

# Alibaba Cloud Resource Access Management

FAQ

Issue: 20180929

# 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.	 <b>Danger:</b> 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.	 <b>Warning:</b> 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.	 <b>Note:</b> 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.	 <b>Note:</b> You can use <b>Ctrl + A</b> to select all files.
>	Multi-level menu cascade.	<b>Settings &gt; Network &gt; Set network type</b>
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click <b>OK</b> .
Courier font	It is used for commands.	Run the <code>cd /d C:/windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand / slave}</code>

# Contents

---

<b>Legal disclaimer.....</b>	<b>I</b>
<b>Generic conventions.....</b>	<b>I</b>
<b>1 Authorization for ECS instances.....</b>	<b>1</b>
<b>2 Authorization for OSS instances.....</b>	<b>4</b>
<b>3 Authorization for RDS instances.....</b>	<b>12</b>
<b>4 Authorization for SLB instances.....</b>	<b>14</b>
<b>5 Authorization for CDN.....</b>	<b>17</b>
<b>6 OSS authorization policy samples.....</b>	<b>18</b>
<b>7 RDS authorization policy samples.....</b>	<b>21</b>
<b>8 Server Load Balancer authorization policy samples.....</b>	<b>22</b>
<b>9 CDN authorization policy samples.....</b>	<b>24</b>
<b>10 RAM user logon.....</b>	<b>25</b>

# 1 Authorization for ECS instances

---

## Questions

- [View ECS permission definitions](#)
- [Assign full ECS service management permissions to a subaccount](#)
- [Assign 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:DescribeRegions",  
    "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 administrator 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:CreateSnapshot",  
    "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.

## 2 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:ListObjects",
      "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:ListBuckets",
      "Resource": "acs:oss:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:ListObjects",
        "oss:GetBucketAcl"
      ],
      "Resource": "acs:oss:*:*:myphotos"
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:GetObject",
        "oss:GetObjectAcl"
      ],
      "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:ListBuckets"
      ],
      "Resource": [

```

```

        "acs:oss:*:*:*"
    ],
    },
    {
        "Sid": "To allow only the users in the specified IP
address segment to obtain the information in the myphotos directory",
        "Effect": "Allow",
        "Action": [
            "oss:ListObjects",
            "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:ListBuckets"
            ],
            "Resource": [
                "acs:oss:*:*:*"
            ]
        },
        {
            "Sid": "To allow obtaining the information in the myphotos
directory",
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects",
                "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": {
      "NotIpAddress": {
        "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:ListObjects"
      ],
      "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:ListBuckets",
        "oss:GetBucketAcl"
      ],
      "Resource": [
        "acs:oss:*:*:*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:GetObject",
        "oss:GetObjectAcl"
      ],
      "Resource": [
        "acs:oss:*:*:myphotos/hangzhou/2015/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:ListObjects"
      ],

```

```

    "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:ListObjects"
      ],
      "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:ListBuckets",
      "Resource": "acs:oss:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:ListObjects",
        "oss:GetBucketAcl"
      ],
      "Resource": "acs:oss:*:*:myphotos"
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:GetObject",
        "oss:GetObjectAcl"
      ],
      "Resource": "acs:oss:*:*:myphotos/*"
    }
  ]
}
```

## 3 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:LoginDatabase",  
    "Effect": "Allow",  
    "Resource": "acs:rds:*:*:dbinstance/rds783a0639ks5k7328y"  
  }  
]  
  
"Version": "1"
```

Replace `rds783a0639ks5k7328y` 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:LoginDatabase",  
    "Effect": "Allow",  
    "Resource": "acs:rds:*:*:*"  
  }  
]  
  
"Version": "1"
```

## 4 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:*:*:loadbalancer/i-001",  
      "acs:slb:*:*:loadbalancer/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:AddBackendServers",  
    "Resource": ["acs:slb:*:*:loadbalancer/slb-001"]  
  },  
  {  
    "Effect": "Allow",  
    "Action": "slb:AddBackendServers",  
    "Resource": ["acs:ecs:*:*:instance/i-001"]  
  },  
  {  
    "Effect": "Allow",  
    "Action": "slb:DescribeLoadBalancers",  
    "Resource": "acs:slb:*:*:loadbalancer/*"  
  }  
]  
  
"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:*:*:loadbalancer/i-001",  
      "acs:slb:*:*:loadbalancer/i-002"  
    ]  
  },  
  {  
    "Effect": "Allow",  
    "Action": "slb:Describe*",  
    "Resource": "*"   
  }  
]
```

```
"Effect": "Allow",  
"Action": "slb:*",  
"Resource": "acs:ecs:*:*:*"  
  
"Version": "1"
```

## 5 Authorization for CDN

---

### 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:PushObjectCache",
      "cdn:RefreshObjectCaches"
    ],
    "Resource": "acs:cdn:*:*:*:*",
    "Effect": "Allow"
  }
]
```

Then, assign the authorization policy to this user.

## 6 OSS authorization policy samples

---

- Use Case #1

The following policy sample allows a RAM user to do READ operations on a specified OSS bucket (for example, myphotos) through the OSS web console.

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

  "Effect": "Allow",
  "Action": "oss:ListBuckets",
  "Resource": "acs:oss:*:*:*"

  "Effect": "Allow",
  "Action": [
    "oss:ListObjects",
    "oss:GetBucketAcl"
  ],
  "Resource": "acs:oss:*:*:myphotos"

  "Effect": "Allow",
  "Action": [
    "oss:GetObject",
    "oss:GetObjectAcl"
  ],
  "Resource": "acs:oss:*:*:myphotos/*"
```

- se Case #2

The following policy sample allows a RAM user to do READ operations on a specified OSS bucket (for example, myphotos) through the OSS SDK, where the Source IP address of an HTTP request must be "42.120.88.18" or "42.120.66.0/24 ".

