Alibaba Cloud
Resource Access Management

RAM User Management

Issue: 20190917

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⛔	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⛔ Danger: Resetting will result in the loss of user configuration data.
⚠	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	⚠ Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
📋	This indicates warning information, supplementary instructions, and other content that the user must understand.	ⓘ Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	📋 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *`Instance_ID`*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *`[-all|-t]`*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

1 Overview of a RAM user

A RAM user is a RAM identity with a fixed ID and credential information. Specifically, a RAM user corresponds to an identity, which can be either a person or an application.

- An Alibaba Cloud account owner can create multiple RAM users (which correspond to employees, systems, or applications of their enterprise) under their account.
- RAM users do not own resources. Rather, the fees incurred by RAM users are billed to the Alibaba Cloud accounts to which they belong. RAM users do not receive individual bills and cannot make payments.
- RAM users are visible only to the corresponding Alibaba Cloud account to which they belong.
- RAM users have permissions for only the Alibaba Cloud resources under the Alibaba Cloud account to which they belong after they are authorized to operate on these resources.

Note:

Enterprises that have multiple Alibaba Cloud resources can use RAM to manage user permissions and resources. For more information, see #unique_4.

2 Create a RAM user

A RAM user is an entity that you create in Alibaba Cloud to represent the person or application to interact with Alibaba Cloud. You can create a RAM user and grant it the relevant permissions to access the necessary Alibaba Cloud resources.

Procedure

1. Log on to the RAM console.
2. Choose Identities > Users.
3. Click Create User, and enter the logon name and display name.

   Note:
   You can click Add User to create multiple RAM users at a time.
4. Select an access mode. The available access modes are Console Password Logon and Programmatic Access.

   - Console Password Logon: If you select this check box, you must also complete the basic security settings for logon, including deciding whether to automatically generate a password or customize the logon password, setting whether the user must reset the password upon the next logon, and setting whether to enable multi-factor authentication (MFA).
   - Programmatic Access: If you select this check box, an access key is automatically created for the RAM user. The user can access Alibaba Cloud resources by calling an API action or by using a development tool.

   Note:
   We recommend that you set only one access mode for the user to maintain the security of your Alibaba Cloud account.
5. Click OK.

What's next

- You can add the RAM user to one or more RAM user groups and grant permission to the user as needed. For more information, see #unique_6.
- You can also attach one or more policies to the RAM user to grant the user access permission. For more information, see #unique_7.

3 View basic information about a RAM user

This topic describes how to view basic information about a RAM user, such as the username, the display name, and the user ID (UID).

Procedure

1. Log on to the RAM console.
2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, click the username of the target RAM user.
4. In the Basic Information section, view the user information.

4 Modify basic information about a RAM user

This topic describes how to modify basic information about a RAM user, such as the username and the display name.

Procedure

1. Log on to the RAM console.
2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, click the username of the target RAM user.
4. In the Basic Information section, click Modify Basic Information.
5. Click OK.

5 Grant permission to a RAM user

This topic describes how to grant permission to a RAM user. A RAM user can access Alibaba Cloud resources after obtaining relevant permissions.

Procedure

1. Log on to the RAM console.
2. Choose Permissions > Grants.
3. Click Grant Permission.
4. In the Principal field, enter the username or the user ID, and click the target RAM user.

   Note:
   You can also enter keywords to search for a specific username.
5. In the Policy Name column, select the target policy and click OK.

   Note:
   You can click X to revoke your selection.

6 Remove permission from a RAM user

This topic describes how to remove permission from a RAM user when the RAM user no longer needs a permission or when the RAM user leaves your organization.

Procedure

1. Log on to the RAM console.
2. Choose Permissions > Grants.
3. In the Principal column, find the target RAM user and click Revoke Permission.
4. Click OK.

7 Log on to the console as a RAM user

This topic describes how to log on to the RAM console as a RAM user, including the address and method to log on to the console.

Procedure

1. Log on to the RAM console as a RAM user.

   Note:
   To view the address that is used by a RAM user to log on to the console, use your Alibaba Cloud account to log on to the RAM console. The address is displayed on the Overview page.

