

Identity and Access Management

Perguntas frequentes sobre o IAM

Edição 01
Data 24-08-2023



Copyright © Huawei Technologies Co., Ltd. 2024. Todos os direitos reservados.

Nenhuma parte deste documento pode ser reproduzida ou transmitida em qualquer forma ou por qualquer meio sem consentimento prévio por escrito da Huawei Technologies Co., Ltd.

Marcas registadas e permissões



HUAWEI 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 Grupos de usuários e gerenciamento de permissões.....	1
1.1 Por que não consigo encontrar permissões para um serviço de nuvem?.....	1
1.2 Como conceder permissões de serviço de nuvem na região EU-Dublin para usuários do IAM?.....	2
1.3 Por que as permissões concedidas a um usuário não entram em vigor?.....	3
1.4 Como conceder a um usuário do IAM permissões para fazer pedidos, mas não permitir o pagamento do pedido?.....	4
2 Gerenciamento de usuários do IAM.....	8
2.1 Por que o logon de usuário do IAM falha?.....	8
2.2 Como controlar o acesso de usuários do IAM ao console?.....	9
3 Configurações de segurança.....	10
3.1 Como ativar a verificação de logon?.....	10
3.2 Como desativar a verificação de logon?.....	11
3.3 Como alterar o método de verificação para executar operações críticas?.....	13
3.4 Como desativar a proteção de operação?.....	16
3.5 Como vincular um dispositivo de MFA virtual?.....	17
3.6 Como obter um código de verificação de MFA virtual?.....	18
3.7 Como desvincular ou remover um dispositivo de MFA virtual?.....	19
3.8 Por que a autenticação MFA falha?.....	21
3.9 Por que não estou recebendo o código de verificação?.....	22
3.10 Por que minha conta está bloqueada?.....	23
3.11 Por que minha política de controle de acesso à API não entra em vigor?.....	23
3.12 Por que ainda preciso executar a MFA durante o logon após desvincular o dispositivo de MFA virtual?.....	24
4 Senhas e credenciais.....	26
4.1 O que devo fazer se eu esqueci minha senha?.....	26
4.2 Como alterar minha senha?.....	30
4.3 Como obter uma chave de acesso (AK/SK)?.....	30
4.4 O que devo fazer se eu esqueci minha chave de acesso (AK/SK)?.....	31
4.5 O que são credenciais de segurança temporárias (AK/SK e token de segurança)?.....	31
4.6 Como obter um token com permissões de Security Administrator?.....	32
4.7 Como obter uma chave de acesso (AK/SK) na região EU-Dublin?.....	33
5 Gerenciamento de projetos.....	35
5.1 Quais são as diferenças entre IAM e Enterprise Management?.....	35
5.2 Quais são as diferenças entre projetos do IAM e projetos empresariais?.....	37

5.3 Quais são as diferenças entre usuários do IAM e contas de membros empresariais?.....	37
6 Gerenciamento da agência.....	39
6.1 Como obter permissões para criar uma agência?.....	39
7 Gerenciamento de contas.....	40
7.1 Por que o logon da conta falha?.....	40
7.2 Quais são as relações entre uma conta da Huawei Cloud, uma HUAWEI ID, um usuário do IAM e um usuário federado?.....	42
7.3 Quais são as possíveis causas de uma falha de atualização da HUAWEI ID?.....	45
7.4 Posso fazer logon com minha conta da HUAWEI CLOUD depois de atualizá-la para uma HUAWEI ID?.....	46
8 Outros.....	47
8.1 Como obter um token de usuário usando o Postman?.....	47
8.2 Por que a ajuda em nível de campo é sempre exibida?.....	50
8.3 Como desativar o preenchimento automático de senha no Google Chrome?.....	50
8.4 Região e AZ.....	51
8.5 Como solicitar as permissões para acessar recursos em uma região da aliança de nuvem usando minha conta da Huawei Cloud ou HUAWEI ID?.....	53

1 Grupos de usuários e gerenciamento de permissões

- 1.1 Por que não consigo encontrar permissões para um serviço de nuvem?
- 1.2 Como conceder permissões de serviço de nuvem na região EU-Dublin para usuários do IAM?
- 1.3 Por que as permissões concedidas a um usuário não entram em vigor?
- 1.4 Como conceder a um usuário do IAM permissões para fazer pedidos, mas não permitir o pagamento do pedido?

1.1 Por que não consigo encontrar permissões para um serviço de nuvem?

Sintoma

Não é possível encontrar permissões para um serviço de nuvem específico ao atribuir permissões a um grupo de usuários ou a uma agência no console do IAM.

Possíveis causas

- O serviço não é suportado pelo IAM. Não há permissões disponíveis para o serviço no IAM. Para os serviços de nuvem suportados pelo IAM, consulte [Serviços de nuvem com suporte](#).
- O nome do serviço ou o nome da permissão está incorreto.

Soluções

- [Envie um tíquete de serviço](#) e solicite o registro de permissões para o serviço específico no IAM.
- Verifique o nome do serviço no console de gerenciamento ou na central de ajuda e visualize as permissões definidas pelo sistema fornecidas pelo serviço em [Permissões definidas pelo sistema](#).

1.2 Como conceder permissões de serviço de nuvem na região EU-Dublin para usuários do IAM?

Sintoma


O administrador ativou os serviços de nuvem na região **EU-Dublin** e precisa autorizar os usuários do IAM a usar os serviços de nuvem nessa região.

Os usuários acessam os serviços de nuvem na região **EU-Dublin** como usuários virtuais autorizados por meio de autenticação federada. Eles não são usuários reais que existem no sistema de serviço de nuvem e precisam ser autorizados nas regiões padrão da Huawei Cloud e na região **EU-Dublin**, respectivamente.

Pré-requisitos

- Você criou um usuário do IAM em uma região padrão da Huawei Cloud e adicionou o usuário a um grupo de usuários. Por exemplo, você criou o usuário do IAM **User-001** e o adicionou ao grupo de usuários **UserGroup-001**. Para obter detalhes, consulte [Criação de um usuário do IAM](#) e [Adição de usuários a um grupo de usuários ou remoção de usuários de um grupo de usuários](#).
- Se esta for a primeira vez que concede permissões de serviço de nuvem para usuários do IAM na região **EU-Dublin**, será necessário usar uma conta em vez de um usuário do IAM com permissões de administrador para realizar operações de autorização.

Procedimento

Passo 1 Faça login na Huawei Cloud como um administrador, clique em  na página inicial do console e selecione a região **EU-Dublin**.

Passo 2 No console, escolha **Management & Governance** > **Identity and Access Management**.

Passo 3 No console do IAM, escolha **User Groups** no painel de navegação e clique em **Create User Group** no canto superior direito para criar um grupo com o mesmo nome (**UserGroup-001**).

Passo 4 Na página **User Groups**, clique em **Modify** na linha que contém o grupo de usuários criado em **3**.

Passo 5 Na área **Group Permissions**, clique em **Attach Policy** na linha que contém a região de destino para autorização do usuário, selecione as permissões desejadas e clique em **OK**.

As permissões atribuídas a esse grupo também se aplicarão aos usuários do IAM no grupo de usuários da Huawei Cloud.

Passo 6 Clique em **OK** para concluir a autorização para usuários do IAM na região **EU-Dublin**.

----Fim

Após a conclusão da autorização, faça login no console da Huawei Cloud como um usuário do IAM. Selecione a região **EU-Dublin** e use os recursos da nuvem com base nas permissões atribuídas.

1.3 Por que as permissões concedidas a um usuário não entram em vigor?

Sintoma

As permissões que você concede a um usuário do IAM não entram em vigor.

Solução de problemas

1. Causa: permissões incorretas foram concedidas ao grupo de usuários ao qual o usuário pertence.

Solução: peça ao administrador para modificar as permissões concedidas ao grupo de usuários ao qual o usuário do IAM pertence. Para obter detalhes, consulte [Modificação de permissões de grupos de usuários](#). Para obter detalhes sobre permissões, consulte [Permissões definidas pelo sistema](#).
2. Causa: as ações são negadas pelas permissões concedidas ao usuário.

Visualize as permissões definidas pelo sistema concedidas ao usuário do IAM e verifique se há uma declaração de política que nega a ação. Para obter detalhes, consulte [Sintaxe da política](#). Se as permissões definidas pelo sistema não puderem atender aos seus requisitos, crie uma política personalizada para permitir a ação. Para obter detalhes, consulte [Criação de uma política personalizada](#).
3. Causa: o usuário do IAM não foi adicionado ao grupo de usuários com permissões atribuídas.

Solução: adicione o usuário ao grupo de usuários de destino como administrador. Para obter detalhes, consulte [Adição de usuários a um grupo de usuários](#).
4. Causa: para um serviço regional, o grupo de usuários não é atribuído com permissões em regiões específicas.

Atribua permissões ao grupo de usuários em regiões específicas. Se você tiver atribuído ao usuário apenas permissões para um projeto específico de região padrão, o usuário não terá permissões para os subprojetos. Nesse caso, atribua permissões para o subprojeto necessário. Para obter detalhes, consulte [Atribuição de permissões a um grupo de usuários](#).
5. Causa: o usuário do IAM não mudou para a região em que foi autorizado a usar os recursos de nuvem.

Lembre o usuário de mudar para a região onde o usuário está autorizado a usar os recursos de nuvem. Para obter detalhes, consulte [Mudança de regiões](#).
6. Causa: se o administrador tiver concedido permissões do OBS ao usuário, as permissões entrarão em vigor de 15 a 30 minutos após a autorização.

Verifique as permissões após 15 a 30 minutos e tente novamente.
7. Causa: o cache do navegador não foi limpo por um longo tempo.

Limpe o cache do navegador e tente novamente.
8. Causa: o serviço (como OBS) fornece controle de permissões separado.

Conceda permissões ao usuário consultando a documentação do serviço. Por exemplo, consulte [Introdução ao controle de permissões do OBS](#).
9. Causa: se você concedeu permissões a um usuário no IAM e no Enterprise Management, as permissões para projetos empresariais podem não entrar em vigor. A autenticação do

IAM tem precedência sobre a autenticação do Enterprise Management. Se um usuário do IAM tiver a permissão **ECS ReadOnlyAccess** para todos os recursos e o projeto empresarial A, ele poderá visualizar todos os recursos do ECS.

Modifique as permissões do usuário no console do IAM.

Pergunta frequente relacionada

Sintoma: você concedeu a um usuário do IAM apenas as permissões necessárias, mas o usuário tem mais permissões.

Possíveis causas:

1. As permissões necessárias concedidas ao usuário do IAM têm permissões de dependência, que são atribuídas automaticamente para que as permissões necessárias entrem em vigor para o usuário.
2. Você concedeu outras permissões ao usuário do IAM no Gerenciamento de projetos empresariais. Se você gerencia projetos e usuários usando o IAM, cancele as permissões configuradas lá. Para obter detalhes, consulte [Exclusão de projetos empresariais gerenciados por um usuário](#).

1.4 Como conceder a um usuário do IAM permissões para fazer pedidos, mas não permitir o pagamento do pedido?

Sintoma

Você deseja conceder a um usuário do IAM permissões para fazer pedidos, mas não permitir que o usuário pague pelos pedidos.

Soluções

No entanto, as permissões do sistema do Central de cobrança registrado no IAM não podem atender aos seus requisitos. Você precisa criar uma política personalizada contendo as permissões necessárias e usar a política para conceder permissões ao usuário do IAM.

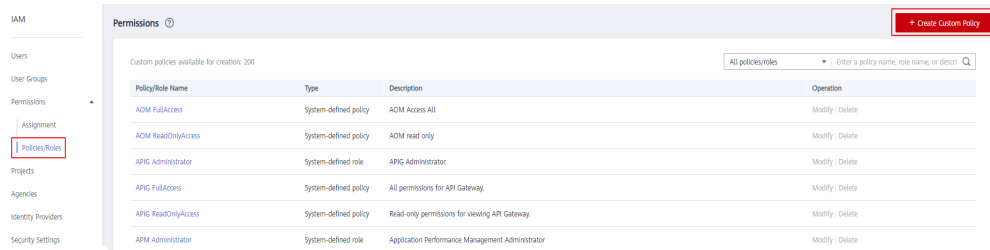
Pré-requisitos

Você já criou o usuário A do IAM e o grupo B de usuários e adicionou o usuário ao grupo de usuários. Para obter detalhes, consulte [Criação de um usuário do IAM](#).

Procedimento

- Passo 1** Faça logon no console de gerenciamento da HUAWEI CLOUD.
- 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.
- Passo 3** No console do IAM, escolha **Permissions > Policies/Roles** no painel de navegação e clique em **Create Custom Policy** no canto superior direito.

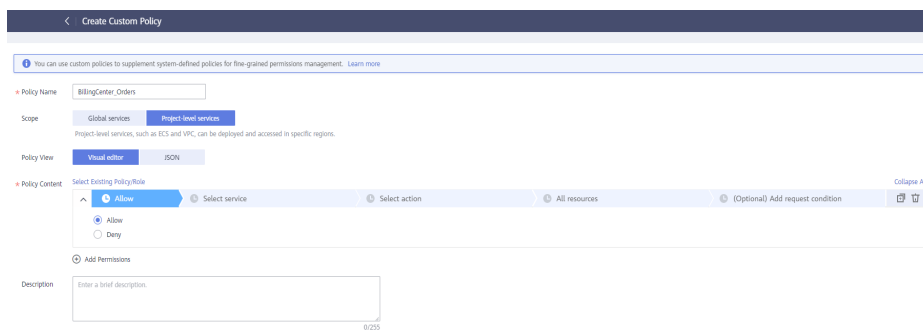
Figura 1-1 Criação de uma política personalizada



Passo 4 Defina o nome da política como **BillingCenter_Orders**.

Passo 5 Defina o escopo para **Project-level services**.

Figura 1-2 Configurar o escopo

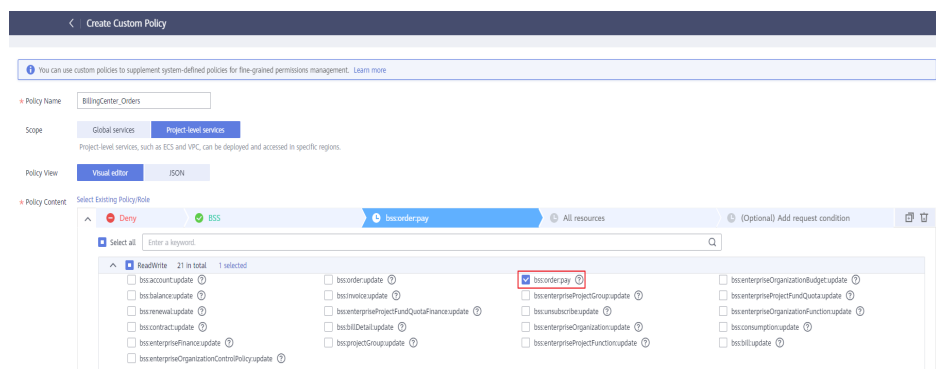


Passo 6 Selecione **Visual editor**.

Passo 7 Na área **Policy Content**, configure as permissões que permitem ao usuário fazer pedidos, mas não permitem que o usuário pague pelos pedidos.

- Configurar permissões para não permitir o pagamento de pedidos
 - a. Selecione **Deny**.
 - b. Para o serviço de nuvem, selecione **BSS (BSS)**.
 - c. Na etapa **Select action**, expanda a área **ReadWrite** e selecione a ação **bss:order:pay**.

