ALIBABA CLOUD

Alibaba Cloud

Message Queue for Apache Kafka

Access control

Document Version: 20210507

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 `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Overview

This topic describes two access control mechanisms supported by Message Queue for Apache Kafka : Resource Access Management (RAM) and access control list (ACL).

Access control mechanism	Description	Documentation
RAM	RAM is a service provided by Alibaba Cloud to manage user identities and resource access permissions. You can only grant permissions to RAM users in the Message Queue for Apache Kafka console or by using the corresponding API operations. No matter whether RAM users are authorized or not, RAM users can use SDKs to send and subscribe to messages. For more information, see What is RAM?.	• RAM policies • Grant permissions to RAM users • Grant permissions across Alibaba Cloud accounts • Service-linked roles
ACL	The ACL feature is provided by Message Queue for Apache Kafka to manage the permissions of Simple Authentication and Security Layer (SASL) users and clients to send and subscribe to messages by using SDKs. It is consistent with the ACL feature in open-source Apache Kafka. The ACL feature is only applicable to scenarios where you want to implement access control for users that use Message Queue for Apache Kafka SDK to send and subscribe to messages. It is not applicable to scenarios where you want to implement access control for users that send and subscribe to messages in the Message Queue for Apache Kafka console or by using API operations. For more information, see Authorization and ACLs.	Authorize SASL users

2.RAM policies

Alibaba Cloud offers Resource Access Management (RAM), which allows you to manage permissions for the Message Queue for Apache Kafka console and API. RAM allows you to avoid sharing the AccessKey pair, which includes an AccessKey ID and an AccessKey secret, of your Alibaba Cloud account with other users. Instead, you can grant users only the minimum required permissions.

RAM policies

In RAM, policies are a set of permissions that are described based on the policy structure and syntax. You can use policies to describe the authorized resource sets, authorized operation sets, and authorization conditions. For more information, see Policy structure and syntax.

In RAM, a policy is a resource entity. Message Queue for Apache Kafka supports the following types of policies:

- System policies: System policies are created and updated by Alibaba Cloud and you cannot modify them. These policies are applicable to coarse-grained control of RAM user permissions.
- Custom policies: You can create, update, and delete custom policies and maintain policy versions. These policies are applicable to fine-grained control of RAM user permissions.

System policies

The following table lists the system policies supported by Message Queue for Apache Kafka .

Policy	Description
AliyunKafkaFullAccess	The management permission of Message Queue for Apache Kafka . The RAM user who has been granted this permission has the permission equivalent to the Alibaba Cloud account, that is, all operation permissions of the console and API.
AliyunKafkaReadOnlyAccess	The read-only permission of Message Queue for Apache Kafka . The RAM user who has been granted this permission has only the read-only permission of all resources of the Alibaba Cloud account, and does not have the operation permissions of the console and API.

Examples of system policies

Use the system policy AliyunKafkaFullAccess as an example. The RAM user who has been granted this permission has the permission equivalent to the Alibaba Cloud account, that is, all operation permissions of the console and API. The following code displays the policy content:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "alikafka:*",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

Custom policies

The following table lists the custom policies supported by Message Queue for Apache Kafka .

Action	Permission description	Read-only or not
ReadOnly	Only reads all resources.	Yes
ListInstance	Views instances.	Yes
StartInstance	Deploys instances.	No
UpdateInstance	Changes instance configuration.	No
ReleaseInstance	Releases instances.	No
ListTopic	Views topics.	Yes
CreateTopic	Creates topics.	No
UpdateTopic	Changes topic configuration.	No
DeleteTopic	Deletes topics.	No
ListGroup	Views consumer groups.	Yes
CreateGroup	Creates consumer groups.	No
UpdateGroup	Changes consumer group configuration.	No
DeleteGroup	Deletes consumer groups.	No
QueryMessage	Queries messages.	Yes
SendMessage	Sends messages.	No
DownloadMessage	Downloads messages.	Yes
CreateDeployment	Creates connector tasks.	No
DeleteDeployment	Deletes connector tasks.	No

Action	Permission description	Read-only or not
ListDeployments	Views connector tasks.	Yes
UpdateDeploymentRemark	Updates connector task description.	No
GetDeploymentLog	Obtains the operational logs of connector tasks.	Yes
EnableAcl	Enables the access control list (ACL) feature.	No
CreateAcl	Creates an ACL.	No
DeleteAcl	Deletes an ACL.	No
ListAcl	Queries ACLs.	Yes
CreateSaslUser	Creates a Simple Authentication and Security Layer (SASL) user.	No
DeleteSaslUser	Deletes an SASL user.	No
ListSaslUser	Queries SASL users.	Yes

