阿里云
日志服务

访问控制RAM

文档版本：20190920

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
	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。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	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。	`swich` *{stand | slave}*

目录

1 简介

RAM (Resource Access Management) 是阿里云为客户提供的 用户身份管理 与 资源访问控制服务。使用 RAM，您可以创建、管理用户账号（比如员工、系统或应用程序），并可以控制这些用户账号对您名下资源具有的操作权限。当您的企业存在多用户协同操作资源时，使用 RAM 可以让您避免与其他用户共享云账号密钥，按需为用户分配最小权限，从而降低您的企业信息安全风险。

为了更精细地管理和操作日志服务资源，您可以通过阿里云RAM产品为您名下的子账号、日志服务的RAM服务角色和用户角色赋予相应的访问权限。

身份管理

您可以通过RAM进行用户身份管理。例如在您的账号下创建并管理用户账号/用户组、创建服务角色以代表日志服务、创建用户角色以进行跨账号的资源操作与授权管理。

日志服务支持收集API网关、SLB等云产品的日志数据，您需要在配置前通过快速授权页完成服务角色的创建与授权。

角色	默认权限	说明
AliyunLogArchiveRole	AliyunLogArchiveRolePolicy	日志服务默认使用此角色访问您的SLB云产品日志，默认授权策略用于导出SLB服务日志。快速授权请单击快速授权页
AliyunLogDefaultRole	AliyunLogRolePolicy	用于日志服务默认角色的授权策略，包含OSS的写入权限。快速授权请单击快速授权页。
AliyunLogETLRole	AliyunLogETLRolePolicy	用于日志服务ETL功能角色的授权策略，日志服务默认使用此角色来访问您在其他云产品中的资源。快速授权请单击快速授权页。
AliyunMNSLoggingRole	AliyunMNSLoggingRolePolicy	日志服务默认使用此角色访问您的MNS云产品日志，默认授权策略用于导出MNS服务日志，包含OSS的写入权限。快速授权请单击快速授权页。

资源访问控制

您可以为名下的用户账号/用户组以及角色授予对应的授权策略。

您也可以创建自定义授权策略，或者以自定义授权策略和系统授权策略为模板，参考#unique_4编辑更细粒度的授权策略。

日志服务支持以下系统授权策略。

授权策略	类型	说明
AliyunLogFullAccess	系统策略	日志服务的全部管理权限。
AliyunLogReadOnlyAccess	系统策略	只读访问日志服务的权限。

应用场景

授权RAM子用户访问日志服务

在实际的应用场景中，主账号可能需要将日志服务的运营维护工作交予其名下的RAM子用户，由RAM子用户对日志服务进行日常维护工作；或者主账号名下的RAM子用户可能有访问日志服务资源的需求。此时，主账号需要对其名下的RAM子用户进行授权，授予其访问或者操作日志服务的权限。出于安全性的考虑，日志服务建议您将RAM子用户的权限设置为需求范围内的最小权限。

配置详情请参考#unique_5。

授权服务角色读日志

日志服务目前提供基于用户日志内容报警功能，为了读取日志数据，需要用户显式授权日志服务服务账号访问用户数据。

配置详情请参考#unique_6。

授权用户角色操作日志服务

RAM 用户角色是一种虚拟用户，它没有确定的身份认证密钥，且需要被一个受信的实体用户（比如云账号、RAM-User 账号、云服务账号）扮演才能正常使用。扮演成功后实体用户将获得 RAM 用户角色的临时安全令牌，使用这个临时安全令牌就能以RAM用户角色身份访问被授权的资源。

- 将日志服务的操作权限授予一个受信实体用户，允许该实体用户下的RAM角色操作日志服务。配置详情请参考#unique_6。
- 授权移动应用客户端通过直连方式访问日志服务，将APP的日志直接上传到日志服务中。配置详情请参考#unique_7。

2 授权RAM用户

为RAM用户授权后，用户可以访问日志服务。本文为您介绍如何为RAM用户授权。

背景信息

在实际的应用场景中，主账号可能需要将日志服务的运营维护工作交予其名下的RAM用户，由RAM用户对日志服务进行日常维护工作；或者主账号名下的RAM用户可能有访问日志服务资源的需求。此时，主账号需要对其名下的RAM用户进行授权，授予其访问或者操作日志服务的权限。出于安全性的考虑，日志服务建议您将RAM用户的权限设置为需求范围内的最小权限。

