ALIBABA CLOUD

Alibaba Cloud

消息队列Kafka版

权限控制

文档版本：20210608

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.权限控制概述 05
2.RAM权限策略 06
3.RAM主子账号授权 09
4.RAM跨云账号授权 11
5.服务关联角色 14
6.SASL用户授权 20

1.权限控制概述

本文介绍消息队列Kafka版支持的两种权限控制服务类型：RAM和ACL。

权限控制服务	说明	文档
RAM	RAM是阿里云提供的管理阿里云用户身份与阿里云资源访问权限的服务。RAM只针对消息队列Kafka版控制台和API操作，客户端使用SDK收发消息与RAM无关。详情请参见什么是访问控制。	• RAM主子账号授权 • RAM跨云账号授权 • RAM权限策略 • 服务关联角色
ACL	ACL是消息队列Kafka版提供的管理SASL用户和客户端使用SDK收发消息权限的服务，和开源Apache Kafka保持一致。ACL只针对客户端使用SDK收发消息，与消息队列Kafka版控制台和API操作无关。详情请参见Authorization and ACLs。	SASL用户授权

2.RAM权限策略

消息队列Kafka版的控制台和API的权限管理通过访问控制RAM（Resource Access Management）实现。RAM可以让您避免与其他用户共享阿里云云账号密钥，即AccessKey（包含AccessKey ID和AccessKey Secret），按需为其他用户分配最小权限。

RAM权限策略

在RAM中，权限策略是用语法结构描述的一组权限的集合，可以精确地描述被授权的资源集、操作集以及授权条件。权限策略是描述权限集的一种简单语言规范，RAM支持的语言规范请参见权限策略语法和结构。

在RAM中，权限策略是一种资源实体。消息队列Kafka版支持以下两种类型的权限策略：

- 系统权限策略：统一由阿里云创建，您只能使用不能修改，策略的版本更新由阿里云维护，适用于粗粒度地控制RAM用户权限。
- 自定义权限策略：您可以自主创建、更新和删除，策略的版本更新由您自己维护，适用于细粒度地控制RAM用户权限。

系统权限策略

消息队列Kafka版支持以下系统权限策略。

权限策略名称	说明
AliyunKafkaFullAccess	消息队列Kafka版的管理权限，被授予该权限的RAM用户具有等同于阿里云账号的权限，即控制台和API的所有操作权限。
AliyunKafkaReadOnlyAccess	消息队列Kafka版的只读权限，被授予该权限的RAM用户只具有阿里云账号所有资源的只读权限，不具有控制台和API的操作权限。

系统权限策略示例

以系统权限策略AliyunKafkaFullAccess为例，被授予该权限的RAM用户具有等同于阿里云账号的权限，即控制台和API的所有操作权限。策略内容如下：

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

自定义权限策略

消息队列Kafka版支持以下自定义权限策略。

Action名称	权限说明	是否为只读类权限
ReadOnly	只读所有资源	是
ListInstance	查看实例	是
StartInstance	部署实例	否
UpdateInstance	更新实例配置	否
ReleaseInstance	释放实例	否
ListTopic	查看Topic	是
CreateTopic	创建Topic	否
UpdateTopic	更新Topic配置	否
DeleteTopic	删除Topic	否
ListGroup	查看ConsumerGroup	是
CreateGroup	创建ConsumerGroup	否
UpdateGroup	更新ConsumerGroup配置	否
DeleteGroup	删除ConsumerGroup	否
QueryMessage	查询消息	是
SendMessage	发送消息	否
DownloadMessage	下载消息	是
CreateDeployment	创建Connector任务	否
DeleteDeployment	删除Connector任务	否
ListDeployments	查看Connector任务	是
UpdateDeploymentRemark	修改Connector任务说明	否
GetDeploymentLog	获取Connector任务运行日志	是
EnableAcl	开启ACL	否
CreateAcl	创建ACL	否
DeleteAcl	删除ACL	否
ListAcl	查询ACL	是
CreateSaslUser	创建SASL用户	否

Action名称	权限说明	是否为只读类权限
DeleteSaslUser	删除SASL用户	否
ListSaslUser	查询SASL用户	是

自定义权限策略示例

以自己创建的自定义权限策略AliyunKafkaCustomAccess为例，被授予该权限策略的RAM用户只具有实例alikafka_post-cn-xxx的查看实例、查看Topic、查看Consumer Group、查询消息和下载消息的控制台和API的权限。策略内容如下：

