阿里云
文件存储

用户指南

文档版本：20200709

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. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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
	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。	 **禁止：** 重置操作将丢失用户配置数据。
	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。
	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。
	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。	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 管理权限

1.1 使用RAM实现用户访问控制

您可以创建RAM用户用于管理NAS用户身份与资源访问控制服务，降低云账户信息安全风险。

背景信息

RAM允许在一个云账户（主账户）下创建并管理多个RAM用户，并允许给RAM用户分配不同的授权策略，从而实现不同RAM用户拥有不同的云资源访问权限。使用RAM还可以让您避免与其他用户共享云账号密钥（AccessKey），按需为用户分配最小权限，从而降低您的企业信息安全风险。

创建RAM用户

1. 使用主账号登录 RAM访问控制台。
2. 在左侧导航栏中，选择**人员管理** > **用户**，单击**创建用户**。
3. 配置用户账号信息。
4. 配置访问方式，选中**控制台登录密码**和**编程访问**。
5. 选中**自定义登录密码**，输入一个初始密码，并选中**用户在下次登录时必须重置密码**。
6. （可选）启动多因素认证设备，单击**确定**。
7. 保存生成的账号、密码、AccessKeyID和AccessKeySecret。

> **说明:**
> 请及时保存该 AccessKey 信息，并妥善保管。

创建用户组

如果您需要创建多个RAM用户，您可以选择通过创建用户组对职责相同的RAM用户进行分类并授权，从而更方便地管理用户及其权限。

1. 使用主账号登录 RAM访问控制台。
2. 在左侧导航栏中，选择**人员管理** > **用户组**，单击**创建用户组**。
3. 填写用户组名称和显示名称，单击**确认**。

为RAM用户或用户组分配授权策略

新建的RAM用户或用户组默认没有任何操作权限，只有在被授权策略之后，才能通过控制台和API操作资源。此处以RAM用户为例，介绍授权操作步骤。

阿里云系统权限策略提供两种NAS策略，您可以根据需求为子账号授权。

- AliyunNASFullAccess：管理文件存储服务（NAS）的权限
- AliyunNASReadOnlyAccess：查看文件存储服务（NAS）的权限

> **说明：**
> 由于系统权限策略的授权粒度比较粗，如果这种粗粒度权限策略不能满足您的需求，您可以创建自定义权限策略，详情请参见创建自定义权限策略。

1. 在**用户**页面，选择要授权的子账号，单击**添加权限**。
2. 在**添加权限**页面，选择NAS权限，为子账号授权。

1.2 创建自定义权限策略

本文介绍如何创建及授权自定义权限策略。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。

前提条件

已创建RAM用户或用户组，详情请参见使用RAM实现用户访问控制。

操作步骤

1. 使用主账号登录 RAM访问控制台。
2. 在左侧导航栏中，选择**权限管理** > **权限策略管理**，单击**创建权限策略**，根据页面提示，创建策略。此处以创建查看NAS资源的权限策略（NASReadOnlyAccess）为例。 脚本语法的详细介绍请参见#unique_6。

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

NAS操作的权限如下表所示。

操作（Action）	说明
DescribeFileSystems	列出文件系统实例
DescribeMountTargets	列出文件系统挂载点
DescribeAccessGroup	列出权限组
DescribeAccessRule	列出权限组规则

操作（Action）	说明
CreateMountTarget	为文件系统添加挂载点
CreateAccessGroup	创建权限组
CreateAccessRule	添加权限组规则
DeleteFileSystem	删除文件系统实例
DeleteMountTarget	删除挂载点
DeleteAccessGroup	删除权限组
DeleteAccessRule	删除权限组规则
ModifyMountTargetStatus	禁用或激活挂载点
ModifyMountTargetAccessGroup	修改挂载点权限组
ModifyAccessGroup	修改权限组
ModifyAccessRule	修改权限组规则