主账号授权RAM用户访问日志服务资源，需要按照以下步骤完成。关于RAM用户的详细信息，请参考#unique_9。

创建RAM用户

1. 云账号登录RAM控制台。
2. 在左侧导航栏的人员管理菜单下，单击用户。
3. 单击新建用户。

   说明:
   单击添加用户，可一次性创建多个RAM用户。
4. 输入登录名称和显示名称。
5. 在访问方式区域下，选择控制台密码登录或编程访问。
   - 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。
   - 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。
6. 单击确认。

授权RAM用户

日志服务提供两种系统授权策略，即`AliyunLogFullAccess`和`AliyunLogReadOnlyAccess`，分别表示管理权限和只读权限。您还可以在RAM控制台自定义授权策略，创建方法参考创建自定

义授权策略，权限策略示例请参考RAM自定义授权场景和日志服务RAM授权策略。本文档以赋予用户AliyunLogReadOnlyAccess权限为例。

1. 在左侧导航栏的权限管理菜单下，单击授权。
2. 单击新增授权。
3. 在被授权主体区域下，输入RAM用户名称后，单击需要授权的RAM用户。
4. 在左侧权限策略名称列中选择 AliyunLogReadOnlyAccess，并单击确认。
5. 单击确定。
6. 单击完成。

RAM登录控制台

完成创建用户和用户授权之后，用户就有权限访问日志服务控制台了。您可以通过以下两种方式以RAM用户身份登录控制台。

- 在访问控制服务控制台概览页面，单击用户登录地址链接，使用已创建的RAM用户用户名和密码登录。

- 直接访问RAM用户通用登录页面，使用已创建的RAM用户用户名和密码登录。
  - 方式一：<$username>@<$AccountAlias>.onaliyun.com 。例如：username@company-alias.onaliyun.com。

    说明：
    ，RAM 用户登录账号为 UPN（User Principal Name）格式，即 RAM 控制台用户列表中所见的用户登录名称此时。<$username>为 RAM 用户名称，<$AccountAlias>.onaliyun.com 为默认域名。
  - 方式二：<$username>@<$AccountAlias>。例如：username@company-alias。

    说明：
    <$username>为 RAM 用户名称，<$AccountAlias> 为账号别名。

3 授权用户角色

如果您需要将日志服务的操作权限授予一个受信实体用户，允许该实体用户下的RAM角色操作日志服务，您需要创建RAM用户角色并指定受信云账号、为RAM用户角色授权、为受信账号下的RAM用户授予AssumeRole权限、获取RAM用户角色的临时安全令牌。

背景信息

#unique_13与#unique_14一样，都是RAM中使用的身份。与RAM用户相比，RAM用户角色是一种虚拟用户，它没有确定的身份认证密钥，且需要被一个受信的实体用户（例如云账号、RAM-User账号、云服务账号）扮演才能正常使用。扮演成功后实体用户将获得RAM用户角色的临时安全令牌，使用这个临时安全令牌就能以RAM用户角色身份访问被授权的资源。

步骤1 创建用户角色并指定受信云账号

1. 云账号登录RAM控制台。
2. 在左侧导航栏，单击RAM角色管理。
3. 单击新建RAM角色，选择可信实体类型为阿里云账号，单击下一步。
4. 输入角色名称和备注。
5. 选择云账号为当前云账号或其他云账号

   说明:

   - 若创建的角色是给您自己名下的RAM用户使用（例如授权移动App客户端直接操作LOG资源），请选择当前云账号为受信云账号。
   - 若创建的角色是给其他云账号名下的RAM用户使用（例如跨账号的资源授权），请选择其他云账号，并在受信云账号ID中填写其他云账号的ID。

6. 单击完成。

步骤2 为RAM用户角色授权

成功创建用户角色后，该用户角色没有任何权限，您需要为RAM用户角色授予操作日志服务的权限。您上一步中指定的受信云账号将有权限扮演该RAM用户角色操作日志服务。

说明:

您可以赋予RAM用户角色一个或多个授权策略，包括系统授权策略和自定义授权策略。本文档以授予RAM用户角色管理日志服务的权限为例。

1. 在左侧导航栏，单击RAM角色管理。

2. 在RAM角色名称列表下，找到目标RAM角色。
3. 单击添加权限，被授权主体会自动填入。
4. 在左侧权限策略名称列表下，单击需要授予RAM角色的权限策略AliyunLogFullAccess。
5. 单击确定。
6. 单击完成。

