

ALIBABA CLOUD

阿里云

专有云企业版

文件存储
用户指南

产品版本：v3.16.2

文档版本：20220915

 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 <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> <code>Instance_ID</code>
[] 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

1.什么是文件存储NAS	06
2.使用须知	07
3.快速入门	09
3.1. 登录文件存储NAS控制台	09
3.2. 创建文件系统	09
3.3. 创建权限组及规则	10
3.4. 添加挂载点	12
3.5. 挂载NFS文件系统	14
3.6. 挂载SMB文件系统	17
4.文件系统	20
4.1. 查看文件系统详情	20
4.2. 删除文件系统	20
4.3. 扩容文件系统	20
5.挂载点	22
5.1. 查看挂载点列表	22
5.2. 禁用或启用挂载点	22
5.3. 删除挂载点	23
5.4. 修改挂载点的权限组	23
6.权限组	25
6.1. 查看权限组列表	25
6.2. 删除权限组	25
6.3. 管理权限组规则	25
7.管理配额	27
8.统一命名空间	31
9.生命周期管理	39
10.目录级读写权限ACL	45

10.1. 简介	45
10.2. 特性	46
10.3. 使用POSIX ACL进行权限管理	56
10.4. 使用NFSv4 ACL进行权限管理	59

1.什么是文件存储NAS

阿里云文件存储NAS（Apsara File Storage NAS）是面向阿里云ECS实例、E-HPC和容器服务等计算节点的文件存储服务。

文件存储NAS提供标准的文件访问协议，您无需对现有应用做任何修改，即可使用可共享访问、弹性扩展、高可靠以及高性能的分布式文件系统。此外，同一个NAS文件系统可以同时挂载到多个计算节点上，从而节约大量拷贝和同步成本。

NAS相关操作：

- 创建NAS文件系统实例和挂载点。
- 为NAS文件系统实例创建权限组，并向权限组中添加规则，从而允许特定IP地址或网段访问文件系统，或为不同IP地址或网段授予不同级别的访问权限。
- 在ECS、容器服务等计算节点内通过标准的NFS或SMB协议挂载文件系统，并使用标准的POSIX接口访问文件系统。
- 在文件存储NAS控制台对文件系统、挂载点、权限组进行基础和高级操作。
- 调用NAS API对文件系统进行基础和高级操作。

2. 使用须知

在使用文件存储NAS前，您需要了解以下限制。

文件系统限制

- 单个文件系统最大文件数：10亿。
- 文件系统名称的最大长度：255字节。
- 单个文件的最大大小：32 TB。
- 最大目录深度：1000级。
- 单个文件系统容量上限：容量型10 PB。
- 单个文件系统最多能够被10000个计算节点同时挂载访问。
- 协议包的数据大小最大为4 MB。
- 支持的最多change notify请求个数为512个。

NFS客户端限制

NFS客户端的使用限制如下所示。

- NFS客户端上最多可同时打开32768个文件。list目录及其下面的文件不会统计为打开文件。
- NFS客户端上的每个挂载最多可以在256个文件或进程中获取8192个锁。例如，单个进程可以在256个单独文件上获取一个或多个锁，或者8个进程中的每个进程均可以在32个文件上获取一个或多个锁。
- 不推荐在Microsoft Windows上使用NFS客户端访问NFS文件系统。


SMB客户端限制

在所有挂载文件系统的计算节点上和所有共享访问文件系统的用户中，任何一个特定文件或目录最多可以同时打开8192次，即8192个活跃文件句柄。文件系统级别最多可以有65536个活跃文件句柄。

NFS协议限制

- 文件存储NAS目前支持NFSv3和NFSv4协议。
- NFSv4.0不支持的Attributes包括：FATTR4_MIMETYPE、FATTR4_QUOTA_AVAIL_HARD、FATTR4_QUOTA_AVAIL_SOFT、FATTR4_QUOTA_USED、FATTR4_TIME_BACKUP、FATTR4_TIME_CREATE，客户端将显示NFS4ERR_ATTRNOTSUPP错误。
- NFSv4.1不支持的Attributes包括：FATTR4_DIR_NOTIF_DELAY、FATTR4_DIRENT_NOTIF_DELAY、FATTR4_DACL、FATTR4_SACL、FATTR4_CHANGE_POLICY、FATTR4_FS_STATUS、FATTR4_LAYOUT_HINT、FATTR4_LAYOUT_TYPES、FATTR4_LAYOUT_ALIGNMENT、FATTR4_FS_LOCATIONS_INFO、FATTR4_MDSTHRESHOLD、FATTR4_RETENTION_GET、FATTR4_RETENTION_SET、FATTR4_RETENT_EVT_GET、FATTR4_RETENT_EVT_SET、FATTR4_RETENTION_HOLD、FATTR4_MODE_SET_MASKED、FATTR4_FS_CHARSET_CAP，客户端将显示NFS4ERR_ATTRNOTSUPP错误。
- NFSv4不支持的OP包括：OP_DELEGPURGE、OP_DELEGRETURN、NFS4_OP_OPENATTR，客户端将显示NFS4ERR_NOTSUPP错误。
- NFSv4暂不支持Delegation功能。
- 关于UID和GID的问题：
 - 对于NFSv3协议，如果Linux本地账户中存在文件所属的UID或GID，则根据本地的UID和GID映射关系显示相应的用户名和组名；如果本地账户不存在文件所属的UID或GID，则直接显示UID和GID。

- 对于NFSv4协议，如果本地Linux内核版本低于3.0，则所有文件的UID和GID都将显示nobody；如果内核版本高于3.0，则显示规则同NFSv3协议。

 **注意** 若使用NFSv4协议挂载文件系统，且Linux内核版本低于3.0，则建议最好不要对文件或目录进行change owner或change group操作，否则该文件或目录的UID和GID将变为nobody。

SMB协议限制

- 支持SMB 2.1及以上的SMB协议版本，支持Windows 7和Windows Server 2008 R2及以上的各Windows版本，不支持Windows Vista和Windows Server 2008及以下的各Windows版本。与SMB 2.1及以后的版本相比，SMB 1.0由于协议设计的巨大差异导致在性能和功能上有严重的不足，并且只支持SMB 1.0或更早协议版本的Windows产品已经完全退出微软支持的生命周期。
- 不支持文件扩展属性（Extended attributes）以及基于Lease的客户端缓存。
- 不支持Sparse files、文件压缩、网卡状态查询、重解析点（Reparse Point）等IOCTL或FSCTL操作。
- 不支持交换数据流（Alternate Data Streams）。
- 暂时不支持AD或LDAP身份认证功能。
- 不支持SMB Direct、SMB Multichannel、SMB Directory Leasing、Persistent File Handle等SMB 3.0及以上版本的一些协议功能。
- 不提供文件或目录级别的ACL权限控制。

其他限制

删除NAS资源时，您需要先卸载计算节点（ECS实例、容器）中通过挂载点挂载的文件系统，再删除挂载点，最后删除创建的文件系统。

3. 快速入门

3.1. 登录文件存储NAS控制台

本章节介绍如何登录文件存储NAS控制台。


前提条件

- 登录Apsara Uni-manager运营控制台前，确认您已从部署人员处获取Apsara Uni-manager运营控制台的服务域名地址。
- 推荐使用Chrome浏览器。

操作步骤

1. 在浏览器地址栏中，输入Apsara Uni-manager运营控制台的服务域名地址，按回车键。
2. 输入正确的用户名及密码。


请向运营管理员获取登录控制台的用户名和密码。

 **说明** 首次登录Apsara Uni-manager运营控制台时，需要修改登录用户名的密码，请按照提示完成密码修改。为提高安全性，密码长度必须为10~32位，且至少包含以下两种类型：

- 英文大写或小写字母（A~Z、a~z）
- 阿拉伯数字（0~9）
- 特殊符号（感叹号（!）、at（@）、井号（#）、美元符号（\$）、百分号（%）等）

3. 单击**账号登录**。
4. 如果账号已激活MFA多因素认证，请根据以下两种情况进行操作：
 - 管理员强制开启MFA后的首次登录：
 - a. 在绑定虚拟MFA设备页面中，按页面提示步骤绑定MFA设备。
 - b. 按照步骤2重新输入账号和密码，单击**账号登录**。
 - c. 输入6位MFA码后单击**认证**。
 - 您已开启并绑定MFA：

输入6位MFA码后单击**认证**。

 **说明** 绑定并开启MFA的操作请参见Apsara Uni-manager运营控制台用户指南中的**绑定并开启虚拟MFA设备**章节。

5. 在页面上方的导航栏中，选择**产品**，在**存储区域**，单击**文件存储 NAS**。

3.2. 创建文件系统

本文介绍如何在文件存储NAS控制台创建文件系统。

背景信息

在创建文件系统时，需要了解以下注意事项。

- 每个账号最多可以创建1000个文件系统。
- 容量型文件系统容量上限为10 PB。

如果需要提高容量上限，请联系管理员。

操作步骤

1. 登录[文件存储NAS控制台](#)。
2. 选择文件系统 > 文件系统列表，单击创建文件系统。
3. 在创建文件系统面板，配置参数。

重要参数说明如下所示。

参数	说明
地域	选择要创建文件系统的地域。
组织	选择实例所属的组织。
资源集	选择实例所属的资源集。
可用区	选择实例所属的可用区。
集群	选择实例所属的集群。
文件系统名称	输入文件系统的名称。文件系统命名规则如下： <ul style="list-style-type: none">○ 长度为2~128个字符。○ 以大小写英文字母或中文开头，不能以http://或https://开头。○ 支持数字，可包含下划线（_）、短划线（-）和半角冒号（:）特殊字符。
存储类型	选择存储类型为容量型。 容量型文件系统容量上限为10 PB。
协议类型	包括NFS和SMB，请根据需求进行选择。 Linux客户端建议使用NFS协议，Windows客户端建议使用SMB协议。
容量限制（TB）	设置文件系统的容量。取值范围为0.5 TB~10240 TB。


4. 单击提交，完成文件系统的创建。

3.3. 创建权限组及规则

本文介绍如何在文件存储NAS控制台创建权限组及权限组规则。

背景信息

在文件存储NAS中，权限组是一个白名单机制。您可以添加权限组规则，允许指定的IP地址或网段访问文件系统，并可以给不同的IP地址或网段授予不同级别的访问权限。

 **说明** 每个用户最多创建100个权限组。如果需要提高上限，请联系管理员。

创建权限组

1. 登录[文件存储NAS控制台](#)。
2. 选择文件系统 > 权限组，单击创建权限组。
3. 在创建NAS权限组页面，配置参数。

重要参数说明如下所示。

参数	说明
组织	选择权限组所属的组织。
资源集	选择权限组所属的资源集。
地域	选择要创建权限组的地域。
权限组名称	设置权限组的名称。权限组命名规则如下： <ul style="list-style-type: none">长度为3~64个字符。支持英文字母、数字和短划线（-）。
网络类型	包括经典类型和专有类型，请根据需求选择。

4. 单击提交，完成权限组的创建。

创建权限组规则

1. 登录[文件存储NAS控制台](#)。
2. 在权限组页面，找到目标权限组，单击管理规则。
3. 单击添加规则。
4. 在添加规则对话框中，配置参数。

添加规则

* 授权地址 ?

10.10.10.23

* 读写权限

读写

* 用户权限 ?

所有用户不匿名 (no_squash)

* 优先级 ?

-

1

+

确定

取消

重要参数说明如下所示。

参数	说明
授权地址	本条规则的授权对象，可以为单个IP地址或网段（经典网络类型只支持单个IP地址）。
读写权限	允许授权对象对文件系统进行只读操作或读写操作，包括只读和读写。
用户权限	<p>是否限制授权对象的Linux系统用户对文件系统的访问权限。</p> <ul style="list-style-type: none">所有用户不匿名（no_squash）：将允许使用root用户访问文件系统。root用户匿名（root_squash）：以root用户身份访问时，映射nobody用户。所有用户匿名（all_squash）：无论以何种用户身份访问，均映射为nobody用户。 <p>nobody用户是Linux系统的默认用户，只能访问服务器上的公共内容，具有低权限，高安全性的特点。</p>
优先级	当同一个授权对象匹配到多条规则时，高优先级规则将覆盖低优先级规则。可选择1~100，1为最高优先级。

5. 单击**确定**，完成权限组规则的创建。

3.4. 添加挂载点

在文件存储NAS中，需要通过挂载点将文件系统挂载至计算节点（ECS实例、容器），本文介绍如何添加挂载点。

前提条件

您已完成以下操作：

- 创建文件系统。
- 创建权限组及规则。

背景信息

挂载点是文件系统实例在专有网络或经典网络内的一个访问目标地址，每个挂载点都对应一个域名。NAS支持两种类型的挂载点：专有网络类型和经典网络类型。

④ 说明 同一挂载点可以被多个计算节点（ECS实例、容器）同时挂载，共享访问。

操作步骤

1. 登录[文件存储NAS控制台](#)。
2. 选择文件系统 > 文件系统列表。
3. 找到目标文件系统，单击管理。
4. 在左侧导航栏中选择挂载使用。
5. 在挂载点区域，单击添加挂载点。
6. 在添加挂载点对话框中，配置参数。

挂载点类型：包括专有网络和经典网络。

说明 经典网络类型的挂载点暂时只支持同一账号下的ECS实例访问。

添加挂载点

×

文件系统

1 [REDACTED] fs

* 挂载点类型 ?

