

统一身份认证

用户指南

文档版本 25
发布日期 2024-12-25



版权所有 © 华为技术有限公司 2024。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



HUAWEI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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

目录

1 使用前必读	1
2 登录华为云	5
3 IAM 用户	14
3.1 创建 IAM 用户	14
3.2 给 IAM 用户授权	19
3.3 IAM 用户登录	20
3.4 查看或修改 IAM 用户信息	22
3.5 删除 IAM 用户	27
3.6 修改 IAM 用户密码	28
3.7 管理 IAM 用户访问密钥	28
4 用户组及授权	31
4.1 创建用户组并授权	31
4.2 用户组添加/移除用户	35
4.3 删除用户组	36
4.4 查看或修改用户组	37
4.5 移除用户组权限	40
4.6 依赖角色的授权方法	42
5 权限管理	43
5.1 权限基本概念	43
5.2 角色	44
5.3 策略	45
5.3.1 策略内容	45
5.3.2 策略语法	46
5.3.3 策略变量	57
5.3.4 策略鉴权规则	59
5.4 系统策略更名详情	59
5.5 查看授权记录	64
5.6 自定义策略	65
5.6.1 创建自定义策略	65
5.6.2 修改、删除自定义策略	70
5.6.3 自定义策略使用样例	71
5.6.4 支持 IAM 资源粒度授权的云服务	74

6 项目	78
7 委托	81
7.1 委托其他账号管理资源	81
7.1.1 基本流程	81
7.1.2 创建委托（委托方操作）	82
7.1.3（可选）分配委托权限（被委托方操作）	84
7.1.4 切换角色（被委托方操作）	86
7.2 委托其他云服务管理资源	87
7.3 删除或修改委托	88
8 安全设置	90
8.1 安全设置概述	90
8.2 基本信息	91
8.3 敏感操作	92
8.4 登录验证策略	107
8.5 密码策略	109
8.6 访问控制	111
9 身份提供商	113
9.1 身份提供商概述	113
9.2 虚拟用户 SSO 与 IAM 用户 SSO 的适用场景	116
9.3 基于 SAML 协议的虚拟用户 SSO	118
9.3.1 基于 SAML 协议的虚拟用户 SSO 配置概述	118
9.3.2 步骤 1：创建身份提供商	121
9.3.3 步骤 2：配置企业 Idp	126
9.3.4 步骤 3：配置身份转换规则	126
9.3.5 步骤 4：登录验证	129
9.3.6（可选）步骤 5：配置企业管理系统登录入口	130
9.4 基于 SAML 协议的 IAM 用户 SSO	131
9.4.1 基于 SAML 协议的 IAM 用户 SSO 配置概述	131
9.4.2 步骤 1：创建身份提供商	134
9.4.3 步骤 2：配置企业 IdP	139
9.4.4 步骤 3：配置外部身份 ID	140
9.4.5 步骤 4：登录验证	141
9.4.6（可选）步骤 5：配置企业管理系统登录入口	142
9.5 基于 OIDC 协议的虚拟用户 SSO	143
9.5.1 联邦身份认证配置概述	143
9.5.2 步骤 1：创建身份提供商	144
9.5.3 步骤 2：配置身份转换规则	149
9.5.4（可选）步骤 3：配置企业管理系统登录入口	152
9.6 身份转换规则详细说明	153
10 自定义身份代理	159
10.1 使用委托方式配置自定义身份代理配置步骤	159

10.2 使用委托方式创建云服务登录地址.....	161
10.3 使用 token 方式配置自定义身份代理配置步骤.....	164
10.4 使用 token 方式创建云服务登录地址.....	166
11 多因素认证与虚拟 MFA.....	169
11.1 多因素认证.....	169
11.2 虚拟 MFA.....	169
12 查看 IAM 操作记录.....	174
12.1 开通云审计服务.....	174
12.2 在 CTS 事件列表查看云审计事件.....	178
13 调整配额.....	182

1 使用前必读

IAM 的使用对象

IAM的使用对象为管理员：

- 账号：账号可以使用所有服务，包括IAM。
- admin用户组中的用户：IAM默认用户组admin中的用户，可以使用所有服务，包括IAM。
- 授予了“Security Administrator”权限的用户：具备该权限的用户为IAM管理员，可以使用IAM。

推荐您在使用IAM前，开通云审计服务CTS，方便查看、审计以及回溯IAM的关键操作记录。详情请参考：[开通云审计服务](#)。

如何进入 IAM 控制台

步骤1 登录华为云，在右上角单击“控制台”。

图 1-1 进入控制台



步骤2 在控制台页面，鼠标移动至右上方的账号名，在下拉列表中选择“统一身份认证”。

图 1-2 进入统一身份认证



----结束

账号

您注册华为云后，系统自动创建账号，账号是资源的归属以及使用计费的主体，对其所拥有的资源具有完全控制权限，可以访问所有云服务。账号不能在IAM中修改和删除，如果您需要删除账号，可以在账号中心进行注销。

如下图所示，使用账号登录后，在IAM的“用户”中可以看到账号对应的用户，在IAM中标识为“企业管理员”。

IAM 用户

由管理员在IAM中创建的用户，如下图所示，“James”为管理员创建的IAM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。

图 1-3 管理员创建的 IAM 用户

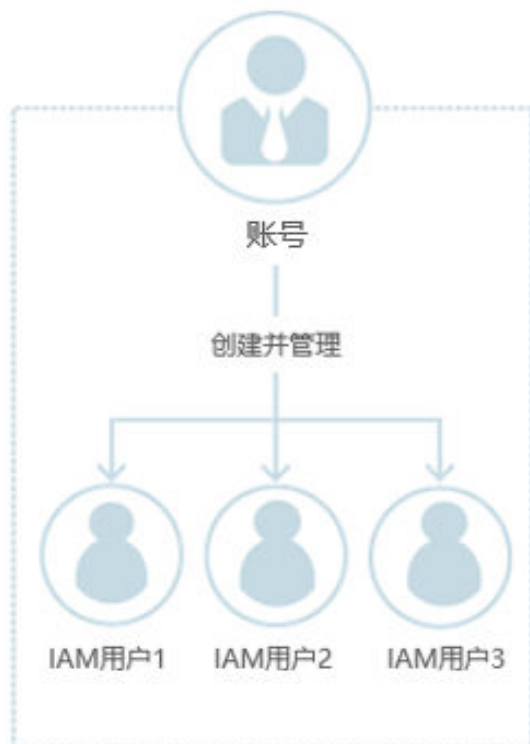


账号与 IAM 用户的关系

账号与IAM用户可以类比为父子关系，账号是资源归属以及计费的主体，对其所拥有的资源具有完全控制权限。

IAM用户由管理员创建，权限由管理员分配，管理员可以随时修改或者撤销IAM用户的权限。IAM用户进行资源操作时产生的费用统一计入账号中，IAM用户不需要为资源付费。

图 1-4 账号和 IAM 用户的关系



用户组

用户组是用户的集合，IAM可以通过用户组功能实现用户的授权。您创建的IAM用户，加入特定用户组后，将具备对应用户组的权限，可以基于权限对云服务进行操作。当某个用户加入多个用户组时，此用户同时拥有多个用户组的权限，即多个用户组权限的全集。

“admin”为缺省用户组，具有所有云服务资源的操作权限。将用户加入该用户组后，用户可以操作并使用所有云资源，包括但不限于创建用户组及用户、修改用户组权限、管理资源等。

图 1-5 用户组



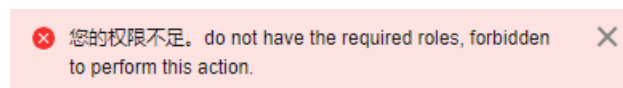
权限

IAM预置了各服务的常用权限，例如管理员权限、只读权限，您可以直接使用这些权限。默认情况下，管理员创建的IAM用户没有任何权限。管理员可以将其加入用户组，并给用户组授予策略或角色，用户组中的用户将获得用户组的权限。同时，IAM用户也可以为自身授予权限。这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

- 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。

如下图所示，如果您授予IAM用户弹性云服务器ECS的权限，则该IAM用户除了ECS，不能访问其他任何服务，如果尝试访问其他服务，系统将会提示没有权限。

图 1-6 系统提示没有权限

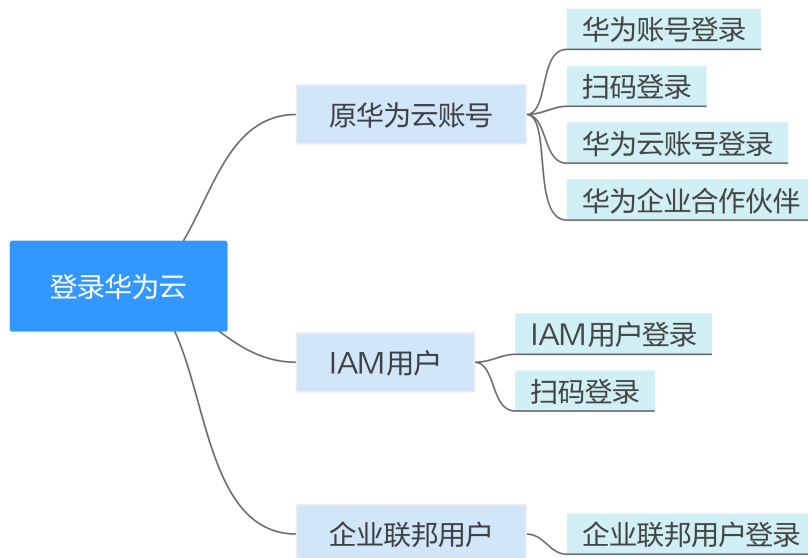


2 登录华为云

您可以通过以下方式登录华为云，如[图2-1](#)所示。

- **华为云账号**：您首次使用华为云时创建的账号，该账号是您的华为云资源归属、资源使用计费的主体，对其所拥有的资源及云服务具有完全的访问权限。如果您需要以账号身份登录华为云，请参考：
 - **华为账号登录**：华为账号是您访问华为各网站的统一“身份标识”，您只需注册华为账号，即可访问所有华为服务。**华为账号和华为云账号**不同，请确认您已注册华为账号。如果您暂未注册华为账号，建议您先注册华为账号并开通华为云，请参考[注册华为账号并开通华为云](#)。
 - **扫码登录**：如果您在华为云APP上登录了账号或IAM用户，可以通过APP扫描界面二维码登录华为云。
 - **华为云账号登录**：使用您已注册的华为云账号登录。如果您是首次使用华为云，建议您[注册华为账号并开通华为云](#)。
 - **华为企业合作伙伴账号登录**：您可以通过**华为企业合作伙伴登录**华为云，首次登录时需要根据系统提示创建或绑定已有华为云账号，后续可以通过该账号自动跳转登录，也可以为创建的华为云账号设置密码或绑定已有华为云账号，通过账号登录华为云。
- **IAM用户**：由**管理员**在IAM中创建的用户，是云服务的使用人员，根据账号授予的权限使用资源。如果您是IAM用户，登录方法请参考：
 - **IAM用户登录**：**账号与IAM用户**可以类比为父子关系，IAM用户是由**管理员**在IAM中创建的用户，IAM用户登录后可根据权限使用云服务。
 - **扫码登录**：如果您在华为云APP上登录了账号或IAM用户，可以通过APP扫描界面二维码登录华为云。
- **企业联邦用户**：由**管理员**在IAM中创建的企业身份提供商用户。
 - **企业联邦用户登录**：如果您已知创建该身份提供商的华为云账号名称、身份提供商名称、企业管理系统的账号和密码，可以通过此方式登录华为云。

图 2-1 登录华为云



华为账号登录

华为账号是用户访问华为各网站的统一“身份标识”，您只需注册一个华为账号，即可访问所有华为服务。您可以在[华为账号网站](#)注册和管理华为账号或在华为云[注册华为账号并开通华为云](#)。在通过华为账号登录华为云控制台时，可使用“手机号/邮件地址/账号名/原华为云账号”方式。

通过华为账号登录方法如下：

- 步骤1** 在华为云的登录页面，输入手机号/邮件地址/账号名/原华为云账号、账号密码，单击“登录”。

图 2-2 华为账号登录

说明

- 如您输入的账号信息为原华为云账号或已经注册华为账号并开通了华为云业务，可直接登录成功。
- 如您输入的账号信息为华为账号且该账号使用的手机号/邮件地址开通了华为云业务，请参照[步骤2](#)完成操作。
- 如您输入的账号信息为华为账号但该账号使用的手机号/邮件地址未开通华为云业务，请参照[步骤3](#)完成操作。

步骤2 选择本次登录账号。

系统根据您输入账号信息进行检测，如您使用同一手机号或邮件地址分别注册过华为账号和华为云账号，需要选择任意一种进行登录。

- 选择华为账号登录：单击“确定”，参照[步骤3](#)继续完成登录操作。
- 选择原华为云账号登录：单击“确定”，登录华为云成功。

步骤3 单击“获取验证码”并输入验证码，单击“确定”。

如您注册时，同时绑定手机号和邮件地址，您还可以切换邮件地址进行身份验证。

步骤4 在“是否信任此浏览器？”弹框中，单击“信任”。

步骤5 在“账号提醒”弹框中，单击“直接开通华为云”或“切换账号登录”。

- 直接开通华为云：为该华为账号开通华为云业务。开通后，可以通过该华为账号登录华为云。单击后，参照[步骤6](#)继续完成操作。
- 切换账号登录：使用已注册的华为云账号登录。单击后，跳转至“华为账号登录”页面，参照[步骤1](#)通过其他账号登录华为云。

步骤6 （如系统没有检测出注册过华为云账号，无需执行此步骤）选择华为云账号进行升级。

说明

系统会根据您华为账号的手机号或邮件地址，检测您可能注册过的华为云账号，您可以选其一升级成为华为账号，即可使用一个统一账号访问华为云、华为开发者联盟、华为商城等更多华为服务。

- 选择华为云账号进行升级
 - a. 如您需要升级，请选择华为云账号，并单击“下一步”。
 - b. 输入原华为云账号密码，单击“下一步”。
 - c. 确认升级后的华为账号信息，单击“确定”，系统提示升级成功。
 - d. 单击“完成”，系统跳转至华为云页面。

说明

- 此时华为账号已成功关联华为云业务，下次请使用华为账号登录，原华为云账号失效。
- 如果升级失败，请参考“常见问题>账号管理类>升级华为账号失败怎么办”。
- 重新开通华为云
 - 单击“跳过此步，直接开通华为云”，请参照**步骤7**继续完成操作。

步骤7 在“开通华为云”页面，勾选服务条款，单击“开通”，系统提示开通成功。
开通成功即可通过该华为账号登录华为云。

----结束

扫码登录

华为云APP是华为云的手机客户端，通过华为云APP，您可以在手机上远程管理您的华为云服务资源。如果您在华为云APP上登录了账号或IAM用户，通过APP扫描页面二维码即可登录华为云，无需重复输入账号信息。

说明

华为云APP暂不支持国际站账号登录，因此国际站账号暂不支持扫码登录，请通过账号、密码登录华为云。

通过华为云APP扫码登录方法如下：

步骤1 在华为云的登录页面，单击右上角的二维码，进入“扫码登录”页面。

图 2-3 扫码登录



步骤2 使用华为云APP扫描页面二维码，登录华为云。

----结束

华为企业合作伙伴账号登录

如果您已有“[华为企业合作伙伴账号](#)”，可以通过此方式登录华为云，无需记录多套身份信息。

步骤1 单击“华为企业合作伙伴账号”，如下图所示。

图 2-4 华为企业合作伙伴账号



步骤2 根据界面指引登录华为企业合作伙伴账号。

- 首次登录时：页面自动跳转至创建或关联华为云账号页面，输入账号名和手机号、验证码。单击“创建并绑定”，登录华为云控制台。
- 后续登录时：直接跳转至华为云控制台。

首次登录成功后，后续可以使用**步骤2**中设置的账号名或手机号，通过华为云账号登录华为云控制台。

----结束

华为云账号登录

如果您已注册华为云账号，可以通过该账号直接登录华为云。该账号是您的华为云资源归属、资源使用计费的主体，对其所拥有的资源及云服务具有完全的访问权限，可以重置用户密码、分配用户权限等。所有IAM用户产生的费用账单由账号统一接收并付费。账号在登录华为云控制台时，可使用“账号名/邮件地址”或“手机号登录”方式。

📖 说明

已升级华为账号的华为云账号暂不支持登录，请使用[华为账号登录](#)。

通过华为云账号登录方法如下：

步骤1 单击“华为云账号”，如图所示。

图 2-5 华为云账号



步骤2 输入您的账号信息，单击“登录”。

- 账号名/邮件地址：华为云账号名/与账号绑定的邮件地址。

📖 说明

账号名不区分大小写。

- 密码：账号密码，如果您忘记了账号的登录密码，可以单击“忘记密码”进行重置，重置方法请参见：[忘记账号密码](#)。
- 手机号登录：如果您忘记了华为云账号，可以单击“手机号登录”，可以通过已绑定的手机号、账号密码登录华为云。

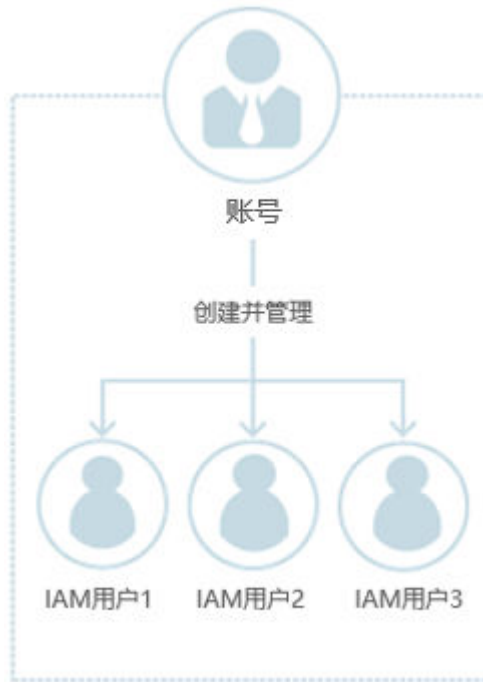
----结束

IAM 用户登录

IAM用户是由华为云账号或[管理员](#)在IAM中创建的用户，是云服务的使用人员，具有独立的身份凭证（密码和访问密钥），根据账号授予的权限使用资源。IAM用户不进行独立的计费，由所属账号统一付费。

账号与IAM用户可以类比为父子关系，如下图所示。

图 2-6 账号与 IAM 用户



IAM用户登录方法如下：

步骤1 在华为云的登录页面，单击登录下方的“IAM用户”，在“IAM用户登录”页面，输入账号名，IAM用户名/邮件地址和密码。

图 2-7 IAM 用户登录



- 租户名/原华为云账号：IAM用户所属的账号，即华为云账号。如果不知道账号名，请向**管理员**获取。
- IAM用户名/邮件地址：在IAM创建用户时，输入的**IAM用户**名/邮件地址。如果不知道用户名及初始密码，请向**管理员**获取。

- IAM用户密码：IAM用户的密码，非账号密码。

步骤2 单击“登录”。

----结束

企业联邦用户登录

企业联邦用户是在企业管理系统中创建的用户，账号在IAM控制台创建[身份提供商](#)后，企业联邦用户可以登录华为云并根据对应权限使用云服务。详情请参考：[身份提供商概述](#)。

如果您已知创建该身份提供商的华为云账号名称、身份提供商名称、企业管理系统的账号和密码，可以通过此方式登录华为云。

步骤1 在华为云的登录页面，单击登录下方的“企业联邦用户”，在“企业联邦身份登录”页面，输入账号名，选择身份提供商名称。

图 2-8 企业联邦身份登录



- 原华为云账号名/租户名：创建身份提供商的华为云账号名称。如果不知道账号名，请向[管理员](#)获取。
- 身份提供商名称：[管理员](#)创建身份提供商时，设置的名称。如果不知道身份提供商名称，请向[管理员](#)获取。

步骤2 单击“前往登录”，跳转至企业管理系统登录页面。

步骤3 在企业管理系统登录页面，输入企业管理系统用户名、密码。

步骤4 单击“登录”，登录华为云。

----结束

3 IAM 用户

3.1 创建 IAM 用户

如果您是**管理员**，在华为云购买了多种资源，例如弹性云服务器、云硬盘、裸金属服务器等，您需要将资源分配给企业中不同的员工或者应用程序使用，为了避免分享自己的账号密码，您可以使用IAM的用户管理功能，给员工或应用程序创建IAM用户。

默认情况下，**新创建的IAM用户没有任何权限**。管理员可以为其授予权限，或将其加入用户组，并**给用户组授权**，用户组中的用户将获得用户组的权限。IAM用户也可以为自身授予权限。IAM用户拥有权限后，IAM用户就可以基于权限对云服务进行操作。

“admin”为缺省用户组，具有所有云服务资源的操作权限。将用户加入该用户组后，用户可以操作并使用所有云服务资源，包括但不仅限于创建用户组及用户、修改用户组权限、管理资源等。

📖 说明

如果删除并重新创建同名用户，则需要重新授权。

操作步骤

步骤1 管理员登录**IAM控制台**。

步骤2 在左侧导航窗格中，选择“用户”，单击右上方的“创建用户”。

图 3-1 创建用户



步骤3 在“创建用户”页面配置“用户信息”。如需一次创建多个用户，可以单击“添加用户”进行批量创建，每次最多可创建10个用户。

表 3-1 用户信息

参数	描述
用户名	自定义，不可与账号、或账号中其他IAM用户重复。
邮件地址	自定义，不可与账号、或账号中其他IAM用户重复。可用于IAM用户身份验证、重置密码。
手机号	自定义，不可与账号、或账号中其他IAM用户重复。可用于IAM用户身份验证、重置密码。
外部身份ID	IAM SSO类型的联邦用户单点登录中，与当前实体IAM用户对接的，企业自身用户的身份ID值。 为IAM用户配置 基于SAML协议的虚拟用户SSO 时，“外部身份ID”为必选参数（不超过128个字符）。

 说明

- 用户可以使用此处设置的用户名、邮件地址或手机号任意一种方式登录华为云。
- 当用户忘记密码时，可以通过此处绑定的邮箱或手机自行重置密码，如果用户没有绑定邮箱或手机号码，只能由管理员重置密码。

步骤4 选择“访问方式”。

图 3-2 选择访问方式



表 3-2 访问方式

访问方式	说明
编程访问	为IAM用户启用 访问密钥或密码 ，支持用户通过API、CLI、SDK等开发工具访问云服务。
管理控制台访问	为IAM用户启用 密码 ，支持用户登录管理控制台访问云服务。此时凭证类型“密码”为必选项。

说明

- 如果IAM用户**仅需登录管理控制台访问云服务**，建议访问方式选择**管理控制台访问**，凭证类型为**密码**。
- 如果IAM用户**仅需编程访问云服务**，建议访问方式选择**编程访问**，凭证类型为**访问密钥**。
- 如果IAM用户**需要使用密码作为编程访问的凭证**（部分API要求），建议访问方式选择**编程访问**，凭证类型为**密码**。
- 如果IAM用户使用部分云服务时，需要在其**控制台验证访问密钥**（由IAM用户输入），建议访问方式选择**编程访问和管理控制台访问**，凭证类型为**密码和访问密钥**。例如IAM用户在控制台使用云数据迁移CDM服务创建数据迁移，需要通过访问密钥进行身份验证。

步骤5 选择“凭证类型”。

图 3-3 选择凭证类型



表 3-3 配置凭证类型

凭证类型	说明
访问密钥	创建用户完成后即可下载本次创建的所有用户的 访问密钥 (AK/SK) 。 一个用户最多拥有两个访问密钥。
密码	自定义 自定义用户密码，并选择用户首次登录时是否需要重置密码。 如果您是用户的使用主体，建议您选择该方式，设置自己的登录密码，且无需勾选首次登录时重置密码。
	自动生成 系统自动生成IAM用户的登录密码，创建完用户即可下载excel形式的密码文件。将密码文件提供给用户，用户使用该密码登录。 密码文件需在创建完用户后及时下载，如取消下载将无法再次获取该密码文件。可以通过 修改IAM用户密码 重新设置用户密码。 仅在创建单个用户时适用。

凭证类型		说明
	首次登录时设置	系统通过邮件发一次性登录链接给用户，用户登录控制台并设置密码。 如果您不是用户的使用主体，建议选择该方式，同时输入用户的邮件地址和手机，用户通过邮件中的一次性链接登录华为云，自行设置密码。该链接 7天 内有效。
USB KEY		USB KEY是一种通过硬件存储用户凭证的设备。使用USB KEY进行身份验证，无需输入密码，可以避免密码意外泄漏带来的账号安全问题。 勾选后，该IAM用户只能使用USB KEY登录，IAM用户将无法使用密码相关功能。

表 3-4 配置建议

管理控制台访问	编程访问	访问凭证	建议访问方式	建议凭证类型
勾选	不勾选	无特殊要求。	管理控制台	密码
不勾选	勾选	无特殊要求。	编程访问	访问密钥
不勾选	勾选	需要使用密码作为编程访问的凭证（部分API要求）。	编程访问	密码
勾选	勾选	需要在控制台验证访问密钥（由IAM用户输入）。 例如：例如IAM用户在控制台使用云数据迁移CDM服务创建数据迁移，需要通过访问密钥进行身份验证。	编程访问和管理控制台	密码和访问密钥

步骤6 选择“登录保护”设置。仅访问方式勾选管理控制台访问时，可以开启。

图 3-4 选择登录保护



- 开启登录保护（推荐）：**开启登录保护后，IAM用户登录时，除了在登录页面输入用户名和密码外（第一次身份验证），还需要在登录验证页面输入验证码（第二次身份验证），该功能是一种安全实践，建议开启登录保护，多次身份认证可以提高安全性。

您可以选择通过手机、邮箱、虚拟MFA进行登录验证。

- 不开启：创建完成后，如需开启登录保护，请参见：[登录保护](#)。

步骤7 单击“下一步”，（可选）勾选要加入的用户组，将用户加入到用户组。加入用户组后，用户将具备用户组的权限。

图 3-5 加入用户组



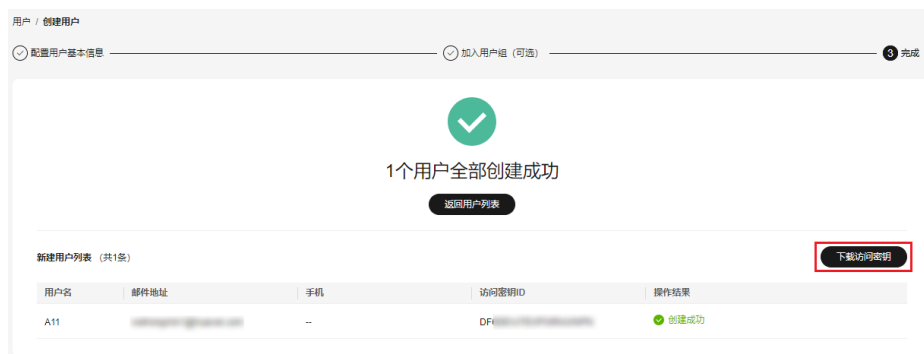
说明

- 如需创建新的用户组，可单击“创建用户组”，创建完成并勾选该用户组，用户将加入到新创建的用户组中。
- 如果该用户是管理员，可以将用户加入默认用户组“admin”中。
- 一个用户最多可以同时加入10个用户组。

步骤8 单击“创建用户”，IAM用户创建完成，用户列表中显示新创建的IAM用户。

- 如果“5>凭证类型”勾选了“访问密钥”，可在此页面下载访问密钥。
- 如果“5>凭证类型”勾选了“密码>自动生成”，可在此页面下载密码。

图 3-6 创建成功



----结束

后续操作

- 如果管理员在创建IAM用户时，没有将其加入任何用户组，**新创建的IAM用户没有任何权限**，管理员或IAM用户自身可以在IAM控制台为其授予权限。授权后，用户即可根据权限使用账号中的云服务资源。详情请参考[给IAM用户授权](#)。
- IAM用户的登录方式与华为账号/华为云账号的登录方式不同，详情请参见[IAM用户登录](#)。

3.2 给 IAM 用户授权

如果管理员在**创建IAM用户**时，没有将其加入任何用户组，**新创建的IAM用户没有任何权限**，管理员或IAM用户自身可以在IAM控制台为其授予权限。授权后，用户即可根据权限使用账号中的云服务资源。

约束与限制

一个用户基于企业项目可绑定的权限数（包括系统权限和自定义策略）上限为500个。

操作步骤

步骤1 管理员登录**IAM控制台**。

步骤2 管理员在用户列表中，单击新建的用户，右侧的“授权”。

图 3-7 IAM 用户授权



步骤3 在授权页面，选择授权方式和权限。

- **继承所选用户组的策略**：将IAM用户加入用户组，用户将拥有所选用户组的所有权限。

选择“继承所选用户组的策略”，请勾选用户需要加入的用户组。

图 3-8 暂未开通企业项目



- **直接给用户授权（适用于企业项目授权）**：直接给IAM用户授予云服务权限。该授权方式仅在您开通企业项目后支持，如需开通请参考：[开通企业项目](#)。

选择“直接给用户授权”，请勾选需要授予用户的权限，并单击页面右下角“下一步”，进入“选择授权范围”页面，参考3继续完成操作。

图 3-9 已开通企业项目



说明

- 如果将IAM用户加入默认用户组“admin”，则IAM用户为管理员，可以对所有云服务执行任意操作。
- 当某个用户加入多个用户组时，此用户同时拥有多个用户组的权限，即取多个用户组权限的全集。
- 所有使用IAM授权的云服务的系统策略，请参见：[系统权限](#)。
- 如果您开通了企业管理，将不能创建IAM项目，请谨慎操作。

步骤4 （如授权方式选择“继承所选用户组的策略”，无需执行此步骤）在“设置最小授权范围”页面，选择授权IAM用户使用的企业项目。

步骤5 单击“确定”，完成IAM用户授权。

授权完成后，管理员可以在“权限管理>授权管理”页面查看、修改该IAM用户的权限。

说明

企业项目授权场景下，授予OBS相关的权限后，大概需要等待15~30分钟策略才能生效。

----结束

3.3 IAM 用户登录

管理员创建IAM用户后，这个新建的IAM用户可以登录华为云。登录方式包括IAM控制台提供的“IAM用户登录链接”。

登录方法 1：华为云登录页面

步骤1 在华为云的登录页面，单击登录下方的“IAM用户”，在“IAM用户登录”页面，输入账号名，IAM用户名/邮件地址和密码。

图 3-10 IAM 用户登录



- 租户名/原华为云账号：IAM用户所属的账号，即华为云账号。如果不知道账号名，请向**管理员**获取。
- IAM用户名/邮件地址：在IAM创建用户时，输入的**IAM用户**名/邮件地址。如果不知道用户名及初始密码，请向**管理员**获取。
- IAM用户密码：IAM用户的密码，非账号密码。

步骤2 单击“登录”，完成登录。

📖 说明

- 如果创建IAM用户时，IAM用户没有加入任何用户组，则IAM用户不具备任何权限，不能对云服务进行操作，需要联系管理员参考**创建用户组并授权**和**用户组添加/移除用户**给IAM用户授权。
- 如果创建IAM用户时，IAM用户加入了默认用户组“admin”，则IAM用户为管理员，可以对所有云服务执行任意操作。

----结束

登录方法：IAM 用户专属链接

此方法需要向管理员获取专属登录链接，获取后建议您保存该链接，方便后续快速登录。使用IAM用户专属链接登录时，系统会自动识别用户的账号名，用户仅需要填写用户名和密码，方便用户快速登录。

步骤1 管理员在**IAM控制台**，复制“IAM用户登录链接”，并将链接发送给用户。

图 3-11 IAM 用户登录链接



步骤2 用户在浏览器中打开复制的地址，输入“用户名/邮件地址”和“密码”，单击“登录”，完成登录。

图 3-12 IAM 用户通过链接登录


----结束

3.4 查看或修改 IAM 用户信息

管理员在IAM用户列表中，单击用户名，或者单击右侧的“安全设置”，可以查看或修改IAM用户的基本信息、所属用户组、安全设置，并查看或删除授权记录。

图 3-13 进入 IAM 用户安全设置页面



管理员单击搜索框右侧的“”，可以修改用户列表展示项目，用户名、状态、操作为默认展示项目。可选项目：描述、最近活动时间、创建时间、访问方式、登录验证方式、MFA（状态）、密码使用时长、访问密钥状态、外部身份ID。

