# IAM

# Service Overview

**Edição** 01

**Data** 03-04-2023

**HUAWEI TECHNOLOGIES CO., LTD.**

### Marcas registadas e permissões


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

### Aviso

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

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

## Huawei Technologies Co., Ltd.

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

Site: https://www.huawei.com

Email: support@huawei.com

# Índice



# 1 Infográficos

# 2 O que é IAM?

O Gerenciamento de identidade e acesso (IAM) é um serviço básico da HUAWEI CLOUDque fornece gerenciamento de permissões para ajudá-lo a controlar com segurança o acesso aos seus serviços e recursos na nuvem.

O IAM é gratuito. Você paga apenas para recursos na nuvem em sua conta.

## Vantagens

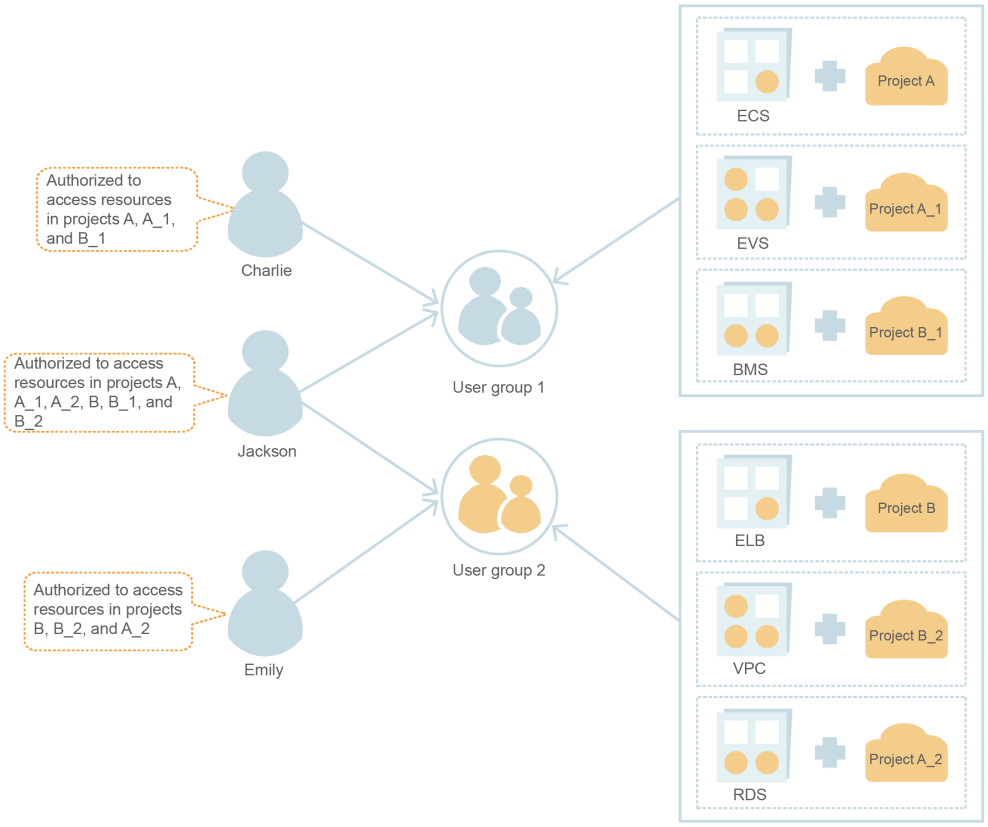
**Controle de acesso refinado para recursos da HUAWEI CLOUD**

Uma conta é criada depois de você se registrar com sucesso na HUAWEI CLOUD. Sua conta tem permissões de acesso total dos seus serviços e recursos na nuvem e efetuar pagamentos para uso desses recursos.

Se você comprar vários recursos na HUAWEI CLOUD como Elastic Cloud Servers (ECSs), Elastic Volume Services (EVSs) e Bare Metal Servers (BMSs), para diferentes equipes ou aplicações em sua empresa, você pode criar usuários do IAM para os membros da equipe ou aplicações e conceder a eles as permissões necessárias para concluir tarefas. Os usuários do IAM usam seus próprios nomes de usuário e senhas para fazer login na da HUAWEI CLOUD e acessar os recursos em sua conta.

Além do IAM, você pode usar o Enterprise Management para controlar o acesso aos recursos em nuvem. O Enterprise Management suporta o gerenciamento de permissões mais refinado e de projetos corporativos. Você pode escolher o IAM ou o Enterprise Management para atender às suas necessidades. Para obter detalhes, consulte **Quais são as diferenças entre o IAM e o Enterprise Management**

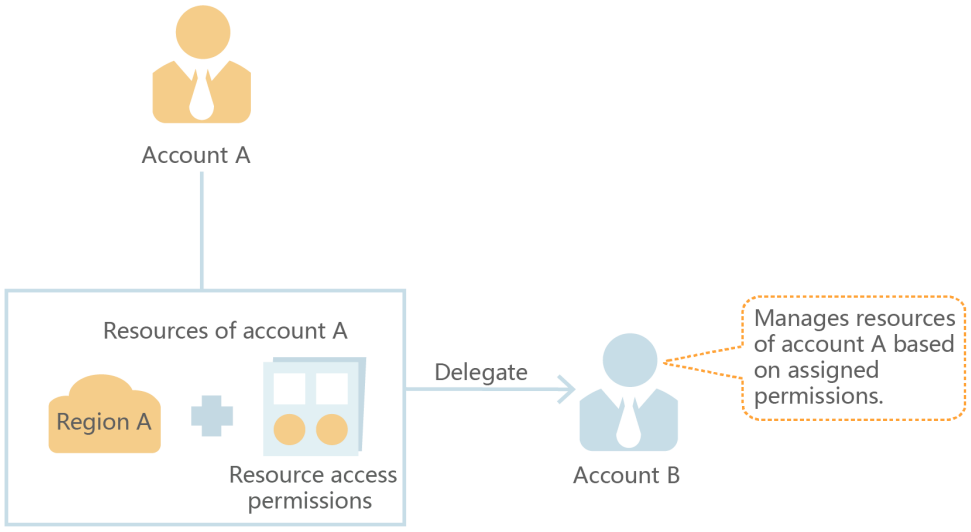
  




**Delegação de acesso a recursos entre contas**

Se você comprar vários recursos na HUAWEI CLOUD, poderá delegar outra conta para gerenciar recursos específicos para uma O&M eficiente.

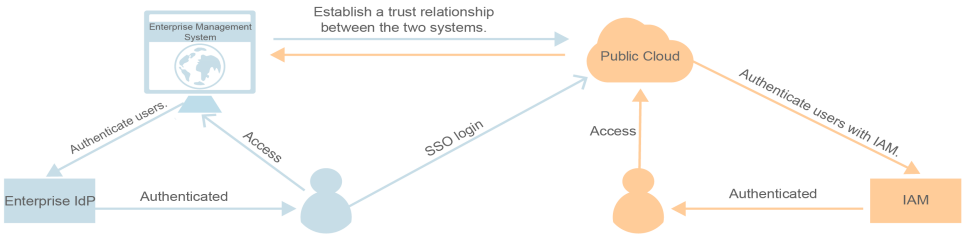
Por exemplo, você cria uma agência para uma empresa profissional de O&M para gerenciar recursos específicos com a própria conta da empresa. Você pode cancelar ou modificar as permissões delegadas em qualquer momento se a delegação for alterada. Na seguinte figura, a conta A é a parte delegante e a conta B é a parte delegada.



**Acesso federado à HUAWEI CLOUD com contas empresariais existentes**

Se sua empresa tiver um sistema de identidade, você poderá criar um provedor de identidade no IAM para fornecer acesso de logon único (SSO) à HUAWEI CLOUD para funcionários em sua empresa. O provedor de identidade estabelece uma relação de confiança entre sua empresa e a HUAWEI CLOUD, permitindo que os funcionários acessem a HUAWEI CLOUD usando suas contas existentes.




## Métodos de acesso

Você pode acessar o IAM usando um dos seguintes métodos:

- **Console de gerenciamento**

  Acesse o IAM por meio do console de gerenciamento – uma interface visual baseada em navegador. Para obter detalhes, consulte **Acessar o console do IAM**.

- **APIs REST**

  Acesse o IAM usando as APIs REST de maneira programável. Para obter detalhes, consulte **Referência API**.

# 3 Conceitos básicos

Você precisa entender os seguintes conceitos básicos antes de começar a usar o serviço IAM.

## Conta

Uma conta é criada depois de você se registrar com sucesso na HUAWEI CLOUD. Sua conta tem permissões de acesso total dos seus recursos na nuvem e efetuar pagamentos para uso desses recursos. Você pode usar a conta para redefinir senhas de usuário e atribuir permissões.

