Identity and Access Management

Melhores práticas

Edição	01
Data	2024-08-30

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Marcas registadas e permissões

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

Aviso

Os produtos, os serviços e as funcionalidades adquiridos são estipulados pelo contrato estabelecido entre a Huawei Cloud e o cliente. Os produtos, os serviços e as funcionalidades descritos neste documento, no todo ou em parte, podem 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 ESTÃO" sem garantias ou representações de qualquer tipo, sejam expressas ou implícitas.

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 Cloud Computing Technologies Co., Ltd.

Endereço: Huawei Cloud Data Center, Rua Jiaoxinggong
Avenida Qianzhong
Novo Distrito de Gui'an
Guizhou 550029
República Popular da China

Site: https://www.huaweicloud.com/intl/pt-br/

Índice

1 Recomendações para usar o IAM

Para estabelecer acesso seguro aos seus recursos da Huawei Cloud, siga estas recomendações para o serviço Identity and Access Management (IAM).

Não crie chaves de acesso para sua conta

Sua conta tem todas as permissões necessárias para acessar recursos e fazer pagamentos pelo uso de recursos. A senha e as chaves de acesso (AKs/SKs) são credenciais de identidade para sua conta. A senha é necessária para efetuar logon no console, e as chaves de acesso são suas credenciais de identidade secundárias que permitem solicitações programáticas com ferramentas de desenvolvimento. As chaves de acesso são complementares à senha e não são obrigatórias. As chaves de acesso podem ser perdidas ou divulgadas acidentalmente. Para melhorar a segurança da conta, não crie chaves de acesso para sua conta.

Não grave chaves de acesso no código

Se você usar APIs, CLI ou SDKs para acessar serviços em nuvem, não grave suas chaves de acesso no código.

Criar usuários individuais do IAM

Se alguém precisar acessar recursos em sua conta, não compartilhe sua senha com essa pessoa. Em vez disso, crie um usuário individual do IAM para eles e conceda as permissões necessárias ao usuário do IAM. Você também pode criar um usuário do IAM para si mesmo, conceder permissões de administrador ao usuário do IAM e realizar o gerenciamento de rotina usando o usuário do IAM.

Definir tipo de acesso adequado

Você pode definir o tipo de acesso dos usuários do IAM, incluindo acesso programático e acesso ao console de gerenciamento. Observe o seguinte quando você definir o tipo de acesso:

- Se o usuário acessar os serviços da Huawei Cloud somente usando o console de gerenciamento, selecione **Management console access** para **Access Type** e **Password** para **Credential Type**.
- Se o usuário acessar os serviços da Huawei Cloud somente por meio de chamadas programáticas, selecione **Programmatic access** para **Access Type** e **Access key** para **Credential Type**.

- Se o usuário precisar usar uma senha como credencial para acesso programático a determinadas APIs, selecione **Programmatic access** para **Access Type** e **Password** para **Credential Type**.
- Se o usuário precisar executar a verificação da chave de acesso ao usar determinados serviços no console, como criar um trabalho de migração de dados no console do Cloud Data Migration (CDM), selecione **Programmatic access** e **Management console access** para **Access Type** e **Access key** e **Password** para **Credential Type**.

Conceder privilégio mínimo

É uma medida de segurança padrão para conceder aos usuários apenas as permissões necessárias para executar tarefas específicas. Você pode conseguir isso usando as políticas personalizadas ou definidas pelo sistema do IAM. O princípio do privilégio mínimo (PoLP) ajuda você a estabelecer acesso seguro aos seus recursos da Huawei Cloud.

Para usuários do IAM que acessam serviços em nuvem usando APIs, CLI ou SDKs, conceda permissões aos usuários usando políticas personalizadas para evitar perdas devido à divulgação ou perda acidental da chave de acesso.

Ativar MFA virtual

A autenticação multifator (MFA) adiciona uma camada adicional de proteção de segurança às credenciais de identidade de uma conta. É recomendável que você ative a autenticação MFA para sua conta e usuários privilegiados criados usando sua conta. Para efetuar logon no console de gerenciamento, os usuários devem inserir seus nomes de usuário e senhas e um código de verificação gerado pelo dispositivo de MFA virtual vinculado.

Um dispositivo de MFA pode ser baseado em hardware ou software. Atualmente, a Huawei Cloud suporta dispositivos de MFA virtuais baseados em software. É um programa que é executado em um dispositivo portátil (como um celular) e gera um código de verificação de seis dígitos para autenticação de identidade.

Definir uma política de senha forte

Para garantir que os usuários do IAM usem somente senhas complexas e as alterem periodicamente, defina uma política de senhas para definir requisitos de senhas fortes, como o comprimento mínimo de senha, se devem ser permitidos caracteres idênticos consecutivos em uma senha e se devem ser permitidas senhas usadas anteriormente.

Ativar proteção contra operação crítica

Ative a proteção de operações críticas para evitar operações incorretas. Quando você ou usuários criados usando sua conta executam uma operação crítica, como excluir um recurso ou gerar uma chave de acesso, você e os usuários precisam fornecer a senha e um código de verificação para prosseguir com a operação.

Alterar periodicamente suas credenciais de identidade

A alteração periódica de sua senha e chaves de acesso pode evitar riscos causados por sua divulgação ou perda acidental.

- Defina um período de validade de senha para exigir que você e os usuários criados usando sua conta alterem senhas. O IAM começará a exibir um prompt 15 dias antes de a senha expirar.

- Você pode criar duas chaves de acesso e usá-las de forma intercambiável. Por exemplo, você pode usar a chave de acesso 1 para um determinado período e, em seguida, usar a chave de acesso 2 para o próximo período. Você também pode excluir a chave de acesso 1 e gerar outra chave de acesso.

Excluir credenciais de identidade desnecessárias

Para os usuários que só precisam usar o console, é recomendável não criar chaves de acesso para eles e excluir as chaves de acesso que já foram criadas. Se um usuário não tiver efetuado logon por um longo período, altere a senha do usuário e exclua as chaves de acesso do usuário. Além disso, defina um período de validade da conta para desativar automaticamente as contas de usuário que não são usadas há muito tempo.

Delegar acesso a recursos para aplicações executadas em ECSs

As aplicações executadas em Elastic Cloud Servers (ECSs) podem acessar outros serviços da Huawei Cloud somente com uma credencial fornecida. Para fornecer credenciais de forma segura às aplicações, crie uma agência no IAM para conceder as permissões necessárias ao ECS em que as aplicações são executadas e configure a agência para o ECS para que as aplicações possam obter chaves de acesso temporárias. O ECS solicita uma credencial temporária do IAM para acessar com segurança os recursos com base nas permissões concedidas pela agência. O ECS rotaciona automaticamente as credenciais temporárias para garantir que elas sejam seguras e válidas.

Ao iniciar um ECS, você pode especificar uma agência para o ECS como um parâmetro de inicialização. As aplicações executadas no ECS podem acessar os recursos da Huawei Cloud fornecendo a chave de acesso temporária obtida usando a agência. A agência determina quais aplicações podem acessar recursos específicos.

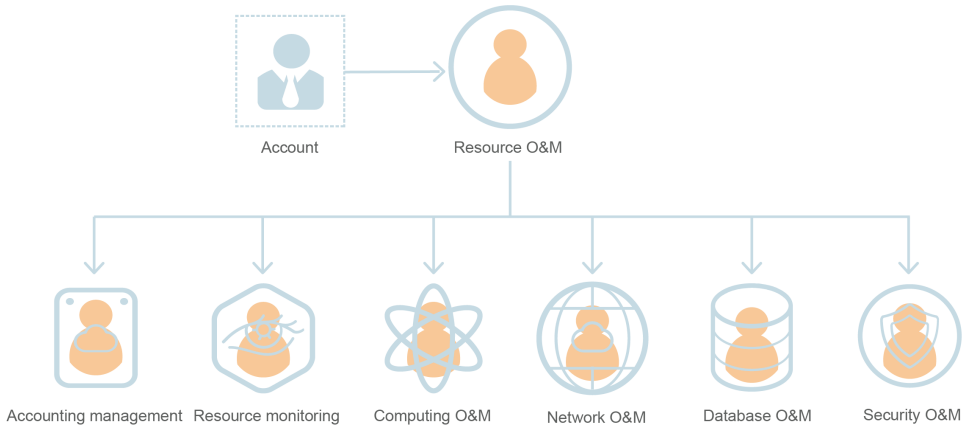
Ativação de CTS

Cloud Trace Service (CTS) é um serviço de auditoria de logs fornecido pela Huawei Cloud. Ele coleta, armazena e consulta registros de operações no IAM, facilitando a análise de segurança, a auditoria de conformidade, o rastreamento de recursos e a localização de falhas. É recomendável ativar o serviço CTS para registrar as principais operações do IAM, como criar e excluir usuários do IAM.

2 Atribuição de permissões ao pessoal de O&M

Suponha que uma empresa tenha comprado recursos diferentes na Huawei Cloud e tenha várias equipes funcionais que precisam usar um ou mais tipos de recursos. A empresa pode usar o IAM para atribuir permissões a diferentes funcionários com base em suas funções de trabalho para controle de permissões refinado.

Figura 2-1 Modelo de gerenciamento de permissões



- Equipe de O&M de recursos
- Equipe de gerenciamento contábil
- Equipe de monitoramento de recursos
- Equipe de O&M de computação
- Equipe de O&M de rede
- Equipe de O&M de banco de dados
- Equipe de O&M de segurança

Atribua as permissões necessárias a diferentes equipes funcionais da empresa de acordo com **Tabela 2-1**. Para obter detalhes sobre as permissões de todos os serviços da Huawei Cloud, consulte **Permissões definidas pelo sistema**.

Tabela 2-1 Permissões definidas pelo sistema

Equipe funcional	Política	Descrição das permissões
Equipe de O&M de recursos	Tenant Administrator	Permissões totais para todos os serviços em nuvem, incluindo a Central de cobrança, a Central de recursos e a Minha conta. A função **Tenant Administrator** inclui as permissões para compra de recursos, gerenciamento de renovações e exibição de faturas. Não inclui as permissões para o serviço IAM.
Equipe de gerenciamento contábil	BSS Administrator	Permissões completas para Central de cobrança, Central de recursos e Minha conta. A função **BSS Administrator** inclui as permissões para gerenciar faturas, pedidos, contratos e renovações e exibir faturas. **Os usuários aos quais foi atribuída apenas esta função não podem comprar recursos, a menos que você conceda a eles as permissões de administrador do serviço correspondente.**
Equipe de monitoramento de recursos	Tenant Guest	Permissões somente leitura para todos os serviços de nuvem, exceto o IAM.
Equipe de O&M de computação	ECS FullAccess	Permissões completas para o Elastic Cloud Server (ECS), incluindo permissões para a compra de recursos do ECS. Os usuários aos quais foi atribuída apenas a política **ECS FullAccess** não podem visualizar o uso dos recursos do ECS e de outros recursos, a menos que você atribua a eles a função **BSS Administrator**.