最近活动时间记录IAM用户和账号5分钟内的第一次登录时间，如果5分钟内登录多次，仅记录第一次登录时间。如果不登录账号，仅使用账号密码获取token，也将会刷新最近活动时间。

基本信息

只能修改IAM用户的基本信息，不能修改账号的基本信息。用户名称、用户ID、创建时间仅支持查看，不支持修改。

图 3-14 修改 IAM 用户状态、访问方式、描述、外部身份 ID



- **状态：**修改IAM用户的状态，IAM用户的状态默认为启用，如果需要停止使用该IAM用户，可以将IAM用户的状态设置为“停用”。停用后，该IAM用户将无法通过任一方式访问华为云，包括管理控制台访问和编程访问。IAM用户也可以自行修改该状态。
- **访问模式：**修改iam用户的访问方式。

📖 说明

- 请参考如下说明，修改访问模式：
 - 如果IAM用户**仅需登录管理控制台访问云服务**，建议访问方式选择**管理控制台访问**，凭证类型为**密码**。
 - 如果IAM用户**仅需编程访问华为云服务**，建议访问方式选择**编程访问**，凭证类型为**访问密钥**。
 - 如果IAM用户**需要使用密码作为编程访问的凭证**（部分API要求），建议访问方式选择**编程访问**，凭证类型为**密码**。
 - 如果IAM用户使用部分云服务时，需要在**其控制台验证访问密钥**（由IAM用户输入），建议访问方式选择**编程访问和管理控制台访问**，凭证类型为**密码和访问密钥**。例如IAM用户在控制台使用云数据迁移CDM服务创建数据迁移，需要通过访问密钥进行身份验证。
 - 如果当前IAM用户的访问模式为**编程访问**或**编程访问和管理控制台访问**，取消编程访问可能会使IAM用户无法访问华为云服务，请谨慎修改。
- **描述：**修改IAM用户的描述信息。
- **外部身份ID：**IAM SSO类型的联邦用户单点登录中，与当前实体IAM用户对接的，企业自身用户的身份ID值。

所属用户组

所属用户组表示用户具备的权限，**通过修改IAM用户的所属用户组可以修改用户的权限**。如需修改用户所属用户组权限，请参见：[查看或修改用户组](#)。

只能修改IAM用户的所属用户组，账号属于默认用户组“admin”，不能修改。

- 单击“加入到用户组”，在“配置用户组”中选择需要加入的用户组。一个用户可以加入一个或是多个用户组。用户加入用户组后，拥有用户组的所有权限。

图 3-15 将 IAM 用户加入用户组



- 单击IAM用户所属用户组右侧的“移除”，单击“是”，退出选中的用户组，用户将不再拥有该用户组权限。

图 3-16 将 IAM 用户移出用户组



安全设置

管理员可以该页面修改IAM用户的多因素认证设备、登录凭证、登录保护和访问密钥。IAM用户如需修改自己的手机号、邮件地址、虚拟MFA设备，请参考[安全设置概述](#)。

图 3-17 IAM 用户安全设置



- 多因素认证设备，只能修改IAM用户的多因素认证设备，不能修改账号的多因素认证设备。
 - 修改用户的手机、邮件地址。支持清空IAM用户的手机号和邮件地址。

说明

修改IAM用户绑定手机号和邮件地址不可与账号、其他IAM用户重复。

- 虚拟MFA设备：给用户重置虚拟MFA设备。更多有关多因素认证以及MFA的介绍，详情请参见：[多因素认证与虚拟MFA](#)。
- 登录凭证：修改IAM用户的登录密码，详情请参见：[修改IAM用户密码](#)。支持清空IAM用户的登录密码，该操作将导致其无法使用原有密码访问华为云，请谨慎操作。
- 登录保护：修改IAM用户的登录验证方式，支持虚拟MFA、手机和邮箱。
登录保护表示用户登录控制台时，除了在登录页面输入用户名和密码（第一次身份认证），还需要在“登录验证”页面输入验证码（第二次身份验证），该功能默认关闭。
- 访问密钥：管理IAM用户的访问密钥，详情请参见：[管理IAM用户访问密钥](#)。

授权记录

管理员可以查看或删除IAM用户所拥有的权限。如需修改该IAM用户的权限，请参考[所属用户组](#)。

图 3-18 IAM 用户授权记录

权限	权限描述	项目[所属区域]	授权主体	主体描述	主体类型	操作
ADN FullAccess	应用加速网络服务所有权限	所有资源 [包含未来新增...]	开发人员组	--	用户组	删除
AOM FullAccess	应用运维管理服务所有权限	所有资源 [包含未来新增...]	开发人员组	--	用户组	删除
Astro Pro FullAccess	Astro企业应用管理员权限	所有资源 [包含未来新增...]	开发人员组	--	用户组	删除

如需查看账号下所有授权记录，请参考：[查看授权记录](#)。

说明

删除授权记录，将删除该IAM用户所属用户组的权限，该用户组中所有IAM用户不再拥有该权限，请谨慎操作。

批量修改 IAM 用户信息

IAM支持批量修改IAM用户状态、访问方式、验证方式、登录密码、手机和邮件地址，修改方式类似，以修改IAM用户状态为例，说明批量修改IAM用户信息的方法。

步骤1 进入IAM控制台，在左侧导航栏选择“用户”页签。

步骤2 在用户列表中，勾选需要修改的用户。勾选完成后，单击用户列表上方的“编辑”。

图 3-19 编辑用户信息



步骤3 选择需要修改的IAM用户属性，以修改IAM用户状态为例，选择“状态”。

图 3-20 选择状态



步骤4 选择要给IAM用户配置的目标状态，若要停用IAM用户则选择“停用”，启用IAM用户则选择“启用”。

图 3-21 修改状态



说明

请排查用户是否有其他服务或场景在使用，停用正在使用的用户可能会对业务产生影响。

步骤5 单击“确定”，确定IAM用户配置。

步骤6 单击“确认”，完成所选IAM用户状态的修改。

----结束

3.5 删除 IAM 用户

⚠ 注意

请谨慎删除IAM用户，删除后该IAM用户将无法登录，该用户的IAM用户名、IAM密码、访问密钥、及其所有IAM授权关系将被清除且不可恢复。

- 请排查要删除的用户是否有其他服务或场景在使用，若无法确定，建议先使用“停用”功能，以免业务运行失败后无法回退。如需暂时停用IAM用户，请参考[基本信息](#)，批量停用请参考[批量修改IAM用户信息](#)。
- 如需将IAM用户从某个用户组移除，请参见：[用户组添加/移除用户](#)。
- IAM用户可以自行完成用户删除。

操作步骤

步骤1 进入IAM控制台，在左侧导航栏选择“用户”页签。

步骤2 单击需要删除的IAM用户操作列的“删除”，确认弹窗中删除用户的信息，单击“是”，删除成功。

图 3-22 删除 IAM 用户



----结束

批量删除 IAM 用户

步骤1 进入IAM控制台，在左侧导航栏选择“用户”页签。

步骤2 在用户列表中，勾选需要删除的用户。勾选完成后，单击用户列表上方的“删除”。

图 3-23 批量删除 IAM 用户



步骤3 弹窗中单击“是”，完成所选IAM用户删除。

----结束

3.6 修改 IAM 用户密码

如果IAM用户忘记了登录密码，并且没有绑定邮件地址或者手机，可以由管理员在IAM中重置密码。


管理员在IAM用户列表中，单击右侧的“安全设置”，在“安全设置”页签，单击“登录凭证>登录密码”右侧的，重置IAM用户的登录密码。

图 3-24 修改 IAM 用户密码



说明

- IAM提供的安全设置功能，适用于管理员重置IAM用户的密码。
- 账号自动生成的IAM用户无法通过“安全设置”修改密码，请前往“账号中心>基本信息”修改账号密码。
- IAM用户可以在[基本信息](#)页面修改自己的密码。账号如需修改密码，请参考[如何修改密码](#)。
- 通过邮件地址设置：用户通过邮件中的一次性链接登录控制台时，自行设置密码。
- 自动生成：系统自动生成随机密码，创建用户成功后可以下载并将新密码发送给用户。
- 自定义：管理员自定义用户的密码，并将新密码发送给用户。

3.7 管理 IAM 用户访问密钥

访问密钥即AK/SK（Access Key ID/Secret Access Key），是您通过开发工具（API、CLI、SDK）访问华为云时的身份凭证，不能登录控制台。系统通过AK识别访问用户的身份，通过SK进行签名验证，通过加密签名验证可以确保请求的机密性、完整性和请求者身份的正确性。

如果IAM用户不能登录控制台，在需要使用访问密钥或者访问密钥遗失的情况下，可以由管理员在IAM中管理IAM用户的访问密钥。

管理员在IAM用户列表中，单击右侧的“安全设置”，新增或者删除用户的访问密钥。

图 3-25 管理 IAM 用户访问密钥



说明

- 企业联邦用户不能创建访问密钥，但可以创建临时访问凭证（临时AK/SK和SecurityToken），具体内容请参见：[临时访问密钥](#)。
- IAM提供的“安全设置”功能，适用于管理员管理IAM用户的访问密钥。在我的凭证中也可以[管理访问密钥](#)，我的凭证适用于所有用户在可以登录控制台的情况下，自行管理访问密钥。
- 账号和IAM用户的访问密钥是单独的身份凭证，即账号和IAM用户仅能使用自己的访问密钥进行API调用。
- 访问密钥的“最近使用时间”记录IAM用户15分钟内的第一次使用时间，如果15分钟内多次使用访问密钥，仅记录第一次使用时间。
- 新增访问密钥并下载
 - a. 单击“新增访问密钥”。

图 3-26 新增访问密钥



说明

- 每个用户最多可以拥有2个访问密钥，有效期为永久。为了账号安全性，建议管理员定期给用户更换访问密钥。
- b. 若开启操作保护，则管理员需输入验证码或密码。
 - c. 单击“确定”，生成并下载访问密钥后，将访问密钥提供给用户。
- 删除访问密钥
 - a. 单击“删除”。

图 3-27 删除访问密钥



- b. 若开启操作保护，则管理员需输入验证码或密码。
- c. 单击“确定”。
- 启用、停用访问密钥
新创建的访问密钥默认为启用状态，如需停用该访问密钥，步骤如下：
 - a. 在“访问密钥”页签中，在需要停用的访问密钥右侧单击“停用”。

图 3-28 停用访问密钥



- b. 若开启操作保护，则需输入验证码或密码。然后单击“是”，停用访问密钥。

启用访问密钥方式与停用类似，请参考以上步骤。

4 用户组及授权

4.1 创建用户组并授权

管理员可以创建用户组，并给用户组授予策略或角色，然后将用户加入用户组，使得用户组中的用户获得相应的权限。IAM用户也可以为自身授予权限。IAM预置了各服务的常用权限，例如管理员权限、只读权限，管理员可以直接使用这些系统权限给用户组授权，授权后，用户就可以基于权限对云服务进行操作。详情请参见[给IAM用户授权](#)。如需查看所有云服务的系统权限，请参见：[系统权限](#)。

前提条件

在创建用户组前，建议管理员提前了解并规划以下内容：

- 了解权限的[基本概念及分类](#)。
- 所有使用IAM授权的云服务的系统策略，请参考：[系统权限](#)。

创建用户组

步骤1 管理员登录[IAM控制台](#)。

步骤2 在统一身份认证服务，左侧导航窗格中，选择“用户组”页签，单击右上方的“创建用户组”。

图 4-1 创建用户组



步骤3 在“创建用户组”界面，输入“用户组名称”。

步骤4 单击“确定”，用户组创建完成，用户组列表中显示新创建的用户组。

说明

您最多可以创建20个用户组，如果当前资源配额无法满足业务需要，您可以申请扩大配额，具体方法请参见：[如何申请扩大配额？](#)。

----结束

给用户组授权

以下步骤仅适用于给用户组**新增权限**。如需**移除权限**，请参见：[移除用户组权限](#)。

步骤1 在用户组列表中，单击新建用户组右侧的“授权”。

图 4-2 进入用户组权限设置页面



步骤2 在用户组选择策略页面中，勾选需要授予用户组的权限。单击“下一步”。

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](#)。

图 4-3 选择权限



步骤3 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 4-1 授权范围方案

可选方案	方案说明
所有资源	授权后，IAM用户可以根据权限使用账号中所有资源，包括企业项目、区域项目和全局服务资源。
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 。

可选方案	方案说明
指定区域项目资源	<p>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。</p> <p>说明 不支持选择专属云DEC的区域项目。</p>
全局服务资源	<p>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。</p> <p>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。</p>

步骤4 单击“确定”，完成用户组授权。

----结束

表4-2为常用权限，完整的权限列表请参见：[系统权限](#)。

 **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](#)、[依赖角色的授权方法](#)、[自定义策略使用样例](#)。
- 企业项目授权场景下，授予OBS相关的权限后，大概需要等待15~30分钟策略才能生效。

表 4-2 常用权限

权限	需要授予的策略	权限说明	授权范围
总负责人	FullAccess	支持基于策略授权服务的所有权限	所有资源
管理资源	Tenant Administrator	除IAM外，其他所有服务的管理员权限	所有资源
查看资源	Tenant Guest	所有资源的只读权限	所有资源
管理IAM用户	Security Administrator	IAM的管理员权限	全局服务资源
管理费用	BSS Administrator	<p>费用中心的管理员权限，包括管理发票、管理订单、管理合同、管理续费、查看账单等权限。</p> <p>说明 授权时，需要授予所有区域的“BSS Administrator”权限。</p>	指定区域项目资源

权限	需要授予的策略	权限说明	授权范围
计算域运维	ECS FullAccess	弹性云服务器的管理员权限	指定区域项目资源
	CCE FullAccess	云容器引擎的管理员权限	指定区域项目资源
	CCI FullAccess	云容器实例管理员权限	指定区域项目资源
	BMS FullAccess	裸金属服务器的管理员权限	指定区域项目资源
	IMS FullAccess	镜像服务的管理员权限	指定区域项目资源
	AutoScaling FullAccess	弹性伸缩的管理员权限	指定区域项目资源
网络域运维	VPC FullAccess	虚拟私有云的管理员权限	指定区域项目资源
	ELB FullAccess	弹性负载均衡的管理员权限	指定区域项目资源
数据库运维	RDS FullAccess	云数据库的管理员权限	指定区域项目资源
	DDS FullAccess	文档数据库服务的管理员权限	指定区域项目资源
	DDM FullAccess	分布式数据库中间件的管理员权限	指定区域项目资源
安全领域运维	Anti-DDoS Administrator	Anti-DDoS流量清洗服务的管理员权限	指定区域项目资源
	AAD Administrator	DDoS高防服务的管理员权限	指定区域项目资源
	WAF Administrator	Web应用防火墙的管理员权限	指定区域项目资源
	VSS Administrator	漏洞扫描服务的管理员权限	指定区域项目资源
	CGS Administrator	容器安全服务的管理员权限	指定区域项目资源
	KMS Administrator	数据加密服务的管理员权限	指定区域项目资源
	DBSS System Administrator	数据库安全服务的管理员权限	指定区域项目资源
	SES Administrator	安全专家服务的管理员权限	指定区域项目资源
	SC Administrator	SSL证书管理服务的管理员权限	指定区域项目资源

4.2 用户组添加/移除用户

管理员创建用户组并授权后，将用户加入用户组中，使用户具备用户组的权限，实现用户的授权。给已授权的用户组中添加或者移除用户，快速实现用户的权限变更。

用户组添加用户

步骤1 管理员在用户组列表中，单击新建的用户组，例如“开发人员组”，右侧的“用户组管理”。

图 4-4 用户组管理



步骤2 在“可选用户”中选择需要添加至用户组中的用户。

图 4-5 选择用户



步骤3 单击“确定”，完成用户授权。

----结束

用户组移除用户

步骤1 管理员在用户组列表中，单击新建的用户组，例如“开发人员组”，右侧的“用户组管理”。

图 4-6 用户组管理



步骤2 在“已选用户”中，单击用户名称右侧的删除图标，单击“确定”，完成移除用户。

图 4-7 移除用户组中的用户



----结束

4.3 删除用户组

操作步骤

当您需要删除用户组，请参考以下操作：

步骤1 进入IAM控制台，在左侧导航栏选择“用户组”页签。

步骤2 在用户组列表中，单击用户组右侧的“删除”。

图 4-8 删除用户组



步骤3 在弹窗中选择“是”，删除勾选的用户组。

----结束

批量删除用户组

当您需要一次性删除多个用户组时，请参考以下操作：

步骤1 进入IAM控制台，在左侧导航栏选择“用户组”页签。

步骤2 勾选需要删除的用户组，单击用户组列表上方的“删除”。

图 4-9 批量删除用户组



步骤3 在弹窗中，选择“是”，删除用户组。

----结束

4.4 查看或修改用户组

查看用户组信息

管理员在用户组列表中，单击用户组名称，可以查看用户组的基本信息、权限和包含用户。

图 4-10 查看用户组信息



修改用户组权限

您可以进入用户组详情，在“授权记录”页签查看或修改用户组已经拥有的权限。

说明

- 修改用户组权限，将影响该用户组中所有用户的权限，请谨慎操作。
 - 无法修改默认管理员用户组admin的权限。
1. 单击用户组的名称，例如“开发人员组”，进入用户组详情页面，在“授权记录”页签查看用户组已拥有的权限。
 2. 单击需要修改权限右侧的“删除”。

图 4-11 删除授权记录



3. 在确认弹窗中，单击“是”，删除当前授权。
4. 单击“授权记录”页签中的“授权”，进入给用户组授权页面。

图 4-12 给用户组授权



5. 在授权页面选择对应的权限、作用范围，单击“确定”，完成用户组权限修改。
6. 单击“返回”，跳转至“用户组>授权记录”页签，确认修改后的用户组权限。

图 4-13 单击返回



修改用户组名称和描述

管理员在用户组列表中，单击用户组右侧的“编辑”，修改用户组名称和描述。

图 4-14 修改用户组名称和描述



说明

如果该用户组名称已配置在身份提供商的身份转换规则中，修改用户组名称将导致对应身份转换规则失效，请谨慎操作。

修改用户组中的用户

步骤1 管理员在用户组列表中，单击用户组右侧的“用户组管理”。

图 4-15 修改用户组中的用户



步骤2 在“可选用户”中选择需要添加的用户。

步骤3 在“已选用户”中选择移除对应用户。

----结束

📖 说明

系统缺省用户组“admin”，只能修改其中包含的用户，不能修改描述信息与权限。

4.5 移除用户组权限

操作步骤

当您需要移除用户组中的某个权限，请参考以下操作：

步骤1 进入IAM控制台，在左侧导航栏选择“用户组”页签。

步骤2 单击用户组名称，进入用户组详情页面。

图 4-16 单击用户组名称



步骤3 在“授权记录”页签下，单击需要移除权限最右侧的“删除”。

图 4-17 移除策略



步骤4 在弹窗中，单击“是”，移除用户组权限。

----结束

批量移除用户组权限

当您需要移除用户组中多个权限，请参考以下操作：

步骤1 进入IAM控制台，在左侧导航栏选择“用户组”页签。

步骤2 单击用户组名称，进入用户组详情页面。

图 4-18 查看用户组



步骤3 在“授权记录”页签下，勾选需要移除的权限，单击权限列表上方的“删除”。

图 4-19 批量删除权限



步骤4 在弹窗中，单击“是”，移除用户组权限。

----结束

4.6 依赖角色的授权方法

由于华为云各服务之间存在业务交互关系，个别服务的角色依赖其他服务的角色实现功能。因此管理员在基于角色授权时，对于有依赖则需要授予依赖的角色才会生效。策略不存在依赖关系，不需要进行依赖授权。

操作步骤

- 步骤1** 管理员登录IAM控制台。
- 步骤2** 在用户组列表中，单击新建用户组右侧的“授权”。
- 步骤3** 在授权页面进行授权时，管理员在权限列表的搜索框中搜索需要的角色。
- 步骤4** 选择角色，系统将自动勾选依赖角色。

图 4-20 选择角色




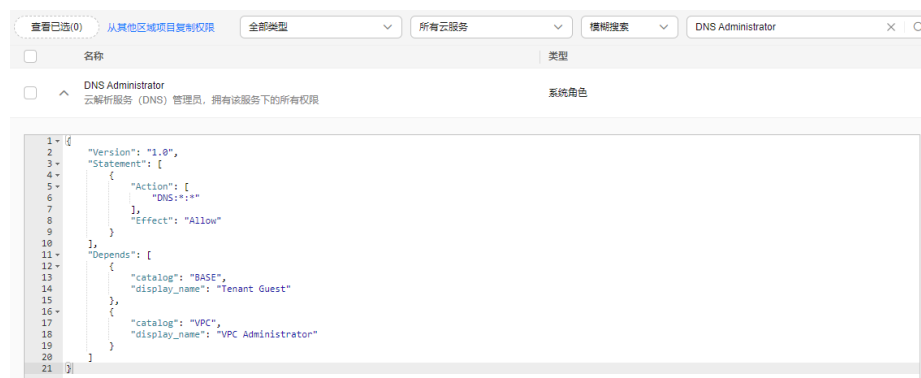
- 步骤5** 单击勾选权限下方的 ，查看角色的依赖关系。

图 4-21 查看角色的依赖关系



例如“DNS Administrator”，角色内容中存在“Depends”字段，表示存在依赖关系。给用户组授予“DNS Administrator”角色时，还需要在同项目同时授予“Tenant Guest”和“VPC Administrator”角色，“DNS Administrator”才能生效。

- 步骤6** 单击“确定”，完成依赖角色的授权。

----结束

5 权限管理

5.1 权限基本概念

权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

权限的分类

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](#)。

策略-系统策略

云服务在IAM预置了常用授权项，称为系统策略。管理员给用户组授权时，可以直接使用这些系统策略，系统策略只能使用，不能修改。[如需查看所有云服务的系统策略，请参见：系统权限。](#)

如果管理员在IAM控制台给用户组或者委托授权时，无法找到特定服务的系统策略，原因是该服务暂时不支持IAM，管理员可以通过[给对应云服务提交工单](#)，申请该服务在IAM预置权限。

策略-自定义策略

如果系统策略无法满足授权要求，管理员可以根据各服务支持的授权项，创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制，自定义策略是对系统策略的扩展和补充。目前IAM支持可视化视图、JSON视图两种自定义策略配置方式。

5.2 角色

角色是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。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。

由于华为云各服务之间存在业务依赖关系，因此给用户或用户组授予角色时，需要将依赖的其他角色一并授予该用户或用户组，保证权限生效。具体请参见：[依赖角色的授权方法](#)。

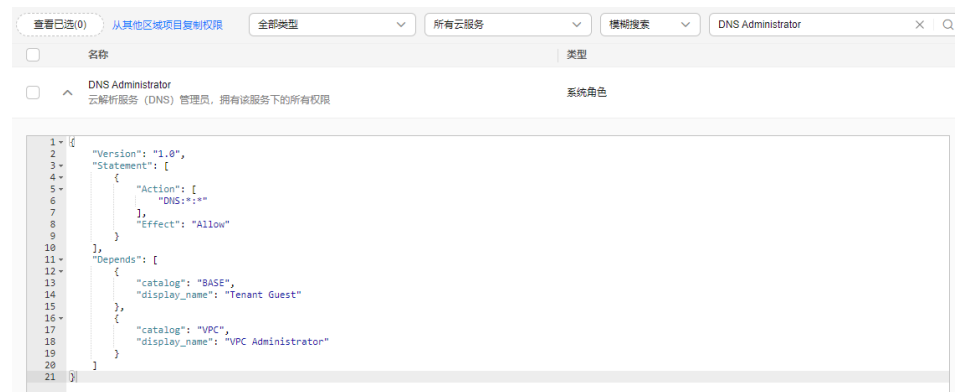
约束与限制

企业项目授权场景下不支持授予角色。

角色内容

给用户组选择角色时，单击角色前面的 \vee ，可以查看角色的详细内容，以“DNS Administrator”为例，说明角色的内容。

图 5-1 DNS Administrator 角色内容



```
{
  "Version": "1.0",
  "Statement": [
    {
      "Action": [
        "DNS:Zone:*",
        "DNS:RecordSet:*",
        "DNS:PTRRecord:*"
      ],
      "Effect": "Allow"
    }
  ],
  "Depends": [
    {
      "catalog": "BASE",
      "display_name": "Tenant Guest"
    }
  ],
}
```

```
{
  {
    "catalog": "VPC",
    "display_name": "VPC Administrator"
  }
}
```

参数说明

表 5-1 参数说明

参数		含义	值
Version		角色的版本	1.0: 代表基于角色的访问控制。
Statement: 角色的授权语句	Action: 授权项	操作权限	格式为: 服务名:资源类型:操作 "DNS:Zone:*": 表示对DNS的Zone所有操作。其中“DNS”为服务名;“Zone”为资源类型;“*”为通配符,表示对Zone资源类型可以执行所有操作。
	Effect: 作用	定义Action中的操作权限是否允许执行	<ul style="list-style-type: none"> Allow: 允许执行。 Deny: 不允许执行。 说明 当同一个Action的Effect既有Allow又有Deny时,遵循Deny优先的原则。
Depends: 角色的依赖关系	catalog	依赖的角色所属服务	服务名称。例如: BASE、VPC。
	display_name	依赖的角色名称	角色名称。 说明 给用户组授予示例的“DNS Administrator”角色时,必须同时勾选该角色依赖的角色“Tenant Guest”和“VPC Administrator”,“DNS Administrator”才会生效。 了解更多角色依赖关系,请参考: 系统权限 。

5.3 策略

5.3.1 策略内容

可以单击策略名称查看策略所包含的内容,从而进行选用策略。

查看策略内容

步骤1 在左侧导航栏选择“用户组”,单击需授权的用户组“操作”列下的“授权”。


步骤2 给用户组选择策略时,单击策略前面的 ,可以查看策略的详细内容,以系统策略“IAM ReadOnlyAccess”为例。

图 5-2 IAM ReadOnlyAccess 策略内容



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

----结束

5.3.2 策略语法

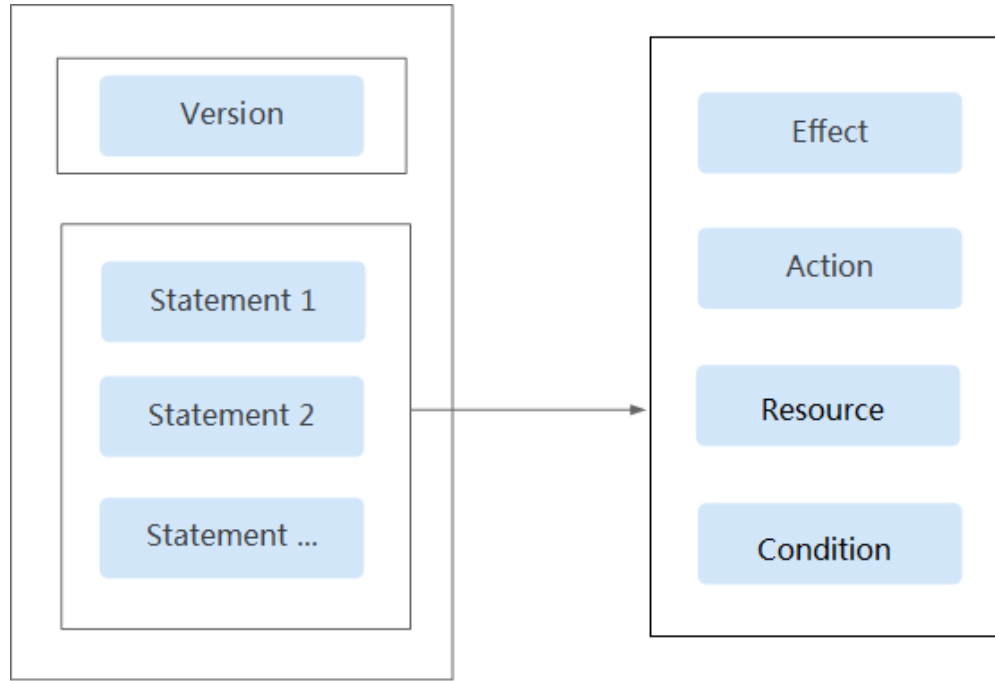
下面以OBS的自定义策略为例，说明策略的语法。

```
{  
  "Version": "1.1",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "obs:bucket:ListAllMyBuckets",  
        "obs:bucket:HeadBucket",  
        "obs:bucket:ListBucket",  
        "obs:bucket:GetBucketLocation"  
      ],  
      "Condition": {  
        "StringEndWithIfExists": {  
          "g:UserName": [  
            "specialCharacter"  
          ]  
        },  
        "Bool": {  
          "g:MFAPresent": [  
            "true"  
          ]  
        }  
      },  
      "Resource": [  
        "obs:*:bucket:*"  
      ]  
    }  
  ]  
}
```

策略结构

策略结构包括Version（策略版本号）和Statement（策略权限语句）两部分，其中Statement可以有多个，表示不同的授权项。

图 5-3 策略结构



策略参数

策略参数包含Version和Statement两部分，下面介绍策略参数详细说明。了解策略参数后，您可以根据场景自定义策略，如[自定义策略使用样例](#)。

表 5-2 策略参数说明

参数		含义	值
Version		策略的版本。	1.1：代表基于策略的访问控制。
Statement： 策略的授权语句	Effect：作用	定义Action中的操作权限是否允许执行。	<ul style="list-style-type: none">● Allow：允许执行。● Deny：不允许执行。 说明 当同一个Action的Effect既有Allow又有Deny时，遵循Deny优先的原则。

参数		含义	值
	Action: 授权项	操作权限。	<p>格式为“服务名:资源类型:操作”。授权项支持通配符号*, 通配符号*表示所有。授权项不区分大小写。</p> <p>示例:</p> <p>"obs:bucket:ListAllMybuckets": 表示查看OBS桶列表权限, 其中obs为服务名, bucket为资源类型, ListAllMybuckets为操作。</p> <p>您可以在对应服务“API参考”资料中查看该服务所有授权项, 如OBS授权项。</p>
	Condition: 条件	使策略生效的特定条件, 包括 条件键 和 运算符 。	<p>格式为“条件运算符:{条件键: [条件值1,条件值2]}”。其中, 条件键不区分大小写。</p> <p>如果您设置多个条件, 同时满足所有条件时, 该策略才生效。</p> <p>示例:</p> <p>"StringEndWithIfExists": { "g:UserName": ["specialCharacter"] }": 表示当用户输入的用户名以"specialCharacter"结尾时该条statement生效。</p>
	Resource: 资源类型	策略所作用的资源。	<p>格式为“服务名:region:domainId:资源类型:资源路径”, 资源类型支持通配符号*, 通配符号*表示所有。资源类型不区分大小写。</p> <p>支持资源粒度授权的云服务和资源类型参见: 支持IAM资源粒度授权的云服务。</p> <p>示例:</p> <ul style="list-style-type: none"> "obs:*:*:bucket:*": 表示所有的OBS桶。 "obs:*:*:object:my-bucket/my-object/*": 表示my-bucket桶my-object目录下的所有对象。

- **条件键**

条件键表示策略语句的 Condition 元素中的键值。根据适用范围, 分为全局条件键和服务条件键。

- 全局级条件键 (前缀为g:) 适用于所有操作, IAM提供两种全局条件键: **通用全局条件键**和**其他全局条件键**。
 - 通用全局条件键: 在鉴权过程中, 云服务不需要提供用户身份信息, IAM将自动获取并鉴权。详情请参见: [通用全局条件键](#)。

- 其他全局条件键：在鉴权过程中，IAM通过云服务获取条件信息并鉴权。仅部分已对接的云服务支持其他全局条件键。
- 服务级条件键（前缀为服务缩写，如obs:）仅适用于对应服务的操作，详情请参见对应云服务的用户指南，如[OBS请求条件](#)。

