组织

最佳实践

文档版本	03
发布日期	2025-08-07

华为云计算技术有限公司

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

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

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 通过 Terraform 创建成员账号

Terraform是一款开源工具，用于安全有效地构建、更改和版本控制基础设施。用户通过这些配置文件声明他们想要的基础设施最终状态，而不需要具体指定如何实现这个状态。

Terraform的优势：

- 提升架构一致性：减少手动配置过程中的错误和配置漂移。
- 降低运维成本：通过编程方式管理虚拟机，减少手动配置硬件及更新的需求。
- 提升操作效率：简化系统配置、维护和管理，加速软件开发和部署。
- 加快部署速度：将繁琐的配置工作转变为简单的脚本执行，缩短应用发布时间。
- 降低操作风险：支持版本控制，降低配置错误的风险。

本章节将指导开发者如何使用Terraform创建成员账号，方便开发者高效地创建成员账号。

前提条件

获取访问密钥

获取访问密钥方式请参考**访问密钥**，该访问密钥必须具有管理账号内通过Organizations服务创建成员账号的权限。

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访问华为云API。

创建访问密钥成功后，您可以在访问密钥列表中查看访问密钥ID（AK），在下载的.csv文件中查看访问密钥（SK）。

准备 Terraform 环境

1. 安装Terraform执行环境

   Terraform提供了多种环境的安装包，具体可以参考官网(**https://developer.hashicorp.com/terraform/downloads**)。

   下面以Linux CentOS (系统需要有访问公网权限)为例指导安装Terraform。

   使用root用户登录linux系统，新建目录/home/Terraform，cd到Terraform目录执行如下命令:

```
sudo yum install -y yum-utils
sudo yum-config-manager --add-repo https://rpm.releases.hashicorp.com/RHEL/hashicorp.repo
sudo yum -y install terraform
```

2. 查看Terraform命令详情

   执行Terraform后会显示Terraform命令详情，查看更多命令详情请参考**https://developer.hashicorp.com/terraform/cli**。

3. 查看Terraform语法简介

   Terraform配置语言主要基于HCL语法，具有配置简单、可读性强等特点，并且兼容JSON语法。详情参见官网介绍**https://developer.hashicorp.com/terraform/language**，此文不做赘述。

编写账号资源脚本

华为云在Terraform已经注册了provider，函数作为资源挂在华为云的provider下。参考文档**https://registry.terraform.io/providers/huaweicloud/huaweicloud/latest/docs/resources/organizations_account**。

提供如下样例：

在服务器创建一个main.tf文件，将如下脚本拷贝到main.tf上并保存。

```
terraform {
  required_providers {
    huaweicloud = {
      source  = "huaweicloud/huaweicloud"
      version = ">= 1.40.0"
    }
  }
}

provider "huaweicloud" {
  access_key = "*******"   #前面获取的key
  secret_key = "*******"   #前面获取的key
}
resource "huaweicloud_organizations_account" "test"{
  name  = "account_test_name"
}
```

access_key secret_key 需要替换为**访问密钥**生成的密钥。

使用 Terraform 命令创建成员账号

进入文件路径，执行terraform init命令初始化一个包含Terraform代码的工作目录。

```
[root@function-deploy [redacted]# terraform init

Initializing the backend...

Initializing provider plugins...
- Reusing previous version of local-registry/huaweicloud/huaweicloud from the dependency lock file
- Using previously-installed local-registry/huaweicloud/huaweicloud v1.45.1

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
```

执行terraform apply命令，在Enter a value: 处输入yes。

执行成功代表成员账号创建完成。

2 通过 IAM 身份中心登录新创建的账号

应用场景

企业深度上云场景下，新业务上云或者现有业务扩展常常意味着全新的成员账号创建以及账号内资源配置。鉴于业界最佳实践，组织内成员账号的账号凭证（如账号级密钥以及账号密码等）需进行强管控，防止权限扩展造成业务风险。

本文主要介绍Organizations新建账号后，业务人员如何登录该账号进行操作。

前提条件

已开启IAM身份中心服务。

步骤一：创建业务账号

1. 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台，进入组织管理页面。
2. 单击组织结构树上方的“添加”，单击“添加账号”。
3. 在弹窗中，选择“创建新账号”。
4. 输入账号名称，账号描述根据需要选择输入。
5. 单击“确定”，创建成功的账号将会显示在列表中。

