ALIBABA CLOUD

阿里云

资源管理

资源目录

文档版本：20220627

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.资源目录概述

资源目录RD（Resource Directory）是阿里云面向企业客户提供的一套多级账号和资源关系管理服务。

应用场景

资源目录支持您快速建立一套符合企业业务关系的目录结构，并将企业多个账号分布到这个目录结构中的相应位置，从而形成资源间的多层级关系。企业可依赖目录结构进行账号与资源的集中管理，满足企业在网络部署、账单结算、用户权限、安全合规和日志审计等方面的统一管控要求。具体如下：

- **依据企业业务环境构建目录结构**

  企业拥有不同的分公司、部分或项目，资源目录可以根据企业业务环境在云上构建企业的目录结构。

- **集中管理企业的账号和资源**

  当企业拥有多个阿里云账号时，企业希望可以集中管理这些账号和资源。资源目录支持将分散的账号纳入到企业的目录结构下，实现企业对账号下所有资源的集中管理。

- **统一管理企业的账单与票据**

  企业可以在资源目录内创建具有统一结算账号的成员，集中管理账单和发票。

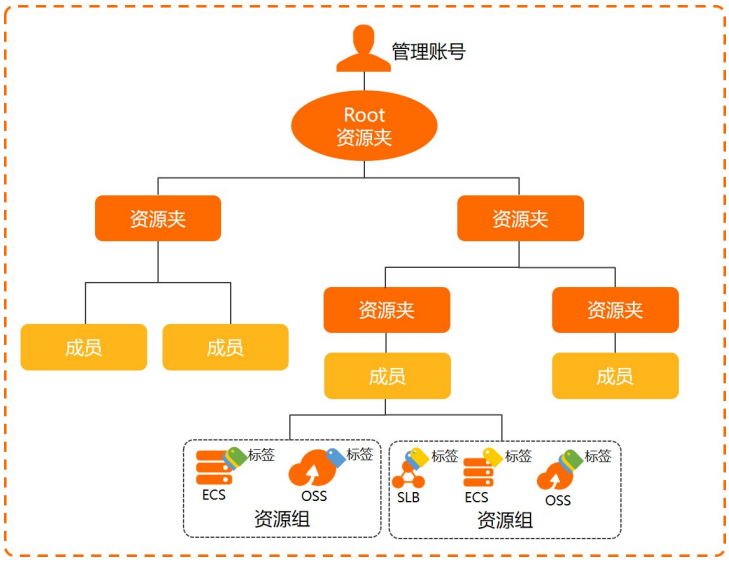
- **依赖目录结构满足权限及合规性要求**

  企业可以为不同的账号、目录结构设定不同的资源访问规则，通过RAM权限策略和资源目录管控策略，打通人员和资源间的授权与管控通道，保障企业资源的访问安全。

- **开放式接入众多阿里云企业级应用**

  依赖目录结构，阿里云财资平台、合规审计平台、云安全平台及网络平台等集成资源目录，提供企业级服务并确保企业管理在相同的架构之内，为企业提供标准的、一致的企业级服务。

基本概念



概念	说明

概念	说明
管理账号	管理账号（Management Account，简称MA）是资源目录的超级管理员，也是开通资源目录的初始账号，对其创建的资源目录和成员拥有完全控制权限。只有通过企业实名认证的阿里云账号才能开通资源目录，每个资源目录有且只有一个管理账号。 为了确保管理账号的安全，建议您创建一个新的阿里云账号作为管理账号的根用户，避免将已有用途的阿里云账号作为管理账号开通资源目录。同时，您可以为管理账号创建一个RAM用户并授予管理员权限，使用该RAM用户管理整个资源目录。资源目录中的所有操作都必须由管理账号或具有管理员权限的RAM用户执行。 **说明** 管理账号位于资源目录外部，不归属于资源目录，所以不受资源目录的任何管控策略影响。
Root资源夹	Root资源夹位于资源目录的顶层，没有父资源夹。资源关系依据Root资源夹向下分布。
资源夹	资源夹是资源目录内的组织单元，通常用于指代企业的分公司、业务线或产品项目。每个资源夹下可以放置成员，并允许嵌套子资源夹，最终形成树形的资源组织关系。
成员	在资源目录内，成员作为资源容器，是一种资源分组单位。成员通常用于指代一个项目或应用，每个成员中的资源相对其他成员中的资源是物理隔离的。您可以通过管理账号授予RAM用户或RAM角色相应权限，用于登录和访问成员。 成员分为如下两种类型： • 资源账号 您在资源目录中创建的成员默认为资源账号。资源账号不允许开启Root登录权限，具有更高的安全性。关于创建资源账号的具体操作，请参见创建成员。 • 云账号 云账号就是阿里云账号作为资源目录成员的称呼，您可以邀请已存在的阿里云账号加入到资源目录中。阿里云账号具有Root登录权限。关于邀请阿里云账号的具体操作，请参见邀请阿里云账号加入资源目录。
RDPath	RDPath是指资源实体（资源夹或成员）在资源目录中的位置信息，即从资源实体当前位置（资源实体ID）向上直到资源目录（资源目录ID）的全部路径ID组合。格式： • 资源夹RDPath：`<资源目录ID>/<Root资源夹ID>/……/<当前资源夹ID>`。 • 成员RDPath：`<资源目录ID>/<Root资源夹ID>/……/<当前成员ID>`。例如：成员181761095690****的RDPath为`rd-r4****/r-oG****/fd-RIErN0****/fd-XVxh6D****/181761095690****`。 关于查看资源夹RDPath和成员RDPath的具体操作，请参见查看资源夹基本信息和查看成员详情。
管控策略	资源目录管控策略是一种基于资源结构（资源夹或成员）的访问控制策略，可以统一管理资源目录各层级内资源访问的权限边界，建立企业整体访问控制原则或局部专用原则。管控策略只定义权限边界，并不真正授予权限，您还需要在某个成员中使用访问控制（RAM）设置权限后，相应身份才具备对资源的访问权限。 关于管控策略的更多信息，请参见管控策略概述。

概念	说明
可信服务	可信服务是指支持与资源目录组合使用的其他阿里云服务。资源目录允许可信服务访问资源目录中的成员、资源夹等信息。您可以使用管理账号或可信服务的委派管理员账号，在可信服务中基于组织进行业务管理，从而简化企业对云服务的统一管理。例如：配置审计集成资源目录后，管理账号可以在可信服务配置审计中查看所有成员的资源列表、资源配置历史和资源合规状态，并监控资源配置合规性。 关于可信服务的更多信息，请参见可信服务概述。
委派管理员账号	资源目录的管理账号可以将资源目录中的成员设置为可信服务的委派管理员账号。设置成功后，委派管理员账号将获得管理账号的授权，可以在对应可信服务中访问资源目录组织和成员信息，并在该组织范围内进行业务管理。通过委派管理员账号，可以将组织管理任务与业务管理任务相分离，管理账号执行资源目录的组织管理任务，委派管理员账号执行可信服务的业务管理任务，这符合安全最佳实践的建议。 关于添加或移除委派管理员的具体操作，请参见管理委派管理员账号。

使用流程

1. 使用管理账号登录资源管理控制台。
2. 开通资源目录。

   具体操作，请参见开通资源目录。
3. 创建资源夹，搭建企业的组织结构。

   具体操作，请参见创建资源夹。
4. 创建成员，或者邀请已有的阿里云账号，并将这些成员移动到对应的资源夹下。

   具体操作，请参见创建成员、邀请阿里云账号加入资源目录和移动成员。

使用限制

限制项	最大值	提升配额方式	备注
每个阿里云账号允许创建的资源目录数量	1个	无	如果账号是资源目录的成员，将不能创建资源目录。
目录中的Root资源夹数量	1个	无	无
目录中的资源夹数量	100个	配额申请	不包含Root资源夹。
资源夹层级深度	5级	无	从Root资源夹向下算起，不包含Root资源夹。
目录中的成员数量	20个	配额申请	无
每日有效邀请数	20条	配额申请	不包含已接受状态的邀请。
邀请记录过期时间	14天	无	无

限制项	最大值	提升配额方式	备注
设置安全手机号码时每天发送验证码的次数	100次	无	无

2.管理账号

2.1. 管理资源目录

2.1.1. 开通资源目录

使用资源目录，企业可以将阿里云上承载的所有业务账号集合在资源目录内，按业务关系将其分类，以结构化方式统一管理。资源目录需要开通后，才能正常使用。

前提条件

请使用经过企业实名认证的阿里云账号开通资源目录。个人实名认证账号不能开通资源目录。

开通方式

开通资源目录的阿里云账号默认为资源目录的管理账号，具有管理资源目录的所有权限，承担对资源目录中的所有业务账号及其下资源的管理责任。建议企业使用专门的阿里云账号作为资源目录的管理账号，不要同时使用管理账号部署业务，尽量避免因管理账号承担的责任过于宽泛而可能导致的管理问题。

在开通过程中，系统会自动检查当前登录账号的企业实名认证、安全信息（手机号码或电子邮箱）及资源保有情况，然后判断其是否具备开通资源目录的条件，并根据判断结果推荐以下两种方式中的一种去开通资源目录。

- 使用当前登录账号开通资源目录

  该方式适用于当前登录账号已完成企业实名认证、已设置安全信息且账号下没有资源的情况。

- 创建新的管理账号开通资源目录

  该方式适用于当前登录账号已完成企业实名认证，但未设置安全信息或账号下存在资源的情况。该方式会创建一个新的阿里云账号作为资源目录的管理账号，新账号会继承当前登录账号的企业实名认证信息，同时，当前登录账号会成为该资源目录的成员。