专有网络

▼

* VPC网络 ?

nas-[REDACTED]

▼

* 交换机 ?

tes[REDACTED]

▼

* 权限组 ?

test01

▼

确定

取消

- 如果您要添加专有网络类型的挂载点，请配置以下参数。

参数	说明
VPC网络	选择已创建的VPC网络。 <div>❓ 说明 必须与计算节点（ECS实例、容器）选择一样的VPC网络和交换机。</div>
交换机	选择VPC网络下创建的交换机。
权限组	选择已创建的权限组。

- 如果您要添加经典网络类型的挂载点，请配置以下参数。

参数	说明
权限组	选择已创建的权限组。

- 单击**确定**，完成挂载点的添加。

3.5. 挂载NFS文件系统

创建文件系统及挂载点完成后，您可以通过挂载点将文件系统挂载到计算节点（ECS实例、容器）。本文介绍如何挂载NFS文件系统。

前提条件

- 已创建文件系统。具体操作，请参见[创建文件系统](#)。
- 已创建权限组及规则。具体操作，请参见[创建权限组及规则](#)。
- 已添加挂载点，本文以专有网络的挂载点为例。具体操作，请参见[添加挂载点](#)。
 - 如果挂载点类型为专有网络，则只支持与挂载点同一VPC网络的云服务器ECS实例挂载文件系统，且挂载点所绑定的权限组规则中的授权地址必须包含云服务器ECS实例的VPC IP地址。
 - 如果挂载点类型为经典网络，则只支持与挂载点同一账号的云服务器ECS实例挂载文件系统，且挂载点所绑定的权限组规则中的授权地址必须包含云服务器ECS实例的内网IP地址。
- 已有可用的服务器，本文以ECS Linux系统为例。

步骤一：安装NFS客户端

将NFS文件系统挂载至云服务器ECS（Linux系统），您需要先安装NFS客户端。如果已安装NFS客户端，请跳过此步骤。

- 登录云服务器（Linux系统）。具体操作，请参见[ECS用户指南](#)中的[快速入门 > 连接实例](#)章节。
- 安装NFS客户端。
 - 如果您使用CentOS、Redhat、Aliyun Linux操作系统，请执行以下命令。

```
sudo yum install nfs-utils
```

- 如果您使用Ubuntu或Debian操作系统，请执行以下命令。

```
sudo apt-get update
```

```
sudo apt-get install nfs-common
```

步骤二：挂载NFS文件系统

- 1. 登录云服务器ECS（Linux系统）。具体操作，请参见ECS用户指南中的快速入门 > 连接实例章节。
- 2. 挂载NFS文件系统。

执行以下命令挂载NFS文件系统，其中 `file-system-id.region.nas.aliyuncs.com:/mnt` 要根据实际情况替换。

- o 使用NFS v4协议挂载文件系统：

```
sudo mount -t nfs -o vers=4.0,minorversion=0,rsz=1048576,wsz=1048576,hard,timeo=600,retrans=2,noresvport file-system-id.region.nas.aliyuncs.com:/mnt
```

- o 使用NFS v3协议挂载文件系统：

```
sudo mount -t nfs -o vers=3,nolock,proto=tcp,rsz=1048576,wsz=1048576,hard,timeo=600,retrans=2,noresvport file-system-id.region.nas.aliyuncs.com:/mnt
```

挂载命令说明表

参数	说明
file-system-id.region.nas.aliyuncs.com:/mnt	<p>表示<挂载点地址>:<NAS文件系统目录> <当前服务器上待挂载的本地路径>，请根据实际情况替换。</p> <ul style="list-style-type: none">■ 挂载点地址：您可以在文件存储NAS控制台上，找到目标文件系统，单击管理，进入挂载使用页面获取挂载点地址。■ NAS文件系统目录：NAS的根目录（/）或任意子目录（例如/sub1），如果是子目录，请确保子目录已存在。■ 当前服务器上待挂载的本地路径：Linux ECS实例的根目录（/）或任意子目录（例如/mnt），如果是子目录，请确保子目录已存在。
vers	<p>文件系统版本，目前只支持NFS v3和NFS v4。</p> <ul style="list-style-type: none">■ vers=3：使用NFS v3协议挂载文件系统。■ vers=4.0：使用NFS v4协议挂载文件系统。

参数	说明
挂载选项	<p>挂载文件系统时，可选择多种挂载选项，挂载选项使用半角逗号（,）分隔，说明如下：</p> <ul style="list-style-type: none">■ <i>rsize</i>：定义数据块的大小，单位为字节。用于客户端与文件系统之间读取数据。建议值为1048576。■ <i>wsiz</i>e：定义数据块的大小，单位为字节。用于客户端与文件系统之间写入数据。建议值为1048576。 <div><p> 说明 如果您需要更改IO大小参数（<i>rsize</i>和<i>wsiz</i>e），建议您尽可能使用最大值（1048576），以避免性能下降。</p></div> <ul style="list-style-type: none">■ <i>hard</i>：在文件存储NAS暂时不可用的情况下，使用文件系统上某个文件的本地应用程序时会停止并等待至该文件系统恢复在线状态。建议启用该参数。■ <i>timeo</i>：指定时长，单位为0.1秒，即NFS客户端在重试向文件系统发送请求之前等待响应的的时间。建议值为600（60秒）。 <div><p> 说明 如果您必须更改超时参数（<i>timeo</i>），建议您使用150或更大的值。该<i>timeo</i>参数的单位为0.1秒，因此150表示的时间为15秒。</p></div> <ul style="list-style-type: none">■ <i>retrans</i>：NFS客户端重试请求的次数。建议值为2。■ <i>noresvport</i>：在网络重连时使用新的TCP端口，保障在网络发生故障恢复时不会中断连接。建议启用该参数。 <div><p> 说明 配置参数时，应注意以下内容：</p><ul style="list-style-type: none">■ 不建议使用<i>soft</i>选项，有数据一致性风险。如果您要使用<i>soft</i>选项，相关风险需由您自行承担。■ 避免设置不同于默认值的任何其他挂载选项。如果更改读或写缓冲区大小或禁用属性缓存，会导致性能下降。</div>

3. 执行 `mount -l` 命令，查看挂载结果。

如果回显包含如下类似信息，说明挂载成功。

```
fsid=1 on /tmp/keron1zmbq type debugfs (rw,relatime)
squashfs on /dev/squashfs type squashfs (ro,relatime)
hugobtrfs on /dev/hugobtrfs type hugobtrfs (rw,relatime)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw,relatime)
nfs on /mnt type nfs4 (rw,relatime,vers=4.0,rsiz=1048576,wsiz=1048576,namlen=255,hard,noresvport,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=10.10.10.100,local_lock=none,addr=10.10.10.100,netdev)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=2097152,mode=700)
```

挂载成功后，您还可以通过 `df -h` 命令，查看文件系统的当前容量信息。

4. 挂载成功后，您可以在ECS上访问NAS文件系统，执行读取或写入操作。

您可以把NAS文件系统当作一个普通的目录来访问和使用，示例如下：

```
[root@i7n5e6owi-qw421dup9f16qz ~]# mkdir /mnt/dir1
[root@i7n5e6owi-qw421dup9f16qz ~]# mkdir /mnt/dir2
[root@i7n5e6owi-qw421dup9f16qz ~]# touch /mnt/file1
[root@i7n5e6owi-qw421dup9f16qz ~]# echo 'some file content' > /mnt/file2
[root@i7n5e6owi-qw421dup9f16qz ~]# ls /mnt
dir1 dir2 file1 file2 tmp
```

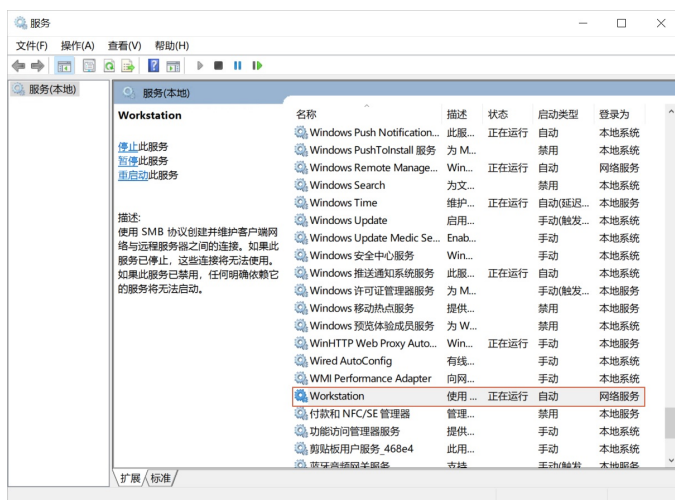

3.6. 挂载SMB文件系统

创建文件系统及挂载点完成后，您可以通过挂载点将文件系统挂载到ECS等计算节点中。本文介绍如何挂载SMB文件系统。

前提条件

1. 已创建文件系统。具体操作，请参见[创建文件系统](#)。
2. 已创建权限组及规则。具体操作，请参见[创建权限组及规则](#)。
3. 已添加挂载点，本文以专有网络的挂载点为例。具体操作，请参见[添加挂载点](#)。
 - 如果挂载点类型为专有网络，则只支持与挂载点同一VPC网络的云服务器ECS实例挂载文件系统，且挂载点所绑定的权限组规则中的授权地址必须包含云服务器ECS实例的VPC IP地址。
 - 如果挂载点类型为经典网络，则只支持与挂载点同一账号的云服务器ECS实例挂载文件系统，且挂载点所绑定的权限组规则中的授权地址必须包含云服务器ECS实例的内网IP地址。
4. 已有可用的服务器，本文以ECS Windows系统为例。
5. 确保Windows系统服务中的以下两项服务均已启动。
 - Workstation
 - a. 选择**所有程序 > 附件 > 运行**或使用快捷键 `Win+R`，输入 `services.msc`，按回车键，进入本地服务。
 - b. 在服务中找到Workstation，确认运行状态为**已启动**，启动类型为**自动**。

正常情况下，Workstation服务默认为启动状态。

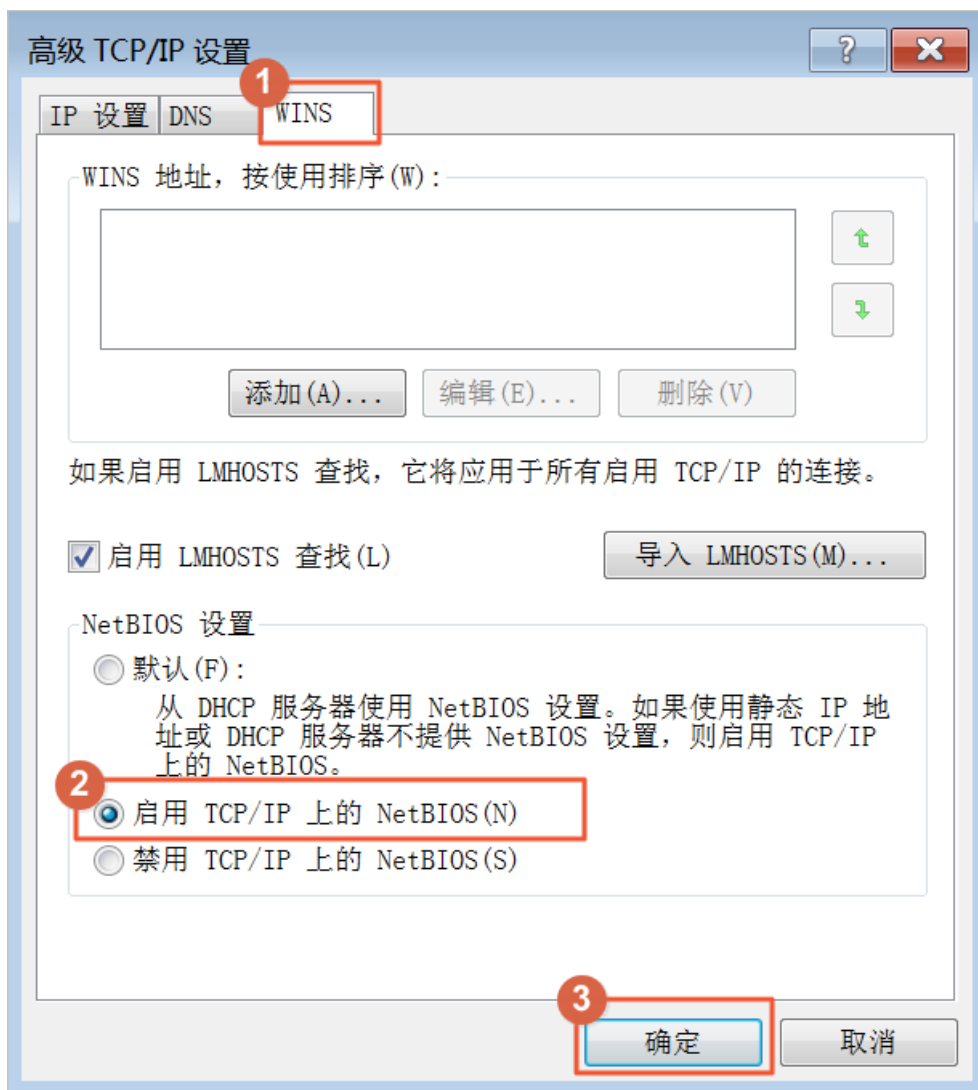


- TCP/IP NetBIOS Helper

开启TCP/IP NetBIOS Helper服务步骤如下所示:

