Alibaba Cloud
Resource Access Management

Best Practices

Issue: 20190228

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 Use RAM to maintain security of your cloud-based services

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

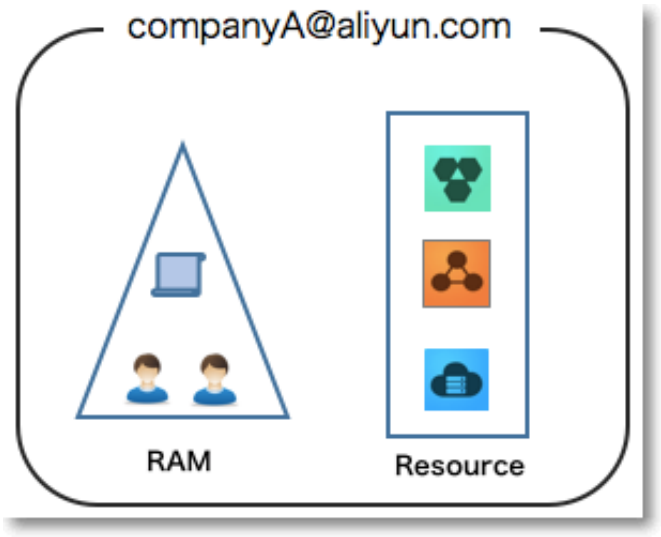
Scenario

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 services may create higher security management issues as follows:

- The responsibilities of the RAM users are not clear.
- The account owner does not want to share the account AccessKey with RAM users due to security risks involved.
- RAM users can access resources 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 apply resource access permissions to them. Specifically, you can use RAM to separate the account AccessKey from RAM users and grant minimum permissions to users as needed to ensure that the security of your resources is maintained.



Security management solution

- Create independent RAM users.

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

  For more information, see *Create a RAM user*.

- Separate console users from API users.

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

  - To allow an application to access cloud resources only through open APIs, you only need to create an AccessKey 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 *Create a RAM user*.

- Create RAM users and group them.

  If your 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 *(Optional) Create a RAM user group*.

- 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 *Policy management*.

- 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 AccessKey on a regular basis.

  For more information, see *Set up initial RAM configurations*.

- Enable MFA for your account.

  You can enable multi-factor authentication (MFA) for your account to enhance the account security. After MFA is enabled, the system asks the RAM user logging on to Alibaba Cloud to enter the following two security factors:

  - First security factor: account name and password
  - Second security factor: a variable verification code from the virtual MFA device

  For more information, see *(Optional) Set MFA*.

- 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 *Configure the SAML of an account*.

- Do not share the AccessKey of your account.

  Your account has full control permissions over resources under it, and its AccessKeys have the same permissions as logon passwords. However, AccessKeys 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 AccessKey,

we recommend that you do not share or use the AccessKey of your account. Instead , create a RAM user and grant this user the relevant permissions.

For more information, see *Manage AccessKeys*.

- 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 *Policy elements*.

- Manage permissions of your cloud resources.

  By default, all your resources are under your 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 AccessKey for it, and then grant the RAM user the relevant permissions as needed.

  For more information, see *Authorize RAM users*.

- 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_13*.

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 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 *Manage permissions of different O&M engineers by using RAM*.

2 Manage permissions of different O&M engineers by using RAM

You can grant and manage the permissions of different O&M engineers by using RAM to meet various O&M requirements while also facilitating better management and control.

Scenario

Your company purchases several Alibaba Cloud products and deploys a number of application systems on the cloud, which brings greater O&M requirements.

- Different O&M owners are responsible for different Alibaba Cloud products.
- Different O&M engineers require different permissions to access, operate, and manage cloud resources.

Solution

You can categorize the O&M requirements by product to make them easier to manage. More specifically, you can set an O&M owner and assign different O&M engineers to different categories of requirements and attach your specified policies to these engineers, as shown in the following figure.