Examples of custom policies

Use the custom policy AliyunKafkaCustomAccess as an example. The RAM user who has been granted this permission only has the permissions to view the alikafka_post-cn-xxx instance, view topics, view consumer groups, query messages, and download messages in the console and by using API operations. The following code displays the policy content:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
       "alikafka:ListInstance",
       "alikafka:ListTopic",
       "alikafka:ListGroup",
       "alikafka:QueryMessage",
       "alikafka:DownloadMessage"
            ],
      "Resource": "acs:alikafka:*:*:alikafka_post-cn-xxx",
      "Effect": "Allow"
    }
  ]
}
```

3.Grant permissions to RAM users

By using Resource Access Management (RAM), you can grant different permissions to different RAM users to avoid security risks caused by exposure of your Alibaba Cloud account's AccessKey pair.

Scenarios

An enterprise has activated Message Queue for Apache Kafka and wants to grant different permissions to its employees with different duties to operate Message Queue for Apache Kafka resources. This enterprise has the following requirements:

- For security reasons, the enterprise does not want to disclose the AccessKey pair of its Alibaba Cloud account to employees. Instead, it prefers to create different RAM users for the employees and grant different permissions to these users.
- A RAM user can only use resources under authorization. Resource usage and costs are not calculated separately for that RAM user. All expenses are billed to the Alibaba Cloud account of the enterprise.
- The enterprise can revoke the permissions granted to RAM users and delete RAM users at any time.

Instructions

Before authorizing RAM users, note the following:

You can only grant permissions to RAM users in the console or by using the corresponding API operations of Message Queue for Apache Kafka. No matter RAM users are authorized or not, the RAM users can use the Message Queue for Apache Kafka SDK to send and subscribe to messages.

You can use the SDK to send and subscribe to messages in the same way as in open-source clients. To manage the IP addresses that can use the SDK to send and subscribe to messages, log on to the Message Queue for Apache Kafka console, and set an IP address whitelist on the **Instance Details** page.

Step 1: Create a RAM user

Use your Alibaba Cloud account to log on to the RAM console and create a RAM user.

1. Log on to the RAM console.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click **Create User**.
4. On the **Create User** page, set **Logon Name** and **Display Name** in the **User Account Information** section.
5. If you want to create multiple RAM users at a time, click **Add User**, and repeat the previous step.
6. In the **Access Mode** section, select **Console Password Logon** or **Programmatic Access**, and then click **OK**.

   > **Note** For security purposes, select only one access mode.

   - If you select **Console Password Logon**, perform further settings. For example, you can select Automatically Generate Default Password or Custom Logon Password for Console Password, Required at Next Logon or Not Required for Password Rest, and Required to Enable MFA or Not Required for Multi-factor Authentication.
   - If you select **Programmatic Access**, RAM automatically generates an AccessKey pair for the

RAM user. Then, the RAM user can access your Message Queue for Apache Kafka by calling the corresponding API operations.

> **Notice** For security reasons, the RAM console allows you to view or download the AccessKey secret only once. Therefore, when creating an AccessKey pair, record the AccessKey secret safely.

7. In the **Verify by Phone Number** dialog box, click **Get Verification Code**, enter the verification code sent to your mobile phone, and then click **OK**.

Step 2: Grant permissions to the RAM user

Before using a RAM user, you must grant permissions to the RAM user.

1. Log on to the RAM console.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, find the target user, and click **Add Permissions** in the **Actions** column.
4. On the **Add Permissions** page, select a permission policy in the **Select Policy** drop-down list. Enter the permission policy you want to add to the text box, click the permission policy displayed, and then click **OK**.

   - System policy

     Currently, Message Queue for Apache Kafka supports two coarse-grained system policies.

Policy	Description
AliyunKafkaFullAccess	The permission to manage Message Queue for Apache Kafka . It is equivalent to the permission that the Alibaba Cloud account has. A RAM user to which this permission is granted can send and subscribe to all messages and use all the features of the console.
AliyunKafkaReadOnlyAccess	The read-only permission of Message Queue for Apache Kafka . A RAM user to which this permission is granted can only read all resources of the Alibaba Cloud account.

> **Note** We recommend that you grant AliyunKafkaFullAccess to O&M personnel to create and delete resources. We recommend that you grant AliyunKafkaReadOnlyAccess to developers, so that developers can view resources but cannot delete or create resources. If you want to control the permissions of developers in a more fine-grained manner, you can use the following custom policy.

   - Custom policy

     If you need more fine-grained authorization, you can create a custom policy for access control.

     For more information about how to create a custom policy, see Create a custom policy.

     To help you customize RAM policies, the following table lists mapping of custom policies for Message Queue for Apache Kafka .

Mapping of custom policies for Message Queue for Apache Kafka

Action	Description	Read-only or not
ReadOnly	Reads all resources only. It is a compound permission.	Yes
ListInstance	Views instances.	Yes
StartInstance	Deploys instances.	No
UpdateInstance	Changes instance configuration.	No
ReleaseInstance	Releases instances.	No
ListTopic	Views topics.	Yes
CreateTopic	Creates topics.	No
UpdateTopic	Changes topic configuration.	No
DeleteTopic	Deletes topics.	No
ListGroup	Views consumer groups.	Yes
CreateGroup	Creates consumer groups.	No
UpdateGroup	Changes consumer group configuration.	No
DeleteGroup	Deletes consumer groups.	No
QueryMessage	Queries messages.	Yes
SendMessage	Sends messages.	No
DownloadMessage	Downloads messages.	Yes

Example 1: Grant a RAM user the read-only permission on the `alikafka_post-cn-xxx` instance

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
       "alikafka:ReadOnly"
            ],
      "Resource": "acs:alikafka:*:*:alikafka_post-cn-xxx",
      "Effect": "Allow"
    }
  ]
}
```