表 5-3 通用全局条件键

全局条件键	类型	说明
g:CurrentTime	时间	接收到鉴权请求的时间。以 ISO 8601 格式表示，例如：2012-11-11T23:59:59Z。示例参见 1 。
g:DomainName	字符串	请求者的账号名称。示例参见 2 。
g:MFAPresent	布尔值	是否使用MFA多因素认证方式获取Token。示例参见 3 。
g:MFAAge	数值	通过MFA多因素认证方式获取的Token的生效时长。该条件需要和g:MFAPresent一起使用。示例参见 4 。
g:PKITokenIssueTime	时间	PKI Token的签发时间。以ISO 8601格式表示，例如：2012-11-11T23:59:59Z。示例参见 5 。
g:ProjectName	字符串	项目名称。示例参见 6 。
g:UserId	字符串	IAM用户ID。示例参见 7 。
g:UserName	字符串	IAM用户名。示例参见 8 。

表 5-4 其他全局条件键

全局条件键	类型	说明
g:SourceIp	IP Address	请求用户的IP地址
g:SourceVpc	String	请求用户的VPC ID
g:SourceVpcEndpoint	String	请求用户的VPC Endpoint ID
g:TagKeys	String	资源标签键
g:ResourceTag/{TagKey}	String	资源标签键值

a. **g:CurrentTime**

示例：表示用户在北京时间2023年3月1日8点到北京时间2023年3月30日8点可以创建IAM委托。注意：策略中g:CurrentTime条件键值的时间格式为UTC时间。

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iam:roles:createRoles"],
    "Condition": {
      "DateGreaterThan": {
        "g:CurrentTime": ["2023-03-01T00:00:00Z"]
      },
      "DateLessThan": {
        "g:CurrentTime": ["2023-03-30T00:00:00Z"]
      }
    }
  ]
}
```

b. **g: DomainName**

示例：表示仅有用户zhangsan可以创建委托。

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iam:roles:createRoles"],
    "Condition": {
      "StringEquals": {
        "g:DomainName": ["zhangsan"]
      }
    }
  ]
}
```

c. **g:MFAPresent**

示例：表示请求者获取身份凭证时采用了MFA认证后才可以创建IAM委托。

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iam:roles:createRoles"],
    "Condition": {
      "Bool": {
        "g:MFAPresent": ["true"]
      }
    }
  ]
}
```

d. **g:MFAAge**

示例：表示请求者获取身份凭证时采用了MFA认证的时间必须大于900s才可以创建IAM委托。

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iam:roles:createRoles"],
    "Condition": {
      "NumberGreaterThanEquals": {
        "g:MFAAge": ["900"]
      }
    }
  ]
}
```

e. **g:PKITokenIssueTime**

示例：表示用户在北京时间2023年3月1日8点前请求签发的PKI Token可以创建IAM委托。

说明

策略中g:PKITokenIssueTime条件键值的时间格式为UTC时间。

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iam:roles:createRoles"],
    "Condition": {
      "DateLessThan": {
        "g:PKITokenIssueTime": ["2023-03-01T00:00:00Z"]
      }
    }
  }]
}
```

f. g:ProjectName

示例：表示请求者获取的凭证范围必须是在北京四时才可以创建IAM委托。

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iam:roles:createRoles"],
    "Condition": {
      "StringEquals": {
        "g:ProjectName": ["cn-north-4"]
      }
    }
  }]
}
```

g. g:UserId

示例：表示用户ID为xxxxxxxxxx...的用户才可以创建IAM委托。

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iam:roles:createRoles"],
    "Condition": {
      "StringEquals": {
        "g:UserId": ["xxxxxxxxxx..."]
      }
    }
  }]
}
```

h. g:UserName

示例：表示用户lisi才可以创建IAM委托。

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["iam:roles:createRoles"],
    "Condition": {
      "StringEquals": {
        "g:UserName": ["lisi"]
      }
    }
  }]
}
```

- 多值条件键

i. ForAllValues：测试请求集的每个成员的值是否为条件键集的子集。如果请求中的每个键值均与策略中的至少一个值匹配，则条件返回true。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ims:images:share"
      ],
      "Condition": {
        "ForAllValues:StringEquals": {
          "ims:TargetOrgPaths": [
            "orgPath1",
            "orgPath2",
            "orgPath3"
          ]
        }
      }
    }
  ]
}
```

此策略描述的是对于请求者发起共享的组织中所有组织路径必须是orgPath1、orgPath2或者orgPath3，那么允许共享。

假如请求者想共享镜像给组织路径orgPath1、orgPath3下的成员，策略匹配成功。

假如请求者想共享镜像给组织路径orgPath1、orgPath2、orgPath3、orgPath4下的成员，策略匹配失败。

- ii. ForAnyValue：测试请求值集的至少一个成员是否与条件键值集的至少一个成员匹配。如果请求中的任何一个键值与策略中的任何一个条件值匹配，则条件返回true。对于没有匹配的键或空数据集，条件返回false。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ims:images:share"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "ims:TargetOrgPaths": [
            "orgPath1",
            "orgPath2",
            "orgPath3"
          ]
        }
      }
    }
  ]
}
```

此策略描述的是对于请求者发起共享的组织中任一个组织路径是orgPath1、orgPath2或者orgPath3，那么允许共享。

假如请求者想共享镜像给组织路径orgPath1、orgPath4下的成员，策略匹配成功。

假如请求者想共享镜像给组织路径orgPath4、orgPath5下的成员，策略匹配失败。

条件键运算逻辑

图 5-4 条件键运算逻辑示意图



- a. 对于同一条件键的多个条件值，采用OR运算逻辑，即请求值按照条件运算符匹配到任意一个条件值则返回true。

须知

当运算符表示否定含义的时候（例如：StringNotEquals），则请求值按照条件运算符不能匹配到所有的条件值。

- b. 同一运算符下的不同条件键之间，采用AND运算逻辑。不同运算符之间，采用AND运算逻辑。

运算符

运算符与条件键、条件值一起构成完整的条件判断语句，当请求信息满足该条件时，策略才能生效。运算符可以增加后缀“IfExists”，表示对应请求值为空或满足条件的请求值均使策略生效，如“StringEqualsIfExists”表示请求值为空或请求值等于条件值均使策略生效。运算符为字符串型运算符，表格中如未增加说明，不区分大小写。

- String类型

表 5-5 String 类型运算符

类型	运算符	说明
String	StringEquals	请求值与任意一个条件值相同（区分大小写）。
	StringNotEquals	请求值与所有条件值都不同（区分大小写）。
	StringEqualsIgnoreCase	请求值与任意一个条件值相同。
	StringNotEqualsIgnoreCase	请求值与所有条件值都不同。

类型	运算符	说明
	StringMatch	请求值符合任意一个条件值的正则表达式（区分大小写，正则表达式仅支持*和?）。
	StringNotMatch	请求值不符合所有条件值的正则表达式（区分大小写，正则表达式仅支持*和?）。

示例：指定用户名为ZhangSan的请求者才能够获取对象内容、获取对象元数据。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "obs:object:GetObject"
      ],
      "Condition": {
        "StringEquals": {
          "g:DomainName": [
            "ZhangSan"
          ]
        }
      }
    }
  ]
}
```

- Number类型

表 5-6 Number 类型运算符

类型	运算符	说明
Number	NumberEquals	请求值等于任意一个条件值。
	NumberNotEquals	请求值不等于所有条件值。
	NumberLessThan	请求值小于任意一个条件值。
	NumberLessThanEquals	请求值小于或任意一个等于条件值。
	NumberGreaterThan	请求值大于任意一个条件值。
	NumberGreaterThanEquals	请求值大于或等于任意一个条件值。

示例：请求者一次最多可以在example_bucket桶中列出10个对象。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
```

```

    "Action": [
      "obs:bucket:ListBucket"
    ],
    "Resource": [
      "OBS:*:*:bucket:example_bucket"
    ],
    "Condition": {
      "NumberLessThanEquals": {
        "obs:max-keys": [
          "10"
        ]
      }
    }
  }
]

```

- Date类型

表 5-7 Date 类型运算符

类型	运算符	说明
Date	DateLessThan	请求值早于任意一个条件值。
	DateLessThanEquals	请求值早于或等于任意一个条件值。
	DateGreaterThan	请求值晚于任意一个条件值。
	DateGreaterThanEquals	请求值晚于或等于任意一个条件值。

示例：请求者只能在2022年8月1日前创建桶资源。

```

{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "obs:bucket:CreateBucket"
      ],
      "Condition": {
        "DateLessThan": {
          "g:CurrentTime": [
            "2022-08-01T00:00:00Z"
          ]
        }
      }
    }
  ]
}

```

- Bool类型

表 5-8 Bool 类型运算符

类型	运算符	说明
Bool	Bool	条件值可选值：true、false。请求值等于条件值。

示例：请求者必须使用开启了MFA认证的凭证才能修改指定永久访问密钥。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:credentials:updateCredential"
      ],
      "Condition": {
        "Bool": {
          "g:MFAPresent": [
            "true"
          ]
        }
      }
    }
  ]
}
```

- Null类型

表 5-9 Null 类型运算符

类型	运算符	说明
Null	Null	条件值可选值：true、false。条件值为true，要求请求值不存在或者值为null；条件值为false，要求请求值必须存在且值不为null。

示例：请求者的创建桶请求必须来源于VPC。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "obs:bucket:CreateBucket"
      ],
      "Condition": {
        "Null": {
          "obs:SourceVpc": [
            "false"
          ]
        }
      }
    }
  ]
}
```

- “IfExists” 运算符后缀

除Null运算符以外，您可以在任何条件运算符名称的末尾添加IfExists，例如：StringEqualsIfExists。如果请求的内容中存在条件键，则依照策略所述来进行匹配。如果该键不存在，则该条件元素的匹配结果将为true。

5.3.3 策略变量

策略变量简介

在创建自定义策略时，策略中Resource元素或Condition元素的值可以使用策略变量作为占位符。在策略实际鉴权的时候，这些占位符将会被自动替换成请求上下文中指定条件键的值。

策略变量语法与替换规则说明

策略变量结构支持使用\$前缀，后跟一对大括号{}。在大括号内，需要填入想要使用的请求上下文中的条件键的名称，例如\${g:UserName}。在实际策略鉴权的时候，\${g:UserName}将被自动替换为条件键g:UserName的值。

📖 说明

Condition条件值的变量可以填写在任意位置，Resource元素的变量只能填写在Resource以":"分隔的五段式中的最后一段，例如：OBS:*:*:bucket:\${g:UserName}。

如果指定条件键在请求上下文中不存在，或者指定条件键是多值条件键，那么将会替换失败，可能会导致整个语句无效。例如当且仅当访问身份是IAM用户时，请求中才会存在g:UserName。如果以其他身份访问，那么所有包含\${g:UserName}的资源条件和条件键都将视作不匹配。同理，对于多值条件键（指一个条件键对应多个值），即使它存在于请求上下文中，由于它是多值条件键，依然会被判定为替换失败，从而视作不匹配。

如果变量指定的条件键替换失败，您可以为它提供原定设置文本作为默认值。要向变量添加默认值，请用单引号'括起默认值，并用英文逗号和空格分隔条件键名称和默认值，例如\${key, 'default'}，表示当key不存在或者替换失败时，将\${key, 'default'}替换为文本串default。条件键名称不区分大小写，但是默认值区分大小写。此外，条件键名称与默认值引号前后的空格都会被忽略。例如\${ g:username , 'Default_User_Name' }表示如果访问身份是IAM用户，则替换成g:UserName的值，否则替换成文本串Default_User_Name。

对于策略变量中具有特殊含义的字符"\$"（策略变量标识符），如果您不想让这个字符表示特殊含义，请将它们改写为\${\$}；在策略变量默认值中，如果您想表达一个单引号字符（'），请使用一对连续的单引号（''）来表示。例如\${g:UserName, 'A single quote is ', two quotes are ''.'}，当使用默认值进行替换时，它将被替换成A single quote is ', two quotes are ''。

IAM只会进行一轮替换，这意味着即使替换完毕后包含新的策略变量结构，它仍然不会被替换。例如\${g:UserName, '\${g:UserName}'}，当使用默认值进行替换时，它将被替换成\${g:UserName}，不会继续迭代。

策略变量替换失败场景说明

在以下场景下将会出现策略变量替换失败的情况：

- 变量在上下文中不存在，替换失败，例如非IAM用户登录时：“\${g:UserName}”。
- 变量标识符不匹配，替换失败，例如：“\${foo}”、“\${foo, 'default'}”。
- 变量中默认值标识符不匹配，替换失败，例如：“\${key, value}”、“\${foo, 'default'}”、“\${foo, 'default'}”等。

- 变量为空，替换失败，例如"\${}"、"\${ }"、"\${ }"等。
- 变量不允许存在空格，如果变量中存在空格，替换失败，例如："\${g:user id}"等。
- 变量嵌套，替换失败，例如：\${var1\${var2}}。

策略变量使用示例

- 在资源中使用变量：
 - 该示例表示，如果以IAM用户身份登录，且IAM用户名是test_user_name的情况下（g:UserName获取到的值是test_user_name）对资源OBS:*:*:bucket:test_user_name（"*"代表通配表示任意多个字符）执行obs:bucket:CreateBucket的行为结果是Allow。

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "obs:bucket:CreateBucket"
    ],
    "Resource": [
      "OBS:*:*:bucket:${g:UserName}"
    ]
  }]
}
```

- 该示例表示，以IAM用户身份登录，且IAM用户名是test_user_name的情况下（g:UserName获取到的值是test_user_name）对资源OBS:*:*:bucket:prefix_test_user_name_suffix（"*"代表通配表示任意多个字符）执行obs:bucket:CreateBucket的行为结果是Allow。

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "obs:bucket:CreateBucket"
    ],
    "Resource": [
      "OBS:*:*:bucket:prefix_${g:UserName}_suffix"
    ]
  }]
}
```

- 在条件值中使用变量：

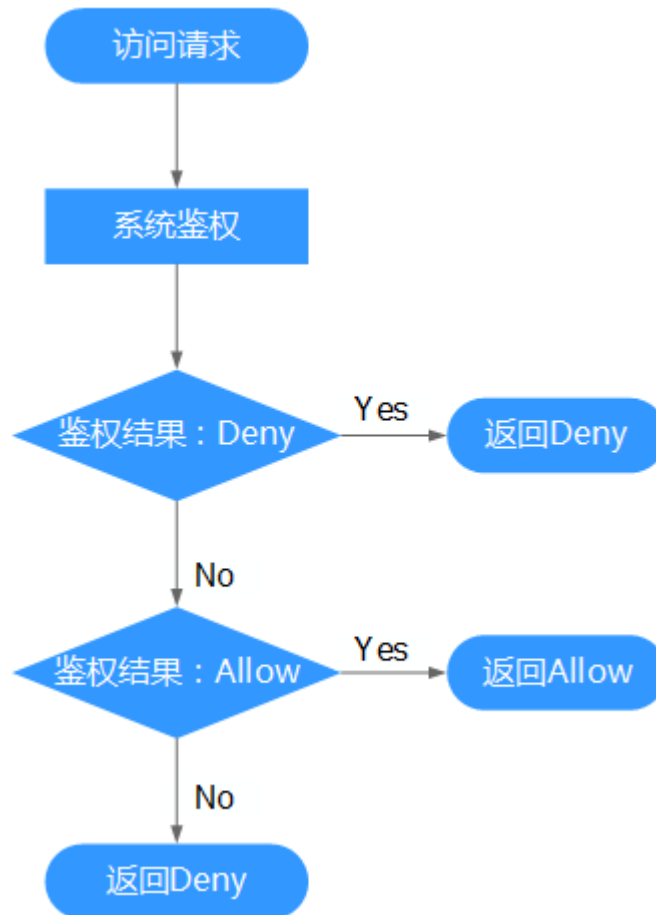
该示例表示，以IAM用户身份登录，且IAM用户名是test_user_name的情况下（g:UserName获取到的值是test_user_name）执行iam:agencies:getAgency的行为结果是Allow。

```
{
  "Version": "1.1",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:agencies:getAgency"
    ],
    "Condition": {
      "StringEquals": {
        "g:UserName": [
          "${g:UserName}"
        ]
      }
    }
  }]
}
```


5.3.4 策略鉴权规则

用户在发起访问请求时，系统根据用户被授予的访问策略中的action进行鉴权判断。鉴权规则如下：

图 5-5 系统鉴权逻辑图



1. 用户发起访问请求。
2. 系统在用户被授予的策略中寻找请求对应的action，优先寻找Deny指令。如果找到一个适用的Deny指令，系统将返回Deny决定。
3. 如果没有找到Deny指令，系统将寻找适用于请求的任何Allow指令。如果找到一个Allow指令，系统将返回Allow决定。
4. 如果找不到Allow指令，最终决定为Deny，鉴权结束。

5.4 系统策略更名详情

现对系统策略（即细粒度策略类型）名称进行调整，新的策略名称将于2020/2/6 22:30:00（北京时间）正式生效。本次调整仅涉及对系统策略名称的修改，不会影响您的业务，请放心使用。原始系统策略为Version 1.0，目标系统策略为Version 1.1，当前IAM兼容两个版本。

表 5-10 系统策略更名详情

服务	原始系统策略名称	目标系统策略名称
AOM	AOM Admin	AOM FullAccess
	AOM Viewer	AOM ReadOnlyAccess
APM	APM Admin	APM FullAccess
	APM Viewer	APM ReadOnlyAccess
Auto Scaling	AutoScaling Admin	AutoScaling FullAccess
	AutoScaling Viewer	AutoScaling ReadOnlyAccess
BMS	BMS Admin	BMS FullAccess
	BMS User	BMS CommonOperations
	BMS Viewer	BMS ReadOnlyAccess
BSS	EnterpriseProject_BSS_Administrator	EnterpriseProject BSS FullAccess
CBR	CBR Admin	CBR FullAccess
	CBR User	CBR BackupsAndVaultsFullAccess
	CBR Viewer	CBR ReadOnlyAccess
CCE	CCE Admin	CCE FullAccess
	CCE Viewer	CCE ReadOnlyAccess
CCI	CCI Admin	CCI FullAccess
	CCI Viewer	CCI ReadOnlyAccess
CDM	CDM Admin	CDM FullAccess
	CDM Operator	CDM FullAccessExceptUpdateEIP
	CDM Viewer	CDM ReadOnlyAccess
	CDM User	CDM CommonOperations
CDN	CDN Domain Configuration Operator	CDN DomainConfigureAccess
	CDN Domain Viewer	CDN DomainReadOnlyAccess

服务	原始系统策略名称	目标系统策略名称
	CDN Logs Viewer	CDN LogsReadOnlyAccess
	CDN Refresh And Preheat Operator	CDN RefreshAndPreheatAccess
	CDN Statistics Viewer	CDN StatisticsReadOnlyAccess
CES	CES Admin	CES FullAccess
	CES Viewer	CES ReadOnlyAccess
CS	CS Admin	CS FullAccess
	CS Viewer	CS ReadOnlyAccess
	CS User	CS CommonOperations
CSE	CSE Admin	CSE FullAccess
	CSE Viewer	CSE ReadOnlyAccess
DCS	DCS Admin	DCS FullAccess
	DCS Viewer	DCS ReadOnlyAccess
	DCS User	DCS UseAccess
DDM	DDM Admin	DDM FullAccess
	DDM Viewer	DDM ReadOnlyAccess
	DDM User	DDM CommonOperations
DDS	DDS Admin	DDS FullAccess
	DDS DBA	DDS ManageAccess
	DDS Viewer	DDS ReadOnlyAccess
DLF	DLF Admin	DLF FullAccess
	DLF Developer	DLF Development
	DLF Operator	DLF OperationAndMaintenanceAccess
	DLF Viewer	DLF ReadOnlyAccess
DMS	DMS Admin	DMS FullAccess
	DMS Viewer	DMS ReadOnlyAccess
	DMS User	DMS UseAccess

服务	原始系统策略名称	目标系统策略名称
DNS	DNS Admin	DNS FullAccess
	DNS Viewer	DNS ReadOnlyAccess
DSS	DSS Admin	DSS FullAccess
	DSS Viewer	DSS ReadOnlyAccess
DWS	DWS Admin	DWS FullAccess
	DWS Viewer	DWS ReadOnlyAccess
ECS	ECS Admin	ECS FullAccess
	ECS Viewer	ECS ReadOnlyAccess
	ECS User	ECS CommonOperations
ELB	ELB Admin	ELB FullAccess
	ELB Viewer	ELB ReadOnlyAccess
EPS	EPS Admin	EPS FullAccess
	EPS Viewer	EPS ReadOnlyAccess
EVS	EVS Admin	EVS FullAccess
	EVS Viewer	EVS ReadOnlyAccess
GES	GES Admin	GES FullAccess
	GES Viewer	GES ReadOnlyAccess
	GES User	GES Development
ICITY	iCity Admin	iCity FullAccess
	iCity Viewer	iCity ReadOnlyAccess
IMS	IMS Admin	IMS FullAccess
	IMS Viewer	IMS ReadOnlyAccess
Image Recognition	Image Recognition User	Image Recognition FullAccess
KMS	DEW Keypair Admin	DEW KeypairFullAccess
	DEW Keypair Viewer	DEW KeypairReadOnlyAccess
	KMS CMK Admin	KMS CMKFullAccess
LTS	LTS Admin	LTS FullAccess
	LTS Viewer	LTS ReadOnlyAccess

服务	原始系统策略名称	目标系统策略名称
MRS	MRS Admin	MRS FullAccess
	MRS Viewer	MRS ReadOnlyAccess
	MRS User	MRS CommonOperations
ModelArts	ModelArts Admin	ModelArts FullAccess
	ModelArts User	ModelArts CommonOperations
Moderation	Moderation User	Moderation FullAccess
NAT	NAT Admin	NAT FullAccess
	NAT Viewer	NAT ReadOnlyAccess
OBS	OBS Operator	OBS OperateAccess
	OBS Viewer	OBS ReadOnlyAccess
RDS	RDS Admin	RDS FullAccess
	RDS DBA	RDS ManageAccess
	RDS Viewer	RDS ReadOnlyAccess
RES	RES Admin	RES FullAccess
	RES Viewer	RES ReadOnlyAccess
ROMA Connect	ROMA Admin	ROMA FullAccess
	ROMA Viewer	ROMA ReadOnlyAccess
SCM	SCM Admin	SCM FullAccess
	SCM Viewer	SCM ReadOnlyAccess
	SCM Viewer	SCM ReadOnlyAccess
SFS	SFS Admin	SFS FullAccess
	SFS Viewer	SFS ReadOnlyAccess
SFS Turbo	SFS Turbo Administrator	SFS Turbo FullAccess
	SFS Turbo Viewer	SFS Turbo ReadOnlyAccess
ServiceStage	ServiceStage Admin	ServiceStage FullAccess
	ServiceStage Developer	ServiceStage Development
	ServiceStage Viewer	ServiceStage ReadOnlyAccess

服务	原始系统策略名称	目标系统策略名称
VPC	VPC Admin	VPC FullAccess
	VPC Viewer	VPC ReadOnlyAccess

5.5 查看授权记录

如果您需要查看当前账号下的所有授权关系，可以进入“权限管理>授权管理”页面。IAM权限管理为您呈现账号中的所有授权关系，支持使用“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。

- 如果您已开通并使用企业项目，可以选择IAM项目视图、企业项目视图，分别查看IAM项目、企业项目的授权关系。

图 5-6 已开通并使用企业项目



- 如果您暂未开通企业项目，将自动显示IAM项目视图。如需开通企业项目，请参见[开通企业项目](#)。

图 5-7 暂未开通企业项目



IAM 项目视图

在IAM项目视图下，您可以选择如下过滤条件查看对应授权记录。

- 策略名：**权限的名称。单击权限名称可以查看权限详情。
如需查看指定权限的授权记录，选择过滤条件为“策略名”，输入指定权限名称，查看该权限的授权记录。如需查看所有云服务的系统权限，请参见：[系统权限](#)。
- 用户名/用户组名/委托名：** IAM用户、用户组、委托的名称。
如需查看指定IAM用户/用户组/委托的IAM项目授权记录，选择过滤条件为“用户名”、“用户组名”或“委托名”，输入指定对应名称，查看其授权记录。

📖 说明

基于IAM项目授权，最小授权单位为用户组。查看IAM项目视图下指定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项目或区域名称，即权限的作用范围。查看IAM项目授权情况，请选择：
 - 全局服务：查看所有全局服务授权记录。
 - 所有项目：查看基于所有项目授权的授权记录。基于“所有项目”授权，权限对所有项目都生效，包括全局服务和所有项目（包括未来创建的项目）。
 - 指定项目（如“ap-southeast-1”）：查看基于默认区域、子项目授权的授权记录。
- **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，并输入企业名称，将自动切换至[企业项目视图](#)。

企业项目视图

在企业项目视图下，您可以选择如下过滤条件查看对应授权记录。

- **策略名**：权限的名称。单击权限名称可以查看权限详情。
如需查看指定权限的授权记录，选择过滤条件为“策略名”，输入指定权限名称，查看该权限的授权记录。如需查看企业项目支持的云服务权限，请参见：[云服务权限说明](#)。
- **用户名/用户组名/委托名**：IAM用户、用户组、委托的名称。
如需查看指定IAM用户/用户组的企业项目授权记录，选择过滤条件为“用户名”、“用户组名”，输入指定对应名称，查看其授权记录。

📖 说明

- 基于企业项目授权，最小授权单位为用户，查看企业项目视图下指定IAM用户授权记录时，显示该IAM用户及其所属用户组的授权记录。
- **企业项目**：企业项目的名称，即权限的作用范围。查看指定企业项目的授权记录，选择区域过滤条件为“企业项目”，输入企业名称，查看基于该企业项目的授权记录。
- **主体类型**：授权对象类型，可以选择用户、用户组、委托3种。
- **项目区域**：IAM项目或区域。如果您在企业项目视图下，选择“项目区域”为过滤条件，并选择指定项目，将自动切换至[IAM项目视图](#)。

5.6 自定义策略

5.6.1 创建自定义策略

如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制，自定义策略是对系统策略的扩展和补充。

目前IAM支持以下两种方式创建自定义策略：

- 可视化视图：通过可视化视图创建自定义策略，无需了解JSON语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图：通过JSON视图创建自定义策略，可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

本节为您介绍在“权限管理>权限”页面创建自定义策略。您还可以在授权过程中创建自定义策略，如图5-8所示，管理员无需取消正在进行的授权操作，创建自定义策略完成后可继续完成授权。

图 5-8 授权过程中创建策略



可视化视图配置自定义策略

步骤1 登录IAM控制台。

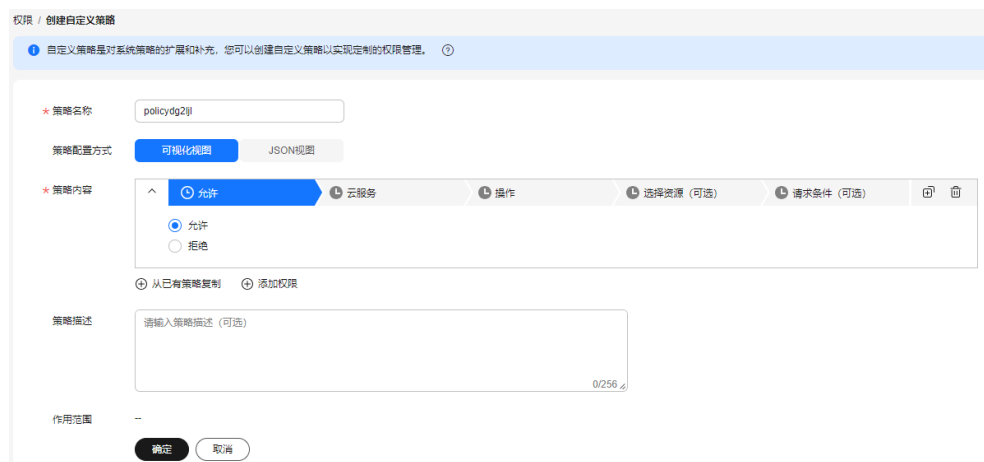
步骤2 在统一身份认证服务，左侧导航窗格中，选择“权限管理>权限”页签，单击右上方的“创建自定义策略”。

图 5-9 创建自定义策略



步骤3 输入“策略名称”。

图 5-10 输入策略名称



步骤4 “策略配置方式”选择“可视化视图”。

步骤5 在“策略内容”下配置策略。

1. 选择“允许”或“拒绝”。
2. 选择“云服务”。

说明

- 此处只能选择一个云服务，如需配置多个云服务的自定义策略，请在完成此条配置后，单击“添加权限”，创建多个服务的授权语句；或使用[JSON视图配置自定义策略](#)。
 - 暂不支持一个自定义策略同时包含全局级云服务和项目级云服务。如果需要同时设置全局级服务和项目级服务的自定义策略，请创建两条自定义策略，便于授权时设置最小授权范围。
3. 选择“操作”，根据需求勾选产品权限。
 4. （可选）选择资源类型，如选择“特定资源”可以单击“通过资源路径指定”来指定需要授权的资源。

支持为特定资源授权的云服务请参考：[支持IAM资源粒度授权的云服务](#)。

表 5-11 资源类型

类型	说明
特定资源	<p>授予IAM用户特定资源的相应权限。如授予IAM用户以TestBucket命名开头的桶相应权限，需将bucket设置为通过资源路径指定，添加资源路径：OBS:*:*:bucket:TestBucket*。</p> <p>说明</p> <ul style="list-style-type: none"> - 指定桶资源： 【格式】OBS:*:*:bucket:桶名称 对于桶资源，IAM自动生成资源路径前缀“obs:*:*:bucket:”。通过桶名称指定具体的资源路径，支持通配符*。例如：obs:*:*:bucket:*表示任意OBS桶。 - 指定对象资源： 【格式】OBS:*:*:object:桶名称/对象名称 对于对象资源，IAM自动生成资源路径前缀“obs:*:*:object:”。通过桶名称/对象名称指定具体的资源路径，支持通配符*。例如：obs:*:*:object:my-bucket/my-object/*表示my-bucket桶下my-object目录下的任意对象。
所有资源	授予IAM用户所有资源的相应权限。

5. （可选）添加条件，单击“添加条件”，选择“条件键”，选择“运算符”，根据运算符类型填写相应的值。

表 5-12 条件参数

参数名称	参数说明
条件键	条件键表示策略语句的Condition元素中的键值。分为全局条件键和服务级条件键。全局级条件键（前缀为g:）适用于所有操作，详情请参见： 全局级请求条件 ；服务级条件键（前缀为服务缩写，如obs:）仅适用于对应服务的操作，详情请参见对应云服务的用户指南，如 OBS请求条件 。条件键不区分大小写。

参数名称	参数说明
运算符	与条件键、条件值一起使用，构成完整的条件判断语句。
值	与条件键、运算符一起使用，当运算符需要某个关键字时，需要输入关键字的值，构成完整的条件判断语句。

图 5-11 添加请求条件

表 5-13 全局级请求条件

全局条件键	条件类型	说明
g:CurrentTime	时间	接收到鉴权请求的时间。以 ISO 8601 格式表示，例如：2012-11-11T23:59:59Z。
g:DomainName	字符串	账号名称。
g:MFAPresent	布尔值	是否使用MFA多因素认证方式获取Token。
g:MFAAge	数值	通过MFA多因素认证方式获取的Token的生效时长。该条件需要和g:MFAPresent一起使用。
g:ProjectName	字符串	项目名称。
g:UserId	字符串	IAM用户ID。
g:UserName	字符串	IAM用户名。

步骤6 (可选) 在“策略配置方式”选择JSON视图，将可视化视图配置的策略内容转换为JSON语句，您可以在JSON视图对策略内容进行修改。

说明

如果您修改后的JSON语句有语法错误，将无法创建策略，可以自行检查修改内容或单击界面弹窗中的“重置”，将JSON文件恢复到未修改状态。

- 步骤7** (可选) 如需创建多条自定义策略, 请单击“添加权限”; 也可在已创建的策略最右端单击“+”, 复制此权限。
- 步骤8** 输入“策略描述”(可选)。
- 步骤9** 单击“确定”, 自定义策略创建完成。
- 步骤10** 将新创建的自定义策略授予用户组, 使得用户组中的用户具备自定义策略中的权限。