步骤二：创建业务团队用户组

1. 进入“IAM身份中心”控制台。
2. 单击左侧导航栏的“用户组管理”，进入“用户组管理”页面。
3. 单击页面右上方的“创建组”，进入创建用户组页面。
4. 在“创建用户组”界面，输入“名称”和“描述”。
5. 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。

步骤三：创建业务团队用户

1. 单击“IAM身份中心”控制台左侧导航栏的“用户管理”，进入“用户管理”页面。
2. 单击页面右上方的“创建用户”，进入创建用户页面。
3. 配置用户信息（包括用户名、邮箱地址等，勾选“向用户发送一封包含密码设置说明的邮件”），配置完成后，单击页面右下角的“下一步”。

4. 进入“分配用户组”页面，勾选要加入的业务团队用户组，将用户加入到用户组。配置完成后，单击页面右下角的“下一步”。
5. 进入“确认创建”页面，确认配置无误后，单击页面右下角的“确定”，用户创建完成，用户列表中显示新创建的用户。

步骤四：创建权限集

1. 在“IAM身份中心”控制台左侧导航栏中，选择“多账号权限 > 权限集”，进入“权限集”页面。
2. 单击页面右上方的“创建权限集”，进入创建权限集页面。
3. 在“基本信息”页签中配置权限集的基本信息，配置完成后，单击“下一步”。
4. 进入“策略设置”页签，配置权限集的系统策略、自定义身份策略和自定义策略，单击“下一步”。
5. 进入“配置确认”页面，确认配置无误后，单击页面右下角的“确定”，权限集创建完成。

步骤五：业务账号关联用户组和权限集

1. 在“IAM身份中心”控制台左侧导航栏中，选择“多账号权限 > 账号权限管理”，进入“账号权限管理”页面。
2. 在账号列表中勾选新建的业务账号，单击左上方的“关联用户或组”。
3. 进入“分配用户/组”页面，在列表中勾选需要关联的业务用户组，单击“下一步”。
4. 进入“选择权限集”页面，在权限集列表中勾选需要关联的权限集，单击“下一步”。
5. 进入“配置确认”页面，确认配置无误后，单击页面右下角的“确定”，为账号关联用户/组和权限集完成。

步骤六：用户登录并访问资源

1. 业务团队用户打开邮箱空间，点击华为云发送的“密码设置”邮件内的“接受邀请”入口。
2. 修改登录密码后点击“完成”，输入用户名点击“下一步”后填写及密码，点击“登录”。
3. 业务账号下的资源根据关联的权限集将显示登录入口，单击操作列的“访问控制台”，即可访问此账号下对应权限集控制的资源。

3 通过 CTS 跨账号收集组织内操作审计日志

应用场景

企业用户普遍采用多账号策略隔离云上不同的业务以及职能，但多账号场景下合规审计人员如何获取各个业务环境下发生的历史操作成为一个难题，侵入每个账号进行日志采集存在误操作风险而且效率极低。

本文主要介绍如何基于Organizations可信服务，配置多账号环境下，将组织内操作审计日志汇聚在日志存档账号内。

开启云审计可信服务

1. 以组织管理员或管理账号的身份登录华为云，进入华为云Organizations控制台。
2. 左侧菜单栏选择“可信服务”，找到云审计服务，单击“启用”，即可开启云审计可信服务。
3. 单击云审计服务右侧的“设置委托管理员”按钮并选中日志存档账号，为云审计服务设置委托管理员。

配置组织追踪器

1. 登录委托管理员账号（即日志存档账号）管理控制台，进入云审计服务控制台。
2. 在左侧导航栏选择“追踪器”，单击右上方的“开通云审计服务”按钮，系统会自动为您创建一个名为system的管理类事件追踪器，详情请参见**开通云审计服务**。
3. 在“追踪器”列表中，单击管理类事件追踪器右侧的“配置”按钮。
4. 进入配置追踪器基本信息页面，开启“应用到我的组织”开关，点击“下一步”。
5. 在配置转储页面，打开转储到OBS桶并选择日志存档账号内已创建的日志桶。
6. 单击“下一步 > 配置”，完成配置组织追踪器。