Equipe funcional	Política	Descrição das permissões
	CCE FullAccess	Permissões completas para o Cloud Container Engine (CCE), incluindo permissões para comprar recursos do CCE. Os usuários aos quais foi atribuída apenas a política **CCE FullAccess** não podem visualizar o uso dos recursos do CCE e de outros recursos, a menos que você atribua a eles a função **BSS Administrator**.
	AutoScaling FullAccess	Permissões completas para Auto Scaling (AS), incluindo a compra de recursos do AS. Os usuários aos quais foi atribuída apenas a política **AutoScaling FullAccess** não podem visualizar o uso de recursos do AS e outros recursos, a menos que você atribua a eles a função **BSS Administrator**.
Equipe de O&M de rede	VPC FullAccess	Permissões completas para Virtual Private Cloud (VPC), incluindo a compra de recursos da VPC. Os usuários aos quais foi atribuída apenas a política **VPC FullAccess** não podem visualizar o uso dos recursos da VPC e de outros recursos, a menos que você atribua a eles a função **BSS Administrator**.

Equipe funcional	Política	Descrição das permissões
	ELB FullAccess	Permissões completas para o Elastic Load Balance (ELB), incluindo a compra de balanceadores de carga. Os usuários aos quais foi atribuída apenas a política **ELB FullAccess** não podem visualizar o uso dos recursos do ELB e de outros recursos, a menos que você atribua a eles a função **BSS Administrator**.
Equipe de O&M de banco de dados	RDS FullAccess	Permissões completas para o Relational Database Service (RDS), incluindo a compra de recursos do RDS. Os usuários aos quais foi atribuída apenas a política **RDS FullAccess** não podem visualizar o uso dos recursos do RDS e de outros recursos, a menos que você atribua a eles a função **BSS Administrator**.
	DDS FullAccess	Permissões completas para o Document Database Service (DDS), incluindo a compra de recursos do DDS. Os usuários aos quais foi atribuída apenas a política **DDS FullAccess** não podem exibir o uso de recursos do DDS e outros recursos, a menos que você lhes atribua a função **BSS Administrator**.
	DDM FullAccess	Permissões completas para o Distributed Database Middleware (DDM).
Equipe de O&M de segurança	Anti-DDoS Administrator	Permissões completas para Anti-DDoS.
	CAD Administrator	Permissões completas para Advanced Anti-DDoS (AAD).

Equipe funcional	Política	Descrição das permissões
	KMS Administrator	Permissões completas para o Data Encryption Workshop (DEW), incluindo a compra de recursos do DEW. Os usuários aos quais foi atribuída apenas a função **KMS Administrator** não podem exibir o uso de recursos do DEW e outros recursos, a menos que você atribua a eles a função **BSS Administrator**.

Atribuição de permissões ao pessoal de O&M

Veja a seguir um exemplo de procedimento para especificar um funcionário da empresa como proprietário de O&M da rede na região **CN-Hong Kong**. Se você quiser especificar um funcionário como qualquer outro proprietário de O&M, conceda as permissões necessárias ao funcionário de acordo com **Tabela 2-1**.

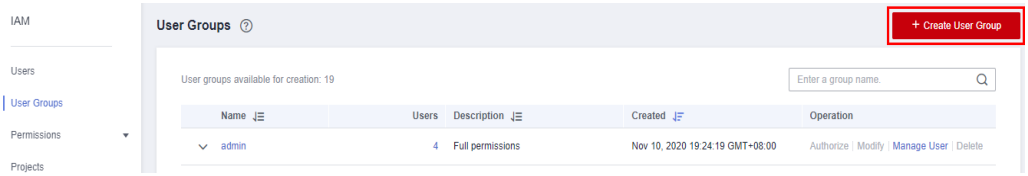
Etapa 1: criar um grupo de usuários e atribuir permissões

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

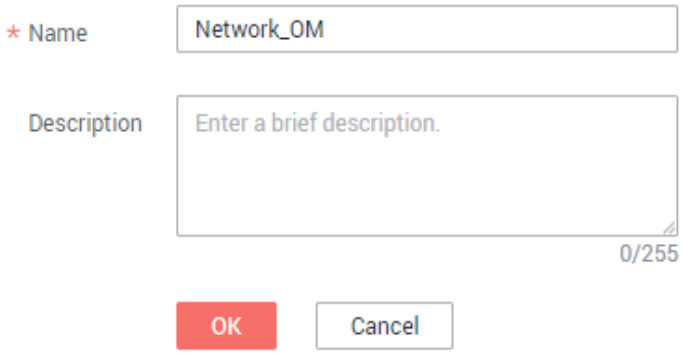
Passo 2 No console de gerenciamento, passe o ponteiro do mouse sobre o nome de usuário no canto superior direito e escolha **Identity and Access Management**.

Passo 3 No console do IAM, escolha **User Groups** no painel de navegação. Em seguida, clique em **Create User Group**.

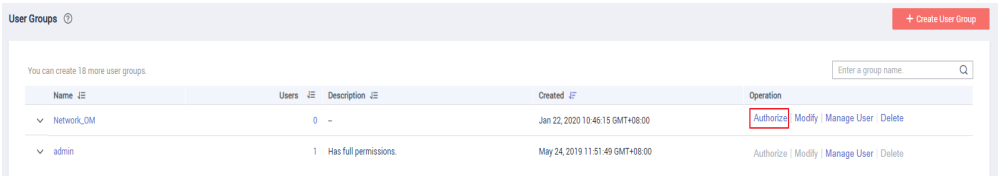
Figura 2-2 Criação de um grupo de usuários



Passo 4 Digite o nome do grupo de usuários **Network_OM** e clique em **OK**.



Passo 5 Na linha que contém o grupo de usuários, clique em **Authorize**.



Passo 6 Pesquise e selecione **VPC FullAccess** e **ELB FullAccess** e clique em **Next**.

Passo 7 Especifique o escopo da autorização como **Region-specific projects** e selecione **CN-Hong Kong**.

NOTA

- Se os usuários do grupo precisarem exibir o uso de recursos, anexe a função **BSS Administrator** ao grupo para o mesmo projeto.
- Ao especificar um funcionário como o proprietário de O&M de segurança de acordo com **Tabela 2-1**, você deve conceder ao funcionário outras permissões relacionadas porque os serviços de segurança interagem com outros serviços de nuvem. Para obter mais informações, consulte **Atribuição de funções de dependência**.

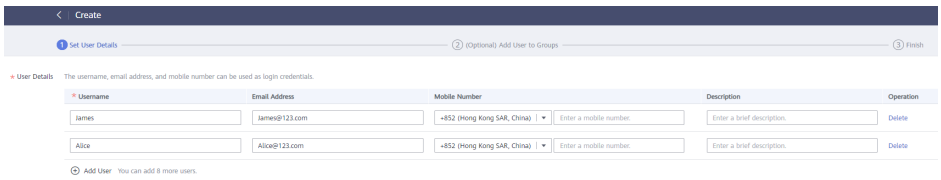
----Fim

Etapa 2: criar um usuário de IAM

Passo 1 No painel de navegação do console do IAM, escolha **Users**. Em seguida, clique em **Create User**.

Passo 2 Especifique os detalhes do usuário e o tipo de acesso. Para criar mais usuários, clique em **Add User**. Podem ser criados no máximo 10 usuários por vez.

Figura 2-3 Configuração de informações do usuário



NOTA

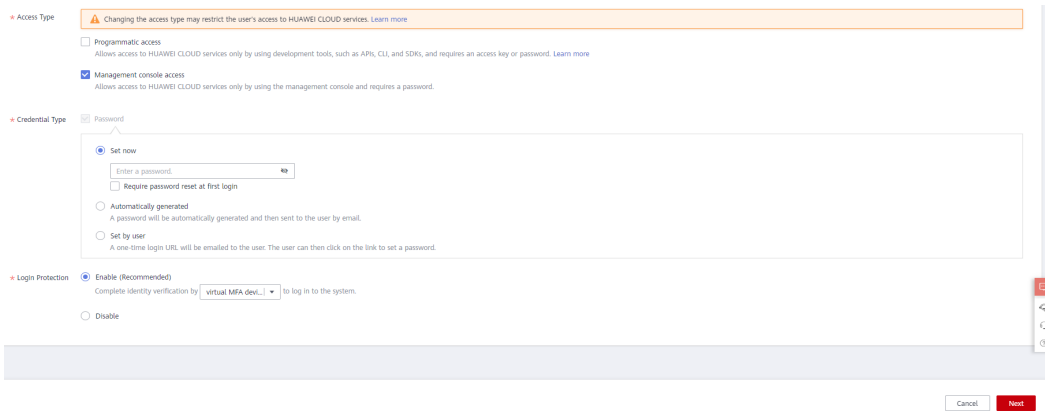
- Os usuários podem fazer logon na Huawei Cloud usando o nome de usuário, endereço de e-mail ou número de celular.
- Se os usuários esquecerem a senha, poderão redefini-la por meio da verificação de endereço de e-mail ou número de celular. Se nenhum endereço de e-mail ou número de celular tiver sido vinculado aos usuários, os usuários precisarão entrar em contato com o administrador para redefinir suas senhas.

Tabela 2-2 Informações do usuário

Parâmetro	Descrição
Username	Nome de usuário que será usado para fazer logon na Huawei Cloud, por exemplo, **James** e **Alice**. Este campo é obrigatório.

Parâmetro	Descrição
Email Address	Endereço de e-mail do usuário do IAM que pode ser usado como uma credencial de logon. Os usuários do IAM podem vincular um endereço de e-mail depois que eles são criados. Este campo é obrigatório se você tiver especificado **Set by user** como o tipo de credencial.
Mobile Number	Número de telefone celular do usuário do IAM que pode ser usado como credencial de logon. Os usuários do IAM podem vincular um número de celular depois que eles são criados. Este campo é opcional.
Description	Informações adicionais sobre o usuário do IAM. Este campo é opcional.

