

Alibaba Cloud

Realtime Compute Preparation

Document Version: 20220125

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
 Danger	A danger notice 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.
 Warning	A warning notice 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 restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1. Grant permissions to a RAM user	05
2. Activate Realtime Compute for Apache Flink and create a proj... ..	07
3. Role authorization	11
3.1. Assign a RAM role to an account that uses Realtime Comp... ..	11

1. Grant permissions to a RAM user

You can use an Alibaba Cloud account to purchase Realtime Compute for Apache Flink and create projects. You can also use the Alibaba Cloud account to authorize Resource Access Management (RAM) users to access Realtime Compute for Apache Flink projects that are created by the Alibaba Cloud account. This topic describes how to create a RAM user and authorize the RAM user to access Realtime Compute for Apache Flink.

What is a RAM user?

A physical identity that has a fixed ID and credential information. A RAM user represents a person or an application. A RAM user has the following characteristics:

- A RAM user can be created by an Alibaba Cloud account. In this case, the RAM user belongs to the Alibaba Cloud account. A RAM user can also be created by a RAM user or a RAM role that has administrative rights. In this case, the RAM user belongs to the Alibaba Cloud account that creates the RAM user or the RAM role.
- A RAM user does not own resources. Resource usage fees of the RAM user are billed to the Alibaba Cloud account to which the RAM user belongs. A RAM user does not receive individual bills and cannot make payments.
- Before RAM users can log on to the Alibaba Cloud Management Console or call operations, they must be authorized by Alibaba Cloud accounts. After RAM users are authorized, the RAM users can access resources that are owned by the Alibaba Cloud accounts.
- RAM users have independent passwords or AccessKey pairs for logon.
- An Alibaba Cloud account can create multiple RAM users. RAM users can be employees, systems, and applications within an enterprise.

You can create RAM users and authorize the RAM users to access different resources. If multiple users in your enterprise need to simultaneously access resources, you can use RAM to assign the least permissions to the users. This prevents the users from sharing the username and password or AccessKey pair of an Alibaba Cloud account and reduces the security risks.

Procedure

1. Create a RAM user.

For more information about how to create a RAM user, see [Create a RAM user](#).

Note

- You must initialize RAM when you use RAM for the first time. For more information, see [Configure a password policy for RAM users](#) and [Configure security policies for RAM users](#).
- To ensure account security, Realtime Compute for Apache Flink provides the account verification feature. If you do not manage a job for a long period of time, the system sends a text message and an email to you for account verification.

