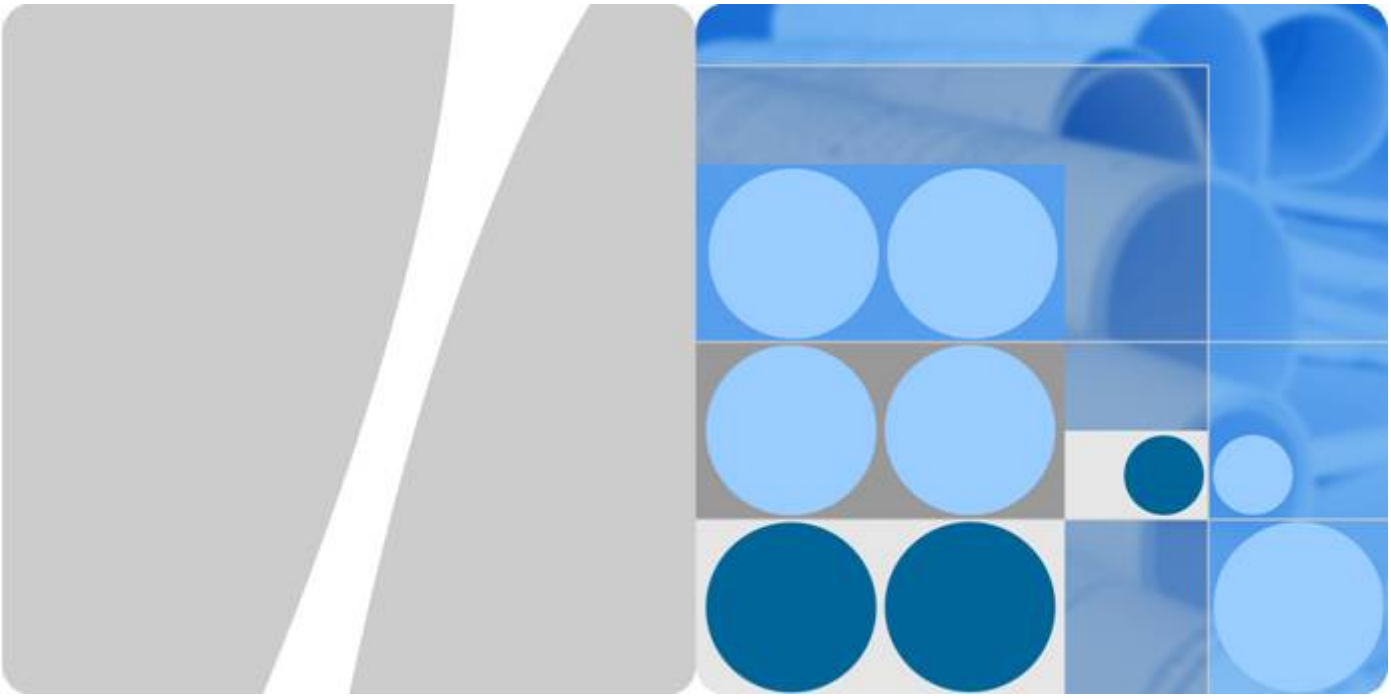


统一身份认证服务

用户指南

文档版本　11

发布日期　2018-02-13

华为技术有限公司

版权所有 © 华为技术有限公司 2018。 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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

版权所有 © 华为技术有限公司

版权所有 © 华为技术有限公司

1 概述

统一身份认证（Identity and Access Management，简称IAM）为公有云系统（华为云）提供身份管理和访问控制功能。

通过IAM您可以管理用户（比如员工、系统或应用程序）账号，并且可以管控这些用户账号对您名下资源（如：虚拟私有云、云审计服务等）具有的操作权限，从而避免与其他用户共享您的密码或访问密钥。也可以通过设置登录验证策略、密码策略、访问控制列表来确保用户账号的安全，从而降低您的企业信息安全风险。

IAM无需付费即可使用，您只需要为您账号中的资源进行付费。

1.1 IAM 功能

IAM为您提供身份认证及权限管理等基本功能，帮助您控制哪些用户可以访问您账号中的资源。

- 资源的共享访问

  当您想与其他用户共享您账号中的资源时，您不需要与他人共享您的密码或访问密钥。您可以使用账号登录IAM创建用户并授予其管理和使用您账号中的资源的权限。其他用户可以使用自己的账号登录公有云系统访问您账号中的资源。
- 资源的隔离管理

  您可以使用IAM将您账号中的资源按区域进行隔离，或按照部门或项目组进行分组，使这些部门或项目组之间的资源完全隔离。
- 便捷的用户授权

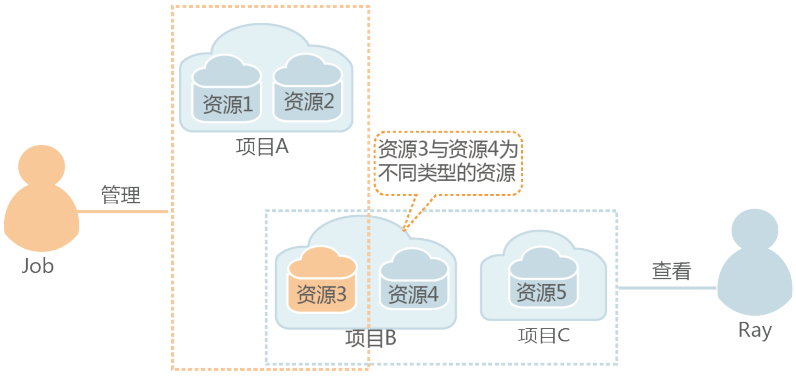
  使用IAM完成用户授权仅需要两步：

  a. 按照用户职责规划用户组，并将对应职责的权限授予用户组。

  b. 将用户加入用户组。
- 精细的权限管理

  使用IAM您可以针对不同的项目以及项目中的某个资源进行授权，从而控制不同的用户访问不同的资源。如：控制某些人员访问并使用对象存储服务，而让另外一些人只能从对象存储服务中读取数据。

华为专有和保密信息
版权所有 © 华为技术有限公司



- 联邦身份认证管理

  您可以将公有云系统和其他系统建立信任关系，并允许其他系统的用户访问您账号中的资源。您可以通过设置规则来管控哪些用户能够访问哪些资源。
- 支持第三方系统的用户管理公有云系统的资源

  第三方系统与公有云系统成功对接后，将第三方系统中的用户与IAM中的账号进行绑定（如果没有账号，需要创建后绑定）。绑定后的用户可以通过第三方系统登录后直接访问公有云系统并管理资源。
- 委托其他账号管理您账号中的资源
- 为公有云其他服务提供认证和授权功能

  使用IAM认证后的用户可以根据权限使用公有云系统中的其他服务，如：关系型数据库、云审计服务、对象存储服务等。
- 集中管理安全策略

  通过设置登录验证策略、密码策略及访问控制列表来提高用户信息和系统数据的安全性。
- 自主管理账号信息

  用户可以管理自己的登录密码、访问密钥、绑定的邮箱和手机号码等信息，也可以查询用户ID以及可管理的项目信息等。
- 使用伙伴云

  云联盟用户可以在归属云华为云的管理控制台跳转到伙伴云Orange Cloud for Business 的管理控制台来使用伙伴云的资源及服务。

1.2 IAM 访问方式

介绍访问公有云系统的IAM服务的方式。

- 通过公有云系统的登录界面访问IAM

  通过公有云系统的登录界面直接登录进入管理控制台，选择“管理与部署 > 统一身份认证服务”即可访问IAM。
  - 账号登录方法请参考：**3.1 账号登录管理控制台**。
  - IAM用户登录方法请参考：**3.5 IAM用户登录管理控制台**。
- 通过API访问IAM

  通过调用IAM接口以编程的方式访问IAM。该方法通过Token或访问密钥的方式进行身份认证。

华为专有和保密信息
版权所有 © 华为技术有限公司

1.3 IAM 身份管理

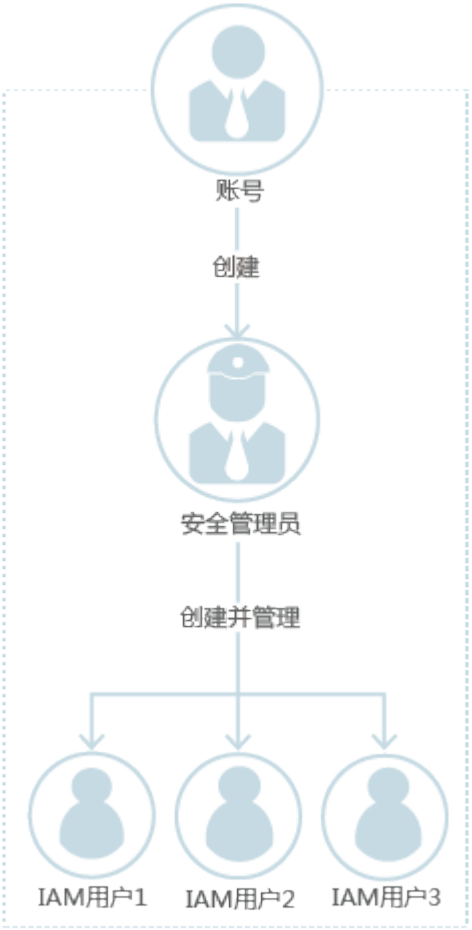
您可以通过IAM管理您账号中的用户及其安全凭证，也可以通过IAM的联邦身份认证让其他系统的用户直接访问公有云系统，实现单点登录，让用户管理更简单。

账号

用户注册华为云后自动创建，该账号对其所拥有的资源具有完全的访问权限。

由于账号是费用承载的主体，为了确保账号的安全性，建议您为自己的账号创建安全管理员（具有Security Administrator权限），使用安全管理员管理账号中的用户及其权限。

图 1-1 账号管理模型

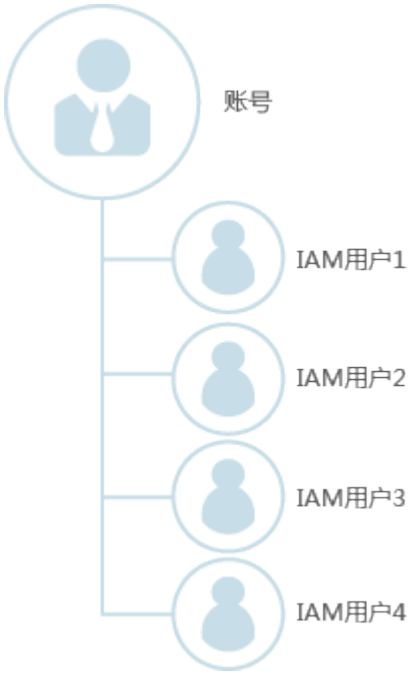


IAM 用户

由管理员在IAM中创建的用户，是云服务的使用人员，对应员工、系统或应用程序，具有身份凭证（密码和访问密钥），可以登录管理控制台或者访问API。

版权所有 © 华为技术有限公司

图 1-2 账号与 IAM 用户的关系



联邦用户

通过联邦身份认证方式访问公有云系统的用户称为联邦用户。

联邦身份认证是指用户通过身份提供商认证后，不需要通过服务提供商再次认证即可访问服务提供商的资源。

- 身份提供商（Identity Provider，简称IdP ）是为用户提供身份认证的系统。在IAM联邦身份认证中身份提供商指企业自身的身份认证系统（如：企业管理系统）。
- 服务提供商（Service Provider，简称SP）是指为用户提供服务的系统，指公有云系统。

IdP的用户通过联邦身份认证访问公有云系统时，仅需要使用IdP提供的安全凭证（无需IAM为其生成新的安全凭证）即可访问公有云系统，即实现单点登录。

图 1-3 联邦用户访问公有云系统流程

1.4 IAM 权限管理

您可以通过IAM控制不同用户访问不同的资源。

版权所有 © 华为技术有限公司

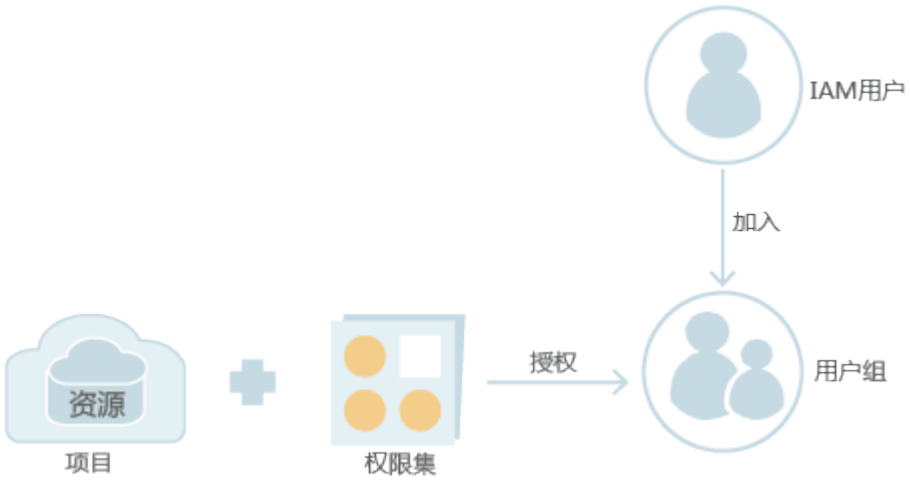
为 IAM 用户授权

您需要先了解表1中的基本概念。

表 1-1 基本概念

概念	含义
用户组	用户组是拥有相同职责的IAM用户的集合。将项目中的资源对应的权限集授予用户组，再将IAM用户加入到用户组，使用户组中的IAM用户继承用户组中的权限。
项目	项目用于将OpenStack的资源（计算资源、存储资源和网络资源等）进行分组和隔离。项目可以是一个部门或者一个项目组。一个账号可以在不同的区域下创建多个项目。可以基于项目为用户授权。
资源	资源是公有云系统中可以使用的服务。如：弹性云服务器、云硬盘、云审计服务等。
权限	权限是控制用户可以执行的操作。权限分为两类：用户管理权限和资源管理权限。 ● 用户管理权限：管理用户、管理用户组、为用户组授权、管理委托、设置安全策略等。 ● 资源管理权限：可以对资源执行的操作。如：是否可以创建云硬盘。
权限集	权限集指一组权限的集合。如：Security Administrator为一个权限集，包括创建用户、删除用户、为用户组授权等权限。