Figura 2-4 Configuração do tipo de acesso



- **Programmatic access**: selecione essa opção para permitir que o usuário acesse os serviços da Huawei Cloud usando ferramentas de desenvolvimento, como APIs, CLI e SDKs. Você pode gerar uma **access key** ou definir uma **password** para o usuário.
- **Management console access**: selecione esta opção para permitir que o usuário acesse os serviços da Huawei Cloud usando o console de gerenciamento. Você pode definir ou gerar uma senha para o usuário ou solicitar que o usuário defina uma senha no primeiro logon.

  NOTA

  – Se o usuário **acessar os serviços de nuvem somente usando o console de gerenciamento**, selecione **Management console access** para **Access Type** e **Password** para **Credential Type**.
  – Se o usuário **acessar os serviços em nuvem somente por meio de chamadas programáticas**, selecione **Programmatic access** para **Access Type** e **Access key** para **Credential Type**
  – Se o usuário **precisar usar uma senha como credencial para acesso programático** a determinadas APIs, selecione **Programmatic access** para **Access Type** e **Password** para **Credential Type**
  – Se o usuário precisar **executar a verificação da chave de acesso** ao usar determinados serviços no console, selecione **Programmatic access** e **Management console access** para **Access Type** e **Access key** e **Password** para **Credential Type**. Por exemplo, o usuário precisa executar a verificação da chave de acesso ao criar um trabalho de migração de dados no console do Cloud Data Migration (CDM).

Tabela 2-3 Configurar o tipo de credencial e a proteção de logon

Tipo de credencial e proteção de logon		Descrição
Access key		Depois que os usuários são criados, você pode baixar as **chaves de acesso (AK/SK)** geradas para esses usuários. **Cada usuário pode ter no máximo duas chaves de acesso.**
Password	Set now	Defina uma senha para o usuário e determine se deve exigir que o usuário redefina a senha no primeiro logon. Se você for o usuário, selecione essa opção e defina uma senha para o logon. Você não precisa selecionar **Require password reset at first login**.
	Automatically generated	O sistema gera automaticamente uma senha de logon para o usuário. Depois que o usuário for criado, baixe o arquivo de senha EXCEL e forneça a senha ao usuário. O usuário pode então usar essa senha para logon. **Essa opção está disponível somente quando você cria um único usuário.**
	Set by user	Um URL de logon único será enviado por e-mail ao usuário. O usuário pode clicar no link para fazer logon no console e definir uma senha. Se você não usar o usuário do IAM, selecione essa opção e insira o endereço de e-mail e o número de celular do usuário do IAM. O usuário pode então definir uma senha clicando no URL de logon único enviado por e-mail. O URL de logon é válido por **seven days**.
Login Protection	Enable (Recommended)	Se a proteção de logon estiver ativada, o usuário precisará digitar um código de verificação além do nome de usuário e senha durante o logon. Habilite esta função para a segurança da conta. Você pode selecionar SMS, e-mail ou dispositivo de MFA virtual para verificação durante o logon.
	Disable	Se a proteção de logon estiver desativada, você poderá ativá-la posteriormente seguindo as instruções fornecidas em **Visualização ou modificação das informações do usuário do IAM**.

Passo 3 (Opcional) Clique em **Next** para adicionar os usuários aos grupos de usuários.

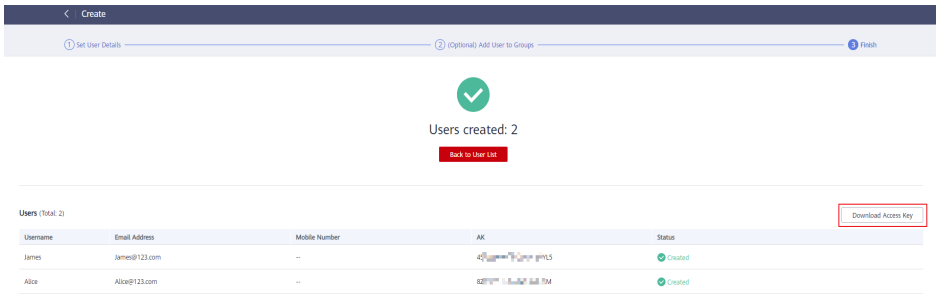
- O usuário herdará as permissões atribuídas aos grupos de usuários aos quais o usuário pertence.
- Você também pode criar novos grupos conforme necessário.

NOTA

- Se o usuário for um administrador, adicione-o ao grupo padrão **admin**.
- Cada usuário pode ser adicionado a vários grupos de usuários.

Passo 4 Clique em **Next**. Se você especificou o tipo de acesso como **Programmatic access** na **Etapa 2**, baixe a chave de acesso na página **Finish**.

Figura 2-5 Usuários criados com sucesso



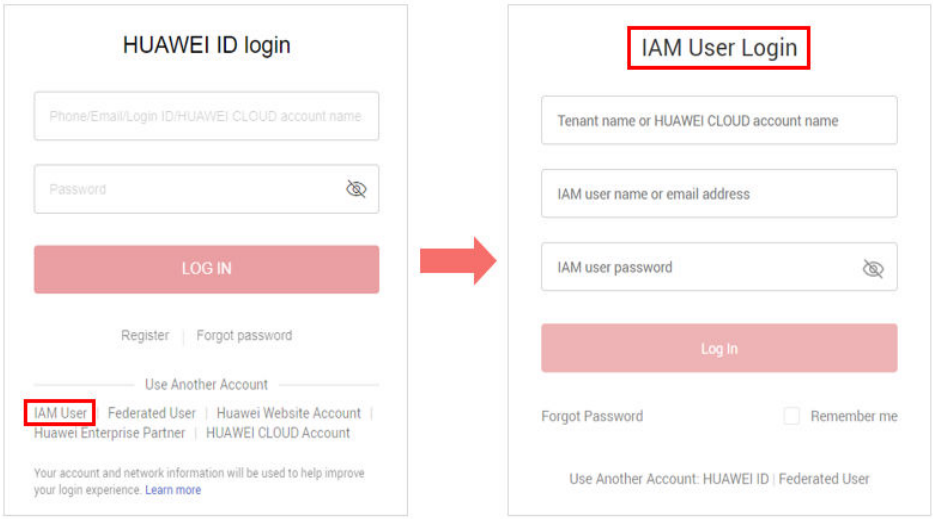
----Fim

Etapa 3: fazer logon como um usuário do IAM e verificar as permissões

Um usuário do IAM pode fazer logon usando métodos diferentes. A seguir, descreve-se como efetuar logon por meio da página de logon. Para obter mais métodos de logon, consulte **Fazer logon na Huawei Cloud**.

Passo 1 Na página de logon da Huawei Cloud, clique em **IAM User**.

Passo 2 Na página **IAM User Login**, insira o nome da conta, o nome do usuário e a senha do usuário criado.



- Nome da conta: nome da conta usada para criar o usuário do IAM
- Nome de usuário e senha: o nome de usuário e a senha especificados para o usuário do IAM

Passo 3 No console de gerenciamento, mude para a região **CN-Hong Kong**.

Passo 4 Escolha **Service List** > **Virtual Private Cloud**, **Elastic Load Balance** e **Domain Name Service** e execute operações em cada console de serviço para verificar se as permissões foram atribuídas com sucesso.

Passo 5 Escolha um serviço diferente dos serviços anteriores na **Service List** para garantir que o serviço não possa ser acessado.

Passo 6 No console de gerenciamento, alterne para uma região diferente de **CN-Hong Kong** e certifique-se de que os consoles de VPC, ELB e DNS não possam ser acessados.

----Fim

3 Atribuição de permissões definidas pelo sistema para serviços comuns de nuvem

Atribua permissões para serviços de nuvem comuns a usuários do IAM consultando os seguintes links:

- **Criação de um usuário e concessão de permissões do ECS**
- **Criação de um usuário e concessão de permissões**
- **Criação de um usuário e concessão de permissões**
- **Criação de um usuário e concessão de permissões do EVS**
- **Criação de um usuário e concessão de permissões**
- **Permissões de cluster (baseadas em IAM)**
- **Gerenciamento de acesso aos dados públicos do departamento**
- **Criação de um usuário e concessão de permissões do CBR**
- **Criação de um usuário e concessão de permissões da VPC**
- **Criação de um usuário e concessão de permissões do DCS**
- **Criação de um usuário e concessão de permissões**
- **Criação de um usuário e atribuição de permissões**

4 Delegação de acesso entre contas e gerenciamento de recursos

A empresa A e a empresa B criaram a conta A e a conta B, respectivamente. Se a conta A quiser autorizar a conta B a gerenciar seus recursos, a conta A pode criar uma agência no IAM para estabelecer uma relação de confiança entre as duas contas.

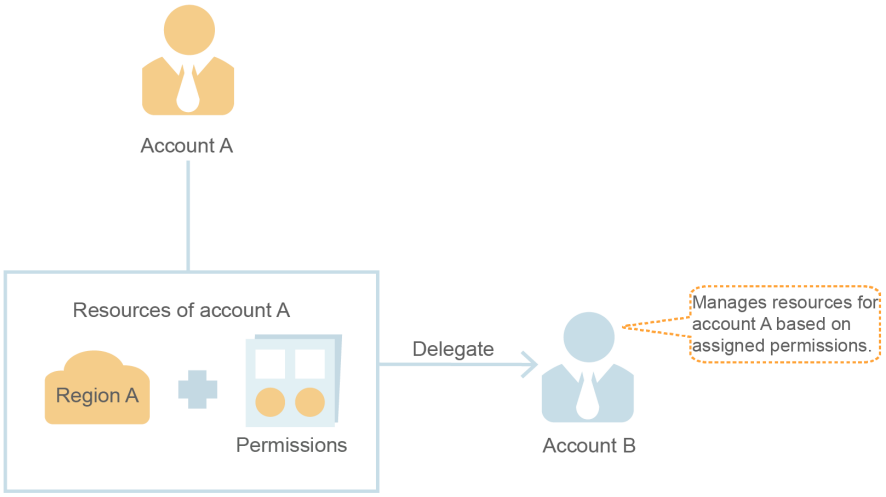
Requisitos

- A conta A comprou diferentes tipos de recursos na Huawei Cloud. A conta A quer autorizar a conta B a gerenciar seus recursos de VPC na região **CN-Hong Kong**.
- A conta B pode autorizar um ou mais funcionários (usuários do IAM) da empresa B a gerenciar os recursos da conta A.
- A conta A pode modificar ou cancelar a autorização fornecida à conta B a qualquer momento.

