统一身份认证服务

最佳实践

文档版本 03

发布日期 2025-02-11

华为技术有限公司

商标声明


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

注意

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

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 IAM 的安全使用最佳实践

为了帮助您安全地控制对华为云资源的访问，请您遵循安全使用IAM的建议。

不给华为账号创建访问密钥

华为账号是您华为云资源归属、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。密码与访问密钥（AK/SK）都是账号的身份凭证，具有同等效力，密码用于登录界面控制台，是您必须具备的身份凭证，访问密钥用于使用开发工具进行编程调用，是第二个身份凭证，为辅助性质，非必须具备。为了提高账号安全性，建议您仅使用密码登录控制台即可，不要给账号创建第二个身份凭证（访问密钥），避免因访问密钥泄露带来的信息安全风险。

不将访问密钥嵌入到代码中

当您使用API、CLI、SDK等开发工具来访问云服务时，请勿直接将访问密钥嵌入到代码中，减少访问密钥被泄露的风险。

创建单独的 IAM 用户

如果有任何人需要访问您华为账号中的资源，请不要将账号的密码共享给他们，而是在您的账号中给他们创建单独的IAM用户并分配相应的权限，同时，作为华为账号主体，建议您不使用账号访问华为云，而是为自己创建一个IAM用户，并授予该用户管理权限，以使用该IAM用户代替账号进行日常管理工作，保护账号的安全。

合理设置访问方式

IAM支持为用户设置编程访问、管理控制台访问方式，请参考如下说明为IAM用户设置访问方式：

- 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。

授予最小权限

最小权限原则是标准的安全建议，您可以使用IAM提供的系统权限，或者自己创建自定义策略，给账号中的用户仅授予刚好能完成工作所需的权限，通过最小权限原则，可以帮助您安全地控制用户对华为云资源的访问。

同时，建议为使用API、CLI、SDK等开发工具访问云服务的IAM用户，授予自定义策略，通过精细的权限控制，减小因访问密钥泄露对您的账号造成的影响。

开启虚拟 MFA 功能

Multi-Factor Authentication (简称MFA) 是一种非常简单的安全实践方法，建议您给华为账号以及您账号中具备较高权限的用户开启MFA功能，它能够在用户名和密码之外再额外增加一层保护。启用MFA后，用户登录控制台时，系统将要求用户输入用户名和密码（第一安全要素），以及来自其MFA设备的验证码（第二安全要素）。这些多重要素结合起来将为您的账户和资源提供更高的安全保护。

MFA设备可以基于硬件也可以基于软件，系统目前仅支持基于软件的虚拟MFA，虚拟MFA是能产生6位数字认证码的应用程序，此类应用程序可在移动硬件设备（包括智能手机）上运行，非常方便。

设置强密码策略

在IAM控制台设置强密码策略，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，保证用户使用复杂程度高的强密码。

设置敏感操作

设置敏感操作后，如果您或者您账号中的用户进行敏感操作时，例如删除资源、生成访问密钥等，需要输入验证码进行验证，避免误操作带来的风险和损失。

定期修改身份凭证

如果您不知道自己的密码或访问密钥已泄露，定期进行修改可以将不小心泄露的风险降至最低。

- 定期轮换密码可以通过设置密码有效期策略进行，您以及您账号中的用户在设置的时间内必须修改密码，否则密码将会失效，IAM会在密码到期前15天开始提示用户修改密码。
- 轮换访问密钥可以通过创建两个访问密钥进行，将两个访问密钥作为一主一备，一开始先使用主访问密钥一，一段时间后，使用备访问密钥二，然后在控制台删除主访问密钥一，并重新生成一个访问密钥，在您的应用程序中定期轮换使用。

删除不需要的身份凭证

对于仅需要登录控制台的IAM用户，不需要使用访问密钥，请不要给他们创建，或者及时删除访问密钥。您还可以通过账号中IAM用户的“最近一次登录时间”，来判断该用户的凭证是否已经属于不需要的范畴，对于长期未登录的用户，请及时修改他们的身份凭证，包括修改密码和删除访问密钥，您还可以设置“账号停用策略”来控制长期未使用的账号到期自动停用。

在 ECS 实例上运行的应用程序使用 ECS 委托

在华为云ECS实例上运行的应用程序需要凭证才能访问其他华为云服务。若要以安全的方式提供应用程序所需的凭证，可使用ECS委托获取临时访问密钥。在ECS获取临时访问密钥，需要在IAM上对ECS授权，并对相应的弹性云服务器资源进行授权委托管理。ECS通过向IAM申请指定委托的临时凭证，从而安全访问资源。ECS会为您自动轮换这些临时凭证，从而确保每次申请的临时凭证安全、有效。

当您启动ECS实例时，您可指定实例的委托，以作为启动参数。在ECS实例上运行的应用程序在访问华为云资源时可使用委托的临时访问密钥，同时委托的权限将确定允许访问资源的应用程序。

开通云审计服务

您可以通过云审计服务（Cloud Trace Service，CTS）对IAM的关键操作事件进行收集、存储和查询，用于安全分析、合规审计、资源跟踪和问题定位等。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，建议您开启云审计服务。

2 通过 IAM 对多运维人员进行权限设置

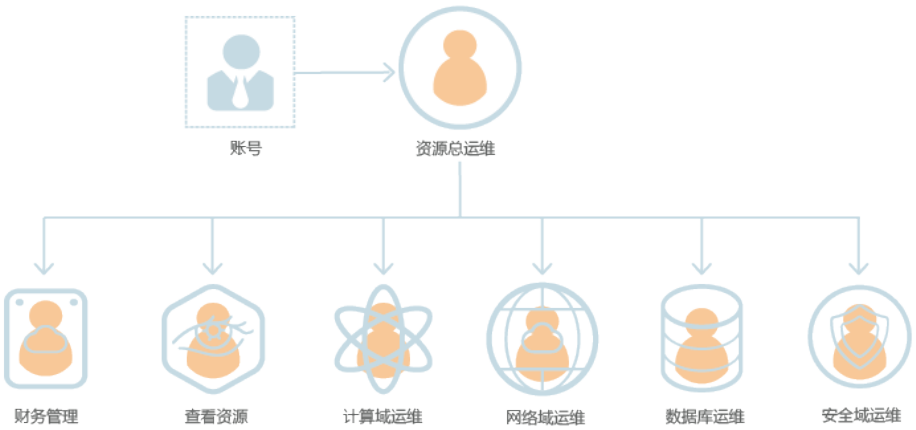
方案概述

A公司在华为云中购买了多种资源，公司中有多个职能团队，这些职能团队需要使用一种或者多种资源，因此涉及到多运维人员权限设置需求，通过IAM的权限管理功能可以实现该需求。

资源规划

根据A公司中员工所负责的不同职能，将员工划分为以下七个团队：

图 2-1 权限设置模型



- 资源总运维：负责管理公司所有资源的团队。
- 财务管理：负责管理公司财务的团队。
- 查看资源：负责查看并监控所有资源使用情况的团队。
- 计算域运维：负责计算域运维的团队。
- 网络域运维：负责网络域运维的团队。
- 数据库运维：负责数据库运维的团队。
- 安全域运维：负责安全域运维的团队。

