IAM 抽屉式帮助

文档版本 01

发布日期 2025-04-18

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2025。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 如何查看授权关系..... 1
2 如何查看授权关系..... 3
3 如何选择授权范围..... 5
4 身份提供商协议说明..... 7
5 身份提供商类型说明..... 8
6 虚拟 MFA 说明..... 9
7 授权操作说明..... 14
8 创建身份提供商..... 16
9 配置 OIDC 身份转换规则..... 22
10 配置 SAML 身份转换规则..... 26
11 身份策略说明..... 30
12 绑定安全密钥..... 36

 版权所有 © 华为云计算技术有限公司

1 如何查看授权关系

授权管理为您呈现账号中所有授权关系，您可以使用**“策略名”**、**“用户名/用户组名/委托名”**、**“项目区域”**、**“主体类型”**为条件筛选指定授权关系。

- **策略名**：权限的名称。如选择过滤条件为“策略名”，输入指定权限名称，查看指定权限的授权记录。
- **用户名/用户组名/委托名**：IAM用户、用户组、委托的名称。如选择过滤条件为“用户名”，输入指定IAM用户名称，查看该IAM用户拥有的权限。IAM的最小授权单位为用户组，查看指定IAM用户授权记录时，将显示该IAM用户所属用户组的授权记录。
- **项目区域**：IAM项目、企业项目的名称。如选择过滤条件为“项目区域”，输入指定IAM项目或企业项目的名称，查看基于该项目授权的授权关系。
- **主体类型**：授权对象类型，支持用户、用户组和委托三种。如选择过滤条件为“主体类型”，输入用户组，查看用户组

下面为您详细介绍授权管理页面各项参数。

权限

权限根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对ECS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

  策略根据创建的对象，分为**系统策略**和**自定义策略**。

您可以在“权限管理>权限”页面创建自定义策略并查看系统角色、系统策略、自定义策略。

项目

区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以默认项目为单位进行授权，用户可以访问您账号中该

 版权所有 © 华为云计算技术有限公司

区域的所有资源。如果您希望进行更加精细的权限控制，可以在区域默认的项目中创建子项目，并在子项目中购买资源，然后以子项目为单位进行授权，使得用户仅能访问特定子项目中资源，使得资源的权限控制更加精确。

除IAM项目外，您可以使用企业项目，企业项目是项目的升级版，针对企业不同项目间资源的分组和管理，是逻辑隔离。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。关于企业项目特性的详细信息，请参见《**企业管理服务用户指南**》。

您可以在“项目”页面创建子项目，并查看所有默认区域项目、子项目；如需创建企业项目，请参考**创建企业项目**。

授权主体

授权主体是权限授予的对象，即当用户组。

主体类型

主体类型可以为用户、用户组和委托。

- 用户：由管理员在IAM中创建的用户。IAM用户可以使用账号名、IAM用户名和密码登录华为云，并根据权限使用所属账号中的资源。IAM不拥有资源，不进行独立的计费，IAM用户的权限和资源由所属账号统一控制和付费。

  您可以在“用户”页面创建、管理用户。
- 用户组：用户组是用户的集合，IAM通过用户组功能实现用户的授权。您创建的IAM用户，需要加入特定用户组后，才具备对应的权限，否则IAM用户无法访问您账号中的任何资源或者云服务。当某个用户加入多个用户组时，此用户同时拥多个用户组的权限，即多个用户组权限的全集。

  您可以在“用户组”页面创建、管理用户组。
- 委托：委托根据委托对象的不同，分为账号委托和云服务委托。
  - 账号委托：通过委托信任功能，您可以将自己账号中的资源操作权限委托给更专业、高效的其他华为云账号，被委托的账号可以根据权限代替您进行资源运维工作。
  - 云服务委托：由于华为云各服务之间存在业务交互关系，一些云服务需要与其他云服务协同工作，需要您创建云服务委托，将操作权限委托给该服务，让该服务以您的身份使用其他云服务，代替您进行一些资源运维工作。

  您可以在“委托”页面创建、管理账号委托和云服务委托。

 版权所有 © 华为云计算技术有限公司

2 如何查看授权关系

“授权记录”页签为您显示该用户组所有授权关系，您可以选择**“策略名”**、**“用户名/用户组名/委托名”**、**“项目区域”**、**“企业项目（已开启企业项目）”**“**主体类型**”为过滤条件查看指定授权关系。如需查看账号下所有授权关系，请前往“权限管理>授权管理”页面。

- **策略名**：权限的名称。如选择过滤条件为“策略名”，输入指定权限名称，查看该用户组指定权限的授权记录。
- **用户名/用户组名/委托名**：IAM用户、用户组、委托的名称。输入指定对应名称，查看其授权记录。
- **项目区域**：IAM项目或企业项目的名称，即权限的作用范围。如选择过滤条件为“项目区域”，输入指定IAM项目或企业项目的名称，查看该用户组基于该项目授权的授权关系。
- **主体类型**：授权对象类型，可以选择用户、用户组、委托3种。IAM项目视图下，可以选择主体类型为“用户组”、“委托”，如果选择“用户”，筛选结果为空。
- **企业项目**：企业项目的名称。如果您在IAM用户视图下，选择“企业项目”为过滤条件，并输入企业项目名称，将自动切换至企业项目视图。

如您已开通企业项目，可以选择IAM项目视图、企业项目视图，查看该用户组基于IAM项目或企业项目的授权记录。关于企业项目特性的详细信息，请参见《**企业管理服务用户指南**》。如您暂未开通企业项目，将直接显示IAM项目视图。

下面为您详细介绍授权管理页面各项参数及其修改方法。

权限

权限根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对ECS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

 版权所有 © 华为云计算技术有限公司

策略根据创建的对象，分为**系统策略**和**自定义策略**。

管理权限：您可以在“权限管理>权限”页面创建自定义策略并查看系统角色、系统策略、自定义策略。

给用户组授权：单击“授权记录”页签下的“授权”，为用户组授予权限。

项目

区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以默认项目为单位进行授权，用户可以访问您账号中该区域的所有资源。如果您希望进行更加精细的权限控制，可以在区域默认的项目中创建子项目，并在子项目中购买资源，然后以子项目为单位进行授权，使得用户仅能访问特定子项目中资源，使得资源的权限控制更加精确。

除IAM项目外，您可以使用企业项目，企业项目是项目的升级版，针对企业不同项目间资源的分组和管理，是逻辑隔离。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。关于企业项目特性的详细信息，请参见《**企业管理服务用户指南**》。

管理项目：您可以在“项目”页面创建子项目，并查看所有默认区域项目、子项目；如需创建企业项目，请参考**创建企业项目**。

基于项目给用户组授权：

- IAM项目：单击“授权记录”页签下的“授权”，跳转至给用户组授权页面，选择权限“作用范围”为全局服务、指定区域项目、所有资源。
- 企业项目：请进入“企业>项目管理”页面，参考**为企业项目添加用户组并授权**。