步骤3 为受信云账号的RAM用户授权

RAM用户角色需要被一个受信的实体用户扮演才能正常使用，但是受信实体用户不能以自己的身份扮演RAM用户角色，必须以RAM用户的身份和形式扮演。即RAM用户角色只能通过RAM用户身份来扮演使用。

另外，受信云账号必须为其名下的RAM用户进行AssumeRole授权，授予该RAM用户调用STS服务AssumeRole接口的权限，此RAM用户才能代表受信云账号扮演步骤1中创建的RAM用户角色。

1. 使用受信云账号登录RAM控制台。
2. 在左侧导航栏的权限管理菜单下，单击授权。
3. 单击新增授权。
4. 在被授权主体区域下，输入RAM用户名称后，单击需要授权的RAM用户。
5. 在左侧权限策略名称列表下，单击需要授予RAM用户的权限策略AliyunSTSAssumeRoleAccess。
6. 单击确定。
7. 单击完成。

步骤4 获取RAM用户角色的临时安全令牌

当RAM用户被授予AssumeRole权限之后，可以使用其AccessKey调用安全令牌服务（STS）的AssumeRole接口，以获取某个角色的临时安全令牌。

关于AssumeRole API的调用方法，请参见#unique_15。

使用STS SDK拿到AccessKeyId、AccessKeySecret 、SecurityToken之后就可以使用日志服务的SDK访问日志服务了。

下面是使用AccessKeyId、AccessKeySecret 、SecurityToken初始化LogClient的示例，Java SDK使用请参见#unique_16。

```
package sdksample;
import java.util.ArrayList;
import java.util.List;
import java.util.Vector;
import java.util.Date;
```

```
import com.aliyun.openservices.log.Client;
import com.aliyun.openservices.log.common.*;
import com.aliyun.openservices.log.exception.*;
import com.aliyun.openservices.log.request.*;
import com.aliyun.openservices.log.response.*;
import com.aliyun.openservices.log.common.LogGroupData;
import com.aliyun.openservices.log.common.LogItem;
import com.aliyun.openservices.log.common.Logs.Log;
import com.aliyun.openservices.log.common.Logs.Log.Content;
import com.aliyun.openservices.log.common.Logs.LogGroup;
import com.aliyun.openservices.log.common.Consts.CursorMode;
public class sdksample {
    public static void main(String args[]) throws LogException,
InterruptedException {
        String endpoint = "<log_service_endpoint>"; // 选择与上面步骤创
建 Project 所属区域匹配的Endpoint
        String accessKeyId = "<your_access_key_id>"; // 使用您的阿里云访
问密钥 AccessKeyId
        String accessKeySecret = "<your_access_key_secret>"; // 使用您
的阿里云访问密钥AccessKeySecret
    String securityToken = "<your_security_token>"; //角色的SecurityTo
ken
        String project = "<project_name>"; // 上面步骤创建的项目名称
        String logstore = "<logstore_name>"; // 上面步骤创建的日志库名称
        // 构建一个客户端实例
        Client client = new Client(endpoint, accessKeyId, accessKeyS
ecret);
    // 设置SecurityToken
    client.SetSecurityToken(securityToken);
        // 写入日志
        String topic = "";
        String source = "";
        // 连续发送 10 个数据包，每个数据包有 10 条日志
        for (int i = 0; i < 10; i++) {
            Vector<LogItem> logGroup = new Vector<LogItem>();
            for (int j = 0; j < 10; j++) {
                LogItem logItem = new LogItem((int) (new Date().
getTime() / 1000));
                logItem.PushBack("index"+String.valueOf(j), String.
valueOf(i * 10 + j));
                logGroup.add(logItem);
            }
            PutLogsRequest req2 = new PutLogsRequest(project, logstore
, topic, source, logGroup);
            client.PutLogs(req2);
    }
    }
}
```

4 RAM自定义授权场景

通过RAM访问控制可以为名下的RAM用户（子用户）授权。

主账号可以对其名下的RAM用户（子用户）进行授权，授予其访问或者操作日志服务的权限。您可以为RAM用户授予系统授权策略和自定义授权策略。

注意事项

- 出于安全性的考虑，日志服务建议您将RAM用户的权限设置为需求范围内的最小权限。
- 通常情况下，您需要为RAM用户授予Project列表的只读权限，否则RAM用户无法进入Project列表查看资源。
- 动作`log:ListProject`提供Project列表的查看权限：
  - 具备此权限时，支持只读查看所有Project，暂不支持仅查看某几个Project。
  - 不具备此权限时，无法查看任何Project。