2. Create a custom policy.

For more information about how to create a custom policy in the RAM console, see [Create a custom policy](#). The following code shows a policy of Realtime Compute for Apache Flink:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "stream:*",
      "Resource": "acs:stream:*:*:*",
      "Effect": "Allow"
    },
    {
      "Action": "ram:PassRole",
      "Resource": "acs:ram:*:*:*",
      "Effect": "Allow"
    }
  ]
}
```

 **Note** The policy of Realtime Compute for Apache Flink allows you to grant permissions on different projects to different RAM users. To authorize a RAM user to access a single project, change Resource in the preceding code to "Resource": "acs:stream:*:*:projectname". projectname is the name of the project that you want to authorize the RAM user to access.

3. Authorized RAM users or user groups.

Attach the preceding policy to specified RAM users or RAM user groups. For more information, see [Grant permissions to a RAM user](#) and [Grant permissions to a RAM user group](#).

4. Use the credentials of a RAM user to log on to the Realtime Compute for Apache Flink console.

In the left-side navigation pane of the [RAM console](#), click **Overview** and view the logon address of the RAM user in the **Account Management** section.

2. Activate Realtime Compute for Apache Flink and create a project

This topic describes how to activate Realtime Compute for Apache Flink in exclusive mode. This topic also describes how to create Realtime Compute for Apache Flink clusters and projects in exclusive mode.

Activate Realtime Compute for Apache Flink in exclusive mode

Note

- Realtime Compute for Apache Flink in exclusive mode cannot be purchased from April 28, 2021. You can only scale out, scale in, or renew the existing projects of Realtime Compute for Apache Flink in exclusive mode. If you want to purchase Realtime Compute for Apache Flink, we recommend that you purchase [fully managed Flink](#). If you have questions, [submit a ticket](#).
- A Realtime Compute for Apache Flink cluster in exclusive mode can access only storage resources in the same virtual private cloud (VPC), region, and security group as the cluster. To allow the cluster to access resources in another VPC, use [Express Connect](#) to access the VPC.

After you place an order for Realtime Compute for Apache Flink in exclusive mode, you must create a cluster before you create a project.

1. Activate Realtime Compute for Apache Flink.
 - i. Log on to the [product page of Realtime Compute for Apache Flink](#).

 **Note** Use your Alibaba Cloud account instead of a RAM user to activate Realtime Compute for Apache Flink and create a project. If you do not have an Alibaba Cloud account, create one first.

- ii. Click **Buy Now**.
 - iii. Configure the parameters, including the region, master node specifications, number of master nodes, slave node specifications, number of slave nodes, and billing duration based on your business requirements.
 - iv. Click **Buy Now**.
 - v. Read the terms of service and select **I have read and agree to Realtime Compute Exclusive Mode (Subscription) Agreement of Service**.
 - vi. Click **Pay**.
2. Create a Realtime Compute for Apache Flink cluster.
 - o Preparations

- After you activate Realtime Compute for Apache Flink in exclusive mode, Realtime Compute for Apache Flink creates a security group in your VPC and applies for an elastic network interface (ENI). For more information, see [Overview](#).

 **Note** Do not delete the security group or the ENI. Otherwise, the cluster cannot be created.

- If you have VPCs, specify a VPC for Realtime Compute for Apache Flink.
- If you do not have a VPC, activate the Alibaba Cloud VPC service. For more information about how to activate the Alibaba Cloud VPC service, see [Plan networks](#).

 **Note** Make sure that the VPC you created meets the following requirements:

- Sufficient Elastic Compute Service (ECS) instances are available in the VPC. If ECS instances are insufficient, [submit a ticket](#).
- The number of available IP addresses in a vSwitch is greater than or equal to the number of nodes in a Realtime Compute for Apache Flink cluster. For more information, see [View the nodes of a Realtime Compute for Apache Flink cluster](#) and [Work with vSwitches](#).

- You can upload a UDF package to a Realtime Compute for Apache Flink cluster in exclusive mode. To ensure data security, Realtime Compute for Apache Flink stores the UDF package to an Object Storage Service (OSS) bucket. You must specify the OSS bucket. If you do not have OSS buckets, create one first. For more information about how to create an OSS bucket, see [Create buckets](#).
 - Assign a RAM role to an account that uses Realtime Compute for Apache Flink in exclusive mode. For more information, see [Assign a RAM role to an account that uses Realtime Compute for Apache Flink in exclusive mode](#).
- o Procedure
- a. After you complete the payment, click **Console**.
 - b. On the **Clusters** page, click **Create Cluster**.

 **Note** If no project is created for an order, a red number is displayed on **Create Cluster** in the upper-right corner of the **Clusters** page. The number indicates the number of orders for which no project is created.

- c. In the **Select Order** step, select an order in **Order ID** and click **Next**.
- d. In the **Basic Information** step, configure **Cluster Name** and **Cluster Description** and click **Next**.
- e. In the **Cluster Settings** step, enter the configuration information and click **Next**.

 **Note** The Realtime Compute for Apache Flink cluster must reside in the same security group, region, and VPC as the upstream and downstream storage that you purchased.

■ OSS Bucket

Select an OSS bucket in which you want to store your UDF package. If you do not have OSS buckets, create one first. For more information, see [Create buckets](#). When you create an OSS bucket, you must specify **Standard** for **Storage Class**. We recommend that you specify **Private** for **Access Control List (ACL)**. Do not select **Public Read**.

The screenshot shows the 'Create Bucket' dialog box with the following configuration:

- Endpoint: oss-cn-beijing.aliyuncs.com
- Storage Class: Standard (highlighted with a red box)
- Zone-redundant Storage: Disabled
- Versioning: Enabled (highlighted with a red box)
- Access Control List (ACL): Private (highlighted with a red box)

Informational messages in the dialog:

- Zone-redundant Storage:** Zone-redundant storage improves the availability of data. This feature incurs extra costs. For more information about the pricing of this feature, visit [price details](#). This feature cannot be disabled after it is enabled.
- Versioning:** After versioning is enabled for a bucket, data that is overwritten or deleted is saved as a previous version. [Learn more](#). However, if versioning is enabled for the bucket, mirroring back-to-origin cannot be enabled for the bucket and the versioning status of the bucket cannot be set back to disabled.

■ VPC

Select the VPC that you want to access and customize the name of the VPC.

Note Realtime Compute for Apache Flink can identify only custom VPC names.

- **Zone**

After you properly configure the VPC, the system automatically displays the available zones.

-  **Note** No available zone or vSwitch is displayed in the following scenarios:
- ECS instances in the selected zone are insufficient. For more information about how to add an ECS instance, see [Create an instance by using the wizard](#).
 - The number of available IP addresses in the vSwitch that you select is less than the number of nodes in a Realtime Compute for Apache Flink cluster. For more information, see [View the nodes of a Realtime Compute for Apache Flink cluster](#) and [Work with vSwitches](#).

- **CIDR Block**

The available CIDR blocks are automatically displayed.

f. In the **Confirm** step, click **Create**.

-  **Note** The cluster is created after it enters the **Running** state from the **Starting** state. This process takes about half an hour. If the cluster remains in the **Starting** state for a long period of time, [submit a ticket](#).

3. Create a project.

- In the left-side navigation pane, choose **Cluster Management > Clusters**. Find the cluster for which you want to create a project and click **Create Project** in the **Actions** column.
- In the **Create Project** dialog box, configure **Project Name** and **Project Description**, and slide the pointer on the right side of **Specified CUs** to specify the required number of compute units (CUs).
- Click **OK**.

3. Role authorization

3.1. Assign a RAM role to an account that uses Realtime Compute for Apache Flink in exclusive mode

This topic describes how to assign a Resource Access Management (RAM) role to an account that uses Realtime Compute for Apache Flink in exclusive mode.

Assign a RAM role to an account

You must assign a RAM role to your Alibaba Cloud account before you use Realtime Compute for Apache Flink.

1. Click **Authorize** to go to the authorization page.

 **Note** If you do not assign the default RAM role to your Alibaba Cloud account, the preceding message appears when you use Realtime Compute for Apache Flink.

2. Click **AliyunStreamDefaultRole** and click **Authorize**.

 **Note** After your account is assigned the RAM role, refresh the page in the Realtime Compute for Apache Flink console. Then, you can perform operations in the console.

View the authorization information about the current role

1. Log on to the RAM console.
 - Log on to the **RAM console** by using your Alibaba Cloud account.
 - Log on to the **RAM console** as a RAM user.
2. In the left-side navigation pane, click **Roles**. On the Roles page, click **AliyunStreamDefaultRole** in the **Role Name** column of the role list.
3. On the **AliyunStreamDefaultRole** page, click **AliyunStreamRolePolicy** in the Policy column on the **Permissions** tab.
4. On the **Policy Document** tab, view the current policy information of Realtime Compute for Apache Flink.

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "ots:List*",
        "ots:DescribeTable",
        "ots:Get*",
        "ots:*Row"
      ],
      "Resource": "*"
    }
  ]
}
```

```
"Effect": "Allow"
},
{
  "Action": [
    "dhs:Create*",
    "dhs:List*",
    "dhs:Get*",
    "dhs:PutRecords",
    "dhs>DeleteTopic"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "log:List*",
    "log:Get*",
    "log:Post*"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "mns:List*",
    "mns:Get*",
    "mns:Send*",
    "mns:Publish*",
    "mns:Subscribe"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "drds:DescribeDrdsInstance",
    "drds:ModifyDrdsIpWhiteList"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "rds:Describe*",
    "rds:ModifySecurityIps*"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "vpc:DescribeVpcs",
    "vpc:DescribeVSwitches"
  ],
  "Resource": "*",
  "Effect": "Allow"
}
```

```
"Resource": "*",
  "Effect": "Allow"
},
{
  "Action": [
    "ecs:CreateSecurityGroup",
    "ecs:AuthorizeSecurityGroup",
    "ecs:CreateNetworkInterface",
    "ecs:DescribeNetworkInterfaces",
    "ecs:AttachNetworkInterface",
    "ecs:DescribeNetworkInterfacePermissions",
    "ecs:CreateNetworkInterfacePermission"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": "oss:*",
  "Resource": "*",
  "Effect": "Allow"
}
]
```

