ALIBABA CLOUD

阿里云

消息队列 MQ
访问控制（权限管理）

文档版本：20200908

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.RAM 主子账号授权

消息队列 RocketMQ 版

支持云账户（主账号）给 RAM 用户（子账号）授予 Topic 资源级别的权限，避免因暴露阿里云账号（主账号）密钥造成的安全风险。仅限有权限的 RAM 用户在

消息队列 RocketMQ 版

的控制台上管理资源，以及通过 SDK/API 发布与订阅消息。

应用场景

企业 A 购买了

消息队列 RocketMQ 版

服务，企业 A 的员工需要操作这些服务所涉及的资源，例如实例、Topic 或 Group 资源，有的员工负责创建资源，有的负责发布消息，还有的负责订阅消息。由于每个员工的工作职责不一样，需要的权限也不一样。

具体场景说明如下：

- 出于安全或信任的考虑，企业 A 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，不需要对用户账号单独计量计费，所有开销都计入企业 A 云账号名下。
- 企业 A 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。

此种场景下，A 的云账号可以将需要员工进行操作的资源进行细粒度的权限分隔。

操作步骤

1. 企业 A 云账号创建 RAM 用户。 具体步骤参见创建RAM用户。
2. （可选）企业 A 云账号可根据需求为刚创建的 RAM 用户创建自定义的策略。

   具体步骤参见创建自定义策略。

   目前，

   消息队列 RocketMQ 版

   支持实例、Topic 和 Group 粒度的权限设置。详情参见权限策略和示例。
3. 企业 A 云账号为 RAM 用户授权。 具体步骤参见为RAM用户授权。

后续步骤

使用阿里云账号（主账号）创建好 RAM 用户后，即可将 RAM 用户的登录名称及密码或者 AccessKey 信息分发给其他用户。其他用户可以按照以下步骤使用 RAM 用户登录控制台或调用 API。

- 登录控制台。
  i. 在浏览器中打开 RAM 用户登录入口 *https://signin.aliyun.com/login.htm*。
  ii. 在 **RAM 用户登录**页面上，输入 RAM 用户登录名称，单击**下一步**，并输入 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（主账号）的 ID。

iii. 在**子用户用户中心**页面上单击有权限的产品，即可访问控制台。

- 使用 RAM 用户的 AccessKey 调用 API。

  在代码中使用 RAM 用户的 AccessKeyId 和 AccessKeySecret 即可。

更多信息

- 跨云账号授权
- 权限策略概览
- 什么是RAM
- 基本概念
- 创建自定义策略
- 创建RAM用户
- 为RAM用户授权

2.跨云账号授权

使用企业 A 的阿里云账号（主账号）创建 RAM 角色并为该角色授权，并将该角色赋予企业 B，即可实现使用企业 B 的主账号或其 RAM 用户（子账号）访问企业 A 的阿里云资源的目的。

背景信息

企业 A 购买了

消息队列 RocketMQ 版

服务来开展业务，并希望将部分业务授权给企业 B。

需求说明：

- A 希望能专注于业务系统，仅作为资源 Owner；而消息发布和订阅等任务委托或授权给企业 B。
- 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 A 的资源访问权限分配给 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 随时可以撤销对企业 B 的授权。

操作步骤

1. 首先需要使用企业 A 的阿里云账号（主账号）登录 RAM 控制台并为企业 B 的云账号创建 RAM 角色。具体步骤参见创建可信实体为阿里云账号的RAM角色。
2. （可选）企业 A 为刚创建的 RAM 角色创建自定义策略。

   具体步骤参见创建自定义策略。

   目前，

   消息队列 RocketMQ 版

   支持实例、Topic 和 Group 粒度的权限设置。详情参见权限策略和示例。
3. 新创建的角色没有任何权限，因此企业 A 必须为该角色添加权限。可添加系统权限策略或自定义权限策略。 具体步骤参见为RAM角色授权。
4. 使用企业 B 的阿里云账号（主账号）登录 RAM 控制台并创建 RAM 用户。