说明

给用户组授予自定义策略与系统策略操作一致, 详情请参考: [创建用户组并授权](#)。

----结束

JSON 视图配置自定义策略

- 步骤1** 登录IAM控制台。
- 步骤2** 在统一身份认证服务, 左侧导航窗格中, 选择“权限管理>权限”页签, 单击右上方的“创建自定义策略”。

图 5-12 创建自定义策略



- 步骤3** 输入“策略名称”。

图 5-13 输入策略名称



步骤4 “策略配置方式”选择“JSON视图”。

步骤5 （可选）在“策略内容”区域，单击“从已有策略复制”，例如选择“EVS FullAccess”作为模板。

📖 说明

此处可以同时选择多个服务的策略，这些策略的作用范围必须一致，即都是全局级服务或者项目级服务。如果需要同时设置全局服务和项目级服务的自定义策略，请创建两条自定义策略，便于授权时设置最小授权范围。

步骤6 单击“确定”。

步骤7 修改模板中策略授权语句。

- 作用（Effect）：允许（Allow）和拒绝（Deny）。
- 权限集（Action）：写入各服务API授权项列表（如图5-14所示）中“授权项”中的内容，例如：“evs:volumes:create”，来实现细粒度授权。

图 5-14 授权项示例

权限	对应API接口	授权项
管理员查询IAM用户列表	GET /v3/users	iam:users:listUsers

📖 说明

- 自定义策略版本号（Version）固定为1.1，不可修改。
- 各服务支持的API授权列表，详情请参见：[系统权限](#)。

步骤8 （可选）输入“策略描述”。

步骤9 单击“确定”后，系统会自动校验语法，如跳转到策略列表，则自定义策略创建成功；如提示“策略内容错误”，请按照语法规则进行修改。

步骤10 将新创建的自定义策略授予用户组，使得用户组中的用户具备自定义策略中的权限。

📖 说明

给用户组授予自定义策略与系统策略操作一致，详情请参考：[创建用户组并授权](#)。

----结束

5.6.2 修改、删除自定义策略

本章为您介绍如何修改和删除已创建的自定义策略。

修改自定义策略

修改自定义策略名称、描述和内容。

1. 管理员在[IAM控制台](#)左侧导航窗格中，选择“权限管理>权限”页签。
2. 在指定策略的操作列中单击“编辑”，或者单击需要修改的策略名称，进入策略详情页。

图 5-15 修改自定义策略



3. 可根据需要修改“策略名称”和“策略描述”。
4. 按[可视化视图配置自定义策略](#)方式修改策略。
5. 单击“确定”完成修改。

删除自定义策略

说明

如果当前自定义策略已被授权给用户组或委托，则无法删除。移除该用户组或委托中的自定义策略后，才可删除自定义策略。

1. 管理员在IAM控制台左侧导航窗格中，选择“权限管理>权限”。
2. 在指定策略的操作列中单击“删除”。

图 5-16 删除自定义策略



3. 单击“确定”完成删除。

5.6.3 自定义策略使用样例

配合较高权限系统策略使用

如果您给IAM用户授予较高权限的系统策略，例如“FullAccess”，但不希望IAM用户拥有某个服务的权限，例如云审计服务。您可以创建一个自定义策略，并将自定义策略的Effect设置为Deny，然后将较高权限的系统策略和自定义策略同时授予用户，根据Deny优先原则，则授权的IAM用户除了云审计服务，可以对其他所有服务执行所有操作。

以下策略样例表示：拒绝IAM用户使用云审计服务。

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

说明

- Action为授权项，格式为：服务名:资源类型:操作。
"cts:*": 表示对云审计的所有操作。其中cts为服务名；“*”为通配符，表示对所有的资源类型可以执行所有操作。
- Effect为作用，Deny表示拒绝，Allow表示允许。

配合单个服务系统策略使用

- 如果您给IAM用户授予单个服务系统策略，例如“BMS FullAccess”，但不希望用户拥有BMS FullAccess中的创建裸金属服务器权限（bms:servers:create），可以创建一条相同Action的自定义策略，并将自定义策略的Effect设置为Deny，然后将系统策略BMS FullAccess和自定义策略同时授予用户，根据Deny优先原则，则用户可以对BMS执行除了创建裸金属服务器外的所有操作。

以下策略样例表示：拒绝IAM用户创建裸金属服务器。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "bms:servers:create"
      ]
    }
  ]
}
```

- 如果您给IAM用户授予“OBS ReadOnlyAccess”权限，但不希望部分用户查看指定OBS资源（例如，不希望用户名以“TestUser”开头的用户查看以“TestBucket”命名开头的桶），可以再创建一条自定义策略来指定特定的资源，并将自定义策略的Effect设置为Deny，然后将OBS ReadOnlyAccess和自定义策略同时授予用户。根据Deny优先原则，则用户可以对以“TestBucket”命名开头之外的桶进行查看操作。

以下策略样例表示：拒绝以TestUser命名开头的用户查看以TestBucket命名开头的桶。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "obs:bucket:ListAllMybuckets",
        "obs:bucket:HeadBucket",
        "obs:bucket:ListBucket",
        "obs:bucket:GetBucketLocation"
      ],
      "Resource": [
        "obs:*:bucket:TestBucket*"
      ],
      "Condition": {
        "StringStartWith": {
          "g:UserName": [
            "TestUser"
          ]
        }
      }
    }
  ]
}
```

说明

当前仅部分服务支持资源级授权，例如OBS 对象存储服务；对于不支持资源级别授权的服务，若自定义策略中含有资源类型，则无法创建成功。

完全使用自定义策略

您也可以不使用系统策略，只创建自定义策略，实现IAM用户的指定服务授权。

- 以下策略样例表示：仅允许IAM用户使用ECS、EVS、VPC、ELB、AOM

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:*",
        "evs:*",
        "vpc:*",
        "elb:*",
        "aom:*"
      ]
    }
  ]
}
```

- 以下策略样例表示：允许特定IAM用户（以TestUser命名开头）删除特定OBS对象（my-bucket桶my-object目录下的所有对象）。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "obs:object:DeleteObject"
      ],
      "Resource": [
        "obs:*:object:my-bucket/my-object/*"
      ],
      "Condition": {
        "StringStartsWith": {
          "g:UserName": [
            "TestUser"
          ]
        }
      }
    }
  ]
}
```

- 以下策略样例表示：允许IAM用户使用除了ECS、EVS、VPC、ELB、AOM、APM外的其他所有服务。

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "*"
      ]
    },
    {
      "Action": [
        "ecs:*",
        "evs:*",
        "vpc:*",
        "elb:*",
        "aom:*",
        "apm:*"
      ]
    }
  ]
}
```