2. Enter the logon name and then click Next.

   - Method 1: Use the default domain name to log on to the console. The format of the logon name for a RAM user is `<$username>@<$AccountAlias>.onaliyun.com`, for example, username@company-alias.onaliyun.com.

     Note:
     The logon name of a RAM user must be in the User Principal Name (UPN) format. All logon names listed in the RAM console use this format. <$username> represents the username of the RAM user. <$AccountAlias>.onaliyun.com represents the default domain name.

   - Method 2: Use the enterprise alias to log on to the console. The format of the logon name for a RAM user is `<$username>@<$AccountAlias>`, for example, username@company-alias.

     Note:
     <$username> represents the username of the RAM user. <$AccountAlias> represents the enterprise alias.

   - Method 3: If you have set a domain alias, you can also use the domain alias to log on to the console. The format of the logon name for a RAM user is `<$username>@<$DomainAlias>`, for example, username@example.com.

     Note:

<$username> represents the username of the RAM user. <$DomainAlias> represents the domain alias.

3. Enter the logon password and click Log On.

8 Delete a RAM user

This topic describes how to delete a RAM user. You can delete a RAM user when the user leaves your organization. After a RAM user is deleted, the access key, multi-factor authentication (MFA) device, and permissions of the RAM user are also deleted.

Procedure

1. Log on to the RAM console.
2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, select the target RAM user and click Delete.
4. Click OK.

Note:

Deleting an active RAM user may result in service failure. Exercise caution when performing this action.

9 Best practices

9.1 Use RAM to maintain security of your Alibaba Cloud resources

This topic describes how to use RAM to apply access and security settings to your Alibaba Cloud resources so that you can better manage access permissions with fine-grained access control.

Prerequisites

An Alibaba Cloud account is created. If not, create one before proceeding. To create an Alibaba Cloud account, click Create a new Alibaba Cloud account.

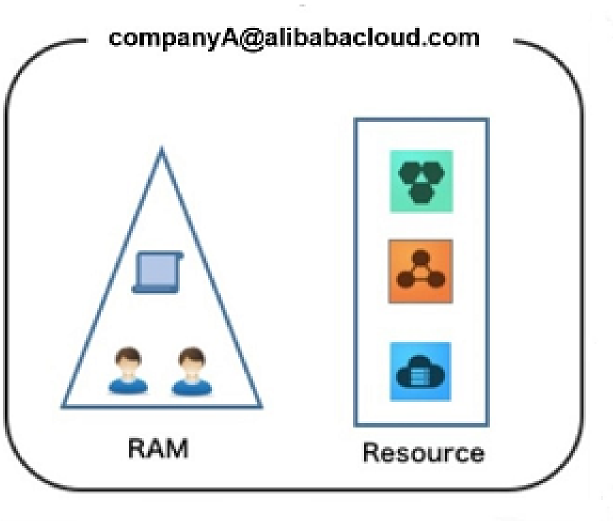
Scenario

When you migrate your business resources to the cloud, the traditional organizati onal structures and previous management methods of your resources may no longer meet your requirements. As a result, the migration of your resources may create higher security management issues as follows:

- The responsibilities of the RAM users are not clear.
- The Alibaba Cloud account owner does not want to share the access key with RAM users due to security risks involved.
- RAM users can access resources by using different methods, which is not unified and may mistakenly cause security risks.
- The resource access permissions of RAM users need to be frequently recalled when the users no longer require these permissions.

Solution

To resolve the preceding issues, you can use RAM to create RAM users and grant resource access permissions to RAM users. Specifically, you can use RAM to separate the access key of your Alibaba Cloud account from RAM users and grant minimum permissions to users as needed to maintain the security of your resources.



Security management solution

- Create independent RAM users.

  An enterprise needs only one Alibaba Cloud account. As a best practice, the Alibaba Cloud account is not used for daily tasks. However, multiple RAM users can be created under the account, and granted the necessary access permissions to resources as needed.

  For more information, see #unique_16.
- Separate console users from API users.

  We recommend that you do not create a logon password for console operations and an access key for API operations for a RAM user at the same time.