授权主体

授权主体是权限授予的对象，即当前用户组。

主体类型

主体类型可以为用户、用户组和委托。当前页面仅呈现该用户组的授权关系，因此主体类型为用户组。

用户组是用户的集合，IAM通过用户组功能实现用户的授权。您创建的IAM用户，需要加入特定用户组后，才具备对应的权限，否则IAM用户无法访问您账号中的任何资源或者云服务。当某个用户加入多个用户组时，此用户同时拥多个用户组的权限，即多个用户组权限的全集。

管理用户组：您可以在“用户组”页面创建、管理用户组。

 版权所有 © 华为云计算技术有限公司

3 如何选择授权范围

解释说明

根据您所选择的策略，系统将自动推荐授权范围方案，便于为用户选择合适的授权作用范围。下面为您介绍所有授权范围：

- **所有资源**

  IAM用户可以根据权限使用账号中所有的企业项目、区域项目、全局服务资源。

- **指定企业项目资源**

  选择指定企业项目，IAM用户可以根据权限使用该企业项目中的资源。

  如果您暂未开通企业项目，将不支持基于企业项目授权，了解企业项目请参考：**什么是企业项目管理**。如需开通，请参考：**开通企业项目**。

  当前仅部分服务支持基于企业项目授权，详情请参考：**支持企业项目授权的云服务**。

- **指定区域项目资源**

  选择指定区域项目，IAM用户可以根据权限使用该区域项目中的资源。

  华为云的每个区域默认对应一个项目，如果您希望进行更加精细的权限控制，可以在区域默认的项目中创建子项目，并在子项目中购买资源，然后以子项目为单位进行授权，使得IAM用户仅能访问特定子项目中的资源。如需创建项目，请参考：**创建项目**。

  说明

  如果您已开通企业项目，将不支持创建区域子项目。

- **全局服务资源**

  IAM用户可以根据权限使用全局服务。服务部署时不区分物理区域，为全局级服务。访问全局级服务时，不需要切换区域，如对象存储服务（OBS）、内容分发网络（CDN）等。

常见问题

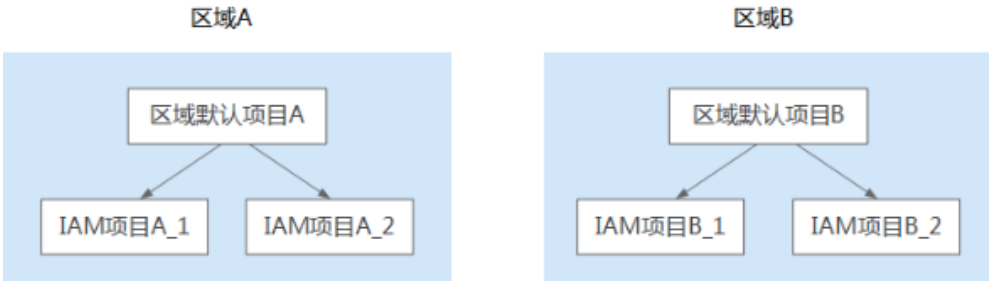
区域项目和企业项目的区别

- 区域项目

  区域项目是针对同一个区域内的资源进行分组和隔离，是物理隔离。在区域项目中的资源不能转移，只能删除后重建。

 版权所有 © 华为云计算技术有限公司

区域项目在统一身份认证服务中管理，使用区域项目，请参考：**项目**。



- 企业项目

  企业项目是区域项目的升级版，针对企业不同项目间资源的分组和管理，是逻辑隔离。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。企业项目可以实现对特定云资源的授权，例如：将一台特定的ECS添加至企业项目，对企业项目进行授权后，可以控制用户仅能管理这台特定的ECS。

  企业项目在企业管理服务中管理，使用企业项目，请参考：**创建企业项目**。

为什么看不到“企业项目”授权范围?

您暂未开通企业项目，如需开通请参考：**开通企业项目**。如果您开通了企业项目，将不能创建区域子项目，请谨慎操作。

 版权所有 © 华为云计算技术有限公司

4 身份提供商协议说明

IAM支持基于SAML、OIDC协议的单点登录，如果您已经有自己的企业管理系统，同时您的用户需要使用您账号内的云服务资源，您可以使用IAM的身份提供商功能，实现用户使用企业管理系统账号单点登录华为云，这一过程称之为联邦身份认证。

基本概念

- SAML 2.0

  安全断言标记语言（Secturity Assertion Markup Language 2.0，缩写为SAML 2.0）是一个由一组协议组成，用来传输安全声明的XML框架。SAML2.0是由标准化组织OASIS提出的用于安全操作的标准，是很多身份提供商（IdP）使用的一种开放标准，关于SAML2.0的详细描述请参见：**SAML 2.0技术概述**。IAM支持使用SAML2.0协议进行联邦身份认证，因此与华为云建立联邦身份认证的企业IdP必须支持SAML2.0协议。

- OIDC

  OIDC是OpenID Connect的简称，是一个基于OAuth 2.0协议的身份认证标准协议。IAM支持使用OIDC 1.0协议进行联邦身份认证，因此与华为云建立联邦身份认证的企业IdP必须支持OIDC 1.0协议。关于OIDC的详细描述请参见：**欢迎使用OpenID Connect**。

选用原则：根据与华为云建立联邦身份认证的企业IdP支持的协议进行选择。

后续操作

- **基于SAML协议的联邦身份认证操作步骤**
- **基于OIDC协议的联邦身份认证操作步骤**

 版权所有 © 华为云计算技术有限公司

5 身份提供商类型说明

一个账号下只能存在一种类型的身份提供商。OIDC协议仅支持虚拟用户SSO。

- 虚拟用户SSO：该身份提供商中的用户登录华为云后，系统为其自动创建虚拟用户信息。一个账号可以创建多个虚拟用户SSO类型的身份提供商。
- IAM用户SSO：该身份提供商中的用户登录华为云后，系统将自动匹配外部身份ID绑定的对应IAM子用户，从而拥有该子用户所在用户组的权限。一个账号下只能创建一个IAM用户SSO类型的身份提供商。如果选择该类型，请确保您已为用户创建对应的IAM用户并设置外部身份ID，请参考**创建IAM用户**。

 版权所有 © 华为云计算技术有限公司

6 虚拟 MFA 说明

什么是虚拟 MFA

虚拟Multi-Factor Authentication (MFA) 是能产生6位数字认证码的设备，遵循基于时间的一次性密码（TOTP）标准。MFA设备可以基于硬件也可以基于软件，目前仅支持基于软件的虚拟MFA，即虚拟MFA应用程序，可以在移动硬件设备（包括智能手机）上运行，非常方便，虚拟MFA是多因素认证方式中的一种。

