ALIBABA CLOUD

阿里云

服务网格

授权管理

文档版本：20220323

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.授权概述 05
2.RAM授权 06
2.1. 为RAM用户和RAM角色授权 06
2.2. 授予RAM用户和RAM角色RBAC权限 11
3.服务网格产品授权 13
3.1. 管理ASM服务关联角色 13

1.授权概述

服务网格ASM实例的授权分为RAM授权和RBAC授权两部分。本文介绍两种授权的内容以及如何进行授权。

服务网格产品授权

如果您想要完整地使用服务网格ASM的各项能力，您必须为ASM授权，使其能够访问您的其他云产品，例如ASM需要访问日志服务为您创建审计日志Project和LogStore，您才能使用日志服务采集数据平面的AccessLog。ASM通过服务关联角色获取相应的云产品权限，您需要创建服务关联角色，完成对服务网格产品的授权。具体操作，请参见管理ASM服务关联角色。

RAM用户授权

通过RAM用户使用服务网格时涉及RAM权限和RBAC权限，您需要根据需求为RAM用户针对两种权限分别进行授权。

RAM授权

在企业对接RAM的账号系统中，运维人员通过RAM用户（即子账号）管理云服务资源是一个常见场景。然而默认情况下RAM用户没有使用云服务OpenAPI的任何权限，为了保证RAM用户的正常使用，需要对RAM用户授权。

您可以通过授予RAM用户OpenAPI的权限，控制RAM用户ASM控制台操作的权限和OpenAPI操作的权限，实现细粒度的云资源访问控制。更多信息，请参见为RAM用户和RAM角色授权。

RBAC授权

RBAC授权是网格维度的权限控制，用于控制RAM用户ASM自定义资源（例如虚拟服务、目标规则等）的操作权限，一个RAM用户对不同的网格实例可以有不同的RBAC权限。

ASM内置了以下三种角色，分别对应不同的RBAC权限，您可以通过ASM控制台给RAM用户授予以下预置角色。

角色	集群内RBAC权限
网格管理人员	对所有命名空间下所有资源（即ASM的自定义资源）的读写权限。
网格管理受限人员	对所有命名空间或所选命名空间下控制台可见资源（即ASM的自定义资源）的只读权限。
无权限	对所有命名空间下所有资源（即ASM的自定义资源）没有任何读写权限。

为RAM用户授权

1. 在RAM控制台创建RAM用户。具体操作，请参见创建RAM用户。
2. 根据需要授予RAM用户相应的RBAC权限。具体操作，请参见授予RAM用户和RAM角色RBAC权限。
3. 根据需要授予RAM用户相应的RAM策略。具体操作，请参见为RAM用户和RAM角色授权。

2.RAM授权

2.1. 为RAM用户和RAM角色授权

您可以按需为RAM用户和RAM角色赋予不同的权限，仅具有权限的RAM用户和RAM角色才可以在ASM控制台上进行创建网格实例、更新服务网格功能配置等操作，避免因暴露阿里云账号密钥而造成安全风险。本文以RAM用户为例，介绍如何为RAM用户和RAM角色进行RAM授权。

前提条件

- 已创建RAM用户和RAM角色。具体操作，请参见创建RAM用户和创建可信实体为阿里云账号的RAM角色。
- 已了解授权策略语言的基本结构和语法。更多信息，请参见权限策略语法和结构。

背景信息

RAM用户和RAM角色的使用场景不同，授予的权限也不同，具体区别如下：

- 如果RAM用户和RAM角色只需要服务网格的操作权限，不涉及集群的操作，您只需要授予RAM用户服务网格权限。具体操作，请参见授予RAM用户和RAM角色系统策略和授予RAM用户和RAM角色自定义策略。
- 如果RAM用户和RAM角色需要服务网格和集群的操作权限（例如添加或删除网格内的ACK集群），您需要授予RAM用户服务网格和对应集群的权限。具体操作，请参见授予RAM用户和RAM角色系统策略、授予RAM用户和RAM角色自定义策略和授予RAM用户集群权限。