Example 2: Grant a RAM user permissions to view instances, topics, and consumer groups and query and download messages on the `alikafka_post-cn-xxx` instance

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
       "alikafka:ListInstance",
       "alikafka:ListTopic",
       "alikafka:ListGroup",
       "alikafka:QueryMessage",
       "alikafka:DownloadMessage"
            ],
      "Resource": "acs:alikafka:*:*:alikafka_post-cn-xxx",
      "Effect": "Allow"
    }
  ]
}
```

Example 3: Grant a RAM user all permissions on the `alikafka_post-cn-xxx` instance

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
       "alikafka:*Instance",
       "alikafka:*Topic",
       "alikafka:*Group",
       "alikafka:*Message"
            ],
      "Resource": "acs:alikafka:*:*:alikafka_post-cn-xxx",
      "Effect": "Allow"
    }
  ]
}
```

5. On the **Add Permissions** page, view the authorization information summary in the **Authorization Result** section, and then click **Finished**.

What to do next

After creating a RAM user with an Alibaba Cloud account, you can distribute the logon name and password of the RAM user or AccessKey pair information to other employees. Other employees can log on to the console or call an API operation with the RAM user through the following steps.

- Log on to the console
  1. Open the RAM User Logon page.
  2. On the **RAM User Logon** page, enter the logon name of the RAM user, click **Next**, enter the password, and then click **Log on**.

     > ⓘ **Note** The logon name of the RAM user is in the format of `<$username>@<$AccountAlias>` or `<$username>@<$AccountAlias>.onaliyun.com`. `<$AccountAlias>` is the account alias. If no account alias is set, the ID of the Alibaba Cloud account is used.

  3. On the **Users** page, click a product with the permission to access the console.
- Call an API operation

  Call an API operation with the RAM user's AccessKey pair.

  Use the AccessKey ID and AccessKey secret of the RAM user in the code.

References

- What is RAM?
- Terms
- Create a RAM user
- Grant permissions to a RAM user
- Log on to the console as a RAM user

4.Grant permissions across Alibaba Cloud accounts

You can use a RAM role to grant permissions across Alibaba Cloud accounts so that an enterprise can access the Message Queue for Apache Kafka instance of another enterprise.

Context

Enterprise A has activated Message Queue for Apache Kafka . Enterprise A requires Enterprise B to manage Message Queue for Apache Kafka resources, such as instances, topics, and consumer groups. Enterprise A has the following requirements:

- Enterprise A can focus on its business systems and only act as the owner of Message Queue for Apache Kafka . Enterprise A can authorize Enterprise B to maintain, monitor, and manage Message Queue for Apache Kafka .
- If an employee joins or leaves Enterprise B, no permission change is required. Enterprise B can grant its RAM users fine-grained permissions on cloud resources of Enterprise A. The RAM user credentials can be assigned to either employees or applications.
- If the agreement between Enterprise A and Enterprise B ends, Enterprise A can revoke the permissions from Enterprise B.

Step 1: Enterprise A creates a RAM role

Use the Alibaba Cloud account of Enterprise A to log on to the RAM console, and create a RAM role for the Alibaba Cloud account of Enterprise B.

1. Log on to the RAM console.
2. In the left-side navigation pane, click **RAM Roles**.
3. On the **RAM Roles** page, click **Create RAM Role**.
4. In the **Create RAM Role** panel, select **Alibaba Cloud Account** and click **Next**.
5. In the **RAM Role Name** field, enter a RAM role name. Set the **Select Trusted Alibaba Cloud Account** parameter to **Other Alibaba Cloud Account** and enter the ID of the Alibaba Cloud account of Enterprise B. Then, click **OK**.

