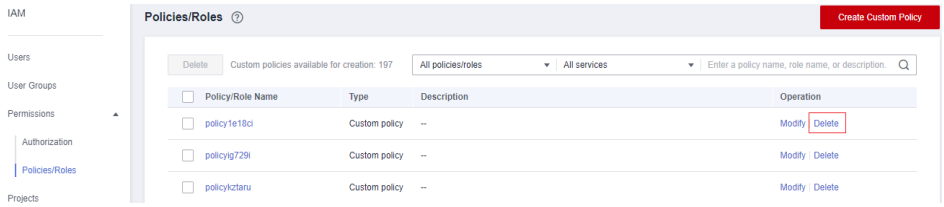
Exclusão de uma política personalizada

NOTA

Somente políticas personalizadas que não estão 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, desanexar a política e, em seguida, excluí-la.

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

Figura 5-15 Exclusão de 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 de permissão total

Se você quiser atribuir permissões completas a um usuário, mas não permitir que ele acesse um serviço específico, como o CTS (Cloud Trace Service), 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 sobrepõe-se a qualquer permissão, o usuário pode executar operações em todos os serviços, exceto o CTS.

Política de exemplo negando acesso somente ao CTS:

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

NOTA

- **Action**: Operações a serem realizadas. Cada action 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 do CTS.
- **Effect**: Determina se deve negar ou permitir a operação.

Uso de uma política personalizada junto com políticas definidas pelo sistema

- Se você quiser atribuir permissões completas a um usuário, mas não permitir através de criar BMSs, crie uma política personalizada negando a action **bms:servers:create** e anexe essa política personalizada junto com a política **BMS FullAccess** ao usuário. Como uma negação explícita em qualquer política sobrepõe-se a qualquer permissão, o usuário pode executar operações em todos os serviços no BMS, exceto a criação dos BMSs.

  Exemplo de política negando a criação do BMS:

  ```
  {
      "Version": "1.1",
  ```



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

- Se você quiser atribuir permissões somente leitura do OBS a todos os usuários, mas não permitir que determinados usuários exibam recursos específicos, por exemplo, não permite que usuários cujos nomes começam com **TestUser** exibam buckets cujos nomes começam com **TestBucket**, criando uma política personalizada para negar tais operações e anexar essa política personalizada juntamente com a política OBS ReadOnlyAccess para esses usuários. Como uma negação explícita em qualquer política sobrepõe-se a qualquer permissão, certos usuários não podem ver buckets cujos nomes começam com **TestBucket**.

  Exemplo de política que impede que usuários cujos nomes começam com **TestUser** exibam 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.

Usar apenas uma política personalizada

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

- Veja a seguir um exemplo de política que permite acesso somente a ECS, EVS, VPC, ELB e AOM (Application Operations Management).

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow"
                        "Action": [
```