使用当前登录账号开通资源目录

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**开通资源目录**。
4. 选择**使用当前账号开通**。
5. 单击**开通**。
6. 在**安全校验**对话框中，通过手机号码或电子邮箱完成安全验证，然后单击**确定**。

   开通资源目录后，系统会为您创建一个**Root**资源夹，并将当前的登录账号设置为管理账号。

   同时，系统会在管理账号内自动创建一个服务关联角色（AliyunServiceRoleForResourceDirectory），用于设置资源目录可信服务的访问权限。关于服务关联角色的更多信息，请参见资源目录中的RAM角色。

创建新的管理账号开通资源目录

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**开通资源目录**。

4. 选择**创建新管理账号开通**。
5. 输入自定义的管理账号名称。
6. 设置管理账号的安全手机号码。

   系统会自动继承当前登录账号的安全手机号码。您也可以单击**修改**，为新创建的管理账号设置其他的手机号码。
7. 单击**开通**。
8. 在**安全校验**对话框中，通过步骤设置的手机号码完成安全验证，然后单击**确定**。

   开通资源目录后，系统会为您创建一个**Root**资源夹，并将新创建的账号设置为资源目录的管理账号，将当前的登录账号设置为资源目录的成员。

   > **说明** 对于新创建的管理账号，您需要通过密码找回功能，使用步骤设置的手机号码设置登录密码，然后登录资源管理控制台管理资源目录。

   同时，系统会在管理账号内自动创建一个服务关联角色（AliyunServiceRoleForResourceDirectory），用于设置资源目录可信服务的访问权限。关于服务关联角色的更多信息，请参见资源目录中的RAM角色。

2.1.2. 查看资源目录基本信息

本文为您介绍如何查看资源目录的基本信息，包括目录ID、创建时间和管理账号。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 设置**。
3. 查看资源目录的基本信息，包括目录ID、创建时间和管理账号。

2.1.3. 关闭资源目录

当您不再需要使用资源目录时，可以将其关闭。此操作不可恢复，请您慎重操作。

前提条件

关闭资源目录前，请确认已完成以下操作：

- 资源目录内所有成员已被移除。
- 资源目录内除**Root**资源夹外的资源夹已全部删除。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 设置**。
3. 单击**关闭资源目录**。

执行结果

关闭资源目录后，会有以下影响：

- 您创建的组织关系和管控策略等数据将会被清理。
- 已启用的可信服务中的相关数据将会被清理。例如：如果您在操作审计中创建了多账号跟踪，当关闭资源目录后，操作审计中的多账号跟踪数据将会被清理。

- 可信服务中集成了资源目录的功能可能会被禁用。例如：云SSO的多账号权限管理功能，只有资源目录已启用时才能正常运行。

2.1.4. 资源目录中的RAM角色

本文为您介绍在资源目录中为管理账号和成员自动创建的RAM角色。

总览

资源目录管理账号和成员内自动创建的RAM角色如下表所示。

账号类型	RAM角色名称	RAM角色类型
管理账号	AliyunServiceRoleForResourceDirectory	服务关联角色
成员	AliyunServiceRoleForResourceDirectory	服务关联角色
	ResourceDirectoryAccountAccessRole	可信实体为阿里云账号的RAM角色
	AliyunServiceRoleFor***	服务关联角色

AliyunServiceRoleForResourceDirectory

应用场景

服务关联角色（AliyunServiceRoleForResourceDirectory）用于为资源目录可信服务提供访问通道。资源目录服务通过该服务关联角色为可信服务创建服务关联角色，使其可以获取其他云服务的访问权限。关于服务关联角色的更多信息，请参见服务关联角色。

权限策略

名称：AliyunServiceRolePolicyForResourceDirectory

内容：

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

信任策略

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "resourcemanager.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}
```

创建角色

系统会在以下场景中自动创建服务关联角色（AliyunServiceRoleForResourceDirectory）：

- 资源目录开通成功后，在管理账号内创建该服务关联角色。
- 成员创建成功后，在成员内创建该服务关联角色。
- 被邀请账号成功加入资源目录后，在被邀请账号内创建该服务关联角色。

删除角色

系统会在以下场景中尝试自动删除服务关联角色（AliyunServiceRoleForResourceDirectory）：

- 关闭资源目录时，系统将自动删除管理账号内的该服务关联角色。
- 从资源目录中移除成员时，系统将自动删除成员内的该服务关联角色。

当服务关联角色（AliyunServiceRoleForResourceDirectory）没有被任何云资源使用时，您也可以手动删除该服务关联角色。具体操作，请参见删除RAM角色。

ResourceDirectoryAccountAccessRole

应用场景

RAM角色（ResourceDirectoryAccountAccessRole）用于资源目录管理员登入成员进行相关管理操作，该角色中的可信实体为资源目录管理账号。

权限策略

名称：AdministratorAccess

内容：

```
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

信任策略

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "RAM": [
          "acs:ram::151266687691****:root"  //151266687691****为管理账号ID。
        ]
      }
    }
  ],
  "Version": "1"
}
```

创建角色

系统会在以下场景中自动在成员内创建RAM角色（ResourceDirectoryAccountAccessRole）：

- 成员创建成功后，在成员内创建该RAM角色。
- 被邀请账号成功加入资源目录后，在被邀请账号内创建该RAM角色。

删除角色

从资源目录中移除成员时，系统将自动删除成员内的RAM角色（ResourceDirectoryAccountAccessRole）。

当RAM角色（ResourceDirectoryAccountAccessRole）下没有任何授权时，您也可以手动删除该服务关联角色。具体操作，请参见删除RAM角色。

AliyunServiceRoleFor***

应用场景

服务关联角色（AliyunServiceRoleFor***）用于可信服务执行预定任务，解决可信服务与资源目录之间的跨服务访问问题。关于服务关联角色的更多信息，请参见服务关联角色。

> **说明** AliyunServiceRoleFor***中的***表示可信服务，例如：配置审计的服务关联角色AliyunServiceRoleForConfig。

权限策略

权限策略由可信服务制定，一般包含以下两类权限：

- 可信服务执行预定任务所需的云服务操作权限。
- 可信服务删除该服务关联角色的权限。

信任策略

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "***.aliyuncs.com"  //***表示可信服务，例如：config.aliyuncs.com。
        ]
      }
    }
  ],
  "Version": "1"
}
```

创建角色

启用某个可信服务时，资源目录通过服务关联角色（AliyunServiceRoleForResourceDirectory）在成员中创建服务关联角色（AliyunServiceRoleFor***）。

删除角色

从资源目录移除成员时，资源目录会广播该消息给可信服务，可信服务会自主决定是否联动删除服务关联角色（AliyunServiceRoleFor***）。一般情况下，可信服务会自动删除该服务关联角色。但某种特定情况下可能不会自动删除，此时，您可以登入成员，尝试手动删除该服务关联角色。具体操作，请参见删除RAM角色。

2.2. 管理资源夹

2.2.1. 创建资源夹

资源夹是资源目录中的组织单元。使用资源夹，您可以构建资源组织结构。

背景信息

资源夹下可以创建子资源夹，最多支持创建5级资源夹。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**资源组织**页签。
4. 在左侧的Root资源夹下，选择目标资源夹，然后在右侧的页面中单击**创建资源夹**。

   您将会在目标资源夹下创建一个子资源夹。
5. 在**创建资源夹**面板，填写**资源夹名称**。

   > **说明** 资源夹名称在资源目录内必须唯一。
6. 单击**确定**。

后续步骤

您可以在资源夹中创建成员，对成员进行统一管理。具体操作，请参见创建成员。

2.2.2. 查看资源夹基本信息

本文为您介绍如何查看资源夹的基本信息，包括资源夹名称、资源夹ID、资源夹创建时间、资源夹在资源目录中的路径ID（RDPath）和资源夹内的成员列表。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**资源组织**页签。
4. 在Root资源夹下，找到目标资源夹，查看资源夹基本信息，包括资源夹名称、资源夹ID、资源夹创建时间、资源夹RDPath和资源夹内的成员列表。

   > **说明** 关于RDPath的含义，请参见基本概念。

2.2.3. 修改资源夹名称

本文为您介绍如何修改资源夹名称。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**资源组织**页签。
4. 在Root资源夹下，单击目标资源夹。
5. 在右侧的资源夹页面，将鼠标悬停在资源夹名称上，单击图标。

6. 修改资源夹名称，然后单击**确定**。

> **说明** 资源夹名称在资源目录内必须唯一。

2.2.4. 删除资源夹

当资源夹下不存在任何成员和子资源夹时，可以将其删除。资源夹删除后不可恢复，请慎重操作。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**资源组织**页签。
4. 在**Root**资源夹下，找到目标资源夹。
5. 在右侧的资源夹页面，单击**删除资源夹**。

> **说明** 当资源夹下不存在任何成员和子资源夹时，才会显示**删除资源夹**按钮。

6. 在**删除资源夹**对话框，单击**确定**。

2.3. 管理成员

2.3.1. 创建成员

成员是资源目录中的资源容器，可以将资源进行物理隔离，形成独立的资源分组单元。您可以在资源夹中创建成员，对成员进行统一管理。

背景信息

- 资源目录已全面支持金融云账号开通使用，新创建的成员将自动继承金融云业务标签。
- 关于创建成员的数量限制，请参见资源目录使用限制。
- 创建成员的入口存在以下几种：
  - 选择**资源目录 > 概览**，在**资源组织**页签，先创建资源夹，然后在对应资源夹下创建成员。本文将介绍这种方式。
  - 选择**资源目录 > 概览**，在**成员列表**页签，直接创建成员。创建的成员默认归属于Root资源夹，您需要将成员移动到对应资源夹。关于如何移动成员的操作，请参见移动成员。
  - 选择**资源目录 > 创建成员**，直接创建成员。创建的成员默认归属于Root资源夹，您需要将成员移动到对应资源夹。关于如何移动成员的操作，请参见移动成员。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 在**资源组织**页签，单击目标资源夹。
4. 单击**创建成员**。
5. 在**创建成员**页面，输入**阿里云账号名称**。

