# 统一身份认证服务

# 快速入门

**文档版本** 13

**发布日期** 2021-11-30

**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 入门前必读.....1
2 步骤 1：创建用户组并授权.....3
3 步骤 2：创建 IAM 用户并登录.....7
4 修订记录.....12

# 1 入门前必读

您可以通过本手册了解：

- 为什么要创建IAM用户
- 如何基于企业项目职能创建用户组
- 如何为用户组授权
- 如何为企业员工创建IAM用户
- 新创建的IAM用户如何登录华为云

## 前提条件

请确保您已拥有账号，若您还没有账号，请先进行注册。

## 示例场景

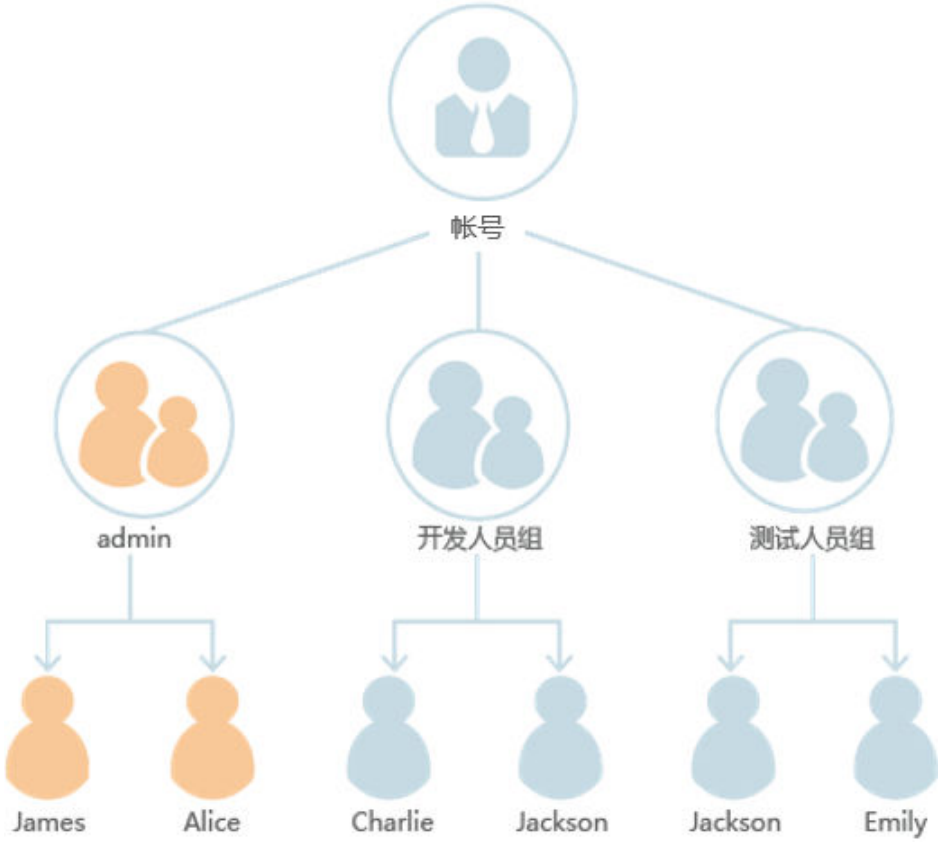
A公司是一家负责网站开发的公司，公司地址位于中国上海，公司中有三个职能团队。为了方便A公司统一购买、分配资源并管理用户，A公司的人员不需要每人都注册账号，而是由公司的管理员注册一个账号，在这个账号下创建IAM用户并分配权限，然后将创建的IAM用户分发给公司的人员使用。关于账号和IAM用户的概念，详情请参见：**IAM基本概念**。

本文以A公司使用IAM创建用户及用户组为例，帮助您快速了解，企业如何使用IAM完成服务权限的配置。

**A公司人员组成**

- 负责管理公司的人员以及资源的管理团队（对应**图1-1**中的“admin”），进行权限分配，资源调配等。团队成员包括James和Alice。
- 负责开发公司网站的开发团队（对应**图1-1**中的“开发人员组”）。团队成员包括Charlie和Jackson。
- 对开发团队开发出的网站进行测试的测试团队（对应**图1-1**中的“测试人员组”）。团队成员包括Jackson和Emily。其中Jackson同时负责开发及测试，因此他需要同时加入“开发人员组”及“测试人员组”，以分别获得两个用户组的权限。