```
                                "ecs:*:*",
                                "evs:*:*",
                                "vpc:*:*",
                                "elb:*:*",
                                "aom:*:*"
                        ],
                }
        ]
}
```

- Veja a seguir um exemplo de política que permite apenas que usuários do IAM cujos nomes começam com **TestUser** para excluir 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 suportados pelo IAM

Se você quiser conceder permissões de 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 permissões a um usuário do IAM 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 oferecem suporte à autorização de nível de recurso e os tipos de recursos suportados.

Tabela 5-9 Serviços de nuvem que suportam autorização de nível de recurso e os tipos de recursos suportados

Serviço	Tipo de recurso	Nome do recurso
Object Storage Service (OBS)	bucket	Bucket
	object	Objeto
Intelligent EdgeFabric (IEF)	product	Produto
	node	nó da borda
	group	Grupo de nós da borda
	deployment	implantação
	batchjob	Trabalho em lote
	application	Modelo de aplicação
	appVersion	Versão do modelo de aplicação
	IEFInstance	Instância IEF
Data Lake Insight (DLI)	queue	Fila DLI
	database	Banco de dados DLI
	table	Tabela DLI
	column	Coluna DLI
	datasourceauth	Informações de autenticação de segurança DLI
	jobs	Trabalho DLI
Graph Engine Service (GES)	graphName	Nome do gráfico GES
	backupName	Nome do backup GES
FunctionGraph	function	Função
	trigger	Gatilho
Distributed Message Service (DMS)	rabbitmq	Instância RabbitMQ
	kafka	Instância Kafka
Data Encryption Workshop (DEW)	KeyId	ID de chave
Data Warehouse Service (DWS)	cluster	Cluster

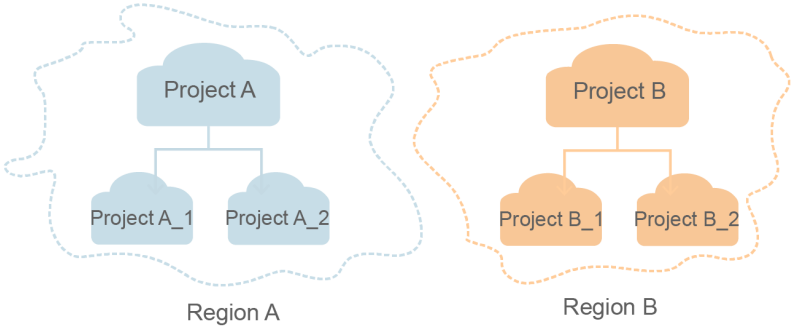
6 Projetos

Os projetos são usados para isolar recursos (incluindo recursos de computação, armazenamento e rede) entre 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, fornece aos usuários permissões para acessar recursos em subprojetos específicos.

Projetos IAM são diferentes de projetos empresariais. Para obter mais informações, consulte **Diferenças entre projetos do IAM e projetos empresariais**.

Figura 6-1 Isolamento do projeto



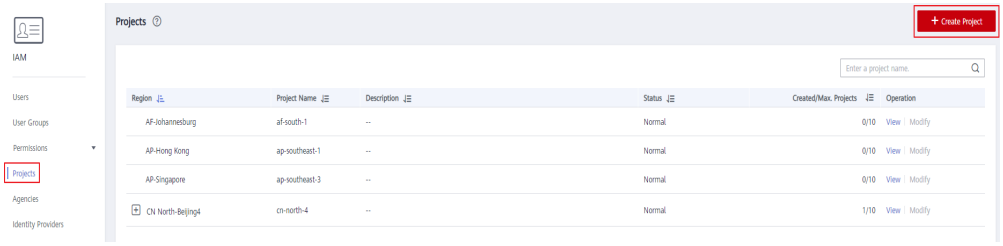
NOTA

- Os recursos não podem ser transferidos entre projetos do IAM.
- Não é possível criar projetos no IAM após habilitar a função Projeto empresarial.

Criação de um projeto

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

Figura 6-2 Criação de 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) Inserir uma descrição para o projeto.

Passo 5 Clique em **OK**.

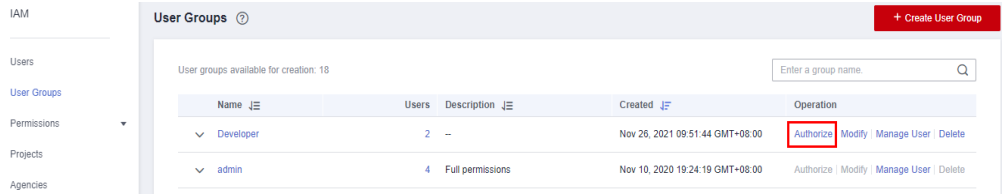
----Fim

Atribuição de permissões a um grupo de usuários baseada em 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 alvo.

Figura 6-3 Gerenciamento de permissões



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

Passo 3 Especifique o escopo de 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

Mudação de regiões ou projetos

Para serviços de nível de projeto, mude para uma região ou projeto no qual você tenha sido autorizado a acessar serviços de nuvem. Você não precisa mudar de regiões ou projetos para serviços globais.

Passo 1 Faça login no console de gerenciamento da HUAWEI CLOUD.

Passo 2 Aceda a uma página de serviço de nuvem de nível de 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 perimte que você delegue outra conta para implementar O&M em seus recursos com base nas permissões atribuídas.

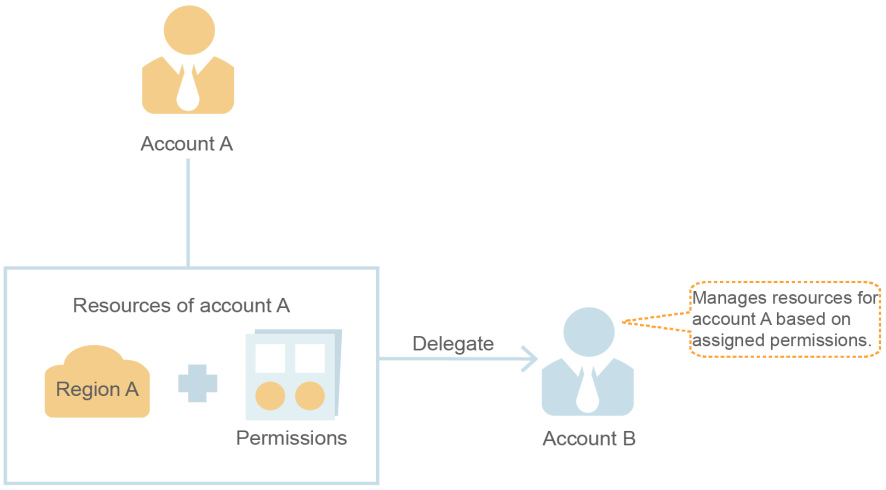
NOTA

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 de uma conta para 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.

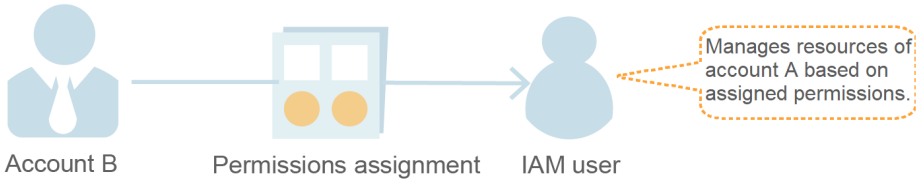
Figura 7-1 (Conta A) Criação de uma agência



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

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

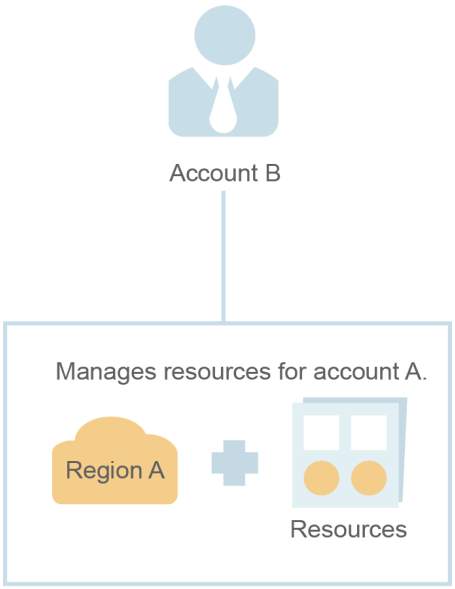
Figura 7-2 (Conta B) Autorização de um usuário do IAM a gerenciar recursos delegados



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

1. Faça login na conta da conta B e mude 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) Alternação da 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 e as chaves de acesso) com a parte delegada. Em vez disso, a parte delegada pode fazer login 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:

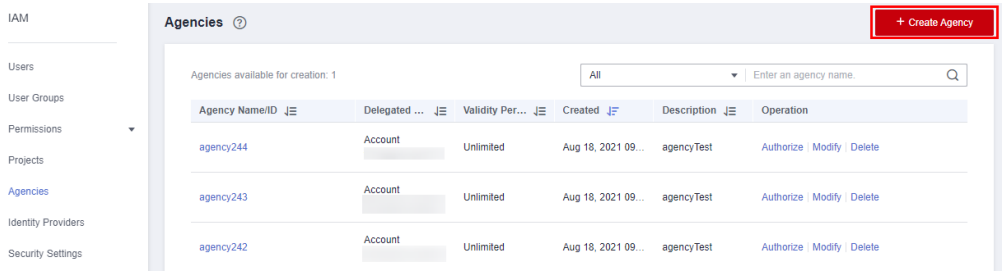
- Entenda os **conceitos básicos** de permissões.
- Determine as **permissões do sistema** a serem atribuídas à agência e verifique se as permissões têm dependências. Para obter mais detalhes, consulte **Atribuição de funções de dependência**.

Procedimento

Passo 1 Faça login no console do IAM.

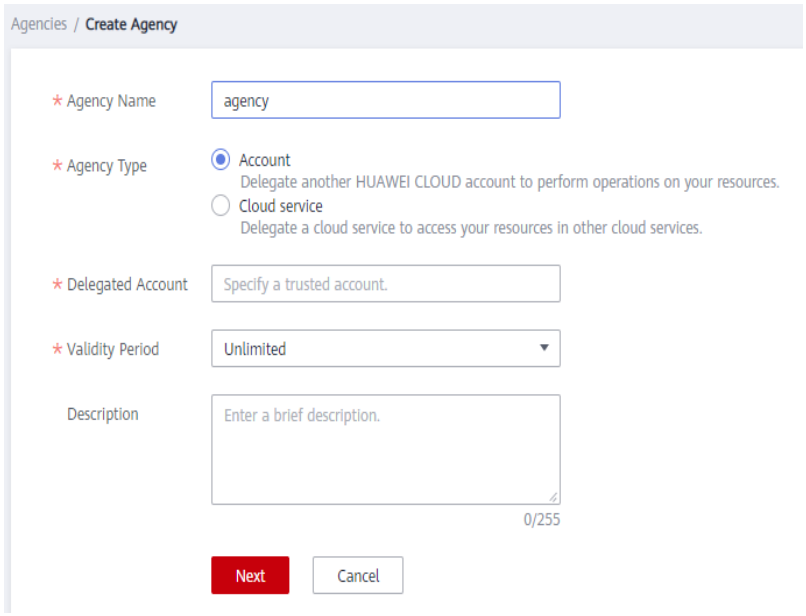
Passo 2 No console do IAM, escolha **Agencies** no painel de navegação e clique em **Create Agency** no canto superior direito.

Figura 7-4 Criação de uma agência



Passo 3 Insira um nome de agência.

Figura 7-5 Configuração do nome da agência



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

NOTA

- **Account**: Compartilhar seus recursos com outra conta ou delegar 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**: Delegar um serviço específico para acessar outros serviços. Para obter mais informações, consulte **7.2 Delegação de serviço 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

- Atribuir permissões a uma agência é semelhante a atribuir 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**.
- Não é possível atribuir às agências a função **Security Administrator**. Para a segurança da conta, conceda as permissões necessárias às agências com base no princípio do privilégio mínimo.

Passo 8 Clique em **OK**.

NOTA

Depois de criar uma agência, forneça o nome da conta, o nome da agência, o ID da agência e as permissões da agência à 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, apenas a sua conta e os membros do grupo do **admin** podem gerir 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 Criar um grupo de usuários e atribua 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

   Esse passo é usado 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 o nome de uma 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

   - Substituir *b36b1258b5dc41a4aa8255508xxx...* com o ID da agência obtido de uma parte delegante. Não faça nenhuma outra alteração.
   - Para obter mais informações sobre permissões, consulte **5 Permissões**.

   e. Clique em **Next**.
6. Selecione a política criada no passo anterior ou a função **Agent Operator** e clique em **Next**.
   - Políticas personalizadas: Permite que um usuário gerencie recursos apenas para uma agência específica.
   - Função **Agent Operator**: Permite que um usuário gerencie recursos para todas as agências.
7. Especifique o escopo de autorização.
8. Clique em **OK**.

Passo 2 Criar um usuário do IAM e adicionar o usuário ao grupo de usuários.

1. Na página **Users**, clique em **Create User**.
2. Na página **Create User**, insira um nome de usuário.
3. Para o tipo de acesso, selecione **Management console access** e **Set by user**.
4. Ative a proteção de login 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 sob a conta.

----Fim

Operações relacionadas

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

7.1.4 Mudança de funções (por uma parte delegada)

Quando uma conta estabelece uma relação de confiança com a sua conta, torna-se uma parte delegada. Você e todos os usuários autorizados podem alternar para a conta delegante e gerenciar recursos sob a conta com base nas permissões atribuídas.

Pré-requisitos

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

Procedimento

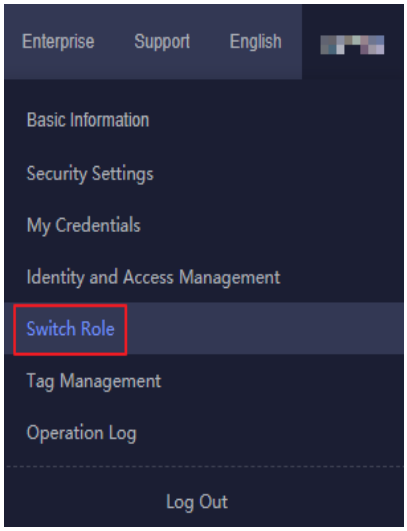
Passo 1 Faça login no console da HUAWEI CLOUD usando sua conta ou faça login como o usuário do IAM criado em **Passo 2**.

NOTA

O usuário do IAM criado em **Passo 2** de **7.1.3 (Opcional) Atribuição de permissões a um usuário do IAM (por uma parte delegada)** pode alternar funções para gerenciar recursos para a parte delegante.

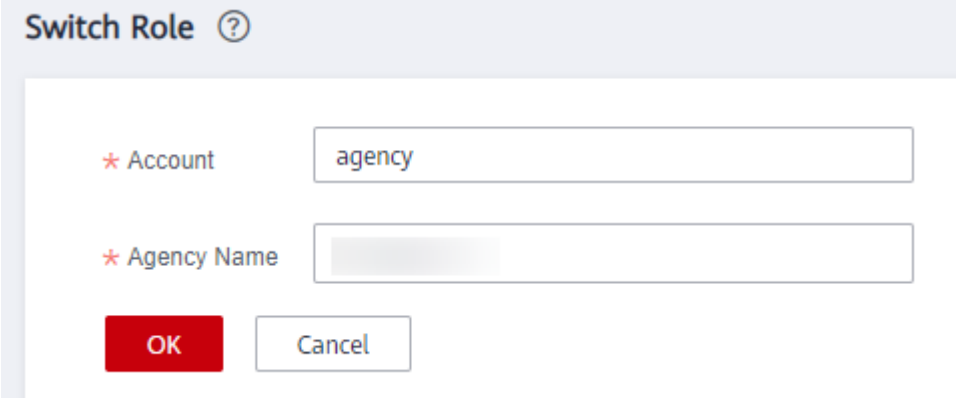
Passo 2 Passe o ponteiro do mouse sobre o nome de usuário no canto superior direito e escolha **Switch Role**.

Figura 7-6 Mudança da função



Passo 3 Na página **Switch Role**, insira 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 de inserir um nome de conta, as agências criadas sob essa conta serão automaticamente exibidas 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 delegante.

----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 Delegação de serviço de nuvem

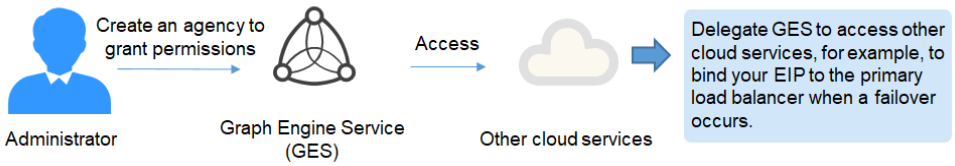
Serviços da HUAWEI CLOUD interagem um ao outro, e alguns serviços de nuvem dependem de outros serviços. Para delegar um serviço de nuvem para acessar outros serviços e executar O&M de recursos, crie uma agência para o serviço.

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

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

   A seguir, uma agência do GES (Graph Engine Service) é usada como exemplo. A agência permite que o GES use outros serviços de nuvem, por exemplo, para vincular seu EIP ao balanceador de carga primário se ocorrer um failover.

Figura 7-8 Delegação de serviço de nuvem



2. Criar automaticamente uma agência de serviços em nuvem para usar determinados recursos

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

   a. Acesse o console do SFS.

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

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

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

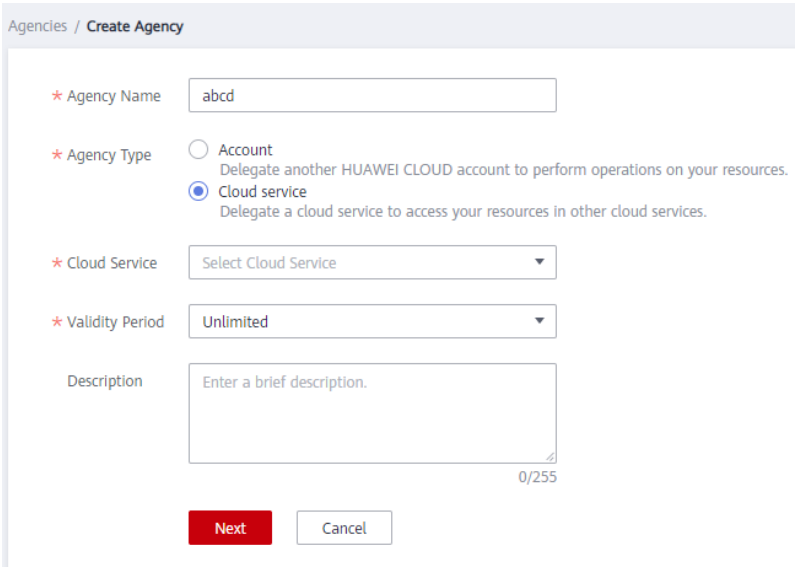
Criação de uma agência de serviço de nuvem no console do IAM

Passo 1 Faça login 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 de **Cloud service** e, em seguida, selecione um serviço.

Passo 5 Selecione um período de validade.

Passo 6 (Opcional) Inserir 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**.

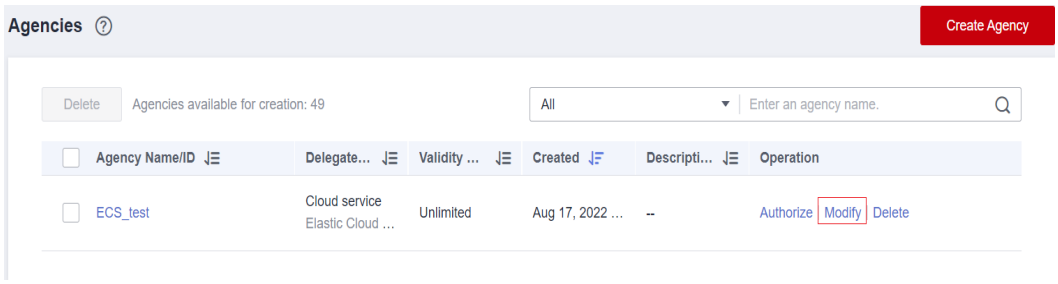
----Fim

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



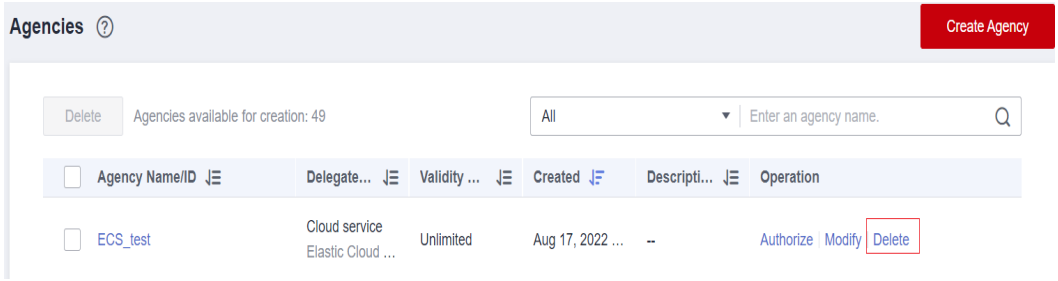
NOTA

- 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.
- Modificar as 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**.

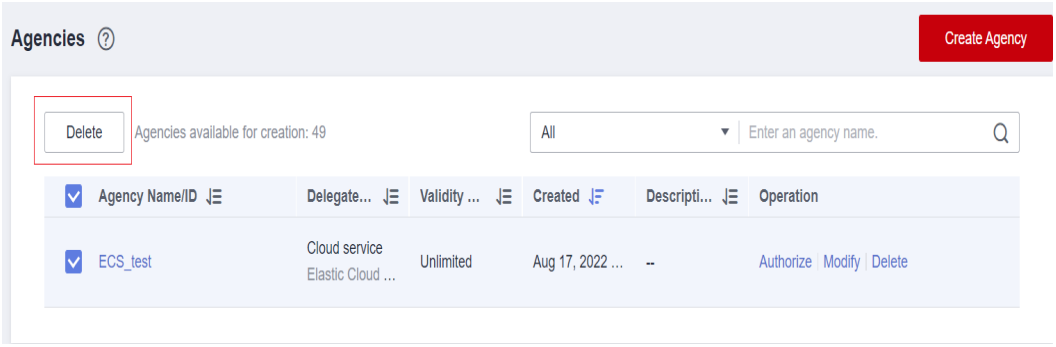
Figura 7-11 Exclusão de uma agência



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 configurar as configurações da conta, a autenticação de operação crítica, a política de autenticação de login, 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 operação crítica**, **8.4 Política de autenticação de acesso**, **8.5 Política de senhas**, e **8.6 ACL**. Este capítulo descreve como acessar a página **Security Settings** e quem é o público-alvo pretendido.

Público-alvo pretendido

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

Tabela 8-1 Público-alvo pretendido

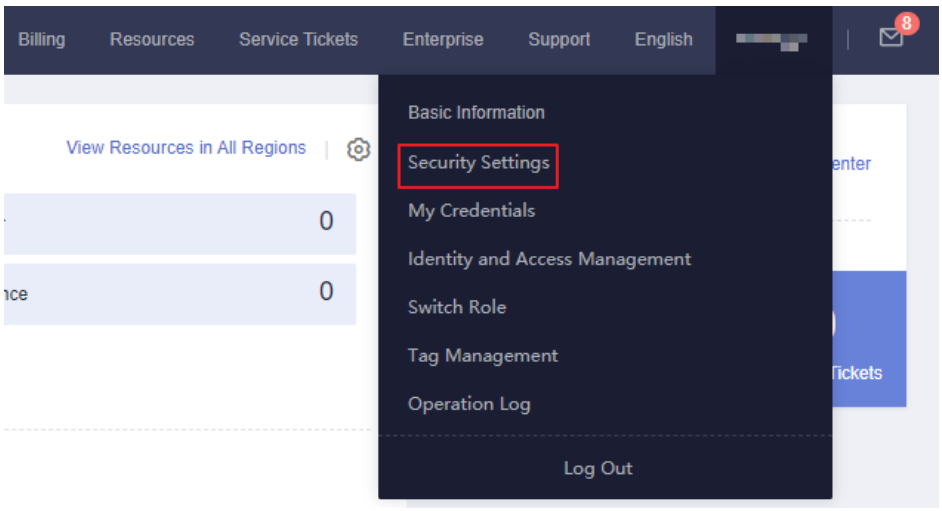
Função	Público-alvo pretendido
Informações básicas	● Usuários do IAM: Acesso completo ● Conta: Para alterar as informações básicas, consulte Informações básicas.
Operações críticas	● **Administrador**: Acesso completo ● Usuários do IAM: Sem acesso

Função	Público-alvo pretendido
Política de autenticação de acesso	● **Administrador**: Acesso completo ● Usuários do IAM: Acesso somente leitura
Política de senhas	● **Administrador**: Acesso completo ● Usuários do IAM: Acesso somente leitura
ACL	● **Administrador**: Acesso completo ● Usuários do IAM: Sem acesso

Acesso à página de configurações de segurança

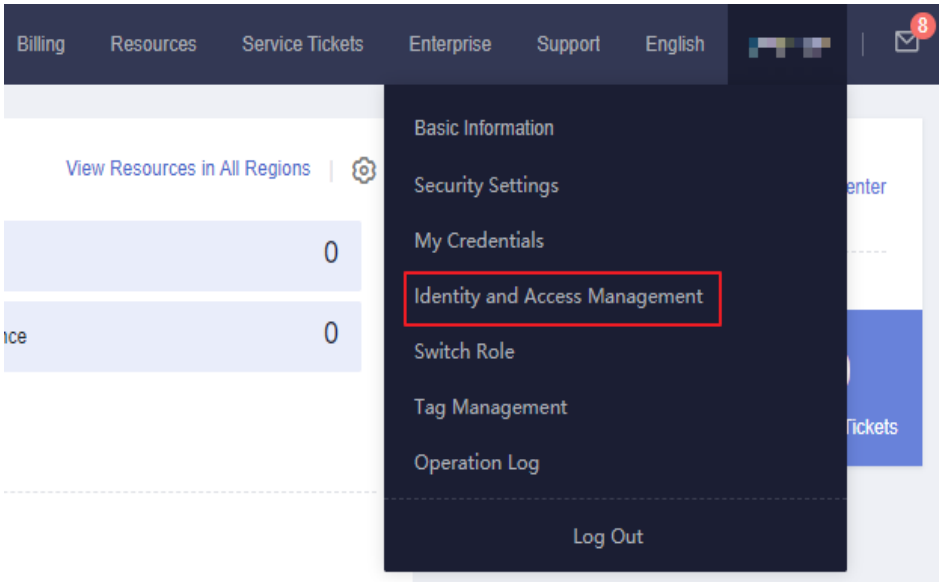
- Você e todos os usuários do IAM criados usando sua conta podem acessar a página **Security Settings** no console de gerenciamento.
  a. Faça login na HUAWEI CLOUD e clique em **Console** no canto superior direito.
  b. No console de gerenciamento, passe o ponteiro do mouse sobre o nome de usuário no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

  Figura 8-1 Acesse a página de configurações de segurança



- Como um **administrador**, você também pode acessar a página **Security Settings** no console do IAM.
  a. Faça login 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 do IAM



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

8.2 Informações básicas

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

NOTA

- Um número de celular ou um endereço de e-mail podem ser vinculados apenas a uma conta ou usuário do IAM.
- Somente um número de celular, endereço de e-mail, e MFA virtual podem ser vinculados a uma conta ou usuário do IAM.

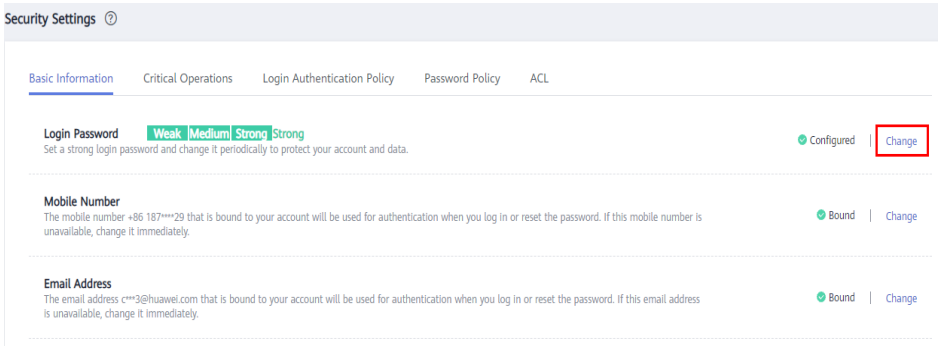
Alteração da senha de login, número de celular, ou o endereço de e-mail

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

Passo 1 Acesse a página **Security Settings**.

Passo 2 Clique na guia **Account Settings** e clique em **Change** na linha **Login Password**.

Figura 8-3 Alteração da senha de login



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

NOTA

Os dois modos de verificação estão disponíveis apenas se você tiver vinculado um endereço de e-mail e um número de celular.

Passo 4 Insira a senha antiga e a nova senha e a nova senha novamente.

NOTA

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

Passo 5 Clique em **OK**.

----Fim

8.3 Proteção de operação crítica

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

Os usuários federados não precisam verificar sua identidade ao executar operações críticas.

Dispositivo MFA virtual

Um dispositivo MFA gera códigos de verificação de 6 dígitos em conformidade com o TOTP (Time-based One-time Password Algorithm). Os dispositivos MFA podem ser baseados em hardware ou software. Atualmente, apenas dispositivos MFA virtuais baseados em software são suportados e são programas de aplicações executados em dispositivos inteligentes, como celulares.

Esta seção descreve como vincular um dispositivo MFA virtual, por exemplo, a aplicação HUAWEI CLOUD. Se você instalou outra aplicação 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 MFA virtual**.

O método para vincular um dispositivo MFA virtual varia dependendo se sua conta da HUAWEI CLOUD foi atualizada para um HUAWEI ID.

NOTA

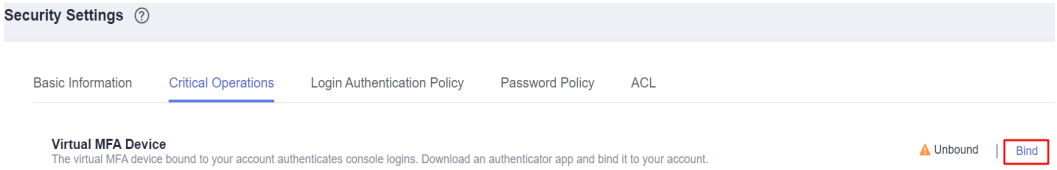
Antes de vincular um dispositivo MFA virtual, certifique-se de que você instalou uma aplicação MFA (como a aplicação Authenticator) em seu dispositivo móvel.

- **Conta da HUAWEI CLOUD**

Passo 1 Acesse a página **Security Settings**.

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

Figura 8-4 Dispositivo MFA virtual



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

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

- Digitalização do código QR

  Abra a aplicação MFA em seu celular e use a aplicação para digitalizar o código QR exibido na página **Bind Virtual MFA Device**. Sua conta é então adicionada à aplicação.

- Inserir manualmente a chave secreta

  Abra a aplicação MFA no seu celular e insira a chave secreta.

  NOTA

  Sua conta é adicionada manualmente usando o algoritmo baseado em tempo. Certifique-se de que a definição automática da hora foi activada no seu celular.

Passo 4 Visualize o código de verificação na aplicação 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**.

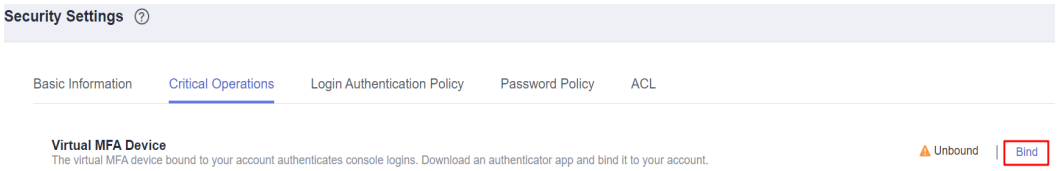
----Fim

- **HUAWEI ID**

Passo 1 Acesse a página **Security Settings**.

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

Figura 8-5 Vinculação de um dispositivo MFA virtual



Passo 3 Na página **Account & security** do centro de contas do HUAWEI ID, associe um autenticador ao seu HUAWEI ID conforme as instruções.

----Fim

Proteção de login

Depois de a proteção de login for 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 login. **Habilitar esta função para a segurança da conta.**

Para a conta, somente o administrador da conta pode habilitar a proteção de login para ela. Para usuários do IAM, o administrador da conta e outros administradores podem habilitar esse recurso para os usuários.

- **(Administrador) Habilitação da proteção de login para um usuário do IAM**

  Para habilitar a proteção de login 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 exibida **Security Settings**, clique em ao lado de **Verification Method** e selecione um método de verificação de SMS, e-mail ou dispositivo MFA virtual.

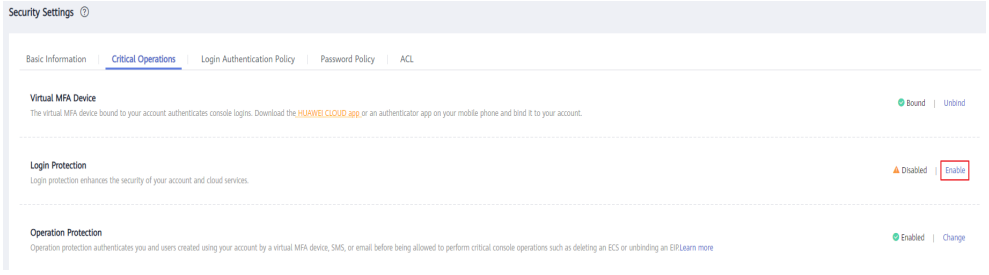
  NOTA

  Depois de habilitar a proteção de login, os usuários do IAM precisam realizar 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.

- **Habilitação da proteção de login para sua conta da HUAWEI CLOUD**

  Se a sua conta HUAWEI CLOUD não tiver sido atualizada para um HUAWEI ID, pode habilitar a proteção de login na página **Security Settings**. Acesse a página **Security Settings** e clique na guia **Critical Operations**. Clique em **Enable** ao lado de **Login Protection**, selecione um método de verificação, insira o código de verificação e clique em **OK**.

  Figura 8-6 Configuração da proteção de login

- **Habilitação da proteção de login para seu HUAWEI ID**

Se a sua conta da HUAWEI CLOUD não tiver sido atualizada para um HUAWEI ID, pode habilitar a proteção de login no centro de conta do HUAWEI ID. Acesse a **HUAWEI ID account center**, 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 login com um HUAWEI ID. Se você usar um novo terminal para fazer login, você será autenticado com seu número de celular de segurança no primeiro login. Se a verificação em duas etapas não estiver ativada, clique em **Trust** para adicionar seu terminal à lista de permissões. Então você não precisará mais realizar autenticação ao fazer login usando este terminal na próxima vez.

Proteção da operação

- **Habilitação da proteção de Operação**

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

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

Passo 1 Acesse a página **Security Settings**.

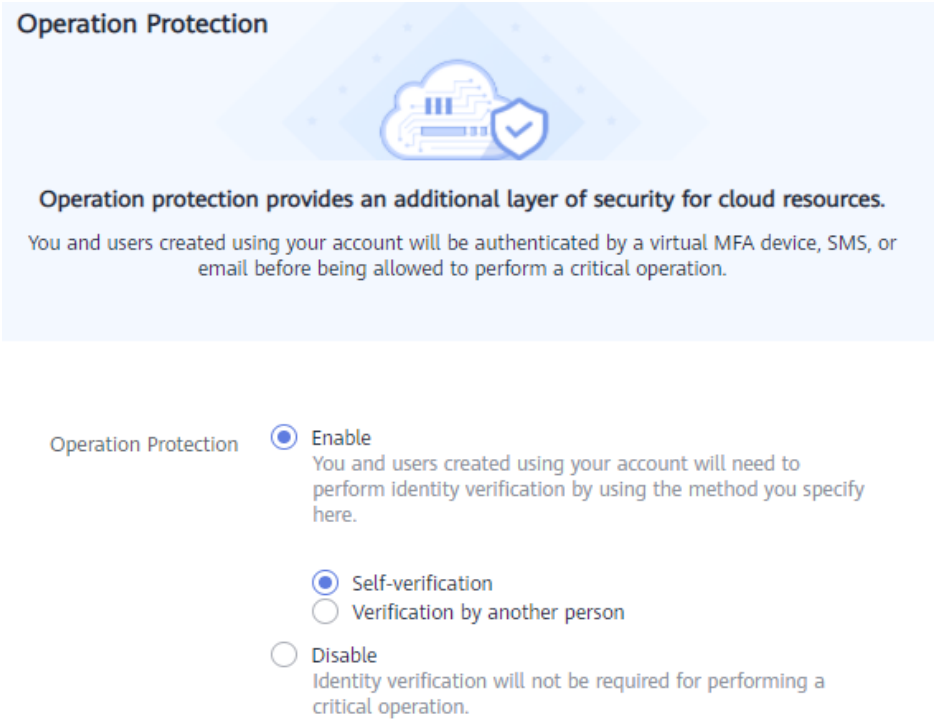
Passo 2 Clique na guia **Critical Operations** na página **Security Settings**, clique em **Enable** ao lado de **Operation Protection**, selecione **Enable** e clique em **OK**.

Figura 8-7 Habilitação da proteção de operação

Passo 3 Selecione **Enable** e 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 de operação



- **Auto-verificação**: Você ou os próprios usuários do IAM executam verificação ao executar uma operação crítica.
- **Verificação por outra pessoa**: A pessoa especificada conclui a verificação quando você ou os usuários do IAM executam uma operação crítica. Apenas verificações de SMS e e-mail são suportadas.

Passo 4 Clique em **OK**.

----Fim

- **Desabilitação da proteção de operação**

Se a proteção de 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**.

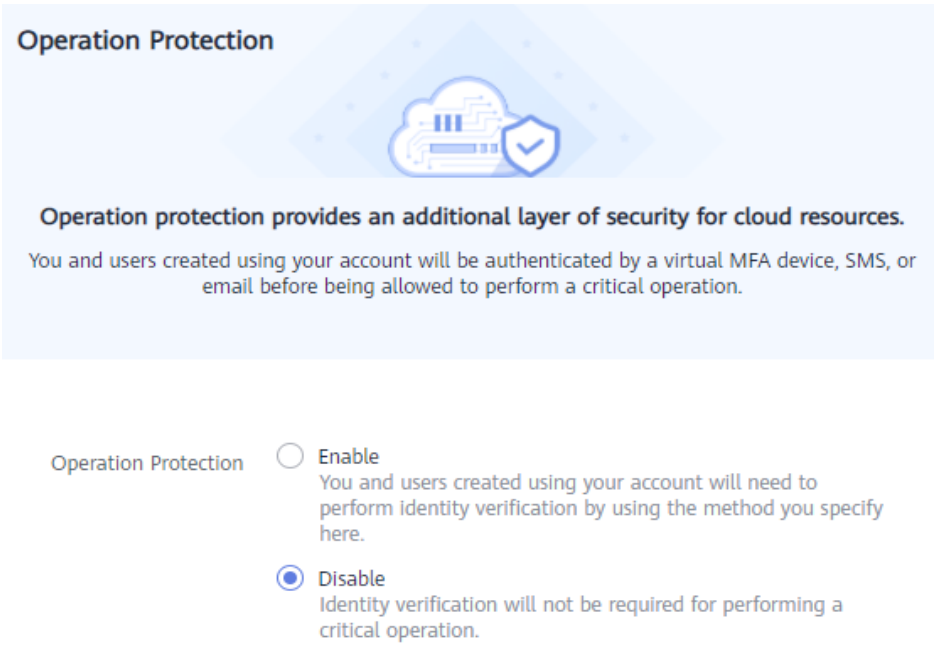
Passo 1 Acesse a página **Security Settings**.

Passo 2 Clique na guia **Critical Operations** na página **Security Settings**, clique em **Change** na linha **Operation Protection**.

Figura 8-9 Desabilitação da proteção de operação

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

Figura 8-10 Desabilitação da proteção de operação



Passo 4 Insira um código de verificação.

- **Auto-verificação**: O administrador que deseja desabilitar a proteção de operação conclui a verificação. As verificações de SMS, e-mail e MFA virtual são suportadas.
- **Verificação por outra pessoa**: A pessoa especificada conclui a verificação. Apenas verificações de SMS e e-mail são suportadas.

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 MFA virtual.
  - Se um usuário estiver associado apenas a um número de celular, apenas a verificação por SMS estará disponível.
  - Se um usuário estiver associado apenas a um endereço de e-mail, apenas a verificação de e-mail estará disponível.
  - Se um usuário não estiver associado a um endereço de e-mail, número de celular ou dispositivo MFA virtual, o usuário precisará associar pelo menos um deles antes que o usuário possa executar quaisquer operações críticas.
- Códigos de verificação de e-mail ou SMS podem não ser recebidos devido a erros de comunicação. É aconselhável usar um dispositivo MFA virtual.
- **Você pode alterar o número de celular ou endereço de e-mail em Minha Conta e alterar o dispositivo MFA virtual na página Configurações de segurança do console do IAM.**