如何绑定虚拟 MFA

您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。不同的场景绑定操作步骤如下所示。

已升级华为账号

步骤1 单击“虚拟MFA”右侧的“前往绑定”。

步骤2 跳转至“华为账号>安全验证”页面，根据提示绑定虚拟MFA。

----结束

暂未升级华为账号的华为云账号

步骤1 单击“虚拟MFA”右侧的“前往绑定”。

步骤2 根据右侧弹出的绑定虚拟MFA页面，在您的MFA应用程序中添加用户。

 版权所有 © 华为云计算技术有限公司

图 6-1 绑定虚拟 MFA

您可以通过扫描二维码、手动输入两种方式绑定MFA设备，下面以“华为云”手机应用程序为例绑定虚拟MFA：

- 扫描二维码

  打开手机上已安装好的“华为云”手机应用程序，选择“控制台-MFA-添加-扫码添加”，扫描“绑定虚拟MFA”弹窗中的二维码。扫描成功后，“华为云”手机应用程序会自动添加用户，虚拟MFA列表中出现账号/IAM用户名及对应的MFA动态码。

- 手动输入

  打开手机上已安装好的“华为云”手机应用程序，选择“控制台-MFA-添加-手动输入”。账号绑定虚拟MFA，输入账号和密钥；IAM用户绑定虚拟MFA，输入IAM用户名和密钥。单击“添加”手动添加用户。

  说明

  手动输入添加用户方式只支持基于时间模式，建议在移动设备中开启自动设置时间功能。

步骤3 添加用户完成，在“华为云”手机应用程序“虚拟MFA页面”，查看虚拟MFA的动态口令页面。动态口令每30秒自动更新一次。

 版权所有 © 华为云计算技术有限公司

步骤4 在“绑定虚拟MFA”页面输入连续的两组口令，然后单击“确定”，完成绑定虚拟MFA设备的操作。

----结束

IAM 用户绑定

IAM用户可自行在IAM控制台绑定虚拟MFA，操作与**暂未升级华为账号的华为云账号**相同。

若管理员重置了IAM用户的虚拟MFA或IAM用户首次登录，且该IAM用户开启了登录保护并设置虚拟MFA为验证方式，则IAM用户登录过程中需要重新绑定虚拟MFA，操作如下：

步骤1 以IAM用户身份登录控制台。

步骤2 在登录验证页，单击“绑定虚拟MFA”。

步骤3 页面右侧会弹出绑定虚拟MFA页面，请根据提示绑定虚拟MFA。

----结束

常见问题

如何获取虚拟 MFA 验证码

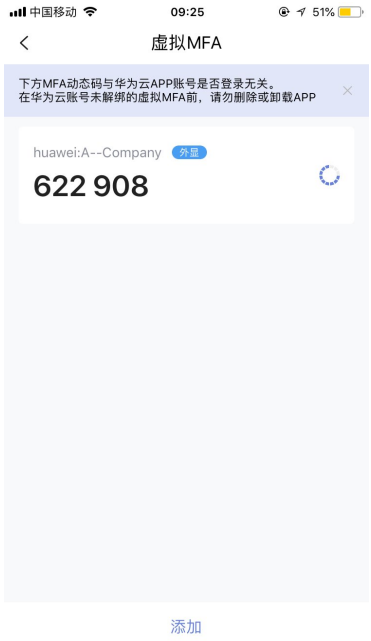
绑定虚拟MFA并开启登录保护或操作保护后，用户在进行登录或进行敏感操作时，需要输入MFA应用程序的动态验证码，下图以登录验证为例。

图 6-2 虚拟 MFA 登录验证

 版权所有 © 华为云计算技术有限公司

此时，您需要打开智能设备上的虚拟MFA应用程序，查看并输入用户已绑定账号的验证码，下图以华为云App为例。

图 6-3 查看 MFA 验证码



如何解绑虚拟 MFA

解绑虚拟MFA适用于手机未丢失或者没有删除虚拟MFA应用程序的IAM用户或账号，IAM用户或账号可以在界面自助完成解绑虚拟MFA的操作。

- 手机丢失或已删除虚拟MFA应用程序的IAM用户，请联系管理员**重置虚拟MFA**。
- 手机丢失或已删除虚拟MFA应用程序的华为云账号和华为账号，请联系客服为您重置虚拟MFA。

步骤1 单击“虚拟MFA”右侧的“前往解绑”。

说明

如果您已升级华为账号，将跳转至华为账号网站，请在“账号中心>账号与安全>安全验证”单击“虚拟MFA”后的“解绑”。

步骤2 在“解绑虚拟MFA”页面中输入从虚拟MFA设备获取的动态验证码。

步骤3 单击“确定”，验证成功后，完成解绑MFA操作。

----结束

如何重置虚拟 MFA

手机丢失或已删除虚拟MFA应用程序的**华为云账号和华为账号**，请联系客服为您重置虚拟MFA。

手机丢失或已删除虚拟MFA应用程序的**IAM用户**，请联系管理员重置虚拟MFA，管理员的操作步骤如下所示。

 版权所有 © 华为云计算技术有限公司

步骤1 登录统一身份认证服务管理控制台。

步骤2 在“统一身份认证服务>用户”页签中的用户列表中，单击用户右侧的“安全设置”。

步骤3 在“安全设置”页面中，单击“虚拟MFA设备”右侧的“重置”。

步骤4 单击“确定”，重置成功。

----结束

 版权所有 © 华为云计算技术有限公司

7 授权操作说明

操作步骤

步骤1 在用户组选择策略页面中，勾选需要授予用户组的权限。完整的权限列表请参见：**系统权限**。常用的系统权限设置案例请参见下方**常用系统权限设置案例**。

如果系统策略不满足授权要求，可以单击权限列表右上角的“新建策略”创建自定义策略，并勾选新创建的策略来进行精细的权限控制，自定义策略是对系统策略的扩展和补充。详情请参考**创建自定义策略**。

步骤2 选择权限的作用范围。系统会根据您所选择的策略，自动推荐授权范围方案，便于为用户选择合适的授权作用范围，**表1**为IAM提供的所有授权范围方案。

表 7-1 授权范围方案

可选方案	方案说明
所有资源	IAM用户可以根据权限使用账号中所有的区域项目、全局服务资源。
指定企业项目资源	选择指定企业项目，IAM用户可以根据权限使用该企业项目中的资源。**仅开通企业项目后可选。** 如果您暂未开通企业项目，将不支持基于企业项目授权，了解企业项目请参考：**什么是企业项目管理**。如需开通，请参考：**开通企业项目**。
指定区域项目资源	选择指定区域项目，IAM用户可以根据权限使用该区域项目中的资源。 如果选择作用范围为“区域项目”，且所勾选的策略包含全局服务权限，系统自动将全局服务权限的作用范围设置为**所有资源**，勾选的区域项目权限的作用范围仍为指定区域项目。
全局服务资源	IAM用户可以根据权限使用全局服务。全局服务部署时不区分物理区域。访问全局级服务时，不需要切换区域，如对象存储服务（OBS）、内容分发网络（CDN）等。 如果选择作用范围为“全局服务”，且所勾选的策略包含项目级服务权限，系统自动将项目权限作用范围设置为**所有资源**，勾选的全局服务权限的作用范围仍为全局服务。

