Organizations

Service Overview

Issue	01
Date	2024-07-22

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei 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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 What Is Organizations?

Overview

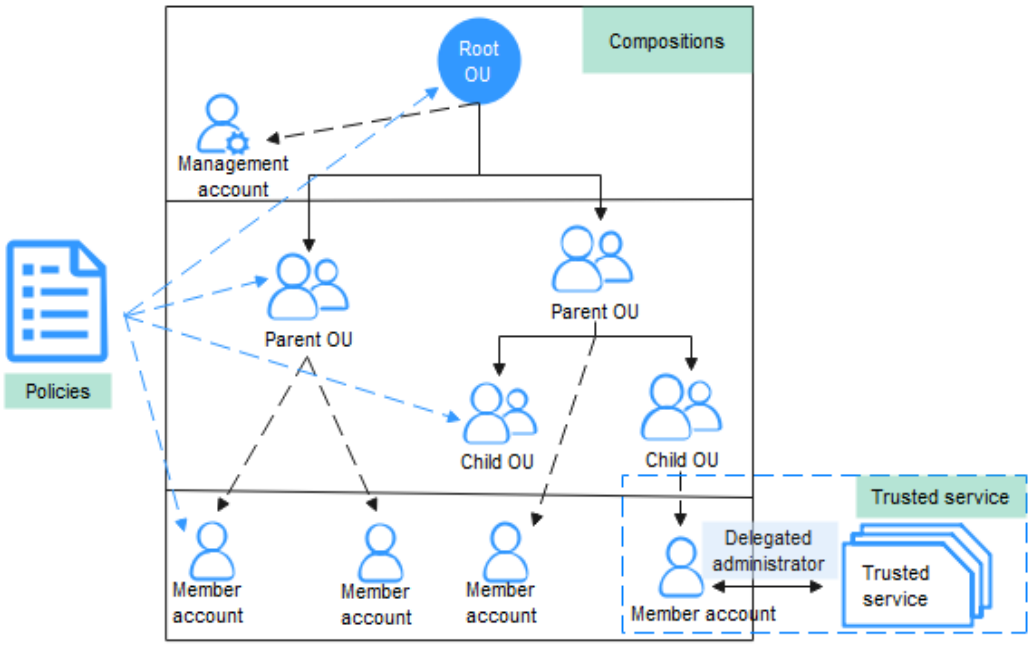
The Organizations service helps you govern multiple accounts within your organization. It enables you to consolidate multiple Huawei Cloud accounts into a single organization so you can manage them all in one place. You can centrally manage policies in Organizations. This helps you better meet the security and compliance requirements of your business.

Organizations is a free service. You only need to pay for the cloud services or resources used in your accounts.

System Architecture

The system architecture of an organization consists of entities, policies, and trusted services.

Figure 1-1 Organizations system architecture



Entities

- **Organization**

  An entity that you create to manage multiple accounts. Each organization is composed of one management account, multiple member accounts, a root organizational unit (OU), and other OUs. An organization has exactly one management account along with several member accounts. You can organize the accounts in a hierarchical, tree-like structure with the root OU at the top and nested OUs under it. Each member account can be directly under the root OU or placed under one of the other OUs.

- **Root OU**

  Organizations automatically generates the root OU for you when you create an organization. The root OU is located at the top of the tree, and its branches represent other OUs and accounts reaching down.

- **OU**

  A container or grouping unit for member accounts. It can be understood as a department, a subsidiary, a project team, or the like, of your enterprise. An OU can also contain other OUs. Each OU can have exactly one parent OU, but a parent OU can have multiple child OUs or nested member accounts.

- **Management account**

  A standard Huawei Cloud account. With the Organizations service, you can use the management account to create an organization and manage OUs, accounts, and policies for the organization. You can also use the management account to manage policies within the organization and enable trusted services for Organizations.

- **Member account**

  An account you created in your organization or you invited to join your organization via the Organizations service. Each member account is a standard HUAWEI ID or Huawei Cloud account and can be directly in the root OU or placed in one of the other OUs.

