ALIBABA CLOUD

阿里云

文件存储

文件存储NAS公共云合集（NAS）

文档版本：20220711

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.动态与公告

1.1. 新功能发布记录

本文列举了文件存储NAS产品功能发布的时间、发布地域及相关文档。

2022年04月

功能名称	功能概述	发布时间	发布地域	相关文档
NFS传输加密	提供端到端的安全性，保证整个传输过程中没有任何人或者组织能够窥探用户数据，从而充分保证用户数据在传输中的安全性。	2022-04-01	全部	• NFS文件系统传输加密 • SMB文件系统传输加密

2022年03月

功能名称	功能概述	发布时间	发布地域	相关文档
容量监控	通用型NAS支持容量监控，通过云监控服务可实时监控文件系统实例的存储概况，包括通用型NAS数据量（不含低频介质）、低频介质数据量和文件数。	2022-03-15	• 华东2（上海） • 澳大利亚（悉尼） • 印度尼西亚（雅加达） • 菲律宾（马尼拉）	• NAS监控概述 • 查看容量监控

2021年12月

功能名称	功能概述	发布时间	发布地域	相关文档
SMB超级用户	超级用户能够在不改动ACL的情况下对任何文件夹里的任何文件进行操作，可以将超级用户配置为群组。	2021-12-17	全部	• 文件存储NAS SMB ACL特性 • 将SMB文件系统挂载点接入AD域

功能名称	功能概述	发布时间	发布地域	相关文档
IPv6	极速型NAS中国内地各地域支持IPv6。	2021-12-14	• 华北1（青岛） • 华北2（北京） • 华北3（张家口） • 华北5（呼和浩特） • 华北6（乌兰察布） • 华东1（杭州） • 华东2（上海） • 华南1（深圳） • 华南2（河源） • 华南3（广州） • 西南1（成都）	管理挂载点

2021年11月

功能名称	功能概述	发布时间	发布地域	相关文档
回收站	通用型NAS支持回收站，无需业务改造，轻松实现数据保护。	2021-11-01	全部	回收站

2021年08月

功能名称	功能概述	发布时间	发布地域	相关文档
回收站	通用型NAS支持回收站，无需业务改造，轻松实现数据保护。	2021-08-20	• 华北2（北京） • 华东2（上海） • 华南2（河源） • 华南3（广州） • 中国（香港） • 澳大利亚（悉尼） • 马来西亚（吉隆坡） • 印度尼西亚（雅加达） • 美国（硅谷） • 美国（弗吉尼亚）	回收站

功能名称	功能概述	发布时间	发布地域	相关文档
一键挂载	支持在NAS控制台挂载、查询和卸载通用型NAS NFS协议文件系统，并自动适配Linux版本，应用最佳挂载参数。	2021-08-18	全部	• 通过控制台实现ECS实例一键挂载文件系统 • 多台ECS实例批量挂载同一NAS文件系统

2021年06月

功能名称	功能概述	发布时间	发布地域	相关文档
数据取回	通用型NAS生命周期管理新增支持SMB协议文件系统、低频文件查看以及取回低频文件至热介质。	2021-06-15	全部	管理低频介质中的文件

2021年03月

功能名称	功能概述	发布时间	发布地域	相关文档
资源包	资源包是一种预付费计费方式，相对于按量付费，资源包提供了更高的折扣优惠。相对于存储包，资源包无需绑定文件系统即可直接使用。资源包支持叠加购买，能抵扣多个文件系统的服务费用。	2021-03-26	全部	资源包购买指南

历史年份

2020年

功能名称	功能概述	发布时间	发布地域	相关文档
IPv6	极速型NAS支持IPv6，您可以灵活选择适配协议。	2020-09-18	华北5（呼和浩特）	管理挂载点
低频介质	通过配置生命周期管理，对冷热数据进行分级存储，优化TCO成本。	2020-06-30	全部	• 低频介质 • 设置生命周期策略

2019年

功能名称	功能概述	发布时间	发布地域	相关文档
按量付费	极速型NAS支持按量付费模式，用户按需使用付费，降低TCO成本。	2019-05-06	全部	极速型NAS计费说明
极速型NAS	文件存储NAS推出极速型规格，针对海量小文件的工作负载进行时延优化，提升IOPS性能，同时增强数据保护能力。	2019-04-05	全部	极速型NAS

2018年

功能名称	功能概述	发布时间	发布地域	相关文档
传输加密	提供端到端的安全性，保证整个传输过程中，没有任何人或者组织能够窥探用户数据，从而充分保证用户数据在传输中的安全性。	2018-09-30	• 美国西部（硅谷） • 美国东部（弗吉尼亚） • 英国（伦敦） • 澳大利亚（悉尼）	• 服务器端加密 • NFS文件系统传输加密 • SMB文件系统传输加密
文件备份	定期备份NAS文件，并在数据丢失或受损时及时恢复文件。	2018-05-31	全部	备份和恢复文件
性能监控	通过云监控服务查看文件系统读写吞吐、IOPS、延时和元数据操作QPS等性能指标，同时可以对指标设置报警规则及时获取异常信息。	2018-01-05	全部	创建报警规则
NAS SMB协议	SMB协议更适用于Windows客户端，Windows应用程序不经修改即可通过SMB协议访问阿里云文件存储服务。建议Windows客户优先使用SMB文件系统。	2018-01-05	全部	• 功能特性 • 通用型NAS

2017年

功能名称	功能概述	发布时间	发布地域	相关文档
NAS SMB协议（公测）	SMB协议更适用于Windows客户端，Windows应用程序不经修改即可通过SMB协议访问阿里云文件存储服务。建议Windows客户优先使用SMB文件系统。	2017-06-15	• 华东1（杭州） • 华北2（北京）	• 功能特性 • 通用型NAS
容量型NAS	支持低成本大容量的文件存储。	2017-05-31	• 华东1（杭州） • 华北2（北京） • 华东2（上海）	通用型NAS
容量型NAS	支持低成本大容量的文件存储场景。	2017-03-23	华东2（上海）	通用型NAS

2.数据迁移

2.1. 迁移说明

本文介绍了将NAS中的数据迁移至其他存储介质，或者将数据由其他存储介质迁移至NAS的方法。

- 本地到线上的数据迁移

  NFS文件系统数据的上传下载

  SMB文件系统数据的上传下载

- OSS和NAS之间的数据迁移

  NAS迁移至OSS教程

  OSS迁移至NAS教程

- NAS文件系统之间的数据迁移

  NAS之间迁移教程

  文件存储NFS文件系统间的数据迁移

2.2. NFS文件系统数据的上传下载

本文介绍如何通过公网将本地数据上传至NFS文件系统，或者将NFS文件系统内的数据下载到本地。

配置ECS实例

在方案一：通过SFTP客户端迁移数据及方案二：通过rsync命令行工具迁移数据中，需要配置ECS作为中转节点从公网访问阿里云文件存储NAS。推荐您选择新购ECS实例挂载NAS作为中转节点，您也可以选择使用已有ECS挂载NAS作为中转节点。

> **说明** 上传下载文件数据需要占用ECS公网带宽，建议您新购一台ECS实例专门负责文件数据的上传与下载，避免占用业务带宽。

- （推荐）使用新购ECS实例挂载NAS作为中转节点。挂载步骤，请参见新购ECS时挂载NAS文件系统。

基础配置：

参数	说明
镜像	建议您选择CentOS 8.0镜像。

网络和安全：

参数	说明
公网 IP	选中**分配公网 IPv4 地址**。
带宽计费模式	选中**按使用流量**。
带宽峰值	带宽峰值设为最大的100 Mbps。

- 使用已有ECS挂载NAS作为中转节点。具体操作，请参见Linux系统挂载NFS文件系统。

> **说明** 弹性公网IP对入方向流量不收费，仅对出方向流量收费。也就是说，从公网上传数据到NAS不会收取流量费用，而从NAS下载数据则会收取流量费用。计费详情，请参见弹性公网IP按量付费。

方案一：通过SFTP客户端迁移数据

当有少量文件需要一次性上传和下载时，建议您在本地系统上安装使用SFTP客户端来完成，此方案具有以下优点：

- 支持众多操作系统平台。
- 提供图形化操作界面。

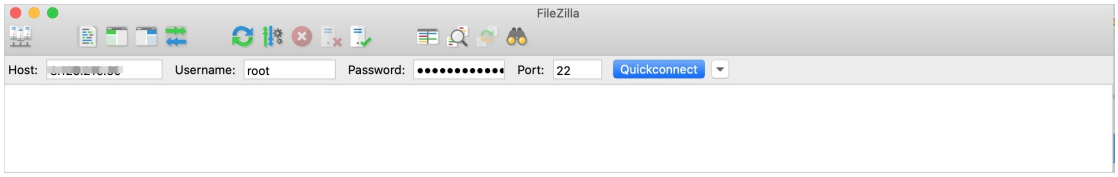
1. 安装工具。

   SFTP的客户端工具有多种版本，以下示例中使用的是FileZilla，请选择适合您本地操作系统的版本并下载安装SFTP客户端。

2. 建立SFTP客户端与中转节点ECS之间的连接。

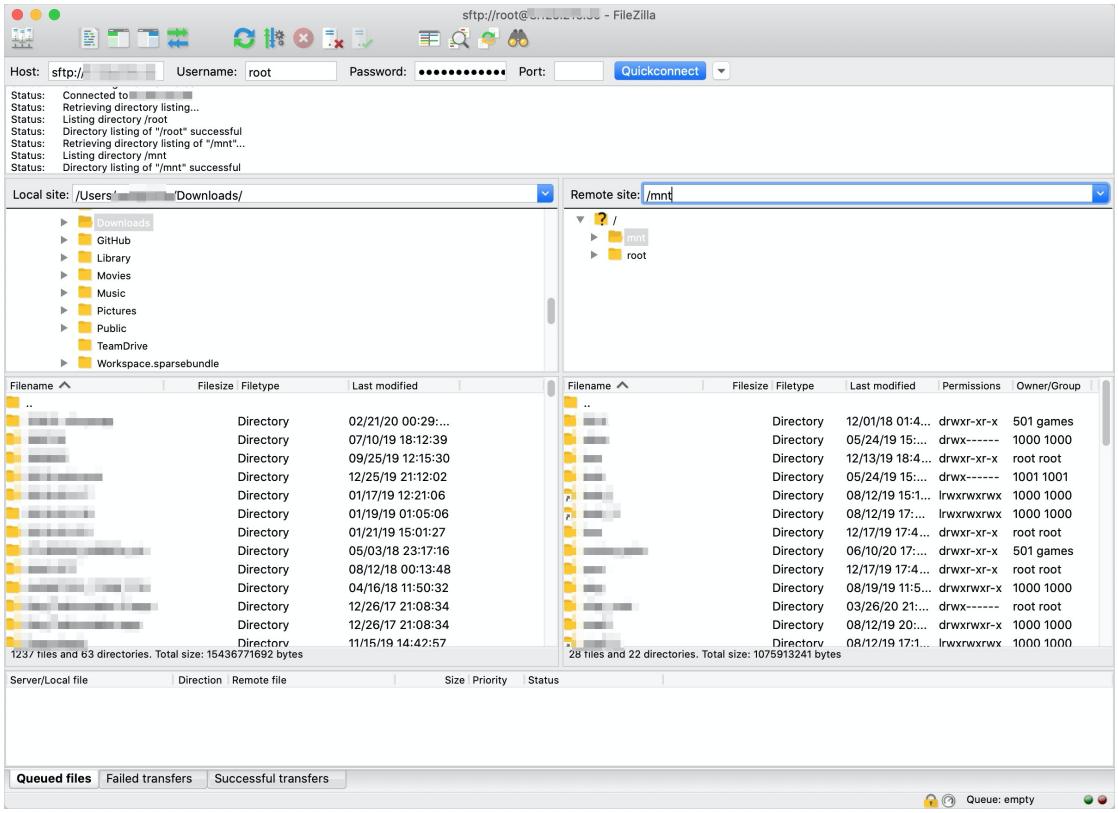
   i. 打开FileZilla客户端，按照如下说明进行配置。单击**Quickconnect**，建立连接。

   在本地客户端与ECS服务端的连接建立之后，左侧区域会显示本地文件系统，右侧区域会显示服务端ECS的文件系统。



参数	说明
Host	ECS的公网IP地址，例如192.0.2.1。
用户名	例如root。
密码	例如root登录密码。
Port	SFTP端口号，默认为22。

ii. 在页面右侧区域，设置**Remote site**中的路径为挂载了NAS文件系统的路径（例如*/mnt*），单击回车即可查看到NAS中的文件列表。



3. 上传下载数据。
   - 将左侧区域中的文件或目录拖拽到右侧区域，即完成数据上传。
   - 将右侧区域中的文件或目录拖拽到左侧区域，即完成数据下载。

方案二：通过rsync命令行工具迁移数据

当有大量文件上传和下载或需要频繁上传和下载的任务时，建议您在本地系统安装使用rsync命令行工具执行上传下载任务，此方案具有以下优点：

- 上传下载后的文件元数据不变（包括属主及权限信息）。
- 支持数据增量同步。
- 本地Linux或macOS系统可配置crontab向云上NAS自动备份数据。

1. 安装rsync工具。
   - Linux
     - 如果您使用的是CentOS或Redhat操作系统，请执行以下命令，使用yum包管理器安装rsync。

       ```
       sudo yum install rsync
       ```

     - 如果您使用的是Ubuntu或Debian操作系统，请执行以下命令，使用apt包管理器安装rsync。

       ```
       sudo apt-get install rsync
       ```

   - macOS

     请下载安装homebrew包管理器，然后执行以下命令安装rsync工具。

```
brew install rsync
```

- Windows

  请下载安装Cygwin模拟环境，您可以在安装过程中搜索安装rsync工具，也可以手动下载编译安装rsync。

2. 上传数据。

   执行以下命令，将本地目录以增量同步的方式，上传到阿里云NAS。

   ```
   rsync -avP DirToSync/ root@1.2.3.4:/mnt/DirToSync/
   ```

   命令中的参数请根据实际值修改，参数含义如下：

参数	说明
DirToSync	需要上传的本地目录名。
root	上传目标NAS文件系统目录的属主。
1.2.3.4	已挂载NFS文件系统的Linux ECS公网IP。
/mnt	ECS实例中用来挂载NAS的路径。

   > **说明** rsync命令中的源路径结尾必须带有正斜线（/），否则同步后数据路径不匹配。

3. 下载数据。

   执行以下命令，从阿里云NAS下载数据到本地目录。

   ```
   rsync -avP root@1.2.3.4:/mnt/DirToSync/ DirToSync/
   ```

4. 自动上传。

   本地Linux或macOS操作系统，可以基于rsync命令，通过crontab配置定时上传备份任务。

   - Linux操作系统：

     a. 创建本地系统到ECS的无密码通道。具体操作，请参见通过密钥认证登录Linux实例。

     执行以下命令，确认连接成功。

     ```
     ssh -i ~/.ssh/ecs.pem root@1.2.3.4
     ```

     > **说明** *~/.ssh/ecs.pem*为密钥文件在本地的存储路径。

     b. 配置crontab。

     执行 `crontab -e` 命令打开编辑器，配置定时上传任务，配置内容如下。

     ```
     0 23 * * * rsync -av -e "ssh -i ~/.ssh/ecs.pem" ~/Documents/ root@1.2.3.4:/mnt/Documents/
     ```

     这项crontab配置将会在每天23时0分把本机登录用户的Documents目录自动上传备份数据到阿里云NAS。您可以根据实际需求替换配置中的参数。

   - macOS操作系统

a. 为*/usr/sbin/cron*目录配置硬盘访问权限。

请进入系统设置，单击**Security & Privacy > Privacy > Full Disk Access**，单击**解锁**，单击**+**，选择Macintosh HD目录，按**cmd+shift+.**组合键显示隐藏目录，选择*/usr/sbin/cron*。

b. 创建本地系统到ECS的无密码通道。具体操作，请参见通过密钥认证登录Linux实例。

执行以下命令，确认连接成功。

```
ssh -i ~/.ssh/ecs.pem root@1.2.3.4
```

> **说明** *~/.ssh/ecs.pem*为密钥文件在本地的存储路径。

c. 配置crontab。

执行 `crontab -e` 命令打开编辑器，配置定时上传任务，配置内容如下。

```
0 23 * * * rsync -av -e "ssh -i ~/.ssh/ecs.pem" ~/Documents/ root@1.2.3.4:/mnt/Documents/
```

这项crontab配置将会在每天23时0分把本机登录用户的Documents目录自动上传备份数据到阿里云NAS。您可以根据实际需求替换配置中的参数。

> **说明** 当您使用rsync工具迁移数据性能较差时，可以尝试使用fpsync工具实现多线程迁移。具体操作，请参见附录：通过fpsync命令行工具实现多线程迁移数据。

方案三：将数据上传至OSS再迁移到NAS

如果您需要上传大量数据到NAS，而公网访问ECS的带宽无法满足您的需求，建议先上传数据到OSS，然后将OSS数据迁移到NAS。具体操作，请参见上传文件和迁移实施。

> **说明**
> - 目前迁移服务在公测阶段，如果您的业务需要使用数据迁移服务请提交工单申请白名单。
> - 迁移服务无法保证文件元数据不变，迁移完成后可以再执行rsync修复元数据信息。

方案四：本地数据中心挂载NAS

以上三种方案相对简便，但如果您需要从本地数据中心频繁读写NAS上的大量数据，则需要创建网络专线，从数据中心直接挂载NAS进行访问。更多信息，请参见通过VPN网关实现本地数据中心访问阿里云NAS和通过NAT网关实现本地数据中心访问阿里云NAS。

访问上传数据

数据上传后，您可以在业务所属的ECS或容器上挂载NAS文件系统，共享访问NAS文件系统上的数据。

以ECS为例，您可以用Linux系统挂载NFS文件系统，然后就像访问本地数据一样访问NAS上的文件数据。具体操作，请参见Linux系统挂载NFS文件系统。

您也可以在云上搭建业务应用，在多台计算节点上通过程序大量读写NAS上的数据，例如使用Nginx代理服务器代理阿里云NAS。

附录：通过fpsync命令行工具实现多线程迁移数据

以下方案以Linux操作系统为例介绍使用fpsync工具进行数据迁移。

1. 下载并安装fpsync工具。

```
wget -N https://github.com/martymac/fpart/archive/fpart-1.1.0.tar.gz -P /tmp
tar -C /tmp/ -xvf /tmp/fpart-1.1.0.tar.gz
cd /tmp/fpart-fpart-1.1.0
sudo yum install -y automake libtool
autoreconf -i
./configure
make
sudo make install
sudo yum install parallel -y
printf "will cite" | parallel --bibtex
sudo yum install -y rsync
```

2. 拷贝整个文件目录。

```
fpsync -n 10 -f 10000 /data/src/ /data/dst/
```

> **说明** 更多关于fpsync工具的信息，请参见fpsync工具。

2.3. SMB文件系统数据的上传下载

本文介绍如何通过公网将本地数据上传至SMB文件系统，或者将SMB文件系统内的数据下载到本地。

前提条件

- 已创建SMB文件系统。具体操作，请参见创建文件系统。
- 已创建挂载点。具体操作，请参见管理挂载点。

方案一：IIS FTP

当有少量文件需要一次性上传和下载时，建议您在本地系统配置FTP客户端来完成，此方案具有以下优点：

- 支持众多操作系统平台。
- 提供图形化操作界面。

1. 配置ECS。

   从公网访问阿里云文件存储NAS，需要配置ECS作为中转节点。

   > **说明** 上传下载文件数据占用ECS公网带宽，建议您新购一台ECS实例专门负责文件数据的上传与下载，避免占用业务带宽。

   - （推荐）使用新购ECS实例挂载NAS作为中转节点。建议配置项如下，挂载步骤请参见新购ECS时挂载NAS文件系统。

基础配置：

参数	说明
镜像	建议您选择Windows 2019镜像。

网络和安全：

参数	说明
公网 IP	选中**分配公网 IPv4 地址**。
带宽计费模式	选中**按使用流量**。
带宽峰值	带宽峰值设为最大的100 Mbps。

- 使用已有ECS挂载NAS作为中转节点。具体操作，请参见Windows系统挂载SMB文件系统。

2. 在ECS上配置IIS FTP服务以及在本地系统配置FTP客户端，具体配置方式请参见设置Windows IIS Web服务。

> **说明**
> - 需在VPC安全组打开对应的FTP TCP端口。
> - 您也可以配置其他FTP服务端和客户端进行公网上传下载数据。
> - 弹性公网IP对入方向流量不收费，仅对出方向流量收费。也就是说，从公网上传数据到NAS不会收取流量费用，而从NAS下载数据则会收取流量费用。计费详情请参见弹性公网IP按量付费。

方案二：rsync

当有大量文件上传和下载或需要频繁上传和下载的任务时，建议您在本地系统安装使用rsync命令行工具执行上传下载任务，此方案具有以下优点：

- 上传下载后的文件元数据不变（包括属主及权限信息）。
- 支持数据增量同步。
- 本地Linux或macOS系统可配置crontab向云上NAS自动备份数据。

1. 配置ECS。

   从公网访问阿里云文件存储NAS，需要配置ECS作为中转节点。

   > **说明** 上传下载文件数据需要占用ECS公网带宽，建议您新购一台ECS实例专门负责文件数据的上传与下载，避免占用业务带宽。

   - （推荐）使用新购ECS实例挂载NAS作为中转节点。建议配置项如下，挂载步骤请参见新购ECS时挂载NAS文件系统。

基础配置：

参数	说明
镜像	建议您选择CentOS 8.0镜像。

网络和安全：

参数	说明
公网 IP	选中**分配公网 IPv4 地址**。
带宽计费模式	选中**按使用流量**。
带宽峰值	带宽峰值设为最大的100 Mbps。

- 使用已有ECS挂载NAS作为中转节点。具体操作，请参见Linux系统挂载SMB文件系统。

2. 安装rsync工具。

> **说明** 需在VPC安全组打开SSH（TCP 22）端口。

- Windows

  请下载安装Cygwin模拟环境，您可以在安装过程中搜索安装rsync工具，也可以手动下载编译安装rsync。

- Linux
  - 如果您使用的是CentOS或Redhat操作系统，请执行以下命令，使用yum包管理器安装rsync。

    ```
    sudo yum install rsync
    ```

  - 如果您使用的是Ubuntu或Debian操作系统，请执行以下命令，使用apt包管理器安装rsync。

    ```
    sudo apt-get install rsync
    ```

  - 如果您使用的其他版本Linux，请使用对应的包管理器安装rsync工具。

- macOS

  请下载安装homebrew包管理器，然后执行以下命令安装rsync工具。

  ```
  brew install rsync
  ```

3. 上传数据。

   执行以下命令，将本地目录以增量同步的方式，上传到阿里云NAS。

```
rsync -avP DirToSync/ root@1.2.3.4:/mnt/DirToSync/
```

命令中的参数请根据实际值修改，参数含义如下：

参数	说明
DirToSync	需要上传的本地目录名。
root	上传目标的NAS文件系统目录的属主。
1.2.3.4	已挂载SMB文件系统的Linux ECS公网IP。
/mnt	ECS实例中用来挂载NAS的路径。

> **说明** rsync命令中的源路径结尾必须带有/，否则同步后数据路径不能匹配。

4. 下载数据。

   执行以下命令，从阿里云NAS下载数据到本地目录。

   ```
   rsync -avP root@1.2.3.4:/mnt/DirToSync/ DirToSync/
   ```

5. 自动上传。

   本地Linux或macOS操作系统，可以基于rsync命令，通过crontab配置定时上传备份任务。

   - Linux操作系统

     a. 连通从本地系统到ECS的无密码通道。具体操作，请参见通过密钥认证登录Linux实例。

     执行以下命令，确认连接成功。

     ```
     ssh -i ~/.ssh/ecs.pem root@1.2.3.4
     ```

     > **说明** *~/.ssh/ecs.pem*为密钥文件在本地的存储路径。

     b. 配置crontab。

     执行 `crontab -e` 命令打开编辑器，配置定时上传任务，配置内容如下。

     ```
     0 23 * * * rsync -av -e "ssh -i ~/.ssh/ecs.pem" ~/Documents/ root@1.2.3.4:/mnt/Documents/
     ```

     这项crontab配置将会在每天23时0分把本机登录用户的Documents目录自动上传备份到阿里云NAS。您可以根据实际需求替换配置中的参数。

   - macOS操作系统

     a. 为*/usr/sbin/cron*目录配置硬盘访问权限。

     请进入系统设置，单击**Security & Privacy > Privacy > Full Disk Access**，单击**解锁**，点击**+**，选择Macintosh HD目录，按**cmd+shift+.**组合键显示隐藏目录，选择*/usr/sbin/cron*。

b. 连通从本地系统到ECS的无密码通道。具体操作，请参见通过密钥认证登录Linux实例。

执行以下命令，确认连接成功。

```
ssh -i ~/.ssh/ecs.pem root@1.2.3.4
```

> **说明** *~/.ssh/ecs.pem*为密钥文件在本地的存储路径。

c. 配置crontab。

执行 `crontab -e` 命令打开编辑器，配置定时上传任务，配置内容如下。

```
0 23 * * * rsync -av -e "ssh -i ~/.ssh/ecs.pem" ~/Documents/ root@1.2.3.4:/mnt/Documents/
```

这项crontab配置将会在每天23时0分把本机登录用户的Documents目录自动上传备份数据到阿里云NAS。您可以根据实际需求替换配置中的参数。

方案三：将数据上传至OSS再迁移到NAS

如果您需要上传大量数据到NAS，而公网访问ECS的带宽无法满足您的需求，建议先上传数据到OSS，然后将OSS数据迁移到NAS。更多信息，请参见上传文件和迁移实施。

> **说明**
> - 目前迁移服务仍在公测阶段，需要提交工单申请白名单。
> - 迁移服务无法保证文件元数据不变，迁移完成后可以再执行rsync修复元数据信息。

方案四：本地数据中心挂载NAS

以上三种方案相对简便，但如果您需要从本地数据中心频繁读写NAS上的大量数据，则需要创建网络专线，从数据中心直接挂载NAS进行访问。

> **说明** 需在VPC安全组开启SMB（TCP 445）端口。

- VPN网关方案

  实现方法请参见通过VPN网关实现本地数据中心访问阿里云NAS和macOS客户端连接阿里云NAS SMB文件系统。

  访问成功后，Windows客户端可以采用robocopy进行多线程数据传输，示例如下。

  ```
  robocopy c:\dirA z:\dirB /e /z /b /mt:32
  ```

- NAT网关方案

  实现方法请参见通过NAT网关实现本地数据中心访问阿里云NAS。过程中可能需要转换SMB的TCP 445端口到其他端口，注意需要在安全组打开对应的端口。

访问上传数据

数据上传后，您可以在业务所属的ECS或容器上挂载NAS文件系统，共享访问NAS文件系统上的数据。

以ECS为例，您可以用Windows系统挂载SMB文件系统，然后就像访问本地数据一样访问NAS上的文件数据。具体操作，请参见Windows系统挂载SMB文件系统。

您也可以在云上搭建业务应用，在多台计算节点上通过程序大量读写NAS上的数据，例如通过Windows IIS服务访问阿里云NAS。

2.4. 文件存储NFS文件系统间的数据迁移

本文介绍如何在阿里云文件存储NFS文件系统之间迁移数据。

前提条件

拥有一个存有数据的NFS文件系统，并且拥有一个专有网络类型挂载点。

准备工作

1. 查看源挂载点信息。

   迁移之前请记录源文件系统的挂载点和所属的专有网络VPC信息。更多信息，请参见查看挂载点列表。

   > **说明** 如果您的文件系统只有经典网络挂载点，需要创建一个专有网络挂载点。具体操作，请参见添加挂载点。

2. 配置目标挂载点。

   > **说明** 如果目标文件系统和源文件系统在同一地域，为了方便迁移操作，请尽量保证目标挂载点与源挂载点在同一个VPC网络内。

   给目标NFS文件系统准备挂载点，可以采用以下三种方式：

   - 在目标地域和可用区创建新的文件系统，自动创建新的挂载点。具体操作，请参见通过控制台创建通用型NAS文件系统。

     > **说明** 如果您购买按量付费的通用型（容量型/性能型）NFS文件系统，请选择与源挂载点相同的VPC网络和虚拟交换机，即可自动生成目标挂载点。在新的文件系统创建之后，可以再购买存储包进行绑定，以节省费用。

   - 在已有的文件系统上找到已有的挂载点。具体操作，请参见查看挂载点地址。
   - 在已有的文件系统上创建新的挂载点。具体操作，请参见添加挂载点。

     以下情况需要添加挂载点：

     - 如果您希望将数据迁移至已有的文件系统，而已有的挂载点与源挂载点属于不同的VPC网络。
     - 创建新的文件系统后，没有自动生成挂载点。

实施迁移

在准备好源和目标挂载点后，创建新的ECS，同时挂载两个NFS文件系统后，使用rsync工具进行复制即可实现数据迁移。迁移数据的操作如下所示。

1. 挂载源和目标文件系统。

   > **注意** 推荐购买新的临时ECS执行迁移操作。如果使用已有的ECS执行迁移操作，会与正在运行的业务争抢CPU和网络带宽资源。

   登录ECS管理控制台单击**创建实例**后，在**基础配置**页面配置如下信息。

- 地域及可用区：选择源文件系统所在的地域及可用区。
- 实例规格：一般选择最低规格即可。
- 镜像：选择CentOS 7.6。
- 存储：单击**共享盘NAS**下方的**增加文件存储**进行配置，详情请参考下图示例。

> **说明**
>
> - 如果源和目标挂载点都在同一个VPC网络中，可以在ECS购买页面中配置NAS挂载信息，ECS启动后，源和目标NAS文件系统会自动挂载。
> - 如果源和目标挂载点不在同一个VPC网络中，在ECS购买页面中只需配置源文件系统。在ECS完成创建后，手动挂载目标文件系统，详情请参见同地域跨VPC挂载文件系统。

在ECS创建成功后，源和目标NAS文件系统挂载完成，请执行以下命令确认。

```
mount | grep nas.aliyuncs.com
```

如果挂载成功，界面会显示以下信息。源文件系统挂载到了`/mnt/volumeA`目录，目标文件系统挂载到了`/mnt/volumeB`目录。

```
[root@ ~]# mount | grep nas.aliyuncs.com
.nas.aliyuncs.com:/ on /mnt/volumeA type nfs (rw,relatime,vers=3,rsize=1048576,wsize=1048576,namlen=255,hard,nolock,noresvport,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=192.168.0.198,mountvers=3,mountport=4002,mountproto=tcp,local_lock=all,addr=192.168.0.198,_netdev)
.nas.aliyuncs.com:/ on /mnt/volumeB type nfs (rw,relatime,vers=3,rsize=1048576,wsize=1048576,namlen=255,hard,nolock,noresvport,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=192.168.0.213,mountvers=3,mountport=2049,mountproto=tcp,local_lock=all,addr=192.168.0.213,_netdev)
```

2. 安装迁移工具。

   执行以下命令安装迁移工具。

   ```
   sudo yum install -y rsync tmux
   ```

   > **说明**
   >
   > - rsync是负责执行复制的工具。
   > - tmux是帮助查看进度的工具。更多信息，请参见tmux用户指南。

3. 迁移存量数据。

   执行以下命令，将源文件系统中的存量数据同步到目标文件系统中。

   ```
   tmux
   sudo rsync -avP /mnt/volumeA/ /mnt/volumeB/
   ```

> 注意
>
> - rsync命令中的源路径结尾必须带有/，否则同步后数据路径不能匹配。
> - tmux命令会新建tmux session。在tmux session中运行 `rsync` 可以帮助查看进度。如果在迁移过程中，与ECS的连接断开了，重新登录ECS后执行 `tmux attach` 恢复tmux session，即可继续观察迁移进度。
> - 在测试使用的源文件系统中，共有一百万个100 KiB的文件，实际容量100 GiB，使用rsync迁移共耗时320分钟。

4. 迁移增量数据。

   在存量数据迁移过程中，如果源文件系统被其它ECS上运行的业务应用写入，那么在存量数据迁移结束后，需要另外同步新的增量数据。

   i. 停止业务应用。

   为了避免不断有新的数据写入，需要在同步增量数据之前，在所有ECS和容器上停止使用源文件系统的业务应用。

   > 注意
   >
   > - 在停止业务应用后，请不要手动删除源文件系统的任何数据，否则会在下一步操作中造成数据丢失。
   > - 请妥善选择业务低峰期操作。可以使用 `fuser -mv<dir>` 命令找到读写NAS的进程PID。

   ii. 同步增量数据。

   执行rsync命令，将存量数据迁移开始后的增量数据同步到目标文件系统中。

   ```
   sudo rsync -avP --delete /mnt/volumeA/ /mnt/volumeB/
   ```

   > 注意
   >
   > - --delete选项代表从目标文件系统中删除已在源文件系统中被删除的数据，请谨慎使用，避免将目标文件系统中的数据意外删除。
   > - rsync命令会先扫描源路径，所以即使增量数据不多，也可能需要较长的时间完成。

5. 检查迁移结果。

   在迁移完成后，执行以下rsync命令，检查目标文件系统是否与源文件系统一致。

   ```
   sudo rsync -rvn /mnt/volumeA/ /mnt/volumeB/
   ```

   如果两者数据一致，应该显示以下信息，中间不包含任何文件路径。

   ```
   sending incremental file list

   sent 13,570,658 bytes  received 5,008 bytes  17,173.52 bytes/sec
   total size is 100,000,000,000  speedup is 7,366.12 (DRY RUN)
   ```

切换应用到新的文件系统

在数据迁移完成后，如果您需要将现有业务从旧的文件系统切换到新的文件系统上，请在所有ECS和容器上卸载旧的文件系统，然后挂载新的文件系统。

- 使用ECS直接挂载NAS文件系统。
  i. 执行 `mount | grep nas.aliyuncs.com` 记录现有NAS挂载信息，注意NAS挂载到的本地路径*<dir>*。
  ii. 使用 `fuser -mv <dir>` 找到读写NAS的进程PID，将其全部通过 `kill -9` 命令停止。
  iii. 执行 `umount <dir>` 卸载旧的文件系统。
  iv. 挂载新文件系统到原本的<dir>路径。更多有关挂载参数的信息，请参见手动挂载NFS文件系统。
  v. 启动访问NAS的进程，确认读写正常。
  vi. 修改*/etc/fstab*中的自动挂载信息，将旧的挂载点替换为新的挂载点。
- 使用K8s管理的容器挂载NAS文件系统。
  i. 修改现有的动态卷或静态卷YAML配置文件，将旧的挂载点替换为新挂载点。
  ii. 用修改后的配置文件生成新pod，确认其挂载新的文件系统成功并可正常读写。
  iii. 回收使用旧的文件系统的所有pod。

> **注意** 在业务切换到新的文件系统后，请继续保留旧的文件系统的数据至少一个星期。不要立刻删除旧的文件系统里的数据，以避免因数据误删除或误同步而造成数据丢失。

3.基础管理

3.1. 管理文件系统

3.1.1. 创建文件系统

创建NAS文件系统，并通过多台计算实例挂载使用，实现文件系统的共享访问。您可以选择创建通用型NAS或极速型NAS。

背景信息

通用型NAS文件系统与极速型NAS文件系统特性不同，且适用于不同的业务场景。更多信息，请参见通用型NAS和极速型NAS。

通过控制台创建通用型NAS文件系统

1. 登录NAS控制台。
2. 在**概览**页面**文件系统选型指南**区域，单击**创建通用型NAS文件系统**。
3. 在**创建通用型NAS文件系统**面板，配置文件系统相关信息。