Solução

- A conta A cria uma agência no console do IAM para autorizar a conta B a gerenciar seus recursos.
- A conta B atribui permissões a seus usuários do IAM para gerenciar os recursos da conta A especificados na agência.
- A conta A pode modificar ou excluir a agência a qualquer momento. A exclusão da agência cancelará automaticamente as permissões atribuídas à conta B e seus usuários do IAM para gerenciar os recursos da conta A.

Figura 4-1 Modelo de autorização entre contas



Delegação de uma conta para gerenciar recursos

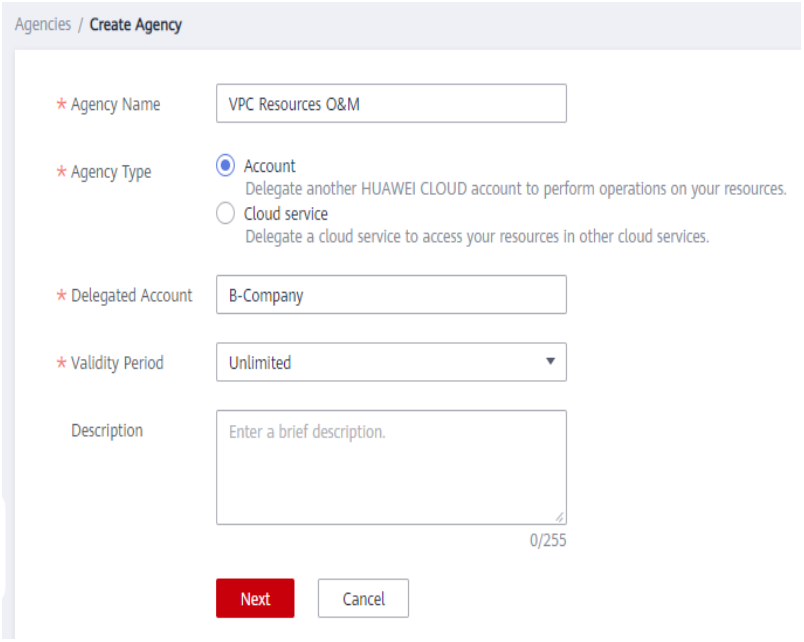
A conta A realiza o procedimento a seguir para delegar a conta B para gerenciar seus recursos de VPC na região **CN-Hong Kong**.

Passo 1 Faça logon na Huawei Cloud usando a conta A. No console do IAM, escolha **Agencies** no painel de navegação.

Passo 2 Clique em **Create Agency** e insira um nome de agência, por exemplo, **VPC Resources O&M**.

Passo 3 Selecione o tipo de agência **Account** e insira o nome da conta delegada, por exemplo, **B-Company**.

Passo 4 Defina o **Validity Period** como **Unlimited**.



Passo 5 Clique em **Next**.

Passo 6 Selecione **VPC FullAccess** e clique em **Next**.

Passo 7 Especifique o escopo da autorização como **Region-specific projects** e selecione **CN-Hong Kong**.

Passo 8 Clique em **OK**.

A agência é exibida na lista de agências.

NOTA

A conta A pode modificar as permissões ou o período de validade da agência ou excluir a agência com base nos requisitos de serviço.

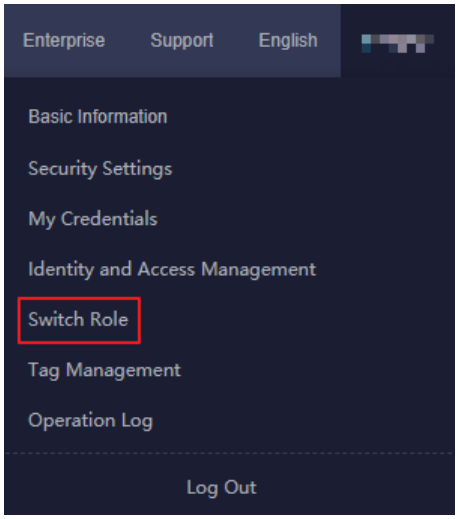
----Fim

Gerenciamento de recursos de uma conta

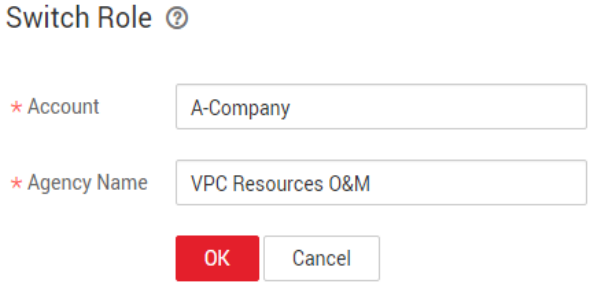
Depois que a agência é criada, a conta B pode alternar funções para a conta A para gerenciar os recursos da conta A. Para fazer isso, a conta B precisa ter obtido o nome da conta A e o nome da agência.

Passo 1 Faça logon no console de gerenciamento da Huawei Cloud usando a conta B.

Passo 2 Clique no nome de usuário no canto superior direito e escolha **Switch Role**.



Passo 3 Insira o nome da conta A. A agência criada pela conta A é exibida automaticamente.



Passo 4 Clique em **OK** para alternar para a conta A.

----Fim

5 Configuração da agência

5.1 Autorização de usuários do IAM para gerenciar recursos de uma conta

A empresa B é uma empresa profissional de O&M. Ela se torna uma parte delegada após ser autorizada pela empresa A. A empresa B atribui permissões a um ou mais de seus usuários de IAM para gerenciar os recursos da empresa A.

Requisitos

- A empresa B quer autorizar seus funcionários (usuários do IAM) a gerenciar os recursos delegados da empresa A.
- Se a empresa A cria várias agências para a empresa B, a empresa B pode alocar as agências para diferentes funcionários. Isso permitirá que cada funcionário gerencie apenas recursos de agências específicas.

Solução

- A conta B cria usuários no console do IAM e concede as permissões (incluindo Agent Operator) necessárias para o gerenciamento de recursos delegados aos usuários.
- A conta B cria uma política personalizada com apenas as permissões necessárias para gerenciar os recursos delegados de uma agência. Em seguida, a conta B anexa a política ao grupo ao qual um usuário pertence, para que o usuário só possa gerenciar os recursos da agência.

Procedimento

A conta B executa o procedimento a seguir para autorizar os usuários do IAM a gerenciar recursos de agências específicas. Após a autorização, os usuários do IAM da conta B podem mudar suas funções para a conta A para gerenciar os recursos da conta A. Para fazer isso, a conta B precisa ter obtido a conta (HUAWEI ID), o nome da agência e o ID da agência da parte delegante.

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

1. No painel de navegação, escolha **User Groups**.

2. Na página **User Groups**, clique em **Create User Group**.
3. Digite o nome do grupo de usuários, por exemplo, **Agency Management**.
4. Clique em **OK**.

   O grupo de usuários é exibido na lista de grupos de usuários.
5. Na linha que contém o grupo de usuários de destino, clique em **Authorize**.

   NOTA

   - Para autorizar um usuário a gerenciar apenas os recursos de uma agência específica, execute as etapas a seguir.
   - Para autorizar um usuário a gerenciar os recursos de todas as agências, vá para a **próxima etapa**.

   a. Na página **Select Policy/Role**, clique em **Create Policy** no canto superior direito.

   b. Digite um nome de política, por exemplo, **Agency 1 for Managing Company A**.

   c. Selecione **JSON** para **Policy View**.

   d. Na área **Policy Content**, insira o seguinte conteúdo:

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

   NOTA

   Substitua *b36b1258b5dc41a4aa8255508xxx...* pelo ID da agência obtido de uma parte delegante. Não faça nenhuma outra alteração.

   e. Clique em **Next**.
6. Selecione a agência **Agency 1 for Managing Company A** criada na **etapa anterior** ou a função **Agent Operator**.

   NOTA

   - A política personalizada permite que o usuário gerencie apenas recursos de um ID de agência específica.
   - A função **Agent Operator** permite que o usuário gerencie os recursos de todas as agências.
7. Especifique o escopo da autorização.
8. Clique em **OK**.

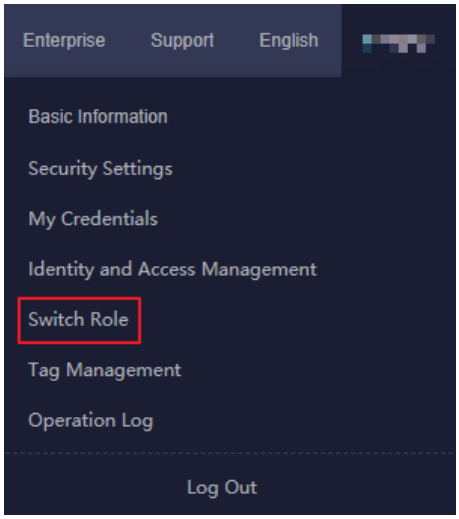
Passo 2 Crie um usuário e adicione o usuário ao grupo de usuários.

1. No painel de navegação, escolha **Users**.
2. Na página **Users**, clique em **Create User**.
3. Na página **Create User**, insira um nome de usuário e um endereço de e-mail.

4. Para **Access Type**, selecione **Management console access**.
5. Para **Credential Type**, selecione **Set by user**.
6. Habilite a proteção de logon, selecione um modo de verificação e clique em **Next**.
7. Selecione o grupo de usuários **Agency Management** criado em **2** e clique em **Create**.

Passo 3 Mude o papel.

1. Faça logon na Huawei Cloud como o usuário criado em **Passo 2**. Para obter mais informações, consulte **Fazer logon como um usuário do IAM**.
2. Clique no nome de usuário no canto superior direito e escolha **Switch Role**.



3. Insira o nome da conta da parte delegante. A agência criada pela parte delegante é exibida automaticamente.

   NOTA

   Se uma agência diferente das agências criadas pela parte delegante for exibida, uma mensagem será exibida indicando que você não tem permissões de acesso. Selecione a agência correta na caixa de listagem suspensa **Agency Name**.