- **Invitation**

  The process of inviting other accounts to join your organization. Only the management account can issue invitations. The invited accounts can join an organization only after they accept the invitations. The billing of these accounts is not changed after they join the organization.

Policies

- **Service control policies (SCPs)**

  A type of organization policy that you can use to manage permissions in your organization. The management account can use SCP to limit the permissions that can be assigned to member accounts in an organization. You can attach an SCP to your organization, OUs, or member accounts. Any SCP attached to an organization or OU affects all the accounts within the organization or under the OU. For details, see **Overview of an SCP**.

- **Tag policies**

  Tag policies are a type of policy that can help you standardize tags across resources in your organization's accounts. You can attach tag policies to organizations, OUs, and member accounts. A tag policy is only applied to tagged resources and tags that are defined in that policy.

Trusted Services

- **Trusted service**

  A Huawei Cloud service that is entrusted by Organizations to provide organizational management capabilities. After you enable a Huawei Cloud service as a trusted service, the trusted service creates a service-linked agency in the member account. The agency allows the trusted service to execute the tasks that are described in the trusted service's documentation. The trusted service extends management capabilities across multiple accounts within your organization. For details about supported trusted services, see **Trusted Services for Organizations**.

- **Delegated administrator account**

  A member account that has special permissions in an organization. The management account of your organization can designate a member account to be a delegated administrator account for a trusted service. All the users in the delegated administrator account will have organizational management capabilities.

Accessing Organizations

You can access Organizations using the management console or HTTPS-compliant application programming interfaces (APIs).

- Using the management console

  The management console is a web-based GUI where you can easily perform various operations. Log in to the **management console**, and choose **Management & Governance** > **Organizations**.

- Using APIs

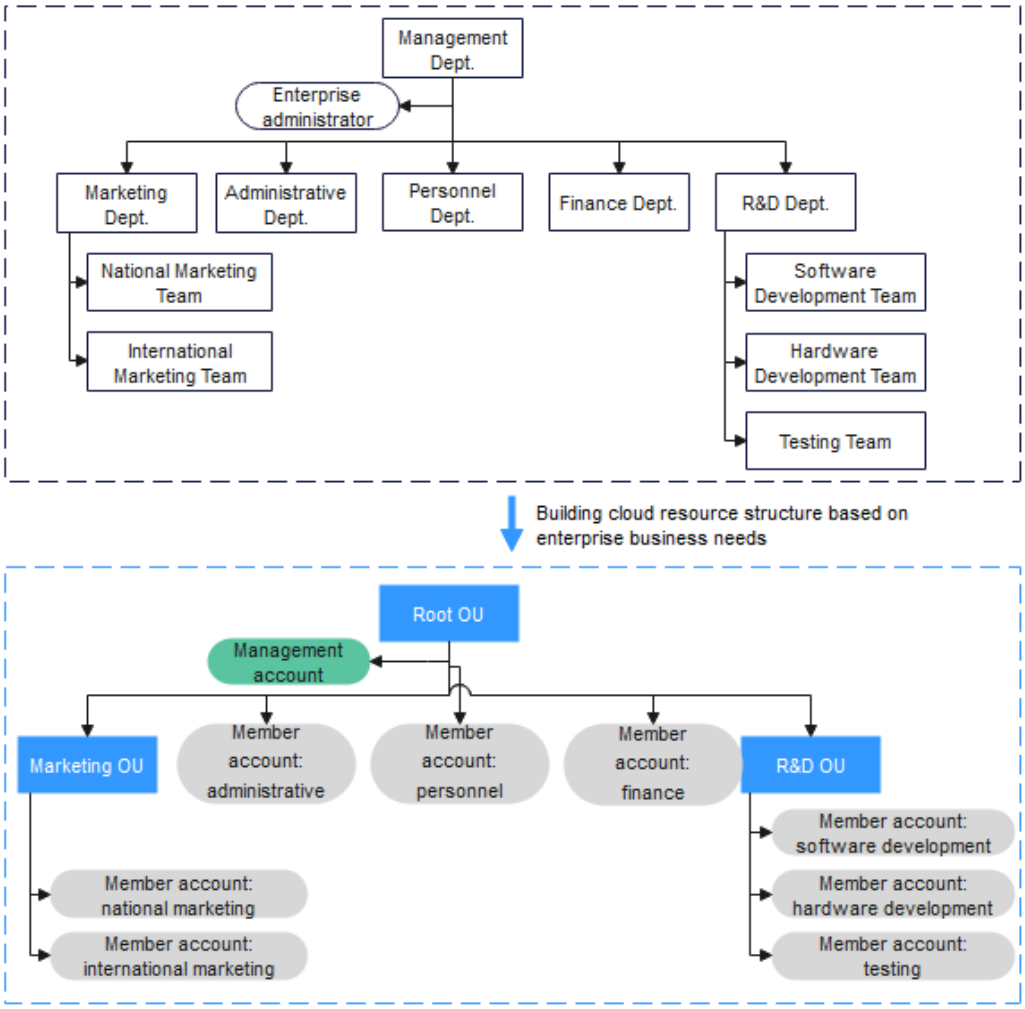
  You can use APIs to integrate Organizations into a third-party system for secondary development. For detailed operations, see **Organizations API Reference**.