Attach a policy to a RAM role

After you create a RAM role, you can attach a specific policy to the RAM role.

1. Log on to the RAM console.
 - Log on to the [RAM console](#) by using your Alibaba Cloud account.
 - Log on to the [RAM console](#) as a RAM user.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the Policies page, click **Create Policy**.
4. On the Create Policy page, configure **Name** and **Note**. In this example, the policy name is **AliyunStreamDefaultRolePolicy**.
5. In the code editor below **Policy Document**, enter the following code and click **OK**:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "vpc:DescribeVpcs",
        "vpc:DescribeVSwitches"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ecs:CreateSecurityGroup",
        "ecs:AuthorizeSecurityGroup",
        "ecs:CreateNetworkInterface",
        "ecs:DescribeNetworkInterfaces",
        "ecs:AttachNetworkInterface",
        "ecs:DescribeNetworkInterfacePermissions",
        "ecs:CreateNetworkInterfacePermission"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

 **Note** You can delete the following permissions after you create a cluster:

- o ecs:CreateSecurityGroup
- o ecs:AuthorizeSecurityGroup

6. In the left-side navigation pane, click **Roles**. On the Roles page, find **AliyunStreamDefaultRole** in the role list and click **Add Permissions** in the **Actions** column.
7. In the Add Permissions panel, click **Custom Policy** in the **Select Policy** section and enter *AliyunOSSFullAccess* in the search box below **Custom Policy**.
8. Click **AliyunOSSFullAccess** in the **Authorization Policy Name** column.
9. In the **Add Permissions** panel, click **Custom Policy** in the **Select Policy** section.
10. In the search box below **Custom Policy** of the **Select Policy** section, enter *AliyunStreamDefaultRolePolicy*.
11. Click **AliyunStreamDefaultRolePolicy** in the **Authorization Policy Name** column.
12. Click **OK**.