Organizations

Best Practices

Issue	03
Date	2025-08-07

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Creating a Member Account Using Terraform

Terraform is an open-source tool that lets you build, change, and version infrastructures securely and efficiently. You just define the desired final state of your infrastructure in configuration files. There is no need to specify how to achieve that state.

Terraform advantages:

- More consistent architecture: Manual configuration errors and drift are reduced.
- Lower O&M costs: VMs are managed with programming, reducing the need for manual hardware configuration and update.
- Improved operational efficiency: System configuration, maintenance, and management are simplified, and software development and deployment are accelerated.
- Faster deployment: Complex configuration tasks are simplified using scripts, which speeds up application release.
- Fewer operation risks: Version control is supported, reducing configuration errors.

This section describes how developers use Terraform to efficiently create member accounts.

Prerequisites

You have obtained an access key.

For details about how to obtain an access key, see **Access Keys**. The access key must have the permission to create member accounts using the management account in Organizations.

An access key comprises an access key ID (AK) and secret access key (SK) and is used as a long-term identity credential to access Huawei Cloud APIs.

After an access key is created, you can view the AK in the access key list and the SK in the downloaded CSV file.

Preparing a Terraform Environment

1. Install Terraform.

   Terraform provides installation packages for different environments. For details, see **https://developer.hashicorp.com/terraform/downloads**.

   The following uses Linux CentOS (public network accessible) as an example to describe how to install Terraform.

   Log in to the Linux OS as the user **root**, create the **/home/Terraform** directory, use **cd** to navigate to this directory, and then install Terraform:

   ```
   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. View Terraform command details.

   After Terraform commands are executed, command details are displayed. For details, see **https://developer.hashicorp.com/terraform/cli**.

3. View the Terraform syntax.

   Terraform's configuration uses HashiCorp Configuration Language (HCL) syntax. It is easy to configure and read and is compatible with the JSON syntax. For details, see **https://developer.hashicorp.com/terraform/language**.

Compiling Scripts for Account Resources

Huawei Cloud has been registered with Terraform as a provider. You can add your functions as the resources of the provider. For details, see **https://registry.terraform.io/providers/huaweicloud/huaweicloud/latest/docs/resources/organizations_account**.

The following is an example:

Create file **main.tf** on the server, copy the following script to this file, and save it.

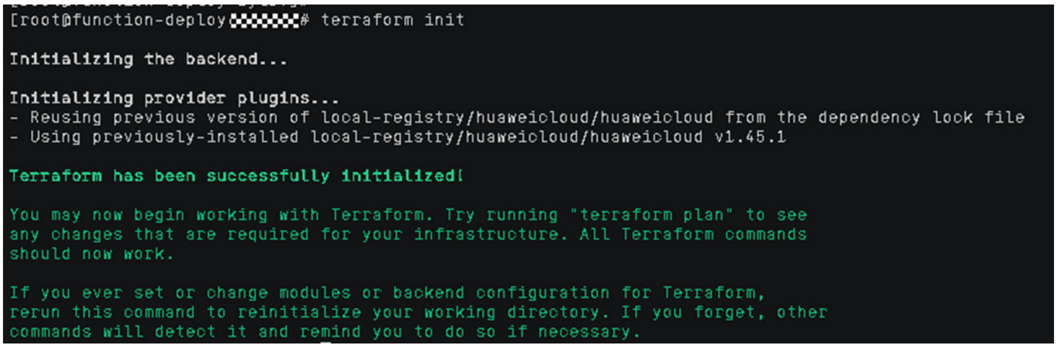
```
terraform {
  required_providers {
    huaweicloud = {
      source  = "huaweicloud/huaweicloud"
      version = ">= 1.40.0"
    }
  }
}

provider "huaweicloud" {
  access_key = "*******"   # Obtained AK
  secret_key = "*******"   # Obtained SK
}
resource "huaweicloud_organizations_account" "test"{
  name  = "account_test_name"
}
```

Replace **access_key** and **secret_key** with the keys generated in **Access Keys**.

Creating a Member Account by Running Terraform Commands

Go to the file path and run the **terraform init** command to initialize a working directory that contains the Terraform code.