   具体步骤参见为企业 B 创建 RAM 用户。
5. 企业 B 为 RAM 用户添加 AliyunSTSAssumeRoleAccess 权限。

   具体步骤参见为RAM用户授权。

   企业 B 必须为其主账号下的 RAM 用户添加 AliyunSTSAssumeRoleAccess 权限，RAM 用户才能扮演企业 A 创建的 RAM 角色。
6. 企业 B 的 RAM 用户通过控制台或 API 访问企业 A 的资源。 具体步骤参见后续步骤。

后续步骤

完成上述操作后，企业 B 的 RAM 用户即可按照以下步骤登录控制台访问企业 A 的云资源或调用 API。

- 登录控制台访问企业 A 的云资源
  i. 在浏览器中打开 RAM 用户登录入口 https://signin.aliyun.com/login.htm。
  ii. 在 **RAM 用户登录**页面上，输入 RAM 用户登录名称，单击**下一步**，并输入 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（主账号）的 ID。

iii. 在**子用户用户中心**页面上，将鼠标指针移到右上角头像，并在浮层中单击**切换身份**。

iv. 在**阿里云 - 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**切换**。

v. 对企业 A 的阿里云资源执行操作。

- 使用企业 B 的 RAM 用户通过 API 访问企业 A 的云资源

  要使用企业 B 的 RAM 用户通过 API 访问企业 A 的云资源，必须在代码中提供 RAM 用户的 AccessKeyId、AccessKeySecret 和 SecurityToken（临时安全令牌）。使用 STS 获取临时安全令牌的方法参见 AssumeRole。

STS 在消息队列 RocketMQ 版中的使用

> 注意 STS 功能只适用于
>
> 消息队列 RocketMQ 版
>
> 的 Java SDK 1.7.8.Final 及以上版本。

- 初始化

  消息队列 RocketMQ 版

  的客户端时，您只需将获取到的 AccessKeyId、AccessKeySecret 和 SecurityToken 填入到以下属性中即可：

```
Properties properties = new Properties();
// STS 的 AccessKeyId
properties.put(PropertyKeyConst.AccessKey,"STS.XXX");
// STS 的 AccessKeySecret
properties.put(PropertyKeyConst.SecretKey, "XXX");
// STS 的 SecurityToken
properties.put(PropertyKeyConst.SecurityToken, "XXX");
//其他属性
properties.put(PropertyKeyConst.NAMESRV_ADDR, "XXX");
......
Producer client = ONSFactory.createProducer(properties);
client.start();
```

- 当 SecurityToken 过期时，调用 updateCredential 方法动态更新。

```
Properties properties = new Properties();
// STS 的 AccessKeyId
properties.put(PropertyKeyConst.AccessKey,"STS.XXX");
// STS 的 AccessKeySecret
properties.put(PropertyKeyConst.SecretKey, "XXX");
// STS 的 SecurityToken
properties.put(PropertyKeyConst.SecurityToken, "XXX");
client.updateCredential(properties);
```

更多信息

- RAM 主子账号授权
- 权限策略概览
- 什么是RAM
- 基本概念
- 创建自定义策略
- 创建RAM用户
- 为RAM用户授权

3.服务关联角色

本文介绍

消息队列 RocketMQ 版

服务关联角色 AliyunServiceRoleForOns 的应用场景以及删除该角色的操作步骤。

背景信息

消息队列 RocketMQ 版

服务关联角色 AliyunServiceRoleForOns 是

消息队列 RocketMQ 版

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。更多关于服务关联角色的信息请参见服务关联角色。

应用场景

消息队列 RocketMQ 版

需要通过自动创建的

消息队列 RocketMQ 版

服务关联角色 AliyunServiceRoleForOns 获取访问云监控的权限，以实现监控报警相关功能。

AliyunServiceRoleForOns 权限说明

AliyunServiceRoleForOns 具备的访问权限如下：

```
{
 "Version": "1",
 "Statement": [
  {
   "Action": [
    "cms:DescribeMetricRuleList",
    "cms:DescribeMetricList",
    "cms:DescribeMetricData"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "ram:DeleteServiceLinkedRole",
   "Resource": "*",
   "Effect": "Allow",
   "Condition": {
    "StringEquals": {
     "ram:ServiceName": "ons.aliyuncs.com"
    }
   }
  }
 ]
}
```

删除 AliyunServiceRoleForOns 角色

删除 AliyunServiceRoleForOns 角色后，将无法再继续使用云监控相关功能，请谨慎操作。如需再次使用云监控相关功能，则需重新创建该角色。创建步骤请参见创建服务关联角色。