2 Application Scenarios

Building a Cloud Resource Structure

If your enterprise has multiple branches, departments, or different service applications, you can use Organizations to build a hierarchical cloud resource structure suited to your own management and operational methods.

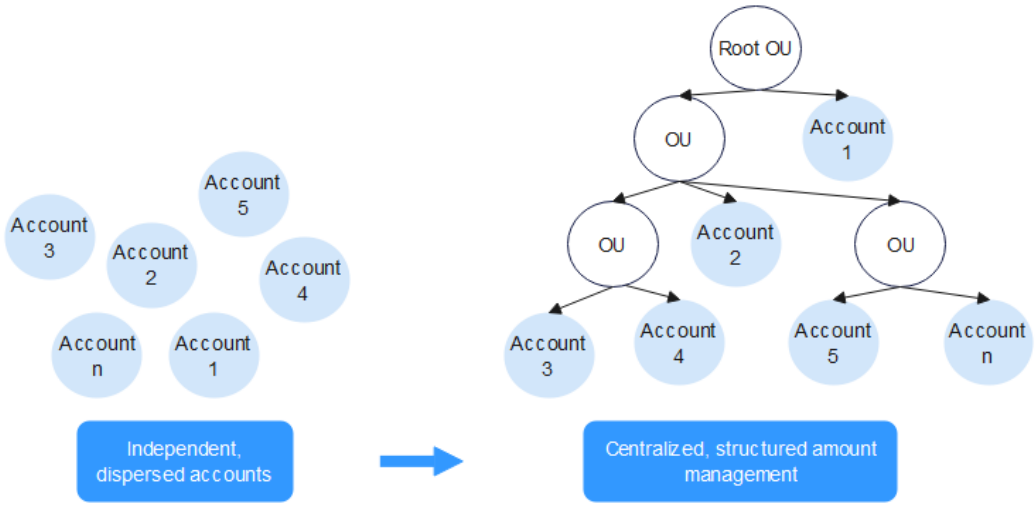
Figure 2-1 Sample cloud resource structure tailored for enterprise requirements



Centrally Managing Multiple Enterprise Accounts

If your enterprise has multiple Huawei Cloud accounts and you want to centrally manage these accounts and their resources, you can use Organizations to create an organization for centralized management of these otherwise scattered accounts.