Figure 2-1: O&M owner

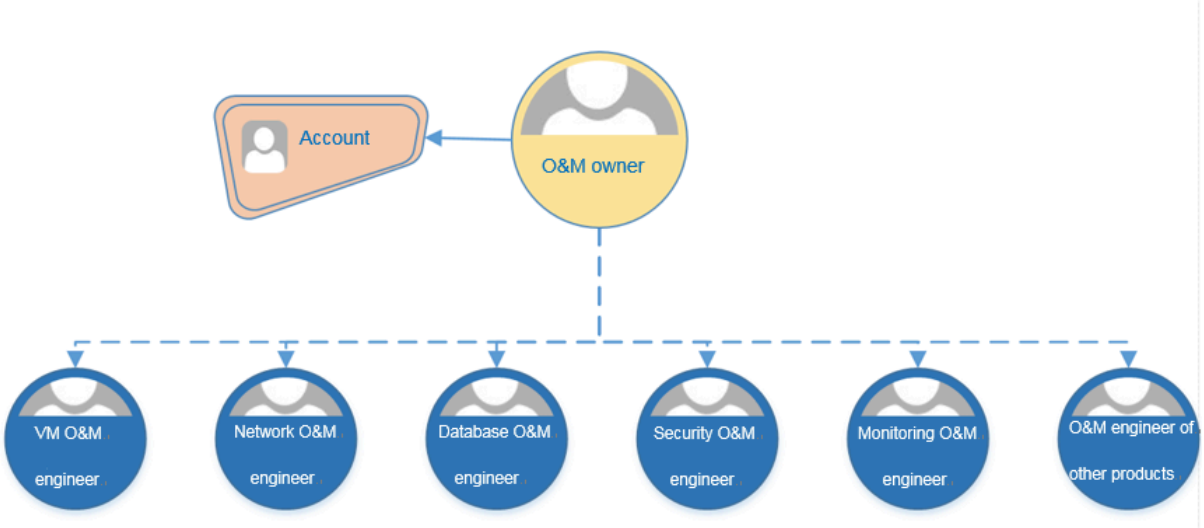


Table 2-1: Policies

O&M owner	Policy	Description
O&M owner	AdministratorAccess	This policy grants the O&M owner the permission to manage all Alibaba Cloud resources.
VM O&M engineer	AliyunECSFullAccess	This policy grants the VM O&M engineer the permission to manage Elastic Compute Service (ECS).
	AliyunESSFullAccess	This policy grants the VM O&M engineer the permission to manage Elastic Scaling Service (ESS).
	AliyunSLBFullAccess	This policy grants the VM O&M engineer the permission to manage Server Load Balancer (SLB).
	AliyunNASFullAccess	This policy grants the VM O&M engineer the permission to manage Network Attached Storage (NAS).
	AliyunOSSFullAccess	This policy grants the VM O&M engineer the permission to manage Object Storage Service (OSS).
	AliyunOTSFullAccess	This policy grants the VM O&M engineer the permission to manage Table Store (OTS).
Network O&M engineer	AliyunCDNFullAccess	This policy grants the network O&M engineer the permission to manage Content Delivery Network (CDN).
	AliyunCENFullAccess	This policy grants the network O&M engineer the permission to manage Cloud Enterprise Network (CEN).

O&M owner	Policy	Description
	AliyunCommonBandwidthPackageFullAccess	This policy grants the network O&M engineer the permission to manage Internet Shared Bandwidth.
	AliyunEIPFullAccess	This policy grants the network O&M engineer the permission to manage Elastic IP (EIP).
	AliyunExpressConnectFullAccess	This policy grants the network O&M engineer the permission to manage ExpressConnect.
	AliyunNATGatewayFullAccess	This policy grants the network O&M engineer the permission to manage NAT Gateway.
	AliyunSCDNFullAccess	This policy grants the network O&M engineer the permission to manage Secure Content Delivery Network (SCDN).
	AliyunSmartAccessGatewayFullAccess	This policy grants the network O&M engineer the permission to manage Smart Access Gateway.
	AliyunVPCFullAccess	This policy grants the network O&M engineer the permission to manage Virtual Private Cloud (VPC).
	AliyunVPNGatewayFullAccess	This policy grants the network O&M engineer the permission to manage VPN Gateway.
Database O&M engineer	AliyunRDSFullAccess	This policy grants the database O&M engineer the permission to manage Relational Database Service (RDS).
	AliyunDTSFullAccess	This policy grants the database O&M engineer the permission to manage Data Transmission Service (DTS).
Security O&M engineer	AliyunYundunFullAccess	This policy grants the security O&M engineer the permission to manage Alibaba Cloud Security.

O&M owner	Policy	Description
Monitoring O&M engineer	AliyunActionTrailFullAccess	This policy grants the monitoring O&M engineer the permission to manage ActionTrail.
	AliyunARMSFullAccess	This policy grants the monitoring O&M engineer the permission to manage Application Real-Time Monitoring Service ARMS).
	AliyunCloudMonitorFullAccess	This policy grants the monitoring O&M engineer the permission to manage CloudMonitor.
	(Optional) ReadOnlyAccess	(Optional) This policy grants the monitoring O&M engineer the read-only permission to all Alibaba Cloud resources.
	AliyunSupportFullAccess	This policy grants the monitoring O&M engineer the permission to manage Alibaba Cloud support systems.

Example

This example describes how to set the RAM user `alice @ secloud . onaliyun . com` as the database O&M owner, so that the user can manage RDS and DTS.

1. Log on to the *RAM console*.
2. *Create a RAM user* and name the user `alice @ secloud . onaliyun . com` .
3. Find the created RAM user and click Add Permissions.
4. In the Policy Name column, select `AliyunRDSF ullAccess` and `AliyunDTSF ullAccess` , and click Ok.