```

    ],
    "Effect": "Deny"
  }
]
}

```

5.6.4 支持 IAM 资源粒度授权的云服务

如果您需要授予IAM用户特定资源的相应权限，可以[创建自定义策略](#)并选择特定资源，该IAM用户将仅拥有对应资源的使用权限。例如创建自定义策略时，选择资源类型并添加资源路径：OBS:*:*:bucket:TestBucket*，即可授予IAM用户以TestBucket命名开头的桶相应权限。

下表为当前华为云支持资源级别授权的云服务及对应资源类型。

表 5-14 支持资源粒度授权的云服务及其资源类型

服务	资源类型	资源名称
API开放平台SaaS (Apiexplorer-saas)	product	产品
	portal	门户
云堡垒机 (CBH)	instanceld	实例ID
云容器引擎 (CCE)	cluster	集群
云服务操作中心 (COC)	schedule	定时运维
	document	文档
	drillPlan	演练规划
	attackTask	攻击任务
	contingencyPlan	应急预案
	drillTask	演练任务
	accountBaseline	账号基线
	faultMode	故障模式
	drillRecord	演练记录
	job	任务
	slaTemplate	sla模板
	attackTargetRecord	攻击任务的攻击目标记录
	parameter	配置项
凭据管理服务 (CSMS)	secretName	凭据名称
智能数据洞察 (DataArtsInsight)	workspace	工作空间
分布式缓存服务 (DCS)	instance	实例
文档数据库服务 (DDS)	instanceName	实例名称

服务	资源类型	资源名称
数据湖探索 (DLI)	queue	队列
	database	数据库
	table	表
	column	列
	datasourceauth	安全认证信息
	jobs	作业
	resource	资源包
	elasticresourcepool	弹性资源池
	group	资源包组
	variable	全局变量
分布式消息服务 (DMS)	rabbitmq	RabbitMQ实例
	kafka	Kafka实例
	rocketmq	RocketMQ实例
数据仓库服务 (DWS)	cluster	集群
弹性云服务器 (ECS)	instance	弹性云服务器
云硬盘 (EVS)	volume	云硬盘
函数 workflow 服务 (FunctionGraph)	function	函数
	trigger	触发器
图引擎服务 (GES)	graphName	图名称
	backupName	备份名称
	metadataName	元数据名称
智能边缘平台 (IEF)	product	产品
	node	边缘节点
	group	边缘节点组
	deployment	应用部署
	batchjob	批量作业
	application	应用模板
	appVersion	应用模板版本
	IEFInstance	IEF实例
数据加密服务 (KMS)	KeyId	密钥ID

服务	资源类型	资源名称
MapReduce服务 (MRS)	cluster	集群
对象存储服务 (OBS)	bucket	桶
	object	对象
云数据库 (RDS)	instance	RDS实例
资源编排服务 (RFS)	privateModule	私有模块
	stack	堆栈
	stackSet	堆栈集
	privateTemplate	私有模板
	privateProvider	私有Provider
应用与数据集成平台 ROMA Connect	graph	业务流图ID
证书管理服务 (SCM)	cert	证书ID
安全云脑 (SecMaster)	alert	告警
	search	查询
	playbook	剧本
	workflow	流程
	subscription	订购
	indicator	威胁情报
	alertRule	告警模型
	connection	资产连接
	mapping	分类映射
	dataclass	数据类
	report	报告
	searchCondition	检索条件
	agency	委托
	resource	资源
	layout	布局
	dataobject	数据对象
	emergencyVulnerability	应急漏洞
workspace	工作空间	

服务	资源类型	资源名称
	metric	指标
	dataspace	数据空间
	catalogue	目录
	task	待办
	alertRuleTemplate	告警模板
	pipe	数据管道
	incident	事件
	table	表
	vulnerability	漏洞
容器镜像服务（SWR）	chart	Chart
	repository	仓库
	instance	企业版实例
虚拟私有云（VPC）	publicip	弹性公网IP

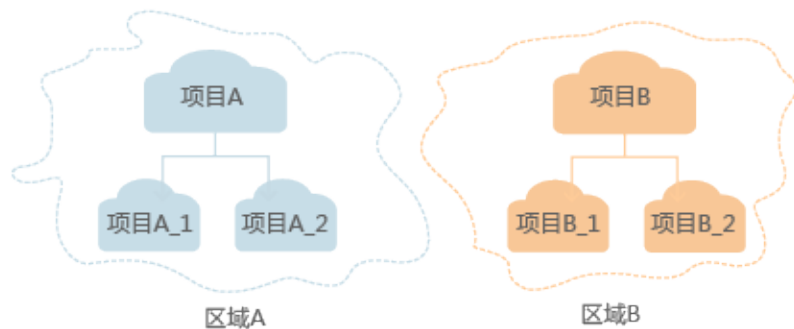
6 项目

华为云的每个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），以区域默认单位为项目进行授权，IAM用户可以访问您账号中该区域的所有资源。预置项目不支持删除。

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，使得资源的权限控制更加精确。

本章描述的IAM项目与企业项目不同，具体内容请参见：[IAM项目和企业项目的区别](#)。

图 6-1 项目隔离模型



说明

- IAM项目中的资源不能转移。
- 如果您已开通企业项目，将不支持创建IAM项目。

创建项目

步骤1 在IAM控制台的左侧导航窗格中，选择“项目”页签，单击“创建项目”。

图 6-2 创建项目



步骤2 在“所属区域”下拉列表中选择需要创建子项目的区域。

步骤3 输入“项目名称”。

说明

- 项目名称的格式为：区域默认项目名称_子项目名称，区域默认项目名称不允许修改。
- 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4 （可选）输入“描述”。

步骤5 单击“确定”，项目列表中显示新创建的项目。

----结束

基于项目给用户组授权

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，使得资源的权限控制更加精确。

步骤1 在用户组列表中，单击用户组右侧的“授权”，进入授权页面。

图 6-3 权限配置



步骤2 在授权页面中，勾选需要授予用户组的区域级项目权限，并单击“下一步”。

步骤3 选择作用范围。此处选择区域项目，则还需要选择待授权的项目。

步骤4 单击“确定”，完成授权。

说明

更多有关用户组授权的内容，请参见[创建用户组并授权](#)。

----结束

切换项目或区域

登录后需要先切换区域或项目，才能访问并使用授权的云服务，否则系统将提示没有权限。全局区域服务无需切换。

步骤1 登录华为云控制台。

步骤2 进入具体的云服务页面，若云服务为项目级服务，则单击页面左上角下拉框，选择区域。

----**结束**

7 委托

7.1 委托其他账号管理资源

7.1.1 基本流程

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。

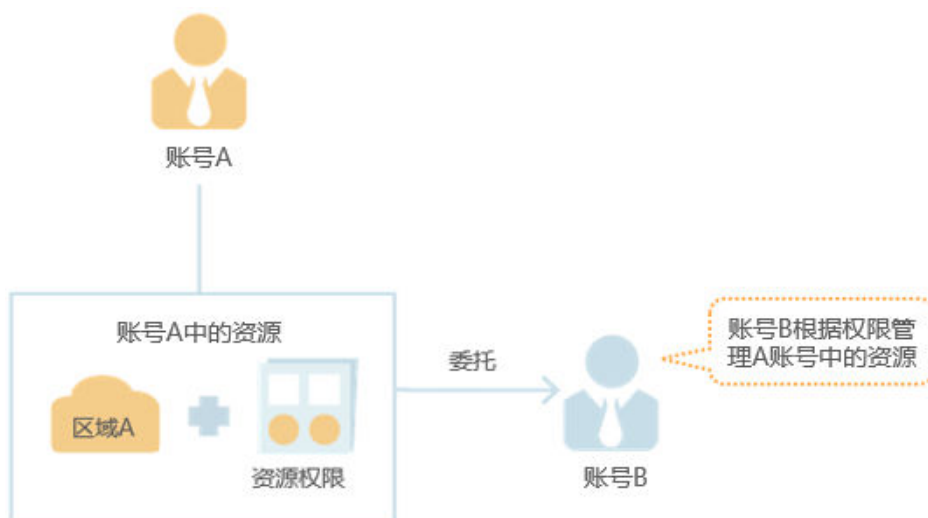
说明

只能对账号进行委托，不能对IAM用户进行委托。

如下以A账号委托B账号管理资源为例，讲述委托的原理及方法。A账号为委托方，B账号为被委托方。

步骤1 账号A创建委托。

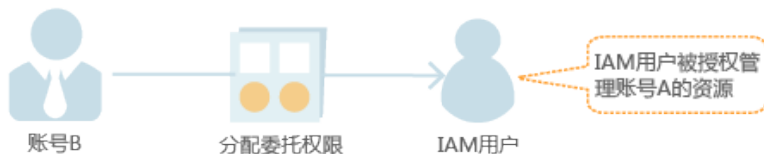
图 7-1 账号 A 创建委托



步骤2 （可选）账号B分配委托权限。

1. 创建用户组并授予用户组管理委托的权限。
2. 创建用户并将用户加入到用户组中。

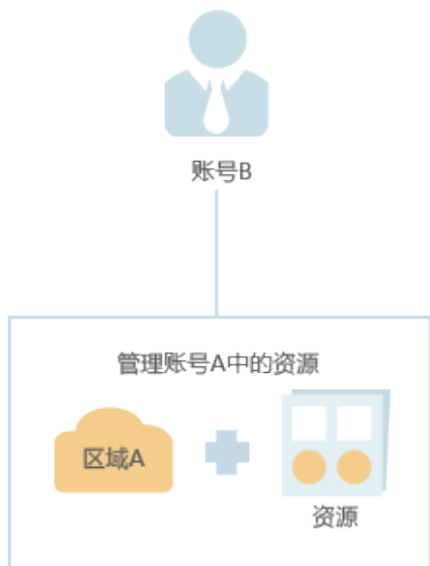
图 7-2 账号 B 分配委托权限



步骤3 账号B或者IAM用户管理委托资源。

1. 被委托方登录自己的账号，切换角色到账号A。
2. 切换到被授权的区域A，管理账号A的资源。

图 7-3 账号 B 切换角色



----结束

7.1.2 创建委托（委托方操作）

通过创建委托，可以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资源。被委托方使用自己的账号登录后，切换到委托方账号，即可管理委托方委托的资源，避免委托方共享自己的安全凭证（密码/密钥）给他人，确保账号安全。

前提条件

在创建委托前，建议管理员提前了解并规划以下内容：

- 了解权限的**基本概念及分类**。
- 规划委托需要的**系统权限**，并确认权限是否有依赖，如果有，需要同时**设置依赖的权限**。

操作步骤

步骤1 登录IAM控制台。

步骤2 在统一身份认证服务的左侧导航窗格中，选择“委托”页签，单击右上方的“创建委托”。

图 7-4 创建委托



步骤3 在创建委托页面，设置“委托名称”。

图 7-5 委托名称



步骤4 “委托类型”选择“普通账号”，在“委托的账号”中输入需要建立委托关系的其他账号的账号名。

说明

- 普通账号：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。委托的账号只能是账号，不能是联邦用户、IAM用户。
- 云服务：授权指定云服务使用其他云服务。详情请参见：[委托其他云服务管理资源](#)。

步骤5 选择“持续时间”，填写“描述”信息。

步骤6 单击“完成”。

如您不需要给委托授权，在授权的确认弹窗中单击“取消”，可以直接返回委托列表进行查看创建成功的委托。此时的委托将不包含任何权限。

步骤7 在授权的确认弹窗中，单击“立即授权”。

步骤8 勾选需要授予委托的权限，单击“下一步”，选择权限的作用范围。

说明

- 给委托授权即给其他账号授权，给用户组授权即给账号中的IAM用户授权，两者操作方法相同，仅可选的权限个数不同，授权操作请参见：[给用户组授权](#)。
- 当前委托支持添加Security Administrator权限，但为了保障您的账号安全，建议您按照业务场景为委托授予最小权限。

步骤9 单击“确定”，委托创建完成。

说明

委托方操作完成，将自己的账号名称、创建的委托名称、委托ID以及委托的资源权限告知被委托方后，被委托方可以通过切换角色至委托方号中管理委托资源。

---结束

7.1.3（可选）分配委托权限（被委托方操作）

当其他账号与您创建了委托关系，即您是被委托方，默认情况下只有较大权限的用户（账号本身以及admin用户组中的成员）可以管理委托资源，如果您需要普通IAM用户帮助您管理委托，可以将管理委托的权限分配给IAM用户。

如果您有多个委托关系，可以授予IAM用户较大的委托权限，即管理所有的委托，也可以授予IAM用户精细的权限，仅管理指定的委托，即IAM用户进行角色切换时，仅能切换到被授权的委托中，不能切换其他委托，您可以创建细粒度的委托权限，授权IAM用户管理指定的委托。

前提条件

- 已有其他账号与您创建了委托关系。
- 您已经获取到委托方的账号名称、所创建的委托名称以及委托ID。

操作步骤

步骤1 创建用户组并授权。

1. 在用户组界面，单击“创建用户组”。
2. 输入“用户组名称”。
3. 单击“确定”，用户组创建完成。
4. 单击新建用户组右侧的“授权”。
5. 创建自定义策略。

说明

如果需要授予IAM用户精细的委托权限，仅管理指定的委托，请执行以下步骤创建细粒度的委托权限。如果不需要进行精细的委托授权，授予IAM用户管理所有的委托权限，请跳过该步骤，直接执行**f**。

- a. 在选择策略页面，单击权限列表右上角“新建策略”。
- b. 输入“策略名称”。
- c. “策略配置方式”选择“JSON视图”。
- d. 在“策略内容”区域，填入以下内容：

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

📖 说明

- "b36b1258b5dc41a4aa8255508xxx..."需要替换为待授权委托的ID，需要提前向委托方获取，其他内容不需修改，直接拷贝即可。
 - 本文简要讲述快速完成委托细粒度授权的必要操作，更多权限内容，详情请参考[权限管理](#)。
- e. 单击“下一步”，继续完成授权。
6. 选择上一步创建的自定义策略或者“Agent Operator”权限，单击“下一步”。
 - 自定义策略：用户仅能管理指定ID的委托，不能管理其他委托。
 - “Agent Operator”权限：用户可以管理所有委托。
 7. 选择授权范围方案。
 8. 单击“确定”，用户组授权完成。

步骤2 创建IAM用户并加入用户组。

1. 在用户界面，单击“创建用户”。
2. 在创建用户界面，输入用户信息。
3. “访问方式”选择“管理控制台访问”中的“首次登录时设置”。
4. “登录保护”选择“开启”，并选择身份验证方式，单击“下一步”。
5. 在“可选用户组”中，选择[步骤1](#)中新创建的用户组，单击“创建用户”。
6. 完成IAM用户创建。

📖 说明

分配委托权限操作完成，新创建的IAM用户可以通过切换角色至委托方账号中，帮助您管理委托资源。

---结束

后续操作

被委托方账号或分配了委托权限的IAM用户均可以[切换角色](#)至委托方账号中，查看并根据权限使用委托资源。

7.1.4 切换角色（被委托方操作）

当其他账号与您创建了委托关系，即您是被委托方，您已经分配了委托权限的用户，可以切换角色至委托方账号中，根据权限管理委托方的资源。

前提条件

- 已有账号与您创建了委托关系。
- 您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 使用账号或者“分配委托权限”步骤中新建的用户登录华为云。

📖 说明

“分配委托权限”步骤中新建的用户具有管理委托的权限，可以切换角色。

步骤2 鼠标移动至右上方的用户名，选择“切换角色”。

图 7-6 切换角色



步骤3 在“切换角色”页面中，输入委托方的账号名称。

图 7-7 输入委托方的账号名称、委托名称



说明

输入账号名称后，系统将会按照顺序自动匹配委托名称，如果自动匹配的是没有授权的委托，系统将提示您没有权限访问，您可以删除委托名称，在下拉框中选择已授权的委托名称。

步骤4 单击“确定”，切换至委托方账号中。

----结束

后续步骤

鼠标移动至右上角的用户名，选择“切换角色”，可以返回到您自己的账号中。

7.2 委托其他云服务管理资源

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。

当前IAM提供两种创建委托方式：

1. 在IAM控制台创建云服务委托

以图引擎服务 GES为例：将操作权限委托给GES，允许GES以您的身份使用其他服务，例如发生故障转移时，GES使用这个委托将您的弹性IP绑定到主GES负载均衡实例。

图 7-8 云服务委托



2. 在云服务控制台使用某项资源时，系统提示您自动创建委托，以完成云服务间的协同工作。

以创建弹性文件服务SFS委托为例：

- 在SFS控制台创建文件系统。
- 在创建文件系统页面，开启“静态数据加密”。
- 弹窗提示需要创建SFS委托，单击“确定”，系统自动为您在当前项目创建SFS委托，并授予KMS CMKFullAccess权限，授权成功后，SFS可以获取KMS密钥用来加解密文件系统。
- 您可以在IAM控制台的委托列表中查看已创建的委托。

在 IAM 控制台创建云服务委托

步骤1 登录IAM控制台。

步骤2 在统一身份认证服务的左侧导航窗格中，选择“委托”页签，单击“创建委托”。

步骤3 在创建委托页面，设置“委托名称”。

图 7-9 云服务委托名称

* 委托名称

* 委托类型 普通账号
将账号内资源的操作权限委托给其他华为云账号。
 云服务
将账号内资源的操作权限委托给华为云服务。

* 云服务

* 持续时间

描述

0/255

步骤4 “委托类型”选择“云服务”，在“云服务”中选择需要授权的云服务。

步骤5 选择“持续时间”。

步骤6 （可选）填写“委托描述”。建议填写描述信息。

步骤7 单击“完成”。

如您不需要给委托授权，在授权的确认弹窗中单击“取消”，可以直接返回委托列表进行查看创建成功的委托。此时的委托将不包含任何权限。

步骤8 在授权的确认弹窗中，单击“立即授权”。

步骤9 勾选需要授予委托的权限，单击“下一步”，选择权限的作用范围，给委托授权。

步骤10 单击“确定”，委托创建完成。

----结束

7.3 删除或修改委托

修改委托

如果需要修改委托的权限、持续时间、描述等，可以在委托列表中，单击委托右侧的“修改”，修改委托。

图 7-10 修改委托



说明

- 云服务委托支持修改云服务、持续时间、描述、权限，委托名称、类型不支持修改。
- 修改云服务委托权限后可能会影响该云服务部分功能的使用，请谨慎操作。

删除委托

如果不再需要使用委托，可以在委托列表中，单击委托右侧的“删除”，删除委托。

图 7-11 删除单个委托



批量删除委托

如果需要删除多个委托，可在委托列表中勾选需要删除的委托，然后单击列表上方的“删除”。

图 7-12 批量删除委托



说明

删除委托后，将撤销被委托方账号的权限，被委托方将无法管理您的委托资源，对您的其他业务合作伙伴没有影响。

8 安全设置

8.1 安全设置概述

当您需要对账号的安全信息进行设置时，可以通过“安全设置”进行操作。“安全设置”包括“[基本信息](#)”、“[敏感操作](#)”、“[登录验证策略](#)”、“[密码策略](#)”、“[访问控制](#)”。本章为您介绍“安全设置”的使用对象和如何进入“安全设置”。

使用对象

表 使用对象为安全设置中不同页签下对应的不同使用对象。

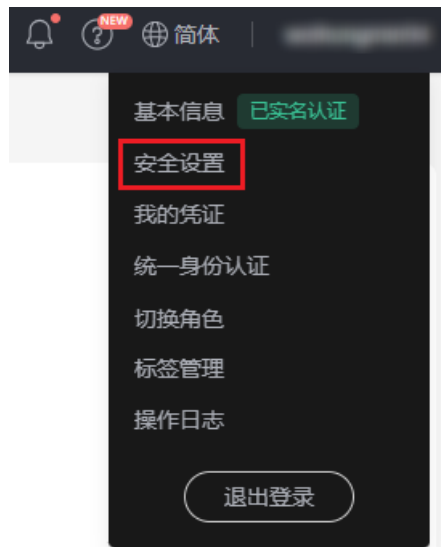
表 8-1 使用对象

功能	使用对象
基本信息	所有IAM用户可以修改，华为云账号请参考 基本信息管理 。
敏感操作	管理员 可以修改，普通IAM用户不可查看。
登录验证策略	管理员 可以修改，普通IAM用户仅可查看。
密码策略	管理员 可以修改，普通IAM用户仅可查看。
访问控制	管理员 可以修改，普通IAM用户不可查看。

如何进入安全设置

- 所有用户均可通过控制台入口进入“安全设置”。
 - a. 登录华为云，在右上角单击“控制台”。
 - b. 在“控制台”页面，鼠标移动至右上方的用户名，在下拉列表中选择“安全设置”。

图 8-1 进入安全设置



- **管理员**可通过IAM控制台进入“安全设置”。
 - a. 登录华为云，在右上角单击“控制台”。
 - b. 在控制台页面，鼠标移动至右上方的用户名，在下拉列表中选择“统一身份认证”。

图 8-2 进入统一身份认证服务



- c. 进入IAM控制台，在左侧导航栏中，选择“安全设置”页签，进入“安全设置”。

8.2 基本信息

本页面的所有操作允许账号和IAM用户修改。账号也可以参考[基本信息管理](#)修改登录密码、关联手机号、绑定邮件地址。

📖 说明

- 手机号和邮件地址只能绑定一个用户（IAM用户或账号），不可重复绑定。
- 一个用户（IAM用户或账号）仅能绑定一个手机、邮件地址、虚拟MFA设备，即为敏感操作进行二次验证的设备。

登录密码、关联手机号、绑定邮件地址

修改登录密码、关联手机号、绑定邮件地址类似，以修改密码为例。

步骤1 进入安全设置。

步骤2 在“安全设置”页面中，选择“基本信息”页签，单击“登录密码”右侧的“立即修改”，进入“修改密码”页面。

图 8-3 修改密码



步骤3 （可选）选择身份验证方式，获取并输入验证码。

📖 说明

如果邮件地址和手机都未绑定，则无需验证。

步骤4 输入原密码、新密码并确认密码。

📖 说明

- 密码不能是用户名或者用户名的倒序，例如：用户名为A12345，则密码不能为A12345、a12345、54321A和54321a。
- 密码的强弱程度，例如密码的最小长度等，可以由管理员在**密码策略**中进行设置。

步骤5 单击“确定”，完成密码修改。

----结束

8.3 敏感操作

只有**管理员**可以设置敏感操作，普通IAM用户只有查看权限，不能对其进行设置，如需修改，请联系管理员为您操作或添加权限。

📖 说明

联邦用户在执行敏感操作时，不需要进行身份验证。

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，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。

本节以“华为云App”为例介绍如何绑定虚拟MFA，如果您已安装其他MFA应用程序，请根据应用程序指引添加用户。如需了解有关解绑虚拟MFA、重置虚拟MFA的操作，请参见：[虚拟MFA](#)。

[暂未升级华为账号](#)、[已升级华为账号](#)绑定虚拟MFA的操作方法不同。

📖 说明

您需要先在智能设备上安装一个MFA应用程序（例如：“华为云”手机应用程序），才能绑定虚拟MFA设备。

- [暂未升级华为账号](#)

步骤1 [进入安全设置](#)。

步骤2 在“安全设置>敏感操作”页面，单击“虚拟MFA”右侧的“前往绑定”。

图 8-4 虚拟 MFA



步骤3 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。

您可以通过扫描二维码、手动输入两种方式绑定MFA设备：

- **扫描二维码**
打开手机已安装好的MFA应用程序，选择“扫描条形码”，扫描“绑定虚拟MFA”弹窗中的二维码。扫描成功后，应用程序会自动添加用户。
- **手动输入**
打开手机已安装好的MFA应用程序，选择“输入提供的密钥”，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4 添加用户完成，在返回MFA应用程序首页，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。

步骤5 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**

- [已升级华为账号](#)

步骤1 [进入安全设置](#)。

步骤2 在“安全设置>敏感操作”页面，单击“虚拟MFA”右侧的“前往绑定”。

图 8-5 绑定虚拟 MFA



步骤3 跳转至“华为账号>安全验证”页面，根据提示绑定虚拟MFA。


----结束

登录保护

开启登录保护后，您或账号中的IAM用户在登录华为云时，除了在登录页面输入用户名和密码外（第一次身份验证），还需要在登录验证页面输入验证码（第二次身份验证），该功能是一种安全实践，**建议开启登录保护**，多次身份认证可以提高账号安全性。

账号只能自己开启登录保护，账号或管理员都可以为IAM用户开启登录保护。

- **管理员为IAM用户开启登录保护**

管理员在IAM用户列表中，单击操作列的“安全设置”，单击“登录保护>验证方式”右侧的“”，选择验证方式为手机、邮件地址或虚拟MFA，为IAM用户开启登录保护。

说明

登录保护仅影响使用管理控制台访问华为云的IAM用户，对编程访问用户无影响。

- **未升级华为账号的华为云账号开启登录保护**

如果您的华为云账号暂未升级华为账号，**进入安全设置**后，账号可以在“安全设置 > 敏感操作 > 登录保护”中单击“立即设置”，选择“开启”，并设置验证方式，开启登录保护。

图 8-6 开启登录保护



- **华为账号开启登录保护**

如果您的华为云账号已升级为华为账号，将不支持在“安全设置”页面开启登录保护，请在“**华为账号中心**>账号与安全>安全验证>双重验证”中单击“开启”，输入验证信息，开启登录保护。

图 8-7 华为账号开启登录保护



系统会对华为账号登录进行安全认证，如果您更换终端，初次登录将进行安全认证(安全手机二次验证)。如果您没有开启“双重验证”，初次登录完成后，单击“信任”，将终端添加到信任列表中，后续将无需二次认证。

操作保护

- 开启操作保护

开启后，账号以及账号中的IAM用户进行敏感操作时，例如删除弹性云服务器资源，需要输入验证码进行验证，避免误操作带来的风险和损失。“操作保护”默认为开启状态，为了您的资源安全，建议保持开启状态。

开启操作保护后，默认在敏感操作验证成功后的15分钟之内，进行敏感操作无需再次验证。

步骤1 管理员[进入安全设置](#)。

步骤2 在“敏感操作 > 操作保护 > ”中，单击“立即启用”。

图 8-8 开启操作保护



步骤3 在右侧弹窗中选择“开启”，勾选“操作员验证”或“指定人员验证”。

如选择“指定人员验证”，开启操作保护时，需要进行初次身份核验，确保指定人员验证方式可用。

图 8-9 操作保护设置



- 操作保护 开启
执行敏感操作时，需要再次进行身份验证，请选择操作保护的验证方式。
- 操作员验证 指定人员验证
- 关闭
执行敏感操作时，无需进行身份验证。

- 操作员验证：触发敏感操作的账号或IAM用户进行二次验证。
- 指定人员验证：账号及IAM用户触发的敏感操作均由指定人员进行验证。支持手机号、邮件地址，不支持虚拟MFA验证。

步骤4 单击“确定”开启操作保护。

----结束

- **关闭操作保护**

关闭后，账号以及账号中的IAM用户进行**敏感操作**时，不需要输入验证码进行验证。

步骤1 管理员**进入安全设置**。

步骤2 管理员在“敏感操作>操作保护>”中，单击“立即修改”。

图 8-10 单击立即修改



步骤3 在右侧弹窗中选择“关闭”，并单击“确定”。

图 8-11 关闭操作保护



- 操作保护 开启
执行敏感操作时，需要再次进行身份验证，请选择操作保护的验证方式。
- 关闭
执行敏感操作时，无需进行身份验证。

步骤4 在“身份验证”弹窗中输入验证码。

- 操作员验证：关闭操作保护管理员本人进行二次验证。支持手机号、邮件地址、虚拟MFA。
- 指定人员验证：由指定人员进行验证。支持手机号、邮件地址，不支持虚拟MFA验证。

步骤5 单击“确定”，关闭操作保护。


----结束

📖 说明

- 敏感操作由各个云服务单独定义。
- 用户如果进行敏感操作，将进入“操作保护”页面，选择认证方式，包括邮件地址、手机和虚拟MFA三种认证方式。
 - 如果用户只绑定了手机号，则认证方式只能选择手机。
 - 如果用户只绑定了邮件地址，则认证方式只能选择邮件地址。
 - 如果用户未绑定邮件地址、手机和虚拟MFA，进行敏感操作时，将提示用户绑定邮件地址、手机或虚拟MFA。
- 使用邮件地址、手机进行认证可能出现收不到验证码故障，建议您使用MFA验证方式。
- 如需修改验证手机号、邮件地址，请在[账号中心](#)修改；如需修改虚拟MFA设备，请在[虚拟MFA](#)中修改。
- 开启操作保护后，执行敏感操作时，需要输入验证码进行验证，此验证码将会发送至进行操作的IAM用户所绑定的手机号或邮件地址，而不是该IAM用户所属的账号。


访问密钥保护

- **开启访问密钥保护**
开启后，仅管理员才可以创建、启用/停用或删除IAM用户的访问密钥。由于“访问密钥保护”默认为关闭状态，为了保障资源安全，建议开启访问密钥保护功能。

管理员[进入安全设置](#)后，在“敏感操作>访问密钥保护>”中，单击“”，开启访问密钥保护。

- **关闭访问密钥保护**

关闭后，所有IAM用户可以创建、启用/停用或删除自己的访问密钥。

管理员[进入安全设置](#)后，在“敏感操作>访问密钥保护”中，单击“”，关闭访问密钥保护。

自主管理用户属性

- **开启自主管理用户属性**

开启后，所有IAM用户可以管理自己的[基本信息](#)，可以根据场景选择IAM用户可以修改的属性信息，可以选择登录密码、手机号、邮件地址。默认开启，且支持IAM用户修改所有属性。

管理员[进入安全设置](#)后，在“安全设置>敏感操作>自主管理用户属性>”中，单击“立即启用”。在“自主管理用户属性设置”弹窗中，选择“开启”并勾选支持IAM用户自主修改的属性，单击“确定”，开启IAM用户自主管理用户属性。

- **关闭自主管理用户属性**

关闭后，仅管理员可以管理自己的[基本信息](#)。IAM用户如需修改登录密码、手机号、邮件地址，请联系管理员参考[查看或修改IAM用户信息](#)进行操作。

管理员[进入安全设置](#)后，在“安全设置>敏感操作>自主管理用户属性>”中，单击“立即修改”。在“自主管理用户属性设置”弹窗中，选择“关闭”，单击“确定”，关闭IAM用户自主管理用户属性。

敏感操作有哪些

当您开启操作保护后，进行以下操作时，需要进行身份认证。

表 8-2 各云服务定义的敏感操作

类型	服务	敏感操作
计算	弹性云服务器 (ECS)	<ul style="list-style-type: none"> ● 关闭、重启、删除弹性云服务器 ● 重置弹性云服务器密码 ● 卸载磁盘 ● 解绑弹性公网IP
	裸金属服务器 (BMS)	<ul style="list-style-type: none"> ● 关机、重启裸金属服务器 ● 重置裸金属服务器的密码 ● 卸载磁盘 ● 解绑弹性公网IP
	弹性伸缩 (AS)	删除伸缩组

类型	服务	敏感操作
存储	对象存储服务 (OBS)	<ul style="list-style-type: none"> ● 删除桶 ● 创建、编辑、删除桶策略 ● 配置对象策略 ● 创建、编辑、删除桶ACL ● 配置日志记录 ● 配置防盗链 ● 增加、编辑桶清单
	云硬盘服务 (EVS)	删除云硬盘
	云备份 (CBR)	<ul style="list-style-type: none"> ● 删除存储库 ● 删除备份 ● 备份恢复 ● 删除策略 ● 解绑资源 ● 接受备份
存储	专属分布式存储服务 (DSS)	删除磁盘
CDN与智能边缘	内容分发网络 (CDN)	域名下线策略
容器	云容器引擎 (CCE)	删除集群
	应用编排服务 (AOS)	删除堆栈
网络	云解析服务 (DNS)	<ul style="list-style-type: none"> ● 修改、暂停、删除记录集 ● 修改、删除反向解析 ● 删除自定义线路
	虚拟私有云 (VPC)	<ul style="list-style-type: none"> ● 释放、解绑弹性公网IP ● 删除对等连接 ● 安全组 <ul style="list-style-type: none"> - 删除入 (出) 方向规则 - 修改入 (出) 方向规则 - 批量删除入 (出) 方向规则

类型	服务	敏感操作
	弹性负载均衡 (ELB)	<ul style="list-style-type: none"> ● 共享型负载均衡 <ul style="list-style-type: none"> - 删除负载均衡器 - 删除监听器 - 删除证书 - 删除后端云服务器 - 解绑弹性公网IP - 解绑IPv4公网/私有IP ● 独享型负载均衡 <ul style="list-style-type: none"> - 删除负载均衡器 - 删除监听器 - 删除证书 - 删除后端云服务器 - 解绑弹性公网IP - 解绑IPv4公网/私有IP - 解绑IPv6地址 - 移出IPv6共享带宽
	弹性公网IP (EIP)	<ul style="list-style-type: none"> ● 删除共享带宽 ● 释放、解绑弹性公网IP ● 批量释放、批量解绑弹性公网IP
	NAT网关 (NAT)	<ul style="list-style-type: none"> ● 私网NAT网关: <ul style="list-style-type: none"> - 删除SNAT规则 - 删除DNAT规则 - 删除中转IP ● 公网NAT网关: <ul style="list-style-type: none"> - 删除SNAT规则 - 删除DNAT规则

类型	服务	敏感操作
网络	虚拟专用网络 (VPN)	<ul style="list-style-type: none"> ● 删除/修改VPN连接 ● 退订包年/包月VPN网关 ● 删除/修改 VPN网关 ● 删除/修改对端网关 ● 修改VPN网关规格 ● 解绑弹性公网IP ● 修改服务端 ● 删除/修改服务端证书 ● 删除客户端CA证书 ● 创建/删除/修改用户和用户组 ● 批量删除用户 ● 创建/删除/修改访问策略 ● 重置用户密码
	云专线 (DC)	删除虚拟接口
安全与合规	SSL证书管理 (SCM)	<ul style="list-style-type: none"> ● 删除证书 ● 吊销证书
	数据加密服务 (DEW)	<ul style="list-style-type: none"> ● 删除密钥 ● 删除密钥别名 ● 撤销密钥授权 ● 删除凭据 ● 删除凭据事件 ● 删除密钥对 ● 删除专属加密集群 ● 删除密码服务管理集群 ● 删除密码服务管理应用 ● 删除密码服务管理密钥 ● 删除管理制度 ● 删除物理与环境信息

类型	服务	敏感操作
管理与监管	统一身份认证服务 (IAM)	<ul style="list-style-type: none"> ● 关闭操作保护 ● 关闭登录保护 ● 修改手机号 ● 修改邮件地址 ● 修改登录密码 ● 修改登录保护验证方式 ● 删除IAM用户 ● 停用IAM用户 ● 删除委托 ● 删除用户组 ● 删除策略 ● 删除授权 ● 新增访问密钥 ● 删除访问密钥 ● 停用访问密钥 ● 删除项目 ● 修改访问密钥保护状态
	消息通知服务 (SMN)	删除主题
管理与监管	云日志服务 (LTS)	<ul style="list-style-type: none"> ● 删除日志流/组 ● 卸载ICAgent
应用中间件	分布式缓存服务 (DCS)	<ul style="list-style-type: none"> ● 重置密码 ● 删除实例 ● 清空数据
	分布式消息服务 Kafka版	删除实例
	分布式消息服务 RabbitMQ版	删除实例
	分布式消息服务 RocketMQ版	删除实例

类型	服务	敏感操作
数据库	云数据库 RDS for MySQL	<ul style="list-style-type: none"> ● 重置管理员密码 ● 删除数据库实例 ● 删除数据库备份 ● 通过备份文件恢复到已有实例 ● 按指定时间点恢复到已有实例 ● 切换主备节点 ● 修改数据库端口 ● 删除数据库账号 ● 删除数据库 ● 修改实例内网IP ● 解绑弹性公网IP ● 下载全量备份文件
数据库	云数据库 RDS for PostgreSQL	<ul style="list-style-type: none"> ● 重置管理员密码 ● 删除数据库实例 ● 删除数据库备份 ● 切换主备节点 ● 修改数据库端口 ● 修改实例内网IP ● 解绑弹性公网IP ● 下载全量备份文件
数据库	云数据库 TaurusDB	<ul style="list-style-type: none"> ● 删除实例 ● 重启实例 ● 重启节点 ● 删除只读节点 ● 解绑弹性公网IP ● 删除数据库 ● 重置数据库账号密码 ● 删除数据库账号 ● 重置管理员密码 ● 修改内网域名 ● 修改读写内网地址 ● 将数据库实例恢复到指定时间点

类型	服务	敏感操作
数据库	文档数据库服务 (DDS)	<ul style="list-style-type: none"> ● 重置密码 ● 重启、删除实例 ● 重启节点 ● 副本集主备切换 ● 删除安全组规则 ● 申请Shard或Config节点IP ● 备份恢复到当前实例 ● 备份恢复到已有实例 ● 包周期实例转按需计费
大数据	数据仓库服务 GaussDB(DWS)	<ul style="list-style-type: none"> ● 扩容、调整大小 ● 重启 ● 节点修复 ● 重置密码
	MapReduce服务 (MRS)	<ul style="list-style-type: none"> ● 集群 <ul style="list-style-type: none"> - 删除集群 - 按需转包周期集群 - 停止所有组件 - 同步配置 ● 节点 <ul style="list-style-type: none"> - 停止所有角色 - 隔离主机 - 取消隔离主机 ● 组件: <ul style="list-style-type: none"> - 停止服务 - 重启服务 - 滚动重启服务 - 停止实例 - 重启实例 - 滚动重启实例 - 入服 - 退服 - 保存服务配置 ● 补丁: <ul style="list-style-type: none"> - 安装补丁 - 卸载补丁 - 回滚补丁

类型	服务	敏感操作
开发与运维	需求管理 CodeArts Req	<ul style="list-style-type: none">● 删除项目● 删除项目成员● 修改成员信息● 修改、删除权限● 修改项目基本信息● 删除工作项

类型	服务	敏感操作
企业应用	云桌面 Workspace	<ul style="list-style-type: none"> ● 云桌面： <ul style="list-style-type: none"> - 注销云办公服务 - 关闭云专线接入 - 关闭互联网接入 - 切换接入VPC - 删除桌面池 - 桌面池重建系统盘 - 桌面池删除磁盘 - 操作桌面池（开机、关机、重启、休眠） - 桌面池执行脚本 - 删除桌面 - 操作桌面（开机、关机、重启） - 重建桌面 - 解绑用户 - 切换桌面网络 - 迁移桌面 - 删除专享主机 - 解绑桌面EIP - 删除桌面快照 - 恢复桌面快照 - 删除桌面数据盘 - 操作用户（锁定、解锁和重置密码） - 删除用户组 - 删除策略组 - 删除用户 - 删除桌面应用 - 删除站点 - 修改站点接入方式 - 取消云办公带宽 ● 云应用： <ul style="list-style-type: none"> - 删除应用组 - 启用应用 - 移除应用组授权 - 删除服务器组 - 删除服务器 - 重装服务器 - 关闭服务器 - 删除WKS存储

类型	服务	敏感操作
		<ul style="list-style-type: none"> - 删除个人存储目录 - 删除策略组 - 切换服务器镜像
企业应用	消息&短信 (MSGSMS)	<ul style="list-style-type: none"> ● 签名删除 ● 模板删除 ● 获取app_secret ● 指定手机号、邮件地址绑定华为账号 ● 指定IP白名单 ● 续订套餐包
用户服务	费用中心	<ul style="list-style-type: none"> ● 订单支付 ● 订单退订 ● 资源释放

8.4 登录验证策略

进入安全设置后，选择“登录验证策略”页签，可以对[会话超时策略](#)、[账号锁定策略](#)、[账号停用策略](#)、[最近登录提示](#)、[登录验证提示](#)进行修改，登录验证策略对账号和账号中的IAM用户生效。

只有[管理员](#)可以设置登录验证策略，普通IAM用户只有查看权限，不能对其进行设置，如需修改，请联系管理员为您操作或添加权限。

会话超时策略

如果用户超过设置的时长未操作界面，会话将会失效，需要重新登录。

图 8-12 会话超时策略

会话超时策略 修改后需重新登录后生效

用户在 内没有操作，退出当前账号。

管理员可以设置会话超时的时长，会话超时时长默认为1个小时，可以在15分钟~24小时之间进行设置。

账号锁定策略

如果在限定时间长度内达到登录失败次数后，用户会被锁定一段时间。锁定时，账号不能为自己或IAM用户解锁，锁定时间结束后，才能重新登录。

图 8-13 账号锁定策略

账号锁定策略 对华为云账号、账号下的IAM用户均生效

账号锁定时长	<input type="text" value="15"/>	分钟 <input type="button" value="v"/>
锁定前允许的最大登录失败次数	<input type="text" value="5"/>	
重置账号锁定计数器的时间	<input type="text" value="15"/>	分钟

管理员可以设置账号锁定时长、锁定前允许的最大登录失败次数、重置账号锁定计数器的时间。

- 账号锁定时长（分钟）：默认为15分钟，可以在15~30分钟之间进行设置。
- 锁定前允许的最大登录失败次数：默认为5次，可以在3~10次之间进行设置。
- 重置账号锁定计数器的时间：默认为15分钟，可以在15~60分钟之间进行设置。

账号停用策略

如果IAM用户在设置的有效期内没有通过界面控制台或者API访问华为云，再次登录时将会被停用。

账号停用策略默认关闭，管理员可以选择开启，并在1~240天之间进行设置。

该策略仅对账号下的IAM用户生效，对账号本身不生效。IAM用户被停用后，可以联系管理员重新启用。

最近登录提示

如果开启最近登录提示，用户登录成功后，将在“登录验证”页面中看到上次登录成功时间，最近登录提示可以帮助用户查看是否存在异常登录信息，如果存在不是本人的登录信息，建议立即修改密码。

最近登录提示默认关闭，管理员可以选择开启。

登录验证提示

管理员可以在最近登录提示中进行公告，例如欢迎语，或者提示用户谨慎删除资源等。

登录验证提示默认关闭，管理员可以选择开启。

图 8-14 登录验证提示

登录验证提示

登录成功时，将看到自定义的验证信息。

welcome

7/60 ↕

开启后，用户将在“登录验证”页面中看到公告信息。

图 8-15 登录验证



USB KEY 证书策略

设置证书过期提前提醒时间，证书过期前提醒用户及时重新申请，保障业务连续性。用户在USB KEY证书的有效期内必须重新申请，否则USB KEY将会失效，无法登录云服务平台。USB KEY证书过期提前提醒时间默认为10天，可以在1~10天之间进行设置。

修改USB KEY证书策略，将对账号以及账号下的IAM用户立即生效。

8.5 密码策略

进入安全设置后，选择“密码策略”页签，可以对[密码设置策略](#)、[密码有效期策略](#)、[密码最短使用时间策略](#)进行修改。

只有[管理员](#)可以设置密码策略，普通IAM用户只有查看权限，不能对其进行设置，如需使用，请联系IAM管理员为您操作或添加权限。

建议IAM管理员设置密码策略，例如密码最小长度、密码中同一字符连续出现的最大次数、密码不能与历史密码相同，保证用户在修改密码时，新密码都是满足密码策略的复杂程度高的强密码。

📖 说明

如果您的华为云账号已升级为华为账号，密码策略将对账号不生效。

密码设置策略

图 8-16 密码设置策略

密码设置策略 对华为云账号、账号下的IAM用户均生效

至少包含以下字符中的 种：大写字母、小写字母、数字和特殊字符。

密码最小长度

设置密码时同一字符不能连续出现

新密码不能与最近的历史密码相同

密码不能与历史密码重复次数

- 密码至少包含字符种类（大写字母、小写字母、数字、特殊字符）默认为2种，可以在2~4种之间设置。
- 密码最小长度默认为8个字符，可以在8~32个字符之间设置。
- （可选）开启“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。例如设置为1，表示密码中不允许出现相同字符。
- （可选）开启“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。例如设置为3，表示不能使用最近三次的历史密码，用户在设置新密码时，如果新密码与历史密码相同，系统将会提示用户不能使用最近三次的历史密码，需要重新设置密码。

修改密码设置策略，将对后续新增IAM用户和后续修改密码的账号以及账号下的IAM用户生效。

密码有效期策略

用户在设置的时间内必须修改密码，否则密码将会失效，无法登录华为云，IAM会在密码到期前15天开始提示用户修改密码。密码有效期策略可以强制用户修改密码，提高账号安全性。

密码有效期策略默认关闭，管理员可以选择开启，在1~180天之间进行设置。

修改密码有效期策略，将对账号以及账号下的IAM用户立即生效。

说明

密码过期后，请通过邮箱链接设置新密码，新密码不允许与旧密码相同。

密码最短使用时间策略

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。密码最短使用时间策略可以防止用户频繁修改密码，导致忘记密码。

密码最短使用时间策略默认关闭，管理员可以选择开启，在0~1440分钟之间进行设置。

修改密码最短使用时间策略，将对账号以及账号下的IAM用户立即生效。

8.6 访问控制

进入安全设置后，选择“访问控制”页签，可以对允许访问的IP地址区间、允许访问的IP地址或网段、允许访问的VPC Endpoint进行修改。

管理员可以设置访问控制策略，限制账号下的所有IAM用户只能从特定IP地址区间、网段及VPC Endpoint访问华为云。普通IAM用户没有权限查看此页面，如需使用，请联系管理员为您操作或添加权限。

访问控制生效条件：

- 控制台访问（推荐）：仅对账号下的所有IAM用户和联邦用户（SP方式）登录控制台生效，对账号本身不生效。
- API访问：仅对账号下的所有IAM用户和联邦用户通过API网关访问API接口生效，修改后2小时生效。

说明

- 访问控制策略最多可设置200条。
- 如果IAM用户或联邦用户通过代理访问华为云，需按照代理IP设置允许访问的IP地址区间/IP地址或网段；如果IAM用户或联邦用户通过公网访问华为云，请按照公网IP进行设置。
- 仅支持IPv4类型的地址。

允许访问的 IP 地址区间

图 8-17 允许访问的 IP 地址区间



限制用户只能从设定范围内的IP地址访问华为云，可以在0.0.0.0~255.255.255.255之间设置。默认值为0.0.0.0~255.255.255.255。如不设置或设置为默认值意味着您的IAM用户可以从任意地方访问华为云。

允许访问的 IP 地址或网段

限制用户只能从设定的IP地址或网段访问华为云，例如：10.10.10.10/32。

允许访问的 VPC Endpoint

仅在“API访问”页签中可进行配置。限制用户只能从具有设定ID的VPC Endpoint访问华为云API，例如：0ccad098-b8f4-495a-9b10-613e2a5exxxx。若未进行访问控制配置，则默认用户从所有VPC Endpoint都能访问API。

图 8-18 允许访问的 VPC Endpoint

允许访问的VPC Endpoint 仅对IAM用户生效

Endpoint ID	描述	操作
暂无数据		

⊕ 添加

📖 说明

- “允许访问的IP地址区间”、“允许访问的IP地址区间或网段”和“允许访问的VPC Endpoint”，如果同时设置，只要满足其中一种即可允许访问。
- 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地址区间或网段”、“允许访问的VPC Endpoint”清空。

9 身份提供商

9.1 身份提供商概述

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

表 9-1 基本概念

概念	说明
身份提供商（Identity Provider，简称IdP）	负责收集、存储用户身份信息，如用户名、密码等，在用户登录时负责认证用户的服务。在企业与华为云联邦身份认证的过程中，身份提供商指企业自身的身份提供商，目前常用的第三方IdP有Microsoft Active Directory（AD FS）、Shibboleth。
服务提供商（Service Provider，简称SP）	服务提供商通过与身份提供商IdP建立信任关系，使用IdP提供的用户信息，为用户提供具体的服务。在企业与华为云联邦身份认证的过程中，服务提供商指华为云。
联邦身份认证	身份提供商IdP与服务提供商SP 建立信任关系并完成交互流程 ，实现用户单点登录的过程，称之为联邦身份认证。
单点登录（Single Sign-On，简称SSO）	用户在身份提供商IdP系统登录后，就可以通过跳转链接访问已建立互信关系的服务提供商SP系统，这一过程称之为单点登录。如：企业管理系统与华为云建立互信关系后，企业管理系统中的用户通过华为云提供的登录入口，使用已有的账号密码在企业管理系统中登录后，即可跳转访问华为云。华为云支持两类单点登录方式，分别是虚拟用户SSO和IAM用户SSO。

概念	说明
SAML 2.0	安全断言标记语言（Security 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OIDC1.0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 。
OAuth 2.0	OAuth 2.0是Open Authorization 2.0的简称，是一种开放授权协议，授权框架支持第三方应用程序以自己的名义获取访问权限。

使用联邦身份认证的优势

- 管理用户简单

使用联邦身份认证前，管理员需要在企业管理系统和华为云分别为用户创建账号。

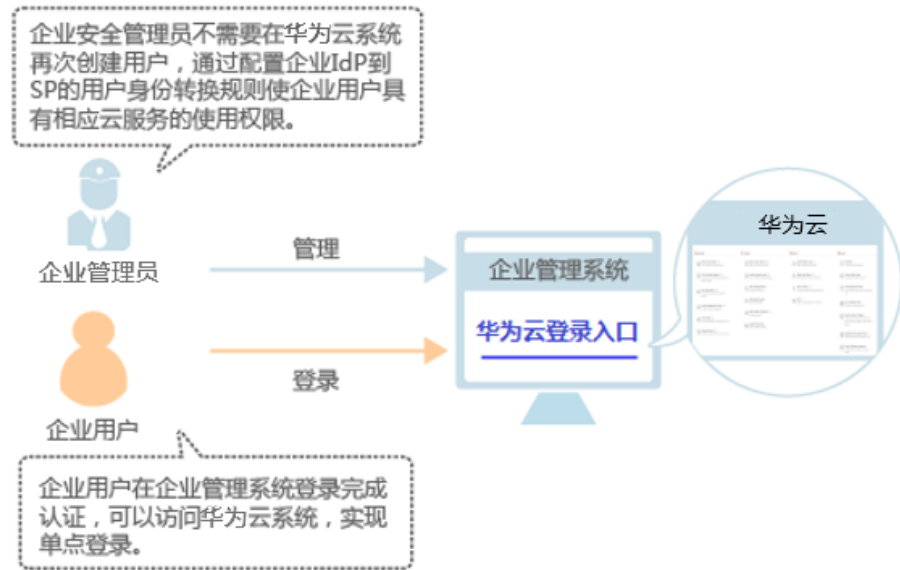
使用联邦身份认证后，企业管理员只需要在企业管理系统中为用户创建账号，用户即可同时访问两个系统，降低了人员管理成本。

- 用户操作方便

使用联邦身份认证前，用户访问企业管理系统和华为云时需要使用两个系统的账号登录。

使用联邦身份认证后，用户在本企业管理系统中登录即可访问两个系统。

图 9-1 使用联邦身份认证的优势



SSO 方式

目前IAM支持两类SSO方式，分别是虚拟用户SSO和IAM用户SSO。选择SSO方式请参见[虚拟用户SSO与IAM用户SSO的适用场景](#)。

- 虚拟用户SSO
企业IdP用户登录华为云后，系统为其自动创建虚拟用户信息，并根据您配置的身份转换规则为其授予访问权限。
- IAM用户SSO
企业IdP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。

目前IAM支持两种联邦登录的形式，分别是浏览器页面单点登录（Web SSO）和调用API接口。

- 浏览器页面单点登录（Web SSO）：浏览器作为通讯媒介，适用于普通用户通过浏览器访问华为云。您可以从IdP侧或SP侧发起Web SSO：
 - IdP侧发起登录：[配置企业管理系统登录入口](#)后，通过企业管理系统单点登录华为云。
 - SP侧发起登录：通过华为云提供的[企业联邦用户登录](#)入口，输入对应华为云用户名称，选择身份提供商，跳转至企业管理系统进行登录认证。
- 调用API接口：开发工具/应用程序作为通讯媒介，例如OpenStack Client、ShibbolethECP Client，适用于企业或用户通过API调用方式访问华为云。

表 9-2 联邦认证方式

SSO 方式	支持协议	是否支持 Web SSO	是否支持 API 调用	从 IdP 侧发起登录	从 SP 侧发起登录	多个 IdP
虚拟用户 SSO	SAML 2.0与 OIDC	是	是	支持	支持	支持
IAM 用户 SSO	SAML 2.0	是	是	支持	支持	不支持

本章为您介绍通过浏览器页面单点登录华为云的过程（Web SSO），如需了解通过API调用方式访问华为云，请参见：[联邦身份认证管理](#)。

注意事项

- 企业IdP服务器的时间需要和华为云的时间、时区一致，即都使用GMT时间（Greenwich Mean Time），否则会导致联邦身份认证失败。
- 由于联邦用户的身份信息（如邮件地址、手机号码）保存在企业IdP中，是企业IdP映射到华为云的虚拟用户，因此，联邦用户通过身份提供商功能访问华为云时有以下约束：
 - 如果账号开启了[敏感操作保护](#)（登录保护或操作保护），对联邦用户不生效，即联邦用户在执行敏感操作时，不需要二次验证。
 - 不支持创建永久访问密钥（AK/SK），支持通过用户或委托token来获取临时访问凭证（临时AK/SK和securitytoken），具体方法请参见：[获取临时AK/SK和securitytoken](#)。

如需使用永久AK/SK，只能由账号或是实体IAM用户创建密钥，共享给联邦用户。由于密钥表示用户所拥有的权限，因此建议由与联邦用户同在一个用户组的实体IAM用户创建并分享密钥。

9.2 虚拟用户 SSO 与 IAM 用户 SSO 的适用场景

华为云目前支持两种身份提供商类型：虚拟用户SSO和IAM用户SSO。本文为您介绍两种身份提供商的适用场景和选择依据，帮助您根据整体业务需求选择合适的身份提供商类型。

虚拟用户 SSO

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，并按照身份转换规则授权。虚拟用户SSO适用于以下场景：

- 出于管理成本考虑，您不希望在云平台创建和管理IAM用户，从而避免用户同步带来的工作量。

- 您希望根据用户在本地企业IdP中加入的组或者用户的某个特殊属性，来区分云上拥有的权限。当企业IdP用户进行权限调整时，只需要在本地进行分组或属性的更改，即可同步到云平台。
- 您的各个分支机构存在多个企业IdP，都需要访问同一个华为云账号，您需要在一个华为云账号中内配置多个IdP进行联邦认证。

IAM 用户 SSO

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。IAM用户SSO适用于以下场景：

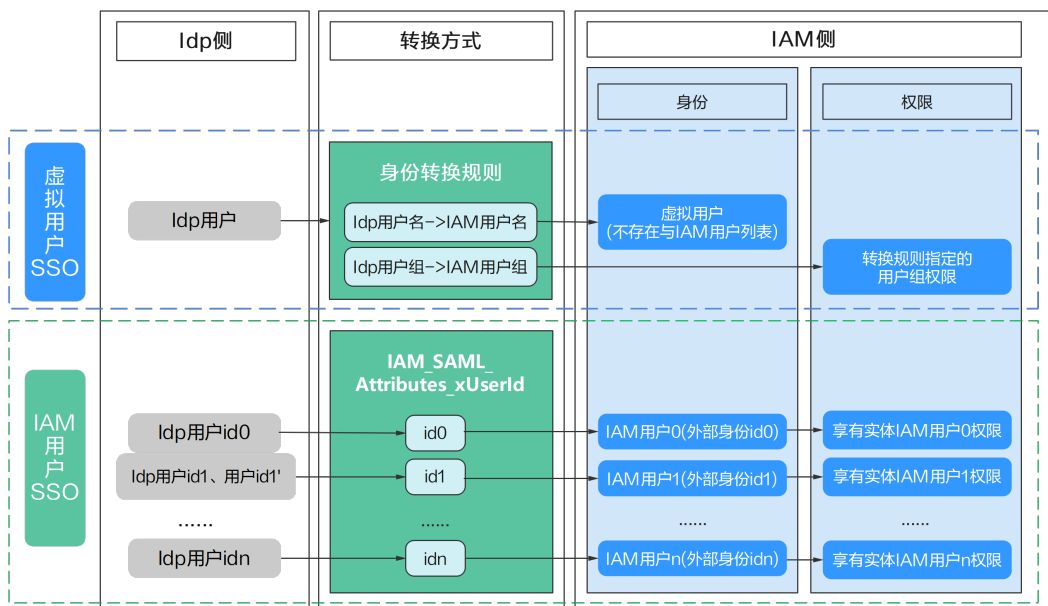
- 您需要使用的云产品中有部分暂时不支持虚拟用户SSO访问，例如[软件开发平台](#)。
- 您没有上述需要使用虚拟用户SSO的业务需求，而又希望尽量简化IdP配置。

两者的区别

虚拟用户SSO和IAM用户SSO的区别有身份转换方式、IAM用户身份、IAM侧权限分配3个方面的区别：

- 1、身份转换方式：虚拟用户SSO通过[身份转换规则](#)进行Idp用户和IAM用户的身份转换。IAM用户SSO使用外部身份ID来进行身份转换，Idp用户的IAM_SAML_Attributes_xUserId值与IAM用户的[外部身份ID](#)一一对应，一个或多个具有相同IAM_SAML_Attributes_xUserId值的Idp用户均可跳转至对应ID值的SP用户。因此，使用IAM用户SSO登录，请务必在Idp侧断言中设置IAM_SAML_Attributes_xUserId，在SP侧设置IAM用户外部身份ID。
- 2、IAM侧用户身份：虚拟用户SSO无法在IAM用户列表中找到Idp用户对应的IAM用户，跳转时系统临时为其自动创建虚拟用户信息。IAM用户SSO则在IAM用户列表中存在Idp用户对应的绑定外部身份ID的IAM子用户。
- 3、IAM侧权限分配：虚拟用户SSO中，Idp用户跳转后的权限取决于身份转换规则，规则中说明跳转后临时生成的虚拟用户拥有哪些用户组权限。IAM用户SSO中，Idp用户跳转后直接集成IAM子用户所在用户组的权限。

图 9-2 IAM 用户 SSO 与虚拟用户 SSO 的区别



9.3 基于 SAML 协议的虚拟用户 SSO

9.3.1 基于 SAML 协议的虚拟用户 SSO 配置概述

华为云与企业进行联邦认证登录时，华为云是服务提供者（SP），企业自有的身份管理系统是身份提供者（IdP）。本节为您介绍企业IdP与华为云，基于SAML协议进行虚拟用户SSO联邦认证的内部实现流程和配置步骤，以及常用的企业IdP与华为云对接示例。

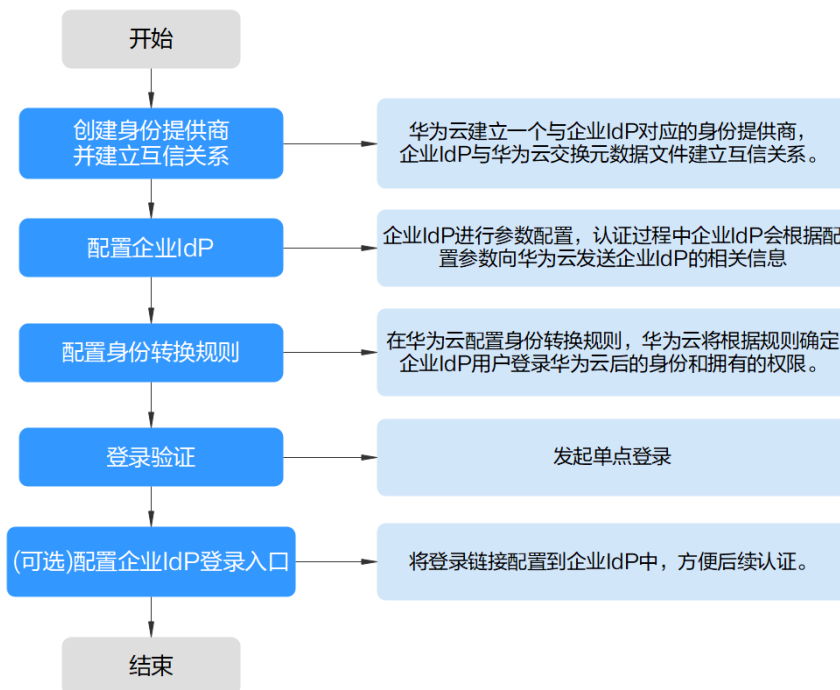
⚠ 注意

请确保您使用的企业IdP支持SAML 2.0协议。

联邦身份认证的配置步骤

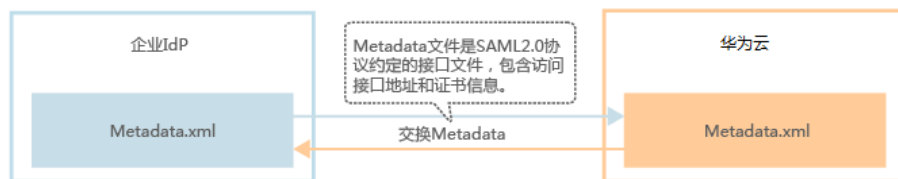
建立企业管理系统与华为云的联邦身份认证关系，配置流程如下。

图 9-3 基于 SAML 的虚拟 SSO 配置流程



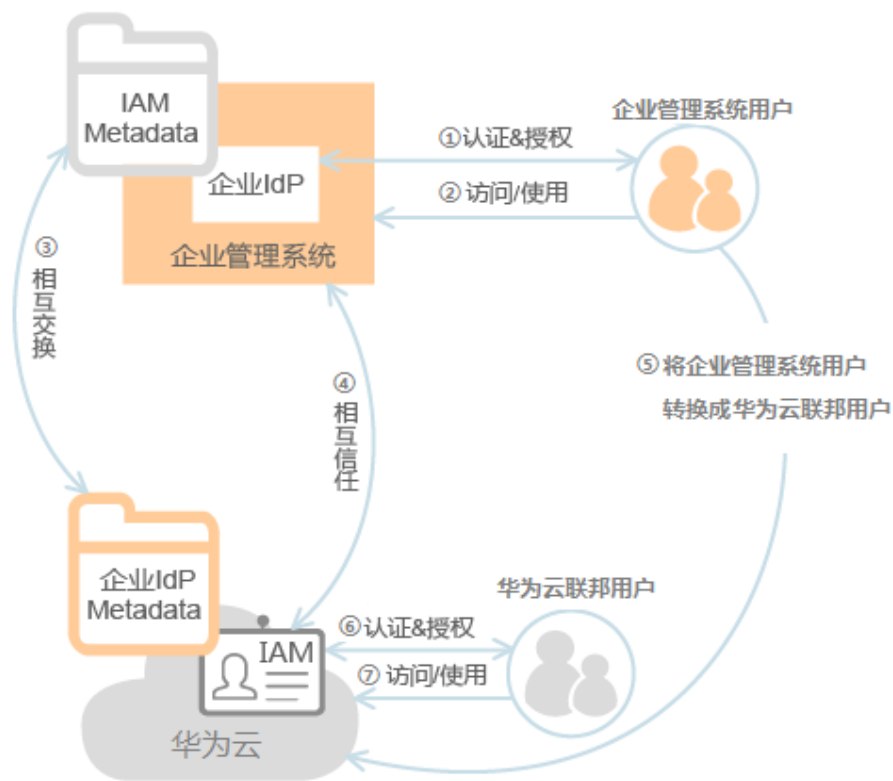
1. **创建身份提供商并建立互信关系**：华为云与企业IdP建立联邦认证，需要华为云平台创建一个与企业IdP对应的身份提供商程序。然后，建立联邦认证的双方需首先建立互信关系，双方交换元数据文件，在企业IdP中上传华为云元数据文件，在华为云上传企业IdP的元数据文件。

图 9-4 交换 Metadata 文件模型



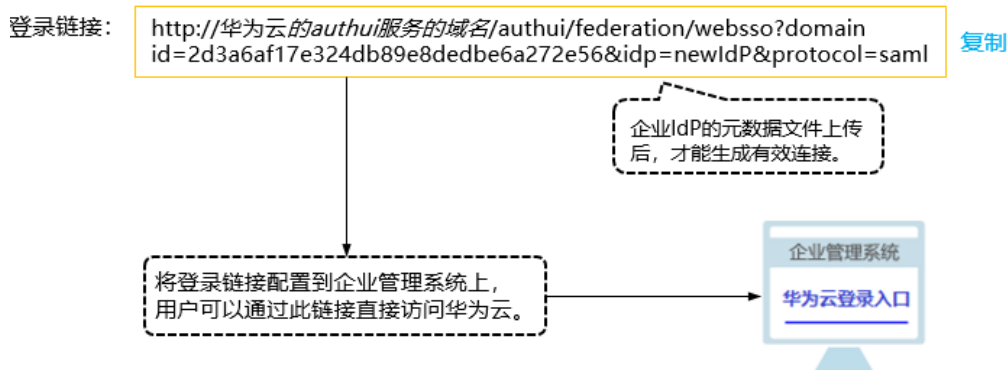
2. **配置企业IdP参数**，规定在交互过程中，企业IdP向华为云发送哪些信息。
3. **在华为云配置身份转换规则**：通过配置身份转换规则，明确企业IdP用户登录华为云后的身份和权限，例如登录华为云后的用户名、加入的用户组和拥有的访问权限。

图 9-5 用户转换模型



4. **登录验证**：发起单点登录，测试是否能成功从企业IdP跳转登录华为云。
5. **(可选) 配置企业管理系统登录入口**：将华为云的访问入口配置到企业管理系统中，用户可通过登录企业管理系统直接访问华为云，如图9-6所示。

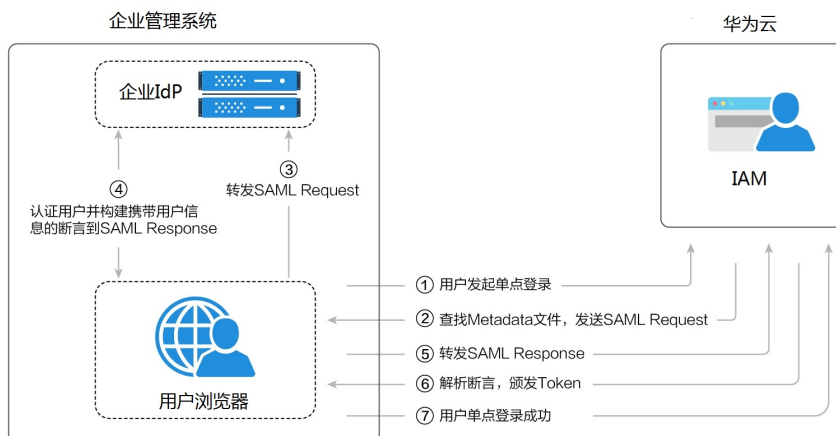
图 9-6 配置单点登录模型



企业管理系统与华为云联邦身份认证交互流程

图9-7为用户在发起单点登录请求后, 企业管理系统与华为云间的交互流程。

图 9-7 联邦身份认证交互流程



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”。

从图9-7中可知, 联邦身份认证的步骤为:

1. 用户在浏览器中打开创建身份提供商后生成的登录链接, 浏览器向华为云发起单点登录请求。
2. 华为云根据登录链接中携带的信息, 查找IAM身份提供商中对应的Metadata文件, 构建SAML Request, 发送给浏览器。
3. 浏览器收到请求后, 转发SAML Request给企业IdP。
4. 用户在企业IdP推送的登录页面中输入用户名和密码, 企业IdP对用户提供的身份信息验证, 并构建携带用户信息的SAML断言, 向浏览器发送SAML Response。

5. 浏览器响应后转发SAML Response给华为云。
6. 华为云从SAML Response中取出断言，并根据已配置的身份转换规则映射到具体的IAM用户组，颁发Token。
7. 用户完成单点登录，访问华为云。

📖 说明

断言中要携带签名，否则会导致登录失败。

9.3.2 步骤 1：创建身份提供商

配置联邦身份认证，需要在企业IdP上传华为云的元数据文件（Metadata文件），并在IAM控制台上创建身份提供商、上传企业IdP的元数据文件，来建立两个系统之间的互信关系。

前提条件

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，华为云帮助文档对于企业IdP的配置不做详述，获取企业IdP的元数据文件、华为云元数据上传至企业IdP等具体操作请参考企业IdP的帮助文档。

建立企业 IdP 对华为云的信任关系

在企业IdP中配置华为云的元数据文件，以建立企业IdP对华为云的信任。

步骤1 下载华为云系统的元数据文件（metadata文件）。

访问网址：<https://auth-intl.huaweicloud.com/authui/saml/metadata.xml>（推荐使用Chrome浏览器）。下载华为云元数据文件，并设置文件名称，例如“SP-metadata.xml”。

步骤2 将上述文件上传到企业IdP服务器上。上传方法请参见企业IdP的帮助文档。

步骤3 获取企业IdP的元数据文件。获取方法请参见企业IdP的帮助文档。

----结束

在华为云上创建身份提供商

在IAM控制台上创建身份提供商，配置身份提供商的元数据文件后，可以在IAM中建立对企业IdP的信任关系，使得企业用户可以直接访问华为云。

步骤1 进入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”。

图 9-8 创建身份提供商



步骤2 在“创建身份提供商”窗口中设置名称、协议、类型、状态、描述。

图 9-9 填写身份提供商参数

The screenshot shows a form for creating an identity provider. It contains the following elements:

- * 名称**: A text input field containing the value "saml".
- * 协议**: A dropdown menu with "SAML" selected and a help icon (?) to its right.
- * 类型**: A dropdown menu with "虚拟用户SSO" selected and a help icon (?) to its right.
- * 状态**: Two radio buttons, "启用" (selected) and "停用".
- 描述**: A large text area with the placeholder text "请输入身份提供商信息。" and a character count "0/255" at the bottom right.
- At the bottom, there are two buttons: "确定" (black) and "取消" (white).

表 9-3 身份提供商基本参数

参数	含义
名称	身份提供商的名称。身份提供商名称在全局范围内不能重复，建议以域名唯一标识命名。
协议	身份提供商协议。当前华为云支持基于SAML、OIDC的身份提供商，如需创建基于OIDC协议的联邦身份认证，请参考 基于OIDC协议的虚拟用户SSO 。
类型	身份提供商类型。一个账号下只能存在一种类型的身份提供商。本章介绍虚拟用户SSO，此处选择虚拟用户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。
状态	身份提供商的状态。默认设置为“启用”。

步骤3 单击“确定”，创建身份提供商成功。

----结束

在华为云上配置元数据文件

配置元数据文件，即把企业IdP的Metadata文件配置到华为云。IAM支持“上传文件”和“手动编辑”两种配置，选择其中一种即可。如果元数据文件超过500KB，请通过“手动编辑”配置元数据。如果后续元数据有更新，需要用户重新上传或者编辑元数据，否则会影响联邦用户登录华为云。

说明

企业IdP的Metadata文件获取方法请参考企业IdP提供商的帮助文档。

- **上传元数据:**
 - a. 单击身份提供商列表中“操作”列的“修改”。

图 9-10 修改身份提供商



- b. 单击“上传文件”左侧的“添加文件”，选择获取的企业IdP的元数据文件。

图 9-11 上传元数据文件

元数据配置

系统将从您上传的文件中提取元数据信息，请上传500KB以内的文件，超过500KB的文件请您手动编辑元数据信息。

点击右侧按钮先添加再上传

添加文件

上传文件

- c. 单击“上传文件”。弹出页面显示系统提取到的元数据，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”，保存设置信息。
- **手动编辑元数据**
 - a. 单击“手动编辑”。

图 9-12 手动编辑元数据

元数据配置

系统将从您上传的文件中提取元数据信息，请上传500KB以内的文件，超过500KB的文件请您手动编辑元数据信息。

点击右侧按钮先添加再上传

添加文件

上传文件

- b. 在“手动编辑元数据”页面中，输入从企业IdP元数据文件中获取的“Entity ID”、“签名证书”和“SingleSignOnService”等参数。

参数	是否必选	含义
Entity ID	是	对应IdP元数据文件中“entityID”的值。 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	是	企业IdP与服务提供商之间，通过SAML协议完成联邦身份认证。 不需要手动选择，系统自动生成。
支持的NameIdFormat	否	对应IdP元数据文件中“NameIdFormat”的值。 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。 支持配置多个，华为云默认使用第一个。
签名证书	是	对应IdP元数据文件中“<X509Certificate>”的值。 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。IAM通过元数据文件中的签名证书来确认联邦身份认证过程中断言消息的可信性、完整性。 支持配置多个，华为云默认使用第一个。
SingleSignOnService	是	对应IdP元数据文件中“SingleSignOnService”的值。 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。 支持配置多个，华为云默认使用第一个。
SingleLogoutService	否	对应IdP元数据文件中“SingleLogoutService”的值。 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。 支持配置多个，华为云默认使用第一个。

示例：以下为某企业IdP的元数据文件和手动编辑元数据信息时需要填入的内容。

图 9-13 某企业 IdP 的元数据文件