Figura 1-3 Configurar permissões para não permitir o pagamento de pedidos

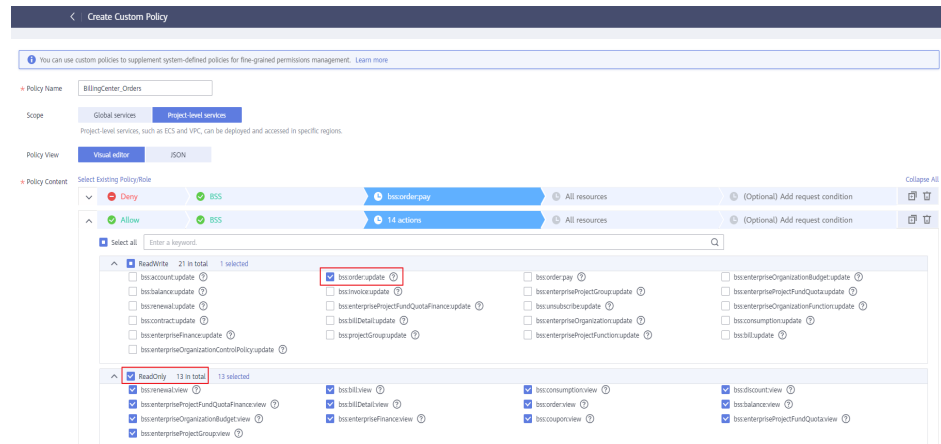


d. Defina o tipo de recurso como **All**.

- Configurar permissões para permitir a colocação de pedidos

- a. Selecione **Allow**.
- b. Para o serviço de nuvem, selecione **BSS (BSS)**.
- c. Na etapa **Select action**, expanda a área **ReadWrite**, selecione a ação **bss:order:update** e selecione todas as ações na área **ReadOnly**.

Figura 1-4 Configurar permissões para permitir a colocação de pedidos



- d. Defina o tipo de recurso como **All**.

Passo 8 Defina uma descrição para a política, por exemplo, "Permissões para fazer pedidos, mas não permitir o pagamento do pedido".

Passo 9 Clique em **OK**.

Passo 10 Anexe a política ao grupo B de usuários. Os usuários do grupo herdam as permissões definidas nesta política.

NOTA

Você pode anexar políticas personalizadas a um grupo de usuários da mesma forma que anexa políticas definidas pelo sistema. Para obter detalhes, consulte [Criação de um grupo de usuários e atribuição de permissões](#).

Passo 11 Quando o usuário do IAM faz logon e acessa a página **My Orders** de Central de cobrança, o botão **Pay** não é exibido na coluna **Operation**.

Figura 1-5 A página Meus pedidos é exibida se as permissões forem concedidas com sucesso

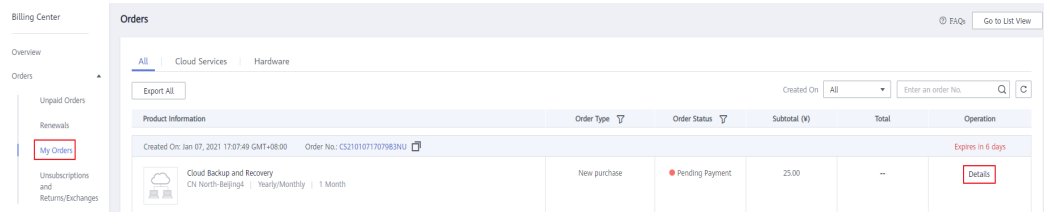
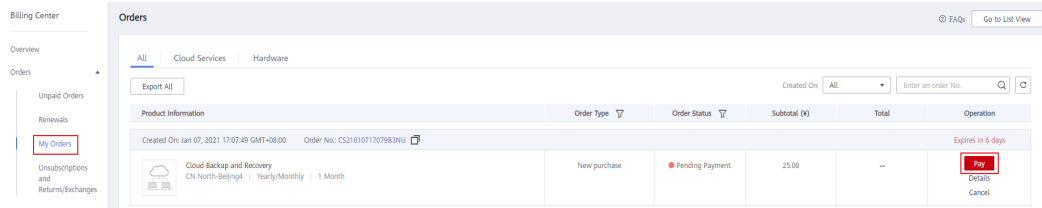


Figura 1-6 Página Meus pedidos exibida se as permissões não foram concedidas



----Fim

2 Gerenciamento de usuários do IAM

[2.1 Por que o logon de usuário do IAM falha?](#)

[2.2 Como controlar o acesso de usuários do IAM ao console?](#)

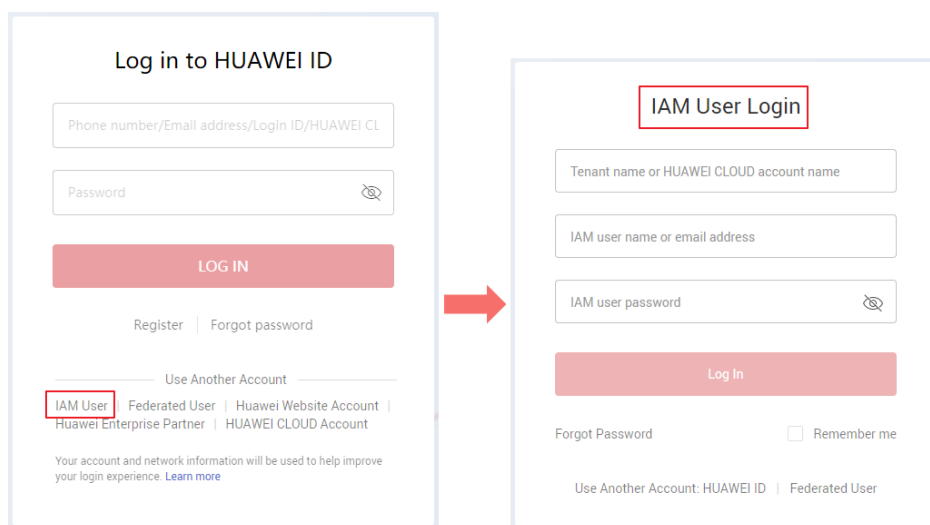
2.1 Por que o logon de usuário do IAM falha?

Sintoma

Um usuário do IAM não consegue efetuar logon e vê uma mensagem indicando que o nome de usuário ou a senha está incorreto ou que o logon do dispositivo atual não é permitido devido às regras de controle de acesso definidas pelo administrador.

Solução de problemas

- **Nome de usuário ou senha incorretos**
 - a. Você selecionou uma entrada de logon incorreta.
Clique em **IAM User** na página de logon.



- b. Nome do locatário/nome da conta da Huawei Cloud ou nome de usuário do IAM incorretos.

- Digite o nome do locatário/nome da conta da Huawei Cloud e o nome de usuário do IAM incorretos. Se você não souber seu nome de usuário do IAM ou o nome da conta usada para criar o usuário do IAM, entre em contato com o administrador.
- c. Senha incorreta.
Insira a senha correta. Se você esqueceu sua senha, redefina-a consultando [Como redefinir minha senha?](#)
 - d. Você não limpou o cache do navegador depois de alterar ou redefinir a senha.
Limpe o cache do navegador e faça logon novamente.
- **Logon do dispositivo atual não é permitido devido às regras de controle de acesso definidas pelo administrador.**
 - a. O administrador definiu regras de controle de acesso no console do IAM para limitar o acesso da Huawei Cloud a intervalos de endereços IP específicos, blocos CIDR IPv4 ou pontos de extremidade da VPC.
Solução: entre em contato com o administrador para verificar as regras de ACL no console e faça logon na Huawei Cloud a partir de um dispositivo permitido ou peça ao administrador para modificar as regras de ACL. Para obter detalhes, consulte [Controle de acesso](#)

2.2 Como controlar o acesso de usuários do IAM ao console?

Para garantir a segurança das informações do usuário e do sistema, é possível configurar uma ACL que permita o acesso do usuário somente a partir de endereços IP específicos.

Procedimento

Passo 1 Faça logon no console do IAM.

Passo 2 No painel de navegação, escolha **Security Settings > ACL**.

NOTA

A ACL entrará em vigor apenas para os usuários do IAM que você criou usando sua conta.

Passo 3 Clique na guia **Console Access** e defina endereços IP ou blocos CIDR IPv4 com permissão para acessar o console.

- **IP Address Ranges:** permitir que os usuários acessem o sistema usando endereços IP em intervalos específicos.
- **IPv4 CIDR Blocks:** permitir que os usuários acessem o sistema usando blocos CIDR IPv4 específicos.

Por exemplo: **10.10.10.10/32**.

NOTA

Se você especificar **IP Address Ranges** e **IPv4 CIDR Blocks**, os usuários terão permissão para acessar o sistema se seus endereços IP atenderem às condições especificadas por um dos dois parâmetros.

Passo 4 Clique em **Save**.

----Fim

3 Configurações de segurança

[3.1 Como ativar a verificação de logon?](#)

[3.2 Como desativar a verificação de logon?](#)

[3.3 Como alterar o método de verificação para executar operações críticas?](#)

[3.4 Como desativar a proteção de operação?](#)

[3.5 Como vincular um dispositivo de MFA virtual?](#)

[3.6 Como obter um código de verificação de MFA virtual?](#)

[3.7 Como desvincular ou remover um dispositivo de MFA virtual?](#)

[3.8 Por que a autenticação MFA falha?](#)

[3.9 Por que não estou recebendo o código de verificação?](#)

[3.10 Por que minha conta está bloqueada?](#)

[3.11 Por que minha política de controle de acesso à API não entra em vigor?](#)

[3.12 Por que ainda preciso executar a MFA durante o logon após desvincular o dispositivo de MFA virtual?](#)

3.1 Como ativar a verificação de logon?

Para garantir a segurança da conta, é aconselhável ativar a verificação de logon.

Depois de ativar essa função, você e os usuários do IAM criados usando sua conta precisam inserir códigos de verificação gerados pelo dispositivo de MFA virtual vinculado, códigos de verificação de SMS ou códigos de verificação de e-mail na página **Login Verification** durante o logon.

Se você desativar essa função, você e os usuários do IAM só precisarão inserir o nome da conta/nome de usuário e a senha durante o logon.

Procedimento

- Ativar a verificação de logon para um usuário do IAM no console do IAM como administrador

Passo 1 No painel de navegação, escolha **Users**.

Passo 2 Clique em **Security Settings** na linha que contém o usuário de destino.

Passo 3 Na guia **Security Settings**, na área **Login Protection**, selecione um método de verificação e insira um código de verificação.

Passo 4 Clique em **OK**.

----Fim

- Ativar a verificação de logon para si mesmo (administrador da conta) na página **Security Settings**

Execute as etapas a seguir se sua conta da Huawei Cloud não tiver sido atualizada para uma HUAWEI ID. Para habilitar a verificação de logon para uma HUAWEI ID, acesse o [site da HUAWEI ID](#).

Passo 1 Passe o ponteiro do mouse sobre o nome de usuário no canto superior direito e selecione **Security Settings** na lista suspensa.

Passo 2 Clique na guia **Critical Operations** e clique em **Enable** ao lado de **Login Protection**.


Passo 3 Na página **Login Protection**, selecione **Enable**, selecione um método de verificação e insira um código de verificação.

Passo 4 Clique em **OK**.

----Fim

Operações relacionadas

Você pode alterar o método de verificação de logon de seus usuários ou conta do IAM:

- Para alterar o método de verificação de logon de um usuário do IAM, vá para a lista de usuários no console do IAM, clique em **Security Settings** na linha que contém o usuário, clique em  ao lado de **Verification Method** em **Login Protection** e altere o método de verificação.
- Para alterar o método de verificação de logon da sua conta, vá para a página **Security Settings**. Na guia **Critical Operations**, clique em **Change** ao lado de **Login Protection** e, em seguida, altere o método de verificação.

3.2 Como desativar a verificação de logon?

Para garantir a segurança da conta, é aconselhável ativar a verificação de logon.

Depois de ativar essa função, você e os usuários do IAM criados usando sua conta precisam inserir códigos de verificação gerados pelo dispositivo de MFA virtual vinculado, códigos de verificação de SMS ou códigos de verificação de e-mail na página **Login Verification** durante o logon.


Se você desativar essa função, você e os usuários do IAM só precisarão inserir o nome da conta/nome de usuário e a senha durante o logon.

Desativação da verificação de logon do usuário do IAM como um administrador

- Um administrador pode desativar a verificação de logon para um usuário do IAM no console do IAM da seguinte maneira:

Passo 1 No painel de navegação, escolha **Users**.

Passo 2 Clique em **Security Settings** na linha que contém o usuário de destino.

Passo 3 Na página de guia **Security Settings**, clique em  ao lado de **Verification Method** em **Login Protection** e selecione **Disabled**.

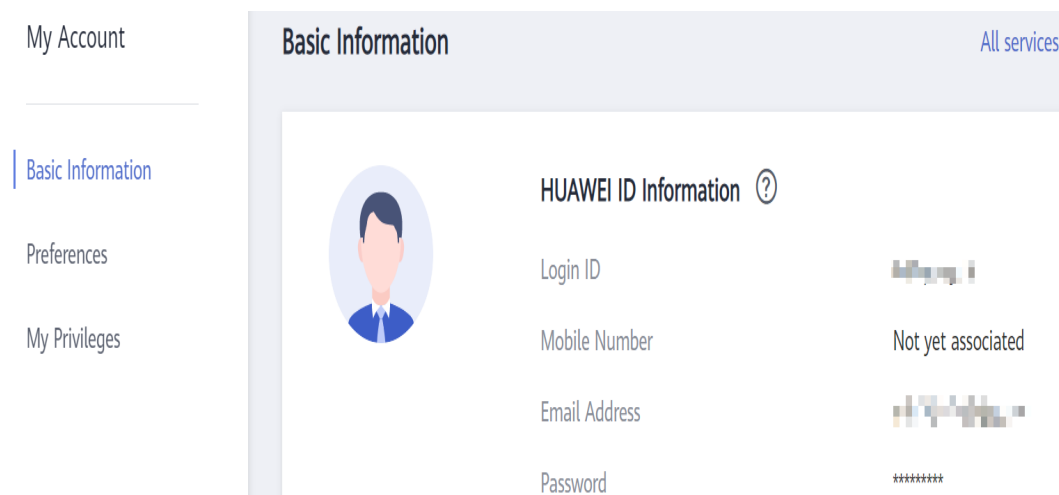
Passo 4 Clique em **OK**.

----Fim

Desativação da verificação de logon do administrador

Verifique se a conta atual é uma HUAWEI ID ou conta da Huawei Cloud passando o mouse sobre o nome da conta de logon no canto superior direito e clicando em **Basic Information** na lista suspensa. Se **HUAWEI ID Information** for exibido na área de **Basic Information**, a conta atual é uma HUAWEI ID. Caso contrário, a conta atual é uma conta da Huawei Cloud. Desative a verificação de logon para uma HUAWEI ID realizando as operações descritas em [Desativação da função de verificação de logon para uma Huawei ID](#). Desative a verificação de logon para uma conta da Huawei Cloud executando as operações descritas em [Desativação da verificação de logon para você mesmo \(administrador da conta\)](#).

Figura 3-1 Informações da HUAWEI ID



- Desativar a função de verificação de logon para uma HUAWEI ID
Escolha **Huawei Account Center** > **Account & Security** > **Security Verification** > **Two-step verification**, clique em **Disable** e insira as informações de verificação para desativar a proteção de logon.
- Desativar a verificação de logon para você mesmo (administrador da conta) na página **Security Settings**

Passo 1 Passe o ponteiro do mouse sobre o nome de usuário no canto superior direito e selecione **Security Settings** na lista suspensa.

Passo 2 Clique na guia **Critical Operations** e clique em **Change** ao lado de **Login Protection**.

Passo 3 Na página **Login Protection**, selecione **Disable**.

Passo 4 Clique em **OK**.