参数	说明
地域	选择要创建文件系统的地域。 **说明** ○ 不同地域的文件系统与云服务器ECS不能直接连通，建议文件系统与待挂载的云服务器ECS实例在同一地域。您还可以通过云企业网实现跨地域挂载，但跨地域挂载传输性能较差。更多信息，请参见同地域跨VPC挂载文件系统。 ○ 每个阿里云账号在单个地域内最多可以创建20个文件系统。
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。同一地域不同可用区之间的文件系统与云服务器ECS互通。 选择可用区时，建议与云服务器ECS实例在同一可用区，避免跨可用区产生时延。
存储规格	文件系统存储规格。包括**性能型**或**容量型**。 容量型NAS和性能型NAS的性能对比请参见通用型NAS。
协议类型	文件系统协议类型。包括**NFS**和**SMB**。 NFS协议适用于Linux ECS文件共享，SMB协议适用于Windows ECS文件共享。

参数	说明
生命周期管理	配置文件系统生命周期管理功能。 ○ **启用**：默认配置，创建文件系统后会开启生命周期管理功能。 启用生命周期管理功能，您可以将一定时间内没有访问过的数据转化为低频存储，从而节约存储成本。更多信息，请参见低频介质。 ○ **不启用**：不开启生命周期管理功能。
生命周期管理策略	当选择启用生命周期管理时，配置生命周期管理策略。更多信息，请参见设置生命周期策略。
加密类型	服务器端加密类型。包括： ○ **不加密**：不启用服务器端加密。 ○ **NAS托管密钥**：使用NAS完全托管的密钥加密每个文件系统。 ○ **用户管理密钥（KMS）**：使用您托管给KMS服务的用户管理密钥对文件系统进行加解密操作。 当您选择**NAS托管密钥**或**用户管理密钥（KMS）**时，均由密钥管理服务（KMS）托管的密钥加密文件系统中的数据。当您访问数据时，数据将自动解密。更多信息，请参见服务器端加密。 **说明** 仅以下地域支持用户管理密钥（KMS）功能。 ○ 美国（硅谷） ○ 美国（弗吉尼亚） ○ 英国（伦敦） ○ 澳大利亚（悉尼） ○ 德国（法兰克福） ○ 印度（孟买） ○ 新加坡
密钥ID	当加密类型为**用户管理密钥（KMS）**时，请您在下拉列表中选择需要配置的密钥ID。
密钥别名	当加密类型为**用户管理密钥（KMS)**时，请您核对密钥别名。
加密关联角色授权	当加密类型为**用户管理密钥（KMS)**时，必须授权加密服务关联角色。更多信息，请参见NAS服务关联角色。

参数	说明
数据备份	是否启用数据备份。包括： ○ **不启用**：不启用备份服务。 ○ **启用**：使用全托管备份服务，您可以恢复任一历史备份点的数据。 更多信息，请参见阿里云NAS备份。
服务关联角色	当启用数据备份时，必须授权NAS访问备份服务资源的权限关联角色。更多信息，请参见NAS服务关联角色。
挂载点类型	挂载点网络类型。包括**专有网络**和**经典网络**。 **说明** ○ 仅中国内地部分地域支持添加经典网络类型的挂载点。 ○ 经典网络类型的挂载点仅支持ECS实例挂载，且ECS实例的网络类型必须与NAS挂载点的网络类型一致，即经典网络类型的ECS实例只能使用经典网络类型的挂载点，专有网络类型的ECS实例只能使用专有网络类型的挂载点。
专有网络VPC	当**挂载点类型**为专有网络时，选择与ECS实例相同的VPC。如果您还未创建，请前往VPC控制台创建。 **说明** 必须选择与云服务器ECS实例相同的VPC。若选择不同的VPC，则需要先通过云企业网连通网络才能挂载文件系统。更多信息，请参见同地域跨VPC挂载文件系统。
虚拟交换机	当**挂载点类型**为专有网络时，选择VPC下创建的交换机。

4. 单击**立即购买**，根据页面提示，完成购买。

说明 创建文件系统成功后会绑定默认的权限组。如果您要修改权限组，请参见管理权限组。

通过控制台创建极速型NAS文件系统

1. 登录NAS控制台。
2. 在**概览**页面**文件系统选型指南**区域，单击**创建极速型NAS文件系统**。
3. 在**创建极速型NAS文件系统**面板，配置文件系统相关信息。

参数	说明

参数	说明
地域	选择要创建文件系统的地域。 **说明** ○ 不同地域的文件系统与云服务器ECS不能直接连通，建议文件系统与待挂载的云服务器ECS实例在同一地域。您还可以通过云企业网实现跨地域挂载，但跨地域挂载传输性能较差。更多信息，请参见同地域跨VPC挂载文件系统。 ○ 每个阿里云账号在单个地域内最多可以创建20个文件系统。 ○ 当前仅极速型NAS中国内地各地域支持IPv6功能，如果其他地域需要开启IPv6功能请提交工单申请。
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。同一地域不同可用区之间的文件系统与云服务器ECS互通。 选择可用区时，建议与云服务器ECS实例在同一可用区，避免跨可用区产生时延。
存储规格	极速型NAS存储规格。包括： ○ **标准型**：适用于大量小文件高速读写，元数据操作密集型，要求时延较低，总体吞吐量不大的共享文件存储。 ○ **高级型**：适用于大量小文件高速读写，要求时延较低，总体吞吐量不大的共享文件存储。后端使用RDMA网络，相对于标准型读写时延进一步优化，写性能更优。 **说明** 任一可用区仅支持标准型或高级型中的一种类型，建议您将业务部署在支持高级型的可用区。
协议类型	极速型NAS仅支持**NFS**协议。
配置容量	移动滑块选择文件系统的存储容量，范围为100 GiB~256 TiB。
加密类型	服务器端加密类型。包括： ○ **不加密**：不启用服务器端加密。 ○ **NAS托管密钥**：使用NAS完全托管的密钥加密每个文件系统。 ○ **用户管理密钥（KMS）**：使用您托管给密钥管理服务（KMS）的用户管理密钥对文件系统进行加解密操作。 当您选择**NAS托管密钥**或**用户管理密钥（KMS）**时，均由KMS托管的密钥加密文件系统中的数据。当您访问数据时，数据将自动解密。更多信息，请参见服务器端加密。
密钥ID	当加密类型为**用户管理密钥（KMS）**时，请您在下拉列表中选择需要配置的密钥ID。

4. 单击**立即购买**，根据页面提示，完成购买。

通过快照创建极速型NAS文件系统

您还可以调用API，通过文件系统快照创建极速型NAS文件系统。

1. 安装Python SDK。

```
pip install aliyun-python-sdk-core
pip install aliyun-python-sdk-nas
```

2. 创建文件系统。

```
#!/usr/bin/env python3
import json
from aliyunsdkcore.client import AcsClient
from aliyunsdknas.request.v20170626.CreateFileSystemRequest import CreateFileSystemRequ
est
def create_file_system():
    client = AcsClient('<accessKeyId>', '<accessSecret>', '<Region>')
    request = CreateFileSystemRequest()
    request.set_accept_format('json')
    # 按量付费
    request.set_ChargeType("PayAsYouGo")
    request.set_StorageType("standard")
    request.set_ProtocolType("NFS")
    request.set_FileSystemType("extreme")
    request.set_Capacity("100")
    request.set_ZoneId("cn-hangzhou-h")
    request.set_SnapshotId("s-extreme-xxxxxxxxxx")
    response = client.do_action_with_exception(request)
    res = json.loads(response)
    print(res)
```

重要参数说明如下所示。更多信息，请参见CreateFileSystem。

参数	说明
accessKeyId	您阿里云账号的AccessKey ID和AccessKey Secret。更多信息，请参见如何获取AccessKey。
accessSecret	
Region	快照所在的地域。例如：`cn-hangzhou`，您可以调用DescribeRegions查询地域信息。
Zone	快照所在的地域下的可用区。例如：`cn-hangzhou-h`，您可以调用DescribeZones查询可用区信息。
ProtocolType	文件系统支持的协议类型。极速型NAS文件系统仅支持NFS v3协议。

参数	说明
StorageType	文件系统的存储规格。取值： ○ standard：标准型 ○ advance：高级型 例如，标准型文件系统创建了快照B_Snapshot，使用快照B_Snapshot创建文件系统时，`StorageType`必须配置为`standard`。
Capacity	极速型NAS文件系统的存储容量，需要和创建快照的文件系统保持一致。 例如，100 GiB的极速型NAS文件系统A创建了快照A_Snapshot，使用快照A_Snapshot创建文件系统时，`Capacity`必须配置为`100`。
SnapshotId	快照ID。

3.1.2. 删除文件系统

当您不再使用NAS文件系统时，可以清空文件系统中的文件并删除文件系统实例。

警告 文件系统实例一旦删除，数据将不可恢复，请谨慎操作。

1. 登录NAS控制台。
2. 在左侧导航栏，单击**文件系统 > 文件系统列表**。
3. 在**文件系统列表**页面，找到目标文件系统，单击**更多 > 删除**。
4. 在**删除文件系统**对话框，确认待删除的文件系统名称，单击**确定**。

说明

- 只有当通用型NAS的挂载点数量为0时，您才可以删除该文件系统实例。
- 包年包月类型的极速型NAS实例不支持在控制台删除，若您需要删除包年包月类型的极速型NAS实例，请提交工单申请。

3.1.3. 查询文件系统详情

您可以在文件系统详情页了解您的文件系统概况，例如各地域文件系统数量、文件系统资源使用量等信息。

查询文件系统资源使用量

您可以通过以下方式快速查询当前阿里云账号下文件系统资源使用量，例如容量型或性能型使用量、低频介质用量、回收站存储量等。

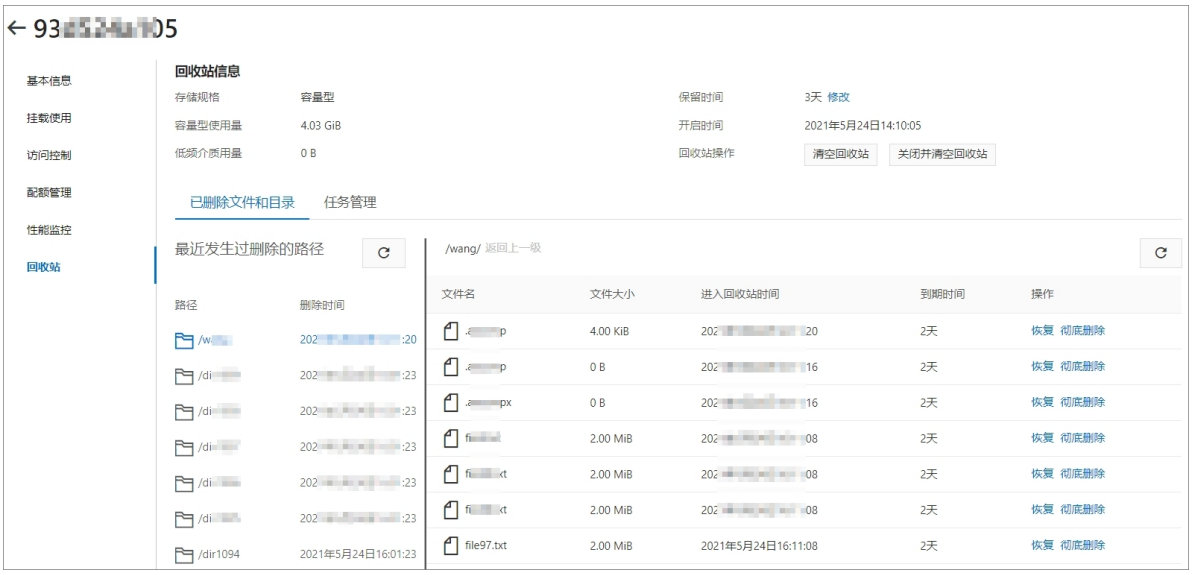
说明 文件系统详情页的数据平均延迟1~3小时，不作为计量数据。若您希望查询更详细的计量数据，请参见查看消费明细。

- 查询存储用量

您可以在**基础信息**页签查询指定文件系统存储用量，包括容量型或性能型使用量、极速型使用量和低频介质用量。

- 查询回收站存储量

  您可以在**回收站**页签查询指定文件系统回收站存储用量。更多回收站的介绍，请参见回收站。



> **说明** 在查询文件存储NAS账单时，通用型NAS存储用量包括容量型或性能型存储使用量及回收站存储用量。更多信息，请参见查看消费明细。

查询文件系统列表

1. 登录NAS控制台。
2. 在左侧导航栏，选择**文件系统 > 文件系统列表**。
3. 在**文件系统列表**页面，可以查询您账号下当前地域所有文件系统。

查询文件系统性能指标

1. 登录NAS控制台。
2. 在左侧导航栏，单击**文件系统 > 文件系统列表**。
3. 在**文件系统列表**页面，单击目标文件系统。
4. 在文件系统详情页面，单击**性能监控**。
5. 在**性能监控**页签，您可以查询IOPS、数据吞吐等性能指标。

查询ECS实例挂载状态

1. 登录NAS控制台。
2. 在左侧导航栏，选择**文件系统 > 文件系统列表**。
3. 在**文件系统列表**页面，单击待查询文件系统的名称。
4. 在文件系统详情页，单击**挂载使用**。
5. 在**挂载使用**页签，单击目标挂载点操作列的**查询**。
6. 在**查询ECS挂载状态**对话框，选择目标ECS实例并查看其挂载详情。

3.1.4. 极速型NAS扩容

本文介绍如何在阿里云NAS控制台扩容极速型NAS文件系统。

前提条件

已创建极速型NAS文件系统，详情请参见通过控制台创建极速型NAS文件系统。

背景信息

创建极速型NAS文件系统时配置的容量即为您能使用的最大容量，当数据写满后，将导致数据无法写入。为了防止因为数据无法写入影响业务使用，请在数据写满前扩容当前极速型NAS文件系统。

在扩容极速型NAS时，请注意以下事项：

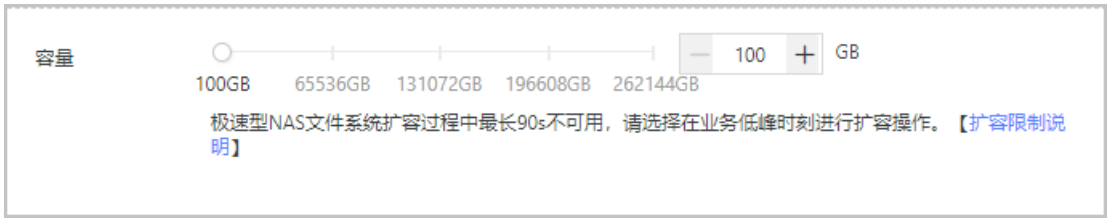
- 文件系统必须处于运行中状态，否则不支持扩容。
- 文件系统在扩容过程中，服务不可用时间最长为90s，请选择在业务低谷时刻进行扩容。服务影响时长正在持续优化中。
- 文件系统只支持扩容，不支持缩容。
- 2020年5月20日之前创建的极速型文件系统为版本1，之后创建的极速型文件系统为版本2。您可以在文件系统的详情页查看版本号。

  文件系统版本1最大支持32 TB，扩容时带宽不随容量增长；文件系统版本2最大支持256 TB，扩容时带宽和性能随容量增长，详细性能指标请参见极速型NAS规格说明。

  文件系统不支持版本转换，建议您使用迁移服务将数据迁移到版本2的文件系统，详情请参见NAS之间迁移教程。
- 正在创建快照的文件系统不能扩容。由于文件系统扩容时会自动对数据进行快照保护，所以正在创建快照的文件系统不支持扩容，建议您避开快照周期进行扩容或者删除当前正在执行的快照任务。

操作步骤

1. 登录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**更多 > 扩容**。
4. 在**扩容**页面的**容量**区域，滑动滑块调节容量大小。



5. 在**服务协议**区域，选中服务协议。
   - 如果是**按量付费**的文件系统，选中**极速型NAS（按量付费）服务协议**。
   - 如果是**包年包月**的文件系统，选中**极速型NAS服务协议**。
6. 单击**立即购买**，根据页面提示，完成购买。

3.2. 管理挂载点

本文介绍如何在NAS控制台上管理挂载点，包括添加挂载点、查看挂载点列表、删除挂载点、修改挂载点权限组、禁用和启用挂载点等。

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云服务器ECS，添加挂载点的操作如下。

> **说明**
> - 通用型NAS支持专有网络类型和经典网络类型挂载点，每个文件系统可添加两个挂载点。
> - 极速型NAS只支持专有网络类型的挂载点，每个文件系统仅支持添加一个挂载点。

1. 登录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**更多 > 添加挂载点**。
4. 在**添加挂载点**页面，配置如下参数。

   挂载点类型：包括专有网络和经典网络。

   - 如果您要添加**专有网络**类型的挂载点，请配置以下参数。

     > **说明**
     > - 一个专有网络类型挂载点可以被同VPC下的不同交换机下的ECS实例使用。
     > - 添加挂载点时，文件系统会占用一个IP地址，建议您选择内网IP较多的交换机。
     > - 极速型NAS中国内地各地域已支持IPv6功能。在开启IPv6功能前，您还需要为目标文件系统搭建IPv6专有网络。具体操作，请参见搭建IPv6专有网络。

参数	说明
VPC网络	选择已创建的VPC网络。如果还未创建，请前往VPC控制台创建。 必须与云服务器ECS选择一样的VPC网络。如果是不同的VPC，则需要先通过云企业网连通网络，才能挂载文件系统。更多信息，请参见同地域跨VPC挂载文件系统。

参数	说明
交换机	选择VPC网络下创建的交换机。
权限组	根据需求选择权限组。 初始情况下，每个账号都会自动生成一个VPC默认权限组，允许同一VPC网络下的任何IP地址通过该挂载点访问文件系统。您也可以根据业务场景创建权限组。具体操作，请参见创建权限组和规则。
开启IPv6	开启IPv6功能。 当文件系统在支持IPv6的地域且VPC网络和交换机符合IPv6规则时，**开启IPv6**开关生效。关于搭建IPv6专有网络的具体操作，请参见搭建IPv6专有网络。

- 如果您要添加**经典网络**类型的挂载点，请根据业务需求选择权限组。

> 注意
> - 仅中国大陆部分地域支持添加经典网络类型的挂载点。
> - 经典网络类型的挂载点仅支持ECS实例挂载，且ECS实例的网络类型必须与NAS挂载点的网络类型一致，即经典网络类型的ECS实例只能使用经典网络类型的挂载点。

5. 配置完成后，单击**确定**。

挂载点创建完成后，将开放如下端口用于访问NFS服务和SMB服务：

- 通用型NAS文件系统
  - NFS服务端口
    - 2049：用于访问NFS服务。
    - 4001：用于访问NLM锁服务。
    - 4002：用于访问Mount服务。
    - 111：用于访问RPC bind服务。
  - SMB服务端口

    445：用于访问SMB服务。
- 极速型NAS文件系统

  极速型NAS仅支持NFS协议，NFS服务端口说明如下：
  - 2020年05月20日之前创建的文件系统
    - 2049：用于访问NFS服务。
    - 4001：用于访问NLM锁服务。
    - 4002：用于访问Mount服务。
    - 111：用于访问RPC bind服务。
  - 2020年05月20日及之后创建的文件系统
    - 2049：用于访问NFS服务、NLM锁服务及Mount服务。
    - 111：用于访问RPC bind服务。

查看挂载点列表

在**文件系统列表**页面，找到目标文件系统，单击**管理**，在**文件系统详情**页面，单击左侧**挂载使用**，在**挂载点**区域，查看挂载点列表。

查看挂载点地址

在挂载点列表的**挂载点地址**列，将鼠标置于图标，查看目标文件系统的挂载点地址。

查看已挂载的客户端列表

通用型NAS支持在控制台查看已挂载的客户端列表。

单击**客户端列表**，查看已挂载该挂载点的客户端列表，列表中显示客户端的IP地址。

> **说明** 客户端列表中显示近一分钟内正在使用NAS的客户端，部分已挂载而没有使用的客户端可能未显示在此列表中。

禁用和激活挂载点

通用型NAS支持禁用和激活挂载点，您可以通过禁止和激活功能，控制客户端对挂载点的访问。

- 单击**禁用**，暂时阻止任何客户端对该挂载点的访问。
- 单击**启用**，重新允许客户端对挂载点的访问。

删除挂载点

> **警告** 删除挂载点后，无法恢复，请谨慎操作。

单击**删除**，删除挂载点。

修改挂载点权限组

单击**修改权限组**，可修改挂载点的权限组。更多信息，请参见管理权限组。

FAQ

- 挂载点是什么？有什么作用？
- 挂载点是否可以转换类型？
- 怎么删除由阿里云内部服务创建的挂载点？

更多管理挂载点FAQ，请参见基础管理FAQ。

3.3. 管理权限组

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，并给不同的IP地址或网段授予不同的访问权限。

背景信息

初始情况下，每个阿里云账号会自动生成一个默认权限组，默认权限组允许任何IP地址以最高权限（可读写且不限制Linux系统用户对文件系统的访问权限）访问文件系统。默认权限组不支持删除或修改。

使用限制

- 一个阿里云账号在单个地域内最多可以创建20个权限组。
- 一个权限组最多支持添加300个规则。

创建权限组和规则

> **说明** 为了最大限度保障您的数据安全，建议您谨慎添加权限组规则，仅为必要的IP地址或网段授权。

1. 登录NAS控制台。
2. 创建权限组。
   i. 在左侧导航栏，单击**文件系统 > 权限组**。
   ii. 在**权限组**页面，选择**通用型NAS**页签或者**极速型NAS**，单击**创建权限组**。
   iii. 在**新建权限组**页面，配置相关信息。

重要参数说明如下所示。

参数	说明
名称	设置权限组名称。 **说明** 权限组名称不能与已存在权限组名称重复。
网络类型	包括**专有网络**和**经典网络**。 **说明** 极速型NAS只支持专有网络类型的权限组。

3. 添加权限组规则。
   i. 找到目标权限组，单击**管理规则**。

ii. 在**权限组规则列表**页面，单击**添加规则**，配置相关规则信息。

参数	说明
授权类型	本条规则的授权类型。取值包括**IPv4访问地址**和**IPv6访问地址**。仅在地域为华北5（呼和浩特）时，该配置有效。
授权地址	本条规则的授权对象。 **说明** 经典网络类型权限组规则授权地址只能是单个IP地址而不能是网段。
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	是否限制授权对象的Linux系统用户对文件系统的访问权限。SMB文件系统不支持该权限项，配置后不生效。 ■ **所有用户不匿名（no_squash）**：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。 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。
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的整数，1为最高优先级。 **说明** 若多条规则中包含重叠的网段，且这些规则权限不同、优先级相同，则先配置的规则生效，请尽量避免重叠网段的配置。

iii. 单击**确定**。

其他操作

在**权限组**页面，您可以进行如下操作。

操作	说明
查看权限组及详情	查看当前区域已创建的权限组及相关信息，包括类型、规则数目、绑定文件系统数目等信息。
编辑权限组	找到目标权限组，单击**编辑**，可编辑权限组的描述信息。
删除权限组	找到目标权限组，单击**删除**，删除权限组。
查看权限组规则	找到目标权限组，单击**管理规则**，查看此权限组下的规则。

操作	说明
编辑权限组规则	单击**管理规则**，找到目标权限组规则，单击**编辑**，可修改授权地址、读写权限，用户权限和优先级。
删除权限组规则	单击**管理规则**，找到目标权限组规则，单击**删除**，删除权限组规则。

3.4. 基础管理FAQ

每个账号可以创建多少个文件系统、文件系统有什么限制？

- 每个账号在单个地域内最多支持创建20个通用型NAS文件系统和20个极速型NAS文件系统。
- 单个文件系统容量上限：容量型10 PiB；性能型1 PiB。
- 单个文件系统最多可以支持10亿个文件。

更多使用限制，请参见使用限制。

为什么在创建文件系统时，会显示库存不足？

创建文件系统时显示库存不足，则表示当前地域当前可用区储备已用尽，建议您更换可用区购买。

挂载点是什么？有什么作用？

挂载点是计算节点（ECS实例、E-HPC或容器服务）访问文件系统的入口。挂载点定义了什么类型网络的计算节点，采用怎样的权限来访问文件系统。同一个挂载点可以被多个计算节点同时挂载，共享访问。

挂载点是否可以转换类型？

如果文件系统已添加挂载点，则不支持转换挂载点类型。您可以新建一个挂载点，使计算节点通过新挂载点重新挂载文件系统，从而达到转换挂载点类型的目的。

> **说明** 通用型NAS可以添加两个挂载点，极速型NAS只支持添加专有网络类型的挂载点。

假设您创建了容量型NAS文件系统，并已通过经典网络类型的挂载点完成挂载。您希望将挂载点类型更换成专有网络类型，可以通过以下步骤实现。

1. 新增一个专有网络类型挂载点。具体操作，请参见添加挂载点。
2. 卸载原使用经典网络类型挂载点的文件系统。具体操作，请参见卸载文件系统。

   请您登录NAS控制台，在目标文件系统详情页的**挂载使用**页签，单击**客户端列表**，确保**客户端列表**列表为空。
3. 使用专有网络类型挂载点重新挂载文件系统至原目标路径。具体操作，请参见挂载文件系统。
4. 在原经典网络挂载点**操作**列，单击**禁用**。
5. 确保业务无影响后，单击**删除**。

怎么删除由阿里云内部服务创建的挂载点？

- 删除由Cloudshell服务创建的挂载点

当您使用Cloudshell服务管理NAS资源时，会自动创建一个挂载点，如下图所示：

请按照以下步骤删除由Cloudshell服务创建的挂载点：

i. 登录Cloudshell。

ii. 在顶部菜单栏，选择 > **解绑存储空间**。

iii. 在**解绑存储空间**对话框，确认需要解绑的文件系统ID。

- 若此挂载点由当前RAM用户创建，选中**当前用户**，单击**解绑**。
- 若此挂载点由其他RAM用户创建，请使用主账号登录，选中**RAM用户**，单击**解绑**。

- 删除由备份服务创建的挂载点

当您使用文件系备份服务管理NAS资源时，会自动创建一个挂载点，如下图所示：

请按照以下步骤删除由备份服务创建的挂载点：

i. 登录NAS控制台。

ii. 在左侧导航栏，单击**文件备份**。

iii. 在**文件备份**页面，单击**管理备份挂载点**。

iv. 在**管理备份挂载点**面板，找到目标文件系统，单击**删除备份挂载点**。

v. 按照对话框提示，单击**确认**，删除备份服务挂载点。

如何查看已挂载的客户端列表？

> **说明** 通用型NAS支持查看使用中的已挂载客户端列表；极速型NAS不支持查看已挂载客户端列表。

1. 登录NAS控制台。
2. 在左侧导航栏，单击**文件系统 > 文件系统列表**。
3. 在**文件系统列表**，单击目标文件系统名称。
4. 在文件系统详情页，单击**挂载使用**。

5. 在目标挂载点**操作**列，单击**客户端列表**。

   在**客户端列表**对话框，查看已挂载客户端的IP地址。

   > **说明** 客户端列表中显示近一分钟内正在使用NAS的客户端，部分已挂载而没有使用的客户端不在此列表中显示。

4.高级管理

4.1. 管理用户权限

4.1.1. 使用RAM权限策略控制NAS访问权限

RAM（Resource Access Management）是阿里云提供的管理用户身份与资源访问的服务。使用RAM，您可以创建、管理RAM用户（例如员工、系统或应用程序），以及控制RAM用户对资源的操作权限，例如限制您的RAM用户只拥有对某一个文件系统的操作权限。

> **警告** 授予RAM用户对NAS文件系统的访问控制权限时，请遵循最小授权原则，选择合理的授权范围。授权范围过大有安全风险。

为RAM用户授权的流程

1. 创建RAM用户。具体操作，请参见创建RAM用户。
2. 选择需要授予RAM用户的权限策略。

   权限策略分为**系统策略**和**自定义策略**。

   - **系统策略**：阿里云提供多种具有不同管理目的的默认权限策略。NAS常用的系统策略包括以下两种：
     - AliyunNASFullAccess（不推荐）：为RAM用户授予文NAS文件系统的完全管理权限。该权限风险很高，不推荐使用。
     - AliyunNASReadOnlyAccess：为RAM用户授予文NAS文件系统的只读访问权限。
   - **自定义策略**：自定义权限策略可以更大程度的满足您的细粒度的要求，从而实现更灵活的权限管理。

     您可以结合实际使用场景，并参照下文列举的常见自定义策略示例，然后通过脚本配置方式创建自定义策略。具体操作，请参见创建自定义权限策略。
3. 为RAM用户授权。

   为RAM用户授予步骤2中选择的权限策略。具体操作，请参见为RAM用户授权。

示例一：授权RAM用户对文件系统的权限

- 授予RAM用户拥有对文件系统（实例ID：`07d****294`）的完全控制权限。

> **说明** 由于RAM不支持授予RAM用户单一文件系统的查看权限，当要授予RAM用户单一文件系统完全控制权限时，请您先授予RAM用户全部文件系统的查看权限，然后再授予RAM用户单一文件系统的操作（删除、修改）权限。

```
{
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "nas:*"
            ],
            "Resource": [
                "acs:nas:*:*:filesystem/07d****294"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "nas:CreateMountTarget",
            "Resource": [
                "acs:vpc:*:*:vswitch/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "cms:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "nas:DescribeFileSystems",
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

- 授予RAM用户修改文件系统（实例ID：`07d****294`）属性的权限。

```
{
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "nas:DescribeFileSystems",
            "nas:ModifyFileSystem"
        ],
        "Resource": "acs:nas:*:*:filesystem/07d****294"
    }],
    "Version": "1"
}
```

- 授予RAM用户查看所有文件系统的权限。

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

示例二：授权RAM用户对文件系统挂载点的权限

授予RAM用户对文件系统（实例ID：`07d****294`）的挂载点拥有完全控制权限。

```
{
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "nas:CreateMountTarget",
            "nas:DescribeMountTargets",
            "nas:ModifyMountTarget",
            "nas:DeleteMountTarget"
        ],
        "Resource": [
            "acs:nas:*:*:filesystem/07d****294",
            "acs:vpc:*:*:vswitch/*"
        ]
    }],
    "Version": "1"
}
```

示例三：授权RAM用户对文件系统权限组的权限

授予RAM用户对所有文件系统权限组拥有完全控制权限。

```
{
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "nas:CreateAccessGroup",
            "nas:DescribeAccessGroups",
            "nas:ModifyAccessGroup",
            "nas:DeleteAccessGroup",
            "nas:CreateAccessRule",
            "nas:DescribeAccessRules",
            "nas:ModifyAccessRule",
            "nas:DeleteAccessRule"
        ],
        "Resource": "acs:nas:*:*:accessgroup/*"
    }],
    "Version": "1"
}
```

示例四：授权RAM用户查看文件系统性能监控指标的权限

授予RAM用户通过控制台查看任一文件系统性能监控指标的权限。

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

示例五：授权RAM用户对文件系统回收站的管理权限

- 授予RAM用户拥有对文件系统（实例ID：`07d****294`）回收站完全控制的权限。

```
{
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "nas:EnableRecycleBin",
                "nas:DisableAndCleanRecycleBin ",
                "nas:UpdateRecycleBinAttribute",
                "nas:GetRecycleBinAttribute",
                "nas:CreateRecycleBinRestoreJob",
                "nas:CreateRecycleBinDeleteJob",
                "nas:CancelRecycleBinJob",
                "nas:ListRecycleBinJobs",
                "nas:ListRecycledDirectoriesAndFiles",
                "nas:ListRecentlyRecycledDirectories"
            ],
            "Resource": [
                "acs:nas:*:*:filesystem/07d****294"
            ]
        }
    ],
    "Version": "1"
}
```

- 授予RAM用户恢复文件系统（实例ID：`07d****294`）回收站中暂存文件的权限。

```
{
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "nas:GetRecycleBinAttribute",
                "nas:CreateRecycleBinRestoreJob",
                "nas:CancelRecycleBinJob",
                "nas:ListRecycleBinJobs",
                "nas:ListRecycledDirectoriesAndFiles",
                "nas:ListRecentlyRecycledDirectories"
            ],
            "Resource": [
                "acs:nas:*:*:filesystem/07d****294"
            ]
        }
    ],
    "Version": "1"
}
```

- 授予RAM用户彻底删除文件系统（实例ID：`07d****294`）回收站中暂存文件的权限。

```
{
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "nas:GetRecycleBinAttribute",
                "nas:CreateRecycleBinDeleteJob",
                "nas:CancelRecycleBinJob",
                "nas:ListRecycleBinJobs",
                "nas:ListRecycledDirectoriesAndFiles",
                "nas:ListRecentlyRecycledDirectories"
            ],
            "Resource": [
                "acs:nas:*:*:filesystem/07d****294"
            ]
        }
    ],
    "Version": "1"
}
```

- 授予RAM用户修改文件系统（实例ID：`07d****294`）回收站配置的权限。