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

3.RAM主子账号授权

借助访问控制RAM的RAM用户，您可以实现阿里云账号（主账号）和RAM用户（子账号）权限分割，按需为RAM用户赋予不同的权限，并避免因暴露阿里云账号密钥而造成安全风险。

背景信息

企业A开通了消息队列Kafka版服务，该企业需要员工操作消息队列Kafka版服务所涉及的资源，例如实例、Topic、Consumer Group。由于每个员工的工作职责不一样，需要的权限也不一样。企业A的需求如下：

- 出于安全或信任的考虑，不希望将云账号密钥直接透露给员工，而希望能给员工创建相应的用户账号。
- 用户账号只能在授权的前提下操作资源，不需要对用户账号进行独立的计量计费，所有开销都计入企业账号名下。
- 随时可以撤销用户账号的权限，也可以随时删除其创建的用户账号。

步骤一：创建RAM用户

使用企业A的阿里云账号登录RAM控制台并为员工创建RAM用户。

1. 登录RAM控制台。
2. 在左侧导航栏，选择**人员管理 > 用户**。
3. 在**用户**页面，单击**创建用户**。
4. 在**创建用户**页面的**用户账号信息**区域的**登录名称**，输入登录名称，在**显示名称**文本框，输入显示名称。

   > **说明**
   > - 登录名称允许英文字母、数字、英文句号（.）、下划线（_）和短划线（-），长度不超过128个字符。
   > - 显示名称长度不超过24个字符或汉字。

5. （可选）如需创建多个RAM用户，单击**添加用户**，重复上一步。
6. 在**访问方式**区域，选择访问方式，然后单击**确定**。

   > **说明** 为提高安全性，建议您只为RAM用户选择一种访问方式。

   - 如果选择**控制台访问**，则需完成进一步设置，包括控制台密码设置、登录时是否要求重置密码、是否开启多因素认证。
   - 如果选择**编程访问**，则RAM会自动为RAM用户创建AccessKey。

     > **注意** 出于安全考虑，RAM控制台只提供一次查看或下载AccessKey Secret的机会，即创建AccessKey时，因此请务必将AccessKey Secret记录到安全的地方。

7. 在**手机验证**对话框，单击**获取验证码**，输入收到的手机验证码，然后单击**确定**。

步骤二：为RAM用户添加权限

为不同员工的RAM用户授予不同的权限。

1. 在RAM控制台的左侧导航栏，单击**人员管理 > 用户**。

2. 在**用户**页面，找到需要授权的用户，在其右侧**操作**列，单击**添加权限**。
3. 在**添加权限**面板的**选择权限**区域，选择策略类型，通过关键字搜索需要添加的权限策略，并单击权限策略将其添加至右侧的已选择列表中，然后单击**确定**。

   > **说明** 支持授予的访问消息队列Kafka版的权限策略请参见RAM权限策略。

4. 在**添加权限**面板，查看授权信息，然后单击**完成**。

后续步骤

企业A的员工的RAM用户可以通过以下方式访问企业A的消息队列Kafka版。

- 控制台
  i. 在浏览器打开RAM用户登录入口。
  ii. 在**RAM用户登录**页面，输入RAM用户名称，单击**下一步**，输入RAM用户密码，然后单击**登录**。

  > **说明** RAM用户登录名称的格式为*<$username>@<$AccountAlias>*或*<$username>@<$AccountAlias>.onaliyun.com*。*<$AccountAlias>*为账号别名，如果没有设置账号别名，则默认值为阿里云账号的ID。

- API

  在代码中使用RAM用户的AccessKey ID和AccessKey Secret调用API访问消息队列Kafka版。

4.RAM跨云账号授权

借助访问控制RAM的RAM角色，您可以跨云账号授权，使某个企业访问另一个企业的消息队列Kafka版。

背景信息

企业A开通了消息队列Kafka版，该企业需要企业B代为操作消息队列Kafka版的资源，例如实例、Topic、Consumer Group。企业A的需求如下：

- 企业A希望能专注于业务系统，仅作为消息队列Kafka版所有者。企业A希望可以授权企业B来操作部分业务，例如：消息队列Kafka版的运维、监控以及管理等。
- 企业A希望当企业B的员工加入或离职时，无需做任何权限变更。企业B可以进一步将企业A的资源访问权限分配给企业B的RAM用户（员工或应用），并可以精细控制其员工或应用对资源的访问和操作权限。
- 企业A希望如果双方合同终止，企业A随时可以撤销企业B的授权。