- 打开网络与共享中心，单击主机所连网络。
- 单击属性，双击 Internet 协议版本 4 进入属性框，单击高级。

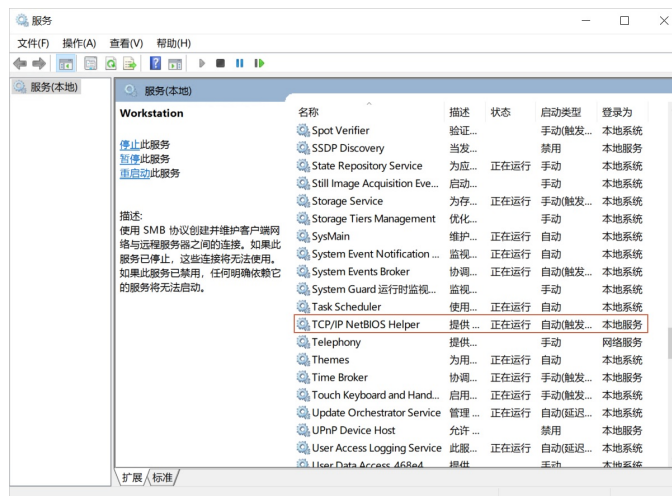
- c. 在高级TCP/IP设置对话框中，选择 WINS > 启用TCP/IP上的NetBIOS。



- d. 选择所有程序 > 附件 > 运行或使用快捷键 Win+R，输入 services.msc，按回车键，进入本地服务。

e. 在服务中找到TCP/IP NetBIOS Helper，确认运行状态为已启动，启动类型为自动。

正常情况下，TCP/IP NetBIOS Helper服务默认为启动状态。



操作步骤

1. 登录云服务器ECS（Windows系统），详情请参见ECS用户指南中的快速入门 > 连接实例章节。
2. 打开命令行窗口，执行以下命令挂载文件系统。

```
net use D: \\file-system-id.region.nas.aliyuncs.com\myshare
```

挂载命令格式：`net use <挂载目标盘符> \\<挂载点地址>\myshare`。

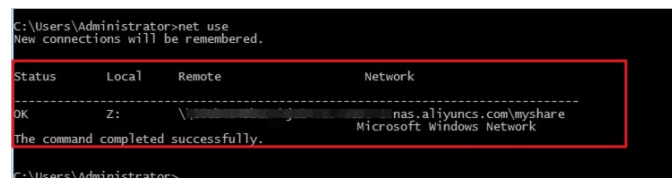
- 挂载目标盘符：指当前Windows系统上要挂载的目标盘符，请根据实际值替换。

说明 目标盘符需配置为当前不存在的盘符。

- 挂载点地址：指创建文件系统挂载点时，自动生成的挂载点地址，请根据实际情况替换。您可以在文件存储NAS控制台，找到目标文件系统，单击管理，进入详情页面获取挂载点地址。
- myshare：SMB的共享名称，不允许变更。

3. 执行 `net use` 命令，检查挂载结果。

如果回显包含如下类似信息，说明挂载成功。



4. 挂载成功后，您可以在ECS上访问NAS文件系统，执行读取或写入操作。

4. 文件系统

4.1. 查看文件系统详情

您可以在NAS控制台上查看已创建的文件系统的详细信息，包括系统详情和挂载点。

前提条件

已创建文件系统。具体操作，请参见[创建文件系统](#)。

操作步骤

1. 登录[文件存储NAS控制台](#)。
2. 选择文件系统 > 文件系统列表。
3. 找到目标文件系统，单击管理，进入文件系统详情页面。

文件系统详情页面包括以下部分：

- **基本信息**：展示文件系统的基本信息，包括文件系统ID、地域、协议类型、存储规格等信息。
- **挂载使用**：展示文件系统的挂载点列表，您可以在这里对挂载点进行管理并查看已挂载客户端。
- **配额管理**：展示文件系统目录配额状态，您可以对每个目录进行配额管理，包括添加配额、编辑配额和删除配额。

4.2. 删除文件系统

您可以在NAS控制台删除已创建的文件系统。

前提条件

文件系统的挂载点数量为0。关于查看文件系统挂载点数量的具体操作，请参见[查看文件系统详情](#)。

操作步骤

1. 登录[文件存储NAS控制台](#)。
2. 选择文件系统 > 文件系统列表。
3. 找到目标文件系统，单击删除。

注意

- 只有当文件系统的挂载点数目为0时，您才可以删除文件系统。
- 文件系统一旦删除，数据将不可恢复，请谨慎操作。


4. 在删除文件系统对话框中，单击确定，完成删除。

4.3. 扩容文件系统

当NAS文件系统达到配置存储容量后，无法继续写入数据。为保障您业务的正常进行，建议您在NAS文件系统达到配置容量前对其进行扩容。本文介绍如何在控制台扩容NAS文件系统。

前提条件

已创建文件系统。具体操作，请参见[创建文件系统](#)。

 **注意** 文件系统只支持扩容，不支持缩容。容量型NAS最大可扩容至10 PB。

操作步骤

1. 登录[文件存储NAS控制台](#)。
2. 在左侧导航栏，选择[文件系统](#) > [文件系统列表](#)。
3. 找到目标文件系统，单击操作列[扩容](#)。
4. 在[扩容](#)对话框中的新的总容量区域，填入文件系统扩容需要达到的容量值。
5. 单击[确定](#)。

5. 挂载点

5.1. 查看挂载点列表

您可以在NAS控制台查看已经创建的挂载点列表。

背景信息

您已完成以下操作：

- [创建文件系统](#)。
- [创建权限组及规则](#)。
- [添加挂载点](#)。

操作步骤

1. 登录[文件存储NAS控制台](#)。
2. 选择文件系统 > 文件系统列表。
3. 找到目标文件系统，单击管理。
4. 在左侧导航栏中选择[挂载使用](#)，在[挂载点](#)页面，查看该文件系统的挂载点列表。



5.2. 禁用或启用挂载点

您可以通过禁止和启用功能，控制客户端对挂载点的访问。本文介绍如何禁用或启用挂载点。

前提条件

您已完成以下操作：

- [创建文件系统](#)。
- [创建权限组及规则](#)。
- [添加挂载点](#)。

操作步骤

1. 登录[文件存储NAS控制台](#)。
2. 选择文件系统 > 文件系统列表。
3. 找到目标文件系统，单击管理。
4. 在左侧导航栏中单击[挂载使用](#)。找到目标挂载点，您可以执行以下操作。
 - 单击禁用，在弹出的对话框中单击确定，暂时阻止任何客户端访问该挂载点。
 - 单击启用，在弹出的对话框中单击确定，重新允许客户端访问该挂载点。

挂节点

添加挂节点

挂节点类型	VPC	交换机	挂节点	挂节点命令	权限组	状态	操作
专有网络	vpc-2z9vz9u0	vsw-2z9vz9u0		net use z: \\10.10.10.100\single-emb6-d01.nas.ops-emb6.shuguang.com\myshare	 test01	 可用	修改权限组 禁用 删除

5.3. 删除挂载点

您可以在NAS控制台删除已添加的挂载点。

前提条件

- 已卸载计算节点（ECS实例、容器）中通过挂载点挂载的文件系统。
- 已移除**统一命名空间跨域编排**添加的挂载点。

操作步骤

1. 登录[文件存储NAS控制台](#)。
2. 选择文件系统 > 文件系统列表。
3. 找到目标文件系统，单击管理。
4. 在左侧导航栏中选择挂载使用。
5. 找到目标挂载点，单击删除。

 **注意** 删除挂载点后无法恢复，请谨慎操作。

6. 在删除确认框中，单击确定。

5.4. 修改挂载点的权限组

每个挂载点都需要绑定一个权限组，您可以在NAS控制台上为挂载点修改已绑定的权限组。


前提条件

您已完成以下操作：

- 创建文件系统。
- 创建权限组及规则。
- 添加挂载点。

操作步骤

1. 登录[文件存储NAS控制台](#)。
2. 选择[文件系统](#) > [文件系统列表](#)。
3. 找到目标文件系统，单击[管理](#)。
4. 单击[挂载使用](#)，进入[挂载点](#)页面。
5. 找到目标挂载点，单击[修改权限组](#)。

-
- 
6. 在修改权限组对话框中，修改权限组，单击确定。

6. 权限组

6.1. 查看权限组列表

您可以在 NAS 控制台查看已经创建的权限组列表。

前提条件

已创建权限组。具体操作，请参见[创建权限组及规则](#)。

操作步骤

1. 登录[文件存储NAS控制台](#)。
2. 选择[文件系统](#) > [权限组](#)，查看该页面内的权限组列表。

文件存储 / 权限组

权限组

通用型NAS

[创建权限组](#) 权限组名称/描述 ▼ 请输入权限组名称或者描述，支持模糊匹配

权限组名称	组织	资源组	类型	规则数目	绑定文件系统数目	创建时间	描述	操作
access-for-mount-target-test1643166291		ResourceSet(cds-cesh-i-xa)	专有网络	0	0	2022年1月26日 11:03:26	-	管理规则 编辑 删除
nas-test-stable		ResourceSet(cds-cesh-i-xa)	经典网络	1	1	2022年1月26日 09:48:39	-	管理规则 编辑 删除

6.2. 删除权限组


您可以在 NAS 控制台删除已经创建的权限组列表。

前提条件

已创建权限组，详情请参见[创建权限组及规则](#)。

操作系统

1. 登录[文件存储NAS控制台](#)。
2. 选择[文件系统](#) > [权限组](#)。
3. 找到目标权限组，单击[删除](#)。

 **说明** 无法删除正在使用的权限组。如果要删除，请先在挂载点列表中解绑此权限组。

4. 在删除确认框中，单击[确定](#)。

6.3. 管理权限组规则

您可以在 NAS 控制台管理权限组规则，包括查看规则、编辑规则和删除规则。

前提条件

已创建权限组及规则，详情请参见[创建权限组及规则](#)。

操作步骤

- 1. 登录文件存储NAS控制台。
- 2. 选择文件系统 > 权限组。
- 3. 找到目标权限组，单击管理规则。
- 4. 在规则列表页面，您可以执行以下操作。

- 查看该权限组的所有规则。

NAS文件系统 / 权限组 / test01 的规则列表

← test01 的规则列表

添加规则

✕

授权地址	读写权限	用户权限	优先级	操作
10.10.10.10/10	读写	所有用户不匿名 (no_anon)	1	编辑 删除
10.10.10.10	只读	root用户匿名 (root_anon)	2	编辑 删除

共2条 < 上一页 1 下一页 >

- 编辑规则：找到目标规则，单击编辑，可修改该规则的授权地址、读写权限、用户权限和优先级。
- 删除规则：找到目标规则，单击删除，在删除对话框中，单击确定。

7. 管理配额

本文介绍如何通过阿里云quota_tool工具在已挂载NAS的机器上管理NAS配额，包括设置配额、查询配额及取消配额。

前提条件

已挂载容量型或性能型NAS下的NFS文件系统。具体操作，请参见[挂载NFS文件系统](#)。

背景信息

阿里云NAS配额功能可以帮助您轻松的查看和管理NAS目录级的配额。目录级配额是指NAS目录下面包含的所有文件的数量和所占用的空间大小。

从配额统计的范围分类，包括全量配额和用户（组）配额。全量配额统计目录下所有用户的文件使用量，用户（组）配额统计目录下某个用户（组）的文件使用量。

从限制级别的范围分类，包括统计型配额和限制型配额。统计型配额只统计使用量，方便用户查看。限制型配额，则会在文件使用量超过限制后，导致创建文件或目录、追加写等操作失败。

注意

- 目前只支持设置统计型配额。
- NAS的配额计算是后台异步的，因此您通过quota_tool工具查询得到的统计信息是有延迟的（正常情况下5~15分钟）。

设置配额

本文文件系统的挂载目录以/mnt为例进行说明。

1. 以root用户登录云服务器ECS（Linux系统）。

quota_tool工具需要运行在已挂载了NAS的机器（如ECS）上，且必须以root用户运行。本文以在ECS上运行quota_tool工具为例进行说明。


2. 下载quota_tool工具。

```
wget https://nasimport.oss-cn-shanghai.aliyuncs.com/quota_tool_v1.0 -O quota_tool
```

3. 添加quota_tool工具的执行权限。

```
sudo chmod a+x quota_tool
```

4. 设置配额。

 **说明** 目前对于单个文件系统，最多只能对10个目录设置配额。

设置配额命令格式为 `sudo ./quota_tool set --dir [DIR] [OPTION]`。

参数	说明
--dir [DIR]	设置配额的目录。例如--dir /mnt/data/。

参数	说明
OPTION	<p>根据需求，选择OPTION进行设置。</p> <div><p> 说明 在选择OPTION时，--accounting为必选，--alluser/--uid/--gid为必选且只能选其一。</p><ul style="list-style-type: none">◦ --accounting：设置统计型配额。◦ --alluser：设置通用目录级配额。◦ --uid：用户Uid。例如--uid 505，只统计Uid为505用户的配额。◦ --gid：用户组Gid。例如--gid 1000，只统计Gid为1000用户组的配额。</div>