阿里云账号名称是成员的唯一标识，在资源目录内必须唯一。阿里云账号名称长度为2~50个字符，允许输入英文字母、数字和特殊字符 `_.-` ，必须以英文字母或数字开头和结尾，且不能输入连续的特殊字符 `_.-` 。

6. 在**创建成员**页面，输入**显示名**。

   显示名长度为2~50个字符或汉字，允许输入汉字、英文字母、数字和特殊字符 `_.-` 。

7. 选择**结算账号**。
   - **使用管理账号为新成员付款**：指定资源目录的管理账号作为托管结算账号。
   - **使用已有成员为新成员付款**：指定资源目录的已有成员作为托管结算账号。您需要在**指定一个成员**面板中，从资源目录的目录树中选择一个成员。

     > **说明**
     >
     > 若成员不具备付款能力则无法被选中。关于如何判断成员是否具备付款能力，请参见财务托管业务须知。

   - **新成员自主付款**：指定当前成员作为结算账号。
8. 单击**确定**。

> **说明** 资源目录内创建的成员将继承管理账号的法律实体，即成员的实名认证信息与管理账号的一致。

执行结果

创建成员成功后，资源目录会对成员进行统一管理：

- 资源目录会自动为成员开通访问控制（RAM）服务。
- 资源目录会自动为成员创建RAM角色（ResourceDirectoryAccountAccessRole），授权给资源目录的管理账号进行统一管理。
- 每个成员仅归属于一个资源夹，管理账号可以根据需要移动成员到资源目录内的其他资源夹。成员位置改变后，成员下的资源也随之移动到新的资源夹。

2.3.2. 邀请成员

2.3.2.1. 邀请阿里云账号加入资源目录

您可以邀请资源目录以外的阿里云账号加入到资源目录，作为资源目录的成员，实现资源的统一管理。

前提条件

发起邀请前，请确认以下事项：

- 请确保被邀请方不存在待确认状态的邀请记录，否则不能被再次邀请。
- 请确保每日邀请数量不超过20个，否则不能发起邀请。
- 请确保处于**等待确认**状态的邀请数量不超过20个，否则不能发起邀请。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 邀请成员**。

3. 单击**邀请成员**。
4. 填写目标成员的阿里云账号UID或登录邮箱。

   > **说明** 此处邮箱是注册账号时的登录邮箱，而非注册账号后绑定的备用邮箱。您可以一次性输入多个阿里云账号实现批量邀请，使用英文逗号（,）分隔。

5. 填写**备注**。

   > **说明** 您需要合理填写邀请备注，便于被邀请方确认邀请行为的可信性，使流程快速完成。

6. 确认并选中风险提示框。
7. 单击**确定**。

   > **说明**
   > - 若您邀请账号时填写的是邮箱，系统会向您指定的邮箱发送确认邮件。
   > - 若您邀请账号时填写的是账号UID，系统会向账号关联的邮箱发送确认邮件。
   > - 若您邀请账号时填写的是账号UID但账号无关联邮箱，被邀请方可以登录资源管理控制台查看并处理邀请。

执行结果

被邀请方成功加入资源目录后，会作为资源目录的成员，由资源目录统一管理：

- 被邀请的阿里云账号名称将默认作为资源目录内该成员的成员名称和账号名称。管理账号可以修改该成员的成员名称，但不能修改账号名称。
- 资源目录会为该成员自动创建RAM角色（ResourceDirectoryAccountAccessRole），授权给资源目录的管理账号进行统一管理。
- 管理账号可以调整该成员在资源目录中的位置。

2.3.2.2. 邀请方查看邀请信息

发送邀请后，您可以通过资源管理控制台查看发出的邀请信息，包括邀请ID、邀请的账号UID、邀请时间及当前状态等信息。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 邀请成员**。
3. 查看邀请账号的相关信息。
   - **邀请ID**：系统随机发放的ID。
   - **邀请的账号UID/账号登录邮箱**：系统会根据您邀请账号时填写的内容显示阿里云账号UID或登录邮箱。
   - **邀请时间**：发起邀请的时间。
   - **过期时间**：邀请发起后有效期为14天，超出有效期邀请将失效。
   - **当前状态**：发起邀请后，有**等待确认**、**已取消**、**已接受**、**已拒绝**和**已超时**几种状态。
   - **备注**：发起邀请时，填写的备注信息。

- **操作**：发起邀请后，单击**取消邀请**可以撤销**等待确认**状态的邀请。

> **说明** 系统会在30天后自动删除无效的邀请记录，无需手动操作。

2.3.2.3. 被邀请方处理邀请

被邀请方收到邀请后，可以通过资源管理控制台或邀请邮件查阅邀请信息，然后评估加入资源目录将产生的影响，最后选择接受或拒绝邀请。

前提条件

- 请确保被邀请方未加入任何资源目录，一个阿里云账号只能加入一个资源目录。
- 请确保被邀请方已完成企业实名认证，没有实名认证的账号和个人实名认证账号都不能加入资源目录。具体操作，请参见企业实名认证。
- 如果被邀请方想使用RAM用户处理邀请，则该RAM用户必须具备的最小权限策略如下：