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

----Fim

5.2 Configuração de uma agência para um ECS

Você pode criar uma agência para delegar o acesso aos serviços oferecidos pela Huawei Cloud. Este exemplo mostra como criar uma agência e delegar permissões ao Elastic Cloud Server (ECS) da Huawei Cloud, um servidor de nuvem de provisionamento escalável e sob demanda.

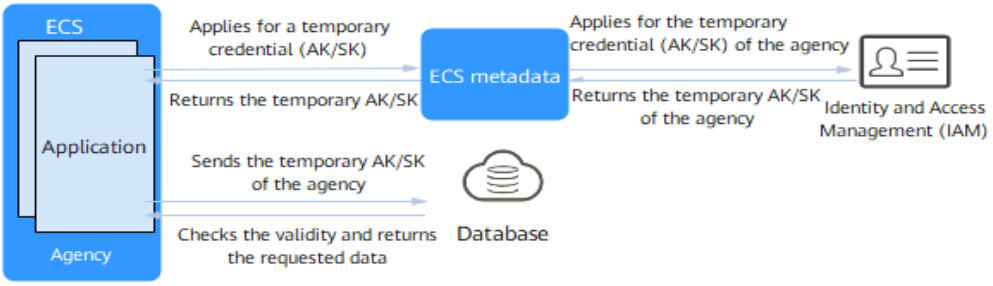
Cenários de aplicações

As aplicações executadas em um ECS devem fornecer credenciais de segurança para acessar os serviços da Huawei Cloud.

As aplicações podem usar credenciais de longo prazo (como nome de usuário e senha) ou temporárias para acesso. Credenciais temporárias são mais seguras porque têm uma vida útil limitada e são rotacionadas automaticamente. Para usar credenciais temporárias para acessar

os recursos da Huawei Cloud, configure uma agência com permissões delegadas ao ECS onde as aplicações estão sendo executadas e as aplicações obterão a credencial temporária da agência.

Figura 5-1 Obtenção de uma credencial temporária



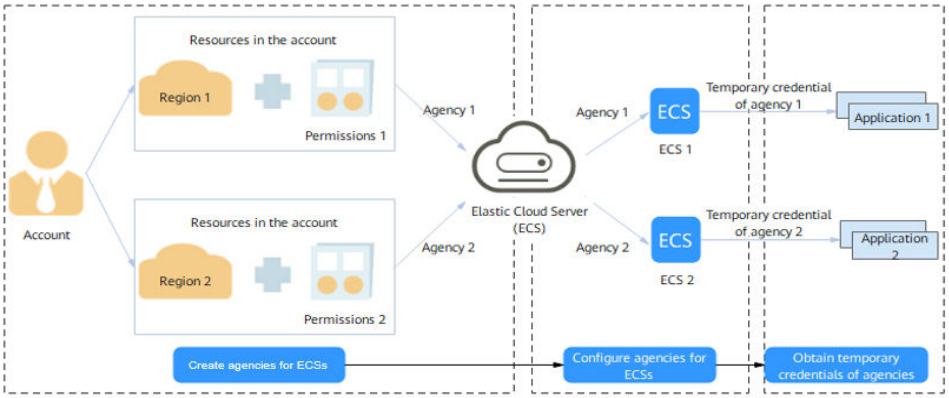
Por exemplo, configure uma agência para o ECS para permitir que as aplicações em execução em um ECS usem uma credencial temporária para acessar um banco de dados da Huawei Cloud. O ECS envia uma solicitação para obter uma credencial temporária (AK/SK) dos metadados do ECS. Os metadados do ECS obtêm uma AK/SK temporária da agência do IAM e retornam a AK/SK para o ECS. O banco de dados só permite acesso após verificar se a credencial temporária enviada do ECS é válida.

Solução

Crie uma agência no console do IAM e especifique as permissões e o escopo para delegar permissões ao ECS. Configure a agência para o ECS em que as aplicações estão sendo executadas. Em seguida, o ECS obterá uma credencial temporária da agência para acessar recursos com base nas permissões atribuídas.

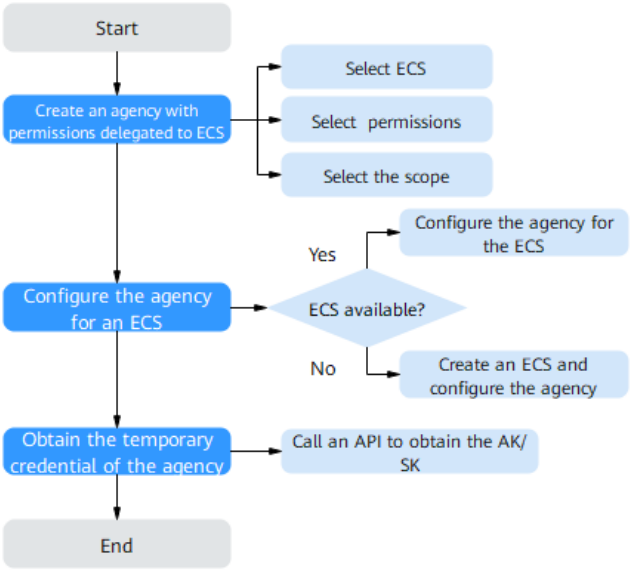
1. Crie uma agência com permissões delegadas ao ECS e selecione as permissões e o escopo da agência.
2. Configure a agência criada para o ECS. Somente uma agência pode ser configurada para um ECS.
3. Obtenha a credencial temporária (AK/SK) da agência para permitir que aplicações em execução no ECS acessem outros recursos da Huawei Cloud com base nas permissões atribuídas no escopo autorizado.

Figura 5-2 Agência do ECS



Fluxo do processo

Figura 5-3 Fluxograma



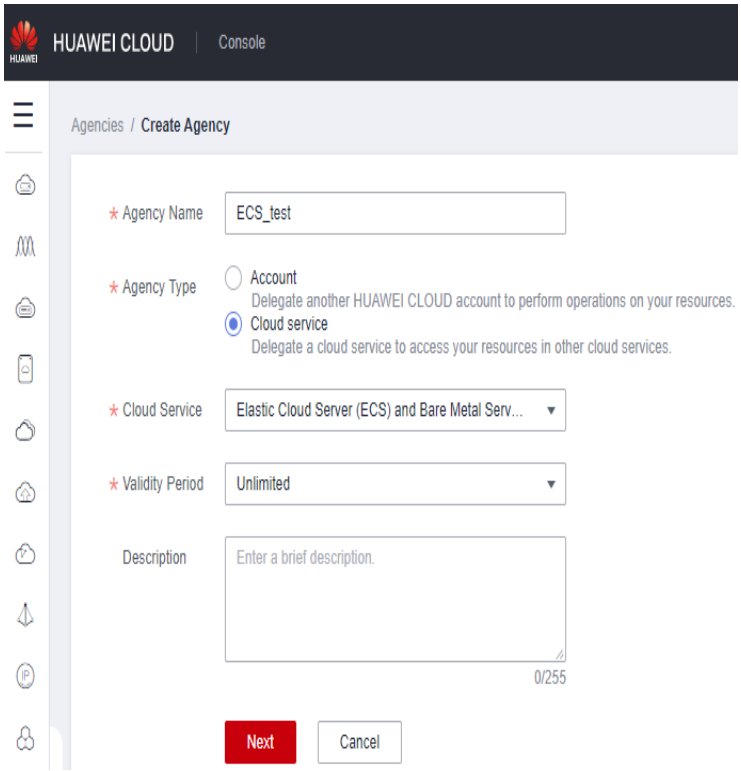
Procedimento

Para permitir que aplicações em execução em um ECS acessem recursos em outros serviços da Huawei Cloud, faça o seguinte:

Passo 1 Crie uma agência para o ECS como administrador.

1. Faça logon no console do IAM.
2. No console do IAM, escolha **Agencies** no painel de navegação à esquerda e clique em **Create Agency** na página exibida.

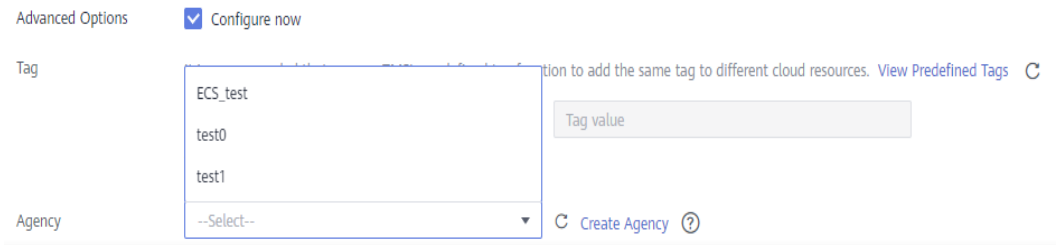
3. Insira um nome de agência.
4. Selecione o **Cloud service** para **Agency Type** e o **Elastic Cloud Server (ECS) and Bare Metal Server (BMS)** para **Cloud Service**.



5. Selecione um período de validade.
6. (Opcional) Digite uma descrição para a agência para facilitar a identificação.
7. Clique em **Next**.
8. Selecione as permissões a serem atribuídas à agência, clique em **Next** e especifique o escopo da autorização.
9. Clique em **OK**.

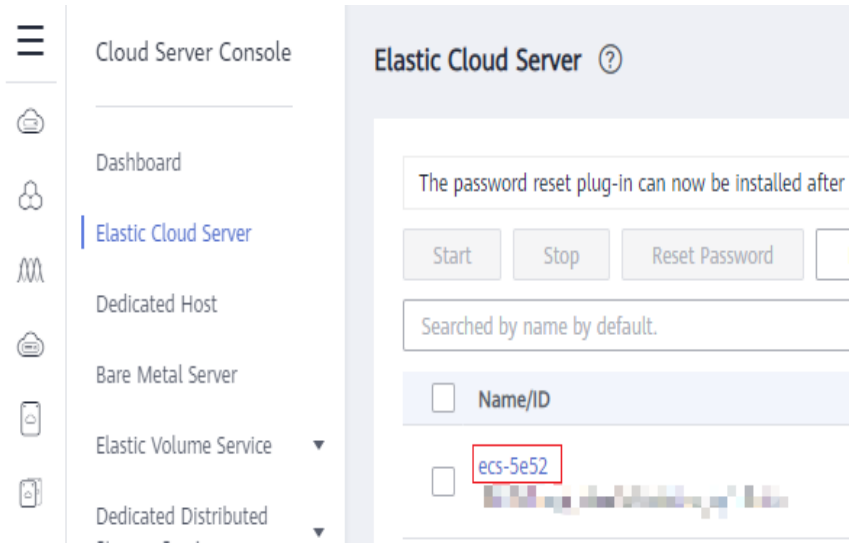
Passo 2 Configure a agência para o ECS como administrador ou um usuário do IAM com permissões do ECS.