```
<md:EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Name="urn:keycloak">
  <md:EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="http://localhost:8080/auth/realms/master">
    <md:IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <md:KeyDescriptor use="signing">
        <ds:KeyInfo>
          <ds:KeyName>
            <ds:X509Data>
              <ds:X509Certificate>
                [Redacted Certificate Data]
              </ds:X509Data>
            </ds:KeyName>
          </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://localhost:8080/auth/realms/master/protocol/saml"/>
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://localhost:8080/auth/realms/master/protocol/saml"/>
        <md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
        <md:NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
        <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
        <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
        <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://localhost:8080/auth/realms/master/protocol/saml"/>
        <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://localhost:8080/auth/realms/master/protocol/saml"/>
        <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="http://localhost:8080/auth/realms/master/protocol/saml"/>
      </md:IDPSSODescriptor>
    </md:EntityDescriptor>
  </md:EntitiesDescriptor>
```

图 9-14 根据企业 IdP 元数据文件手动编辑元数据

提取元数据 ×

Entity ID

Entity ID

支持的协议

支持的NameIDFormat

签名证书

c. 单击“确定”，保存设置信息。

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。

后续任务

- **配置企业IdP：**在企业IdP系统中配置单点登录相关参数，决定向华为云提供哪些用户信息。
- **配置身份转换规则：**在“身份转换规则”区域，配置身份转换规则，建立企业管理系统用户与IAM用户组间的映射关系，使得企业管理系统用户登录华为云后，获得对应的华为云操作权限。身份转换规则详情请参见：[步骤3：配置身份转换规则](#)。
- **登录验证：**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登录入口直接访问华为云，方法请参考：[步骤4：登录验证](#)。

9.3.3 步骤 2：配置企业 Idp

您可以在企业IdP中配置单点登录相关参数，决定向华为云提供哪些用户信息。企业IdP与华为云交互过程中，需要将企业IdP用户的相关信息发送给华为云，华为云会结合接收到的信息和身份转换规则，确定联邦用户的身份和权限。

常用的企业 IdP 配置参数

表 9-4 常用的企业 IdP 配置参数

参数名	描述	适用场景
IAM_SAML_Attributes_redirected_url	指定联邦登录重定向的目标网址	用户在SSO登录过程中，希望跳转到华为云控制台的指定页面。例如指定跳转到香港局点，云监控服务CES主页。
IAM_SAML_Attributes_domain_id	与企业IdP建立联邦认证的华为账号或华为云账号ID值	从企业IdP侧发起联邦认证登录，必须在企业IdP侧配置该参数。
IAM_SAML_Attributes_idp_id	与企业IdP建立联邦认证的华为账号或华为云账号中，创建的身份提供商名称	从企业IdP侧发起联邦认证登录，必须在企业IdP侧配置该参数。

9.3.4 步骤 3：配置身份转换规则

企业IdP用户登录华为云后，华为云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中的用户名默认为“FederationUser”，权限默认仅能访问华为云，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资源的权限。由于华为云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，从而使联邦用户获得对应用户组的权限，使用华为云上的资源。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 9-15 创建规则-1

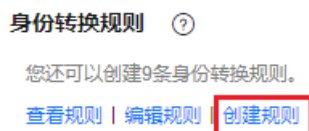


图 9-16 创建规则-2

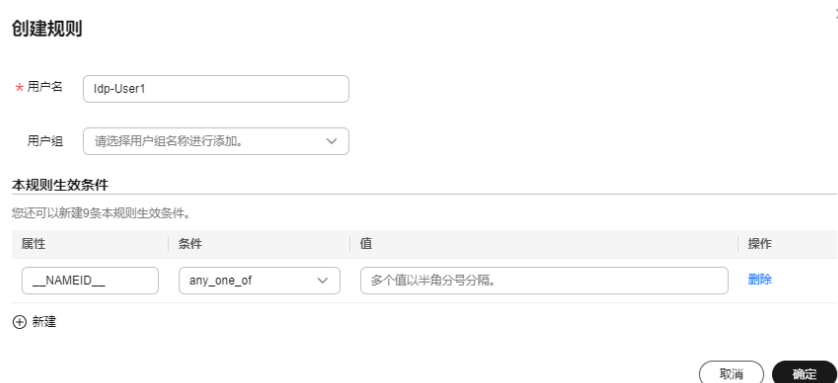


表 9-5 参数说明

参数名	描述	说明
用户名	联邦用户在华为云中显示的用户名，以下简称“联邦用户名”。	<p>为了区分华为云的用户与联邦用户，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。</p> <p>须知</p> <ul style="list-style-type: none"> 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。	<p>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。一个身份转换规则最多可以创建10条生效条件。</p> <p>“属性”、“值”为企业IdP通过SAML断言返回给华为云用户信息；“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。</p> <p>说明</p> <ul style="list-style-type: none"> 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。

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，进入 [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 9-17 修改身份提供商



- c. 在“身份转换规则”区域单击“编辑规则”。

图 9-18 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](#)。

9.3.5 步骤 4：登录验证

登录验证

按照登录请求发起方可将联邦用户登录方式分为两类：

- Idp侧登录：用户从IdP侧（企业自己的身份提供商侧）发起登录请求，例如从 Microsoft Active Directory（AD FS）、Shibboleth侧发起登录华为云控制台的请求。
- SP侧登录：用户从SP侧（服务提供商侧）发起登录请求，在企业与华为云联邦身份认证的过程中，服务提供商指华为云，SP侧登录链接可在IAM控制台身份提供商详情页面获取。

不同的企业IdP发起Idp侧登录的方式差异较大，华为云帮助文档不做详述，具体操作请参考企业IdP的帮助文档。本节重点介绍SP侧发起登录的方法：

步骤1 联邦用户登录。

在控制台的“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。

图 9-19 登录链接



步骤2 查看联邦用户是否具有所属用户组的权限。

---结束

跳转到指定区域或服务

如需指定联邦用户登录的目标页面，比如联邦用户登录时，指定跳转到香港局点，云监控服务CES主页。有以下两种配置方式：

- SP侧登录配置方法
拼接控制台获取的登录链接与指定url，拼接格式为“**登录链接&service=指定url**”。例如：获取的登录地址为https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml，指定跳转的控制台地址为<https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1>，按照拼接格式拼接得到的登录链接为：https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml&service=<https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1>。
- IdP侧登录配置方法
在企业IdP的SAML断言中配置IAM_SAML_Attributes_redirect_url声明，声明值为指定跳转的目标URL。

9.3.6（可选）步骤 5：配置企业管理系统登录入口

将身份提供商的登录链接配置到企业管理系统上，企业用户通过该链接访问华为云。

📖 说明

华为云提供企业联邦用户登录入口，如您未配置企业管理系统登录入口，企业联邦用户可以通过该方法登录华为云，详情请参考：[企业联邦用户登录](#)。

前提条件

- 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](#)。

- 企业管理系统界面已创建华为云登录入口。

操作步骤

步骤1 在IAM控制台的左侧导航窗格中，单击“身份提供商”。

步骤2 单击目标身份提供商列表右侧的“查看”。

图 9-20 查看身份提供商详情



步骤3 单击“登录链接”右侧的“□”。

图 9-21 复制登录链接



步骤4 将以下语句添加在企业管理系统页面文件中。

```
<a href="<登录链接>"> 华为云登录入口 </a>
```

步骤5 用户登录企业管理系统后通过单击“华为云登录入口”可以直接访问华为云。

----结束

9.4 基于 SAML 协议的 IAM 用户 SSO

9.4.1 基于 SAML 协议的 IAM 用户 SSO 配置概述

华为云与企业进行联邦认证登录时，华为云是服务提供商（SP），企业自有的身份管理系统是身份提供商（IdP），通过基于SAML协议的单点登录，企业员工在登录以后，将跳转至华为云平台，以IAM用户的方式访问华为云。

本节为您介绍企业IdP与华为云，基于SAML协议进行IAM用户SSO联邦认证的内部实现流程和配置步骤。

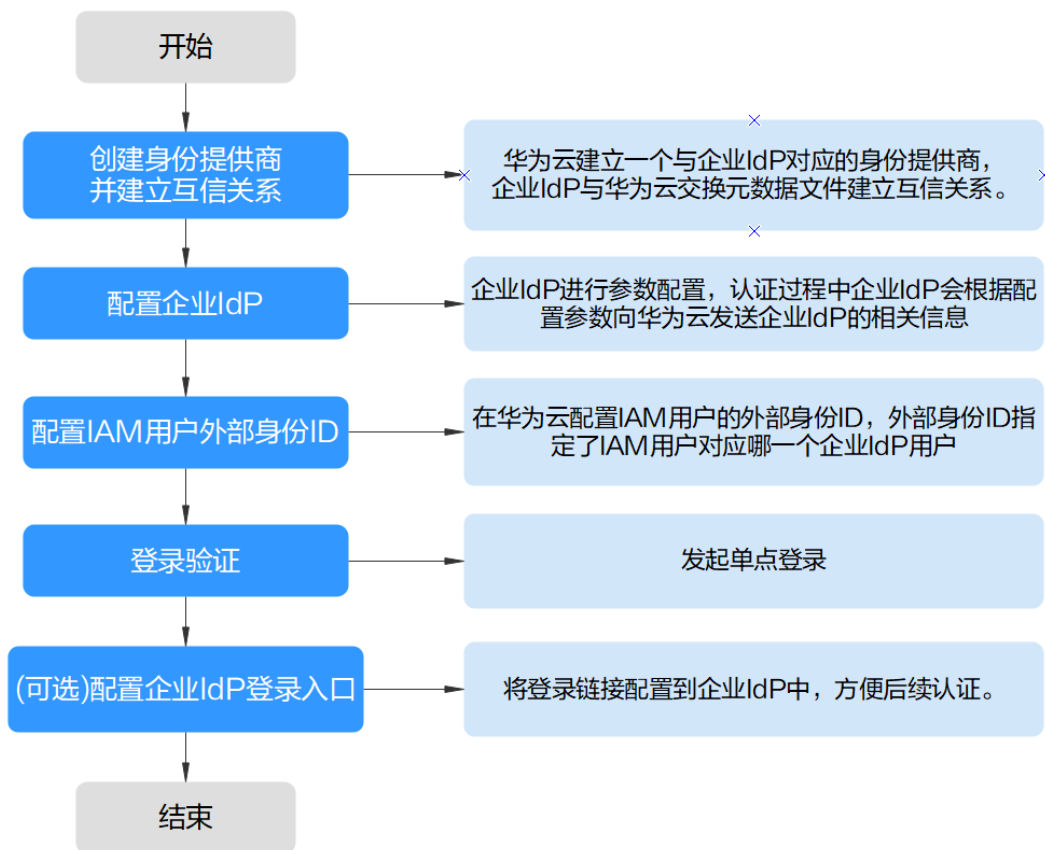
注意

请确保您使用的企业IdP支持SAML 2.0协议。

联邦身份认证的配置步骤

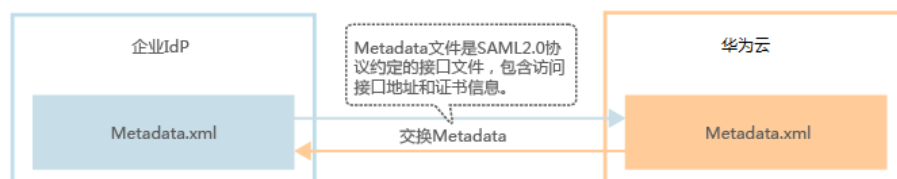
建立企业管理系统与华为云的联邦身份认证关系，配置流程如下。

图 9-22 基于 SAML 的 IAM 用户 SSO 配置流程



1. **创建身份提供商并建立互信关系**：华为云与企业IdP建立联邦认证，需要华为云平台创建一个与企业IdP对应的身份提供商程序。然后，建立联邦认证的双方需首先建立互信关系，双方交换元数据文件，在企业IdP中上传华为云元数据文件，在华为云上传企业IdP的元数据文件。

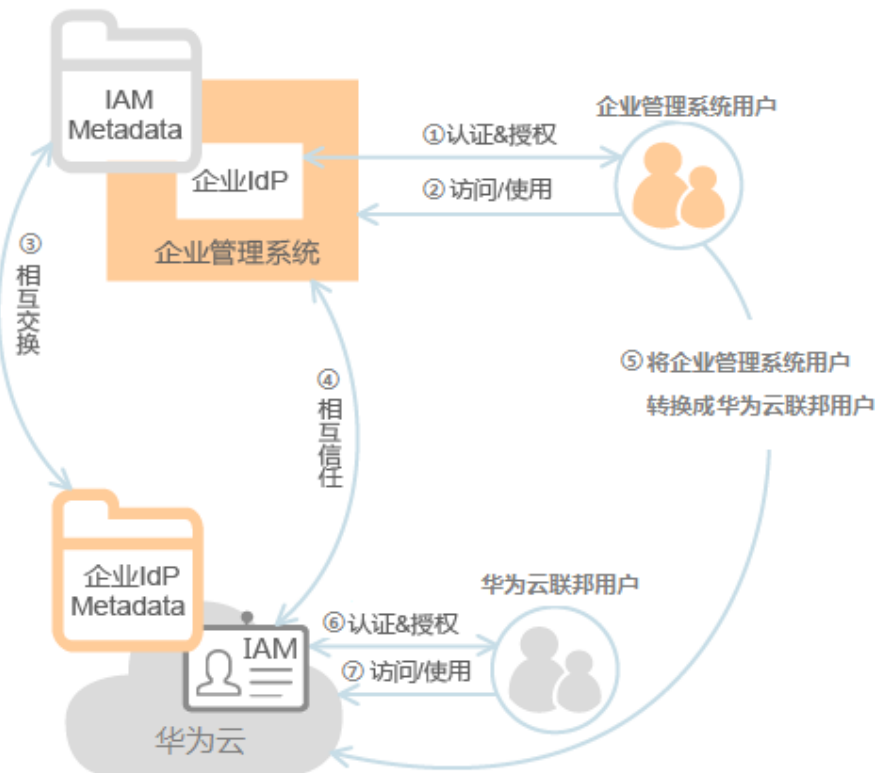
图 9-23 交换 Metadata 文件模型



2. **配置企业IdP**：配置企业IdP参数，规定在交互过程中，企业IdP向华为云发送哪些信息。

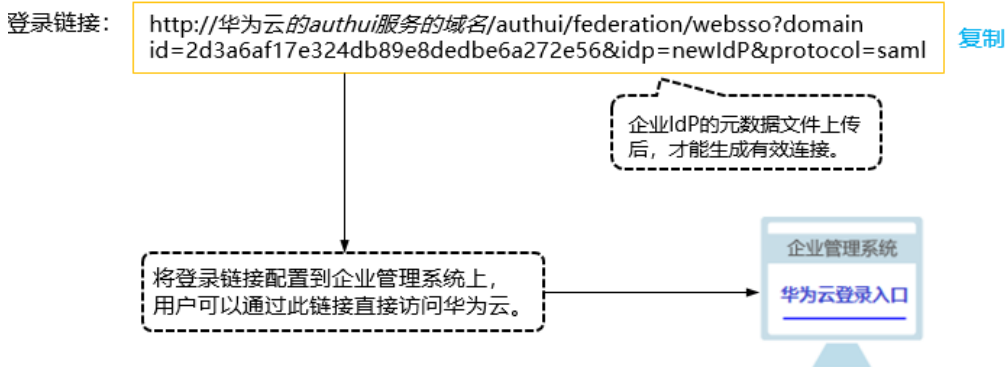
3. **配置外部身份ID**: 配置外部身份ID, 建立IAM用户与企业IdP用户的对应关系, 当企业IdP用户使用IAM用户SSO时, 会以指定外部身份ID的IAM用户身份登录华为云。例如, 企业用户"IdP_Test_User"的ID值与IAM用户“Alice”的外部身份ID一致, 则IdP_Test_User会以Alice的身份登录IAM。

图 9-24 用户转换模型



4. **登录验证**: 发起单点登录, 测试是否能成功从企业IdP跳转登录华为云。
5. **(可选) 配置企业管理系统登录入口**: 将华为云的访问入口配置到企业管理系统中, 用户可通过登录企业管理系统直接访问华为云, 如图9-25所示。

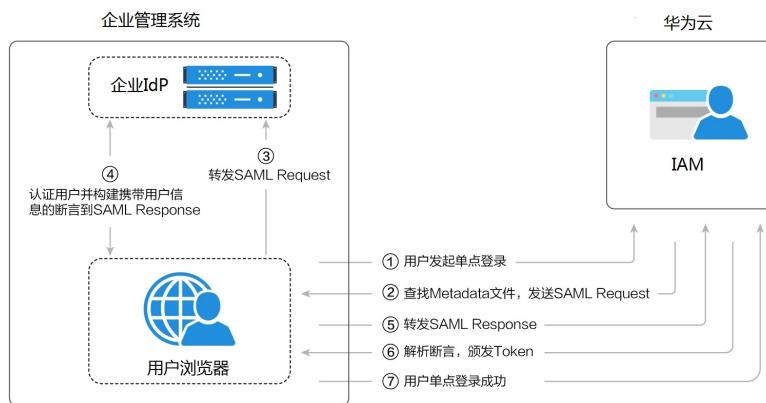
图 9-25 配置单点登录模型



企业管理系统与华为云联邦身份认证交互流程

图9-26为用户在发起单点登录请求后，企业管理系统与华为云间的交互流程。

图 9-26 联邦身份认证交互流程



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”。

从图9-26中可知，联邦身份认证的步骤为：

1. 用户在浏览器中打开创建身份提供商后生成的登录链接，浏览器向华为云发起单点登录请求。
2. 华为云根据登录链接中携带的信息，查找IAM身份提供商中对应的Metadata文件，构建SAML Request，发送给浏览器。
3. 浏览器收到请求后，转发SAML Request给企业IdP。
4. 用户在企业IdP推送的登录页面中输入用户名和密码，企业IdP对用户提供的身份信息验证，并构建携带用户信息的SAML断言，向浏览器发送SAML Response。
5. 浏览器响应后转发SAML Response给华为云。
6. 华为云从SAML Response中取出断言，并根据已配置的身份转换规则映射到具体的IAM用户组，颁发Token。
7. 用户完成单点登录，访问华为云。

说明

断言中要携带签名，否则会导致登录失败。

9.4.2 步骤 1：创建身份提供商

配置联邦身份认证，需要在企业IdP上传华为云的元数据文件（Metadata文件），并在IAM控制台上创建身份提供商、上传企业IdP的元数据文件，来建立两个系统之间的互信关系。

建立企业 IdP 对华为云的信任关系

在企业IdP中配置华为云的元数据文件，以建立企业IdP对华为云的信任。

步骤1 下载华为云系统的元数据文件（metadata文件）。

访问网址：<https://auth-intl.huaweicloud.com/authui/saml/metadata.xml>（推荐使用Chrome浏览器）。下载华为云元数据文件，并设置文件名称，例如“SP-metadata.xml”。

步骤2 将上述文件上传到企业IdP服务器上。上传方法请参见企业IdP的帮助文档。

步骤3 获取企业IdP的元数据文件。获取方法请参见企业IdP的帮助文档。

----结束

在华为云上创建身份提供商

在IAM控制台上创建身份提供商，配置身份提供商的元数据文件后，可以在IAM中建立对企业IdP的信任关系，使得企业用户可以直接访问华为云。

步骤1 进入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”。

图 9-27 创建身份提供商



步骤2 在“创建身份提供商”窗口中设置名称、协议、类型、状态、描述。

图 9-28 填写身份提供商参数

表 9-6 身份提供商基本参数

参数	含义
名称	身份提供商的名称。身份提供商名称在全局范围内不能重复，建议以域名唯一标识命名。
协议	身份提供商协议。当前华为云支持基于SAML、OIDC的身份提供商，如需创建基于OIDC协议的联邦身份认证，请参考 基于OIDC协议的虚拟用户SSO 。
类型	身份提供商类型。一个账号下只能存在一种类型的身份提供商。本章介绍IAM用户SSO，此处选择IAM用户SSO。 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 。
状态	身份提供商的状态。默认设置为“启用”。

步骤3 单击“确定”，创建身份提供商成功。

----结束

在华为云配置元数据文件

配置元数据文件，即把企业IdP的Metadata文件配置到华为云。IAM支持“上传文件”和“手动编辑”两种配置，选择其中一种即可。如果元数据文件超过500KB，请通过“手动编辑”配置元数据。如果后续元数据有更新，需要用户重新上传或者编辑元数据，否则会影响联邦用户登录华为云。

说明

企业IdP的Metadata文件获取方法请参考企业IdP提供商的帮助文档。

- 上传元数据：

- 单击身份提供商列表中“操作”列的“修改”。

图 9-29 修改身份提供商



- 单击“上传文件”左侧的“添加文件”，选择获取的企业IdP的元数据文件。

图 9-30 上传元数据文件

元数据配置

系统将从您上传的文件中提取元数据信息，请上传500KB以内的文件，超过500KB的文件请您[手动编辑](#)元数据信息。



- c. 单击“上传文件”。弹出页面显示系统提取到的元数据，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”，保存设置信息。
- **手动编辑元数据**
 - a. 单击“手动编辑”。

图 9-31 手动编辑元数据

元数据配置

系统将从您上传的文件中提取元数据信息，请上传500KB以内的文件，超过500KB的文件请您[手动编辑](#)元数据信息。



- b. 在“手动编辑元数据”页面中，输入从企业IdP元数据文件中获取的“Entity ID”、“签名证书”和“SingleSignInService”等参数。

参数	是否必选	含义
Entity ID	是	对应IdP元数据文件中“entityID”的值。 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	是	企业IdP与服务提供商之间，通过SAML协议完成联邦身份认证。 不需要手动选择，系统自动生成。
支持的NameIdFormat	否	对应IdP元数据文件中“NameIdFormat”的值。 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。 支持配置多个，华为云默认使用第一个。

参数	是否必选	含义
签名证书	是	<p>对应IdP元数据文件中“<X509Certificate>”的值。</p> <p>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。IAM通过元数据文件中的签名证书来确认联邦身份认证过程中断言消息的可信性、完整性。</p> <p>支持配置多个，华为云默认使用第一个。</p>
SingleSignOnService	是	<p>对应IdP元数据文件中“SingleSignOnService”的值。</p> <p>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。</p> <p>支持配置多个，华为云默认使用第一个。</p>
SingleLogoutService	否	<p>对应IdP元数据文件中“SingleLogoutService”的值。</p> <p>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。</p> <p>“SingleLogoutService”需要支持HTTP Redirect或HTTP POST方式。</p> <p>支持配置多个，华为云默认使用第一个。</p>

示例：以下为某企业IdP的元数据文件和手动编辑元数据信息时需要填入的内容。

图 9-32 某企业 IdP 的元数据文件

