Alibaba Cloud
Resource Access Management

FAQ

Issue: 20190912

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 informatio n, 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 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:DescribeInstances"` (view ECS instances), `"rds:DescribeDBInstances"` (view RDS instances), and `"slb:DescribeLoadBalancer"` (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.

2 STS FAQ

Why does an error occur when I use STS?

If the following error message is displayed, it means that the AliyunSTSAssumeRoleAccess policy is not attached to the authorized user:

```
Error   message :  You   are   not   authorized   to   do   this
action .  You   should   be   authorized   by   RAM
```

Attach the AliyunSTSAssumeRoleAccess policy to the authorized user and then continue to use STS.

What permissions does an STS token have?

The permissions of an STS token are the specified role's permissions that are included in the policy set when the AssumeRole API is called.

If you do not set the policy parameter when calling the AssumeRole API, the returned STS token will have all the permissions of the specified role.

What is the validity period of an STS token?

The validity period of an STS token ranges from 900 seconds to 3600 seconds. The default value is 3600 seconds. You can set the DurationSeconds parameter when calling the AssumeRole API to limit the valid period of an STS token.

Is there an upper limit to the number of times that STS API can be called?

STS supports up to 100 Queries Per Second (QPS). If the call requests exceed 100 QPS, an error is reported.

If multiple STS tokens have been obtained at different times, are the old and new tokens valid at the same time?

Both the new and old STS tokens are valid before their expiration time.

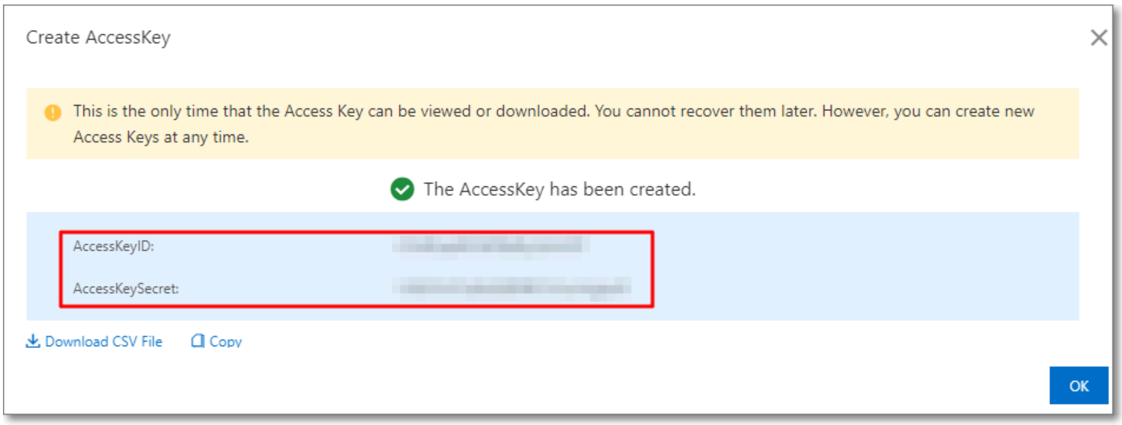
3 FAQ about AccessKey pairs

This topic describes FAQ about AccessKey pairs.

What information is displayed when I create an AccessKey pair for the first time?

When you create an AccessKey pair for the first time, the following information is displayed:

- AccessKey ID
- AccessKey secret



Create AccessKey

This is the only time that the Access Key can be viewed or downloaded. You cannot recover them later. However, you can create new Access Keys at any time.

The AccessKey has been created.

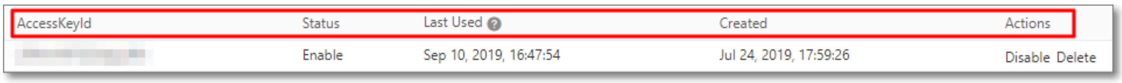
AccessKeyID: [redacted]

AccessKeySecret: [redacted]

What information can be viewed after I create an AccessKey pair?

After creating an AccessKey pair, you can query the basic information of the AccessKey pair. For more information, see #unique_8.

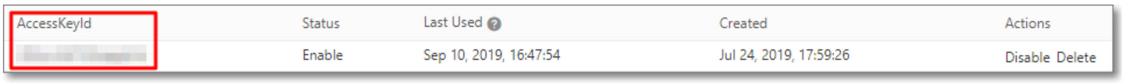
> **Note:**
> You can only view the basic information of the AccessKey pair, such as the AccessKey ID, status, creation time, and the time when the pair was last used.



AccessKeyId	Status	Last Used	Created	Actions
[redacted]	Enable	Sep 10, 2019, 16:47:54	Jul 24, 2019, 17:59:26	Disable Delete

Can I view the AccessKey ID after I create an AccessKey pair?