**图 1-1** 用户管理模型




**A公司业务组成**

- admin组主要负责公司人员权限分配，需要使用IAM服务。
- 开发人员组在网站开发过程中，需要使用弹性云服务器（ECS）、弹性负载均衡（ELB）、虚拟私有云（VPC）、关系型数据库（RDS）、云硬盘（EVS）以及对象存储服务（OBS）。
- 测试人员主要负责网站的功能及性能测试，需要使用应用性能管理（APM）。

## 用户管理流程

1. A公司的管理员使用注册的账号登录华为云，创建“开发人员组”及“测试人员组”，并给用户组授权。操作步骤请参见：**步骤1：创建用户组并授权**。
2. A公司的管理员给三个职能团队中的成员创建IAM用户，并让他们使用新创建的用户登录华为云。操作步骤请参见：**步骤2：创建IAM用户并登录**。

# 2 步骤 1：创建用户组并授权

A公司的团队分为管理组（admin）、开发人员组和测试人员组。由于系统默认内置了admin组，用于拥有账号所有资源的使用及管理权限，因此A公司的团队只需要在IAM中再创建开发人员组及测试人员组即可。

## 创建用户组

**步骤1** A公司管理员，使用注册的华为账号开通并登录华为云。

**图 2-1** 登录华为云


**步骤2** 进入华为云“控制台”。

**图 2-2** 进入控制台


**步骤3** 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 2-3** 进入统一身份认证


**步骤4** 在统一身份认证服务，左侧导航窗格中，单击“用户组”>“创建用户组”。

**图 2-4** 创建用户组


**步骤5** 在“创建用户组”界面，输入“用户组名称”，单击“确定”，完成用户组创建。

**图 2-5** 输入用户组信息


**步骤6** 按照**步骤4**和**步骤5**的方法，创建“测试人员组”。

**----结束**

## 给用户组授权

A公司的开发人员需要使用的云服务为ECS、RDS、ELB、VPC、EVS和OBS，需要为“开发人员组”授予这六个服务的管理员权限。测试人员需要使用云服务APM，需要为“测试人员组”授予此服务的权限。完成用户组的授权后，用户组中的用户才可以使用这些云服务。**如需查看所有云服务的系统权限，请参见：系统权限**。

**步骤1** 确定所需权限。

通过查看**系统权限**，需要设置的权限如**表1**所示。其中“作用范围”由该服务的物理部署位置决定。对于项目级服务，如果在某个区域的项目中设置策略，则策略只在该项目中生效。

**表 2-1** 所需权限

| 用户组 | 使用的服务 | 所属区域 | 设置策略或角色 |
| --- | --- | --- | --- |
| 开发人员组 | ECS | 除全局区域外的其他区域 | ECS FullAccess |
| | RDS | 除全局区域外的其他区域 | RDS FullAccess |
| | ELB | 除全局区域外的其他区域 | ELB FullAccess |
| | VPC | 除全局区域外的其他区域 | VPC FullAccess |
| | EVS | 除全局区域外的其他区域 | EVS FullAccess |
| | OBS | 全局区域 | OBS OperateAccess |

| 用户组 | 使用的服务 | 所属区域 | 设置策略或角色 |
| --- | --- | --- | --- |
| 测试人员组 | APM | 除全局区域外的其他区域 | APM FullAccess |

**步骤2** 在用户组列表中，单击新建用户组“开发人员组”，右侧的“授权”。

**图 2-6** 授权


**步骤3** 设置区域级项目的权限。

1. 由表1可知，除OBS外，其它服务都是项目级服务。勾选需要授予用户组的项目级服务权限，单击“下一步”。
2. 选择授权范围方案为“区域项目”，并选择“华东-上海二”，单击“确定”。

   由于A公司位于上海，因此可以在“华东-上海二”设置权限，这样A公司成员访问华为云可减少网络时延，获得更快的访问速度。设置完成后，开发人员组仅在“华东-上海二”有访问权限，访问其它区域将提示没有权限。

**步骤4** 设置全局服务的权限。

1. 勾选需要授予用户组的全局服务权限“OBS OperateAccess”，单击“下一步”。
2. 选择授权范围方案为“全局服务”，单击“确定”。

**步骤5** 参考2-5的方法，给“测试人员组”授予“华东-上海二”“APM FullAccess”的权限。

**----结束**

# 3 步骤 2：创建 IAM 用户并登录

上一个章节已完成用户组的创建，本节将描述A公司使用已注册的账号，给公司成员创建IAM用户并加入用户组的操作，使得他们拥有独立的用户和密码，可以独立登录华为云平台并使用权限范围内的资源。