通过表1，给公司中不同的职能团队设置不同的权限，可以实现各团队之间权限隔离，各司其职。**如需了解华为云所有云服务的系统权限，请参见：系统权限。**

表 2-1 系统权限

职能团队	需要授予的策略	权限说明
资源总运维	Tenant Administrator	除IAM外，其他所有云资源的所有执行权限，包括费用中心、资源中心、账号中心的权限，可以购买资源，管理续费，查看账单等。
财务管理	BSS Administrator	费用中心、资源中心、账号中心的所有执行权限，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。**仅拥有该权限的用户不能购买资源，用户如果购买资源需要拥有对应资源的管理员权限。**
查看资源	Tenant Guest	除IAM外，其他所有资源的只读权限。
计算域运维	ECS FullAccess	弹性云服务器（ECS）的所有执行权限，包括购买ECS的权限，仅拥有该权限的用户不能查看ECS以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。
	CCE FullAccess	云容器引擎（CCE）的所有执行权限，包括购买CCE的权限，仅拥有该权限的用户不能查看CCE以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。
	AutoScaling FullAccess	弹性伸缩（AS）的所有执行权限，包括购买AS的权限，仅拥有该权限的用户不能查看AS以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。
网络域运维	VPC FullAccess	虚拟私有云（VPC）的所有执行权限，包括购买VPC的权限，仅拥有该权限的用户不能查看VPC以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。
	ELB FullAccess	弹性负载均衡（ELB）的所有执行权限，包括购买ELB的权限，仅拥有该权限的用户不能查看ELB以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。
数据库运维	RDS FullAccess	云数据库（RDS）的所有执行权限，包括购买RDS的权限，仅拥有该权限的用户不能查看RDS以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。
	DDS FullAccess	文档数据库服务（DDS）的所有执行权限，包括购买DDS的权限，仅拥有该权限的用户不能查看DDS以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。

职能团队	需要授予的策略	权限说明
	DDM FullAccess	分布式数据库中间件的所有执行权限。
安全领域运维	Anti-DDoS Administrator	Anti-DDoS流量清洗服务的所有执行权限。
	CAD Administrator	DDoS高防服务的所有执行权限。
	KMS Administrator	数据加密服务（DEW）的所有执行权限，包括购买DEW的权限，仅拥有该权限的用户不能查看DEW以及其他资源的总体消费情况，如果需要查看消费情况，需要配合BSS Administrator使用。

根据以上职能团队的划分，资源规划情况包含以下内容：

表 2-2 资源规划

资源	资源名称	资源说明	数量
管理员账号	Company-A	A公司用于管理资源和权限所创建的账号。	1
IAM用户组	网络域运维	A公司根据团队职能需要划分为七个用户组，此处仅以创建用户组“网络域运维”为例。	1
IAM用户	James、Alice	此处仅以创建IAM用户“James”和“Alice”为例。	2
权限	VPC FullAccess、ELB FullAccess	根据上表可知，需要为“网络域运维”用户组配置两个权限。	2

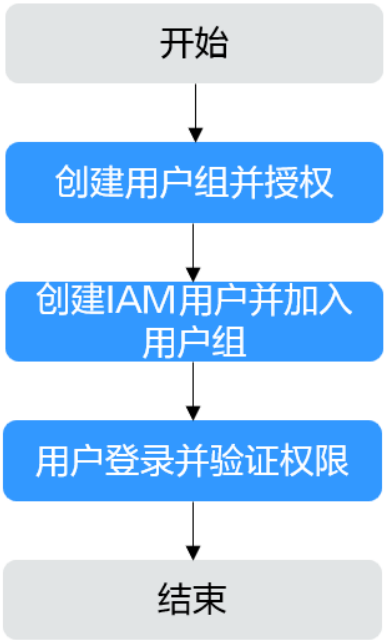
说明

因为统一身份认证服务为免费服务，因此此最佳实践中不涉及费用。

操作流程

IAM通过用户组功能实现用户的授权。本文档以A公司将一个员工配置为“华东-上海二”区域的网络域运维负责人为例，介绍如何通过IAM实现多运维人员权限设置需求，流程如图2-2所示。如果需要将员工配置为其他运维负责人，请参考表1，为相关负责人授予相应的系统权限。

图 2-2 操作流程



步骤一：创建用户组并授权

步骤1 A公司管理员登录并进入华为云控制台。

步骤2 在控制台页面中将鼠标移动至右上角的用户名，选择“统一身份认证”。

步骤3 在统一身份认证服务的左侧导航空格中，单击“用户组”>“创建用户组”。

图 2-3 创建用户组

步骤4 在“创建用户组”界面，输入“用户组名称”为“网络域运维”，单击“确定”。

用户组名称只能包含中文、大小写字母、数字、空格或特殊字符(-_)。

图 2-4 输入名称

步骤5 单击新建用户组右侧的“授权”。

图 2-5 授权

步骤6 在搜索框中搜索“VPC FullAccess”和“ELB FullAccess”，勾选并单击“下一步”。

图 2-6 勾选权限

步骤7 选择授权范围方案为“指定区域项目资源”，并选择“华东-上海二”区域。

图 2-7 选择权限生效的区域

说明

- 如果员工还需要查看资源的消费情况，请在同区域选择“BSS Administrator”权限。
- 如果您参考**表1**，将员工配置为安全域运维负责人，由于安全域与其他服务存在业务交互关系，授权时，必须同时添加依赖的其他服务的权限，方法请参见：**依赖授权**。

步骤8 单击“确定”，完成对“网络域运维”用户组的授权。创建成功的用户组将会展示在用户组列表中。

可以单击“网络域运维”用户组的名称，在“授权记录”页签下查看已授予的权限。

----结束

步骤二：创建 IAM 用户并加入用户组

步骤1 A公司管理员在统一身份认证服务，左侧导航中，选择“用户”。

步骤2 在用户页面，单击右上角“创建用户”。

图 2-8 创建用户

步骤3 配置用户基本信息。在“创建用户”界面填写“用户信息”和“访问方式”。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。

图 2-9 配置用户信息

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。

表 2-3 用户信息

用户信息	说明	取值样例
用户名	必填。IAM用户登录华为云的用户名。	James、Alice

用户信息	说明	取值样例
邮件地址	“凭证类型”选择“首次登录时设置”时必填，选择其他时选填。IAM用户绑定的邮件地址可作为IAM用户的登录凭证，也可由IAM用户自己绑定。	暂不配置
手机号	选填。IAM用户绑定的手机号，可作为IAM用户的登录凭证，也可由IAM用户自己绑定。	暂不配置
描述	选填。记录IAM用户相关信息。	暂不配置

图 2-10 配置访问方式

表 2-4 访问方式

访问方式	说明	取值样例
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。	勾选
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。	勾选

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。

表 2-5 配置凭证类型和登录保护

凭证类型与登录保护		说明	取值样例
访问密钥		访问密钥（AK/SK，Access Key ID/Secret Access Key）包含访问密钥ID（AK）和秘密访问密钥（SK）两部分，是您在华为云的长期身份凭证，您可以通过访问密钥对华为云API的请求进行签名。 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）。	不勾选
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。	选择
	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。 **仅在创建单个用户时适用。**	-
	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。	-
登录保护	开启登录保护	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，您可以选择通过手机、邮件地址、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。	选择