下面举例说明设置配额的操作。

- 如果您要为/mnt/data/目录设置统计型配额，统计目录下面所有的文件，请执行以下命令。

```
sudo ./quota_tool set --dir /mnt/data/ --accounting --alluser
```

- 如果您要为/mnt/data/目录设置统计型配额，统计目录下Uid为505用户的所有文件，请执行以下命令。

```
sudo ./quota_tool set --dir /mnt/data/ --accounting --uid 505
```


查询配额

设置了NAS目录级配额后，可以查询目录当前的配额统计信息。

1. 以root用户登录云服务器ECS。
2. 执行以下命令查询配额。

```
sudo ./quota_tool get --dir /mnt/data/ --all
```

其中，--all为可选，可以查询该文件系统当前设置的所有配额。

 **说明**

- 设置配额后初次查询时，有个初始化过程，这期间查询状态为Initializing，初始化完成之后，查询的结果为success。初始化过程时长取决于文件系统的文件和目录数目。
- 初始化完成后日常查询时，由于配额是后台异步计算的，因此查询显示的FileCountReal和SizeReal会有5~10分钟的更新延迟。

```
{
  "Reports": [
    {
      "Path": "/mnt/data",
      "Report": [
        {
          "FileCountLimit": "Empty",
          "FileCountReal": "2",
          "Gid": "All",
          "QuotaType": "Accounting",
          "SizeLimit": "Empty",
          "SizeReal": "4KB",
          "Uid": "All"
        }
      ],
      "ReportStatus": "Success"
    }
  ],
  "Status": 0
}
```

返回的JSON格式数据中每一项参数说明如下所示。

参数	说明
Path	查询的目录。
Report	针对已设置的Uid/Gid的具体统计信息。
ReportStatus	查询状态。
FileCountLimit	文件数量限制，无限制则为Empty。
FileCountReal	当前目录下真实的文件数（包括目录、文件和特殊文件）。
QuotaType	Accounting（统计型配额）和Force（限制型配额）。
Uid	统计对应的Uid（All代表所有Uid）。
Gid	统计对应的Gid（All代表所有Gid）。
SizeLimit	文件大小限制，无限制则为Empty。
SizeReal	当前目录下文件的总大小。


取消配额

设置配额后，您也可以取消配额。

- 1. 登录云服务器ECS。
- 2. 执行以下命令取消配额。

取消配额的命令格式为 `sudo ./quota_tool cancel --dir [DIR] [OPTION]`。

参数	说明
--dir [DIR]	取消配额的目录，例如 <code>--dir /mnt/data/</code> 。

参数	说明
OPTION	<p>根据需求，选择OPTION进行设置。</p> <div><p> 说明 在选择OPTION时，--alluser/--uid/--gid为必选且只能选其一。</p><ul style="list-style-type: none">◦ --alluser：取消通用目录级配额。◦ --uid：用户Uid。例如--uid 505，取消Uid为505用户的配额。◦ --gid：用户Gid。例如--gid 1000，取消Gid为1000用户组的配额。</div>

下面举例说明取消配额的操作。

- 如果您为 */mnt/data/* 目录设置了配额，现在要取消Uid为100用户的配额，请执行以下命令。

```
sudo ./quota_tool cancel --dir /mnt/data/ --uid 100
```

- 如果您为 */mnt/data/* 目录设置了配额，现在要取消全量配额，请执行以下命令。

```
sudo ./quota_tool cancel --dir /mnt/data/ --alluser
```

8. 统一命名空间

本文介绍如何通过阿里云文件存储NAS控制台创建统一命名空间及挂载点，并向统一命名空间添加、移除和修改文件系统、查看统一命名空间详情，实现统一命名空间跨域编排的功能。

功能介绍

统一命名空间允许用户将一个NAS集群内的多个文件系统使用统一的域名挂载使用，这样用户不需要自己维护多个挂载点，以及对应的挂载路径。

和文件系统一样，统一命名空间可以创建自己的挂载点。通过统一命名空间，在操作多个文件系统时，用户可以获得和单个文件系统一致的使用体验。

统一命名空间构建了一个虚拟的根目录，其中的文件系统就是它的一级子目录。添加到统一命名空间的文件系统，依然可以使用自己的挂载点独立挂载。

使用限制

统一命名空间有如下的使用限制：

- 单个统一命名空间下最多只能添加1000个文件系统。
- 文件系统在统一命名空间中的映射名不能超过255个字符，且只能使用大小写字母、数字和以下特殊字符：
.
+
_
(
<
>
@
#
- 对于统一命名空间跨域编排，挂载目录名不超过255个字符，且只能使用大小写字母、数字和以下特殊字符：
.
+
_
(
<
>
@
#
- 单个统一命名空间最多支持创建2个挂载点。
- 同一个地域下，用户可创建的统一命名空间个数不超过20个。
- 统一命名空间目前只支持NFSv3协议挂载。
- 添加到统一命名空间的文件系统，必须和统一命名空间在一个集群的同一个用户下，且存储类型、协议类型、加密类型必须相同。
- 在单个统一命名空间下，文件系统映射名不能重复。
- 文件系统在统一命名空间中只能被映射成一级子目录，且不能修改访问权限和Owner，以及不能设置ACL。

统一命名空间基本功能

- 创建统一命名空间及挂载点。
 - i. 登录[文件存储NAS控制台](#)。
 - ii. 在左侧导航栏，选择统一命名空间 > 统一命名空间列表。
 - iii. 在统一命名空间列表页面，单击创建命名空间并按照提示创建命名空间及挂载点，创建步骤与创建文件系统相似。

NAS文件系统

文件系统

文件系统列表

权限组

统一命名空间

统一命名空间列表

跨域挂载编排

数据服务

生命周期管理

NAS文件系统 / 统一命名空间列表

统一命名空间列表

创建命名空间

文件系统类型: 通用型

存储规格: 全部

命名空间ID

请输入

命名空间ID/描述	组织	资源组	文件系统类型	存储规格	创建时间	协议类	操作
1NS2449433 test_wang	NAS跨域编排	ResourceSet(NAS跨域编排)	通用型NAS	容量型	2020年1月20日 17:49:35	NFS	管理 删除
1NS474acbf four	NAS跨域编排	ResourceSet(NAS跨域编排)	通用型NAS	容量型	2020年1月20日 14:58:23	NFS	管理 删除
1NSb74b48b three	NAS跨域编排	ResourceSet(NAS跨域编排)	通用型NAS	容量型	2020年1月20日 14:57:55	NFS	管理 删除
1NS294afbe two	NAS跨域编排	ResourceSet(NAS跨域编排)	通用型NAS	容量型	2020年1月20日 14:57:41	NFS	管理 删除
1NS1e484f2 one	NAS跨域编排	ResourceSet(NAS跨域编排)	通用型NAS	容量型	2020年1月20日 14:57:29	NFS	管理 删除
1NSba49a75 as	katy	默认资源组	通用型NAS	容量型	2020年1月20日 10:33:06	NFS	管理 删除
1NS624a809 skns3	ascm	DefaultResourceSet (ascm)	通用型NAS	容量型	2020年1月20日 11:05:54	NFS	管理 删除

说明 为了方便后续的跨域挂载，建议不同地域统一命名空间挂载点使用的VPC网段要相互区分。例如：地域1使用 192.168.0.0/16，地域2使用 172.16.0.0/16。关于跨域挂载统一命名空间的具体操作，请参见[统一命名空间跨域编排中的创建VPC](#)。

- 向统一命名空间添加文件系统。
创建好统一命名空间后，您可以添加文件系统，并设置映射名。

说明 这个映射名就是文件系统对应的虚拟目录名。

- 从统一命名空间移除文件系统。
您可以从统一命名空间中移除已添加的文件系统。

说明 这个操作并不会删除文件系统本身，只是从统一命名空间的文件系统列表中移除。

- 修改文件系统的映射名。
您可以修改统一命名空间中文件系统的映射名。

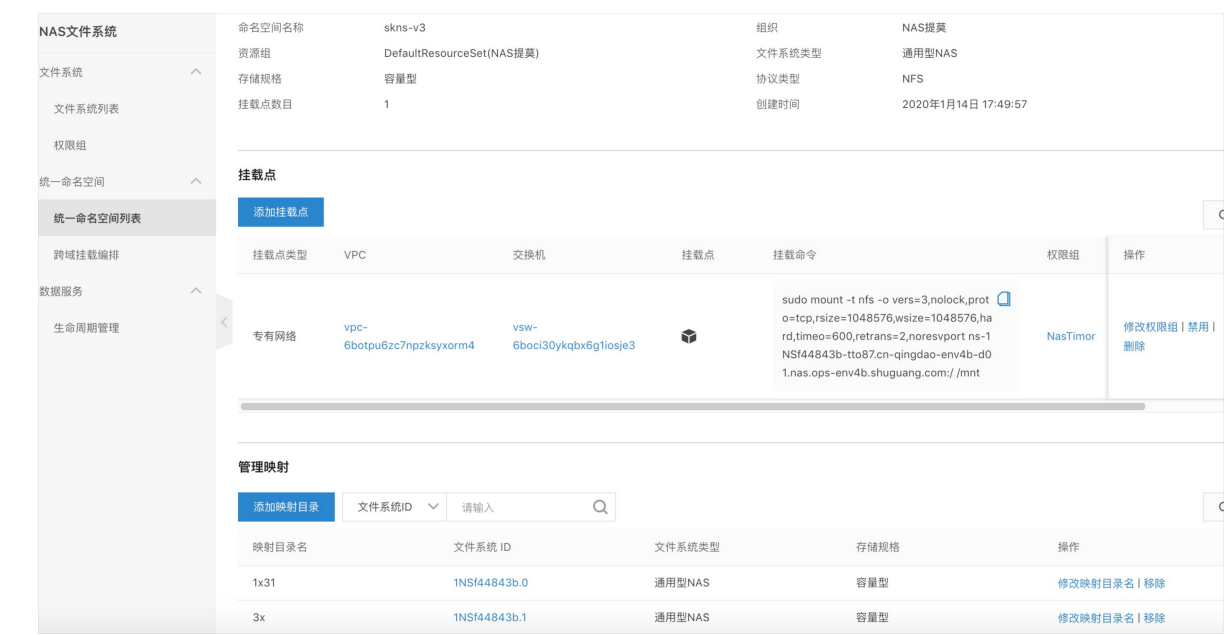
说明 如果存在跨文件系统的软硬连接，修改映射名会导致连接失效。

- 查看统一命名空间详情。
统一命名空间详情有以下三部分数据：
 - 统一命名空间的属性信息
 - 统一命名空间的挂载点列表

说明 您可以创建、删除挂载点。

- 统一命名空间内的文件系统列表

说明 您可以添加、移除文件系统。



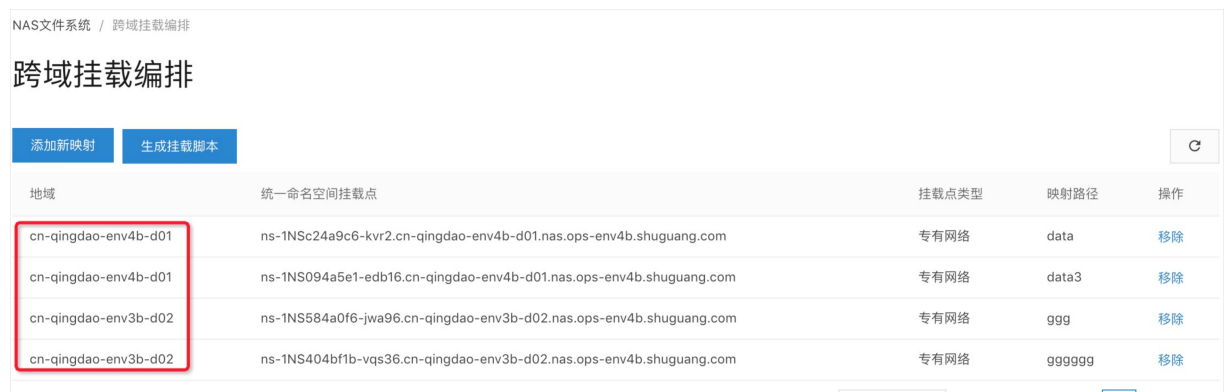
统一命名空间跨域编排

单个命名空间只能添加本域内的文件系统，不能跨域。为了解决跨域使用的问题，引入了跨域编排的功能。跨域编排的使用方式如下所示。

- 在各个域创建一个统一命名空间，以及挂载点。
- 通过跨域编排功能，映射到客户端的本地目录树上。
- 编排完成后，用户指定根目录，生成自动挂载脚本。

注意 跨域编排添加的挂载点和绑定的目录一经设置不能修改。可以移除，但再次添加时，只能绑定到第一次设置的目录上。

各客户端直接使用自动脚本将各域名挂载到对应的本地目录上，达到跨域统一访问的目的。对于各统一命名空间，最终挂载的本地路径就是：`<用户自定根目录>/<统一命名空间的映射路径>`。