- Se a proteção de operação estiver ativada, os usuários IAM precisarão inserir um código de verificação ao executar uma operação crítica. O código de verificação é enviado para o número de celular ou endereço de e-mail vinculado aos usuários do IAM.

Gerenciamento de chaves de acesso

- **Habilitação do gerenciamento de chaves de acesso**

  Depois de o gerenciamento de chaves de acesso estar habilitado, somente o administrador poderá criar, habilitar, desabilitar ou excluir chaves de acesso de usuários do IAM. Esta função está desabilitada por padrão. Para garantir a segurança do recurso, habilite essa função.

  Para habilitar o gerenciamento de chaves de acesso, clique na guia **Critical Operations** na página **Security Settings** e clique em  ao lado de **Access Key Management**.

- **Desabilitação do gerenciamento de chaves de acesso**

  Depois de o gerenciamento de chaves de acesso estar desabilitado, todos os usuários do IAM poderão criar, habilitar, desabilitar ou excluir suas próprias chaves de acesso.

  Para habilitar o gerenciamento de chaves de acesso, clique na guia **Critical Operations** na página **Security Settings** e clique em  na linha **Access Key Management**.

Autogerenciamento de informações

- **Habilitação do autogerenciamento de informações**

  Por padrão, o autogerenciamento de informações é habilitado, indicando que todos os usuários do IAM podem gerenciar suas próprias **informações básicas** (senha de login, 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 habilitar o autogerenciamento de chaves de acesso, clique na guia **Critical Operations** na página **Security Settings** e clique em **Enable** ao lado de **Information Self-Management**. Selecione em **Enable**, selecione os tipos de informações que os usuários do IAM podem modificar e clique em **OK**.

- **Desabilitação do autogerenciamento de informações**

  Depois de desabilitar o autogerenciamento de informações, somente os administradores podem gerenciar suas próprias **informações básicas**. Se os usuários do IAM precisarem modificar a senha de login, o número de celular ou o endereço de e-mail, eles poderão entrar em contato com o administrador. Para obter detalhes, consulte **3.4 Exibição ou modificação das informações do usuário do IAM**.

  Para habilitar o autogerenciamento de informações, clique na guia **Critical Operations** na página **Security Settings** 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

Tipo de serviço	Serviço	Operação crítica
Computação	Elastic Cloud Server (ECS)	● Interrupção, reiniciação ou exclusão de um ECS ● Redefinição da senha para fazer login em um ECS ● Desanexação de um disco ● Desvinculação de um EIP
	Bare Metal Server (BMS)	● Interrupção ou reiniciação de um BMS ● Redefinição da senha BMS ● Desanexação de um disco ● Desvinculação de um EIP
	Auto Scaling (AS)	Exclusão de um grupo AS
Armazenamento	Object Storage Service (OBS)	● Exclusão de um bucket ● Criação, edição ou exclusão de uma política de bucket ● Configuração de uma política de objetos ● Criação, edição ou exclusão de uma ACL de bucket ● Configuração do registro de acesso ● Configuração da validação de URL ● Criação ou edição de um inventário de bucket
	Elastic Volume Service (EVS)	Exclusão de um disco EVS
	Content Delivery Network (CDN)	Configuração de política de encerramento de serviço
Contêineres	Cloud Container Engine (CCE)	Exclusão de um cluster
	Application Orchestration Service (AOS)	Exclusão de uma pilha
Rede	Domain Name Service (DNS)	● Modificação, suspensão ou exclusão de um nome de domínio ● Modificação, desabilitação ou exclusão de um conjunto de registros ● Modificação ou exclusão de um registro PTR ● Exclusão de uma linha personalizada

Tipo de serviço	Serviço	Operação crítica
	Virtual Private Cloud (VPC)	● Desvinculação de um EIP ● Exclusão de uma conexão de emparelhamento de VPC ● Operações de grupo de segurança – Exclusão de uma regra de entrada ou de saída – Modificação de uma regra de entrada ou de saída – Exclusão de regras de entrada ou saída
	Elastic Load Balance (ELB)	● Balanceadores de cargas clássicos – Exclusão de um balanceador de carga – Exclusão de um ouvinte – Exclusão de um certificado – Desabilitação de um balanceador de carga ● Balanceadores de cargas compartilhadoes – Exclusão de um balanceador de carga – Exclusão de um ouvinte – Exclusão de um certificado – Removimento de um servidor de back-end – Desvinculação de um EIP – Desvinculação de um endereço IPv4 privado ou público – Desvinculação de um endereço IPv6 – Removimento da largura de banda compartilhada IPv6
	Elastic IP (EIP)	● Exclusão de uma largura de banda compartilhada ● Liberação ou desvinculação de um EIP ● Liberação ou desvinculação dos EIPs
	Virtual Private Network (VPN)	● Exclusão de uma conexão VPN ● Cancelamento da assinatura de um gateway VPN anual/mensal
	Direct Connect	Exclusão de uma interface virtual
Segurança e conformidade	SSL Certificate Manager (SCM)	● Exclusão de um certificado ● Revogação de um certificado

Tipo de serviço	Serviço	Operação crítica
Gerenciamento e governança	Identity and Access Management (IAM)	● Desabilitação da proteção de operação ● Desabilitação da proteção de login ● Alteração do número de celular ● Alteração do endereço de e-mail ● Alteração da senha de login ● Alteração do método de autenticação de login
	Cloud Trace Service (CTS)	Desabilitação de um rastreador do sistema
	Log Tank Service (LTS)	● Exclusão de um fluxo de logs ou grupo de logs ● Desinstalação do ICAgent
Aplicação	Distributed Cache Service (DCS)	● Redefinição da senha de uma instância do DCS ● Exclusão de uma instância do DCS ● Eliminação dos dados de instância do DCS
Nuvem dedicada	Dedicated Distributed Storage Service (DSS)	Exclusão de um disco

Tipo de serviço	Serviço	Operação crítica
Banco de dados	Relational Database Service (RDS)	● Redefinição da senha do administrador ● Reinicialização, exclusão ou restauração de instâncias de banco de dados ● Exclusão de um backup de banco de dados ● Restauração da instância de banco de dados atual a partir de um arquivo de backup ● Restauração de uma instância de banco de dados existente a partir de um arquivo de backup ● Restauração da instância de banco de dados atual para um ponto no tempo ● Restaurando uma instância de banco de dados existente para um ponto no tempo ● Restauração de uma tabela para um ponto no tempo especificado ● Alternação entre instâncias de banco de dados primárias e em espera ● Alteração da porta do banco de dados ● Exclusão de uma conta de banco de dados ● Exclusão de um banco de dados ● Redefinição da senha de uma conta de banco de dados ● Alteração de um endereço IP flutuante ● Desvinculação de um EIP ● Habilitação ou desabilitação do relatório de alarme com um clique
	Document Database Service (DDS)	● Redefinição da senha ● Modificação ou exclusão de uma instância de banco de dados ● Reiniciação de um nó ● Alternação dos nós primário e secundário de um conjunto de réplicas ● Exclusão de uma regra de grupo de segurança ● Habilitação de endereços IP de nós de shard e config ● Restauração da instância de banco de dados atual a partir de um backup ● Restauração de uma instância de banco de dados existente a partir de um backup ● Alteração de uma instância anual/mensal para pagar por uso

Tipo de serviço	Serviço	Operação crítica
Inteligência empresarial	Data Warehouse Service (DWS)	● Dimensionamento ou redimensionamento de um cluster ● Reiniciação de um cluster ● Reparação de um nó ● Redefinição da senha
	MapReduce Service (MRS)	● Clusters – Exclusão de um cluster – Alteração de um cluster de pagar por uso para faturamento anual/mensal – Interrupção de todos os componentes – Sincronização de configurações de cluster ● Nós – Interrupção de todas as funções – Isolação de um host – Cancelamento do isolamento de um host ● Componentes – Desabilitação de um serviço – Reiniciação de um serviço – Realização de uma reinicialização do serviço de rolamento – Interrupção de uma instância de função – Reiniciação de uma instância de função – Realização de uma reinicialização da instância de rolamento – Recomissionamento de uma instância de função – Encerramento de uma instância de função – Guarda de configurações de serviço ● Patches – Instalação de um patch – Desinstalação de um patch – Reversão de um patch

Tipo de serviço	Serviço	Operação crítica
Comunicações em nuvem	Message&SMS	● Exclusão de uma assinatura ● Exclusão de um modelo ● Obtenção de um app_secret ● Vinculação de um número de celular ou endereço de e-mail a uma conta da HUAWEI CLOUD ● Configuração de uma lista de permissões de endereços IP ● Renovação de um pacote
DevCloud	ProjectMan	● Exclusão de um projeto ● Exclusão de um membro do projeto ● Modificação de informações do membro ● Modificação ou exclusão de permissões ● Modificação de informações básicas do projeto ● Exclusão de um item de trabalho
Suporte para usuários	Centro de cobrança	● Pagamento para um pedido ● Cancelamento da assinatura de um pedido ● Liberação de recursos

8.4 Política de autenticação de acesso

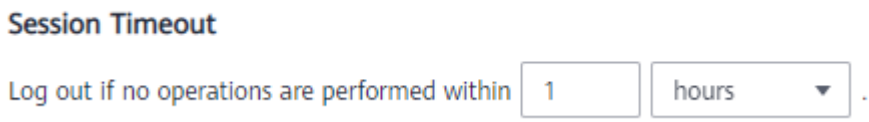
A guia **Login Authentication Policy** da página **Security Settings** fornece as configurações de **Tempo limite da sessão**, **Bloqueio de conta**, **Desabalitação de conta**, **Informações de login recentes**, e **Informações personalizadas**. Essas configurações entram em vigor para sua conta e para os usuários do IAM criados usando a conta.

Somente um **administrador** pode configurar a política de autenticação de login, 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.

Tempo limite da sessão

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

Figura 8-11 Tempo limite da sessão

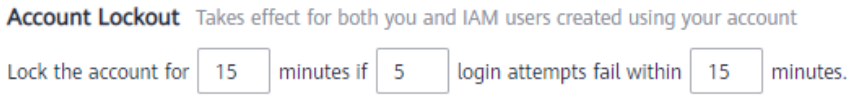


O tempo limite varia de 15 minutos a 24 horas, e o tempo limite padrão é de 1 hora.

Bloqueio de conta

Defina uma duração para bloquear os usuários se um número específico de tentativas de login malsucedidas for alcançado 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



Você pode definir o tempo para redefinir o contador de bloqueio de conta, o número máximo de tentativas de login malsucedidas e a duração do bloqueio de conta.

- Hora de redefinir o contador de bloqueio de conta: O valor varia de 15 a 60 minutos, e o valor padrão é **15 minutos**.
- Número máximo de tentativas de login malsucedidas: O valor varia de 3 a 10, e o valor padrão é de **5**.
- Duração do bloqueio: O valor varia de 15 a 30 minutos, e o valor padrão é **15 minutos**.

Desabalitação de conta

Defina um período de validade para desabilitar usuários do IAM se eles não tiverem acessado a HUAWEI CLOUD usando o console ou APIs dentro de um determinado período.

Essa opção está desabilitada por padrão. O prazo de validade varia de 1 a 240 dias.

Se você habilitar essa opção, a configuração entrará em vigor apenas para usuários do IAM criados usando sua conta. Se um usuário do IAM estiver desabilitado, ele poderá solicitar que o administrador habilite sua conta novamente.

Informações de login recentes

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

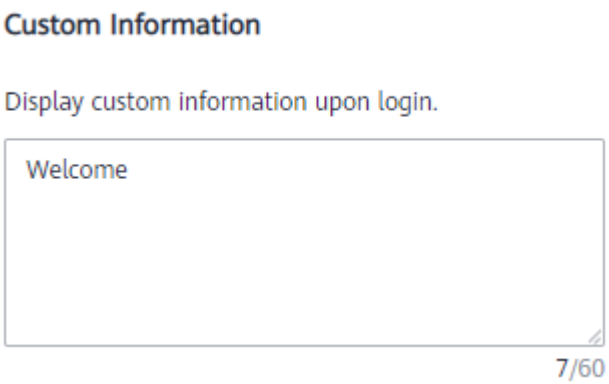
Essa opção está desabilitada por padrão e pode ser habilitada pelo administrador.

Informações personalizadas

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

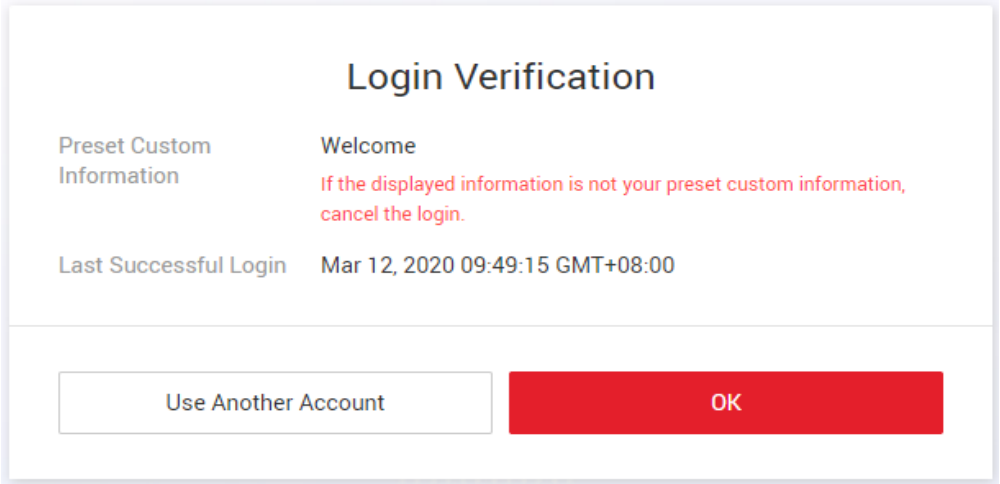
Nenhuma informação é exibida por padrão, e o administrador pode definir informações personalizadas que serão exibidas.

Figura 8-13 Informações personalizadas



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

Figura 8-14 Verificação de fazer login



8.5 Política de senhas

A guia **Password Policy** da página **Security Settings** fornece as configurações de **Composição e reutilização de senhas**, **Expiração de senha**, e **Duração mínima da senha**.

Somente um **administrador** pode configurar a política de senha 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.

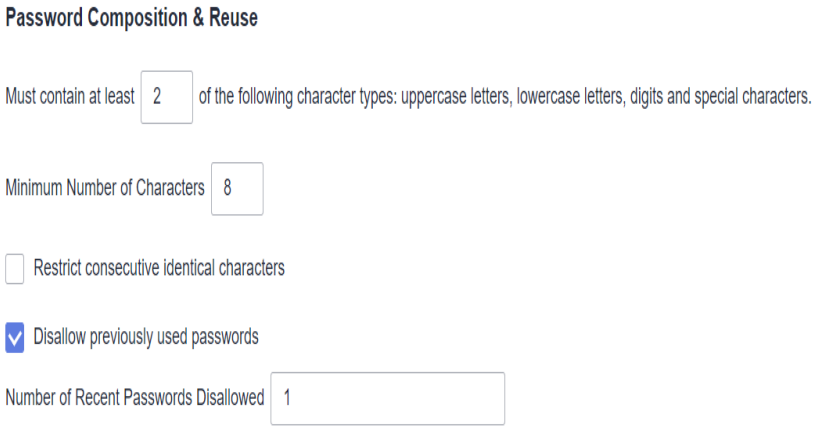
Você pode configurar a política de senha para garantir que os usuários do IAM criem senhas fortes e alterná-las periodicamente. Na política de senha, você pode definir requisitos de senha, como o comprimento mínimo da senha, se deve permitir caracteres idênticos consecutivos em uma senha e se deve permitir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

NOTA

Se sua conta da HUAWEI CLOUD já tiver sido atualizada para um 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 contenha 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 2 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) Habilite 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 os caracteres idênticos consecutivos não são permitidos em uma senha.
- (Opcional) Habilite 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 três últimas 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. Os usuários do IAM criados posteriormente também aderirão à política de senha atualizada

Expiração de 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 login na HUAWEI CLOUD.

Essa opção está desabilitada por padrão. O prazo 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 de 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 antiga.

Duração 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.

Essa opção está desabilitada por padrão. Se você habilitar essa opção, poderá definir um período de 0 a 1440 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 **Security Settings** fornece as configurações de **Intervalos de endereços IP**, **Blocos IPv4 CIDR**, e **VPC Endpoints** para permitir o acesso do usuário apenas de intervalos de endereços IP especificados, blocos IPv4 CIDR ou VPC endpoints.

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.

Tipo de acesso:

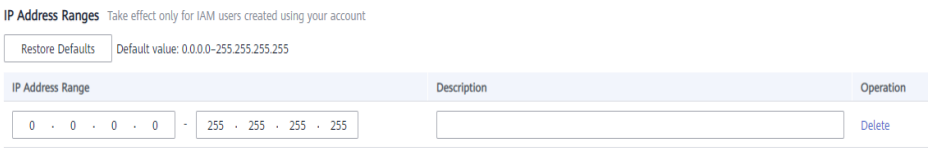
- **Console Access** (recomendado): A ACL entra em vigor apenas para usuários do IAM e usuários federados que são criados usando sua conta e têm acesso ao console.
- **API Access**: A ACL controla o acesso à API dos usuários por meio do API Gateway e entra em vigor apenas para usuários do IAM e usuários 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 proxy, defina os endereços IP permitidos, intervalos de endereços ou blocos CIDR 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, definia 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, seus usuários do IAM poderão acessar o console da HUAWEI CLOUD de qualquer lugar.

Blocos IPv4 CIDR

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

VPC Endpoints

Especifique VPC endpoints, 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 todo o VPC endpoints por padrão.

NOTA

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

9 Provedores de identidade

9.1 Introdução

A HUAWEI CLOUD fornece a função de provedor de identidade para implementar a autenticação de identidade federada com base 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).

O IAM suporta dois tipos de autenticação de identidade federada:

- Web SSO: Os navegadores são usados como meio de comunicação. Esse tipo de autenticação permite que usuários comuns acessem a HUAWEI CLOUD usando navegadores. Você pode implementar o SSO usando um dos seguintes métodos:
  - **Configure um link de login no sistema de gerenciamento empresarial**. Os usuários da sua empresa podem usar o link para fazer login na HUAWEI CLOUD a partir do sistema de gerenciamento empresarial.
  - Forneça o **link de login de usuário federado** aos usuários da sua empresa. Eles podem fazer login na HUAWEI CLOUD usando suas contas e senhas no sistema de gerenciamento empresarial.
- Chamada da API: Ferramentas de desenvolvimento (como OpenStack Client e ShibbolethECP Client) são usadas como meios de comunicação. Esse tipo de autenticação permite que os usuários empresariais e os usuários comuns acessem a HUAWEI CLOUD chamando as APIs.

Este capítulo descreve como acessar a HUAWEI CLOUD por meio de login via Web SSO. Para obter detalhes sobre como acessar a HUAWEI CLOUD chamando APIs, consulte **Gerenciamento de autenticação de identidade federada**.

Conceitos básicos

- Provedor de Identidade (IdP)

  Um provedor de identidade recolhe e armazena informações de identidade do usuário, como nomes de usuários e senhas, e autentica os usuários durante o login. Para a autenticação de identidade federada entre uma empresa e HUAWEI CLOUD, o sistema de autenticação de identidade da empresa é um provedor de identidade e também é chamado por "enterprise IdP". Os IdPs de terceiros populares incluem o Microsoft Active Directory Federation Services (AD FS) e Shibboleth.

- Provedor de serviços (SP)

  Um provedor de serviços estabelece uma relação de confiança entre um IdP e ele mesmo, e usa as informações do usuário fornecidas pelo IdP para fornecer serviços. Para a autenticação de identidade federada entre uma empresa e a HUAWEI CLOUD, HUAWEI CLOUD é um provedor de serviços.

- Autenticação de identidade federada

  A autenticação de identidade federada é um processo no qual **uma relação de confiança é estabelecida** entre um IdP e um SP para implementar o SSO.

- Logon único (SSO)

  O SSO é um tipo de acesso que permite que os usuários acessem um SP confiável após efetuar login no IdP empresarial. Por exemplo, após uma relação de confiança ser estabelecida entre um sistema de gerenciamento empresarial e HUAWEI CLOUD, os usuários no sistema de gerenciamento empresarial podem usar suas contas e senhas existentes para acessar a HUAWEI CLOUD através do link de login no sistema de gerenciamento empresarial.

- SAML 2.0

  O SAML 2.0 é um protocolo baseado em XML que usa securityTokens contendo asserções para passar informações sobre um usuário final entre um IdP e um SP. É um padrão aberto ratificado pela OASIS (Organização para o Avanço de Padrões de Informação Estruturada) e está sendo usado por vários IdPs. Para obter mais informações sobre esse padrão, consulte **Visão geral técnica do SAML 2.0**. A HUAWEI CLOUD implementa autenticação de identidade federada em conformidade com o SAML 2.0. Para federar com sucesso os usuários existentes à HUAWEI CLOUD, certifique-se de que seu IdP empresarial seja compatível com este protocolo.

- OpenID Connect

  O OpenID Connect é uma camada de identidade simples em cima do protocolo Open Authorization 2.0 (OAuth 2.0). O IAM implementa a autenticação de identidade federada em conformidade com o OpenID Connect 1.0. Para federar com sucesso os usuários existentes à HUAWEI CLOUD, certifique-se de que seu IdP empresarial seja compatível com este protocolo. Para obter mais informações sobre o OpenID Connect, consulte **Bem-vindo 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 de autenticação de identidade federada

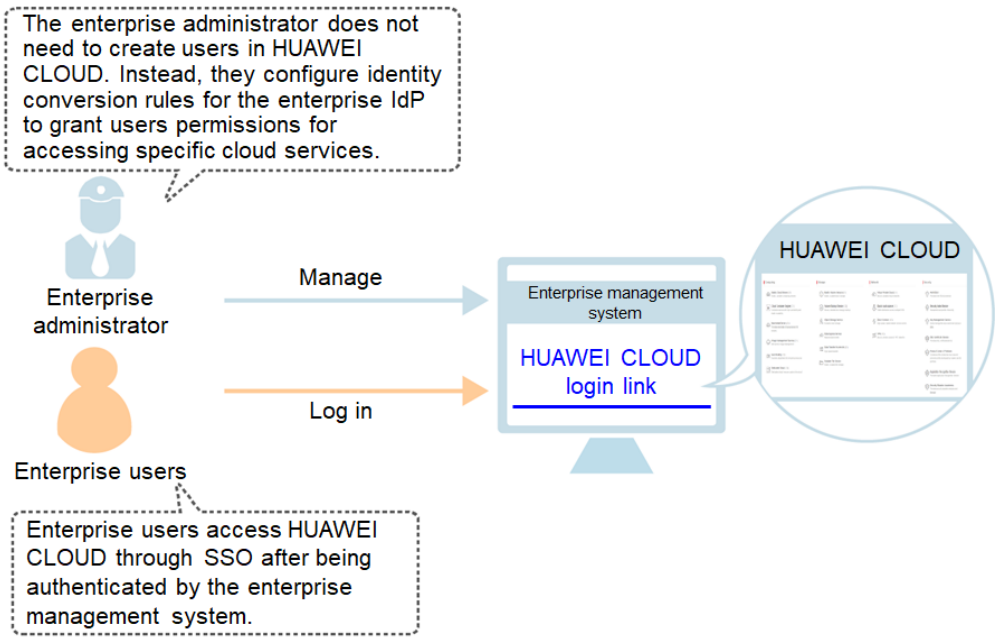
- Facilidade no gerenciamento de usuários

  Como um administrador, você só precisa criar usuários em seu sistema de gerenciamento empresarial. Os usuários podem usar suas próprias contas para acessar o sistema de gerenciamento empresarial e HUAWEI CLOUD.

- Operações simplificadas

  Os usuários podem fazer login na HUAWEI CLOUD através do sistema de gerenciamento empresarial.

Figura 9-1 Vantagens de autenticação de identidade federada



Precauções

- Para implementar a autenticação de identidade federada, certifique-se de que o servidor IdP da sua empresa e HUAWEI CLOUD usam o horário GMT (Greenwich Mean Time) no mesmo fuso horário.
- Os usuários federados são identidades virtuais que seu IdP empresarial mapeia para HUAWEI CLOUD. As informações de identidade dos usuários federados são armazenadas no IdP empresarial, portanto, seu acesso à HUAWEI CLOUD tem as seguintes restrições:
  - Os usuários federados não podem executar verificação ao executar operações críticas. As configurações de **proteção de operação crítica** não se aplicam a usuários federados.
  - Os usuários federados não podem criar chaves de acesso com validade ilimitada, mas podem obter credenciais de acesso temporárias (chaves de acesso e securityTokens) usando tokens de usuário ou agência. Para obter detalhes, consulte **Obtenção de uma chave de acesso e SecurityToken**.