本文档为您演示常见的自定义授权场景和授权内容，包括：

- 控制台场景：Project列表和指定Project的只读权限
- 控制台场景：指定Logstore的只读权限和快速查询的创建、使用权限
- 控制台场景：指定Project中所有快速查询、仪表盘和指定Logstore的只读权限
- API场景：指定Project的写入权限
- API场景：指定Project的消费权限
- API场景：指定Logstore的消费权限

更多信息：

- 可授权的资源
- 可授权的动作
- #unique_25

控制台场景：Project列表和指定Project的只读权限

例如，主账号需要赋予RAM用户以下权限：

1. RAM用户可以看到主账号的日志服务Project列表。
2. RAM用户对主账号的指定Project有只读的访问权限。

同时满足1、2的授权策略如下：

```
{
   "Version": "1",
```

```
   "Statement": [
     {
       "Action": ["log:ListProject"],
       "Resource": ["acs:log:*:*:project/*"],
       "Effect": "Alow"
      },
     {
       "Action": [
         "log:Get*",
         "log:List*"
       ],
       "Resource": "acs:log:*:*:project/<指定的project名称>/*",
       "Effect": "Allow"
     }
   ]
 }
```

控制台场景：指定Logstore的只读权限和快速查询的创建、使用权限

例如，主账号需要赋予RAM用户以下权限：

1. RAM用户登录控制台可以看到主账号的日志服务Project列表。

2. RAM用户对指定Logstore具有只读权限，且可以创建、使用快速查询。

同时满足1、2的授权策略如下：

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "log:ListProject"
      ],
      "Resource": "acs:log:*:*:project/*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "log:List*"
      ],
      "Resource": "acs:log:*:*:project/<指定的Project名称>/logstore/*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "log:Get*",
        "log:List*"
      ],
      "Resource": [
        "acs:log:*:*:project/<指定的Project名称>/logstore/<指定的Logstore
名称>"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "log:List*"
      ],
      "Resource": [
        "acs:log:*:*:project/<指定的Project名称>/dashboard",
        "acs:log:*:*:project/<指定的Project名称>/dashboard/*"
```

```
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "log:Get*",
        "log:List*",
        "log:Create*"
      ],
      "Resource": [
        "acs:log:*:*:project/<指定的Project名称>/savedsearch",
        "acs:log:*:*:project/<指定的Project名称>/savedsearch/*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

控制台场景：指定Project中所有快速查询、仪表盘和指定Logstore的只读权限

例如，主账号需要赋予RAM用户以下权限：

1. RAM用户可以看到主账号的日志服务Project列表。
2. RAM用户仅能查看指定Logstore，同时可以查看所有的快速查询和仪表盘列表。

> 说明：
> 如果希望赋予RAM用户指定Logstore的只读权限，则必须同时赋予该RAM用户所有的快速查询和仪表盘列表的查看权限。

同时满足1、2的授权策略如下：

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "log:ListProject"
      ],
      "Resource": "acs:log:*:*:project/*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "log:List*"
      ],
      "Resource": "acs:log:*:*:project/<指定的Project名称>/logstore/*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "log:Get*",
        "log:List*"
      ],
      "Resource": [
        "acs:log:*:*:project/<指定的Project名称>/logstore/<指定的Logstore
名称>"
      ],
      "Effect": "Allow"
```

```
    },
    {
      "Action": [
        "log:Get*",
        "log:List*"
      ],
      "Resource": [
        "acs:log:*:*:project/<指定的Project名称>/dashboard",
        "acs:log:*:*:project/<指定的Project名称>/dashboard/*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "log:Get*",
        "log:List*"
      ],
      "Resource": [
        "acs:log:*:*:project/<指定的Project名称>/savedsearch",
        "acs:log:*:*:project/<指定的Project名称>/savedsearch/*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

API场景：指定Project的写入权限

RAM用户只能向某一Project写入数据，无法进行查询等其他操作。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "log:Post*"
      ],
      "Resource": "acs:log:*:*:project/<指定的project名称>/*",
      "Effect": "Allow"
    }
  ]
}
```

API场景：指定Project的消费权限

RAM用户只能消费某一Project的数据，无法进行数据写入、查询等其他操作。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "log:ListShards",
        "log:GetCursorOrData",
        "log:GetConsumerGroupCheckPoint",
        "log:UpdateConsumerGroup",
        "log:ConsumerGroupHeartBeat",
        "log:ConsumerGroupUpdateCheckPoint",
        "log:ListConsumerGroup",
        "log:CreateConsumerGroup"
      ],
```

```
      "Resource": "acs:log:*:*:project/<指定的project名称>/*",
      "Effect": "Allow"
    }
  ]
}
```