```
<md:EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Name="urn:keycloak">
  <md:EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="http://localhost:8080/auth/realms/master">
    <md:IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <md:KeyDescriptor use="signing">
        <ds:KeyInfo>
          <ds:KeyName>
            <ds:KeyName>
              <ds:X509Data>
                <ds:X509Certificate>
                  <!-- Certificate content -->
                </ds:X509Data>
              </ds:KeyName>
            </ds:KeyName>
          </ds:KeyInfo>
        </md:KeyDescriptor>
      </md:IDPSSODescriptor>
    </md:EntityDescriptor>
  </md:EntitiesDescriptor>
```


图 9-33 根据企业 IdP 元数据文件手动编辑元数据

c. 单击“确定”，保存设置信息。

9.4.3 步骤 2：配置企业 IdP

您可以在企业 IdP 中配置单点登录相关参数，决定向华为云提供哪些用户信息。企业 IdP 与华为云交互过程中，需要将企业 IdP 用户的相关信息发送给华为云，华为云会结合接收到的信息，确定联邦用户的身份和权限。

说明

IAM 用户 SSO 类型的单点登录，企业 IdP 必须要配置 IAM_SAML_Attributes_xUserId 断言。

常用的企业 IdP 配置参数

表 9-7 常用的企业 IdP 配置参数

参数名	描述	适用场景
IAM_SAML_Attributes_xUserId	选择 IAM 用户 SSO 时，企业 IdP 用户的 ID 值。	使用 IAM SSO 时，必须配置此参数。企业 IdP 用户与华为云 IAM 用户一一对应，企业 IdP 用户的 IAM_SAML_Attributes_xUserId 值，与对应 IAM 用户的外部身份 ID 相同。
IAM_SAML_Attributes_reldirect_url	指定联邦登录重定向的目标网址	用户在 SSO 登录过程中，希望跳转到华为云控制台的指定页面。例如指定跳转到香港局点，云监控服务 CES 主页。

参数名	描述	适用场景
IAM_SAML_Attributes_domain_id	与企业IdP建立联邦认证的华为账号或华为云账号ID值	从企业IdP侧发起联邦认证登录，必须在企业IdP侧配置该参数。
IAM_SAML_Attributes_idp_id	与企业IdP建立联邦认证的华为账号或华为云账号中，创建的身份提供商名称	从企业IdP侧发起联邦认证登录，必须在企业IdP侧配置该参数。

9.4.4 步骤 3：配置外部身份 ID

IAM用户SSO类型的单点登录，华为云必须要为企业IdP用户对应的IAM用户配置外部身份ID。外部身份ID值要与企业IdP的IAM_SAML_Attributes_xUserId保持一致。您可以在IAM用户创建时配置外部身份ID，或者直接修改现有IAM用户的外部身份ID：

- [创建IAM用户并设置外部身份ID](#)
- [修改现有IAM用户的外部身份ID](#)

创建 IAM 用户并设置外部身份 ID

- 步骤1** 管理员登录IAM控制台。
- 步骤2** 在统一身份认证服务，左侧导航窗格中，选择“用户”，单击右上方的“创建用户”。
- 步骤3** 在“创建用户”页面配置IAM“用户信息>外部身份ID”。其他创建IAM用户详情参见[创建IAM用户](#)。

图 9-34 创建 IAM 用户



----结束

修改现有 IAM 用户的外部身份 ID

管理员在IAM用户列表中，单击用户名，或者单击右侧的“安全设置”，可以查看或修改IAM用户外部身份ID。

图 9-35 修改 IAM 用户外部身份 ID



9.4.5 步骤 4：登录验证

登录验证

按照登录请求发起方可将联邦用户登录方式分为两类：

- Idp侧登录：用户从IdP侧（企业自己的身份提供商侧）发起登录请求，例如从 Microsoft Active Directory（AD FS）、Shibboleth侧发起登录华为云控制台的请求。
- SP侧登录：用户从SP侧（服务提供商侧）发起登录请求，在企业与华为云联邦身份认证的过程中，服务提供商指华为云，SP侧登录链接可在IAM控制台身份提供商详情页面获取。

不同的企业IdP发起Idp侧登录的方式差异较大，华为云帮助文档不做详述，具体操作请参考企业IdP的帮助文档。本节重点介绍SP侧发起登录的方法：

步骤1 联邦用户登录。

在控制台的“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。

图 9-36 登录链接



步骤2 查看联邦用户是否跳转至实体IAM用户。

----结束

跳转到指定区域或服务

如需指定联邦用户登录的目标页面，比如联邦用户登录时，指定跳转到香港局点，云监控服务CES主页。有以下两种配置方式：

- SP侧登录配置方法

拼接控制台获取的登录链接与指定url，拼接格式为“**登录链接&service=指定url**”。例如：获取的登录地址为https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml，指定跳转的控制台地址为<https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1>，按照拼接格式拼接得到的登录链接为：https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml&service=<https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1>。

- IdP侧登录配置方法

在企业IdP的SAML断言中配置IAM_SAML_Attributes_redirect_url声明，声明值为指定跳转的目标URL。

9.4.6（可选）步骤 5：配置企业管理系统登录入口

将身份提供商的登录链接配置到企业管理系统上，企业用户通过该链接访问华为云。

📖 说明

华为云提供“企业联邦用户登录”入口，如您未配置企业管理系统登录入口，企业联邦用户可以通过该方法登录华为云，详情请参考：[企业联邦用户登录](#)。

前提条件

- 已在华为云创建身份提供商，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](#)。
- 企业管理系统界面已创建华为云登录入口。

操作步骤

步骤1 在IAM控制台的左侧导航窗格中，单击“身份提供商”。

步骤2 单击目标身份提供商列表右侧的“查看”。

图 9-37 查看身份提供商详情



步骤3 单击“登录链接”右侧的“🔗”。

图 9-38 复制登录链接



步骤4 将以下语句添加在企业管理系统页面文件中。

```
<a href="<登录链接">"> 华为云登录入口 </a>
```

步骤5 用户登录企业管理系统后通过单击“华为云登录入口”可以直接访问华为云。

----结束

9.5 基于 OIDC 协议的虚拟用户 SSO

9.5.1 联邦身份认证配置概述

本章为您介绍基于OIDC协议的企业IdP与华为云进行联邦身份认证的内部实现流程和配置步骤。

联邦身份认证的配置步骤

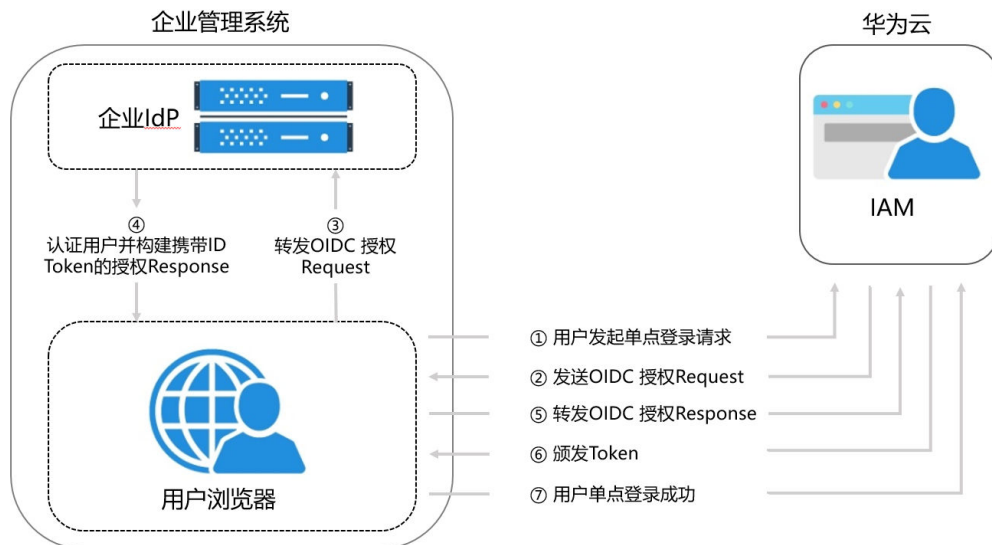
建立企业管理系统与华为云的联邦身份认证关系，需要完成以下配置步骤。

1. **创建身份提供商并创建互信关系**：在企业IdP中创建OAuth 2.0凭据，在华为云平台创建身份提供商并配置授权信息，从而建立企业管理系统和华为云平台的信任关系。
2. **配置身份转换规则**：通过在华为云平台配置身份转换规则，将IdP中的用户、用户组及其访问权限映射到华为云平台。
3. **配置企业管理系统登录入口**：将华为云平台的访问入口配置到企业管理系统中，用户可通过登录企业管理系统直接访问华为云平台。

企业管理系统与华为云联邦身份认证交互流程

图9-39为用户在发起单点登录请求后，企业管理系统与华为云间的交互流程。

图 9-39 联邦身份认证交互流程



从上图中可知，联邦身份认证的步骤为：

1. 用户在浏览器中打开从IAM上获取到的登录链接，浏览器向华为云发起单点登录请求。
2. 华为云根据登录链接中携带的信息，查找IAM身份提供商中对应的配置信息，构建OIDC授权Request，发送给浏览器。
3. 浏览器收到请求后，转发OIDC授权Request给企业IdP。
4. 用户在企业IdP推送的登录页面中输入用户名和密码，企业IdP对用户提供的身份信息验证，并构建携带用户信息的ID Token，向浏览器发送OIDC授权Response。
5. 浏览器响应后转发OIDC授权Response给华为云。
6. 华为云从OIDC授权Response中取出ID Token，并根据已配置的身份转换规则映射到具体的IAM用户组，颁发Token。
7. 用户完成单点登录，访问华为云。

9.5.2 步骤 1：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。

步骤1 进入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”。

图 9-40 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 9-41 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 9-42 修改身份提供商



步骤2 在修改身份提供商页面，选择“访问方式”。

图 9-43 访问方式



表 9-8 访问方式

访问方式	说明
编程访问和管理控制台访问	<ul style="list-style-type: none"> 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。 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。 如果您需要使用SSO方式访问华为云，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。

步骤3 在修改身份提供商页面，填写“配置信息”。

表 9-9 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： <i>https://{base URL}/.well-known/openid-configuration</i> ，其中 <i>base URL</i> 由企业IdP定义，如Google提供的Openid-configuration为 <i>https://accounts.google.com/.well-known/openid-configuration</i> 。
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： <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • form_post：选择form_post模式时，请在身份提供商侧将redirect url配置为：<i>https://auth.huaweicloud.com/authui/oidc/post</i>。 • fragment：选择fragment模式时，请在身份提供商侧将redirect url配置为：<i>https://auth.huaweicloud.com/authui/oidc/redirect</i>。 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。

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 9-44 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。

- 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，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：[步骤2：配置身份转换规则](#)。

----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。

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操作权限。身份转换规则详情请参见：[步骤2：配置身份转换规则](#)。
- 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登录入口直接访问华为云，方法请参考：[（可选）步骤3：配置企业管理系统登录入口](#)。

9.5.3 步骤 2：配置身份转换规则

在IAM上创建身份提供商后，联邦用户在华为云中的用户名默认为“FederationUser”，且联邦用户仅能访问华为云，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中显示不同的用户名。
- 赋予企业管理系统用户使用华为云资源的权限。由于华为云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 9-45 创建规则-1

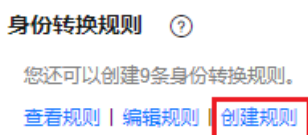


图 9-46 创建规则-2

创建规则

用户名

用户组

本规则生效条件

您还可以新建9条本规则生效条件。

属性	条件	值	操作
<input type="text" value="_NAMEID_"/>	<input type="text" value="any_one_of"/>	<input type="text" value="多个值以半角分号分隔。"/>	删除

[+ 新建](#)

[确定](#) [取消](#)

表 9-10 参数说明

参数名	描述	说明
用户名	联邦用户在华为云中显示的用户名，以下简称“联邦用户名”。	为了区分华为云的用户与联邦用户，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 <ul style="list-style-type: none"> 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。一个身份转换规则最多可以创建10条生效条件。 说明 <ul style="list-style-type: none"> 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。

示例：为企业管理系统管理员设定规则。

- 用户名：FederationUser-IIdP_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的用户在华为云中映射的IAM用户名为 FederationUser-IIdP_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，进入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 9-47 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

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](#)。

9.5.4（可选）步骤 3：配置企业管理系统登录入口

将身份提供商的登录链接配置到企业管理系统上，企业用户通过该链接访问华为云。

说明

华为云提供企业联邦用户登录入口，如您未配置企业管理系统登录入口，企业联邦用户可以通过该方法登录华为云，详情请参考：[企业联邦用户登录](#)。

前提条件

- 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](#)。
- 企业管理系统界面已创建华为云登录入口。

操作步骤

步骤1 在IAM控制台的左侧导航窗格中，单击“身份提供商”。

步骤2 单击目标身份提供商列表右侧的“查看”。

图 9-48 查看身份提供商详情



步骤3 单击“登录链接”右侧的“📄”。

图 9-49 复制登录链接



步骤4 将以下语句添加在企业管理系统页面文件中。

```
<a href="<登录链接>"> 华为云登录入口 </a>
```

步骤5 用户登录企业管理系统后通过单击“华为云登录入口”可以直接访问华为云。

----结束

9.6 身份转换规则详细说明

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

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

参数说明：

- local：表示联邦用户映射到IAM中的身份信息。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。
- 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：联邦用户映射到IAM时，身份转换规则的生效条件。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。

须知

映射到IAM中的用户身份信息只能包含：大小写字母、空格、数字或特殊字符（-_.）且不能以数字开头。

empty 条件示例

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

- 以下示例表示联邦用户在IAM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*Group*，*Group*属性的值只能有一个。

```
[
  {
```

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

假设传入以下断言，则联邦用户在IAM中的用户名为John Smith，John Smith在IAM中只属于“admin”用户组。（为了方便理解，简化了断言的结构，之后的示例也将做类似的简化，不再重复提示）

```
{FirstName: John}
{LastName: Smith}
{Group: admin}
```

- 如果联邦用户需要在IAM中属于多个用户组，身份转换规则如下所示。
以下示例表示联邦用户在IAM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`。

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

假设传入以下断言，则联邦用户在系统中的用户名为John Smith，John Smith属于“admin”和“manager”用户组。


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

any one of、not any of 条件示例

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。

- 以下示例表示联邦用户在IAM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。

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

- 如果联邦用户需要在IAM中属于多个用户组，身份转换规则如下所示。

以下示例表示联邦用户在IAM中的用户名为“remote”的第一个属性，即*UserName*。所属用户组为“admin”和“manager”。该规则仅对在IdP中属于“idp_admin”用户组的用户生效。

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

```
    "type": "UserName"
  },
  {
    "type": "Groups",
    "any_one_of": [
      "idp_admin"
    ]
  }
]
}
```

- 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华为云。

```
{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访问华为云。

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

含有正则表达式的条件示例

您可以在条件里指定一个“`regex: true`”用来表示华为云将以正则匹配的方式来计算结果。

以下示例表示该规则对在IdP中用户组名以任意值开头，“@mail.com”结尾的用户生效，在IAM中的用户名为*UserName*，所属用户组为“admin”。

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

条件组合示例

多个条件间，以“逻辑与”的方式组合。

以下示例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IAM中的用户名为*UserName*，所属用户组为“admin”。

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

以上规则等同于：

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

多个规则组合示例

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，否则华为云不允许此用户登录；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。

以下示例表示针对IdP中属于“idp_admin”用户组的用户生效，在IAM中的用户名为*UserName*，所属用户组为“admin”。

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

10 自定义身份代理

10.1 使用委托方式配置自定义身份代理配置步骤

如果您的企业IdP不支持SAML、OIDC协议，可以使用自定义身份代理，通过编写代码获得华为云登录链接，使企业用户通过企业IdP验证身份后，即可登录华为云。

📖 说明

自定义身份代理适用于不支持SAML、OIDC的企业IdP，如果您使用了支持SAML、OIDC的IdP（身份提供商），推荐您通过配置[联邦身份认证](#)实现用户使用企业管理系统账号单点登录华为云。

前提条件

- 企业已有企业管理系统。
- 企业管理员在华为云上注册了可用的账号（账号名以DomainA为例），并已在IAM中创建用户组（用户组名以GroupC为例）并授予Agent Operator权限，具体方法请参见：[创建用户组并授权](#)。

操作步骤

步骤1 在DomainA中创建IAM用户（用户名以UserB为例），并加入GroupC用户组中，具体方法请参见：[用户组添加用户](#)。

📖 说明

请确认该IAM用户支持[编程访问](#)华为云服务。如需修改IAM用户访问方式，请参考：[查看或修改IAM用户信息](#)。

步骤2 将UserB的[访问密钥](#)或用户名和密码（推荐使用访问密钥）配置到企业IdP的配置文件中，以便获取用户认证token和调用API。为了保障您的账号安全，密码和访问密钥建议加密存储。

步骤3 在IAM控制台左侧导航栏选择“委托”，单击右上方的“创建委托”。

步骤4 在创建委托页面，设置委托参数。

“委托名称”以“testagency”为例，“委托类型”必须选择“普通账号”，“委托的账号”填写“DomainA”，“持续时间”根据具体情况选择，并单击“下一步”。

图 10-1 创建委托

委托 / 创建委托

* 委托名称

* 委托类型 普通账号
将账号内资源的操作权限委托给其他华为云账号。
 云服务
将账号内资源的操作权限委托给华为云服务。

* 委托的账号

* 持续时间

描述

0/255

下一步 取消

步骤5 选择权限的作用范围，勾选需要授予委托的权限，给委托授权。

步骤6 在企业IdP创建用户组“testagency”（与**步骤4**中的委托名称相同），将企业本地用户按需加入本地用户组，授予其自定义代理登录华为云时所需权限，具体方法请参见企业IdP帮助文档。

步骤7 企业本地用户登录企业管理系统后，访问企业IdP的自定义代理，从委托列表（由安全管理员来查询租户的委托列表，根用户默认为安全管理员）中选择所需要使用的委托，具体方法请参见企业管理系统帮助文档。

📖 说明

自定义代理的委托列表是企业IdP创建的用户组名称与华为云创建的委托名称的交集。

步骤8 企业IdP自定义代理根据委托，携带IAM用户userB的token调用API（POST /v3.0/OS-CREDENTIAL/securitytokens），获取具有临时身份的securityToken，调用方法请参见：[通过委托获取临时AK/SK和securitytoken](#)。

📖 说明

通过委托获取securitytoken时，请求体中必须填写session_user.name参数。

步骤9 企业IdP自定义代理携带获取到的临时AK/SK和securitytoken通过全局域名（iam.myhuaweicloud.com）调用API（POST /v3.0/OS-AUTH/securitytoken/logintokens）获取登录票据loginToken。登录票据位于Response Header中的X-Subject-LoginToken。获取方式请参见：[获取自定义代理登录票据](#)。

📖 说明

- 调用API (POST /v3.0/OS-AUTH/securitytoken/logintokens) 获取登录票据loginToken时，需要使用全局域名： iam.myhuaweicloud.com。
- logintoken是系统颁发给自定义代理用户的登录票据，承载用户的身份、session等信息，默认有效期为10分钟。调用FederationProxyUrl登录云服务控制台时，需要使用logintoken进行认证。
- 调用API (POST /v3.0/OS-AUTH/securitytoken/logintokens) 时可以设置logintoken的有效时间，有效时间设置范围为10分钟~12小时。如果传入的值大于临时安全凭证securitytoken剩余的过期时间，则使用临时安全凭证securitytoken剩余的过期时间。

步骤10 企业IdP自定义代理根据规范创建云服务登录地址FederationProxyUrl，作为Location返回给浏览器。FederationProxyUrl如下：

```
https://auth.huaweicloud.com/authui/federation/login?
idp_login_url={enterprise_system_loginURL}&service={console_service_region_url}&
logintoken={logintoken}
```

示例：

```
https://auth.huaweicloud.com/authui/federation/login?idp_login_url=https%3A%2F%2Fexample.com&service=https%3a%2f%2fconsole.huaweicloud.com%2fapm%2f%3fregion%3dcn-north-4%23%2fapm%2fatps%2ftopology&logintoken=*****
```

表 10-1 参数说明

参数	说明
idp_login_url	企业管理系统登录地址。
service	需要访问的华为云服务地址。
logintoken	自定义代理登录票据。

为了浏览器正常识别参数内容，需要将以上三个参数都进行UrlEncode编码。

您可以参考以下Demo示例创建云服务登录地址FederationProxyUrl：[使用委托方式创建云服务登录地址](#)

📖 说明

该FederationProxyUrl包含从IAM获得的登录票据，票据用于对访问的用户进行身份验证。FederationProxyUrl需要经过UrlEncode编码。

步骤11 华为云认证登录票据loginToken成功后，浏览器自动重定向到需要访问的华为云服务地址，即云服务代理登录地址中**service**设定的地址，企业用户成功访问华为云的控制台。

loginToken认证失败，则重定向到**idp_login_url**设定的地址。

----结束

10.2 使用委托方式创建云服务登录地址

该章节提供使用委托方式创建登录华为云云服务的联邦代理登录地址的示例代码。

Java 示例代码

以下示例说明了如何使用java编程的方式创建云服务登录地址FederationProxyUrl。

```
import java.net.*;
import java.util.Collections;
import com.huaweicloud.sdk.core.auth.GlobalCredentials;
import com.huaweicloud.sdk.core.exception.ClientRequestException;
import com.huaweicloud.sdk.core.exception.ServerResponseException;
import com.huaweicloud.sdk.core.http.HttpConfig;
import com.huaweicloud.sdk.iam.v3.IamClient;
import com.huaweicloud.sdk.iam.v3.model.*;

// 使用全局域名获取自定义代理登录票据
String endpoint = "https://iam.myhuaweicloud.com";

// 配置客户端属性
HttpConfig config = HttpConfig.getDefaultHttpConfig()
    .withIgnoreSSLVerification(true)
    .withProxyHost("proxy.huawei.com")
    .withProxyPort(8080);

// 使用IAM userB的domainID/ak/sk,初始化指定IAM客户端 {Service}Client,用户B的创建方式见“创建IAM用户”章节
IamClient iamClient = IamClient.newBuilder().withCredential(new GlobalCredentials()
    .withDomainId("domainId")
    .withAk("ak")
    .withSk("sk"))
    .withEndpoint(endpoint)
    .withHttpConfig(config)
    .build();

/*CreateTemporaryAccessKeyByAgency
调用通过委托获取临时访问密钥和securitytoken接口获取具有临时身份的访问密钥和securityToken。
访问密钥和securitytoken的默认有效期为900秒，即15分钟，取值范围为15分钟-24小时，这里设置有效期为3600秒，即一小时。
注意：下一步获取自定义代理登录票据logintoken时，如果您设置了有效期，则有效期不能大于这里获取的securitytoken的剩余有效时间。
*/
IdentityAssumerole identityAssumerole = new IdentityAssumerole().
    withAgencyName("testagency").withDomainId("0525e2c87exxxxxx").withSessionUser(new
AssumeroleSessionuser().withName("ExternalUser").withDurationSeconds(3600);
AgencyAuth agencyAuth = new AgencyAuth().withIdentity(new
AgencyAuthIdentity().withAssumeRole(identityAssumerole).

withMethods(Collections.singletonList(AgencyAuthIdentity.MethodEnum.fromValue("assume_role"))));
CreateTemporaryAccessKeyByAgencyRequestBody createTemporaryAccessKeyByAgencyRequestBody = new
CreateTemporaryAccessKeyByAgencyRequestBody().withAuth(agencyAuth);
CreateTemporaryAccessKeyByAgencyResponse createTemporaryAccessKeyByAgencyResponse =
iamClient.createTemporaryAccessKeyByAgency(new
CreateTemporaryAccessKeyByAgencyRequest().withBody(createTemporaryAccessKeyByAgencyRequestBody));
Credential credential = createTemporaryAccessKeyByAgencyResponse.getCredential();

/*CreateLoginToken
获取自定义代理登录票据logintoken。
logintoken是系统颁发给自定义代理用户的登录票据，承载用户的身份、session等信息。
调用自定义代理URL登录云服务控制台时，可以使用本接口获取的logintoken进行认证。
自定义代理登录票据logintoken的有效期默认为600秒，即10分钟，取值范围为10分钟-12小时，这里设置为1800秒，即半小时。
注意：自定义代理登录票据logintoken的有效期不能大于上一步获取的securitytoken的剩余有效时间。
通过委托获取securitytoken时，请求体中必须填写session_user.name参数。
*/
CreateLoginTokenRequestBody createLoginTokenRequestBody = new CreateLoginTokenRequestBody().
    withAuth(new LoginTokenAuth().withSecurityToken(new LoginTokenSecurityToken().
        withAccess(credential.getAccess()).
        withId(credential.getSecurityToken()).
        withSecret(credential.getSecret()).withDurationSeconds(1800)));
CreateLoginTokenResponse createLoginTokenResponse = iamClient.createLoginToken(new
```



```
CreateLoginTokenRequest().withBody(createLoginTokenRequestBody));
String loginToken = createLoginTokenResponse.getXSubjectLoginToken();

//自定义代理登录地址
String authURL = "https://auth.huaweicloud.com/authui/federation/login";
//企业管理系统登录地址
String enterpriseSystemLoginURL = "https://example.com/";
//需要访问的华为云服务地址
String targetConsoleURL = "https://console.huaweicloud.com/iam/?region=cn-north-4";

//创建云服务登录地址FederationProxyUrl, 作为Location返回给浏览器
String FederationProxyUrl = authURL + "?idp_login_url=" +
    URLEncoder.encode(enterpriseSystemLoginURL, "UTF-8") +
    "&service=" + URLEncoder.encode(targetConsoleURL, "UTF-8") +
    "&logintoken=" + URLEncoder.encode(loginToken, "UTF-8");
```