```
{
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "nas:EnableRecycleBin",
                "nas:UpdateRecycleBinAttribute",
                "nas:DisableAndCleanRecycleBin",
                "nas:GetRecycleBinAttribute"
            ],
            "Resource": [
                "acs:nas:*:*:filesystem/07d****294"
            ]
        }
    ],
    "Version": "1"
}
```

附录：自定义权限策略鉴权列表

您可以通过RAM控制台或者调用RAM API CreatePolicy创建一个自定义策略，当**配置模式**为**脚本配置**时，您需要根据JSON模板文件填写策略内容。其中的Action和Resource参数取值请参见如下鉴权列表。更多信息，请参见权限策略基本元素。

API		Action	Resource	说明
文件系统	CreateFileSystem	nas:CreateFileSystem	acs:nas:<region>:<account-id>:filesystem/*	创建文件系统。
	DeleteFileSystem	nas:DeleteFileSystem	acs:nas:<region>:<account-id>:filesystem/<filesystemid>	删除文件系统。
	ModifyFileSystem	nas:ModifyFileSystem	acs:nas:<region>:<account-id>:filesystem/<filesystemid>	修改文件系统配置。
	DescribeFileSystems	nas:DescribeFileSystems	acs:nas:<region>:<account-id>:filesystem/<filesystemid>	列出文件系统实例。
挂载点	CreateMountTarget	nas:CreateMountTarget	• acs:nas:<region>:<account-id>:filesystem/<filesystemid> • acs:vpc:*:*:vswitch/*	创建挂载点。
	DeleteMountTarget	nas:DeleteMountTarget	acs:nas:<region>:<account-id>:filesystem/<filesystemid>	删除挂载点。

API		Action	Resource	说明
	ModifyMountTarget	nas:ModifyMountTarget	acs:nas:<region>:<account-id>:filesystem/<filesystemid>	修改挂载点配置。
	DescribeMountTargets	nas:DescribeMountTargets	acs:nas:<region>:<account-id>:filesystem/<filesystemid>	列出文件系统挂载点。
权限组	CreateAccessGroup	nas:CreateAccessGroup	acs:nas:<region>:<account-id>:accessgroup/<accessgroupname>	创建权限组。
	DeleteAccessGroup	nas:DeleteAccessGroup	acs:nas:<region>:<account-id>:accessgroup/<accessgroupname>	删除权限组。
	ModifyAccessGroup	nas:ModifyAccessGroup	acs:nas:<region>:<account-id>:accessgroup/<accessgroupname>	修改权限组。
	DescribeAccessGroups	nas:DescribeAccessGroups	acs:nas:<region>:<account-id>:accessgroup/<accessgroupname>	列出权限组。
	CreateAccessRule	nas:CreateAccessRule	acs:nas:<region>:<account-id>:accessgroup/<accessgroupname>	添加权限组规则。
	DeleteAccessRule	nas:DeleteAccessRule	acs:nas:<region>:<account-id>:accessgroup/<accessgroupname>	删除权限组规则。
	ModifyAccessRule	nas:ModifyAccessRule	acs:nas:<region>:<account-id>:accessgroup/<accessgroupname>	修改权限组规则。
	DescribeAccessRule	nas:DescribeAccessRule	acs:nas:<region>:<account-id>:accessgroup/<accessgroupname>	列出权限组规则。

API		Action	Resource	说明
极速型NAS快照	ApplyAutoSnapshotPolicy	nas:ApplyAutoSnapshotPolicy	acs:nas:<region>:<account-id>:snapshot/<snapshotid>	为一个或者多个文件系统应用自动快照策略。
	CancelAutoSnapshotPolicy	nas:CancelAutoSnapshotPolicy	acs:nas:<region>:<account-id>:snapshot/<snapshotid>	取消一个或者多个文件系统的自动快照策略。
	CreateAutoSnapshotPolicy	nas:CreateAutoSnapshotPolicy	acs:nas:<region>:<account-id>:snapshot/<snapshotid>	创建一条自动快照策略。
	DeleteAutoSnapshotPolicy	nas:DeleteAutoSnapshotPolicy	acs:nas:<region>:<account-id>:snapshot/<snapshotid>	删除一条自动快照策略。
	ModifyAutoSnapshotPolicy	nas:ModifyAutoSnapshotPolicy	acs:nas:<region>:<account-id>:snapshot/<snapshotid>	修改一条自动快照策略。
	DescribeAutoSnapshotPolicies	nas:DescribeAutoSnapshotPolicies	acs:nas:<region>:<account-id>:snapshot/<snapshotid>	查询已创建的自动快照策略。
	CreateSnapshot	nas:CreateSnapshot	acs:nas:<region>:<account-id>:snapshot/*	创建快照。
	DeleteSnapshot	nas:DeleteSnapshot	acs:nas:<region>:<account-id>:snapshot/<snapshotid>	删除指定的快照。
	DescribeAutoSnapshotTasks	nas:DescribeAutoSnapshotTasks	acs:nas:<region>:<account-id>:snapshot/<snapshotid>	查询自动快照的任务。
	DescribeSnapshots	nas:DescribeSnapshots	acs:nas:<region>:<account-id>:snapshot/<snapshotid>	查询一个文件系统所有的快照列表。
	ResetFileSystem	nas:ResetFileSystem	acs:nas:<region>:<account-id>:snapshot/<snapshotid>	使用文件系统的历史快照回滚至某一阶段的文件系统状态。

API		Action	Resource	说明
生命周期管理	CreateLifecyclePolicy	nas:CreateLifecyclePolicy	acs:nas:<region>:<account-id>:lifecyclepolicy/<lifecyclerulename>	创建生命周期管理策略。
	ModifyLifecyclePolicy	nas:ModifyLifecyclePolicy	acs:nas:<region>:<account-id>:lifecyclepolicy/<lifecyclerulename>	修改生命周期管理策略。
	DeleteLifecyclePolicy	nas:DeleteLifecyclePolicy	acs:nas:<region>:<account-id>:lifecyclepolicy/<lifecyclerulename>	删除生命周期管理策略。
	DescribeLifecyclePolicies	nas:DescribeLifecyclePolicies	acs:nas:<region>:<account-id>:lifecyclepolicy/*	查询生命周期管理策略列表。

FAQ

- 创建经典网络挂载点时为什么需要RAM授权？
- 如何获取AccessKey？

4.1.2. NAS服务关联角色

为了完成NAS文件系统的某个功能，NAS将自动创建NAS服务关联角色获取访问云服务器ECS、专有网络VPC等云服务的权限。

应用场景

NAS服务关联角色的应用场景如下：

- AliyunServiceRoleForNasStandard

  创建通用型NAS文件系统的经典网络类型挂载点时，需要通过AliyunServiceRoleForNasStandard角色访问您的云服务器ECS服务，获取资源列表实现鉴权逻辑。

- AliyunServiceRoleForNasExtreme

  极速型NAS文件系统创建挂载点时，需要通过AliyunServiceRoleForNasExtreme角色访问您的专有网络VPC服务与云服务器ECS服务。

- AliyunServiceRoleForNasEncryption

  创建用户管理密钥（KMS）加密的文件系统时，需要通过AliyunServiceRoleForNasEncryption角色访问密钥管理服务KMS，获取您托管给密钥管理服务KMS的密钥信息，并为您选择的密钥添加标签，防止您误删除密钥导致文件系统不可用。

- AliyunServiceRoleForNasLogDelivery

  使用NAS日志分析功能时，需要通过AliyunServiceRoleForNasLogDelivery角色访问日志服务SLS，并在您的日志服务中创建Project和Logstore，将NAS中存储的日志数据转储至Logstore中。

- AliyunServiceRoleForNasBackup

在创建通用型文件系统时，若要使用文件备份功能，需要通过AliyunServiceRoleForNasBackup角色开通混合云备份服务并创建备份计划。

- AliyunServiceRoleForNasEcsHandler

  当您在NAS控制台使用一键挂载功能挂载文件系统时，需要通过AliyunServiceRoleForNasEcsHandler角色访问ECS云助手，并使用ECS云助手为一台或多台ECS实例触发一条云助手命令，实现挂载、卸载文件系统及查询ECS挂载状态。

更多服务关联角色的信息，请参见服务关联角色。

权限说明

NAS服务关联角色的权限内容如下：

AliyunServiceRoleForNasStandard

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

AliyunServiceRoleForNasExtreme

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "vpc:DescribeVSwitchAttributes",
        "vpc:DescribeVpcs",
        "vpc:DescribeVSwitches"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ecs:CreateSecurityGroup",
        "ecs:DescribeSecurityGroups",
        "ecs:DescribeSecurityGroupAttribute",
        "ecs:DeleteSecurityGroup",
        "ecs:AuthorizeSecurityGroup",
        "ecs:CreateNetworkInterface",
        "ecs:DeleteNetworkInterface",
        "ecs:DescribeNetworkInterfaces",
        "ecs:CreateNetworkInterfacePermission",
        "ecs:DescribeNetworkInterfacePermissions",
        "ecs:DeleteNetworkInterfacePermission"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

- AliyunServiceRoleForNasEncryption

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Listkeys",
        "kms:Listaliases",
        "kms:ListResourceTags",
        "kms:DescribeKey",
        "kms:TagResource",
        "kms:UntagResource"
      ],
      "Resource": "acs:kms:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "acs:kms:*:*:*/*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "kms:tag/acs:nas:instance-encryption": "true"
        }
      }
    }
  ],
  "Version": "1"
}
```

☐ AliyunServiceRoleForNasLogDelivery

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

☐ AliyunServiceRoleForNasBackup

```
{
 "Version": "1",
 "Statement": [{
   "Action": [
    "hbr:OpenHbrService",
    "hbr:CreateTrialBackupPlan"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "ram:DeleteServiceLinkedRole",
   "Resource": "*",
   "Effect": "Allow",
   "Condition": {
    "StringEquals": {
     "ram:ServiceName": "backup.nas.aliyuncs.com"
    }
   }
  },
  {
   "Action": "ram:CreateServiceLinkedRole",
   "Resource": "*",
   "Effect": "Allow",
   "Condition": {
    "StringEquals": {
     "ram:ServiceName": "nasbackup.hbr.aliyuncs.com"
    }
   }
  }
 ]
}
```

- AliyunServiceRoleForNasEcsHandler

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "ecs-handler.nas.aliyuncs.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:InvokeCommand"
      ],
      "Resource": [
        "acs:ecs:*:*:instance/*",
        "acs:ecs:*:*:command/cmd-ACS-NAS-ClickMount-*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeInstances",
        "ecs:DescribeCloudAssistantStatus"
      ],
      "Resource": [
        "acs:ecs:*:*:instance/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeInvocations",
        "ecs:DescribeInvocationResults"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

删除NAS服务关联角色

如果您暂时不需要使用NAS服务关联角色，例如不需要创建用户管理密钥（KMS）加密的文件系统时，可以删除NAS服务关联角色。删除时，请先删除该角色关联的文件系统实例。具体操作，请参见删除文件系统和删除服务关联角色。

FAQ

为什么我的RAM用户无法自动创建NAS服务关联角色？

您需要拥有指定的权限，才能自动创建或删除NAS服务关联角色。因此，在RAM用户无法自动创建NAS服务关联角色时，您需为其添加以下权限策略。具体操作，请参见为RAM角色授权。

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateServiceLinkedRole"
            ],
            "Resource": "acs:ram:*:主账号ID:role/*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "standard.nas.aliyuncs.com",
                        "extreme.nas.aliyuncs.com",
                        "encryption.nas.aliyuncs.com",
                        "logdelivery.nas.aliyuncs.com",
                        "ecs-handler.nas.aliyuncs.com"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

说明 请将 主账号ID 替换为您实际的阿里云账号ID。

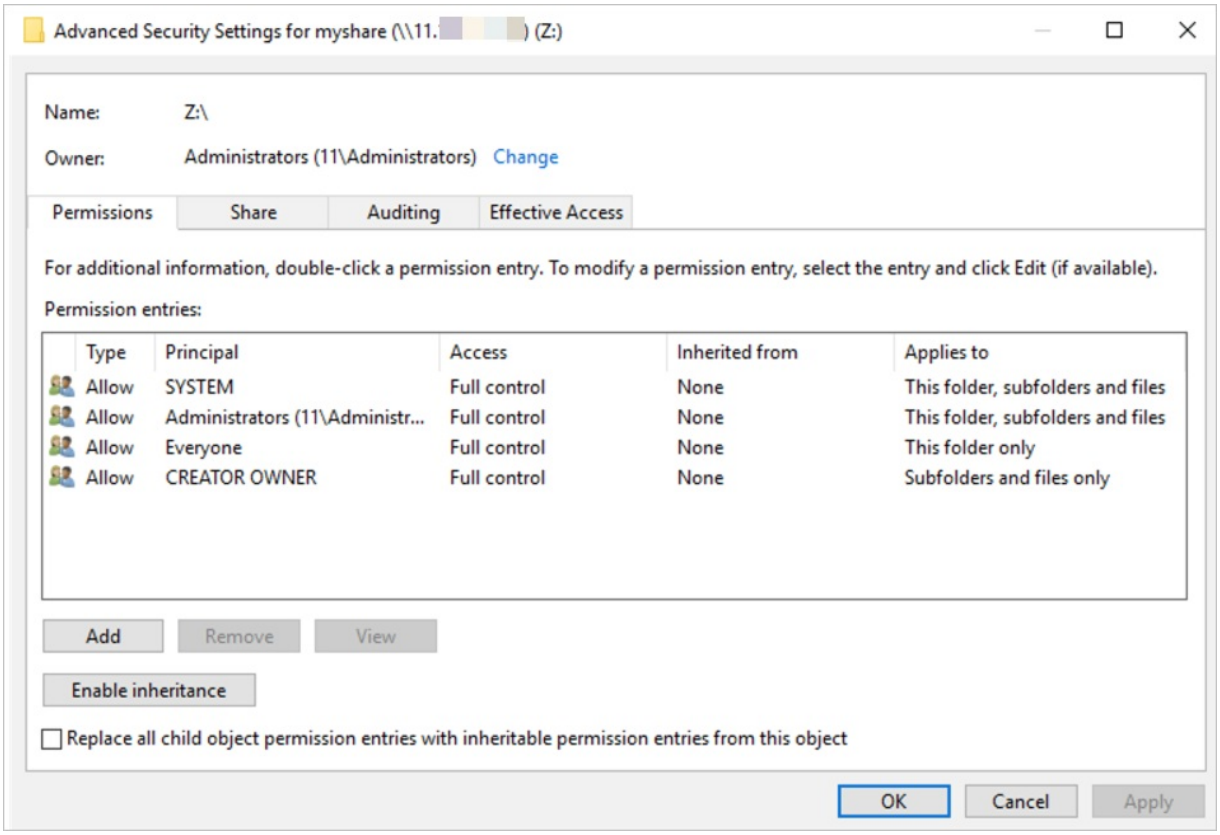
4.1.3. NAS SMB ACL

4.1.3.1. 文件存储NAS SMB ACL特性

ACL权限控制表是一项重要的企业级特性。在SMB文件系统不连通AD服务时，NAS SMB卷的ACL是只读的，用户登录身份为匿名（Everyone）。您可以将自建的AD服务与NAS SMB卷连通，通过AD域身份或者Everyone的方式挂载NAS SMB卷，从而对文件、文件夹设置ACL权限。本文简要介绍NAS SMB ACL的默认值设计及其相关特性。

默认值设计

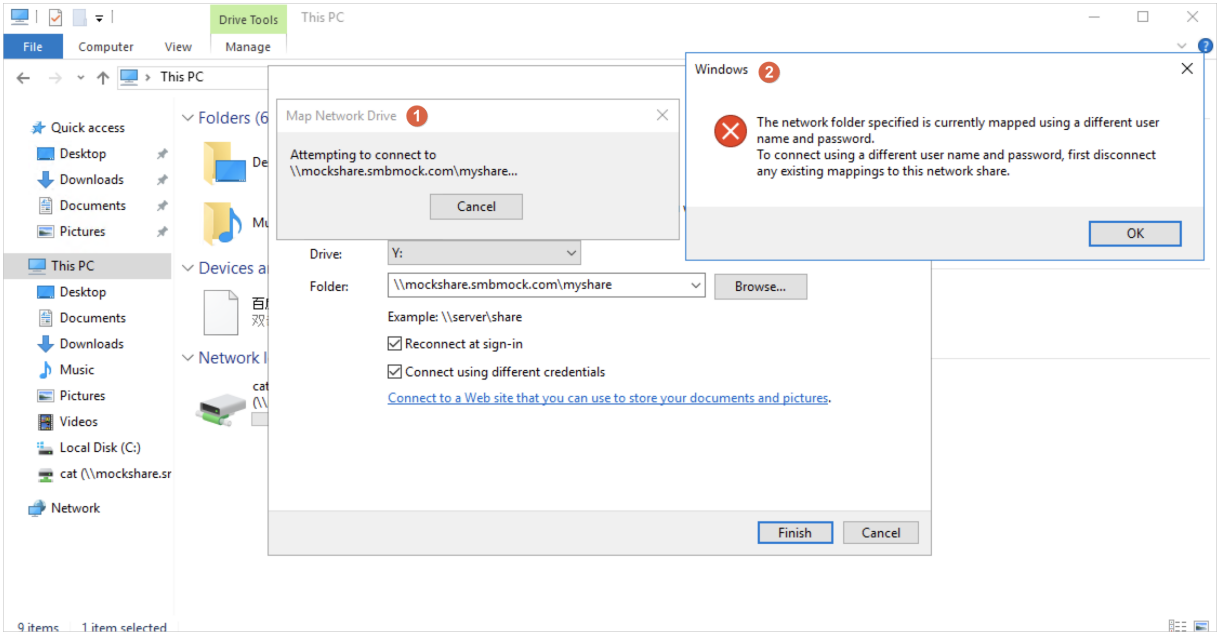
文件存储NAS SMB ACL的卷根目录权限默认值如图所示：



- 默认值设计的原因
  - SYSTEM和Administrators这两个ACL权限项是为了与Windows NTFS的权限对齐，保证管理员权限的程序能够正常运行。同时，在连通阿里云RAM账号系统之后，为超级用户提供管理员权限提供可能性。
  - CREATOR OWNER是为了实现继承机制，也为了与Windows NTFS权限对齐。
  - NAS SMB ACL可以修改配置，将**允许匿名访问**设置为**否**，在卷上禁止以Everyone身份进行访问，只有域身份用户才能访问。
- 兼容用户使用习惯
  - 为了兼容不使用AD的用户，对于AD功能打开之前创建的文件或文件夹，Everyone身份拥有所有权限（Full Control），保证不使用AD的用户不受影响。不使用AD的用户可以通过NTLM协议以Everyone的身份挂载文件卷并能访问Everyone所拥有的内容。
  - 新的AD用户创建的文件或文件夹不会继承Everyone权限，所以不使用AD的用户并不能访问新的AD用户创建的文件或文件夹，只有创建者用户和管理员用户可以访问。
  - AD用户可以访问不使用AD的用户（即Everyone）创建的文件或文件夹。

不支持多重身份挂载同一NAS SMB卷

只能以一种身份挂载一个NAS SMB卷。如果尝试以另一身份挂载会出现以下错误：



逃逸机制

如果出现恶意用户强行删除了管理者权限以及其他人的权限，导致文件、文件夹不可用，需要用管理员身份挂载并重写该文件、文件夹的权限。

阿里云NAS SMB文件卷实现了超级用户功能，您可以在控制台上配置某个用户或群组为超级用户，直接查看和修改任何文件及其相关权限，不受现有文件权限的限制。例如：当恶意用户把文件夹的拥有者改成自己，然后设置Deny Everyone之后，超级用户就可以将改坏的权限恢复回正确的权限。

> **注意** 在控制台更新超级用户之后，请重新挂载SMB文件系统。

Cygwin应用

Cygwin可以在Windows环境中虚拟POSIX环境，运行POSIX程序。但是在启用SMB ACL之后，用户SID、群组SID和Windows DACL权限在Cygwin中会转化成POSIX uid、gid和POSIX ACL。转化细节请参见Cygwin ntsec.html。

- 在*/etc/fstab*中加入noacl选项，如图所示。

```
# /etc/fstab
#
#    This file is read once by the first process in a Cygwin process tree.
#    To pick up changes, restart all Cygwin processes.  For a description
#    see https://cygwin.com/cygwin-ug-net/using.html#mount-table

# This is default anyway:
none /cygdrive cygdrive binary,noacl,posix=0,user 0 0
```

加入noacl选项后，Cygwin不会启用复杂的ACL转化，而是对新生成的文件和文件夹使用默认mode值。USER和GROUP则为当前Windows登录用户的用户名和群组。基本规则如下：

- 文件夹默认mode和uid、gid（755）

```
drwxr-xr-x 1 cat Domain Users 0 Jul 25 06:18 dir
```

- 文件的默认mode和uid、gid（644）

  ```
  -rw-r--r-- 1 cat Domain Users 0 Jul 25 06:42 file
  ```

- 文件的mode值可以为644或者444。

  如果是444，则文件设置了DOS Read-only权限。noacl只会转换文件的DOS Read-only权限。

- **chmod**命令不能修改文件夹的权限，可以修改文件的mode值到644或444。
- chown或chgrp命令无效。
- getfacl或setfacl命令不支持。
- 因为客户端文件夹权限只会显示成755，文件权限只会显示成644或444。可能会出现客户端显示有权限，但是服务端拒绝请求的情况。

- 在*/etc/fstab*中使用acl选项

  因为NAS SMB的默认挂载使用Everyone权限，而Everyone在Cygwin对应为OTHER。Cygwin在生成文件或文件夹时，会有类似Linux的行为，在创建文件之后自动执行chmod操作使文件或文件夹mode达到默认值。因为文件夹的other默认值是*r-x*，文件的默认值是*r--*，所以Everyone只有*r-x*或者*r--*的权限，导致新生成的文件夹里Everyone无法创建新文件，新生成的文件对于Everyone也是只读的。

  因此，强烈建议用户在Cygwin下使用noacl选项，不要使用acl选项。

在Linux下使用AD和ACL

- 在Linux下使用 `mount -t cifs` 挂载时，您可以指定挂载的域用户身份，以及挂载后的文件gid、uid、file mode、dir mode等。
- 在使用文件卷时，客户端会根据挂载的uid、gid和登录的真实用户身份进行基本的POSIX权限检查。
- 在文件服务器端，无论Linux用户以何种uid、gid身份登录，都将映射到该域用户身份进行操作。Linux Root身份也没有管理员权限，而是该域用户的权限。chmod、chown、chgrp、 getfacl或setfacl等Linux权限操作都将不起作用。

更多信息，请参见Linux客户端以AD域用户身份挂载并使用SMB文件系统。

4.1.3.2. 使用AD域实现用户身份认证和文件级别的权限访问控制

您可以基于AD（Active Directory）域来实现对阿里云SMB协议文件系统的用户身份和访问权限的管理。

背景信息

阿里云SMB协议文件存储服务支持基于AD域系统的用户身份认证及文件系统级别的权限访问控制。以域用户身份连接并访问SMB文件系统，可以实现对SMB协议文件系统中的文件及目录级别的访问控制的要求。目前的阿里云SMB协议文件存储服务不支持多用户的文件和目录级别的权限访问控制，只提供了支持云账号以及源地址IP权限组的白名单机制为基础的文件系统级别的鉴权和访问控制。

> **说明** 您可以在NAS控制台开启SMB AD ACL功能，如果您有其他问题，请提交工单。

前提条件

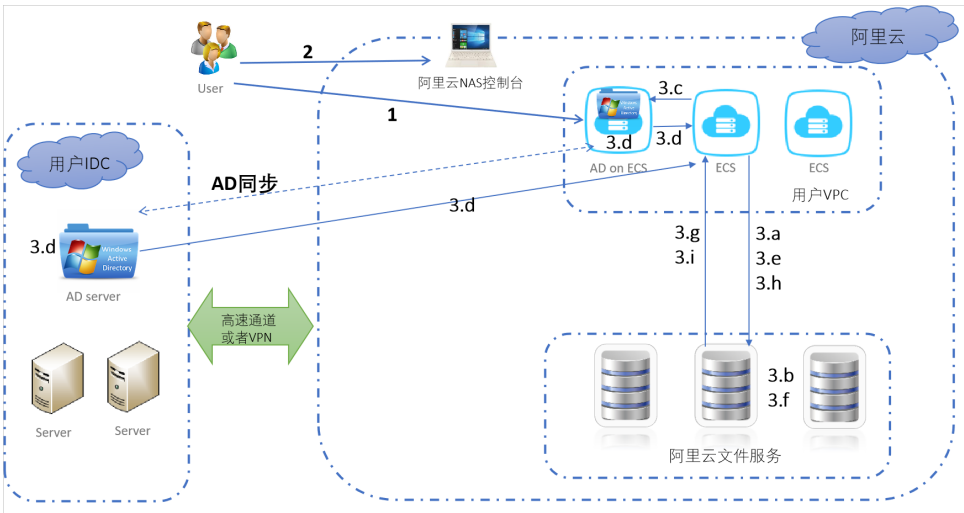
- 已安装和启用AD域服务与DNS服务，详情请参见安装并启用AD域服务与DNS服务。
- 支持SMB文件系统的Kerberos认证，详情请参见Kerberos网络身份认证协议介绍及SMB文件系统对其的支

持。

- 已创建SMB文件系统，详情请参见Windows系统挂载SMB文件系统。

创建用户认证及访问控制的流程

目前，阿里云文件存储NAS支持用户VPC（Virtual Private Cloud）或者用户IDC（Internet Data Center）内的AD域控制器的用户管理和文件系统访问权限控制，这样可以打通混合云用户的云上和云下用户认证以及文件系统权限控制。阿里云SMB协议文件存储服务可以依赖用户部署在线下或者阿里云上的AD域控制器，通过Kerberos网络身份认证协议来进行AD域用户身份的认证。用户可以在配置了域控制器的Windows或者Linux服务器上，以域用户身份连接并访问SMB文件系统，文件系统服务器可以得到用户的域身份，然后达到目录和文件级别的访问权限控制。如下图所示。



1. 将阿里云SMB协议文件系统挂载点接入AD域内。

   详情请参见将SMB文件系统挂载点接入AD域。

   i. 创建阿里云NAS文件系统的服务账号。

   ii. 注册NAS文件系统挂载点域名。

   iii. 为NAS文件系统挂载点服务生成Keytab密钥表文件。

   iv. 下载并上传阿里云文件系统服务账号的keytab。

2. 登录阿里云NAS控制台管理NAS文件系统。

   选择**文件系统 > 文件系统列表**，找到目标文件系统，单击文件系统ID或者**管理**。在**访问控制**区域，单击**开启**（或**关闭**），配置文件系统的用户认证和访问控制，上传Keytab文件。

   完成Keytab文件上传后，Keytab信息就保存到了阿里云NAS文件系统。这样，阿里云SMB文件系统挂载点接入到了AD域内，您可以开始以AD域用户身份挂载使用阿里云SMB协议文件系统。 详情请参见以AD域用户身份挂载使用阿里云SMB协议文件系统。

3. 通过客户端实现用户认证和访问控制。

   用户通过VPC内的VM或者IDC内的应用资源访问SMB文件系统建立连接的时候，首先可以通过目前已经实现的文件系统权限组进行权限验证，根据配置的权限组信息控制客户端的连接及访问，然后根据下面的逻辑进行用户认证和访问控制。

   i. 用户通过AD域访问文件系统建立连接后，通过SMB协议协商用户认证协议。

   ii. 文件服务器通过查找用户文件系统的配置，查询是否配置了Kerberos认证支持。

   详情请参见Kerberos网络身份认证协议介绍及SMB文件系统对其的支持。

   iii. 用户客户端向AD（用户VPC或是用户IDC内的AD服务器）发出访问阿里云文件系统服务的请求。

iv. AD域控制器认证用户后用阿里云文件系统服务账号的密钥加密用户信息，返回给用户客户端。

v. 用户客户端将加密的用户信息通过SMB Session Setup传给SMB文件服务器。

vi. 文件服务器通过用户提供的文件系统Keytab解密用户信息。

> 说明 其后在该Session上的所有访问都用该用户做为授权对象。

vii. 通过认证后，文件系统返回给用户客户端认证通过。否则拒绝Session Setup请求。

viii. 应用向文件系统发出文件系统访问，读写及其它请求。

ix. 文件服务器向用户系统返回文件访问结果。

文件访问控制由文件系统服务器执行。文件服务器根据Session的用户信息和文件系统的目录或文件的访问权限配置，允许或者拒绝用户访问。

4.1.3.3. 将SMB文件系统挂载点接入AD域

通过将SMB文件系统的挂载点接入AD域内，您可以在AD域中实现文件系统用户身份的认证管理和文件级别的访问权限控制。以AD域用户身份挂载使用SMB文件系统之前，您需要在AD域内为SMB文件系统注册服务，生成Keytab密钥表文件并上传至NAS控制台开启SMB ACL功能。

前提条件

已创建SMB文件系统。具体操作，请参见创建SMB文件系统。

步骤一：生成Keytab文件

您可以通过以下两种方式生成Keytab文件：

- 自动生成Keytab文件
  i. 登录需要安装AD域控制器和DNS服务的ECS服务器。
  ii. 在Powershell工具或者Powershell ISE工具中执行以下命令下载脚本。

```
Invoke-WebRequest https://code.aliyun.com/nas_team/nas-client-tools/raw/master/windows_client/alinas_smb_windows_inspection.ps1 -OutFile alinas_smb_windows_inspection.ps1
```

  iii. 执行以下命令自动安装AD域控制器和DNS服务，生成Keytab文件。

```
.\alinas_smb_windows_inspection.ps1 -MountAddress abcde-123.region-id.nas.aliyuncs.com -ConfigAD $true -Userdomain "example.com" -Username "administrator" -Password "password" -Locale zh-CN
```

> 注意 首次运行脚本安装完AD域服务后并首次启动AD域时，Windows AD服务器将会重启。重启后再次运行上述脚本，完成生成Keytab的步骤。

  其中，`example.com` 为您想要搭建的AD域名。

- 手动配置keytab文件
  i. 安装并启用AD域服务及DNS服务。具体操作，请参见安装AD域控制器。
  ii. 登录AD控制器所在的ECS服务器。
  iii. 打开CMD命令窗口，执行以下命令为SMB文件系统创建服务账号。

```
dsadd user CN=<AD服务账号名>,DC=<AD域域名>,DC=com
  -samid <AD服务账号名>
  -display <用户描述文字>
  -pwd <用户密码>
  -pwdneverexpires yes
```

示例：

```
dsadd user CN=alinas,DC=EXAMPLE,DC=com -samid alinas -display "Alibaba Cloud NAS Service Account" -pwd tHeRd123**** -pwdneverexpires yes
```

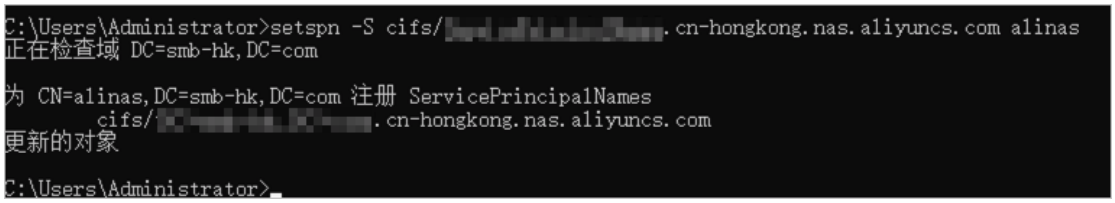
iv. 执行 `setspn -S cifs/<SMB协议NAS文件系统挂载点> <AD服务账号名>` 命令，为SMB文件系统挂载点注册并添加服务主体。

- 执行命令示例

```
setspn -S cifs/nas-mount-target.nas.aliyuncs.com alinas
```

- 返回示例

如果返回如下类似信息，则说明SMB文件系统挂载服务主体已添加成功。



v. 检查Windows AD服务器或Windows客户端的setspn配置。

a. 在Powershell工具或者Powershell ISE工具中执行以下命令下载脚本。

```
Invoke-WebRequest https://code.aliyun.com/nas_team/nas-client-tools/raw/master/windows_client/alinas_smb_windows_inspection.ps1 -OutFile alinas_smb_windows_inspection.ps1
```

b. 检查setspn配置。

```
.\alinas_smb_windows_inspection.ps1 -MountAddress abcde-123.region-id.nas.aliyuncs.com -CheckAD $true -Userdomain "example.com" -Username "administrator" -Password "password" -Locale zh-CN
```

其中，`example.com` 为您已搭建的AD域名。

vi. 在AD域服务器上，打开CMD命令窗口，执行以下命令为SMB文件系统挂载点生成Keytab密钥表文件。

```
ktpass
  -princ cifs/<SMB文件系统挂载点>
  -ptype KRB5_NT_PRINCIPAL
  -crypto All
  -out <生成的密钥表文件的文件路径>
  -pass <用户密码>
```

示例：

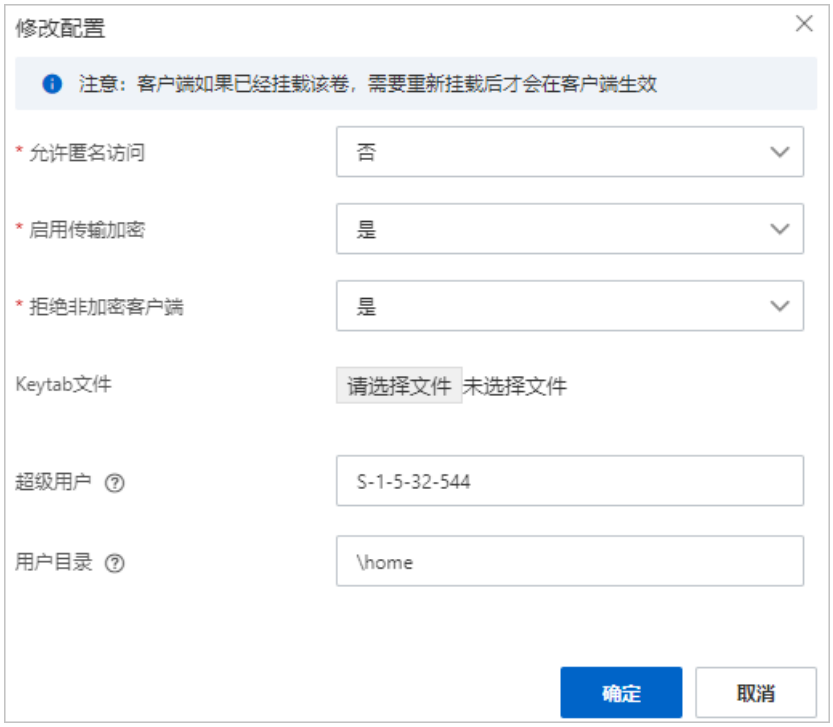
```
ktpass -princ cifs/nas-mount-target.nas.aliyuncs.com@EXAMPLE.com -ptype KRB5_NT_PRINCIPAL -mapuser alinas@example.com -crypto All -out c:\nas-mount-target.keytab -pass tHeP****d123
```

步骤二：上传Keytab文件

在NAS控制台，上传阿里云SMB文件系统服务账号的Keytab文件。

1. 登录NAS控制台。
2. 在左侧导航栏，选择**文件系统 > 文件系统列表**。
3. 在**文件系统列表**页面，单击目标文件系统ID或**管理**。
4. 在**访问控制**页签，单击**开启**。
5. 在**开启SMB ACL**对话框，上传阿里云文件系统服务账号的Keytab文件，单击**确定**。

6. 在**访问控制**页签，单击**修改配置**。
7. 在**修改配置**对话框，请参见如下说明对参数进行修改。



参数	描述

参数	描述
允许匿名访问	是否允许匿名访问文件系统。取值范围如下： ○ 是：允许任何人以NTLM方式挂载该文件系统，挂载后用户身份为Everyone，ACL仍然生效。 ○ 否（默认值）：不允许匿名用户访问文件系统。
启用传输加密	是否开启SMB文件系统传输加密功能。取值范围如下： ○ 是：开启SMB文件系统传输加密功能。 ○ 否（默认值）：不开启SMB文件系统传输加密功能。 更多信息，请参见SMB文件系统传输加密。
拒绝非加密客户端	配置访问SMB文件系统的客户端类型。取值范围如下： ○ **是**：仅支持使用传输加密的客户端挂载该SMB文件系统，即支持SMB传输加密的操作系统以AD域身份挂载SMB文件系统。 当以匿名身份挂载或使用不支持传输加密的客户端挂载SMB文件系统时，挂载将会失败。 ○ **否**：所有客户端均能挂载该SMB文件系统，但只有支持传输加密的操作系统以AD域身份挂载SMB文件系统才会启用传输加密功能。
Keytab文件	上传Keytab文件。
超级用户	超级用户能够在不改动ACL的情况下对任何文件夹中的任何文件进行操作，您可以将超级用户配置为用户或群组。配置时需符合SID格式，例如S-1-5-32-544。默认值为空。
用户目录	每个用户的用户目录主路径。例如用户目录是\home，则对于用户A，文件系统会在A登录时自动创建\home\A的目录。如果\home\A已经存在，则跳过。默认值为空。 **注意** \home目录要有允许用户A创建目录的权限，否则\home\A无法创建。

