

Identity and Access Management

Primeiros passos

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 Antes de começar.....	1
2 Etapa 1: criar grupos de usuários e atribuir permissões.....	3
3 Etapa 2: criar usuários do IAM e fazer logon.....	7
4 História de mudanças.....	12

1 Antes de começar

A leitura deste documento irá ajudá-lo a:

- Criar usuários do Identity and Access Management (IAM).
- Criar grupos de usuários com base nas funções de negócios da sua organização.
- Atribuir permissões a grupos de usuários.
- Criar usuários do IAM para funcionários em sua organização.
- Permitir que os usuários do IAM façam logon na Huawei Cloud.

Pré-requisitos

Você já tem uma conta. Se você não tiver uma conta, crie uma.

Cenário de exemplo

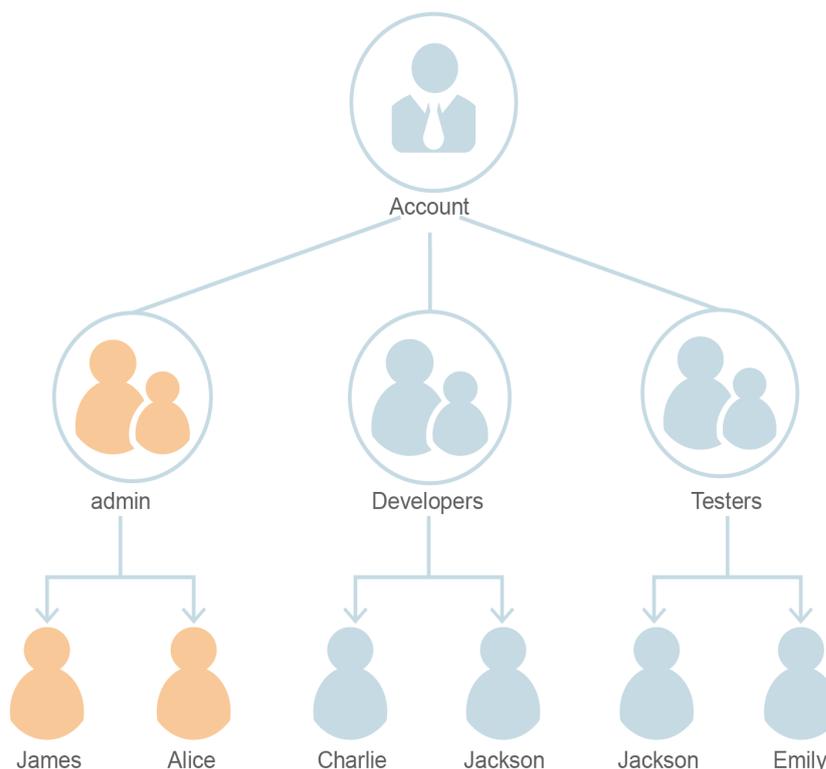
Uma empresa de desenvolvimento de sites tem três equipes funcionais em Hong Kong. Com o IAM, o administrador da empresa pode criar apenas uma conta e, em seguida, usar essa conta para criar usuários do IAM para funcionários e atribuir permissões com base em suas responsabilidades de trabalho. Para obter as definições de uma conta e de um usuário do IAM, consulte [Conceitos básicos](#).

A seguir, usamos a empresa como exemplo para mostrar como usar o IAM para gerenciar permissões.

Estrutura organizacional

- Equipe de gerenciamento (grupo **admin** em [Figura 1-1](#)): gerencia funcionários e recursos, atribui permissões e aloca recursos. Os membros da equipe incluem James e Alice.
- Equipe de desenvolvimento (grupo **Developers** em [Figura 1-1](#)): desenvolve sites. Os membros da equipe incluem Charlie e Jackson.
- Equipe de teste (grupo **Testers** em [Figura 1-1](#)): testa sites. Os membros da equipe incluem Jackson e Emily. Jackson desenvolve e testa sites, então ele precisa se juntar aos grupos **Developers** e **Testers** para obter as permissões necessárias.

Figura 1-1 Modelo de gerenciamento de usuários



Grupos de usuários e recursos necessários

- Grupo **admin**: gerencia permissões de usuário usando o IAM.
- Grupo **Developers**: desenvolve sites usando Elastic Cloud Server (ECS), Elastic Load Balance (ELB), Virtual Private Cloud (VPC), Relational Database Service (RDS), Elastic Volume Service (EVS) e Object Storage Service (OBS).
- Grupo **Testers**: realiza testes funcionais e de desempenho em sites usando o serviço Application Performance Management (APM).

