Resource Access Manager

Service Overview

Issue 01

Date 2024-03-15

HUAWEI

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 RAM?

Overview

Resource Access Manager (RAM) helps you securely share resources across accounts. If you have several Huawei Cloud accounts, you can create resources once in one account and use RAM to share those resources with the other accounts, eliminating the need to create duplicate resources in each account. For the specific cloud services and resource types supported by RAM, see **Sharable Cloud Services and Resource Types**.

If your account is managed by **Organizations**, you can directly share resources with member accounts, OUs, or the entire organization. You can also specify an account ID to share resources with that account, regardless of whether the account is part of an organization.

Functions

Managing resource shares

You can use RAM to centrally manage resource shares. Specifically, as a resource owner, you can share a specified resource with an organization, OU, or account, and also update or delete the resource share at any time.

As a principal, you can accept or reject resource sharing invitations, view the information about the resource shares, and leave the resource shares if you no longer need to access their shared resources.

Viewing resource shares

A resource owner can view the information about the shared resources and the principals.

A principal can view the information about the shared resources and the resource owner.

Sharing with Organizations

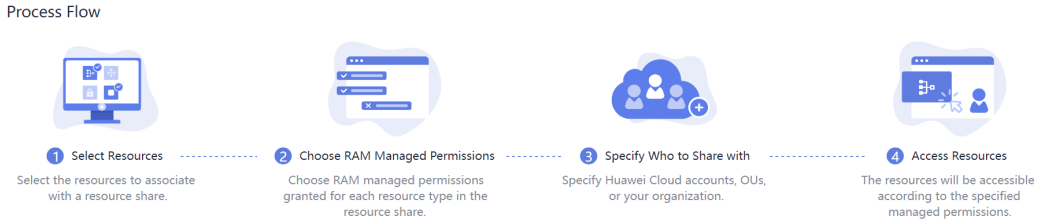
When sharing resources with Organizations is enabled, resource owners can share specified resources with an organization, OUs, or member accounts. By default, the accounts in the organization accept the sharing invitation.

How RAM Works

When you share resources with another account, you are granting principals in that account permissions to access the shared resources. Only those permissions selected for resource sharing can be granted to principals. The permissions associated with the resource share determine what the principals can do with the resources in the resource share.

The following figure demonstrates how RAM works.

Figure 1-1 How RAM works



Accessing RAM

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

- Using the management console

  Access RAM through the management console — a browser-based visual interface. Log in to the **management console**, click ☰ in the upper left corner, and choose **Management & Governance** > **Resource Access Manager**.

- Using APIs

  Use this method if you want to integrate RAM into a third-party system for secondary development. For detailed operations, see **Resource Access Manager API Reference**.

2 RAM Advantages

Simplified Resource Management

You can create a resource once in one account and use RAM to share that resource with other accounts, eliminating the need to create and provision duplicate resources in each account. This simplifies resource management and reduces operational overhead. The resource owner can use RAM to centrally manage different types of resources and configure resource shares to share resources with other accounts. This ensures consistent resource configurations and improves operational efficiency.

Improved Management Security

RAM has a single set of permissions preconfigured for different types of resources, and principals are only allowed to access the resources they have the permissions for. This improves the security of resource sharing.

Organizational Resource Sharing

When you use RAM to share resources with an organization or an OU, RAM automatically grants or denies the permissions to access the shared resources in an account if the account joins or leaves that organization or OU.

3 Application Scenarios

An enterprise may need to create multiple accounts and deploy different business applications in each account for administrative and billing isolation. The enterprise may also need to centrally manage certain resources and share these resources with different accounts. For example, the enterprise needs to plan, create, and manage internal networks and domain names used by all business applications in a unified manner.

4 Permissions

If you need to assign different permissions to employees in your enterprise, 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 to securely access your Huawei Cloud resources.

With IAM, you can create IAM users and assign permissions to control their access to RAM resources. If your account does not need individual IAM users for permissions management, you can skip this section.

IAM is a free service. You pay only for the resources in your account. For more information about IAM, see **IAM Service Overview**.

RAM 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 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.

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

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

Table 4-1 System-defined permissions for RAM

Permission	Description
RAM FullAccess	Full permissions for RAM.
RAM ReadOnlyAccess	Read-only permissions for RAM.
RAM ResourceSharePartici-pantAccess	Permissions for accepting or reject a resource sharing invitation.

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

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

Operation	RAM FullAccess	RAM ReadOnlyAccess	RAM ResourceSharePar-ticipantAccess
Listing RAM managed permissions	Supported	Supported	Not supported
Getting the details about RAM managed permissions	Supported	Supported	Not supported
Creating a resource share	Supported	Not supported	Not supported
Searching for resource shares	Supported	Supported	Supported
Updating a resource share	Supported	Not supported	Not supported
Deleting a resource share	Supported	Not supported	Not supported
Associating principals and resources with a resource share	Supported	Not supported	Not supported
Disassociating principals and resources from a resource share	Supported	Not supported	Not supported

Operation	RAM FullAccess	RAM ReadOnlyAccess	RAM ResourceSharePar-ticipantAccess
Searching for associated principals and resources	Supported	Supported	Not supported
Attaching or replacing RAM managed permissions	Supported	Not supported	Not supported
Detaching RAM managed permissions	Supported	Not supported	Not supported
Listing attached RAM managed permissions	Supported	Supported	Not supported
Searching for shared resources	Supported	Supported	Supported
Searching for principals	Supported	Supported	Supported
Accepting a resource sharing invitation	Supported	Not supported	Supported
Rejecting a resource sharing invitation	Supported	Not supported	Supported
Searching for a resource sharing invitation	Supported	Supported	Supported
Enabling sharing with Organizations	Supported	Not supported	Not supported
Disabling sharing with Organizations	Supported	Not supported	Not supported
Checking whether sharing with Organizations is enabled	Supported	Supported	Not supported

5 Service Quotas

Your account has the following quotas for RAM. If the default quotas cannot meet your service requirements, apply for a higher quota. For details, see **Adjusting Quotas**.