   > Note
   >
   > - The RAM role name can be up to 64 characters in length and can contain letters, digits, and hyphens (-).
   > - You can view the account ID on the **Security Settings** page of the **Account Management** console.

Step 2: Enterprise A grants permissions to the RAM role

Grant the RAM role the permissions to access the Message Queue for Apache Kafka resources of Enterprise A. The permissions are to be granted to Enterprise B.

1. In the left-side navigation pane of the RAM console, click **RAM Roles**.
2. On the **RAM Roles** page, find the RAM role, and click **Add Permissions** in the **Actions** column.
3. In the **Select Policy** section of the **Add Permissions** panel, click System Policy or Custom Policy.

Enter the keyword of the policy that you want to attach to the RAM role in the search box, click the displayed policy, and then click **OK**.

> ? **Note** For more information about the policies that authorize RAM roles and RAM users to access Message Queue for Apache Kafka , see RAM policies.

4. In the **Add Permissions** panel, check the authorization information and click **Complete**.

Step 3: Enterprise B creates a RAM user

Use the Alibaba Cloud account of Enterprise B to log on to the RAM console and create a RAM user.

1. Log on to the RAM console.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click **Create User**.
4. In the **User Account Information** section, enter a logon name in the **Logon Name** field and a display name in the **Display Name** field.

   > ? **Note**
   >
   > - The logon name can be up to 128 characters in length and can contain letters, digits, periods (.), underscores (_), and hyphens (-).
   > - The display name can be up to 24 characters in length.

5. (Optional)To create multiple RAM users, click **Add User** and repeat the previous step.
6. In the **Access Mode** section, select an access mode and click **OK**.

   > ? **Note** For security reasons, we recommend that you select only one access mode.

   - If you select **Console Access**, you must complete further settings, including the console password setting, whether to reset the password upon the next logon, and whether to enable multi-factor authentication.
   - If you select **Programmatic Access**, RAM automatically creates an AccessKey pair for the RAM user.

     > **Notice** For security reasons, the RAM console allows you to view or download the AccessKey secret only once. Therefore, when you create an AccessKey pair, you must keep your AccessKey secret strictly confidential.

7. In the **Verify by Phone Number** dialog box, click **Get Verification Code**, enter the verification code sent to your mobile phone, and then click **OK**.

Step 4: Enterprise B grants permissions to the RAM user

Attach the AliyunSTSAssumeRoleAccess permission policy to the RAM user.

1. In the left-side pane, choose **Identities > Users**.
2. On the **Users** page, find the RAM user and click **Add Permissions** in the **Actions** column.
3. In **Select Policy** section of the **Add Permissions** panel, click **System Policy**. Enter *AliyunSTSAssumeRoleAccess* in the search box, click the displayed policy to add it to the Selected list, and then

click **OK**.

4. In the **Add Permissions** panel, check the authorization information and click **Complete**.

What's next

The RAM user of Enterprise B can access the Message Queue for Apache Kafka resources of Enterprise A in the following ways:

- Use the Alibaba Cloud Management console

  i. Open the RAM Account Login page in your browser.

  ii. On the **RAM Account Login** page, enter the name of the RAM user, click **Next**, enter the password, and then click **Login**.

  > ? **Note** The logon name of the RAM user is in the format of *<$username>@<$AccountAlias>* or *<$username>@<$AccountAlias>.onaliyun.com*. *<$AccountAlias>* is the alias of the RAM user. If no alias is set, use the ID of the Alibaba Cloud account.

  iii. On the RAM user center page, move the pointer over the profile in the upper-right corner and click **Switch Identity**.

  iv. On the **Switch Role** page, enter the enterprise alias or default domain name of Enterprise A, and the RAM role name, and then click **Submit**.

  > ? **Note**
  >
  > ▪ To view the enterprise alias, use the Alibaba Cloud account of Enterprise A to log on to the Alibaba Cloud user center. Move the pointer over the profile picture in the upper-right corner and view the value on the floating layer.
  >
  > ▪ To view the default domain name, use the Alibaba Cloud account of Enterprise A to log on to the RAM console. On the **Settings** page, click the **Advanced** tab to view the default domain name.

- Call API operations

  i. Call the AssumeRole operation to obtain the AccessKey ID, AccessKey secret, and Security Token Service (STS) token. For more information, see AssumeRole.

  ii. Use the obtained AccessKey ID, AccessKey secret, and STS token to call a specific API operation to access the corresponding Message Queue for Apache Kafka resources.