  - To allow an application to access cloud resources only through APIs, you only need to create an access key for the application.
  - To allow an employee to operate on cloud resources only through the console, you only need to set a logon password for the employee.

  For more information, see #unique_16.
- Create RAM users and group them.

  If your Alibaba Cloud account has multiple RAM users, you can group RAM users with same responsibilities and grant permissions to the group as needed.

  For more information, see #unique_17.
- Grant the minimum permissions to different RAM user groups.

  You can attach proper system policies to RAM users or user groups as needed. You can also create custom policies for fine-grained permission management. In this way, by granting the minimum permissions to different RAM users and user groups, you can better manage the RAM users' operations on the cloud resources.

For more information, see #unique_18.

- Configure strong password policies.

  You can configure password policies with custom conventions regarding the minimum length, mandatory characters, and validation period, for RAM users in the RAM console. If a RAM user is allowed to change their logon password, the user must create a strong logon password and rotate the password or access key on a regular basis.

  For more information, see #unique_19.

- Enable an MFA device for your Alibaba Cloud account.

  You can enable a multi-factor authentication (MFA) device for your Alibaba Cloud account to enhance the account security. When you log on to Alibaba Cloud with MFA enabled, the system requires the following two security factors:

  1. Your username and password
  2. Verification code provided by the MFA device

  For more information, see #unique_20.

- Enable SSO for RAM users.

  After Single Sign On (SSO) is enabled, all the internal accounts of your enterprise will be authenticated. Then, users can log on to Alibaba Cloud to access corresponding resources only by using an internal account.

  For more information, see #unique_21.

- Do not share the access key of your Alibaba Cloud account.

  Your Alibaba Cloud account has full control permissions over resources under it, and its access keys have the same permissions as logon passwords. However, access keys are used for programmatic access whereas logon passwords are used to log on to the console. Therefore, to avoid information leaks due to misuse of an access key, we recommend that you do not share or use the access key of your Alibaba Cloud account.

  Instead, create a RAM user and grant this user the relevant permissions.

  For more information, see #unique_22.

- Specify operation conditions to enhance security.

  You can specify the operational conditions that a RAM user must meet before they can use your cloud resources. For example, you can specify that the RAM user must use a secure channel (such as SSL), use a specified source IP address, or operate within a specified period of time.

  For more information, see #unique_23.
- Manage permissions of your cloud resources.

  By default, all your resources are under your Alibaba Cloud account. A RAM user can use the resources but do not own the resources. This allows you to easily manage the instances or data created by RAM users.

  - For an existing RAM user that you no long require, you can remove all of its corresponding permissions by simply removing the RAM user account.
  - For a RAM user that requires a permission, you need to first create the RAM user , set the logon password or access key for it, and then grant the RAM user the relevant permissions as needed.

  For more information, see #unique_7.
- Use STS to grant temporary permissions to RAM users.

  The Security Token Service (STS) is an extended authorization service of RAM. You can use STS to grant temporary permissions to RAM users and specify the permission and automatic expiration time of the tokens as needed.

  For more information, see #unique_24

Result

After migrating your services to the cloud, you can use the preceding solutions to ensure you manage your cloud-based resources effectively and keep your Alibaba Cloud account and all business assets secure.

What to do next

You can use RAM to categorize your O&M requirements and assign tasks to different engineers as needed. For more information, see #unique_25.

9.2 Use RAM to manage user permissions and resources

This topic describes how to use RAM to manage user permissions and resources.

Prerequisites

An Alibaba Cloud account is created. If not, create one before proceeding. To create an Alibaba Cloud account, click Create a new Alibaba Cloud account.