After creating an AccessKey, you can query the AccessKey ID.



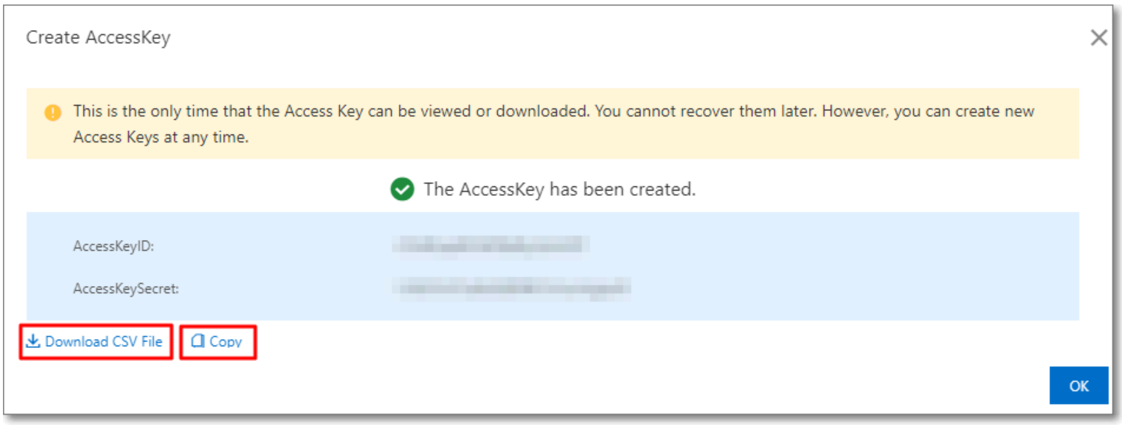
AccessKeyId	Status	Last Used	Created	Actions
[redacted]	Enable	Sep 10, 2019, 16:47:54	Jul 24, 2019, 17:59:26	Disable Delete

Can I view the AccessKey secret after I create an AccessKey pair?

The AccessKey secret is only displayed when you create an AccessKey pair, and is unavailable for subsequent queries. We recommend that you save the AccessKey secret for subsequent use.

How can I view the AccessKey secret?

When creating an AccessKey pair, you can manually save the AccessKey pair information to an on-premises device by using either of the following two methods:


Create AccessKey

This is the only time that the Access Key can be viewed or downloaded. You cannot recover them later. However, you can create new Access Keys at any time.

The AccessKey has been created.

AccessKeyID: [redacted]

AccessKeySecret: [redacted]

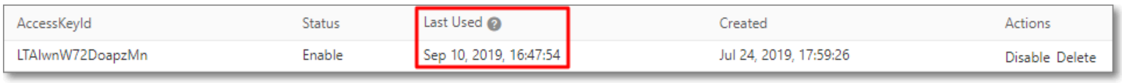
- Click Download CSV file to download an excel that contains the AccessKey pair information to an on-premises device. The information includes the status, AccessKey ID, and AccessKey secret.
- Click Copy to save the AccessKey ID and AccessKey secret to an on-premises device.

How can I check whether the AccessKey pair is in use?

You can view the time when the AccessKey pair was last used to check whether the pair is in use.

Note:

Use caution when you delete an AccessKey pair. If the AccessKey pair is being used by an app, system errors may occur on the app.



AccessKeyId	Status	Last Used	Created	Actions
LTAIwnW72DoapzMn	Enable	Sep 10, 2019, 16:47:54	Jul 24, 2019, 17:59:26	Disable Delete

4 What can I do if the permissions of RAM users are missing after I have attached tags to a group of RDS instances and granted permissions to RAM users?

This topic describes how to troubleshoot the problem if RAM users cannot access a group of tagged RDS instances on which the users are granted the permissions.

Problem

After you use tags to group the target RDS instances and grant relevant permissions to an RAM user, the following problem occurs. When you log on to the ApsaraDB for RDS console as the RAM user, an error message appears and shows that you are not authorized to perform any operations.

Troubleshooting

1. Check whether tags are attached to correct instances.
2. Check whether tag keys and values specified in permission policies are the same with those attached to the instances.

   Note:

   Tag keys and values attached to the instances cannot contain uppercase letters. If you enter uppercase letters, they are automatically converted to lowercase letters when saved.
3. Check whether you have been granted the required permissions before logging on to the ApsaraDB for RDS console.
4. Check whether the current region displayed in the console is the expected region.
5. Check whether you have selected the corresponding tag value to filter the intended resources.
6. If the problem persists and an error message shows that you are not authorized to perform operations in the ApsaraDB for RDS console, close the error message.

   Note:

The message is "You do not have permission for this operation. Please go to the RAM console for authorization." This message appears because all resources are displayed in the console, and the current RAM user is not authorized to view all resources.