不同地域有不同的VPC网络，要跨域挂载统一命名空间，需要做不同地域之间的跨域打通。下面以两个Region的两个VPC为例，介绍如何实现跨域打通和NAS挂载。

1. 创建VPC。
 - i. 登录文件存储NAS控制台。
 - ii. 在顶部菜单栏，单击产品 > 网络 > 专有网络VPC。

iii. 在创建专有网络VPC页面，为Region1和Region2分别创建两个VPC网络，网段选择为：

- Region1: 192.168.1.0/24 (命名skvpc1)
- Region2: 192.168.2.0/24 (命名skvpc2)

创建专有网络VPC

区域

组织 * daily_test

资源集 * ResourceSet(daily_test)

地域 * cn-qingdao-env15-d01

基本配置

共享范围 本资源集

专有网络名称 skvpc1
长度为2~128个字符，以英文大小写字母或中文开头，可包含数字、下划线 () 和连字符 (-)

IPv4网段 ☐ 推荐网段 ☒ 高级配置网段

自定义网段 * 192.168.1.0/24
请输入正确的网段，填写示例：192.168.0.0/16

IPv6网段 不分配

描述

描述长度为2~256个字符，不能以http://和https://开头。

提交

2. 设置跨域高速通道。

在两个Region内分别为对方设置VPC高速通道。

首先，在Region1 (skvpc1) 内为Region2 (skvpc2) 设置VPC高速通道。

- i. 配置Region1 VPC的路由表。
- 将skvpc2的地址段（ 192.168.2.0/24 ）添加到skvpc1的路由表中。
- a. 在左侧导航栏，选择路由表。
- b. 在路由表页面，选择skvpc1对应的实例ID，单击管理。



- c. 选择路由条目列表页签，单击添加路由条目。填写信息。单击创建VPC互联，为skvpc1设置到skvpc2的高速通道。

说明

- 目标网段必须与skvpc2严格一致。
- 下一跳类型选择路由器接口（专有云网络方向）。
- 首次使用是没有可选的专有网络实例的。

添加路由条目

目标网段

IPv4网段

IPv4网段

192.168.2.0 / 24

下一跳类型 *

路由器接口（专有网络方向）

专有网络 *

请选择

创建VPC互联

取消

确定

ii. 创建VPC互联。

- a. 在创建VPC互连页面，选择发起端和接收端VPC ID，互联带宽根据实际需要选择。单击提交。

地域 * cn-qingdao-env15-d01

路由器类型 * VPC路由器

发起端 VPC ID * vpc-ew2 / skvpc1

对端配置

组织 * daily_test

资源集 * ResourceSet(daily_test)

对端地域 * cn-qingdao-env122-d02

接收端路由器类型 * VPC路由器

接收端VPC ID * vpc-jz8 / skvpc2

基本配置

带宽值 * 10000Mbps

提交

- b. 创建成功后，单击返回管理控制台跳转到VPC互联页面，状态已激活，表明从skvpc1到skvpc2互联成功（反向需要在skvpc2设置）。

VPC互联

您可以通过创建对端连接实现VPC互通。

+ 创建VPC互联 返回 刷新

发起端实例	发起端地域	接收端实例	接收端地域	同账号	带宽	创建时间	状态	操作
vpc-ew2 ri-ew2ral	cn-qingdao-env15-d01	vpc-jz8 ri-jz84c	cn-qingdao-env122-d02	否	5 Mbps	2021年12月23日 16:28:42	发起端: 已激活 接收端: 已激活	删除 重建连接

共 1 页 < 1/1 >

iii. 查看VPC互联。

创建成功后，回到添加路由条目页面，新创建的VPC互联就出现在列表里了。

添加路由条目

目标网段 IPv4网段

IPv4网段 192.168.2.0 / 24

下一跳类型 * 路由器接口 (专有网络方向)

专有网络 * vpc-jz8 创建VPC互联

取消 确定

其次，在Region2（skvpc2）内为Region1（skvpc1）设置VPC高速通道。

接着上面的操作：选择新创建的VPC互联，单击确定，添加路由条目。



同样的操作，在Region2为skvpc2添加到skvpc1的路由条目。由于已经创建了skvpc1到skvpc2的高速互联，在添加Region1的路由条目时，可以直接选择。 `vpc-ew2xxxx` 就是skvpc1的VPC ID。

3. 添加NAS权限规则。

- i. 在顶部菜单栏，单击产品 > 存储 > 文件存储NAS。
- ii. 在左侧导航栏，单击权限组，在权限组列表找到目标权限组或者新增权限组后，单击管理规则。
- iii. 单击添加规则。在NAS挂载点使用的VPC权限规则中，添加各VPC网段，设置读写权限。例如：添加skvpc1的IP段，如下图所示。



4. 创建挂载点。

在Region2上，可以创建skvpc2上的挂载点，在指定的统一命名空间上。

在Region1上，可以创建skvpc1上的挂载点，在指定的统一命名空间上。

5. 创建ECS。

以Region1为例，创建ECS时选择打通了VPC的skvpc1后，ECS就可以直接挂载到两个挂载点上了。创建ECS如下图所示。

ECS概览 / 实例 / 创建云服务器

创建云服务器

1

基础配置

2

网络配置

网络

专有网络vpc *

vpc-ew2-3/skvp1

创建VPC

交换机 VSwitch *

vsw-ew2

创建交换机

私网IP

请输入私网IP,格式示例192.168.100.102,且指定的IP地址必须在所选择的虚拟交换机网段内。

IPv6

不分配

安全组 *

请选择

创建安全组

 说明 在实际使用中，ECS通常使用独立的VPC。两个Region上的统一命名空间的挂载点使用的VPC之间是不需要相互打通的，需要打通的是ECS的VPC到各挂载点的VPC。

9. 生命周期管理

本文介绍如何通过阿里云文件存储NAS控制台实现生命周期管理功能，配置生命周期管理策略，将文件系统的冷数据转储至低频（IA）介质，包括如何添加生命周期管理策略、查看生命周期管理策略、修改生命周期管理策略、查询通用型存储和低频（IA）介质存储的使用量。

前提条件

已挂载容量型或性能型NAS下的NFS文件系统。具体操作，请参见[挂载NFS文件系统](#)。

背景信息

阿里云文件存储NAS生命周期管理功能可以帮助您管理NAS上数据的冷热分离，通过配置生命周期策略，用户可以将长时间没有访问的文件，自动保存到低频（IA）介质存储容量。低频（IA）介质存储容量的成本更低，通过将冷数据转存到低频（IA）介质存储容量，用户可以降低这部分存储量的成本。在低频（IA）介质存储容量保存的数据，用户依然按照原有的方式进行访问。

使用限制

文件存储NAS生命周期管理功能目前只支持NFS类型的文件系统，目前不支持SMB类型的文件系统，也不支持启用了加密功能的文件系统。

重要提示


专有云NAS的生命周期管理功能是将冷数据转储到用户指定的OSS Bucket上。该用户为NAS文件系统和OSS Bucket的所有者。

- 在将数据手动召回到NAS之前，用户不能删除该Bucket。否则会导致数据丢失，还可能导致NAS集群逐渐不可使用。
- 用户也不能收回对NAS的RAM授权。
- 用户需要保证对应OSS Bucket的权限，防止数据泄露。
- 强烈建议用户为NAS生命周期管理功能使用独立的OSS Bucket，以降低因为和其它业务使用同一个OSS Bucket导致误删除NAS冷数据的风险。

准备工作

1. 开通RAM授权。

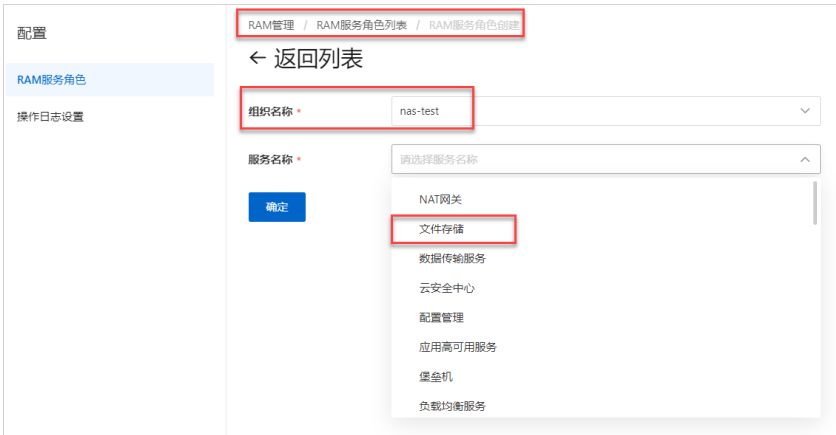
要使用生命周期管理功能，您需要首先开通OSS对NAS服务的授权，这样NAS可以访问您的OSS Bucket来存取数据。

 **注意** 创建RAM角色时指定的组织就是当前所在的部门（例如：nas-test）。

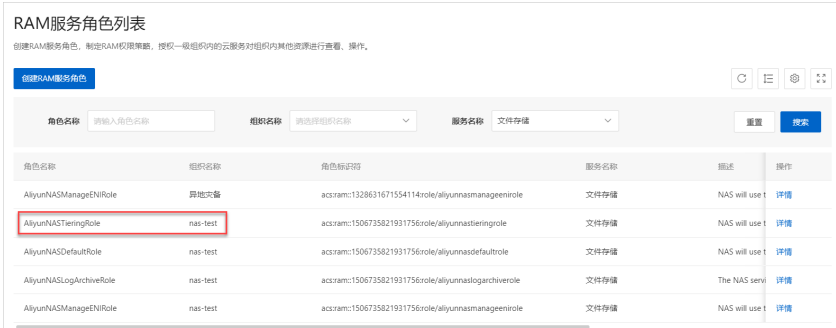
对同一个部门，RAM授权只需要开通一次，不需要在每次为文件系统配置生命周期管理功能时都执行一次。

- i. 登录Apsara Uni-manager运营控制台。
- ii. 在顶部菜单栏，单击**配置**。

iii. 在RAM服务角色列表页面，单击创建RAM服务角色，为用户开通OSS授权。



iv. 查看角色列表中nas-test组织的NAS授权情况，确认有AliyunNASTieringRole。



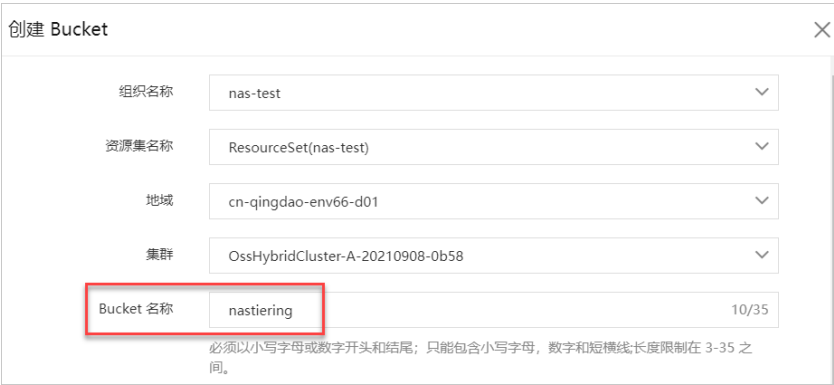
2. 创建OSS Bucket。

您既可以使用已有的一个OSS Bucket，也可以新创建一个OSS Bucket。您可以为每个文件系统分别设置不同的OSS Bucket，NAS服务对此不做限制。

说明 如果使用已有的一个OSS Bucket，需要保证：

- Bucket在地域内的第一个集群中。集群的分辨方法为：第一个集群域名以oss-开头，其后面的集群则是以ossxxxx-开头。
- Bucket和绑定的文件系统的归属部门需要保持一致。

在顶部菜单栏，选择产品 > 对象存储 OSS。在左侧导航栏，选择Bucket列表，单击创建Bucket。为冷数据存储创建一个OSS Bucket（例如：nastiering）。



② 说明 在创建Bucket时，需要保证：

- 存储类型选择标准存储，OSS集群选择地域内的第一个集群。集群的分辨方法为：第一个集群域名以oss-开头，其后面的集群则是以ossxxx-开头。
- Bucket和绑定的文件系统的归属部门需要保持一致。

开始使用

1. 添加生命周期管理策略

- i. 在上方的导航栏中，选择产品 > 文件存储NAS。
- ii. 在左侧导航栏，单击生命周期管理。

iii. 在生命周期管理页面，单击创建策略，创建生命周期管理策略。

创建生命周期管理策略

* 策略名称 ?

fortest

* 分级存储类型 ?

低频型

* 文件系统

15a3d4b8b4/nas-test

* 目录路径 ?

/

☒ 递归子目录 ?

* 管理规则 ?