删除服务关联角色的具体操作请参见删除服务关联角色。

常见问题

为什么我的 RAM 用户无法自动创建

消息队列 RocketMQ 版

服务关联角色 AliyunServiceRoleForOns？

如果主账号已经创建了服务关联角色，RAM 用户就会继承该主账号的服务关联角色。如果没有继承，请登录 RAM 控制台为其添加以下权限策略。

```
{
  "Statement": [
    {
      "Action": [
        "ram:CreateServiceLinkedRole"
      ],
      "Resource": "acs:ram:*:主账号 ID:role/*",
      "Effect": "Allow",
      "Condition": {
       "StringEquals": {
        "ram:ServiceName": "ons.aliyuncs.com"
        }
      }
    }
  ],
  "Version": "1"
}
```

> **说明** 请将 主账号 ID 替换为您实际的阿里云账号（主账号）ID。

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 AliyunServiceRoleForOns，请为该 RAM 用户授予以下任一权限策略：

- AliyunMQFullAccess
- AliyunMQPubOnlyAccess
- AliyunMQSubOnlyAccess

以上权限策略的详细说明请参见系统策略。

4.权限策略和示例

消息队列 RocketMQ 版

的权限管理是通过阿里云的访问控制 RAM（Resource Access Management）产品实现的。使用 RAM 可以让您避免与其他用户共享云账号密钥，即 AccessKey（包含 AccessKey ID 和 AccessKey Secret），按需为用户分配最小权限。本文介绍

消息队列 RocketMQ 版

在 RAM 中的权限策略和示例。

背景信息

在 RAM 中，权限策略是用权限策略语法和结构描述的一组权限的集合，可以精确地描述被授权的 Resource（资源集）、Action（操作集）以及授权条件。详情请参见权限策略语法和结构。

消息队列 RocketMQ 版

有以下两类 RAM 的权限策略：

- 系统策略。
- 自定义策略。

  您需到 RAM 控制台编辑相应权限策略，再添加至相应用户。您可以自主创建、更新和删除权限策略，策略的版本更新由您自己维护。具体的权限策略示例，请参见下文中的权限策略示例。

系统策略

消息队列 RocketMQ 版

目前提供以下 4 种系统默认的权限策略。

权限策略名称	说明
AliyunMQFullAccess	管理 消息队列 RocketMQ 版 的权限，等同于主账号的权限，被授予该权限的 RAM 用户具有所有消息收发权限且有控制台所有功能操作权限。
AliyunMQPubOnlyAccess	消息队列 RocketMQ 版 的发布权限，被授予该权限的 RAM 用户具有使用主账号所有资源通过 SDK 发送消息的权限。
AliyunMQSubOnlyAccess	消息队列 RocketMQ 版 的订阅权限，被授予该权限的 RAM 用户具有使用主账号所有资源通过 SDK 订阅消息的权限。
AliyunMQReadOnlyAccess	消息队列 RocketMQ 版 的只读权限，被授予该权限的 RAM 用户仅有通过访问控制台或调用管控 API 读取资源信息的权限。

自定义策略

自定义权限策略（Policy）可以满足您更细粒度的授权需求。

在

消息队列 RocketMQ 版

中，实例、Topic 和 Group 各为一种 Resource，对这些 Resource 授予的权限即为 Action。Topic 和 Group 的 Resource 命名格式因实例是否有命名空间而异。您可在

消息队列 RocketMQ 版

控制台的实例详情页面查看实例是否有命名空间。

消息队列 RocketMQ 版

的 Resource 和 Action 的可选值和对应规则如下。

> 说明 {instanceId}、{topic} 和 {groupId} 均需替换为您实际的资源信息。例如，{groupId} 替换为 GID_xxx。

Resource	命名格式		Action		备注
	有命名空间	无命名空间	Action 名称	说明	
实例	acs:mq:*:*:{instanceId} 示例：acs:mq:*:*:MQ_INST_13801 5630679****_B cZwWZ9k	acs:mq:*:*:{instanceId} 示例：acs:mq:*:*:MQ_INST_13801 5630679****_B cZwWZ9k	mq:QueryInst anceBaseInfo	查询实例基本信息	授予某 RAM 用户 Topic 和 Group 的相关权限前，需授予该用户 Topic 和 Group 所在实例的 mq:QueryInst anceBaseInfo 权限。
			mq:UpdateInt ance	更新实例	无
			mq:CreateIns tance	创建实例	无
			mq:DeleteInt ance	删除实例（慎用）	无