    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 Autenticação de identidade federada baseada em SAML

9.2.1 Configuração da autenticação de identidade federada baseada em SAML

Esta seção descreve o processo e a configuração da autenticação de identidade federada baseada em SAML entre um IdP empresarial e a HUAWEI CLOUD.

⚠ CUIDADO

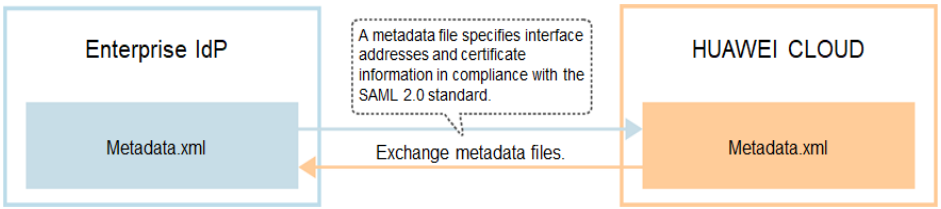
Certifique-se de que o IdP empresarial suporta ao SAML 2.0.

Configuração de Autenticação de identidade federada

Para implementar a autenticação de identidade federada entre um sistema de gerenciamento empresarial e a HUAWEI CLOUD, conclua a seguinte configuração:

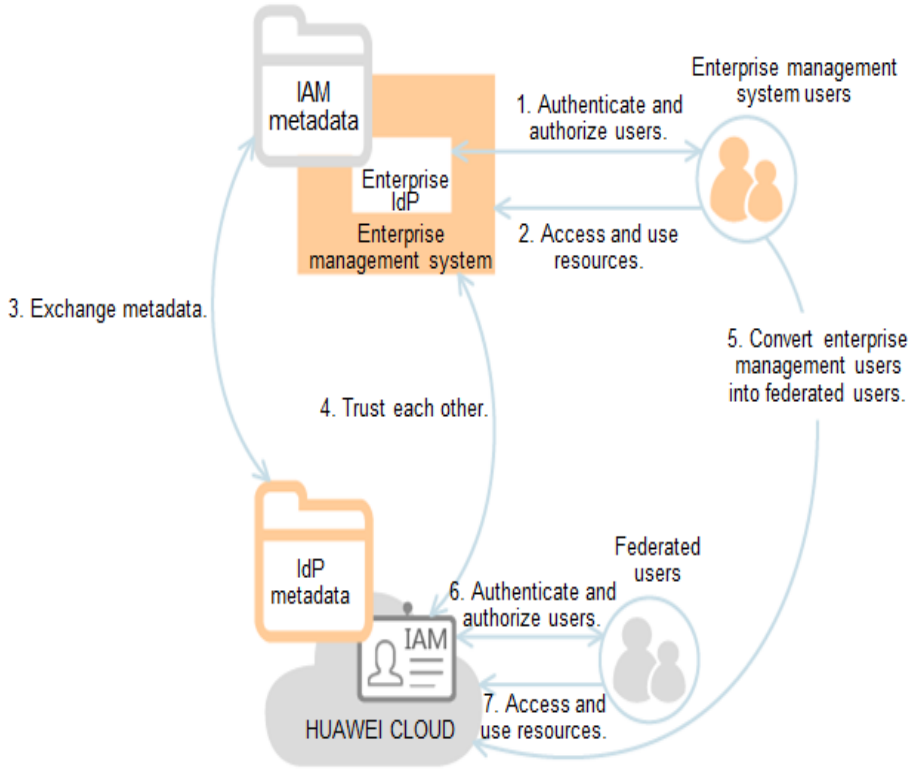
1. **Estabelecer uma relação de confiança e criar um provedor de identidade**: Troque os arquivos de metadados do IdP empresarial e da HUAWEI CLOUD (consulte **Figura 9-2**).

   Figura 9-2 Modelo de troca de arquivos de metadados

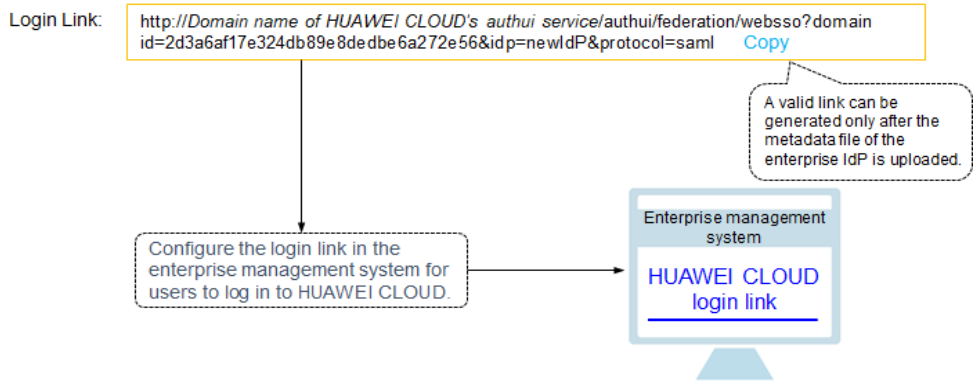
2. **Configurar regras de conversão de identidade**: Mapeie os usuários, grupos de usuários e permissões no IdP empresarial para a HUAWEI CLOUD (consulte **Figura 9-3**).

Figura 9-3 Modelo de conversão de identidade do usuário



3. **Configurar um link de login**: Configure um link de login (consulte **Figura 9-4**) no sistema de gerenciamento empresarial para permitir que os usuários acessem a HUAWEI CLOUD por meio do SSO.

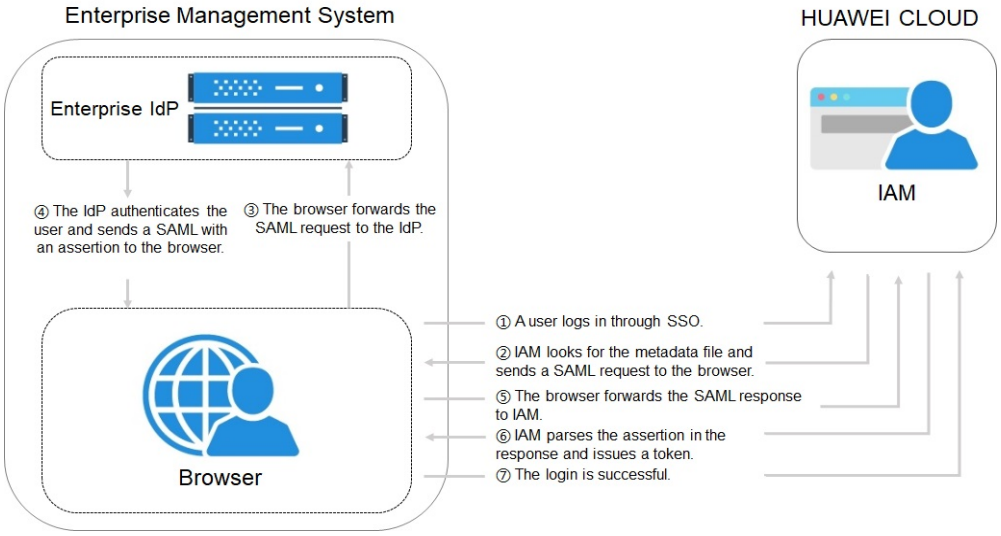
Figura 9-4 Modelo de login do SSO



Processo de autenticação de identidade federada

Figura 9-5 mostra a interação entre um sistema de gerenciamento empresarial e a HUAWEI CLOUD depois de um usuário iniciar uma solicitação SSO.

Figura 9-5 Processo de autenticação de identidade federada



NOTA

Para visualizar afirmações e solicitações interativas com uma experiência melhor, recomendamos que você use o Google Chrome e instale o plug-in SAML Message Decoder.

Conforme mostrado em **Figura 9-5**, o processo de autenticação de identidade federada é o seguinte:

1. Um usuário usa um navegador para abrir o link de login do provedor de identidade e, em seguida, o navegador envia uma solicitação SSO para a HUAWEI CLOUD.
2. A HUAWEI CLOUD procura um arquivo de metadados com base no link de login e envia uma SAML request ao navegador.
3. O navegador encaminha a SAML request para o IdP empresarial.
4. O usuário insere seu nome de usuário e senha na página de login exibida no IdP da empresa. Depois de o IdP empresarial autentica a identidade do usuário, ele constrói uma asserção SAML contendo as informações do usuário e envia a asserção para o navegador como SAML response.
5. O navegador responde e encaminha a SAML response para a HUAWEI CLOUD.
6. A HUAWEI CLOUD analisa a asserção na SAML response e emite um token para o usuário depois de identificar o grupo para o qual o usuário está mapeado, de acordo com as regras de conversão de identidade configuradas.
7. Se o login for bem-sucedido, o usuário acessa a HUAWEI CLOUD com sucesso.

NOTA

A asserção deve levar uma assinatura; caso contrário, o login falhará.

9.2.2 Passo 1: criar um provedor de identidade

Para estabelecer uma relação de confiança entre um IdP empresarial e a HUAWEI CLOUD, faça upload do arquivo de metadados da HUAWEI CLOUD para o IdP empresarial e, em seguida, crie um provedor de identidade e faça upload do arquivo de metadados do IdP empresarial no console do IAM.

Pré-requisitos

- Você registrou uma conta na HUAWEI CLOUD como um administrador empresarial e criou grupos de usuários e concedeu a eles permissões no IAM. Para obter detalhes, consulte **4.1 Criação de um grupo de usuários e atribuição de permissões**. Os grupos de usuários criados no IAM serão usados para atribuir permissões a usuários de IdP empresarial mapeados para a HUAWEI CLOUD.
- Você leu a documentação do IdP empresarial ou entendeu como usar o IdP empresarial. As configurações dos IdPs diferentes empresariais existem muitas diferenças, por isso, não são descritas neste documento. Para obter detalhes sobre como obter o arquivo de metadados do IdP empresarial e como fazer upload dos metadados da HUAWEI CLOUD para o IdP empresarial, consulte a documentação do IdP.

Estabelecimento de 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 Faça download do arquivo de metadados da HUAWEI CLOUD.

Visite **https://auth-intl.huaweicloud.com/authui/saml/metadata.xml** (O Google Chrome é recomendado). Faça 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 sobre como fazer upload do arquivo de metadados, consulte a documentação do seu IdP empresarial.

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

----Fim

Criação de um provedor de identidade na HUAWEI CLOUD

Crie um provedor de identidade e configure o arquivo de metadados no IAM.

Passo 1 Faça login 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 do provedor de identidade.

Tabela 9-1 Parâmetros básicos de um provedor de identidade

Parâmetro	Descrição
Nome	Nome do provedor de identidade. O nome do provedor de identidade deve ser exclusivo em sua conta.

Parâmetro	Descrição
Protocolo	Protocolo do provedor de Identidade. A HUAWEI CLOUD suporta provedores de identidade SAML e OpenID Connect. Para obter detalhes sobre como configurar a autenticação de identidade federada baseada em OpenID Connect, consulte **9.3 Autenticação de identidade federada baseada em OpenID Connect**.
Tipo SSO	Tipo do provedor de identidade. Apenas um tipo de SSO de provedor de identidade pode ser criado sob uma conta. ● **Virtual user**: Depois de um usuário fazer login na HUAWEI CLOUD por meio de um provedor de identidade, o sistema cria automaticamente uma identidade virtual para o usuário. Vários provedores de identidade do tipo SSO de usuário virtual podem ser criados sob uma conta. ● **IAM user**: Depois de um usuário fazer login na HUAWEI CLOUD por meio de um provedor de identidade, o sistema mapeia o usuário para um usuário do IAM com base nas regras de conversão de identidade configuradas. Apenas um provedor de identidade do tipo SSO de usuário do IAM pode ser criado sob uma conta. Se você selecionar esse tipo, certifique-se de que criou um usuário do IAM e defina a ID de identidade externa. Para obter detalhes, consulte **3.1 Criação de um usuário do IAM**.
Status	Status do provedor de identidade. O valor padrão é **Enabled**.

Passo 3 Clique em **OK**.

----Fim

Configuração do arquivo de metadados do provedor de identidade

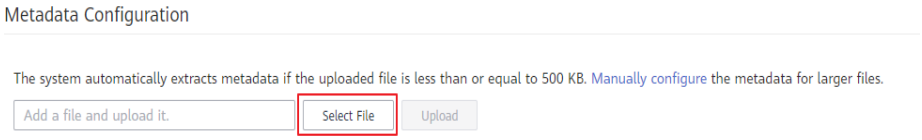
Configure o arquivo de metadados do IdP empresarial na HUAWEI CLOUD. Você pode fazer upload ou editar manualmente as configurações de metadados no IAM. Para um arquivo de metadados maior que 500 KB, configure manualmente os metadados. Se os metadados tiverem sido alterados, faça upload do arquivo de metadados mais recente ou edite os metadados existentes para garantir que os usuários federados possam fazer login na HUAWEI CLOUD com êxito.

NOTA

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

- **Fazer upload de um arquivo de metadados.**
  a. Clique em **Modify** na linha contendo o provedor de identidade.
  b. Clique em **Select File** e selecione o arquivo de metadados que você obteu.

  Figura 9-6 O upload de um arquivo de metadados



c. Clique em **Upload**. Os metadados extraídos do arquivo carregado são exibidos. Clique em **OK**.

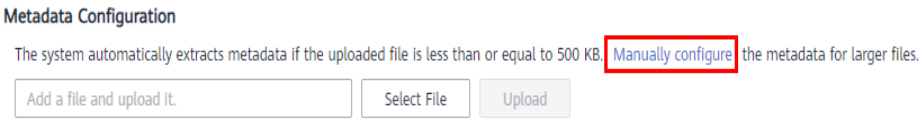
- Se o arquivo de metadados carregado contiver vários provedores de identidade, selecione o provedor de identidade que deseja usar na lista suspensa **Entity ID**.
- Se uma mensagem for exibida indicando que nenhum entity ID é especificado ou que o signing certificate expirou, verifique o arquivo de metadados e faça upload novamente ou configure os metadados manualmente.

d. Clique em **OK**.

- **Configurar metadados manualmente.**

a. Clique em **Manually configure**.

Figura 9-7 Configuração manual de metadados



b. Na caixa de diálogo **Configure Metadata**, defina os parâmetros de metadados, como entity ID, signing certificate e **SingleSignOnService**.

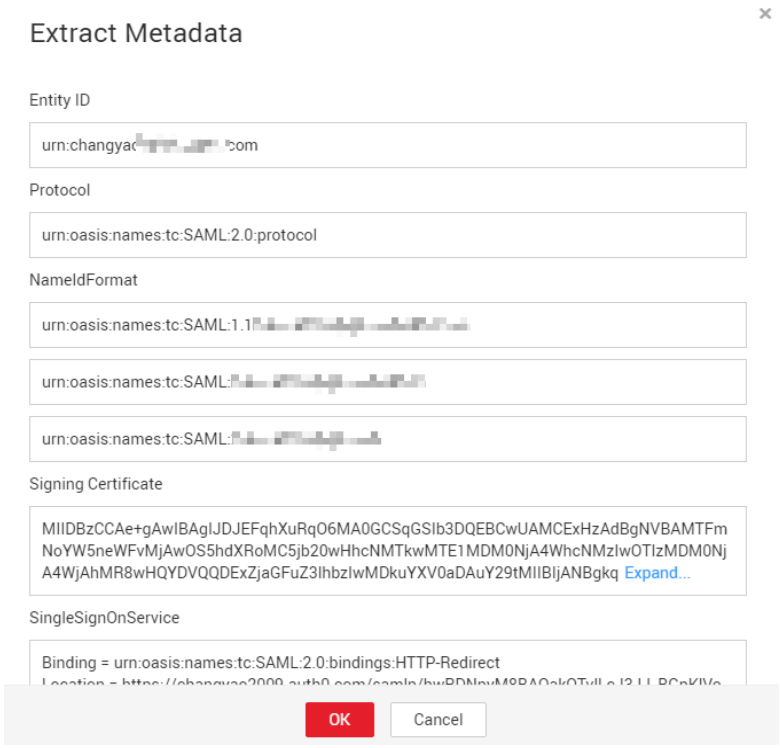
Parâmetro	Obrigatório	Descrição
Entity ID	Sim	O identificador exclusivo de um provedor de identidade. Inserir o valor de **entityID** exibido no arquivo de metadados do IdP empresarial. Se o arquivo de metadados contiver vários provedores de identidade, escolha aquele que você deseja usar.
Protocolo	Sim	O protocolo SAML é usado para autenticação de identidade federada entre um IdP empresarial e um SP. **O sistema gera automaticamente um valor depois de selecionar o protocolo.**
NameIdFormat	Não	Inserir o valor **NameIdFormat** exibido no arquivo de metadados. Esse parâmetro indica o nome de usuário e o formato de ID usados para comunicação entre o provedor de identidade e os usuários federados. **Se você configurar vários valores, a HUAWEI CLOUD usará o primeiro valor por padrão.**

Parâmetro	Obrigatório	Descrição
Signing Certificate	Sim	Inserir o valor **<X509Certificate>** exibido no arquivo de metadados. Um signing certificate é um certificado de chave pública usado para verificação de assinatura. Para fins de segurança, insira uma chave pública contendo pelo menos 2048 bits. O signing certificate é usado durante a autenticação de identidade federada para garantir que as afirmações sejam confiáveis e completas. **Se você configurar vários valores, a HUAWEI CLOUD usará o primeiro valor por padrão.**
SingleSignOnService	Sim	Inserir o valor **SingleSignOnService** exibido no arquivo de metadados. Esse parâmetro define como as solicitações SAML são enviadas durante o processo de SSO. O parâmetro **SingleSignOnService** no arquivo de metadados deve suportar HTTP Redirect ou HTTP POST. **Se você configurar vários valores, a HUAWEI CLOUD usará o primeiro valor por padrão.**
SingleLogoutService	Não	Inserir o valor **SingleLogoutService** exibido no arquivo de metadados. Este parâmetro indica o endereço para o qual os utilizadores federados serão redireccionados após terminarem a sessão. O parâmetro **SingleLogoutService** no arquivo de metadados deve suportar HTTP Redirect ou HTTP POST. **Se você configurar vários valores, a HUAWEI CLOUD usará o primeiro valor por padrão.**

O exemplo a seguir mostra o arquivo de metadados de um IdP empresarial e as informações de metadados que precisam ser concluídas durante a configuração manual.

Figura 9-8 Arquivo de metadados de um IdP empresarial

Figura 9-9 Configuração manual de metadados



c. Clique em **OK**.

Fazer login como um usuário federado

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

1. Na página **Identity Providers** page, clique em **View** (consulte **Figura 9-10**) na coluna **Operation** do provedor de identidade. Copie o link de login (consulte **Figura 9-11**) exibido na página de detalhes do provedor de identidade e visite o link usando um navegador.

Figura 9-10 Visualização de um provedor de identidade

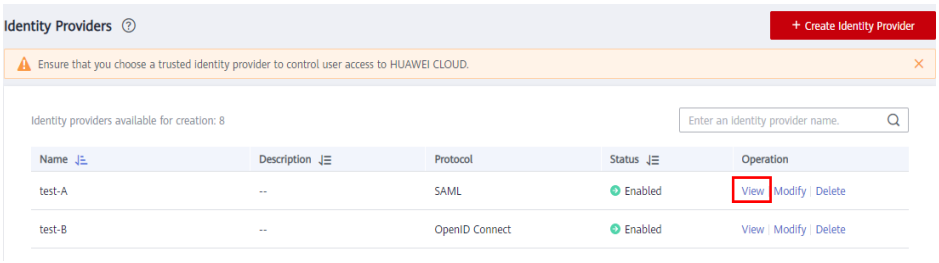
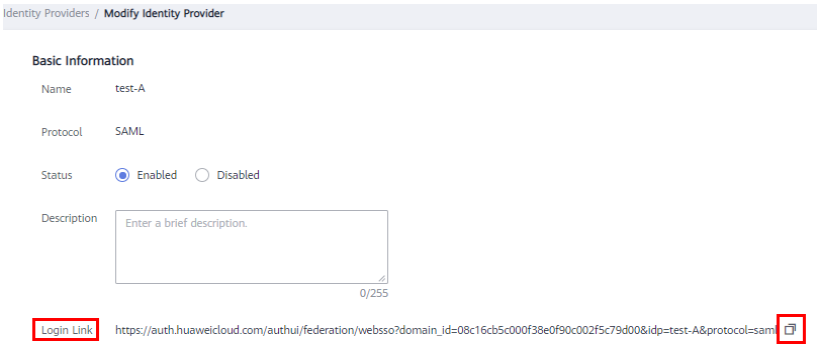


Figura 9-11 Cópia de um link de login



2. Se a página de login não for exibida, verifique o arquivo de metadados e as configurações do servidor IdP empresarial.

Passo 2 Insira o nome de usuário e a senha de um usuário criado no IdP empresarial.

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

NOTA

Os usuários federados só têm permissões de leitura para a HUAWEI CLOUD por padrão. Para atribuir permissões a usuários federados, configure regras de conversão de identidade para o provedor de identidade. Para obter mais informações, consulte **9.2.3 Passo 2: configurar regras de conversão de identidade**.

----Fim

Operações relacionadas

- Visualização de informações do provedor de identidade: Na lista de provedores de identidade, clique em **View** na linha que contém o provedor de identidade e exiba suas informações básicas, metadados e regras de conversão de identidade.

  NOTA

  Para modificar as configurações de um provedor de identidade, clique em **Modify** na parte inferior da página de detalhes.

- Modificação de um provedor de identidade: Na lista de provedores de identidade, clique em **Modify** na linha que contém o provedor de identidade e, em seguida, altere seus status ou modifique a descrição, metadados ou regras de conversão de identidade.
- Exclusão de um provedor de identidade: Na lista do provedor de identidade, clique em **Delete** na linha que contém o provedor de identidade e clique em **Yes**.

Procedimento de acompanhamento

- Na área **Identity Conversion Rules**, configure regras de conversão de identidade para mapear usuários do sistema de gerenciamento empresarial para grupos de usuários do IAM e conceder permissões aos usuários. Para obter detalhes, consulte **9.2.3 Passo 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 obter detalhes, consulte **9.2.5 (Opcional) Passo 3: configurar um link de login no sistema de gerenciamento empresarial**.

9.2.3 Passo 2: configurar regras de conversão de identidade

Os usuários federados são nomeados **FederationUser** por padrão na HUAWEI CLOUD. Esses usuários só podem fazer login na HUAWEI CLOUD e não têm nenhuma permissão. Você pode configurar regras de conversão de identidade no console do IAM para obter o seguinte:

- Exibir usuários do sistema de gerenciamento empresarial com nomes diferentes na HUAWEI CLOUD.
- Conceda permissões aos usuários do sistema de gerenciamento empresarial para usar os recursos da HUAWEI CLOUD mapeando esses usuários para grupos de usuários do IAM. Certifique-se de que você criou os grupos de usuários necessários. Para obter detalhes, consulte **Criação de um grupo de usuários e atribuição de permissões**.

NOTA

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

Pré-requisitos

Um provedor de identidade foi criado e o link de login do provedor de identidade é acessível. (Para obter detalhes sobre como criar e verificar um provedor de identidade, consulte **9.2.2 Passo 1: criar um provedor de identidade**.)

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 obter detalhes, consulte **9.4 Sintaxe das regras de conversão de identidade**.

- **Criação de uma regra**
  a. Escolha **Identity Providers** no painel de navegação.
  b. Na lista do provedor de identidade, clique em **Modify** na linha que contém o provedor de identidade.
  c. Na área **Identity Conversion Rules**, clique em **Create Rule**. Em seguida, configure as regras na caixa de diálogo **Create Rule**.

Figura 9-12 Clique em Create Rule

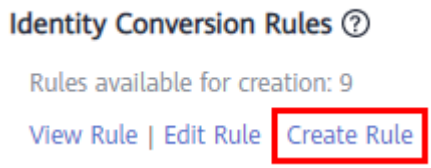


Figura 9-13 Criação de uma regra

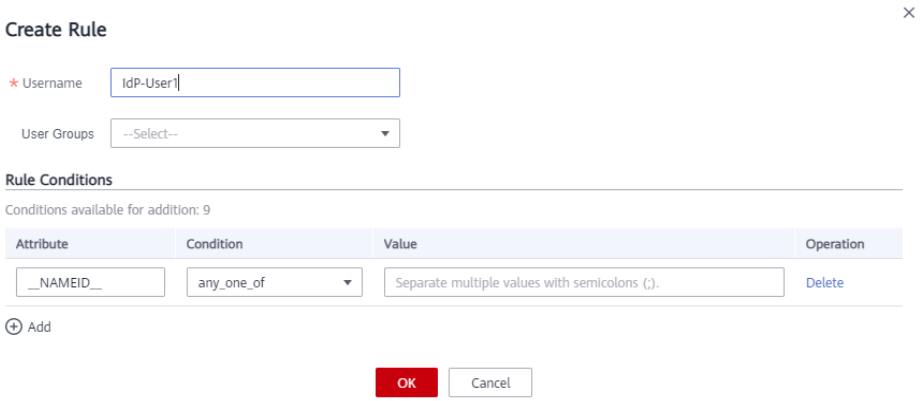


Tabela 9-2 Descrição do parâmetro

Parâmetro	Descrição	Observações
Nome do usuário	Nome de usuário dos usuários federados a serem exibidos na HUAWEI CLOUD.	Para distinguir usuários federados de usuários da HUAWEI CLOUD, é recomendável que você defina o nome de usuário como "**FederationUser-***IdP_XXX*". *IdP* indica um nome de provedor de identidade, por exemplo, AD FS e Shibboleth. *XXX* indica um nome personalizado. **AVISO** ● Cada nome de usuário federado deve ser exclusivo sob o provedor de identidade. Nomes de usuário federados idênticos sob o mesmo provedor de identidade serão identificados como 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
Grupos de usuários	Grupos de usuários aos quais os usuários federados pertencerão na HUAWEI CLOUD.	Os usuários federados herdarão permissões dos grupos aos quais o usuário pertence. **NOTA** O nome do grupo 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

Parâmetro	Descrição	Observações
Condições da regra	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 provedor de identidade 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 cumpridas. ● Um provedor de identidade pode ter várias regras de conversão de identidade. Se um usuário federado não atender a nenhuma das regras, o usuário não terá permissão para 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**
- Condições da regra: **_NAMEID_** (atributo), **any_one_of** (condição), and **000000001** (valor).

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

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

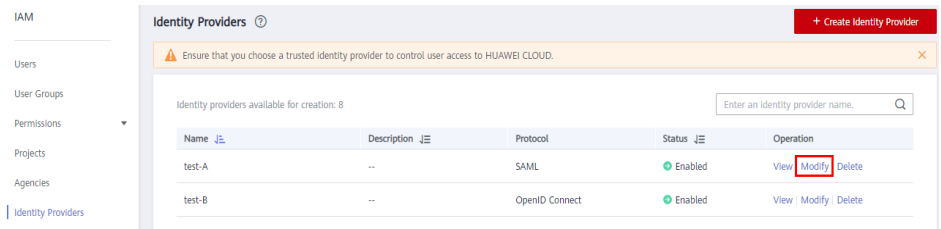
e. Na página **Modify Identity Provider**, clique em **OK**.

- **Edição de uma regra**

a. Faça login na HUAWEI CLOUD como um administrador e acesse o console do IAM. A seguir, escolha **Identity Providers** no painel de navegação.

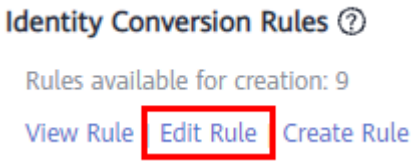
b. Na lista do provedor de identidade, clique em **Modify** na linha que contém o provedor de identidade.

Figura 9-14 Modificação de um provedor de identidade



c. Na área **Identity Conversion Rules**, clique em **Edit Rule**. Em seguida configure as regras na caixa de diálogo **Edit Rule**.

Figura 9-15 Edição das regras de conversão de identidade



d. Edite a regra de conversão de identidade no formato JSON. Para obter detalhes, consulte **9.4 Sintaxe das regras de conversão de identidade**.

e. Clique em **Validate** para verificar a sintaxe da regra.

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 a instrução ou clique em **Cancel** para cancelar as modificações.

Operações relacionadas

Visualização das 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 formato JSON, consulte **Sintaxe das regras de conversão de identidade**.

9.2.4 Passo 3: verificar o login

Verificação do login

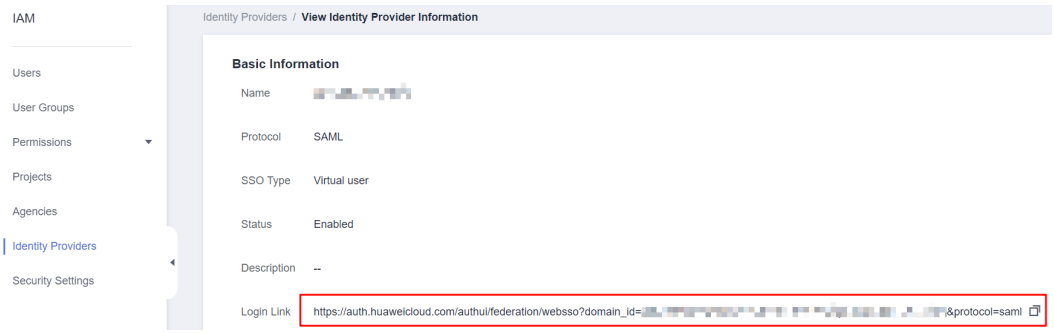
Os usuários federados podem iniciar um login a partir do Idp ou SP.

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

Os métodos de login iniciados pelo IdP variam de acordo com os IdPs. Para obter detalhes, consulte a documentação do IdP. Este tópico descreve como iniciar um login a partir do SP.

Passo 1 Fazer Login como um usuário federado.

Na página **Identity Providers** do console, clique em **View** na linha contendo o provedor de identidade. Copie o link de login exibido na página de detalhes do provedor de identidade, abra o link usando um navegador e insira 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 grupo de usuários.

Por exemplo, uma regra de conversão de identidade definiu permissões completas para todos os serviços de nuvem para usuário federado **ID1** no grupo de usuários **admin**. No console de gerenciamento, selecione qualquer serviço de nuvem e verifique se você pode acessar ao serviço.

----Fim

Saltar para uma região ou serviço especificado

Você precisa especificar a página de login de destino para o usuário federado, por exemplo, a página inicial do Cloud Eye em CN-Hong Kong. Você pode configurar a página de login de destino usando um dos seguintes métodos:

- Configuração do link de login no SP

  Combine o link de login obtido no console com o URL especificado no formato de **Login link &service=Specified URL**. Por exemplo, se o link de login 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 login configurado no SP é **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**
- Configuração do link de login no IdP

  Configure a declaração IAM_SAML_Attributes_redirect_url (o URL a ser redirecionado para) na declaração SAML do IdP empresarial.

9.2.5 (Opcional) Passo 3: configurar um link de login no sistema de gerenciamento empresarial

Configure o link de login do provedor de identidade no sistema de gerenciamento empresarial para que os usuários empresariaias possam usar esse link para acessar a HUAWEI CLOUD.

NOTA

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

Pré-requisitos

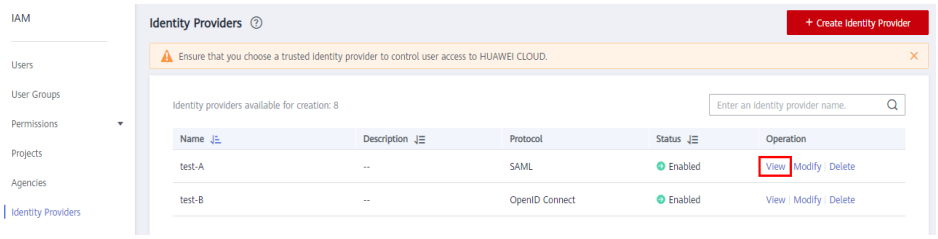
- Um provedor de identidade foi criado e o link de login do provedor de identidade é acessível. (Para obter detalhes sobre como criar e verificar um provedor de identidade, consulte **9.2.2 Passo 1: criar um provedor de identidade**.)
- O link de login do provedor de identidade já foi configurado no sistema de gerenciamento empresarial para fazer login na HUAWEI CLOUD.

Procedimento

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

Passo 2 Clique em **View** na linha contendo o provedor de identidade.

Figura 9-16 Visualização dos detalhes do provedor de identidade



Passo 3 Clique em **Copy** ao lado do link de login.

Figura 9-17 Cópia de um link de login

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