```
[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.
```

Run the **terraform apply** command and enter **yes** in the **Enter a value:** row.

If the execution is complete, the member account is created.

2 Logging In with the New Account via IAM Identity Center

Application Scenarios

When enterprises migrate new services to the cloud or expand existing services for diving into the cloud, they create new member accounts and configure resources for those accounts. In keeping with industry best practices, member account credentials (such as account keys and passwords) must be strictly controlled to prevent service risks caused by permission explosion.

This section describes how to sign in with the new account created in Organizations.

Prerequisites

You have enabled IAM Identity Center.

Step 1: Creating a Service Account

1. Log in to Huawei Cloud as an organization administrator or using the management account, navigate to the Organizations console, and go to the **Organization** page.
2. Click **Add** and click **Add Account**.
3. Select **Create new** in the displayed dialog box.
4. Enter an account name. You can enter the account description as required.
5. Click **OK**. The new account is added to the list.

Step 2: Creating a Group for the Service Team

1. Navigate to the IAM Identity Center console.
2. In the navigation pane, choose **Groups**.
3. Click **Create Group** in the upper right corner.
4. On the displayed page, enter a group name and description.
5. Click **OK**. An IAM Identity Center group is created and displayed in the group list.

Step 3: Creating a User for the Service Team

1. In the navigation pane of IAM Identity Center, choose **Users**.
2. Click **Create User** in the upper right corner.
3. Configure user information (including the username and email address), select **Send an email to this user with password setup instructions**, and click **Next**.
4. On the displayed page, select a group, add the user to this group, and click **Next**.
5. On the **Confirm** page, confirm the configuration and click **OK**. The IAM Identity Center user you created is displayed in the user list.

Step 4: Creating a Permission Set

1. In the navigation pane of IAM Identity Center, choose **Multi-Account Permissions** > **Permission Sets**.
2. On the displayed page, click **Create Permission Set** in the upper right corner.
3. On the **Specify Details** page, configure basic information for the permission set and click **Next**.
4. On the **Set Policy** page, configure system-defined policies, custom identity policies, and custom policies for the permission set, and click **Next**.
5. On the **Confirm** page, confirm the configuration and click **OK**.

Step 5: Associating the Service Account with the Group and Permission Set

1. In the navigation pane of IAM Identity Center, choose **Multi-Account Permissions** > **Accounts**.
2. Select the new service account from the account list and click **Assign User/Group** in the upper left corner.
3. On the **Select User/Group** page, select the group to be associated and click **Next**.
4. On the **Select Permission Set** page, select the permission set to be associated and click **Next**.
5. On the **Confirm** page, confirm the configuration and click **OK**.

Step 6: Logging In as an IAM Identity Center User and Accessing Resources

1. Open your email and click the link to accept the invitation in the password setting email sent by Huawei Cloud.
2. Change the password. Then, enter the username and click **Next**. Enter the password and click **Lon In**.
3. Click **Access Console** in the **Operation** column to access resources allowed by the permission set associated with the service account.

3 Collecting Operation Logs Across Accounts Using CTS

Application Scenarios

Enterprises typically use different accounts to isolate different services and functions on the cloud. However, it is difficult for compliance auditors to obtain operation records for each service in an environment with multiple accounts. Collecting all the logs generated by all of the different accounts is time-consuming and error-prone.

This section describes how to aggregate operation audit logs of multiple accounts in an organization into the log archive account using an Organizations' trusted service.

Configuring CTS as a Trusted Service

1. Log in to Huawei Cloud as an organization administrator or using the management account and navigate to the **Organizations** console.
2. In the navigation pane, choose **Services**. On the displayed page, locate CTS and click **Enable Access** in the **Operation** column to configure CTS as a trusted service.
3. Locate CTS and click **Specify Delegated Administrator** in the **Operation** column. In the displayed dialog box, select the log archive account to set a delegated administrator for CTS.

Configuring an Organization Tracker

1. Log in to the management console as the delegated administrator (log archive account) and navigate to the CTS console.
2. In the navigation pane, choose **Tracker List** and click **Enable CTS** in the upper right corner. The system automatically creates a management tracker called **system**. For details about how to enable CTS, see **Enabling CTS for the First Time**.
3. In the tracker list, locate tracker **system** and click **Configure** in the **Operation** column.
4. On the **Modify Tracker** page, toggle on **Apply to Organization** and click **Next**.

5. On the **Configure Tracker** page, toggle on **Transfer to OBS** and select the log bucket created by the log archive account.
6. Click **Next** and click **Configure**. The organization tracker is configured.