注意 如果客户端已挂载SMB文件系统，在修改配置后请重新挂载SMB文件系统，使AD域服务账号配置生效。

后续步骤

将SMB文件系统挂载点接入到了AD域后，您可以通过AD域身份挂载并使用SMB文件系统。具体操作，请参见Windows客户端以AD域用户身份挂载并使用SMB文件系统和Linux客户端以AD域用户身份挂载并使用SMB文件系统。

4.1.3.4. Windows客户端以AD域用户身份挂载并使用SMB文件系统

本文介绍在Windows操作系统中，如何以AD域身份挂载SMB文件系统。以及挂载成功后，如何以AD域身份访问SMB协议文件系统，查看和编辑文件或目录的ACL。

前提条件

SMB文件系统挂载点已接入AD域。具体操作，请参见将SMB文件系统挂载点接入AD域。

背景信息

在SMB文件系统挂载点接入AD域前，仅支持以匿名用户身份挂载并使用SMB文件系统。在SMB文件系统挂载点接入AD域后，您可以设置是否继续允许匿名用户身份挂载访问。

- 如果继续允许匿名访问文件系统，设备可以通过Kerberos认证以域身份访问文件系统，也可以通过NTLM认证以Everyone身份访问文件系统。
- 如果已设置为不允许匿名访问文件系统，该文件系统将只允许通过Kerberos认证协议的Windows客户端以AD域用户身份进行挂载。

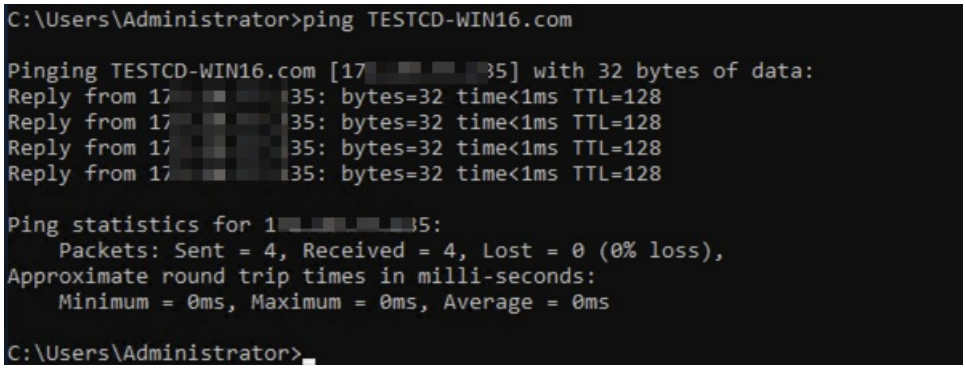
方式一：Windows客户端加入AD域并挂载SMB文件系统

以下步骤将以Windows Server 2012版本操作系统为例介绍如何将Windows客户端加入AD域并挂载SMB文件系统。

1. 配置Windows客户端的DNS服务器地址。
   i. 登录Windows客户端。
   ii. 在桌面左下角，单击**开始**。
   iii. 在**开始**菜单栏，单击**控制面板**。
   iv. 在**控制面板**对话框，选择**网络和Internet > 网络和共享中心**。
   v. 在**网络与共享中心**对话框**查看活动网络**区域，单击**以太网**。
   vi. 在**以太网属性**对话框，单击**属性**。
   vii. 在**以太网属性**对话框**此连接使用下列项目：**区域，选中**Internet协议版本4（TCP/IPv4）**，单击**属性**。

viii. 在**Internet协议版本4（TCP/IPv4）属性**对话框，选中**使用下面的DNS服务器地址**，设置DNS服务器地址为AD域服务器的IP地址。

ix. 使用命令提示符工具执行**ping**命令，**ping**AD域名，验证Windows客户端和AD域之间的连通性。



2. 将Windows客户端加入AD域。
   i. 在**控制面板**对话框，选择**系统和安全 > 系统**。
   ii. 在**系统**对话框**计算机名、域和工作组设置**区域，单击**更改设置**。
   iii. 在**系统属性**对话框，单击**更改**。

iv. 在**计算机名/域更改**对话框，填写已搭建的AD域名。根据界面提示，单击**确定**完成配置。

v. 重启Windows客户端，使修改配置生效。

3. 挂载SMB文件系统。

以AD域身份登录Windows客户端，使用命令提示符工具执行以下命令，挂载SMB文件系统。

```
net use z: \\nas-mount-target.nas.aliyuncs.com\myshare
```

方式二：Windows客户端连接AD服务器并挂载SMB文件系统

以下步骤将以Windows Server 2012版本操作系统为例介绍通过配置DNS服务器连接AD服务器，然后挂载SMB文件系统。

1. 配置Windows客户端的DNS服务器地址。

i. 登录Windows客户端。

ii. 在桌面左下角，单击**开始**。

iii. 在**开始**菜单栏，单击**控制面板**。

iv. 在**控制面板**对话框，选择**网络和Internet > 网络和共享中心**。

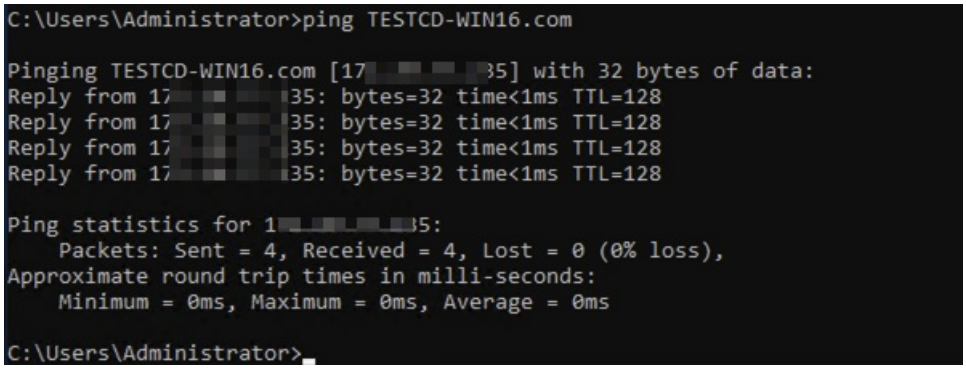
v. 在**网络与共享中心**对话框**查看活动网络**区域，单击**以太网**。

vi. 在**以太网属性**对话框，单击**属性**。

vii. 在**以太网属性**对话框**此连接使用下列项目：**区域，选中**Internet协议版本4（TCP/IPv4）**，单击**属性**。

viii. 在**Internet协议版本4（TCP/IPv4）属性**对话框，选中**使用下面的DNS服务器地址**，设置DNS服务器地址为AD域服务器的IP地址。

ix. 使用命令提示符工具执行**ping**命令，**ping**AD域名，验证Windows客户端和AD域之间的连通性。



2. 挂载SMB文件系统。

   在Windows客户端，使用命令提示符工具执行以下命令，以AD域身份挂载SMB文件系统。

   ```
   net use z: \\nas-mount-target.nas.aliyuncs.com\myshare /user:EXAMPLE.com\USERNAME PASSWORD
   ```

   其中，`EXAMPLE.com`为您已搭建的AD域名。

管理SMB文件系统ACL

开启ACL功能并以AD域身份挂载SMB文件系统后，您可以采用以下方式查看和编辑文件或目录ACL。

- mklink命令行工具

您可以使用mklink命令行工具，在Windows本地磁盘为SMB文件系统挂载点生成符号链接，同时查看和编辑文件或目录的ACL。

i. 使用命令提示符工具创建文件系统映射。

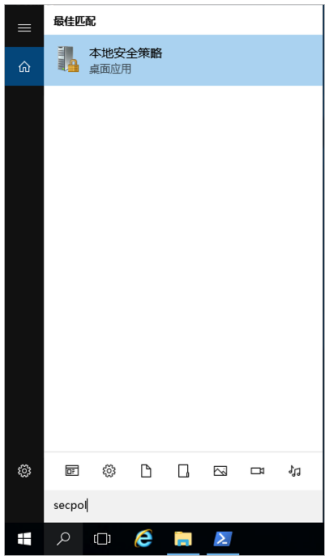
```
mklink /D c:\myshare \\nas-mount-target.nas.aliyuncs.com\myshare
```

其中，`\myshare`为符号链接的文件系统路径，`\nas-mount-target.nas.aliyuncs.com\myshare`为SMB文件系统的挂载点。

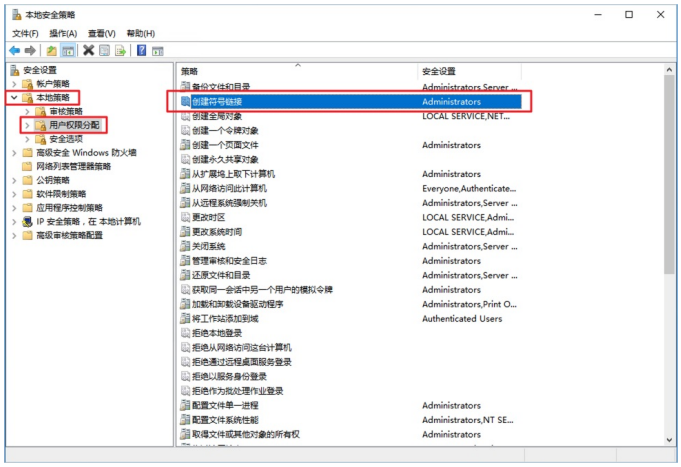
ii. 为普通用户添加使用符号链接的权限。

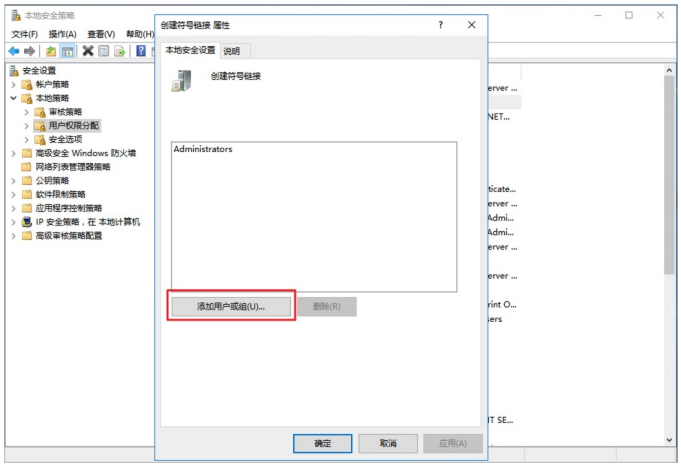
如果您使用系统管理员Administrator，请跳过此步骤。

a. 使用系统管理员Administrator搜索并运行secpol.msc。



b. 在**本地安全策略**对话框，选择**本地策略 > 用户权限分配**，按照页面提示将指定用户加入**创建符号链接**的权限组中。





c. 使用普通用户重新登录Windows客户端。

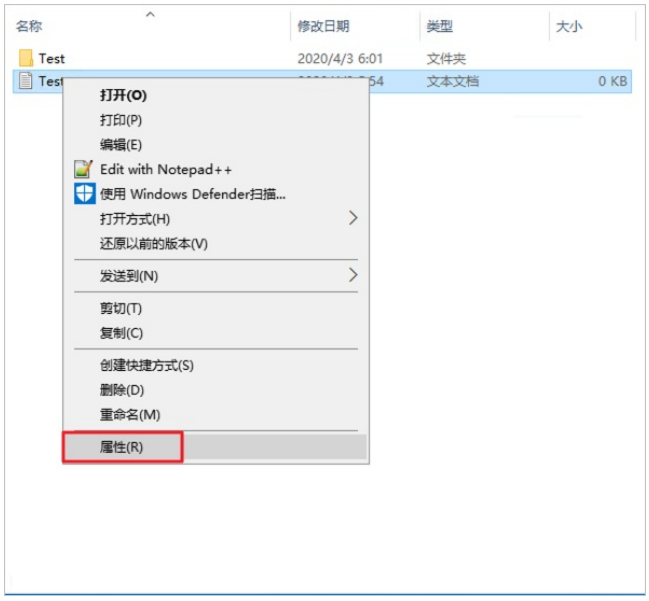
iii. 访问SMB文件系统并查看文件或目录ACL。

生成符号链接后，您可以以访问Windows本地磁盘子目录的形式访问SMB文件系统，同时支持查看和编辑文件或目录的ACL。

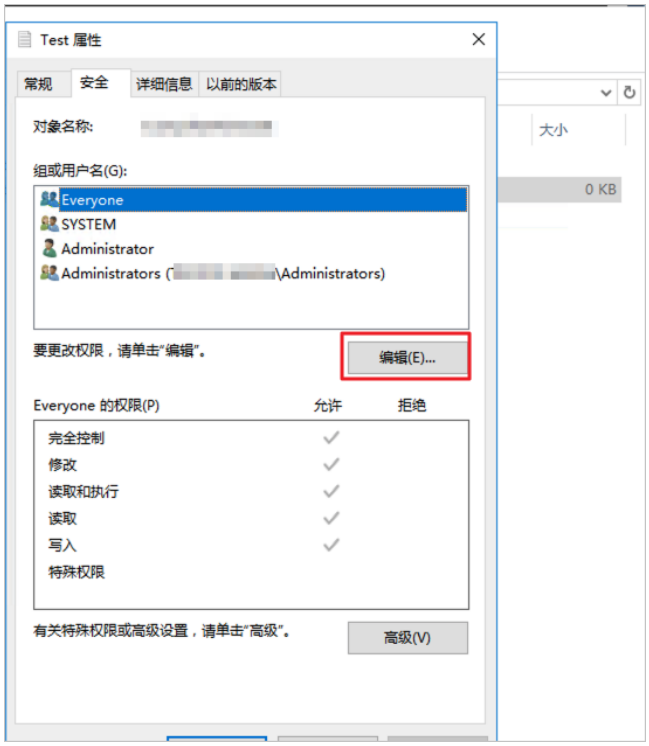
- Windows文件资源管理器

在Windows本地磁盘为SMB文件系统挂载点生成符号链接，可以通过Windows的文件资源管理器（File Explorer）查看、编辑文件和目录的ACL。

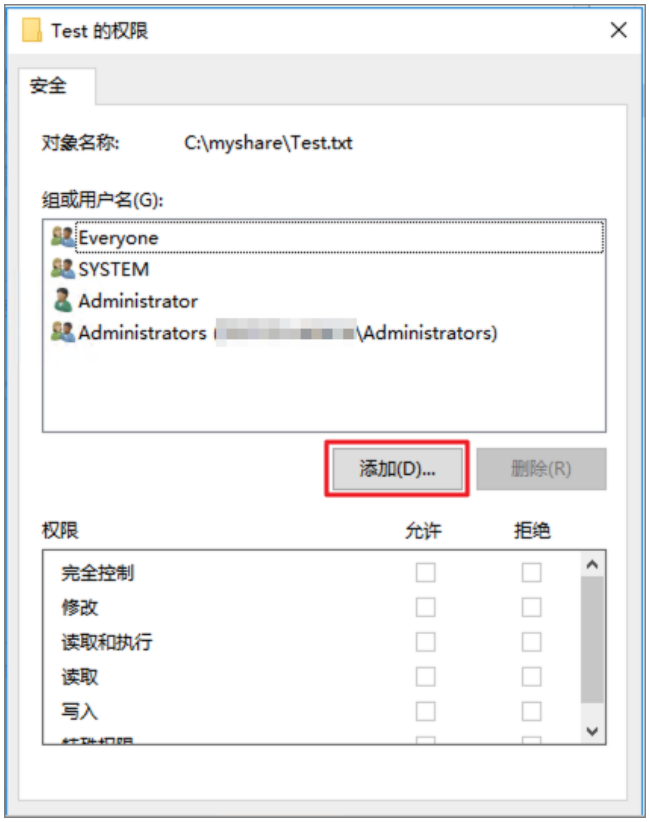
i. 找到目标文件或目录，右键单击**属性**。

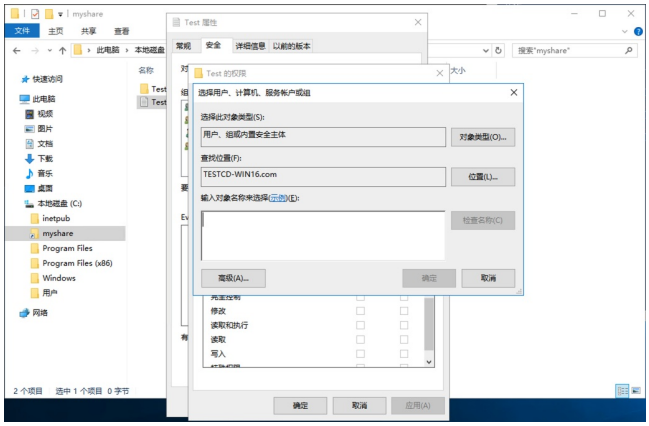


ii. 在**属性**对话框，单击**安全**页签，然后单击**编辑**。



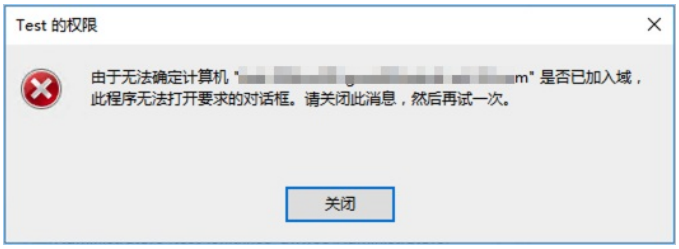
iii. 在权限对话框，单击**添加**，按照页面提示填写相关信息。

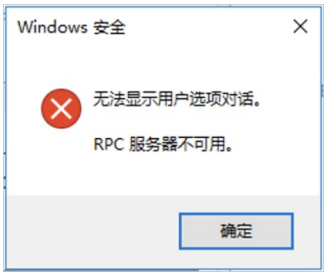




在使用Windows文件资源管理器查看SMB文件系统时，如果需要回退本地磁盘路径，请单击回退（下图中的标注1）或者上退（下图中的标注2）按钮，但是不要选中路径中的某一段（下图中的标注3）来回退。

在使用Windows文件资源管理器访问和使用文件系统时，阿里云SMB文件系统并没有实际加入用户的AD域。如果不是通过本地磁盘路径*C:\myshare*访问文件系统，而是通过普通网络路径*\\nas-mount-point.nas.aliyuncs.com\myshare*访问，在设置ACL时，会遇到因RPC服务器不可用而无法确定NAS挂载点是否已加入域的情况。





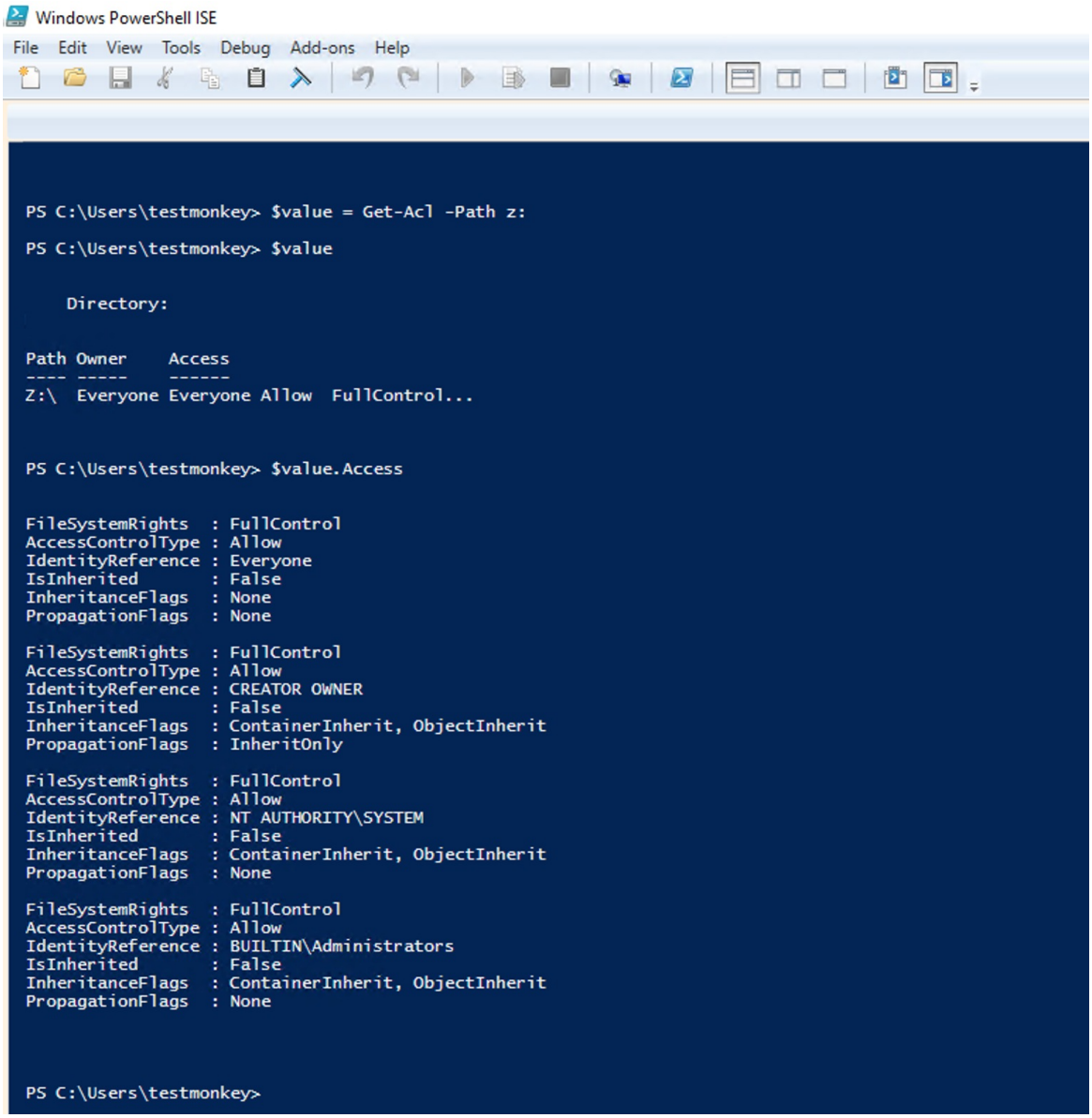
> 注意　Windows文件资源管理器对*C:\myshare*修改权限并不会应用到文件系统的根目录。修改根目录权限需要使用 `Set-Acl Powershell` 命令或者 `icacls` 命令行。

- Powershell命令

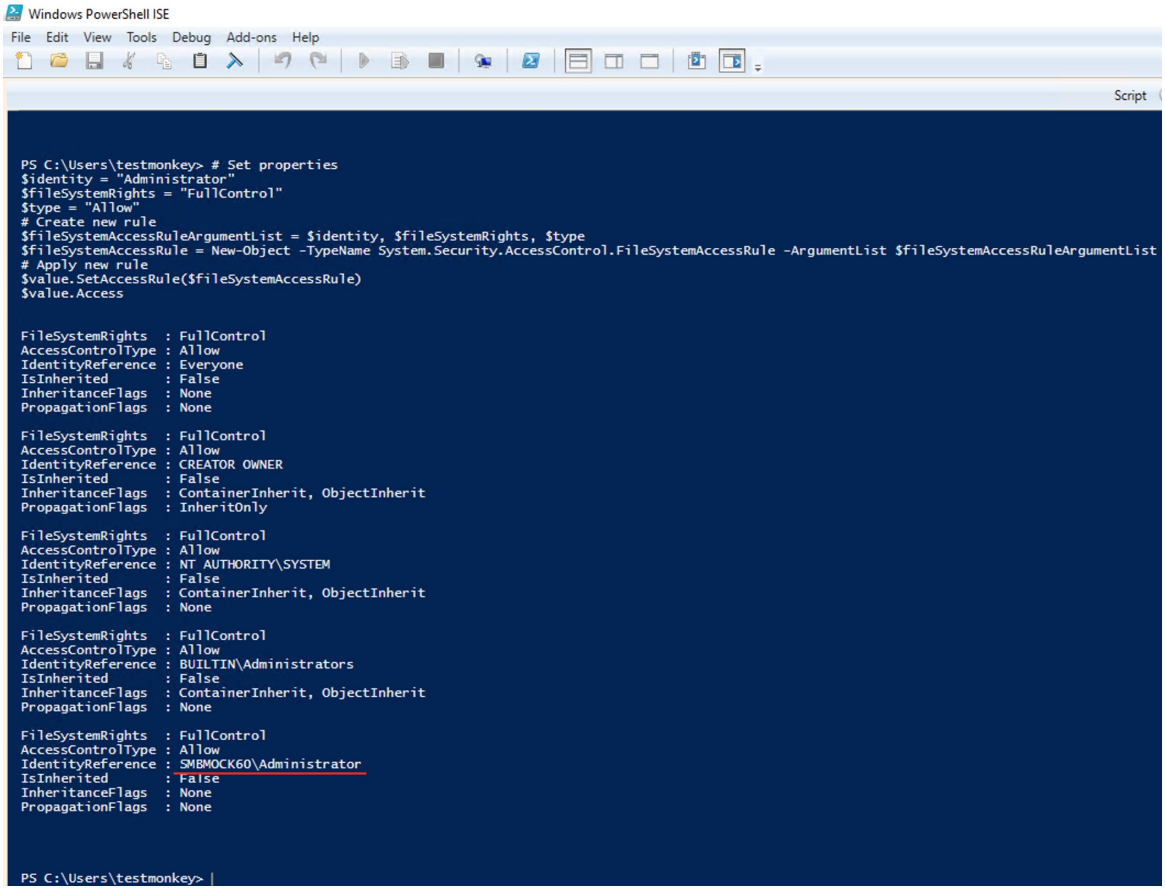
  Windows Powershell支持 `Get-Acl` 和 `Set-Acl` 来查看和编辑文件或目录ACL。

  - Get-Acl

    ```
    $value = Get-Acl -Path "Z:"# Set properties
    $value.Access
    ```




```
Set properties
$identity = "Administrator"
$fileSystemRights = "FullControl"
$type = "Allow"
# Create new rule
$fileSystemAccessRuleArgumentList = $identity, $fileSystemRights, $type
$fileSystemAccessRule = New-Object -TypeName System.Security.AccessControl.FileSystemAc
cessRule -ArgumentList $fileSystemAccessRuleArgumentList
# Apply new rule
$value.SetAccessRule($fileSystemAccessRule)
$value.Access
```



- Set-Acl

  Set-Acl命令修改权限不需要 `mylink c:\myshare` 快捷方式，可以直接修改挂载盘路径，也可以修改根目录权限。

  ```
  Set-Acl $value -Path "Z:"
  ```

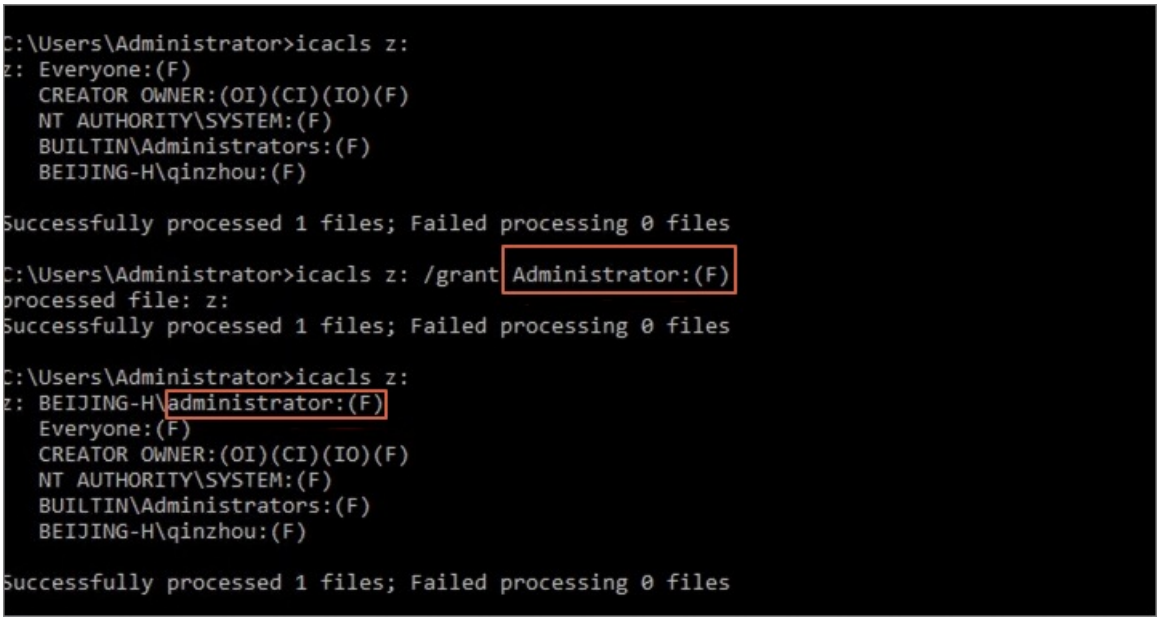
  > **注意** 根目录权限修改最好在文件系统刚创建时就设置妥当，否则由于继承机制，命令会需要修改子目录和子文件。

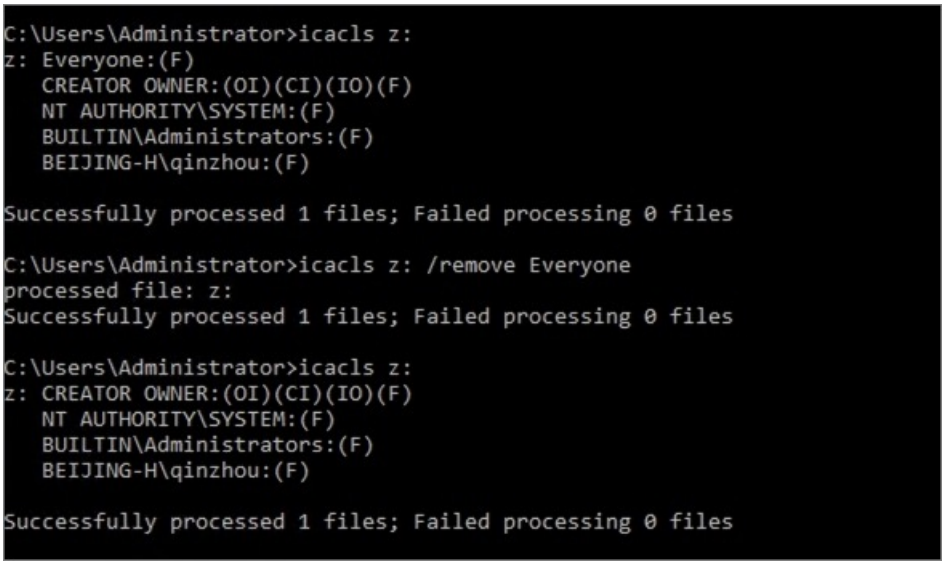
- icacls命令

  icacls命令是Windows命令行中的ACL操作标准命令。您可以通过 `icacls` 命令查看和编辑文件或目录ACL。

  示例：

```
icacls z:
#添加用户的完全控制权限
icacls z: /grant <用户名>:(F)
#添加administrator的完全控制权限
icacls z: /grant administrator:(F)
icacls z:
#删除用户的所有权限
icacls z: /remove <用户名>
#删除Everyone的所有权限
icacls z: /remove <用户名>
icacls z:
```





4.1.3.5. Linux客户端以AD域用户身份挂载并使用SMB文件系统

本文介绍在Linux操作系统中，如何以AD域身份挂载SMB文件系统。以及挂载成功后，如何以AD域身份访问SMB协议文件系统，查看和编辑文件或目录的ACL。

前提条件

- SMB文件系统挂载点已接入AD域。具体操作，请参见将SMB文件系统挂载点接入AD域。
- 使用适配SMB文件系统的Linux操作系统版本。更多信息，请参见使用限制和推荐内核镜像。

背景信息

在SMB文件系统挂载点接入AD域前，仅支持以匿名用户身份挂载并使用SMB文件系统。在SMB文件系统挂载点接入AD域后，您可以设置是否继续允许匿名用户身份挂载访问。

- 如果继续允许匿名访问文件系统，设备可以通过Kerberos认证以域身份访问文件系统，也可以通过NTLM认证以Everyone身份访问文件系统。
- 如果已设置为不允许匿名访问文件系统，该文件系统将只允许通过Kerberos认证协议的Linux客户端以AD域用户身份进行挂载。

以下步骤以Ubuntu和CentOS为例介绍如何以AD域身份挂载访问SMB文件系统。

方式一：Linux客户端加入AD域并挂载SMB文件系统

1. 登录Linux客户端。
2. Linux客户端加入AD域。
   - Ubuntu操作系统
     a. 安装AD服务器配置包。

```
sudo apt-get update
```

```
sudo apt-get -y install realmd libnss-sss libpam-sss sssd sssd-tools adcli samba-common-bin oddjob oddjob-mkhomedir packagekit krb5-user
```

     b. 配置Linux客户端在AD域的机器名。

```
sudo hostnamectl set-hostname myubuntu.example-company.com
```

     其中，`example-company.com`为AD域名称，请您根据实际业务场景配置。

     配置完成后，执行**hostnamectl**命令检查已配置的客户端机器名称。

```
user1@myubuntu:/home$ sudo hostnamectl set-hostname myubuntu.example-company.com
user1@myubuntu:/home$ hostnamectl
   Static hostname: myubuntu.example-company.com
         Icon name: computer-vm
           Chassis: vm
        Machine ID: 20210623112404781463487467590001
           Boot ID: 0702ff766c504355a16f9b27e467a6f6
    Virtualization: kvm
  Operating System: Ubuntu 20.04.2 LTS
            Kernel: Linux 5.4.0-77-generic
      Architecture: x86-64
user1@myubuntu:/home$
```

c. 配置DNS。

执行以下命令停止DNS的自动更新。

```
sudo systemctl disable systemd-resolved
sudo systemctl stop systemd-resolved
```

然后将AD服务器IP写入*/etc/resolv.conf*中。

```
# Generated by NetworkManager
search example-company.com
nameserver 172.19.0.61
```

执行ping命令，pingAD服务器名称验证连通性。

```
user1@myubuntu:/home$ ping example-company.com
PING example-company.com (172.19.0.61) 56(84) bytes of data.
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=1 ttl=128 time=0.274 ms
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=2 ttl=128 time=0.289 ms
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=3 ttl=128 time=0.270 ms
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=4 ttl=128 time=0.273 ms
^C
--- example-company.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3073ms
rtt min/avg/max/mdev = 0.270/0.276/0.289/0.007 ms
```

d. 查找AD域。

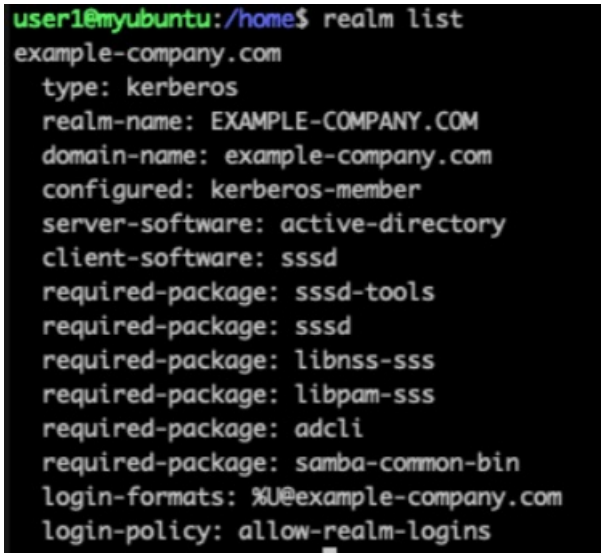
```
realm discover <AD domain>
```

```
user1@myubuntu:/home$ realm discover example-company.com
example-company.com
  type: kerberos
  realm-name: EXAMPLE-COMPANY.COM
  domain-name: example-company.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
  login-formats: %U@example-company.com
  login-policy: allow-realm-logins
```

e. Linux客户端加入AD域。

```
sudo kinit Administrator@EXAMPLE-COMPANY.COM
sudo realm join -U Administrator example-company.com
```