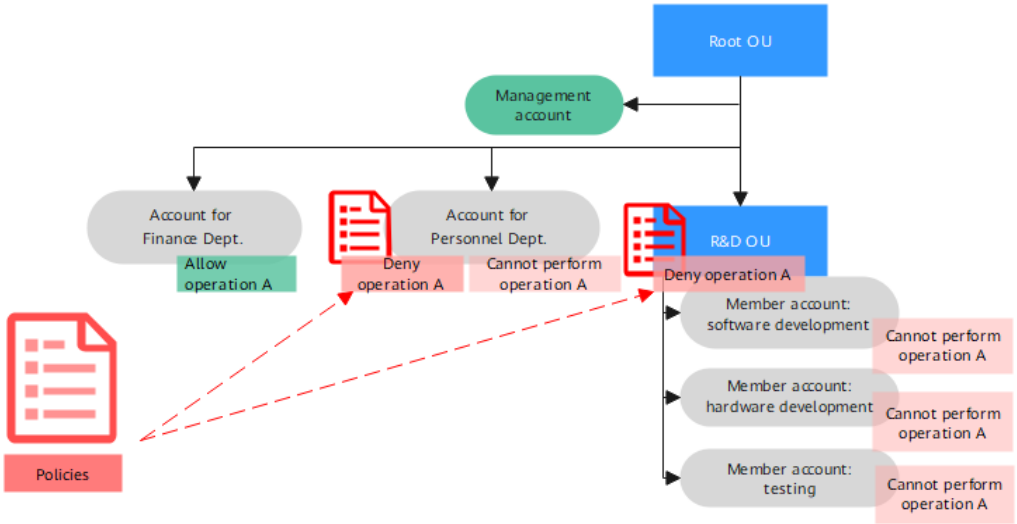
Figure 2-2 Centralized management of multiple enterprise accounts



Preventing Business Violations

To meet certain internal or external requirements, your enterprise may need to specify regulations for different departments and business environments (production, testing, or development). Organizations can help you proactively intercept nonconforming behavior and prevent compliance violations.

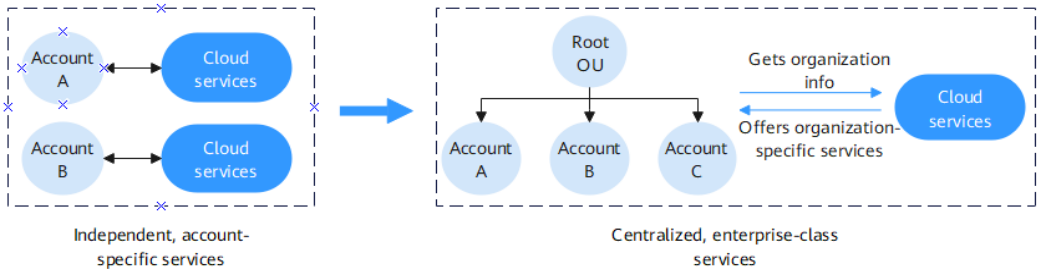
Figure 2-3 Policy-based behavior control



Providing Enterprise-Class Governance Capabilities

Cloud services, such as Config, are integrated into Organizations to provide you with enterprise-class capabilities, such as centralized resource audits, operational audits, and resource sharing among multiple services within a given resource architecture.

Figure 2-4 Enterprise-class governance



3 Function Overview

The Organizations service provides the following functions:

- Centralized account management

  Invite multiple accounts to join an organization or create accounts in the organization and then group them hierarchically to meet enterprise management or operational requirements.
- Centralized action control per account

  The organization administrator uses service control policies (SCPs) to limit the permissions that can be assigned to an organization or the OUs in an organization. The SCPs limit which cloud service consoles and APIs the member accounts in the organization can access.
- Integration with other Huawei Cloud services

  Integrate Organizations with other Huawei Cloud services (trusted services) to enable the services to perform organization-wide operations. For details about trusted services and related operations, see **Trusted Services for Organizations**.

