ALIBABA CLOUD

阿里云

日志服务

访问控制RAM

文档版本：20201026

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.简介

本文介绍RAM的基本概念和相关操作，包括身份管理、资源访问控制、授权RAM用户访问日志服务、授权服务角色读日志和授权用户角色操作日志服务。

基本概念

RAM（Resource Access Management）是阿里云提供的用户身份管理与资源访问控制服务。您可以通过RAM创建、管理用户账号（例如员工、系统或应用程序），并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。

相关操作

- **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**云资源访问授权**页面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。快速授权请单击云资源访问授权。
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。快速授权请单击云资源访问授权。
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。快速授权请单击云资源访问授权。
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。快速授权请单击云资源访问授权。

- **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，参见鉴权规则概览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。

- **授权RAM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。

  配置详情请参见创建RAM用户及授权。

- **授权服务角色读日志**

  日志服务提供基于用户日志内容的报警功能。为了读取日志数据，需要您授权日志服务账号访问日志数据。

  配置详情请参见授权服务角色。

- **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。详情请参见授权用户角色。
  - 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。详情请参见采集-搭建移动端日志直传服务。

2.配置权限助手

日志服务提供权限助手功能，简化日志服务相关的RAM权限策略配置。本文介绍如何在日志服务控制台上配置权限助手。

操作步骤

1. 登录日志服务控制台。
2. 在**Project列表**区域，单击目标Project。
3. 在左侧导航栏中，单击**权限助手**。
4. 在**权限助手**页签，完成如下配置，并单击**下一步**。模式包括**普通项目**和**APP**，具体配置如下表所示。
   - **普通项目**

     普通项目模式包括日志服务的所有功能模块权限的配置。

参数	说明
预设角色选择	不同的角色已配置不同的功能模块，您可以根据需求选择已预设的角色，也可以自定义选择功能模块。 功能模块的权限包括管理权限和只读权限，请根据需求选择。 **说明** 功能模块之间存在依赖关系如下所示： ■ 必须配置项目的只读或管理权限，否则无法操作其他功能。 ■ 数据接入模块依赖于Logstore模块，所以勾选数据接入中的任意一项都会默认勾选Logstore模块。 ■ 可视化模块依赖于数据查询模块。 ■ 告警、订阅和数据接入（云产品接入）等模块依赖于数据可视化模块。其中，使用告警和订阅模块时需要配置数据可视化模块的管理权限。

参数	说明
资源	配置功能模块的权限后，您可以配置权限能使用的资源。项目名称和Logstore名称支持用 * 号表示，例如： ■ 拥有如下权限的用户或角色能操作日志服务的所有资源。 "Action": "log:*", "Resource": "*", ■ 拥有如下权限的用户或角色只能操作project01项目下的资源。 acs:log:*:*:project/project01 acs:log:*:*:project/project01/* ■ 拥有如下权限的用户或角色只能操作project01项目下logstore01日志库下的资源。 acs:log:*:*:project/project01/logstore/logstore01 acs:log:*:*:project/project01/logstore/logstore01/*
限制条件	根据需求，配置限制条件，详情请参见权限策略基本元素。

- **APP**

  APP模式包括成本管家和日志审计服务的权限配置。

配置项	说明
APP列表	请根据需求选择您要配置的APP及其权限，权限包括允许和禁止。
预设角色选择	当APP的权限选择允许时，会自动选中相关的功能模块，您也可以自定义选择。 功能模块的权限包括管理权限和只读权限，请根据需求选择。 说明 功能模块之间存在依赖关系如下所示： ■ 必须配置项目的只读或管理权限，否则无法操作其他功能。 ■ 数据接入模块依赖于Logstore模块，所以勾选数据接入中的任意一项都会默认勾选Logstore模块。 ■ 可视化模块依赖于数据查询模块。 ■ 告警、订阅和数据接入（云产品接入）等模块依赖于数据可视化模块。其中，使用告警和订阅模块时需要配置数据可视化模块的管理权限。

配置项	说明
资源	系统根据已选择的APP指定资源，无法修改。
限制条件	根据需求，配置限制条件，详情请参见权限策略基本元素。

5. 预览权限策略确认规则信息，同时您还可以编辑已生成的权限策略，具体操作如下表所示。 完成后单击下一步。

操作	说明
格式化	对手动编辑过的json代码进行格式化。
压缩	由于应用策略配置时有长度限制，压缩功能可以去掉多余的空格和换行。
重置	还原手动编辑的内容。
复制到剪贴板	将当前编辑器中的内容复制到剪贴板，方便后续使用。
添加到自定义模板	将当前的权限策略添加到自定义策略模板中，方便后续使用。 说明 该模板只存放在浏览器的本地存储中，更换浏览器后无法查看。

6. 根据页面指引步骤应用上线该权限策略，完成授权。

相关操作

- 应用常见策略模板

  在权限助手页签，已设置常用策略模板，您可以根据需求选用模板。

- 应用自定义策略模板

  在权限助手页签，还可以将自定义的权限策略添加到自定义策略模板中，方便后续使用。

  说明 自定义策略模板保存在浏览器的本地存储中，更换浏览器后无法查看。

3.创建RAM用户及授权

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见入门概述。

创建RAM用户

1. 登录RAM控制台。
2. 在左侧导航栏，单击**人员管理 > 用户**。
3. 单击**创建用户**。
4. 输入**登录名称**和**显示名称**。
5. 选中**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，创建方法参见创建自定义授权策略，权限策略示例请参见RAM自定义授权场景和日志服务RAM授权策略。下文以赋予用户`AliyunLogReadOnlyAccess`权限为例。