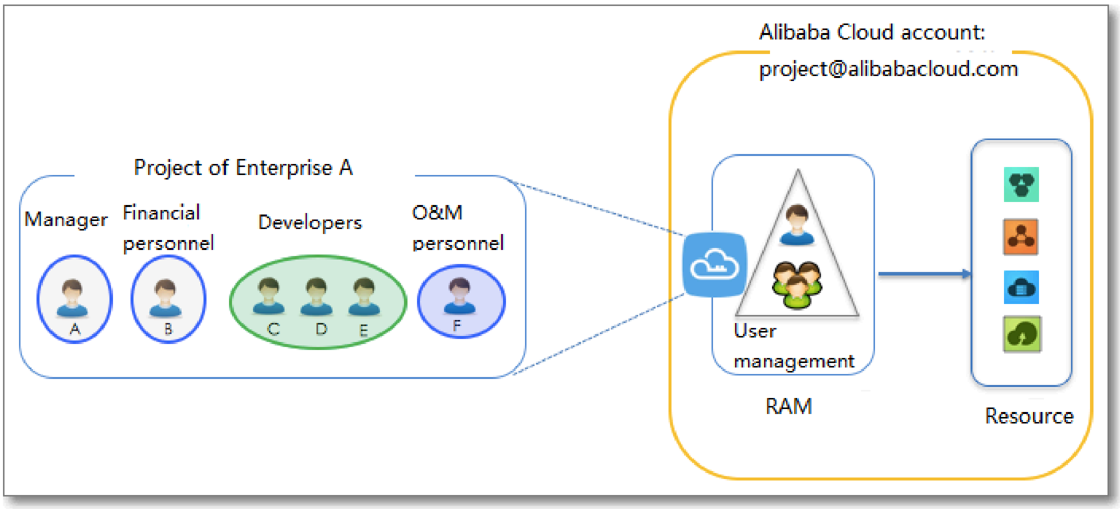
Scenario

Enterprise A has bought several types of Alibaba Cloud resources, such as ECS instances, RDS instances, SLB instances, and OSS buckets for a project. During this project, many employees need to perform operations on these cloud resources, but different employees require different permissions to complete different operations.

The requirements of Enterprise A are as follows:

- Employees do not share the Alibaba Cloud account to avoid mistaken disclosure of the account password or AccessKey pair.
- Independent RAM users are created for different employees and the RAM users are granted independent permissions.
- All operations of all RAM users can be audited by Enterprise A.
- The permissions of RAM users can be removed at any time, and users under an Alibaba Cloud account can be deleted by Enterprise A.
- Fees are not charged to each RAM user, but are instead charged to the correspond ing Alibaba Cloud account to which the RAM users belong.

Solution



- Set multi-factor authentication (MFA) for you Alibaba Cloud account to avoid risks associated with mistaken disclosure of the password. For more information, see #unique_20.
- Create RAM users for different employees (or applications) and set logon passwords or create AccessKey pairs. For more information, see #unique_16.
- If multiple RAM users require the same permissions, we recommend that you create a user group and add the corresponding users to this group. For more information, see #unique_17.
- Attach one or more system policies to the groups or users. For more information, see #unique_7 or #unique_27. For finer-grained permission management, you can create one or more custom policies and attach them to individual users or to a user group. For more information, see #unique_18.
- Remove permissions from groups or RAM users when they no longer need the permissions. For more information, see #unique_28 or #unique_29.

10 FAQ

10.1 RAM user FAQ

How do I log on to the Alibaba Cloud console as a RAM user?

You can visit the RAM user logon page or visit the RAM user logon URL on the right of the Overview page in the RAM console.

The user name for logon can be in either of the following formats: <$username>@<$AccountAlias> and <$username>@<$AccountAlias>.onaliyun.com. If you have created a domain alias, you can also use the domain alias in <$username>@<$DomainAlias> format for logon.

Note:

If you log on to the Alibaba Cloud console by visiting the RAM user logon URL on the right of the Overview page in the RAM console, the system automatically provides a default domain name. You only need to enter the user name.

What are the default domain name, account alias, and domain alias? How do I use and manage them?

For details about the default domain name, account alias, and domain alias, see Terms.

To view and manage the default domain name, account alias, and domain alias of your account, log on to the RAM console by using your account or as a RAM user with the RAM permission, choose Identities > Settings, and click Advanced.

What permissions are required for a RAM user to purchase Alibaba Cloud services?

- For Pay-As-You-Go services, permission to create service instances, or similar permissions are required.
- For Subscription services, permission to create service instances and permission to make payments (the AliyunBSSOrderAccess policy) are required.
- For services that must be purchased with the use or creation of some other resources, the permission for reading or creating the corresponding resources is

required. The following example describes the permissions required for creating an ECS instance.