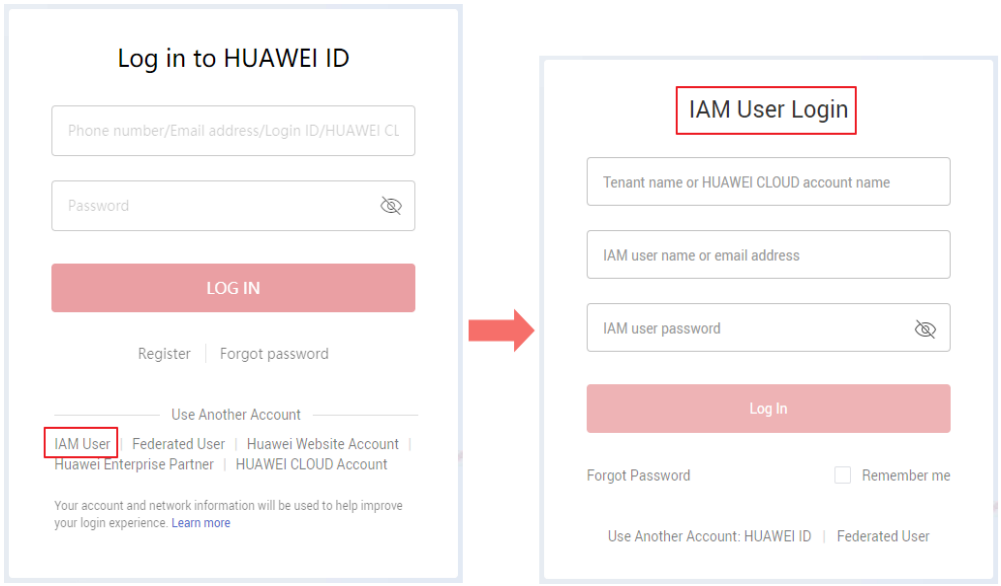
Você não pode modificar ou excluir sua conta no IAM, mas pode fazê-lo em Minha Conta.

## Usuário do IAM

Você pode usar sua conta para criar usuários do IAM e atribuir permissões para recursos específicos. Cada usuário do IAM tem suas próprias credenciais de identidade (senha e chaves de acesso) e usa recursos de nuvem com base nas permissões atribuídas. Os usuários do IAM não podem efetuar pagamentos. Você pode usar sua conta para pagar suas contas.

Se um usuário do IAM esquecer sua senha, o usuário poderá redefinir a senha consultando **O que posso fazer se minha senha for esquecida?**

**Figura 3-1** Login de usuários do IAM

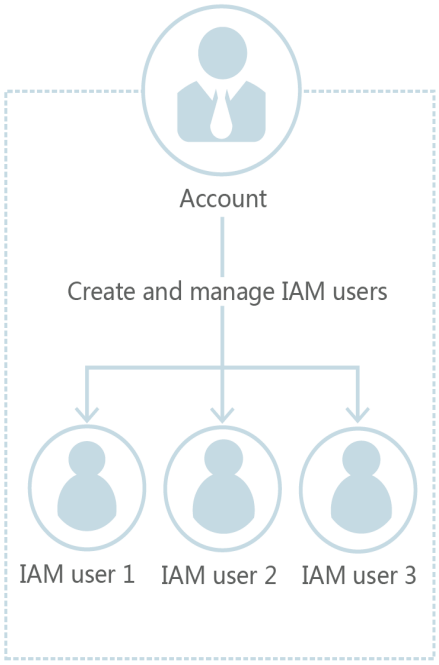


## Relação entre uma conta e seus usuários do IAM

Uma conta e seus usuários do IAM compartilham uma relação pai-filho. A conta é proprietária dos recursos e faz pagamentos dos recursos usados pelos usuários do IAM. Ele tem permissões completas para esses recursos. Os usuários do IAM são criados usando uma conta e têm apenas as permissões concedidas pela conta. O administrador da conta pode modificar ou cancelar as permissões dos usuários do IAM em qualquer momento.

**Figura 3-2** Conta e usuários do IAM




## Autorização

Autorização é o processo de conceder as permissões necessárias para que um usuário execute uma tarefa.

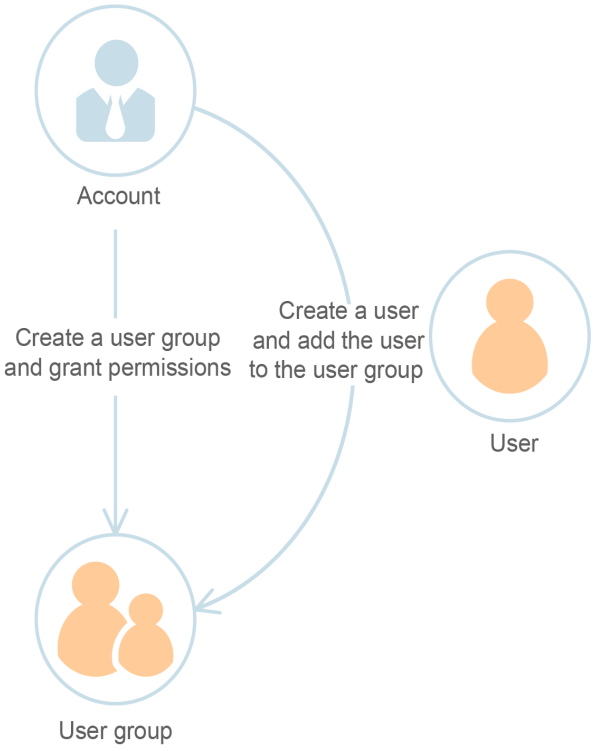
## Grupo de usuários

Você pode usar grupos de usuários para atribuir permissões a usuários do IAM. Os usuários do IAM adicionados a um grupo de usuários obtêm automaticamente as permissões atribuídas ao grupo. Se um usuário for adicionado a vários grupos de usuários, o usuário herdará as permissões atribuídas a todos esses grupos.

O **admin** do grupo de usuários padrão tem todas as permissões necessárias para usar todos os recursos na nuvem. Os usuários desse grupo podem executar operações em todos os recursos, incluindo, mas não limitado a, criar grupos de usuários e usuários, atribuir permissões e gerenciar recursos.

**Figura 3-3** Grupo de usuários e usuários



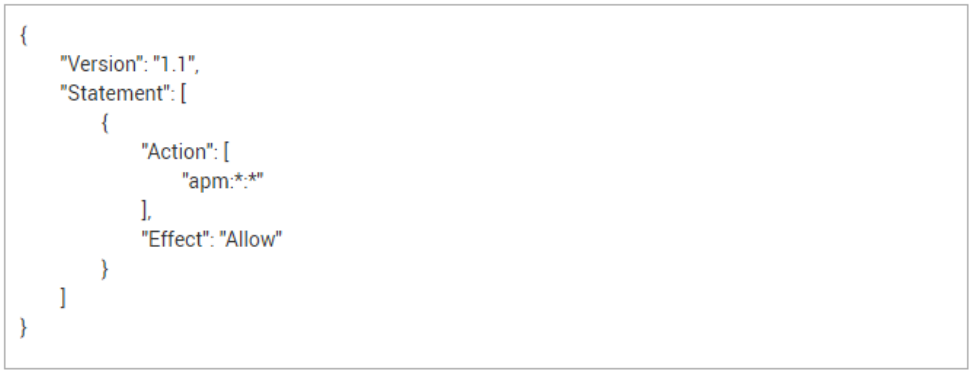

## Permissão

Você pode conceder permissões usando funções e políticas.

- Funções: Um tipo de mecanismo de autorização de granulação grosseira que define permissões em nível de serviço com base nas responsabilidades do usuário. Há apenas um número limitado de funções para conceder permissões aos usuários.
- Políticas: um tipo de mecanismo de autorização refinado que define as permissões necessárias para realizar operações em recursos de nuvem específicos sob determinadas condições. Esse mecanismo permite uma autorização baseada em política mais flexível e o controle de acesso seguro. Por exemplo, você pode conceder aos usuários ECS somente as permissões necessárias para gerenciar um determinado tipo de recursos ECS. O IAM oferece suporte a políticas definidas pelo sistema e personalizadas.
  - Uma **política definida pelo sistema** define as ações comuns de um serviço em nuvem. Políticas definidas pelo sistema podem ser usadas para atribuir permissões a grupos de usuários e não podem ser modificadas. Se você precisar atribuir permissões para um serviço específico a um grupo de usuários ou agência no console do IAM, mas não conseguir encontrar políticas correspondentes, isso indica que o serviço não oferece suporte ao gerenciamento de permissões via IAM.**Envie um ticket de serviço** e solicite que as permissões para o serviço sejam disponibilizadas no IAM.
  - Você pode criar **políticas personalizadas** usando as ações suportadas pelos serviços de nuvem e usar políticas personalizadas para complementar políticas definidas pelo sistema para um controle de acesso mais refinado. Você pode criar políticas personalizadas no editor visual ou na visualização JSON.

**Figura 3-4** Exemplo de permissões




## Credenciais

As credenciais confirmam a identidade de um usuário quando o usuário acessa a HUAWEI CLOUD através do console ou APIs. As credenciais incluem uma senha e chaves de acesso. Você pode gerenciar suas credenciais e as credenciais dos usuários do IAM que você criou.

- Senha: Uma credencial comum para fazer login no console de gerenciamento ou chamar as APIs.
- Chave de acesso: Um par de ID de chave de acesso/chave de acesso secreta (AK/SK), que só pode ser usado para chamar as APIs. Cada chave de acesso fornece uma assinatura para autenticação criptográfica para garantir que as solicitações de acesso sejam secretas, completas e corretas.