---Fim

3.3 Como alterar o método de verificação para executar operações críticas?

Sintoma

Se a proteção de operação estiver ativada, os usuários sob sua conta poderão prosseguir com uma operação crítica, como excluir um recurso e criar uma chave de acesso, somente depois que os usuários ou a pessoa especificada concluírem a verificação.

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

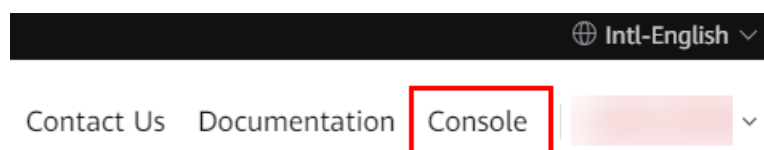
- Para alterar o método de verificação de **Self-verification** para **Verification by another person**, consulte [Autoverificação](#).
- Para alterar o método de verificação de **Verification by another person** para **Self-verification** ou para alterar o número de celular ou endereço de e-mail para verificação, consulte [Verificação por outra pessoa](#).

Procedimento

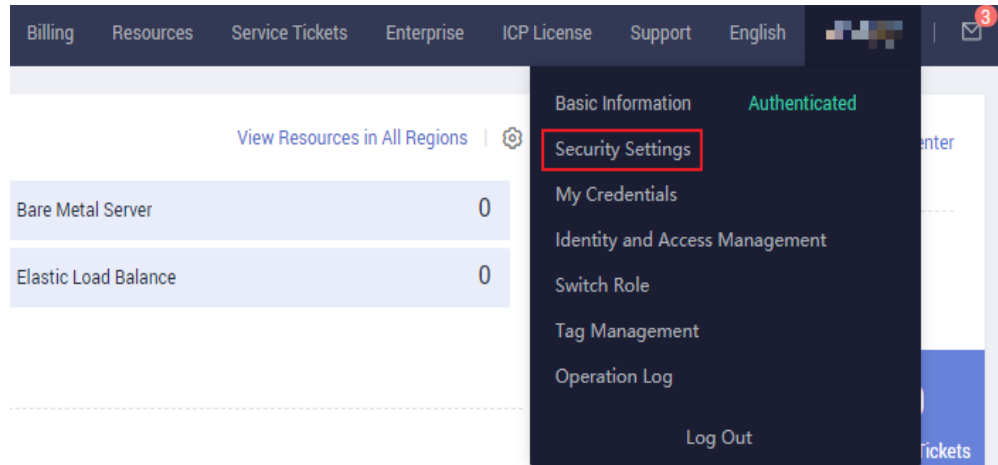
- **O método de verificação atual é a autoverificação.**

Passo 1 Faça logon no console de gerenciamento.

Figura 3-2 Fazer logon no console de gerenciamento



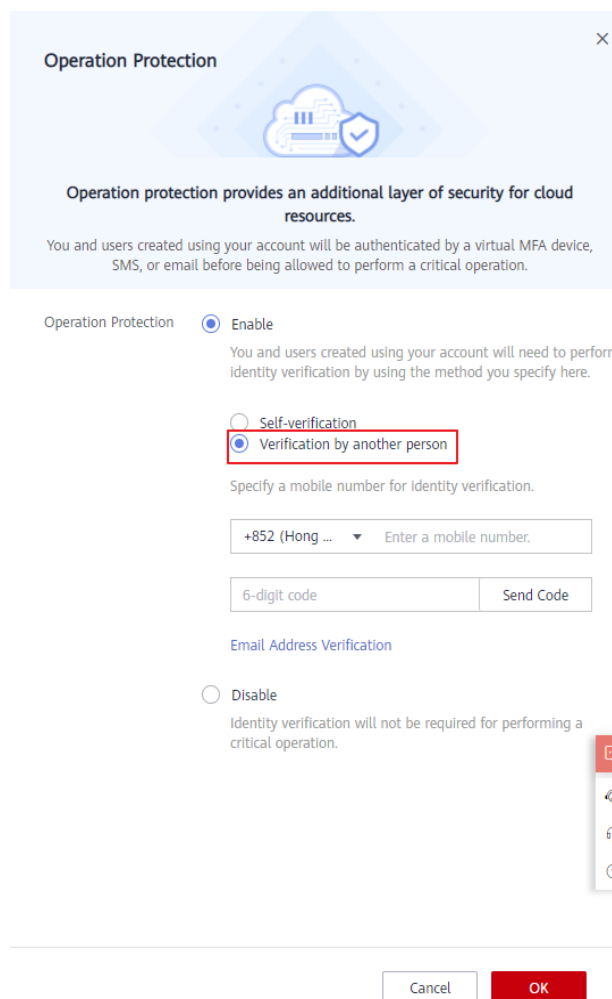
Passo 2 No console de gerenciamento, passe o ponteiro do mouse sobre o nome de usuário no canto superior direito e escolha **Security Settings** na lista suspensa.



Passo 3 Na página **Security Settings**, clique na guia **Critical Operations** e clique em **Change** ao lado de **Operation Protection**.

Passo 4 Na página **Operation Protection**, selecione **Verification by another person**, insira o número de celular ou endereço de e-mail para verificação e insira o código de verificação.

Figura 3-3 Configurações de proteção de operação



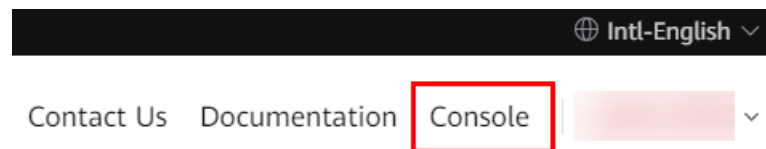
Passo 5 Clique em **OK**.

----Fim

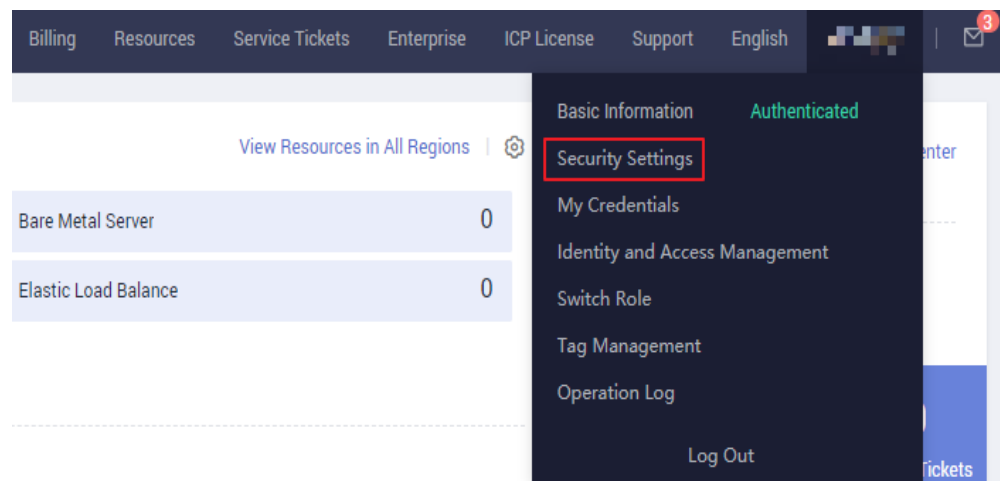
- **O método de verificação atual é Verification by another person.**

Passo 1 Faça login no console de gerenciamento.

Figura 3-4 Fazer login no console de gerenciamento



Passo 2 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.



Passo 3 Na página **Security Settings**, clique na guia **Critical Operations** e clique em **Change** ao lado de **Operation Protection**.

Passo 4 Na página **Operation Protection**, selecione **Disable** e clique em **OK**. Digite o código de verificação e clique em **OK**.

Passo 5 Na página de guia **Critical Operations**, clique em **Enable** ao lado de **Operation Protection**.

Passo 6 Na página **Operation Protection**, selecione **Self-verification** ou **Verification by another person**.

Se você selecionar **Verification by another person**, conclua a verificação para garantir que o método de verificação esteja disponível.

- **Self-verification**: você ou os próprios usuários do IAM executam a verificação ao executar uma operação crítica.
- **Verification by another person**: a pessoa especificada executa a verificação quando você ou um usuário do IAM executa uma operação crítica. Apenas a verificação de SMS e e-mail é suportada.

Passo 7 Clique em **OK**.

----Fim

3.4 Como desativar a proteção de operação?

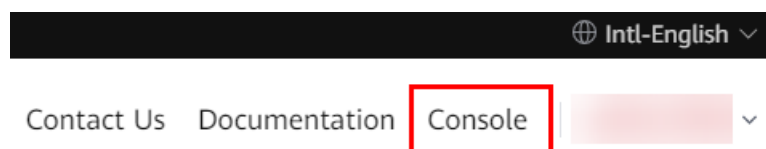
Sintoma

Se a proteção de operação estiver ativada, os usuários sob sua conta poderão prosseguir com uma operação crítica (como excluir um recurso e criar uma chave de acesso) somente depois que os usuários ou a pessoa especificada concluírem a verificação. Para desativar a proteção de operação, execute o procedimento a seguir.

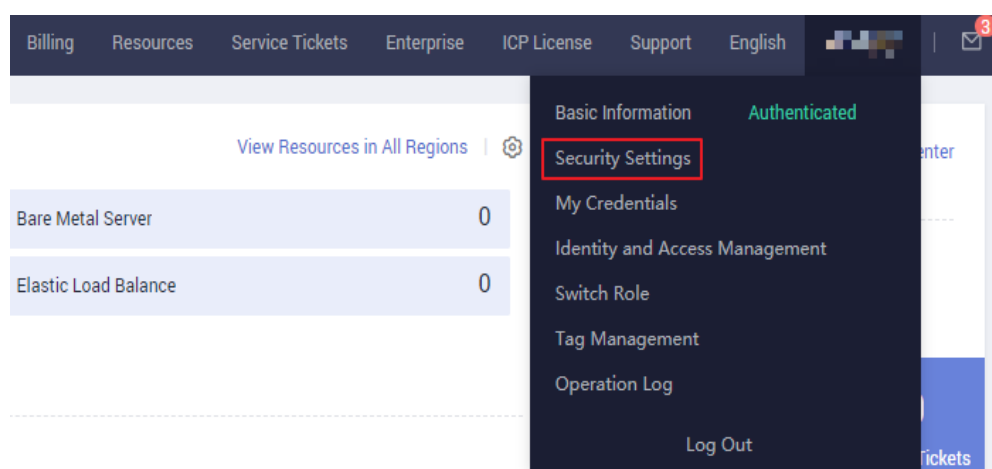
Procedimento

Passo 1 Faça login no console de gerenciamento.

Figura 3-5 Fazer login no console de gerenciamento



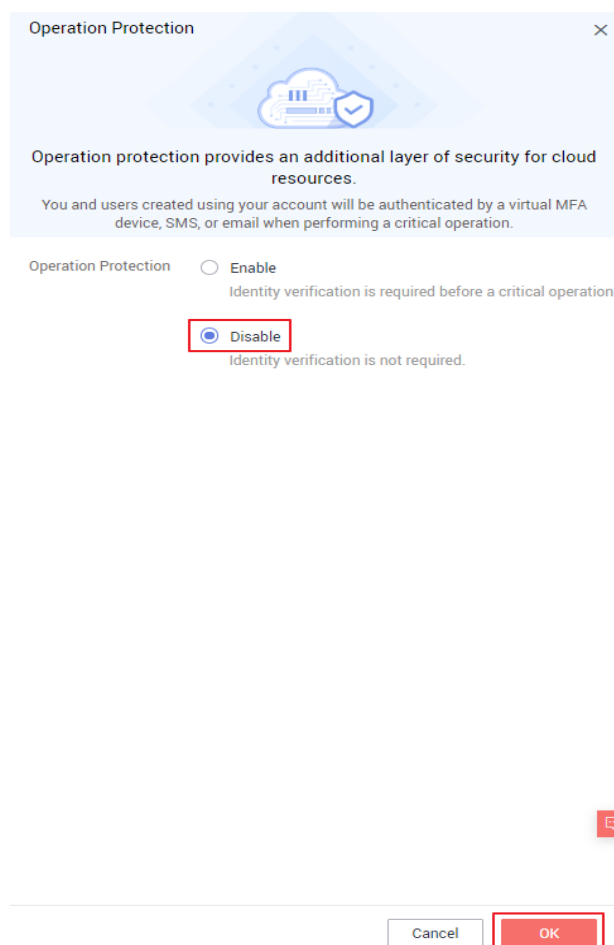
Passo 2 No console de gerenciamento, passe o ponteiro do mouse sobre o nome de usuário no canto superior direito e escolha **Security Settings** na lista suspensa.



Passo 3 Na página **Security Settings**, clique na guia **Critical Operations** e clique em **Change** ao lado de **Operation Protection**.

Passo 4 Selecione **Disable** e clique em **OK**. Digite o código de verificação e clique em **OK**.

Figura 3-6 Desativar a proteção de operação



----Fim

3.5 Como vincular um dispositivo de MFA virtual?

A autenticação multifator (MFA) adiciona uma camada extra de proteção além do seu nome de usuário e senha. Depois que a autenticação MFA for ativada, você precisará inserir códigos de verificação depois que seu nome de usuário e senha forem autenticados. A MFA, juntamente com seu nome de usuário e senha, garante a segurança de sua conta e recursos.

Os dispositivos de MFA podem ser baseados em hardware ou software. No entanto, o IAM suporta apenas dispositivos de MFA virtuais.

Um dispositivo de MFA virtual é uma aplicação que gera códigos de 6 dígitos em conformidade com o TOTP (Algoritmo de senha de uso único com base no tempo). As aplicações de MFA podem ser executadas em dispositivos móveis (incluindo smartphones) e são fáceis de usar.

Pré-requisitos

Você instalou uma aplicação de MFA (por exemplo, aplicativo de Huawei Cloud ou Google Authenticator) no seu celular.

Procedimento

- **Conta da Huawei Cloud ou usuário do IAM**

Passo 1 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.

Passo 2 Na guia **Critical Operations**, clique em **Bind** ao lado de **Virtual MFA Device**.

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

- Digitalize o código QR

Abra a aplicação de MFA em seu telefone 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 a chave secreta

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

 **NOTA**

Para garantir que você pode executar a verificação baseada em MFA com sucesso, confirme que você ativou a opção de configuração automática de tempo em seu telefone celular.

Passo 4 Visualize o código de verificação na aplicação de MFA. O código é atualizado automaticamente a cada 30 segundos.

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

----Fim

- **HUAWEI ID**

Passo 1 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.

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

Passo 3 No site da HUAWEI ID, selecione **Account & security** e vincule um dispositivo de MFA virtual na área **Security verification**.

----Fim

Perguntas frequentes relacionadas

[3.6 Como obter um código de verificação de MFA virtual?](#)

[3.7 Como desvincular ou remover um dispositivo de MFA virtual?](#)

[3.8 Por que a autenticação MFA falha?](#)

3.6 Como obter um código de verificação de MFA virtual?

Se você ativar a proteção de logon baseada em MFA virtual ou a proteção de operação, precisará fornecer códigos de verificação de MFA ao efetuar logon na plataforma de nuvem ou executar uma operação crítica. A figura a seguir mostra a página de verificação de logon.

Login Verification

Authentication Method	Login Authentication by Virtual MFA
Verification Code	<input type="text" value="6-digit code"/>

Abra a aplicação de MFA vinculada e visualize os códigos de verificação exibidos para sua conta.