- Se não houver ECSs disponíveis, crie um consultando **Compra de um ECS**. Ao configurar **configurações avançadas**, selecione a agência criada na **Etapa 1** na lista suspensa.

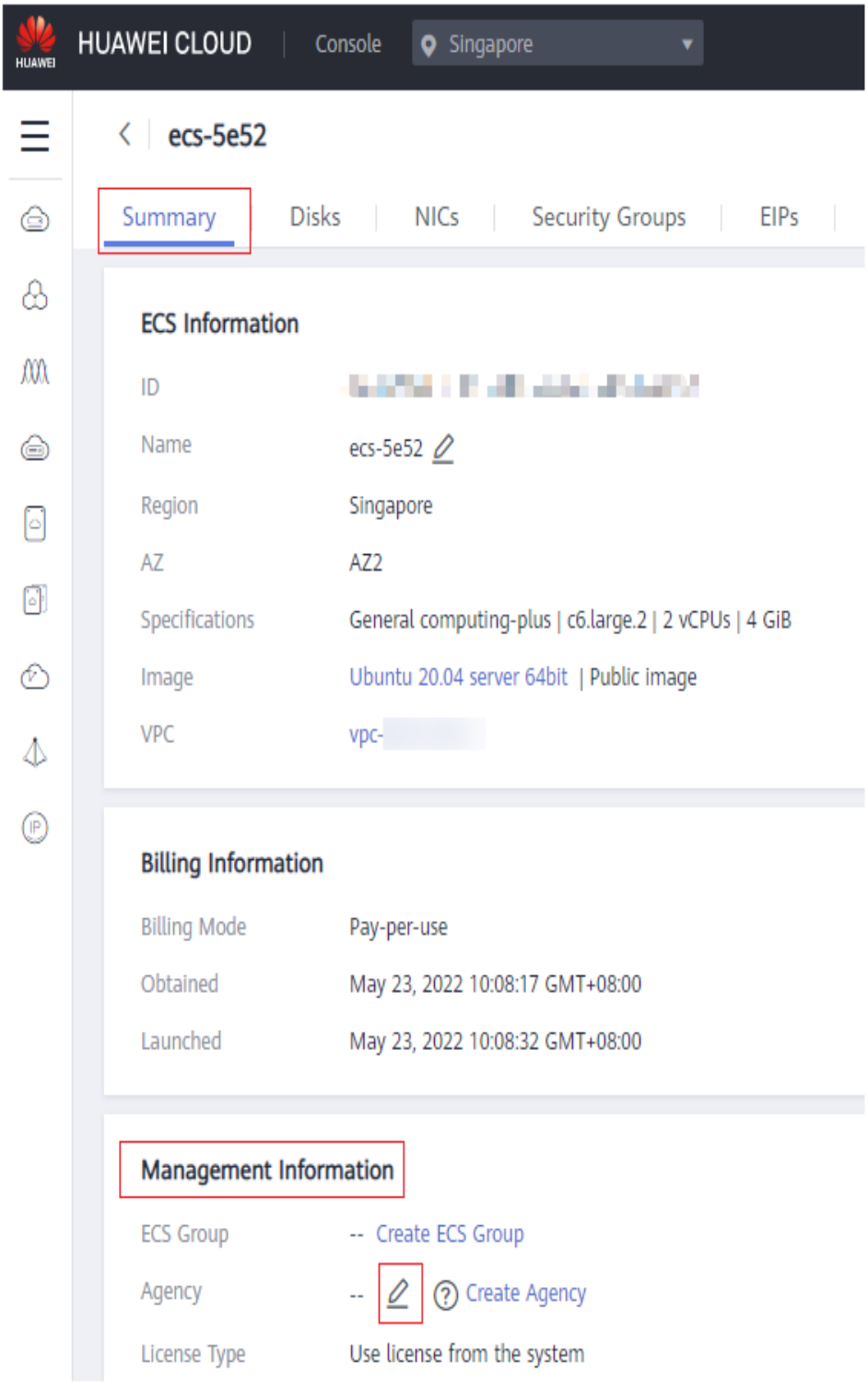


- Se houver ECSs disponíveis, configure a agência criada para um ECS da seguinte maneira:

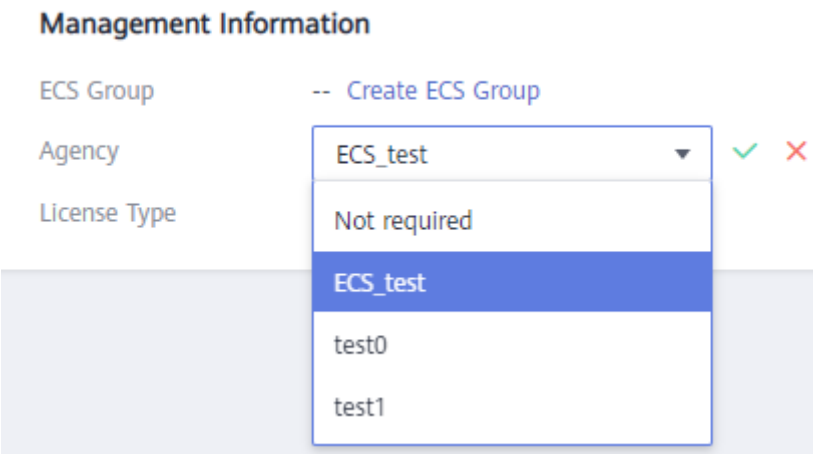
1. No console do ECS, clique em um ECS para o qual você deseja configurar a agência.



2. Na área **Management Information**, clique em .



3. Selecione a agência criada na **Etapa 1** na lista suspensa.



4. Clique em ✓ para concluir a configuração.

Passo 3 Permita que aplicações no ECS obtenham uma credencial temporária.

Configure aplicações em execução no ECS para chamar API de **Chave de segurança (API de metadados do OpenStack)** para obter a credencial temporária (AK/SK) da agência para acessar outros serviços da Huawei Cloud.

- URI

/openstack/latest/securitykey

- Método

Suporta solicitações GET.

- Exemplo

Linux:

curl http://169.254.169.254/openstack/latest/securitykey

Windows:

Invoke-RestMethod http://169.254.169.254/openstack/latest/securitykey

NOTA

O ECS rotaciona automaticamente as credenciais temporárias para garantir que elas sejam seguras e válidas.

----Fim

6 Atribuição de permissões entre regiões (gerenciamento original de vários projetos)

6.1 Cenário

A empresa A é um usuário empresarial da Huawei Cloud e possui várias equipes de projeto que exigem diferentes recursos e pessoal. Esta seção apresenta as melhores práticas para o gerenciamento de vários projetos para atender aos requisitos da empresa A.

Requisitos

- **Requisito 1**: a empresa A pode comprar vários tipos de recursos em **CN-Hong Kong** e **AP-Singapore** para duas equipes de projeto. Os recursos das duas equipes de projeto precisam ser isolados um do outro. O acesso a serviços de nuvem específicos precisa ser autorizado, por exemplo, apenas usuários autorizados do IAM podem acessar e usar o ECS.
- **Requisito 2**: cada membro das equipes de projeto pode acessar somente os recursos da equipe de projeto à qual o membro pertence e só tem as permissões necessárias para concluir tarefas.
- **Requisito 3**: cada equipe de projeto faz pagamentos apenas pelos recursos usados por seus membros, e as despesas do projeto são claras.

Solução

- **Solução para o requisito 1**: o Enterprise Management (EPS) e o Identity and Access Management (IAM) são dois serviços de nuvem da Huawei Cloud que podem isolar recursos entre projetos. No entanto, a lógica de implementação e as funções dos dois serviços são diferentes.
  - **Enterprise Management**: você pode criar projetos empresariais para agrupar e gerenciar recursos entre regiões. Os recursos em projetos empresariais são logicamente isolados uns dos outros. **Cada projeto empresarial pode conter recursos de várias regiões** e os recursos podem ser adicionados ou removidos de projetos empresariais. Recursos especificados de determinados serviços, por exemplo, um ECS específico, podem ser adicionados ou removidos de projetos empresariais.

  - **IAM**: os projetos do IAM agrupam e isolam fisicamente os recursos em uma região, **e cada projeto do IAM só pode conter recursos na mesma região.**

Em conclusão, o Enterprise Management oferece um isolamento de recursos entre regiões mais flexível entre projetos do que o IAM. Portanto, recomenda-se que a empresa A use o Enterprise Management para gerenciar os recursos do projeto. As soluções para os requisitos a seguir são propostas usando o serviço Enterprise Management. Para obter detalhes sobre os dois serviços, consulte **Quais são as diferenças entre o IAM e o Enterprise Management?**

- **Solução para o requisito 2**: no IAM, a empresa A cria usuários do IAM para funcionários e adiciona os usuários do IAM a grupos diferentes. No Enterprise Management, a empresa A adiciona os grupos de usuários aos projetos empresariais criados para atender ao **Requisito 1** e atribui as permissões de acesso aos recursos necessárias (consulte **Tabela 6-1**) a cada grupo de usuários.

