

Alibaba Cloud

消息服务MNS

访问控制（权限管理）

文档版本：20210823

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 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.为RAM用户授权	05
2.授权策略和示例	07
3.创建RAM用户	11
4.FAQ	12
4.1. 如何保证我的消息队列中的消息是安全的？	12
4.2. 如何确保在MNS中存储的数据的可靠性？	12

1. 为RAM用户授权

消息服务MNS支持阿里云账号（主账号）给RAM用户（子账号）授予资源级别的权限，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用户在消息服务MNS的控制台上管理资源，以及SDK/API发布与订阅消息。

应用场景

企业A购买了消息服务MNS服务，企业A的员工需要操作这些服务所涉及的资源，例如队列、主题等资源。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，请参见[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，请参见[创建自定义策略](#)。

目前，消息服务MNS支持资源粒度的权限设置。更多信息，请参见[自定义策略](#)。

3. 企业A账号为RAM用户授权。

具体步骤，请参见[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API。

- 登录控制台。
 - i. 在浏览器中打开[RAM用户登录入口](#)。
 - 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. 在阿里云控制台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AccessKey ID和AccessKey Secret即可。

相关文档

- 什么是访问控制
- 授权策略和示例

2. 授权策略和示例

消息服务MNS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。本文介绍消息服务MNS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。更多信息，请参见[权限策略语法和结构](#)。

消息服务MNS支持的RAM的权限策略有以下类型：

- 系统策略**
系统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。
- 自定义策略**
自定义策略可由您自主创建、更新和删除，策略的版本更新由您自己维护。您需到[RAM控制台](#)编辑相应权限策略，再给相应用户授予该权限。

系统策略

消息服务MNS提供以下系统默认的权限策略。

权限策略名称	说明
AliyunMNSFullAccess	消息服务MNS的管理权限，等同于阿里云账号的权限，被授予该权限的RAM用户具有所有消息收发权限和控制台所有功能操作权限。
AliyunMNSReadOnlyAccess	消息服务MNS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API读取资源信息的权限。

自定义策略

自定义策略可以满足您更细粒度的授权需求。消息服务MNS提供以下自定义策略。

API	Action	Resource
OpenService	mns:OpenService	acs:mns:\$region:\$accountid:/commonbuy/openservice
ListQueue	mns:ListQueue	acs:mns:\$region:\$accountid:/queues
CreateQueue	mns>CreateQueue	acs:mns:\$region:\$accountid:/queues/\$queueName
DeleteQueue	mns>DeleteQueue	acs:mns:\$region:\$accountid:/queues/\$queueName
SetQueueAttributes	mns:SetQueueAttributes	acs:mns:\$region:\$accountid:/queues/\$queueName

API	Action	Resource
GetQueueAttributes	mns:GetQueueAttributes	acs:mns:\$region:\$accountId:/queues/\$queueName
SendMessage或BatchSendMessage	mns:SendMessage	acs:mns:\$region:\$accountId:/queues/\$queueName/messages
ReceiveMessage或BatchReceiveMessage	mns:ReceiveMessage	acs:mns:\$region:\$accountId:/queues/\$queueName/messages
DeleteMessage	mns>DeleteMessage	acs:mns:\$region:\$accountId:/queues/\$queueName/messages
PeekMessage或BatchPeekMessage	mns:PeekMessage	acs:mns:\$region:\$accountId:/queues/\$queueName/messages
ChangeMessageVisibility	mns:ChangeMessageVisibility	acs:mns:\$region:\$accountId:/queues/\$queueName/messages
ListTopic	mns:ListTopic	acs:mns:\$region:\$accountId:/topics
CreateTopic	mns>CreateTopic	acs:mns:\$region:\$accountId:/topics/\$topicName
DeleteTopic	mns>DeleteTopic	acs:mns:\$region:\$accountId:/topics/\$topicName
SetTopicAttributes	mns:SetTopicAttributes	acs:mns:\$region:\$accountId:/topics/\$topicName
GetTopicAttributes	mns:GetTopicAttributes	acs:mns:\$region:\$accountId:/topics/\$topicName
ListSubscriptionByTopic	mns:ListSubscriptionByTopic	acs:mns:\$region:\$accountId:/topics/\$topicName/subscriptions
Subscribe	mns:Subscribe	acs:mns:\$region:\$accountId:/topics/\$topicName/subscriptions/\$subscriptionName
Unsubscribe	mns:Unsubscribe	acs:mns:\$region:\$accountId:/topics/\$topicName/subscriptions/\$subscriptionName
SetSubscriptionAttributes	mns:SetSubscriptionAttributes	acs:mns:\$region:\$accountId:/topics/\$topicName/subscriptions/\$subscriptionName
GetSubscriptionAttributes	mns:GetSubscriptionAttributes	acs:mns:\$region:\$accountId:/topics/\$topicName/subscriptions/\$subscriptionName