NOTA

Se a verificação falhar, resolva o problema referindo-se a [3.8 Por que a autenticação MFA falha?](#)

3.7 Como desvincular ou remover um dispositivo de MFA virtual?

- Se o dispositivo de MFA virtual vinculado à sua conta estiver disponível, você poderá desvincular o dispositivo de MFA consultando [Desvinculação de um dispositivo de MFA virtual](#).
- Se o dispositivo de MFA virtual vinculado à sua conta não estiver disponível, você não poderá desvincular o dispositivo de MFA, mas poderá removê-lo consultando a [Remoção do dispositivo de MFA virtual](#).

Os usuários do IAM podem vincular outro dispositivo de MFA virtual na página **Security Settings**. Para mais detalhes, consulte [3.5 Como vincular um dispositivo de MFA virtual?](#)

Desvinculação de um dispositivo de MFA virtual

1. Faça logon no console de gerenciamento.
2. Passe o ponteiro do mouse sobre o nome de usuário no canto superior direito e selecione **Security Settings** na lista suspensa.
3. Na guia **Critical Operations**, clique em **Unbind** ao lado de **Virtual MFA Device**.

NOTA

Se você atualizou sua conta da Huawei Cloud para uma HUAWEI ID, você será redirecionado para **Account & security** do site da HUAWEI ID. Na área **Security verification**, clique em **Disassociate** na linha **Authenticator**.

4. Insira os códigos de verificação gerados pela aplicação de MFA.
5. Clique em **OK**.

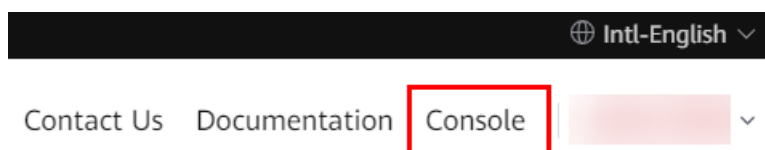
Remoção do dispositivo de MFA virtual

- Conta da Huawei Cloud ou HUAWEI ID: se o seu celular não estiver disponível ou se o dispositivo de MFA virtual vinculado tiver sido excluído do seu telefone, [envie um](#)

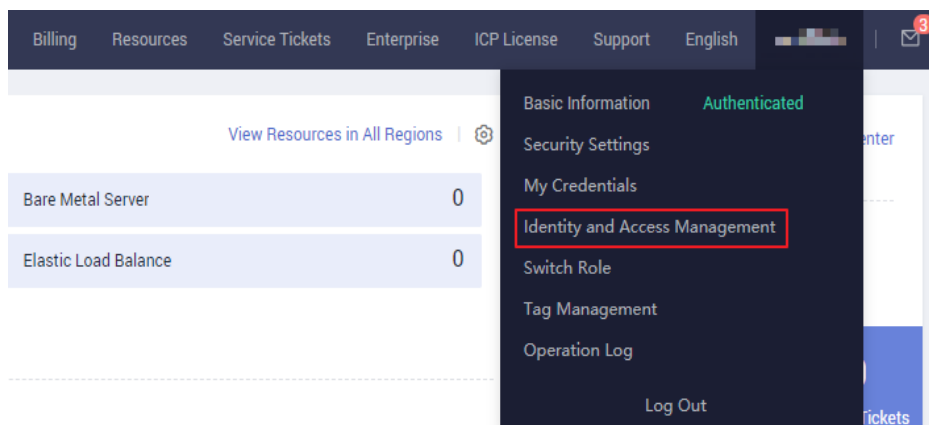
tíquete de serviço escolhendo **Identity and Access Management > Security Settings** para remover o dispositivo de MFA virtual da sua conta ou ligue para +86 4000-955-988 para entrar em contato com o atendimento ao cliente.

- Usuário do IAM: se o seu telefone celular não estiver disponível ou se o dispositivo de MFA virtual vinculado tiver sido excluído do seu telefone, solicite ao **administrador** para remover o dispositivo de MFA virtual. O procedimento de remoção de um dispositivo de MFA virtual é o seguinte:
 1. Faça login no console de gerenciamento.

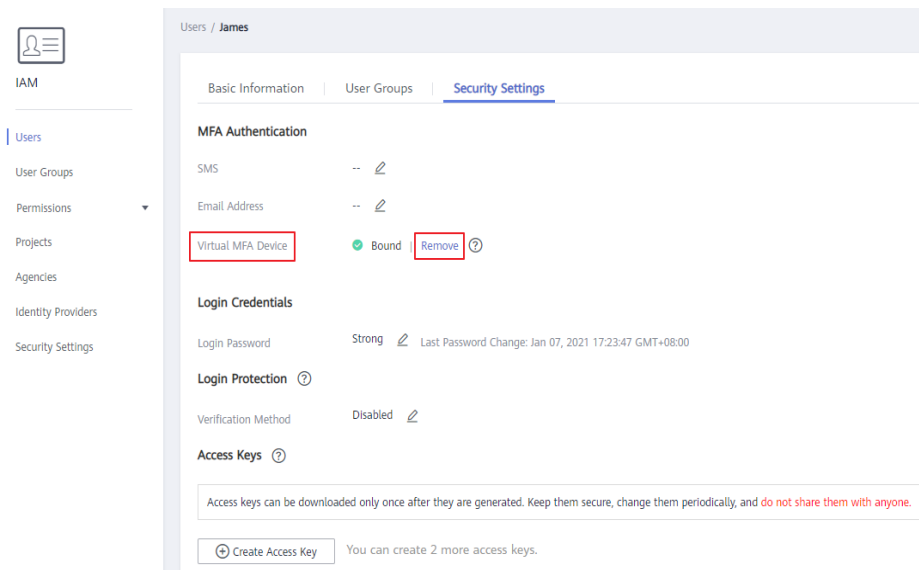
Figura 3-7 Fazer login no console de gerenciamento



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.



3. Faça login no console do IAM.
4. Na página **Users**, clique em **Security Settings** à direita do usuário de destino.
5. Na página da guia **Security Settings**, clique em **Remove** ao lado de **Virtual MFA Device**.



6. Clique em **Yes**.

3.8 Por que a autenticação MFA falha?

Sintoma

A autenticação MFA falha quando você faz logon ou executa uma operação crítica, ou vincula ou desvincula um dispositivo de MFA virtual.

Possíveis causas

- Os códigos de verificação estão incorretos.
- Os códigos de verificação expiraram.
- Os códigos de verificação pertencem a outra conta.
- Quando você vinculou um dispositivo de MFA virtual novamente após desvincular o anterior, não adicionou sua conta ao dispositivo de MFA.
- A geração de códigos de verificação de MFA está sujeita ao tempo. Se a diferença de tempo entre o seu telefone celular e o dispositivo de MFA virtual for superior a 30 segundos, os códigos de verificação de MFA gerados no seu telefone celular falharão na verificação.

Soluções

- Insira os códigos de verificação corretos.
- Os códigos de verificação são atualizados automaticamente a cada 30 segundos. Digite dois códigos de verificação consecutivos.
- Verifique se o nome da conta exibido acima do código de verificação no autenticador é o mesmo que o nome da conta usada para solicitar autenticação MFA.
- Para vincular um dispositivo de MFA virtual novamente, exclua as informações de sua conta no dispositivo de MFA e, em seguida, adicione sua conta a ele.
- Certifique-se de que a hora no seu celular seja a mesma do dispositivo de MFA virtual e tente novamente. (Você não precisa considerar o fuso horário em seu telefone celular, porque a autenticação MFA será baseada no horário UTC.)

3.9 Por que não estou recebendo o código de verificação?

Quando você vincula ou altera o número de celular ou o endereço de e-mail ou redefine a senha, é necessário obter um código de verificação para autenticação. Se você não conseguir obter o código, execute as operações descritas nesta seção.

Por que não estou recebendo o código de verificação de SMS?

- Verifique se o número de celular que você digitou está correto. Se estiver incorreto, insira o número de celular correto e tente novamente.
- Verifique se o seu serviço móvel foi suspenso devido a atrasos. Se tiver sido suspenso, limpe o valor pendente e tente novamente após retomar o serviço móvel. Você também pode alterar o número de celular associado à sua conta.
- Verifique se o SMS que contém o código de verificação foi filtrado ou bloqueado como uma mensagem de lixo eletrônico. Se isso acontecer, desative a função de filtragem ou bloqueio de mensagens SMS.

NOTA

Verifique se há mensagens contendo um código de verificação enviado pela HUAWEI CLOUD em mensagens de lixo eletrônico ou spam.

- Em alguns cenários, as mensagens SMS podem não ser entregues devido a problemas de rede. Nesse caso, envie um código de verificação novamente ou tente novamente mais tarde. Como alternativa, instale o cartão SIM em outro telefone e tente novamente.

Se a falha persistir após a execução das operações anteriores, tente a verificação de e-mail ou MFA virtual.

Se o seu telefone celular e endereço de e-mail não podem receber o código de verificação, entre em contato com o atendimento ao cliente.

Por que não estou recebendo o código de verificação de e-mail?

- Verifique se o endereço de e-mail que você inseriu está correto. Se estiver incorreto, insira o endereço de e-mail correto e tente novamente.
- Verifique se a sua caixa de correio é normal e verifique a pasta de lixo eletrônico.
- Adicione os seguintes endereços de e-mail à lista branca:
noreplyhk01@mail01.huawei.com e **noreplydl01@mail01.huawei.com**.
- Os e-mails podem não ser entregues devido a problemas de rede. Nesse caso, envie um código de verificação novamente ou tente novamente mais tarde.

Se a falha persistir depois de executar as operações anteriores, tente a verificação de SMS ou MFA virtual.

Se o seu telefone celular e endereço de e-mail não podem receber o código de verificação, entre em contato com o atendimento ao cliente.

3.10 Por que minha conta está bloqueada?

Sintoma

- Quando você faz logon no sistema, uma mensagem é exibida, indicando que sua conta está bloqueada e pode ser usada para fazer logon novamente após 15 minutos.
- Quando você chama uma API (como a API usada para [obter um token de usuário](#)) cujos parâmetros de solicitação incluem uma senha, a seguinte resposta é exibida:

```
{
  "error": {
    "code": 401,
    "message": "The account is locked.",
    "title": "Unauthorized"
  }
}
```

Possíveis causas

Sua conta está bloqueada por 15 minutos devido a exceções de segurança, por exemplo, você digitou senhas incorretas várias vezes ou a conta foi usada com frequência para logon de diferentes locais.

Soluções

- Se a sua conta estiver bloqueada devido a operações incorretas, aguarde 15 minutos e tente novamente. Não faça logon ou digite a senha dentro desse período.
- Se você esqueceu sua senha de logon, redefina-a. Para mais detalhes, consulte [4.1 O que devo fazer se eu esqueci minha senha?](#)
- Se a conta estiver bloqueada sem motivo, altere a senha. Para mais detalhes, consulte [4.2 Como alterar minha senha?](#)

3.11 Por que minha política de controle de acesso à API não entra em vigor?

Sintoma

Você definiu uma política de controle de acesso à API, mas os usuários do IAM que não atendem aos requisitos da política ainda podem acessar a Huawei Cloud usando APIs.

Soluções

1. A política de controle de acesso à API ainda não entrou em vigor.
As políticas de controle de acesso à API entram em vigor dentro de **2 horas** após serem definidas.
2. O controle de acesso à API não é compatível com sua região atual.
Atualmente, o controle de acesso à API não é suportado em **CN North-Beijing4**. Você pode mudar para outra região.

NOTA

A API para obter um token de usuário do IAM (usando uma senha) não é afetada pela política de controle de acesso à API.

3. O controle de acesso à API não entra em vigor para o OBS.

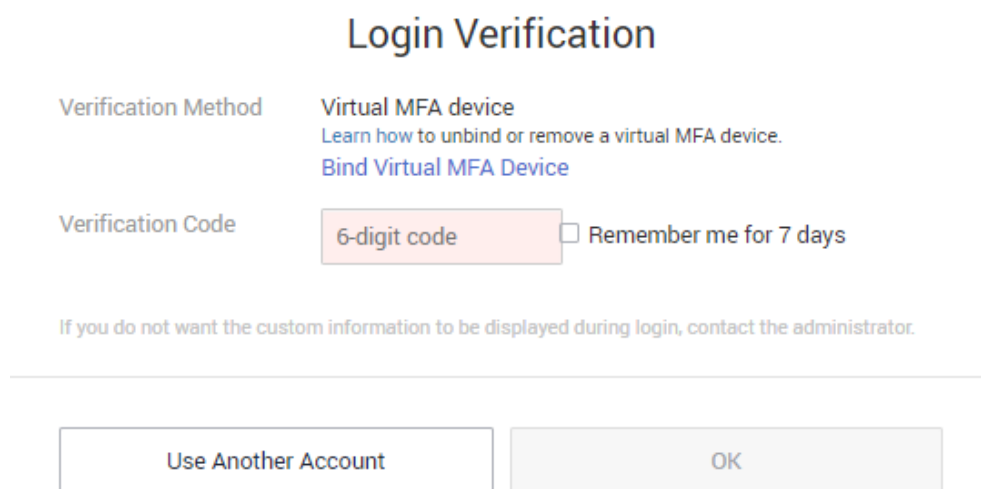
O OBS não oferece suporte a políticas de controle de acesso à API. Para restringir o acesso aos recursos do OBS, consulte [Restringir o acesso ao bucket a endereços IP especificados](#).

Se nenhum dos cenários anteriores se aplicar, modifique sua política de controle de acesso à API. Se a política ainda não entrar em vigor, [envie um tíquete de serviço](#) escolhendo **Identity and Access Management > Account Security Settings** e especificando "Controle de acesso à API" ou entre em contato conosco pelo telefone +86 4000-955-988.

3.12 Por que ainda preciso executar a MFA durante o logon após desvincular o dispositivo de MFA virtual?

Sintoma

Você desvinculou ou removeu o dispositivo de MFA virtual, mas ainda precisa verificar sua identidade por meio de MFA ao fazer logon na Huawei Cloud.



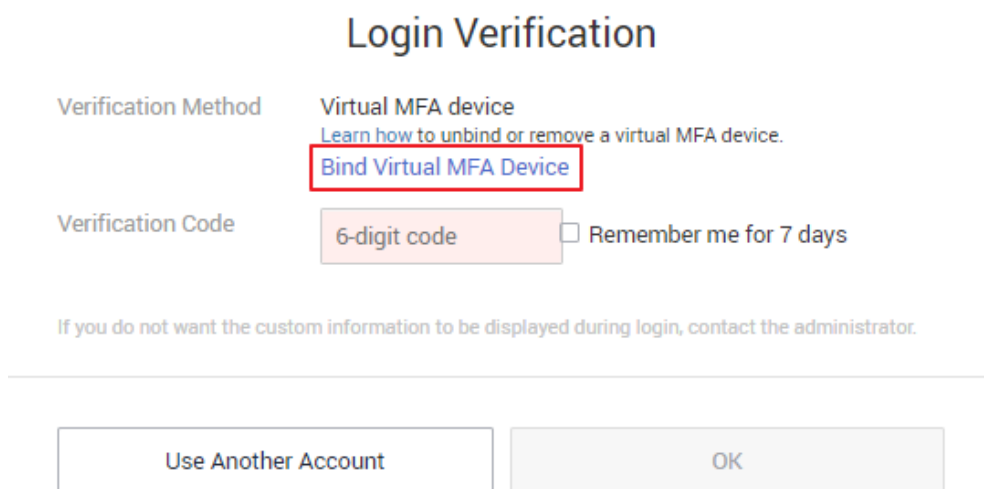
Possíveis causas

Embora o dispositivo de MFA virtual tenha sido desvinculado ou removido, a proteção de logon ainda está ativada. A verificação de logon ainda é necessária.

Soluções

- Ao efetuar logon na Huawei Cloud, vincule um dispositivo de MFA virtual novamente e use-o para verificar sua identidade.