CAUTION

Accounts of different types cannot share resources with each other.

- Accounts registered with the Huawei Cloud Chinese Mainland website and accounts registered with the Huawei Cloud International website cannot share resources with each other.
- Huawei internal and external accounts cannot share resources with each other.

Table 5-1 Quotas for RAM

Item	Default Quota	Adjustable
Number of resource shares in an account	1000	Yes
Number of shared resources associated with a resource share	50	Yes
Number of permissions associated with a resource share	50	Yes
Number of principals associated with a resource share	50	Yes
Number of shared resources associated with all resource shares per account	5000	Yes
Number of permissions associated with all resource shares per account	5000	Yes
Number of principals associated with all resource shares per account	5000	Yes

Item	Default Quota	Adjustable
Number of pending sharing invitations per sharing account **NOTE** • This quota applies only to accounts who are sharing with accounts outside the same organization. • There is no quota to limit how many pending invitations a receiving account can have. • Invitations are not required for resource sharing between accounts in the same organization if you have enabled sharing with Organizations.	50	Yes
Number of tags allowed for a resource share	20	Yes
Retention period of a deleted resource share	48 hours	No
Retention period of a disassociated resource share	48 hours	No
Maximum number of VPC subnets that can be shared with a principal	100	No

6 Billing

RAM is a free service. You will not be billed for using RAM-related functions. For details about the billing for using shared resources, see the billing description for the shared resources.

7 Sharable Cloud Services and Resource Types

Table 7-1 Sharable cloud services and resource types

Cloud Service	Resource Type	Leaving a Resource Share	Application Scenario
Virtual Private Cloud (VPC)	Subnets	Supported	VPC sharing allows multiple accounts to create and manage cloud resources, such as ECSs, load balancers, and RDS instances, in one VPC. The owner of a VPC can share subnets in the VPC with one or more accounts. With VPC sharing, you can centrally manage resources in multiple accounts, improving the resource management efficiency and reducing O&M costs. For more information, see **VPC Sharing Overview**.

Cloud Service	Resource Type	Leaving a Resource Share	Application Scenario
Domain Name Service (DNS)	Private zones	Supported	Working with RAM, DNS allows you to share private zones across accounts if you are the owner of these private zones. When a resource owner shares private zones with you and you accept the resource sharing invitation, you can access and use the private zones. For more information, see **Sharing a Private Zone**.
	Resolver rules	Supported	Working with RAM, DNS allows you to share endpoint rules across accounts if you are the owner of these endpoint rules. When a resource owner shares endpoint rules with you and you accept the resource sharing invitation, you can access and use the endpoint rules. For more information, see **Sharing an Endpoint Rule**.

Cloud Service	Resource Type	Leaving a Resource Share	Application Scenario
SSL Certificate Manager (SCM)	Certificates	Supported	SCM allows you to share an SSL certificate with all member accounts in the same organizational unit. These member accounts can then deploy the shared certificate on services such as ELB, WAF, and CDN to enable HTTPS. For more information, see **Certificate Sharing Overview**.
Private Certificate Authority (PCA)	Private CAs	Supported	PCA allows you to share a private CA with all member accounts in the same organizational unit. These member accounts can then use the shared CA to issue certificates. For more information, see **Private CA Sharing Overview**.
Enterprise Router	Instances	Supported	None

Cloud Service	Resource Type	Leaving a Resource Share	Application Scenario
FunctionGraph	Functions	Supported	Working with RAM, FunctionGraph allows you to share functions across accounts if you are the owner of these functions. When a resource owner shares functions with you and you accept the sharing invitation, you can access and use the functions. For more information, see **Function Sharing Overview**.

8 Basic Concepts

Principal Sharing with You (Resource Owner)

An account used to create and manage resources. A resource owner can use RAM to create a resource share to share specified resources with other accounts.

Principal You Share With

The principal that the resource owner shares resources with. A principal is usually an individual account. When sharing with Organizations is enabled, a principal can also be an organization or organization unit (OU).

Resource Share

A unit for resource sharing. Resource shares are created by resource owners. Each resource share consists of one or more resource groups, RAM managed permissions, and principals.

RAM Managed Permission

A permission that defines what actions principals can take on shared resources. There is at least one RAM managed permission for each shareable resource type. If a resource type has only one RAM managed permission, it is used automatically by default. If a resource type has more than one RAM managed permission, you can choose which one to use in a resource share.

Resource Sharing Invitation

When a resource owner attempts to share resources with principals, RAM issues an invitation. The principals can accept or reject the invitation. When sharing with Organizations is enabled, resource owners can share resources with accounts in an organization on the assumption that the accounts would accept the sharing invitation by default.

9 Change History

Released On	Description
2024-03-15	This issue is the second official release, which incorporates the following changes: Resource Access Manager (RAM) is put into commercial use.
2022-10-29	This issue is the first official release.