## Dispositivo MFA virtual

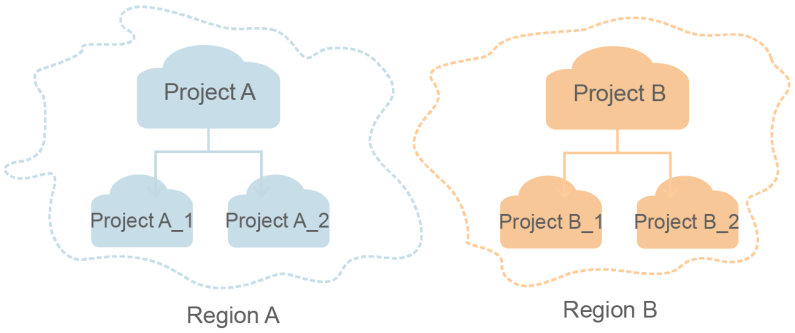
Um dispositivo MFA virtual é uma aplicação que gera códigos de verificação de 6 dígitos em conformidade com o padrão TOTP (One-time Password Algorithm) baseado em tempo. Os dispositivos MFA podem ser baseados em hardware ou software. Atualmente, a HUAWEI CLOUD suporta dispositivos MFA virtuais baseados em software, que são programas de aplicações executadas em dispositivos inteligentes, como celulares. Para obter detalhes sobre como usar dispositivos MFA virtual, consulte **Dispositivo MFA virtual**.

## Projeto

Uma região corresponde a um projeto. Os projetos padrão são definidos para agrupar e isolar fisicamente recursos (incluindo recursos de computação, armazenamento e rede) entre regiões. Você pode conceder permissões aos usuários em um projeto padrão para acessar todos os recursos na região associada ao projeto. Se precisar de um controlo de acesso mais refinado, pode criar subprojetos num projeto predefinido e comprar recursos em subprojetos. Em seguida, você pode atribuir permissões necessárias para que os usuários acessem apenas recursos em subprojetos específicos.

**Figura 3-5** Projeto




## Projeto empresarial

Os projetos empresariais permitem agrupar e gerenciar recursos entre regiões. Os recursos em projetos empresariais são logicamente isolados uns dos outros. Um projeto da empresa pode conter recursos de várias regiões e você pode facilmente adicionar recursos ou remover recursos de projetos empresariais.

Para obter detalhes sobre como obter os IDs e funcionalidades dos projetos empresariais, consulte **Guia de usuário do Enterprise Management**.

## Agência

Uma relação de confiança que pode estabelecer entre a sua conta e outra conta ou um serviço de nuvem para delegar o acesso a recursos.

- Delegação de conta: Você pode delegar outra conta para implementar O&M em seus recursos com base nas permissões atribuídas.
- Delegação de serviço de nuvem: serviços da HUAWEI CLOUD interagem um ao outro, e alguns serviços de nuvem dependem de outros serviços. Você pode criar uma agência para delegar um serviço de nuvem para acessar outros serviços.

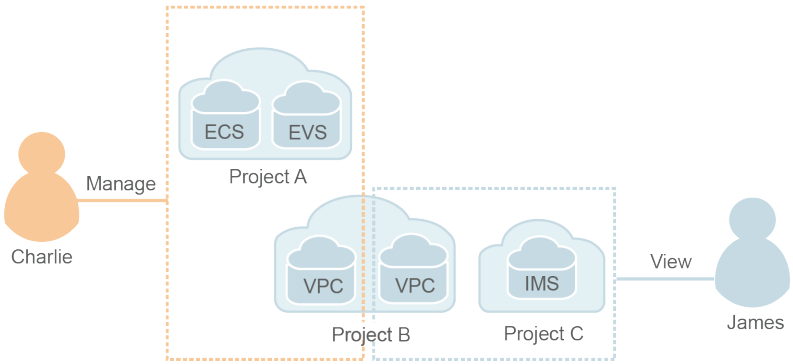
# 4 Funções

O IAM oferece as seguintes funções: gerenciamento de permissões refinado, acesso seguro, proteção de operação crítica, atribuição de permissões baseada em grupo de usuários, isolamento de recursos baseado em projeto, autenticação de identidade federada, delegação de gerenciamento de recursos e configurações de segurança da conta.

## Gerenciamento refinado de permissões

Você pode conceder permissões aos usuários do IAM para gerenciar diferentes recursos em sua conta. Por exemplo, o Charlie recebe apenas as permissões necessárias para gerenciar recursos de Virtual Private Cloud (VPC) no projeto B.

**Figura 4-1** Modelo de gerenciamento de permissões




## Acesso seguro

Em vez de compartilhar a senha da conta com outras pessoas, você pode criar usuários do IAM para funcionários ou aplicações em sua organização e gerar credenciais de identidade para que eles acessem em segurança recursos específicos baseados nas permissões atribuídas.

## Proteção de operação crítica

O IAM fornece proteção de login e operação crítica, tornando sua conta e seus recursos mais seguros. Quando você ou os usuários criados usando sua conta fazem login no console ou

executam uma operação crítica, você e os usuários precisam concluir a autenticação por e-mail, SMS ou dispositivo MFA virtual.

## Atribuição de permissões baseada em grupo de usuários

Com o IAM, você não precisa atribuir permissões a usuários únicos. Em vez disso, você pode gerenciar usuários por grupo e atribuir permissões ao grupo. Em seguida, cada usuário herda permissões dos grupos dos quais são membros. Para alterar as permissões de um usuário, você pode remover o usuário dos grupos originais ou adicionar o usuário a outros grupos.

## Isolamento de recursos baseado em projetos

Você pode criar subprojetos em uma região para isolar recursos.

## Autenticação de identidade federada

A função de autenticação de identidade federada permite que empresas com sistemas de autenticação de identidade acessema HUAWEI CLOUD por meio de logon único (SSO), eliminando a necessidade de criar usuários na HUAWEI CLOUD.

## Delegação de gerenciamento de recursos

Você pode delegar contas mais profissionais e eficientes ou outros serviços em nuvem para gerenciar recursos especificados.

## Configurações de segurança da conta

As políticas de autenticação e senha de login e a lista de controle de acesso (ACL) melhoram a segurança das informações do usuário e dos dados do sistema.

## Consistência eventual

Os resultados de suas operações de IAM, como a criação de usuários e grupos de usuários e a atribuição de permissões, podem não entrar em vigor imediatamente porque os dados são replicados em diferentes servidores nos centros dos dados na HUAWEI CLOUD em todo o mundo. Certifique-se de que os resultados da operação tenham efeito antes de executar qualquer outra operação que dependa deles.

# 5 Serviços em nuvem suportados

O IAM fornece autenticação de identidade e gerenciamento de permissões para outros serviços da HUAWEI CLOUD. Os usuários criados no IAM podem acessar esses serviços com base nas permissões atribuídas. Para obter todas as permissões dos serviços suportados pelo IAM, consulte **System Permissions**. **Para serviços que não são suportados pelo IAM, você só pode usar sua conta para acessar esses serviços.**

- Serviço: Nome de um serviço em nuvem que suporta o gerenciamento de permissões usando o IAM. **Clique no link no nome do serviço para exibir as permissões suportadas pelo serviço.**
- Escopo: a região onde um serviço tem permissões de acesso pode ser atribuída usando o IAM.
  - Região global: os serviços implantados sem especificar regiões físicas são chamados serviços globais. As permissões para esses serviços devem ser atribuídas na região global. Os usuários não precisam mudar de região quando acessam esses serviços.
  - Regiões específicas: os serviços implantados em regiões específicas são chamados serviços em nível de projeto. As permissões para esses serviços precisam ser atribuídas em regiões específicas e entrarão em vigor apenas para as regiões correspondentes. Os usuários precisam mudar para uma dessas regiões quando acessam os serviços.
- Painel: indica se um serviço oferece suporte ao gerenciamento de permissões usando o console do IAM.
- API: indica se um serviço oferece suporte ao gerenciamento de permissões usando as APIs.
- Agência: indica se um serviço pode ser delegado para acessar e gerenciar outros serviços em nuvem em seu nome.
- Política: indica se um serviço oferece suporte ao gerenciamento de permissões baseado em políticas. Uma política é um conjunto de permissões que define as operações que podem ser executadas em recursos de nuvem específicos.
- Projeto empresarial: Indica se um serviço suporta autorização por projeto empresarial. Para obter detalhes sobre projetos empresariais, consulte **Guia de usuário do Enterprise Management**.