距最近访问14天以上

* OSS Bucket ?

rick-test-005

确定

取消

通过为指定文件系统的特定目录创建生命周期管理策略，NAS服务会自动将满足条件的文件转存到低频（IA）介质，无需用户介入。您在创建生命周期管理策略时可以选择以下配置项：

- 策略名称：自定义的名字，不同策略不能重复。
- 文件系统：选择一个需要配置生命周期管理策略的文件系统实例。
- 目录路径：指定该实例上的一个目录路径（以“/”开始）。
可以填写“/”，表示根目录。
选中递归子目录复选框，可以递归该路径下的所有子目录。
- 管理规则：目前支持用户选择系统预置的4个条件之一，可以选择最近14/30/60/90天未访问的文件。
- OSS Bucket：需要归档到的OSS Bucket。

? 说明 一个文件系统只允许归档到同一个OSS Bucket中。
列表中只会显示文件系统所在组织的OSS Bucket列表。

2. 查看已配置的生命周期管理策略

在生命周期管理页面，查看已配置的生命周期管理策略。还可以根据文件系统ID进行筛选。

NAS文件系统 / 生命周期管理							
生命周期管理							
创建策略		文件系统 ID: 请选择					
策略名称	存储类型	文件系统ID	目录路径	是否递归子目录	策略详情	创建时间	操作
spark	低频存储	1NS854b0...	/smzq	是	关联规则: 距最近访问14天以上	2020年1月22日 16:41:13	修改 删除
quota	低频存储	193b749f62	/quota	是	关联规则: 距最近访问60天以上	2020年1月17日 15:35:26	修改 删除
lifecycle1	低频存储	15ab64b7...	/aaaaah	是	关联规则: 距最近访问90天以上	2020年1月17日 10:18:44	修改 删除
test	低频存储	15333490...	/home	否	关联规则: 距最近访问60天以上	2020年1月16日 18:00:03	修改 删除
guaguag	低频存储	15333490...	/gugu	是	关联规则: 距最近访问60天以上	2020年1月16日 17:10:55	修改 删除
timoraa	低频存储	169084a9...	/cccccc	是	关联规则: 距最近访问14天以上	2020年1月16日 14:54:26	修改 删除

3. 修改生命周期管理策略

在生命周期管理页面，选择已配置的生命周期管理策略进行修改。

修改生命周期管理策略

* 策略名称 ?

test

* 分级存储类型 ?

低频型

* 文件系统

129f1491d8

* 目录路径 ?

/

☐ 递归子目录 ?

* 管理规则 ?

距最近访问14天以上

距最近访问14天以上

距最近访问30天以上

距最近访问60天以上

距最近访问90天以上

取消

用户可以选择以下配置项完成对生命周期管理策略的修改：

- 递归子目录
- 管理规则

4. 查询通用型存储和低频（IA）介质存储的使用量

在导航栏，单击文件系统列表，选择配置了生命周期管理策略的文件系统，查询主存储和低频（IA）介质存储的使用量。

基础信息			
文件系统ID	129f1491d8	命名空间ID	-
文件系统类型	通用型NAS	地域	cn-qingdao-env66-d01
文件系统名称	TESTLIUNAS	组织	appstreaming
资源组	ResourceSet(appstreaming)	存储规格	容量型
使用量	0 MB	低频介质用量	0 MB
状态	✓ 运行中	最大容量	102.40 GB
挂载点	1	协议类型	NFS
创建时间	2021年12月17日 19:03:23	数据生命周期管理	已启用 配置策略

10. 目录级读写权限ACL

10.1. 简介

阿里云NAS支持NFSv4 ACL和POSIX ACL。本文简要介绍POSIX ACL和NFSv4 ACL的概念及其相关注意事项。

企业级用户通过共享文件系统在多个用户和群组之间共享文件时，权限的控制和管理成为了不可缺少的功能。针对不同目录或文件，文件系统管理员需要给不同的用户和群组设置相应的权限，实现访问隔离。针对这个需求，阿里云NAS支持NFS ACL功能，ACL是与文件或目录关联的权限列表，由一个或多个访问控制项（ACE）组成。

POSIX ACL是NFSv3协议能够扩展支持的权限控制协议。POSIX ACL对mode权限控制进行了扩展，能够对owner、group、other以外的特定用户和群组设置权限，也支持权限继承。更多信息，请参见[acl - Linux man page](#)。

NFSv4 ACL是NFSv4协议能够扩展支持的权限控制协议，提供比POSIX ACL更细粒度的权限控制。更多信息，请参见[nfs4_acl - Linux man page](#)。

您可以使用NFSv3协议挂载含有NFSv4 ACL的文件系统，挂载后NFSv4 ACL会被转化为POSIX ACL。您也可以使用NFSv4协议挂载含有POSIX ACL的文件系统，挂载后POSIX ACL会被转化为NFSv4 ACL。但由于NFS4 ACL和POSIX ACL并不完全兼容，加上mode和ACL之间的互操作也无法尽善尽美，另外NAS NFSv3挂载不支持锁，所以建议您在使用的NFS ACL功能时尽量只使用NFSv4协议挂载并设置NFS4 ACL，不使用mode和POSIX ACL。更多关于特性的信息，请参见[特性](#)。

POSIX ACL注意事项

- 使用继承（default）方式让子目录树获得相同的ACL，避免每次创建文件或目录都需要设置ACL。
- 因为每次系统进行权限检查时，都需要扫描所有ACE，所以尽量减少ACE数量。滥用ACL会造成文件系统性能下降。
- 请谨慎使用递归方式（`setfacl -R`）设置ACL。针对大的目录树进行递归操作时，可能产生较大的元数据压力影响业务运行。
- 请在设置ACL前，先规划好用户组及其权限，每个用户可属于一个或多个用户组。如果您要增加、删除、修改用户权限，只需调整用户所在的用户组，只要用户组结构不变就无需修改用户组的ACL。在设置ACL时，尽量使用用户组而非单个用户，通过用户组设置ACL，简单省时，权限清晰易于管理。
- 如果跨客户端使用POSIX ACL，需要给相同的用户名或群组名设置相同的UID/GID，因为NAS后端存储的是UID/GID。
- 建议将other的权限设置到最低，因为other允许的权限对任何用户都适用。如果某个ACE的权限低于other，则可能是个安全漏洞。
- 建议将other的权限设置到最低，所以在操作前先执行 `umask 777`，这样创建文件或目录时传入的mode会变成000，使默认的权限最小化。更多信息，请参见[umask与默认mode](#)。
- 启动POSIX ACL后other会变为everyone，mode的other也会变为everyone。在权限判断时other的权限会作为everyone的权限进行判断。

NFSv4 ACL注意事项

- 使用UID/GID（如UID 1001）设置ACL。
- 强烈建议使用NFSv4 ACL之后请勿使用mode。
- `nfs4_setfacl` 提供了-a、-x、-m等命令行选项去增加、删除、修改ACE的参数，但建议使用 `nfs4_setfacl -e <file>` 可以更直观的进行交互式编辑。
- NAS NFSv4 ACL只支持Allow不支持Deny，所以建议将everyone的权限设置到最低，因为被everyone允许

的权限对任何用户都适用。如果某个ACE的权限低于everyone，则很可能是个安全漏洞。

- NFS4 ACL对权限划分很细，尤其是写权限细分在绝大多数场景下是不必要的。例如：当一个文件有写权限（w）但没有追加写的权限（a）时，执行写文件操作可能返回错误，在目录下做修改也有类似情况。为了避免意想不到的权限错误，建议使用 `nfs4_setfacl` 操作写权限时使用大写W，`nfs4_setfacl` 会将大写W转化为完整的写权限（对文件为wadT，对目录为wadTD）。
- 使用继承的方式让子目录树获得相同的ACL，避免每次创建文件或目录都需要设置ACL。
- 因为每次系统进行权限检查时，都需要扫描所有ACE，所以尽量减少ACE数量。滥用ACL会造成文件系统性性能下降。
- 请谨慎使用递归方式（`nfs4_setfacl -R`）设置ACL。针对大的目录树进行递归操作时，可能产生较大的元数据压力影响业务运行。
- 请在设置ACL前，先规划好用户组及其权限。每个用户可属于一个或多个用户组，如果您要增加、删除、修改用户权限，只需调整用户所在的用户组，只要用户组结构不变就无需修改用户组的ACL。在设置ACL时，尽量使用用户组而非单个用户，通过用户组设置ACL，简单省时，权限清晰易于管理。

10.2. 特性

本文介绍NFSv4 ACL和POSIX ACL相关的特性。

NAS NFSv4 ACL特性

- ACE类型只支持Allow，不支持Deny、Audit和Alarm。

Deny ACE会极大增加权限设置的复杂性，容易给用户造成混淆而留下安全问题。业界已达成共识应尽量避免使用Deny ACE。关于不支持Deny ACE的更多信息，请参见[常见问题](#)。

Audit ACE和Alarm ACE在阿里云NAS NFS上不起作用。如果需要审计和报警功能，可以在阿里云控制台上进行配置。

- 未设置ACL的文件或目录会呈现与之mode对应的默认ACL。示例如下：

i. 执行 `touch file` 命令，进入file文件。

ii. 执行 `ls -l file` 命令，查看file文件的权限。

```
-rw-r--r--. 1 root root 0 May  6 14:27 file
```

iii. 执行 `nfs4_getfacl file` 命令，查看file文件当前的ACL权限。

```
# file: file
A::OWNER@:rwatTnNcCy
A::GROUP@:rtncy
A::EVERYONE@:rtncy
```

- ACE按照一定顺序排列并去重，使ACL显示结果更清晰易懂。

用户增加或修改ACE时，如果ACL中已经存在继承类型完全的ACE，则新的ACE会和旧的ACE的Allow bits进行合并。例如：

- 执行 `nfs4_getfacl file` 命令，查看file文件ACL权限。

排序时owner、group、everyone对应的ACE总是排在最前面。

```
# file: file
A::OWNER@:rwxtTnNcCy
A::GROUP@:rtncy
A::EVERYONE@:rtncy
A::1001:rwxtTnNcCy
```

- 为用户1009增加一条读写权限的ACE，按照顺序排序后排在用户1001后面。

- 执行命令

```
nfs4_setfacl -a A::1009:X file
nfs4_getfacl file
```

- 返回示例

```
# file: file
A::OWNER@:rwxtTcCy
A::GROUP@:rwatcy
A::EVERYONE@:tcy
A::1001:rwxtTnNcCy
A::1009:waxtTncCy
```

- 为用户1009增加执行权限的ACE，系统自动将新增的执行权限合并到用户1009已有的ACE中。

- 执行命令

```
nfs4_setfacl -a A::1009:W file
nfs4_getfacl file
```

- 返回示例

```
# file: file
A::OWNER@:rwxtTcCy
A::GROUP@:rwatcy
A::EVERYONE@:tcy
A::1001:rwxtTnNcCy
A::1009:waxtTncCy
```

- 为用户1009增加fd继承权限的ACE，系统会将它拆分为只拥有继承能力的ACE和只对本文件起作用的ACE，并将两个ACE与ACL中同继承类型的ACE进行合并。

- 执行命令

```
nfs4_setfacl -a A:fd:1009:R file
nfs4_getfacl file
```

- 返回示例

```
# file: file
A::OWNER@:rwaxTcCy
A::GROUP@:rwtcy
A::EVERYONE@:tcy
A::1001:rwaxTNCy
A::1009:rwaxTNCy
A:fdi:1009:r
```

- 支持所有继承特性。

- i. 假设当前目录dir的权限是owner可写，group可读，everyone不能访问。

- 执行命令

```
nfs4_getfacl dir
```

- 返回示例

```
# file: dir
A::OWNER@:rwaDxtTnNcCy
A::GROUP@:rxtcy
A::EVERYONE@:tnCy
```

- ii. 给用户1000增加读写权限并且可继承。

- 执行命令

```
nfs4_setfacl -a A:fd:1000:rwx dir
nfs4_getfacl dir
```

- 返回示例

```
# file: dir
A::OWNER@:rwaDxtTcCy
A::GROUP@:rxtcy
A::EVERYONE@:tcy
A::1000:rwx
A:fdi:1000:rwx
```

- iii. 在目录dir下创建的文件或目录就自动带有继承的ACE。

- 在目录dir下创建文件

- 执行命令

```
touch dir/file
nfs4_getfacl dir/file
```

- 返回示例

```
# file: dir/file
A::OWNER@:rwatTcCy
A::GROUP@:rwatcy
A::EVERYONE@:rwatcy
A::1000:rwX
```

- 在目录dir下创建目录

- 执行命令

```
mkdir dir/subdir
nfs4_getfacl dir/subdir
```

- 返回示例

```
# file: dir/subdir
A::OWNER@:rwaDxtTcCy
A::GROUP@:rwaDxtcy
A::EVERYONE@:rwaDxtcy
A:fdi:1000:rwX
```

② 说明

- 建议EVERYONE权限尽量小。在操作前请先执行 `umask 777`，这样创建文件或目录时传入的mode会变成000，可以让默认的权限最小化。更多信息，请参见[umask与默认mode](#)。
- Linux文件或目录的系统调用，默认会传入mode作为参数。按照RFC7530协议标准，需要在继承ACL之后再叠加上mode操作修改ACL，而按照协议如果修改了group的mode，需要保证所有群组的ACE都小于等于group mode的权限。而这会导致群组的继承失效。例如：子文件原本要继承Group A: RWX，但是默认传入的mode是GROUPS: R，则子文件的Group A的ACE会变成Group A: R。为了规避该问题，实际情况mode不会修改ACL除owner、group、everyone之外的其他群组，语义更简单。需要移除某个群组的权限可以直接删除对应的ACE。

- 多个机器间的用户名与UID/GID的映射需要自行维护。

目前阿里云NAS NFS鉴权采用的是IP安全组，不支持用户名鉴权。用户设置的NFSv4 ACL在后端存储的是UID/GID的ACE，在NFSv4 ACL客户端显示时会自动加载本地的`/etc/passwd`将UID/GID转化为用户名/群组名。您需要管理多个机器间的用户名与UID/GID之间的映射，确保同一个用户名或群组名映射到相同的UID/GID，以免发生错误。