 Note:

To grant other O&M permissions to the RAM user, see the policies described in the preceding table.

3 Use tags to authorize ECS instances by group

This topic describes how to use tags to authorize resources (such as ECS instances) by group so that RAM users can only view and operate on the tagged resources.

Scenario

You have 10 ECS instances. You want your dev team to manage 5 of them, and your ops team to manage the other 5. However, you want each team to see only their authorized resources (not the authorized resources of the other team).

Preparations

Make sure that you can log on to the *RAM console* by using your RAM account.

Solution

Create two RAM user groups, tag these two groups, and grant permissions to the groups.

- Tag five of them with the key as team and the value as dev.
- Tag the other five with the key as team and the value as ops.

Procedure

1. Log on to the ECS console, click Instances, and select the target instance. In the Actions column, choose More > Instance Settings > Edit Tag.
2. Click Create, enter the key and value, and click Confirm.
3. Log on to the RAM console, create two RAM user groups, and name the groups as dev and ops.

   For more information, see *(Optional) Create a RAM user group*.
4. Create RAM users and add the users to different user groups.

   For more information, see *Create a RAM user*.
5. Create two custom policies and attach them to different user groups.

   For more information, see *Permission granting in RAM*.

Note:

After you attach a policy to a user group, the RAM users in this group inherit the relevant permissions.

In this example, the policy name of the dev user group is policyForDevTeam. The policy content is as follows:

```
{
    " Statement ": [
    {
        " Action ": " ecs :*",
        " Effect ": " Allow ",
        " Resource ": "*",
        " Condition ": {
            " StringEqua  ls ": {
                " ecs : tag / team ": " dev "
            }
        }
    },
    {
        " Action ": " ecs : DescribeTa  g *",
        " Effect ": " Allow ",
        " Resource ": "*"
    }
    ],
    " Version ": " 1 "
}
```

In the preceding policy,

- The `" Action ": " ecs :*"` element with "Condition" is used to filter the instances tagged as `" team ": " dev "`.
- The `" Action ": " ecs : DescribeTa  g *"` element is used to display all tags. When a user performs operations in the ECS console, the system displays all the tags for the user to select, and then filters the instances according to the tag key and value selected by the user.

 Note:
You can create the policy policyForOpsTeam according to the example and grant this policy to the ops user group.

Display authorized instances

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

 Note:
After a user logs on to the ECS console, the system navigates to the ECS overview page by default. In this case, the number of the ECS instances displayed on the page is 0. To view relevant instances, click Instances.

2. Click Instances and click Tags next to the search box.

   Note:
   You need make sure that the region displayed in the console is the region to which the instances belong.

3. Move the pointer over Tag Key. The Tag Value list is displayed. Select a value, and the system then filters the corresponding instances.

What to do next

You can use the procedures described in this topic to tag and authorize security groups, disks, snapshots, and images by group.

Note:
Only custom images can be tagged.

4 Use tags to authorize RDS instances by group

This topic describes how to use tags to authorize resources (such as RDS instances) by group so that RAM users can only view and operate on the tagged resources.

Scenario

You have 10 RDS instances. You want your dev team to manage 5 of them, and your ops team to manage the other 5. However, you want each team to see only their authorized instances (not the authorized resources of the other team).

Preparations

For more information, see *Use tags to authorize ECS instances by group*.

The following is an example of the custom policy relevant to RDS:

```
{
  " Statement ": [
    {
      " Action ": " rds :*",
      " Effect ": " Allow ",
      " Resource ": "*",
      " Condition ": {
        " StringEqua  ls ": {
          " rds : ResourceTa  g / team ": " dev "
        }
      }
    },
    {
       " Action ": " rds : DescribeTa  g *",
       " Effect ": " Allow ",
       " Resource ": "*"
    }
  ],
  " Version ": " 1 "
}
```

In the preceding policy,

- The `" Action ": " rds :*"` element with "Condition" is used to filter the instances tagged as `" team ": " dev "`. The keyword of "Condition" is `rds : ResourceTa  g`.
- The `" Action ": " rds : DescribeTa  g *"` element is used to display all tags. When a user performs operations in the RDS console, the system displays all the tags for the user to select, and then filters the instances according to the tag key and value selected by the user.

What to do next

If the relevant permissions of a RAM user are missing after you have tagged RDS instances into groups and granted permissions, see #unique_20.

5 Use ActionTrail to record RAM operations

This topic describes how to use ActionTrail to record the operations of an Alibaba Cloud account or a RAM user on resources.

Prerequisite

RAM and ActionTrail have been integrated.

Use ActionTrail to view RAM operations

1. Log on to the *ActionTrail console*.
2. On the History Search page, select Username from the Filter drop-down list.
3. Enter the target user name, select an event type and time, and click Search.