5.Service-linked roles

This topic describes the background information, policies, and usage notes of service-linked roles in Message Queue for Apache Kafka and provides answers to frequently asked questions (FAQ) about these roles.

Context

An Alibaba Cloud service may need to access other Alibaba Cloud services to implement a feature that it has. In this case, the Alibaba Cloud service must assume a service-linked role to obtain the permissions to access other Alibaba Cloud services. A service-linked role is a Resource Access Management (RAM) role. When you use the feature in the console of the Alibaba Cloud service for the first time, the system automatically creates a service-linked role and notifies you that the service-linked role is created. For more information, see Service-linked roles.

Message Queue for Apache Kafka can assume the following service-linked roles:

- AliyunServiceRoleForAlikafka: Message Queue for Apache Kafka assumes this RAM role to access other Alibaba Cloud services. If you activate Message Queue for Apache Kafka for the first time in the Message Queue for Apache Kafka console, the system automatically creates the AliyunServiceRoleForAlikafka role and notifies you that the role is created.
- AliyunServiceRoleForAlikafkaConnector: Message Queue for Apache Kafka assumes this RAM role to obtain access permissions on the services to which connectors can connect. This way, Message Queue for Apache Kafka implements the connector feature. If you create a connector in the Message Queue for Apache Kafka console for the first time, the system automatically creates the AliyunServiceRoleForAlikafkaConnector role and notifies you that the role is created. For more information, see Create a Function Compute sink connector.
- AliyunServiceRoleForAlikafkaInstanceEncryption: Message Queue for Apache Kafka assumes this RAM role to obtain the access and encryption permissions of Key Management Service (KMS). This way, your instance can provide the encryption feature. The instance encryption feature can be used only by calling API operations. This feature will be provided in the console later. If you deploy an encrypted instance for the first time by calling the StartInstance operation provided in Message Queue for Apache Kafka , the system automatically creates the AliyunServiceRoleForAlikafkaInstanceEncryption role for you.

Policies

- The following policy is attached to the AliyunServiceRoleForAlikafka role:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "ecs:CreateNetworkInterface",
        "ecs:DeleteNetworkInterface",
        "ecs:DescribeNetworkInterfaces",
        "ecs:CreateNetworkInterfacePermission",
        "ecs:DescribeNetworkInterfacePermissions",
        "ecs:DeleteNetworkInterfacePermission",
        "ecs:CreateSecurityGroup",
        "ecs:AuthorizeSecurityGroup",
        "ecs:DescribeSecurityGroupAttribute",
        "ecs:RevokeSecurityGroup",
        "ecs:DeleteSecurityGroup",
        "ecs:DescribeSecurityGroups"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "vpc:DescribeVSwitches",
        "vpc:DescribeVpcs"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "alikafka.aliyuncs.com"
        }
      }
    }
  ]
}
```

- The following policy is attached to the AliyunServiceRoleForAlikafkaConnector role:

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fc:InvokeFunction",
        "fc:GetFunction",
        "fc:ListServices",
        "fc:ListFunctions",
        "fc:ListServiceVersions",
        "fc:ListAliases",
        "fc:CreateService",
        "fc:DeleteService",
        "fc:CreateFunction",
        "fc:DeleteFunction"
      ],
      "Resource": "*"
    },
    {
      "Action": [
        "rds:DescribeDatabases"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "oss:ListBuckets",
        "oss:GetBucketAcl"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "elasticsearch:DescribeInstance",
        "elasticsearch:ListInstance"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "dataworks:CreateRealTimeProcess",
        "dataworks:QueryRealTimeProcessStatus"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "connector.alikafka.aliyuncs.com"
        }
      }
    }
  ]
}
```

- The following policy is attached to the AliyunServiceRoleForAlikafkaInstanceEncryption role:

```
{
  "Version":"1",
  "Statement":[
    {
      "Action":[
        "kms:Listkeys",
        "kms:Listaliases",
        "kms:ListResourceTags",
        "kms:DescribeKey",
        "kms:TagResource",
        "kms:UntagResource"
      ],
      "Resource":"*",
      "Effect":"Allow"
    },
    {
      "Action":[
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource":"*",
      "Effect":"Allow",
      "Condition":{
        "StringEqualsIgnoreCase":{
          "kms:tag/acs:alikafka:instance-encryption":"true"
        }
      }
    },
    {
      "Action":"ram:DeleteServiceLinkedRole",
      "Resource":"*",
      "Effect":"Allow",
      "Condition":{
        "StringEquals":{
          "ram:ServiceName":"instanceencryption.alikafka.aliyuncs.com"
        }
      }
    }
  ]
}
```

Considerations

If you delete a service-linked role that is automatically created by the system, the dependent feature can no longer be used due to insufficient permissions. Exercise caution when you delete a service-linked role. For more information about how to create the service-linked role again and grant permissions to it, see Create a RAM role for a trusted Alibaba Cloud service and Grant permissions to a RAM role.