执行realm list命令，如果回显包含如下类似信息，说明Linux客户端已加入AD域。



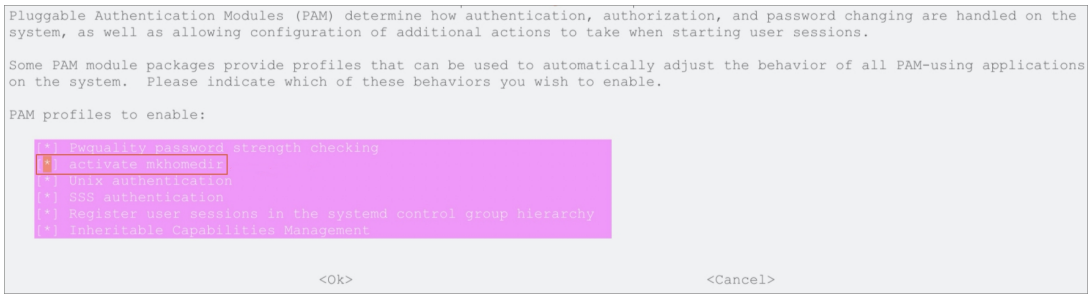
f. 配置以AD域用户登录时的home目录。

```
sudo bash -c "cat > /usr/share/pam-configs/mkhomedir" <<EOF
Name: activate mkhomedir
Default: yes
Priority: 900
Session-Type: Additional
Session:
        required                        pam_mkhomedir.so umask=0022 skel=/etc/ske
l
EOF
```

执行以下命令激活该配置。

```
pam-auth-update
```

激活后，通过上下键移动光标，并使用空格键增加选项标记 `*` ，请确保 `activate mkhomedir` 选项前标记为 `*` ，然后使用Tab键将光标移动至**Ok**，即完成设置。



g. 配置Linux sssd服务。

在配置文件*/etc/sssd/sssd.conf*中，写入 `krb5_ccname_template=FILE:%d/krb5cc_%U` 。

```
[sssd]
domains = example-company.com
config_file_version = 2
services = nss, pam

[domain/example-company.com]
default_shell = /bin/bash
krb5_store_password_if_offline = True
cache_credentials = True
krb5_realm = EXAMPLE-COMPANY.COM
realmd_tags = manages-system joined-with-adcli
id_provider = ad
fallback_homedir = /home/%u@%d
ad_domain = example-company.com
use_fully_qualified_names = True
ldap_id_mapping = True
access_provider = ad
krb5_ccname_template=FILE:%d/krb5cc_%U
```

执行以下命令重启sssd服务并确认服务状态。

```
sudo systemctl restart sssd
sudo systemctl status sssd
```

如果回显包含如下类似信息，说明Linux sssd服务已配置成功。

```
root@iZrj90myfgaf70i4jqsmr9Z:~# systemctl status sssd
● sssd.service - System Security Services Daemon
     Loaded: loaded (/lib/systemd/system/sssd.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2021-03-12 14:00:21 CST; 3s ago
   Main PID: 21279 (sssd)
      Tasks: 4 (limit: 9315)
     Memory: 42.2M
     CGroup: /system.slice/sssd.service
             ├─21279 /usr/sbin/sssd -i --logger=files
             ├─21300 /usr/libexec/sssd/sssd_be --domain example.com --uid 0 --gid 0 --logger=files
             ├─21301 /usr/libexec/sssd/sssd_nss --uid 0 --gid 0 --logger=files
             └─21302 /usr/libexec/sssd/sssd_pam --uid 0 --gid 0 --logger=files
```

- CentOS操作系统

a. 安装AD服务器配置包。

```
sudo yum update
sudo yum install sssd realmd oddjob oddjob-mkhomedir adcli samba-common samba-com
mon-tools krb5-workstation openldap-clients policycoreutils-python-utils -y
```

b. 配置Linux客户端在AD域的机器名。

```
sudo hostnamectl set-hostname mycentos.example-company.com
```

其中，`example-company.com`为AD域名称，请您根据实际业务场景配置。

配置完成后，执行**hostnamectl**命令检查已配置的客户端机器名称。

```
[user1@mycentos root]$ sudo hostnamectl set-hostname mycentos.example-company.com
[user1@mycentos root]$ hostnamectl
   Static hostname: mycentos.example-company.com
         Icon name: computer-vm
           Chassis: vm
        Machine ID: 20210623110808105647395700239158
           Boot ID: e8fded82c87f4fe783e3c75263c854d9
    Virtualization: kvm
  Operating System: CentOS Linux 8
       CPE OS Name: cpe:/o:centos:centos:8
            Kernel: Linux 4.18.0-305.12.1.el8_4.x86_64
      Architecture: x86-64
```

c. 配置DNS。

将AD服务器IP写入*/etc/resolv.conf*中，删除默认的DNS服务器。

```
# Generated by NetworkManager
search example-company.com
nameserver 172.19.0.61
```

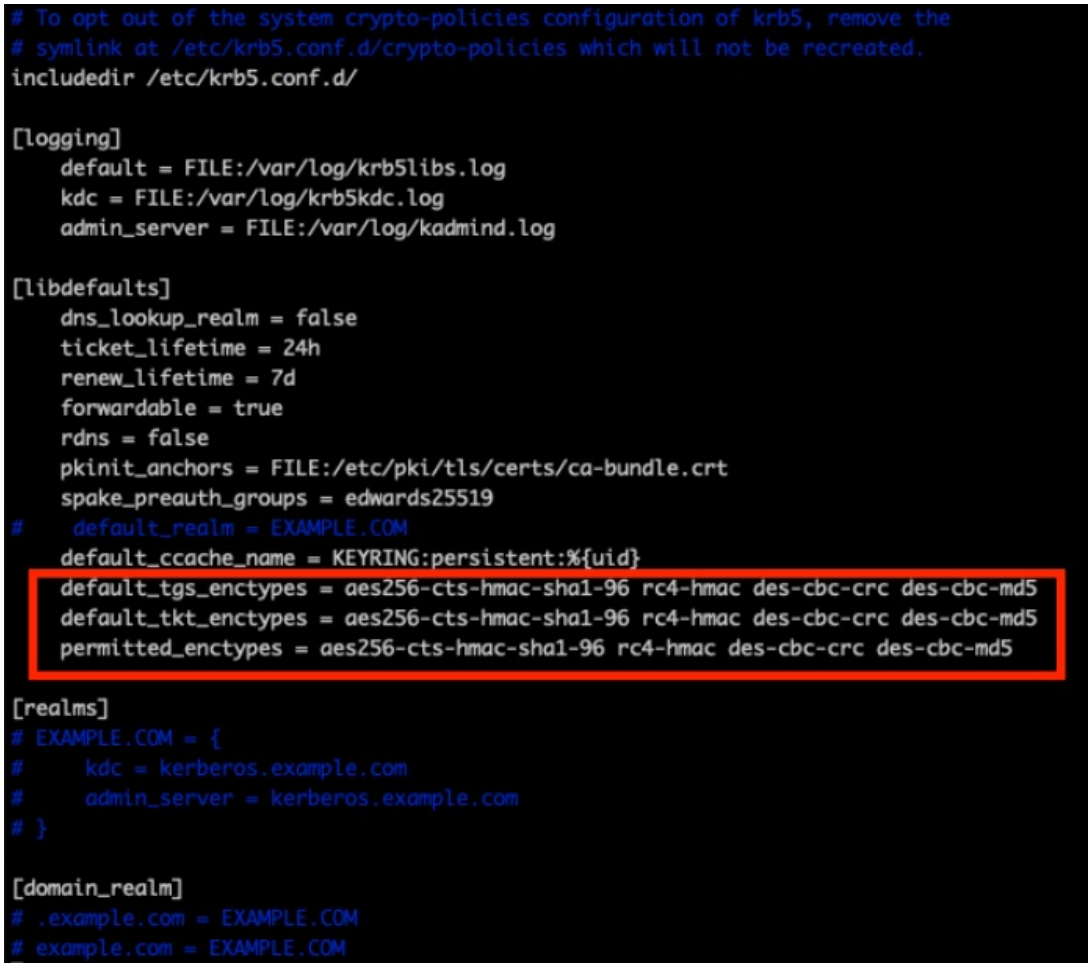
执行**ping**命令，**ping**AD服务器名称验证连通性。

```
[user1@mycentos root]$ ping example-company.com
PING example-company.com (172.19.0.61) 56(84) bytes of data.
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=1 ttl=128 time=0.221 ms
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=2 ttl=128 time=0.334 ms
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=3 ttl=128 time=0.314 ms
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=4 ttl=128 time=0.323 ms
^C
--- example-company.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3044ms
rtt min/avg/max/mdev = 0.221/0.298/0.334/0.045 ms
```

d. 配置Kerberos。

请在配置文件*/etc/krb5.conf*中添加如下内容。

```
    default_tgs_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-m
d5
    default_tkt_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-m
d5
    permitted_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
```



e. 查找AD域。

```
realm discover example-company.com
```

```
[user1@mycentos root]$ realm discover example-company.com
example-company.com
  type: kerberos
  realm-name: EXAMPLE-COMPANY.COM
  domain-name: example-company.com
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
```

f. Linux客户端加入AD域。

```
sudo realm join -U Administrator example-company.com
```

执行**realm list**命令，如果回显包含如下类似信息，说明Linux客户端已加入AD域。

```
[user1@mycentos root]$ realm list
example-company.com
  type: kerberos
  realm-name: EXAMPLE-COMPANY.COM
  domain-name: example-company.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
  login-formats: %U@example-company.com
  login-policy: allow-realm-logins
```

3. 执行**id**命令，查询AD域用户身份状态。

```
id testuser@example-company.com
```

如果回显包含如下类似信息，说明AD域用户身份能被正常识别。

```
[user1@mycentos root]$ id usera1@example-company.com
uid=371801107(usera1@example-company.com) gid=371800513(domain users@example-company.com) groups=371800513(domain users@example-company.com)
```

4. 添加AD域用户登录权限。
   - 授予指定用户登录Linux客户端的权限。

     ```
     sudo realm permit usera1@example-company.com
     sudo realm permit userb1@example-company.com userb2@example-company.com
     ```

   - 授予指定用户组登录Linux客户端的权限。

```
sudo realm permit -g 'Security Users'
sudo realm permit -g 'Domain Users' 'Domain Admins'
```

- 授予所有用户登录Linux客户端的权限。

```
sudo realm permit --all
```

- 授予禁止所有用户登录Linux客户端的权限。

```
sudo realm deny --all
```

5. 为AD域用户添加sudo权限。

   执行以下命令打开sudo配置文件，并根据业务场景配置sudo权限。

```
sudo vim /etc/sudoers.d/domain_admins
```

   - 为指定用户添加sudo权限。

```
usera1@example-company.com     ALL=(ALL)    ALL
userb2@example-company.com     ALL=(ALL)    ALL
```

   - 为指定用户组添加sudo权限。

```
%admingroupc1@example-company.com     ALL=(ALL)    ALL
```

   - 为指定多word组成组名的用户组添加sudo权限。

```
%domain\ admins@example-company.com       ALL=(ALL)       ALL
```

6. 配置SSH登录项。

   打开SSH配置文件*/etc/ssh/sshd_config*，修改如下登录配置项：

```
PasswordAuthentication yes
```

   执行以下命令重启SSHD服务。

   - CentOS

```
service sshd restart
```

   - Ubuntu

```
service ssh restart
```

7. 以AD域身份登录Linux客户端。

```
ssh localhost -l usera1@example-company.com
```

   如果回显包含如下类似信息，说明已使用AD域身份登录Linux客户端。

```
[user1@mycentos root]$ ssh localhost -l usera1@example-company.com
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:t/sEr63muG4UvBiAODXW9cHuMDBUlWUXO3cQ4xxmN78.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
usera1@example-company.com@localhost's password:

Welcome to Alibaba Cloud Elastic Compute Service !

Activate the web console with: systemctl enable --now cockpit.socket
```

8. 挂载SMB文件系统。
   i. 安装挂载工具包。
      - Ubuntu

        ```
        sudo apt-get install keyutils cifs-utils
        ```

      - CentOS

        ```
        sudo yum install keyutils cifs-utils
        ```

   ii. 查询keytab信息。

   执行**id**命令查看登录后的uid、gid信息。

   ```
   [usera1@example-company.com@mycentos ~]$ klist
   Ticket cache: KCM:371801107:64031
   Default principal: usera1@EXAMPLE-COMPANY.COM

   Valid starting       Expires              Service principal
   08/31/2021 07:56:42  08/31/2021 17:56:42  krbtgt/EXAMPLE-COMPANY.COM@EXAMPLE-COMPANY.COM
           renew until 09/07/2021 07:56:42
   [usera1@example-company.com@mycentos ~]$ id
   uid=371801107(usera1@example-company.com) gid=371800513(domain users@example-company.com) groups=371800513(domain users@example-company.com),371801110(groupa@example-company.com)
   ```

   iii. 执行以下命令挂载文件系统。

   ```
   sudo mount -t cifs //205dee494a3-uub48.us-west-1.nas.aliyuncs.com/myshare /mnt -o v
   ers=2.1,sec=krb5,cruid=371801107,uid=371801107,gid=371800513  --verbose
   ```

   > **说明** 如果控制台SMB ACL选项中选择了**启用传输加密**，则需要使用*vers=3.0*挂载。

9. 添加自动挂载配置。

   挂载完成后，添加自动挂载配置。重启Linux客户端，将自动完成挂载。

   i. 在配置文件*/etc/auto.master*中，添加如下选项：

   ```
   /share    /etc/auto.cifs    --timeout=30 --ghost
   ```

   ii. 按如下示例修改配置文件*/etc/auto.cifs*内容：

   ```
   * -fstype=cifs,vers=2.1,sec=krb5,cruid=${UID},uid=${UID},gid=${GID},file_mode=0700,
   dir_mode=0700 ://205dee494a3-uub48.us-west-1.nas.aliyuncs.com/myshare/&
   ```

   iii. 重启autofs服务。

   ```
   systemctl restart autofs.service
   ```

iv. 确认自动挂载配置结果。

假设创建了*//205dee494a3-uub48.us-west-1.nas.aliyuncs.com/myshare/usera1*目录，权限设置为用户usera1拥有所有权限。

在AD域用户登录后，执行`ls /share/usera1`命令，就能够查看到SMB文件系统目录usera1下的内容即配置成功。

方式二：Linux客户端连接AD服务器并挂载SMB文件系统

1. 登录Linux客户端。
2. 连接AD服务器。
   - Ubuntu操作系统
     a. 安装AD服务器配置包。

```
sudo apt-get -y install keyutils cifs-utils krb5-user
```

     b. 配置DNS。

     执行以下命令停止DNS的自动更新。

```
sudo systemctl disable systemd-resolved
sudo systemctl stop systemd-resolved
```

     然后将AD服务器IP写入*/etc/resolv.conf*中。

```
# Generated by NetworkManager
search example-company.com
nameserver 172.19.0.61
```

     执行ping命令，ping AD服务器名称验证连通性。

```
user1@myubuntu:/home$ ping example-company.com
PING example-company.com (172.19.0.61) 56(84) bytes of data.
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=1 ttl=128 time=0.274 ms
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=2 ttl=128 time=0.289 ms
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=3 ttl=128 time=0.270 ms
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=4 ttl=128 time=0.273 ms
^C
--- example-company.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3073ms
rtt min/avg/max/mdev = 0.270/0.276/0.289/0.007 ms
```

   - CentOS操作系统
     a. 安装AD服务器配置包。

```
sudo yum install keyutils cifs-utils krb5-workstation
```

b. 配置DNS。

将AD服务器IP写入*/etc/resolv.conf*中，删除默认的DNS服务器。

```
# Generated by NetworkManager
search example-company.com
nameserver 172.19.0.61
```

执行ping命令，pingAD服务器名称验证连通性。

```
[user1@mycentos root]$ ping example-company.com
PING example-company.com (172.19.0.61) 56(84) bytes of data.
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=1 ttl=128 time=0.221 ms
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=2 ttl=128 time=0.334 ms
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=3 ttl=128 time=0.314 ms
64 bytes from 172.19.0.61 (172.19.0.61): icmp_seq=4 ttl=128 time=0.323 ms
^C
--- example-company.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3044ms
rtt min/avg/max/mdev = 0.221/0.298/0.334/0.045 ms
```

c. 配置Kerberos。

请在配置文件*/etc/krb5.conf*中添加如下内容。

```
    default_tgs_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-m
d5
    default_tkt_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-m
d5
    permitted_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
```

```
# To opt out of the system crypto-policies configuration of krb5, remove the
# symlink at /etc/krb5.conf.d/crypto-policies which will not be recreated.
includedir /etc/krb5.conf.d/

[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
#    default_realm = EXAMPLE.COM
    default_ccache_name = KEYRING:persistent:%{uid}
    default_tgs_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
    default_tkt_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
    permitted_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5

[realms]
# EXAMPLE.COM = {
#     kdc = kerberos.example.com
#     admin_server = kerberos.example.com
# }

[domain_realm]
# .example.com = EXAMPLE.COM
# example.com = EXAMPLE.COM
```

3. 以本地用户身份保存SMB文件系统挂载点的票据信息。
   i. 新建本地用户并记录新建用户的UID和GID。

```
useradd usera1
su - usera1
id usera1
```

```
[root@iZrj9gqbtl7kefeq  ~]# useradd usera1
[root@iZrj9gqbtl7kefeq  ~]# su - usera1
[usera1@iZrj9gqbtl7kefe  ~]$ id
uid=1004(usera1) gid=1004(usera1) groups=1004(usera1)
```

ii. 使用新建的本地用户保存SMB文件系统挂载点的票据信息。

```
kinit administrator@EXAMPLE-COMPANY.COM
klist
```

```
user1@iZrj9gqbtl7kefeqa3o6z9Z:~$ kinit administrator@EXAMPLE-COMPANY.COM
Password for administrator@EXAMPLE-COMPANY.COM:
user1@iZrj9gqbtl7kefeqa3o6z9Z:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: administrator@EXAMPLE-COMPANY.COM

Valid starting       Expires              Service principal
09/08/2021 05:47:53  09/08/2021 15:47:53  krbtgt/EXAMPLE-COMPANY.COM@EXAMPLE-COMPANY.COM
        renew until 09/09/2021 05:47:49
user1@iZrj9gqbtl7kefeqa3o6z9Z:~$
```

4. 挂载SMB文件系统。

i. 安装挂载工具包。

- Ubuntu

```
sudo apt-get install keyutils cifs-utils
```

- CentOS

```
sudo yum install keyutils cifs-utils
```

ii. 执行以下命令挂载文件系统。

```
sudo mount -t cifs //205dee494a3-uub48.us-west-1.nas.aliyuncs.com/myshare /mnt -o v
ers=2.1,sec=krb5,cruid=1004,uid=1004,gid=1004  --verbose
```

其中，`cruid`和`uid`为本地usera1用户的ID，`gid`为本地usera1用户的group。

> **说明** 如果控制台SMB ACL选项中选择了**启用传输加密**，则需要使用*vers=3.0*挂载。

5. 添加自动挂载配置。

挂载完成后，添加自动挂载配置。重启Linux客户端，将自动完成挂载。

i. 在配置文件*/etc/auto.master*中，添加如下选项：

```
/share    /etc/auto.cifs    --timeout=30 --ghost
```

ii. 按如下示例修改配置文件*/etc/auto.cifs*内容：

```
* -fstype=cifs,vers=2.1,sec=krb5,cruid=${UID},uid=${UID},gid=${GID},file_mode=0700,
dir_mode=0700 ://205dee494a3-uub48.us-west-1.nas.aliyuncs.com/myshare/&
```

iii. 重启autofs服务。

```
systemctl restart autofs.service
```

iv. 确认自动挂载配置结果。

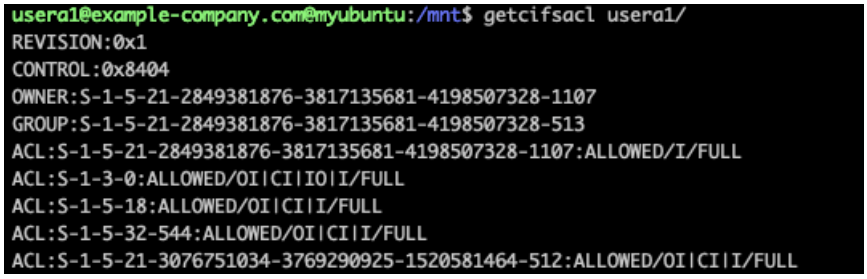
假设创建了*//205dee494a3-uub48.us-west-1.nas.aliyuncs.com/myshare/usera1*目录，权限设置为用户usera1拥有所有权限。

在AD域用户登录后，执行`ls /share/usera1`命令，就能够查看到SMB文件系统目录usera1下的内容即配置成功。

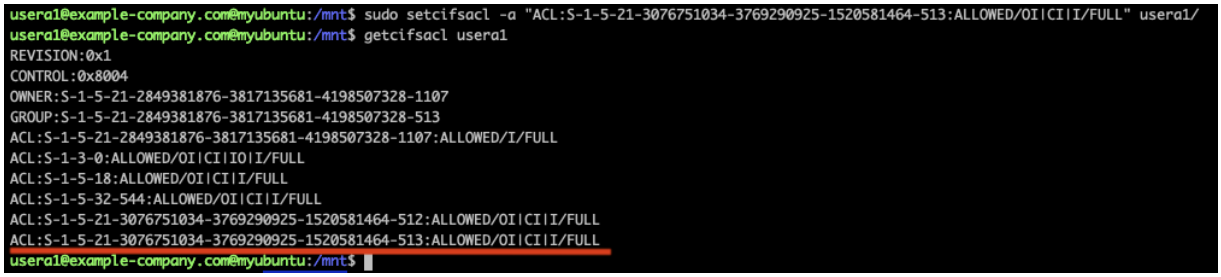
使用cifsacl工具管理SMB文件系统ACL

您可以使用getcifsacl和setcifsacl命令管理SMB文件系统ACL。示例如下：

```
getcifsacl /mnt/usera1/
```




```
setcifsacl -a "ACL:S-1-5-21-3076751034-3769290925-1520581464-513:ALLOWED/OI|CI/FULL" /mnt/usera1
```



4.1.4. NAS NFS ACL

4.1.4.1. 简介

阿里云NAS支持NFS v4 ACL和POSIX ACL。本文简要介绍POSIX ACL和NFS v4 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。

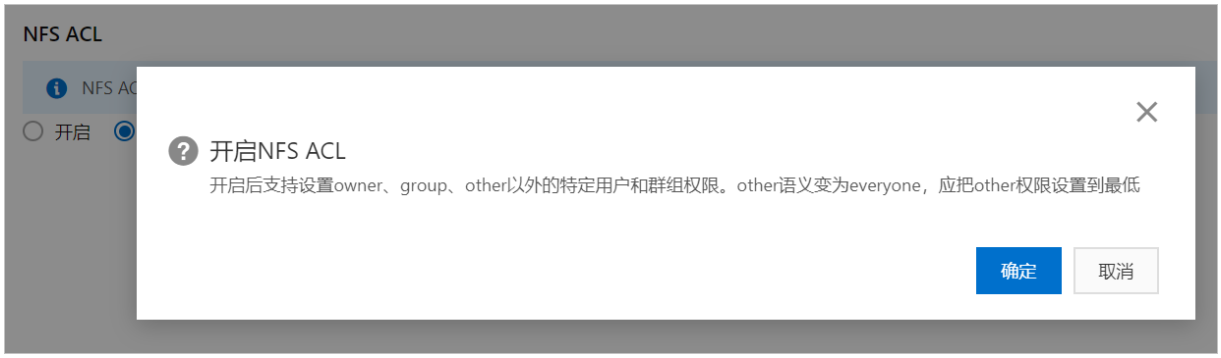
POSIX ACL是NFS v3协议能够扩展支持的权限控制协议。POSIX ACL对mode权限控制进行了扩展，能够对owner、group、other以外的特定用户和群组设置权限，也支持权限继承。详细介绍请参见acl - Linux man page。

NFS v4 ACL是NFS v4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。详细介绍请参见nfs4_acl - Linux man page。

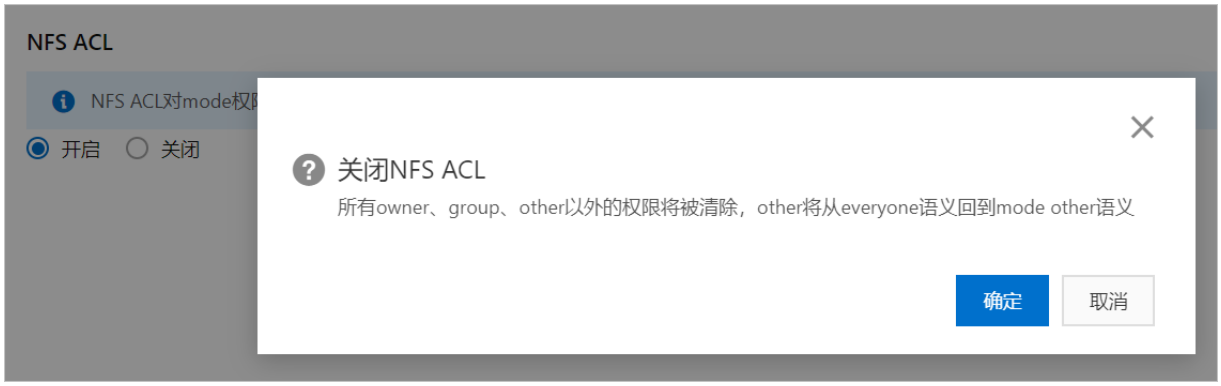
您可以使用NFS v3协议挂载含有NFS v4 ACL的文件系统，挂载后NFS v4 ACL会被转化为POSIX ACL。您也可以用NFS v4协议挂载含有POSIX ACL的文件系统，挂载后POSIX ACL会被转化为NFS v4 ACL。但由于NFS v4 ACL和POSIX ACL并不完全兼容，加上mode和ACL之间的互操作也无法尽善尽美，另外NAS NFS v3挂载不支持锁，所以建议您在使用NFS v4 ACL功能时尽量只使用NFS v4协议挂载并设置NFS v4 ACL，不使用mode和POSIX ACL。相关特性说明请参见特性。

通过控制台配置NFS ACL功能

登录阿里云NAS控制台，选择**文件系统 > 文件系统列表**，找到目标文件系统，单击文件系统ID或者**管理**。选择**访问控制**页签，单击**开启**，打开NFS ACL功能。



单击**关闭**（默认状态），停止NFS ACL功能。



POSIX ACL注意事项

- ACL的设置
  - 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/目录都需要设置ACL。
  - 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或GID，因为NAS后端存储的是UID或GID。
- ACL的使用
  - 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。
- other的权限设置

- 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，所以在执行相应的代码前先执行 `umask 777` ，这样创建文件和目录时传入的mode会变成000，使默认的权限最小化，详情请参见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。

NFS v4 ACL注意事项

- ACL的设置
  - 使用UID或GID（例如：UID 1001）设置ACL。
  - 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。
  - 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。
- ACL的使用
  - 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。
- ACL权限设置
  - 强烈建议使用NFS v4 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。
  - 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）。
  - 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。
  - NAS NFS v4 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。

4.1.4.2. 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。不支持Deny ACE的详细介绍，请参见常见问题。

  Audit ACE和Alarm ACE在阿里云NAS NFS上不生效。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mode对应的默认ACL。

```
touch file
```

```
[root@vbox test]# ls -l file
-rw-r--r--. 1 root root 0 May  6 14:27 file
```

```
[root@vbox test]# nfs4_getfacl file
# 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：

  - 排序时owner、group、everyone对应的ACE总是排在最前面。

    ```
    [root@vbox test]# nfs4_getfacl file
    # file: file
    A::OWNER@:rwaxtTnNcCy
    A::GROUP@:rtncy
    A::EVERYONE@:rtncy
    A::1001:rwaxtTNcCy
    ```

  - 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。

    ```
    [root@vbox test]# nfs4_setfacl -a A::1009:X file
    [root@vbox test]# nfs4_getfacl file
    # file: file
    A::OWNER@:rwaxtTcCy
    A::GROUP@:rwatcy
    A::EVERYONE@:tcy
    A::1001:rwaxtTNcCy
    A::1009:xtcy
    ```

  - 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。

    ```
    [root@vbox test]# nfs4_setfacl -a A::1009:W file
    [root@vbox test]# nfs4_getfacl file
    # file: file
    A::OWNER@:rwaxtTcCy
    A::GROUP@:rwatcy
    A::EVERYONE@:tcy
    A::1001:rwaxtTNcCy
    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。

```
[root@vbox test]# nfs4_setfacl -a A:fd:1009:R file
[root@vbox test]# nfs4_getfacl file
# file: file
A::OWNER@:rwaxtTcCy
A::GROUP@:rwatcy
A::EVERYONE@:tcy
A::1001:rwaxtTNcCy
A::1009:rwaxtTNcCy
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。

```
[root@vbox nfs]# nfs4_getfacl dir
# 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。

```
[root@vbox nfs]# nfs4_setfacl -a A:fd:1000:rwx dir
[root@vbox nfs]# nfs4_getfacl dir
# 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。

```
[root@vbox nfs]# touch dir/file
[root@vbox nfs]# nfs4_getfacl dir/file
# file: dir/file
A::OWNER@:rwatTcCy
A::GROUP@:rwatcy
A::EVERYONE@:rwatcy
A::1000:rwx
```

```
[root@vbox nfs]# mkdir dir/subdir
[root@vbox nfs]# nfs4_getfacl dir/subdir
# file: dir/subdir
A::OWNER@:rwaDxtTcCy
A::GROUP@:rwaDxtcy
A::EVERYONE@:rwaDxtcy
A:fdi:1000:rwx
```

> **说明**
>
> - 建议EVERYONE权限尽量小。在执行相应的代码前请先执行 `umask 777` ，这样创建文件和目录时传入的mode会变成000，可以让默认的权限最小化，详情请参见umask与默认mode。
> - Linux文件和目录的系统调用，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，实际情况下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和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和GID的ACE，在NFSv4 ACL客户端显示时会自动加载本地的*/etc/passwd*将UID和GID转化成用户名和群组名。您需要管理多个机器间的用户名与UID和GID之间的映射，确保同一个用户名或同一群组名映射到相同的UID和GID，以免发生错误。

- 支持通过Extended Attributes输出NFSv4 ACL。

```
[root@vbox nfs]# getfattr -n system.nfs4_acl file
# file: file
system.nfs4_acl=0sAAAABgAAAAAAAAAAABYBhwAAAAZPV05FUkAAAAAAAAAAAAAAAABIAhwAAAAZHUk9VUEAAAAAA
AAAAAAAAAABIAhwAAAAlFVkVSWU9ORUAAAAAAAAAAAAAAAAAAAAAEAAAAEMTAwMAAAAAAAAALAAAAAwAAAQxMDAw
AAAAAAAAAEAAFgGQAAAABTEwMDAxAAAA
```

- 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。

```
[root@vbox nfs]# nfs4_getfacl file1
# file: file1
A::OWNER@:rwatTcCy
A::GROUP@:rwatcy
A::EVERYONE@:rwatcy
A::1000:rtncy
[root@vbox nfs]# cp --preserve=xattr file1 file2
```

```
[root@vbox nfs]# nfs4_getfacl file2
# file: file2
A::OWNER@:rwatTcCy
A::GROUP@:rwatcy
A::EVERYONE@:rwatcy
A::1000:rtncy
[root@vbox nfs]# cp -ar dir1 dir2
```

- 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。

```
[root@vbox nfs]# ls -l file
-rw-rw-rw-. 1 root root 0 May  3  2019 file
[root@vbox nfs]# nfs4_getfacl file
# 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。

```
[root@vbox nfs]# chmod u+x file
[root@vbox nfs]# ls -l file
-rwxrw-rw-. 1 root root 0 May  3  2019 file
[root@vbox nfs]# nfs4_getfacl file
# 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。

```
[root@vbox nfs]# nfs4_setfacl -a A::GROUP@:x file
[root@vbox nfs]# ls -l file
-rwxrwxrw-. 1 root root 0 May  3  2019 file
```

> 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。

- mode与NFSv4 ACL权限的对应关系。
  - 执行**chmod**命令改变mode时，NFSv4 ACL就会发下表中的对应改变。
  - 执行**nfs4_setfacl**命令改变NFSv4 ACL时，如果修改的是文件权限，且NFSv4 ACL属性wa不全都存在，则mode不会显示w属性。
  - 执行**nfs4_setfacl**命令改变NFSv4 ACL时，如果修改的是目录权限，NFSv4 ACL属性waD不全都存在，则mode不会显示w属性。
  - 如果目录NFSv4 ACL有Dx权限，此时mode显示没有w属性，但是目录可以进行子文件子目录创建和删除动作，相当于有mode的wx属性。
  - nfs4_setfacl时最好使用大写RWX设置权限。大写RWX会自动对应到mode的rwx，避免NFSv4 ACL和mode的兼容问题。

mode other	NFSv4 ACL EVERYONE on file	NFSv4 ACL EVERYONE on dir
---	A::EVERYONE@:tncy	A::EVERYONE@:tncy

mode other	NFSv4 ACL EVERYONE on file	NFSv4 ACL EVERYONE on dir
--x	A::EVERYONE@:xtncy	A::EVERYONE@:xtncy
-w-	A::EVERYONE@:watncy	A::EVERYONE@:waDtncy
-wx	A::EVERYONE@:waxtncy	A::EVERYONE@:waDxtncy
r--	A::EVERYONE@:rtncy	A::EVERYONE@:rtncy
r-x	A::EVERYONE@:rxtncy	A::EVERYONE@:rxtncy
rw-	A::EVERYONE@:rwatncy	A::EVERYONE@:rwaDtncy
rwx	A::EVERYONE@:rwaxtncy	A::EVERYONE@:rwaDxtncy

mode group	NFSv4 ACL GROUP on file	NFSv4 ACL GROUP on dir
---	A::GROUP@:tncy	A::GROUP@:tncy
--x	A::GROUP@:xtncy	A::GROUP@:xtncy
-w-	A::GROUP@:watncy	A::GROUP@:waDtncy
-wx	A::GROUP@:waxtncy	A::GROUP@:waDxtncy
r--	A::GROUP@:rtncy	A::GROUP@:rtncy
r-x	A::GROUP@:rxtncy	A::GROUP@:rxtncy
rw-	A::GROUP@:rwatncy	A::GROUP@:rwaDtncy
rwx	A::GROUP@:rwaxtncy	A::GROUP@:rwaDxtncy

mode owner	NFSv4 ACL OWNER on file	NFSv4 ACL OWNER on dir
---	A::OWNER@:tTnNcCy	A::OWNER@:tTnNcCy
--x	A::OWNER@:xtTnNcCy	A::OWNER@:xtTnNcCy
-w-	A::OWNER@:watTnNcCy	A::OWNER@:waDtTnNcCy
-wx	A::OWNER@:waxtTnNcCy	A::OWNER@:waDxtTnNcCy
r--	A::OWNER@:rtTnNcCy	A::OWNER@:rtTnNcCy
r-x	A::OWNER@:rxtTnNcCy	A::OWNER@:rxtTnNcCy
rw-	A::OWNER@:rwatTnNcCy	A::OWNER@:rwaDtTnNcCy
rwx	A::OWNER@:rwaxtTnNcCy	A::OWNER@:rwaDxtTnNcCy