图 1-4 授权模型



1. 按照人员的职责规划用户组，再基于项目将职责相关的权限集授予用户组。
2. 将IAM用户加入到用户组中，使这些IAM用户具有该用户组中的权限。

说明

用户在访问资源时需要先切换到对应的项目/区域。方法请参考：**4.1.4 如何切换项目或区域**。

华为专有和保密信息
版权所有 © 华为技术有限公司

当人员变动时，只需要修改用户所属的用户组。使用用户组管理权限更加高效。

为其他账号授权

您（账号A）的安全管理员通过在IAM上创建委托，指定委托账号（账号B）及对应的权限，即可与账号B共享指定资源。账号B的安全管理员为IAM用户分配Agent Operator权限后，账号B的IAM用户即可通过切换角色（切换到账号A）的方式访问您账号中的资源。

为联邦用户授权

通过在IAM上创建身份提供商并为联邦用户创建相关的规则，使得联邦用户转换为IAM中的身份，实现通过IAM控制联邦用户访问公有云资源的权限。

图 1-5 联邦用户身份转换原理

华为专有和保密信息
版权所有 © 华为技术有限公司

2 开始使用

获取账号

- 如果您已有华为云的账号，可以直接使用。
- 如果您没有账号，可以访问**https://www.huaweicloud.com/**注册，注册账号时需要提供手机号码作为您的凭证。 注册方法请参考：**2.1 如何注册账号**。

给用户授权

访问权限类型	授权场景	授权方法
IAM用户	通过IAM创建用户，并管理他们的权限： ● 可以使用哪些资源。 ● 是否可以管理用户。	1. 需要先根据用户职责创建用户组，并将职责相关的权限授予用户组。方法请参考：**4.1.2 如何创建用户组并授权**。 2. 创建用户并将用户加入到对应职责的用户组中。方法请参考：**4.1.3 如何创建用户**。
联邦用户的访问权限	允许其他IdP的用户访问的资源。	1. 创建身份提供商。方法请参考：**4.4.4 如何创建身份提供商**。 2. 配置联邦身份用户单点登录，方法请参考：**4.4.4 如何创建身份提供商**。 3. 为联邦身份用户授权，方法请参考：**4.4.7 如何通过规则控制联邦用户访问公有云资源**。
其他账号的访问权限	您想要与其他账号共享某些资源。	1. 创建委托并定义委托的访问权限，方法请参考：**4.3.1 如何创建委托**。 2. 被委托方可以通过切换角色来访问您账号中的资源，方法请参考：**4.3.2 如何切换角色**。

2.1 如何注册账号

当用户首次使用华为云时，需要注册华为云的账号。

华为专有和保密信息
版权所有 © 华为技术有限公司

操作步骤

步骤1 打开**https://www.huaweicloud.com**。

进入华为云首页。

步骤2 单击右上方“注册”。

步骤3 在“注册”页面，设置用户名、密码和手机号信息。

说明

定期修改密码可以提高账号的安全性。密码符合如下复杂度要求：

- 密码不能是用户名或者用户名的倒序（不区分大小写），例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a;
- 不能包含手机号;
- 不能少于6个字符且不超过32个字符;
- 包括大写字母（A~Z），小写字母（a~z），数字（0~9）和特殊字符（空格!"#$%&'()*+,-./:;<=>?@[]^`{_|}~）至少2种的组合。

步骤4 单击“获取短信验证码”并输入短信验证码。

步骤5 单击“同意协议并注册”，完成注册。

----结束

华为专有和保密信息
版权所有 © 华为技术有限公司

3 新手入门

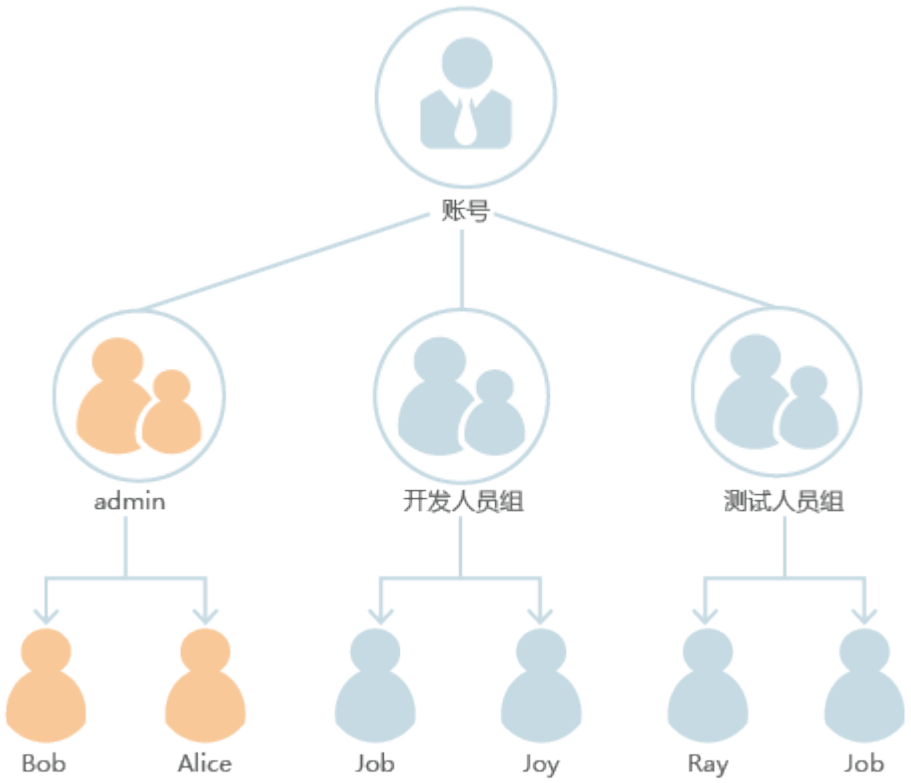
首先需要为您的账号创建一个安全管理员。

示例

我们以如下示例帮助您快速了解如何使用IAM。

账号中有3种职责的用户，一个职责对应一个用户组：安全管理员组（名称为admin）、开发人员用户组和测试人员用户组。每个用户组可以有多个用户，同一个用户也可以属于多个用户组。

图 3-1 用户管理模型



华为专有和保密信息
版权所有 © 华为技术有限公司

1. 使用您的账号创建一个安全管理员（Bob），并将Bob加入到缺省用户组“admin”中。方法请参考：**3.2 创建安全管理员**。
2. 使用您的安全管理员（Bob）创建其他安全管理员（Alice），并将Alice加入到缺省用户组“admin”中。方法请参考：**3.2 创建安全管理员**。
3. 由安全管理员（Bob或Alice）创建用户组“开发人员组”和“测试人员组”并分别为两个用户组授予对应的权限。方法请参考：**3.3 创建用户组并授权**。
4. 由安全管理员（Bob或Alice）创建开发人员用户（Job、Joy），并将Job和Joy加入到“开发人员组”用户组中；创建测试人员用户（Ray），并将Ray和Job加入到“测试人员组”用户组中。方法请参考**3.4 创建IAM用户并加入用户组**。

3.1 账号登录管理控制台

使用账号登录公有云系统后，您具有所有资源的访问权限，并可以管理IAM用户。为了确保账号安全，请妥善保管账号的密码和访问密钥。

操作步骤

步骤1 打开**https://www.huaweicloud.com**。

进入华为云首页。

步骤2 单击页面右上方“登录”。

进入“账号登录”页面。

步骤3 输入“账号名/邮箱/电话号码”和“密码”，并单击“登录”。

登录成功后，进入华为云首页。

步骤4 单击页面右上方“控制台”。

进入华为云管理控制台。

----结束

3.2 创建安全管理员

为了确保安全性，建议您为自己创建安全管理员来代替使用账号管理IAM用户。

前提条件

已使用账号或安全管理员（具备“Security Administrator”权限）登录公有云系统。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“用户”。

步骤3 在“用户”界面，单击“创建用户”。

步骤4 在“创建用户”界面，输入“用户名”。

步骤5 选择“凭证类型”为“密码”。

版权所有 © 华为技术有限公司

说明

- 密码用于登录管理控制台，也可以用于API、CLI、SDK等开发工具进行认证，认证成功后可以访问资源。安全管理员用于管理IAM用户，因此建议您选择“凭证类型”为“密码”。
- 访问密钥用于API、CLI、SDK等开发工具认证，完成认证后可以访问资源。

步骤6 在“所属用户组”的下拉复合框中，选择“admin”用户组。

步骤7 单击“下一步”。

步骤8 选择“密码生成方式”为“自定义”。

说明

安全管理员用于登录管理控制台管理IAM用户。如果您为自己创建安全管理员，建议使用自定义方式设置密码。如果您为他人创建安全管理员，建议使用“首次登录时设置”的方式，由用户自己设置密码。

步骤9 输入“邮箱”、“手机”、“密码”和“确认密码”。

说明

- 建议您为管理员设置邮箱或手机号码，作为安全管理员的凭证。
- 密码必须满足如下复杂度要求:

  不能少于6个字符且不超过32个字符。

  包括大写字母（A~Z），小写字母（a~z），数字（0~9）和特殊字符（空格!"#$%&'()*+,-./:;<=>?@[]^`{_|}~）至少2种的组合。

  不能是用户名或者用户名的倒序（不区分大小写），例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a。

  不能包含手机号或邮箱。

  新密码不能与旧密码相同。

步骤10 单击“确定”。

----结束

3.3 创建用户组并授权

您可以根据用户职责规划用户组。使用安全管理员访问IAM并创建用户组，再根据职责赋予用户组对应的权限。

前提条件

已使用安全管理员（具备“Security Administrator”权限）登录公有云系统。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“用户组”。

步骤3 在“用户组”界面中，单击“创建用户组”。

步骤4 输入“用户组名称”。

步骤5 （可选）输入“描述”。

步骤6 单击“确定”。

华为专有和保密信息
版权所有 © 华为技术有限公司

返回用户组列表，用户组列表中显示新创建的用户组。

步骤7 单击新建用户组“操作”列的“修改”。

进入“修改用户组”界面。

步骤8 在“用户组权限”区域中，单击需要授权项目“操作”列的“修改”。

说明

授予的权限仅对当前项目生效。如果需要为用户组授予多个项目的权限，请分别单击所需要授权的项目对应的“修改”进行授权。

步骤9 在“修改用户组权限”对话框中的“可选择权限集”区域选择权限集。

说明

- 系统默认提供的权限集请参见：**默认权限**。
- 选中某一权限集名称，在下侧“权限集信息”区域可以查看该权限集的详细信息（JSON格式）。具体说明请参见：**权限集信息**。

步骤10 单击“确定”。

步骤11 单击“确定”。

----结束

3.4 创建 IAM 用户并加入用户组

您可以使用安全管理员访问IAM并创建用户并将用户加入到对应的用户组中，使其继承用户组中的权限。

前提条件

已使用安全管理员（具备“Security Administrator”权限）登录公有云系统。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“用户”。

步骤3 在“用户”界面，单击“创建用户”。

步骤4 在“创建用户”界面，输入“用户名”。

步骤5 选择“凭证类型”。

凭证类型	适用场景
密码	● 登录管理控制台。 ● 使用支持密码认证的API、CLI、SDK等开发工具来访问云服务。
访问密钥	使用支持密钥认证的API、CLI、SDK等开发工具来访问云服务。

步骤6 在“所属用户组”的下拉框中，选择需要加入的用户组。

华为专有和保密信息
版权所有 © 华为技术有限公司

说明

- 您也可以通过输入关键字快速找到相关用户组。
- 一个用户可以同时加入多个用户组。

根据步骤5中选择的凭证类型，进行后续操作。

凭证类型	后续操作
密码	请执行步骤7。
访问密钥	单击“确认”。下载生成的密钥，创建用户操作完成。 **说明** 访问密钥是在IAM中认证的凭证，如果不下载生成的密钥则无法获取对应的访问密钥。如果该用户需要使用访问密钥在IAM中认证，需要重新生成。生成方法请参考：**4.5.3 如何管理访问密钥**。

步骤7 选择“密码生成方式”。

密码生成方式	说明	后续操作
首次登录时设置	系统会通过邮件发送一次性登录链接给用户。用户使用该链接登录管理控制台时设置密码。	1. 输入“邮箱”。用于接收登录链接。 2. （可选）输入“手机”。 3. 单击“确定”。
自动生成	由系统随机生成10位密码。适用于使用支持密码认证的API、CLI、SDK等开发工具来访问云服务。	1. （可选）输入“邮箱”。 2. （可选）输入“手机”。 3. 单击“确定”。 4. 下载密码文件。

华为专有和保密信息
版权所有 © 华为技术有限公司

密码生成方式	说明	后续操作
自定义	自定义用户的登录密码。	1. （可选）输入“邮箱”。 2. （可选）输入“手机”。 3. 输入“密码”和“确认密码”。 **说明** 密码必须满足如下策略: – 不能少于6个字符且不超过32个字符。 – 包括大写字母（A~Z），小写字母（a~z），数字（0~9）和特殊字符（空格!"#$%&'()*+,-./:;<=>?@[]^`{_|}~）至少2种的组合。 – 不能是用户名或者用户名的倒序（不区分大小写），例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a。 – 不能包含手机号或邮箱。 4. 单击“确定”。