   Note:
   You can also select Event Name, Resource Type, Resource Name, or AccessKeyId from the Filter drop-down list to search for relevant operations.
4. Click the target event and click View event.

Operations recorded by ActionTrail

ActionTrail can record the following RAM operations:

- Logon information of an Alibaba Cloud account or a RAM user. For more information, see *ConsoleSignin event log examples*.
- Operations on the RAM console. The following is an example:

```
{
    " apiVersion ":" 2015 - 05 - 01 ",
    " eventId ":" 2cc52dee - d8d2 - 40c2 - 8de0 - 3a2cf1df07  a0 ",
    " eventName ":" DeleteGrou  p ",
    " eventSourc  e ":" ram . aliyuncs . com ",
    " eventTime ":" 2015 - 11 - 03T13 : 41 : 49Z ",
    " eventType ":" ApiCall ",
    " eventVersi  on ":" 1 ",
    " requestId ":" 9AE24F49 - C52C - 4F0F - BCF9 - 9A4B8C22B1  47
 ",
    " requestPar  ameters ":{
        " GroupName ":" grp1 ",
    },
    " serviceNam  e ":" Ram ",
    " sourceIpAd  dress ":" 42 . 120 . 74 . 90 ",
    " userAgent ":" AliyunCons  ole ",
    " userIdenti  ty ":{
        " type ":" ram - user ",
        " principalI  d ":" 2741806465  48292385 ",
```

```
        " accountId ":" 43274 ",
        " userName ":" Alice ",
        " sessionCon  text ":{
            " sessionAtt  ributes ":{
                " creationDa  te ":" 2015 - 11 - 03T13 : 41 : 48Z ",
                " mfaAuthent  icated ":" true "
            }
        }
    }
}
```

- **RAM and STS API calls for resource creation, change, and deletion. The following is an example:**

```
{
    " apiVersion ": " 2015 - 05 - 01 ",
    " eventId ": " 234ef3c7 - 8938 - 4bd7 - bb80 - 11754b7bdd  4c ",
    " eventName ": " CreateGrou  p ",
    " eventSourc  e ": " ram . aliyuncs . com ",
    " eventTime ": " 2016 - 01 - 04T08 : 58 : 50Z ",
    " eventType ": " ApiCall ",
    " eventVersi  on ": " 1 ",
    " recipientA  ccountId ": " 43274 ",
    " requestId ": " 1485748C - DB62 - 4693 - AB7E - 4BA3F3A970  E1
 ",
    " requestPar  ameters ": {
        " Comments ": " this   is   a   test   group ",
        " GroupName ": " grp1 "
    },
    " serviceNam  e ": " Ram ",
    " sourceIpAd  dress ": " 42 . 120 . 74 . 96 ",
    " userAgent ": " aliyuncli / 2 . 0 . 6 ",
    " userIdenti  ty ": {
        " type ": " ram - user ",
        " principalI  d ": " 2741806465  48292385 ",
        " accountId ": " 43274 ",
        " accessKeyI  d ": " f6IzzFZMmz  NwEI4d ",
        " userName ": " Alice "
    }
}
```

What to do next

For more information about operation records, see *ActionTrail event log syntax*.

6 Authorization for ECS instances

Questions

- *View ECS permission definitions*
- *Assign full ECS service management permissions to a subaccount*
- *ssign the ECS read-only permission to a subaccount*
- *Allow a RAM user to view ECS instances in the Qingdao region but disallow the user to view disk or snapshot information*
- *Authorize a RAM user to manage two specified ECS instances*
- *Authorize a RAM user to create snapshots*

View ECS permission definitions

See *Authorization rules* in the ECS OpenAPI document.

Assign full ECS service management permissions to a subaccount

Add the system authorization policy “AliyunECSFullAccess” to the subaccount (or the group to which the subaccount belongs) on the RAM console.

Assign the ECS read-only permission to a subaccount

Create a subaccount on the RAM console and add the system authorization policy “AliyunECSReadOnlyAccess” to the subaccount.

For more information about how to add an authorization policy, see *Authorization*.

Allow a RAM user to view ECS instances in the Qingdao region but disallow the user to view disk or snapshot information

The permission for viewing ECS resource lists can be assigned based on region and resource type.

The following example describes how to authorize a subaccount to view only ECS instance information in the Qingdao region.

```
" Statement ": [

    " Effect ": " Allow ",
    " Action ": " ecs : DescribeRe  gions ",
    " Resource ": "*"
```

```
      " Effect ": " Allow ",
      " Action ": " ecs : Describe *",
      " Resource ": " acs : ecs : cn - qingdao :*: instance /*"


  " Version ": " 1 "
```

Authorize a RAM user to manage two specified ECS instances

Assume that 10 ECS instances have been bought under your tenant account. As a RAM administrator, you want to authorize a RAM user to use only two of the ECS instances. In this case, you can create the following authorization policy:

Note:

he authorized RAM user can view all the ECS instances but can perform operations (such as the StopInstance operation) on only two of them. Currently, you cannot authorize a RAM user to view only the ECS instances that the user can operate.