Table 3-1 Organizations functions

Function	Description	Reference
Organization management	You can create an organization and invite other accounts to join your organization. You can also view details about your organization, root OU, other OUs, and accounts. If the organization is no longer needed, you can delete it.	**Managing Organizations**
OU management	You can use your management account to add, modify, view, and delete OUs.	**Managing OUs**

Function	Description	Reference
Account management	You can use your management account to invite member accounts to join your organization, create accounts, close accounts, change the OU holding member accounts, view details about the member accounts, remove member accounts, and enable or disable regions.	**Managing Accounts**
Service control policies	You can use your management account to create, modify, and delete SCPs, and also to attach SCPs to or detach SCPs from OUs and accounts.	**Managing SCPs**
Tag policies	You can use your management account to create, modify, and delete tag policies, and also to attach tag policies to or detach tag policies from OUs and accounts.	**Managing Tag Policies**
Trusted services	You can use your management account to enable or disable a trusted service for Organizations and also to designate a member account as the delegated administrator of that trusted service.	**Managing Trusted Services**
Tag management	You can use tags to identify and search for cloud resources. You can add tags to the following organization entities: root OU, other OUs, accounts, and service control policies (SCPs).	**Managing Tags**

4 Permissions

If you need to assign different permissions to personnel in your management account, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely access Huawei Cloud resources.

With IAM, you can create IAM users and assign permissions enabling them to control their access to specific resources. For example, if you want some of your employees to invite member accounts to join an organization but do not want them to manage policies, you can create IAM users in the management account and grant permission to invite member accounts but not permission to create or modify policies.

If your Huawei Cloud account does not require individual IAM users for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account.

For more information about IAM, see **Identity and Access Management Service Overview**.

System-defined Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach permissions policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

Organizations is a global service deployed for all regions. When you set the authorization scope to **Global services**, users have permission to access Organizations in all regions.

You can grant permissions by using roles and policies.

- Roles: A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. Huawei Cloud services depend on each other. When you grant permissions using roles, you also need to attach any existing role dependencies. Roles are not ideal for fine-grained authorization and least privilege access.

- Policies: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by Organizations, see **Permissions and Supported Actions**.

Table 4-1 lists all the system-defined permissions for Organizations.

Table 4-1 System-defined permissions for Organizations

Role/Policy Name	Description	Type	Dependencies
Organizations FullAccess	Users with these permissions can create, modify, delete, and view any information about Organizations.	System-defined policy	N/A
Organizations ReadOnlyAccess	Users with these permissions can view organization information, but not make any changes.	System-defined policy	N/A

Table 4-2 lists the common operations supported by system-defined permissions for Organizations.

Table 4-2 Common operations supported by system-defined permissions

Operation	Organizations FullAccess	Organizations ReadOnlyAccess
Creating an organization	Supported	Not supported
Viewing details about an organization	Supported	Supported
Deleting an organization	Supported	Not supported
Creating an OU	Supported	Not supported
Modifying an OU	Supported	Not supported
Viewing details about an OU	Supported	Supported
Deleting an OU	Supported	Not supported
Inviting an account to join your organization	Supported	Not supported
Creating an Account	Supported	Not supported
Closing an account	Supported	Not supported

Operation	Organizations FullAccess	Organizations ReadOnlyAccess
Moving an account to another OU	Supported	Not supported
Viewing details about an account	Supported	Supported
Removing a member account from your organization	Supported	Not supported
Enabling SCP	Supported	Not supported
Disabling SCP	Supported	Not supported
Creating an SCP	Supported	Not supported
Modifying an SCP	Supported	Not supported
Viewing details about an SCP	Supported	Supported
Deleting an SCP	Supported	Not supported
Attaching an SCP	Supported	Not supported
Detaching an SCP	Supported	Not supported
Enabling a trusted service	Supported	Not supported
Disabling a trusted service	Supported	Not supported
Configuring a delegated administrator	Supported	Not supported
Adding a tag	Supported	Not supported
Editing a tag	Supported	Not supported
Viewing tag details	Supported	Supported
Deleting a tag	Supported	Not supported

Helpful Links

- **What Is IAM?**
- **Creating an IAM User and Granting Organizations Permissions**
- **Permissions and Supported Actions**

5 Notes and Constraints

Notes

- Before using Organizations, you need to enable Enterprise Center. For details, see **Enabling Enterprise Center**.
- You can only use the master account of the Enterprise Center to create an organization.
- The management account of an organization cannot invite accounts of a different type to join the organization. For example, the management account registered with the Huawei Cloud Chinese Mainland website cannot invite any accounts from the Huawei Cloud International website to join its organization, and vice versa.