Processo de gerenciamento de usuários

1. O administrador da empresa faz login na Huawei Cloud, cria grupos de usuários **Developers** e **Testers** e concede-lhes permissões. Para mais detalhes, consulte [2 Etapa 1: criar grupos de usuários e atribuir permissões](#).
2. O administrador cria usuários do IAM para os membros das três equipes funcionais. Em seguida, os membros fazem login na Huawei Cloud, como usuários do IAM. Para mais detalhes, consulte [3 Etapa 2: criar usuários do IAM e fazer login](#).

2 Etapa 1: criar grupos de usuários e atribuir permissões

Uma empresa tem três equipes funcionais, incluindo as equipes de gerenciamento (grupo **admin**), desenvolvimento e teste. Depois que o administrador da empresa cria uma conta, o grupo padrão **admin** é gerado automaticamente e tem permissões completas para todos os serviços de nuvem. O administrador só precisa criar outros dois grupos no IAM para as equipes de desenvolvimento e teste, respectivamente.

Criação de grupos de usuários

Passo 1 Use sua HUAWEI ID para ativar os serviços da Huawei Cloud e, em seguida, faça logon na Huawei Cloud.

Figura 2-1 Fazer logon na Huawei Cloud

HUAWEI ID login

Phone/Email/Login ID/HUAWEI CLOUD account name

Password

LOG IN

Register | Forgot password

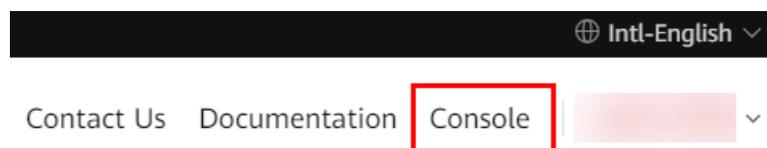
Use Another Account

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](#)

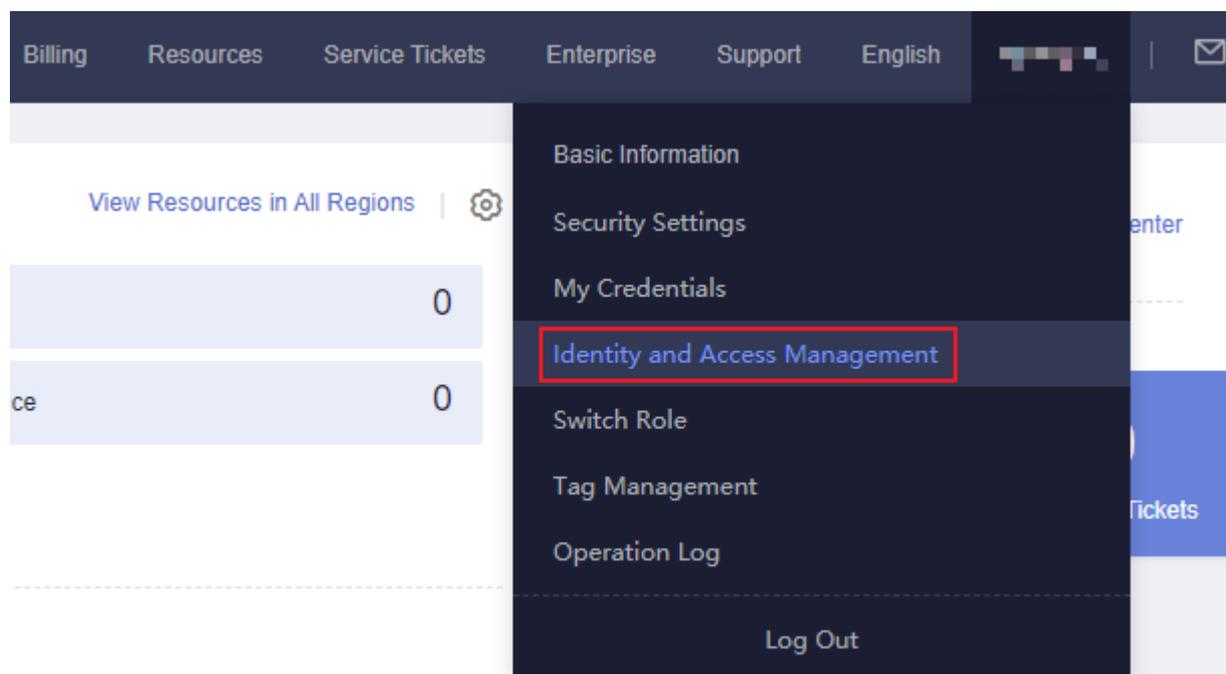
Passo 2 Faça login no console de gerenciamento.