NFSv4 ACL支持比mode更丰富的权限定义，每个权限位有不同的功能。实际上某些权限功能需要多个权限位同时存在才能起效，某些权限位代表的功能需要其他权限位来表达。对于文件和目录，同样的权限位也可能有不同的功能。文件和目录的NFSv4 ACL权限表如下：

文件的NFSv4 ACL权限表

权限位	功能介绍	注意事项
r	读文件	无
w	写文件/创建文件	需要wa同时存在才起效，单独w无效。
a	追加写文件	需要wa同时存在才起效，单独a无效。
x	执行文件	需要rx同时存在才起效，单独x无效。
d	删除文件	d权限无效。用户如果有父目录的wx权限，就可以删除当前文件，不受文件上的d权限影响。
D	-	文件不能设置D权限，nfs4_setfacl D会被客户端过滤掉。
t	读文件属性信息	默认最小权限tncy之一，不允许去除。
T	修改文件属性信息	无
n	读文件的named attributes属性信息	默认最小权限tncy之一，不允许去除。
N	修改文件的named attributes属性信息	NAS NFS不支持设置named attributes。N权限无效。
c	读文件的ACL	默认最小权限tncy之一，不允许去除。
C	修改文件的ACL	无
o	修改文件的拥有者(owner)信息	有o权限的当前用户可以把文件拥有者(owner)改为自己，但是不允许改成其他用户，除非当前用户是root。
y	允许同步访问	默认最小权限tncy之一，不允许去除。

目录的NFSv4 ACL权限表

权限位	功能介绍	注意事项
r	查询目录	无
w	创建文件、目录	w权限无效。w权限功能包含在D权限中，需要Dx同时存在才起效。
a	创建子目录	a权限无效。a权限功能包含在D权限中，需要Dx同时存在才起效。
x	进入目录	无

权限位	功能介绍	注意事项
d	删除目录	d权限无效。用户如果有父目录的wx权限，就可以删除当前目录，不受目录上的d权限影响。
D	目录删除子文件、子目录	需要Dx同时存在才起效，单独D无效。
t	读目录属性信息	默认最小权限tncy之一，不允许去除。
T	修改目录属性信息	无
n	读目录的named attributes属性信息	默认最小权限tncy之一，不允许去除。
N	修改目录的named attributes属性信息	NAS NFS不支持设置named attributes。N权限无效。
c	读目录的ACL	默认最小权限tncy之一，不允许去除。
C	修改目录的ACL	无
o	修改文件的拥有者(owner)信息	有o权限的当前用户可以把文件拥有者(owner)改为自己，但是不允许改成其他用户，除非当前用户是root。
y	允许同步访问	默认最小权限tncy之一，不允许去除。

注意

- 默认OWNER最小权限为：tTnNcCy，不允许少于这个权限。
- 默认GROUP和EVERYONE最小权限为：tncy，不允许少于这个权限。

- 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。

  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，权限如下。

```
[root@vbox test] sudo nfs4_getfacl dir0
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。

```
[root@vbox test] sudo getfacl dir0
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。

```
[root@vbox test] sudo nfs4_getfacl dir0/file
A::OWNER@:tTnNcCy
A::GROUP@:tncy
A::EVERYONE@:tncy
A:g:19064:rxtncy
A:g:19065:rwaxtTnNcCy
```

POSIX ACL的dir0/file权限如下。

```
[root@vbox test] sudo getfacl dir0/file
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。

  ```
  [root@vbox 3]# getfacl myfile
  # 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。

  ```
  [root@vbox 3]# getfacl myfile
  # 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` 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。

  ```
  [root@vbox 3]# getfacl myfile
  # 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。

```
[root@vbox 3]# getfacl myfile
# 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。

```
[root@vbox 3]# getfacl myfile
# 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值由所有用户和群组的权限或操作产生，并无实际意义，也不会被修改。

- 多个机器间的用户名与UID和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和GID的ACE，在POSIX ACL客户端显示时会自动加载本地的*/etc/passwd*将UID和GID转化成用户名和群组名。您需要管理多个机器间的用户名与UID和GID之间的映射，确保同一个用户名或同一群组名映射到相同的UID和GID，以免发生错误。

- 支持通过Extended Attributes输出POSIX ACL。

  ```
  [root@vbox nfs]# getfattr -n system.posix_acl_access file
  # 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。

```
[root@vbox nfs]# getfacl file1
user::---
user:player:r-x
group::---
mask::r-x
other::--x
[root@vbox nfs]# cp --preserve=xattr file1 file2
```

```
[root@vbox nfs]# getfacl file2
# file: file2
user::---
user:player:r-x
group::---
mask::r-x
other::--x
[root@vbox nfs]# cp -ar dir1 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。

4.1.4.3. 使用POSIX ACL进行权限管理

本文介绍在使用NFS v3协议挂载的文件系统上，如何设置POSIX ACL来进行文件和目录权限管理。

前提条件

已使用NFS v3协议挂载文件系统。具体操作，请参见Linux系统挂载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。
getfacl file1 | setfacl --set-file=- file2	将文件*file1*的ACL复制到文件*file2*上。
setfacl -b file1	删除文件*file1*上的所有非mode的ACE。
setfacl -k file1	删除文件*file1*上的所有default的ACE。
setfacl -R -m g:players:rw dir	对目录树*dir*下的文件和目录增加用户组players读写的权限。
setfacl -d -m g:players:rw dir1	用户组players对目录*dir1*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。

   本示例假设创建普通用户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. 对目录和文件设置POSIX ACL实现权限管理。

   本示例假设创建目录*dir0*，针对目录*dir0*中的所有文件，授予players只读权限，授予adminis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:rwx 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:rwx 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。

```
[root@vbox test] sudo su admini -c 'touch dir0/file'
[root@vbox test] sudo su admini -c 'echo 123 > dir0/file'
```

ii. 验证用户player具有只读权限。

```
[root@vbox test] sudo su player -c 'touch dir0/file'
touch: cannot touch ‘dir0/file’: Permission denied
[root@vbox test] sudo su player -c 'cat dir0/file'
123
[root@vbox test] sudo su player -c 'echo 456 >> dir0/file'
bash: dir0/file: Permission denied
[root@vbox test] sudo su player -c 'getfacl dir0/file'
# 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。

```
[root@vbox test] sudo su anonym -c 'ls dir0'
ls: cannot open directory dir0: Permission denied
[root@vbox test] sudo su anonym -c 'cat dir0/file'
cat: dir0/file: Permission denied
[root@vbox test] sudo su anonym -c 'getfacl dir0/file'
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NFS v4 ACL时，尽量把每个用户归类到群组中。在设置NFS v4 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：见以下命令将用户admini移出群组adminis，移入群组adminis2。

```
[root@vbox test] sudo groupadd adminis2
[root@vbox test] sudo usermod -g adminis2 admini
[root@vbox test] id admini
uid=1057(admini) gid=1057(admini) groups=1061(adminis2)
[root@vbox test] sudo su admini -c 'ls dir0'
ls: cannot open directory dir0: Permission denied
[root@vbox test] sudo su admini -c 'cat dir0/file'
cat: dir0/file: Permission denied
[root@vbox test] sudo su admini -c 'getfacl dir0/file'
getfacl: dir0/file: Permission denied
```

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

```
[root@vbox test] sudo su admini -c 'touch dir0/file'
[root@vbox test] sudo su admini -c 'echo 123 > dir0/file'
```

ii. 验证用户player具有只读权限。

```
[root@vbox test] sudo su player -c 'touch dir0/file'
touch: cannot touch ‘dir0/file’: Permission denied
[root@vbox test] sudo su player -c 'echo 456 >> dir0/file'
bash: dir0/file: Permission denied
[root@vbox test] sudo su player -c 'cat dir0/file'
123
[root@vbox test] sudo su player -c 'nfs4_getfacl dir0/file'
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。

```
[root@vbox test] sudo su anonym -c 'ls dir0'
ls: cannot open directory dir0: Permission denied
[root@vbox test] sudo su anonym -c 'cat dir0/file'
cat: dir0/file: Permission denied
[root@vbox test] sudo su anonym -c 'nfs4_getfacl dir0/file'
Invalid filename: di
```

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。

```
[root@vbox test] sudo groupadd adminis2
[root@vbox test] sudo usermod -g adminis2 admini
[root@vbox test] id admini
uid=1057(admini) gid=1057(admini) groups=1054(adminis2)
[root@vbox test] sudo su admini -c 'ls dir0'
ls: cannot open directory dir0: Permission denied
[root@vbox test] sudo su admini -c 'cat dir0/file'
cat: dir0/file: Permission denied
[root@vbox test] sudo su admini -c 'nfs4_getfacl dir0/file'
Invalid filename: dir0/file
```

4.2. 配置生命周期管理

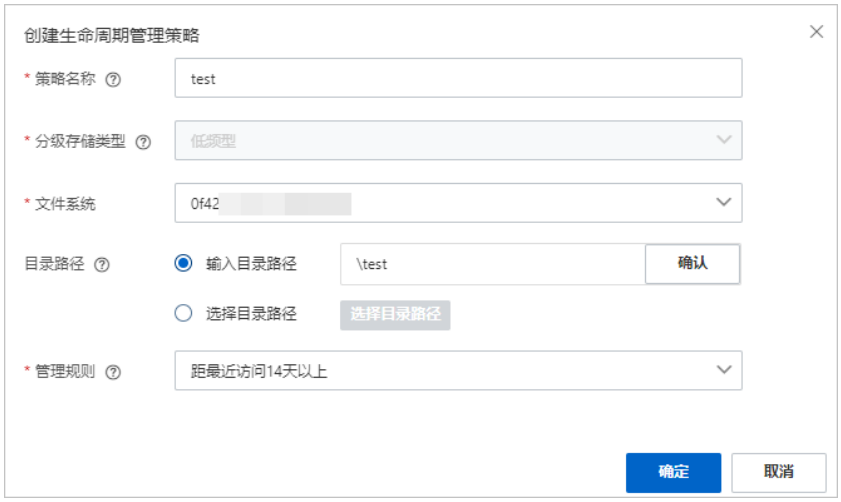
4.2.1. 设置生命周期策略

如果您存储在通用型NAS文件系统中的数据超过14天未访问，您可以使用生命周期管理功能将这部分冷数据转储至成本更低的低频介质中。本文介绍如何在NAS控制台上管理生命周期策略。

创建生命周期策略

1. 登录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**数据生命周期管理**列**配置策略**。
4. 在**生命周期管理**页面，单击**创建策略**。
5. 在**创建生命周期管理策略**对话框，配置如下参数。



参数	说明
策略名称	长度为3~64个字符，必须以大写字母或小写字母开头，可以包含英文字母、数字、下划线（_）或者短划线（-）。
文件系统	选择需要进行生命周期管理的文件系统。
目录路径	设置需要进行生命周期管理的目录路径，最多支持设置10条路径。 ○ **输入目录路径**：路径必须以正斜线（/）开头，字符仅支持大小写英文字母、中文、数字、空格和以下符号 `./+-=*@%()、` 。 ○ **选择目录路径**：单击**选择目录路径**，在弹出的对话框中，选择文件或目录路径后，单击**确定**。 **说明** 生命周期策略对冷数据文件进行转储，不改变文件系统的目录结构。例如，*/test*目录下仅有1个文件a1，当文件a1符合管理规则转储后，*/test*目录依然可以写入数据且受管理规则约束。
管理规则	系统为您预置了生命周期管理规则，当指定目录符合预置天数未被访问，文件将会转储至低频介质。包括以下选项： ○ **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**

6. 单击**确定**。

> **说明** 转储时间会和文件系统的大小和转储数据量有关，功能开启后，符合生命周期管理策略的文件，第一次转储最快2个小时完成，一般在24小时内完成。后续周期性转储会在一周内某个时间完成。您可在文件系统详情页查询低频介质用量。也可以通过NAS控制台查看已转储至低频介质的文件。更多信息，请参见查看低频介质存储文件。

查看生命周期策略

1. 登录NAS控制台。
2. 在左侧导航栏，选择**生命周期管理 > 生命周期策略列表**。
3. 在**生命周期策略列表**页面，查看该地域下所有的生命周期策略。

查看文件系统低频介质用量

1. 登录NAS控制台。
2. 在左侧导航栏，选择**文件系统 > 文件系统列表**。
3. 在**文件系统列表**页面，单击目标文件系统名称或**管理**，在文件系统**基础信息**查看低频介质用量。

> **说明** 转储时间会和文件系统的大小和转储数据量有关，功能开启后，符合生命周期管理策略的文件，第一次转储最快2个小时完成，一般在24小时内完成。后续周期性转储会在一周内某个时间完成。您可在文件系统详情页查询低频介质用量。也可以通过NAS控制台查看已转储至低频介质的文件。更多信息，请参见查看低频介质存储文件。

相关操作

操作	说明
修改生命周期策略	在**生命周期策略列表**页面，找到目标生命周期策略，单击**修改**。 只能修改策略的**管理规则**，不能修改其他策略参数。
删除生命周期策略	在**生命周期策略列表**页面，找到目标生命周期策略，单击**删除**，根据提示信息删除策略。 已经转储到低频介质的数据会继续保持在低频介质存储状态。

FAQ

- 如何设置生命周期管理策略？
- 如果一个目录配置了多项生命周期管理策略，文件系统会执行哪一项策略？
- 删除生命周期管理策略会有什么影响？
- 更多生命周期管理FAQ

4.2.2. 管理低频介质中的文件

启用生命周期管理功能后，符合管理规则的文件会自动转储至低频介质。如果您需要频繁访问低频介质中存储的文件，建议您取回目标数据，避免频繁访问产生读写流量费用。本文介绍如何查看低频介质存储文件及管理数据取回任务。

查看低频介质存储文件

您可以通过NAS控制台查看已转储至低频介质中的文件及其最近一次被访问时间等信息。

1. 登录NAS控制台。
2. 在左侧导航栏，选择**生命周期管理 > 低频存储文件管理**。
3. 在**低频存储文件管理**页面左侧，选中或搜索目标文件系统。
4. 在**低频存储文件管理**页面右侧，查看目标文件系统已转储至低频介质中的文件及该文件最近一次被访问的时间等信息。

创建数据取回任务

您可以创建数据取回任务，将低频介质中的文件取回至通用型NAS存储空间。取回的数据将按照通用型NAS存储容量计费。更多信息，请参见通用型NAS计费说明。

1. 登录NAS控制台。
2. 在左侧导航栏，选择**生命周期管理 > 数据取回任务列表**。
3. 在**数据取回任务列表**页面，单击**创建数据取回任务**。
4. 在**创建数据取回任务**对话框，配置目标文件所在文件系统及目标文件所在路径。
5. 单击**确定**。

相关操作

任务	说明	操作步骤
查看数据取回任务	创建数据取回任务后，您可以在控制台查看任务进度及任务状态。任务状态包括： • 运行中：数据取回任务执行中。 • 已完成：数据取回任务已完成。 • 已取消：已取消数据取回任务。 • 任务失败：数据取回任务执行失败，请您重试。	在**数据取回任务列表**页面，查看已创建的数据取回任务的进度及状态。
取消数据取回任务	仅支持任务状态为**运行中**的数据取回任务执行取消操作。 执行取消操作后会立刻停止数据取回任务，已经取回的数据将按照通用型NAS存储容量计费。更多信息，请参见通用型NAS计费说明。	在**数据取回任务列表**页面，找到运行中的目标任务，单击**取消**。
重试数据取回任务	仅支持任务状态为**任务失败**的任务执行重试操作。	在**数据取回任务列表**页面，找到执行失败的任务，单击**重试**。

4.2.3. 生命周期管理FAQ

什么时候应该开启生命周期管理功能？

当文件系统中包含每月访问频率低于2次的文件时，可以开启通用型NAS生命周期管理功能，符合生命周期管理策略的文件将自动转储至低频介质，采用低频介质计费方式，从而降低存储成本。

为什么我的文件系统不支持生命周期管理功能？

目前仅支持2020年06月01日后创建的通用型NAS文件系统开启生命周期管理功能并配置生命周期管理策略。已开启数据加密的文件系统暂不支持生命周期管理功能。2020年6月以前创建的文件系统如果需要使用生命周期管理功能，请提交工单咨询。

如何设置生命周期管理策略？

您可以通过NAS控制台或OpenAPI设置生命周期管理策略。具体操作，请参见设置生命周期策略和生命周期管理API。

如何选择生命周期管理策略，应该配置在哪个目录上？

为了方便您选择生命周期管理策略和需配置的目录，阿里云文件存储NAS提供了NAS分层策略分析工具。您可以使用该工具设置的生命周期管理策略，对指定目录及该目录下的子目录进行扫描并按照冷数据量降序排序，将指定目录中冷数据量最高的几个子目录打印出来。根据冷数据量来设置生命周期管理策略和需配置目录。更多信息，请参见使用指南。

所有文件都可以转储到低频介质中吗？

一个文件被转储到低频介质中需要满足以下三个条件：

- 文件所在目录配置了生命周期管理策略。
- 文件需大于或等于64 KB。
- 文件的最近访问时间需符合生命周期管理策略。

  创建生命周期管理策略时，可以配置管理规则，将距最近一次访问14天、30天、60天、90天以上的文件转换为低频存储文件。生命周期管理会依照文件的访问时间（即atime）来进行判断。

  - 以下操作会更新访问时间：
    - 读取文件
    - 写入文件
  - 以下操作不会更新访问时间：
    - 重命名一个文件
    - 修改文件的用户（user）、用户组（group）、模式（mode）等文件属性

如果一个目录配置了多项生命周期管理策略，文件系统会执行哪一项策略？

如果一个目录配置了多项生命周期管理策略，该目录下的文件只要满足任何一项生命周期管理策略的管理规则，就会被转储到低频介质中。

如果一个目录及其上层目录配置了不同的生命周期管理策略，文件系统会执行哪一项策略？

文件数据满足其任一策略规则目录下文件即会转储至低频介质中。

例如：当前目录配置了14天未访问转储的生命周期管理策略，其父目录或更上层目录配置了60天未访问转储的生命周期管理策略。那么目录中的14天未访问的文件会被转储至低频介质中，而父目录或更上层目录策略在扫描当前目录时，会跳过已转储至低频介质的文件。

生命周期管理策略是对目标路径所有数据生效吗？

是的。目标目录的所有文件数据只要满足生命周期管理策略，即会自动转储至低频介质中。

设置生命周期管理策略后，文件多久会被转储到低频介质？

转储时间会和文件系统的大小和转储数据量有关，功能开启后，符合生命周期管理策略的文件，第一次转储最快2个小时完成，一般在24小时内完成。后续周期性转储会在一周内某个时间完成。

目录重命名会影响生命周期管理策略执行吗？

生命周期管理策略中关联的目录被重命名后，目录下的文件将不再受原生命周期管理策略约束。已经转储至低频介质中的文件仍将维持存储状态。

当目录重命名后重新配置生命周期管理策略，则该目录下的文件会受该生命周期管理策略约束，符合生命周期管理规则的文件会被转储至低频介质中。

删除生命周期管理策略会有什么影响？

被删除的生命周期管理策略所关联目录下的文件将不会被转储至低频介质中。关联目录下已经转储至低频介质中的文件仍将维持当前存储状态。

已设置生命周期管理策略的目录删除策略后，重新设置新的生命周期管理策略，会重复转储文件吗？

不会。重新配置生命周期管理策略后，该策略通过检查机制跳过目录下已经被转储到低频介质中的文件，确保不会重复转储。

文件存储在低频介质中可以正常读写吗？

一个文件系统内的低频介质中的文件和其他普通文件一样可以被正常读写访问。

我的文件系统中有哪些文件存储在低频介质？

您可以通过NAS控制台或OpenAPI查询存储在低频介质中的文件。具体操作，请参见查看低频介质存储文件和ListDirectoriesAndFiles。

低频介质中文件的读写延时比性能型NAS和容量型NAS高吗？

第一次读低频介质中存储文件内容时可能延时会相对较高，但同一个文件内容在后续的一定时间内的读延时会与性能型NAS或容量型NAS普通文件的读延时基本一致。

写低频存储文件的延时与写性能型NAS或容量型NAS文件基本一致。

文件转储到低频介质中，怎么收费？

当文件转储到低频介质中，会采用低频介质的计费方式。更多信息，请参见低频介质计费说明。

转储至低频介质的冷数据被访问后，会自动转为热数据吗？

不会。数据一旦转储至低频介质，将持续存储在低频介质中。访问低频介质中的冷数据将产生低频介质读写流量费用。更多信息，请参见低频介质计费说明。

如果需要频繁访问低频介质中的文件，请您创建数据取回任务将冷数据转为热数据。具体操作，请参见创建数据取回任务。

如何创建低频介质存储文件的数据取回任务？

您可以通过NAS控制台或OpenAPI创建数据取回任务。具体操作，请参见创建数据取回任务和CreateLifecycleRetrieveJob。

执行数据取回任务是否影响文件的读写性能？

不影响，执行数据取回任务时可以正常读写数据。

执行数据取回任务收费吗？

收费。执行数据取回任务时，需要读取目标文件中的数据，将按照目标文件大小收取低频介质读流量费用。数据取回任务完成后，文件占用通用型NAS存储容量，将按照文件大小收取通用型NAS文件系统存储容量费用。更多信息，请参见低频介质计费说明。

备份低频介质中存储的文件时，怎么收费？

当您使用混合云备份（HBR）服务备份通用型NAS低频介质中的文件时，HBR会收取相应的服务费用。更多信息，请参见计费方式与计费项。

在备份低频介质中的文件时，备份服务需要读取目标文件中的数据，文件存储NAS将收取低频介质访问流量费用。更多信息，请参见低频介质计费说明。

4.3. 目录配额

阿里云NAS配额功能可以帮助您轻松管理NAS目录级配额，包括添加配额、编辑配额和删除配额等。

前提条件

- 已创建文件系统。更多信息，请参见创建文件系统。
- 已添加挂载点。更多信息，请参见添加挂载点。
- 已创建权限组和规则。更多信息，请参见创建权限组和规则。
- 已根据挂载场景，完成挂载文件系统。更多信息，请参见挂载场景。

配额类型

分类依据	配额类型
配额统计的范围	• 全量配额：统计目录下所有用户的文件系统使用量。 • 用户（组）配额：统计目录下某个用户（组）下的文件系统使用量。
配额的限制级别	• 统计型配额：只统计文件系统使用量，方便用户查看。 • 限制型配额：当您为指定目录配置限制型配额时，若文件系统使用量超出配额后，将导致创建文件或目录、追加写入等操作失败。

使用限制

- 文件系统实例

  仅NFS文件系统支持配额管理。

- 配额

  对于单个文件系统，最多可以对500个目录设置配额，支持配置的最大目录深度为8层。（例如，根目录/深度为0层，*/workspace*深度为1层，*/workspace/dir1*深度为2层，依此类推。）

> **注意**
>
> - 设置限制型配额后，如果文件使用量超过限制会导致写入操作（包括增加文件长度、创建文件、目录、移动文件到目录等操作）失败，应用层会收到IOError。
> - 由于限制型配额的高风险性，强烈建议您在业务关键路径上谨慎评估和测试验证后再配置限制型配额。
> - NAS配额的设置为异步执行，因此限制型配额的生效和失效都有延迟（正常情况下5分钟~15分钟）。

新建目录配额

1. 登录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，单击文件系统ID或者单击**管理**，进入**配额管理**页面，单击**新建目录配额**。
4. 在**新建目录配额**对话框，配置**目录路径**（例如：*/dir/subdir1*），完成目录的添加。

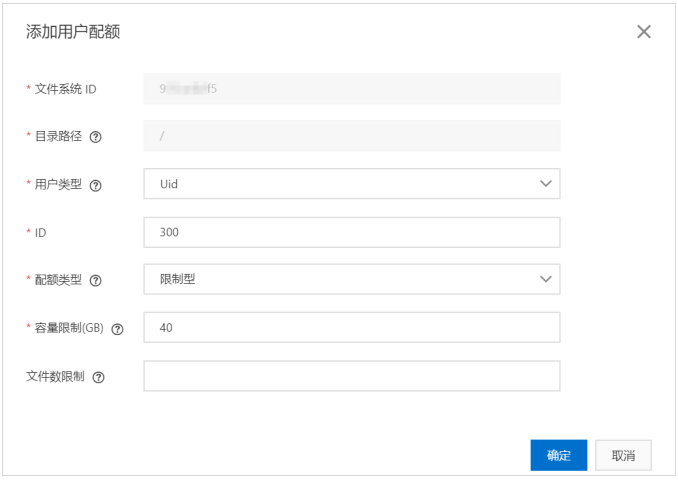
   > **说明**
   >
   > - 仅支持为NAS上已创建的目录设置配额。
   > - 由于配额是设置在文件系统的某个目录上的，配额的目录路径就是目录在文件系统的绝对路径。

5. 查询目录配额状态。

   新建目录配额后，会有初始化过程，状态为**初始化中**。初始化过程时长取决于文件系统的文件和目录数目。初始化完成之后，状态为**运行中**。同时，在用户配额列表中，会自动生成一条统计型配额。

添加用户配额

在**配额管理**区域，找到目标目录路径，单击**管理配额 > 添加用户配额**，配置相关信息。



参数	是否必选	说明
用户类型	是	指定用户ID的类型，包括Uid、Gid、所有用户三种。分别限制用户、用户组、全部用户。同一个路径下，可以为多个用户设置不同的配额。

参数	是否必选	说明
ID	否	如果用户类型为Uid或Gid时，该项代表用户的Uid或用户组的Gid。 • 当用户类型是Uid或Gid时，UserId为必填。 • 当用户类型是AllUsers时，UserId可不填。 例如： • 要限制Uid=500的用户，UserType是Uid，UserId是500。 • 要限制Gid=100的用户组，UserType是Gid，UserId是100。 • 要限制所有用户，UserType是AllUsers，UserId可不填。
配额类型	是	• **统计型**：仅统计指定目录路径的文件系统使用量。 • **限制型**：除了统计和展示外，超出配额后，I/O会被限制。
容量限制(GiB)	否	配额用户在配额路径下所拥有文件和目录的最大存储量。 **说明** 当配额类型为限制型时，可以配置，且容量限制和文件数限制至少填写其中一项。
文件数限制	否	配额用户在配额路径下所拥有文件和目录的最大数量。 **说明** 当配额类型为限制型时，可以配置，且容量限制和文件数限制至少填写其中一项。

删除单条用户配额

在用户配额列表中，找到目标配额条目，单击**删除**。

编辑单条用户配额

在用户配额列表中，找到目标配额条目，单击**编辑**。可编辑的选项有配额类型、容量限制、文件数限制。

说明 只有当配额类型为限制型时，可以编辑容量限制和文件数限制，且至少编辑其中一项。

API

管理配额功能提供了以下的API接口：

- SetDirQuota
- DescribeDirQuotas
- CancelDirQuota

4.4. 快照

极速型NAS支持快照功能。在重大操作之前，您可以创建快照提前备份数据。当数据丢失时，您可以通过快照找回某一时刻文件系统的部分或全部数据。本文介绍如何在阿里云NAS控制台上管理快照，包括创建快照、创建快照策略、应用快照策略等。

前提条件

文件系统必须处于**运行中**状态，否则无法创建快照。

使用说明

- 一个文件系统最多支持手动创建128个快照实例和自动创建128个快照实例。
- 如果文件系统存在创建中的快照，您无法为该文件系统再次创建快照。
- 如果创建快照时，文件系统正好达到过期释放时间，文件系统被释放的同时也会删除创建中的快照。
- 执行快照任务时可能会稍微降低文件系统的性能，I/O性能短暂变慢，请避免在业务高峰期进行的快照操作。
- 快照只备份某一时间点的数据，创建快照期间，操作文件系统产生的增量数据不会同步到快照中。

手动创建快照

在执行重大操作前，建议您手动创建快照，提升操作容错率。

- 手动创建的快照将永久保留，请定期删除已废弃的快照，避免快照容量持续扣费。
- 手动创建的快照将永久保留，直至账户欠费停止服务15天后，会被删除。

1. 登录NAS控制台。
2. 在左侧导航栏，选择**数据服务 > 快照**。
3. 在**快照**页面，单击**手动创建快照**。
4. 在**手动创建快照**对话框中，配置相关参数，重要参数说明如下。

参数	说明
文件系统	选中需要创建快照的极速型NAS文件系统。
保留时间	您可根据业务需求选择如下保留时间： ○ **自定义时长**：保留天数范围为1~65536天。 ○ **永久保留，直至快照数量达到额度上限后被自动删除**：已创建的快照将永久保留，当手动创建的快照数量超过128个后，文件系统会自动删除最早手动创建的快照实例。

5. 单击**确定**。

创建自动快照

将自动快照策略应用到极速型NAS文件系统上，在您设置的时间点自动为极速型NAS文件系统创建快照。通过自动备份极速型NAS文件系统中的数据，提高业务数据安全性。

- 一条自动快照策略可以应用到多个文件系统上。
- 每个文件系统的自动快照实例数量达到128个后，文件系统会自动删除最早创建的自动快照，手动快照不受影响。
- 修改自动快照策略的保留时间时，仅对新增快照生效，历史快照沿用原快照策略保留时间。
- 如果文件系统数据较多，单次创建自动快照的时长超过两个时间点间隔，则自动跳过下一时间点。

  例如：您设置了09:00、10:00、11:00和12:00为自动快照时间点。由于文件系统数据较多，09:00开始创建快照，10:20完成创建快照，实际耗时80分钟。系统会跳过10:00时间点，等到11:00继续为您创建自动快照。

- 创建的自动快照具有统一命名格式auto_yyyyMMdd_X。

  例如：auto_20140418_1表示2014年04月18日创建的第一份自动快照。其中，auto表示自动快照，与手动快照区分。yyyyMMdd表示创建快照的日期，yyyy表示年份、MM表示月份、dd表示日期。X表示当日创建的第几份自动快照。

1. 登录NAS控制台。
2. 在左侧导航栏，选择**数据服务 > 快照**。
3. 创建自动快照策略。
   i. 在**快照**页面，单击**自动快照策略**页签。
   ii. 在**自动快照策略**页签，单击**创建自动快照策略**。
   iii. 在**创建自动快照策略**对话框中，配置相关参数，重要参数说明如下。

参数	说明
创建时间	一天内创建自动快照的时间点，支持在00:00~23:00共24个整点中选择一个或多个时间点。 **说明** 创建快照会暂时降低文件系统I/O性能，出现短暂瞬间变慢。建议您选择避开业务高峰的时间点。
重复日期	创建自动快照的日期，支持在周一至周日之间选择一个或多个日期。
保留时间	自动快照的保留时间，默认保留30天，支持以下选项： ■ **自定义时长**：保留天数范围为1~65536天。 ■ **永久保留，直至快照数量达到额度上限后被自动删除**：已创建的自动快照将永久保留，在自动快照数量达到128个后，文件系统会删除最早创建的自动快照。

   iv. 单击**确定**。
4. 应用自动快照策略。
   i. 找到目标自动快照策略，单击**应用到文件系统**。
   ii. 在**应用到文件系统**对话框**文件系统ID**区域，选中要应用自动快照策略的文件系统，然后单击>添加到**应用到文件系统**区域。
   iii. 单击**确定**。

   应用到文件系统后，该文件系统会执行自动快照策略，创建自动快照。

通过快照创建文件系统

您还可以使用SDK，通过某一时刻的快照创建文件系统。

注意 如果需要恢复某一时刻快照中的数据至现有文件系统中，您可以通过该时刻的快照创建新的文件系统，然后将新的文件系统中的数据拷贝至现有文件系统中。

1. 安装Python SDK。

```
pip install aliyun-python-sdk-core
pip install aliyun-python-sdk-bssopenapi
pip install aliyun-python-sdk-nas
```

2. 运行代码创建文件系统。

   重要参数说明如下所示，其他参数说明请参见后付费NAS文件存储询价示例。

   - accessKeyId和accessSecret：配置您阿里云账号的AccessKey ID和AccessKey Secret，AccessKey信息请参见如何获取AccessKey？。
   - set_parameters：配置为待创建的文件系统的相关参数。

参数	说明
Region	快照所在的地域。例如：`cn-shanghai`，您可以调用 DescribeRegions查询地域信息。
Zone	快照所在的地域下的可用区。例如：`cn-shanghai-g`，您可以调用 DescribeZones查询可用区信息。
ProtocolType	文件系统支持的协议类型。极速型NAS文件系统仅支持NFS v3协议。
StorageType	文件系统的存储规格。取值： ■ standard：标准型 ■ advance：高级型
Capacity	极速型NAS文件系统的存储容量，需要和创建快照的文件系统保持一致。
SnapshotId	快照ID。