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resourcemanager:GetResourceDirectory",
                "resourcemanager:ListHandshakesForAccount",
                "resourcemanager:GetHandshake",
                "resourcemanager:AcceptHandshake",
                "resourcemanager:DeclineHandshake"
            ],
            "Resource": "*"
        }
    ]
}
```

具体操作，请参见创建自定义权限策略和为RAM用户授权。

背景信息

被邀请方处理邀请时，请仔细阅读接受邀请将产生的以下影响，确认安全后再选择是否加入资源目录。

- 被邀请方加入资源目录后，会成为资源目录中云账号类型的成员，被邀请方的阿里云账号名称将会成为资源目录中该成员的显示名称。
- 资源目录的管理账号将获得被邀请方阿里云账号的全部权限，且该账号将无法主动退出资源目录。
- 资源目录的管理账号基于组织安全或合规等考虑，可以通过管控策略控制成员允许访问的云服务和API。
- 资源目录的管理账号或委派管理员账号，可以在资源目录的可信服务中对成员执行特定的管理操作。例如：在操作审计中查看成员的日志数据，在资源编排中为成员一键部署云资源。更多信息，参见可信服务概述。
- 如果被邀请方的企业实名信息与资源目录的管理账号相同，管理账号可以将成员类型由云账号切换为资源账号。否则，将不允许切换类型。

接受邀请

1. 登录资源管理控制台。

2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**查看邀请**。
4. 在**操作**列，单击**处理邀请**。
5. 在**处理邀请**对话框，仔细阅读邀请信息，然后选中风险提示框，最后单击**接受邀请**。
   被邀请方成功加入资源目录后，可以在资源目录的**设置**页面，查看到资源目录相关信息。

拒绝邀请

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**查看邀请**。
4. 在**操作**列，单击**处理邀请**。
5. 在**处理邀请**对话框，单击**拒绝邀请**。
6. 在**拒绝邀请**对话框，单击**拒绝邀请**。

2.3.3. 查看成员详情

本文为您介绍如何查看成员详情，包括成员类型、成员名称、账号名称、账号UID、实名信息、结算账号、状态和成员在资源目录中的路径ID（RDPath）。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**资源组织**或**成员列表**页签。
4. 在成员列表中，单击目标成员名称。
5. 在**成员详情**面板，查看成员的详细信息，包括成员类型、成员名称、账号名称、账号UID、实名信息、结算账号、状态和成员RDPath。

> **说明** 关于RDPath的含义，请参见基本概念。

2.3.4. 修改成员显示名称

本文为您介绍如何修改成员显示名称。成员显示名称在资源目录内必须唯一。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**资源组织**或**成员列表**页签，在成员列表中，单击目标成员显示名称。
4. 将鼠标悬浮在成员显示名称上，单击编辑图标。
5. 修改成员显示名称，然后单击**确定**。

2.3.5. 移动成员

资源目录允许将成员从当前资源夹移动到另一个资源夹，调整账号及其下资源的分配情况，以满足企业的业务需求。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**资源组织**或**成员列表**页签。
4. 在成员列表中，单击目标成员**操作**列的**移动**。
5. 在**成员移动**面板，选择目标资源夹，然后单击**确定**。

执行结果

您可以在目标资源夹中查看移动成功的成员。

2.3.6. 访问成员

您可以通过RAM角色、RAM用户或根用户访问成员。为安全起见，建议通过RAM角色或RAM用户访问成员，不建议通过根用户发起访问。

通过RAM角色访问成员

资源目录会自动为成员创建RAM角色（ResourceDirectoryAccountAccessRole），并将该角色的可信实体设置为资源目录的管理账号，这使得管理账号拥有对成员进行角色扮演并访问的权限。您可以使用管理账号的RAM用户扮演资源目录成员的RAM角色（ResourceDirectoryAccountAccessRole），实现对该成员的访问。

1. 使用管理账号创建RAM用户。

   本示例中使用的RAM用户名为Alice。具体操作，请参见创建RAM用户。

2. 为RAM用户（Alice）授权。

   您需要为RAM用户（Alice）至少授予以下权限：

   - AliyunSTSAssumeRoleAccess：调用STS服务AssumeRole接口的权限。
   - AliyunResourceDirectoryFullAccess：管理资源目录服务（ResourceDirectory）的权限。

     > **说明** 如果该RAM用户（Alice）用作管理员，您也可以直接授予AdministratorAccess权限。

   具体操作，请参见为RAM用户授权。

3. 使用RAM用户（Alice）登录资源管理控制台。
4. 在左侧导航栏，选择**资源目录 > 概览**。
5. 单击**资源组织**或**成员列表**页签。
6. 在成员列表中，单击目标成员**操作**列的**登入账号**。

   登录之后，管理账号的RAM用户（Alice）将扮演目标成员的RAM角色（ResourceDirectoryAccountAccessRole），进行角色（ResourceDirectoryAccountAccessRole）定义范围内的操作。

通过RAM用户访问成员

您可以为成员创建RAM用户，使用RAM用户身份登录并访问成员。

1. 使用管理账号的RAM用户通过RAM角色扮演的方式访问成员。

具体操作，请参见通过RAM角色访问成员。

2. 为成员创建RAM用户。

   本示例中使用的RAM用户名为Tom。具体操作，请参见创建RAM用户。

3. 为RAM用户（Tom）授权。

   如果要访问成员的所有资源，授予AdministratorAccess权限。其他情况，请根据需要授予合适的权限。具体操作，请参见为RAM用户授权。

4. 使用RAM用户（Tom）登录控制台。

   具体操作，请参见RAM用户登录阿里云控制台。

通过根用户访问成员

对于云账号类型的成员，您可以通过根用户身份登录并访问成员。

> **说明** 为安全起见，不建议通过根用户登录并访问成员。

1. 登录阿里云控制台。

   > **说明** 如果您有其他账号已登录阿里云，请先退出后再重新登录。

2. 输入账号和登录密码。
3. 单击**登录**。

2.3.7. 为资源账号设置安全手机号码

安全手机号码常用于核实阿里云上用户身份和接收重要变更通知，例如：密码找回、实例释放和资费变更等。本文为您介绍如何为资源账号类型的成员设置安全手机号码。

前提条件

为确保系统可以记录到管理操作的具体操作者，请使用管理账号下具有资源目录管理权限（AliyunResourceDirectoryFullAccess）的RAM用户或RAM角色执行本操作。

使用限制

- 不支持为云账号类型的成员设置安全手机号码。如您需要，请访问安全设置进行设置。
- 本文所述操作仅适用于首次设置资源账号安全手机号码的场景，不能用于修改已有的安全手机号码。
- 每天最多发送100次验证码。

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**资源组织**或**成员列表**页签。
4. 在成员列表中，单击目标资源账号**操作**列的**绑定安全手机**。
5. 在**绑定安全手机**对话框，输入安全手机号码，然后获取并输入验证码。
6. 单击**确定**。

2.3.8. 资源账号切换为云账号

当您遇到必须使用根用户才能操作的业务场景时，您可以将资源账号切换为云账号。操作完成后，建议您及时将云账号切换回资源账号，以确保安全。

前提条件

- 为确保系统可以记录到管理操作的具体操作者，请使用管理账号下具有资源目录管理权限（AliyunResourceDirectoryFullAccess）的RAM用户或RAM角色执行本操作。
- 请确保已为资源账号设置了安全手机号码，否则，不能将其切换为云账号。具体操作，请参见为资源账号设置安全手机号码。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**资源组织**或**成员列表**页签。
4. 在成员列表中，单击目标成员**操作**列的**切换为云账号**。
5. 在**切换为云账号**对话框，阅读风险提示并选中风险提示框，然后单击**确定**。

执行结果

切换成功后，该成员的根用户登录权限将被启用。

您可以通过密码找回功能设置登录密码，然后登录阿里云控制台。如果您之前设置过根用户登录密码，您可以继续使用，不用重新设置。

启用根用户后将会增加账号安全风险，请谨慎保管根用户的账号和密码，以防泄露。

2.3.9. 云账号切换为资源账号

企业邀请外部阿里云账号加入资源目录后，该阿里云账号将成为资源目录内的云账号类型成员。阿里云账号默认开启根用户并拥有完全权限，一旦根用户账密泄露，将导致无法挽回的损失。为确保安全，建议您将其切换为资源账号。

前提条件

- 为确保系统可以记录到管理操作的具体操作者，请使用管理账号下具有资源目录管理权限（AliyunResourceDirectoryFullAccess）的RAM用户或RAM角色执行本操作。
- 需要切换的云账号类型成员同时满足以下条件时，才允许将其切换为资源账号：
  - 成员的实名信息必须与管理账号的一致。
  - 成员已设置安全信息（安全手机号码或邮箱）。
  - 成员中不存在已启用状态的阿里云账号（主账号）访问密钥（AccessKey）。

    如果存在，请通过AccessKey管理禁用该访问密钥（AccessKey）。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**资源组织**或**成员列表**页签。
4. 在成员列表中，单击目标云账号**操作**列的**切换为资源账号**。
5. 在**切换为资源账号**对话框，阅读风险提示并选中风险提示框，然后单击**确定**。

6. 在**安全校验**对话框，获取并输入验证码，然后单击**确定**。

执行结果

切换成功后，该成员的根用户登录权限将被禁用。您可以通过资源目录的管理账号创建RAM用户并授予最小权限统一访问该成员。

2.3.10. 移除云账号类型的成员

您可以从资源目录中移除云账号类型的成员。

前提条件

如果成员是可信服务的委派管理员，则不能直接从资源目录中移除，您需要先移除委派管理员。具体操作，请参见移除委派管理员账号。

背景信息

资源账号是资源目录管理账号创建的资源容器，仅限于在资源目录内安全使用，您无法从资源目录内移除资源账号类型的成员。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 概览**。
3. 单击**资源组织**或**成员列表**页签。
4. 在成员列表中，单击目标云账号**操作**列的**移除**。
5. 在**移除**对话框，单击**确定**。
   移除成功后，将产生以下影响：
   - 该成员将作为独立的阿里云账号存在，不再被资源目录的管理账号管控，也不再受到资源目录任何管控策略的影响。
   - 该成员的付款关系不会发生变化，如需更新当前账号的付款关系，请至财务系统处理。更多信息，请参见企业财务。

2.4. 管理管控策略

2.4.1. 管控策略概述

资源目录管控策略是一种基于资源结构（资源夹或成员）的访问控制策略，可以统一管理资源目录各层级内资源访问的权限边界，建立企业整体访问控制原则或局部专用原则。管控策略只定义权限边界，并不真正授予权限，您还需要在某个成员中使用访问控制（RAM）设置权限后，相应身份才具备对资源的访问权限。

应用场景

当企业创建了一个资源目录，并为每个部门创建了成员后，如果对各成员的行为不加以管控，就会破坏运维规则，带来安全风险和成本浪费。资源目录提供管控策略功能，企业可以通过管理账号集中制定管理规则，并将这些管理规则应用于资源目录的各级资源结构（资源夹、成员）上，管控各成员内资源的访问规则，确保安全合规和成本可控。例如：禁止成员申请域名、禁止成员删除日志记录等。

管控策略类型

- **系统管控策略**

  系统自带的管控策略。您只能查看，不能创建、修改和删除系统管控策略。开启管控策略功能后，资源目录内所有的资源夹和成员默认绑定了系统策略FullAliyunAccess，该策略允许对您在阿里云上的所有资源进行任何操作。

- **自定义管控策略**

  用户自定义的管控策略。您可以创建、修改和删除自定义管控策略。自定义管控策略创建成功后，您需要将自定义管控策略绑定到资源夹或成员上，才能生效。不需要时，也可以随时解绑。

工作原理

管控策略的工作原理如下：

1. 使用管理账号开启管控策略功能。更多信息，请参见开启管控策略功能。

   开启管控策略功能后，系统策略FullAliyunAccess将默认绑定到资源目录内的所有资源夹及成员，此策略允许所有操作，以防止管控策略的不当配置造成意料之外的访问失败。

2. 使用管理账号创建管控策略。更多信息，请参见创建自定义管控策略。
3. 使用管理账号将管控策略绑定到资源目录节点（资源夹、成员）。更多信息，请参见绑定自定义管控策略。

   管控策略允许绑定到资源目录中的任何资源夹或成员。管控策略具备向下继承的特点，例如：为父资源夹设置管控策略A，为子资源夹设置管控策略B，则管控策略A和管控策略B都会在子资源夹及其下的成员中生效。

   > **说明** 请先进行局部小范围测试，确保策略的有效性与预期一致，然后再绑定到全部目标节点（资源夹、成员）。

4. 当成员中的RAM用户或RAM角色访问阿里云服务时，阿里云将会先进行管控策略检查，再进行账号内的RAM权限检查。具体如下：
   - 管控策略鉴权从被访问资源所在账号开始，沿着资源目录层级逐级向上进行。
   - 在任一层级进行管控策略鉴权时，命中拒绝（Deny）策略时都可以直接判定结果为拒绝（Explicit Deny），结束整个管控策略鉴权流程，并且不再进行账号内基于RAM权限策略的鉴权，直接拒绝请求。
   - 在任一层级进行管控策略鉴权时，如果既未命中拒绝（Deny）策略，也未命中允许（Allow）策略，同样直接判定结果为拒绝（Explicit Deny），不再进入下一个层级鉴权，结束整个管控策略鉴权流程，并且不再进行账号内基于RAM权限策略的鉴权，直接拒绝请求。
   - 在某一层级鉴权中，如果未命中拒绝（Deny）策略，而命中了允许（Allow）策略，则本层级鉴权通过，继续在父节点上进行管控策略鉴权，直至Root资源夹为止。如果Root资源夹鉴权结果也为通过，则整个管控策略鉴权通过，接下来进入账号内基于RAM权限策略的鉴权。更多信息，请参见权限策略判定流程。
   - 管控策略对服务关联角色不生效。关于服务关联角色的详情，请参见服务关联角色。
   - 阿里云将会评估被访问的账号自身及其所在的每一层级上绑定的管控策略，从而确保绑定在较高层级上的管控策略可以在其下的所有账号上生效。

   > **说明** RD管控策略对所有资源账号以及云账号中的RAM用户和RAM角色生效，但对云账号的根用户不生效。

避免指定云服务访问被管控

管控策略将对被管控成员中的资源访问权限限定边界，边界之外的权限将不允许生效，此限定同样影响阿里云服务对该成员访问的有效性。

阿里云服务可能使用服务角色访问您账号中的资源，以实现云服务的某些功能。当一个服务角色的权限超过管控策略的边界时，此权限会受到管控策略的约束，这可能导致云服务的某些功能不能正常使用。如果这正是您配置管控策略期望的结果，则无需进行其他额外操作，但是，如果您不希望这些云服务被管控，您可以采用以下方法进行处理：

1. 确认您不希望被管控的云服务所使用的服务角色名称。

   您可以登录RAM控制台，查看账号下的所有服务角色。

2. 在造成管控效果的管控策略中增加 `Condition key: "acs:PrincipalArn"` 的条件，将受影响的云服务所使用的服务角色名称写入到 `PrincipalArn` 字段，以避免该服务角色被误管控。示例如下：