Quotas

Table 5-1 Quotas for Organizations

Item	Default Value	Applying for a Higher Quota
Number of organizations allowed in an account	1 **NOTE** Member accounts are not allowed to create organizations.	N/A
Number of root OUs in an organization	1	N/A
Number of OUs in an organization	1,000 **NOTE** The root OU is excluded from this number.	N/A
Number of OU levels allowed in an organization	5 **NOTE** The root OU and member accounts are excluded from this number.	N/A

Item	Default Value	Applying for a Higher Quota
Number of member accounts in an organization	10	Submit a service ticket.
Maximum number of member accounts the organization administrator can create concurrently	5	N/A
Maximum number of member accounts the organization administrator can close in a 30-day period	10% of active member accounts (The maximum account closure is 200 even if 10% of the active accounts exceeds 200.)	N/A
Maximum number of member accounts the organization administrator can close concurrently	3	N/A
Maximum number of invitation attempts you can perform in a 24-hour period	20	N/A
Valid period of an invitation	14 days	N/A
Duration for storing invitation records in lists	1 year	N/A
Number of SCPs you can create in an organization	1,000	N/A
Length of an SCP	5,120 characters	N/A
Number of tag policies you can create in an organization	1,000	N/A
Length of a tag policy	10,000	N/A
Number of tags you can attach to a root, OU, account, SCP, or tag policy	20	N/A
Maximum number of SCPs you can attach to a root, OU, or account	5	N/A

Item	Default Value	Applying for a Higher Quota
Maximum number of tag policies you can attach to a root, OU, or account	10	N/A

6 Basic Concepts

The commonly used concepts in Organizations include organization, root organizational unit (OU), other OUs, service control policies, URN, and principals.

Organization

An organization is an entity that you create to manage multiple accounts. Each organization is composed of one management account, multiple member accounts, a root OU, and other OUs. An organization has exactly one management account along with several member accounts. You can organize the accounts in a hierarchical, tree-like structure with the root OU at the top and nested OUs under it. Each member account can be directly under the root OU or placed under one of the other OUs.

Root OU

Organizations automatically generates the root OU for you when you enable Organizations to create an organization. The root OU is located at the top of the tree, and its branches represent other OUs and accounts reaching down.

OUs

An OU is a container or grouping unit for member accounts. It can be understood as a department, a subsidiary, a project team, or the like, of your enterprise. An OU can also contain other OUs. Each OU can have exactly one parent OU, but a parent OU can have multiple child OUs or nested member accounts.

Service Control Policies

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. The management account can use SCP to limit the permissions that can be assigned to member accounts in an organization. You can attach an SCP to your organization, OUs, or member accounts. Any SCP attached to an organization or OU affects all the accounts within the organization or under the OU. For details, see **Overview of an SCP**.

Tag Policies

Tag policies are a type of policy that can help you standardize tags across resources in your organization's accounts. A tag policy is only applied to tagged

resources and tags that are defined in that policy. For details, see **Overview of a Tag Policy**.

URN

A uniform resource name (URN) is used to uniquely identify a cloud service resource.

A URN is in the following format: <service-name>:<region>:<account-id>:<type-name>:<resource-path>

- **service-name**: the abbreviation of a cloud service name in lowercase, for example, **ecs**. The abbreviation must be valid and cannot be a wildcard.
- **region**: the region where the resource is located, for example, **cn-north-1**. If the resource is a global service resource, leave this field blank or use asterisks (*) to replace it.
- **account-id**: the ID of the account. The value **system** indicates public system resources, such as system-defined policies.
- **type-name**: the resource type in lower camel case.
- **resource-path**: the resource path whose format is defined by the cloud service.