步骤一：企业A创建RAM角色

使用企业A的阿里云账号登录RAM控制台为企业B的阿里云账号创建RAM角色。

1. 登录RAM控制台。
2. 在左侧导航栏，单击**RAM角色管理**。
3. 在**RAM角色管理**页面，单击**创建RAM角色**。
4. 在**创建RAM角色**面板，选择**阿里云账号**，单击**下一步**。
5. 在**角色名称**文本框，输入RAM角色名称，在**选择云账号**区域，选择**其他云账号**，输入企业B的阿里云账号的账号ID，然后单击**完成**。

> **说明**
> - RAM角色名称允许英文字母、数字和短划线（-），长度不超过64个字符。
> - 账号ID可以在**账号管理**控制台的**安全设置**页面查看。

步骤二：企业A为RAM角色添加权限

为RAM角色添加需要授予给企业B的访问消息队列Kafka版的权限。

1. 在RAM控制台的左侧导航栏，单击**RAM角色管理**。
2. 在**RAM角色管理**页面，找到创建的RAM角色，在其右侧**操作**列，单击**添加权限**。
3. 在**添加权限**面板的**选择权限**区域，选择策略类型，通过关键字搜索需要添加的权限策略，并单击权限策略将其添加至右侧的已选择列表中，然后单击**确定**。

> **说明** 支持授予的访问消息队列Kafka版的权限策略请参见RAM权限策略。

4. 在**添加权限**面板，查看授权信息，然后单击**完成**。

步骤三：企业B创建RAM用户

使用企业B的阿里云账号登录RAM控制台并创建RAM用户。

1. 登录RAM控制台。
2. 在左侧导航栏，选择**人员管理 > 用户**。

3. 在**用户**页面，单击**创建用户**。
4. 在**用户账号信息**区域的**登录名称**文本框，输入登录名称，在**显示名称**文本框，输入显示名称。

   > **说明**
   > - 登录名称允许英文字母、数字、英文句号（.）、下划线（_）和短划线（-），长度不超过128个字符。
   > - 显示名称长度不超过24个字符或汉字。

5. （可选）如需创建多个RAM用户，单击**添加用户**，重复上一步。
6. 在**访问方式**区域，选择访问方式，然后单击**确定**。

   > **说明** 为提高安全性，建议您只为RAM用户选择一种访问方式。

   - 如果选择**控制台访问**，则需完成进一步设置，包括控制台密码设置、登录时是否要求重置密码、是否开启多因素认证。
   - 如果选择**编程访问**，则RAM会自动为RAM用户创建AccessKey。

     > **注意** 出于安全考虑，RAM控制台只提供一次查看或下载AccessKey Secret的机会，即创建AccessKey时，因此请务必将AccessKey Secret记录到安全的地方。

7. 在**手机验证**对话框，单击**获取验证码**，输入收到的手机验证码，然后单击**确定**。

步骤四：企业B为RAM用户添加权限

为RAM用户添加AliyunSTSAssumeRoleAccess的权限。

1. 在RAM控制台的左侧导航栏，选择**人员管理 > 用户**。
2. 在**用户**页面，找到创建的RAM用户，在其右侧**操作**列，单击**添加权限**。
3. 在**添加权限**面板的**选择权限**区域，选择**系统策略**，输入*AliyunSTSAssumeRoleAccess*，单击该权限策略将其添加至右侧的已选择列表中，然后单击**确定**。
4. 在**添加权限**面板，查看授权信息，然后单击**完成**。

后续步骤

企业B的RAM用户可以通过以下方式访问企业A的消息队列Kafka版。

- 控制台
  i. 在浏览器打开RAM用户登录入口。
  ii. 在**RAM用户登录**页面，输入RAM用户名称，单击**下一步**，输入RAM用户密码，然后单击**登录**。

  > **说明** RAM用户登录名称的格式为*<$username>@<$AccountAlias>*或*<$username>@<$AccountAlias>.onaliyun.com*。*<$AccountAlias>*为账号别名，如果没有设置账号别名，则默认值为阿里云账号的ID。

  iii. 在RAM用户的用户中心页面，将鼠标指针移到右上角头像，在浮层单击**切换身份**。
  iv. 在**角色切换**页面，输入企业A的企业别名或默认域名，以及角色名，然后单击**提交**。