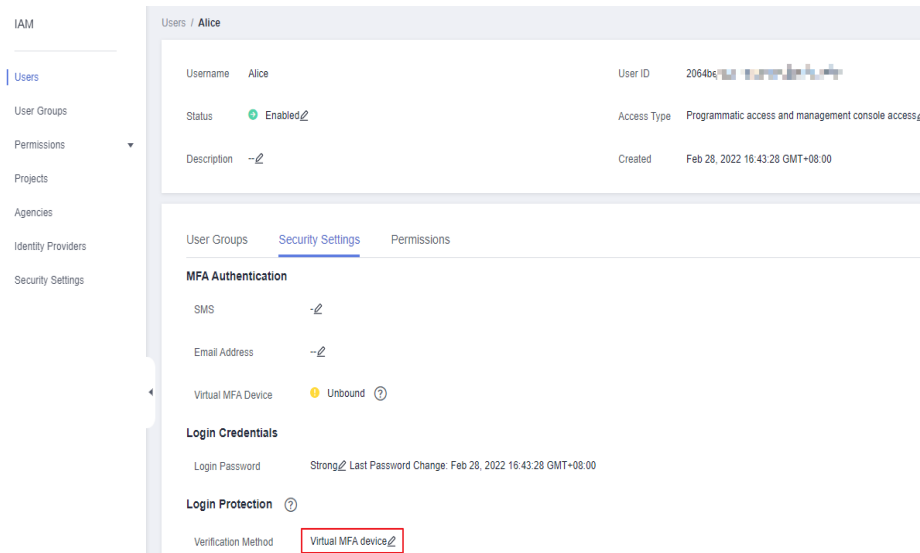
Clique em **Bind Virtual MFA Device** na caixa de diálogo **Login Verification**. Para mais detalhes, consulte [3.5 Como vincular um dispositivo de MFA virtual?](#).



- Se você for um usuário do IAM, solicite ao administrador que altere o modo de verificação de login para número de celular ou endereço de e-mail e, em seguida, efetue login novamente.

Se você for um administrador, faça login no console do IAM, clique no nome de usuário para acessar a página de detalhes do usuário e altere o modo de verificação de login na página de guia **Security Settings**.

Figura 3-8 Autenticação MFA virtual



4 Senhas e credenciais

- [4.1 O que devo fazer se eu esqueci minha senha?](#)
- [4.2 Como alterar minha senha?](#)
- [4.3 Como obter uma chave de acesso \(AK/SK\)?](#)
- [4.4 O que devo fazer se eu esqueci minha chave de acesso \(AK/SK\)?](#)
- [4.5 O que são credenciais de segurança temporárias \(AK/SK e token de segurança\)?](#)
- [4.6 Como obter um token com permissões de Security Administrator?](#)
- [4.7 Como obter uma chave de acesso \(AK/SK\) na região EU-Dublin?](#)

4.1 O que devo fazer se eu esqueci minha senha?

Se você é um usuário do IAM e esqueceu sua senha, redefina a senha referindo-se a [Redefinição da senha de um usuário do IAM](#).

Se você esqueceu a senha da sua conta, redefina a senha referindo-se a [Redefinição da senha de uma conta](#).

NOTA

Esta seção descreve como recuperar a senha de um usuário do IAM, conta da Huawei Cloud ou HUAWEI ID.

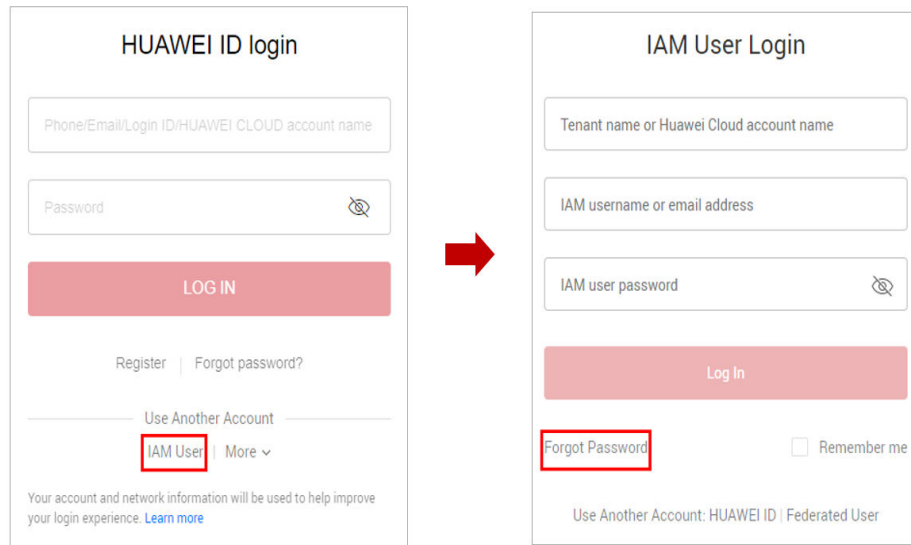
Se uma mensagem de erro for exibida indicando que a conta é inválida ou não suportada durante a recuperação de senha, isso significa que a conta não é um usuário do IAM, conta da Huawei Cloud ou HUAWEI ID. Verifique se o nome da conta inserido está correto. Se você não tiver uma HUAWEI ID, crie uma e use-a para habilitar os serviços da Huawei Cloud. Para obter detalhes, consulte [Registro de uma HUAWEI ID e ativação dos serviços da Huawei Cloud](#).

Redefinição da senha de um usuário do IAM

Se você for um usuário do IAM e não tiver vinculado um endereço de e-mail ou número de celular, não poderá alterar a senha por conta própria. Você precisa entrar em contato com o administrador para [redefinir sua senha](#).

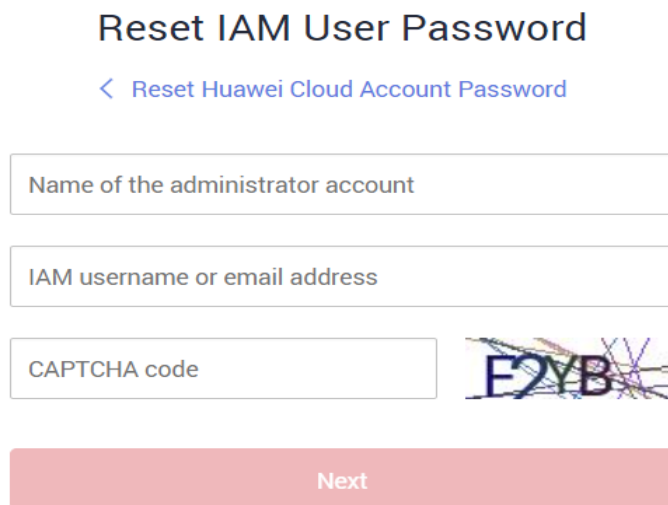
Passo 1 Na página de logon da HUAWEI ID, clique em **IAM User**. Na página de logon exibida, clique em **Forgot Password**.

Figura 4-1 Página de logon do usuário do IAM



Passo 2 Digite a conta de administrador, o nome de usuário ou o endereço de e-mail do IAM e o código de verificação.

Figura 4-2 Redefinição da senha do usuário do IAM



NOTA

- Conta: criada após o registro bem-sucedido na Huawei Cloud. A conta tem permissões de acesso total para todos os seus serviços e recursos de nuvem e faz pagamentos pelo uso desses recursos. Após o logon da conta, você verá a conta marcada como **Enterprise administrator** na página **Users**.
- Usuário do IAM: criado usando sua conta. Os usuários do IAM podem fazer logon na Huawei Cloud usando o nome da 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.
- Se você é um usuário do IAM e não vinculou um endereço de e-mail ou número de celular à sua conta, peça ao administrador para redefinir sua senha. Para obter detalhes, consulte [Alteração da senha de logon de um usuário do IAM](#).

Passo 3 Selecione um método de verificação, insira o código de verificação e clique em **Next**.

NOTA

- Verifique se o número de celular ou endereço de e-mail que você digitou está correto, ou a senha não pode ser redefinida.
- Se você não receber o código de verificação, consulte [3.9 Por que não estou recebendo o código de verificação?](#)

Passo 4 Digite uma nova senha, confirme-a e clique em **OK**.

Passo 5 Clique em **Log In** ou aguarde para ser redirecionado para a página de logon e use a nova senha para fazer logon.

----Fim

Redefinição da senha de uma conta

Passo 1 Na página de logon, clique em **Forgot password**.

Figura 4-3 Redefinição da senha da HUAWEI ID

The image shows the HUAWEI ID login interface. At the top, it says 'HUAWEI ID login'. Below this are two input fields: the first is labeled 'Phone/Email/Login ID/HUAWEI CLOUD account name' and the second is labeled 'Password' with a toggle icon for visibility. A large red 'LOG IN' button is positioned below the input fields. Underneath the button are two links: 'Register' and 'Forgot password?'. The 'Forgot password?' link is highlighted with a red rectangular box. Below these links is a horizontal line with the text 'Use Another Account' in the center. Underneath that line are the links 'IAM User' and 'More' with a dropdown arrow. At the bottom of the page, there is a small text block: 'Your account and network information will be used to help improve your login experience. [Learn more](#)'.

Passo 2 Insira seu ID de logon, o número de celular ou o endereço de e-mail usado para criar sua HUAWEI ID e clique em **NEXT**.

Figura 4-4 Redefinição da senha

Reset password

Enter your HUAWEI ID

Phone/Email/Login ID/HUAWEI CLOUD account name

NEXT

To increase the chances of success, reset your password on a device you frequently use.

Passo 3 Obtenha o código de verificação na etapa **Passo 2**.

Passo 4 Digite o código de verificação e clique em **NEXT**.

 **NOTA**

- Se você não receber o código de verificação, consulte **3.9 Por que não estou recebendo o código de verificação?**
- Para contas da Huawei Cloud, se o número de celular não estiver disponível, entre em contato com o atendimento ao cliente pelo telefone +86 4000-955988 (China continental) ou +85 2800-931122 (Hong Kong, China) ou **envie um ticket de serviço**.
- Para HUAWEI IDs, se o número de celular ou endereço de e-mail não estiver disponível, **altere primeiro o número de celular ou endereço de e-mail vinculado à sua HUAWEI ID** e, em seguida, use o novo número de celular ou endereço de e-mail para redefinir a senha.

Passo 5 (Opcional) Redefina a senha de uma HUAWEI ID usando um dos seguintes métodos:

- Registre uma HUAWEI ID no site oficial do Petal Mail gratuitamente. Após a conclusão do registro, o número de telefone será usado como seu número de telefone de segurança.

 **CUIDADO**

A conta recém-registrada não pode usar os recursos da conta de HUAWEI ID original.

- Redefina a senha da conta de HUAWEI ID original.
 - a. Se a senha for redefinida em um dispositivo usado com pouca frequência, a verificação será necessária. Selecione um método de verificação apropriado e clique em **NEXT**.
 - b. Preencha as seguintes informações para verificação:
 - Informações sobre o nome real do número de telefone

- Informações de segurança
 - Informações básicas
 - Informações históricas
 - Informações do dispositivo

Em seguida, envie as informações para verificação. Se a senha ainda não puder ser redefinida, [altere sua conta](#). Os resultados serão enviados a você por SMS. Se o recurso for aprovado, [redefine a senha](#) em até 24 horas.

Passo 6 Digite uma nova senha, confirme-a e clique em **OK**.

Passo 7 (Opcional) Redefina a senha de uma HUAWEI ID adicionando MFA à conta da HUAWEI ID. Para obter detalhes, consulte [Autenticação MFA e dispositivo de MFA virtual](#).

Passo 8 Clique em **RETURN NOW** e use a nova senha para [fazer logon na Huawei Cloud](#).

----Fim

4.2 Como alterar minha senha?

- Se você se lembrar da sua senha e quiser alterá-la, faça o seguinte:
 - **Conta da Huawei Cloud:** altere a senha na página **Basic Information** de Minha conta.
 - **HUAWEI ID:** altere a senha na Central de contas da HUAWEI. Para fazer isso, vá para a página **Basic Information** de Minha conta e clique em **Manage** ao lado de **HUAWEI ID Information**. Você é automaticamente redirecionado para a página **Account & security** da Central de contas da HUAWEI. Redefina a senha na área **Security center**.
 - **Usuário do IAM:** passe o ponteiro do mouse sobre o nome de usuário no canto superior direito do console e escolha **Security Settings**. Em seguida, altere a senha na guia **Basic Information**.
- Se você esqueceu sua senha:
 - Redefina sua senha seguindo as instruções em [4.1 O que devo fazer se eu esqueci minha senha?](#)
 - Se você for um usuário do IAM e não tiver vinculado nenhum endereço de e-mail ou número de celular à sua conta, [solicite ao administrador que redefina sua senha](#).

4.3 Como obter uma chave de acesso (AK/SK)?

- Se você tiver uma senha para fazer logon no console de gerenciamento, faça logon no console, mova o ponteiro para o nome de usuário no canto superior direito e selecione **My Credentials** na lista suspensa. Escolha **Access Keys** no painel de navegação esquerdo e você pode exibir o ID da chave de acesso (AK) na lista de chaves de acesso. Você pode obter a chave de acesso secreta (SK) do arquivo .csv baixado. Para obter mais informações, consulte [Chaves de acesso](#).
- Se você não usar uma senha para fazer logon no console de gerenciamento, solicite ao administrador que crie uma chave de acesso para você no console do IAM. Para obter mais informações, consulte [Gerenciamento de chaves de acesso para um usuário do IAM](#).

4.4 O que devo fazer se eu esqueci minha chave de acesso (AK/SK)?

Se você esqueceu sua chave de acesso original, crie uma nova chave de acesso e use-a para substituir a chave de acesso original em uso. Certifique-se de que os serviços não são afetados e, em seguida, exclua ou desabilite a chave de acesso original. Para obter detalhes, consulte [Chaves de acesso](#).

NOTA

- Cada usuário do IAM pode criar no máximo duas chaves de acesso. A cota não pode ser aumentada.
- Se você for um usuário do IAM, mova o ponteiro para o nome da conta no canto superior direito do console de gerenciamento, escolha **Security Settings**, clique na guia **Critical Operations** e verifique o status de ativação do recurso **Access Key Management**.
 - Desativado: todos os usuários do IAM sob a conta podem gerenciar (criar, ativar, desativar e excluir) suas próprias chaves de acesso.
 - Ativado: somente os usuários do IAM que receberam as permissões necessárias podem gerenciar chaves de acesso.
- Se você não conseguir gerenciar suas chaves de acesso:
 - Solicite que o **administrador** gerencie suas chaves de acesso. Para obter detalhes, consulte [Gerenciamento de chaves de acesso para um usuário do IAM](#).
 - Solicite que o **administrador** atribua as permissões necessárias a você ou desative o gerenciamento de chaves de acesso. Para obter detalhes, consulte [Atribuição de permissões a um usuário do IAM](#) ou [Gerenciamento de chaves de acesso](#).

4.5 O que são credenciais de segurança temporárias (AK/SK e token de segurança)?

Credenciais de segurança temporárias

As credenciais de segurança temporárias incluem chaves de acesso temporárias (AK/SK) e tokens de segurança. Elas têm apenas **permissões de acesso temporárias** e são ligeiramente diferentes das credenciais de segurança permanentes.

Diferenças entre credenciais de segurança temporárias e permanentes

A tabela a seguir fornece as diferenças entre os dois tipos de credenciais de segurança.