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

  "Effect": "Allow",
  "Action": [
    "oss:ListBuckets"
  ],
  "Resource": [
    "acs:oss:*:*:*"
  ]

  "Effect": "Allow",
  "Action": [
    "oss:ListObjects",
    "oss:GetObject"
  ],
  "Resource": "acs:oss:*:*:myphotos/*"
```



```

    "Resource": [
      "acs:oss:*:*:myphotos",
      "acs:oss:*:*:myphotos/*"
    ],
    "Condition": {
      "IpAddress": {
        "acs:SourceIp": [ "42.120.88.18", "42.120.66.0/24" ]
      }
    }
  ]

```

- Use Case #3

The following policy sample allows a RAM user to do READ operations on a specified OSS path (for example, myphotos/hangzhou/2015/) through the OSS web console.

```

"Version": "1",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "oss:ListBuckets",
      "oss:GetBucketAcl"
    ],
    "Resource": [
      "acs:oss:*:*:*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "oss:GetObject",
      "oss:GetObjectAcl"
    ],
    "Resource": [
      "acs:oss:*:*:myphotos/hangzhou/2015/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "oss:ListObjects"
    ],
    "Resource": [
      "acs:oss:*:*:myphotos"
    ],
    "Condition": {
      "StringLike": {
        "oss:Delimiter": "/",
        "oss:Prefix": [
          "hangzhou/",
          "hangzhou/2015/"
        ]
      }
    }
  }
]

```



## 7 RDS authorization policy samples

---

If your tenant account has 10 RDS instances, but as a RAM administrator, you would like to grant only two instances to a RAM user. You can create a policy as follows:

**Note:**

One RAM user with this policy can view all RDS instances, but can only operate (for example, DeleteDBInstance) the granted two instances. Currently, RAM does not support to view only the authorized RDS instances.

```
"Statement ":[

  "Action": "RDS :*",
  "Effect": "allow ",
  "Resource ":[
    "ACS: RDS: *: dbinstance/i-001 ",
    "ACS: RDS: *: dbinstance/i-002"

  ]

  "Action": "RDS: Describe *",
  "Effect": "allow ",
  "Resource ":"*"

"Version": "1"
```

## 8 Server Load Balancer authorization policy samples

---

- Use Case #1

Suppose your tenant account has 10 Server Load Balancer instances. As a RAM administrator, you want to grant only two Server Load Balancer instances to a RAM user. Then, you can create a policy as follows:

**Note:**

One RAM user with this policy can view all Server Load Balancer instances, but can only operate (for example, DeleteLoadBalancer) the granted two Server Load Balancer instances. Currently, RAM does not support to view only the authorized Server Load Balancer instances.

```
"Statement": [
  {
    "Effect": "Allow",
    "Action": "slb:*",
    "Resource": [
      "acs:slb:*:*:loadbalancer/i-001",
      "acs:slb:*:*:loadbalancer/i-002"
    ]
  },
  {
    "Effect": "Allow",
    "Action": "slb:Describe*",
    "Resource": "*"
  }
]

"Version": "1"
```

- se Case #2

A RAM user adds a backend ECS server (for example, i-001) to a Server Load Balancer instance (for example, slb-001). The detailed policy is allows:

```
"Statement": [
  {
    "Effect": "Allow",
    "Action": "slb:AddBackendServers",
    "Resource": ["acs:slb:*:*:loadbalancer/slb-001"]
  },
  {
    "Effect": "Allow",
    "Action": "slb:AddBackendServers",
    "Resource": "acs:ecs:*:*:instance/i-001"
  }
]
```

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

- Use Case #3

A RAM user adds any backend ECS server in your tenant account to a Server Load Balancer instance (for example, slb-001). The detailed policy is allows:

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": "slb:*",  
    "Resource": ["acs:slb:*:*:loadbalancer/slb-001"]  
  },  
  {  
    "Effect": "Allow",  
    "Action": "slb:Describe*",  
    "Resource": "*"  
  },  
  {  
    "Effect": "Allow",  
    "Action": "slb:*",  
    "Resource": "acs:ecs:*:*:*"  
  }  
]  
  
"Version": "1"
```

## 9 CDN authorization policy samples

---

The following policy allows a RAM user to perform READ, Push, and Refresh operations on CDN resources.

```
"Version": "1",
"Statement": [
  {
    "Action": [
      "cdn:Describe*",
      "cdn:PushObjectCache",
      "cdn:RefreshObjectCaches"
    ],
    "Resource": "acs:cdn:*:*:*",
    "Effect": "allow"
  }
]
```

# 10 RAM user logon

---

## Questions

- [RAM user logon](#)
- [Enterprise alias](#)

## RAM user logon

on the overview page of the [RAM console](#).

## Enterprise alias

All the RAM user names under the same cloud account are unique, but identical RAM user names under different cloud accounts are allowed. Therefore, you need to specify a cloud account when logging on as a RAM user.

When you log on using the RAM user logon link on the overview page of the RAM console, the system automatically enters an enterprise alias for you.

You can log on to the RAM console using the primary account. Choose **Settings > Enterprise Alias Settings**, and view and set your cloud account alias.