```
<a href="<Login link>"> HUAWEI CLOUD Login </a>
```

Passo 5 Faça login no sistema de gerenciamento empresarial e clique no link de login configurado da HUAWEI CLOUD para acessar a HUAWEI CLOUD.

----Fim

9.3 Autenticação de identidade federada baseada em OpenID Connect

9.3.1 Configuração da autenticação de identidade federada baseada em OpenID Connect

Esta seção descreve o processo e a configuração da autenticação de identidade federada baseada em OpenID Connect entre um IdP empresarial e a HUAWEI CLOUD.

Configuração de autenticação de identidade federada

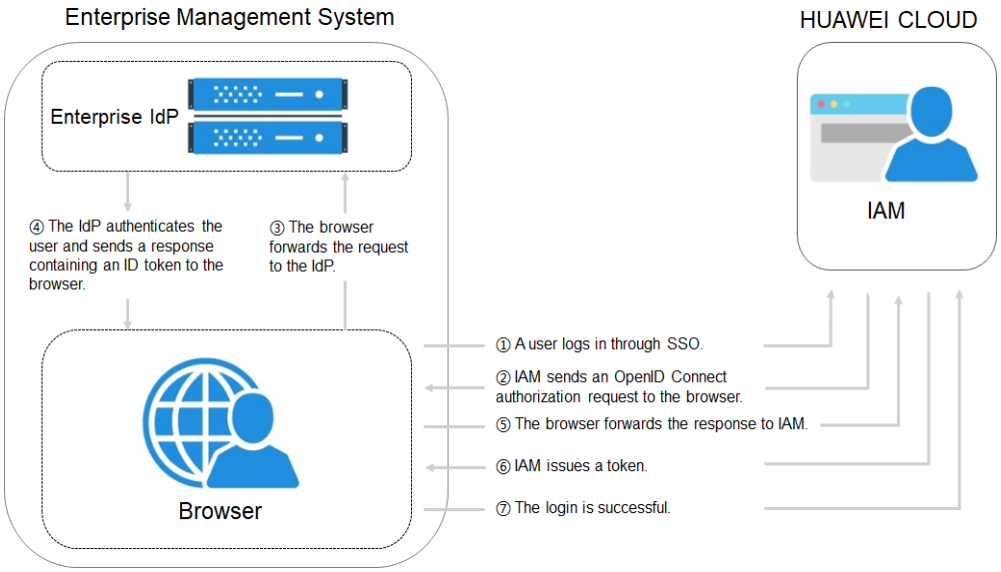
Para implementar a autenticação de identidade federada entre um sistema de gerenciamento empresarial e a HUAWEI CLOUD, conclua a seguinte configuração:

1. **Estabelecer uma relação de confiança e criar um provedor de identidade**: Crie credenciais do OAuth 2.0 no IdP corporativo e crie um provedor de identidade na HUAWEI CLOUD.
2. **Configurar regras de conversão de identidade**: Mapeie os usuários, grupos de usuários e suas permissões no IdP empresarial para a HUAWEI CLOUD.
3. **Configurar um link de login**: Configure um link de login no sistema de gerenciamento empresarial para permitir que os usuários acessem a HUAWEI CLOUD por meio do SSO.

Processo de autenticação de identidade federada

Figura 9-18 mostra a interação entre um sistema de gerenciamento empresarial e a HUAWEI CLOUD depois de um usuário iniciar uma solicitação SSO.

Figura 9-18 Processo de autenticação de identidade federada



O processo de autenticação de identidade federada é o seguinte:

1. Um usuário usa um navegador para abrir o link de login obtido do IAM e, em seguida, o navegador envia uma solicitação SSO para a HUAWEI CLOUD.
2. A HUAWEI CLOUD procura configurações do provedor de identidade com base no link de login e envia um request OpenID Connect authorization ao navegador.

3. O navegador encaminha o request authorization para o IdP empresarial.
4. O usuário insere seu nome de usuário e senha na página de login exibida no IdP empresarial. Depois de o IdP empresarial autentica a identidade do usuário, ele constrói um ID token contendo as informações do usuário e envia o ID token para o navegador como uma response OpenID Connect authorization.
5. O navegador responde e encaminha a response authorization para a HUAWEI CLOUD.
6. A HUAWEI CLOUD analisa o ID token na response authorization e emite um token para o usuário depois de identificar o grupo para o qual o usuário está mapeado, de acordo com as regras de conversão de identidade configuradas.
7. Se o login for bem-sucedido, o usuário acessa a HUAWEI CLOUD com sucesso.

9.3.2 Passo 1: Criar um provedor de identidade

Para estabelecer uma relação de confiança entre um IdP empresarial e a HUAWEI CLOUD, crie um provedor de identidade e configure as informações de autorização no console do IAM, defina os URLs de redirecionamento do usuário e crie credenciais OAuth 2.0 no IdP empresarial.

Pré-requisitos

- Você registrou uma conta na HUAWEI CLOUD como um administrador empresarial e criou grupos de usuários e concedeu a eles permissões no IAM. Para obter detalhes, consulte **4.1 Criação de um grupo de usuários e atribuição de permissões**. Os grupos de usuários criados no IAM serão usados para atribuir permissões a usuários de IdP empresarial mapeados para a HUAWEI CLOUD.
- Você leu a documentação do IdP empresarial ou entendeu como usar o IdP empresarial. As configurações dos IdPs diferentes empresariais existem muitas diferenças, por isso, não são descritas neste documento. Para obter detalhes sobre como obter as credenciais do OAuth 2.0 do IdP empresarial, consulte a documentação do IdP.

Criação de credenciais do OAuth 2.0 no IdP empresarial

Passo 1 Defina URLs 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 ao provedor de identidade OpenID Connect na HUAWEI CLOUD.

Passo 2 Obtenha credenciais do OAuth 2.0 do IdP empresarial.

----Fim

Criação de um provedor de identidade na HUAWEI CLOUD

Crie um provedor de identidade e configure as informações de autorização no IAM.

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

Passo 2 Insira um nome de provedor de identidade, selecione **OpenID Connect** e **Enabled** e clique em **OK**.

NOTA

O nome do provedor de identidade deve ser exclusivo sob sua conta.

----Fim

Configuração das informações de autorização na HUAWEI CLOUD

Passo 1 Clique em **Modify** na coluna **Operation** da linha que contém o provedor de identidade que deseja modificar.

Passo 2 Selecione um tipo de acesso.

Tabela 9-3 Descrição do tipo de acesso

Tipo de acesso	Descrição
Acesso programático e acesso ao console de gerenciamento	● Acesso programático: Os usuários federados podem usar ferramentas de desenvolvimento (incluindo APIs, CLI e SDKs) que suportam autenticação de chave para acessar a HUAWEI CLOUD. ● Acesso ao console de gerenciamento: Os usuários federados podem fazer login no console da HUAWEI CLOUD usando seus próprios nomes de usuário e senhas. **Selecione este tipo de acesso se quiser que os usuários acessem a HUAWEI CLOUD por meio do SSO.**
Acesso programático	Os usuários federados só podem usar ferramentas de desenvolvimento (incluindo APIs, CLI e SDKs) que suportam autenticação de chave para acessar a HUAWEI CLOUD.

Passo 3 Especifique as informações de configuração.

Tabela 9-4 Informações de configuração

Parâmetro	Descrição
Identity Provider URL	URL do provedor de identidade do OpenID Connect. Especifique esse parâmetro como o valor do **issuer** em **Openid-configuration**. **NOTA** **Openid-configuration** indica um URL definido no OpenID Connect, contendo configurações de um IdP empresarial. O formato URL é **https://** *{base URL}*/**.well-known/openid-configuration**, onde o *base URL* é definido pelo IdP empresarial. Por exemplo, a **Openid-configuration** do Google é **https://accounts.google.com/.well-known/openid-configuration**.
Client ID	ID de um cliente registrado com o provedor de identidade do OpenID Connect. O ID do cliente é **uma credencial do OAuth 2.0 criada no IdP empresarial.**
Authorization Endpoint	O Authorization Endpoint do provedor de identidade do OpenID Connect. Especifique esse parâmetro como o valor do **authorization_endpoint** em **Openid-configuration**. **Esse parâmetro só será necessário se você definir Access Type como Programmatic access e management console access.**

Parâmetro	Descrição
Scopes	Escopos das solicitações de autorização. **openid** é selecionado por padrão. **Esse parâmetro só será necessário se você definir Access Type como Programmatic access e management console access.** Valores enumerados: ● openid ● email ● profile
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 e management console access.**
Response Mode	Modo de resposta de solicitações de autorização. As opções incluem **form_post** e **fragment**. **form_post** é recomendado. ● **form_post**: Se esse modo estiver selecionado, defina o URL de redirecionamento como **htauth.huaweicloud.comd.com/authul/oidc/post** no IdP empresarial. ● **fragment**: Se esse modo estiver selecionado, defina o URL de redirecionamento como **httauth.huaweicloud.comd.com/authui/oidc/redirect** no IdP empresarial. **Esse parâmetro só será necessário se você definir Access Type como Programmatic access e management console access.**
Chave de assinatura	Chave pública usada para assinar o ID token do provedor de identidade OpenID Connect. Para fins de segurança da conta, **altere a chave de assinatura periodicamente**.

Passo 4 Clique em **OK**.

----Fim

Fazer login como um usuário federado

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

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

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

- Se o login for bem-sucedido, adicione o link de login ao sistema de gerenciamento empresarial.

- Se o login falhar, verifique o nome de usuário e a senha.

NOTA

Os usuários federados só têm permissões de leitura para a HUAWEI CLOUD por padrão. Para atribuir permissões a usuários federados, configure regras de conversão de identidade para o provedor de identidade. Para obter mais informações, consulte **9.3.3 Passo 2: configurar regras de conversão de identidade**.

----Fim

Operações relacionadas

- Visualização de informações do provedor de identidade: Na lista de provedores de identidade, clique em **View** na linha que contém o provedor de identidade e exiba suas informações básicas, metadados e regras de conversão de identidade.

  NOTA

  Para modificar as configurações de um provedor de identidade, clique em **Modify** na parte inferior da página de detalhes.
- Modificação de um provedor de identidade: Na lista de provedores de identidade, clique em **Modify** na linha que contém o provedor de identidade e, em seguida, altere seus status ou modifique a descrição, metadados ou regras de conversão de identidade.
- Exclusão de um provedor de identidade: Na lista do provedor de identidade, clique em **Delete** na linha que contém o provedor de identidade e clique em **Yes**.

Procedimento de acompanhamento

- Configurar as regras de conversão de identidade para mapear usuários do IdP empresarial para grupos de usuários do IAM e conceder permissões aos usuários. Para obter detalhes, consulte **9.3.3 Passo 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 obter detalhes, consulte **9.3.4 (Opcional) Passo 3: configurar um link de login no sistema de gerenciamento empresarial**.

9.3.3 Passo 2: configurar regras de conversão de identidade

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

- Exibir usuários do sistema de gerenciamento empresarial com nomes diferentes na HUAWEI CLOUD.
- Conceda permissões aos usuários do sistema de gerenciamento empresarial para usar os recursos da HUAWEI CLOUD mapeando esses usuários para grupos de usuários do IAM. Certifique-se de que você criou os grupos de usuários necessários. Para obter detalhes, consulte **Criação de um grupo de usuários e atribuição de permissões**.

NOTA

- As modificações das regras de conversão de identidade entrarão em vigor depois de os usuários federados fazerem login.
- Para modificar as permissões de um usuário, modifique as permissões do grupos de usuários ao qual o usuário pertence. Em seguida, reinicie o IdP empresarial para que as modificações tenham efeito.

Pré-requisitos

Um provedor de identidade foi criado e o link de login do provedor de identidade é acessível. (Para obter detalhes sobre como criar e verificar um provedor de identidade, consulte **9.3.2 Passo 1: Criar um provedor de identidade**.)

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 obter detalhes, consulte **9.4 Sintaxe das regras de conversão de identidade**.

- **Criação de uma regra**
  a. Escolha **Identity Providers** no painel de navegação.
  b. Na lista do provedor de identidade, clique em **Modify** na linha que contém o provedor de identidade.
  c. Na área **Identity Conversion Rules**, clique em **Create Rule**. Em seguida, configure as regras na caixa de diálogo **Create Rule**.

Figura 9-19 Criação de regra

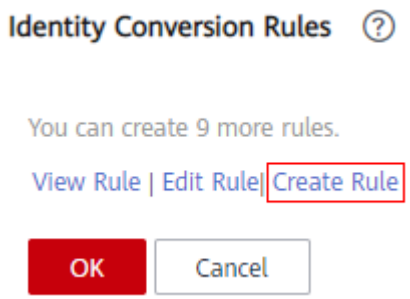


Figura 9-20 Definição dos parâmetros do inicializador

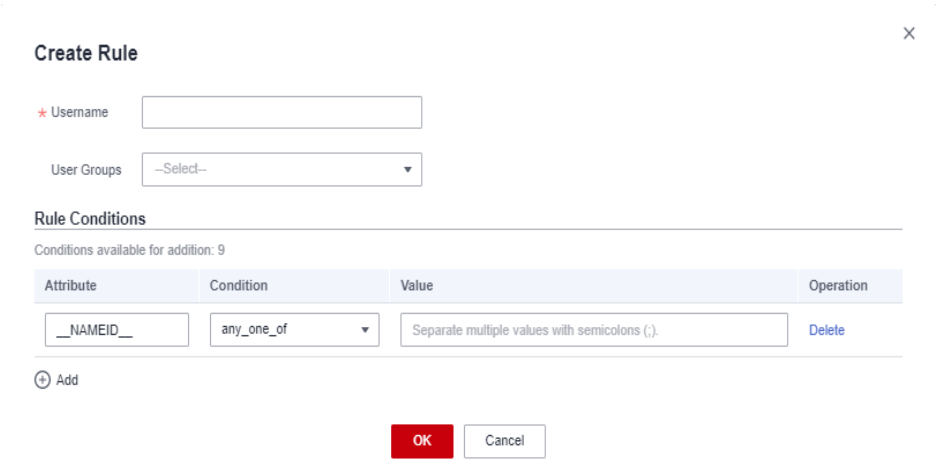


Tabela 9-5 Descrição do parâmetro

Parâmetro	Descrição	Observações
Username	Nome de usuário dos usuários federados a serem exibidos na HUAWEI CLOUD.	Para distinguir usuários federados de usuários da HUAWEI CLOUD, é recomendável que você defina o nome de usuário como "**FederationUser-*IdP_XXX***". *IdP* indica um nome de provedor de identidade, por exemplo, AD FS e Shibboleth. *XXX* indica um nome personalizado. **AVISO** ● Cada nome de usuário federado deve ser exclusivo sob o provedor de identidade. Nomes de usuário federados idênticos sob o mesmo provedor de identidade serão identificados como 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
Grupos de usuários	Grupos de usuários aos quais os usuários federados pertencerão na HUAWEI CLOUD.	Os usuários federados herdarão permissões dos grupos aos quais o usuário pertence. **NOTA** O nome do grupo 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
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 cumpridas. ● Um provedor de identidade pode ter várias regras de conversão de identidade. Se um usuário federado não atender a nenhuma das regras, o usuário não terá permissão para 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**
- Condições da regra: **_NAMEID_** (atributo), **any_one_of** (condição), e **000000001** (valor).

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

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

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

- **Edição de uma regra**

a. Faça login na HUAWEI CLOUD como um administrador e acesse o console do IAM. A seguir, escolha **Identity Providers** no painel de navegação.

b. Na lista do provedor de identidade, clique em **Modify** na linha que contém o provedor de identidade.

c. Na área **Identity Conversion Rules**, clique em **Edit Rule**. Em seguida configure as regras na caixa de diálogo **Edit Rule**.

d. Edite a regra de conversão de identidade no formato JSON. Para obter detalhes, consulte **9.4 Sintaxe das regras de conversão de identidade**.

e. Clique em **Validate** para verificar a sintaxe da regra.

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 a instrução ou clique em **Cancel** para cancelar as modificações.

Verificação de permissões de usuário federado

Depois de configurar as regras de conversão de identidade, verifique as permissões dos usuários federados.

Passo 1 Faça login na HUAWEI CLOUD como um usuário federado, como usuário **ID1**.

Na página **Identity Providers** do console do IAM, clique em **View** na linha contendo o provedor de identidade. Copie o link de login exibido na página de detalhes do provedor de identidade, abra o link usando um navegador e insira 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 grupo de usuários ao qual o usuário pertence.

Por exemplo, uma regra de conversão de identidade definiu permissões completas para todos os serviços de nuvem para usuário federado **ID1** no grupo de usuários **admin**. No console de gerenciamento, selecione qualquer serviço de nuvem e verifique se você pode acessar ao serviço.

----Fim

Operações relacionadas

Visualização das 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 formato JSON, consulte **Sintaxe das regras de conversão de identidade**.

9.3.4 (Opcional) Passo 3: configurar um link de login no sistema de gerenciamento empresarial

Configure o link de login do provedor de identidade no sistema de gerenciamento empresarial para que os usuários empresariaias possam usar esse link para acessar a HUAWEI CLOUD.

NOTA

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

Pré-requisitos

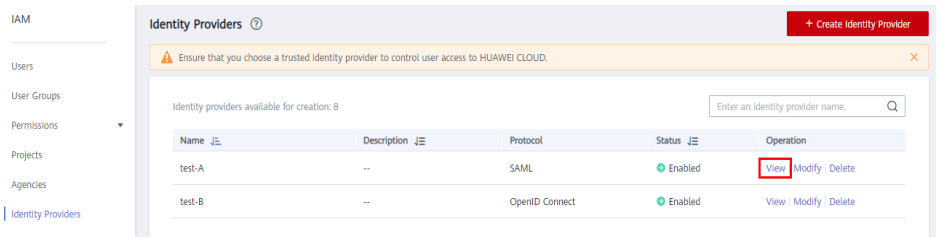
- Um provedor de identidade foi criado e o link de login do provedor de identidade é acessível. (Para obter detalhes sobre como criar e verificar um provedor de identidade, consulte **9.2.2 Passo 1: criar um provedor de identidade**.)
- O link de login do provedor de identidade já foi configurado no sistema de gerenciamento empresarial para fazer login na HUAWEI CLOUD.

Procedimento

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

Passo 2 Clique em **View** na linha contendo o provedor de identidade.

Figura 9-21 Visualização dos detalhes do provedor de identidade



Passo 3 Clique em **Copy** ao lado do link de login.

Figura 9-22 Cópia de um link de login

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