1. 在左侧导航栏，单击**人员管理 > 用户**。
2. 找到目标用户，单击**添加权限**。
3. 在**添加权限**页面，选中**系统策略**下的**AliyunLogReadOnlyAccess**，并单击**确定**。
4. 确认授权结果，单击**完成**。

RAM登录控制台

完成创建用户和用户授权之后，您可以通过以下两种方式以RAM用户身份登录控制台。

- 在**概览**页面右侧**账号管理**区域，单击用户登录地址链接，使用已创建的RAM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用户名和密码登录。

- 方式一：*<$username>*@*<$AccoutAlias>*.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。*<$username>*为RAM用户名称*<$AccoutAlias>*.onaliyun.com为默认域名。

- 方式二：*<$username>*@*<$AccoutAlias>*。例如：*username@company-alias*。

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

4.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

角色和用户都是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、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. 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. 选择可信实体类型为**阿里云账号**，单击**下一步**。
5. 请参考下表说明进行角色配置。

配置项	说明
角色名称	请输入角色名称。
备注	请输入备注信息。
选择云账号	可以选择**当前云账号**或**其他云账号**。 ○ 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客户端直接操作日志服务的资源），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。

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。下文步骤以授予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. 找到目标RAM角色，单击**添加权限**。
3. 在**添加权限**页面，选中**系统策略**下的**AliyunLogFullAccess**，单击**确定**。
4. 确认授权结果，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：创建用户角色并指定受信云账号中创建的RAM用户角色。

1. 在左侧导航栏，单击**人员管理 > 用户**。
2. 找到目标用户，单击**添加权限**。
3. 在**添加权限**页面，选中**系统策略**下的**AliyunSTSAssumeRoleAccess**，单击**确定**。
4. 确认授权结果，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，通过调用STS AssumeRole接口获取步骤1：创建用户角色并指定受信云账号中创建的RAM用户角色的临时安全令牌。

> **说明**
>
> - 关于AssumeRole API的调用方法，请参见Java示例。
> - 使用STS SDK拿到AccessKey ID、AccessKey Secret、SecurityToken之后，通过使用日志服务的SDK访问日志服务，请参见概述。

5.RAM自定义授权场景

通过访问控制RAM可以为名下的RAM用户授权，本文档为您介绍常见的自定义授权场景和授权内容。

背景信息

基于安全考虑，建议您为RAM用户授予最小可用权限。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。具体请参见系统授权策略和自定义授权策略。

控制台场景

- **Project只读权限**

  例如主账号需要授予RAM用户以下权限：

  - RAM用户具有主账号Project列表的查看权限。
  - RAM用户具有主账号指定Project的只读权限。

  同时满足上述权限的权限策略如下：

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

- **指定Logstore的只读权限和快速查询的创建、使用权限**

  例如主账号需要授予RAM用户以下权限：

  - RAM用户具有主账号Project列表的查看权限。
  - RAM用户具有指定Logstore的只读权限，同时具有创建并管理快速查询的权限。

  同时满足上述权限的权限策略如下：

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

```
  "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"
   }
 ]
}
```

> **说明** 授权策略中Resource内容结尾不带*仅表示当前资源，带*表示当前资源下的其他资源，内容用*代替。

- **指定Logstore的只读权限及指定Project中快速查询和仪表盘的只读权限**

  例如主账号需要授予RAM用户以下权限：

  - RAM用户具有主账号Project列表的查看权限。
  - RAM用户具有指定Logstore的只读权限，同时具有查看该Project中所有的快速查询和仪表盘列表的权限。

  同时满足上述权限的权限策略如下：

```
{
 "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**

  授予RAM用户向指定Project写入数据的权限，不包含查询等其他操作权限。

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

- **指定Project的消费权限**

  授予RAM用户消费指定Project数据的权限，不包含数据写入、查询等其他操作权限。

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

- **指定Logstore的消费权限**

  授予RAM用户消费指定Logstore数据的权限，不包含数据写入、查询等其他操作权限。

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

更多参考

更多授权信息请参见：

- 可授权的资源
- 可授权的动作
- 鉴权规则

6.授权服务角色

受信云服务可以通过扮演RAM角色来访问您的云资源，本文介绍如何创建并授权服务角色。

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. 选择可信实体类型为**阿里云服务**，单击**下一步**。
5. 配置角色信息。

   重要参数说明如下表所示。

参数	说明
角色类型	选择**普通角色类型**。
角色名称	输入角色名称，例如aliyunlogreadrole。
备注	输入创建角色的备注信息。
选择受信服务	选择**日志服务**。

6. 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. 找到目标RAM角色，单击**添加权限**。
3. 在**添加权限**页面，选中**系统策略**下的**AliyunLogReadOnlyAccess**，单击**确定**。
4. 确认授权结果，单击**完成**。