授予RAM用户和RAM角色系统策略

ASM默认已创建AliyunASMReadOnlyAccess和AliyunASMFullAccess策略，您直接授权使用即可。以下为系统策略的详细介绍：

- AliyunASMReadOnlyAccess

  只读管理阿里云服务网格(ASM)的权限，仅看服务网格状态等只读接口权限，无法对服务网格进行变更操作。

- AliyunASMFullAccess

  管理阿里云服务网格(ASM)的权限，RAM用户拥有该授权后，对于镜像资源的权限等同于阿里云账号，可以做任意操作。

以下以授予AliyunASMReadOnlyAccess权限策略为例，介绍如何授予RAM用户系统策略：

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 用户**。

   > **说明** 如果您是授予RAM角色权限，此步骤您需要在左侧导航栏选择**身份管理 > 角色**。

3. 在**用户**页面，单击目标RAM用户**操作**列的**添加权限**。

   > **说明** 如果您是授予RAM角色权限，此步骤您需要在**角色**页面单击目标角色右侧**操作**列下的**添加权限**。

4. 在**添加权限**面板，为RAM用户和RAM角色添加权限。

i. 选择授权应用范围。

- **整个云账号**：权限在当前阿里云账号内生效。
- **指定资源组**：权限在指定的资源组内生效。

> **说明** 指定资源组授权生效的前提是该云服务已支持资源组。更多信息，请参见支持资源组的云服务。

ii. 输入被授权主体。

被授权主体即需要授权的RAM用户，系统会自动填入当前的RAM用户，您也可以添加其他RAM用户。

iii. 在**选择权限**下单击**系统策略**，在文本框中输入AliyunASMReadOnlyAccess，然后单击AliyunASMReadOnlyAccess。

iv. 单击**确定**。

5. 单击**完成**。

授予RAM用户和RAM角色自定义策略

如果您想对权限进行细粒度控制，您可以自定义策略，然后授予RAM用户和RAM角色自定义策略权限。

1. 使用具有RAM权限的账号登录RAM控制台。
2. 创建授予访问ASM实例的权限策略。
   i. 在左侧导航栏，选择**权限管理 > 权限策略**。
   ii. 在**权限策略**页面，单击**创建权限策略**。
   iii. 在**创建权限策略**页面单击**脚本编辑**，在策略内容中编写您的授权策略内容，然后单击**下一步**。

   通过改变 `Statement` 中的 `Action` 字段，可以实现API的细粒度鉴权。本文以授予受限访问权限策略为例，受限访问权限策略包括除RBAC授权之外的服务网格的所有RAM权限，拥有该权限的RAM用户不可以对其他用户进行RBAC授权，但拥有除此之外的其他所有权限。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicemesh:Add*",
                "servicemesh:CRBatchDeletion",
                "servicemesh:Create*",
                "servicemesh:Delete*",
                "servicemesh:Describe*",
                "servicemesh:Enable*",
                "servicemesh:Disable*",
                "servicemesh:Get*",
                "servicemesh:InvokeApiServer",
                "servicemesh:List*",
                "servicemesh:Modify*",
                "servicemesh:Re*",
                "servicemesh:Run*",
                "servicemesh:Set*",
                "servicemesh:Sync*",
                "servicemesh:Update*",
                "servicemesh:Upgrade*"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "log:ListLogStores",
                "log:ListDashboard",
                "log:GetDashboard",
                "log:ListSavedSearch",
                "log:ListProject"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "log:GetLogStoreLogs",
            "Resource": "acs:log:*:*:project/*/logstore/audit-*"
        },
        {
            "Effect": "Allow",
            "Action": "log:GetLogStoreLogs",
            "Resource": "acs:log:*:*:project/*/logstore/istio-*"
        },
        {
            "Action": "ram:CreateServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "servicemesh.aliyuncs.com"
                }
            }
        }
    ],
    "Version": "1"
}
```

iv. 在**基本信息**区域输入策略名称，本文设置为ASMPolicy1，然后单击**确定**。

3. 授予RAM用户和RAM角色权限策略。

i. 在左侧导航栏选择**身份管理 > 用户**。

> **说明** 如果您是授予RAM角色权限，此步骤您需要在左侧导航栏选择**身份管理 > 角色**。

ii. 在**用户**页面单击目标RAM用户右侧**操作**列下的**添加权限**。

> **说明** 如果您是授予RAM角色权限，此步骤您需要在**角色**页面单击目标角色右侧**操作**列下的**添加权限**。

iii. 在**添加权限**对话框设置**授权范围**为**整个云账号**，系统会自动填入当前的RAM用户为授权主体，在**选择权限**下单击**自定义策略**，然后输入创建的权限策略名称ASMPolicy1，单击ASMPolicy1，然后单击**确定**。

自定义策略场景示例

场景一：授予单个网格实例的管理权限

您可以使用以下脚本创建拥有单个网格实例管理权限的策略，授予RAM用户或RAM角色该权限策略后，RAM用户或RAM角色只能管理指定ID的网格实例。

> **说明** 创建权限策略时，请将以下脚本中的 `<ServicemeshId>` 替换成实际需要授权的网格实例ID。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "servicemesh:*",
      "Resource": "acs:servicemesh:*:*:servicemesh/<ServicemeshId>"
    },
    {
      "Effect": "Allow",
      "Action": "servicemesh:DescribeServiceMeshes",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "log:GetLogStoreLogs",
      "Resource": "acs:log:*:*:project/*/logstore/audit-<ServicemeshId>"
    },
    {
      "Effect": "Allow",
      "Action": "log:GetLogStoreLogs",
      "Resource": "acs:log:*:*:project/*/logstore/istio-<ServicemeshId>"
    }
  ],
  "Version": "1"
}
```