Tabela 4-1 Diferenças de credenciais

Item	Credenciais temporárias	Credenciais permanentes
Período de validade	15 minutos a 24 horas	Validade ilimitada
Número de credenciais	Ilimitado	2 credenciais para cada usuário do IAM

Item	Credenciais temporárias	Credenciais permanentes
Método de obtenção	Chame a API usada para obter uma chave de acesso temporária .	Crie uma chave de acesso na página Minhas credenciais .
Uso	Não podem ser incorporadas a aplicações ou armazenadas para uso posterior e devem ser obtidas novamente após a expiração.	N/A

Vantagens das credenciais de segurança temporárias

Credenciais de segurança temporárias são úteis para conceder aos usuários federados apenas permissões necessárias com um período de validade específico.

Uso de credenciais de segurança temporárias

Uma chave de acesso deve ser usada junto com um token de segurança. Quando você usa credenciais de segurança temporárias para autenticação, adicione o campo **x-security-token** ao cabeçalho da solicitação. Para obter detalhes, consulte [Guia de assinatura de solicitação de API](#).

4.6 Como obter um token com permissões de Security Administrator?

Um token é uma credencial de acesso emitida para um usuário do IAM para suportar sua identidade e permissões. Ao chamar as APIs do IAM ou de outros serviços de nuvem, você pode usar essa API para obter um token de usuário para autenticação.

As permissões de um token são determinadas pelas permissões do usuário que obtém o token. Somente os usuários que receberam a função de **Security Administrator** podem obter um token com permissões de **Security Administrator**.

Métodos

- Administrador da conta: crie um usuário do IAM, atribua a função de **Security Administrator** ao usuário e chame a API usada para **obter um token de usuário**. O token obtido tem as permissões de **Security Administrator**.
- Usuário do IAM: solicite ao administrador que atribua a você a função de **Security Administrator** e, em seguida, obtenha um token.

Permissões de Security Administrator

Tabela 4-2 Permissões de Security administrator

Nome de permissão	Escopo	Descrição
Security Administrator	Global	Permissões de administrador para o IAM, incluindo, entre outras, as seguintes permissões: <ul style="list-style-type: none">● Criar, modificar e excluir usuários do IAM● Criar, modificar e excluir grupos de usuários e conceder-lhes permissões● Criar, modificar e excluir políticas personalizadas● Criar e modificar projetos● Criar, modificar e excluir agências● Criar, modificar e excluir provedores de identidade● Configurar as configurações de segurança da conta

4.7 Como obter uma chave de acesso (AK/SK) na região EU-Dublin?

Sintoma


O administrador ativou a região **EU-Dublin**. A conta e os usuários do IAM precisam usar chaves de acesso para criptografia e assinatura na região selecionada.

Os usuários acessam os serviços de nuvem na região **EU-Dublin** como usuários virtuais autorizados por meio de autenticação federada. Eles não são usuários reais que existem no sistema de serviço de nuvem e precisam obter uma chave de acesso nas regiões padrão da Huawei Cloud e na região **EU-Dublin**, respectivamente.

O procedimento abaixo o orienta na criação de uma chave de acesso permanente para você como administrador ou para os usuários do IAM. Você e seus usuários do IAM podem criar chaves de acesso temporárias na página **My Credentials**.

Procedimento

Passo 1 Crie um usuário do IAM na região **EU-Dublin** como um administrador. Para criar uma chave de acesso para si mesmo, vá para **Passo 2**.

1. Faça logon na Huawei Cloud como um administrador, clique em  na página inicial do console e selecione a região **EU-Dublin**.
2. No console, na região selecionada, escolha **Management & Governance > Identity and Access Management**.
3. No painel de navegação do console do IAM, escolha **Users**.
4. Clique em **Create User** no canto superior direito.

5. Na página **Create User**, defina as informações do usuário. Para obter detalhes, consulte [Criação de um usuário do IAM](#).
Para identificar a entidade que usa uma chave de acesso, crie um usuário do IAM com o mesmo nome que o usuário do IAM correspondente ou sua conta.
6. Clique em **OK**.

Passo 2 Obtenha uma chave de acesso para o usuário do IAM.

1. Faça login no console do IAM como administrador e selecione a região **EU-Dublin**.
2. Na página **Users** do console do IAM, clique em **Security Settings** na coluna **Operation** da linha que contém o usuário do IAM criado em [1](#).
3. Na guia **Security Settings** da página de detalhes do usuário do IAM, clique em **Create Access Key**.
4. (Opcional) Insira uma descrição para a chave de acesso.
5. Clique em **OK**. A chave de acesso é criada.
6. Baixe o arquivo da chave de acesso.

 **NOTA**

- Cada usuário pode ter no máximo duas chaves de acesso com validade ilimitada. Para garantir a segurança da conta, mantenha-as adequadamente.
 - O administrador e os usuários do IAM podem usar a chave de acesso somente na região **EU-Dublin**.
7. (Opcional) Forneça a chave de acesso ao usuário do IAM.

----Fim

5 Gerenciamento de projetos

[5.1 Quais são as diferenças entre IAM e Enterprise Management?](#)

[5.2 Quais são as diferenças entre projetos do IAM e projetos empresariais?](#)

[5.3 Quais são as diferenças entre usuários do IAM e contas de membros empresariais?](#)

5.1 Quais são as diferenças entre IAM e Enterprise Management?

O Enterprise Management permite que as empresas gerenciem os recursos da nuvem por nível de projeto e organização. Inclui projeto empresarial, contabilidade, aplicação e gerenciamento de pessoal. O IAM é um serviço de gerenciamento de identidade que fornece autenticação de identidade, gerenciamento de permissões e controle de acesso.

Você pode usar o IAM e o Enterprise Management para gerenciar usuários e permissões de acesso. O Enterprise Management também permite contabilidade e gerenciamento de aplicações e oferece suporte a autorizações mais refinadas para uso de recursos. É recomendado para empresas de médio e grande porte. Para obter mais informações sobre o Enterprise Management, consulte [Guia de usuário do Enterprise Management](#).

Diferenças entre IAM e Enterprise Management

- Método de ativação
 - O IAM é gratuito e você pode usá-lo imediatamente após se registrar na Huawei Cloud.
 - O Enterprise Management é um serviço de gerenciamento de recursos na Huawei Cloud. Depois de se registrar no sistema, você precisa solicitar a habilitação do Enterprise Management. Para obter detalhes, consulte [Ativação da Central empresarial](#).
- Isolamento de recursos
 - Usando o IAM, você pode criar vários projetos em uma região para isolar recursos e autorizar os usuários a acessar recursos em projetos específicos. Para obter detalhes, consulte [Projetos](#).
 - Usando o Enterprise Management, você pode criar projetos empresariais para isolar recursos entre regiões. O Enterprise Management facilita a atribuição de permissões

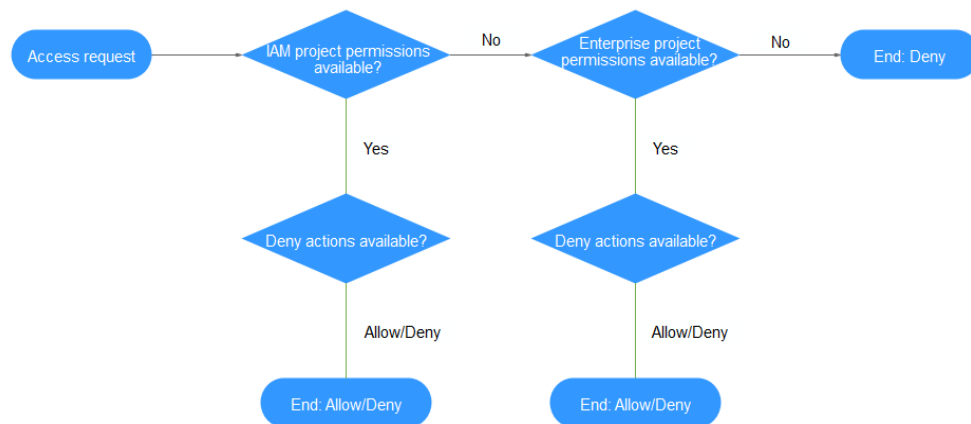
para recursos de nuvem específicos. Por exemplo, você pode adicionar um Elastic Cloud Server (ECS) a um projeto empresarial e atribuir permissões a um usuário para gerenciar o ECS no projeto. Em seguida, o usuário pode gerenciar apenas esse ECS.

- Serviços com suporte
 - Para obter detalhes sobre os serviços suportados pelo IAM, consulte [Serviços de nuvem com suporte](#).
 - Para obter detalhes sobre os serviços suportados pelo Enterprise Management, consulte [Serviços de nuvem com suporte](#).

Processo de autenticação

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

Figura 5-1 Processo de solicitação de autenticação



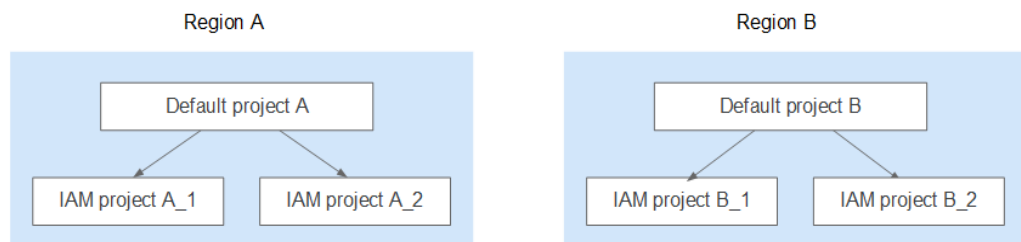
1. Um usuário inicia uma solicitação de acesso.
2. O sistema procura permissões de projeto do IAM e, em seguida, procura ações correspondentes nas permissões.
3. Se uma ação Allow ou Deny correspondente for encontrada, o sistema retornará um resultado de autenticação (Allow ou Deny). Em seguida, a autenticação é concluída.
4. Se nenhuma ação correspondente for encontrada nas permissões de projeto do IAM, o sistema continuará a procurar permissões de projeto empresarial e ações correspondentes.
5. Se uma ação Allow ou Deny correspondente for encontrada, o sistema retornará um resultado de autenticação (Allow ou Deny). Em seguida, a autenticação é concluída.
6. Se nenhuma ação correspondente for encontrada, o sistema retornará um Deny. Em seguida, a autenticação é concluída.

5.2 Quais são as diferenças entre projetos do IAM e projetos empresariais?

Projetos de IAM

Os projetos do IAM podem agrupar e isolar fisicamente recursos. Os recursos não podem ser transferidos entre projetos do IAM, mas só podem ser excluídos e, em seguida, criados ou comprados novamente.

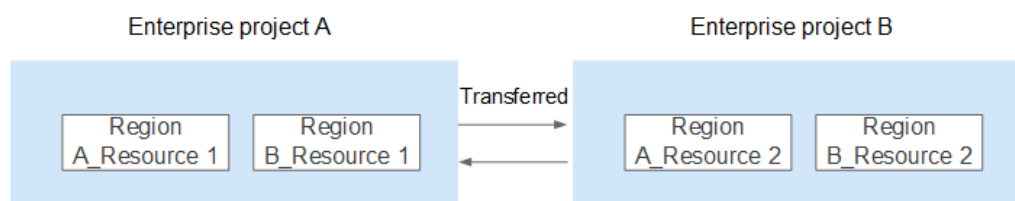
Para obter detalhes sobre projetos do IAM, consulte [Projetos](#).



Projetos empresariais

Os projetos empresariais podem agrupar e isolar logicamente os recursos. Um projeto empresarial pode conter recursos de diferentes regiões e os recursos podem ser transferidos entre projetos empresariais. O Enterprise Management facilita a atribuição de permissões para recursos de nuvem específicos. Por exemplo, você pode adicionar um Elastic Cloud Server (ECS) a um projeto empresarial e atribuir permissões a um usuário para gerenciar o ECS no projeto. Em seguida, o usuário pode gerenciar apenas esse ECS. Não é possível criar projetos no IAM depois de ativar o Enterprise Management.

Para obter detalhes sobre projetos empresariais, consulte [Criação de um projeto empresarial](#).



5.3 Quais são as diferenças entre usuários do IAM e contas de membros empresariais?

Usuários do IAM

Os usuários do IAM são criados usando uma conta no IAM ou no Enterprise Management (página [User Management](#)). Eles são gerenciados e recebem permissões pela conta. **As faturas geradas pelo uso de recursos pelos usuários do IAM são pagas pela conta.**

Em uma empresa, se houver vários funcionários que precisam usar os recursos comprados da Huawei Cloud por meio de uma conta, a conta pode ser usada para criar usuários do IAM para

esses funcionários e atribuir permissões aos usuários para usar os recursos. Os usuários do IAM têm suas próprias senhas para acessar os recursos sob a conta.

Para obter detalhes sobre como criar um usuário do IAM, consulte [Criação de um usuário do IAM](#).

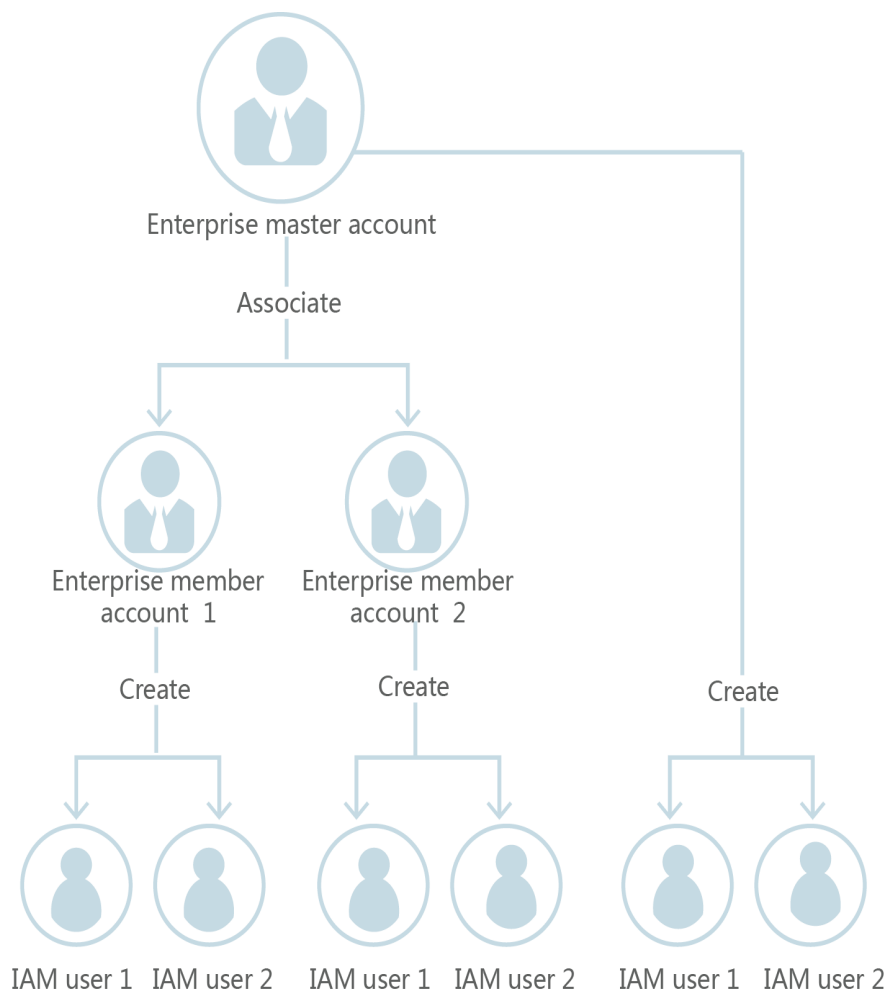
Contas de membros empresariais

As contas principais empresariais e as contas de membro são geradas após o registro bem-sucedido na Huawei Cloud. O **Accounting Management** do Enterprise Management permite que várias contas da Huawei Cloud sejam vinculadas umas às outras para fins contábeis. Você pode criar uma organização hierárquica e uma conta principal, adicionar contas de membros a essa organização e vinculá-las à conta principal.