```
<a href="<Login link>"> HUAWEI CLOUD Login </a>
```


Passo 5 Faça login no sistema de gerenciamento empresarial e clique no link de login configurado da HUAWEI CLOUD para acessar a HUAWEI CLOUD.

----Fim

9.4 Sintaxe das regras de conversão de identidade

Uma regra de conversão de identidade é um objeto JSON que pode ser modificado. O seguinte 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 do remote das informações do usuário, respectivamente.
- **remote**: Informações sobre um usuário federado do provedor de identidade. Este campo é uma expressão que consiste em operadores e atributos de asserção. O valor deste campo é determinado pela asserção.
  - **condition**: Condições para que a regra de conversão de identidade entre em vigor. Os seguintes três tipos de condições 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 argument que é passado como entrada.
    - **any_one_of**: A regra é correspondida somente se qualquer uma das strings especificadas aparecer no tipo de atributo. O resultado da condição é o Boolean em vez do argument que é passado como entrada.
    - **not_any_of**: A regra não é correspondida se qualquer uma das strings especificadas aparecer no tipo de atributo. O resultado da condição é o Boolean em vez do argument que é passado como entrada.

AVISO

As informações do usuário mapeadas para o IAM só podem conter letras, dígitos, espaços, hifens (-), sublinhados (_), e pontos (.), e não podem começar com um dígito.

Exemplos da condição do empty

A condição do **empty** retorna strings de caracteres para substituir os atributos do local **{0..n}**.

- No exemplo a seguir, o nome de usuário de um usuário federado será "o valor do primeiro atributo do remote+espaço+o valor do segundo atributo do remote" no IAM, ou seja, *FirstName LastName*. O grupo ao qual o usuário pertence é o valor do terceiro atributo do remote *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 pertencerá apenas ao grupo **admin**.