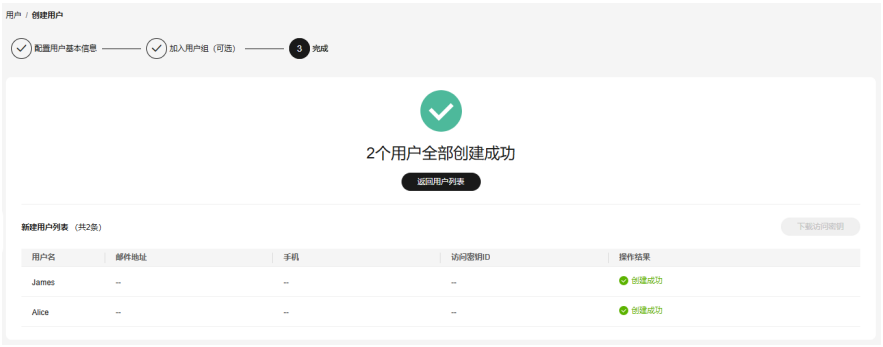
步骤4 单击“下一步”，将IAM用户James、Alice加入到上一步中创建的“网络域运维”用户组。

说明

- 如果该用户是管理员，可以将用户加入默认用户组“admin”中。
- 一个用户可以同时加入多个用户组。

步骤5 单击“下一步”，IAM用户创建完成，用户列表中显示新创建的IAM用户James和Alice。如果3勾选了“凭证类型”中的“访问密钥”，可在此页面下载访问密钥。

图 2-11 创建成功



----结束

步骤 3：IAM 用户登录并验证权限

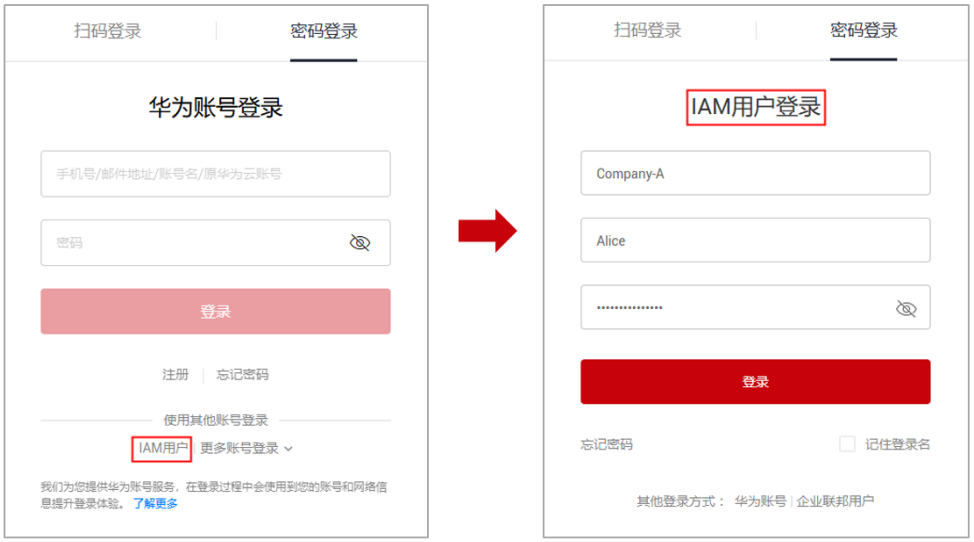
IAM用户登录有多种方式，如下步骤仅讲述其中一种，更多登录方式请参见：登录华为云。

步骤1 IAM用户James或Alice在华为云登录页面，单击右下角的“IAM用户登录”。

步骤2 在“IAM用户登录”页面，输入A公司账号名Company-A、IAM用户名及用户密码。

- 账号名为该IAM用户所属华为云账号的名称。
- 用户名和密码为账号在IAM创建用户时输入的用户名和密码。

图 2-12 IAM 用户登录



步骤3 登录成功后，IAM用户进入华为云控制台，请先切换至授权区域“华东-上海二”。

步骤4 在“服务列表”中选择虚拟私有云VPC、弹性负载均衡ELB，云解析服务DNS，可以进入这些服务的主页面并进行管理操作，权限配置成功。

步骤5 在“服务列表”中选择除以上服务外的任一服务，系统提示权限不足，权限配置成功。

步骤6 切换区域至除“华东-上海二”的任一区域，无法进入任何服务主页面，包括虚拟私有云VPC、弹性负载均衡ELB，云解析服务DNS，表示权限配置成功。

----结束

3 委托其他账号或云服务管理资源

3.1 使用委托实现跨账号的资源授权与管理

A公司和B公司是华为云注册的企业用户，分别拥有自己单独的华为账号。本文主要介绍当A账号希望将部分资源委托给B账号时，使用IAM的委托功能来实现跨账号的资源授权与管理（A账号为委托方，B账号为被委托方）。

企业需求

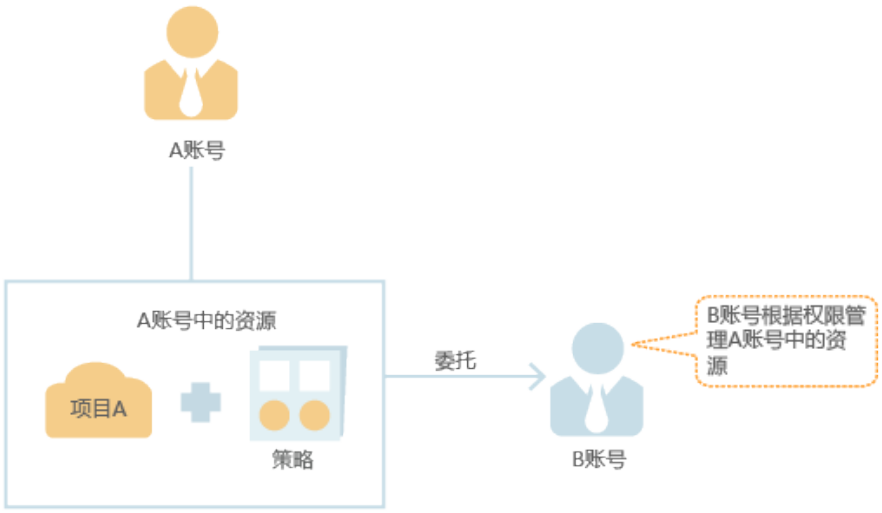
- A账号在华为云购买了多种资源，为了专注自己的业务领域，希望将“华东-上海二”区域的VPC资源委托给B账号进行代运维。
- B账号希望将A账号委托的资源分配给公司中一个或多个员工（IAM用户），进行精细的权限管理。
- 如果合作关系发生变更，A账号希望随时可以修改或撤销对B账号的授权。

解决方案

针对以上企业需求，可以使用IAM的委托功能来实现跨账号的资源授权与管理。

- A账号在IAM控制台创建一个委托，指定委托的使用者为B账号，并将需要代运维的资源授权给这个委托。
- B账号进一步授权，将A账号委托的资源分配给账号下专职管理委托的IAM用户，让IAM用户帮助管理。
- 当合作关系发生变更时，A账号随时可以修改或者删除这个委托，B账号以及账号下可以管理该委托的用户对该委托的使用权限将自动修改或者撤销。