NOTA

√: suportado; x: não suportado

## Computação

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Elastic Cloud Server (ECS) | Regiões específicas | √ | √ | √ | √ | √ |
| Bare Metal Server (BMS) | Regiões específicas | √ | √ | √ | √ | √ |
| Auto Scaling (AS) | Regiões específicas | √ | √ | X | √ | √ |
| Cloud Phone (CPH) | Regiões específicas | √ | √ | X | X | X |
| Image Management Service (IMS) | Regiões específicas | √ | √ | √ | √ | √ |
| FunctionGraph | Regiões específicas | √ | √ | √ | X | √ |
| Dedicated Host (DeH) | Regiões específicas | √ | X | X | √ | √ |

## Armazenamento

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Elastic Volume Service (EVS) | Regiões específicas | √ | √ | X | √ | √ |
| Storage Disaster Recovery Service (SDRS) | Regiões específicas | √ | √ | X | X | X |
| Serviço de backup de servidor na nuvem (CSBS) | Regiões específicas | √ | √ | X | X | X |
| Volume Backup Service (VBS) | Regiões específicas | √ | √ | X | X | X |
| Object Storage Service (OBS) | Global | √ | √ | √ | √ | √ |
| Scalable File Service (SFS) | Regiões específicas | √ | √ | X | √ | √ |

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Content Delivery Network (CDN) | Global | √ | √ | X | √ | √ |
| Cloud Backup and Recovery (CBR) | Regiões específicas | √ | √ | X | √ | √ |

## Rede

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Virtual Private Cloud (VPC) | Regiões específicas | √ | √ | X | √ | √ |
| Elastic Load Balance (ELB) | Regiões específicas | √ | √ | X | √ | √ |
| Domain Name Service (DNS) | Global | √ | √ | X | X | √ |
| NAT Gateway | Regiões específicas | √ | √ | X | √ | √ |
| Direct Connect | Regiões específicas | √ | X | X | X | X |
| Virtual Private Network (VPN) | Regiões específicas | √ | X | X | √ | X |
| Cloud Connect (CC) | Regiões específicas | √ | X | X | √ | √ |
| VPC Endpoint (VPCEP) | Regiões específicas | √ | √ | X | X | X |

## Contêineres

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Cloud Container Engine (CCE) | Regiões específicas | √ | √ | X | √ | √ |

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Cloud Container Instance (CCI) | Regiões específicas | √ | √ | X | √ | √ |
| Software Repository for Container (SWR) | Regiões específicas | √ | √ | X | √ | X |
| Gene Container Service (GCS) | Regiões específicas | √ | √ | X | √ | √ |

## Banco de dados

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Relational Database Service (RDS) | Regiões específicas | √ | √ | X | √ | √ |
| Document Database Service (DDS) | Regiões específicas | √ | X | X | √ | √ |
| Distributed Database Middleware (DDM) | Regiões específicas | √ | √ | X | √ | √ |
| Data Replication Service (DRS) | Regiões específicas | √ | √ | X | √ | √ |
| Data Admin Service (DAS) | Regiões específicas | √ | X | X | X | X |
| GaussDB NoSQL | Regiões específicas | √ | √ | X | √ | √ |

## Segurança e conformidade

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Anti-DDoS | Regiões específicas | √ | √ | X | X | X |

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Advanced Anti-DDoS (AAD) | Regiões específicas | √ | √ | √ | X | √ |
| Cloud Native Anti-DDoS (CNAD) | Global | √ | √ | X | √ | X |
| Web Application Firewall (WAF) | Regiões específicas | √ | X | X | X | √ |
| Cloud Firewall (CFW) | Regiões específicas | √ | X | X | √ | X |
| Vulnerability Scan Service (VSS) | Regiões específicas | √ | X | X | X | X |
| Host Security Service (HSS) | Regiões específicas | √ | X | X | X | √ |
| Database Security Service (DBSS) | Regiões específicas | √ | X | X | √ | X |
| Data Encryption Workshop (DEW) | Regiões específicas | √ | √ | X | X | X |
| Managed Detection and Response (MDR) | Regiões específicas | √ | X | X | X | X |
| SSL Certificate Manager (SCM) | Global | √ | √ | X | √ | X |
| Container Guard Service (CGS) | Regiões específicas | √ | X | X | √ | X |
| Situation Awareness (SA) | Global | √ | √ | √ | √ | X |
| Cloud Bastion Host (CBH) | Regiões específicas | √ | √ | X | √ | X |
| Data Security Center (DSC) | Regiões específicas | √ | √ | X | √ | X |

## Gerenciamento e governança

| Serviço | Escopo | Console | API | Agência | Política refinada | Projeto empresarial |
|---|---|---|---|---|---|---|
| Identity and Access Management (IAM) | Global | √ | √ | X | √ | X |
| Cloud Eye | Regiões específicas | √ | √ | X | X | √ |
| Cloud Trace Service (CTS) | Regiões específicas | √ | √ | X | X | X |
| Application Performance Management (APM) | Regiões específicas | √ | √ | X | √ | √ |
| Application Operations Management (AOM) | Regiões específicas | √ | √ | X | √ | √ |
| Log Tank Service (LTS) | Regiões específicas | √ | √ | X | √ | √ |
| Tag Management Service (TMS) | Global | √ | √ | X | X | X |

## Aplicação

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| ServiceStage | Regiões específicas | √ | √ | X | X | X |
| Distributed Cache Service (DCS) | Regiões específicas | √ | √ | X | √ | √ |
| Distributed Message Service (DMS) | Regiões específicas | √ | √ | √ | √ | √ |
| Distributed Message Service for Kafka (DMS for Kafka) | Regiões específicas | √ | √ | X | √ | √ |

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Distributed Message Service for RabbitMQ (DMS for RabbitMQ) | Regiões específicas | √ | √ | X | √ | √ |
| Distributed Message Service for RocketMQ (DMS for RocketMQ) | Regiões específicas | √ | √ | X | √ | √ |
| Simple Message Notification (SMN) | Regiões específicas | √ | √ | X | X | √ |
| Cloud Service Engine (CSE) | Regiões específicas | √ | √ | X | X | √ |
| Cloud Performance Test Service (CPTS) | Regiões específicas | √ | √ | X | X | X |
| API Gateway | Regiões específicas | √ | √ | X | X | √ |
| Blockchain Service (BCS) | Regiões específicas | √ | √ | X | √ | √ |

## DeC

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Dedicated Distributed Storage Service (DSS) | Regiões específicas | √ | √ | X | √ | X |

## Migração

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Server Migration Service (SMS) | Global | √ | X | X | √ | X |

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Object Storage Migration Service (OMS) | Regiões específicas | √ | X | X | X | X |
| Cloud Data Migration (CDM) | Regiões específicas | √ | √ | √ | √ | √ |

## Borda inteligente

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| EdgeCloud Inteligente (IEC) | Global | √ | X | X | √ | X |

## Inteligência empresarial

| Serviço | Escopo | Console | API | Agência | Política refinada | Projeto empresarial |
|---|---|---|---|---|---|---|
| ModelArts | Regiões específicas | √ | √ | √ | √ | √ |
| Data Lake Governance Center (DGC) | Regiões específicas | √ | √ | √ | √ | X |
| MapReduce Service (MRS) | Regiões específicas | √ | √ | X | √ | √ |
| Data Warehouse Service (DWS) | Regiões específicas | √ | √ | √ | √ | √ |
| CloudTable | Regiões específicas | √ | √ | X | X | √ |
| Data Lake Insight (DLI) | Regiões específicas | √ | √ | X | X | √ |
| Data Ingestion Service (DIS) | Regiões específicas | √ | √ | √ | X | √ |

| Serviço | Escopo | Console | API | Agência | Política refinada | Projeto empresarial |
|---|---|---|---|---|---|---|
| Cloud Search Service (CSS) | Regiões específicas | √ | √ | √ | X | √ |
| Graph Engine Service (GES) | Regiões específicas | √ | √ | √ | X | √ |
| Recommender System (RES) | Regiões específicas | √ | √ | X | √ | √ |
| Moderação de conteúdo | Regiões específicas | √ | √ | X | √ | X |
| Conversational Bot Service (CBS) | Regiões específicas | √ | √ | X | X | X |
| Huawei HiLens | Regiões específicas | √ | X | X | √ | X |
| Trusted Intelligent Computing Service (TICS) | Regiões específicas | √ | X | X | √ | X |

## Aplicações empresariais

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Workspace | Regiões específicas | √ | √ | x | × | x |
| ROMA Connect | Regiões específicas | √ | √ | √ | √ | √ |
| CloudSite | Regiões específicas | √ | X | √ | √ | X |

## Comunicações em nuvem

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Voice Call | Regiões específicas | √ | √ | √ | X | X |
| Message & SMS | Regiões específicas | √ | √ | √ | X | X |
| Número privado | Regiões específicas | √ | √ | √ | √ | X |

## Vídeo

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Media Processing Center (MPC) | Regiões específicas | √ | √ | √ | X | X |
| Video on Demand (VOD) | Regiões específicas | √ | √ | √ | √ | X |

## Devolvimento e O&M

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| DevCloud | Regiões específicas | √ | X | X | √ | √ |
| ProjectMan | Regiões específicas | √ | √ | X | √ | X |
| CloudIDE | Regiões específicas | √ | √ | X | √ | X |

## Suporte para usuários

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| My Account | Regiões específicas | √ | X | X | √ | X |
| Billing Center | Regiões específicas | √ | X | X | √ | X |
| Resource Center | Regiões específicas | √ | X | X | √ | X |
| Enterprise Management | Global | √ | √ | X | √ | X |
| Service Tickets | Global | √ | √ | X | X | X |
| ICP License Service | Global | √ | X | X | X | X |
| Professional Services | Global | √ | X | X | √ | X |

## Outros

| Serviço | Escopo | Console | API | Agência | Política | Projeto empresarial |
|---|---|---|---|---|---|---|
| Message Center | Regiões específicas | √ | X | X | √ | X |

# 6 Mecanismo de proteção de dados pessoais

Para evitar que dados pessoais, como nome de usuário, senha e número de celular, sejam acessados por entidades ou indivíduos não autorizados, o IAM criptografa os dados antes de armazená-los. O IAM também controla o acesso aos dados e registra todas as operações realizadas nos dados.