步骤3 单击“确定”，完成用户组授权。

 版权所有 © 华为云计算技术有限公司

说明

- 当一个用户被加入多个用户组，将会拥有所有已加入用户组的权限。
- 更多有关权限的使用建议请参见：**多运维人员权限设置案例**、**自定义策略使用样例**。

----结束

常用系统权限设置案例

请参考以下文档给IAM用户设置常见云服务的访问权限。

- **设置弹性云服务器（ECS）的权限**
- **设置弹性负载均衡（ELB）的权限**
- **设置关系型数据库（RDS）的权限**
- **设置云硬盘（EVS）的权限**
- **设置云监控（CES）的权限**
- **设置云容器引擎（CCE）的权限**
- **设置对象存储服务（OBS）的权限**
- **设置云备份（CBR）的权限**
- **设置虚拟私有云（VPC）的权限**
- **设置分布式缓存服务（DCS）的权限**
- **设置文档数据库服务（DDS）的权限**
- **设置费用中心的权限**
- **设置提交工单的权限**

 版权所有 © 华为云计算技术有限公司

8 创建身份提供商

配置联邦身份认证，需要在企业IdP通过浏览器将用户重定向到华为云本系统OIDC身份提供商并创建OAuth 2.0凭据，在IAM控制台上创建身份提供商、配置授权信息，来建立两个系统之间的互信关系。

前提条件

- 企业管理员在华为云本系统注册了可用的账号，并已在IAM中创建用户组并授权，具体方法请参见：**创建用户组并授权**。在华为云本系统IAM上创建的用户组是用于与企业IdP上的用户建立映射关系，使得IdP中的用户获取华为云本系统IAM中用户组的权限。
- 企业管理员已获取企业IdP的帮助文档或了解企业IdP使用方法。由于不同的企业IdP的配置存在较大差异，华为云云服务平台帮助文档对于企业IdP的配置不做详述，获取企业IdP的OAuth 2.0凭据等具体操作请参考企业IdP的帮助文档。

在企业 IdP 中创建 OAuth 2.0 凭据

步骤1 企业IdP通过浏览器将用户重定向到华为云本系统OIDC身份提供商。设置授权定向URI为：https://auth.huaweicloud.com/authui/oidc/redirect和https://auth.huaweicloud.com/authui/oidc/post。

步骤2 获取企业IdP的OAuth 2.0凭据。

----结束

在华为云系统上创建身份提供商

在IAM控制台上创建身份提供商，通过配置授权信息，可以在IAM中建立对IdP的信任关系，使得企业用户可以直接访问华为云本系统。

步骤1 进入**IAM控制台**IAM控制台，在左侧导航窗格中，选择“身份提供商”页签，单击右上方的“创建身份提供商”。

 版权所有 © 华为云计算技术有限公司

图 8-1 创建身份提供商

步骤2 在弹出的“创建身份提供商”窗口中填写“名称”，选择“协议”为“OpenID Connect”，选择“状态”为“启用”，单击“确定”，创建身份提供商成功。

图 8-2 填写身份提供商参数

说明

身份提供商名称不能重复，建议以域名唯一标识命名。

----结束

在华为云系统上配置授权信息

步骤1 单击身份提供商列表中“操作”列的“修改”，进入“修改身份提供商”页面。

图 8-3 修改身份提供商

 版权所有 © 华为云计算技术有限公司

步骤2 在修改身份提供商页面，选择“访问方式”。

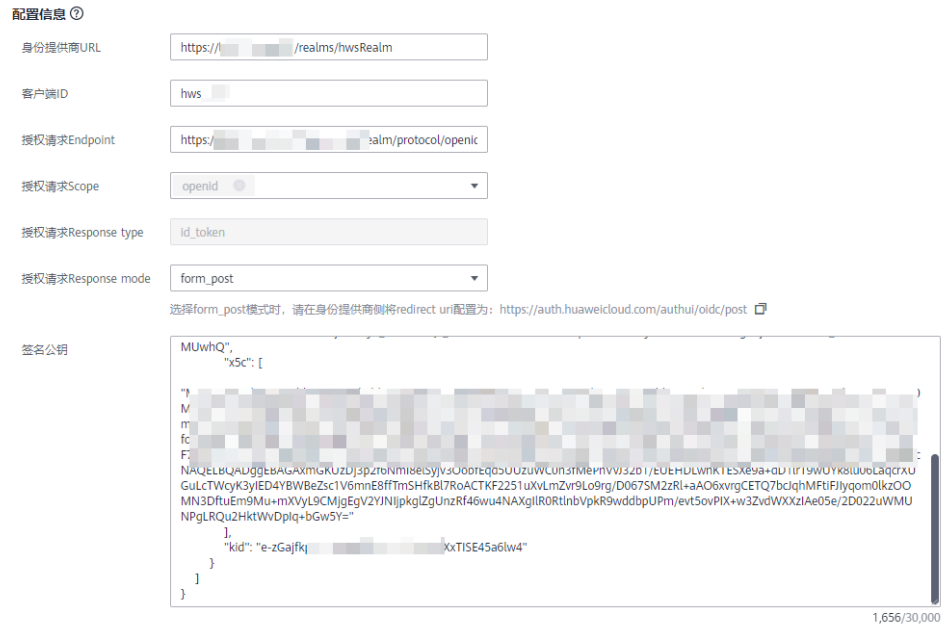
图 8-4 访问方式

表 8-1 访问方式

访问方式	说明
编程访问和管理控制台访问	• 编程访问：可以使用支持访问密钥认证的API、CLI、SDK等开发工具来访问华为云本系统。 • 管理控制台访问：用户可以使用账号密码登录到管理控制台来访问华为云本系统。 **如果您需要使用SSO方式访问华为云本系统，应该选择此方式。**
编程访问	用户仅可以使用支持访问密钥认证的API、CLI、SDK等开发工具来访问华为云本系统。