FAQ

- Why is the AliyunServiceRoleForAlikafka role for Message Queue for Apache Kafka not automatically created for my RAM user?

If the service-linked role is created for your Alibaba Cloud account, your RAM user inherits the service-linked role of your Alibaba Cloud account. If your RAM user fails to inherit the service-linked role, log on to the RAM console, create the following custom policy, and then attach the custom policy to the RAM user:

```
{
  "Statement": [
    {
      "Action": [
        "ram:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
       "StringEquals": {
        "ram:ServiceName": "alikafka.aliyuncs.com"
        }
      }
    }
  ],
  "Version": "1"
}
```

- Why is the AliyunServiceRoleForAlikafkaConnector role for Message Queue for Apache Kafka not automatically created for my RAM user?

  If the service-linked role is created for your Alibaba Cloud account, your RAM user inherits the service-linked role of your Alibaba Cloud account. If your RAM user fails to inherit the service-linked role, log on to the RAM console, create the following custom policy, and then attach the custom policy to the RAM user:

```
{
  "Statement": [
    {
      "Action": [
        "ram:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
       "StringEquals": {
        "ram:ServiceName": "connector.alikafka.aliyuncs.com"
        }
      }
    }
  ],
  "Version": "1"
}
```

- Why is the AliyunServiceRoleForAlikafkaInstanceEncryption role for Message Queue for Apache Kafka not automatically created for my RAM user?

If the service-linked role is created for your Alibaba Cloud account, your RAM user inherits the service-linked role of your Alibaba Cloud account. If your RAM user fails to inherit the service-linked role, log on to the RAM console, create the following custom policy, and then attach the custom policy to the RAM user:

```
{
  "Statement":[
    {
      "Action":[
        "ram:CreateServiceLinkedRole"
      ],
      "Resource":"*",
      "Effect":"Allow",
      "Condition":{
        "StringEquals":{
          "ram:ServiceName":"instanceencryption.alikafka.aliyuncs.com"
        }
      }
    }
  ],
  "Version":"1"
}
```

If the service-linked role is still not automatically created for your RAM user after you attach the policy to the RAM user, attach the AliyunKafkaFullAccess policy to the RAM user. For more information, see Grant permissions to a RAM user.

6.Authorize SASL users

The access control list (ACL) feature of Message Queue for Apache Kafka allows you to authorize Authentication and Security Layer (SASL) to send and subscribe to messages in Message Queue for Apache Kafka .

Prerequisites

Your Message Queue for Apache Kafka instance must meet the following conditions:

- The edition of the instance is Professional Edition.
- The instance is in the Running state.
- The major version of the instance is 2.2.0 or later. For more information about how to upgrade the major version, see Upgrade the open-source version of an instance.
- The minor version of the instance is the latest version. For more information about how to upgrade the minor version, see Upgrade the internal version of an instance.

> **Notice** The default SASL users of a public network/VPC instance have no permissions to perform operations. After the ACL feature is enabled, the default SASL users of a public network/VPC instance fail to send or subscribe to messages because these users have no required permissions. You must grant the default SASL users the read and write permissions to all topics and consumer groups of the instance.

Context

Enterprise A has purchased a Message Queue for Apache Kafka instance. The enterprise wants User A to consume only messages from all topics of the Message Queue for Apache Kafka instance, but not to send messages to the topics of the Message Queue for Apache Kafka instance.

Step 1: Enable the ACL feature

After you upgrade the minor version of an instance, enable ACL for the instance in the Message Queue for Apache Kafka console.