A conta principal pode alocar fundos para contas de membro para que as contas de membro possam usar os fundos para **manage resources**.

Tanto a conta principal quanto as contas de membro podem criar usuários do IAM para controlar o acesso a recursos específicos. Uma conta só pode gerenciar seus próprios usuários do IAM, mas não pode gerenciar os usuários do IAM criados por outras contas.

Para obter detalhes sobre como criar uma conta de membro, consulte [Criação de uma conta de membro](#).



6 Gerenciamento da agência

6.1 Como obter permissões para criar uma agência?

6.1 Como obter permissões para criar uma agência?

Sintoma

Você não tem permissões para criar uma agência no console do IAM.

Possíveis causas

Você não tem permissões para usar o IAM.

Somente os seguintes usuários podem usar o IAM:

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

Soluções

- Entre em contato com o administrador para criar uma agência. Para obter detalhes, consulte [Criação de uma agência \(por uma parte delegante\)](#).
- Entre em contato com o administrador para conceder as permissões para usar o IAM. Para obter detalhes, consulte [Atribuição de permissões a um usuário do IAM](#).

7 Gerenciamento de contas

[7.1 Por que o logon da conta falha?](#)

[7.2 Quais são as relações entre uma conta da Huawei Cloud, uma HUAWEI ID, um usuário do IAM e um usuário federado?](#)

[7.3 Quais são as possíveis causas de uma falha de atualização da HUAWEI ID?](#)

[7.4 Posso fazer logon com minha conta da HUAWEI CLOUD depois de atualizá-la para uma HUAWEI ID?](#)

7.1 Por que o logon da conta falha?

Sintoma

Quando você faz logon no IAM usando uma conta, o sistema exibe uma mensagem indicando que o nome ou a senha da sua conta estão incorretos.

Possíveis causas

- O link de logon está incorreto.
- O ID de logon está incorreto.
- A senha está incorreta.

Soluções

- Use o link de logon correto e insira uma HUAWEI ID ou uma conta da Huawei Cloud. Se você já atualizou sua conta para uma HUAWEI ID, escolha **HUAWEI ID**, conforme mostrado em [Figura 7-1](#). Caso contrário, escolha **Huawei Cloud Account**, conforme mostrado em [Figura 7-2](#).
 - Para fazer logon usando uma conta do site oficial da Huawei ou como um parceiro empresarial da Huawei ou como um usuário federado, consulte [Fazer logon na Huawei Cloud](#).
 - Se você for um usuário do IAM, efetue logon escolhendo **IAM User** na página de logon. Se o logon falhar, consulte [2.1 Por que o logon de usuário do IAM falha?](#).

Figura 7-1 Fazer logon usando uma HUAWEI ID

HUAWEI ID login

Phone number/Email address/Account ID/HUAWEI ID

Password

LOG IN

Register | Forgot password

Use Another Account

IAM User | Federated User | Huawei Website Account | Huawei Enterprise Partner | HUAWEI CLOUD Account

Your account and network information will be used to help improve your login experience. [Learn more](#)

Figura 7-2 Fazer logon usando uma conta da Huawei Cloud

HUAWEI ID login

Phone number/Email address/Login ID/HUAWEI CL

Password

LOG IN

Register | Forgot password

Use Another Account

IAM User | Federated User | Huawei Website Account | Huawei Enterprise Partner | HUAWEI CLOUD Account

Your account and network information will be used to help improve your login experience. [Learn more](#)

Account Login

Account name or email

Password

Mobile Number Login Remember me

Log In

Free Registration | Forgot Password

IAM User Login

Use Another Account ^

<HDC.Cloud> Huawei Official Website
Huawei Enterprise Partner | Huawei Developer Alliance
Federated User | HUAWEI ID

- Ao fazer logon com uma HUAWEI ID, digite o **número do celular, o endereço de e-mail, o ID de logon ou o nome da conta da Huawei Cloud**. Ao fazer logon com uma conta da Huawei Cloud, insira o **nome ou endereço de e-mail da conta**.
 - Se você tiver uma HUAWEI ID, digite o número do celular ou o endereço de e-mail vinculado à HUAWEI ID ou digite o ID de logon dessa HUAWEI ID. Para obter detalhes, consulte [Fazer logon usando uma HUAWEI ID](#).
 - Se você não tiver uma HUAWEI ID, mas tiver uma conta da Huawei Cloud, que não tenha sido atualizada para uma HUAWEI ID, insira o nome da conta da Huawei Cloud.
- Se você fizer logon com uma HUAWEI ID, digite a senha da HUAWEI ID. Se você fizer logon com uma conta da Huawei Cloud, digite a senha da conta da Huawei Cloud.

7.2 Quais são as relações entre uma conta da Huawei Cloud, uma HUAWEI ID, um usuário do IAM e um usuário federado?

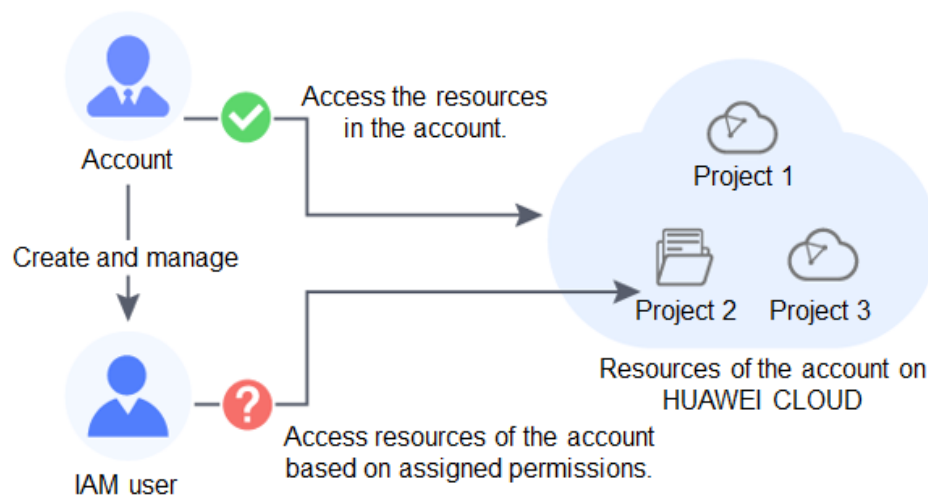
Esta seção apresenta as contas usadas na Huawei Cloud e seus relacionamentos.

Tipos de conta da Huawei Cloud

O sistema de contas da Huawei Cloud consiste em dois tipos de contas:

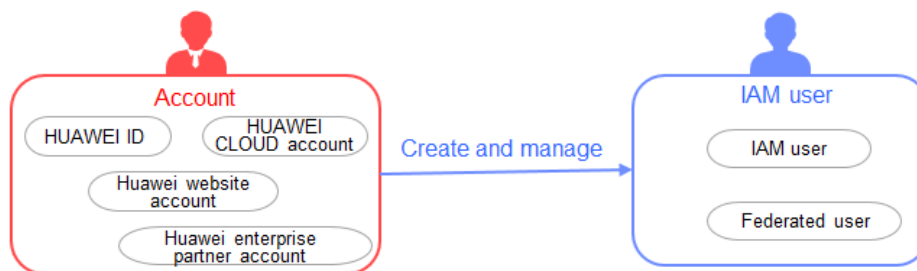
- **Contas:** registradas ou criadas na Huawei Cloud. Uma conta tem as permissões mais altas na Huawei Cloud. Ela pode acessar todos os seus recursos e paga pelo uso desses recursos. As contas incluem HUAWEI IDs e contas da Huawei Cloud.
- **Usuários do IAM:** criados e gerenciados usando uma conta no IAM. O administrador da conta concede permissões aos usuários do IAM e faz o pagamento pelos recursos que eles usam. Os usuários do IAM usam recursos conforme especificado pelas permissões.

Uma conta e seus usuários do IAM têm um relacionamento pai-filho.



Você pode fazer login na Huawei Cloud usando uma HUAWEI ID, uma conta do site da Huawei, uma conta de parceiro empresarial da Huawei ou uma conta da Huawei Cloud e usar seus recursos e serviços de nuvem.

Se você é um usuário do IAM criado por uma conta ou um usuário de um sistema de terceiros que estabeleceu uma relação de confiança com a Huawei Cloud, faça login na Huawei Cloud por meio da página correspondente e use os recursos e serviços de nuvem conforme especificado pelas permissões concedidas pela conta.



HUAWEI ID

Você pode registrar uma HUAWEI ID para acessar todos os serviços da Huawei, como a Huawei Cloud e o Vmall.

Registro: registre uma HUAWEI ID em qualquer site de serviço da Huawei, como o [site da HUAWEI ID](#).

Logon na Huawei Cloud: faça logon na Huawei Cloud clicando em **HUAWEI ID**. Se esta for a primeira vez que você faz logon na Huawei Cloud com uma HUAWEI ID, ative os serviços da Huawei Cloud ou vincule a HUAWEI ID à sua conta da Huawei Cloud seguindo as instruções na tela.

The screenshot shows the 'Log in to HUAWEI ID' interface. It features a title 'Log in to HUAWEI ID' in a red-bordered box. Below the title are two input fields: 'Phone number/Email address/Login ID/HUAWEI CL' and 'Password'. A red 'LOG IN' button is positioned below the input fields. Underneath the button are links for 'Register' and 'Forgot password'. A section titled 'Use Another Account' lists several options: 'IAM User', 'Federated User', 'Huawei Website Account', 'Huawei Enterprise Partner', and 'HUAWEI CLOUD Account'. At the bottom, there is a note: 'Your account and network information will be used to help improve your login experience. [Learn more](#)'.

Conta da Huawei Cloud

As contas da Huawei Cloud só podem ser usadas para fazer logon na Huawei Cloud.

Registro: para melhorar a experiência de logon, unificamos nosso sistema de contas. Você só pode registrar HUAWEI IDs na Huawei Cloud a partir de 30 de outubro de 2021.

Logon na Huawei Cloud: Faça logon na Huawei Cloud clicando em **HUAWEI ID** ou **Huawei Cloud Account**.

Log in to HUAWEI ID

Phone number/Email address/Account ID/HUAWEI ID

Password

LOG IN

Register | Forgot password

Use Another Account

IAM User | Federated User | Huawei Website Account | Huawei Enterprise Partner | HUAWEI CLOUD Account

Your account and network information will be used to help improve your login experience. [Learn more](#)

Usuário do IAM

Os usuários do IAM usam os recursos da Huawei Cloud conforme especificado pelas permissões concedidas por sua conta.

Criação: os usuários do IAM são criados por uma conta no IAM. Para obter detalhes, consulte [Criação de um usuário do IAM](#).

Logon na Huawei Cloud: faça logon na Huawei Cloud clicando em **IAM User**.

Log in to HUAWEI ID

Phone number/Email address/Login ID/HUAWEI CL

Password

LOG IN

Register | Forgot password

Use Another Account

IAM User | Federated User | Huawei Website Account | Huawei Enterprise Partner | HUAWEI CLOUD Account

Your account and network information will be used to help improve your login experience. [Learn more](#)

IAM User Login

Tenant name or HUAWEI CLOUD account name

IAM user name or email address

IAM user password

Log In

[Forgot Password](#) Remember me

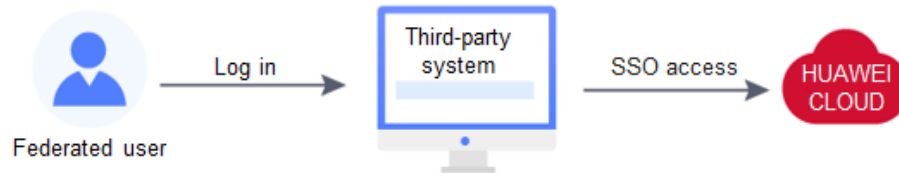
Use Another Account: HUAWEI ID | Federated User

Usuário federado (usuário virtual)

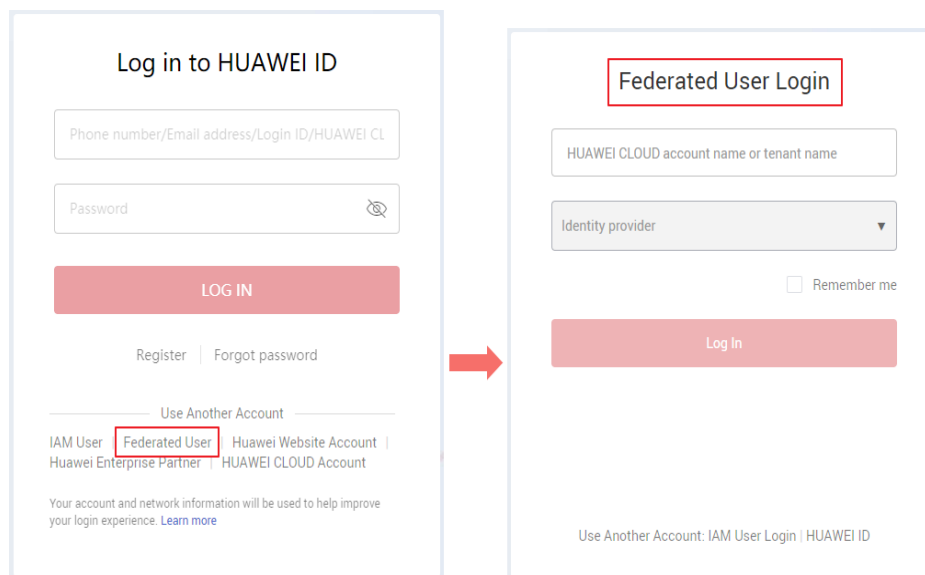
Os usuários federados são registrados em um sistema de terceiros que estabeleceu uma relação de confiança com a Huawei Cloud. Os usuários podem fazer logon na Huawei Cloud

usando contas de sistema de terceiros. Por exemplo, eles podem fazer logon em uma plataforma de jogos usando suas contas de serviço de rede social (SNS).

Criação: quando um usuário empresarial faz logon na Huawei Cloud usando uma conta de um sistema de terceiros, o IAM cria automaticamente um usuário virtual (usuário federado empresarial). O sistema de terceiros corresponde a um provedor de identidade que você criou no IAM. Para obter detalhes, consulte [Introdução ao provedor de identidade](#).



Logon na Huawei Cloud: faça logon na Huawei Cloud clicando em **Federated User**.



Outros

Se você já tiver uma [conta do site da Huawei](#) ou [conta de parceiro empresarial da Huawei](#), faça logon na Huawei Cloud com essas contas e use os recursos como um administrador da conta.

7.3 Quais são as possíveis causas de uma falha de atualização da HUAWEI ID?

Sintoma

Sua conta da Huawei Cloud não foi atualizada para uma HUAWEI ID.

Possíveis causas

1. Causa: você registrou uma conta da Huawei Cloud e uma HUAWEI ID usando o mesmo número de celular ou endereço de e-mail e não usou a HUAWEI ID para ativar os serviços da Huawei Cloud.
Solução: saia da sua conta da Huawei Cloud, faça login novamente usando sua HUAWEI ID e vincule sua HUAWEI ID à sua conta da Huawei Cloud.
2. Causa: você registrou **várias** contas da Huawei Cloud e **uma** HUAWEI ID e usou a HUAWEI ID para se associar ou ativar os serviços da Huawei Cloud. Nesse caso, você não pode atualizar suas contas da Huawei Cloud para a HUAWEI ID.
Solução: faça login usando sua conta da Huawei Cloud e ignore o aviso de atualização.
3. Causa: você registrou uma conta da Huawei Cloud e uma HUAWEI ID em diferentes países ou regiões usando o mesmo número de celular ou endereço de e-mail. Nesse caso, você não pode vincular a conta ao ID.
Solução: faça login usando sua conta da Huawei Cloud e ignore o aviso de atualização.
4. Causa: a sua HUAWEI ID está congelada.
Solução: acesse [o site da HUAWEI ID > Central de segurança > Descongelar conta](#) para descongelar sua conta e tente novamente.
5. Causa: seu número de celular já foi usado para registrar uma HUAWEI ID.
Solução: registre uma nova HUAWEI ID no [site da HUAWEI ID](#) e vincule sua conta da Huawei Cloud à HUAWEI ID.