场景二：授予使用ASM控制台管理Istio资源的读写权限

ASM默认提供的AliyunASMReadOnlyAccess系统策略可以授予RAM用户或RAM角色只读管理阿里云服务网格ASM的权限，但被授予此权限的RAM用户或RAM角色无法管理网格中的Istio资源。

您可以使用以下脚本创建拥有Istio资源读写权限的策略，授予RAM用户或RAM角色该权限策略后，RAM用户或RAM角色可以正常使用ASM控制台管理网格中的Istio资源，同时无法对网格的其它部分（例如功能设置等）进行任何变更。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicemesh:List*",
                "servicemesh:Describe*",
                "servicemesh:Get*",
                "servicemesh:InvokeApiServer"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "log:ListLogStores",
                "log:ListDashboard",
                "log:GetDashboard",
                "log:ListSavedSearch"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "log:GetLogStoreLogs",
            "Resource": "acs:log:*:*:project/*/logstore/audit-*"
        }
    ],
    "Version": "1"
}
```

场景三：授予对其它用户或角色进行RBAC授权的权限

您可以使用以下脚本创建拥有对其它用户或角色进行RBAC授权权限的策略，授予RAM用户或RAM角色该权限策略后，RAM用户或RAM角色可以使用ASM控制台管理其它RAM角色或RAM用户的RBAC权限，同时无法操作或查看任何网格实例。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicemesh:DescribeUserPermissions",
                "servicemesh:GrantUserPermissions",
                "servicemesh:DescribeServiceMeshes",
                "servicemesh:DescribeUsersWithPermissions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ims:ListUserBasicInfos",
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

2.2. 授予RAM用户和RAM角色RBAC权限

您可以通过RBAC授权控制RAM用户和RAM角色ASM自定义资源的操作权限，当RAM用户和RAM角色需要操作ASM内的自定义资源时，您需要对RAM用户和RAM角色进行RBAC授权。本文介绍以RAM用户为例，介绍如何授予RAM用户和RAM角色对应的RBAC权限。

配置说明

阿里云账号或RAM用户都支持给RAM用户授予RBAC权限。

操作步骤

1. 登录ASM控制台。
2. 在左侧导航栏，选择**服务网格 > 授权管理**。
3. 在**授权管理**页面的RAM用户列表中，选择需要授权的RAM用户，单击**授权**。