用户可以使用用户名、邮箱或手机号码任意一种方式登录公有云系统。登录方法请参考：**3.5 IAM用户登录管理控制台**。

----结束

3.5 IAM 用户登录管理控制台

IAM用户可以使用账号名、用户名/邮箱/手机、密码来登录管理控制台。

背景信息

- 如果第三方系统用户未在公有云系统中设置登录密码：
  - 通过公有云系统登录页面的找回密码功能设置登录密码。

    说明

    适用于用户已绑定了邮箱或手机。
  - 请联系并提供邮箱给账号的安全管理员（具有Security Administrator权限的用户）。安全管理员通过统一身份认证的用户管理功能重置用户密码，具体操作请参考：**4.1.5 如何查看或修改用户信息**。
- 当开启以下任一功能时，IAM用户登录成功后，需要在“登录验证”页面单击“确定”后才能进入管理控制台。
  - “账号策略”中开启“最近登录提示”功能。
  - “账号策略”中设置了登录成功时的验证信息。

华为专有和保密信息
版权所有 © 华为技术有限公司

- “我的凭证”中开启“登录时短信验证”功能。

以上设置方法请参考：**4.2 如何设置账号安全策略**和**4.5.2 如何修改安全凭证**。

操作步骤

步骤1 打开**https://www.huaweicloud.com**。

步骤2 单击页面右上方“登录”。

步骤3 单击“IAM用户登录”。

步骤4 输入“账号名”、“用户名/邮箱/手机号码”和“密码”，并单击“登录”。

说明

- IAM用户首次登录时，需在“首次登录”页面修改初始密码，定期修改密码可以提高账号的安全性。
- 密码必须满足如下策略:

  不能少于6个字符且不超过32个字符。

  包括大写字母（A~Z），小写字母（a~z），数字（0~9）和特殊字符（空格!"#$%&'()*+,-./:;<=>?@[]^`{_|}~）至少2种的组合。

  不能是用户名或者用户名的倒序（不区分大小写），例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a。

  不能包含手机号或邮箱。
- 如果IAM用户已经开启登录时短信验证功能，在“登录验证”页面还需输入短信验证码进行验证。若需要更换手机号，可以单击“更换手机号码”，完成更换。

步骤5 单击页面右上方“控制台”。

进入管理控制台。

----结束

3.6 IAM 用户通过开发工具访问公有云系统

IAM用户通过开发工具访问公有云系统时，可以使用Token或访问密钥作为安全凭证。

- Token的获取方法请参考：**获取用户Token**。
- 访问密钥的获取方法请参考：**4.5.3 如何管理访问密钥**。

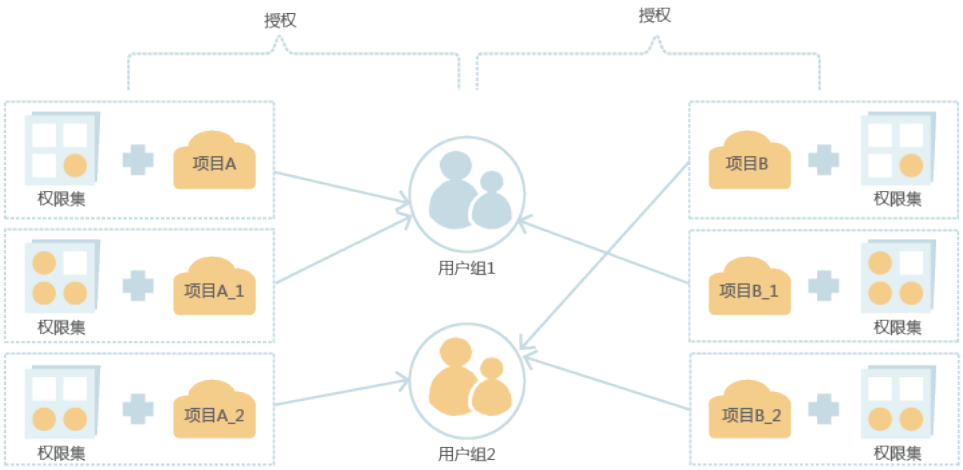
华为专有和保密信息
版权所有 © 华为技术有限公司

4 教程

4.1 管理用户及其权限

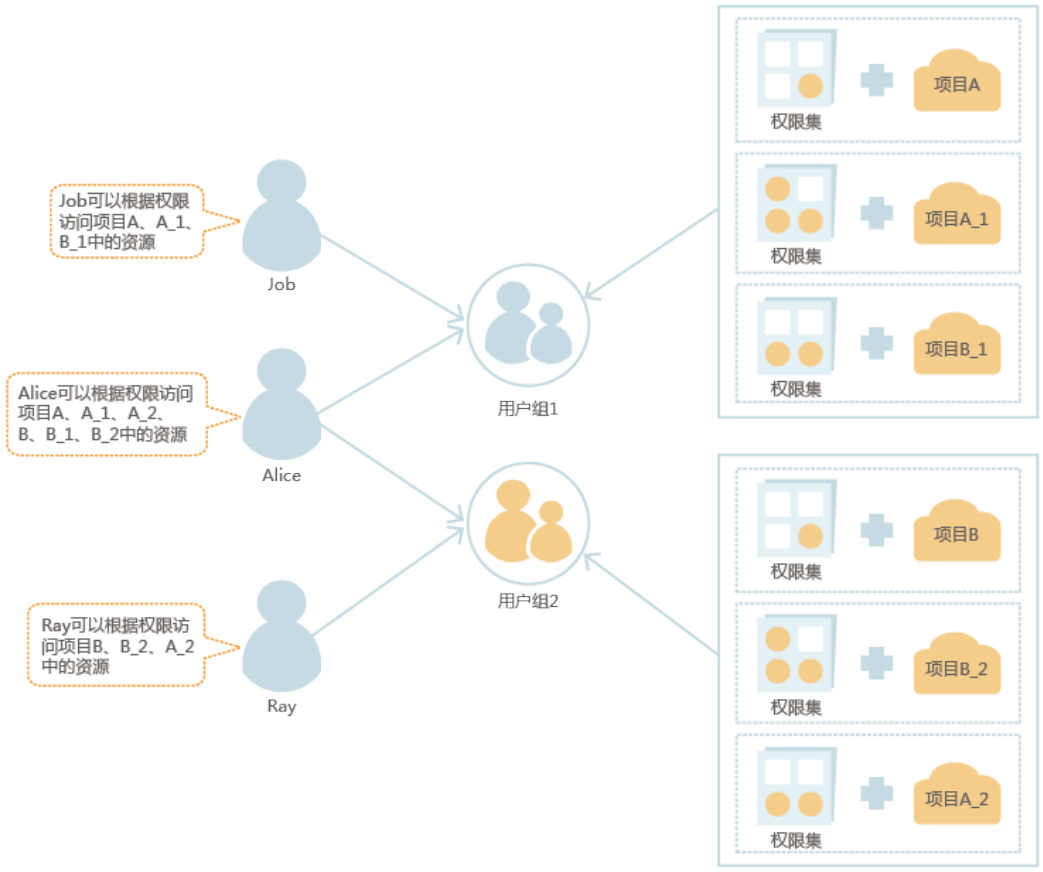
您可以通过为用户组授权并将用户加入到用户组的方式，使用户具有用户组中的权限。用户登录公有云系统后，切换到对应的项目即可根据权限访问公有云资源。

步骤1 安全管理员按照用户职责规划用户组并为用户组授权。方法请参考：**4.1.2 如何创建用户组并授权**。



步骤2 安全管理员创建用户并根据用户职责将用户加入到对应的用户组中。方法请参考：**4.1.3 如何创建用户**。

华为专有和保密信息
版权所有 © 华为技术有限公司



步骤3 用户根据权限访问公有云系统中的资源。

1. 登录公有云系统。方法请参考：**3.5 IAM用户登录管理控制台**。
2. 切换项目或区域。方法请参考：**4.1.4 如何切换项目或区域**。
3. 根据权限访问公有云系统中的资源。

----结束

4.1.1 如何管理项目

项目用于将OpenStack的资源（计算资源、存储资源和网络资源）进行分组和隔离。您账号中的资源必须挂载在项目下，项目可以是一个部门或者项目组。您可以使用安全管理员访问IAM，并在区域下创建项目，来实现资源的隔离管理。

前提条件

登录用户已具备“Security Administrator”权限。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“项目”。

步骤3 在“项目”界面，单击“创建项目”。

华为专有和保密信息
版权所有 © 华为技术有限公司

步骤4 在“所属区域”下拉列表中选择待创建项目所属的区域。

步骤5 输入“项目名称”。

说明

- 项目名称的格式为：*区域名称_项目名称*，区域名称不允许修改。
- 项目名称可以由字母、数字、下划线（_）、中划线（-）组成。“区域名称_项目名称”的总长度不能大于64个字符。

步骤6 （可选）输入“描述”。

步骤7 单击“确定”。

返回项目列表，单击**步骤4**选择的区域对应行的 ，显示新创建的项目，新创建的项目“状态”显示为“正常”。

----结束

后续处理

- 给项目授权

  在“修改用户组”界面，“用户组权限”区域中，单击需要设置的项目对应的“修改”，给对应项目选择需要的云资源权限集。详情请参见**4.1.2 如何创建用户组并授权**。

- 开启云审计服务

  如果需要通过云审计服务记录在新创建的项目中云服务的操作，需要在当前项目下重新开启云审计服务。方法请参考： **开启云审计服务**。

相关任务

- 查看项目的详细信息

  a. 在项目列表单击待查看项目所属区域前的 ，查看对应区域下面的项目。

  b. 在“操作”列单击对应项目的“查看”。

  查看项目的详细信息以及绑定在该项目上面的用户。

  说明

  通过为用户组授予对应项目的权限，再将用户加入到用户组中，使用户继承用户组的权限，并实现用户与项目之间的绑定。用户通过**切换项目**来访问对应的资源。

  c. 单击用户权限列表“权限”列的“查看”。

  查看绑定在项目上面的用户对应的权限。

- 修改项目

  a. 在项目列表单击待修改项目所属区域前的 。

  b. 在“操作”列单击对应项目的“修改”，在“修改项目”页面修改项目名称和描述信息。

  说明

  项目名称的格式为：*区域名称_项目名称*，区域名称不允许修改。

- 切换项目，方法请参考**4.1.4 如何切换项目或区域**。

华为专有和保密信息
版权所有 © 华为技术有限公司

4.1.2 如何创建用户组并授权

您可以根据用户职责规划用户组，并赋予用户组对应职责的权限，使得用户组中的用户拥有对应职责的权限。通过用户组来管理用户权限可以使权限管理更有条理。

前提条件

登录用户已具备“Security Administrator”权限。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“用户组”。

步骤3 在“用户组”界面中，单击“创建用户组”。

步骤4 输入“用户组名称”。

步骤5 （可选）输入“描述”。

步骤6 单击“确定”。

返回用户组列表，用户组列表中显示新创建的用户组。

步骤7 单击新建用户组“操作”列的“修改”。

步骤8 在“用户组权限”区域中，单击需要授权项目“操作”列的“修改”。

说明

授予的权限仅对当前项目生效。如果需要为用户组授予多个项目的权限，请分别单击所需要授权的项目对应的“修改”进行授权。

步骤9 在“修改用户组权限”对话框中的“可选择权限集”区域选择权限集。

说明

- 系统默认提供的权限集请参见：**默认权限**。
- 选中某一权限集名称，在下侧“权限集信息”区域可以查看该权限集的详细信息（JSON格式）。具体说明请参见：**权限集信息**。

步骤10 单击“确定”。

步骤11 在“包含用户”区域的下拉复合框中，选择用户加入到用户组。

说明

您也可以通过输入关键字快速找到相关用户。

步骤12 单击“确定”。

----结束

相关任务

4.1.6 如何查看或修改用户组

华为专有和保密信息
版权所有 © 华为技术有限公司

4.1.3 如何创建用户

当您需要与新用户共享您账号中的资源时，您可以使用安全管理员通过IAM创建用户。创建用户时可以为他们设置安全凭证和权限。这些用户可以通过管理控制台或API、CLI、SDK等开发工具访问公有云系统。

前提条件

登录用户已具备“Security Administrator”权限。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“用户”。

步骤3 在“用户”界面，单击“创建用户”。

步骤4 在“创建用户”界面，输入“用户名”。

步骤5 选择“凭证类型”。

凭证类型	适用场景
密码	● 登录管理控制台。 ● 使用支持密码认证的API、CLI、SDK等开发工具来访问云服务。
访问密钥	使用支持密钥认证的API、CLI、SDK等开发工具来访问云服务。

步骤6 在“所属用户组”的下拉框中，选择需要加入的用户组。

说明

- 您也可以通过输入关键字快速找到相关用户组。
- 一个用户可以同时加入多个用户组。

根据步骤5中选择的凭证类型，进行后续操作。

凭证类型	后续操作
密码	请执行步骤7。
访问密钥	单击“确认”。下载生成的密钥，创建用户操作完成。 **说明** 访问密钥是在IAM中认证的凭证，如果不下载生成的密钥则无法获取对应的访问密钥。如果该用户需要使用访问密钥在IAM中认证，需要重新生成。生成方法请参考：**4.5.3 如何管理访问密钥**。