Python 示例代码

以下示例说明了如何使用Python编程的方式创建云服务登录地址 FederationProxyUrl。

```
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.http.http_config import HttpConfig
from huaweicloudsdkiam.v3 import *

import urllib

# 使用全局域名获取自定义代理登录票据
endpoint = "https://iam.myhuaweicloud.com"

# 配置客户端属性
config = HttpConfig.get_default_config()
config.ignore_ssl_verification = True
config.proxy_protocol = "https"
config.proxy_host = "proxy.huawei.com"
config.proxy_port = 8080
credentials = GlobalCredentials(ak, sk, domain_id)

# 使用IAM userB的domainID/ak/sk,初始化指定IAM客户端 {Service}Client,用户B的创建方式见“创建IAM用户”章节
client = iamClient().new_builder(IamClient) \
    .with_http_config(config) \
    .with_credentials(credentials) \
    .with_endpoint(endpoint) \
    .build()

# CreateTemporaryAccessKeyByAgency
# 调用通过委托获取临时访问密钥和securitytoken接口获取具有临时身份的访问密钥和securityToken
# 访问密钥和securitytoken的默认有效期为900秒,即15分钟,取值范围为15分钟-24小时,这里设置有效期为3600秒,即一小时。
# 注意: 下一步获取自定义代理登录票据logintoken时,如果您设置了有效期,则有效期不能大于这里获取的securitytoken的剩余有效时间。
# 通过委托获取securitytoken时,请求体中必须填写session_user.name参数。
assume_role_session_user = AssumeroleSessionuser(name="ExternalUser")
identity_assume_role = IdentityAssumerole(agency_name="testagency",
    domain_id="0525e2c87exxxxxx",
    session_user=assume_role_session_user,
    duration_seconds=3600)
identity_methods = ["assume_role"]
body = CreateTemporaryAccessKeyByAgencyRequestBody(
    AgencyAuth(AgencyAuthIdentity(methods=identity_methods, assume_role=identity_assume_role)))
request = CreateTemporaryAccessKeyByAgencyRequest(body)
create_temporary_access_key_by_agency_response = client.create_temporary_access_key_by_agency(request)
credential = create_temporary_access_key_by_agency_response.credential

# CreateLoginToken
# 获取自定义代理登录票据logintoken。
# 自定义代理登录票据logintoken的有效期默认为600秒,即10分钟,取值范围为10分钟-12小时,这里设置为
```

```
1800秒，即半小时。
# 注意：自定义代理登录票据logintoken的有效期不能大于上一步获取的securitytoken的剩余有效时间。
login_token_security_token = LoginTokenSecurityToken(access=credential.access, secret=credential.secret,
    id=credential.securitytoken, duration_seconds=1800)
body = CreateLoginTokenRequestBody(LoginTokenAuth(login_token_security_token))
request = CreateLoginTokenRequest(body)
create_login_token_response = client.create_login_token(request)
login_token = create_login_token_response.x_subject_login_token

# 获取自定义代理登录票据URL
auth_URL = "https://auth.huaweicloud.com/authui/federation/login"
# 企业管理系统登录地址
enterprise_system_login_URL = "https://example.com/"
# 需要访问的华为云服务地址
target_console_URL = "https://console.huaweicloud.com/iam/?region=cn-north-4"

# 创建云服务登录地址FederationProxyUrl，作为Location返回给浏览器。
FederationProxyUrl = auth_URL + "?idp_login_url=" + urllib.parse.quote(
    enterprise_system_login_URL) + "&service=" + urllib.parse.quote(
    target_console_URL) + "&logintoken=" + urllib.parse.quote(login_token)
print(FederationProxyUrl)
```

10.3 使用 token 方式配置自定义身份代理配置步骤

如果您的企业IdP不支持SAML、OIDC协议，可以使用自定义身份代理，通过编写代码获得华为云登录链接，使企业用户通过企业IdP验证身份后，即可登录华为云。

📖 说明

自定义身份代理适用于不支持SAML、OIDC的企业IdP，如果您使用了支持SAML、OIDC的IdP（身份提供商），推荐您通过配置[联邦身份认证](#)实现用户使用企业管理系统账号单点登录华为云。

前提条件

- 企业已有企业管理系统。
- 企业管理员在华为云上注册了可用的账号（账号名以DomainA为例）。

操作步骤

- 步骤1** 在DomainA中创建IAM用户（用户名以UserB为例），具体方法请参见：[创建IAM用户](#)。
- 步骤2** （可选）将用户UserB加入用户组中（用户组名以GroupC为例），并为用户组授予必要的权限，具体方法请参见：[创建用户组并授权](#)
- 步骤3** 将UserB的[访问密钥](#)或用户名和密码（推荐使用访问密钥）配置到企业IdP的配置文件中，以便获取用户认证token。为了保障您的账号安全，密码和访问密钥建议加密存储。
- 步骤4** 企业管理员登录企业管理系统后，访问自定义代理，从用户列表中选择需要登录华为云的企业用户，具体操作请参见企业管理系统帮助文档。此处以企业管理员选择2中配置的用户UserB为例。

📖 说明

自定义代理的用户列表是在华为账号下的IAM用户列表，将IAM用户的[访问密钥](#)或用户名和密码（推荐使用访问密钥）配置到企业IdP的配置文件中，即可将这些用户按需赋予不同企业用户。

步骤5 企业IdP自定义代理携带IAM用户UserB的token调用API (POST /v3.0/OS-CREDENTIAL/securitytokens)，获取临时访问密钥和securityToken，调用方法请参见：[通过token获取临时访问密钥和securitytoken](#)。

步骤6 企业IdP自定义代理携带获取到的临时访问密钥和securitytoken通过全局域名 (iam.myhuaweicloud.com)调用API (POST /v3.0/OS-AUTH/securitytoken/logintokens)获取登录票据loginToken。登录票据位于Response Header中的X-Subject-LoginToken。获取方式请参见：[获取自定义代理登录票据](#)。

 **说明**

- 调用API (POST /v3.0/OS-AUTH/securitytoken/logintokens)获取登录票据loginToken时，需要使用全局域名：iam.myhuaweicloud.com。
- logintoken是系统颁发给自定义代理用户的登录票据，承载用户的身份、session等信息，默认有效期为10分钟。
- 调用API (POST /v3.0/OS-AUTH/securitytoken/logintokens)时可以设置logintoken的有效时间，有效时间设置范围为10分钟~12小时。如果传入的值大于临时安全凭证securitytoken剩余的过期时间，则使用临时安全凭证securitytoken剩余的过期时间。

步骤7 企业IdP自定义代理根据如下规范创建云服务代理登录地址，并作为Location返回给浏览器：

```
https://auth.huaweicloud.com/authui/federation/login?
idp_login_url={enterprise_system_loginURL}&service={console_service_region_url}&logintoken={logintoken}
```

示例：

```
https://auth.huaweicloud.com/authui/federation/login?idp_login_url=https%3A%2F%2Fexample.com&service=https%3a%2f%2fconsole.huaweicloud.com%2fapm%2f%3fregion%3dcn-north-4%23%2fapm%2fatps%2ftopology&logintoken=*****
```

表 10-2 参数说明

参数	说明
idp_login_url	企业管理系统登录地址。
service	需要访问的华为云服务地址。
logintoken	自定义代理登录票据。

您可以参考以下Demo示例创建云服务登录地址：[使用token方式创建云服务登录地址](#)

 **说明**

云服务代理登录地址中包含从IAM获得的登录票据loginToken，loginToken用于对访问的用户进行身份验证。云服务代理登录地址中每个参数的值都需要经过UrlEncode编码。

步骤8 华为云认证登录票据loginToken成功后，浏览器自动重定向到需要访问的华为云服务地址，即云服务代理登录地址中service设定的地址，企业用户成功访问华为云的控制台。

loginToken认证失败，则重定向到idp_login_url设定的地址。

----**结束**

10.4 使用 token 方式创建云服务登录地址

该章节提供使用token方式创建登录华为云云服务的联邦代理登录地址的示例代码。

Java 示例代码

以下示例说明了如何使用java编程的方式创建云服务登录地址FederationProxyUrl。

```
import java.net.URLEncoder;
import java.util.Collections;
import com.huaweicloud.sdk.core.auth.GlobalCredentials;
import com.huaweicloud.sdk.core.http.HttpConfig;
import com.huaweicloud.sdk.core.exception.*;
import com.huaweicloud.sdk.iam.v3.IamClient;
import com.huaweicloud.sdk.iam.v3.model.*;

//使用全局域名获取自定义代理登录票据
String endpoint = "https://iam.myhuaweicloud.com";

//配置客户端属性
HttpConfig config = HttpConfig.getDefaultHttpConfig()
    .withIgnoreSSLVerification(true)
    .withProxyHost("proxy.huawei.com")
    .withProxyPort(8080);

// 使用IAM userB的domainID/ak/sk,初始化指定IAM客户端 {Service}Client,用户B的创建方式见“创建IAM用户”章节
IamClient iamClient = IamClient.newBuilder().withCredential(new GlobalCredentials()
    .withDomainId(domainId)
    .withAk(ak)
    .withSk(sk)
    .withEndpoint(endpoint)
    .withHttpConfig(config)
    .build());

/*CreateTemporaryAccessKeyByToken
调用通过token获取临时访问密钥和securitytoken接口获取具有临时身份的访问密钥和securitytoken。
访问密钥和securitytoken的默认有效期为900秒，即15分钟，取值范围为15分钟-24小时，这里设置有效期为3600秒，即一小时。
注意：下一步获取自定义代理登录票据logintoken时，如果您设置了有效期，则有效期不能大于这里获取的securitytoken的剩余有效时间。
*/
TokenAuthIdentity tokenAuthIdentity = new
TokenAuthIdentity().withMethods(Collections.singletonList(TokenAuthIdentity.MethodEnum.fromValue("token")));withToken(new IdentityToken().withDurationSeconds(3600));
CreateTemporaryAccessKeyByTokenRequestBody createTemporaryAccessKeyByTokenRequestBody = new
CreateTemporaryAccessKeyByTokenRequestBody().withAuth(new
TokenAuth().withIdentity(tokenAuthIdentity));
CreateTemporaryAccessKeyByTokenResponse createTemporaryAccessKeyByTokenResponse =
iamClient.createTemporaryAccessKeyByToken(new
CreateTemporaryAccessKeyByTokenRequest().withBody(createTemporaryAccessKeyByTokenRequestBody));
Credential credential = createTemporaryAccessKeyByTokenResponse.getCredential();

/*CreateLoginToken
获取自定义代理登录票据logintoken。
logintoken是系统颁发给自定义代理用户的登录票据，承载用户的身份、session等信息。
调用自定义代理URL登录云服务控制台时，可以使用本接口获取的logintoken进行认证。
自定义代理登录票据logintoken的有效期默认为600秒，即10分钟，取值范围为10分钟-12小时，这里设置为1800秒，即半小时。
注意：自定义代理登录票据logintoken的有效期不能大于上一步获取的securitytoken的剩余有效时间。
*/
CreateLoginTokenRequestBody createLoginTokenRequestBody = new CreateLoginTokenRequestBody().
withAuth(new LoginTokenAuth().withSecurityToken(new LoginTokenSecurityToken()).
withAccess(credential.getAccess()).
withId(credential.getSecurityToken()));
```

```
        withSecret(credential.getSecret()).withDurationSeconds(1800));
CreateLoginTokenResponse createLoginTokenResponse = iamClient.createLoginToken(new
CreateLoginTokenRequest().withBody(createLoginTokenRequestBody));
String loginToken = createLoginTokenResponse.getXSubjectLoginToken();

//获取自定义代理登录票据URL
String authURL = "https://auth.huaweicloud.com/authui/federation/login";
//企业管理系统登录地址
String enterpriseSystemLoginURL = "https://example.com/";
//需要访问的华为云服务地址
String targetConsoleURL = "https://console.huaweicloud.com/iam/?region=cn-north-4";

//创建云服务登录地址FederationProxyUrl, 作为Location返回给浏览器。
String FederationProxyUrl = authURL + "?idp_login_url=" +
    URLEncoder.encode(enterpriseSystemLoginURL, "UTF-8") +
    "&service=" + URLEncoder.encode(targetConsoleURL, "UTF-8") +
    "&logintoken=" + URLEncoder.encode(loginToken, "UTF-8");
```

Python 示例代码

以下示例说明了如何使用Python编程的方式创建云服务登录地址 FederationProxyUrl。

```
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.http.http_config import HttpConfig
from huaweicloudskiam.v3 import *

import urllib

# 使用全局域名获取自定义代理登录票据
endpoint = "https://iam.myhuaweicloud.com"

# 配置客户端属性
config = HttpConfig.get_default_config()
config.ignore_ssl_verification = True
config.proxy_protocol = "https"
config.proxy_host = "proxy.huawei.com"
config.proxy_port = 8080
credentials = GlobalCredentials(ak, sk, domain_id)

# 使用IAM userB的domainID/ak/sk,初始化指定IAM客户端 {Service}Client,用户B的创建方式见“创建IAM用户”章节
client = iamClient().new_builder(iamClient) \
    .with_http_config(config) \
    .with_credentials(credentials) \
    .with_endpoint(endpoint) \
    .build()

# CreateTemporaryAccessKeyByToken
# 调用通过token获取临时访问密钥和securitytoken接口获取具有临时身份的访问密钥和securityToken
# 访问密钥和securitytoken的默认有效期为900秒,即15分钟,取值范围为15分钟-24小时,这里设置有效期为3600秒,即一小时。
# 注意: 下一步获取自定义代理登录票据logintoken时,如果您设置了有效期,则有效期不能大于这里获取的securitytoken的剩余有效时间。
identity_methods = ["token"]
identity_token = IdentityToken(duration_seconds=3600)
body = CreateTemporaryAccessKeyByTokenRequestBody(
    TokenAuth(TokenAuthIdentity(methods=identity_methods, token=identity_token)))
request = CreateTemporaryAccessKeyByTokenRequest(body)
create_temporary_access_key_by_token_response = client.create_temporary_access_key_by_token(request)
credential = create_temporary_access_key_by_token_response.credential

# CreateLoginToken
# 获取自定义代理登录票据logintoken。
# logintoken是系统颁发给自定义代理用户的登录票据,承载用户的身份、session等信息。
# 调用自定义代理URL登录云服务控制台时,可以使用本接口获取的logintoken进行认证。
# 自定义代理登录票据logintoken的有效期默认为600秒,即10分钟,取值范围为10分钟-12小时,这里设置为1800秒,即半小时。
# 注意: 自定义代理登录票据logintoken的有效期不能大于上一步获取的securitytoken的剩余有效时间。
```

```
login_token_security_token = LoginTokenSecurityToken(access=credential.access, secret=credential.secret,
                                                    id=credential.securitytoken, duration_seconds=1800)
body = CreateLoginTokenRequestBody(LoginTokenAuth(login_token_security_token))
request = CreateLoginTokenRequest(body)
create_login_token_response = client.create_login_token(request)
login_token = create_login_token_response.x_subject_login_token

#自定义代理登录地址
auth_URL = "https://auth.huaweicloud.com/authui/federation/login"
#企业管理系统登录地址
enterprise_system_login_URL = "https://example.com/"
#需要访问的华为云服务地址
target_console_URL = "https://console.huaweicloud.com/iam/?region=cn-north-4"

# 创建云服务登录地址FederationProxyUrl, 作为Location返回给浏览器。
FederationProxyUrl = auth_URL + "?idp_login_url=" + urllib.parse.quote(
    enterprise_system_login_URL) + "&service=" + urllib.parse.quote(
    target_console_URL) + "&logintoken=" + urllib.parse.quote(login_token)
print(FederationProxyUrl)
```

11 多因素认证与虚拟 MFA

11.1 多因素认证

什么是多因素认证

多因素认证是一种非常简单安全实践方法，它能够在用户名称和密码之外再额外增加一层保护。启用多因素认证后，用户进行操作时，除了需要提供用户名和密码外（第一次身份验证），还需要提供验证码（第二次身份验证），多因素身份认证结合起来将为您账号和资源提供更高的安全保护。

多因素认证主要应用在登录验证和操作保护中，开启了登录验证功能后，用户登录控制台时，除了需要输入用户名和密码外，还需要在登录验证页面输入验证码；开启了操作保护后，用户进行敏感操作时，需要输入验证码确认操作。

多因素认证支持的设备

多因素认证设备支持手机、邮箱和虚拟MFA设备。

多因素认证应用的场景

多因素认证主要应用于登录保护以及操作保护。若开启多因素认证，则管理控制台和REST API均会受到影响。

- **登录保护**：您以及账号中的IAM用户登录时，除了在登录页面输入用户名和密码外，还需要在登录验证页面输入多因素认证设备中的验证码，再次确认登录者身份，进一步提高账号安全性。
- **操作保护**：您以及账号中的IAM用户进行敏感操作时，例如删除弹性云服务器资源，需要输入多因素认证设备中的验证码对操作进行确认，避免误操作带来的风险和损失。

更多有关登录保护和操作保护的介绍，请参见：[敏感操作](#)。

11.2 虚拟 MFA

本章主要为您介绍[如何绑定虚拟MFA](#)、[如何解绑虚拟MFA](#)，以及IAM用户手机丢失或删除虚拟MFA应用程序时[管理员如何重置虚拟MFA](#)。

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或应用程序，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：Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。

- 暂未升级华为账号的华为云账号

步骤1 进入安全设置。

步骤2 在“安全设置>敏感操作”页面，单击“虚拟MFA”右侧的“前往绑定”。

图 11-1 虚拟 MFA



步骤3 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。

您可以通过扫描二维码、手动输入两种方式绑定MFA设备：

- 扫描二维码
打开手机已安装好的MFA应用程序，选择“扫描条形码”，扫描“绑定虚拟MFA”弹窗中的二维码。扫描成功后，应用程序会自动添加用户。
- 手动输入
打开手机已安装好的MFA应用程序，选择“输入提供的密钥”，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4 添加用户完成，在返回MFA应用程序首页，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。

步骤5 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

- 已升级华为账号

步骤1 进入安全设置。

步骤2 在“安全设置>敏感操作”页面，单击“虚拟MFA”右侧的“前往绑定”。

图 11-2 绑定虚拟 MFA



步骤3 跳转至“华为账号>安全验证”页面，根据提示绑定虚拟MFA。

----结束

- IAM用户

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](#)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”。

图 11-3 登录验证



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

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 11-4 虚拟 MFA 登录验证



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。

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 [进入安全设置](#)。

步骤2 在“安全设置>敏感操作”页面，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3 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。

图 11-5 输入虚拟 MFA 验证码



* 验证码

请输入您从虚拟MFA应用程序中获取的验证码。

步骤4 单击“确定”，验证成功后，完成解绑MFA操作。

----结束

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。

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

12 查看 IAM 操作记录

12.1 开通云审计服务

云审计服务（Cloud Trace Service，以下简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

为了方便查看IAM的关键操作事件，例如创建用户、删除用户等，建议管理员开启云审计服务。

操作步骤

步骤1 登录管理控制台。

步骤2 如果您是以主账号登录华为云，请直接进行**3**；如果您是以IAM用户登录华为云，需要联系管理员对IAM用户授予以下权限：

- Security Administrator
- CTS FullAccess

授权方法请参见[给IAM用户授权](#)。

步骤3 选择“服务列表 > 管理与监管 > 云审计服务”，进入云审计服务授权页面。

步骤4 单击“同意授权并开通”，进入云审计服务页面。

说明

- 后续使用云审计服务，仅需拥有云审计服务相关权限即可，无需拥有Security Administrator权限。
- 同意授权并开通CTS服务后，系统会自动为您创建以下管理追踪器，用于记录管理事件，即针对所有云资源的操作日志，例如创建、登录、删除等：
 - 自动在**当前region**创建1个管理追踪器，用于记录项目级服务的管理事件。
 - 自动在**中国-香港**区域创建1个管理追踪器，用于记录全局服务（如IAM服务）的管理事件。

----结束

在IAM进行操作，例如创建用户、用户组等，CTS将会记录这些操作。CTS支持记录的IAM相关的操作事件，如**下表**所示。

表 12-1 CTS 支持的 IAM 操作列表

操作名称	资源类型	事件名称
用户登录	user	login
用户登录失败（华为账号登录失败不记录）	user	loginFailed
用户登出	user	logout
二维码登录	user	scanQRCodeLogin
二维码登录失败	user	scanQRCodeLoginFailed
OIDC登录成功	user	oidcLoginSuccess
OIDC登录失败	user	oidcLoginFailed
SSO登录成功	user	iamUserSsoLoginSuccess
SSO登录失败	user	iamUserSsoLoginFailed
通过忘记密码修改密码	user	fpwdResetSuccess
创建用户	user	createUser
修改邮件地址、手机号	user	updateUser
删除用户	user	deleteUser
用户在安全设置自行修改密码	user	updateUserPwd
管理员设置用户密码	user	updateUserPwd
修改IAM用户的登录保护状态信息	user	modifyLoginProtect
通过邮箱修改手机号	user	changeMobileByEmail
通过邮箱修改密码	user	updateUserPwdByEmail
企业联邦用户首次登录成功	user	tenantLoginBySamlSuccess
企业联邦用户通过自定义身份代理登录成功	user	federationLoginNoPwdSuccess
企业联邦用户通过自定义身份代理登录失败	user	federationLoginNoPwdFailed
创建用户组	userGroup	createGroup
更新用户组	userGroup	updateGroup

操作名称	资源类型	事件名称
删除用户组	userGroup	deleteGroup
添加用户到用户组	userGroup	addUserToGroup
从用户组删除用户	userGroup	removeUserFromGroup
解绑虚拟MFA设备	MFA	UnBindMFA
绑定虚拟MFA设备	MFA	BindMFA
创建项目	project	createProject
修改项目	project	updateProject
删除项目	project	deleteProject
创建委托	agency	createAgency
修改委托	agency	updateAgency
删除委托	agency	deleteAgency
切换委托	agency	switchRole
为委托授予所有项目服务权限	agency	updateAgencyInheritedGrants
移除委托下的所有项目服务权限	agency	deleteAgencyInheritedGrants
为委托授予全局服务权限	agency	updateAgencyAssignsByRole
为委托授予全局服务权限 (API)	roleAgencyDomain	assignRoleToAgencyOnDomain
更新委托权限	agency	updateAgencyAssignsByRole
注册身份提供商	identityProvider	createIdentityProvider
更新身份提供商	identityProvider	updateIdentityProvider
删除身份提供商	identityProvider	deleteIdentityProvider
更新身份转换规则	identityProvider	updateMapping
更新IDP元数据	identityProvider	metadataConfiguration
手动编辑系统预置的IdP元数据	identityProvider	metadataConfiguration
注册映射	mapping	createMapping

操作名称	资源类型	事件名称
更新映射	mapping	updateMapping
删除映射	mapping	deleteMapping
注册协议	identityProvider	createProtocol
更新协议	identityProvider	updateProtocol
删除协议	identityProvider	deleteProtocol
移除委托的全局服务权限	roleAgencyDomain	unassignRoleToAgencyOnDomain
委托授权项目	roleAgencyProject	assignRoleToAgencyOnProject
解除委托授权项目	roleAgencyProject	unassignRoleToAgencyOnProject
更新账号登录策略	SecurityPolicy	modifySecurityPolicy
更新密码策略	SecurityPolicy	modifySecurityPolicy
更新访问控制列表	SecurityPolicy	modifySecurityPolicy
更新账号登录策略	loginpolicy	securitypolicy
更新密码策略	passwordpolicy	securitypolicy
更新访问控制列表	acl	securitypolicy
创建租户	domain	createDomain
更新租户	domain	updateDomain
删除租户	domain	deleteDomain
OIDC方式登录失败	domain	oidcLoginFailed
注册自定义策略	Policy	createRole
修改自定义策略	Policy	updateRole
删除自定义策略	Policy	deleteRole
用户组添加全局权限 (API)	assignment	createAssignment
用户组添加全局权限	group	updateGroupAssignsByRole
用户组移除全局权限	assignment	deleteAssignment
创建永久AK/SK	credential	createCredential

操作名称	资源类型	事件名称
更新永久AK/SK	credential	updateCredential
删除永久AK/SK	credential	deleteCredential
停用、启用AK/SK	credential	updateCredential
联邦用户通过控制台创建临时访问密钥	credential	CreateTemporaryAccessKeyFromConsole
对用户、企业项目、策略授权	assignment	grantRoleToUserOnEnterpriseProject
移除用户、企业项目、策略授权	enterpriseProject	revokeRoleFromUserOnEnterpriseProject
更新企业项目用户组权限	enterpriseProject	updateRoleFromGroupOnEnterpriseProject
创建用户组	group	createGroup
删除用户组	group	deleteGroup

12.2 在 CTS 事件列表查看云审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

说明

云审计控制台对用户的操作事件日志保留7天，过期自动删除，不支持人工删除。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录。


- [在新版事件列表查看审计事件](#)
- [在旧版事件列表查看审计事件](#)

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。
- 用户通过云审计控制台只能查询最近7天的操作记录。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务(OBS)或云日志服务(LTS)，才可在OBS桶或LTS日志组里面查看历史事件信息。否则，您将无法追溯7天以前的操作记录。
- 云上操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。




- CTS新版事件列表不显示数据类审计事件，您需要在旧版事件列表查看数据类审计事件。

在新版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
 - 事件名称：输入事件的名称。
 - 事件ID：输入事件ID。
 - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
 - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
 - 云服务：在下拉框中选择对应的云服务名称。
 - 资源类型：在下拉框中选择对应的资源类型。
 - 操作用户：在下拉框中选择一个或多个具体的操作用户。
 - 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
 - normal：表示操作成功。
 - warning：表示操作失败。
 - incident：表示比操作失败更严重的情况，例如引起其他故障等。
 - 企业项目ID：输入企业项目ID。
 - 访问密钥ID：输入访问密钥ID（包含临时访问凭证和永久访问密钥）。
 - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。


说明

您可以参考[云审计服务应用示例](#)，来学习如何查询具体的事件。

5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
 - 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
 - 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
 - 单击  按钮，可以获取到事件操作记录的最新信息。
 - 单击  按钮，可以自定义事件列表的展示信息。启用表格内容折行开关 ，
可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。



- 关于事件结构的关键字段详解，请参见[事件结构](#)和[事件样例](#)。
- （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

在旧版事件列表查看审计事件

- 登录管理控制台。
- 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
- 单击左侧导航树的“事件列表”，进入事件列表信息页面。
- 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
- 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
 - 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
 - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
 - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
 - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
 - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
 - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
 - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

说明

您可以参考[云审计服务应用示例](#)，来学习如何查询具体的事件。

- 选择完查询条件后，单击“查询”。
- 在事件列表页面，您还可以导出操作记录文件和刷新列表。
 - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
 - 单击  按钮，可以获取到事件操作记录的最新信息。
- 在需要查看的事件左侧，单击  展开该记录的详细信息。

事件名称	资源类型	云服务	资源ID	资源名称	事件级别	操作用户	操作时间	操作
createDockerConfig	dockerlogincmd	SWR	--	dockerlogincmd	normal		2023/11/16 10:54:04 GMT+08:00	查看详情

request

trace_id

code 200

trace_name createDockerConfig

resource_type dockerlogincmd

trace_rating normal

api_version

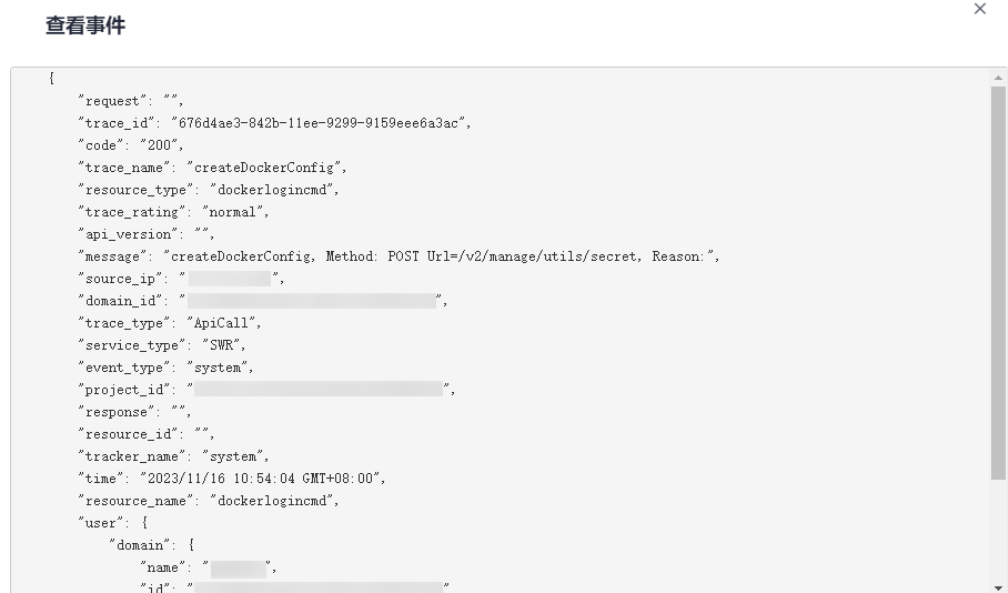
message createDockerConfig, Method: POST Uri=/v2/manager/utils/secret, Reason:

source_ip

domain_id

trace_type ApiCall

9. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。



10. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的[事件结构](#)和[事件样例](#)。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

13 调整配额

什么是配额？

为防止资源滥用，平台限制了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少个IAM用户、用户组等。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额？


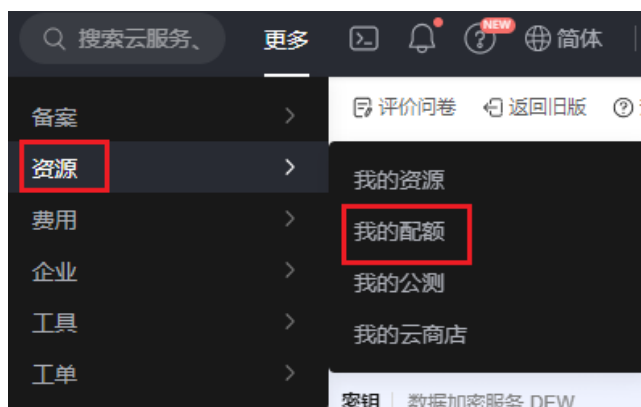
1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 在页面右上角，选择“资源 > 我的配额”。
系统进入“服务配额”页面。

图 13-1 我的配额

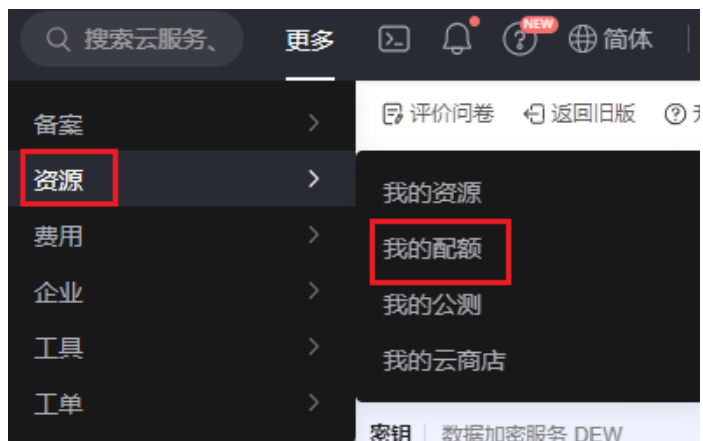


4. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

如何申请扩大配额？

1. 登录管理控制台。
2. 在页面右上角，选择“资源 > 我的配额”。
系统进入“服务配额”页面。

图 13-2 我的配额



3. 单击“申请扩大配额”。
4. 在“新建工单”页面，根据您的需求，填写相关参数。
其中，“问题描述”项请填写需要调整的内容和申请原因。
5. 填写完毕后，勾选协议并单击“提交”。