API	Action	Resource
PublishMessage	mns:PublishMessage	acs:mns:\$region:\$accountid:/topics/\$topicName/messages

自定义策略示例

- 示例一：在Allow授权中增加IP限制

允许通过 42.120.88.0/24, 42.120.66.0/24 两个IP段访问消息服务MNS。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "mns:*",
      "Effect": "Allow",
      "Resource": "acs:mns:*:*:*",
      "Condition": {
        "IpAddress": {
          "acs:SourceIp": ["42.120.88.0/24", "42.120.66.0/24"]
        }
      }
    }
  ]
}
```

- 示例二：在Deny授权中增加IP限制

如果源IP不在 42.120.88.0/24 中，则禁止对消息服务MNS执行任何操作。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "mns:*",
      "Effect": "Deny",
      "Resource": "acs:mns:*:*:*",
      "Condition": {
        "NotIpAddress": {
          "acs:SourceIp": [
            "42.120.88.0/24"
          ]
        }
      }
    }
  ]
}
```



注意 因为Policy的鉴权规则是Deny优先（即如果您的访问操作命中任意一条Deny规则，则禁止访问），所以访问者从 42.120.88.0/24 以外的IP地址访问时，消息服务MNS会通知没有权限。

- 示例三：授予RAM用户队列、主题的可读权限

授予查看队列、主题、队列属性和主题属性的权限，请按以下示例设置。

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mns:ListQueue",
        "mns:ListTopic",
        "mns:GetQueueAttributes",
        "mns:GetTopicAttributes"
      ],
      "Resource": "acs:mns:*:*:*"
    }
  ]
}
```

3. 创建RAM用户

本文介绍在RAM控制台上创建RAM用户（子账号）的具体步骤和后续用户组管理。

操作步骤

1. 登录[RAM控制台](#)。
2. 在左侧导航栏，单击[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，输入登录名称和显示名称。

 **说明** 单击[添加用户](#)，可一次性创建多个RAM用户。

5. 在访问方式区域下，选择访问方式，然后单击[确定](#)。
 - **控制台密码登录**：完成对登录安全的基本设置，包括自动生成或自定义登录密码、是否要求下次登录时重置密码以及是否要求开启多因素认证。

 **说明** 自定义登录密码时，密码必须满足您在[人员管理](#) > [设置](#)中设置的密码复杂度规则。关于如何设置密码复杂度规则，详情请参见[设置RAM用户密码强度](#)。

- **编程访问**：自动为RAM用户生成访问密钥（AccessKey），支持通过API或其他开发工具访问阿里云。

 **说明** 为了保障账号安全，建议仅为RAM用户选择一种登录方式，避免RAM用户离开组织后仍可以通过访问密钥访问阿里云资源。

后续步骤

RAM用户创建成功后，您可以：

- 使用RAM用户登录控制台。详情请参见[RAM用户登录控制台](#)。
- 为用户添加到一个或多个组，对RAM用户进行分类并授权。详情请参见[为用户组添加RAM用户](#)。
- 为用户添加一个或多个权限策略，使RAM用户具有资源的访问能力。详情请参见[为RAM用户授权](#)。

4.FAQ

4.1. 如何保证我的消息队列中的消息是安全的？

本文介绍阿里云如何保证消息队列中的消息是安全的。

消息服务MNS提供了安全可靠的身份验证机制，确保您的队列受到保护，防止遭到未经授权的访问。只有阿里云账户拥有者才能访问其创建的队列。

4.2. 如何确保在MNS中存储的数据的可靠性？

本文介绍阿里云如何确保消息服务MNS中数据可靠性。

消息服务MNS将所有队列和消息存储在阿里云高可靠、高可用的数据中心组成的网络中。所有消息冗余地存储在多台服务器上，当某台服务器出现问题时，冗余数据将会被自动拷贝至其他服务器；这意味着单台服务器不可用或网络故障都不会对队列中消息的可靠性造成任何影响。