步骤7 单击“下一步”。

步骤8 选择“密码生成方式”。

华为专有和保密信息
版权所有 © 华为技术有限公司

密码生成方式	说明	后续操作
首次登录时设置	系统会通过邮件发送一次性登录链接给用户。用户使用该链接登录管理控制台时设置密码。	1. 输入“邮箱”。用于接收登录链接。 2. （可选）输入“手机”。 3. 单击“确定”。
自动生成	由系统随机生成10位密码。适用于使用支持密码认证的API、CLI、SDK等开发工具来访问云服务。	1. （可选）输入“邮箱”。 2. （可选）输入“手机”。 3. 单击“确定”。 4. 下载密码文件。
自定义	自定义用户的登录密码。	1. （可选）输入“邮箱”。 2. （可选）输入“手机”。 3. 输入“密码”和“确认密码”。 **说明** 密码必须满足如下策略: – 不能少于6个字符且不超过32个字符。 – 包括大写字母（A~Z），小写字母（a~z），数字（0~9）和特殊字符（空格!"#$%&'()*+,-./:;<=>?@[]^`{_|}~）至少2种的组合。 – 不能是用户名或者用户名的倒序（不区分大小写），例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a。 – 不能包含手机号或邮箱。 4. 单击“确定”。

说明

- 只有当用户同时绑定“邮箱”和“手机”，才能使用登录时短信验证功能，该功能的开启方法请参见4.5.2 如何修改安全凭证。
- 用户可以使用此处设置的用户名、邮箱或手机号码任意一种方式登录系统。
- 当用户忘记密码时，可以通过此处绑定的邮箱或手机号码来重置密码。

步骤9 单击“确定”。

创建用户完成。

----结束

版权所有 © 华为技术有限公司

相关任务

- 查看用户信息和修改用户信息（包括用户状态、绑定的邮箱、绑定的手机号码、所属用户组、用户日志等）。方法请参考：**4.1.5 如何查看或修改用户信息**。
- 删除用户：在用户列表中，单击“删除”。

4.1.4 如何切换项目或区域

不同区域中的资源互相隔离，仅能访问当前区域下的资源。如果您需要访问其他区域下的资源，需要先切换到对应的区域下。

操作步骤

步骤1 登录公有云系统，进入管理控制台。

步骤2 单击左上角的 ，在下拉框中选择需要访问的项目或区域。

切换至目标项目或区域即可访问对应的资源。

----结束

4.1.5 如何查看或修改用户信息

安全管理员可以查看和修改用户的基本信息、所属用户组以及用户日志。当人员职责发生变动时，安全管理员可以通过修改用户所属的用户组来修改用户所拥有的权限。当用户忘记或遗失密码或访问密钥时，安全管理员可以重置用户的登录认证凭证。

前提条件

登录用户已具备“Security Administrator”权限。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“用户”。

步骤3 在用户列表中，可查看、修改用户的基本信息，以及设置用户的凭证。

- 查看用户基本信息

  在用户列表中，单击 查看用户的详细信息。包括基本信息、所属用户组以及用户日志。

- 修改用户基本信息

  在用户列表中，单击对应用户右侧的“修改”，进入“修改用户”界面，可以修改用户的基本信息和所属用户组。

  - 修改用户状态：用户默认为“启用”状态，如果需要停止使用该用户，可以在“基本信息”区域设置用户“状态”为“停用”。
  - 修改登录时登录时短信验证：
    - 该功能默认不开启，当用户同时绑定了邮箱和手机，才能开启该功能。
    - 开启该功能后，登录公有云系统时，需要在“登录验证”页面输入短信验证码进行验证。
  - 修改用户的邮箱、手机、描述信息。

华为专有和保密信息
版权所有 © 华为技术有限公司

- 修改所属用户组：在“所属用户组”区域的下拉框中选择要加入的用户组，或者单击目标用户组右侧的“删除”，删除选中的用户组。

  说明

  您也可以通过输入关键字快速找到相关用户组。

- 设置用户凭证

  在用户列表中，单击右侧“设置凭证”，可修改用户的密码或管理用户的访问密钥。

凭证类型	生成方式	说明	适用场景
密码	首次登录时设置	系统会通过邮件发送一次性登录链接给用户，用户使用该链接登录管理控制台时设置密码。	已绑定邮箱的用户重置密码。该用户需要使用密码登录管理控制台。
	自动生成	由系统随机生成10位密码。 **说明** 自动生成的密码可以在单击“确认”后下载。	使用支持密码认证的API、CLI、SDK等开发工具通来访问公有云系统的用户重置密码。
	自定义	自定义用户的密码。	任何用户。
访问密钥	用户自己创建或通过安全管理员创建	在“管理访问密钥”区域，可新增或删除访问密钥。	通过访问密钥认证访问公有云系统的用户。

----结束

4.1.6 如何查看或修改用户组

安全管理员可以查看和修改用户组的基本信息、权限及用户组中包含的用户。当多个用户的职责发生相同的变化时可以通过修改用户组的方式快速完成用户权限修改。

前提条件

登录用户已具备“Security Administrator”权限。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“用户组”。

步骤3 在“用户组”列表中，可以查看或修改用户组信息。

- 查看用户组信息

  在用户组列表中，单击 > 查看用户组的详细信息。包括基本信息、用户组权限以及用户组中包含的用户。

- 修改用户组信息

  在用户组列表中，单击对应用户组右侧的“修改”，进入“修改用户组”界面，可以修改用户组的描述信息、用户组权限和用户组中包含的用户。

版权所有 © 华为技术有限公司

说明

系统缺省用户组，只能修改其中包含的用户，不能修改基本信息与权限。

修改信息	修改方法
用户组权限	1. 单击需要授权项目“操作”列的“修改”。 2. 在“可选择权限集”区域中选择权限集。 **说明** ■ 系统默认提供的权限集请参见：**默认权限**。 ■ 选中某一权限集名称，在下侧“权限集信息”区域可以查看该权限集的详细信息（JSON格式）。具体说明请参见：**权限集信息**。 3. 单击“确定”。 4. 单击“确定”。
用户组中包含的用户	- 增加用户 1. 在“包含用户”区域的下拉列表中选择需要加入的用户。 **说明** 您也可以通过输入关键字快速找到相关用户。 2. 单击“确认”。 - 删除用户 1. 在“包含用户”区域的列表中单击需要删除的用户对应“操作”列的“删除”。 2. 单击“确认”。

----结束

相关任务

在用户组列表中，单击 > 可查看用户组的详细信息。

4.1.7 如何修改用户权限

当用户职责发生变化时，您需要通过修改用户所属用户组来修改用户权限。

修改用户权限的方法有以下两种：

- 通过修改用户来修改所属用户组。该方法适用于调整单个用户所属不同的用户组。方法请参考**4.1.5 如何查看或修改用户信息**。
- 通过修改用户组来修改用户组中所包含的用户。该方法适用于将多个用户加入到同一用户组中，或将多个用户从同一用户组中删除。方法请参考：**4.1.6 如何查看或修改用户组**。

4.2 如何设置账号安全策略

拥有安全管理员权限（Security Administrator权限）的用户可以设置登录验证策略、密码策略及访问控制列表来提高用户信息和系统的安全性。

版权所有 © 华为技术有限公司

前提条件

登录用户已具备“Security Administrator”权限。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 设置登录验证策略。

1. 在左侧导航窗格中，选择“账号设置 > 登录验证策略”。
2. 在“账号锁定策略”区域输入“限定时间长度”、“限定时间内登录失败次数”、“账号锁定时长”。

   如果在限定时间长度内达到登录失败次数后，账号会被锁定一段时间。如：在10分钟内连续3次登录失败，用户会被锁定15分钟。15分钟后可以尝试再次登录。
3. 在“账号停用策略”区域，选中“如果账号在有效期内未使用过，则将被停用”，设置“账号有效期限”。
4. 在“最近登录提示”区域中，选中“登录成功时，将看到上次登录的时间等信息”。

   用户将在登录时的“登录验证”页面中看到上次登录的时间等登录提示信息。
5. 在“登录验证提示”区域，自定义登录时的验证信息。

   用户将在“登录验证”页面中看到自定义的验证提示信息。
6. 单击“确定”。

步骤3 设置密码策略。

1. 在左侧导航窗格中，选择“账号设置 > 密码策略”。
2. 在“密码设置策略”区域中，进行如下设置：
   - 设置“密码最小长度”。

     说明

     系统默认值为6个字符。
   - 选择“设置密码时同一字符不能连续出现”，设置密码中允许同一字符连续出现的最大次数。
   - 选择“新密码不能与最近的历史密码相同”，设置新密码不能与最近几次的历史密码相同。
3. 在“密码有效期策略”区域中，选择“密码过期后，系统强制要求修改密码。（距离密码到期15天时开始提示用户修改密码。）”，设置“密码有效期”。

   密码过期后，用户必须根据系统提示修改密码，否则无法登录系统。

   说明

   密码必须满足如下策略:
   - 不能少于6个字符且不超过32个字符。
   - 包括大写字母（A~Z），小写字母（a~z），数字（0~9）和特殊字符（空格!"#$%&'()*+,-./:;<=>? @[]^`{_}~）至少2种的组合。
   - 不能是用户名或者用户名的倒序（不区分大小写），例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a。
   - 不能包含手机号或邮箱。
4. 在“密码最短使用时间策略”区域中，选择“密码初次生成和每次修改之后，密码的使用时间必须超过设置的最短使用时间，才能进行修改”，设置“密码最短使用时间”。

版权所有 © 华为技术有限公司

当用户密码修改后，再次修改密码时需要满足该策略设置的时间后才能修改。

5. 单击“应用”。

步骤4 设置访问控制列表。

1. 在左侧导航窗格中，选择“账号设置 > 访问控制列表”。

   说明

   访问控制列表只对账号下的IAM用户生效，对账号不生效。

2. 在“访问控制列表”界面中，设置允许访问的IP地址或网段。
   - 允许访问的IP地址区间：限制用户只能从设定范围内的IP地址登录系统。
   - 允许访问的IP地址或网段：限制用户只能从设定的IP地址或网段登录系统。

     例如：10.10.10.10/32

   说明

   - 单击“恢复默认值”，可以将“允许访问的IP地址区间”恢复为默认值，即0.0.0.0~255.255.255.255，同时将“允许访问的IP地址或网段”清空。
   - “允许访问的IP地址区间”和“允许访问的IP地址或网段”同时设置时只要满足其中一种即可允许访问。

3. 单击“应用”。

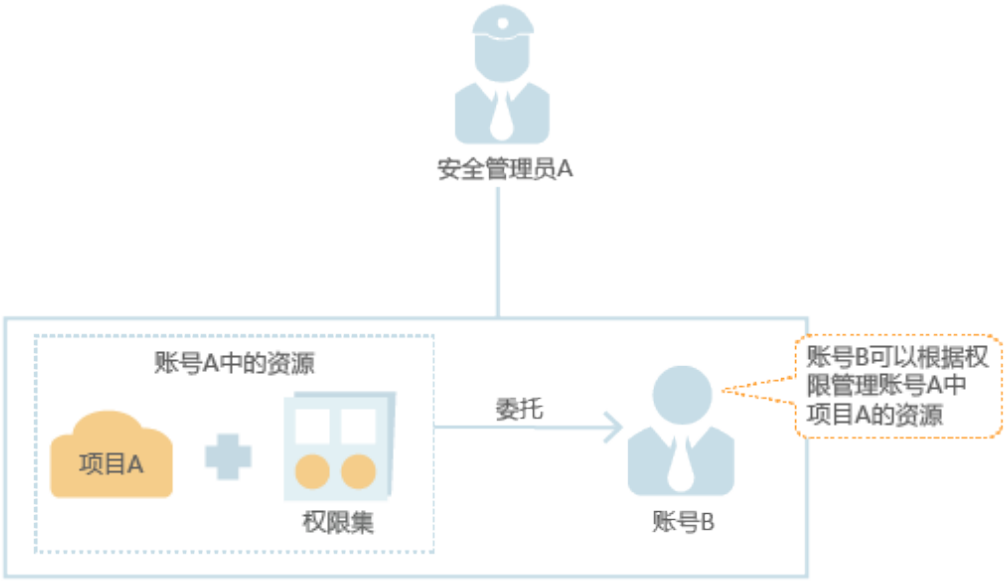
----结束

4.3 委托其他账号管理资源

当需要与其他账号共享资源，或需要委托其他账号管理资源时，可以创建委托并授予被委托方资源管理权限。

以账号A委托账号B管理账号A中的某些资源为例，讲述委托的原理及方法。

步骤1 账号A的安全管理员A创建委托。方法请参考：**4.3.1 如何创建委托**。

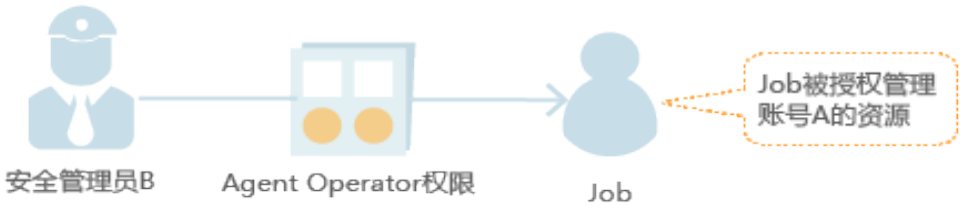


步骤2 账号B的安全管理员B授予用户Job管理账号A资源的权限（Agent Operator）。

1. 创建用户组（如：Agency）并授予Agent Operator权限。

华为专有和保密信息
版权所有 © 华为技术有限公司

2. 将用户Job加入到用户组（Agency）中。



步骤3 账号B的用户Job根据权限管理账号A的资源。

1. Job登录公有云系统。方法请参考：**3.5 IAM用户登录管理控制台**。
2. 切换角色到账号A。方法请参考：**4.3.2 如何切换角色**。
3. 切换到项目A。方法请参考：**4.1.4 如何切换项目或区域**。
4. 根据权限管理账号A的资源。

----结束

4.3.1 如何创建委托

当您希望将您的资源共享给其他账号或委托更专业的人或团队来代理管理您账号中的资源时， 您的安全管理员用户可以通过创建委托的方式使被委托方使用自己的用户登录公有云系统后切换到您的账号下管理您的资源，而不必要将您账号中的用户安全凭证（密码/密钥）共享给其他账号，确保了您的账号安全。