步骤3 在修改身份提供商页面，填写“配置信息”。

图 8-5 配置信息



 版权所有 © 华为云计算技术有限公司

表 8-2 配置信息

配置信息	说明
身份提供商URL	OpenID Connect身份提供商标识。 对应企业IdP提供的Openid-configuration中"issuer"字段的值。 **说明** Openid-configuration是在OpenID Connect中定义的URL，它提供了有关身份提供程序（IdP）的配置信息。URL如下：*https://{base URL}/.well-known/openid-configuration*，其中*base URL*由企业IdP定义，如Google提供的Openid-configuration为https://accounts.google.com/.well-known/openid-configuration.
客户端ID	在OpenID Connect身份提供商注册的客户端ID。即**在企业IdP中创建的OAuth 2.0凭据**。
授权请求Endpoint	OpenID Connect身份提供商授权地址。对应企业IdP提供的Openid-configuration中"authorization_endpoint"字段的值。 **仅访问方式为“编程访问和管理控制台访问”时需要填写。**
授权请求Scope	授权请求信息范围。默认必选openid。 **仅访问方式为“编程访问和管理控制台访问”时需要填写。** 枚举值： • openid • email • profile
授权请求Response type	授权请求返回参数类型，默认必选id_token。 **仅访问方式为“编程访问和管理控制台访问”时需要填写。**
授权请求Response mode	授权请求返回模式，form_post和fragment两种可选模式，推荐选择form_post模式。 • form_post：选择form_post模式时，请在身份提供商侧将redirect url配置为：https://auth.huaweicloud.com/authui/oidc/post。 • fragment：选择fragment模式时，请在身份提供商侧将redirect url配置为：https://auth.huaweicloud.com/authui/oidc/redirect。 **仅访问方式为“编程访问和管理控制台访问”时需要填写。**
签名公钥	验证OpenID Connect身份提供商ID Token签名的公钥。为了您的账号安全，建议您**定期轮换**签名公钥。

步骤4 单击“确定”，完成配置。

----结束

联邦用户登录验证

步骤1 检查登录链接是否可以跳转到企业的IdP服务器提供的登录界面。

 版权所有 © 华为云计算技术有限公司

1. 在IAM控制台的“身份提供商”页面，单击“操作”列的“修改”，进入“修改身份提供商”页面。
2. 在修改身份提供商页面，单击登录链接右侧的“复制”，并在浏览器中打开。

图 8-6 复制登录链接

3. 检查浏览器页面是否跳转到IdP登录界面，如果跳转失败，请确认身份提供商配置信息以及企业IdP服务器配置是否正确。

步骤2 输入企业管理系统的用户名和密码验证是否可以登录到华为云本系统。

- 登录成功：表示单点登录验证成功，您可以将该地址以链接的形式配置到企业管理系统。
- 登录失败：请检查您的用户名和密码。

说明

此时联邦用户只能访问华为云本系统，没有任何权限。为联邦用户配置权限需要配置身份转换规则，具体说明请参见：**9 配置OIDC身份转换规则**。

----结束

相关操作

- 查看身份提供商信息：在身份提供商列表中，单击“查看”，可查看身份提供商的基本信息、元数据详情、身份转换规则。

  说明

  单击“查看身份提供商”页面下方的“修改身份提供商”，可直接进入“修改身份提供商”界面。
- 修改身份提供商信息：在身份提供商列表中，单击“修改”进入“修改身份提供商”界面。可修改身份提供商的状态（“启用”或“停用”）、描述信息、元数据信息和身份转换规则。
- 删除身份提供商：在身份提供商列表中，单击“删除”，删除对应的身份提供商。

 版权所有 © 华为云计算技术有限公司

后续任务

- 配置身份转换规则，建立IdP中的用户与IAM中用户组间的映射关系，使得IdP用户获得用户组对应的华为云本系统操作权限。身份转换规则详情请参见：**9 配置OIDC身份转换规则**。
- 在企业管理系统中配置单点登录，使企业用户可以通过企业管理系统中的华为云本系统登录入口直接访问华为云本系统，方法请参考：**（可选）步骤3：配置企业管理系统登录入口**。

 版权所有 © 华为云计算技术有限公司

9 配置 OIDC 身份转换规则

在IAM上创建身份提供商后，联邦用户在华为云系统中的用户名默认为“FederationUser”，且联邦用户仅能访问华为云云服务平台，没有任何权限。您可以在IAM控制台配置身份转换规则，实现：

- 企业管理系统用户在华为云系统中显示不同的用户名。
- 赋予企业管理系统用户使用华为云系统资源的权限。由于华为云系统权限的最小授权单位是用户组，因此需要建立联邦用户与IAM用户组的映射关系，从而使得联邦用户获得对应用户组的权限，使用华为云上系统中的资源。请确保已创建需要映射的IAM用户组，创建IAM用户组并授权请参见：**创建用户组并授权**。

说明

- 修改身份转换规则后，对已登录的联邦用户不会即时生效，需重新登录后新规则才可生效。
- 如果需要修改用户的权限，修改用户所属用户组的权限即可，修改后，需要重启企业IdP使设置生效。

前提条件

已在本系统创建身份提供商，并验证身份提供商的登录链接可以正常使用，如何创建并验证身份提供商请参见：**步骤1：创建身份提供商**。

操作步骤

您可以使用“创建规则”，IAM会将您填写的身份转换规则参数转换成JSON语言；也可以单击“编辑规则”直接编写JSON语言，编辑身份转换规则的详细说明和示例请参见：**身份转换规则详细说明**。

- **创建规则**
  a. 管理员在**IAM控制台**IAM控制台的左侧导航窗格中，单击“身份提供商”。
  b. 在身份提供商列表中，选择您创建的身份提供商，单击“修改”。
  c. 在“身份转换规则”区域单击“创建规则”。