Assume that the IDs of your ECS instances are i-001 and i-002. You must first create an authorization policy, which includes the permissions for managing i-001 and i-002 and viewing all ECS resources.

```
" Statement ": [

    " Action ": " ecs :*",
    " Effect ": " Allow ",
    " Resource ": [
                " acs : ecs :*:*: instance / i - 001 ",
                " acs : ecs :*:*: instance / i - 002 "


    " Action ": " ecs : Describe *",
    " Effect ": " Allow ",
    " Resource ": "*"


" Version ": " 1 "
```

Then, add the authorization policy for the user.

Authorize a RAM user to create snapshots

If a RAM user cannot create disk snapshots after being assigned the ECS administra tor permissions, you must assign disk permissions to the user because snapshots are created based on disks.

Assume that you want to authorize the RAM user to manage the ECS instance whose ID is inst-01, and to create snapshots for the disk whose ID is dist-01. In this case, you can create the following authorization policy:

```
" Statement ": [

    " Action ": " ecs :*",
    " Effect ": " Allow ",
    " Resource ": [
      " acs : ecs :*:*: instance / inst - 01 "



    " Action ": " ecs : CreateSnap  shot ",
    " Effect ": " Allow ",
    " Resource ": [
      " acs : ecs :*:*: disk / dist - 01 ",
      " acs : ecs :*:*: snapshot /*"



    " Action ": [
      " ecs : Describe *"

    " Effect ": " Allow ",
    " Resource ": "*"


" Version ": " 1 "
```

Then, add the authorization policy for the user.

7 Authorization for OSS instances

Questions

- *View OSS permission definitions*
- *Assign the OSS read-only permission to a RAM user*
- *Assign the full OSS management permission to a RAM user*
- *Authorize a RAM user to list and read resources in a bucket*
- *Apply IP address-specific access control in OSS*
- *Authorization by OSS directory*
- *Authorize a RAM user complete management of a bucket*
- *RAM user authorized to manage a bucket notified of having no operation permissions when logging on to the OSS console*

View OSS permission definitions

See *Access control* in the OSS product document.

Assign the OSS read-only permission to a RAM user

Create a RAM user in the RAM console and add the system authorization policy AliyunOSSReadOnlyAccess to the user. For more information about how to add an authorization policy, see *Authorization*.

Assign the full OSS management permission to a RAM user

Add the system authorization policy AliyunOSSFullAccess to the RAM user in the RAM console.

Authorize a RAM user to list and read resources in a bucket

If you need to authorize a RAM user (such as an application that represents you) to list and read the resources in a bucket using the OSS SDK or OSS CMD, you must create an authorization policy.Resource in, then you need to create a custom Authorization Policy to complete.

Assume that your bucket is named “myphotos”. Create the authorization policy as follows:

```
{
    " Version ": " 1 ",
    " Statement  ":[
```

```
        {
            " Effect ": " Allow ",
            " Action ": " oss : ListObject  s ",
            " Resource ": " acs : oss :*:*: myphotos "
        },
        {
            " Effect ": " Allow ",
            " Action ": " oss : GetObject ",
            " Resource ": " acs : oss :*:*: myphotos /*"
        }
    ]
}
```

If you want the authorized RAM-user to perform operations on the OSS console, add the GetBucketAcl and GetObjectAcl permissions to the authorization policy. (The console needs to call additional OSS APIs to optimize the operation experience.) The following provides an example of the authorization policy definition that allows the RAM-user to perform operations on the OSS console:

```
{
    " Version ": " 1 ",
    " Statement  ":[
        {
            " Effect ": " Allow ",
            " Action ": " oss : ListBucket  s ",
            " Resource ": " acs : oss :*:*:*"
        },
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListObject  s ",
                " oss : GetBucketA  cl "
            ],
            " Resource ": " acs : oss :*:*: myphotos "
        },
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : GetObject ",
                " oss : GetObjectA  cl "
            ],
            " Resource ": " acs : oss :*:*: myphotos /*"
        }
    ]
}
```