7.4 Posso fazer login com minha conta da HUAWEI CLOUD depois de atualizá-la para uma HUAWEI ID?

- **Se você já registrou uma HUAWEI ID:**
Faça login usando o número de celular, endereço de e-mail ou nome da conta, mas apenas se forem os mesmos. Por exemplo, se os endereços de e-mail da sua conta da Huawei Cloud e da HUAWEI ID forem diferentes, você poderá fazer login com o número de celular da conta da Huawei Cloud, mas não com o endereço de e-mail.
- **Se você nunca registrou uma HUAWEI ID:**
Faça login usando o mesmo número de celular, endereço de e-mail ou nome de conta.

8 Outros

[8.1 Como obter um token de usuário usando o Postman?](#)

[8.2 Por que a ajuda em nível de campo é sempre exibida?](#)

[8.3 Como desativar o preenchimento automático de senha no Google Chrome?](#)

[8.4 Região e AZ](#)

[8.5 Como solicitar as permissões para acessar recursos em uma região da aliança de nuvem usando minha conta da Huawei Cloud ou HUAWEI ID?](#)

8.1 Como obter um token de usuário usando o Postman?

Postman é uma ferramenta de edição visual para criar e testar solicitações de API. Ele fornece uma interface de usuário fácil de usar para enviar solicitações HTTP, incluindo solicitações GET, PUT, POST e DELETE. Postman permite que você modifique parâmetros de solicitações HTTP e retorna resposta às suas solicitações.

Um token é uma credencial de acesso do usuário, que inclui identidades e permissões do usuário. Quando você chama uma API para acessar recursos de nuvem, um token é necessário para autenticação de identidade.

Execute o procedimento descrito nesta seção para obter um token de usuário usando o Postman. Para obter detalhes sobre os parâmetros, consulte [Obtenção de um token de usuário](#).

 **NOTA**

● **Período de validade de um token**

O período de validade de um token é de **24 horas**. Armazene seu token em cache para evitar chamadas frequentes de API. Certifique-se de que o token seja válido enquanto você o estiver usando. Usar um token que expirará em breve pode causar falhas de chamada de API.

A obtenção de um novo token não afeta a validade do token existente. No entanto, as seguintes operações invalidarão o token existente:

- Exclusão ou desativação do usuário do IAM
- Alteração da senha ou da chave de acesso do usuário do IAM
- As permissões do usuário do IAM são alteradas (devido a pagamentos pendentes, aprovação de aplicação de OBT ou modificação de permissão).

● **Obtenção de um token**

- Se a sua conta da Huawei Cloud tiver sido atualizada para uma HUAWEI ID, você não poderá obter um token usando a HUAWEI ID. No entanto, você pode criar um usuário do IAM, conceder as permissões necessárias ao usuário e obter um token como usuário.
- Se você for usuário de um sistema de terceiros, não poderá obter um token usando o nome de usuário e a senha que usa para autenticação de identidade federada. Vá para a página de logon da Huawei Cloud, clique em **Forgot password**, clique em **Reset Huawei Cloud account password** e defina uma senha.

Pré-requisitos

Você instalou e se registrou no Postman.

 **NOTA**

- É aconselhável instalar uma versão do Postman que suporte um cabeçalho maior que 32 KB. Caso contrário, poderá ser relatado um erro de estouro de cabeçalho.

Procedimento

Passo 1 Edite o URL da solicitação, o cabeçalho e o corpo da API usada para obter um token para chamar APIs.

● **URL de solicitação**

O URL da solicitação está no formato "**https://IAM region and endpoint/API URI**".

- a. Obtenha a região e o ponto de extremidade do IAM em [Regiões e pontos de extremidade](#).

Figura 8-1 Regiões e pontos de extremidade do IAM

Region Name	Region	Endpoint	Protocol Type
AF-Johannesburg	af-south-1	iam.af-south-1.myhuaweicloud.com	HTTPS
ALL	ALL	iam.myhuaweicloud.com	HTTPS
AP-Bangkok	ap-southeast-2	iam.ap-southeast-2.myhuaweicloud.com	HTTPS
AP-Hong Kong	ap-southeast-1	iam.ap-southeast-1.myhuaweicloud.com	HTTPS
AP-Singapore	ap-southeast-3	iam.ap-southeast-3.myhuaweicloud.com	HTTPS

- b. Obtenha o URI da API em [Obtenção de um token de usuário](#).

Por exemplo, o URL de solicitação na região **ap-southeast-1** é **https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens**.

- c. Selecione um método de solicitação da API e insira o URL da solicitação no Postman.

- **Cabeçalho da solicitação**

Defina **key** como **Content-Type** e **value** como **application/json;charset=utf8**.

- **Corpo da solicitação**

Modifique os parâmetros no corpo da solicitação de exemplo.

```
{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "domain": {
            "name": "Account name"
          },
          "name": "IAM user name",
          "password": "IAM user password"
        }
      }
    },
    "scope": {
      "domain": {
        "name": "Account name"
      }
    }
  }
}
```

 **NOTA**

Para obter detalhes sobre como obter o nome da conta e o nome de usuário do IAM, consulte [Obtenção de informações de conta, usuário do IAM e projeto](#).

Passo 2 Clique em **Send** para enviar a solicitação da API.

Passo 3 Visualize o token no cabeçalho da resposta. Você pode usar esse token para autenticação ao chamar outras APIs do IAM.

 **NOTA**

- Se o erro **401** for retornado, a autenticação falhou. Certifique-se de que os parâmetros no corpo da solicitação estão corretos e envie a solicitação novamente.
- Se o erro **400** for retornado, o formato do corpo está incorreto. Verifique se o formato do corpo está em conformidade com a sintaxe JSON. Para obter detalhes, consulte [Códigos de status](#).
- Se a mensagem "Header Overflow" for exibida, resolva o problema consultando [Por que estou vendo uma mensagem indicando estouro de cabeçalho quando tento usar o Postman para obter um token?](#)

----Fim

Por que estou vendo uma mensagem indicando estouro de cabeçalho quando tento usar o Postman para obter um token?

O Postman da V7.25.0, V7.26.0 ou de uma versão posterior não pode ser usado para obter um token de usuário devido a configurações. A mensagem "Header Overflow" será exibida se você usar qualquer uma dessas versões.

- **Solução 1**

Use uma versão anterior do Postman, como V 5.xx.

- **Solução 2**

Use curl para obter um token e substituir o texto em negrito por valores reais:

```
curl -ik -X POST -H 'Content-Type=application/json;charset=utf8' -d '{"auth": {"identity": {"methods": [{"password": {"user": {"domain": {"name": "Account name"}, "name": "IAM username", "password": "IAM user password"}]}}, "scope": {"domain": {"name": "Account name"}}}}' https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
```

- **Solução 3**

Passa uma variável de ambiente adicional **NODE_OPTIONS=--max-http-header-size=16384 (16 KB)** ao Postman para especificar o tamanho máximo do cabeçalho HTTP (em bytes).

Execute um dos seguintes comandos, dependendo do seu sistema operacional:

- macOS

```
NODE_OPTIONS=--max-http-header-size=16384 /Applications/Postman.app/Contents/MacOS/Postman
```

- Linux

```
NODE_OPTIONS=--max-http-header-size=16384 /path/to/Postman/Postman
```

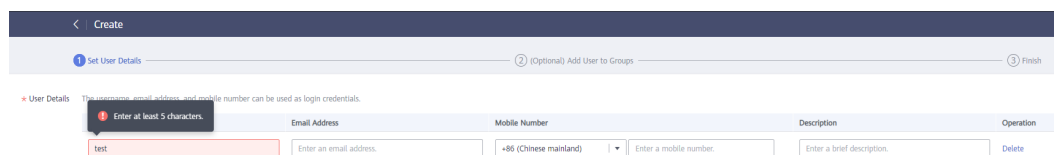
- Windows

```
set NODE_OPTIONS=--max-http-header-size=16384  
C:\users\\AppData\local\Postman\Postman.exe
```

8.2 Por que a ajuda em nível de campo é sempre exibida?

Ao se registrar ou fazer logon na Huawei Cloud, vincular uma conta da Huawei Cloud, criar um usuário ou redefinir ou alterar a senha, a ajuda em nível de campo, como "Enter at least 5 characters." é sempre exibida porque você pode estar usando o Internet Explorer 8 ou uma versão anterior. Nesse caso, corrija o problema usando os seguintes métodos.

Figura 8-2 A ajuda no nível do campo é sempre exibida



- Atualizar o navegador.

Atualize para o Internet Explorer 9 ou uma versão posterior.

- Usar outro navegador.

Use o Mozilla Firefox (versão 38.0 ou posterior) ou o Google Chrome (versão 43.0 ou posterior).

8.3 Como desativar o preenchimento automático de senha no Google Chrome?

Quando você usar o Google Chrome para fazer logon na Huawei Cloud pela primeira vez, será exibida uma mensagem solicitando que você confirme se deseja salvar a senha. Isso

ocorre porque **Offer to save passwords** e **Auto Sign-in** na área **Passwords** da página **Settings** do Google Chrome são selecionados por padrão após a instalação do navegador Google Chrome. Se você confirmar para salvar a senha, a senha será preenchida automaticamente durante o seu próximo logon. Para garantir a segurança de sua conta e senha, execute as seguintes operações para desativar essa função. Esta seção usa o Google Chrome 61.0.3163.100 como um exemplo para descrever como desativar essa função.

Procedimento


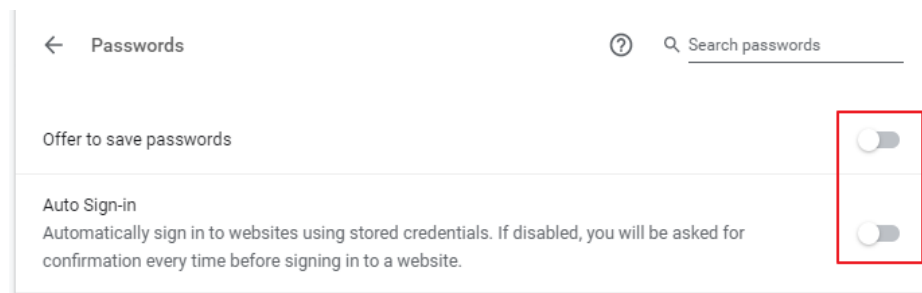

- Passo 1** Abra o navegador Google Chrome, clique em  no canto superior direito do navegador e escolha **Settings**.
- Passo 2** Na área **Autofill**, clique em **Passwords**.
- Passo 3** Desmarque **Offer to save passwords** e **Auto Sign-in**.

Figura 8-3 Desmarcar Offer to save passwords e Auto Sign-in



----Fim

Procedimento de acompanhamento

Para excluir uma senha salva, na área **Saved Passwords**, clique em  ao lado da senha e clique em **Remove**. A senha será excluída.

8.4 Região e AZ

Conceito

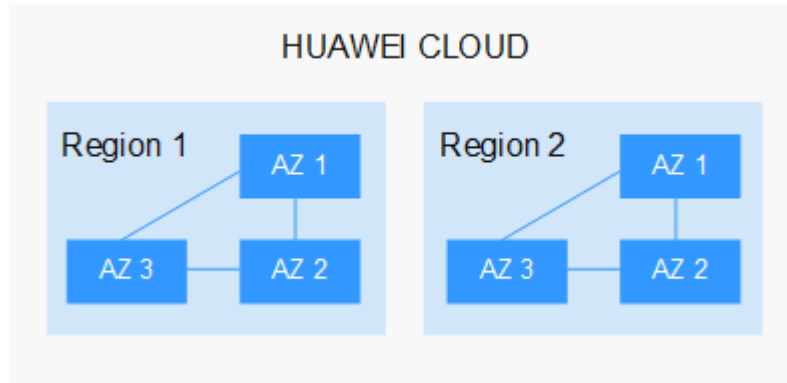
Uma região e uma zona de disponibilidade (AZ) identificam a localização de um centro de dados. Você pode criar recursos em uma região e AZ específicas.

- As regiões são divididas com base na localização geográfica e na latência da rede. Serviços públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) e Image Management Service (IMS), são compartilhados na mesma região. As regiões são classificadas em regiões universais e regiões dedicadas. Uma região universal fornece serviços de nuvem universal para locatários comuns. Uma região dedicada fornece serviços específicos para locatários específicos.
- Uma AZ contém um ou mais centros de data físicos. Cada AZ possui resfriamento, sistema de extinção de incêndio, proteção contra umidade e instalações elétricas

independentes. Dentro de uma AZ, computação, rede, armazenamento e outros recursos são logicamente divididos em vários clusters. As AZs dentro de uma região são interconectadas usando fibras ópticas de alta velocidade, para suportar sistemas de alta disponibilidade entre AZs.

Figura 8-4 mostra a relação entre regiões e AZs.

Figura 8-4 Regiões e as AZs



HUAWEI CLOUD fornece serviços em muitas regiões do mundo. Selecione uma região e uma AZ com base nos requisitos. Para obter mais informações, consulte [Regiões globais do Huawei Cloud](#).

Selecionar uma região

Ao selecionar uma região, considere os seguintes fatores:

- **Localização**
É recomendável selecionar a região mais próxima para menor latência de rede e acesso rápido. As regiões dentro do continente chinês fornecem a mesma infraestrutura, qualidade de rede BGP, bem como operações e configurações de recursos. Portanto, se seus usuários-alvo estiverem no continente chinês, você não precisará considerar as diferenças de latência da rede ao selecionar uma região.
 - Se seus usuários-alvo estiverem na Ásia-Pacífico (excluindo o continente chinês), selecione a região **CN-Hong Kong**, **AP-Bangkok**, ou **AP-Singapore**.
 - Se seus usuários-alvo estão na África, selecione a região **AF-Johannesburg**.
 - Se seus usuários de destino estiverem na América Latina, selecione a região **LA-Santiago**.

NOTA

A região **LA-Santiago** está localizada no Chile.

- **Preço do recurso**
Os preços dos recursos podem variar em diferentes regiões. Para obter detalhes.

Selecionar uma AZ

Ao implantar recursos, considere os requisitos de recuperação de desastres (DR) e latência de rede de seus aplicativos.

- Para alta capacidade de DR, implante recursos nas diferentes AZs dentro da mesma região.
- Para menor latência de rede, implante recursos na mesma AZ.


Regiões e endpoints

Antes de usar uma API para chamar recursos, especifique sua região e endpoint. Para obter mais detalhes, consulte Regions and Endpoints.

8.5 Como solicitar as permissões para acessar recursos em uma região da aliança de nuvem usando minha conta da Huawei Cloud ou HUAWEI ID?

Você pode enviar um tíquete de serviço para solicitar as permissões necessárias para acessar recursos em regiões como **EU-Dublin**.

Procedimento

- Passo 1** [Envie um tíquete de serviço](#) e especifique a região da aliança de nuvem que você deseja acessar.
- Passo 2** Aguarde uma notificação por e-mail de aprovação. Após receber o e-mail, [faça logon no console de gerenciamento](#) e clique em  no canto superior esquerdo para selecionar a região que deseja acessar.

----Fim