图 9-1 创建规则-1

 版权所有 © 华为云计算技术有限公司

图 9-2 创建规则-2

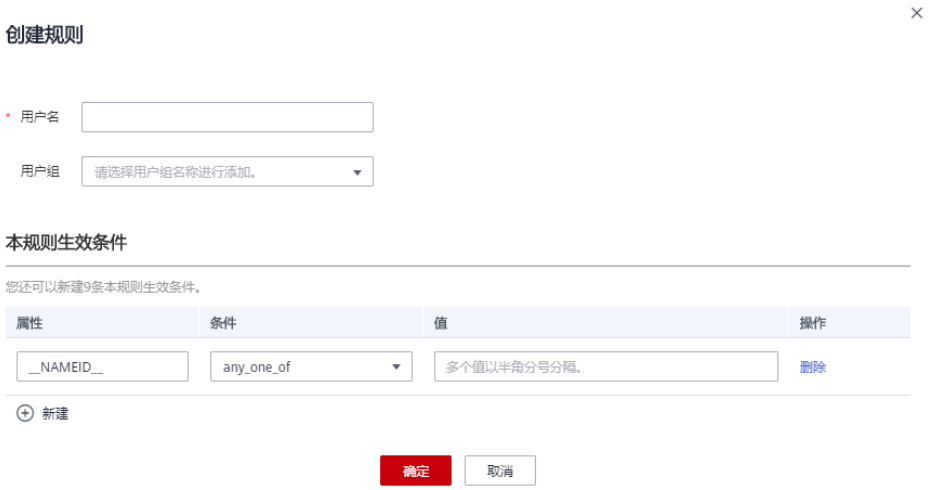


表 9-1 参数说明

参数名	描述	说明
用户名	联邦用户在华为云系统中显示的用户名，以下简称“联邦用户名”。	为了区分华为云系统的用户与联邦用户，建议此处配置用户名为“FederationUser-IdP_XXX”。其中“IdP”为身份提供商名称，如ADFS、Shibboleth等，用于区分不同身份提供商下的联邦用户；“XXX”为自定义的具体名称。 **须知** • 同一身份提供商的联邦用户名需要确保其唯一。如果同一身份提供商内出现重复的联邦用户名，则重名的联邦用户在华为云本系统中对应同一个IAM用户。 • 用户名能包含大小写字母、空格、数字或特殊字符（-_.）且不能以数字开头。不能包含”、\"、\\、\n、\r等特殊字符。
用户组	联邦用户在华为云系统中所属的用户组。	联邦用户拥有所属用户组的权限。可以选择已创建的用户组。
本规则生效条件	联邦用户拥有所选用户组权限的生效条件。	当满足该生效条件时，联邦用户具有所属用户组的权限；当不满足生效条件时，该规则不生效，且不满足生效条件的用户无法访问华为云云服务平台。一个身份转换规则最多可以创建10条生效条件。 **说明** • 一个规则可以创建多条生效条件，所有生效条件均满足，此规则才可以生效。 • 一个身份提供商可以创建多条规则，规则共同作用。如果所有规则对某个联邦用户都不生效，那么该联邦用户禁止访问华为云云服务平台。

 版权所有 © 华为云计算技术有限公司

示例：为企业管理系统管理员设定规则。

- 用户名：FederationUser-IdP_admin
- 用户组：“admin”
- 生效条件：“属性”：“_NAMEID_”；“条件”：“any_one_of”；“值”：“000000001”。

  表示仅用户ID为000000001的用户在华为云云服务平台中映射的IAM用户名为FederationUser-IdP_admin、具有“admin”用户组的权限。

d. 在“创建规则”页面，单击“确定”。

e. 在“修改身份提供商”页面，单击“确定”，使配置生效。

- **编辑规则**

a. 管理员登录华为云云服务平台，进入**IAM控制台**IAM控制台，并在左侧导航窗格中，单击“身份提供商”。

b. 在身份提供商列表中，选择您创建的身份提供商，单击“修改”。

图 9-3 修改身份提供商

c. 在“身份转换规则”区域单击“编辑规则”。

d. 在编辑框内输入JSON格式的身份转换规则，具体说明请参见：**身份转换规则详细说明**。

e. 单击“校验规则”，对已编辑的规则进行语法校验。

f. 界面提示“规则正确”：在“编辑规则”页面，单击“确定”；在“修改身份提供商”页面，单击“确定”，使配置生效。

界面提示“JSON文件格式不完整”：请修改JSON语句，或单击“取消”，取消本次修改内容。

验证联邦用户权限

配置身份转换规则后，查看联邦用户是否已有相应权限。

步骤1 联邦用户登录。

在IAM控制台的“身份提供商”页面，单击“操作”列的“查看”，进入“身份提供商基本信息”页面；单击“登录链接”右侧的“”，在浏览器中打开，输入企业管理系统用户名和密码，登录成功。

步骤2 查看联邦用户是否具有所属用户组的权限。

例如，配置身份转换规则时，使联邦用户“ID1”对应IAM用户组“admin”，拥有所有云服务的权限。进入控制台，选择任一云服务，查看是否可以访问此服务。

----结束

 版权所有 © 华为云计算技术有限公司

相关操作

查看规则：在“身份转换规则”区域单击“查看规则”。新创建的身份转换规则在JSON文件中显示。JSON文件内容说明请参考：**身份转换规则详细说明**。

 版权所有 © 华为云计算技术有限公司

10 配置 SAML 身份转换规则

企业IdP用户登录华为云云服务平台后，华为云系统会根据身份转换规则，决定联邦用户的身份和拥有的权限。身份转换规则需要用户根据自身场景自定义，若不对身份转换规则进行配置，则联邦用户在华为云系统中的用户名默认为“FederationUser”，权限默认仅能访问华为云云服务平台，没有其他任何权限。

您可对联邦用户的以下特征进行配置：

- 用户名：企业IdP用户在华为云系统中显示不同的用户名。
- 用户权限：赋予企业管理系统用户使用华为云系统资源的权限。由于华为云系统权限的最小授权单位是用户组，因此需要建立联邦用户与IAM用户组的映射关系，从而使得联邦用户获得对应用户组的权限，使用华为云上系统中的资源。配置时请确保已创建需要映射的IAM用户组，创建IAM用户组并授权请参见：**创建用户组并授权**。

说明

- 修改身份转换规则后，对已登录的联邦用户不会即时生效，需重新登录后新规则才可生效。
- 如果需要修改用户的权限，修改用户所属用户组的权限即可，修改后，需要重启企业IdP使设置生效。

前提条件

- 企业管理员在华为云上本系统注册了可用的账号，并已在IAM中创建用户组并授权，具体方法请参见：**创建用户组并授权**。
- 已在本系统创建身份提供商，如何创建身份提供商请参见：**步骤1：创建身份提供商**。

操作步骤

您可以使用“创建规则”，IAM会将您填写的身份转换规则参数转换成JSON语言；也可以单击“编辑规则”直接编写JSON语言，编辑身份转换规则的详细说明和示例请参见：**身份转换规则详细说明**。

- **创建规则**
  a. 管理员在**IAM控制台**IAM控制台的左侧导航窗格中，单击“身份提供商”。
  b. 在身份提供商列表中，选择您创建的身份提供商，单击“修改”。
  c. 在“身份转换规则”区域单击“创建规则”。

 版权所有 © 华为云计算技术有限公司

图 10-1 创建规则-1

图 10-2 创建规则-2

表 10-1 参数说明

参数名	描述	说明
用户名	联邦用户在华为云系统中显示的用户名，以下简称“联邦用户名”。	为了区分华为云系统的用户与联邦用户，建议此处配置用户名为“FederationUser-IdP_XXX”。其中“IdP”为身份提供商名称，如ADFS、Shibboleth等，用于区分不同身份提供商下的联邦用户；“XXX”为自定义的具体名称。 **须知** • 同一身份提供商的联邦用户名需要确保其唯一。如果同一身份提供商内出现重复的联邦用户名，则重名的联邦用户在华为云本系统中对应同一个IAM用户。 • 用户名能包含大小写字母、空格、数字或特殊字符（ -_. ）且不能以数字开头。不能包含”、\"、\\、\n、\r等特殊字符。
用户组	联邦用户在华为云系统中所属的用户组。	联邦用户拥有所属用户组的权限。可以选择已创建的用户组。