- 支持通过Extended Attributes输出NFSv4 ACL。

- 执行命令

```
getfattr -n system.nfs4_acl file
```

- 返回示例

```
# file: file
system.nfs4_acl=0sAAABgAAAAAAAAAABYBhwAAAAZPV05FUkAAAAAAAAAAAAAAAAABIAhwAAAAZHUK9VUEAAA
AAAAAAAAAAAAABIAhwAAAAIFVkvSWU9ORUAAAAAAAAAAAAAAAAAAAAAAEAAAAEMTAwMAAAAAAAAAALAAAAwAAAAQx
MDAwAAAAAAAAEAAFGQAAAABTEwMDAxAAAA
```

- 支持cp等工具迁移NFSv4 ACL。

阿里云NAS支持使用[Redhat NFSv4 ACL迁移工具说明](#)中提到的cp、tar、rsync工具迁移NFSv4 ACL。

下面例子中 `cp --preserve=xattr file1 file2` 拷贝file1到file2时拷贝了ACL。 `cp -ar dir1 dir2` 拷贝dir1到dir2时拷贝了ACL。

 说明 rsync工具可能由于版本低于3.1.2而不能迁移NFSv4 ACL。

- 示例一：迁移文件ACL。

a. 执行 `nfs4_getfacl file1` 命令，查看file1文件的ACL权限。

```
# file: file1
A::OWNER@:rwatTcCy
A::GROUP@:rwatcy
A::EVERYONE@:rwatcy
A::1000:rtncy
```

b. 执行 `cp --preserve=xattr file1 file2` 命令，拷贝file1 ACL至file2。

- 示例二：迁移目录ACL。

a. 执行 `nfs4_getfacl file2` 命令，查看file2文件的ACL权限。

b. 执行 `cp -ar dir1 dir2` 命令，拷贝dir1 ACL至dir2。

```
# file: file2
A::OWNER@:rwatTcCy
A::GROUP@:rwatcy
A::EVERYONE@:rwatcy
A::1000:rtncy
```

- 支持NFSv4 ACL和mode之间的互操作，修改ACL可能引起mode的改变，反之亦然。

例如文件file当前mode为0666。文件权限和ACL权限示例如下：

- 执行 `ls -l file` 命令，查看file文件权限。

```
-rw-rw-rw-. 1 root root 0 May 3 2019 file
```

- 执行 `nfs4_getfacl file` 命令，查看file文件的ACL权限。

```
# file: file
A::OWNER@:rwatTcCy
A::GROUP@:rwatcy
A::EVERYONE@:rwatcy
```

- 通过设置mode给owner增加执行权限，相应ACE也会增加执行权限。示例如下：

- 执行 `chmod u+x file` 命令，给owner增加执行权限。
- 执行 `ls -l file` 命令，查看文件权限。

```
-rwxrwx-rw-. 1 root root 0 May  3  2019 file
```

- 执行 `nfs4_getfacl file` 命令，确认owner已增加执行权限。

```
# file: file
A::OWNER@:rwaxtTcCy
A::GROUP@:rwatcy
A::EVERYONE@:rwatcy
```

- 通过设置ACE给group增加执行权限，相应mode也会增加执行权限。

- 执行命令 `nfs4_setfacl -a A::GROUP@:x file` 命令，给group增加执行权限。
- 执行 `ls -l file` 命令，查看file文件权限。

```
-rwxrwxrwx-. 1 root root 0 May  3  2019 file
```

② 说明

- 在互操作中ACL的everyone和UNIX mode中的other等价，修改mode other会直接修改ACE EVERYONE，这对权限语义有轻微的影响。例如：当前mode为rw-----，执行 `chmod o+r` 后，所有人包括owner和group会获得读权限，因为ACE EVERYONE + r；而在纯UNIX mode的模式下owner和group仍然没有读权限。
- 在没有设置过NFSv4 ACL时，mode other仍然保持other的语义。设置过NFSv4 ACL后，mode other将变成everyone的语义并保持everyone语义。强烈建议在使用NFSv4 ACL之后请勿使用mode。

- 支持NFSv4 ACL和POSIX ACL的互操作。

可以使用NFSv3协议挂载含有NFSv4 ACL的文件系统，挂载后NFSv4 ACL会被转化为POSIX ACL。也可以用NFSv4协议挂载含有POSIX ACL的文件系统，挂载后POSIX ACL会被转化为NFSv4 ACL。

② 说明 由于POSIX ACL和NFSv4 ACL的语义不完全相同。例如：POSIX ACL继承不区分文件和目录，POSIX ACL的权限只有rwx而NFSv4 ACL更丰富。强烈建议只使用NFSv4 ACL或者只使用POSIX ACL，尽量避免混用。

假设用NFSv4 ACL设置了dir0，权限示例如下：

- 执行命令

```
sudo nfs4_getfacl dir0
```

- 返回示例

```
A::OWNER@:tTnNcCy
A::GROUP@:tnCy
A::EVERYONE@:tnCy
A:fdi:EVERYONE@:tnCy
A:fdi:OWNER@:tTnNcCy
A:fdi:GROUP@:tnCy
A:g:19064:rxtncy
A:g:19065:rwaDxtTnNcCy
A:fdig:19064:rxtncy
A:fdig:19065:rwaDxtTnNcCy
```

POSIX ACL的dir0权限如下。

- 执行命令

```
sudo getfacl dir0
```

- 返回示例

```
user::---
group::---
group:players:r-x
group:adminis:rwX
mask::rwX
other::---
default:user::---
default:group::---
default:group:players:r-x
default:group:adminis:rwX
default:mask::rwX
default:other::---
```

假设用NFSv4 ACL设置了dir0/file权限如下。

- 执行命令

```
sudo nfs4_getfacl dir0/file
```

- 返回示例

```
A::OWNER@:tTnNcCy
A::GROUP@:tnCy
A::EVERYONE@:tnCy
A:g:19064:rxtncy
A:g:19065:rwaxTnNcCy
```

POSIX ACL的dir0/file权限如下。

- 执行命令


```
sudo getfacl dir0/file
```

- 返回示例

```
user::---
group::---
group:players:r-x
group:adminis:rwX
mask::rwX
other::---
```

- NFSv4 ACL数量限制。

默认情况下，阿里云NAS支持每个文件系统里不完全相同的ACL的数量上限为10万个，每个ACL中ACE数量上限为500个。

 **说明** 使用时请勿滥用ACL和ACE，减少权限判断时占用的时间和资源。

NAS POSIX ACL特性

- other的权限适用于所有人。


包括user、group和所有在ACE里出现的用户，等价于NFSv4 ACL的everyone。

 **说明** 强烈建议任何情况下只给other赋予最小权限。

例如：*myfile*文件中有如下ACL。虽然包含alice的ACE中没有写权限，但因为other有写权限，所以用户alice也拥有写权限。

```
# file: myfile
# owner: root
# group: root
user::rw-
user:alice:r--
group::r--
mask::r--
other::rw-
```

- 执行 `chmod` 命令不会修改非mode的ACE。

 **说明** 对于设置了POSIX ACL的文件尽量避免修改mode，请使用修改ACL的方式设置权限。

- i. 例如：*myfile*文件中有一条ACE为赋予群组players读写权限。

```
# file: myfile
# owner: root
# group: root
user::rw-
user:player:rw-
group::rw-
group:players:rw-
mask::rw-
other::---
```

- ii. 执行 `chmod g-w myfile` 或 `chmod u-w myfile` 命令后，并不会修改用户player和群组players的

权限。这与POSIX ACL规范相比有差异，但是可以保证修改mode不会影响POSIX ACL设置的非通用用户和群组的权限。

```
# file: myfile
# owner: root
# group: root
user::r--
user:player:rw-
group::r--
group:players:rw-
mask::rw-
other::---
```

- 如果文件中的group和other都没有执行权限（x），那么ACE中的执行权限也不起作用。

这是由客户的Linux系统决定的。虽然NAS服务端返回的是允许执行，但是NAS客户端要求group或者other必须带有执行权限才能真正允许执行。

例如myfile文件中的group和other都没有执行权限，则用户player也不能执行该文件。示例如下：

```
# file: myfile
# owner: root
# group: root
user::rw-
user:player:r-x
group::r--
mask::r-x
other::r--
```

如果group有了执行权限，那么用户player也有执行权限。示例如下：

```
# file: myfile
# owner: root
# group: root
user::rw-
user:player:r-x
group::r-x
mask::r-x
other::r--
```

- 如果目录上设置了可继承的NFSv4 ACL，那么在NFSv3下此行为可能会不符合POSIX ACL标准。

因为NFSv4 ACL继承可以分为文件继承和目录继承，而POSIX ACL是文件和目录均继承。

 说明 建议您避免混用NFS4 ACL和POSIX ACL，一个文件系统只使用一种NFS版本进行挂载。

- 不支持修改Mask值。

NAS POSIX ACL的Mask值由所有的用户和群组的权限的或操作产生，并无实际意义，也不会被修改。

- 多个机器间的用户名与UID/GID的映射需要由您自己维护。

目前阿里云NAS NFS鉴权采用的是IP安全组，不支持用户名鉴权。您设置的POSIX ACL在后端存储的是用户UID/GID的ACE，在POSIX ACL客户端显示时会自动加载本地的/etc/passwd将UID/GID转化成用户名/群组名。您需要管理多个机器间的用户名与UID/GID之间的映射，确保同一个用户名或群组名映射到相同的UID/GID，以免发生错误。

- 支持通过Extended Attributes输出POSIX ACL。

- 执行命令

```
getfattr -n system.posix_acl_access file
```


- 返回示例

```
# file: file
system.posix_acl_access=0sAgAAAAEAAAD/////AgAFACAEAAAEAAAA/////xAABQD/////IAABAP/////8=
```

- 支持cp等工具迁移POSIX ACL。

阿里云NAS支持使用[Redhat NFSV4 ACL迁移工具说明](#)中提到的cp、tar、rsync迁移POSIX ACL

下面例子中 `cp --preserve=xattr file1 file2` 拷贝file1到file2时拷贝了ACL。 `cp -ar dir1 dir2` 拷贝dir1到dir2时拷贝了ACL。

 说明 rsync工具可能由于版本低于3.1.2而不能迁移POSIX ACL。

- 示例一：迁移文件ACL权限。

- a. 执行 `getfacl file1` 命令，查看file1文件的ACL权限。

```
user::---
user:player:r-x
group::---
mask::r-x
other::--x
```

- b. 执行 `cp --preserve=xattr file1 file2` 命令，拷贝file1 ACL至file2。

- 示例二：迁移目录ACL。


- a. 执行 `getfacl file2` 命令，查看file2的ACL权限。

```
# file: file2
user::---
user:player:r-x
group::---
mask::r-x
other::--x
```

- b. 执行 `cp -ar dir1 dir2` 命令，拷贝dir1 ACL至dir2。

- POSIX ACL数量限制。

默认情况下，阿里云NAS支持每个文件系统里不完全相同的ACL的数量上限为10万个，每个ACL中ACE数量上限为500个。

 说明 使用时请勿滥用ACL和ACE，减少权限判断时占用的时间和资源。

常见问题

为什么ACE类型不支持Deny?

- ACE在ACL中的位置起决定性作用。

NFSv4 ACL并不强制进行ACE排序，Deny可能被设置在任何位置。假设ACL有两个ACE（A::Alice:r和D::Alice:r），两个ACE的先后顺序会直接决定Alice是否具有读权限。

 说明

您在设置ACL时，需要非常注意ACE的位置。

- ACL中的ACE数量急剧膨胀。
因为没有强制进行ACE排序，ACL列表里的ACE难以合并和去重。长期往ACL里加ACE，可能膨胀到几十上百条ACE，在判断权限控制结果时需要扫描所有ACE，费时费力。
- 因为mode没有Deny功能，如果使用Deny会使ACL与mode的互操作变得更复杂。
 - 在有Deny的情况下，如果mode发生变化，则可能需要往ACL中添加多条ACE。例如把mode改成-rw-rw-rw，则需要按顺序在ACL头部添加如下内容。

```
A::OWNER@:rw
D::OWNER@:x
A::GROUP@:rw
D::GROUP@:x
A::EVERYONE@:rw
D::EVERYONE@:x
```

- 如果没有Deny，ACE可以排序和去重并且不区分everyone和other，如果mode发生变化，修改ACL也非常方便，只需找到owner、group、everyone所在ACE并改成如下内容即可。

```
A::OWNER@:rw
A::GROUP@:rw
A::EVERYONE@:rw
```

- NFSv4 ACL和POSIX ACL无法互相转化。
POSIX ACL并不支持Deny，NFSv4 ACL如果包含Deny则无法转化为POSIX ACL。

10.3. 使用POSIX ACL进行权限管理

本文介绍在使用NFSv3协议挂载的文件系统上，如何设置POSIX ACL来进行文件或目录权限管理。

前提条件

已使用NFSv3协议挂载文件系统，具体操作，请参见[挂载NFS文件系统](#)。

命令说明

在设置POSIX ACL前，请先熟悉相关操作命令。

命令	说明
getfacl <filename>	查看文件当前的ACL。
setfacl -m g::w <filename>	给GROUP设置写权限。
setfacl -m u:player:w <filename>	给用户player设置写权限。
setfacl -m g:players:rwx <filename>	给用户组players设置读写执行权限。
setfacl -x g:players <filename>	删除用户组players的权限。