```
#!/usr/bin/env python3
import json
from aliyunsdkcore.client import AcsClient
from aliyunsdknas.request.v20170626.CreateFileSystemRequest import CreateFileSystemRequ
est
def create_file_system():
    client = AcsClient('<accessKeyId>', '<accessSecret>', '<Region>')
    request = CreateFileSystemRequest()
    request.set_accept_format('json')
    request.set_StorageType("standard")
    request.set_ProtocolType("NFS")
    request.set_FileSystemType("extreme")
    request.set_Capacity("100")
    request.set_ZoneId("cn-hangzhou-h")
    request.set_SnapshotId("s-extreme-xxxxxxxxxx")
    response = client.do_action_with_exception(request)
    res = json.loads(response)
    print(res)
```

相关操作

操作	说明
取消自动快照策略	执行以下步骤取消自动快照策略： 1. 在**文件系统列表**页面，找到目标文件系统，选择**更多 > 快照 > 设置快照策略**。 2. 在**设置快照策略**对话框，关闭**是否应用策略**开关，然后单击**确定**取消自动快照策略。
查看快照	在**快照**页签，查看已创建的所有快照及相关信息。
删除快照	在**快照**页签，找到目标快照，单击**删除**，删除快照。
查看快照策略	在**自动快照策略**页签，查看已创建的所有快照策略及相关信息。
查看已应用快照策略的文件系统列表	在**自动快照策略**页签，找到目标快照策略，单击**应用到文件系统**，查看应用该快照策略的文件系统。
修改快照策略	在**自动快照策略**页签，找到目标快照策略，单击**修改策略**，修改快照策略。
删除快照策略	在**自动快照策略**页签，找到目标快照策略，单击**删除**，删除快照策略。

4.5. 管理标签

阿里云文件存储NAS提供管理标签功能，帮助您从各种维度（例如业务、用途、负责人等）对文件系统进行分类管理。本文档介绍标签的使用限制及如何添加标签、查看标签、编辑标签、删除标签、标签过滤等。

使用限制

- 数量限制

  每个文件系统最多允许添加20个标签。

- 标签键限制

  当一个文件系统添加了多个标签，标签键不允许重复。

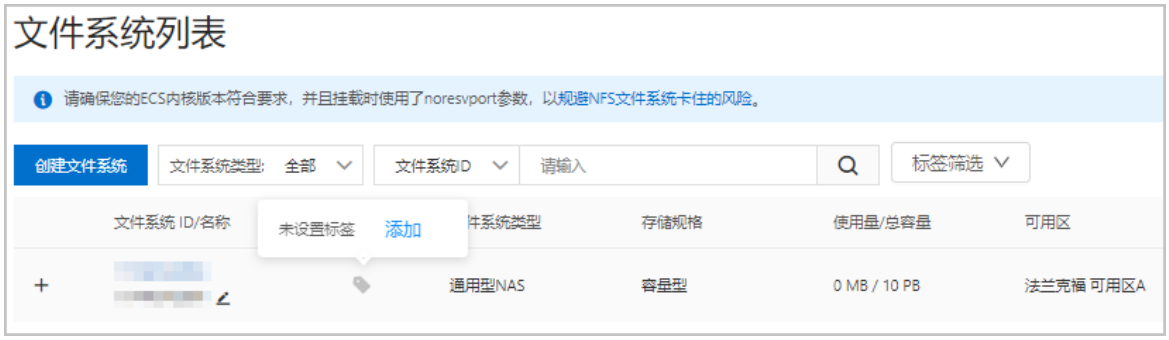
- 地域限制

  不同地域的标签信息不互通，例如在华东1（杭州）添加的标签在华东2（上海）是不可见的。

添加标签

您可以按照以下步骤为文件系统添加标签。

1. 登录NAS控制台。
2. 在左侧导航栏，选择**文件系统>文件系统列表**。
3. 在**文件系统列表**页面，找到目标文件系统并将鼠标悬浮于**标签**列的 图标上，在悬浮框单击**添加**。



4. 在**编辑标签绑定**对话框，请参照如下说明进行配置。

参数	说明
标签键	最大长度128个字符。 不能为空，不能以aliyun和acs:开头，不能包含http://和https://。
标签值	最大长度128个字符。 不能包含http://和https://。

5. 单击**确认**。

查看标签

若您的文件系统已添加标签，您可以通过以下步骤查看标签。

1. 登录NAS控制台。
2. 在左侧导航栏，选择**文件系统>文件系统列表**。
3. 在**文件系统列表**页面，找到目标文件系统并将鼠标悬浮于**标签**列的 图标上，在悬浮框内即可查看已添加的标签。

> 说明
>
> 您也可以在目标文件系**基本信息**页面**标签**区域，查看已添加的标签。

编辑标签

您可以按照以下步骤修改已添加的标签。

1. 登录NAS控制台。
2. 在左侧导航栏，选择**文件系统>文件系统列表**。
3. 在**文件系统列表**页面，找到目标文件系统并将鼠标悬浮于**标签**列的 图标上，在悬浮框单击**编辑**。
4. 在**编辑标签绑定**对话框，编辑已添加的标签，单击**确定**。

> 说明
>
> 您也可以在目标文件系**基本信息**页面**标签**区域，单击**编辑**，修改已添加标签。

删除标签

1. 登录NAS控制台。
2. 在左侧导航栏，选择**文件系统>文件系统列表**。
3. 在**文件系统列表**页面，找到目标文件系统并将鼠标悬浮于**标签**列的 图标上，在悬浮框单击**编辑**。
4. 在**编辑标签绑定**对话框，单击目标标签后的 图标，单击**确定**。

通过标签筛选文件系统

您可以通过以下步骤筛选包含指定标签键信息的文件系统。

1. 登录NAS控制台。
2. 在左侧导航栏，选择**文件系统>文件系统列表**。
3. 在**文件系统列表**页面上方，单击**标签筛选**，输入标签键信息后单击**搜索**，即可在列表中查看到符合搜索信息的文件系统。

4.6. 备份和恢复文件

您可以在NAS控制台定期备份NAS文件，并在数据丢失或受损时及时恢复文件。

备份文件

> **说明** 首次使用NAS文件系统的文件备份功能时，您可以免费试用30天，试用期结束后，您可以选择续费或暂停该备份计划。计费详情，请参见混合云备份计费说明。

1. 登录NAS控制台。
2. 在左侧导航栏，选择**数据服务 > 文件备份**。
3. 在**文件备份**页面，单击**开始备份文件系统**。

   > **说明** 若您首次使用文件备份功能，请按照页面提示开通混合云备份服务并添加服务角色授权。

4. 在**备份文件系统**面板，配置以下参数创建备份计划，然后单击**确定**。
   i. 配置基础参数。

参数	说明
文件系统	选择需要备份的文件系统。
备份计划名称	为该备份计划命名。
备份起始时间	选择备份开始执行的时间。时间精确到秒。
到期付费续用	免费备份计划到期后，是否执行到期付费续用。

ii. （可选）当您需要配置细粒度备份计划时，请您单击**显示高级设置**，然后单击**立即转为付费使用**，启用高级设置，并按以下说明配置高级参数。更多信息，请参见计费方式与计费项。

参数	说明
备份文件路径	输入待备份文件路径。 例如：*/nas/folder*，/表示NAS根目录。
备份执行间隔	选择增量备份的频率。 时间单位：天、周。
备份保留策略	您可以选择**指定保留时间**或**永久**保留备份。
备份保留时间	选择保留该备份的时间。 当您选择**指定保留时间**来保留备份，则需要指定**备份保留时间**，备份保留时间支持的单位为：天、周、月、年。
备份库配置	您可以**选择备份库**来保留备份。 如果您之前没有创建过备份仓库，单击**新建备份库**，然后输入仓库名称即可创建一个新仓库。仓库名称不能超过64个字节。
备份库名称	填写一个备份库名称。 当您选择**新建备份库**来保存备份数据，需要填写一个备份库名称。

5. 在**备份计划**页签，找到已创建的备份计划，单击**立即执行**。

> **说明**
> - 您可以在**备份任务**页签查看已执行的备份任务状态及备份文件数据量等信息。
> - 当备份任务状态较长时间没有更新，请您单击页面右上方**刷新**，然后再次查看任务状态。

恢复文件

1. 登录NAS控制台。
2. 在左侧导航栏，选择**数据服务 > 文件备份**。
3. 在**文件备份**页面，选择**恢复任务**页签，单击**创建恢复任务**。
4. 在**新建恢复任务**面板，按照以下步骤配置参数。
   i. 按照以下说明配置备份文件参数，单击**下一步**。

参数	说明
备份库	选择待恢复的文件所在的备份库。
已备份的NAS	选择待恢复的文件所在的文件系统。
待恢复文件	选择待恢复文件所在的目录。

ii. 根据实际恢复场景，选择适用的恢复规则，单击**下一步**。

iii. 选择将文件恢复至原文件系统或指定文件系统中，单击**下一步**。

iv. 选择将文件恢复至原目录中或指定目录中，单击**创建**。

> 说明
>
> - 您可以在**恢复任务**页签查看已执行的备份任务状态及备份文件数据量等信息。
> - 若您恢复任务的目的端为新指定的文件系统，请在**文件系统**列筛选目的端文件系统后，再查看恢复任务详细信息。

相关操作

分类	说明
备份计划相关操作	• 修改备份计划：您可以根据业务实际修改备份计划的执行间隔、保留策略及备份文件路径等信息。 • 删除备份计划：当不再需要此备份计划，请及时删除。 • 暂停备份计划：当备份计划状态为计划中，您可以暂停该计划。 • 继续备份计划：当备份计划状态为暂停，您可以选择继续执行该计划。
备份任务相关操作	• 查询备份任务：您可以查询近3个月执行的所有备份任务详情，包括任务状态、数据量及进度等信息。 • 取消备份任务：当备份任务状态为等待执行或执行中，您可以取消该备份任务。取消后，该任务中所有已备份文件均会被清理，不会保留在备份库中。若您还需备份改文件，请重新执行备份任务。
恢复任务相关操作	• 查询恢复任务：您可以查询恢复任务的状态、数据量及进度等信息。 • 取消恢复任务：当恢复任务状态为执行中，您可以取消该恢复任务。在您取消文件恢复任务后，该任务中已恢复的文件将保存在指定目录中，任务中其他文件将不再被恢复。

常见问题

- NAS文件备份的免费期是怎么计算的？
- 文件存储NAS是否支持inotify？
- 更多备份和恢复文件的常见问题

4.7. 回收站

当您误删除通用型NAS文件系统中的文件后，可以通过NAS回收站恢复这些文件及其UID、GID和ACL等元数据信息。

背景信息

开启回收站后，被删除的文件或目录将暂存在回收站中，包括但不限于：

- 您在ECS、容器等计算节点上手动删除的NAS中的文件。例如手动执行`rm -f test01.text`命令删除文件*test01.text*，文件*test01.text*将进入回收站。

- 使用应用程序在计算节点上自动删除的NAS中的文件或目录。例如Python使用 `os.remove("test02.text")` 删除文件*test02.text*，文件*test02.text*将进入回收站。
- POSIX rename触发删除的文件或目录。例如同一目录存在文件*test_a.txt*和文件*test_b.txt*，执行 `mv test_a.txt test_b.txt` ，文件*test_b.txt*将进入回收站。
- 应用程序使用NAS文件产生的临时文件。例如执行**vim**命令编辑文件时，产生的 `.swp` 和 `.swpx` 格式的文件将进入回收站。
- 应用程序自动轮转的日志文件。例如使用Nginx配置了自动轮转日志且最多保留20个日志文件，当日志文件*test.log.19*轮转为日志文件*test.log.20*时，原日志文件*test.log.20*将进入回收站。

> **说明** 如果仅覆写文件内容，不删除该文件，不会触发文件进入回收站。例如调用 `open()` 函数以 `w+` 模式打开文件并写入，原始文件不会进入回收站。

使用说明

- 费用说明

  回收站功能本身不收取任何费用，但是暂存在回收站中的文件将按照删除前的存储类型收取存储费用。为节省不必要的存储费用，请您合理配置文件保留时间。计费详情，请参见通用型NAS计费说明和低频介质计费说明。

- 权限说明

  只有文件系统的拥有者及授予了文件系统回收站使用权限的RAM用户才能使用回收站功能。更多信息，请参见授予RAM用户对文件系统回收站的管理权限。

开启回收站

开启回收站后，被删除的文件将自动进入回收站，并在规定的保留时间之后彻底删除。执行以下步骤开启回收站：

1. 登录NAS控制台。
2. 在左侧导航栏，选择**文件系统 > 文件系统列表**。
3. 在**文件系统列表**页面，单击目标文件系统名称。
4. 在文件系统详情页，单击**回收站**页签，单击**开启回收站**。
5. 在**开启回收站**对话框，选择**文件保留时间**为3天，单击**确定**。

恢复回收站中的文件

您可以在保留时间内恢复回收站中暂存的文件。执行恢复操作注意事项如下：

- 单个文件系统一次只能执行一个文件恢复任务。正在恢复文件时，无法发起新的文件恢复任务。
- 单个恢复任务只能恢复一个文件或目录，恢复指定目录会恢复目录中的所有文件。

  > **说明** 如果待恢复目录下同一文件关联的硬链接文件个数超过511个，NAS将随机恢复该目录下的511个硬链接文件，超出数量的文件无法恢复，因此恢复任务状态将显示为部分运行成功。

- 单个恢复任务的文件或目录数量越多，恢复时间越长。

请执行以下步骤恢复回收站中暂存的文件：

1. 登录NAS控制台。
2. 在左侧导航栏，选择**文件系统 > 文件系统列表**。

3. 在**文件系统列表**页面，单击目标文件系统名称。
4. 在文件系统详情页，单击**回收站**。
5. 在**回收站**页签，找到目标文件，单击**恢复**。
6. 在**选择文件的恢复路径**对话框，选择文件恢复后的存储路径，单击**确认**。
   - **恢复至原路径**：当文件被删除前的路径存在时，文件将恢复至该路径下。当文件被删除前的路径不存在，请您选择自定义恢复路径。
   - **自定义恢复路径**：选择一个已存在的路径，存放恢复后的文件。

> **说明**
>
> - 当任务状态为整理中时，文件的读性能稍有下降，建议此时不要调整文件系统的目录结构，否则将增加数据整理的时长。
> - 恢复任务完成后，如果在ECS实例执行ls命令查询不到刚恢复的目录下的文件，请在该ECS实例上执行 `sudo sysctl -w vm.drop_caches=2` 命令清理ECS上的缓存，然后再次查询文件。

相关操作

操作	说明	步骤
清空回收站	当回收站内的文件已废弃，您可以清空回收站，节省存储费用。 **警告** 清空回收站时会彻底删除回收站内的所有文件，已彻底删除的文件将无法找回。	1. 在**回收站**页签，单击**清空回收站**。 2. 再次确认回收站中的文件已废弃，单击**确定**。
修改文件保留时间	您可以根据文件系统的使用情况随时修改文件保留时间，避免回收站中暂存的文件产生过多存储费用。	1. 在**回收站**页签，单击**修改**。 2. 在**修改保留时间**对话框，修改保留时间，单击**确定**。
关闭并清空回收站	关闭回收站时会彻底删除回收站内的所有文件。 已关闭的回收站重新开启后，回收站内容为空，无法找回开启回收站功能前删除的文件。	1. 在**回收站**页签，单击**关闭并清空回收站**。 2. 再次确认回收站中的文件已废弃且不再使用回收站功能，单击**确定**。
查询回收站中的文件	暂存在回收站内的文件，在计算节点上无法查询，只能通过NAS控制台查询。	在**回收站**页签，可以查询回收站中暂存的文件及删除时间等信息。
彻底删除回收站中的文件	彻底删除回收站中的指定目录会同时彻底删除目录中的所有文件。 **警告** 回收站内文件一旦彻底删除将无法找回。	1. 在**回收站**页签，找到目标文件，单击**彻底删除**。 2. 再次确认目标文件已废弃，单击**确定**。

操作	说明	步骤
查询回收站任务列表	您可以通过控制台查看近7日执行的文件恢复或文件彻底删除任务，最多显示50条任务记录。	1. 在**回收站**页签，单击**任务管理**页签。 2. 在**任务管理**页签，查看已执行的文件恢复或文件彻底删除任务。
取消文件彻底删除或文件恢复任务	当文件恢复任务的状态为恢复中、文件彻底删除任务的状态为删除中时，您可以通过控制台取消此任务。 • 文件恢复任务取消后，已恢复的文件可以在文件系统中查询到，未恢复的文件可以在回收站中查询。 • 文件彻底删除任务取消后，已彻底删除的文件或目录不支持找回，未彻底删除的文件或目录可以在回收站中查询。	1. 在**回收站**页签，单击**任务管理**页签。 2. 在**任务管理**页签，找到目标任务，单击**取消**。

FAQ

- 文件系统目录名已变更，执行回收站文件恢复操作能恢复至原目录吗？
- 能否读写回收站中的文件？
- 使用回收站是否收费？
- 更多回收站常见问题

4.8. 数据加密

4.8.1. 服务器端加密

文件存储NAS支持服务器端加密功能。NAS会对存储在文件系统中的数据进行加密，访问数据时，NAS自动将加密数据解密后返回给用户。本文介绍服务器端加密的工作原理及相关操作。

使用限制

- 仅支持在创建文件系统时开启数据加密功能。
- 已开启数据加密功能的文件系统不能关闭此功能。

加密方式

当您对文件存储有高安全性或者合规性要求时，建议您开启服务器端加密功能。服务器端加密密钥采用行业标准AES-256加密算法，保护文件系统静态数据，并通过信封加密机制防止未经授权的数据访问。服务器端加密密钥依托于KMS服务生成和管理。KMS服务能最大程度保障密钥的保密性、完整性和可用性。

NAS针对不同使用场景提供了以下两种服务器端加密方式。

> **说明** 使用NAS托管密钥免费。使用用户管理密钥会产生少量的KMS密钥使用费用。更多信息，请参见KMS计费说明。

- NAS托管密钥

  使用NAS完全托管的密钥加密每个文件系统。该密钥由NAS在KMS（Key Management Service）服务中进行创建和管理，您可以查看密钥并审计密钥的使用权限，但无法删除、禁用该密钥。

- 用户管理密钥

  使用您托管给KMS服务的用户管理密钥对文件系统进行加解密操作。当该密钥被禁用或者删除后，使用该密钥进行加密的NAS文件系统将不可访问。用户管理密钥有以下两种来源：

  - 在KMS服务中创建的密钥：您可以在KMS服务中创建用户主密钥CMK（Customer Master Key），并对CMK进行配置和管理，包括启用、禁用、删除、密钥轮转等操作。
  - 自带密钥BYOK（Bring Your Own Key）：为了满足一些特定的安全需求，您可以将本地或其他途径生成的自带密钥BYOK导入KMS，作为用户主密钥CMK。具体操作，请参见导入密钥材料。

操作方式

在NAS控制台创建文件系统时，根据使用场景配置加密方式为**NAS托管密钥**或**用户管理密钥**。具体操作，请参见通过控制台创建通用型NAS文件系统和通过控制台创建极速型NAS文件系统。

支持地域

- NAS托管密钥加密
  - 通用型NAS：所有地域。
  - 极速型NAS：所有地域。
- 用户管理密钥加密
  - 通用型NAS：
    - 美国（硅谷）
    - 美国（弗吉尼亚）
    - 英国（伦敦）
    - 澳大利亚（悉尼）
    - 德国（法兰克福）
    - 印度（孟买）
    - 新加坡
  - 极速型NAS：所有地域。

FAQ

- 如何使用NAS的服务器端加密功能？
- 我该怎么选择NAS托管密钥和用户管理密钥？
- 如果误操作禁用了CMK或误删了CMK，如何恢复对NAS文件系统中数据的访问？
- 更多服务器端加密FAQ

4.8.2. NFS文件系统传输加密

传输加密功能通过TLS协议保护您的ECS实例与NAS服务之间网络传输链路上的数据安全，确保您的数据在传输过程中不被窃取或篡改。本文介绍如何使用NAS客户端工具挂载文件系统实现数据传输加密。

工作原理

NAS客户端工具定义了一个网络文件系统类型alinas，与标准**mount**命令兼容。在ECS实例挂载alinas类型文件系统时，如果指定 `tls` 参数，NAS客户端工具会启动一个Stunnel监听进程，该进程转发并加密ECS实例对NAS服务器的访问，同时会触发一个后端进程 `aliyun-alinas-mount-watchdog` 保障Stunnel监听进程的可用性。

使用说明

> **注意** 开启传输加密功能时，如果您的目标ECS实例上对应目录（例如/mnt）已挂载NFS文件系统，请先卸载NFS文件系统，再根据本文重新挂载NFS文件系统。关于如何卸载NFS文件系统的操作，请参见在Linux系统中卸载文件系统。

- NAS客户端支持的操作系统

操作系统类型	操作系统版本
Alibaba Cloud Linux	Alibaba Cloud 2.1903 64位
Red Hat	○ Red Hat Enterprise Linux 7.x 64位 ○ Red Hat Enterprise Linux 8.x 64位
CentOS	○ CentOS 7.x 64位 ○ CentOS 8.x 64位
Ubuntu	○ Ubuntu 16.04 64位 ○ Ubuntu 18.04 64位 ○ Ubuntu 20.04 64位
Debian	○ Debian 9.x 64位 ○ Debian 10.x 64位

- 传输加密的性能损耗

  开启传输加密的挂载与未开启传输加密的挂载相比，访问延迟会增加约10%，IOPS会下降约10%。

- 使用NAS客户端的说明
  - NAS客户端工具使用Stunnel监听进程进行TLS加密代理。对于吞吐密集性应用，Stunnel监听进程会消耗大量CPU执行加解密操作。在极端情况下，每个挂载会占用一整个核。
  - NAS客户端传输加密功能依赖第三方证书，第三方证书需要定期更换，NAS会提前一个月通过邮件、站内信发出通知，请您关注信息并及时更新NAS客户端工具aliyun-alinas-utils版本，未更新NAS客户端工具将导致使用传输加密方式挂载的NAS文件系统在证书过期后停止响应。
  - 使用NAS客户端工具会修改您账号下ECS实例的*/etc/hosts*文件。即挂载文件系统时，会将新的挂载点映射写入*/etc/hosts*文件；卸载文件系统时，会删除之前写入的挂载点映射。
  - NAS客户端工具使用Stunnel监听进程进行TLS加密代理时，会占用127.0.1.1~127.0.255.254中的IP作为Stunnel监听进程的IP，并需要使用12049端口，请您确保目标IP和端口可用。

    您可以执行**ss -ant | grep -w 12049**命令判断目标端口是否被占用。如果返回为空，则表示目标端口未被占用。如果端口被占用，请您修改配置文件。具体操作，请参见如何修改NAS客户端配置文件。

支持地域

公共云所有地域，金融云除深圳地域以外所有地域。

步骤一：下载与安装NAS客户端

1. 下载NAS客户端。

- Alibaba Cloud Linux

```
wget https://aliyun-encryption.oss-cn-beijing.aliyuncs.com/aliyun-alinas-utils-1.0-1.al7.noarch.rpm
```

- Red Hat Enterprise Linux 7.x和CentOS 7.x

```
wget https://aliyun-encryption.oss-cn-beijing.aliyuncs.com/aliyun-alinas-utils-1.0-1.el7.noarch.rpm
```

- Red Hat Enterprise Linux 8.x和CentOS 8.x

```
wget https://aliyun-encryption.oss-cn-beijing.aliyuncs.com/aliyun-alinas-utils-1.0-1.el8.noarch.rpm
```

- Ubuntu和Debian

```
wget https://aliyun-encryption.oss-cn-beijing.aliyuncs.com/aliyun-alinas-utils-1.0-1.deb
```

2. 安装NAS客户端。
   - Alibaba Cloud Linux和CentOS

```
sudo yum install aliyun-alinas-utils-*.rpm
```

   - Red Hat Enterprise Linux

```
sudo yum --disablerepo=rhui-rhel-7-server-rhui-extras-debug-rpms install aliyun-alinas-utils-*.rpm
```

   - Ubuntu和Debian

```
sudo apt update
```

```
sudo dpkg -i aliyun-alinas-utils-*.deb
```

```
sudo apt-get install -f
```

```
sudo dpkg -i aliyun-alinas-utils-*.deb
```

3. 检查NAS客户端安装结果。

```
which mount.alinas
```

如果回显包含如下类似信息，说明NAS客户端安装成功。

```
[root@iZ8v[illegible] ~]# which mount.alinas
/usr/sbin/mount.alinas
```

步骤二：以传输加密方式挂载文件系统

1. 挂载NFS文件系统。
   - NFSv3协议

```
sudo mount -t alinas -o tls,vers=3 file-system-id.region.nas.aliyuncs.com:/ /mnt
```

   - NFSv4.0协议

```
sudo mount -t alinas -o tls,vers=4.0 file-system-id.region.nas.aliyuncs.com:/ /mnt
```

挂载命令中的参数说明如下表所示。

> **说明** 挂载文件系统时，NAS客户端工具将自动使用最佳参数进行挂载，无需手动添加。更多信息，请参见挂载参数说明。

参数	说明
file-system-id.region.nas.aliyuncs.com:/ /mnt	表示<挂载地址>:<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。 ■ *挂载地址*：您可以在文件存储NAS控制台**文件系统列表**页面，单击目标文件系统后的**管理**，进入**挂载使用**页面获取挂载地址。更多信息，请参见管理挂载点。 ■ *NAS文件系统目录*：NAS的根目录（/）或任意子目录（例如：*/share*），如果是子目录，请您确保子目录是NAS文件系统中实际已存在的目录。 ■ *当前服务器上待挂载的本地路径*：Linux ECS实例的任意子目录（例如：*/mnt*），请您确保子目录在本地文件系统存在。
vers	NFS文件系统版本。 ■ vers=3：使用NFSv3协议挂载文件系统。 ■ vers=4.0：使用NFSv4.0协议挂载文件系统。
tls	启用数据传输加密。

2. 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。

   ```
   alinas-[redacted].cn-zhangjiakou.tls.127.0.1.3:/ on /mnt type nfs (rw,relatime,vers=3,rsize=1048576,wsize=1048576,namlen=255,hard,nolock,nosvport,proto=tcp,port=12050,timeo=600,retrans=2,sec=sys,mountaddr=127.0.1.3,mountvers=3,mountport=12050,mountproto=tcp,local_lock=all,addr=127.0.1.3)
   ```

   挂载成功后，您可以执行**df -h**命令，查看当前文件系统的容量信息。

3. （可选）配置开机时自动挂载。

   为避免已挂载文件系统的ECS实例重启后，挂载信息丢失，您可以通过在Linux ECS实例中配置*/etc/fstab*文件，实现在ECS实例重启时NFS文件系统自动挂载。

   i. 打开*/etc/fstab*配置文件，添加挂载配置。

   ```
   file-system-id.region.nas.aliyuncs.com:/ /mnt alinas _netdev,tls 0 0
   ```

   示例中主要参数说明，请参见Linux系统挂载NFS文件系统。其余参数说明如下。

参数	说明
_netdev	防止客户端在网络就绪之前开始挂载文件系统。
0（tls后第一项）	非零值表示文件系统应由dump备份。对于NAS文件系统而言，此值默认为0。
0（tls后第二项）	该值表示fsck在启动时检查文件系统的顺序。对于NAS文件系统而言，此值默认为0，表示fsck不应在启动时运行。

ii. 执行 `reboot` 命令，重启ECS实例。

> **说明** 在重启ECS实例前，请确认手动挂载成功，避免ECS实例重启失败。另外，如果自动挂载配置成功，在ECS实例重启后，可以通过 `df -h` 命令查看到挂载的NAS文件系统。

NAS客户端日志

您可以通过访问*/var/log/aliyun/alinas/*路径下的NAS客户端日志定位挂载报错信息。同时可以通过修改日志配置文件*/etc/aliyun/alinas/alinas-utils.conf*中的参数，定制NAS客户端日志内容。修改配置文件后，请您执行**sudo service aliyun-alinas-mount-watchdog restart**命令，重启后端watchdog进程。

日志配置文件中的重要参数如下：

参数	说明
logging_level	日志级别。默认为INFO。
logging_max_bytes	日志文件的最大容量。默认为1048576字节，即单个日志文件最大为1 MB。
logging_file_count	日志文件的最大保留数量。默认为10，即最多保留10个日志文件。
stunnel_debug_enabled	Stunnel监听进程debug日志。默认为false，开启时会占用大量存储容量。
stunnel_check_cert_hostname	检查证书域名。默认为false。
stunnel_check_cert_validity	检查证书合法性。默认为false。

错误排查

- 问题现象

  挂载文件系统时，返回如下报错信息：

```
$sudo mount -t alinas -o tls,vers=4.0 [redacted] cn-hangzhou.nas.aliyuncs.com /mnt
Failed to find a loopback ip from 127.0.1.1 ~ 127.0.0.255.254 with port 12049
```

- 可能原因

  Stunnel监听进程的IP或12049端口被占用，导致文件系统挂载失败。

- 解决方案
  - 方案一：找到并结束占用12049端口的进程，然后重新挂载文件系统。

- 方案二：修改NAS客户端工具配置文件*/etc/aliyun/alinas/alinas-utils.conf*中的proxy_port参数，修改为未被占用的端口号，然后重新挂载文件系统。

```
[DEFAULT]
logging_level = INFO
logging_max_bytes = 1048576
logging_file_count = 10

[mount]
stunnel_debug_enabled = false

# Validate the certificate hostname on mount. This option is not supported by certain stunnel versions.
stunnel_check_cert_hostname = false

# Use OCSP to check certificate validity. This option is not supported by certain stunnel versions.
stunnel_check_cert_validity = false