 版权所有 © 华为云计算技术有限公司

参数名	描述	说明
本规则生效条件	联邦用户拥有所选用户组权限的生效条件。	当满足该生效条件时，联邦用户具有所属用户组的权限；当不满足生效条件时，该规则不生效，且不满足生效条件的用户无法访问华为云云服务平台。一个身份转换规则最多可以创建10条生效条件。 “属性”、“值”为企业IdP通过SAML断言返回给华为云系统用户信息；“条件”可选择：empty、any_one_of、not_any_of，详细说明请参见：**身份转换规则详细说明**。 **说明** • 一个规则可以创建多条生效条件，所有生效条件均满足，此规则才可以生效。 • 一个身份提供商可以创建多条规则，规则共同作用。如果所有规则对某个联邦用户都不生效，那么该联邦用户禁止访问华为云云服务平台。

示例：为企业管理系统管理员设定规则。

- 用户名：FederationUser-IdP_admin
- 用户组：“admin”
- 生效条件：“属性”：“_NAMEID_”；“条件”：“any_one_of”；“值”：“000000001”。

  表示仅用户ID为000000001的用户在华为云云服务平台中映射的IAM用户名为FederationUser-IdP_admin、具有“admin”用户组的权限。

d. 在“创建规则”页面，单击“确定”。

e. 在“修改身份提供商”页面，单击“确定”，使配置生效。

- **编辑规则**

a. 管理员登录华为云云服务平台，进入**IAM控制台**IAM控制台，并在左侧导航窗格中，单击“身份提供商”。

b. 在身份提供商列表中，选择您创建的身份提供商，单击“修改”。

图 10-3 修改身份提供商

c. 在“身份转换规则”区域单击“编辑规则”。

 版权所有 © 华为云计算技术有限公司

图 10-4 编辑身份转换规则

d. 在编辑框内输入JSON格式的身份转换规则，具体说明请参见：**身份转换规则详细说明**。

e. 单击“校验规则”，对已编辑的规则进行语法校验。

f. 界面提示“规则正确”：在“编辑规则”页面，单击“确定”；在“修改身份提供商”页面，单击“确定”，使配置生效。

界面提示“JSON文件格式不完整”：请修改JSON语句，或单击“取消”，取消本次修改内容。

相关操作

查看规则：在“身份转换规则”区域单击“查看规则”。新创建的身份转换规则在JSON文件中显示。JSON文件内容说明请参考：**身份转换规则详细说明**。

 版权所有 © 华为云计算技术有限公司

11 身份策略说明

身份策略授权模型相较于原版本基于角色和策略授权模型能够做到更细粒度、更精准安全的权限控制。身份策略核心关系为“用户-身份策略”。新增资源时，对比角色与策略授权，基于身份策略的授权模型可以更快速地直接给用户授权，灵活性更强，更方便，但相对应的，整体权限管控模型构建更加复杂，对相关人员专业能力要求更高，因此更适用于中大型企业。

身份策略仅适用于如下云服务及区域，如使用自定义身份策略且策略内容中包含未支持的云服务或区域，则该身份策略无法对未支持的云服务或区域生效。

支持身份策略的云服务

计算

序号	服务名称
1	弹性云服务器（ECS）
2	裸金属服务（BMS）
3	镜像服务（IMS）
4	弹性伸缩（AS）

存储

序号	服务名称
1	云备份（CBR）
2	云硬盘（EVS）
3	高性能弹性文件服务 SFS Turbo

网络

 版权所有 © 华为云计算技术有限公司

序号	服务名称
1	虚拟私有云（VPC）
2	弹性公网IP（EIP）
3	NAT网关（NAT）
4	弹性负载均衡（ELB）
5	VPC终端节点（VPCEP）
6	云专线（DC）
7	企业路由器（ER）
8	全球加速服务（GA）
9	云连接（CC）

容器

序号	服务名称
1	云容器引擎（CCE）
2	容器镜像服务（SWR）

大数据

序号	服务名称
1	数据湖探索（DLI）
2	数据治理中心（DataArts Studio）
3	数据仓库服务 GaussDB（DWS）
4	MapReduce服务（MRS）
5	云搜索服务（CSS）

CDN与智能边缘

序号	服务名称
1	内容分发网络（CDN）

数据库

 版权所有 © 华为云计算技术有限公司

序号	服务名称
1	云数据库（RDS）
2	文档数据库服务（DDS）
3	云数据库 GaussDB
4	数据复制服务（DRS）
5	云数据库 TaurusDB

安全与合规

序号	服务名称
1	原生基础防护（Anti-DDoS）
2	DDoS原生高级防护（CNAD）
3	DDoS高防（AAD）
4	数据加密服务（DEW），包含如下微服务： ● 密钥管理服务（KMS） ● 云凭据管理服务（CSMS） ● 密钥对管理服务（KPS） ● 专属加密（DHSM）
5	主机安全服务（HSS）
6	安全云脑（SecMaster）
7	云防火墙（CFW）
8	数据安全中心（DSC）
9	私有证书管理服务（PCA）
10	SSL证书管理服务（SCM）
11	云堡垒机（CBH）
12	数据库安全服务（DBSS）
13	Web应用防火墙（WAF）

IoT物联网

序号	服务名称
1	设备接入（IoTDA）

 版权所有 © 华为云计算技术有限公司

应用中间件

序号	服务名称
1	分布式缓存服务（DCS）
2	微服务引擎（CSE）
3	API网关（APIG）

开发与运维

序号	服务名称
1	应用管理与运维平台（Servicestage）
2	软件开发生产线（CodeArts）
3	流水线（CodeArts Pipeline）
4	开源治理服务 CodeArts Governance
5	性能测试 CodeArts PerfTest

企业应用

序号	服务名称
1	云解析服务（DNS）
2	云桌面（Workspace）

管理与监管

序号	服务名称
1	消息通知服务（SMN）
2	云日志服务（LTS）
3	统一身份认证（IAM）
4	安全令牌服务（STS）
5	资源编排服务（RFS）
6	IAM身份中心（IdentityCenter）
7	组织（Organizations）
8	资源访问管理（RAM）

 版权所有 © 华为云计算技术有限公司

序号	服务名称
9	企业项目管理服务 （ EPS ）
10	标签管理服务（ TMS ）
11	配置审计（ Config ）（ 原 资源管理服务 RMS ）
12	访问分析（ AccessAnalyzer ）
13	云审计服务（ CTS ）
14	资源治理中心（ RGC ）
15	应用运维管理（ AOM ）
16	云监控服务 （ CES ）
17	云运维中心（ COC ）