前提条件

登录用户已具备“Security Administrator”权限。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“委托”。

步骤3 在“委托”页面，单击“创建委托”。

步骤4 在“创建委托”页面，设置“委托名称”和“委托类型”。

表 4-1 委托类型

委托类型	描述
普通账号	公有云系统的其他普通账号，用于将资源共享给其他账号或委托更专业的人或团队来代为管理账号中的资源。

版权所有 © 华为技术有限公司

委托类型	描述
云服务	公有云系统服务，用于授权云服务访问或者维护用户数据。例如，通过与ECS建立委托关系，ECS可以获取用户的访问密钥调用API接口，帮助用户运维或者监控数据。 **说明** 委托类型为云服务的委托创建成功后，不支持修改。

- 如果选择“委托类型”为“普通账号”，在“委托的账号”中输入委托账号名称。
- 如果选择“委托类型”为“云服务”，单击“选择”，选择需要委托管理的云服务。

步骤5 设置“持续时间”及“描述”信息。

步骤6 在“权限选择”区域中，单击需要设置的区域对应项目的“修改”。

步骤7 在“修改权限”对话框中的“可选择权限集”区域，给委托企业选择对应的权限集。

说明

具体权限集说明请参见：**权限说明**。

步骤8 单击“确定”。

委托列表中显示新创建的委托。

----结束

后续操作

在委托列表中，单击“修改”，可以修改新建委托的基本信息，包括委托的账号、持续时间等。

说明

只能修改委托类型为普通账号的委托。

4.3.2 如何切换角色

当其他账号委托您管理他的资源时，您的用户登录公有云系统后通过切换角色的方式来管理其他账号中的资源，只有具有“Agent Operator”权限的用户可以切换角色。

前提条件

- 登录用户已具备“Agent Operator”权限。
- 已有账号通过创建委托的方式与您共享资源或委托您管理他的资源。创建委托的方法请参考：**4.3.1 如何创建委托**。
- 登录用户已经获取到委托方的账号名称及所创建的委托名称。

操作步骤

步骤1 单击右上方已登录的账号，选择“切换角色”。

版权所有 © 华为技术有限公司

步骤2 在“切换角色”页面的“账号”中输入委托方的账号名称。

说明

输入账号名称后，系统将会自动匹配委托名称，如果匹配的不是本次需要使用的委托名称，可以删除委托名称，在下拉框中选择对应的委托名称。

步骤3 单击“确定”。

可以根据委托方授予的权限管理委托方的资源。

----结束

后续操作

单击右上角切换的委托账号，选择“切换至”，可以返回到您的账号管理您的资源。

4.4 配置联邦身份认证

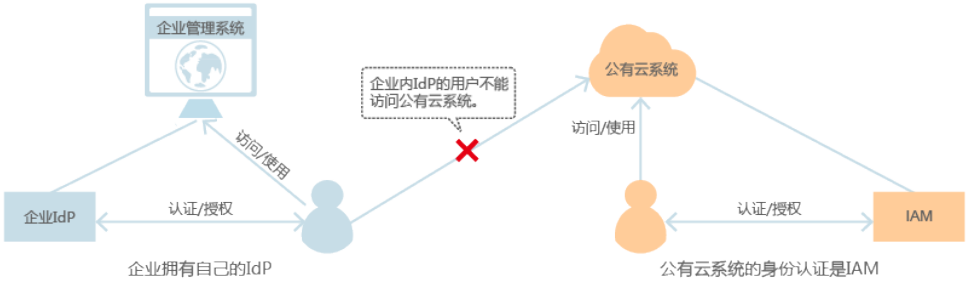
如果您已经有自己的身份认证系统，您可以通过配置联邦身份认证，使得您身份认证系统中的用户可以直接访问公有云系统。

4.4.1 为什么要配置联邦身份认证

未使用联邦身份认证时

- 企业IdP用户不能访问公有云系统

  企业管理系统有自己的IdP（以下称为：企业IdP），通过企业IdP认证的用户无法直接访问公有云系统。



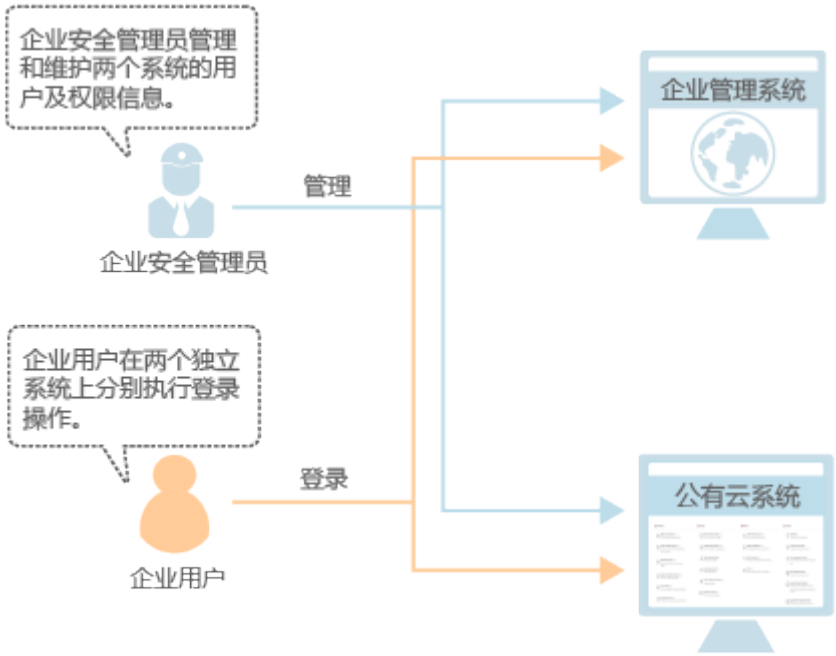
- 用户管理复杂

  管理员需要分别在两个系统中为用户创建账号。

- 用户操作繁琐

  用户访问两个系统时需要使用两个系统的账号登录。

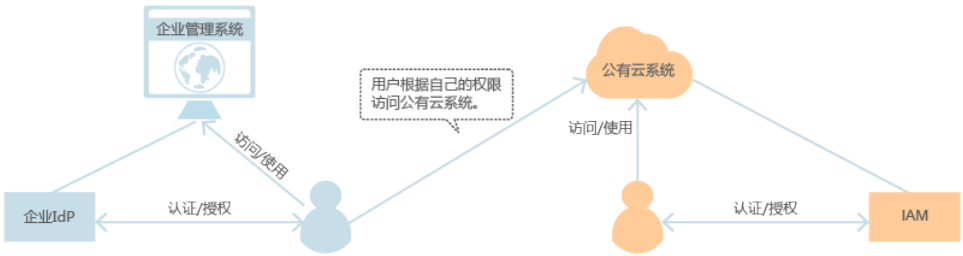
华为专有和保密信息
版权所有 © 华为技术有限公司



使用联邦身份认证后

- IdP用户以直接访问公有云系统

  企业IdP认证通过后，用户即可直接访问公有云系统。企业管理员无需在公有云系统中重复创建用户。



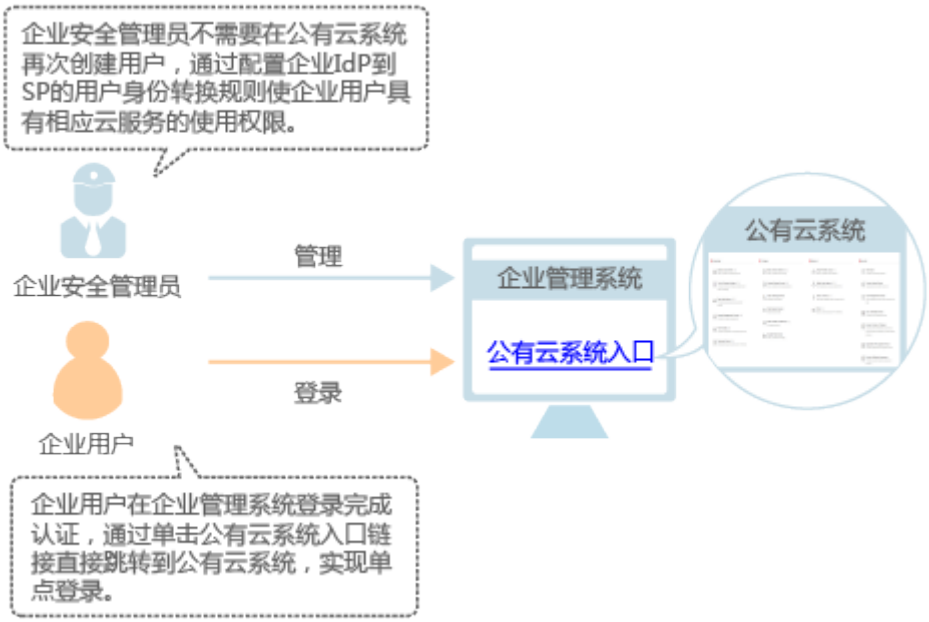
- 用户管理简单

  企业管理员只需要在本企业管理系统中为用户创建账号，用户即可同时访问两个系统。降低了人员管理成本。

- 用户操作方便

  用户在本企业管理系统中登录即可访问两个系统。

华为专有和保密信息
版权所有 © 华为技术有限公司



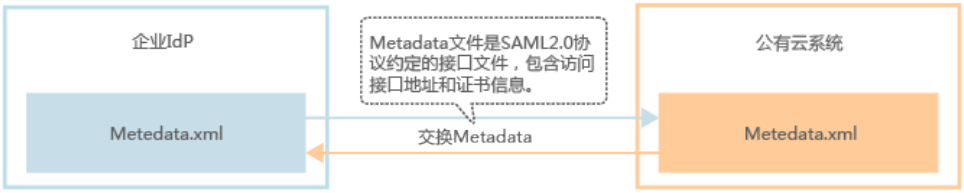
4.4.2 如何配置联邦身份认证

通过配置联邦身份认证，可以简化企业用户的管理，企业用户登录企业管理系统后即可访问公有云系统。

注意

企业IdP服务器的时间需要和公有云系统的时间一致，即都使用世界标准时间（Universal Time Coordinated），否则会导致联邦身份认证失败。

步骤1 建立公有云系统与企业IdP的信任关系。方法请参考：**4.4.3 如何建立公有云系统与企业管理系统的信任关系**。

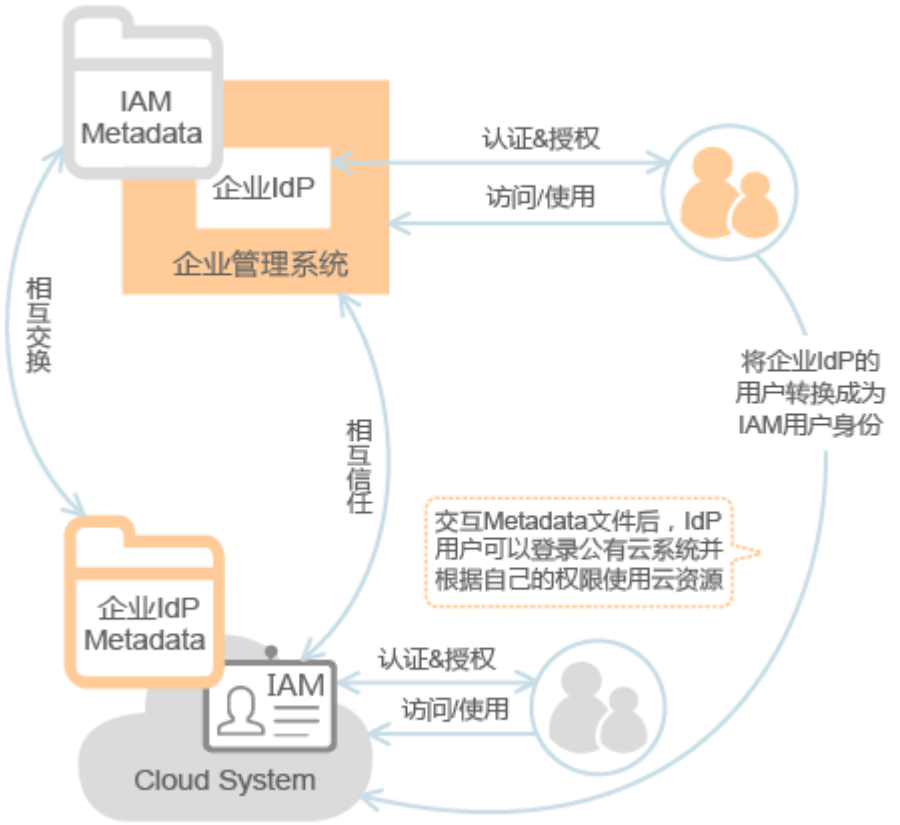


步骤2 在IAM上创建身份提供商。方法请参考：**4.4.4 如何创建身份提供商**。

步骤3 将公有云系统的访问入口配置到企业管理系统中。方法请参考：**4.4.5 如何配置单点登录**。

华为专有和保密信息
版权所有 © 华为技术有限公司

步骤4 在IAM上设置企业IdP用户访问公有云系统的权限。方法请参考：**4.4.7 如何通过规则控制联邦用户访问公有云资源**。



企业IdP的用户登录后，可以单击企业管理系统上的公有云系统入口，直接访问公有云系统。

----结束

4.4.3 如何建立公有云系统与企业管理系统的信任关系

步骤1 下载公有云系统的元数据文件。

版权所有 © 华为技术有限公司

下载方法：访问网址**https://auth.huaweicloud.com/authui/saml/metadata.xml**。单击右键，选择“目标另存为”并设置文件名称，例如publiccloud-metadata.xml。