> **说明**
>
> - 企业别名：使用企业A的阿里云账号在阿里云账号用户中心，将鼠标指针移到右上角头像，在浮层查看。
> - 默认域名：使用企业A的阿里云账号在RAM控制台的**设置**页面，单击**高级设置**页签查看。

- API
  i. 调用AssumeRole接口获取AccessKey ID、AccessKey Secret和SecurityToken（临时安全令牌）。详情请参见AssumeRole。
  ii. 在代码中使用获取的AccessKey ID、AccessKey Secret和SecurityToken（临时安全令牌）调用API访问消息队列Kafka版。

5.服务关联角色

本文介绍消息队列Kafka版服务关联角色的背景信息、策略内容、注意事项和常见问题。

背景信息

服务关联角色是某个云服务在某些情况下，为了完成自身的某个功能，需要获取其他云服务的访问权限而提供的RAM角色。您在该云服务的控制台首次使用该功能时，系统会提示您完成服务关联角色的自动创建。更多服务关联角色相关信息，请参见服务关联角色。

消息队列Kafka版提供以下服务关联角色：

- AliyunServiceRoleForAlikafka：消息队列Kafka版访问您所拥有的其他阿里云资源的角色。如果您是在消息队列Kafka版控制台首次开通消息队列Kafka版服务，系统会提示您完成AliyunServiceRoleForAlikafka的自动创建。
- AliyunServiceRoleForAlikafkaConnector：消息队列Kafka版通过扮演该RAM角色，获取各类与Connector相关的产品的访问权限，以实现Connector的功能。如果您是在消息队列Kafka版控制台首次创建Connector，系统会提示您完成AliyunServiceRoleForAlikafkaConnector的自动创建。更多信息，请参见创建FC Sink Connector。
- AliyunServiceRoleForAlikafkaInstanceEncryption：消息队列Kafka版通过扮演该RAM角色，获取KMS的访问与加密权限，以实现您实例的加密功能。目前实例加密功能暂时只通过OpenAPI开放，控制台功能后续才会放出。如果您通过消息队列Kafka版OpenAPI StartInstance首次部署加密实例，系统会为您完成AliyunServiceRoleForAlikafkaInstanceEncryption的自动创建。

策略内容

- AliyunServiceRoleForAlikafka的权限策略如下：

```
{
  "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"
        }
      }
    }
  ]
}
```

- AliyunServiceRoleForAlikafkaConnector的权限策略如下：

```
{
  "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"
            }
          }
        }
      ]
    }
```

- AliyunServiceRoleForAlikafkaInstanceEncryption的权限策略如下：

```
{
  "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"
        }
      }
    }
  ]
}
```

注意事项

如果您删除了自动创建的服务关联角色，该服务关联角色相关的功能由于权限不足将无法再被使用，请谨慎操作。如需重新创建该服务关联角色并为其授权，请参见创建可信实体为阿里云服务的RAM角色和为RAM角色授权。

常见问题

- 为什么我的RAM用户无法自动创建消息队列Kafka版服务关联角色AliyunServiceRoleForAlikafka?

  如果您的阿里云账号已经创建了服务关联角色，您的RAM用户就会继承该阿里云账号的服务关联角色。如果没有继承，请登录访问控制控制台为RAM用户添加自定义权限策略，权限策略内容如下：

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

- 为什么我的RAM用户无法自动创建消息队列Kafka版服务关联角色AliyunServiceRoleForAlikafkaConnector?

  如果您的阿里云账号已经创建了服务关联角色，您的RAM用户就会继承该阿里云账号的服务关联角色。如果没有继承，请登录访问控制控制台为RAM用户添加自定义权限策略，权限策略内容如下：

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

- 为什么我的RAM用户无法自动创建消息队列Kafka版服务关联角色AliyunServiceRoleForAlikafkaInstanceEncryption?