API场景：指定Logstore的消费权限

RAM用户只能消费指定Logstore的数据，无法进行数据写入、查询等其他操作。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "log:ListShards",
        "log:GetCursorOrData",
        "log:GetConsumerGroupCheckPoint",
        "log:UpdateConsumerGroup",
        "log:ConsumerGroupHeartBeat",
        "log:ConsumerGroupUpdateCheckPoint",
        "log:ListConsumerGroup",
        "log:CreateConsumerGroup"
      ],
      "Resource": [
        "acs:log:*:*:project/<指定的project名称>/logstore/<指定的Logstore
名称>",
        "acs:log:*:*:project/<指定的project名称>/logstore/<指定的Logstore
名称>/*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

5 授权服务角色

日志服务目前提供基于用户日志内容报警功能，为了读取日志数据，需要用户授权日志服务账号访问用户数据。如果已经阅读过该文档并完成授权，可以略过以下内容直接创建报警规则。

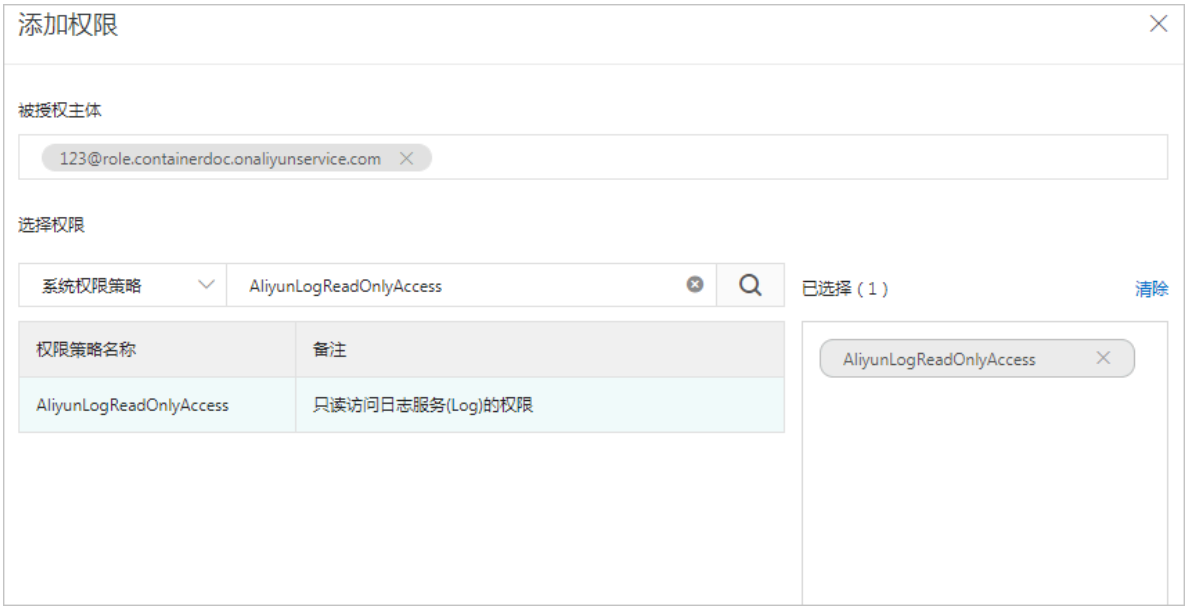
创建RAM角色

1. 云账号登录RAM控制台。
2. 在左侧导航栏，单击RAM角色管理。
3. 单击新建RAM角色，选择可信实体类型为阿里云服务，单击下一步。
4. 输入角色名称和备注。
5. 选择受信服务为日志服务后，单击完成。

授权角色访问日志数据权限

1. 在左侧导航栏，单击RAM角色管理。
2. 在RAM角色名称列表下，找到目标RAM角色。
3. 在RAM角色名称列表下，找到aliyunlogreadrole角色名称。

4. 单击添加权限，被授权主体会自动填入。
5. 在左侧权限策略名称列表下，单击需要授予RAM角色的权限策略AliyunLogReadOnlyAccess。



6. 单击确定。
7. 单击完成。

完成如上步骤后，日志服务即有权限定期读取指定日志库数据进行报警检查。