步骤2 获取企业IdP的元数据文件。获取方法请咨询企业管理系统的管理员。

步骤3 将公有云系统的元数据文件上传到企业IdP服务器上。上传方法请咨询企业管理系统的管理员。

步骤4 将企业IdP的元数据文件上传到IAM服务器上。上传方法请参考：**4.4.4 如何创建身份提供商**。

----结束

4.4.4 如何创建身份提供商

在IAM上创建身份提供商，并配置身份提供商的元数据文件后，可以使企业IdP认证的用户直接访问公有云系统，即无需通过公有云系统的登录界面进行登录认证。

背景信息

IAM仅支持使用SAML2.0协议进行联邦身份认证，因此企业IdP必须支持SAML2.0协议。

SAML（Security Assertion Markup Language）：安全断言标记语言，是一个在信任域之间交互认证、授权信息的XML标准。您可以通过以下网站了解更多关于SAML2.0协议的基本信息：**https://en.wikipedia.org/wiki/SAML_2.0**。

前提条件

- 登录用户已具备“Security Administrator”权限。
- 已建立公有云系统与企业管理系统之间的信任关系。方法请参见**4.4.3 如何建立公有云系统与企业管理系统的信任关系**。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“身份提供商”。

步骤3 在“身份提供商”界面，单击“创建身份提供商”。

步骤4 设置身份提供商的名称、启用或停用状态及描述信息。

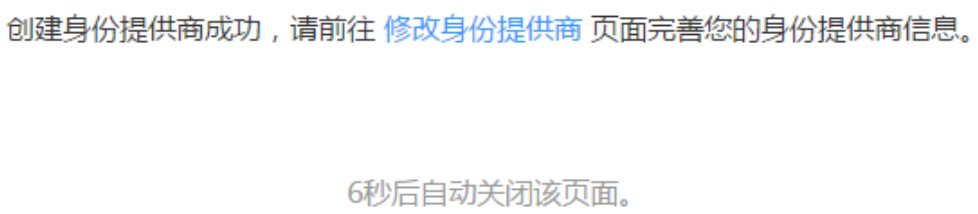
说明

协议类型只支持saml。

步骤5 单击“确定”。

创建身份提供商成功，界面提示如**图4-1**所示：

图 4-1 创建身份提供商成功提示信息



版权所有 © 华为技术有限公司

步骤6 配置身份提供商信息。单击界面提示中的“修改身份提供商”，界面提示关闭后，可以单击目标身份提供商“操作”列的“修改”。

步骤7 在“修改身份提供商”页面的“元数据配置”区域配置元数据，以下两种方式选择其中一种即可。

元数据配置支持系统自动提取和用户手动编辑两种方式，如果元数据文件超过500KB，可以通过“手动编辑”配置元数据。

- 系统自动提取元数据：
  a. 单击“上传”左侧的  ，选择获取的企业IdP的元数据文件。
  b. 单击“上传”。
     弹出页面显示系统提取到的元数据。
  c. 单击“确定”。
     - 提示“系统发现您上传的文件中包含多个身份提供商，请选择您本次需要使用的身份提供商”，请在“Entity ID”下拉框中选择您本次需要使用的身份提供商。
     - 提示元数据文件中Entity ID为空、签名证书过期等内容时，需要您确认元数据文件的正确性后，重新上传或者通过手动编辑提取元数据。
  d. 单击“确定”。
  e. 单击 

，可以查看系统提取的元数据详情。
- 手动编辑元数据
  a. 单击“手动编辑”。
  b. 在“手动编辑元数据”页面中，输入“Entity ID”、“签名证书”和“SingleSignOnService”等参数。

参数	含义
Entity ID	企业身份提供商的唯一标识，元数据文件中可能包含多个身份提供商，需要选择对应的身份提供商。
支持的协议	企业IdP与服务提供商之间，通过SAML协议完成联邦认证，IAM只支持SAML2.0协议。
支持的NameIdFormat	身份提供商支持的用户名称标识格式。 名称标识是身份提供商与联邦用户之间实现通信的一种方式。
签名证书	是一份包含公钥用于验证签名的证书，为了确保安全性，建议使用长度大于等于2048位的公钥。系统通过元数据文件中的签名证书来确认联邦认证过程中断言消息的可信性、完整性。
SingleSignOnService	单点登录过程中发送SAML请求的方式。元数据文件中的“SingleSignOnService ”需要支持HTTP Redirect或HTTP POST方式。 **说明** 单点登录详情请参见**4.4.8 单点登录流程**。

版权所有 © 华为技术有限公司

参数	含义
SingleLogoutService	服务提供商提供会话注销功能，联邦用户在IAM注销会话后返回绑定的地址。 “SingleLogoutService ”需要支持HTTP Redirect或HTTP POST方式。

c. 单击“确定”。

步骤8 单击“确定”，保存设置信息。

----结束

结果验证

步骤1 单击目标身份提供商列表右侧的“查看”。

步骤2 单击“登录链接”右侧的“复制”，复制“登录链接”的地址，并在浏览器中打开。

步骤3 检查是否可以跳转到企业的IdP服务器提供的登录界面。

- 是，执行**步骤4**。
- 否，请确认获取的企业文数据文件以及企业的IdP服务器是否配置正确。

步骤4 输入用户名和密码验证是否可以登录到公有云系统。

- 登录成功，将该地址以链接的形式配置到您自己的企业网站。方法请参考**4.4.5 如何配置单点登录**。
- 登录失败，请检查您的用户名和密码。

----结束

后续处理

- 在“身份转换规则”区域，创建身份转换规则。身份转换规则详情请参见**4.4.7 如何通过规则控制联邦用户访问公有云资源**。
- 在企业管理系统中配置单点登录，方法请参考：**4.4.5 如何配置单点登录**。

相关任务

- 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。

华为专有和保密信息
版权所有 © 华为技术有限公司

- 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。

4.4.5 如何配置单点登录

将身份提供商的登录链接配置到企业管理系统上，企业用户通过企业IdP认证后即可访问公有云系统。

前提条件

- 已创建身份提供商，并验证身份提供商的登录链接可以正常使用。方法请参考：4.4.4 如何创建身份提供商。
- 登录用户已具备“Security Administrator”权限。

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“身份提供商”。

步骤3 单击目标身份提供商列表右侧的“查看”。

步骤4 单击“登录链接”右侧的“复制”。

步骤5 在企业管理系统页面按“F12”将如下内容配置在页面上。

```
<a href="<登录链接>"> 公有云系统入口 </a>
```

用户登录企业管理系统后通过单击“公有云系统入口”可以直接访问公有云系统。

----结束

华为专有和保密信息
版权所有 © 华为技术有限公司

4.4.6 联邦用户身份转换规则说明

联邦身份转换规则采用JSON文件格式呈现。您可以通过编辑JSON文件来修改规则。JSON格式如下：

```
[
       {
           "remote": [
               {
                  "<condition>"
               }
           ],
           "local": [
               {
                 "<user> or <group>"
               }
           ]
       }
     ]
```

- remote：表示联邦用户在IdP中的用户信息，由断言属性及运算符组成的表达式，取值由断言决定。
- condition：表示联邦用户到公有云系统的身份转换规则。当前支持三种条件：
  - empty：无限制，即条件一直生效，返回输入属性的值，值可以用于填充local块中的占位符。
  - any_one_of：输入属性值中只要包含一个指定值即生效，并返回布尔值，返回值不能用于local块中的占位符。
  - not_any_of：输入属性值中不包含任何指定值才生效，并返回布尔值，返回值不能用于local块中的占位符。
- local：表示联邦用户在公有云系统中的用户信息。可以是占位符“{0..n}”，{0}表示remote中用户信息的第一个属性，{1}表示remote中用户信息的第二个属性。

规则条件示例

通过示例来加深您对身份转换规则条件（empty、any_one_of、not_any_of）的理解。

- empty：该条件的特点是能够返回一个具体字串值，该值用于填充local块中的占位符“{0..n}”，如下所示。

```
[
       {
           "local": [
               {
                   "user": {
                       "name": "{0} {1}"
                   }
               },
               {
                   "group": {
                       "name": "{2}"
                   }
               }
           ],
           "remote": [
               {
                   "type": "FirstName"
               },
               {
                   "type": "LastName"
               },
               {
                   "type": "Groups"
               }
```


版权所有 © 华为技术有限公司

```
            ]
        }
    ]
```

表示联邦用户在公有云系统中的用户名称为“remote”的第一个属性值+空格+第二个属性值，即*FirstName LastName*。所属用户组为“remote”的第三个属性值，即*Groups*。

假设传入以下断言（为了方便，我们对断言的结构做了简化，之后的示例也做为类似的简化，将不再重复提示），则联邦用户在公有云系统中的用户名为John Smith，John Smith属于“admin”、“manager”用户组。

```
{FirstName: John}
{LastName: Smith}
{Groups: [admin, manager]}
```

- any one of、not any of：与Empty条件不同，这两个条件返回的是一个布尔值，该值不能用于填充local中的占位符。所以以下示例中，仅有一个占位符“{0}”用于被remote块中的第一个Empty条件填充，第二个group为一个固定的值admin。

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
                {
                    "group": {
                        "name": "admin"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
                },
                {
                    "type": "Groups",
                    "any_one_of": [
                        "idp_admin"
                    ]
                }
            ]
        }
    ]
```

表示联邦用户在公有云中的用户名为“remote”的第一个属性，即*UserName*。所属用户组为“admin”。该规则仅对在IdP中属于“idp_admin”用户组的用户生效。

  - 假设传入以下断言，由于John Smith属于“idp_admin”用户组，所以允许该用户访问公有云系统。联邦用户在公有云系统中的用户名为John Smith，所属用户组为“admin”。

    ```
    {UserName: John Smith}
    {Groups: [idp_user, idp_admin, idp_agency]}
    ```

  - 假设传入以下断言，由于John Smith不属于“idp_admin”用户组，所以该规则对John Smith不生效，不允许John Smith访问公有云系统。

    ```
    {UserName: John Smith}
    {Groups: [idp_user, idp_agency]}
    ```

- 含有正则表达式的条件：你可以在条件里指定一个“"regix": true”用来表示系统将以正则匹配的方式来计算结果，这是一个比较高级的功能，仅推荐您做简单的了解、使用。

```
[
        {
            "local": [
```


版权所有 © 华为技术有限公司

```
            {
                "user": {
                    "name": "{0}"
                }
            },
            {
                "group": {
                    "name": "admin"
                }
            }
        ],
        "remote": [
            {
            "type": "UserName"
            },
            {
                "type": "Groups",
                "any_one_of": [
                    ".*@mail.com$"
                ],
                "regex": true
            }
        ]
    }
]
```

表示该规则对以任意值开头，“@mail.com”结尾的用户生效，在公有云系统中的用户名为*UserName*，所属用户组为“admin”。

- 条件组合：多个条件间，以“逻辑与”的方式组合。

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}"
                }
            },
            {
                "group": {
                    "name": "admin"
                }
            }
        ],
        "remote": [
            {
            "type": "UserName"
            },
            {
                "type": "Groups",
                "not_any_of": [
                    "idp_user"
                ]
            },
            {
                "type": "Groups",
                "not_any_of": [
                    "idp_agent"
                ]
            }
        ]
    }
]
```

表示该规则仅对既不属于IdP的“idp_user”也不属于IdP的“idp_agent”用户组的联邦用户生效。对于生效用户：在公有云系统中的用户名为*UserName*，所属用户组为“admin”。以上规则等同于：

```
[
    {
```


版权所有 © 华为技术有限公司

```
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
                {
                    "group": {
                        "name": "admin"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
                },
                {
                    "type": "Groups",
                    "not_any_of": [
                        "idp_user",
                        "idp_agent"
                    ]
                }
            ]
        }
    ]
```

- 多规则

  多个规则组合，用户名与用户组生成方式不同。

  用户名取第一个生效规则的用户名，所有规则中必须至少有一个用户名规则生效，否则系统不允许此用户登录；而用户组则取所有生效规则用户组名称的集合。

  一种比较实用的多规则配置方式是把用户名配置与用户组配置分离。这样的配置会非常容易阅读。

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}"
                }
            }
        ],
        "remote": [
            {
                "type": "UserName"
            }
        ]
    },
    {
        "local": [
            {
                "group": {
                    "name": "admin"
                }
            }
        ],
        "remote": [
            {
                "type": "Groups",
                "any_one_of": [
                    "idp_admin"
                ]
            }
        ]
    }
]
```


版权所有 © 华为技术有限公司

表示针对IdP中属于“idp_admin”用户组的用户生效，在公有云系统中的用户名为*UserName*，所属用户组为“admin”。

假设传入以下断言，由于John Smith属于“idp_admin”用户组，因此此规则对John Smith生效。在公有云系统中的用户名为John Smith，所属用户组为“admin”。

```
{UserName: John Smith}
{Groups: [idp_user, idp_admin, idp_agency]}
```

4.4.7 如何通过规则控制联邦用户访问公有云资源

联邦用户在访问公有云系统时，可以通过规则将联邦用户在企业管理系统中的权限映射到公有云系统中，实现通过IAM控制联邦身份用户访问公有云资源的权限。您也可以通过设置规则及规则生效条件来管控哪些联邦用户可以访问哪些公有云资源。

前提条件

- 已创建身份提供商，并验证身份提供商的登录链接可以正常使用。方法请参考：**4.4.4 如何创建身份提供商**。
- 登录用户已具备“Security Administrator”权限。
- 了解SAML2.0协议，熟悉元数据文件。
- 了解SAML2.0认证成功后的Assertion结构。

背景信息

联邦用户的身份及权限信息由企业管理员通过企业IdP维护。完成联邦身份认证配置后，联邦用户可以完成单点登录，单点登录的流程可参考：**4.4.8 单点登录流程**。

完成单点登录后，IdP会返回一个称作“断言”的结构体给IAM，断言中包含了本次通过认证的用户的身份及权限信息，这些信息以属性列表的方式嵌套在断言结构体中，以下是某断言中的一些示例属性：