```
{FirstName: John}
{LastName: Smith}
{Group: admin}
```

- Se um usuário federado pertencerá 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 do remote+espaço+o valor do segundo atributo do remote" no IAM, ou seja, *FirstName LastName*. Os grupos aos quais o usuário pertence é o valor do terceiro atributo do remote *Groups*.

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0} {1}"
                    }
                },
                {
                    "groups":  "{2}"
                }
            ],
            "remote": [
                {
                    "type": "FirstName"
                },
                {
                    "type": "LastName"
                },
                {
                    "type": "Groups"
```



```
                }
            ]
        }
]
```

Se a seguinte asserção for recebida, o nome de usuário do usuário federado será **John Smith** e o usuário pertencerá apenas aos grupos **admin** e **manager**.

```
{FirstName: John}
{LastName: Smith}
{Groups: [admin, manager]}
```

Exemplos de 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 do local. No exemplo a seguir, apenas **{0}** será substituído pelo valor retornado da primeira condição do **empty** no bloco **remote**. O valor do **grupo** é fixo como **admin**.

- O nome de usuário do usuário federado no IAM é o valor do primeiro atributo do remote, 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 provedor de identidade.

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
                {
                    "group": {
                        "name": "admin"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
                },
                {
                    "type": "Groups",
                    "any_one_of": [
                        "idp_admin"
                    ]
                }
            ]
        }
]
```

- Se um usuário federado pertencerá 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 do remote, 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 provedor de identidade.

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
```



```
                {
                    "groups": {
                           "name":"admin"
                    }
                },
                {
                    "groups": {
                           "name":"manager"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
                },
                {
                    "type": "Groups",
                    "any_one_of": [
                        "idp_admin"
                    ]
                }
            ]
        }
]
```

– A asserção a seguir indica que o usuário federado John Smith é um 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 um 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.

Essa 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

Múltiplas condições podem ser combinadas usando o operador lógico AND.

Essa regra só entra em vigor para os usuários federados que não pertencem ao grupo de usuários **idp_user** ou **idp_agent** no provedor de identidade. 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 usuário 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 login 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 um membro do grupo **idp_admin** no provedor de identidade e, portanto, atende às regras. O nome de usuário desse usuário será **John Smith** no IAM e o usuário pertence ao grupo **admin**.

```
{UserName: John Smith}
{Groups: [idp_user, idp_admin, idp_agency]}
```


10 Agente identificador personalizado

10.1 Habilitação do acesso do agente de identidade personalizado com uma agência

Se o **IdP da sua empresa** não for compatível com SAML ou OpenID Connect, você poderá criar um agente de identidade personalizado para permitir o acesso à HUAWEI CLOUD. Você pode escrever e executar código para gerar uma URL de login. Os usuários da sua empresa podem usar a URL para fazer login na HUAWEI CLOUD. Os usuários serão autenticados pelo seu IdP empresarial.

NOTA

Se o IdP da sua empresa for compatível com SAML ou OpenID Connect, configure **a autenticação de identidade federada** para permitir que os usuários da sua empresa acessem a HUAWEI CLOUD por meio do SSO.

Pré-requisitos

- Sua empresa possui 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 pode **acessar programaticamente** os serviços da HUAWEI CLOUD. Para obter detalhes sobre como alterar o tipo de acesso, consulte **3.4 Exibição ou modificação das informações do usuário do IAM**.

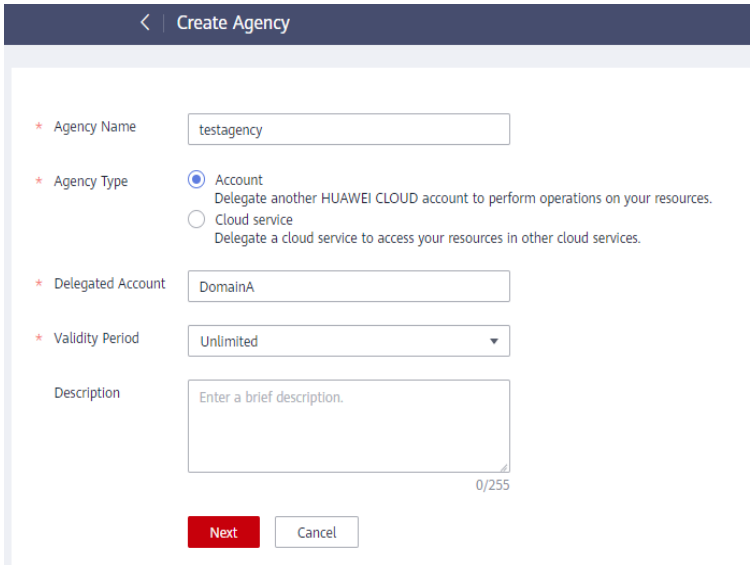
Passo 2 Configure a **chave de acesso** (recomendado) ou o nome de usuário e senha de **UserB** no arquivo de configuração do seu IdP empresarial para que o usuário possa obter um token para chamar as APIs. Para segurança da conta, criptografe a senha e a chave de acesso antes de armazená-las.

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 Criação de 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** (o mesmo nome da agência criada no **Passo 4**), adicione usuários empresariais ao grupo e conceda permissões para fazer login na HUAWEI CLOUD por meio de um agente de identidade personalizado. Para obter detalhes, consulte a documentação do IdP empresarial.

Passo 7 Depois de um usuário empresarial fazer login no sistema de gerenciamento empresarial, o usuário poderá acessar o agente 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 agente de identidade devem existir na HUAWEI CLOUD e ter os mesmos nomes que alguns grupos de usuários criados no IdP empresarial.

Passo 8 O agente de identidade personalizado usa o token de **userB** para chamar a API **POST / v3.0/OS-CREDENTIAL/securitytokens** usada para obter um securityToken temporário. Para obter detalhes, consulte **Obtenção de uma chave de acesso temporária e 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 agente de identidade personalizado usa a chave de acesso temporária, o securityToken e o nome de domínio global do IAM (auth.huaweicloud.com) para chamar a API **POST / v3.0/OS-AUTH/securitytoken/logintokens** para obter um loginToken. O valor de **X-Subject-LoginToken** no response header 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 (auth.huaweicloud.com) do IAM.
- Um loginToken é emitido a um usuário para fazer login através de um agente de identidade personalizado e contém informações de identidade e sessão sobre o usuário. Um loginToken é válido por 10 minutos por padrão. Os LoginTokens são necessários para autenticação quando os usuários fazem login 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 prazo de validade varia de 10 minutos a 12 horas. Se o valor que você especificou for maior que o período de validade restante do securityToken temporário, o período de validade restante do securityToken temporário será usado.

Passo 10 O agente de identidade personalizado gera um FederationProxyUrl e o retorna ao navegador por meio do **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 login do sistema de gerenciamento empresarial.
Serviço	Endereço de acesso de um serviço da HUAWEI CLOUD.
logintoken	LoginToken do agente de identidade personalizado.

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 por porcentual.

Passo 11 Se o loginToken for autenticado com êxito, os usuários federados serão automaticamente redirecionados para o endereço de serviço da HUAWEI CLOUD especificado no parâmetro **service**.

Se o loginToken falhar ao ser 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 exemplo de código usado para criar um FederationProxyUrl programaticamente usando uma agência para fazer login nos serviços da HUAWEI CLOUD.

Exemplo de código usando Java

O código 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://auth.huaweicloud.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 securityToken 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 securityToken.
*/
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 securityToken.
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://auth.huaweicloud.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 securityToken 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 securityToken.
# 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 securityToken.
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 Habilitação do acesso do agente de identidade personalizado com um Token

Se o IdP da sua empresa não for compatível com SAML ou OpenID Connect, você poderá criar um agente de identidade personalizado para habilitar o acesso à HUAWEI CLOUD. Você pode escrever e executar código para gerar uma URL de login. Os usuários da sua empresa podem usar a URL para fazer login na HUAWEI CLOUD. Os usuários serão autenticados pelo seu IdP empresarial.

NOTA

Se o IdP empresarial for compatível com SAML ou OpenID Connect, configure **a autenticação de identidade federada** para permitir que os usuários da sua empresa acessem a HUAWEI CLOUD por meio do SSO.

Pré-requisitos

- Sua empresa possui um sistema de gerenciamento empresarial.
- Você registrou uma conta (por exemplo, **DomainA**) na HUAWEI CLOUD como um administrador empresarial.

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 senha de **UserB** no arquivo de configuração do seu IdP empresarial para que o usuário possa obter um token. Para segurança da conta, criptografe a senha e a chave de acesso antes de armazená-las.

Passo 4 Faça login no sistema de gerenciamento empresarial, acesse o agente 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** criado em **2**.

NOTA

A lista de usuários do agente personalizado é a mesma que a lista de usuários do IAM sob 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 agente 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 temporário e

securityToken. Para obter detalhes, consulte **Obtenção de uma chave de acesso temporária e SecurityToken por meio de um Token**.

Passo 6 O agente de identidade personalizado usa a chave de acesso temporária, o securityToken e o nome de domínio global do IAM (auth.huaweicloud.com) para chamar a API **POST /v3.0/OS-AUTH/securitytoken/logintokens** para obter um loginToken. O valor de **X-Subject-LoginToken** no response header 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 (auth.huaweicloud.com) do IAM.
- Um loginToken é emitido a um usuário para fazer login através de um agente 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 prazo de validade varia de 10 minutos a 12 horas. Se o valor que você especificou for maior que o período de validade restante do securityToken temporário, o período de validade restante do securityToken temporário será usado.

Passo 7 O agente de identidade personalizado gera um FederationProxyUrl e o retorna ao navegador por meio do **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 login do sistema de gerenciamento empresarial.
service	Endereço de acesso de um serviço HUAWEI CLOUD.
logintoken	LoginToken do agente 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 êxito, você será automaticamente redirecionado para o endereço de serviço da HUAWEI CLOUD especificado no parâmetro **service**.

Se o loginToken falhar ao ser 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 um exemplo de código usado para criar um FederationProxyUrl programaticamente usando um token para fazer login nos serviços da HUAWEI CLOUD.

Exemplo de código usando Java

O código 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://auth.huaweicloud.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 securityToken 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 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 securityToken.
*/
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://auth.huaweicloud.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 securityToken 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 securityToken.
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 securityToken.
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 em cima do nome de usuário e senha. Se habilitar a autenticação MFA, os usuários têm de introduzir o nome de usuário e a senha, bem como um código de verificação, antes de poderem fazer login na consola.

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 MFA virtual.

Cenários de aplicação

A autenticação MFA é adequada para proteção de login e proteção de operação crítica.

- Proteção de login: Quando você ou um IAM sob sua conta fizer login no console, você e o usuário precisam inserir um código de verificação além do nome de usuário e senha.
- Proteção da operação: Quando você ou um IAM sob sua conta tenta executar uma operação crítica, como excluir um recurso ECS, você e o usuário precisam inserir um código de verificação para prosseguir.

Para obter mais informações sobre proteção de login e proteção de operação crítica, consulte **8.3 Proteção de operação crítica**.

11.2 Dispositivo MFA virtual

Esta seção descreve como **vincular** e **desvincular** um dispositivo MFA virtual. Se o dispositivo MFA virtual vinculado de um usuário do IAM for excluído ou no celular que é executado não estiver disponível, você poderá **remover** o dispositivo MFA virtual do usuário do IAM.

O que é um dispositivo MFA virtual?

Um dispositivo MFA gera códigos de verificação de 6 dígitos em conformidade com o padrão TOTP (Time-based One-time Password Algorithm). Os dispositivos MFA podem ser baseados em hardware ou software. Atualmente, os dispositivos MFA virtuais baseados em software são suportados. Eles são programas de aplicações executados em dispositivos inteligentes, como celulares.

Vinculação de um dispositivo MFA virtual

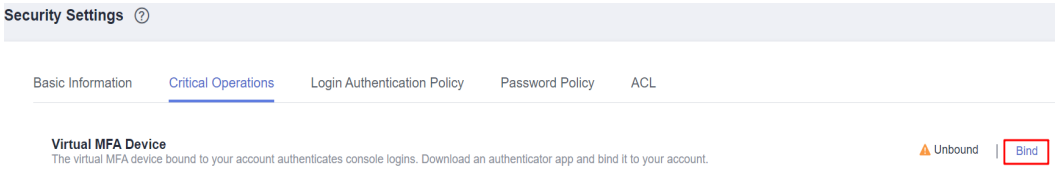
Antes de vincular um dispositivo MFA virtual, verifique se você instalou uma aplicação MFA (como a aplicação Authenticator) em seu dispositivo móvel.

- **Conta da HUAWEI CLOUD**

Passo 1 Acesse a página **Security Settings**.

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

Figura 11-1 Dispositivo MFA virtual



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

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

- Digitalização do código QR

  Abra a aplicação MFA em seu celular e use a aplicação para digitalizar o código QR exibido na página **Bind Virtual MFA Device**. Sua conta é então adicionada à aplicação.

- Inserir manualmente a chave secreta

  Abra a aplicação MFA no seu celular e insira a chave secreta.

  NOTA

  Sua conta é adicionada manualmente usando o algoritmo baseado em tempo. Certifique-se de que a definição automática da hora foi activada no seu celular.

Passo 4 Visualize o código de verificação na aplicação 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**.

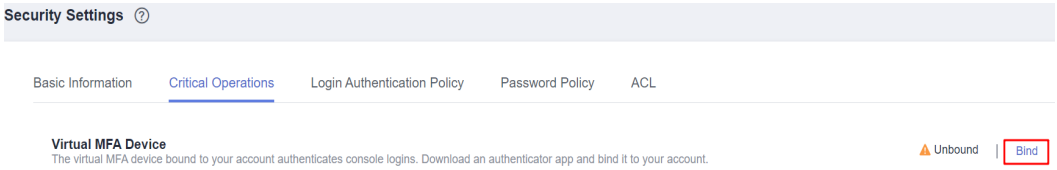
----Fim

- **HUAWEI ID**

Passo 1 Acesse a página **Security Settings**.

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

Figura 11-2 Vinculação de um dispositivo MFA virtual



Passo 3 Na página **Account & security** do centro de contas do HUAWEI ID, associe um autenticador ao seu HUAWEI ID conforme as instruções.

----Fim

Obtenção de um código de verificação do MFA

Se a proteção de login baseada em MFA virtual ou a proteção de operação estiver ativada, será necessário inserir um código de verificação do MFA ao efetuar login no console ou executar uma operação crítica.

Abra a aplicação MFA no seu dispositivo inteligente, veja o código de verificação apresentado junto à sua conta e, em seguida, insira o código na consola.

Desvinculação de um dispositivo MFA virtual

Você pode desvincular o dispositivo MFA virtual, desde que o celular vinculado ao dispositivo MFA virtual esteja disponível e o dispositivo MFA virtual ainda esteja instalado no seu celular.

- Usuário do IAM: Se o celular de um usuário do IAM não estiver disponível ou se o dispositivo MFA virtual tiver sido excluído do celular, solicite ao administrador que **remova o dispositivo MFA virtual**.
- Administrador da conta: Se o celular associado à conta não estiver disponível ou se o dispositivo MFA virtual tiver sido excluído do celular, entre em contato com o atendimento ao cliente para remover o dispositivo MFA virtual.

Passo 1 Acesse a página **Security Settings**.

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 um HUAWEI ID, você será redirecionado para o site do HUAWEI ID. Acesse 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 MFA.

Figura 11-3 Inserção de um código de verificação do MFA virtual

Passo 4 Clique em **OK**.