图 3-1 跨账号授权模型



委托方跨账号授权

以A账号将“华东-上海二”区域的VPC资源，委托给B账号进行代运维为例，说明委托方进行跨账号授权的操作方法。

步骤1 A账号登录华为云，在统一身份认证服务中，单击“委托”。

步骤2 在“委托”页面，单击“创建委托”，设置“委托名称”，例如“VPC资源代运维”。

步骤3 “委托类型”选择“普通账号”，在“委托的账号”中填入B公司的华为账号名称，例如“B-Company”。

步骤4 设置“持续时间”为永久。

图 3-2 创建委托

步骤5 单击“完成”。

步骤6 在授权的确认弹窗中，单击“立即授权”。

步骤7 选择权限“VPC FullAccess”，单击“下一步”。

步骤8 选择授权范围方案为“指定区域项目资源 > 华东-上海一”。

步骤9 单击“确定”。

委托创建完成，委托列表中显示新创建的委托。

说明

当合作关系发生变更时，A账号可以在委托列表中，单击“修改”，修改这个委托的委托账号、权限、持续时间等。

----结束

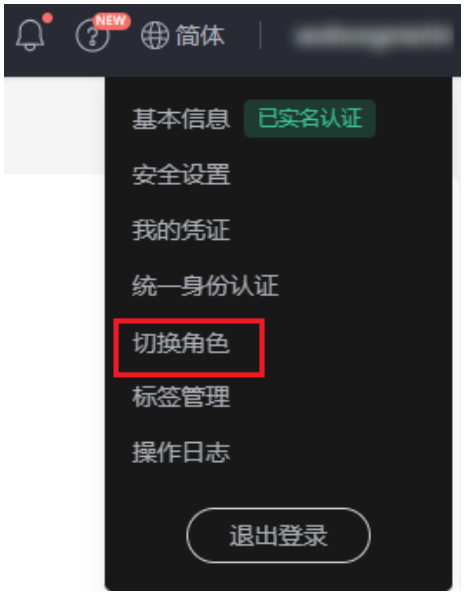
被委托方跨账号管理

当A账号与B账号创建委托关系后，即B账号为被委托方，B账号通过切换角色的方法，可以切换到A账号中，管理委托方授权的资源。B账号需要提前获取A账号的华为账号名称以及所创建的委托名称。

步骤1 B账号登录华为云，进入控制台。

步骤2 在右上方的用户名中，选择“切换角色”。

图 3-3 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，输入账号名称后，系统将会按照顺序自动匹配委托名称。

图 3-4 切换角色

步骤4 单击“确定”，B账号切换至委托方A账号中，直接对A账号华东-上海一区域的VPC资源进行管理。

----结束

被委托方分配委托权限

以B账号将委托分配给IAM用户进行管理为例，实现分配委托以及对委托进行精细授权。委托权限分配完成后，B账号中的IAM用户通过切换角色的方式，可以切换到A账号中，管理委托方授权的资源。

B账号需要提前获取委托公司的华为账号名称、所创建的委托名称以及委托的ID。

步骤1 创建用户组并授权。

1. B账号在统一身份认证服务左侧导航窗格中，单击“用户组”。
2. 在“用户组”界面中，单击“创建用户组”。
3. 输入“用户组名称”，例如“委托管理”。
4. 单击“确定”。

   返回用户组列表，用户组列表中显示新创建的用户组。
5. 单击新建用户组右侧的“授权”，进入授权界面。

   说明

   - 如果需要用户仅管理一个特定的委托，请执行以下步骤对委托进行精细授权。
   - 如果需要用户管理所有委托，请跳过该步骤，直接执行**下一步**。

   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”，例如“管理A公司的委托1”。

   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。

e. 单击“下一步”，继续完成授权。

6. 选择**上一步**中创建的自定义策略“管理A公司的委托1”，或者“Agent Operator”权限。

说明

- 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. 选择授权作用范围。
8. 单击“确定”。

步骤2 创建用户并加入用户组。

1. B账号在统一身份认证服务左侧导航窗格中，单击“用户”
2. 在“用户”界面，单击“创建用户”。
3. 在“创建用户”界面，输入“用户名”“邮箱”。
4. “访问方式”选择“管理控制台访问”。
5. “凭证类型”选择“首次登录时设置”。
6. “登录保护”选择“开启”，并选择身份验证方式，单击“下一步”。
7. 在“加入用户组”页面，选择**步骤2**中创建的用户组“委托管理”，单击“创建用户”。

步骤3 切换角色。

1. 使用**步骤2**创建的IAM用户，通过“IAM用户登录”方式，登录华为云。登录方法，请参见：**IAM用户登录**。
2. IAM用户在控制台页面，右上方的用户名中，选择“切换角色”。

图 3-5 切换角色

3. IAM用户在“切换角色”页面中，输入委托方的账号名称，输入账号名称后，系统将会按照顺序自动匹配委托名称。

   说明

   如果自动匹配的是没有授权的委托，系统将提示没有权限访问，可以删除委托名称，在下拉框中选择已授权的委托名称。

4. 单击“确定”，切换至委托方账号中。IAM用户可以对B账号分配委托权限的A账号资源进行管理操作。

----结束

3.2 在 ECS 上通过委托的临时访问密钥访问其他云服务

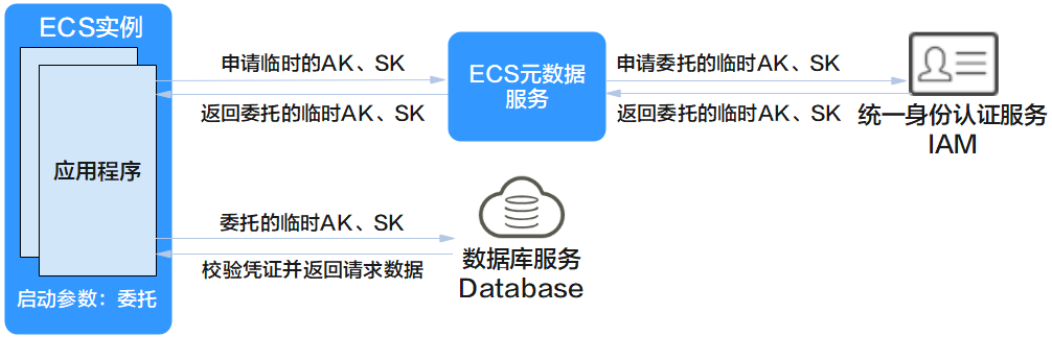
华为云弹性云服务器（Elastic Cloud Server，以下简称ECS）是一种云上可随时自助获取、可弹性伸缩的计算服务。本文将指导用户创建ECS委托，并获取委托的临时访问密钥。

应用场景

假如您是一位开发者，开发了一个应用程序，这个应用程序运行在ECS实例上，应用程序的代码中涉及调用API访问华为云服务。此时，因为华为云服务要求访问请求方出示访问凭证，所以您的API调用将会面临提供访问凭证的问题。

访问凭证按照时效性可分为永久凭证和临时凭证，相较于永久性访问凭证，例如用户名和密码，临时访问密钥因为有效期短且刷新频率高，所以安全性更高。因此，您的应用程序若想要以更安全的方式访问云服务，需要获取临时访问凭证，而IAM的委托功能，则支持通过ECS委托获取临时访问密钥。