```
{
    "Statement": [
        {
            "Action": [
                "ram:UpdateUser"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN":"acs:ram:*:*:role/<服务角色名称>"
                }
            }
        }
    ],
    "Version": "1"
}
```

   关于管控策略的语法，请参见管控策略语言。

使用限制

限制项	最大值
资源目录内最多允许创建自定义管控策略的数量	1500个
每个节点（资源夹、成员）最多允许绑定自定义管控策略的数量	10个
每个自定义策略的最大长度	4096个字符

暂不支持管控策略的云服务

以下云服务暂不支持管控策略，请您注意管控风险。如需涉及对以下云服务的管控，请联系阿里云资源目录的服务经理。

- 微服务引擎MSE暂不支持管控策略。
- 消息队列RocketMQ版的以下应用或集群暂不支持管控策略。
  - 应用mq-http即将下线，不支持管控策略。

- 应用onsbroker在以下地域，暂不支持管控策略。
  - 阿联酋（迪拜）
  - 华东2（上海）：sh-share9集群、shvip-st21ujm8f01集群。
  - 政务云：beijing.gov.vip.v0h0ovmfp02、beijing.gov.vip.nif1zmrlf02即将下线，不支持管控策略；vip-cn-north-2-gov-1-45914plw301集群暂不支持管控策略。

2.4.2. 开启管控策略功能

管控策略功能默认关闭，您需要开启后才能使用。

背景信息

开启管控策略功能后，资源目录的变化如下：

- 资源目录内的资源夹和成员会默认绑定系统策略FullAliyunAccess，该策略允许对您在阿里云上的所有资源进行任何操作。
- 当创建资源夹或成员时，系统会自动为其绑定系统策略FullAliyunAccess。
- 当邀请的阿里云账号加入资源目录后，系统会自动为其绑定系统策略FullAliyunAccess。
- 当移除成员时，该成员绑定的所有管控策略将会自动解绑。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 管控策略**。
3. 单击**开启管控策略**。
4. 单击**确定**。
5. 单击**刷新**，查看开启状态。

后续步骤

您可以创建自定义管控策略（例如：禁止对某资源的某个操作），然后绑定到资源目录的资源夹或成员，限制成员对资源的操作权限。操作方法请参见：

- 创建自定义管控策略
- 绑定自定义管控策略

2.4.3. 查看管控策略详情

您可以查看管控策略名称、策略类型、策略内容和绑定目标等。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 管控策略**。
3. 在**策略列表**页签，单击**操作**列的**查看**。
   - 在**策略详情**区域，查看**策略名称**、**策略类型**、**策略ID**、**最后更新时间**和**策略描述**。
   - 在**策略JSON**页签，查看策略内容。
   - 在**策略目标**页签，查看策略绑定的资源夹或成员。

> **说明** 您也可以在**策略绑定**页签，基于树形组织结构，查看资源夹和成员绑定的管控策略列表及详情。

2.4.4. 关闭管控策略功能

如果您不想限制资源目录内资源夹和成员的权限，则可以关闭管控策略功能。

背景信息

关闭管控策略功能后，您绑定到资源夹和成员上的管控策略会全部自动解绑。但管控策略本身不会被删除，只是不能再绑定到任何目标对象上。

> **说明** 关闭管控策略将会影响整个资源目录内资源夹和成员的权限，请谨慎操作。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 管控策略**。
3. 在**管控策略**页面上方的文字描述区域，单击**关闭管控策略**。
4. 单击**确定**。
5. 单击**刷新**，查看关闭状态。

   当状态显示**管控策略已关闭**时，表示管控策略功能已关闭。

> **说明** 您也可以单击**开启管控策略**，重新开启管控策略功能。开启成功后，默认系统管控策略FullAliyunAccess会自动绑定到资源夹和成员上，但其他自定义管控策略需要您重新绑定。

2.4.5. 管控策略语言

创建或更新自定义管控策略前，您需要了解管控策略的基本元素。管控策略由效果（Effect）、操作（Action）、资源（Resource）和条件（Condition）四个基本元素组成。

元素名称	描述
效果（Effect）	授权效果包括两种：允许（Allow）和拒绝（Deny）。
操作（Action）	操作是指对具体资源的操作。
资源（Resource）	资源是指被授权的具体对象。
条件（Condition）	条件是指授权生效的条件。

效果（Effect）

- 取值：允许（Allow）或拒绝（Deny）。

> **说明** 当权限策略中既有允许（Allow）又有拒绝（Deny）的授权语句时，遵循Deny优先的原则。

- 样例：`"Effect": "Allow"`。

操作（Action）

- 取值：云服务所定义的API操作名称。支持多值。

> **说明** 多数情况下操作与云服务的API一一对应，但也有例外。更多信息，请参见各云服务的帮助文档。

- 格式：`<ram-code>:<action-name>`。
  - `ram-code`：云服务的RAM代码。更多信息，请参见支持RAM的云服务的**RAM代码**列。
  - `action-name`：相关的API操作接口名称。
- 样例：`"Action": ["oss:ListBuckets", "ecs:Describe*", "rds:Describe*"]`。

> **说明** 微服务引擎MSE暂不支持管控策略。更多信息，请参见暂不支持管控策略的云服务。

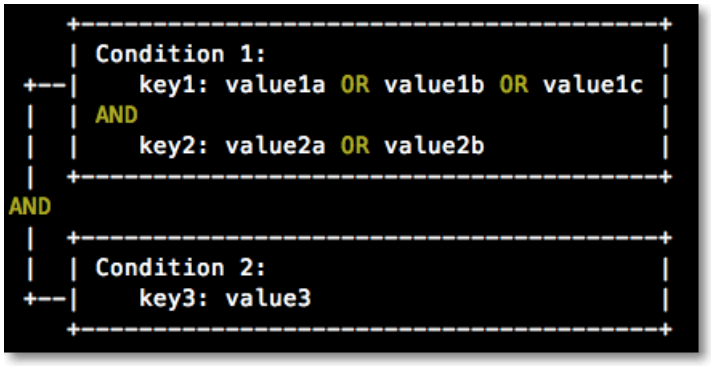
资源（Resource）

- 取值：资源ARN（Aliyun Resource Name）。支持多值。
- 格式：遵循阿里云ARN统一规范，为`acs:<ram-code>:<region>:<account-id>:<relative-id>`。
  - `acs`：Alibaba Cloud Service的首字母缩写，表示阿里云的公共云平台。
  - `ram-code`：云服务RAM代码。更多信息，请参见支持RAM的云服务的**RAM代码**列。
  - `region`：地域信息。对于全局资源（无需指定地域就可以访问的资源），该字段置空。更多信息，请参见地域和可用区。
  - `account-id`：阿里云账号ID。例如：`123456789012****`。
  - `relative-id`：与服务相关的资源描述部分，其语义由具体云服务指定。这部分的格式支持树状结构（类似文件路径）。以OSS为例，表示一个OSS对象的格式为：`relative-id = “mybucket/dir1/object1.jpg”`。
- 样例：`"Resource": ["acs:ecs:*:*:instance/inst-001", "acs:ecs:*:*:instance/inst-002", "acs:oss:*:*:mybucket", "acs:oss:*:*:mybucket/*"]`。

> **说明** 微服务引擎MSE暂不支持管控策略。更多信息，请参见暂不支持管控策略的云服务。

条件（Condition）

条件块（Condition Block）由一个或多个条件子句构成。一个条件子句由条件操作类型、条件关键字和条件值组成。



- 逻辑说明
  - 条件满足：一个条件关键字可以指定一个或多个值，在条件检查时，如果条件关键字的值与指定值中的某一个相同，即可判定条件满足。
  - 条件子句满足：同一条件操作类型的条件子句下，若有多个条件关键字，所有条件关键字必须同时满足，才能判定该条件子句满足。
  - 条件块满足：条件块下的所有条件子句同时满足的情况下，才能判定该条件块满足。
- 条件操作类型

  条件操作类型包括：字符串类型（String）、数字类型（Number）、日期类型（Date and time）、布尔类型（Boolean）和IP地址类型（IP address）。

条件操作类型	支持类型
字符串类型（String）	○ StringEquals ○ StringNotEquals ○ StringEqualsIgnoreCase ○ StringNotEqualsIgnoreCase ○ StringLike ○ StringNotLike
数字类型（Number）	○ NumericEquals ○ NumericNotEquals ○ NumericLessThan ○ NumericLessThanEquals ○ NumericGreaterThan ○ NumericGreaterThanEquals
日期类型（Date and time）	○ DateEquals ○ DateNotEquals ○ DateLessThan ○ DateLessThanEquals ○ DateGreaterThan ○ DateGreaterThanEquals

条件操作类型	支持类型
布尔类型（Boolean）	Bool
IP地址类型（IP address）	○ IpAddress ○ NotIpAddress

- 条件关键字
  - 阿里云通用条件关键字命名格式：`acs:<condition-key>`。

通用条件关键字	类型	描述
`acs:CurrentTime`	Date and time	Web Server接收到请求的时间。以ISO 8601格式表示，例如：`2012-11-11T23:59:59Z`。
`acs:SecureTransport`	Boolean	发送请求是否使用了安全信道。例如：HTTPS。
`acs:SourceIp`	IP address	发送请求时的客户端IP地址。 **说明** `acs:SourceIp` 的取值如果是单个IP地址，需要写明具体的IP地址，不能使用该IP地址的IP地址段形式xx.xx.xx.xx/32。例如：10.0.0.1不能写成10.0.0.1/32。
`acs:MFAPresent`	Boolean	用户登录时是否使用了多因素认证。

通用条件关键字	类型	描述
acs:PrincipalARN	String	仅限资源目录管控策略中使用，用于表示操作执行者的身份。例如：acs:ram:*:*:role/*resourcedirectory*。 说明 目前，只支持指定RAM角色的ARN，且必须为小写英文字母。（您可以在RAM控制台的角色详情页面查看RAM角色的ARN）。

- 阿里云服务级别条件关键字命名格式：<ram-code>:<condition-key>。

服务级别条件关键字	云服务名称	类型	描述
ecs:tag/<tag-key>	ECS	String	ECS资源的标签关键字，可自定义。 说明 <tag-key>为标签键，请在使用时替换为实际值。
rds:ResourceTag/<tag-key>	RDS	String	RDS资源的标签关键字，可自定义。 说明 <tag-key>为标签键，请在使用时替换为实际值。
oss:Delimiter	OSS	String	OSS对Object名字进行分组的分隔符。
oss:Prefix	OSS	String	OSS Object名称的前缀。

相关文档

管控策略语法和结构与RAM的基本相同。更多信息，请参见权限策略语法和结构。

2.4.6. 管理自定义管控策略

2.4.6.1. 创建自定义管控策略

您可以创建自定义管控策略，限制对某些资源执行某些操作，为资源目录内的资源夹和成员定义权限边界。

创建方式

- 通过可视化编辑模式创建自定义管控策略

  系统提供所见即所得的可视化编辑界面，您只需选择效果、云服务、操作、资源和条件，就可以生成自定义管控策略。同时，提供的智能校验功能，帮助您提高管控策略的正确性和有效性。该方式操作简单，易于上手。

- 通过脚本编辑模式创建自定义管控策略

  系统提供JSON脚本编辑界面，您需要按照管控策略语法和结构编写自定义管控策略。该方式使用灵活，适用于对管控策略语法比较熟悉的用户。

通过可视化编辑模式创建自定义管控策略

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 管控策略**。
3. 在**策略列表**页签，单击**创建策略**。
4. 在**创建策略**页面，单击**可视化编辑**页签。
5. 配置管控策略，然后单击**下一步：编辑基本信息**。
   i. 在**效果**区域，选择**允许**或**拒绝**。
   ii. 在**服务**区域，选择云服务。

   > **说明** 支持可视化编辑模式的云服务以控制台界面显示为准。

   iii. 在**操作**区域，选择**全部操作**或**指定操作**。

   系统会根据您上一步选择的云服务，自动筛选出可以配置的操作。如果您选择了**指定操作**，您需要继续选择具体的操作。

   iv. 在**资源**区域，选择**全部资源**或**指定资源**。

   系统会根据您上一步选择的操作，自动筛选出可以配置的资源类型。如果您选择了**指定资源**，您需要继续单击**添加资源**，配置具体的资源ARN。您可以使用**匹配全部**功能，快速选择对应配置项的全部资源。

   > **说明** 为了管控策略的正常生效，对操作关联的必要资源ARN标识了**必要**，强烈建议您配置该资源ARN。

   v. （可选）在**条件**区域，单击**添加条件**，配置条件。

   条件包括阿里云通用条件和服务级条件，系统会根据您前面配置的云服务和操作，自动筛选出可以配置的条件列表。您只需要选择对应条件键配置具体内容。

   vi. 单击**添加语句**，重复上述步骤，配置多条管控策略语句。
6. 输入管控策略**名称**和**备注**。
7. 检查并优化管控策略内容。
   - 基础策略优化

     系统会对您添加的策略语句自动进行基础优化。基础策略优化功能会完成以下任务：

     - 删除不必要的条件。
     - 删除不必要的数组。

- （可选）高级策略优化

  您可以将鼠标悬浮在**可选：高级策略优化**上，单击**执行**，对策略内容进行高级优化。高级策略优化功能会完成以下任务：

  - 拆分不兼容操作的资源或条件。
  - 收缩资源到更小范围。
  - 去重或合并语句。

8. 单击**确定**。

通过脚本编辑模式创建自定义管控策略

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 管控策略**。
3. 在**策略列表**页签，单击**创建策略**。
4. 在**创建策略**页面，单击**脚本编辑**页签。
5. 输入管控策略内容，然后单击**下一步：编辑基本信息**。

   关于管控策略语法结构的详情，请参见管控策略语言。
6. 输入管控策略**名称**和**备注**。
7. 检查并优化管控策略内容。
   - 基础策略优化

     系统会对您添加的策略语句自动进行基础优化。基础策略优化功能会完成以下任务：

     - 删除不必要的条件。
     - 删除不必要的数组。
   - （可选）高级策略优化

     您可以将鼠标悬浮在**可选：高级策略优化**上，单击**执行**，对策略内容进行高级优化。高级策略优化功能会完成以下任务：

     - 拆分不兼容操作的资源或条件。
     - 收缩资源到更小范围。
     - 去重或合并语句。

后续步骤

自定义管控策略创建成功后，需要绑定到资源夹或成员才能生效。具体操作，请参见绑定自定义管控策略。

2.4.6.2. 修改自定义管控策略

您可以根据需要修改自定义管控策略的名称、描述和内容。如果您修改了管控策略内容，则会在绑定了该管控策略的资源夹和成员上立即生效。

背景信息

系统管控策略不支持修改。

操作步骤

1. 登录资源管理控制台。

2. 在左侧导航栏，选择**资源目录 > 管控策略**。
3. 在**策略列表**页签，单击目标管控策略名称。
4. 在**策略详情**页面的右上角，单击**编辑策略**。
5. 通过可视化编辑模式或脚本编辑模式修改管控策略内容，然后单击**下一步：编辑基本信息**。

   具体操作，请参见创建自定义管控策略。
6. 修改**名称**和**备注**，然后单击**确定**。

2.4.6.3. 删除自定义管控策略

对于未绑定任何资源夹或成员的自定义管控策略，您可以随时删除。

背景信息

- 系统管控策略不支持删除。
- 对于已绑定了资源夹或成员的自定义管控策略，需要先解绑，然后才能删除。具体操作，请参见解绑自定义管控策略。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 管控策略**。
3. 在**策略列表**页签，单击目标管控策略**操作**列的**删除**。
4. 单击**确定**。

2.4.6.4. 绑定自定义管控策略

您可以为资源夹或成员绑定自定义管控策略。绑定成功后，资源夹或成员将会立即受到管控策略的管控。请务必确定绑定操作的结果是符合预期的，以免影响您的业务正常运行。

背景信息

- 系统会默认为资源夹和成员绑定系统策略FullAliyunAccess。
- 管控策略在绑定节点下整体生效，即父资源夹绑定的管控策略，会在其子资源夹及其成员上生效。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 管控策略**。
3. 在**策略绑定**页签下的左侧组织结构树中，单击目标资源夹或成员。
4. 在右侧页面，单击**绑定策略**。
5. 在**绑定策略**对话框，选择需要绑定的管控策略。
6. 单击**确定**。

2.4.6.5. 解绑自定义管控策略

您可以随时解绑自定义管控策略，解绑成功后，原绑定的资源夹或成员将会立即失去管控策略的管控。请务必确定解绑操作的结果是符合预期的，以免影响您的业务正常运行。

背景信息

系统策略和自定义管控策略都可以解绑，但资源夹或成员上绑定的最后一条管控策略不允许解绑。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 管控策略**。
3. 在**策略绑定**页签下的左侧组织结构树中，单击目标资源夹或成员。
4. 在右侧的管控策略列表中，单击目标管控策略**操作**列的**解绑**。
5. 单击**确定**。

2.4.6.6. 自定义管控策略示例

本文为您介绍自定义管控策略的常用示例。

总览

示例1：禁止修改和删除RAM用户、RAM用户组、RAM角色

策略内容：