  如果您的阿里云账号已经创建了服务关联角色，您的RAM用户就会继承该阿里云账号的服务关联角色。如果没有继承，请登录访问控制控制台为RAM用户添加自定义权限策略，权限策略内容如下：

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

如果您的RAM用户被授予该权限策略后，仍然无法自动创建服务关联角色，请为该RAM用户授予权限策略AliyunKafkaFullAccess。具体操作，请参见为RAM用户授权。

6.SASL用户授权

借助消息队列Kafka版的ACL，您可以按需为SASL用户赋予向消息队列Kafka版收发消息的权限，从而实现权限分割。

前提条件

您的消息队列Kafka版实例必须满足以下条件：

- 实例规格类型为专业版。
- 实例运行状态为**服务中**。
- 大版本为2.2.0版本及以上。如何升级实例大版本，请参见升级大版本。
- 小版本为最新版。如何升级实例小版本，请参见升级小版本。

> **注意** 公网/VPC实例的默认SASL用户是没有任何权限的。开启ACL后，公网/VPC实例的默认SASL用户会因为没有任何权限而收发消息失败。您需要为该SASL用户授予所有Topic和Consumer Group的读写权限。

背景信息

企业A购买了消息队列Kafka版，企业A希望用户A只能从消息队列Kafka版的所有Topic中消费消息，而不能向消息队列Kafka版的任何Topic生产消息。

步骤一：开启ACL

升级实例的小版本后，在消息队列Kafka版控制台为实例开启ACL。

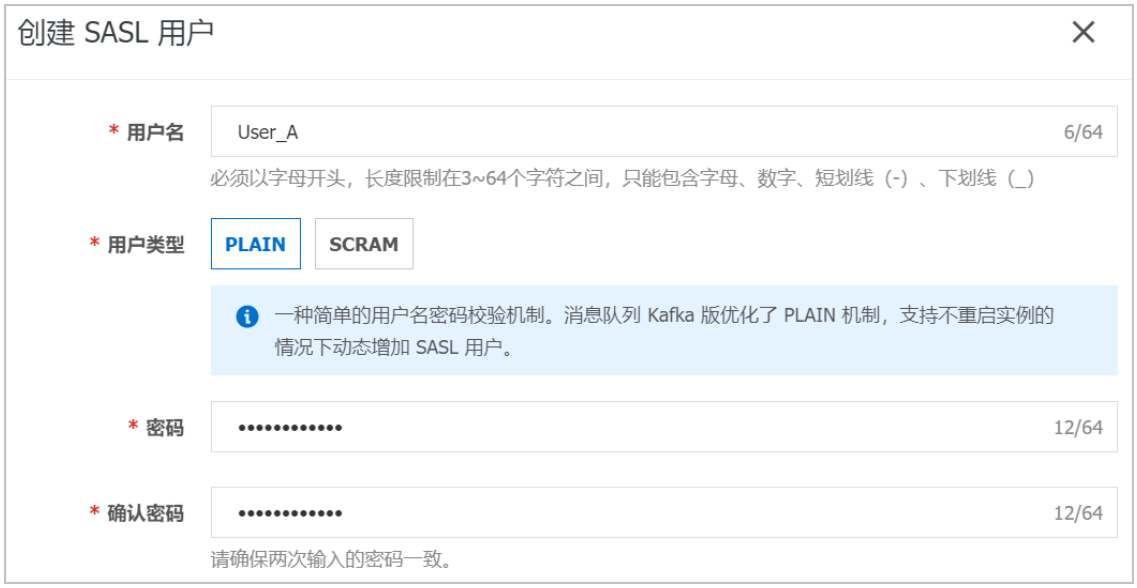
1. 登录消息队列Kafka版控制台。
2. 在**概览**页面的**资源分布**区域，选择地域。
3. 在**实例列表**页面，单击目标实例名称。
4. 在**实例详情**页面，单击**概览**区域右上角的**开启 ACL**。
5. 在**提示**对话框，单击**确认**，然后手动刷新页面。
   手动刷新页面后，**实例详情**页面的**基础信息**区域，运行**状态**显示**升级中**。待实例的**状态**显示**服务中**说明开启ACL任务完成。

   > **注意** 升级完成后，实例才会开启ACL。您才可以创建SASL用户并为其授权后，通过SASL接入点接入。升级预计需要15分钟~20分钟。

步骤二：创建SASL用户

实例开启ACL后，为用户A创建SASL用户。

1. 登录消息队列Kafka版控制台。
2. 在**概览**页面的**资源分布**区域，选择地域。
3. 在**实例列表**页面，选择已经开启ACL的实例。
4. 在**实例详情**页面，单击**SASL 用户管理**页签。
5. 在**SASL 用户管理**页签中，单击**创建 SASL 用户**。
6. 在**创建 SASL 用户**面板，设置SASL用户，然后单击**创建**。