用户服务

序号	服务名称
1	费用中心
2	成本中心
3	账号中心
4	企业中心
5	消息中心
6	客户运营能力

迁移

序号	服务名称
1	对象存储迁移服务（ OMS ）
2	主机迁移服务（ SMS ）

支持身份策略的区域

表 11-1 支持身份策略的区域

区域名称	区域代码
亚太-新加坡	ap-southeast-3

 版权所有 © 华为云计算技术有限公司

区域名称	区域代码
亚太-曼谷	ap-southeast-2
亚太-雅加达	ap-southeast-4
华东-上海一	cn-east-3
华东-上海二	cn-east-2
中国-香港	ap-southeast-1
华北-北京一	cn-north-1
华北-北京四	cn-north-4
华南-广州	cn-south-1
华南-广州-友好用户环境	cn-south-4
华北-乌兰察布-汽车一	cn-north-11
华北-乌兰察布一	cn-north-9
西南-贵阳一	cn-southwest-2
华东-青岛	cn-east-5
土耳其-伊斯坦布尔	tr-west-1
非洲-约翰内斯堡	af-south-1
拉美-墨西哥城一	na-mexico-1
拉美-墨西哥城二	la-north-2
拉美-圣保罗一	sa-brazil-1
拉美-圣地亚哥	la-south-2
中东-利雅得	me-east-1
非洲-开罗	af-north-1
华东二	cn-east-4

 版权所有 © 华为云计算技术有限公司

12 绑定安全密钥

本章主要介绍如何在登录控制台时绑定安全密钥。

约束与限制

一个IAM用户最多支持绑定8个安全密钥。

操作步骤

步骤1 使用账号或IAM用户登录控制台。

步骤2 在登录验证过程中，选择“安全密钥”。单击“立即绑定”。

图 12-1 登录验证

步骤3 在右侧弹窗中，设置MFA设备名称。

仅支持大小写字母、数字或特殊字符(-_)。不能与已有的MFA设备同名。

步骤4 设备类型选择“安全密钥”。单击“下一步”。

 版权所有 © 华为云计算技术有限公司

步骤5 如需要设置Windows Hello的验证方式，需要在弹窗中选择验证方式。

图 12-2 设置 Windows Hello

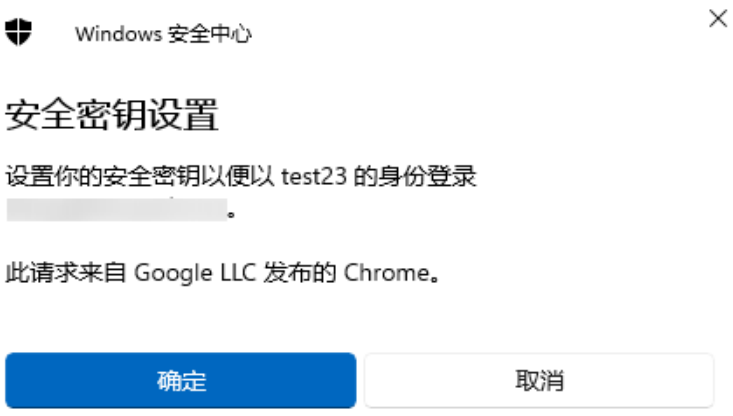
说明

如设备不支持开启人脸识别，则将不会出现“面孔”选项。

步骤6 如需要设置FIDO类型的安全密钥，则在弹窗中单击“取消”。

步骤7 在新的弹窗中，单击“确定”。

图 12-3 确认安全密钥设置



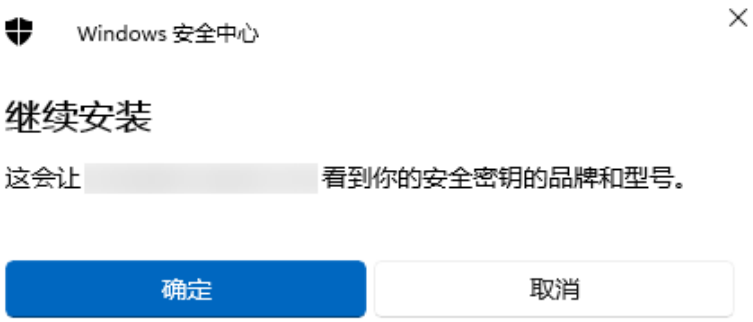
步骤8 将安全密钥设备插入计算机USB端口并轻点密钥上的按钮。

 版权所有 © 华为云计算技术有限公司

图 12-4 插入安全密钥

步骤9 在确认继续的弹窗中，单击“确定”。

图 12-5 确认继续安装



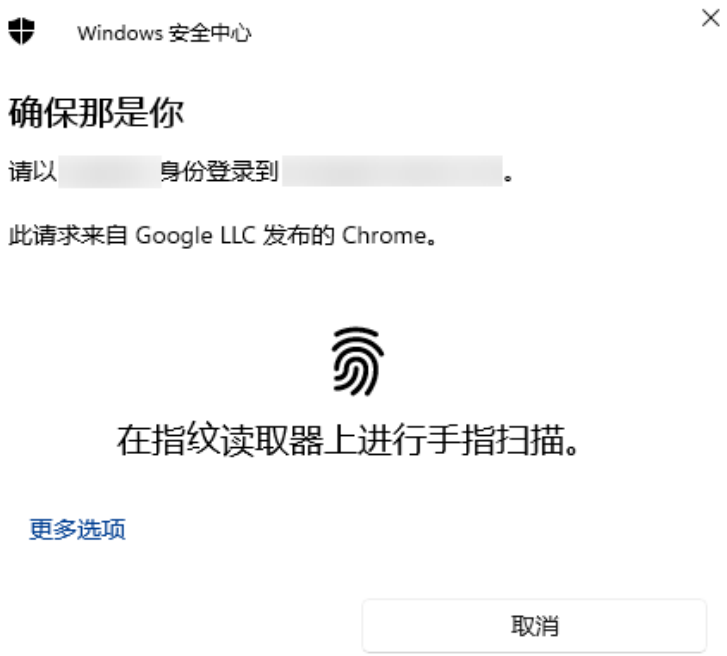
步骤10 系统认证成功后，将会出现“绑定成功”的提示弹窗。单击“确定”。

图 12-6 绑定成功

步骤11 系统将会立即提示需要进行安全密钥身份验证。以下以指纹验证为例。

 版权所有 © 华为云计算技术有限公司

图 12-7 指纹验证



步骤12 验证成功后，成功登录控制台访问云服务。

----结束

 版权所有 © 华为云计算技术有限公司