```
{
    "Statement": [
        {
            "Action": [
                "ram:Attach*",
                "ram:Detach*",
                "ram:BindMFADevice",
                "ram:CreateAccessKey",
                "ram:CreateLoginProfile",
                "ram:CreatePolicyVersion",
                "ram:DeleteAccessKey",
                "ram:DeleteGroup",
                "ram:DeleteLoginProfile",
                "ram:DeletePolicy",
                "ram:DeletePolicyVersion",
                "ram:DeleteRole",
                "ram:DeleteUser",
                "ram:DisableVirtualMFA",
                "ram:AddUserToGroup",
                "ram:RemoveUserFromGroup",
                "ram:SetDefaultPolicyVersion",
                "ram:UnbindMFADevice",
                "ram:UpdateAccessKey",
                "ram:UpdateGroup",
                "ram:UpdateLoginProfile",
                "ram:UpdateRole",
                "ram:UpdateUser"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN":"acs:ram:*:*:role/resourcedirectoryaccountaccessrole
"
                }
            }
        }
    ],
    "Version": "1"
}
```

本策略禁止修改和删除RAM用户、RAM用户组、RAM角色，包括禁止修改其权限。

> **说明** 本策略只允许资源目录默认用来访问成员的角色ResourceDirectoryAccountAccessRole执行此操作。您可以删除该Condition，禁止所有RAM用户和RAM角色执行此操作。您也可以添加或修改PrincipalARN的值，自定义限制条件。

示例2：禁止修改ResourceDirectoryAccountAccessRole角色及其权限

策略内容：