Apply IP address-specific access control in OSS

Example 1: Apply IP address-specific access control using the `Allow` command

The IP address segments `42 . 120 . 88 . 0 / 24` and `42 . 120 . 66 . 0 / 24` are allowed to read the information in the myphotos directory.

```
{
    " Version ": " 1 ",
    " Statement  ":[
        {
```

```
            " Sid ": " To   allow   listing   all   buckets ",
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListBucket  s "
            ],
            " Resource ": [
                " acs : oss :*:*:*"
            ]
        },
        {
            " Sid ": " To   allow   only   the   users   in   the
 specified   IP   address   segment   to   obtain   the   informatio
 n   in   the   myphotos   directory ",
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListObject  s ",
                " oss : GetObject "
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos ",
                " acs : oss :*:*: myphotos /*"
            ],
            " Condition  ":{
                " IpAddress ": {
                    " acs : SourceIp ": " 42 . 120 . 88 . 0 / 24 ", "
 42 . 120 . 66 . 0 / 24 "
                }
            }
        }
    ]
}
```

Example 2: Apply IP address-specific access control using the `Deny` command

If the IP address of a user is not within the `42 . 120 . 88 . 0 / 24` segment, the user cannot perform any OSS operations. Create an authorization policy as follows:

```
{
    " Version ": " 1 ",
    " Statement  ":[
        {
            " Sid ": " To   allow   listing   all   buckets ",
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListBucket  s "
            ],
            " Resource ": [
                " acs : oss :*:*:*"
            ]
        },
        {
            " Sid ": " To   allow   obtaining   the   informatio  n
 in   the   myphotos   directory ",
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListObject  s ",
                " oss : GetObject "
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos ",
                " acs : oss :*:*: myphotos /*"
```

```
            ]
        },
        {
            " Sid ": " To   disallow   IP   addresses   not   in   the
   42 . 120 . 88 . 0 / 24   segment   to   access   OSS ",
            " Effect ": " Deny ",
            " Action ": " oss :*",
            " Resource ": [
                " acs : oss :*:*:*"
            ],
            " Condition  ":{
                " NotIpAddre  ss ": {
                    " acs : SourceIp ": [" 42 . 120 . 88 . 0 / 24 "]
                }
            }
        }
    ]
}
```

NOTE: A policy with the Deny command has a higher priority than the policy with the Allow command. (If the accessing operation of a user meets any policy with the Deny command, the user is disallowed to access the content.) Therefore, when a user whose IP address is not in the 42.120.88.0/24 segment attempts to access the information in the "myphotos" directory, the OSS service notifies the user of having no operation permissions.

Authorization by OSS directory

Authorization by directory is an advanced authorization function.

Background

Assume that you have a photo bucket named "myphotos". The bucket contains directories that indicate the places where the photos were taken. Each directory contains subdirectories that indicate the years when the photos were taken.

The directory tree is as follows:

```
myphotos [ Bucket ]
  ├──  beijing
  │    ├──  2014
  │    └──  2015
  ├──  hangzhou
  │  ├──  2013
  │  ├──  2014
  │  └──  2015  // The   read - only   permission   on   this
directory   must   be   assigned .
  └──  qingdao
       ├──  2014
       └──  2015
```

Assume that you need to assign the read-only permission on the `myphotos / hangzhou / 2015 /` directory to a RAM user. The required authorization policy

depends on the application scenario. The following describes the authorization policies for three scenarios by policy complexity, from simplest to more complex.

Scenario 1: The RAM user knows all file paths, requires only the permission to read file content, and does not require the permission to list files.

In this scenario, the RAM user knows the complete paths of all files and can directly read the files using the complete paths. A software system requires such permission assignment, because the file paths in the software system comply with a certain rule (for example, files are named after employee IDs) or the file paths have persisted in the database of the software system.

```
{
    " Version ": " 1 ",
    " Statement  ":[
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : GetObject "
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos / hangzhou / 2015 /*"
            ]
        }
    ]
}
```

Scenario 2: A RAM user uses the OSS CMD to access the `myphotos / hangzhou / 2015 /` directory, but does not know what files are available in the directory. Therefore, the files must be listed.

Generally, software developers require such permission assignment. The developers do not know what files are available in a directory and use the OSS CMD or API to directly obtain the directory information.

In this scenario, the ListObjects permission that is not required in `scenario 1` must be added. Because only the files in the `myphotos / hangzhou / 2015 /` directory are to be listed, the oss:Prefix condition must be added to the ListObjects permission.

```
{
    " Version ": " 1 ",
    " Statement  ":[
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : GetObject "
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos / hangzhou / 2015 /*"
```

```
            ]
        },
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListObject  s "
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos "
            ],
            " Condition ":{
                " StringLike ":{
                    " oss : Prefix ":" hangzhou / 2015 /"
                }
            }
        }
    ]
}
```

Scenario 3: A RAM user uses the OSS console to access the `myphotos / hangzhou / 2015 /` directory.

This is the most easy-to-use scenario. When the RAM user uses the visual OSS client to access the `myphotos / hangzhou / 2015 /` directory, like Windows File Explorer, the visual OSS client allows the RAM user to access the target directory from the root directory through levels of sub-directories.