## Dados pessoais

Tabela 6-1 lista os dados pessoais gerenciados ou recolhidos pelo IAM.

**Tabela 6-1** Dados pessoais

| Tipo | Origem | Modificável | Obrigatório |
| --- | --- | --- | --- |
| Nome de usuário. | ● Inserido quando você cria um usuário no console de gerenciamento.<br>● Inserido quando você chama uma API. | Não | Sim<br>Os nomes de usuário são usados para identificar usuários. |
| Senha | ● Inserido quando você cria um usuário, modifica credenciais de usuário ou redefine a senha no console de gerenciamento.<br>● Inserido quando você chama uma API. | Sim | Não<br>Você também pode escolher a autenticação AK/SK. |
| Endereço de e-mail | Inserido quando você cria um usuário, modifica credenciais de usuário ou altera o endereço de e-mail no console de gerenciamento. | Sim | Não |
| Número de celular | Inserido quando você cria um usuário, modifica credenciais de usuário ou altera o número de celular no console de gerenciamento. | Sim | Não |

| Tipo | Origem | Modificável | Obrigatório |
| --- | --- | --- | --- |
| AK/SK | Criado na página **My Credentials** ou no console do IAM. | Não<br>As AK/SK não podem ser modificadas, mas podem ser excluídas e criadas novamente. | Não<br>As AK/SK são usadas para assinar as solicitações enviadas para chamar as APIs. |

## Armazenamento de dados pessoais

O IAM usa algoritmos de encriptação para criptografar os dados do usuário antes de armazená-los.

- Nomes de usuário e AKs: dados não sensíveis, que são armazenados em texto não criptografado.
- Senhas, endereços de e-mail, números de celular e SKs: dados sensíveis, que são criptografados antes do armazenamento.

## Controle de acesso

Os dados pessoais são armazenados no banco de dados do IAM após serem criptografados. O acesso ao banco de dados é controlado através do mecanismo da lista de permissões.

## Autenticação MFA

Você pode habilitar a proteção de login e a proteção de operação crítica escolhendo **Security Settings** > **Critical Operations**. Se você habilitar essas funções, os usuários em sua conta devem verificar sua identidade via SMS, e-mail ou dispositivo MFA virtual antes de fazer login ou executar uma operação crítica.

## Restrições API

- A autenticação AK/SK é necessária para chamar as APIs. Você pode criar uma chave de acesso (AK/SK) e baixar o arquivo que contém a chave de acesso. Se você não conseguir localizar o arquivo, poderá criar uma chave de acesso novamente e baixar o arquivo. Não partilhe a sua chave de acesso.
- O IAM não fornece as APIs para consultas em lote e modificação de dados pessoais.

## Logs de operação

O IAM registra todas as operações de dados pessoais, incluindo adição, modificação, consulta e exclusão de dados pessoais. Ele carrega logs de operação para o CTS e permite que os usuários consultem apenas seus próprios logs de operação.

# 7 Gerenciamento de permissões

Se você precisar atribuir permissões diferentes para o IAM aos funcionários da sua organização, o IAM é uma boa opção para o gerenciamento de permissões refinado. O IAM fornece autenticação de identidade, gerenciamento de permissões e controle de acesso, ajudando você a proteger o acesso aos seus recursos da HUAWEI CLOUD.

Com o IAM, você pode criar usuários do IAM em sua conta e atribuir permissões a esses usuários para controlar seu acesso a recursos específicos. Por exemplo, você pode conceder permissões para permitir que determinados planejadores de projeto em sua empresa visualizem dados do IAM, mas não permitir que eles executem operações de alto risco, por exemplo, excluir usuários e projetos do IAM. Para obter todas as permissões dos serviços suportados pelo IAM, consulte **Permissões do sistema**.

## Permissões IAM

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

O IAM é um serviço global que você pode acessar de todas as regiões. Você pode atribuir permissões do IAM a usuários no projeto de serviço global. Dessa forma, os usuários não precisam mudar de região quando acessam o IAM.

Você pode conceder permissões usando funções e políticas.

- Funções: Um tipo de mecanismo de autorização de granulação grosseira que define permissões em nível de serviço com base nas responsabilidades do usuário. Há apenas um número limitado de funções para conceder permissões aos usuários. Quando você concede permissões usando funções, também precisa atribuir funções de dependência.
- Políticas: um tipo de mecanismo de autorização refinado que define as permissões necessárias para realizar operações em recursos de nuvem específicos sob determinadas condições. Esse mecanismo permite uma autorização baseada em política mais flexível e o controle de acesso seguro. Por exemplo, você pode conceder aos usuários ECS somente as permissões necessárias para gerenciar um determinado tipo de recursos ECS. A maioria das políticas contém permissões para APIs específicas, e as permissões são definidas usando ações da API. Para as ações API suportadas pelo IAM, consulte **Permissões e ações suportadas**.

**Tabela 7-1** lista todas as funções e políticas definidas pelo sistema suportadas pelo IAM.

**Tabela 7-1** Funções e políticas definidas pelo sistema suportadas pelo IAM

| Nome da função/política | Descrição | Tipo | Conteúdo |
|---|---|---|---|
| FullAccess | Permissões completas para todos os serviços que suportam autorização baseada em política. Os usuários com essas permissões podem executar operações em todos os serviços. | Política definida pelo sistema | **Conteúdo da Política de FullAccess** |
| IAM ReadOnlyAccess | Permissões somente leitura para o IAM. Os usuários com essas permissões só podem ver dados do IAM. | Política definida pelo sistema | **Conteúdo da Política de IAM ReadOnlyAccess** |
| Security Administrator | Administrador do IAM com permissões completas, incluindo permissões para criar e excluir usuários do IAM. | Função definida pelo sistema | **Conteúdo da Função de Security Administrator** |
| Agent Operator | Operador do IAM (parte delegada) com permissões para alternar funções e acessar recursos de uma parte delegante. | Função definida pelo sistema | **Conteúdo da Função de Agent Operator** |
| Tenant Guest | Permissões somente leitura para todos os serviços, exceto o IAM. | Política definida pelo sistema | **Conteúdo da Função de Tenant Guest** |
| Tenant Administrator | Permissões de administrador para todos os serviços, exceto o IAM. | Política definida pelo sistema | **Conteúdo da Função de Tenant Administrator** |

Tabela 7-2 lista as operações comuns suportadas por cada política definida pelo sistema ou função do IAM. Escolha políticas ou funções apropriadas, conforme necessário.

NOTA

**Tenant Guest** e **Tenant Administrator** são funções básicas fornecidas pelo IAM e não contêm permissões específicas do IAM. Portanto, as duas funções não estão listadas na seguinte tabela.

**Tabela 7-2** Operações comuns suportadas por políticas ou funções definidas pelo sistema

| Operação | Security Administrator | Agent Operator | FullAccess | IAM ReadOnlyAccess |
|---|---|---|---|---|
| Criação de usuários do IAM | Sim | Não | Sim | Não |

| Operação | Security Administrator | Agent Operator | FullAccess | IAM ReadOnlyAccess |
|---|---|---|---|---|
| Consulta dos detalhes do usuário do IAM | Sim | Não | Sim | Sim |
| Modificação das informações do usuário do IAM | Sim | Não | Sim | Não |
| Consulta das configurações de segurança dos usuários do IAM | Sim | Não | Sim | Sim |
| Modificação das configurações de segurança de usuários do IAM | Sim | Não | Sim | Não |
| Exclusão de usuários do IAM | Sim | Não | Sim | Não |
| Criação dos grupos de usuários | Sim | Não | Sim | Não |
| Consulta dos detalhes do grupo de usuários | Sim | Não | Sim | Sim |
| Modificação das informações do grupo de usuários | Sim | Não | Sim | Não |
| Adição dos usuários a grupos de usuários | Sim | Não | Sim | Não |

| Operação | Security Administrator | Agent Operator | FullAccess | IAM ReadOnlyAccess |
|---|---|---|---|---|
| Remoção dos usuários de grupos de usuários | Sim | Não | Sim | Não |
| Eliminação dos grupos de usuários | Sim | Não | Sim | Não |
| Atribuição de permissões a grupos de usuários | Sim | Não | Sim | Não |
| Remoção de permissões de grupos de usuários | Sim | Não | Sim | Não |
| Criação de políticas personalizadas | Sim | Não | Sim | Não |
| Modificação de políticas personalizadas | Sim | Não | Sim | Não |
| Exclusão de políticas personalizadas | Sim | Não | Sim | Não |
| Consulta de detalhes da permissão | Sim | Não | Sim | Sim |
| Criação de agências | Sim | Não | Sim | Não |
| Consulta de agências | Sim | Não | Sim | Sim |
| Modificação de agências | Sim | Não | Sim | Não |
| Alternação de funções | Não | Sim | Sim | Não |
| Exclusão de agências | Sim | Não | Sim | Não |

| Operação | Security Administrator | Agent Operator | FullAccess | IAM ReadOnlyAccess |
|---|---|---|---|---|
| Concessão de permissões a agências | Sim | Não | Sim | Não |
| Remoção de permissões de agências | Sim | Não | Sim | Não |
| Criação dos projetos | Sim | Não | Sim | Não |
| Consulta dos projetos | Sim | Não | Sim | Sim |
| Modificação dos projetos | Sim | Não | Sim | Não |
| Exclusão dos projetos | Sim | Não | Sim | Não |
| Criação dos provedores de identidade | Sim | Não | Sim | Não |
| Importação dos arquivos de metadados | Sim | Não | Sim | Não |
| Consulta dos arquivos de metadados | Sim | Não | Sim | Sim |
| Consulta dos provedores de identidade | Sim | Não | Sim | Sim |
| Consulta dos protocolos | Sim | Não | Sim | Sim |
| Consulta dos mapeamentos | Sim | Não | Sim | Sim |
| Atualização dos provedores de identidade | Sim | Não | Sim | Não |
| Atualização dos protocolos | Sim | Não | Sim | Não |
| Atualização dos mapeamentos | Sim | Não | Sim | Não |

| Operação | Security Administrator | Agent Operator | FullAccess | IAM ReadOnlyAccess |
|---|---|---|---|---|
| Exclusão dos provedores de identidade | Sim | Não | Sim | Não |
| Exclusão dos protocolos | Sim | Não | Sim | Não |
| Exclusão dos mapeamentos | Sim | Não | Sim | Não |
| Consulta de cotas | Sim | Não | Sim | Não |