命令	说明
<code>getfacl file1 setfacl --set-file=- file2</code>	将文件 <i>file1</i> 的ACL复制到文件 <i>file2</i> 上。
<code>setfacl -b file1</code>	删除文件 <i>file1</i> 上的所有非mode的ACE。
<code>setfacl -k file1</code>	删除文件 <i>file1</i> 上的所有default的ACE。
<code>nfs4_setfacl -R -m g:players:rw dir</code>	对目录树 <i>dir</i> 下的文件和目录增加用户组players读写的权限。
<code>setfacl -d -m g:players:rw dir1</code>	用户组players对目录 <i>dir1</i> 下新创建的文件和目录都有读写权限。

操作步骤

您可以参考以下步骤，为目录或文件设置NFS ACL实现权限管理。

1. 创建用户和群组。

本文假设创建普通用户player，属于普通用户群组players；管理员admini，属于管理员群组adminis；另外再创建一个用户anonym。

```
sudo useradd player
sudo groupadd players
sudo usermod -g players player
sudo useradd admini
sudo groupadd adminis
sudo usermod -g adminis admini
sudo useradd anonym
```

2. 对目录或文件设置POSIX ACL实现权限管理。

本文假设创建目录 *dir0*，针对目录 *dir0* 中的所有文件，授予players只读权限，授予admins读写执行权限，不授予其他用户权限。

```
sudo umask 777
sudo mkdir dir0
sudo setfacl -m g:players:r-x dir0
sudo setfacl -m g:adminis:rw-x dir0
sudo setfacl -m u::--- dir0
sudo setfacl -m g::--x dir0
sudo setfacl -m o::--- dir0
sudo setfacl -d -m g:players:r-x dir0
sudo setfacl -d -m g:adminis:rw-x dir0
sudo setfacl -d -m u::--- dir0
sudo setfacl -d -m g::--x dir0
sudo setfacl -d -m o::--- dir0
```

设置完成后，可执行 `sudo getfacl dir0` 查看设置结果。

```
# file: dir0
# owner: root
# group: root
user:---
group:--x
group:players:r-x
group:adminis:rwX
mask::rwX
other:---
default:user:---
default:group:--x
default:group:players:r-x
default:group:adminis:rwX
default:mask::rwX
default:other:---
```

3. 验证ACL设置结果。

i. 验证用户admini具有读写权限。

```
sudo su admini -c 'touch dir0/file'
sudo su admini -c 'echo 123 > dir0/file'
```

ii. 验证用户player具有只读权限。

- 执行 `sudo su player -c 'touch dir0/file'` 命令，在 `dir0` 目录下创建 `file` 文件。

如果返回如下类似信息，表示用户 `player` 无创建 `file` 文件的权限。

```
touch: cannot touch 'dir0/file': Permission denied
```

- 执行 `sudo su player -c 'cat dir0/file'` 命令，查看 `dir0/file` 文件内容。

```
123
```

- 执行 `sudo su player -c 'echo 456 >> dir0/file'` 命令，追加内容。

```
bash: dir0/file: Permission denied
```

- 执行 `sudo su player -c 'getfacl dir0/file'` 命令，查看用户 `player` 对 `dir0/file` 的权限。

```
# file: dir0/file
# owner: admini
# group: adminis
user:---
group:---
group:players:r-x
group:adminis:rwX
mask::rwX
other:---
```

iii. 验证用户anonym无权限。

- 执行 `sudo su anonym -c 'ls dir0'` 命令，查看 `dir0` 目录下的文件。

如果返回如下信息，表示用户anonym无权限访问。

```
ls: cannot open directory dir0: Permission denied
```

- 执行 `sudo su anonym -c 'cat dir0/file'` 命令，查看文件内容。

如果返回如下信息，表示用户anonym无权限查看file文件的内容。

```
cat: dir0/file: Permission denied
```

- 执行 `sudo su anonym -c 'getfacl dir0/file'` 命令，查询用户anonym对file文件的权限。

如果返回如下信息，表示用户anonym无权限访问file文件。

```
getfacl: dir0/file: Permission denied
```

相关操作

如果您要移除用户权限，可参见以下方法。

建议在使用NFSv4 ACL时，尽量把每个用户归类到群组中。在设置NFSv4 ACL时直接设置群组权限而不用设置单个用户的权限。这样在移除用户权限时只需把用户移出某个群组即可。例如：执行以下命令将用户admini移出群组adminis，移入群组adminis2。

1. 执行 `sudo groupadd adminis2` 命令，创建adminis2群组。
2. 执行 `sudo usermod -g adminis2 admini` 命令，将用户admini移出群组adminis，移入群组adminis2。
3. 执行 `id admini` 命令，查询用户ID权限。

```
uid=1057(admini) gid=1057(admini) groups=1061(adminis2)
```

4. 执行以下命令，验证用户admini具备的权限。

- 执行 `sudo su admini -c 'ls dir0'` 命令，如果返回以下信息，表示用户admini无权限访问 `dir0` 目录。

```
ls: cannot open directory dir0: Permission denied
```

- 执行 `sudo su admini -c 'cat dir0/file'` 命令，如果返回以下信息，表示用户admini无权限查看 `dir0/file` 文件的内容。

```
cat: dir0/file: Permission denied
```

- 执行 `sudo su admini -c 'getfacl dir0/file'` 命令，如果返回以下信息，表示用户admini无权限访问 `dir0/file`。

```
getfacl: dir0/file: Permission denied
```

10.4. 使用NFSv4 ACL进行权限管理

本文介绍在使用NFSv4协议挂载的文件系统上，如何设置NFSv4 ACL来进行文件或目录权限管理。

前提条件

已使用NFSv4协议挂载文件系统，详情请参见[挂载NFS文件系统](#)。

背景信息

您可以使用NFSv4协议挂载文件系统，并在已挂载文件系统的机器上安装符合Linux标准的nfs4-acl-tools软件。安装完成后，通过标准工具[nfs4_getfacl](#)和[nfs4_setfacl](#)设置NFSv4 ACL。

命令说明

在设置NFSv4 ACL前，请先熟悉相关操作命令。

命令	说明
<code>nfs4_getfacl <filename></code>	查看文件当前的ACL权限。
<code>nfs4_setfacl -a A::GROUP@:W <filename></code>	给GROUP设置写权限。
<code>nfs4_setfacl -a A::1000:W <filename></code>	给用户1000设置写权限。
<code>nfs4_setfacl -a A:g:10001:W <filename></code>	给用户组10001设置写权限。
<code>nfs4_setfacl -e <filename></code>	交互式编辑设置ACL权限。
<code>nfs4_getfacl <filename> > saved_acl.txt</code>	将文件当前的ACL权限保存为一个文本文件。
<code>nfs4_setfacl -S saved_acl.txt <filename></code>	恢复保存到文本文件里的ACL权限。
<code>nfs4_setfacl -m A::1001:rwaxTNCy A::1001:rxtcy file1</code>	修改文件 <code>file1</code> 中的其中一条ACE的权限。
<code>nfs4_getfacl file1 nfs4_setfacl -S - file2</code>	将文件 <code>file1</code> 的ACL权限复制到文件 <code>file2</code> 上。
<code>nfs4_getfacl file1 grep @ nfs4_setfacl -S - file1</code>	删除文件 <code>file1</code> 上所有非保留的ACE。
<code>nfs4_setfacl -R -a A:g:10001:rW dir</code>	对目录树 <code>dir</code> 下所有文件和目录，增加用户组10001可以读写访问的权限。
<code>find dir -type f -exec sh -c 'for ace in \$(nfs4_getfacl \{} grep "^A.*\:1005\:"); do nfs4_setfacl -x \$ace \{}; done' \;</code>	删除目录树 <code>dir</code> 下所有文件中包含1005的ACE。
<code>nfs4_setfacl -a A:fdg:10001:rW dir1</code>	让用户组10001对目录 <code>dir1</code> 下新创建的文件和目录有读写权限。
<code>nfs4_setfacl -a A:fg:10001:rx dir1</code>	让用户组10001对目录 <code>dir1</code> 下新创建的文件有读和执行权限。

操作步骤

您可以参考以下步骤，为目录或文件设置NFSv4 ACL实现权限管理。

1. 创建用户和群组。

本文假设创建普通用户player，属于普通用户群组players；管理员admini，属于管理员群组adminis；另外再创建一个用户anonym。

```
sudo useradd player
sudo groupadd players
sudo usermod -g players player
sudo useradd admini
sudo groupadd adminis
sudo usermod -g adminis admini
sudo useradd anonym
```

2. 安装NFSv4 ACL工具。

如果已安装NFSv4 ACL工具，请跳过此步骤。

```
sudo yum -y install nfs4-acl-tools
```

3. 获取用户群组players和adminis的id。

打开/etc/group文件，获取用户群组players和adminis的id，如下所示。

```
players:x:19064:player
adminis:x:19065:admini
```

4. 对目录和文件设置NFSv4 ACL。

本文假设创建目录dir0，针对目录dir0中的所有文件，授予群组players只读权限，授予群组adminis读写执行权限，不授予其他用户权限。

```
sudo umask 777
sudo mkdir dir0
sudo nfs4_setfacl -a A:fdg:19064:RX dir0
sudo nfs4_setfacl -a A:fdg:19065:RWX dir0
sudo nfs4_setfacl -a A:fdg:OWNER@: dir0
sudo nfs4_setfacl -a A:fdg:GROUP@: dir0
sudo nfs4_setfacl -a A:fdg:EVERYONE@: dir0
```

设置完成后，可执行 `sudo nfs4_getfacl dir0` 查看设置结果。

```
A::OWNER@:tTnNcCy
A::GROUP@:tncy
A::EVERYONE@:tncy
A:fdi:EVERYONE@:tncy
A:fdi:OWNER@:tTnNcCy
A:fdi:GROUP@:tncy
A:g:19064:rxtncy
A:g:19065:rwaDxtTnNcCy
A:fdig:19064:rxtncy
A:fdig:19065:rwaDxtTnNcCy
```

5. 验证ACL的设置结果。

i. 验证用户admini具有读写权限。

```
sudo su admini -c 'touch dir0/file'
sudo su admini -c 'echo 123 > dir0/file'
```

ii. 验证用户player具有只读权限。

- 执行 `sudo su player -c 'touch dir0/file'` 命令，如果返回以下信息，表示用户player无权限创建 `dir0/file` 文件。

```
touch: cannot touch 'dir0/file': Permission denied
```

- 执行 `sudo su player -c 'echo 456 >> dir0/file'` 命令，如果返回以下信息，表示用户player对 `dir0/file` 无写权限。

```
bash: dir0/file: Permission denied
```

- 执行 `sudo su player -c 'cat dir0/file'` 命令，如果返回以下信息，表示用户player有权限查看 `dir0/file` 文件内容。

```
123
```

- 执行 `sudo su player -c 'nfs4_getfacl dir0/file'` 命令，查看用户player对 `dir0/file` 文件的权限。

```
A::OWNER:tTnNcCy
A::GROUP:tncy
A::EVERYONE:tncy
A:g:19064:rxtncy
A:g:19065:rwaxtTnNcCy
```

iii. 验证用户anonym无权限。

- 执行 `sudo su anonym -c 'ls dir0'` 命令，如果返回以下信息，表示用户anonym无权限访问 `dir0` 目录。

```
ls: cannot open directory dir0: Permission denied
```

- 执行 `sudo su anonym -c 'cat dir0/file'` 命令，如果返回以下信息，表示用户anonym无权限查看 `dir0/file` 文件的内容。

```
cat: dir0/file: Permission denied
```

- 执行 `sudo su anonym -c 'nfs4_getfacl dir0/file'` 命令，如果返回以下信息，表示用户anonym无权限访问 `dir0/file`。

```
Invalid filename: dir0/file
```

相关操作

如果您要移除用户权限，可参见以下方法。

建议在使用NFSv4 ACL时，尽量把每个用户归类到群组中。在设置NFSv4 ACL时直接设置群组权限而不用设置单个用户的权限。这样在移除用户权限时只需把用户移出某个群组即可。例如：参见以下命令将用户admini移出群组adminis，移入群组adminis2。

1. 执行 `sudo groupadd adminis2` 命令，创建adminis2群组。
2. 执行 `sudo usermod -g adminis2 admini` 命令，将用户admini移出群组adminis，移入群组adminis2。
3. 执行 `id admini` 命令，查询用户ID权限。

```
uid=1057(admini) gid=1057(admini) groups=1054(adminis2)
```

4. 执行以下命令，验证用户admini具备的权限。

- 执行 `sudo su admini -c 'ls dir0'` 命令，如果返回以下信息，表示用户admini无权限访问 *dir0* 目录。

```
ls: cannot open directory dir0: Permission denied
```

- 执行 `sudo su admini -c 'cat dir0/file'` 命令，如果返回以下信息，表示用户admini无权限查看 *dir0/file* 文件的内容。

```
cat: dir0/file: Permission denied
```

- 执行 `sudo su admini -c 'nfs4_getfacl dir0/file'` 命令，如果返回以下信息，表示用户admini无权限访问 *dir0/file*。

```
Invalid filename: dir0/file
```