Figura 6-1 Modelo de gerenciamento de pessoal da empresa A

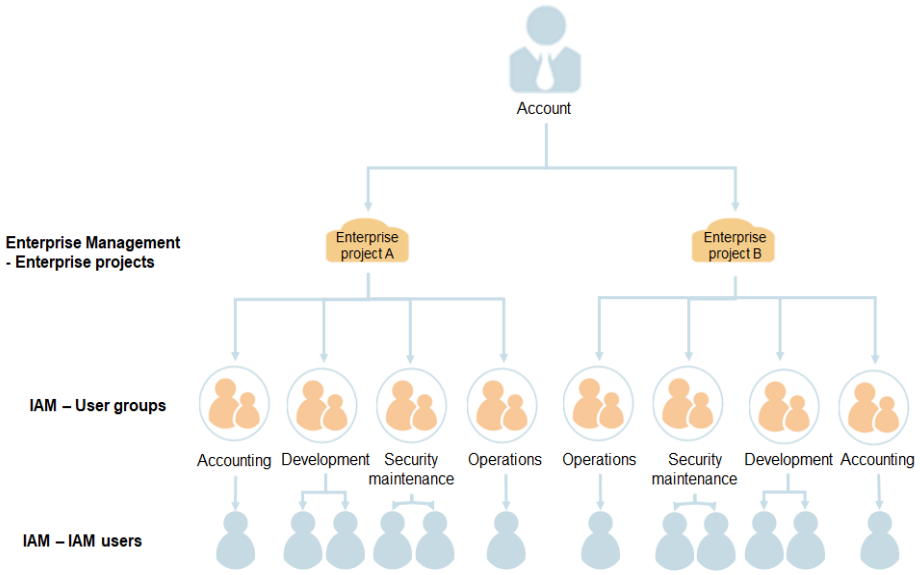


Tabela 6-1 Permissões de grupo de usuários na empresa A

Grupo de usuários	Responsabilidade	Permissões	Descrição
Equipe de contabilidade	Gerenciamento de despesas do projeto	Enterprise Project BSS FullAccess	Permissões para gerenciamento contábil de projetos empresariais
Equipe de desenvolvimento	Desenvolvimento do projeto	ECS FullAccess	Permissões completas para o Elastic Cloud Server (ECS)
		OBS FullAccess	Permissões completas para o Object Storage Service (OBS)
		ELB FullAccess	Permissões completas para o Elastic Load Balance (ELB)

Grupo de usuários	Responsabilidade	Permissões	Descrição
Equipe de manutenção de segurança	O&M de segurança do projeto	ECS CommonOperations	Permissões para operações básicas do ECS
		CAD Administrator	Permissões completas para Advanced Anti-DDoS (AAD)
Equipe de operações	Operações gerais do projeto	EPS FullAccess	Permissões completas para o Enterprise Management, incluindo modificação, ativação, desativação e exibição de projetos empresariais

NOTA

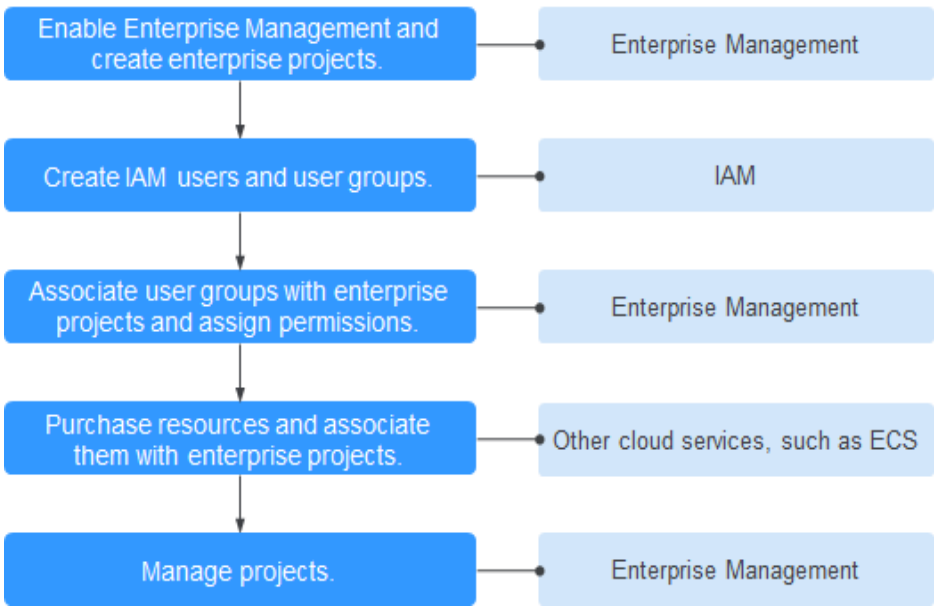
Para obter detalhes sobre as permissões de todos os serviços da Huawei Cloud, consulte **Permissões definidas pelo sistema**.

- **Solução para o requisito 3**: a empresa A usa o Enterprise Management para gerenciar renovações, pedidos, contabilidade, cancelamentos de assinaturas, alterações e cotas de cada projeto empresarial. Para obter detalhes, consulte **Gerenciamento de contabilidade de projetos empresariais**.

6.2 Procedimento

A figura a seguir ilustra o processo de gerenciamento de projetos empresariais para atender aos requisitos da empresa A.

Figura 6-2 Processo de gerenciamento de projetos empresariais



Etapa 1: ative o serviço Enterprise Management e crie projetos empresariais no **console do Enterprise Management**.

Etapa 2: no **console do IAM**, crie um grupo de usuários para cada equipe funcional, crie usuários do IAM para funcionários e adicione os usuários a diferentes grupos de usuários.

Etapa 3: no **console do Enterprise Management**, atribua as permissões necessárias a cada grupo de usuários e adicione o grupo de usuários ao projeto empresarial correspondente. Os usuários do grupo herdam automaticamente suas permissões.

Etapa 4: compre recursos em **outros consoles de serviço de nuvem** e vincule os recursos aos projetos empresariais correspondentes.

Operação de acompanhamento: gerenciamento de projetos empresariais: execute o gerenciamento de pessoal, recursos e contabilidade no **console do Enterprise Management**.

Ativação do gerenciamento empresarial e criação de projetos empresariais

Execute o procedimento a seguir para criar dois projetos empresariais (A e B) no console do Enterprise Management. Se você ativou o Enterprise Project, vá para **Passo 4**.

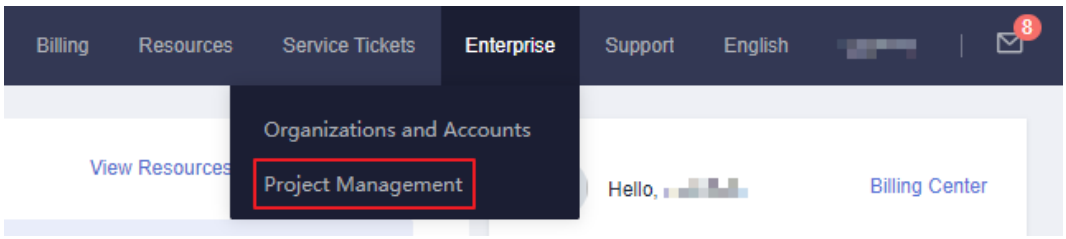
Passo 1 Faça logon no console da Huawei Cloud, passe o mouse sobre o nome da conta no canto superior direito e escolha **Basic Information**.

Passo 2 Na página **Basic Information**, clique em **Enable Enterprise Project Function**.

Passo 3 Leia e concorde com o *Contrato de Enterprise Management da Huawei Cloud* e clique em **Apply Now**.

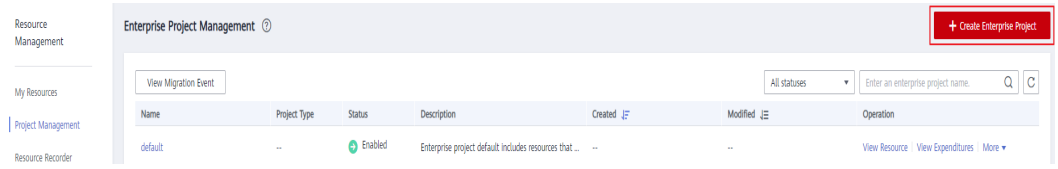
Passo 4 No console de gerenciamento da Huawei Cloud, escolha **Enterprise** > **Project Management**.

Figura 6-3 Acesso à página Gerenciamento de projetos empresariais



Passo 5 Na página **Enterprise Project Management Service**, clique em **Create Enterprise Project**.

Figura 6-4 Criação de um projeto empresarial



Passo 6 Digite **Enterprise_Project_A** para **Name** e clique em **OK**.

Passo 7 Repita as etapas **5** e **6** para criar **Enterprise_Project_B**.

Os dois projetos empresariais são exibidos na página **Enterprise Project Management Service**.

----Fim

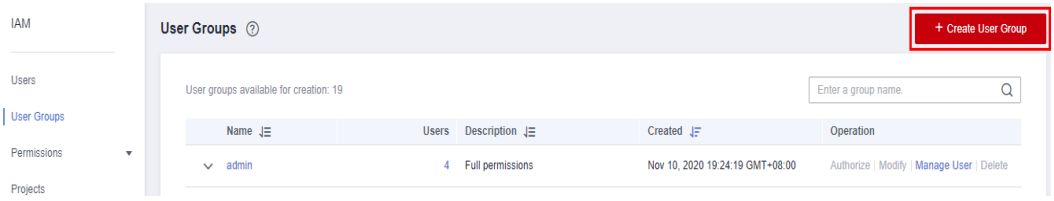
Criação de usuários e grupos de usuários do IAM

Veja a seguir um exemplo de procedimento para criar um grupo de usuários (**Enterprise Project A_Accounting**) e usuário (**Murphy**) e adicionar o usuário ao grupo de usuários.

Passo 1 Crie um grupo de usuários.

1. Vá para o console de gerenciamento da Huawei Cloud e escolha **Service List** > **Management & Governance** > **Identity and Access Management**.
2. No console do IAM, escolha **User Groups** no painel de navegação. Em seguida, clique em **Create User Group**.

Figura 6-5 Criação de um grupo de usuários



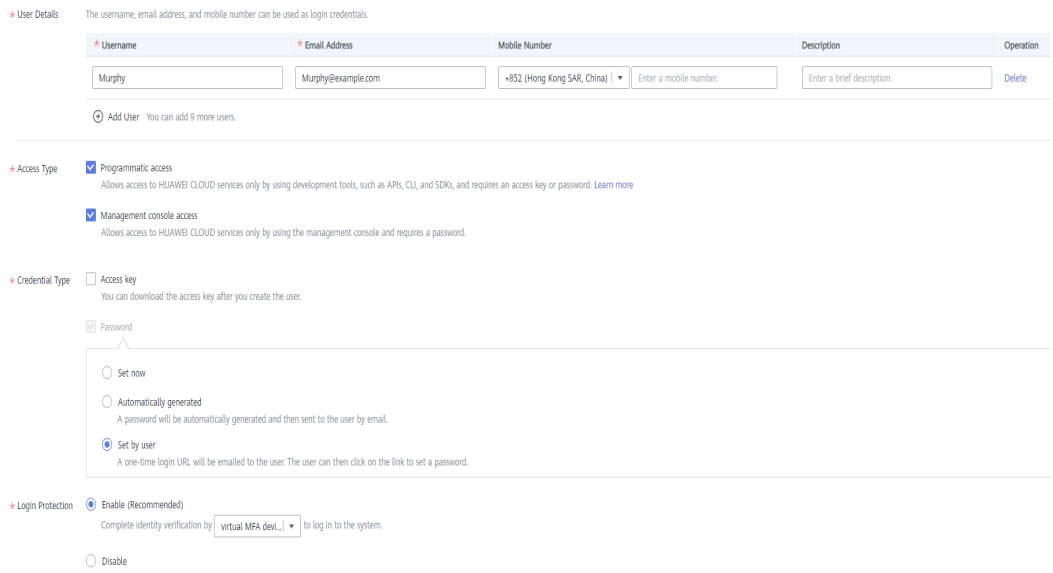
3. Defina o nome do grupo de usuários como **Enterprise Project A_Accounting** e clique em **OK**.
4. Repita as etapas **2** e **3** para criar as equipes de contabilidade, desenvolvimento, manutenção de segurança e operações para os dois projetos empresariais.