Somente administradores podem gerenciar chaves de acesso quando **chaves de acesso de gerenciamento** está habilitado. Se os usuários do IAM precisarem criar, habilitar, desabilitar ou excluir suas próprias chaves de acesso, eles precisarão pedir o administrador para **desabilitar o gerenciamento de chaves de acesso** O gerenciamento de chaves de acesso é desabilitado por padrão.

Se um usuário do IAM quiser gerenciar as chaves de acesso de outros usuários do IAM, consulte a **Tabela 3**. Por exemplo, se o usuário do IAM A quiser criar uma chave de acesso para o usuário do IAM B, o usuário do IAM A deve ter a permissão Security Administrator ou FullAccess.

**Tabela 7-3** Operações de chave de acesso suportadas por políticas ou funções definidas pelo sistema

| Operação | Security Administrator | Agent Operator | FullAccess | IAM ReadOnlyAccess |
|---|---|---|---|---|
| Criação das chaves de acesso (para outros usuários do IAM) | Sim | Não | Sim | Não |
| Consulta das chaves de acesso (para outros usuários do IAM) | Sim | Não | Sim | Sim |
| Modificação das chaves de acesso (para outros usuários do IAM) | Sim | Não | Sim | Não |

| Operação | Security Administrator | Agent Operator | FullAccess | IAM ReadOnlyAccess |
| --- | --- | --- | --- | --- |
| Exclusão das chaves de acesso (para outros usuários do IAM) | Sim | Não | Sim | Não |

## Conteúdo da Política de FullAccess

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

## Conteúdo da Política de IAM ReadOnlyAccess

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

## Conteúdo da Função de Security Administrator

```
{
    "Version": "1.0",
    "Statement": [
        {
            "Action": [
                "iam:agencies:*",
                "iam:credentials:*",
                "iam:groups:*",
                "iam:identityProviders:*",
                "iam:mfa:*",
                "iam:permissions:*",
                "iam:projects:*",
                "iam:quotas:*",
                "iam:roles:*",
                "iam:users:*",
                "iam:securitypolicies:*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

## Conteúdo da Função de Agent Operator

```
{
    "Version": "1.0",
    "Statement": [
        {
            "Action": [
                "iam:tokens:assume"
            ],
            "Effect": "Allow"
        }
    ]
}
```

## Conteúdo da Função de Tenant Guest

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

## Conteúdo da Função de Tenant Administrator

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