Resource	命名格式		Action		备注
	有命名空间	无命名空间	Action 名称	说明	
Topic	acs:mq:*:*:{instanceId}%{topic} 示例：acs:mq:*:*:MQ_INST_13801 5630679****_BcZwWZ9k%Topic-test	acs:mq:*:*:{topic} 示例：acs:mq:*:*:Topic-test	mq:PUB	消息发布	授予某 RAM 用户 Topic 的相关权限前，需授予该用户 Topic 所在实例的 mq:QueryInstanceBaseInfo 权限。
			mq:SUB	消息订阅	
			mq:CreateTopic	创建 Topic	
			mq:DeleteTopic	删除 Topic	
			mq:UpdateTopicInfo	更新 Topic 备注	
Group	acs:mq:*:*:{instanceId}%{groupId} 示例：acs:mq:*:*:MQ_INST_13801 5630679****_BcZwWZ9k%GID_test	acs:mq:*:*:{groupId} 示例：acs:mq:*:*:GID_test	mq:SUB	消息订阅	授予某 RAM 用户 Group 的相关权限前，需授予该用户 Group 所在实例的 mq:QueryInstanceBaseInfo 权限。
			mq:CreateGroup	创建 Group ID	
			mq:DeleteGroup	删除 Group ID	

权限策略示例

> **说明** 如需直接复制示例代码，使用时请删除注释内容，即 “//” 及以后的文字说明。

- **示例一：授予实例中某 Topic 和 Group 的权限**
  - **适用于有命名空间的实例**

```
{
  "Version":"1",
  "Statement":[
    {  // 授予实例的权限，授予 Topic 和 Group 的权限前请先授予相应实例的权限（适用于有命名空间的实例）。
      "Effect":"Allow",
      "Action":[
        "mq:QueryInstanceBaseInfo"
      ],
      "Resource":[
        "acs:mq:*:*:{instanceId}"
      ]
    },
    {  // 授予 Topic 的消息发布和订阅权限。
      "Effect":"Allow",
      "Action":[
        "mq:PUB",
        "mq:SUB"
      ],
      "Resource":[
        "acs:mq:*:*:{instanceId}%{topic}"
      ]
    },
    {  // 授予 Group 的权限。
      "Effect":"Allow",
      "Action":[
        "mq:SUB"
      ],
      "Resource":[
        "acs:mq:*:*:{instanceId}%{groupId}"
      ]
    }
  ]
}
```

- 适用于**无命名空间**的实例

```
{
  "Version":"1",
  "Statement":[
    {  // 授予实例的权限，授予 Topic 和 Group 的权限前请先授予相应实例的权限（适用于无命名空间的实例）。
      "Effect":"Allow",
      "Action":[
        "mq:QueryInstanceBaseInfo"
      ],
      "Resource":[
        "acs:mq:*:*:{instanceId}"
      ]
    },
    {  // 授予 Topic 的消息发布和订阅权限。
      "Effect":"Allow",
      "Action":[
        "mq:PUB",
        "mq:SUB"
      ],
      "Resource":[
        "acs:mq:*:*:{topic}"
      ]
    },
    {  // 授予 Group 的权限。
      "Effect":"Allow",
      "Action":[
        "mq:SUB"
      ],
      "Resource":[
        "acs:mq:*:*:{groupId}"
      ]
    }
  ]
}
```

- 示例二：授权整个实例的权限（只适用于有命名空间的实例）

  若要授予整个实例的权限，即该实例中所有资源的所有操作权限，请按以下示例设置。

```
{  // 仅适用于有命名空间的实例。
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mq:*"
      ],
      "Resource": [
        "acs:mq:*:*:{instanceId}*" // 授予该实例的权限，{instanceId} 用实例 ID 代替。
      ]
    }
  ]
}
```

后续步骤

- 创建自定义策略
- 创建 RAM 用户
- 为 RAM 用户授权
- 通过 RAM 限制用户访问的 IP 地址