proxy_port = 12050

[mount-watchdog]
poll_interval_sec = 1
unmount_grace_period_sec = 30
```

4.8.3. SMB文件系统传输加密

SMB文件系统传输加密采用认证加密算法（Authenticated Encryption），保证您的ECS实例与NAS服务之间网络传输链路上的数据安全，确保您的数据在传输过程中不被窃取或篡改。

使用说明

- 客户端操作系统

  需使用支持SMB 3.0及以上版本文件协议的操作系统，包括：

操作系统类型	操作系统版本
Windows Server	○ 2012 R2 数据中心版 64位中文版及以上版本 ○ 2012 R2 数据中心版 64位英文版及以上版本
Aliyun Linux	Aliyun Linux 4.19.34及以上版本
Red Hat	Red Hat Enterprise Linux 7.5 64位及以上版本
CentOS	CentOS 7.6 64位及以上版本
Ubuntu	Ubuntu 18.04 64位及以上版本
Debian	Debian 10.2 64位及以上版本
Suse Enterprise Server	Suse Enterprise Server 12 SP2 64位及以上版本
OpenSUSE	OpenSUSE 42.3 64位及以上版本
CoreOS	CoreOS 4.19.43及以上版本

- 传输加密权限说明

  不支持匿名用户使用传输加密功能，仅支持AD域身份用户挂载SMB文件系统实现文件传输加密。

- 传输加密的性能损耗

开启传输加密的挂载与未开启传输加密的挂载相比，访问延迟会增加约10%，IOPS会下降约10%。

开启传输加密

仅支持在使用SMB ACL功能时，通过配置如下参数开启SMB文件系统传输加密功能：

参数	说明
启用传输加密	选择**是**，开启SMB文件系统传输加密功能。
拒绝非加密客户端	配置访问SMB文件系统的客户端类型。 • **是**：仅支持使用传输加密的客户端挂载该SMB文件系统，即支持SMB传输加密的操作系统以AD域身份挂载SMB文件系统。 当以匿名身份挂载或使用不支持传输加密的客户端挂载SMB文件系统时，挂载将会失败。 • **否**：所有客户端均能挂载该SMB文件系统，但只有支持传输加密的操作系统以AD域身份挂载SMB文件系统才会启用传输加密功能。

更多操作，请参见SMB ACL概述。

4.9. 数据监控

4.9.1. NAS监控概述

NAS监控服务为您提供了文件系统性能和存储容量两方面的监控数据指标，并且提供自定义报警服务，帮助您跟踪读写吞吐、IOPS、延迟、存储使用情况等，及时发现文件系统的异常信息。

容量指标相关说明

容量监控数据为实时值，不作为账单计算的计量值。若您希望查询更详细的计量数据，请参见查看消费明细。

性能指标相关说明

- 读写IOPS与元数据QPS的数据类型均为整型，若一分钟内的相关请求数小于60，则监控值显示为0。
- 当图表显示**无数据**，表示目标文件系统长时间没有向服务端发起足够多的请求。

监控数据保留策略

监控数据保留90天，过期自动清除。起始时间为数据产生的时间。

NAS报警服务

每个账号最多能够设置1000项报警规则，一个监控指标可以配置为多个不同的报警规则。

- 报警服务相关信息请参见报警服务概览。
- NAS报警服务使用指南请参见创建报警规则。
- 性能监控和容量监控的具体监控指标请参见性能监控项说明和容量监控项说明。

通过API获取监控数据

NAS的监控数据支持通过云监控API查询，具体如下：

- DescribeMetricMetaList：查询云监控开放的时序类指标监控项描述。

- DescribeMetricList：查询指定时间段内的云产品时序指标监控数据。
- DescribeMetricLast：查询指定监控对象的最新监控数据。

NAS的请求参数说明如下表所示。

名称	说明
Namespace	云服务的数据命名空间，NAS为*acs_nas*。
MetricName	监控项名称。取值如下： • 容量监控：AlignedSize、SecondaryAlignedSize、FileCount • 性能监控：IopsRead、IopsWrite、LatencyRead、LatencyWrite、QpsMeta、ThruputRead、ThruputWrite
Dimensions	维度Map，用于查询指定资源的监控数据。 格式为 `{"userId":"xxxxxx","fileSystemId":"xxxxx"}` **说明** Dimensions传入时需要使用JSON字符串表示该Map对象，必须按顺序传入。

4.9.2. 查看容量监控

通用型NAS支持容量监控。本文介绍如何查看通用型NAS的容量监控。

前提条件

已开通云监控服务。

您可以登录云监控产品详情页，根据页面提示开通服务。

容量监控项说明

指标	指标名称	单位	描述
AlignedSize	通用型NAS数据量（不含低频介质）	字节	该文件系统在周期内使用的数据量，不包含低频介质数据量。
SecondaryAlignedSize	低频介质数据量	字节	该文件系统在周期内使用的低频介质数据量。
FileCount	文件数	个	该文件系统在周期内的文件数量，不包含目录。

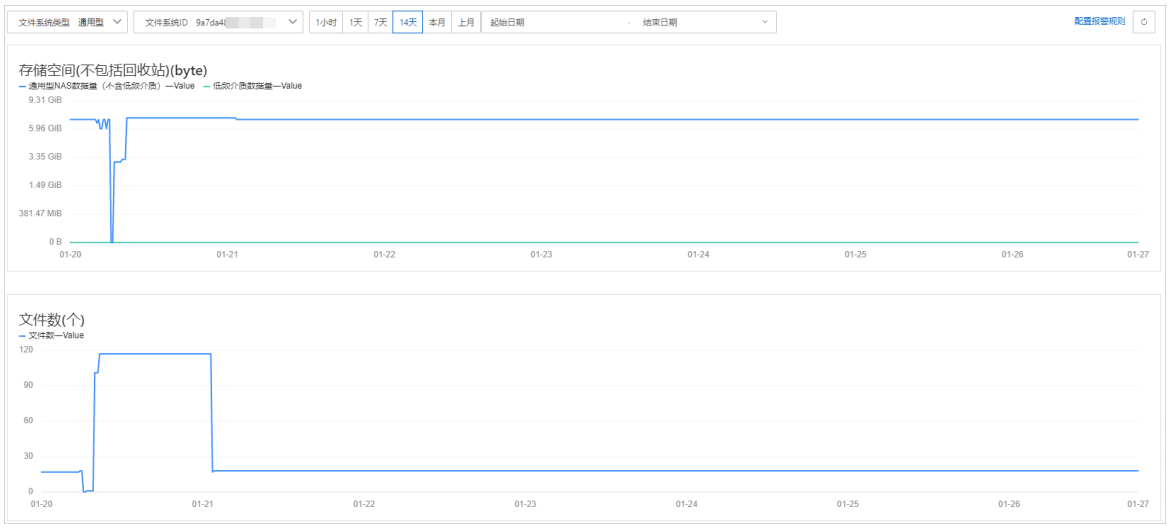
查看容量监控详情

说明 您也可以通过云监控控制台，查看NAS容量监控详情。具体操作，请参见查看监控数据。

1. 登录NAS控制台。
2. 在左侧导航栏中，选择**监控审计 > 容量监控**。

3. 在**容量监控**页面，执行以下操作，查看目标文件系统的容量监控详情。
   i. 在**文件系统ID**下拉列表，选择目标文件系统ID。
   ii. 选择查询时间（**1小时**、**1天**、**7天**、**14天**、**上月**或**本月**）或者在自定义时间框中自定义起始时间和结束时间。

容量监控页面主要包括存储空间（不包括回收站）和文件数两部分的监控指标图。



> **注意** 容量监控数据为实时值，不作为账单计算的计量值。若您希望查询更详细的计量数据，请参见查看消费明细。

相关操作

- 创建报警规则
- 您也可以为多个文件系统创建分组，从分组维度管理报警规则，查看监控数据，降低管理复杂度，提高监控使用效率。具体操作，请参见创建应用分组。

4.9.3. 查看性能监控

本文介绍如何查看NAS的性能监控。

前提条件

已开通云监控服务。

您可以登录云监控产品详情页，根据页面提示开通服务。

性能监控项说明

指标	指标名称	单位	描述
IopsRead	读IOPS	次/秒	该文件系统在周期内每秒平均读IOPS次数。
IopsWrite	写IOPS	次/秒	该文件系统在周期内每秒平均写IOPS次数。
ThruputRead	读吞吐	字节/秒	该文件系统在周期内每秒平均读吞吐字节。

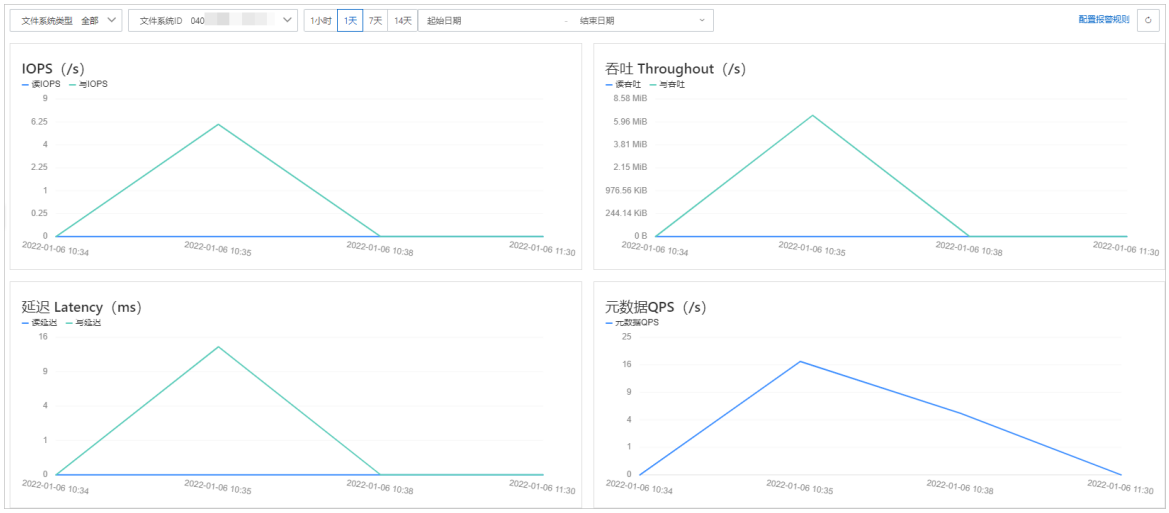
指标	指标名称	单位	描述
ThruputWrite	写吞吐	字节/秒	该文件系统在周期内每秒平均写吞吐字节。
LatencyRead	读延迟	ms	该文件系统在周期内每毫秒平均读延迟。
LatencyWrite	写延迟	ms	该文件系统在周期内每毫秒平均写延迟。
QpsMeta	元数据QPS	次/秒	该文件系统在周期内每秒平均请求元数据次数。

查看性能监控详情

> **说明** 您也可以通过云监控控制台，查看NAS性能监控详情。具体操作，请参见查看监控数据。

1. 登录NAS控制台。
2. 在左侧导航栏中，选择**监控审计 > 性能监控**。
3. 在性能监控页面，进行以下操作，查看指定文件系统的性能监控详情。
   i. 在**文件系统类型**下拉列表，选择目标文件系统。
   ii. 在**文件系统ID**下拉列表，选择目标文件系统ID。
   iii. 选择查询时间（**1小时**、**1天**、**7天**或**14天**）或者在自定义时间框中自定义起始时间和结束时间。

性能监控页面主要包括IOPS、吞吐、延迟和元数据四部分的监控指标图。



> 说明
> - 当图表显示**无数据**，说明目标文件系统长时间没有向服务端发起足够多的请求。
> - 您可以使用FIO工具测试文件系统性能并在云监控控制台查看性能指标图表。具体操作，请参见NAS性能测试。
>
>   例如，您可以在挂载NAS的ECS实例上执行命令（挂载目录为*/mnt*）：`fio -numjobs=1 -iodepth=128 -direct=1 -ioengine=libaio -sync=1 -rw=randwrite -bs=1M -size=1G -time_based -runtime=600 -name=Fio -directory=/mnt`，用于测试文件系统写吞吐指标。
> - 读写IOPS与元数据QPS的数据类型均为整型，若一分钟内的相关请求数小于60，则监控值显示为0。

相关操作

- 创建报警规则
- 您也可以为多个文件系统创建分组，从分组维度管理报警规则，查看监控数据，降低管理复杂度，提高监控使用效率。具体操作，请参见创建应用分组。

4.9.4. 创建报警规则

当您需要监控NAS文件系统资源的使用情况时，可以创建报警规则。如果资源的监控指标达到报警条件，云监控自动发送报警通知，帮助您及时得知异常监控数据，并快速处理。

前提条件

- 已创建NAS文件系统。具体操作，请参见创建文件系统。
- 已开通云监控服务。

  您可以登录云监控产品详情页，根据页面提示开通服务。

1. 登录云监控控制台。
2. 在左侧导航栏，选择**报警服务 > 报警规则**，单击**创建报警规则**。
3. 在**创建报警规则**面板，配置如下相关信息。

配置项	说明
产品	选择**文件存储NAS**。
资源范围	报警规则作用的资源范围。取值： ○ 全部资源：报警规则作用于NAS的全部资源上。 **说明** 目前NAS和CPFS共用云监控控制台，选择全部资源时，包含CPFS资源。 ○ 应用分组：报警规则作用于NAS的指定应用分组内的全部资源上。 ○ 实例：报警规则作用于NAS的指定资源上。
关联资源	当资源范围为**应用分组**或**实例**时，请在下拉列表中选择需要配置的关联资源。

配置项	说明
规则描述	报警规则的主体。当监控数据满足报警条件时，触发报警规则。 规则描述的设置方法如下： i. 单击**添加规则**。 ii. 在**添加规则描述**面板，设置规则名称、监控指标类型、监控指标、阈值、报警级别和报警方式等。 iii. 单击**确定**。 例如：配置文件系统读延迟连续3个周期超过5毫秒时，触发警告级别的报警。  如果需要监控文件系统的多个性能指标和容量指标，您可以选择**多指标**配置多个监控指标项。
通道沉默周期	报警发生后未恢复正常，间隔多久重复发送一次报警通知。取值：5分钟、15分钟、30分钟、60分钟、3小时、6小时、12小时和24小时。 某监控指标达到报警阈值时发送报警，如果监控指标在通道沉默周期内持续超过报警阈值，在通道沉默周期内不会重复发送报警通知；如果监控指标在通道沉默周期后仍未恢复正常，则云监控再次发送报警通知。 **说明** 单击**高级设置**，可配置该参数。
生效时间	报警规则的生效时间，报警规则只在生效时间内才会检查监控数据是否需要报警。 **说明** 单击**高级设置**，可配置该参数。

配置项	说明
报警联系人组	发送报警的联系人组。 应用分组的报警通知会发送给该报警联系人组中的报警联系人。报警联系人组是一组报警联系人，可以包含一个或多个报警联系人。 关于如何创建报警联系人和报警联系人组，请参见创建报警联系人或报警联系组。
报警回调	公网可访问的URL，用于接收云监控通过POST请求推送的报警信息。目前仅支持HTTP协议。关于如何设置报警回调，请参见使用阈值报警回调。
弹性伸缩	如果您打开**弹性伸缩**开关，当报警发生时，会触发相应的伸缩规则。您需要设置弹性伸缩的**地域**、**弹性伸缩组**和**弹性伸缩规则**。 ○ 关于如何创建弹性伸缩组，请参见创建伸缩组。 ○ 关于如何创建弹性伸缩规则，请参见创建伸缩规则。
日志服务	如果您打开**日志服务**开关，当报警发生时，会将报警信息写入日志服务的日志库。您需要设置日志服务的**地域**、**ProjectName**和**Logstore**。 关于如何创建Project和Logstore，请参见快速入门。
消息服务MNS-Topic	如果您打开**消息服务MNS-Topic**开关，当报警发生时，会将报警信息写入消息服务的主题。您需要设置消息服务的地域和主题。 关于如何创建主题，请参见创建主题。
无数据报警处理方法	无监控数据时报警的处理方式。取值： ○ **不做任何处理**（默认值） ○ **发送无数据报警** ○ **视为正常**

4. 单击**确定**，完成报警规则的设置。

   当文件系统的监控项超过设定阈值后会自动发送报警通知，使您及时获取监控数据异常。

更多参考

- 查看正在报警的资源
- 修改报警规则
- 报警通知合并

4.10. 日志管理

4.10.1. 使用前须知

阿里云文件存储（NAS）联合日志服务推出日志分析功能，提供NAS访问日志的实时采集、查询、分析、加工、消费等一站式服务。本文介绍NAS访问日志功能相关的资产详情、费用说明及使用限制等。

资产详情

- 专属Project和Logstore

  开通日志分析功能后，系统默认在不同的地域各创建一个名为nas-阿里云账号ID-地域ID的Project，以及一个名为nas-nfs的专属Logstore。

  > **说明** 请勿删除NAS日志相关的日志服务Project和Logstore，否则将无法正常采集日志到日志服务。

- 专属仪表盘

  默认生成3个仪表盘。

  > **说明** 专属仪表盘可能随时进行升级与更新，建议您不要修改专属仪表盘。您可以自定义仪表盘用于查询结果展示，详情请参见创建仪表盘。

仪表盘	说明
nas-nfs-nas_summary_dashboard_cn	展示NAS总体运营情况，包括最近访问的Volume个数、写入总流量、读取总量、最近访问的客户端个数等信息。
nas-nfs-nas_audit_dashboard_cn	展示NAS文件系统操作统计信息，包括创建操作数、删除文件数、读取文件数等信息。
nas-nfs-nas_detail_dashboard_cn	展示NAS文件系统明细信息，包括最近访问的文件数量、操作趋势等信息。

费用说明

- 目前，NAS不针对日志分析功能收取额外费用。
- NAS将日志转储到日志服务后，日志服务根据存储空间、读取流量、请求数量、数据加工、数据投递等进行收费，详情请参见日志服务产品定价。

使用限制

- 专属Logstore不支持写入其他数据，但在查询、统计、告警等功能上无特殊限制。
- 目前，仅支持NFS协议的文件系统。

4.10.2. 开通日志分析功能

本文介绍如何在NAS控制台上开通日志分析功能，将日志采集到日志服务中。

前提条件

- 已创建NFS文件系统并完成挂载，详情请参见Linux系统挂载NFS文件系统。
- 已授权NAS使用AliyunNASLogArchiveRole角色访问日志服务。

  单击云资源访问授权，根据提示完成授权。

> 说明
> - 该操作仅在首次配置时需要，需要由阿里云主账号进行授权。
> - 如果您使用的是RAM用户，该RAM用户需具备相关权限，详情请参见RAM用户授权。
> - 请勿取消授权或删除RAM角色，否则将导致NAS日志无法正常推送到日志服务。

操作步骤

1. 登录NAS控制台。
2. 在左侧导航栏，单击**监控审计 > 日志分析**。
3. 在**日志分析**页面，单击**新建日志转储**。
4. 在**新建日志转储**页面，配置**文件系统类型**和**文件系统ID/名称**，并单击**确定**。

后续步骤

日志服务采集到NAS访问日志后，您可以执行查询分析、下载、投递、加工、创建告警等操作，详情请参见云产品日志通用操作。

4.10.3. 日志字段详情

本文介绍NAS访问日志的字段详情。

字段名称	说明
__topic__	日志主题，固定为nas_audit_log
ArgIno	文件系统inode号
AuthRc	授权返回码
NFSProtocolRc	NFS协议返回码
OpList	NFSv4 Procedures编号
Proc	NFSv3 Procedures编号
RWSize	读写大小，单位为字节
RequestId	请求ID
ResIno	lookup的资源inode号
SourceIp	客户端IP地址
User	阿里云账号ID
Vers	NFS协议版本号
Vip	服务端IP地址
Volume	文件系统ID

字段名称	说明
microtime	请求发生时间，单位为微秒

4.11. 高级管理FAQ

- 生命周期管理
  - 什么时候应该开启生命周期管理功能？
  - 为什么我的文件系统不支持生命周期管理功能？
  - 如何设置生命周期管理策略？
  - 如何选择生命周期管理策略，应该配置在哪个目录上？
  - 所有文件都可以转储到低频介质中吗？
  - 如果一个目录配置了多项生命周期管理策略，文件系统会执行哪一项策略？
  - 如果一个目录及其上层目录配置了不同的生命周期管理策略，文件系统会执行哪一项策略？
  - 生命周期管理策略是对目标路径所有数据生效吗？
  - 设置生命周期管理策略后，文件多久会被转储到低频介质？
  - 目录重命名会影响生命周期管理策略执行吗？
  - 删除生命周期管理策略会有什么影响？
  - 已设置生命周期管理策略的目录删除策略后，重新设置新的生命周期管理策略，会重复转储文件吗？
  - 文件存储在低频介质中可以正常读写吗？
  - 我的文件系统中有哪些文件存储在低频介质？
  - 低频介质中文件的读写延时比性能型NAS和容量型NAS高吗？
  - 文件转储到低频介质中，怎么收费？
  - 转储至低频介质的冷数据被访问后，会自动转为热数据吗？
  - 如何创建低频介质存储文件的数据取回任务？
  - 执行数据取回任务是否影响文件的读写性能？
  - 执行数据取回任务收费吗？
  - 备份低频介质中存储的文件时，怎么收费？
  - 安全服务扫描低频介质中存储的文件时，怎么收费？
- 管理权限
  - 创建经典网络挂载点时为什么需要RAM授权？
  - 如何获取AccessKey?
  - RAM用户拥有对文件系统完全控制权限后，进入文件系统列表为什么还报错误提示？
- 数据加密
  - 如何使用NAS的服务器端加密功能？
  - 未开启服务器端加密功能文件系统能否使用该功能？
  - 已开启服务器端加密功能的文件系统能否关闭该功能？
  - 是否可以更改加密文件系统的密钥？
  - 我该怎么选择NAS托管密钥和用户管理密钥？
  - 如果误操作禁用了CMK或误删了CMK，如何恢复对NAS文件系统中数据的访问？

- 开启服务器端加密功能后，每次访问数据需要应用进行解密操作吗？
- 开启服务器端加密功能会影响文件系统的性能吗？
- 文件系统开启服务器端加密且为静态加密类型，有效存储容量是否会缩小？

- 回收站
  - 我删除的文件都会暂存在回收站吗？
  - 文件系统目录名已变更，执行回收站文件恢复操作能恢复至原目录吗？
  - 从回收站中恢复文件和从备份服务中恢复文件，哪种方式恢复文件更快？
  - 使用回收站是否收费？
  - 怎么查询回收站中的文件？
  - 能否读写回收站中的文件？
- 备份和恢复文件
  - 文件存储NAS是否支持inotify？
  - 取消文件备份任务后，已备份的文件是否会被保留？
  - 使用文件备份功能时，取消文件恢复任务后，已恢复的文件是否会被保留？
  - NAS文件备份的免费期是怎么计算的？

什么时候应该开启生命周期管理功能？

当文件系统中包含每月访问频率低于2次的文件时，可以开启通用型NAS生命周期管理功能，符合生命周期管理策略的文件将自动转储至低频介质，采用低频介质计费方式，从而降低存储成本。

为什么我的文件系统不支持生命周期管理功能？

目前仅支持2020年06月01日后创建的通用型NAS文件系统开启生命周期管理功能并配置生命周期管理策略。已开启数据加密的文件系统暂不支持生命周期管理功能。2020年6月以前创建的文件系统如果需要使用生命周期管理功能，请提交工单咨询。

如何设置生命周期管理策略？

您可以通过NAS控制台或OpenAPI设置生命周期管理策略。具体操作，请参见设置生命周期策略和生命周期管理API。

如何选择生命周期管理策略，应该配置在哪个目录上？

为了方便您选择生命周期管理策略和需配置的目录，阿里云文件存储NAS提供了NAS分层策略分析工具。您可以使用该工具设置的生命周期管理策略，对指定目录及该目录下的子目录进行扫描并按照冷数据量降序排序，将指定目录中冷数据量最高的几个子目录打印出来。根据冷数据量来设置生命周期管理策略和需配置目录。更多信息，请参见使用指南。

所有文件都可以转储到低频介质中吗？

一个文件被转储到低频介质中需要满足以下三个条件：

- 文件所在目录配置了生命周期管理策略。
- 文件需大于或等于64 KB。
- 文件的最近访问时间需符合生命周期管理策略。

  创建生命周期管理策略时，可以配置管理规则，将距最近一次访问14天、30天、60天、90天以上的文件转换为低频存储文件。生命周期管理会依照文件的访问时间（即atime）来进行判断。

- 以下操作会更新访问时间：
  - 读取文件
  - 写入文件
- 以下操作不会更新访问时间：
  - 重命名一个文件
  - 修改文件的用户（user）、用户组（group）、模式（mode）等文件属性

如果一个目录配置了多项生命周期管理策略，文件系统会执行哪一项策略？

如果一个目录配置了多项生命周期管理策略，该目录下的文件只要满足任何一项生命周期管理策略的管理规则，就会被转储到低频介质中。

如果一个目录及其上层目录配置了不同的生命周期管理策略，文件系统会执行哪一项策略？

文件数据满足其任一策略规则目录下文件即会转储至低频介质中。

例如：当前目录配置了14天未访问转储的生命周期管理策略，其父目录或更上层目录配置了60天未访问转储的生命周期管理策略。那么目录中的14天未访问的文件会被转储至低频介质中，而父目录或更上层目录策略在扫描当前目录时，会跳过已转储至低频介质的文件。

生命周期管理策略是对目标路径所有数据生效吗？

是的。目标目录的所有文件数据只要满足生命周期管理策略，即会自动转储至低频介质中。

设置生命周期管理策略后，文件多久会被转储到低频介质？

转储时间会和文件系统的大小和转储数据量有关，功能开启后，符合生命周期管理策略的文件，第一次转储最快2个小时完成，一般在24小时内完成。后续周期性转储会在一周内某个时间完成。

目录重命名会影响生命周期管理策略执行吗？

生命周期管理策略中关联的目录被重命名后，目录下的文件将不再受原生命周期管理策略约束。已经转储至低频介质中的文件仍将维持存储状态。

当目录重命名后重新配置生命周期管理策略，则该目录下的文件会受该生命周期管理策略约束，符合生命周期管理规则的文件会被转储至低频介质中。

删除生命周期管理策略会有什么影响？

被删除的生命周期管理策略所关联目录下的文件将不会被转储至低频介质中。关联目录下已经转储至低频介质中的文件仍将维持当前存储状态。

已设置生命周期管理策略的目录删除策略后，重新设置新的生命周期管理策略，会重复转储文件吗？

不会。重新配置生命周期管理策略后，该策略通过检查机制跳过目录下已经被转储到低频介质中的文件，确保不会重复转储。

文件存储在低频介质中可以正常读写吗？

一个文件系统内的低频介质中的文件和其他普通文件一样可以被正常读写访问。

我的文件系统中有哪些文件存储在低频介质？

您可以通过NAS控制台或OpenAPI查询存储在低频介质中的文件。具体操作，请参见查看低频介质存储文件和ListDirectoriesAndFiles。

低频介质中文件的读写延时比性能型NAS和容量型NAS高吗？

第一次读低频介质中存储文件内容时可能延时会相对较高，但同一个文件内容在后续的一定时间内的读延时会与性能型NAS或容量型NAS普通文件的读延时基本一致。

写低频存储文件的延时与写性能型NAS或容量型NAS文件基本一致。

文件转储到低频介质中，怎么收费？

当文件转储到低频介质中，会采用低频介质的计费方式。更多信息，请参见低频介质计费说明。

转储至低频介质的冷数据被访问后，会自动转为热数据吗？

不会。数据一旦转储至低频介质，将持续存储在低频介质中。访问低频介质中的冷数据将产生低频介质读写流量费用。更多信息，请参见低频介质计费说明。

如果需要频繁访问低频介质中的文件，请您创建数据取回任务将冷数据转为热数据。具体操作，请参见创建数据取回任务。

如何创建低频介质存储文件的数据取回任务？

您可以通过NAS控制台或OpenAPI创建数据取回任务。具体操作，请参见创建数据取回任务和CreateLifecycleRetrieveJob。

执行数据取回任务是否影响文件的读写性能？

不影响，执行数据取回任务时可以正常读写数据。

执行数据取回任务收费吗？

收费。执行数据取回任务时，需要读取目标文件中的数据，将按照目标文件大小收取低频介质读流量费用。数据取回任务完成后，文件占用通用型NAS存储容量，将按照文件大小收取通用型NAS文件系统存储容量费用。更多信息，请参见低频介质计费说明。

备份低频介质中存储的文件时，怎么收费？

当您使用混合云备份（HBR）服务备份通用型NAS低频介质中的文件时，HBR会收取相应的服务费用。更多信息，请参见计费方式与计费项。

在备份低频介质中的文件时，备份服务需要读取目标文件中的数据，文件存储NAS将收取低频介质访问流量费用。更多信息，请参见低频介质计费说明。

安全服务扫描低频介质中存储的文件时，怎么收费？

当您使用安全服务（例如云安全中心的防勒索服务）扫描通用型NAS低频介质中的文件时，安全服务会读取目标文件中的数据，文件存储NAS将收取低频介质访问流量费用。更多信息，请参见低频介质计费说明。

创建经典网络挂载点时为什么需要RAM授权？

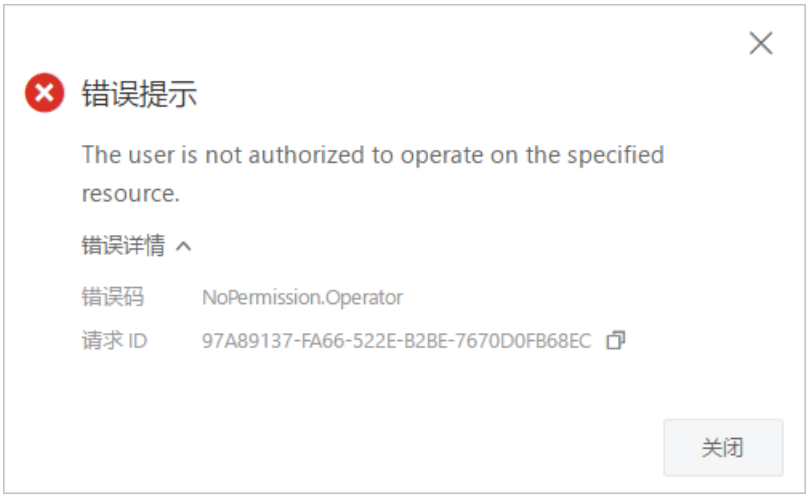
因为NAS需要被授权来对访问您的文件系统的ECS实例进行验证。为确保您的文件系统数据安全，NAS只允许属于您自己的ECS实例通过经典网络挂载点访问您的文件系统，即文件系统实例的账号与ECS实例的账号相同。为了验证访问您的文件系统的ECS实例，您需要通过RAM授权授予NAS获取您的ECS实例列表的权限。

> 注意
>
> - 通过RAM授权后，NAS仅有权限调用DescribeInstances接口的权限，无法调用其他任何接口；NAS通过DescribeInstances接口获取的ECS实例列表不会做任何形式的记录，仅用于权限验证。
> - 通过RAM授权后，请勿删除或编辑RAM中的AliyunNASDefaultRole角色，否则可能遇到无法挂载或文件系统操作异常。

RAM用户拥有对文件系统完全控制权限后，进入文件系统列表为什么还报错误提示？

- 问题现象：

  RAM用户在拥有对文件系统完全控制权限后，登录控制台进入文件系统列表页面时报错。

- 问题原因：

  未配置标签权限。您还需要配置 `tag:ListTagKeys` 权限。

- 解决方案：

  在自定义策略中为目标文件系统增加标签权限。具体操作，请参见使用RAM权限策略控制NAS访问权限。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "nas:*",
            "Resource": "acs:nas:*:*:filesystem/0ddaf487b2"
        },
        {
            "Effect": "Allow",
            "Action": "nas:CreateMountTarget",
            "Resource": "acs:vpc:*:*:vswitch/*"
        },
        {
            "Effect": "Allow",
            "Action": "cms:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "nas:DescribeFileSystems",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "tag:ListTagKeys",
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

如何获取AccessKey?

1. 以阿里云账号登录阿里云控制台。
2. 将鼠标置于页面右上方的账号图标，单击**AccessKey管理**。
3. 在**安全提示**对话框中，选择获取阿里云账号AccessKey还是RAM用户AccessKey。
   - 获取阿里云账号AccessKey。
     a. 单击**继续使用AccessKey**。
     b. 在**安全信息管理**页面，单击**创建AccessKey**。
     c. 在**手机验证**页面，获取验证码，完成手机验证，单击**确定**。
     d. 在**新建用户AccessKey**页面，查看AccessKey ID和AccessKey Secret信息。
        您可以单击**保存AK信息**，下载AccessKey信息。
   - 获取RAM用户AccessKey。
     a. 单击**开始使用子账户AccessKey**。
     b. 在RAM访问控制控制台的**新建用户**页面，创建用户。
        如果是获取已有RAM用户的Accesskey，则跳过此步骤。
     c. 在RAM访问控制控制台的左侧导航栏，选择**人员管理 > 用户**，找到需获取AccessKey的用户。

d. 单击用户登录名称，在**认证管理**页签下的**用户AccessKey**区域，单击**创建新的AccessKey**。

> **说明**
> - 最多可以创建2个AccessKey。
> - 创建AccessKey后，无法再通过控制台查看AccessKey Secret，请您妥善保存AccessKey Secret，谨防泄露。

e. 在**手机验证**页面，获取验证码，完成手机验证，单击**确定**。

f. 在**新建用户AccessKey**页面，查看AccessKey ID和AccessKey Secret信息。

您可以单击**下载CSV文件**或单击**复制**，保存AccessKey信息。

如何使用NAS的服务器端加密功能？

您可以在创建文件系统时，根据使用场景配置加密方式为**NAS托管密钥**或**用户管理密钥**。具体操作，请参见通过控制台创建通用型NAS文件系统和通过控制台创建极速型NAS文件系统。

未开启服务器端加密功能文件系统能否使用该功能？

不能。目前仅支持在创建文件系统时开启服务器端加密功能。

已开启服务器端加密功能的文件系统能否关闭该功能？

不能。服务器端加密功能开启后立即生效，不支持关闭。

是否可以更改加密文件系统的密钥？

不可以。创建文件系统时已绑定密钥，不支持更改。

我该怎么选择NAS托管密钥和用户管理密钥？

两种密钥的管理方式均为将密钥托管给KMS服务，并采用信封加密机制防止未经授权的数据访问。

当您有特定安全需求需要使用自带密钥BYOK时，请选择用户管理密钥，其他场景推荐使用NAS托管密钥。

> **注意** 使用用户管理密钥时，若该密钥被禁用或者删除，将导致使用该密钥进行加密的NAS文件系统无法访问。

如果误操作禁用了CMK或误删了CMK，如何恢复对NAS文件系统中数据的访问？

- 若禁用了CMK，请您重新启用目标CMK。
- 若已对目标密钥执行计划删除操作，请您撤销删除密钥申请。具体操作，请参见计划删除密钥。
- 若删除了自带密钥BYOK的密钥材料，请您重新上传原密钥材料。具体操作，请参见导入密钥材料。
- 若目标CMK已删除，则无法修复，将无法访问文件系统中的数据。

开启服务器端加密功能后，每次访问数据需要应用进行解密操作吗？

不需要。数据加解密过程将由NAS服务自动处理，您不需要修改任何应用程序。

开启服务器端加密功能会影响文件系统的性能吗？

开启服务器端加密功能后，NAS会对写入文件系统的数据进行加密，读取文件系统中的数据时将自动解密。文件系统读写性能主要受每次读写操作中读写块的大小影响。相较于未开启服务器端加密的同规格类型文件系统，开启服务器端加密的文件系统性能约下降5%~25%。更多信息，请参见文件系统的读写性能与什么相关。

文件系统开启服务器端加密且为静态加密类型，有效存储容量是否会缩小？

文件系统有效容量不会缩小。AES属于分组加密，遵循自动补位机制，静态加密自动补位的数据不计算在文件系统实例的有效存储容量中。

文件存储NAS是否支持inotify？

使用inotify配合rsync是一种常见的实时数据备份、同步方案，由于inotify本身的实现机制会导致NAS文件系统上inotifywait无法正常工作。

- inotifywait原理简介

  inotifywait是Linux内核子模块inotify的用户态接口实现，inotify实现在VFS层。当文件操作到达VFS层时，inotify模块会将操作类型（创建、删除、属性改变等）和操作对象（文件名）反馈给用户态，用户态的inotifywait即可将本次操作信息输出给用户。

- NAS上使用inotifywait存在的问题

  由于inotify是在Kernel的VFS层实现的，因此在NFS文件系统上，远程客户端对NFS文件系统的操作无法被本地Kernel所感知，inotify也就无法感知远程客户端的文件修改操作。因此，在NAS上使用inotifywait时，例如在客户端A和B同时挂载一个NAS文件系统，在客户端A启动inotifywait监听挂载目录，会出现以下现象：

  - 在客户端A上操作挂载目录中的文件，可以被inotifywait感知。
  - 在客户端B上操作挂载目录中的文件，inotifywait无法感知任何文件操作。

- 替代方案

  替代方案为使用FAM。FAM是一个用来监听文件或目录的库，均在用户态实现，原理为在后台运行一个daemon，定时扫描目录，获取文件变化情况。但是使用FAM存在以下几个缺陷：

  - 需要用户在客户端编写程序调用FAM接口实现功能。
  - 对于文件数目很多的场景，使用该方案性能会较差，可能消耗大量资源，无法做到很好的实时性。

取消文件备份任务后，已备份的文件是否会被保留？

当您取消备份任务后，该任务中所有已备份文件均会被清理，不会保留在备份库中。如您有需要，请重新执行备份任务。

使用文件备份功能时，取消文件恢复任务后，已恢复的文件是否会被保留？

当您取消文件恢复任务后，该任务中已恢复的文件将保存在指定目录中，任务中其他文件将不再被恢复。

NAS文件备份的免费期是怎么计算的？

对任一NAS文件系统，您首次创建备份计划开始后的30天内，将可免费试用文件备份功能。

例如，2021年5月1日，您为文件系统A创建一个备份计划backup01，直至2021年5月30日，您都可以免费试用文件备份功能。试用到期后，您可以转付费继续使用或删除该备份计划。更多信息，参见混合云备份计费说明。

我删除的文件都会暂存在回收站吗？

开启回收站后，被删除的文件或目录将暂存在回收站中，包括但不限于：

- 您在ECS、容器等计算节点上手动删除的NAS中的文件。例如手动执行 `rm -f test01.text` 命令删除文件*test01.text*，文件*test01.text*将进入回收站。
- 使用应用程序在计算节点上自动删除的NAS中的文件或目录。例如Python使用 `os.remove("test02.text")` 删除文件*test02.text*，文件*test02.text*将进入回收站。
- POSIX rename触发删除的文件或目录。例如同一目录存在文件*test_a.txt*和文件*test_b.txt*，执行 `mv test_a.txt test_b.txt` ，文件*test_b.txt*将进入回收站。
- 应用程序使用NAS文件产生的临时文件。例如执行vim命令编辑文件时，产生的 `.swp` 和 `.swpx` 格式的文件将进入回收站。
- 应用程序自动轮转的日志文件。例如使用Nginx配置了自动轮转日志且最多保留20个日志文件，当日志文件*test.log.19*轮转为日志文件*test.log.20*时，原日志文件*test.log.20*将进入回收站。

> **说明** 如果仅覆写文件内容，不删除该文件，不会触发文件进入回收站。例如调用 `open()` 函数以 `w+` 模式打开文件并写入，原始文件不会进入回收站。

文件系统目录名已变更，执行回收站文件恢复操作能恢复至原目录吗？

执行文件恢复任务时可以选择将回收站内的文件恢复至原目录中，恢复操作以原目录的 `FileId` 作为标识，原目录重命名后同样会被正确识别，并恢复至重命名后的新路径。例如，开启回收站功能后，删除目录*dir1*中的文件*file1.txt*，然后将目录名称*dir1*改为了*dir2*，在NAS控制台回收站中可以查询到文件*file1.txt*在目录*dir2*中，执行文件恢复任务后，在计算节点查询文件*file1.txt*在目录*dir2*中。

从回收站中恢复文件和从备份服务中恢复文件，哪种方式恢复文件更快？

从回收站中恢复文件，文件存储NAS只需要迁移文件的元数据，不需要拷贝数据，因此从回收站恢复文件的速度会明显快于从备份服务中恢复文件的速度。

使用回收站是否收费？

使用回收站功能免费，但回收站中暂存的文件会按照原存储类型收取存储费用。例如，删除容量型文件系统的文件后，该文件将按照容量型存储容量单价计费；删除低频介质的文件后，该文件将按照低频介质存储容量单价计费。更多信息，请参见通用型NAS计费说明和低频介质计费说明。暂存的文件删除前存储在容量型文件系统中则按照容量型存储容量单价计费。

怎么查询回收站中的文件？

您可以通过NAS控制台查询暂存在回收站中的文件及文件删除时间等信息。具体操作，请参见查询回收站中的文件。

能否读写回收站中的文件？

只能查询已删除的文件或目录，不能读写已删除的文件或目录。当开启回收站功能后，已删除的文件将暂存在回收站中，如果您需要读写回收站中的文件，请执行文件恢复操作，恢复完成的文件可以正常读写。具体操作，请参见恢复回收站中的文件。

5.常见问题

产品简介FAQ

- 什么是文件存储NAS?
- 文件存储NAS支持哪些访问协议?
- 如何选择NFS和SMB文件系统协议?
- 每个账户可以创建多少个文件系统、文件系统有什么限制?
- 更多产品简介常见问题

产品定价FAQ

- 开通NAS服务后，就开始计费吗?
- 购买了存储包为什么还会欠费?
- 存储包和存储容量有什么关系?
- 如何查看是否欠费?
- 更多产品定价常见问题

挂载访问FAQ

- Linux挂载NFS文件系统常见问题
- Windows挂载SMB文件系统常见问题
- Linux挂载SMB文件系统常见问题
- Windows挂载NFS文件系统常见问题
- 为什么卸载旧NAS并重新挂载新NAS后，容器Pod仍将数据写入旧NAS?
- 更多挂载访问常见问题

性能测试FAQ

- 文件系统的读写性能与什么相关?
- 为什么使用Nginx写日志到文件系统耗时很长?
- 如何提升IIS访问NAS的性能?
- 为什么Linux操作系统上NFS客户端运行性能差?
- 更多性能测试常见问题

基础管理FAQ

- 为什么在创建文件系统时，会显示库存不足?
- 挂载点是否可以转换类型?
- 每个账号可以创建多少个文件系统、文件系统有什么限制?
- 挂载点是什么？有什么作用?
- 更多基础管理常见问题

高级管理FAQ

- 什么时候应该开启生命周期管理功能?
- 文件存储在低频介质中可以正常读写吗?

- 创建经典网络挂载点时为什么需要RAM授权？
- 文件存储NAS是否支持inotify？
- 更多高级管理常见问题