## 创建 IAM 用户

**步骤1** 在统一身份认证服务，左侧导航窗格中，单击“用户”>“创建用户”。

**步骤2** 配置基本信息。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 3-1** 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 3-1** 用户信息

| 用户信息 | 说明 |
| --- | --- |
| 用户名 | 必填。IAM用户登录华为云的用户名，此处以“James”和“Alice”为例。 |
| 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，可作为登录凭证，也可由IAM用户自己绑定。 |

| 用户信息 | 说明 |
| --- | --- |
| 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。 |
| 描述 | 选填。记录IAM用户相关信息。 |
| 外部身份ID | 选填。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。<br>为IAM用户配置IAM SSO类型的联邦用户单点登录时，“外部身份ID”为必填参数（不超过128个字符）。 |

**图 3-2** 配置访问方式


- 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。

**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。

**表 3-2** 配置凭证类型和登录保护

| 凭证类型与登录保护 | | 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）**。<br>**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。<br>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。<br>**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。<br>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（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账号安全性。<br>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3** 单击“下一步”，将用户加入到用户组（可选）。

- 将用户加入用户组，用户将具备用户组的权限，这一过程即给用户授权。
- 如需创建新的用户组，可单击“创建用户组”，填写用户组名称和描述（可选），创建成功后即可将用户加入到新创建的用户组中。

**说明**

“admin”为系统缺省提供的用户组，具有管理人员以及所有云服务资源的操作权限。A公司人员与用户组对应关系请参见：图1-1。

**步骤4** 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“访问方式”选择了“编程访问”且表2 配置凭证类型凭证类型勾选了“访问密钥”，可在此页面下载访问密钥。

**图 3-3** 用户创建成功


**步骤5** 参考步骤1-步骤4的方法，创建用户Charlie、Jackson和Emily，并加入对应的用户组。

**----结束**

## IAM 用户登录

通过前面章节，A公司在名为“A-Company”的账号中创建了名为James、Alice、Charlie、Jackson和Emily的IAM用户。完成IAM用户创建后，A公司管理员需要将账号名、IAM用户名及初始密码告知对应的员工，这些员工就可以使用自己的用户名及密码访问华为云。如果登录失败，IAM用户可以联系管理员重置密码。

**步骤1** 在登录页面，单击登录下方的“IAM用户”，在“IAM用户登录”页面，输入**“租户名/原华为云账号名”**、**“IAM用户名/邮件地址”**和**“密码”**。

**图 3-4** IAM 用户登录

- 租户名/原华为云账号名：IAM用户所属的账号。
- 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，例如“James”。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”，登录华为云。

**----结束**

# 4 修订记录

**表 4-1** 修订记录

| 日期 | 修订记录 |
| --- | --- |
| 2021-11-30 | 第十三次正式发布。<br>根据“授权”功能优化，修改**步骤1：创建用户组并授权**章节。 |
| 2021-09-02 | 第十二次正式发布。<br>根据“权限管理”功能优化，修改**步骤1：创建用户组并授权**章节。 |
| 2021-03-27 | 第十一次正式发布。<br>根据华为云统一ID进行全文刷新。 |
| 2020-12-30 | 第十次正式发布。<br>根据登录界面变更、安全设置功能变更、界面词条变更进行全文刷新。 |
| 2020-10-27 | 第九次正式发布。<br>根据登录方式变更刷新登录界面截图。 |
| 2020-06-08 | 第八次正式发布。<br>根据新增HUAWEI ID登录方式刷新以下章节：<br>**步骤1：创建用户组并授权**<br>**步骤2：创建IAM用户并登录** |
| 2020-02-10 | 第七次正式发布。<br>根据策略更名修改**步骤1：创建用户组并授权**章节。 |
| 2020-01-19 | 第六次正式发布。<br>根据界面变更刷新**步骤1：创建用户组并授权**章节。 |
| 2020-01-02 | 第五次正式发布。<br>根据界面风格变化刷新各章节图片。 |

| 日期 | 修订记录 |
| --- | --- |
| 2019-12-10 | 第四次正式发布。<br>根据界面变更修改**步骤1：创建用户组并授权**章节。 |
| 2019-11-20 | 第三次正式发布。<br>根据界面变更修改**步骤2：创建IAM用户并登录**章节。 |
| 2019-06-06 | 第二次正式发布。<br>优化**步骤1：创建用户组并授权**中授权步骤。 |
| 2019-02-26 | 第一次正式发布。 |