图 3-6 应用程序获取临时访问密钥



如图1所示，以访问数据库服务举例。因为数据库服务要求访问请求方提供访问凭证，所以应用程序需要获得委托的临时访问密钥AK、SK。应用程序与ECS元数据服务通信，ECS元数据服务再与IAM通信，拿到临时AK、SK后返回给应用程序。然后，应用程序将临时AK、SK作为访问凭证出示给数据库服务，数据库服务收到请求后，先校验访问凭证是否合法，凭证通过校验后，ECS实例上的应用程序才能访问数据库服务。

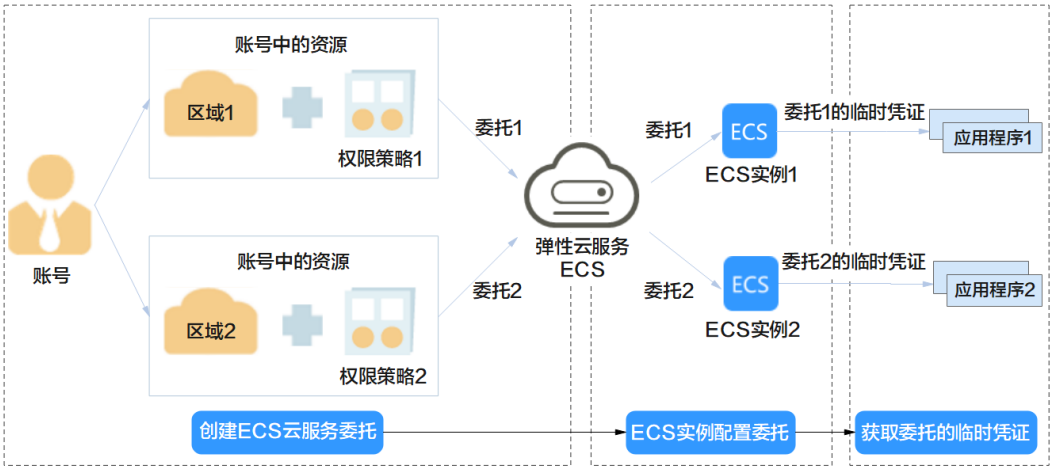
解决方案

针对以上应用场景，可使用IAM对ECS云服务的委托来获取临时访问密钥。在IAM上对ECS云服务授权，并对应用程序所在的ECS实例进行授权委托管理。ECS实例获得委托

权限之后，应用程序可申请指定委托的临时访问密钥，从而以临时访问密钥为凭证安全访问华为云资源。详细方案如下：

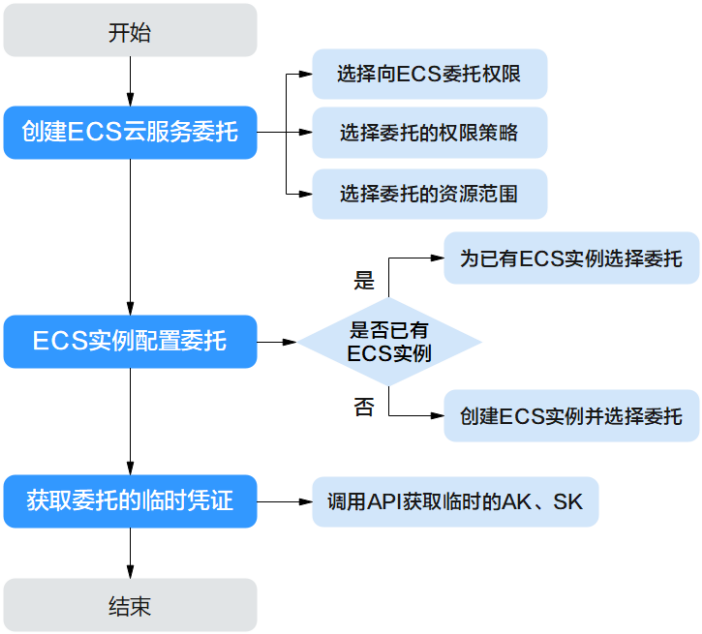
1. 创建ECS云服务委托。账号在IAM控制台创建委托，指定委托对象为ECS云服务。委托创建时，选择权限策略，选择可访问的资源范围，不同的委托对应不同的权限策略。
2. ECS实例配置委托。在ECS实例的配置项中选择上一步创建的委托，一个ECS实例只可以选择一个委托。
3. 获取委托的临时凭证。ECS实例配置了委托参数后，就获得了委托权限。此时，ECS实例上运行的应用程序可获取委托的临时访问密钥AK、SK。拥有临时访问密钥的应用程序可与华为云服务进行交互，交互行为遵循账号授予的权限策略和资源使用范围。

图 3-7 ECS 委托



操作流程

图 3-8 ECS 委托操作流程



实施步骤

如图3所示，配置ECS弹性云服务器委托分为创建ECS云服务委托、ECS实例配置委托、获取委托的临时凭证三步。详细步骤如下：

步骤1 管理员创建ECS云服务委托。

1. 管理员登录统一身份认证服务控制台。
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”。
3. 在创建委托页面，设置“委托名称”
4. “委托类型”选择“云服务”，在“云服务”中选择“弹性云服务器 ECS 裸金属服务器 BMS”。

图 3-9 创建委托

5. 选择“持续时间”。
6. （可选）填写“委托描述”。建议填写描述信息。
7. 单击“完成”。
8. 在授权的确认弹窗中，单击“立即授权”。
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。
10. 单击“确定”，委托创建完成。

步骤2 管理员或拥有ECS权限的IAM用户为ECS实例配置委托。

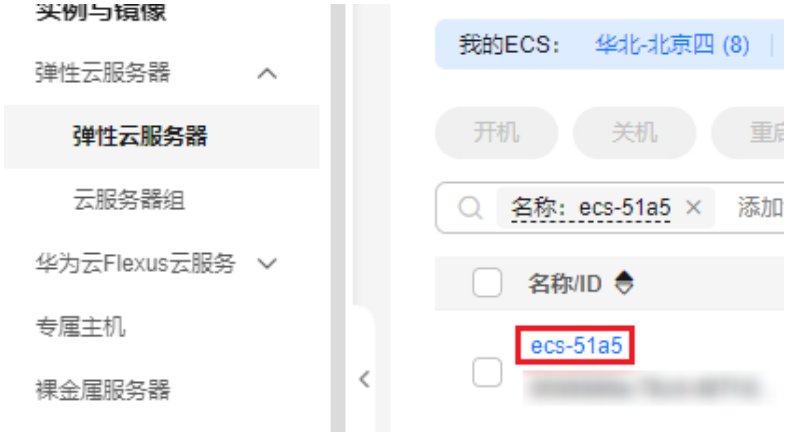
- 若ECS实例未创建，则参考**自定义购买弹性云服务器**，购买并配置ECS云服务器，在**高级配置**过程中，单击下拉列表选择**步骤1**创建的委托，获取相应权限。

图 3-10 选择委托

- 若ECS实例已创建，可按照如下流程配置ECS实例委托：

1. 进入ECS产品页，单击ECS实例名，进入配置页面。

图 3-11 单击 ECS 实例名



2. 管理信息栏目下，单击，为ECS实例选择委托。

图 3-12 为 ECS 实例选择委托

3. 根据委托名选择**步骤1**创建的委托。

图 3-13 选择委托

4. 单击✓，完成配置

步骤3 应用程序获取临时凭证。

运行在ECS实例上的应用程序调用获取委托临时凭证的API，即可获得临时访问密钥，之后可使用该密钥访问其他的华为云服务。AK、SK获取方法如下，如需了解详情，可参见**元数据获取**。