Os grupos de usuários são exibidos na lista de grupos de usuários.

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

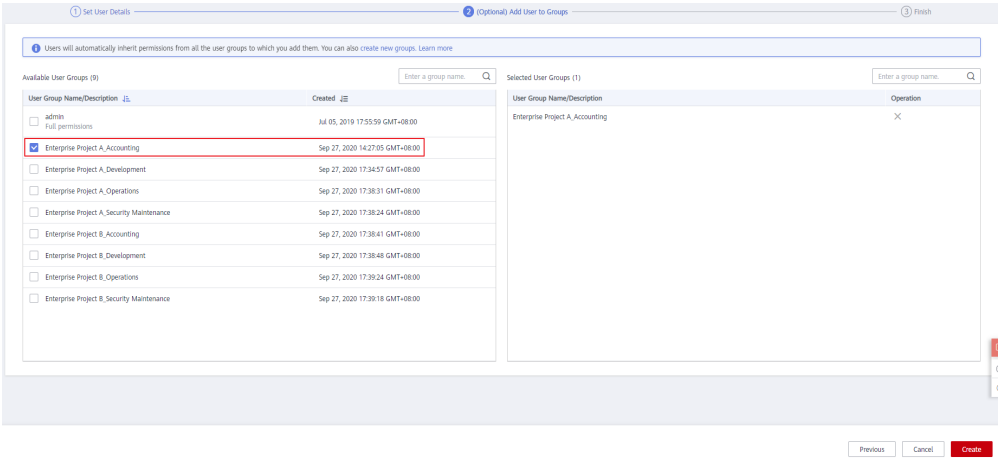
1. No painel de navegação do console do IAM, escolha **Users**. Em seguida, clique em **Create User**.
2. Especifique as informações do usuário, selecione um **tipo de acesso** (consulte **Figura 6-6**) e clique em **Next**.

Figura 6-6 Criação de um usuário do IAM



3. Adicione o usuário **Murphy** ao grupo de usuários **Enterprise Project A_Accounting** e clique em **Create**.

Figura 6-7 Adição do usuário a um grupo de usuários



4. Repita as etapas **1** a **3** para criar usuários para todos os funcionários e adicione os usuários aos grupos de usuários correspondentes.

O usuário é exibido na lista de usuários. Você pode visualizar os usuários do IAM de cada grupo de usuários na página de guia **Users**.

----Fim

Vinculação de grupos de usuários a projetos empresariais

Atribua permissões a um grupo de usuários e aplique permissões de grupo de usuários a projetos empresariais.

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

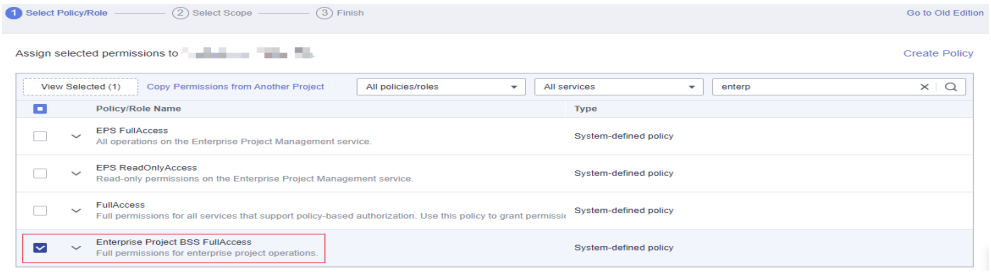
Passo 2 Na lista de grupos de usuários, localize a linha que contém o grupo de usuários de destino e clique em **Authorize** na coluna **Operation**.

Passo 3 Na página exibida, procure **Enterprise Project BSS FullAccess** na caixa de pesquisa, selecione-o e clique em **Next**.

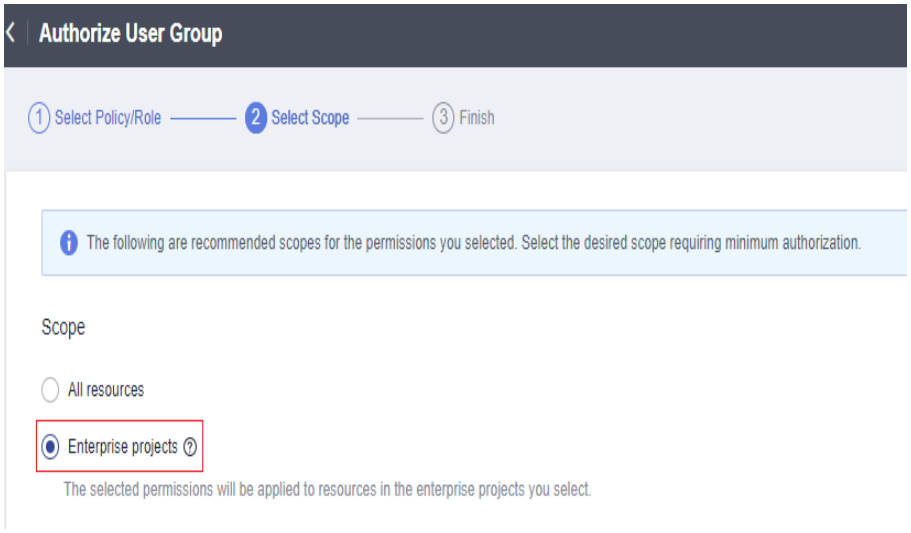
NOTA

Você pode criar políticas personalizadas para complementar políticas definidas pelo sistema para o gerenciamento de permissões refinado. Para obter detalhes, consulte **Criação de uma política personalizada**.

Figura 6-8 Seleção de permissões



Passo 4 Selecione o escopo de autorização de **Enterprise projects**.



Passo 5 Na lista de projetos empresariais, selecione **Enterprise Project A**.

Passo 6 Clique em **OK**.

----Fim

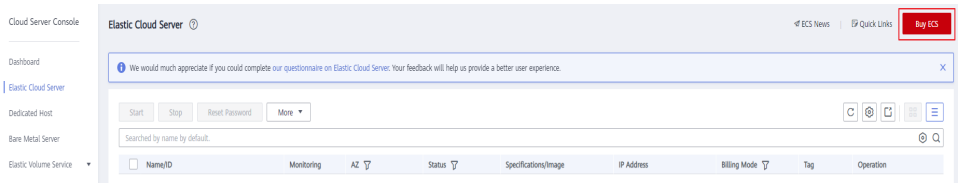
Compra de recursos e sua vinculação a projetos empresariais

Segue-se um exemplo de procedimento para comprar um ECS e vinculá-lo ao projeto empresarial A.

Passo 1 Faça logon no console de gerenciamento da Huawei Cloud, clique em ☰ no canto superior esquerdo e escolha **Compute** > **Elastic Cloud Server**.

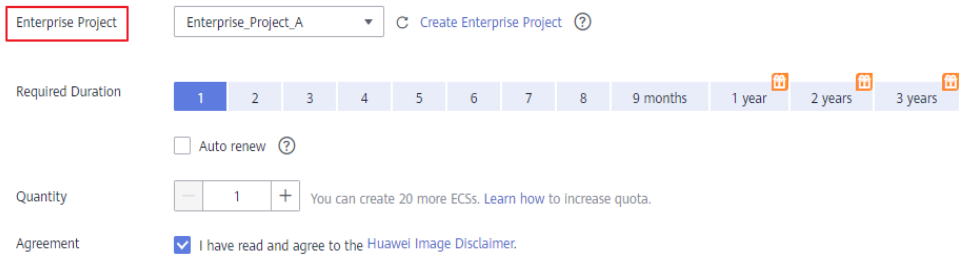
Passo 2 Clique em **Buy ECS** no canto superior direito.

Figura 6-9 Compra de um ECS



Passo 3 Especifique as informações do ECS e selecione **Enterprise_Project_A** na lista suspensa **Enterprise Project**.

Figura 6-10 Seleção de um projeto empresarial



Passo 4 Clique em **Next** no canto inferior direito para exibir os detalhes do recurso e enviar o pedido.

Passo 5 Repita de **Passo 1** a **Passo 4** para comprar os recursos necessários para os dois projetos empresariais.

Para exibir os recursos comprados, vá para o console do Enterprise Management e clique em **View Resource** na linha que contém o projeto empresarial A ou B.

NOTA

- Atualmente, o Enterprise Management oferece suporte apenas a **serviços específicos da Huawei Cloud**.
- Se você já comprou os recursos necessários, pode vinculá-los diretamente aos dois projetos empresariais. Para obter detalhes, consulte **Adição de recursos a um projeto empresarial**.

----Fim

Operação de acompanhamento: gerenciamento de projetos empresariais

Depois de concluir as etapas anteriores, você pode gerenciar seus projetos empresariais na página **Enterprise** > **Project Management** > **Enterprise Project Management Service**.

- **Resource management**: clique em **View Resource** para exibir os recursos existentes de um projeto empresarial e **adicionar mais recursos ao projeto empresarial**.
- **Personnel management**: escolha **More** > **Permissions** para acessar o console do IAM para exibir os usuários e grupos de usuários vinculados a um projeto empresarial e modificar os usuários, grupos de usuários e suas permissões para o projeto empresarial. Para obter detalhes, consulte **Gerenciamento de pessoal**.
- **Accounting management**: clique em **View Expenditures** para exibir as ordens e os faturamentos e gerenciar as renovações de um projeto empresarial. Para obter detalhes, consulte **Gerenciamento de contabilidade de projetos empresariais**.