```
    ]
}
```

# 8 Segurança



## 8.1 Responsabilidades compartilhadas

Huawei garante que seu compromisso com a segurança cibernética nunca será superado pela consideração de interesses comerciais. Para lidar com os desafios emergentes de segurança na nuvem e ameaças e ataques à segurança na nuvem, a Huawei Cloud constrói um sistema abrangente de garantia de segurança de serviços em nuvem para diferentes regiões e indústrias com base nas vantagens exclusivas de software e hardware da Huawei, leis, regulamentos, padrões da indústria e ecossistema de segurança.

**Figura 8-1** ilustra as responsabilidades partilhadas pela Huawei Cloud e pelos usuários.

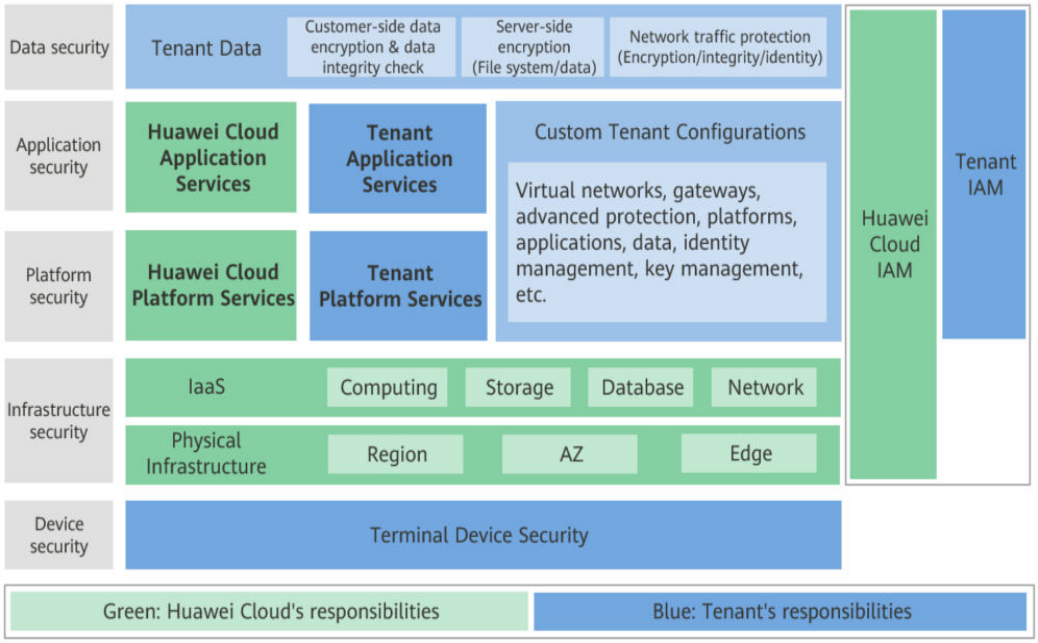
- **Huawei Cloud**: garante a segurança dos serviços de nuvem e fornece nuvens seguras. As responsabilidades de segurança da Huawei Cloud incluem garantir a segurança de nossos serviços de IaaS, PaaS e SaaS, bem como os ambientes físicos dos data centers da Huawei Cloud onde nossos serviços de IaaS, PaaS e SaaS operam. A Huawei Cloud é responsável não apenas pelas funções de segurança e pelo desempenho de nossa infraestrutura, serviços de nuvem e tecnologias, mas também pela segurança geral de O&M na nuvem e, no sentido mais amplo, pela certificação de segurança de nossa infraestrutura e serviços.
- **Locatário**: usa a nuvem com segurança. Os locatários da Huawei Cloud são responsáveis pelo gerenciamento seguro e eficaz das configurações personalizadas dos serviços em nuvem, incluindo IaaS, PaaS e SaaS. Isso inclui, mas não se limita a, redes virtuais, o SO de hosts e convidados de máquinas virtuais, firewalls virtuais, API Gateway, serviços avançados de segurança, todos os tipos de serviços em nuvem, dados de locatários, contas de identidade e gerenciamento de chaves.

**O livro branco de segurança da Huawei Cloud** elabora as ideias e medidas para a construção da segurança da Huawei Cloud, incluindo estratégias de segurança na nuvem, o

modelo de responsabilidade compartilhada, conformidade e privacidade, organizações e pessoal de segurança, segurança de infraestrutura, serviço e segurança de locatários, segurança de engenharia, segurança de O&M e segurança do ecossistema.

**Figura 8-1** Modelo de responsabilidade de segurança compartilhada da Huawei Cloud




# 8.2 Autenticação e controle de acesso

## 8.2.1 Autenticação de identificação

O serviço IAM exige que o solicitante de acesso apresente a credencial de identidade e verifique a validade da identidade. Além disso, o serviço IAM fornece proteção de login e políticas de verificação de login para fortalecer a segurança da autenticação de identidade.

### Credenciais de identidade e sua segurança

O IAM pode ser acessado usando contas e usuários do IAM. Ambos suportam autenticação de identidade usando nomes de usuário, senhas, chaves de acesso e chaves de acesso temporárias. Para obter detalhes, consulte **Tabela 8-1**. O IAM implementa o design de segurança para cada credencial de identidade para proteger os dados do usuário e permitir que os usuários acessem o IAM com mais segurança.

**Tabela 8-1** Credenciais de identidade do IAM e design de segurança

| Credenciais de acesso | Descrição de segurança | Referência |
| --- | --- | --- |
| Nome de usuário e senha | Você pode configurar o tipo de caractere e o comprimento mínimo de uma chave de usuário, conforme necessário. Você pode igualmente configurar a política do período de validade da senha e a política do período mínimo de validade da senha. | **Política de senha** |
| Chave de acesso | A AK é usada em conjunto com a SK para assinar solicitações criptograficamente, garantindo que as solicitações sejam secretas, completas e corretas. | **Chaves de acesso** |
| Chave de acesso temporária | Além do recurso de chave de acesso, a chave de acesso temporária tem um período de validade. Você pode definir o período de validade. Após a expiração do período de validade, a chave de acesso temporária não pode ser usada novamente e só pode ser obtida novamente. | **Chave de acesso temporária (para usuários federados)** |

## Políticas de proteção de login e autenticação de login

Como mostrado em **Tabela 8-2**, além de exigir que os usuários mostrem credenciais e verifiquem sua validade durante o login, o IAM também fornece um mecanismo de proteção de login e suporta políticas de verificação de login para evitar que as informações do usuário sejam roubadas.

**Tabela 8-2** Políticas de proteção de login e autenticação de login

| Método de proteção de login | Descrição | Funções |
| --- | --- | --- |
| Proteção de login | Além de inserir o nome de usuário e a senha na página de login (autenticação pela primeira vez), você precisa inserir um código de verificação na página Verificação de Login (autenticação pela segunda vez).<br>Verifique se os números de celular, endereços de e-mail e dispositivos MFA virtuais são suportados. Para obter detalhes, consulte **Autenticação MFA**. | **Proteção de login** |
| Política de autenticação de acesso | O IAM suporta a política de **tempo limite de sessão**. Se um usuário não fizer login no sistema dentro de um período especificado, ele precisará fazer login novamente. O IAM suporta a política de **bloqueio de conta**. Se o número de falhas de login exceder o limite, a conta será bloqueada. O IAM suporta a política de **desabilitação de conta**. Se um usuário não fizer login no sistema por um longo tempo, a conta será desabilitada. O IAM suporta a exibição de **informações de login recentes** para permitir que os usuários visualizem a hora do último login. | **Política de autenticação de login** |

## 8.2.2 Configuração do controle de acesso

O IAM usa políticas de autorização refinadas e ACLs para controlar o acesso.

**Tabela 8-3** Controle de acesso ao IAM

| Política de acesso | Descrição | Referência |
| --- | --- | --- |
| Política de autorização refinada do IAM | As permissões de serviço do IAM são divididas em funções ou permissões refinadas. As funções e as políticas definem que as operações de usuário são permitidas ou rejeitadas pelo IAM. Por exemplo, se um usuário ou grupo de usuários tiver a permissão ReadOnlyAccess do IAM, o usuário ou grupo de usuários terá apenas a permissão somente leitura nos dados de serviço do IAM. O IAM também suporta **políticas personalizadas** para atribuir permissões de serviço do IAM. | **Permissões IAM** |
| ACL | Definir políticas de controle de acesso para permitir que os usuários façam login no console do IAM ou abram APIs somente a partir de intervalos de endereços IP, segmentos de rede e pontos de extremidade VPC especificados. | **ACL** |

# 8.3 Proteção de dados

## 8.3.1 Lado IAM

Para garantir que seus dados pessoais, como nome de usuário, senha e número de celular, não sejam obtidos por entidades ou indivíduos não autorizados ou não autenticados, o IAM criptografa seus dados durante o armazenamento e a transmissão para evitar vazamento de dados.

### Dados pessoais

**Tabela 8-4** lista os dados pessoais gerenciados ou recolhidos pelo IAM.

**Tabela 8-4** Dados pessoais

| Tipo | Origem | Descrição | Modificável | Obrigatório |
|---|---|---|---|---|
| Nome de usuário. | ● Inserido quando você cria um usuário no console de gerenciamento.<br>● Inserido quando você chama uma API. | ● Identificação de identidade do usuário<br>● Autenticação de identidade durante a interface do console ou chamada API | Os direitos de administrador podem ser modificados através da API. | Sim<br>Os nomes de usuário são usados para identificar usuários. |
| Senha | ● Inserido quando você cria um usuário, modifica credenciais de usuário ou redefine a senha no console de gerenciamento.<br>● Inserido quando você chama uma API. | Autenticação de identidade durante a interface do console ou chamada API | Sim | Não<br>Você também pode escolher a autenticação AK/SK. |
| Endereço de e-mail | Inserido quando você cria um usuário, modifica credenciais de usuário ou altera o endereço de e-mail no console de gerenciamento. | ● Identificação de identidade do usuário<br>● Autenticação de identidade no console<br>● Receção de uma mensagem | Sim | Não |
| Número de celular | Inserido quando você cria um usuário, modifica credenciais de usuário ou altera o número de celular no console de gerenciamento. | ● Identificação de identidade do usuário<br>● Autenticação de identidade no console<br>● Receção de uma mensagem | Sim | Não |

| Tipo | Origem | Descrição | Modificável | Obrigatório |
|---|---|---|---|---|
| AK/SK | Na página My Credential ou escolha Identity and Access Management > User > Security Settings > Access Keys para criar uma AK/SK. | Autenticação de identidade durante a invocação da API | Não<br>As AK/SK não podem ser modificadas, mas podem ser excluídas e criadas novamente. | Não<br>As AK/SK são usadas para assinar as solicitações enviadas para chamar as APIs. |

### Segurança do armazenamento de dados

O IAM usa algoritmos de encriptação para criptografar os dados do usuário antes de armazená-los.

- Nomes de usuário e AKs: dados não sensíveis, que são armazenados em texto não criptografado.
- Senha: A senha é criptografada usando o algoritmo salted SHA512.
- Endereço de e-mail, número de celular e SK: Use o algoritmo AES para criptografá-los e armazená-los.