- URI

/openstack/latest/securitykey

- 方法

支持GET请求

- 示例

Linux操作系统：

curl http://169.254.169.254/openstack/latest/securitykey

Windows操作系统：

Invoke-RestMethod http://169.254.169.254/openstack/latest/securitykey

说明

ECS会为您自动轮换这些临时凭证，从而确保每次申请的临时凭证安全、有效。

----结束

4 通过 IAM 对跨区域的指定资源进行授权

A公司是华为云企业用户，企业中有多个项目团队，需要为项目团队购买资源、配置人员、进行项目管理。本文针对A公司提出的企业需求，给出多项目管理最佳实践。

企业需求

- **需求1：**A公司需要同时在“华北-北京四”和“华东-上海一”多地域购买多种资源，A公司希望将资源按需分配给两个项目团队，某些服务可实现指定资源的分配，例如某一台ECS服务器只分配给指定IAM用户使用，且两个项目中的资源相互隔离。
- **需求2：**每个项目团队的成员只能访问其所在项目团队的资源，且仅拥有能够完成工作的资源使用最小权限。
- **需求3：**A公司希望两个项目团队能够独立核算成本，项目费用一目了然。

解决方案

- **针对需求1：**当前华为云提供的企业管理服务（EPS）和统一身份认证服务（IAM），均可实现项目之间的资源隔离，但两种服务的实现逻辑及功能不同。
  - **企业管理服务**：在企业管理服务中创建企业项目，企业项目之间的资源是逻辑隔离，针对企业不同项目间的资源进行分组和管理，**一个企业项目中可以包含多个区域的资源**。企业项目内的资源可以动态的迁入和迁出，某些服务可以实现指定资源的迁入迁出，例如迁入迁出某一台ECS服务器。
  - **统一身份认证服务**：在统一身份认证服务中创建IAM项目可以实现资源之间的物理隔离，针对同一个区域内的资源进行分组和隔离，**一个IAM项目中只能包含一个区域中的资源**。

综上，企业管理服务能够实现项目间跨区域的资源隔离，隔离逻辑更加灵活，因此，推荐A公司使用企业管理服务进行项目资源管理，以下需求将基于企业管理服务提出解决方案。如需了解更多统一身份认证和企业管理的区别，请参见：**统一身份认证和企业管理的区别**。

- **针对需求2：**A公司需要配合使用企业管理服务和统一身份认证服务，在统一身份认证服务中创建用户组、为每个员工创建IAM用户并加入用户组，再将用户组添加至**需求1**创建的企业项目，并按照**表1**为各企业项目中的用户组授予相应的资源使用权限。

图 4-1 A 公司人员配置模型

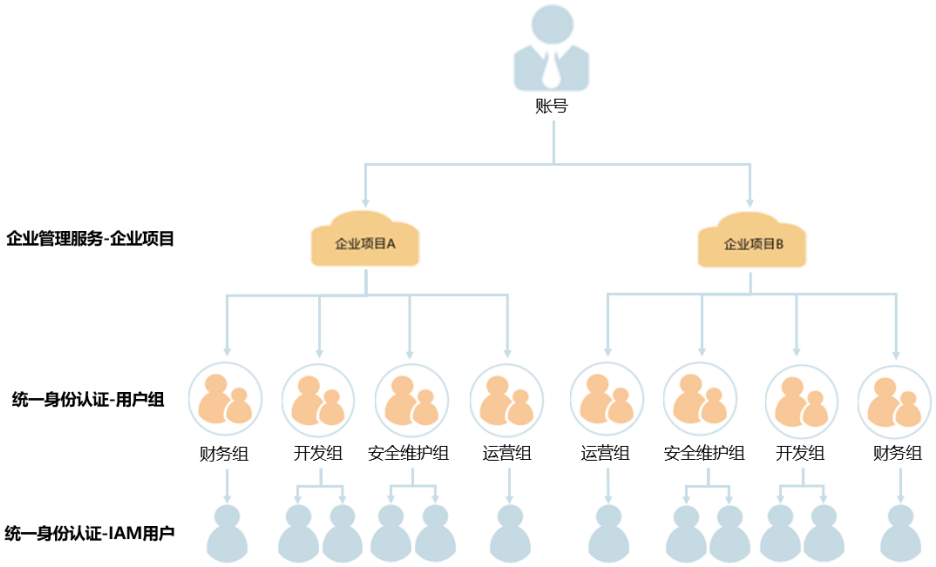


表 4-1 A 公司各用户组权限配置模型

用户组	职责	所需权限	描述
财务组	负责管理项目费用的使用情况。	Enterprise Project BSS FullAccess	企业项目费用的管理权限。
开发组	负责使用资源进行项目开发。	ECS FullAccess	弹性云服务器（ECS）的所有执行权限。
		OBS FullAccess	对象存储服务（OBS）的所有执行权限。
		ELB FullAccess	弹性负载均衡（ELB）的所有执行权限。
安全维护组	负责项目的安全运维。	ECS CommonOperations	弹性云服务器（ECS）的普通操作权限。
		CAD Administrator	DDoS高防服务（AAD）的所有执行权限。
运营组	负责所有项目的总体运营。	EPS FullAccess	企业管理服务的所有执行权限，包括修改、启用、停用、查看企业项目。