```
...
<saml2:AttributeStatement>
    <saml2:Attribute FriendlyName="mail"
     Name="urn:oid:0.9.2342.19200300.100.1.3"
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
     <saml2:AttributeValue>demo@example.org</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="GROUPS"
        Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml2:AttributeValue>dev-adm</saml2:AttributeValue>
        <saml2:AttributeValue>sec-adm</saml2:AttributeValue>
    </saml2:Attribute>
</saml2:AttributeStatement>
...
```

操作步骤

步骤1 选择“管理与部署 > 统一身份认证服务”。

步骤2 在左侧导航窗格中，单击“身份提供商”。

步骤3 在身份提供商列表中，选择您创建的身份提供商，单击“修改”。

进入“修改身份提供商”界面。

步骤4 在“身份转换规则”区域单击“创建规则”。

版权所有 © 华为技术有限公司

说明

- 请不要在规则中配置一些个人敏感信息，例如：不要将个人信用卡号作为用户名。
- 当您创建完身份提供商后，公有云系统会预置一条默认的规则，该规则将联邦用户的用户名统一转换为“FederationUser”，用于在公有云系统中显示用户名称。仅允许当前IdP的联邦用户访问部分资源。若此条规则不符合您的使用要求，您可在“编辑规则”中将其修改。

- 用户名：表示联邦用户登录后在公有云系统中显示的用户名。为了便于区分公有云系统的用户与联邦用户，建议联邦用户使用“FederationUser_”开头。用户名可以自定义具体名称，也可以是一个简单的表达式，如：FederationUser_{email}。规则创建成功后，{email}自动替换为联邦用户的邮箱。即公有云系统中显示的用户名为：FederationUser_XXX@XXX（XXX@XXX为用户邮箱）。如果断言中没有用户邮箱，则该规则不生效。
- 用户组：表示联邦用户登录公有云系统后，在公有云系统中所属的用户组。用户属于哪些用户组，决定了用户具有什么权限。
- 本规则生效条件：定义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公有云系统。

  例如，为企业系统管理员设定规则。

  - 用户名：FederationUser_admin_{email}
  - 用户组：“admin”
  - 生效条件：仅对指定ID的用户生效（“属性”设置为“_NAMEID_”，“条件”设置为“any_one_of”，“值”设置为“ID1;ID2;ID3”）。表示仅用户ID为ID1，ID2或ID3的用户具有公有云系统中的“admin”用户组的权限。该IdP的其他用户不具有“admin”用户组的权限。

    说明

    - 一个规则可以创建多条生效条件，只要有一条生效条件满足，此规则即可生效。
    - 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公有云系统。

版权所有 © 华为技术有限公司

步骤5 在“创建规则”页面，单击“确定”。

步骤6 在“修改身份提供商”页面，单击“确定”，使设置生效。

----结束

相关任务

- 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：**4.4.6 联邦用户身份转换规则说明**。
- 编辑规则：在“身份转换规则”区域单击“编辑规则”。该功能为了满足各种联邦认证要求提供了比较灵活的编辑规则的语法，示例参考：**4.4.6 联邦用户身份转换规则说明**。

  说明

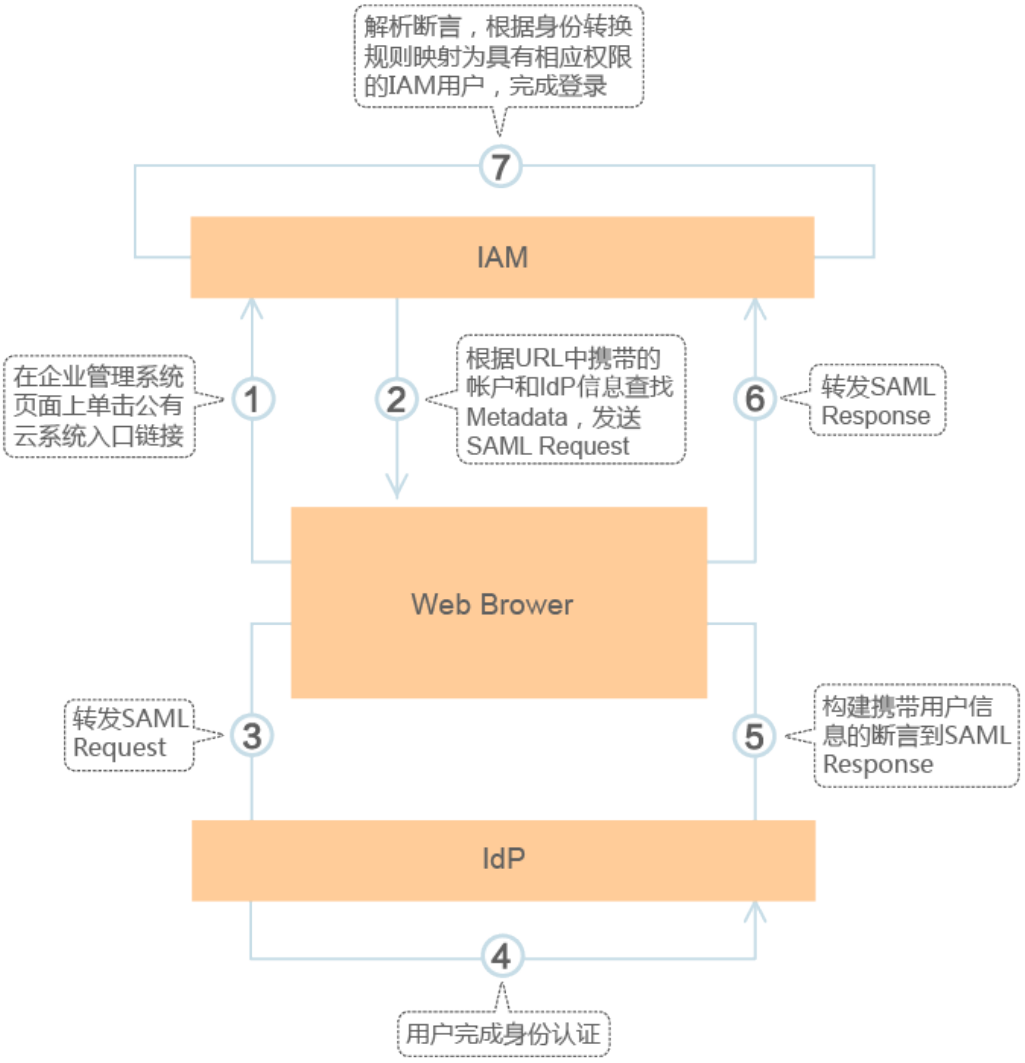
  规则编辑完成后，可以点击页面左下角的“校验规则”，校验规则的正确性。

4.4.8 单点登录流程

完成联邦认证配置后，联邦用户通过企业IdP登录认证后可以直接访问公有云系统中的资源。本章介绍通过IdP认证后如何在IAM中进行认证。

版权所有 © 华为技术有限公司

登录流程



步骤说明

说明

为方便您查看交互的请求及断言消息，建议您使用Chrome浏览器并安装插件“SAML Message Decoder”。

1. 在浏览器中打开创建身份提供商后生成的登录链接，Web Browser发起单点登录。
2. IAM根据链接中携带的账号和IdP信息，查找出企业IdP的Metadata文件，构建SAML Request，响应到浏览器。
3. 浏览器响应后转发SAML Request到企业IdP。
4. 用户在IdP服务器，输入用户名和密码等完成身份认证。
5. IdP服务器构造断言到SAML Response，响应到浏览器中。
6. 浏览响应后转发SAML Response到IAM。
7. IAM从SAML Response取出断言进行解析，并根据配置的规则，生成Token，完成登录。

华为专有和保密信息
版权所有 © 华为技术有限公司

说明

断言中要携带签名，否则会导致登录失败。

4.5 管理安全凭证

用户在登录公有云系统、通过API访问公有云系统或进行公有云系统内业务对接时，需要使用自己的安全凭证。用户可以查看自己的属性信息或安全信息，还可以修改已验证手机号、已验证邮箱、密码等。

4.5.1 如何查看安全凭证

当您需要登录公有云系统，或通过API访问公有云系统或进行公有云系统内业务对接时，需要使用您的安全凭证。安全凭证信息包括用户名、用户ID、账号名、账号ID、已验证邮箱、已验证手机等。

前提条件

用户已登录公有云系统。

操作步骤

步骤1 在公有云系统页面，单击“控制台”。

步骤2 单击右上方登录的用户，在下拉列表中选择“基本信息”。

步骤3 在“基本信息”页面，单击“管理我的凭证”。

版权所有 © 华为技术有限公司

步骤4 在“我的凭证”页面，查看信息。

信息含义参考**表1**。

表 4-2 我的凭证信息

基本信息	说明
用户名	用户的登录名，登录公有云系统时需要提供。
用户ID	用户在公有云系统中的唯一标识ID，由系统自动生成。
账号名	账号的名称。账号是承担费用的主体（例如一个企业），在注册时自动创建，云服务资源按账号完全隔离。 登录公有云系统时需要提供。
账号ID	账号在公有云系统中的唯一标识ID，由系统自动生成。
已验证邮箱	用户绑定的邮箱地址。已验证邮箱可以作为安全认证凭证，通过已验证邮箱登录公有云系统或者重置密码，也可以接收验证码和系统推送信息。
已验证手机	用户绑定的移动手机号码。已验证手机可以作为安全认证凭证，通过已验证手机号登录公有云系统或者重置密码，也可以接收验证码和系统推送信息。
密码	用户在公有云系统中登录密码的安全程度。

华为专有和保密信息
版权所有 © 华为技术有限公司

基本信息	说明
登录时短信验证	开启登录时短信验证功能，开启后，登录时需要在页面上输入手机验证码。
项目	项目用于将OpenStack的资源（计算资源、存储资源和网络资源等）进行分组和隔离。用户拥有的资源必须挂载在项目下，项目可以是一个部门或者项目组。
项目列表	账号可访问的项目列表，在访问OpenStack原生API时需要指定project参数。
访问密钥	用户的Access Key/Secret Key (AK/SK)，最多可创建两对，使用API访问公有云系统时需要使用AK/SK进行加密签名。

----结束

4.5.2 如何修改安全凭证

用户可以修改自己的凭证信息，包括已验证邮箱、已验证手机、密码等。为了确保用户信息的安全，建议您定期修改密码并开启登录时短信验证。

背景信息

如果第三方系统用户没有公有云系统的登录密码，可以通过以下方式设置：

- 如果已经绑定了邮箱或手机，可以通过公有云系统登录页面的找回密码功能设置登录密码。
- 如果未绑定邮箱或手机，请联系并提供邮箱给安全管理员（具有Security Administrator权限的用户）重置密码。重置密码的方法请参考：**4.1.3 如何创建用户**。

前提条件

用户已登录公有云系统。

操作步骤

步骤1 在公有云系统页面，单击“控制台”。

步骤2 单击右上方登录的用户，在下拉列表中选择“基本信息”。

华为专有和保密信息
版权所有 © 华为技术有限公司

步骤3 在“基本信息”页面，单击“管理我的凭证”。

步骤4 在我的凭证页面中，可以修改如下信息：

- 已验证邮箱
  a. 单击“已验证邮箱”对应的“修改”，进入“修改注册邮箱”页面。
  b. 在“验证身份”步骤，选择验证方式：邮箱或者手机。

  说明

  用户只有同时绑定了邮箱和手机，才能选择验证方式。

  c. 输入邮箱或手机获取到的验证码。
  d. 单击“下一步”。
  e. 进入“修改注册邮箱”步骤，输入“新注册邮箱”和“邮箱验证码”。
  f. 单击“确定”，完成修改。
- 已验证手机
  a. 单击“已验证手机”对应的“修改”，进入“修改手机号码”页面。
  b. 在“验证身份”步骤，选择验证方式：邮箱或者手机。

  说明

  用户只有同时绑定了邮箱和手机，才能选择验证方式。

  c. 输入邮箱或手机获取到的验证码。

版权所有 © 华为技术有限公司

d. 单击“下一步”。

e. 进入“修改手机号码”步骤，输入“新手机号码”和“短信验证码”。

f. 单击“确定”，完成修改。

- 密码（定期修改密码可以提高账号的安全性，建议您定期修改密码）

  a. 单击密码对应的“修改”，进入修改密码页面。

  b. 选择验证方式：邮箱或者手机。

  说明

  用户只有同时绑定了邮箱和手机，才能选择验证方式。

  c. 输入邮箱或手机获取到得验证码。

  d. 输入“原密码”、“新密码”和“确认密码”。

  说明

  新密码符合如下要求:

  - 不能是用户名或者用户名的倒序（不区分大小写），例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a。
  - 不能包含邮箱或手机号。
  - 不能少于6个字符且不超过32个字符。
  - 包括大写字母（A~Z），小写字母（a~z），数字（0~9）和特殊字符（空格!"#$%&'()*+,-./:;<=>?@[]^`{_|}~）至少2种的组合。
  - 不能与原密码相同。

  e. 单击“确定”，完成修改。

- 登录时短信验证

  a. 单击“修改”，在弹出的“设置登录时短信验证”提示框中，输入手机验证码。

  b. 单击“确定”。

  开启登录时短信验证功能。

  说明

  - 该功能默认不开启，只有当用户同时绑定了邮箱和手机，才能开启该功能。
  - 开启该功能后，登录公有云系统时，需要在“登录验证”页面输入短信验证码进行验证。

- 头像

  a. 在我的凭证页面，单击头像下方的“更换”。

  进入“更换头像”页面。

  b. 单击“本地上传”，选择图片。

  c. 单击“确定”。

  完成头像更换。

----结束

4.5.3 如何管理访问密钥

当您通过API访问公有云系统时，需要使用访问密钥进行身份认证并对请求进行加密，确保请求的机密性、完整性和请求双方身份的正确性。

版权所有 © 华为技术有限公司

前提条件

用户已登录公有云系统。

操作步骤

步骤1 在公有云系统页面，单击“控制台”。

步骤2 单击右上方登录的用户，在下拉列表中选择“基本信息”。

步骤3 在“基本信息”页面，单击“管理我的凭证”。

步骤4 在“我的凭证”页面，单击“管理访问密钥”页签。可以查看已创建的访问密钥。

步骤5 管理访问密钥。

- 新增访问密钥并下载
  a. 单击列表上方的“新增访问密钥”。

     说明