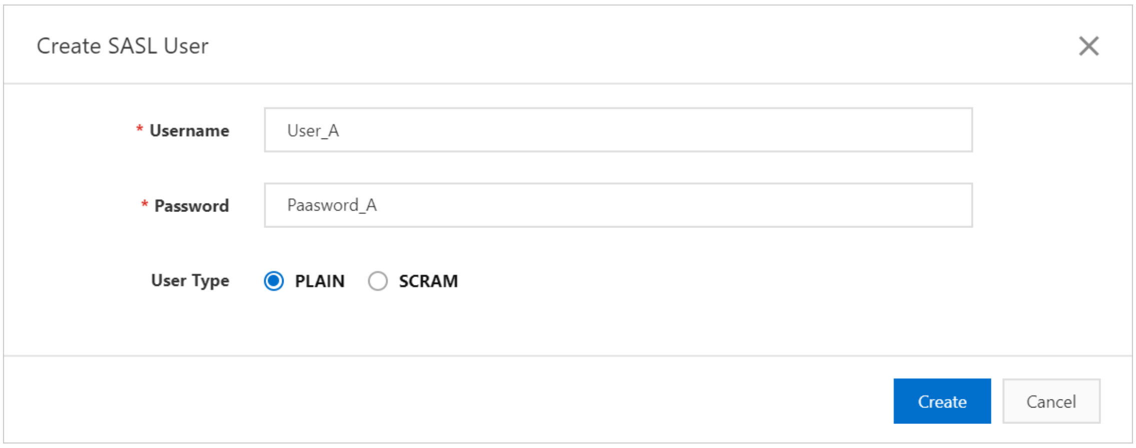
1. Log on to the Message Queue for Apache Kafka console.
2. In the top navigation bar, select the region where your instance is located.
3. In the left-side navigation pane, click **Instances**.
4. On the **Instance Details** page, select the instance and then click the **Instance Details** tab. On the right side of the **Basic Information** section, click **Enable ACL**.
5. In the **Note** dialog box, click **OK**, and then refresh the page.
   After you refresh the page, the SASL endpoint is displayed in the **Basic Information** section of the **Instance Details** page. The status changes to Upgrading.

   > **Notice** After the upgrade, the ACL feature is enabled for the instance. Then, you can create an SASL user and grant the user the required permissions. The SASL user can then access the instance by using the SASL endpoint. The upgrade takes 15 to 20 minutes.

Step 2: Create an SASL user

After you enabled the ACL feature for the instance, create an SASL user for User A.

1. On the **Instance Details** page of the Message Queue for Apache Kafka console, select the instance and click the **SASL Users** tab.
2. On the **SASL Users** tab, click **Create SASL User**.
3. In the **Create SASL User** dialog box, specify the parameters, and then click **OK**.



Create SASL User

* Username: User_A

* Password: Paasword_A

User Type: ● PLAIN ○ SCRAM

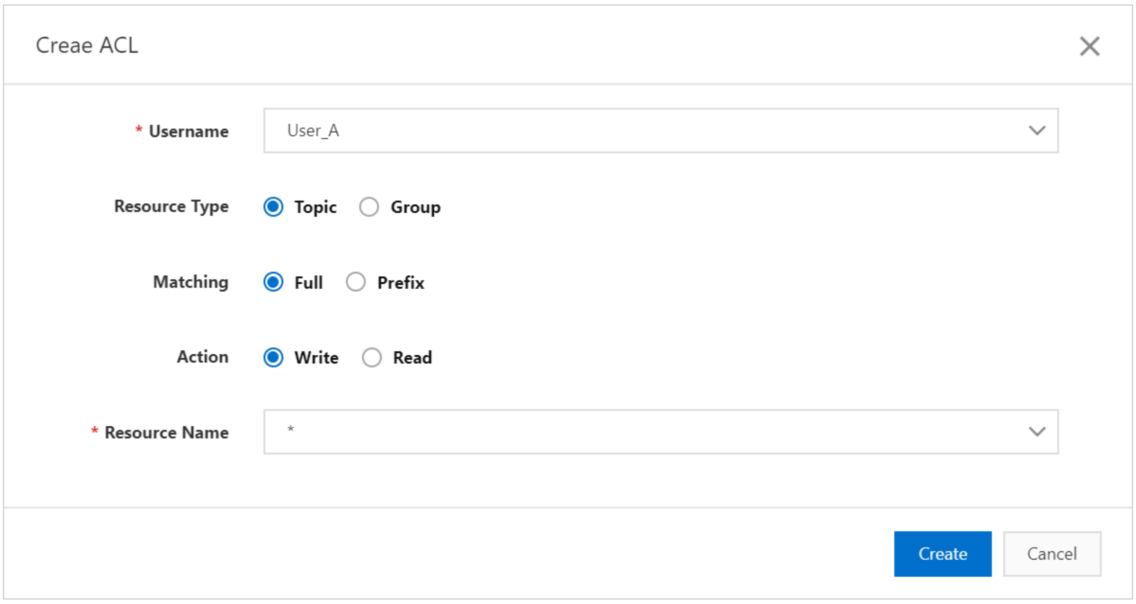
Parameter	Description
Username	The name of the SASL user.
Password	The password of the SASL user.
User Type	Message Queue for Apache Kafka supports the following SASL mechanisms: ○ PLAIN: a simple username and password verification mechanism. Message Queue for Apache Kafka provides an improved PLAIN mechanism that allows you to add SASL users without restarting the instance. ○ SCRAM: a username and password verification mechanism that provides more security than PLAIN. SCRAM-SHA-256 is used in Message Queue for Apache Kafka .