Therefore, you need to add the following permissions to implement this type of directory navigation:

1. **Permission to list all buckets**
2. **Permission to list the subdirectories of the "myphotos" directory (In this example, the subdirectories include beijing, hangzhou, and qingdao.)**
3. **Permission to list the subdirectories under "myphotos/hangzhou" (The subdirectories include 2013, 2014, and 2015.)**

```
{
    " Version ": " 1 ",
    " Statement  ":[
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListBucket  s ",
                " oss : GetBucketA  cl "
            ],
            " Resource ": [
                " acs : oss :*:*:*"
            ]
        },
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : GetObject ",
                " oss : GetObjectA  cl "
```

```
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos / hangzhou / 2015 /*"
            ]
        },
        {
            " Effect ": " Allow ",
            " Action ": [
                " oss : ListObject  s "
            ],
            " Resource ": [
                " acs : oss :*:*: myphotos "
            ],
            " Condition ": {
                " StringLike ": {
                    " oss : Delimiter ": "/",
                    " oss : Prefix ": [
                        "",
                        " hangzhou /",
                        " hangzhou / 2015 /*"
                    ]
                }
            }
        }
    ]
}
```

Authorize a RAM user complete management of a bucket

You need to create an authorization policy first. Assume that your bucket is named “ myphotos”. Create the authorization policy as follows:

```
{
    " Version ": " 1 ",
    " Statement  ":[
        {
            " Effect ": " Allow ",
            " Action ": " oss :*",
            " Resource ": [
                " acs : oss :*:*: myphotos ",
                " acs : oss :*:*: myphotos /*"
            ]
        }
    ]
}
```

Then, add the authorization policy for this user.

RAM user authorized to manage a bucket notified of having no operation permissions when logging on to the OSS console

Assume that you create an authorization policy as follows to authorize a RAM user to read data objects from a bucket (such as “myphotos”):

```
{
  " Version ": " 1 ",
  " Statement  ":[
    {
```

```
      " Effect ": " Allow ",
      " Action ": [
        " oss : ListObject  s "
      ],
      " Resource ": " acs : oss :*:*: myphotos "
    },
    {
      " Effect ": " Allow ",
      " Action ": [
        " oss : GetObject "
      ],
      " Resource ": " acs : oss :*:*: myphotos /*"
    }
  ]
}
```

However, the RAM user was notified of having no operation permissions when logging on to the OSS console.

The reason is that when the RAM user logs on to the OSS console, the OSS console makes the RAM user access the OSS service as authorized. For a better user interaction experience, the OSS console also calls the ListBuckets, GetBucketAcl, and GetObjectAcl operations. (GetBucketAcl specifies whether a bucket is private or public. GetObjectAcl specifies an object is private or public.)

Therefore, to enable the RAM user to manage a bucket on the OSS console, you need to create the authorization policy as follows:

```
{
  " Version ": " 1 ",
  " Statement  ":[
    {
      " Effect ": " Allow ",
      " Action ": " oss : ListBucket  s ",
      " Resource ": " acs : oss :*:*:*"
    },
    {
      " Effect ": " Allow ",
      " Action ": [
        " oss : ListObject  s ",
        " oss : GetBucketA  cl "
      ],
      " Resource ": " acs : oss :*:*: myphotos "
    },
    {
      " Effect ": " Allow ",
      " Action ": [
        " oss : GetObject ",
        " oss : GetObjectA  cl "
      ],
      " Resource ": " acs : oss :*:*: myphotos /*"
    }
  ]
}
```

8 Authorization for RDS instances

Questions

- *View RDS permission definitions*
- *Assign the RDS read-only permission to a RAM user*
- *Assign full RDS service management permissions to a RAM user*
- *Authorize a RAM user to manage two specified RDS instances*
- *Access the content of the DMS management database as a RAM user*

View RDS permission definitions

See RDS resource authorization.

Assign the RDS read-only permission to a RAM user

Create a RAM user in the RAM console and add the system authorization policy ”AliyunRDSReadOnlyAccess” to the user. For more information about how to add an authorization policy, see *Authorization*.

Assign full RDS service management permissions to a RAM user

Add the system authorization policy “AliyunRDSFullAccess” to the RAM user in the RAM console.

Authorize a RAM user to manage two specified RDS instances

You must use the function of customizing authorization policies. For example, you have two instances and the IDs are i-001 and i-002:

First, you must create a custom authorization policy that includes permissions for managing i-001 and i-002 and viewing all RDS resources:

```
" Statement ": [

    " Action ": " rds :*",
    " Effect ": " Allow ",
    " Resource ": [
                " acs : rds :*:*: dbinstance / i - 001 ",
                " acs : rds :*:*: dbinstance / i - 002 "



    " Action ": " rds : Describe *",
    " Effect ": " Allow ",
    " Resource ": "*"
```

```
" Version ": " 1 "
```

Then, add the custom authorization policy for this user.