     每个用户最多可创建2个访问密钥，且一旦生成永久有效，为了账号安全性，建议定期更换访问密钥并妥善保存。

  b. 输入“登录密码”和获取到的验证码。

华为专有和保密信息
版权所有 © 华为技术有限公司

说明

- 用户如果没有设置登录公有云系统的密码，则不需要输入“登录密码”。
- 用户如果没有绑定邮箱和手机，则不需要输入对应的验证码。

c. 单击“确定”，生成访问密钥。

d. 单击“确定”下载访问密钥。

说明

访问密钥是在IAM中认证的凭证，如果不下载生成的密钥则无法获取对应的访问密钥。如果该用户需要使用访问密钥在IAM中认证，需要重新生成。

- 删除访问控制密钥

a. 单击“删除”。

b. 输入“登录密码”和对应验证码。

说明

用户如果没有设置登录密码、未绑定邮箱和手机，则不需要进行身份验证。

c. 单击“确定”。

说明

- 当用户发现访问密钥被异常使用（包括丢失、泄露等情况），可以自行删除或者通知管理员重置访问密钥。
- 删除的访问密钥将无法恢复。

----结束

4.5.4 如何查看项目 ID

项目ID是系统所在区域的ID。用户在使用API接口访问公有云系统（如：创建VPC）时，需要提供项目ID。

前提条件

用户已登录公有云系统。

操作步骤

步骤1 在公有云系统页面，单击“控制台”。

步骤2 单击右上方登录的用户，在下拉列表中选择“基本信息”。

版权所有 © 华为技术有限公司

步骤3 在“基本信息”页面，单击“管理我的凭证”。

步骤4 在“我的凭证”页面的“项目列表”页签查看项目ID。

----结束

华为专有和保密信息
版权所有 © 华为技术有限公司

5 FAQ

5.1 忘记密码怎么办

当用户因忘记密码无法访问公有云系统时，可以通过重置密码功能设置新密码。

背景信息

- 如果忘记账号密码，通过“账号登录”入口找回密码。下面操作以此为例。
- 如果忘记IAM用户密码，通过“IAM用户登录”入口找回密码。
- 如果用户绑定了邮箱或手机，可以通过重置密码功能重置密码。下面操作以此场景为例。
- 如果用户没有绑定邮箱或手机，请联系拥有“Security Administrator”权限的用户重置密码。

操作步骤

步骤1 在公有云系统的登录页面，单击右下方“忘记密码?”。

步骤2 在“确认账号”步骤，选择“通过邮箱找回密码”或者“通过手机找回密码”。

- 选择通过邮箱找回密码，输入“已验证邮箱”。
- 选择通过手机找回密码时，输入“注册手机号”。

步骤3 单击“下一步”。

步骤4 在“重置密码”步骤，输入“新密码”和“确认密码”。

说明

定期修改密码可以提高账号的安全性。新密码必须符合如下复杂度要求:

- 密码不能是用户名或者用户名的倒序（不区分大小写），例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a。
- 不能包含手机号或邮箱。
- 不能少于6个字符且不超过32个字符。
- 包括大写字母（A~Z），小写字母（a~z），数字（0~9）和特殊字符（空格!"#$%&'()*+,-./:;<=>?@[]^`{_|}~）至少2种的组合。

步骤5 单击“获取验证码”，输入获取的验证码。

华为专有和保密信息
版权所有 © 华为技术有限公司

步骤6 单击“下一步”。

显示修改密码成功。

----结束

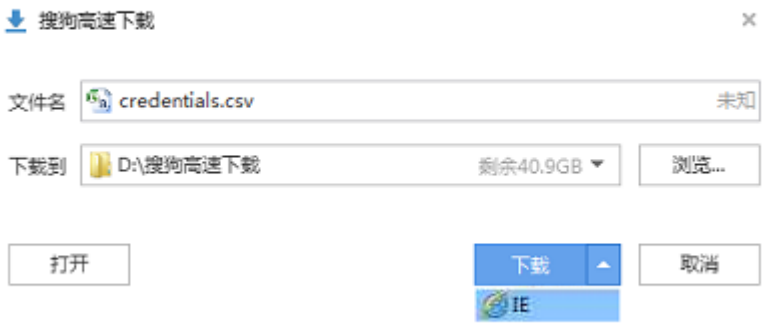
5.2 搜狗浏览器无法下载访问密钥怎么办

用户通过搜狗浏览器登录我的凭证下载访问密钥时，默认使用搜狗高速下载模式进行下载。由于当前不支持搜狗高速下载模式，所以会出现无法正常下载的情况。在搜狗浏览器中下载访问密钥时，可以参照以下操作设置IE下载模式进行下载。

操作步骤

步骤1 通过搜狗浏览器登录到“我的凭证”页面，新增访问密钥时，弹出“下载确认”提示框。

步骤2 单击“确定”后，搜狗浏览器弹出下载页面。



步骤3 选择下载保存的路径并在“下载”下拉框中，单击下拉箭头，然后选择“IE”。

说明

为防止访问密钥泄露，建议您将其保存到安全的位置。

步骤4 从指定路径下获取下载保存的访问密钥。

----结束

5.3 Internet Explorer 浏览器下输入框提示信息无法自动消失怎么办

当用户进行登录、注册、绑定华为云账号、修改手机号码、找回密码、修改密码等操作时，由于当前输入框不能完全支持Internet Explorer 8及以下版本的浏览器，所以出现输入框提示信息（如“最短不能少于5个字符”等提示信息）无法自动消失的情况，可以参照以下方法进行操作。

版权所有 © 华为技术有限公司

操作步骤

- 升级浏览器版本

  将Internet Explorer浏览器升级到IE9及以上版本再进行操作。
- 更换浏览器

  使用Firefox浏览器（38.0及以上版本）或Google Chrome浏览器（43.0及以上版本）进行操作。

5.4 Internet Explorer 浏览器下无法获取短信验证码怎么办

当用户更换手机号码、找回密码等操作时，需要获取短信验证码进行验证。由于当前公有云系统不支持“Internet Explorer 8 兼容性视图”模式及IE8以下版本的浏览器，所以用户操作过程中出现无法获取短信验证码的情况，可以参照以下方法进行操作。

操作步骤

- 设置浏览器模式（针对使用Internet Explorer 8浏览器操作过程中出现无法获取短信验证码的情况）

  a. 在当前使用的Internet Explorer浏览器页面，单击“F12”。

  b. 单击“浏览器模式：IE8 兼容性视图”。

  c. 选择“Internet Explorer 8”。

  d. 单击右上角×，关闭“开发人员工具”窗口，继续进行注册、更换手机号码、找回密码等操作。
- 升级浏览器版本

  将Internet Explorer浏览器升级到IE9及以上版本再进行操作。
- 更换浏览器

  使用Firefox浏览器（38.0及以上版本）或Google Chrome浏览器（43.0及以上版本）进行操作。

5.5 如何在 Google Chrome 浏览器禁用密码联想与保存

当用户首次使用Google Chrome浏览器成功登录华为云，浏览器会默认弹框提示用户并确认是否保存登录密码，这是由于安装Google Chrome浏览器后，浏览器“设置”页面的“密码和表单”区域中“启用自动填充功能，以便点按一次即可填写网络表格”和“询问是否保存您在网页上输入的密码”选项是默认开启的。如果用户根据界面提示确认保存密码后，下次登录华为云时，登录界面的密码输入框会自动联想填充字符，

版权所有 © 华为技术有限公司

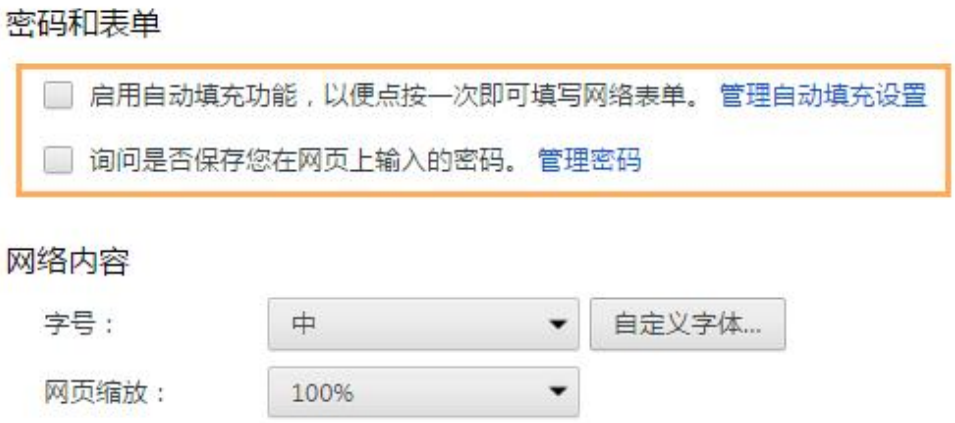
为了确保账号及密码安全，用户可关闭该功能。以Google Chrome浏览器的61.0.3163.100正式版本为例，可以参照以下方法进行操作。

操作步骤

步骤1 打开Google Chrome浏览器，单击右上角≡并选择“设置”。

步骤2 在“设置”页面，单击“显示高级设置”。

步骤3 在“密码和表单”区域，去勾选“启用自动填充功能，以便点按一次即可填写网络表单”和“询问是否保存您在网页上输入的密码”。



----结束

后续处理

清除已保存的账号登录信息的方法如下：

1. 单击“询问是否保存您在网页上输入的密码”右侧的“管理密码”。
2. 在“密码”对话框中“已保存的密码”区域，选中某条登录信息记录，单击右侧的×，可清除对应网站地址、登录用户名及密码信息。

华为专有和保密信息
版权所有 © 华为技术有限公司

A 文档修订记录

表 A-1 文档修订记录

日期	修订记录
2018-02-13	第十一次正式发布。 本次变更说明如下： **4.3.1 如何创建委托**中新增委托类型的表格。
2017-12-15	第十次正式发布。 ● 调整文档大纲。增加**1 概述**、**2 开始使用**、**3 新手入门**、**4.5 管理安全凭证**、**5 FAQ**等内容。 ● 删除权限说明章节，权限说明详情请参考**权限说明**。
2017-07-27	第九次正式发布。 本次变更说明如下： ● 新增“CTS Administrator”权限描述。 ● **4.4.4 如何创建身份提供商**中新增系统自动提取和手动编辑元数据内容。
2017-06-28	第八次正式发布。 本次变更说明如下： ● 修改“Server Administrator”权限描述。 ● 修改“VPC Administrator”权限描述。

华为专有和保密信息
版权所有 © 华为技术有限公司

日期	修订记录
2017-05-19	第七次正式发布。 本次变更说明如下： ● 新增以下内容： – **4.4.3 如何建立公有云系统与企业管理系统的信任关系**章节。 – **4.4.2 如何配置联邦身份认证**章节。 – **4.4.8 单点登录流程**章节。 – “APM Admin”权限描述。 – “CCS Administrator”权限描述。 – “CCS User”权限描述。 – “CDE Admin”权限描述。 – “CDE Developer”权限描述。 – “SvcStg Admin”权限描述。 – “SvcStg Developer”权限描述。 – “SvcStg Operator”权限描述。 – “SWR Admin”权限描述。 ● 修改“RDS Administrator”权限描述。 ● 删除以下内容： – “te_devcloud_project_admin”权限描述。 – “te_devcloud_project_poweruser”权限描述。 – “te_devcloud_project_readonly”权限描述。 – “te_devcloud_codehub_admin”权限描述。 – “te_devcloud_codehub_poweruser”权限描述。 – “te_devcloud_codehub_readonly”权限描述。 – “te_devcloud_codecheck_admin”权限描述。 – “te_devcloud_codecheck_poweruser”权限描述。 – “te_devcloud_codecheck_readonly”权限描述。 – “te_devcloud_codeci_admin”权限描述。 – “te_devcloud_codeci_poweruser”权限描述。 – “te_devcloud_codeci_readonly”权限描述。 – “te_devcloud_test_admin”权限描述。 – “te_devcloud_test_poweruser”权限描述。 – “te_devcloud_test_readonly”权限描述。 – “te_devcloud_release_admin”权限描述。 – “te_devcloud_release_poweruser”权限描述。 – “te_devcloud_release_readonly”权限描述。

版权所有 © 华为技术有限公司

日期	修订记录
2017-04-27	第六次正式发布。 本次变更说明如下： ● 新增**4.3.1 如何创建委托**章节。 ● 新增**4.3.2 如何切换角色**章节。 ● 新增“DWS Administrator”权限描述。
2017-03-30	第五次正式发布。 本次变更说明如下： ● 同步“创建用户”界面的更新，刷新**4.1.3 如何创建用户**章节。 ● 新增“Agent Operator”权限描述。 ● 新增“CRS Administrator”权限描述。
2016-11-30	第四次正式发布。 本次变更说明如下： 同步“账户策略”界面的更新，刷新**4.2 如何设置账号安全策略**章节。
2016-09-30	第三次正式发布。 本次变更说明如下： 新增以下章节： ● **4.4.4 如何创建身份提供商** ● **4.4.7 如何通过规则控制联邦用户访问公有云资源**
2016-08-25	第二次正式发布。 本次变更说明如下： 新增“密码最短使用时间(分钟)”的参数设置。
2016-03-14	第一次正式发布。

版权所有 © 华为技术有限公司