The SASL user that you created is displayed on the **SASL Users** tab.

Step 3: Grant permissions to the SASL user

After you create the SASL user for User A, grant the SASL user permissions to read messages from topics and consumer groups.

1. On the **Instance Details** page of the Message Queue for Apache Kafka console, select the instance with ACL enabled, and then click the **SASL Permissions** tab.
2. On the **SASL Permissions** tab, click **Create ACL**.
3. In the **Create ACL** dialog box, specify the parameters, and then click **OK**.



Creae ACL

* Username: User_A

Resource Type: ● Topic ○ Group

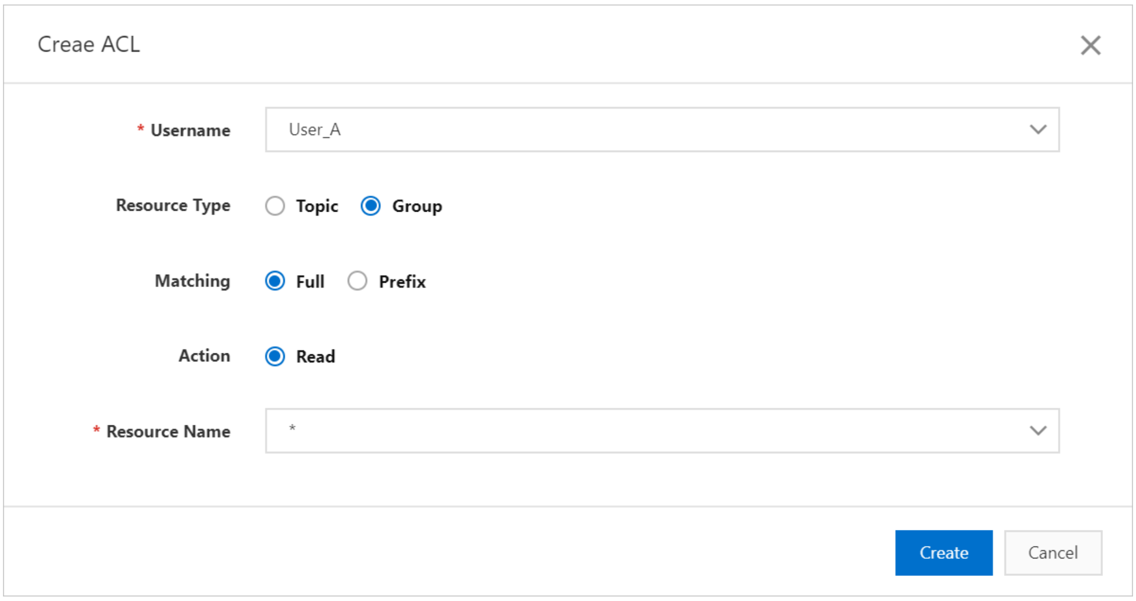
Matching: ● Full ○ Prefix

Action: ● Write ○ Read

* Resource Name: *

Parameter	Description
Username	The name of the SASL user. Message Queue for Apache Kafka supports asterisks (*). You can use an asterisk to represent all user names.
Resource Type	Message Queue for Apache Kafka allows you to grant permissions for the following resource types: - Topic: message topics. - Group: consumer groups.
Matching Mode	Message Queue for Apache Kafka supports the following matching modes: - LITERAL: matches resources by literal value. In this mode, only resources with the same name are matched. - PREFIXED: matches resources by prefix. In this mode, a resource name that starts with the specified prefix is matched.
Permission	Message Queue for Apache Kafka supports the following types of operations: - Write: writes data. - Read: reads data. **Notice** If you set the Resource Type parameter to Group, you must set the Permission parameter to Read.
Resource Name	The name of the resource. The value can be the name of a topic or consumer group. Message Queue for Apache Kafka supports asterisks (*). You can use an asterisk to represent all resource names.

4. On the **SASL Permissions** tab, click **Create ACL**.
5. In the **Create ACL** dialog box, specify the parameters, and then click **OK**.



Creae ACL

* Username: User_A

Resource Type: ○ Topic ● Group

Matching: ● Full ○ Prefix

Action: ● Read

* Resource Name: *

What to do next

After you grant the SASL user the required permissions, User A can connect to Message Queue for Apache Kafka by using the SASL endpoint and use the PLAIN mechanism to consume messages. For information about how to use the SDK, see Overview.