```
{
   "Version": "1",
   "Statement": [
       {
           "Effect": "Deny",
           "Action": [
               "ram:UpdateRole",
               "ram:DeleteRole",
               "ram:AttachPolicyToRole",
               "ram:DetachPolicyFromRole"
           ],
           "Resource": "acs:ram:*:*:role/resourcedirectoryaccountaccessrole"
       }
   ]
}
```

示例3：禁止修改和删除指定的RAM用户

策略内容：

```
{
    "Version": "1",
    "Statement": [{
        "Action": [
            "ram:AttachPolicyToUser",
            "ram:DetachPolicyFromUser",
            "ram:AddUserToGroup",
            "ram:RemoveUserFromGroup",
            "ram:UpdateUser",
            "ram:DeleteUser",
            "ram:CreateLoginProfile",
            "ram:UpdateLoginProfile",
            "ram:DeleteLoginProfile",
            "ram:CreateAccessKey",
            "ram:DeleteAccessKey",
            "ram:UpdateAccessKey",
            "ram:BindMFADevice",
            "ram:UnbindMFADevice",
            "ram:DisableVirtualMFA"
        ],
        "Resource": [
            "acs:ram:*:*:user/Alice"
        ],
        "Effect": "Deny",
        "Condition": {
            "StringNotLike": {
                "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrole"
            }
        }
    }]
}
```

本策略禁止修改和删除指定的RAM用户（例如：Alice），包括禁止修改其权限。您也可以明确指定Alice所在的具体阿里云账号，例如：`acs:ram:*:18299873****:user/Alice`。

> **说明** 本策略只允许资源目录默认用来访问成员的角色ResourceDirectoryAccountAccessRole执行此操作。您可以删除该Condition，禁止所有RAM用户和RAM角色执行此操作。您也可以添加或修改PrincipalARN的值，自定义限制条件。

示例4：禁止开启任何已存在RAM用户的控制台登录

策略内容：

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateLoginProfile",
                "ram:UpdateLoginProfile"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ],
    "Version": "1"
}
```

本策略禁止开启任何已存在RAM用户的控制台登录。本策略仅针对已存在的RAM用户生效，不影响创建RAM用户时开启控制台登录的操作。

> **说明** 本策略只允许资源目录默认用来访问成员的角色ResourceDirectoryAccountAccessRole执行此操作。您可以删除该Condition，禁止所有RAM用户和RAM角色执行此操作。您也可以添加或修改PrincipalARN的值，自定义限制条件。

示例5：删除某些资源时RAM用户或RAM角色必须使用多因素认证（MFA）

策略内容：

```
{
  "Statement": [
    {
      "Action": "ecs:DeleteInstance",
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "Bool": {
          "acs:MFAPresent": "false"
        }
      }
    }
  ],
  "Version": "1"
}
```

本策略以删除ECS实例时RAM用户或RAM角色必须使用多因素认证（MFA）为例。如需删除其它资源，请将策略中的Action部分修改为相应资源的操作。

示例6：禁止修改用户SSO配置

策略内容：

```
{
    "Statement": [
        {
            "Action": [
                "ram:SetSamlSsoSettings"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ],
    "Version": "1"
}
```

说明 本策略只允许资源目录默认用来访问成员的角色ResourceDirectoryAccountAccessRole执行此操作。您可以删除该Condition，禁止所有RAM用户和RAM角色执行此操作。您也可以添加或修改PrincipalARN的值，自定义限制条件。

示例7：禁止修改角色SSO配置

策略内容：

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateSAMLProvider",
                "ram:DeleteSAMLProvider",
                "ram:UpdateSAMLProvider"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ],
    "Version": "1"
}
```

说明 本策略只允许资源目录默认用来访问成员的角色ResourceDirectoryAccountAccessRole执行此操作。您可以删除该Condition，禁止所有RAM用户和RAM角色执行此操作。您也可以添加或修改PrincipalARN的值，自定义限制条件。

示例8：禁止修改操作审计的投递地址、禁止关闭投递功能

策略内容：

```
{
    "Statement": [
        {
            "Action": [
                "actiontrail:UpdateTrail",
                "actiontrail:DeleteTrail",
                "actiontrail:StopLogging"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ],
    "Version": "1"
}
```

说明 本策略只允许资源目录默认用来访问成员的角色ResourceDirectoryAccountAccessRole执行此操作。您可以删除该Condition，禁止所有RAM用户和RAM角色执行此操作。您也可以添加或修改PrincipalARN的值，自定义限制条件。

示例9：禁止访问部分网络服务

策略内容：

```
{
    "Statement": [
        {
            "Action": [
                "vpc:*HaVip*",
                "vpc:*RouteTable*",
                "vpc:*VRouter*",
                "vpc:*RouteEntry*",
                "vpc:*VSwitch*",
                "vpc:*Vpc*",
                "vpc:*Cen*",
                "vpc:*NetworkAcl*"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        },
        {
            "Action": [
                "vpc:*VpnGateway*",
                "vpc:*VpnConnection*",
                "vpc:*CustomerGateway*",
                "vpc:*SslVpnServer*",
                "vpc:*SslVpnClientCert*",
                "vpc:*VpnRoute*",
                "vpc:*VpnPbrRoute*"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ],
    "Version": "1"
}
```

本策略以禁止访问VPC和VPN网关为例。如需禁止访问其它网络云服务，请将策略中的Action部分修改为相应云服务的操作。

> **说明** 本策略只允许资源目录默认用来访问成员的角色ResourceDirectoryAccountAccessRole执行此操作。您可以删除该Condition，禁止所有RAM用户和RAM角色执行此操作。您也可以添加或修改PrincipalARN的值，自定义限制条件。

示例10：禁止创建具有公网访问能力的网络资源，包括EIP和NAT网关

策略内容：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "vpc:AllocateEipAddress",
                "vpc:AllocateEipAddressPro",
                "vpc:AllocateEipSegmentAddress",
                "vpc:CreateNatGateway"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ]
}
```

说明 本策略只允许资源目录默认用来访问成员的角色ResourceDirectoryAccountAccessRole执行此操作。您可以删除该Condition，禁止所有RAM用户和RAM角色执行此操作。您也可以添加或修改PrincipalARN的值，自定义限制条件。

示例11：禁止访问连接云下资源的网络服务

策略内容：

```
{
    "Statement": [
       {
            "Action": [
                "vpc:*PhysicalConnection*",
                "vpc:*VirtualBorderRouter*",
                "cen:*",
                "vpc:*VpnGateway*",
                "vpc:*VpnConnection*",
                "vpc:*CustomerGateway*",
                "vpc:*SslVpnServer*",
                "vpc:*SslVpnClientCert*",
                "vpc:*VpnRoute*",
                "vpc:*VpnPbrRoute*",
                "smartag:*"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ],
    "Version": "1"
}
```

本策略禁止访问连接云下资源的网络服务，包括：高速通道的物理专线和边界路由器、云企业网、VPN网关、智能接入网关。

示例12：禁止访问费用中心的部分功能

策略内容：

```
{
    "Statement": [
       {
            "Action": [
                "bss:DescribeOrderList",
                "bss:DescribeOrderDetail",
                "bss:PayOrder",
                "bss:CancelOrder"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ],
    "Version": "1"
}
```

本策略以禁止访问费用中心的订单功能为例。如需禁止访问其它功能，请将策略中的Action部分修改为相应的操作。

> **说明** 本策略只允许资源目录默认用来访问成员的角色ResourceDirectoryAccountAccessRole执行此操作。您可以删除该Condition，禁止所有RAM用户和RAM角色执行此操作。您也可以添加或修改PrincipalARN的值，自定义限制条件。

示例13：禁止修改云监控配置

策略内容：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "cms:Put*",
                "cms:Update*",
                "cms:Create*",
                "cms:Modify*",
                "cms:Disable*",
                "cms:Enable*",
                "cms:Delete*",
                "cms:Send*",
                "cms:Subscribe*",
                "cms:Unsubscribe*",
                "cms:Remove*",
                "cms:CreateAction",
                "cms:Pause*",
                "cms:Stop*",
                "cms:Start*",
                "cms:BatchCreate*",
                "cms:ProfileSet",
                "cms:ApplyMonitoringTemplate"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ]
}
```

> **说明** 本策略只允许资源目录默认用来访问成员的角色ResourceDirectoryAccountAccessRole执行此操作。您可以删除该Condition，禁止所有RAM用户和RAM角色执行此操作。您也可以添加或修改PrincipalARN的值，自定义限制条件。

示例14：禁止购买预留实例券

策略内容：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "ecs:PurchaseReservedInstancesOffering"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

示例15：禁止在非指定VPC下创建ECS实例

策略内容：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "ecs:CreateInstance",
                "ecs:RunInstances"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "vpc:VPC": "acs:vpc:cn-shenzhen:*:vpc/vpc-wz95ya85js0avrkabc****"
                }
            }
        }
    ]
}
```