说明

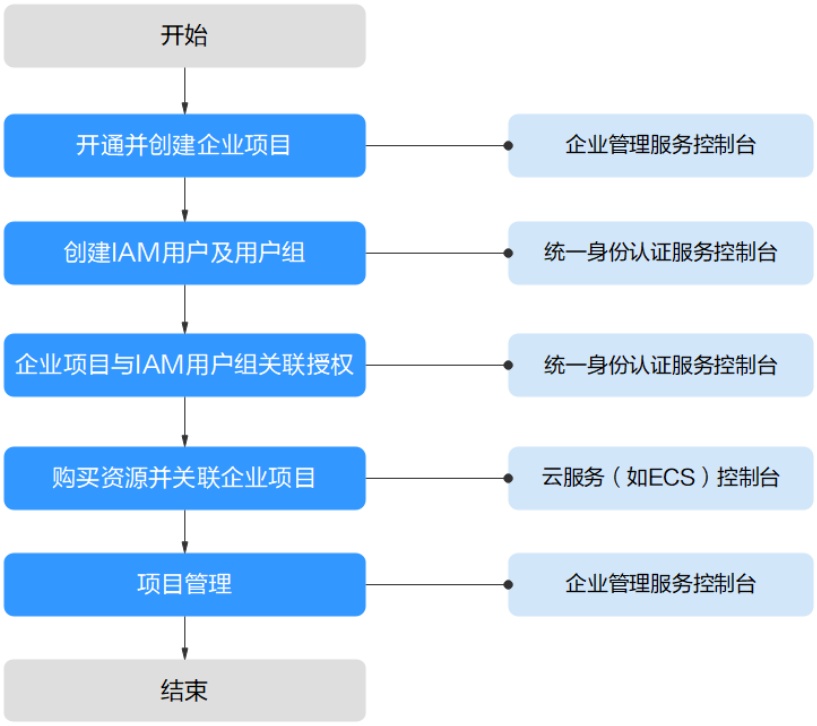
如需了解华为云所有云服务的系统权限，请参见：**系统权限**。

- **针对需求3：**A公司使用企业管理服务，基于企业项目管理项目续费、订单、财务、退订、变更及配额。详情请参考：**管理企业项目的财务信息**。

操作流程

针对A公司的企业需求及其解决方案，按照如下流程构建项目团队、购买资源，实现企业项目管理。

图 4-2 企业项目管理流程图



步骤1：开通并创建企业项目：开通企业项目，并在**企业管理服务控制台**创建企业项目。

步骤2：创建IAM用户及用户组：在**统一身份认证服务控制台**为各职能团队创建用户组、为员工创建IAM用户，并将IAM用户加入用户组，实现人员分组。

步骤3：企业项目与IAM用户组关联授权：在**统一身份认证服务控制台**为各用户组授予应有的权限，并将其加入相应的企业项目，实现人员授权。

步骤4：购买资源并关联企业项目：在**云服务控制台**购买资源，并选择所属企业项目，实现资源隔离。

后续操作：企业项目管理：在**企业管理服务控制台**进行人员、资源、财务管理。

开通并创建企业项目

通过本节在企业管理控制台创建名为“企业项目A”、“企业项目B”的企业项目。如果您已开通企业项目，请直接操作**步骤 4**。

步骤1 A公司使用注册的华为账号登录华为云控制台，单击*“用户名”*，选择“基本信息”。

步骤2 在基本信息页面，单击“开通企业项目”。

说明

如果您为未实名认证的账号，请先进行**企业实名认证**。

步骤3 在开通企业项目页面，勾选“我已阅读并同意《华为云企业管理使用协议》”，单击“申请开通”，开通企业项目。

步骤4 在华为云控制台，单击“企业”，选择“项目管理”。

图 4-3 进入企业管理服务

步骤5 在企业项目管理页面，单击“创建企业项目”。

图 4-4 进入创建企业项目页面

步骤6 在创建企业项目页面，输入*“名称”*为“企业项目A”，单击“确定”，完成“企业项目A”创建。

步骤7 重复步骤5~6，创建“企业项目B”。

创建企业项目后，项目管理列表中显示新创建的“企业项目A”和“企业项目B”。

----结束

创建 IAM 用户及用户组

本节以创建名为“企业项目A_财务”的用户组、名为“Murphy”的用户，并将“Murphy”加入“企业项目A_财务”为例，介绍创建用户组、IAM用户的方法。

步骤1 创建用户组。

1. 在华为云控制台，单击“管理与监管”，选择“统一身份认证服务”。
2. 在统一身份认证服务的左侧导航栏中，单击“用户组”>“创建用户组”。

图 4-5 进入创建用户组页面

3. 在创建用户组页面，输入*“用户组名称”*为“企业项目A_财务”，单击“确定”，用户组“企业项目A_财务”创建完成。
4. 重复2~3为两个企业项目分别创建财务组、开发组、安全维护组、运营组。

创建用户组后，用户组列表中显示新创建的用户组。

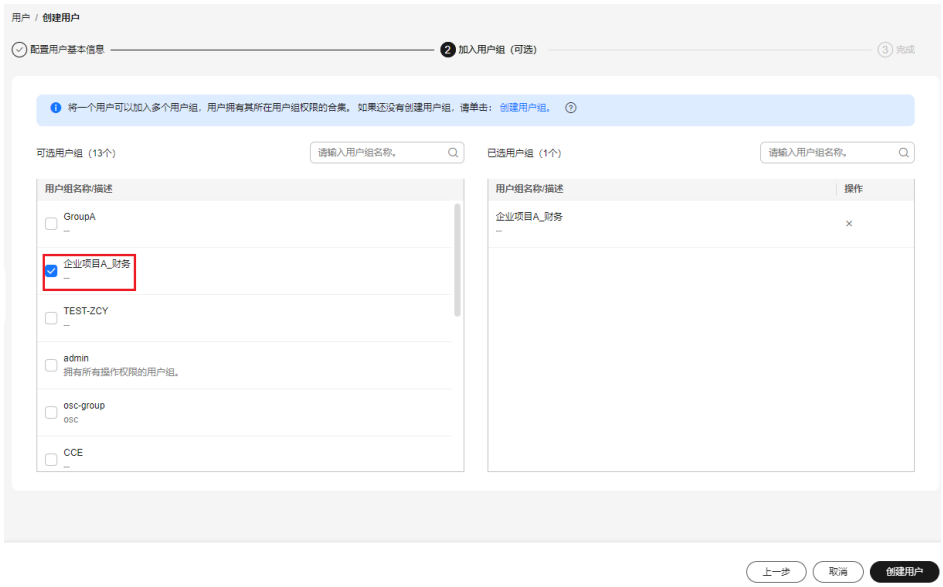
步骤2 创建IAM用户并加入用户组。

1. 在统一身份认证服务的左侧导航中，单击“用户”>“创建用户”。
2. 在创建用户页面，填写“用户信息”，选择“访问方式”（如图4-6），单击“下一步”。

图 4-6 创建 IAM 用户

3. 将创建的IAM用户“Murphy”加入相应的用户组“企业项目A_财务”，单击“创建用户”，IAM用户“Murphy”创建完成。

图 4-7 将 IAM 用户加入用户组



4. 重复1~3为所有员工创建IAM用户，并将其加入相应的用户组。

创建IAM用户后，用户列表中显示新创建的用户。在用户组的“用户组管理”页面可以查看各个用户组中的IAM用户。

----结束

企业项目与 IAM 用户组关联授权

本节介绍在IAM控制台给用户组授予企业项目权限。通过本节，您将了解企业项目与IAM用户组关联授权的详细步骤。

步骤1 管理员登录IAM控制台。

步骤2 在用户组列表中，单击“项目团队A_财务”用户组右侧的“授权”。

步骤3 在用户组选择策略页面中，搜索并选择“Enterprise Project BSS FullAccess”，单击“下一步”。

说明

如果系统策略无法满足需要，您还可以创建授权粒度更细的自定义策略。请单击“创建自定义策略”，跳转至“统一身份认证服务>创建自定义策略”，详情请参考**创建自定义策略**。

图 4-8 选择权限

步骤4 选择权限的作用范围为指定企业项目。

图 4-9 选择企业项目

步骤5 在企业项目列表中选择“企业项目A”。

步骤6 单击“确定”，完成用户组授权。

----结束

购买资源并关联企业项目

本节以购买弹性云服务器ECS并将其关联至企业项目“企业项目A”为例，介绍如何为企业项目购买资源。

步骤1 登录华为云控制台，单击页面左上角的 ☰ ，选择“计算 > 弹性云服务器 ECS”。

步骤2 单击页面右上角的“购买弹性云服务器”，系统进入购买页。

图 4-10 购买弹性云服务器

步骤3 **配置弹性云服务器各项信息**，在*“企业项目”*下拉列表中选择“企业项目A”。

图 4-11 关联企业项目

步骤4 单击页面右下角的“立即购买”跳转至支付页面，查看资源详情并提交订单。

步骤5 按照**步骤1**~**步骤4**的方法，为两个企业项目分别购买所需资源。

购买成功后，可以在企业管理页面中单击“企业项目A”、“企业项目B”右侧的“查看资源”查看企业项目中的资源。

说明

- 目前企业项目支持管理部分华为云，详情请参见：**企业管理服务支持的云服务**。
- 如果您已购买资源，仅需要关联资源与企业项目，可以使用企业管理服务提供的迁入功能，详情请参见：**为企业项目迁入资源**。