Figura 2-2 Fazer login no console de gerenciamento



Passo 3 No console de gerenciamento, passe o ponteiro do mouse sobre o nome de usuário no canto superior direito e escolha **Identity and Access Management** na lista suspensa.

Figura 2-3 Acessar o console do IAM



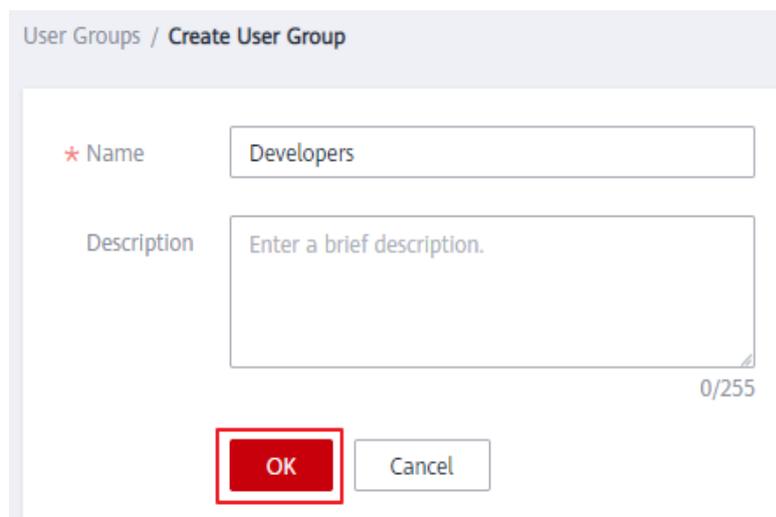
Passo 4 No console do IAM, escolha **User Groups** e clique em **Create User Group**.

Figura 2-4 Criação de um grupo de usuários



Passo 5 Crie um grupo para desenvolvedores e clique em **OK**.

Figura 2-5 Configuração dos detalhes do grupo de usuários



Passo 6 Repita as etapas **Passo 4** e **Passo 5** para criar um grupo para testadores.

----Fim

Atribuição de permissões a grupos de usuários

Os desenvolvedores da empresa precisam usar ECS, RDS, ELB, VPC, EVS e OBS, portanto, o administrador precisa atribuir as permissões necessárias ao grupo de desenvolvedores para ativar o acesso a esses serviços. Os testadores dessa empresa precisam usar o APM, portanto, o administrador precisa atribuir as permissões necessárias ao grupo de testadores para ativar o acesso ao serviço. Depois que as permissões são atribuídas, os usuários dos dois grupos podem acessar os serviços correspondentes. Para obter detalhes sobre as permissões de todos os serviços de nuvem, consulte [Permissões definidas pelo sistema](#).

Passo 1 Determine as políticas de permissões a serem anexadas a cada grupo de usuários.

Determine as políticas (consulte [Tabela 2-1](#)) consultando [Permissões definidas pelo sistema](#). Regiões são áreas geográficas onde os serviços são implementados. Se uma política de serviço em nível de projeto for anexada a um grupo de usuários para um projeto em uma região específica, a política entrará em vigor somente para esse projeto.

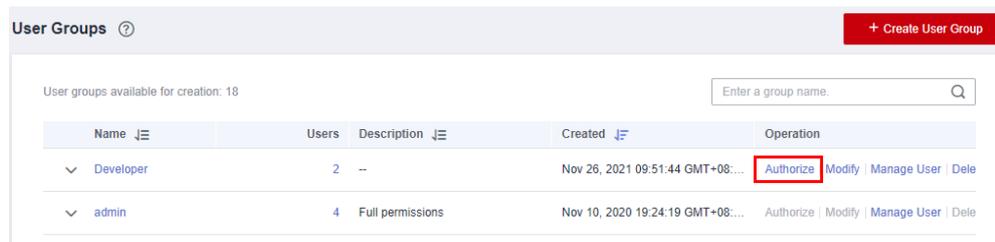
Tabela 2-1 Políticas de permissões necessárias

Grupo de usuários	Serviço de nuvem	Região	Política ou função
Grupo de desenvolvedores	ECS	Regiões específicas	ECS FullAccess
	RDS	Regiões específicas	RDS FullAccess
	ELB	Regiões específicas	ELB FullAccess
	VPC	Regiões específicas	VPC FullAccess
	EVS	Regiões específicas	EVS FullAccess
	OBS	Global	OBS OperateAccess

Grupo de usuários	Serviço de nuvem	Região	Política ou função
Grupo do testador	APM	Regiões específicas	APM FullAccess

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

Figura 2-6 Autorização de um grupo de usuários



Passo 3 Atribua permissões ao grupo de usuários para projetos da região específica.