Access the content of the DMS management database as a RAM user

Access ApsaraDB for RDS through DMS. The corresponding authorization action is “dms:LoginDatabase”.

Authorize the RAM user to log on to the specified RDS instance

Authorization policy example:

```
" Statement ": [

    " Action ": " dms : LoginDatab  ase ",
    " Effect ": " Allow ",
    " Resource ": " acs : rds :*:*: dbinstance / rds783a063
9ks5k7328y "


" Version ": " 1 "
```

Replace `rds783a063 9ks5k7328y` with the ID of the RDS instance to be accessed.

Authorize the RAM user to log on to all RDS instances

Authorization policy example:

```
" Statement ": [

    " Action ": " dms : LoginDatab  ase ",
    " Effect ": " Allow ",
    " Resource ": " acs : rds :*:*:*"


" Version ": " 1 "
```

9 Authorization for SLB instances

Questions

- *View SLB permission definitions*
- *Assign the SLB read-only permission to a RAM user*
- *Assign the SLB full access permission to a RAM user*
- *Authorize a RAM user to manage two specified SLB instances*
- *A RAM user authorized to manage an SLB instance is notified of no operation permission when the user adds or removes ECS servers in the instance or sets weights*

View SLB permission definitions

See *RAM authentication* in the SLB OpenAPI document.

Assign the SLB read-only permission to a RAM user

Create a RAM user in the RAM console and add the system authorization policy "AliyunSLBReadOnlyAccess" to the user. For more information about how to add an authorization policy, see *Authorization*.

Assign the SLB full access permission to a RAM user

Add the system authorization policy "AliyunSLBFullAccess" to the RAM user in the RAM console.

Authorize a RAM user to manage two specified SLB instances

You must use the function of customizing authorization policies. For example, you have two instances and the IDs are i-001 and i-002:

First, you must create a custom authorization policy that includes permissions for managing i-001 and i-002 and viewing all SLB resources:

```
" Statement ": [

    " Effect ": " Allow ",
    " Action ": " slb :*",
    " Resource ": [
                " acs : slb :*:*: loadbalanc  er / i - 001 ",
                " acs : slb :*:*: loadbalanc  er / i - 002 "



    " Effect ": " Allow ",
    " Action ": " slb : Describe *",
```

```
      " Resource ": "*"

  " Version ": " 1 "
```

Then, add the authorization policy for this user.

A RAM user authorized to manage an SLB instance is notified of no operation permission when the user adds or removes ECS servers in the instance or sets weights

In the SLB, ECS server operation interfaces check not only the permissions for SLB resources, but also the permissions for ECS servers. This eliminates the situations in which a RAM user arbitrarily adds servers to an SLB instance after obtaining the permission for the instance.

For example, if you want to add the i-001 ECS server to the slb-001 SLB, you must grant the following permissions to your account:

```
" Statement ": [

    " Effect ": " Allow ",
    " Action ": " slb : AddBackend  Servers ",
    " Resource ": [" acs : slb :*:*: loadbalanc  er / slb - 001 "]


    " Effect ": " Allow ",
    " Action ": " slb : AddBackend  Servers ",
    " Resource ": [" acs : ecs :*:*: instance / i - 001 "]


      " Effect ": " Allow ",
      " Action ": " slb : DescribeLo  adBalancer  s ",
      " Resource ": " acs : slb :*:*: loadbalanc  er /*"


" Version ": " 1 "
```

You can make the authorization process more efficient so that you can grant management permissions for one SLB instance. This allows a user to add any servers to the instance and set the weight of any instances. See the following authorization policy. This authorization policy adds permissions for operations on all the SLB instances to the ECS resource.

```
" Statement ": [

    " Effect ": " Allow ",
    " Action ": " slb :*",
    " Resource ": [
                " acs : slb :*:*: loadbalanc  er / i - 001 ",
                " acs : slb :*:*: loadbalanc  er / i - 002 "
```

```
      " Effect ": " Allow ",
      " Action ": " slb : Describe *",
      " Resource ": "*"


      " Effect ": " Allow ",
      " Action ": " slb :*",
      " Resource ": " acs : ecs :*:*:*"


  " Version ": " 1 "
```

10 Authorization for CDN instances

Questions

Authorize a RAM user to perform the cache refresh and push operations

Authorize a RAM user to perform the cache refresh and push operations

You can create the following authorization policy for the user, which includes the permissions for reading content from CDN, refreshing the cache, and performing the push operation.

```
" Version ": " 1 ",
" Statement ": [

    " Action ": [
      " cdn : Describe *",
      " cdn : PushObject  Cache ",
      " cdn : RefreshObj  ectCaches "

    " Resource ": " acs : cdn :*:*:*",
    " Effect ": " Allow "
```

Then, assign the authorization policy to this user.