The following policy allows a RAM user to create an ECS instance through the console, the ECS API, or the instance launch template:

```
{
  " Version ": " 1 ",
  " Statement ": [
    {
      " Action ": [
        " ecs : DescribeLa  unchTempla  tes ",
        " ecs : CreateInst  ance ",
        " ecs : RunInstanc  es ",
        " ecs : DescribeIn  stances ",
        " ecs : DescribeIm  ages ",
        " ecs : DescribeSe  curityGrou  ps "
      ],
      " Resource ": "*",
      " Effect ": " Allow "
    },
    {
      " Action ": [
        " vpc : DescribeVp  cs ",
        " vpc : DescribeVS  witches "
      ],
      " Resource ": "*",
      " Effect ": " Allow "
    }
  ]
}
```

To allow a user to use or create resources other than ECS instances, log on to the RAM console and click Policies. On the displayed page, create a custom policy and grant permissions to the user according to the following table.

Operation	Policy action
Use a snapshot to create an ECS instance.	`ecs : DescribeSn  apshots`

Create and use a VPC.	`vpc : CreateVpc`
	`vpc : CreateVSwi  tch`

Create and use a security group.	`ecs : CreateSecu  rityGroup`
	`ecs : AuthorizeS  ecurityGro  up`

Operation	Policy action

Specify the instance RAM role.	`ecs : DescribeInstanceRamRole`
	`ram : ListRoles`
	`ram : PassRole`

Use a key pair.	`ecs : CreateKeyPair`
	`ecs : DescribeKeyPairs`

Create an ECS instance on a Dedicated Host (DDH).	`ecs : AllocateDedicatedHosts`

After I grant permission to a user, why is a message displayed when the user accesses the system, indicating that the user does not have the permission?

- Check whether the policy attached to the user is correct.
- Check whether `" Effect ": " Deny "` has been set in the custom policy (including policies of the user and policies of the user's groups) attached to the user for the corresponding resources or operations.

  For example, a user has both the AliyunECSReadOnlyAccess policy (which contains the read-only permission for accessing ECS) and the following policy:

  ```
  {
    " Statement ": [
      {
        " Action ": " ecs :*",
        " Effect ": " Deny ",
        " Resource ": "*"
      }
    ],
    " Version ": " 1 "
  }
  ```

  According to the "Deny takes priority" principle in RAM, the user is not allowed to view the ECS resources.

Why can a user perform operations without the corresponding permission?

If a user does not have the required custom policy or the FullAccess or ReadOnly system policy of ECS and can view the created ECS instances in the console, perform the following operations:

1. Check whether the group policy of the user contains the permission that allows the user to perform the corresponding operations.
2. Check whether other polices attached to the user contain the corresponding permissions.

For example, the system policy of CloudMonitor is AliyunCloudMonitorFullAccess, which contains the following permissions: `" ecs : DescribeIn stances "` (view ECS instances), `" rds : DescribeDB Instances "` (view RDS instances), and `" slb : DescribeLo adBalancer "` (view SLB instances). If you attach the AliyunCloudMonitorFullAccess policy to a user, the user has permission to view the information of ECS, RDS, and SLB instances.

How do I grant permission to a user for renewal management only?

A unified renewal management policy is not currently available. You must customize a policy according to the specific services. You can grant the user the permission for purchasing the service and the payment permission.

For example, if you want a user to perform ECS renewal management, see What permissions are required for a RAM user to purchase Alibaba Cloud services? to grant required permissions and the AliyunBSSOrderAccess policy to the user.

Who will be charged for the resources used by a RAM user?

- Fees incurred by a user when using Alibaba Cloud resources are paid by the account to which the user belongs.
- Users under an account enjoy the discounts of the account by default.
- Users under an account share the same financial attributes such as consumption, credit limit, and payment method. You cannot set a financial attribute for a single user.
- A user under an account can be authorized to add money to the account balance. However, the balance belongs to the account, not the user.
- Users in a group are not billed separately. To obtain bills that detail the charges incurred by each user under an account, open a ticket.