本策略的示例中指定VPC为acs:vpc:cn-shenzhen:*:vpc/vpc-wz95ya85js0avrkabc****，实际使用时请替换为自己的VPC信息。

示例16：禁止购买域名

策略内容：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "domain:CreateOrderActivate"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

示例17：禁止访问工单系统

策略内容：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "support:*",
                "workorder:*"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

示例18：禁止访问特定地域的ECS服务

策略内容：

```
{
    "Version": "1",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "ecs:*"
        ],
        "Resource": "acs:ecs:us-east-1:*:*"
    }]
}
```

本策略禁止在美国东部（弗吉尼亚）地域使用ECS服务。

2.5. 管理可信服务

2.5.1. 可信服务概述

可信服务是指支持与资源目录组合使用的其他阿里云服务。资源目录允许可信服务访问资源目录中的成员、资源夹等信息。您可以使用管理账号或可信服务的委派管理员账号，在可信服务中基于组织进行业务管理，从而简化企业对云服务的统一管理。例如：配置审计集成资源目录后，管理账号可以在可信服务配置审计中查看所有成员的资源列表、资源配置历史和资源合规状态，并监控资源配置合规性。

可信服务使用流程

您可以通过控制台或API使用可信服务。下面以控制台为例说明使用流程。

1. 在资源管理控制台，使用管理账号，开通资源目录。

   具体操作，请参见开通资源目录。

2. 在资源管理控制台，使用管理账号，搭建企业的组织结构。您可以创建新的成员，也可以邀请已有的阿里云账号加入组织。

   具体操作，请参见创建资源夹、创建成员和邀请阿里云账号加入资源目录。

3. （可选）在资源管理控制台，使用管理账号，将成员设置为可信服务的委派管理员账号。

   如果不设置可信服务的委派管理账号，则需使用管理账号在可信服务中进行业务管理。

   关于如何设置委派管理员账号，请参见添加委派管理员账号。

   > **说明** 该步骤仅适用于支持委派管理员的可信服务。

4. 在可信服务控制台，使用管理账号或委派管理员账号，启用多账号管理功能。然后基于资源目录的组织结构选择需要统一管理的成员，并对已选中的成员进行业务管理。

   不同可信服务的操作不一样。具体操作，请参见支持的可信服务的相关文档列。

支持的可信服务

可信服务	功能介绍	是否支持委派管理员账号	相关文档
配置审计	配置审计集成资源目录后，管理账号可以在配置审计中查看所有成员的资源列表、资源配置历史和资源合规状态，并监控资源配置合规性。	是	账号组概述
操作审计	操作审计集成资源目录后，管理账号可以在操作审计中创建多账号跟踪。多账号跟踪将资源目录内的所有成员的操作事件投递到对象存储OSS或日志服务SLS。	是	多账号跟踪
云安全中心	云安全中心集成资源目录后，能够在云安全中心通过统一的界面展示企业内所有成员中检测出的安全风险。	是	多账号安全管控

可信服务	功能介绍	是否支持委派管理员账号	相关文档
云防火墙	云防火墙集成资源目录后，能够统一管理多账号的公网IP资产，统一配置防御策略以及查看日志分析，实现集中安全管控。	是	统一账号管理
全站加速	全站加速集成资源目录后，能够提供多账号管理功能，实现跨账号跨产品的域名资源统一管理。	否	全站加速多账号集成管理
云监控	企业云监控与资源目录集成，轻松实现企业跨阿里云账号的资源统一监控。	是	企业云监控概览
云安全访问服务	云安全访问服务集成资源目录后，可以通过管理账号或委派管理员账号，将成员下的云资产自动添加到管理账号下，方便集中管控内网访问。	是	多账号管理
云SSO	管理账号可以在云SSO中统一管理企业中使用阿里云的用户，一次性配置企业身份管理系统与阿里云的单点登录，并统一配置用户对资源目录中成员的访问权限。	否	多账号授权概述
日志审计服务	日志审计服务支持多账号环境下自动化、中心化采集云产品日志，并进行日志审计分析。	是	配置多账号采集
资源编排服务	管理账号可以在资源目录的成员中一键部署系统所依赖的云资源，满足企业多账号环境下的资源集中管理需求。	是	资源栈组概览
资源共享	管理账号在启用资源目录组织共享后，支持将云资源共享给指定成员、指定资源夹或整个资源目录。新加入资源夹或资源目录的成员将自动获取对共享资源的访问权限，从资源夹或资源目录移除的成员将自动取消对共享资源的访问权限。	否	资源共享概述

可信服务	功能介绍	是否支持委派管理员账号	相关文档
云治理中心	管理账号可以在云治理中心中统一查看企业各成员的资源分布和趋势变化，为企业各成员统一配置合规审计防护规则和统一投递审计日志。	否	• 统一投递审计日志 • 统一配置防护规则 • 查看资源分布和变化趋势
标签	管理账号可以启用标签策略的多账号模式，规范管理资源目录中各成员的标签操作。	否	多账号模式
服务目录	将服务目录的产品组合共享给资源目录中的多个成员，且产品组合配置变更后，也可以实时同步给被共享的多个成员，从而大幅提升管理效率。	是	管理多账号共享

启用或禁用可信服务

您可以通过各可信服务的控制台或API，启用或禁用可信服务。具体操作，请参见各可信服务的相关文档。

您可以在资源管理控制台的左侧导航栏，选择**资源目录 > 可信服务**，查看可信服务的状态。但您不能在资源管理控制台上启用或禁用可信服务。

有些可信服务会在您执行某些特定操作时（例如：在操作审计中创建多账号跟踪或第一次在可信服务中查看资源目录相关的资源时），自动将可信服务状态更新为已启用。

有些可信服务会在您执行某些特定操作时（例如：关闭一个功能时），自动将可信服务状态更新为已禁用。禁用可信服务意味着该可信服务不能再访问资源目录中的账号和资源，同时，该可信服务会删除本服务内与资源目录集成相关的全部资源。

可信服务与服务关联角色

资源目录为每个成员创建了资源目录的服务关联角色（AliyunServiceRoleForResourceDirectory），该角色允许资源目录为可信服务创建服务所需角色的权限。该角色仅允许资源目录扮演。更多信息，请参见资源目录中的RAM角色。

可信服务仅在需要执行管理操作的成员中创建可信服务的服务关联角色（例如：配置审计的服务关联角色AliyunServiceRoleForConfig）。该角色定义了允许可信服务执行特定任务所需的权限。该角色仅允许对应的可信服务扮演。

服务关联角色的权限策略由对应的云服务定义和使用，您不能修改或删除权限策略，也不能为服务关联角色添加或移除权限。更多信息，请参见服务关联角色。

2.5.2. 管理委派管理员账号

本文为您介绍委派管理员账号的定义、使用限制及基本操作。

什么是委派管理员账号

资源目录的管理账号可以将资源目录中的成员设置为可信服务的委派管理员账号。设置成功后，委派管理员账号将获得管理账号的授权，可以在对应可信服务中访问资源目录组织和成员信息，并在该组织范围内进行业务管理。更多信息，请参见支持委派管理员账号的可信服务。

通过委派管理员账号，可以将组织管理任务与业务管理任务相分离，管理账号执行资源目录的组织管理任务，委派管理员账号执行可信服务的业务管理任务，这符合安全最佳实践的建议。

使用限制

- 只有部分可信服务支持委派管理员账号。更多信息，请参见支持的可信服务。
- 只有资源目录的管理账号和其下具有以下权限的RAM用户或RAM角色才可以添加或移除委派管理员账号。

```
{
    "Version": "1",
    "Statement": [{
        "Action": [
            "resourcemanager:RegisterDelegatedAdministrator",
            "resourcemanager:DeregisterDelegatedAdministrator"
        ],
        "Resource": "*",
        "Effect": "Allow"
    }]
}
```

  关于如何创建自定义策略，请参见创建自定义权限策略。

- 委派管理员账号只能是资源目录的成员，不能是管理账号。
- 可信服务允许添加的委派管理员账号数量由各可信服务定义。

添加委派管理员账号

1. 使用管理账号登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 可信服务**。
3. 在**可信服务**页面，单击目标可信服务**操作**列的**管理**。
4. 在**委派管理员账号**区域，单击**添加**。
5. 在**添加委派管理员账号**面板，选中成员。
6. 单击**确定**。
   添加成功后，使用该委派管理员账号访问对应可信服务的多账号管理模块，即可进行资源目录组织范围内的管理操作。

移除委派管理员账号

> **注意** 移除操作可能会对可信服务的正常使用产生影响，请在移除前慎重考虑。

1. 使用管理账号登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 可信服务**。
3. 在**可信服务**页面，单击目标可信服务**操作**列的**管理**。
4. 在**委派管理员账号**区域，单击目标账号**操作**列的**移除**。
5. 在**移除警告**对话框，单击**继续**。
   移除成功后，该账号将不能在可信服务中访问资源目录组织和成员信息。

3.成员

3.1. 查看成员信息

成员登录到资源目录控制台后，可以查看成员所在的资源目录信息和成员基本信息。

背景信息

关于成员、管理账号和RDPath等基本概念，请参见基本概念。

操作步骤

1. 登录资源管理控制台。
2. 在左侧导航栏，选择**资源目录 > 成员信息**。
3. 在**成员信息**页面的**所在资源目录信息**区域，查看成员所在的资源目录的基本信息。

   您可以查看资源目录的ID、资源目录的创建时间、资源目录的管理账号和资源目录的企业名称。
4. 在**成员信息**页面的**成员信息**区域，查看当前成员的基本信息。

   您可以查看成员所在的目录位置、成员的RDPath、成员的显示名和成员加入资源目录的时间。