----结束

后续操作：企业项目管理

经过以上步骤，用户可以在“企业>项目管理>企业项目管理”页面，管理自己的企业项目。

- **资源管理：**单击企业项目右侧的“查看资源”，即可查看企业项目的已有资源，并**为企业项目迁入资源**。
- **人员管理：**单击企业项目右侧的“更多>权限管理”，系统将跳转至IAM控制台界面，在IAM控制台界面可查看企业项目所包含的用户、用户组，并修改用户、用户组及其权限。详细了解企业项目人员管理，请参见：**企业项目人员管理**。

- **财务管理：**单击企业项目右侧的“查看消费”，即可查看企业项目的订单、费用账单，并进行续费管理。详细了解企业项目财务管理，请参见：**管理企业项目的财务信息**。

5 访问密钥泄露处理方案

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。系统通过Access Key ID识别访问用户的身份，通过Secret Access Key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。

访问密钥泄露会对您账号下的资源安全带来威胁，导致账号下的核心资产泄露，产生非预期的费用或恶意勒索等。本文提供疑似泄露访问密钥场景的处理方案，当您的访问密钥疑似泄露时请按照本文方案进行处理，避免造成更大的安全风险。

华为云安全措施

华为云一直致力于保护您的云身份及云资源安全。当华为云发现您的访问密钥已经泄露，将通过您预留的联系方式及时通知您。为避免导致更大的资产损失，华为云有可能会采取限制该访问密钥的部分操作，如会限制该访问密钥创建的身份（如IAM用户、委托等），详情请参见**访问密钥限制性保护说明**。

⚠ 警告

请您务必及时关注短信、邮箱、电话等渠道的通知，并结合业务实际需求及时处置。同时，请及时关注您账号下的云资源情况，以免影响业务的正常运行。

说明

华为云作为云服务提供商，无法也不可能掌握您全部访问密钥的安全现状。根据安全责任共担模型，云上的安全由您和华为云共同承担。其中访问密钥属于账号或IAM用户的访问凭证，相关安全责任完全由您负责，因此建议您妥善保管访问密钥。

华为云账号（主账号）访问密钥疑似泄露处理方案

场景一：

若确认该访问密钥尚未在您的业务中使用，请在**我的凭证页面**直接停用并删除该访问密钥。

场景二：

若确认该访问密钥已经在使用中。请使用以下方案轮转访问密钥。

- **方案1：**在**我的凭证页面**，请先为账号创建一个新的访问密钥并妥善保管。同时将原访问密钥替换为新的访问密钥，验证业务正常运行后及时停用并删除原有的访问密钥。
- **方案2（推荐）：**建议您创建一个IAM用户，为用户创建访问密钥并授予其业务必需的最小权限，使用该访问密钥代替主账号的访问密钥。同时，请停用并删除主账号的原访问密钥。

⚠ 注意

访问密钥删除后无法恢复，建议先停用并确保对业务无影响后再删除。

IAM 用户访问密钥疑似泄露处理方案

场景一：

若确认该访问密钥尚未在您的业务中使用，请在**IAM控制台**直接停用并删除IAM用户的访问密钥。如您无权限，请联系有IAM操作权限的管理员。具体操作请参见**管理IAM用户的访问密钥**。

场景二：

若确认访问密钥已经在使用中且可以直接轮转，请尽快轮转。

请先创建一个新的访问密钥并妥善保管（每个IAM用户最多只能创建两个访问密钥）。同时将原访问密钥替换为新的访问密钥，验证业务正常运行后，在**IAM控制台**及时停用并删除原有的访问密钥。具体操作请参见**管理IAM用户访问密钥**。（访问密钥删除后无法恢复，建议先停用并确保对业务无影响后再删除）

场景三：

若确认访问密钥在使用中且短期内无法轮转，为降低访问密钥泄露的影响，您可以按照如下步骤进行处置。完成后务必尽快轮转。

步骤1 缩小访问密钥权限。

请根据您的实际业务诉求，尽快缩小疑似泄露访问密钥的权限，在不影响正常业务的情况下，禁止高危操作，避免核心资产受损。在访问密钥轮转后再解除该限制。

建议禁止的高危权限，例如：

- 禁止该IAM用户创建新的IAM用户和授权；
- 禁止计算资源实例的操作，如关闭ECS、BMS服务器等；
- 禁止存储资源实例的操作，如删除OBS桶、删除EVS云硬盘，删除RDS实例等；
- 禁止删除日志，如删除云日志LTS上的日志、删除CTS追踪器等。

具体操作，详见**创建自定义策略**、**给IAM用户授权**。

同时建议您明确实际业务需要的权限，将不需要的权限全部移除，确保当前针对该访问密钥的授权符合最小权限集的安全要求。

步骤2 开启IAM用户的登录保护。

建议您为华为云账号下所有可访问控制台的IAM用户开启登录保护，并建议您设置验证方式为安全等级更高的虚拟MFA。

1. 设置华为云账号下的IAM用户登录控制台必须开启登录保护。具体操作请参见**查看或修改IAM用户信息**。
2. 为用户绑定虚拟MFA设备。具体操作请参见**为IAM用户绑定MFA设备**。

步骤3 检查是否存在访问密钥异常操作。

检查访问密钥是否存在异常操作行为，并排查是否有其他疑似泄露的访问密钥。

检查方式：

1. 在**CTS控制台**的事件列表中，过滤筛选“操作用户”为疑似泄露访问密钥的用户，查看是否有异常操作行为。
2. 除检查已知存在泄露风险的访问密钥之外，还需进一步排查是否还有其他IAM用户和访问密钥存在异常操作行为。若发现异常行为，建议与对应人员确认操作是否由本人执行。若排查发现存在疑似泄露风险，建议按以下方式处理：
   - 疑似泄露的IAM用户如需继续使用，建议立即修改IAM用户密码并开启登录保护。
   - 疑似泄露的IAM用户如果为非正常创建或闲置，可先将其禁用，确认对业务无影响后再进行删除。
   - 如果访问密钥存在异常操作，参照上述方法先缩减权限后再进行轮转。

步骤4 检查是否存在异常费用。

若在**费用中心**检查发现存在异常费用和账单，请结合上述操作实施防护措施。

----结束

防止访问密钥泄露的长期方案

详情请参见**安全使用IAM最佳实践**。

6 访问密钥限制性保护说明

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。大量业内云上安全事件表明，访问密钥的泄漏可导致黑客利用访问密钥控制该账号进行退订、删除云上资源等操作，从而破坏云上业务的正常运行，甚至可能导致账号敏感数据的泄漏等严重安全问题。当华为云检测到您的访问密钥可能存在泄漏风险时，经过您的授权后，会对疑似泄漏的访问密钥或访问密钥创建的身份进行限制性保护（如限制登录控制台等），防止风险进一步扩大。

解除限制性保护

当您确认对应的访问密钥无泄漏风险，或已经对访问密钥进行轮转后，需要解除限制性保护时，可通过华为云工单系统**提交工单**进行处理。