### Segurança de transmissão de dados

Os dados sensíveis (incluindo senhas) dos usuários são criptografados usando o TLS 1.2 durante a transmissão. Todas as APIs do IAM são compatíveis com HTTPS para criptografar dados durante a transmissão.

## 8.3.2 Lado do locatário

**As responsabilidades compartilhadas** se aplicam à proteção de dados no IAM da HUAWEI CLOUD. Conforme descrito neste modo, o IAM é responsável pela segurança do próprio serviço e fornece um mecanismo seguro de proteção de dados. Os locatários são responsáveis pelo uso seguro dos serviços IAM, incluindo a configuração de parâmetros de segurança e a divisão e concessão de permissões pelas empresas.

Para fins de proteção de dados, recomendamos que você use o IAM de maneira mais padronizada, referindo-se ao **Recomendações do uso do IAM**.

# 8.4 Resiliência

Os centros de dados de nuvem da Huawei são implantados em todo o mundo de acordo com as regras. Todos os centros de dados estão funcionando corretamente. Os centros de dados em duas cidades são implantados como centro de recuperação de desastres um ao outro. Se um centro de dados na cidade A estiver inoperante, o centro de dados na cidade B assumirá automaticamente o trabalho e atenderá suas aplicações e dados em conformidade com os regulamentos para garantir a continuidade do serviço. Para minimizar as interrupções de

serviço causadas por falhas de hardware, desastres naturais ou outros eventos desastrosos, a Huawei Cloud fornece um plano de DR para todos os centros de dados:

Como um serviço básico de autenticação de identidade, o IAM da HUAWEI CLOUD foi implantado em várias zonas para fornecer aos usuários globais maior disponibilidade, tolerância a falhas e escalabilidade. Para obter detalhes sobre a implantação de AZ, consulte AZ do IAM.

# 8.5 Auditoria e monitoramento

Cloud Trace Service (CTS) registra operações realizadas em recursos de nuvem na sua conta. Os logs de operação podem ser usados para realizar análises de segurança, rastrear alterações de recursos, realizar auditorias de conformidade e localizar falhas.

Para obter detalhes sobre as operações do IAM que podem ser gravadas pelo CTS, consulte "Operações do IAM que podem ser gravadas pelo CTS" em **Habilitação do CTS**. Depois de você habilitar o CTS e criar e configurar um rastreador, o CTS começa a registrar operações para auditoria. Para obter detalhes, consulte **Habilitação do CTS**. Depois de o CTS estiver habilitado, você poderá **exibir logs de auditoria do IAM**. O CTS armazena os logs de operação dos últimos sete dias.

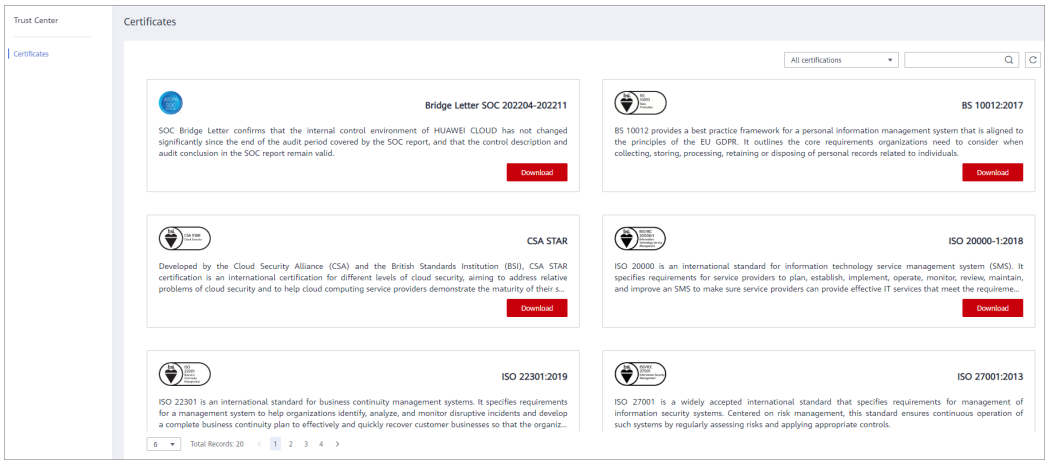
O CTS permite que você **configure notificações de eventos-chave**. Você pode adicionar operações sensíveis e de alto risco relacionadas ao IAM como operações-chave à lista de monitoramento em tempo real do CTS para monitoramento e rastreamento. Se uma operação chave na lista de monitoramento for acionada quando um usuário usar o serviço IAM, o CTS registrará o log de operação e enviará uma notificação ao assinante relacionado em tempo real.

# 8.6 Certificados

## Certificados de conformidade

Os serviços e plataformas da Huawei Cloud obtiveram várias certificações de segurança e de conformidade das organizações autorizadas, como a Organização Internacional de Normalização (ISO).

**Figura 8-2** Download de certificados de conformidade

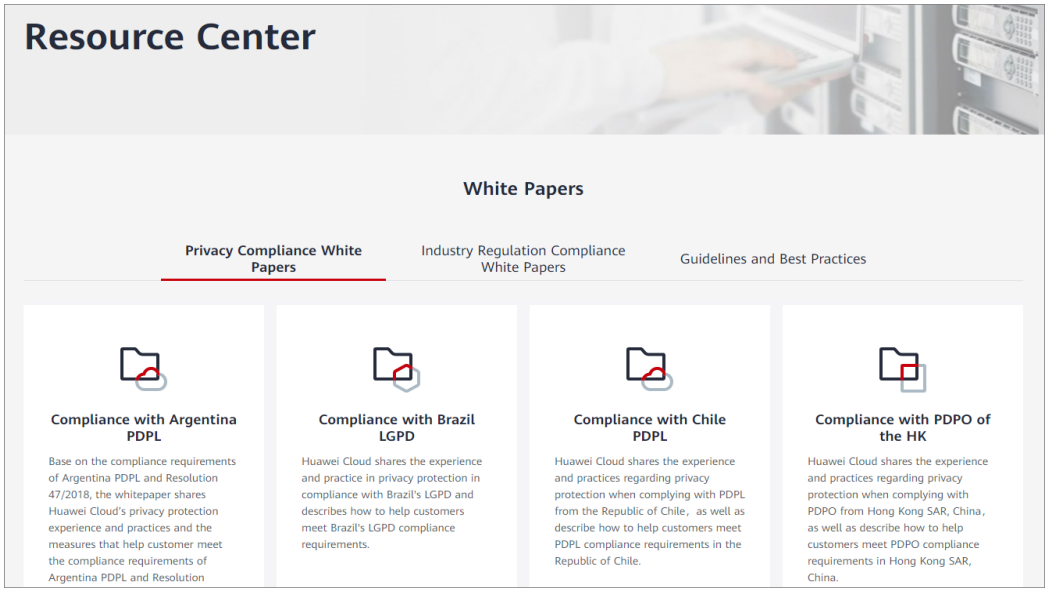


## Central de recursos

A Huawei Cloud também fornece os seguintes recursos para ajudar os usuários a atender aos requisitos de conformidade. Para obter detalhes, consulte **Central de recursos**.

**Figura 8-3** Central de recursos



# 9 Observações e restrições

A seguinte tabela lista as cotas de vários recursos no IAM. A marca "√" indica que você pode aumentar a cota para atender aos requisitos de serviço. Para obter detalhes, consulte **Como faço para aumentar minha cota?**

| Item | Limite | Mutável |
|---|---|---|
| Usuários do IAM | 50 | √ |
| Grupos de usuários | 20 | √ |
| Número máximo de usuários que pode ser adicionado a um grupo de usuários | Número de usuários do IAM que foram criados usando sua conta | x |
| Agências | 50 | √ |
| Número de grupos a qual um usuário pode ser adicionado | 10 | x |
| Número de pares AK/SK que um usuário pode criar | 2 | x |
| Número de dispositivos MFA virtuais que podem ser vinculados a um usuário | 1 | x |
| Políticas personalizadas | 200 | √ |
| Número de permissões (incluindo políticas e funções definidas pelo sistema e políticas personalizadas) que podem ser vinculadas a um grupo de usuários com base em projetos do IAM | 200 | √ |
| Número de permissões (incluindo políticas e funções definidas pelo sistema e políticas personalizadas) que podem ser vinculadas a uma agência | 200 | √ |

| Item | | Limite | Mutável |
|---|---|---|---|
| Número de permissões (incluindo políticas e funções definidas pelo sistema e políticas personalizadas) que podem ser vinculadas a um grupo de usuários com base em projetos empresariais | | 500 | √ |
| Número de permissões (incluindo políticas e funções definidas pelo sistema e políticas personalizadas) que podem ser vinculadas a usuários com base em projetos empresariais | | 500 | √ |
| Número de subprojetos em cada região | | 10 | √ |
| Número de caracteres permitidos em um nome de usuário | | 32 | x |
| Número de caracteres permitidos em um nome de grupo de usuários | | 64 | x |
| Número de caracteres permitidos em um nome de política | | 64 | x |
| Política personalizada | Número máximo de caracteres | 6144 | x |
| | Número máximo de declarações | Até 8 declarações por política | x |
| | Ações | Até 100 ações por declaração | x |
| | Recursos | Até 10 recursos por declaração | x |
| | Condições | Até 10 condições por declaração | x |
| Número de caracteres permitidos em um nome de agência | | 64 | x |
| Provedores de identidade | Quantidade | 10 | √ |
| | Número máximo de caracteres que podem ser contidos em um nome de provedor de identidade | 64 | x |

| Item | | Limite | Mutável |
| --- | --- | --- | --- |
| | Número total de regras de mapeamento de todos os provedores de identidade em uma conta | 10 | √ |

# 10 Histórico de alterações

**Tabela 10-1** Histórico de alterações

| Data | Descrição |
| --- | --- |
| 10/11/2022 | Esta edição é o décimo oitavo lançamento oficial.<br>Adição da introdução a funcionalidades de segurança do IAM em **8 Segurança**. |
| 01/12/2021 | Esta edição é o décimo sétimo lançamento oficial, que inclui as seguintes alterações:<br>Adição da cota de regra de conversão de identidade em **9 Observações e restrições**. |
| 23/11/2021 | Esta edição é o décimo sexto lançamento oficial, que incorpora a seguinte alteração:<br>Adição da descrição de projetos corporativos em **5 Serviços em nuvem suportados**. |
| 25/04/2021 | Esta edição é o décimo quinto lançamento oficial, que incorpora a seguinte alteração:<br>Adição das cotas de permissão em **9 Observações e restrições**. |
| 30/12/2020 | Esta edição é o décimo quarto lançamento oficial, que incorpora a seguinte alteração:<br>Atualização das capturas de tela em **3 Conceitos básicos** com base na alteração para o método de login. |
| 30/11/2020 | Esta edição é o décimo terceiro lançamento oficial, que inclui as seguintes alterações:<br>Atualização da descrição com base nas alterações na página de configuração de segurança. |
| 27/10/2020 | Esta edição é o décimo segundo lançamento oficial, que inclui as seguintes alterações:<br>Atualização das capturas de tela em **3 Conceitos básicos** com base na alteração para o método de login. |

| Data | Descrição |
| --- | --- |
| 30/09/2020 | Esta edição é o décimo primeiro lançamento oficial, que incorpora a seguinte alteração:<br>Seção adicionada **7 Gerenciamento de permissões**. |
| 11/06/2020 | Esta edição é o décimo lançamento oficial, que incorpora a seguinte alteração:<br>Alteração do número máximo de grupos de usuários ao qual um usuário pode ser adicionado para **10** em **9 Observações e restrições**. |
| 08/06/2020 | Esta edição é o nono lançamento oficial, que incorpora a seguinte alteração:<br>Adição das descrições sobre o HUAWEI ID em **3 Conceitos básicos** e atualizadas as capturas de tela da página de login. |
| 19/01/2020 | Esta edição é o oitavo lançamento oficial, que incorpora as seguintes alterações:<br>● Otimização da descrição das permissões em **3 Conceitos básicos**.<br>● Adicionado o limite de subprojetos em uma região em **9 Observações e restrições**. |
| 20/11/2019 | Esta edição é o sétimo lançamento oficial, que inclui as seguintes mudanças:<br>Aumento da cota de política personalizada para 200 em **9 Observações e restrições**. |
| 05/06/2019 | Esta edição é o sexto lançamento oficial.<br>Modificações das descrições em capítulos **2 O que é IAM?**, **3 Conceitos básicos** e **4 Funções**. |
| 05/03/2019 | Esta edição é o quinto lançamento oficial.<br>Adição do capítulo **9 Observações e restrições**. |
| 20/02/2019 | Esta edição é o quarto lançamento oficial.<br>Adição do capítulo **3 Conceitos básicos**. |
| 15/01/2019 | Esta edição é o terceiro lançamento oficial.<br>Adição do capítulo **5 Serviços em nuvem suportados**. |
| 10/08/2018 | Esta edição é o segundo lançamento oficial.<br>Adição do capítulo **6 Mecanismo de proteção de dados pessoais**. |
| 30/03/2018 | Esta edição é o primeiro lançamento oficial. |