----Fim

Removimento de um dispositivo MFA virtual

Como a **account administrator**, Se o seu celular estiver indisponível ou se o dispositivo MFA virtual tiver sido excluído do celular, entre em contato com o atendimento ao cliente para remover o dispositivo MFA virtual.

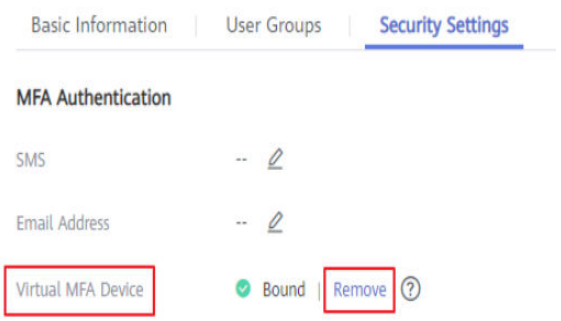
Se o celular de um usuário do IAM não estiver disponível ou se o dispositivo MFA virtual tiver sido excluído do celular, como um **administrator**, pode remover o dispositivo MFA virtual ao realizar o seguinte procedimento:

Passo 1 Faça login 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 MFA virtual vinculado.

Passo 3 Na página de guia **Critical Operations** e clique em **Remove** na linha **Virtual MFA Device**.

Figura 11-4 Removimento do dispositivo MFA virtual para um usuário do IAM



Passo 4 Clique em **Yes**.

----Fim

12 Exibição dos registros de operação do IAM

12.1 Habilitação do CTS

O CTS registra operações realizadas em recursos de nuvem na sua conta. Os logs de operação 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 Acesse o console de gerenciamento.

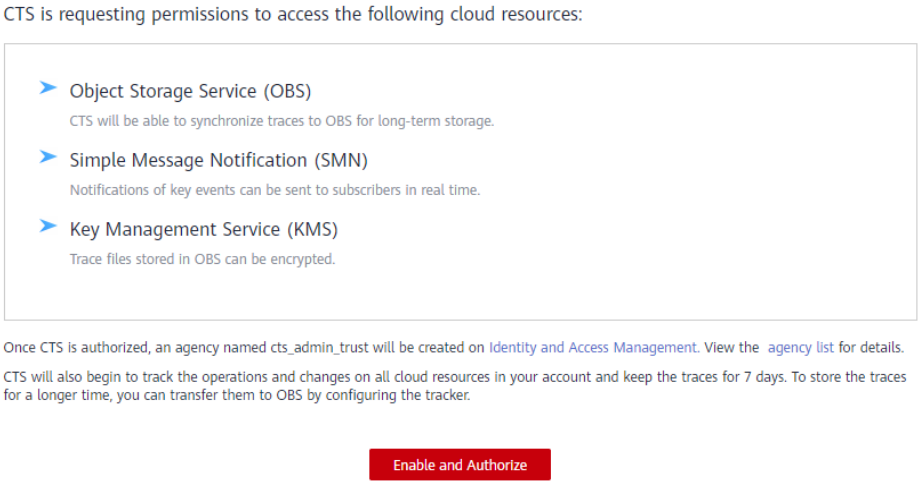
Passo 2 Se iniciar sessão na HUAWEI CLOUD utilizando uma conta, aceda a **3**. Se você fizer login como um usuário do IAM, solicita ao administrador que lhe conceda as seguintes permissões:

- Security Administrator
- CTS FullAccess

Para obter 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 Habilitação 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 ter a função de **administrador de segurança** novamente.
- Depois de você habilitar o CTS, o sistema cria automaticamente dois rastreadores para registrar rastreamentos de gerenciamento, ou seja, operações (como criação, login e exclusão) realizadas em todos os recursos da nuvem.
  - Na **current region**, um rastreador é criado para registrar os rastreamentos de gerenciamento de todos os serviços de nível de projeto implantados nessa região.
  - Na região **CN-Hong Kong**, um rastreador é criado para registrar rastros 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 no IAM que podem ser gravadas pelo CTS

Operação	Tipo de recurso	Nome do rastreamento
Fazer login	user	login
Falha de login do usuário (falha de login no Huawei ID não incluída)	user	loginFailed
Fazer logoff	user	logout
Alteração da senha no primeiro login (por um usuário do IAM)	user	changePassword

Operação	Tipo de recurso	Nome do rastreamento
Redefinição da senha	user	fpwdResetSuccess
Criação de um usuário	user	createUser
Alteração do endereço de e-mail ou número de celular	user	updateUser
Exclusão de um usuário	user	deleteUser
Criação de uma chave de acesso (AK/SK)	user	createCredential
Exclusão de uma chave de acesso (AK/SK)	user	deleteCredential
Alteração da senha	user	updateUserPwd
Fazer login inicial bem-sucedido como um usuário federado	user	tenantLoginBySamlSuccess
Fazer login bem-sucedido usando informações em cache como um usuário federado	user	federationLoginNoPwdSuccess
Criação de um grupo de usuários	userGroup	createGroup
Modificação de um grupo de usuários	userGroup	updateGroup
Exclusão de um grupo de usuários	userGroup	deleteGroup
Adição dos usuários a um grupo de usuários	userGroup	addUserToGroup
Remoção dos usuários de um grupo de usuários	userGroup	removeUserFromGroup

Operação	Tipo de recurso	Nome do rastreamento
Desvinculação de um dispositivo MFA virtual	MFA	UnBindMFA
Vinculação de um dispositivo MFA virtual	MFA	BindMFA
Criação de um projeto	project	createProject
Modificação de um projeto	project	updateProject
Criação de uma agência	agency	createAgency
Modificação de uma agência	agency	updateAgency
Exclusão de uma agência	agency	deleteAgency
Troca de uma agência	agency	switchRole
Registro de um provedor de identidade	identityProvider	createIdentityProvider
Modificação de um provedor de identidade	identityProvider	updateIdentityProvider
Exclusão de um provedor de identidade	identityProvider	deleteIdentityProvider
Atualização da política de autenticação de login	SecurityPolicy	modifySecurityPolicy
Modificação da política de senha	SecurityPolicy	modifySecurityPolicy
Modificação da ACL	SecurityPolicy	modifySecurityPolicy

12.2 Exibição dos logs de auditoria do IAM

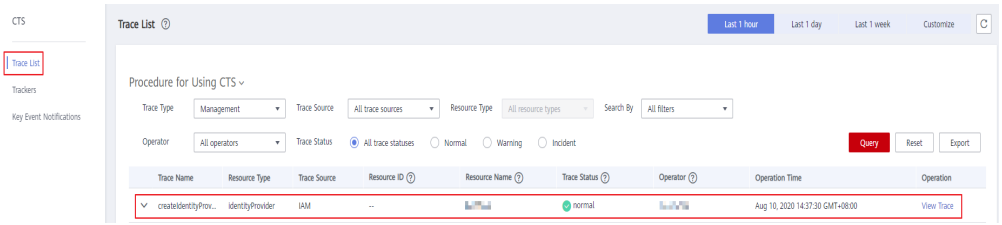
Depois de o CTS ser ativado, ele registra as principais operações executadas no IAM e em outros serviços suportados. O CTS armazena os logs de operação dos últimos 7 dias.

Procedimento

Passo 1 No console do IAM, execute uma operação, como criar um usuário chamado **CTS-Test**.

Passo 2 Faça login no console CTS e visualize os registros de operação do IAM.

Figura 12-2 Exibição dos registros de operação do IAM

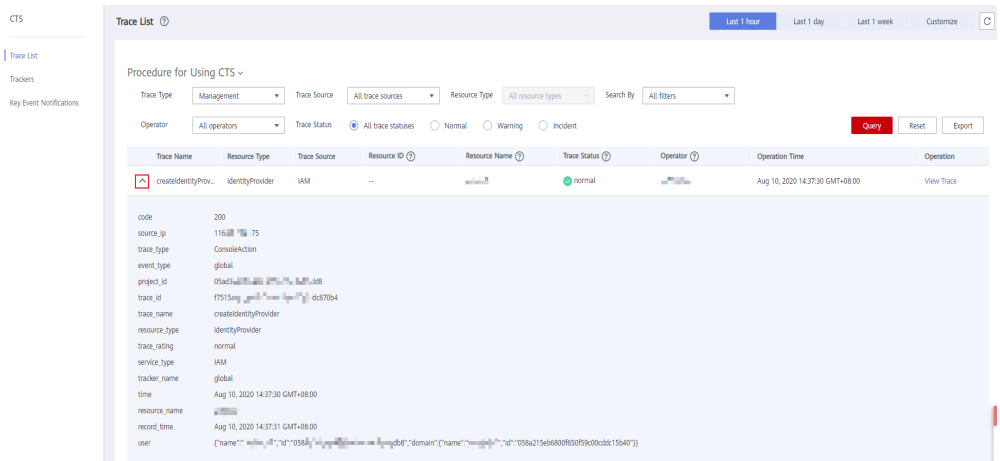


NOTA

O IAM é um serviço global, e as operações no IAM serão registradas pelo CTS sob o projeto **CN-Hong Kong** por padrão. No console do CTS, alterne para a região **CN-Hong Kong**, em seguida, visualize os registros de operação do IAM.

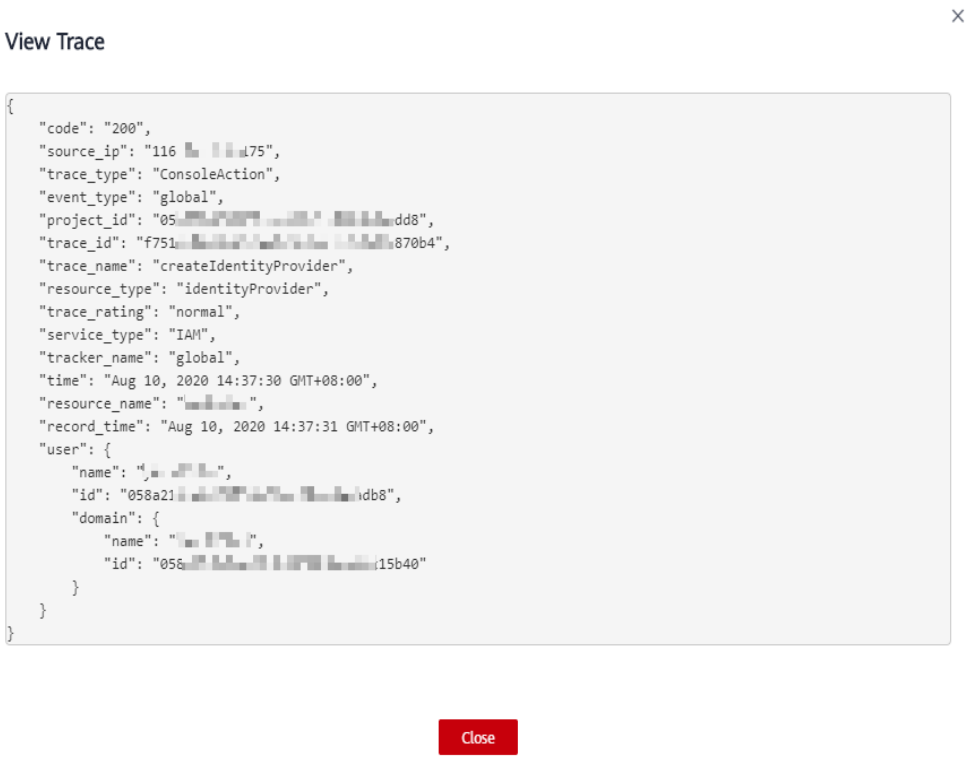
Passo 3 Clique em ⌄ ao lado de um rastreamento para exibir suas informações básicas.

Figura 12-3 Exibição das informações básicas do evento



Passo 4 Clique em **View Trace** à direita de um rastreamento para exibir a estrutura do rastreamento.

Figura 12-4 Exibição dos detalhes do evento



----Fim

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.

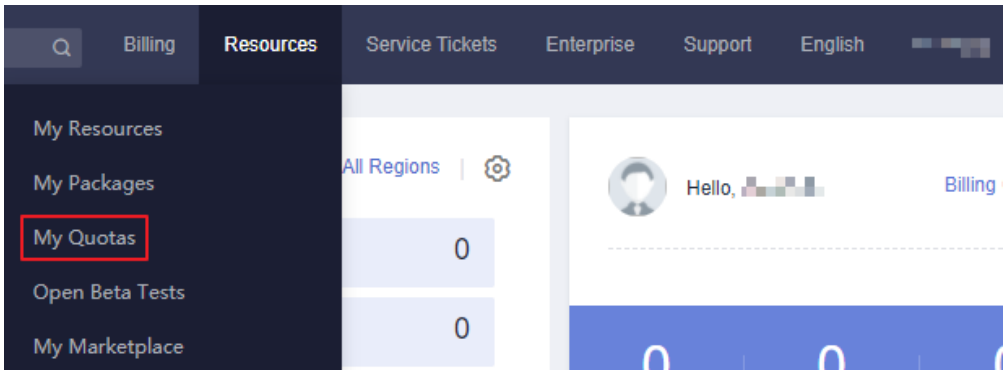
Se a cota de recursos atual não puder atender aos seus requisitos de serviço, você poderá solicitar uma cota mais alta.

Como fazer para ver minhas cotas?

1. Acesse o console de gerenciamento.
2. Clique em no canto superior esquerdo e selecione uma região e projeto.
3. No canto superior direito da página, escolha **Resources** > **My Quotas**.

   A página **Service Quota** é exibida.

   Figura 13-1 Minhas cotas



4. Na página **Service Quota**, exiba as cotas usadas e totais de cada tipo de recursos.

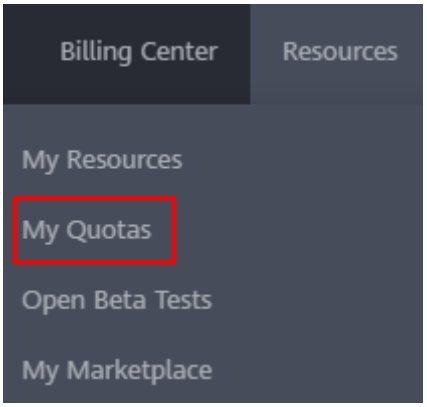
   Se a cota não puder atender aos seus requisitos de serviço, aumente a cota.

Como faço para aumentar minha cota?

1. Acesse o console de gerenciamento.

2. No canto superior direito da página, escolha **Resources** > **My Quotas**.
   A página **Service Quota** 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	Esta é o vigésimo quinto lançamento oficial. Suporte para operações em lote, incluindo informações de modificação em lote sobre usuários do IAM, usuários de exclusão em lote, grupos de usuários, agências, e permissões de revogação em lote.
30/11/2021	Esta edição é o vigésimo quarto lançamento oficial, que inclui as seguintes alterações: Seções atualizadas sobre autorização e políticas personalizadas com base em alterações na função de autorização.
01/11/2021	Esta edição é o vigésimo terceiro lançamento oficial, que inclui as seguintes alterações: Atualizado **2 Faça login na HUAWEI CLOUD** com base na nova funcionalidade de login do HUAWEI ID.
02/09/2021	Esta edição é o vigésimo segundo lançamento oficial, que inclui as seguintes alterações: ● Seção adicionada **5.5 Registros de autorização**. ● Seção adicionada **Permissões**. ● Seção modificada **4.4 Exibição ou modificação das informações do grupo de usuários**.
16/08/2021	Esta edição é o vigésimo primeiro lançamento oficial, que inclui as seguintes alterações: Seção adicionada **Autogerenciamento de informações**.
22/04/2021	Esta edição é o vigésimo lançamento oficial, que inclui as seguintes alterações: Seção adicionada **13 Cotas**.

Lançado em	Descrição
16/04/2021	Esta edição é o décimo nono lançamento oficial, que inclui as seguintes alterações: Seção adicionada **Fazer login como um usuário federado**.
27/03/2021	Esta edição é o décimo oitavo lançamento oficial, que inclui as seguintes alterações: Atualizado **2 Faça login na HUAWEI CLOUD** com base na nova funcionalidade de login do HUAWEI ID.
24/03/2021	Esta edição é o décimo sétimo lançamento oficial, que inclui as seguintes alterações: Seção adicionada **5.6.4 Serviços de nuvem suportados pelo IAM**.
30/12/2020	Esta edição é o décimo sexto lançamento oficial, que inclui as seguintes alterações: Atualizado o documento com base nas alterações na página de login, na função de configurações de segurança e nas strings da interface do usuário.
26/11/2020	Esta edição é o décimo quinto lançamento oficial, que inclui as seguintes alterações: Seção modificada **8 Configurações de segurança** com base nas alterações do console.
05/11/2020	Esta edição é o décimo quarto lançamento oficial, que inclui as seguintes alterações: ● Ajustou a estrutura de **9 Provedores de identidade**. ● Seção adicionada **9.3.1 Configuração da autenticação de identidade federada baseada em OpenID Connect**.
26/10/2020	Esta edição é o décimo terceiro lançamento oficial, que inclui as seguintes alterações: Atualizadas as capturas de tela com base na alteração para o método de fazer login.
11/09/2020	Esta edição é o décimo segundo lançamento oficial, que inclui as seguintes alterações: Seção modificada **3 Usuários do IAM** com base nas alterações do console.
18/08/2020	Esta edição é o décimo primeiro oficial, que inclui as seguintes alterações: Seção adicionada **2 Faça login na HUAWEI CLOUD**.

Lançado em	Descrição
20/04/2020	Esta edição é o décimo lançamento oficial, que inclui as seguintes alterações: Descrições adicionadas sobre a remoção de usuários em **4.2 Adição de usuários a ou remoção de usuários de um grupo de usuários**. Seção adicionada **4.5 Revogação de permissões de um grupo de usuários**.
30/03/2020	Esta edição é o nono lançamento oficial, que inclui as seguintes alterações: Descrições excluídas de testes beta abertos para controle de acesso baseado em política. Esta função está atualmente em uso comercial.
10/02/2020	Esta edição é o oitavo lançamento oficial, que inclui as seguintes alterações: Seção adicionada **5.4 Alteração dos nomes de política definidos pelo sistema**. Seção modificada **4.1 Criação de um grupo de usuários e atribuição de permissões** com base nas alterações do nome de política.
20/01/2020	Esta edição é o sétimo lançamento oficial, que inclui as seguintes alterações: Modificou as seguintes seções com base nas alterações do console: **4 Grupos de usuários e autorização** e **5 Permissões**
20/11/2019	Esta edição é o sexto lançamento oficial, que inclui as seguintes alterações: Adicionado **VPC Endpoints** em **8.6 ACL**. Adicionada **Enabling/Disabling an access key** em **3.7 Gerenciamento das chaves de acesso de um usuário do IAM**.
15/10/2019	Esta edição é o quinto lançamento oficial, que inclui as seguintes alterações: Seção adicionada **5.6.2 Modificação ou exclusão de uma política personalizada**. Adicionadas descrições sobre a criação de políticas personalizadas no editor visual em **5.6.1 Criação de um política personalizada**. Descrições adicionadas 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 quarto lançamento oficial, que inclui as seguintes alterações: Seção adicionada **10 Agente identificador personalizado**.
11/06/2019	Esta edição é o terceiro lançamento oficial, que inclui as seguintes alterações: Capítulos otimizados **1 Antes de começar**, **3 Usuários do IAM**, **4 Grupos de usuários e autorização**, **5 Permissões**, **6 Projetos**, **8 Configurações de segurança**, e **12 Exibição dos registros de operação do IAM**.
13/02/2018	Esta edição é o segundo lançamento oficial, que inclui as seguintes alterações: Adicionada uma tabela que descreve os tipos de agência em **7 Agências**.
30/12/2017	Esta edição é o primeiro lançamento oficial.