1. Todos os serviços em **Tabela 2-1** exceto OBS são implementados em projetos específicos. Selecione as permissões desejadas para serviços no nível do projeto e clique em **Next**.
2. Selecione **Region-specific projects** para **Scope**, selecione **CN-Hong Kong** e clique em **OK**.

A empresa está localizada em Hong Kong. Portanto, selecione **CN-Hong Kong** para reduzir a latência da rede e acelerar o acesso ao serviço. Em seguida, os usuários do grupo de desenvolvedores podem acessar os serviços de nível de projeto especificados em **CN-Hong Kong**, mas não têm permissões para acessar os serviços em outras regiões.

Passo 4 Atribua permissões ao grupo de usuários para os serviços globais.

1. Selecione **OBS OperateAccess** e clique em **Next**.
2. Selecione **Global services** para **Scope** e clique em **OK**.

Passo 5 Repita as etapas **Passo 2** a **Passo 4** para anexar a política **APM FullAccess** ao grupo de testadores na região **CN-Hong Kong**.

---Fim

3 Etapa 2: criar usuários do IAM e fazer logon

Crie usuários do IAM para funcionários e adicione os usuários aos grupos de usuários criados na seção anterior. Cada usuário do IAM tem sua própria senha para fazer logon na Huawei Cloud e pode usar recursos com base nas permissões atribuídas.

Criação de usuários do IAM

Passo 1 Escolha **Users** no painel de navegação e 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 3-1 Configuração de informações do usuário

The screenshot shows the 'Create User' page in the Huawei Cloud IAM console. It features a progress bar at the top with three steps: '1 Set User Details', '2 (Optional) Add User to Group', and '3 Finish'. Below the progress bar, there is a 'User Details' section with a note: 'The username, email address, and mobile number can be used as login credentials.' The section contains a table with columns: Username, Email Address, Mobile Number, Description, External Identity ID, and Operation. Two rows are visible, one for 'James' and one for 'Alice'. Each row has input fields for the first four columns and a 'Delete' button in the 'Operation' column. At the bottom, there is an 'Add User' button and a note 'Users available for addition: 9'.

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 sua senha, poderão redefini-la por meio da verificação do endereço de e-mail ou do número de celular. Se nenhum endereço de e-mail ou número de celular tiver sido vinculado aos usuários, os usuários precisarão solicitar ao administrador que redefina suas senhas.

Tabela 3-1 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 de serem criados. Este campo é obrigatório se você tiver selecionado Set by user para Credential Type .
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 de serem criados. Este campo é opcional.
Description	Informações adicionais sobre o usuário do IAM. Este campo é opcional.
External Identity ID	Identidade de um usuário empresarial no SSO de usuário do IAM. O valor contém no máximo 128 caracteres. Esse campo é obrigatório quando você configura o SSO do usuário do IAM para logon federado.

Figura 3-2 Configuração do tipo de acesso

Access Type
 Programmatic access
Allows access to HUAWEI CLOUD services only by using development tools, such as APIs, CLI, and SDKs, and requires an access key or password. [Learn more](#)

Management console access
Allows access to HUAWEI CLOUD services only by using the management console and requires a password.

Credential Type
 Access key
You can download the access key after you create the user.

Password

Set now

 Require password reset at first login
 Automatically generated
A password will be automatically generated and then sent to the user by email.
 Set by user
A one-time login URL will be emailed to the user. The user can then click on the link to set a password.

Login Protection
 Enable (Recommended)
Complete identity verification by to log in to the system.

Disable

- **Programmatic access:** selecione essa opção para permitir que o usuário acesse serviços de nuvem 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 serviços de nuvem 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.