   > **说明** 如果您是授予RAM角色RBAC权限，此步骤您需要在**授权管理**页面的单击**RAM角色**页签，选择需要授权的RAM角色，然后单击**授权**。

4. 针对每一个网格实例，为该RAM用户选择相应的预置角色，单击**提交**。

   角色权限说明如下表所示。

角色	集群内RBAC权限
网格管理人员	对所有命名空间下所有资源（即ASM的自定义资源）的读写权限。
网格管理受限人员	对所有命名空间或所选命名空间下控制台可见资源（即ASM的自定义资源）的只读权限。

角色	集群内RBAC权限
无权限	对所有命名空间下所有资源（即ASM的自定义资源）没有任何读写权限。

3.服务网格产品授权

3.1. 管理ASM服务关联角色

ASM服务关联角色（AliyunServiceRoleForServiceMesh）是访问控制提供的一种服务关联角色，用于授权服务网格访问关联云资源。本文介绍如何创建和删除ASM服务关联角色。

背景信息

服务关联角色是与云服务关联的角色。通过ASM服务关联角色（AliyunServiceRoleForServiceMesh），服务网格可以获得阿里云容器服务ACK、专有网络VPC、负载均衡SLB、日志服务SLS、链路追踪服务、应用实时监控服务ARMS、云企业网CEN等的访问权限。更多服务关联角色的说明，请参见服务关联角色。

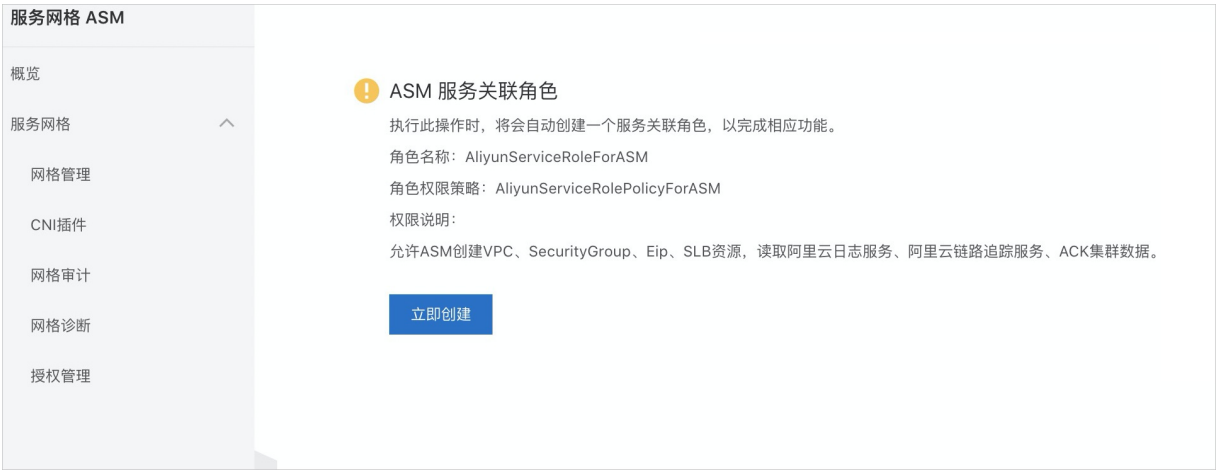
注意事项

如果您使用的是阿里云账号，则默认有创建ASM服务关联角色的权限。如果您使用的是RAM用户，您需要为RAM用户授予创建服务网格服务关联角色的权限，以下为需要授予的权限策略（CreateServiceLinkedRole）。具体操作，请参见为RAM用户授权。

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

创建ASM服务关联角色

在您使用服务网格时，系统会检查当前账号是否已有AliyunServiceRoleForServiceMesh。如果不存在则会提示进行创建，在服务网格提示页面单击**立即创建**，即可创建ASM服务关联角色。



服务关联角色包含的权限策略由对应的云服务定义和使用，您不能为服务关联角色添加、修改或删除权限。您可以在角色详情中查看角色包含的权限策略等信息。具体操作，请参见查看RAM角色基本信息。

删除ASM服务关联角色

如果您暂时不需要使用AliyunServiceRoleForServiceMesh，例如不需要创建或使用服务网格，可以删除AliyunServiceRoleForServiceMesh。

> **说明** 删除AliyunServiceRoleForServiceMesh前，必须先删除当前账号下所有地域中的服务网格实例，否则会提示删除失败。一个阿里云账号下只有一个AliyunServiceRoleForSerivceMesh，删除AliyunServiceRoleForServiceMesh后，阿里云账号和RAM用户都将无法再创建和使用服务网格。

1. 使用阿里云账号登录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，搜索框中搜索AliyunServiceRoleForServiceMesh，找到AliyunServiceRoleForServiceMesh，然后单击AliyunServiceRoleForServiceMesh**操作**列的**删除**。
4. 在提示对话框中单击**确定**。

> **说明** 删除服务关联角色时，**操作**列会先显示**角色删除中...**，您需要等待几秒钟，直至提示删除成功。对于删除失败的情形，请在报错提示信息中单击**查看详情**，根据错误详情进行相应处理。