参数	描述
用户名	SASL用户的名称。
用户类型	消息队列Kafka版支持的SASL机制如下： ○ **PLAIN**：一种简单的用户名密码校验机制。消息队列Kafka版优化了PLAIN机制，支持不重启实例的情况下动态增加SASL用户。 ○ **SCRAM**：一种用户名密码校验机制，安全性比PLAIN更高。消息队列Kafka版使用SCRAM-SHA-256。
密码	SASL用户的密码。
确认密码	确认SASL用户的密码。

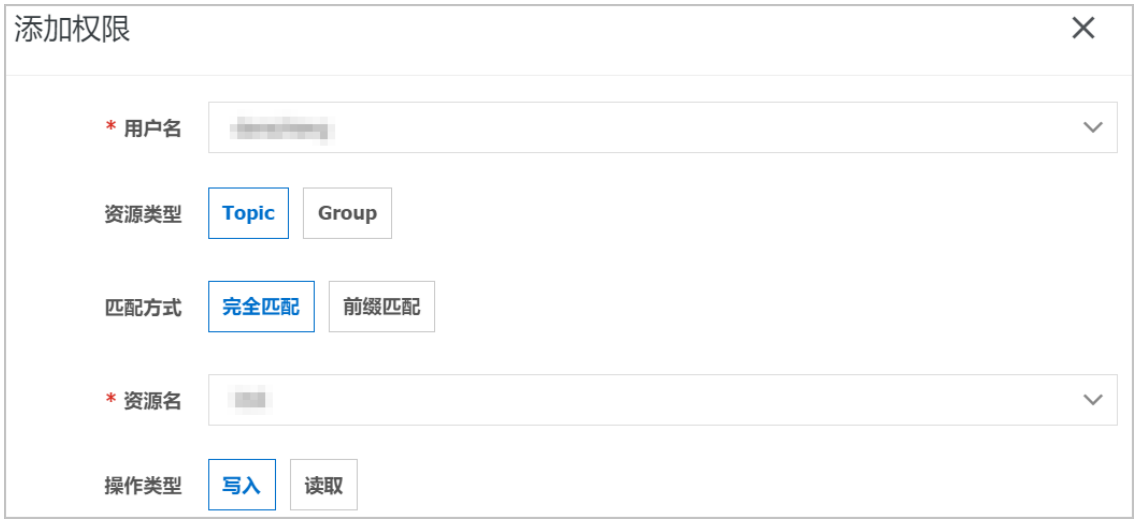
创建完成后，**SASL 用户管理**页签下方显示您创建的SASL用户。

- 如果您需要更改SASL用户的密码，单击其**操作**列的**修改密码**。在**修改SASL用户密码**面板，设置**新密码**并**确认新密码**。单击**确定**。
- 如果您需要删除SASL用户，单击其**操作**列的**删除**。

步骤三：授予SASL用户权限

为用户A创建SASL用户后，为该SASL用户授予从Topic和Consumer Group读取消息的权限。

1. 在**实例详情**页面，单击**SASL 权限管理**页签。
2. 在**SASL 权限管理**页签，单击**添加权限**。
3. 在**添加权限**面板，配置如下参数，然后单击**确定**。



参数	描述
用户名	SASL用户的名称。消息队列Kafka版支持通配符星号（*）表示所有用户名。
资源类型	消息队列Kafka版支持授权的资源类型如下： ○ Topic：消息主题。 ○ Group：消费组。
匹配方式	消息队列Kafka版支持的匹配模式如下： ○ **完全匹配**：按字面值匹配资源名称。全匹配模式只会匹配名称完全相同的资源。 ○ **前缀匹配**：按前缀匹配资源名称。前缀匹配模式会匹配以匹配名称开头的任意资源名称。
资源名	Topic或Consumer Group的名称。消息队列Kafka版支持通配符星号（*）表示所有资源名。
操作类型	消息队列Kafka版支持的操作类型如下： ○ **写入** ○ **读取** **注意** 资源类型Group仅支持操作类型**读取**。

配置完成之后，在**SASL 权限管理**页签，可设置**资源类型**、**匹配方式**、**资源名**与**用户名**，单击**查询**，查看已创建的用户权限。

相关操作

完成授权后，用户A可以通过SASL接入点接入消息队列Kafka版并使用PLAIN机制消费消息。如何使用SDK接入，请参见SDK概述。