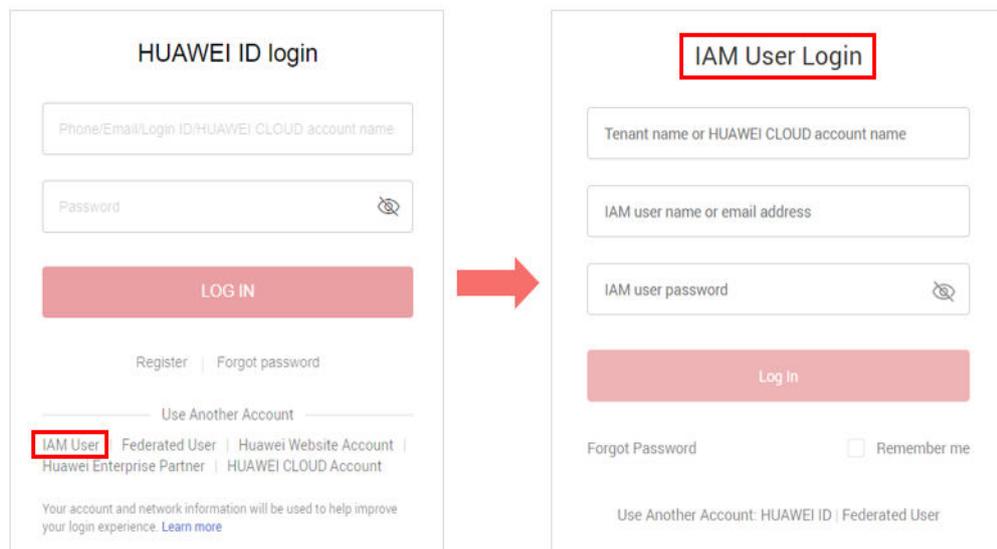
 **NOTA**

- 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 de nuvem somente por meio de acesso programático**, 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 a criação de um trabalho de migração de dados no console de Cloud Data Migration (CDM), selecione **Programmatic access** e **Management console access** para **Access Type** e **Access key** e **Password** para **Credential Type**.

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

Tipo de credencial e proteção de logon		Descrição
Access key		Depois de criar o usuário, você pode baixar a chave de acesso (AK/SK) gerada para o usuário. Cada usuário pode ter no máximo duas chaves de acesso.
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 de 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 escolher entre verificação de logon baseada em SMS, e-mail e MFA virtual.

Figura 3-4 Fazer logon como um usuário do IAM



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

Passo 2 Clique em **Log In**.

----Fim

4 História de mudanças

Tabela 4-1 História de mudanças

Lançado em	Descrição
30/11/2021	Esta edição é o décimo lançamento oficial, que incorpora a seguinte alteração: Modificação de seção 2 Etapa 1: criar grupos de usuários e atribuir permissões de acordo com a otimização da função de autorização.
02/09/2021	Esta edição é o nono lançamento oficial, que incorpora a seguinte alteração: Otimização de seção 2 Etapa 1: criar grupos de usuários e atribuir permissões de acordo com as alterações na função de gerenciamento de permissões.
27/03/2021	Esta edição é o oitavo lançamento oficial, que incorpora a seguinte alteração: Atualização do documento com base no novo recurso de logon do ID da HUAWEI.
30/12/2020	Esta edição é o sétimo lançamento oficial, que incorpora a seguinte alteração: Atualização do documento com base em alterações na página de logon, na função de configurações de segurança e nas cadeias da interface do usuário.
27/10/2020	Esta edição é o sexto lançamento oficial, que incorpora a seguinte alteração: Atualização das capturas de tela da página de logon com base na alteração do método de logon.

Lançado em	Descrição
08/06/2020	Esta edição é o quinto lançamento oficial, que incorpora a seguinte alteração: Atualização das seguintes seções para incluir descrições sobre o logon do ID da HUAWEI: 2 Etapa 1: criar grupos de usuários e atribuir permissões 3 Etapa 2: criar usuários do IAM e fazer logon
10/02/2020	Esta edição é o quarto lançamento oficial, que incorpora a seguinte alteração: Modificação de seção 2 Etapa 1: criar grupos de usuários e atribuir permissões com base nas alterações de nome da política.
19/01/2020	Esta edição é o terceiro lançamento oficial, que incorpora a seguinte alteração: Modificação de seção 2 Etapa 1: criar grupos de usuários e atribuir permissões com base nas alterações do console.
06/06/2019	Esta edição é o segundo lançamento oficial, que incorpora a seguinte alteração: Otimização das etapas para atribuição de permissões em 2 Etapa 1: criar grupos de usuários e atribuir permissões .
26/02/2019	Esta edição é o primeiro lançamento oficial.