NAS可访问的资源如下表所示。

资源（Resource）	注解
*	所有文件存储NAS资源

3. 创建成功后，返回**用户**页面。
4. 选择要授权的子账号，单击**添加权限**，选择NAS权限，为子账号授权。

1.3 管理权限组

本文介绍如何在NAS控制台上管理权限组，包括创建权限组和规则、查看权限组列表、查看规则列表、删除权限组、删除规则等。

背景信息

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

初始情况下，每个账号都会自动生成一个默认权限组，该默认权限组允许任何IP地址以最高权限（读写且不限制root用户）访问文件系统。

说明：

- 为了最大限度保障您的数据安全，强烈建议您谨慎添加权限组规则，仅为必要的地址授权。
- 不可删除或编辑默认权限组及其规则。

- 一个阿里云账号最多可以创建10个权限组。

创建权限组和规则

1. 登录NAS控制台。
2. 创建权限组。

   a) 在左侧导航栏，选择**文件系统** > **权限组** > **通用型NAS**，单击**创建权限组**。

   > **说明:**
   > 如果您要创建极速型NAS的权限组，请进入**文件系统** > **权限组** > **极速型NAS**页面，进行操作。

   b) 在**新建权限组**页面，配置相关信息。

重要参数说明如下所示。

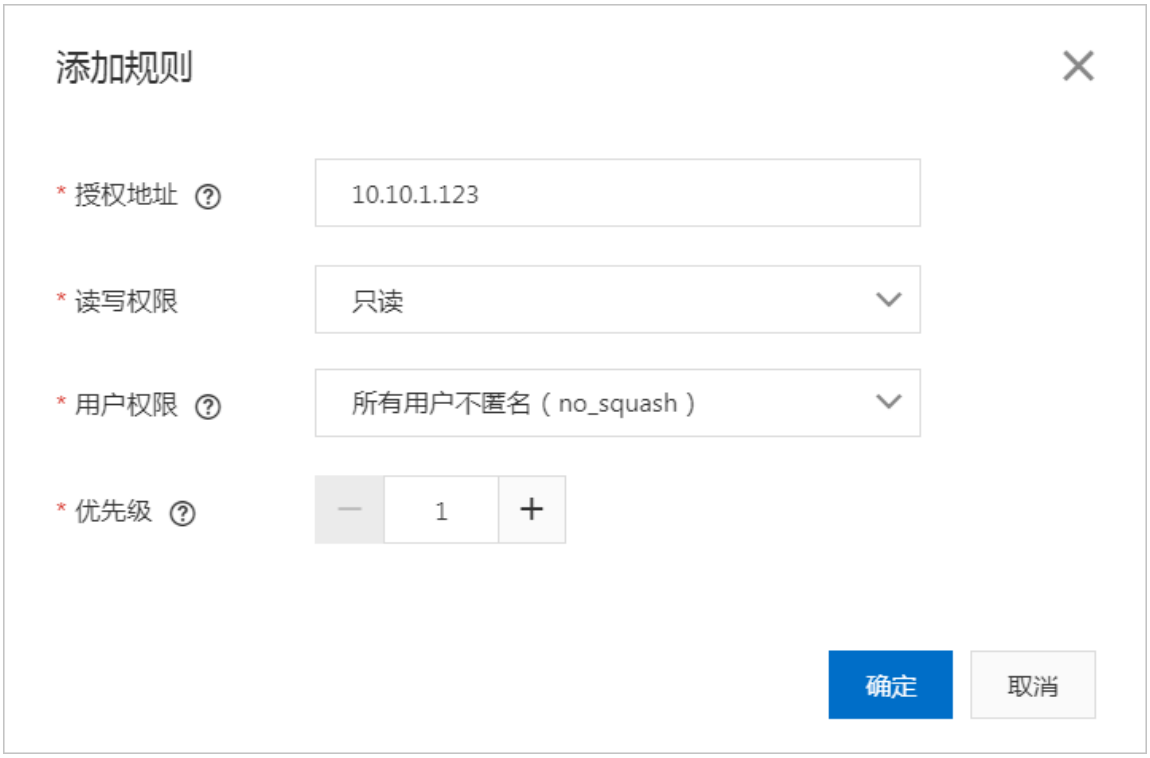
参数	说明
名称	设置权限组名称。
网络类型	包括专有网络和经典网络。 **说明:** 极速型NAS只支持专有网络类型的权限组。

3. 添加权限组规则。

   a) 找到目标权限组，单击**管理规则**。

   b) 在**权限组规则**页面，单击**添加规则**。

   c) 配置规则信息。



参数	说明
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**。

参数	说明
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。 • **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1~100，1为最高优先级。

d) 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。
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。

1.4 NAS SMB ACL

1.4.1 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：

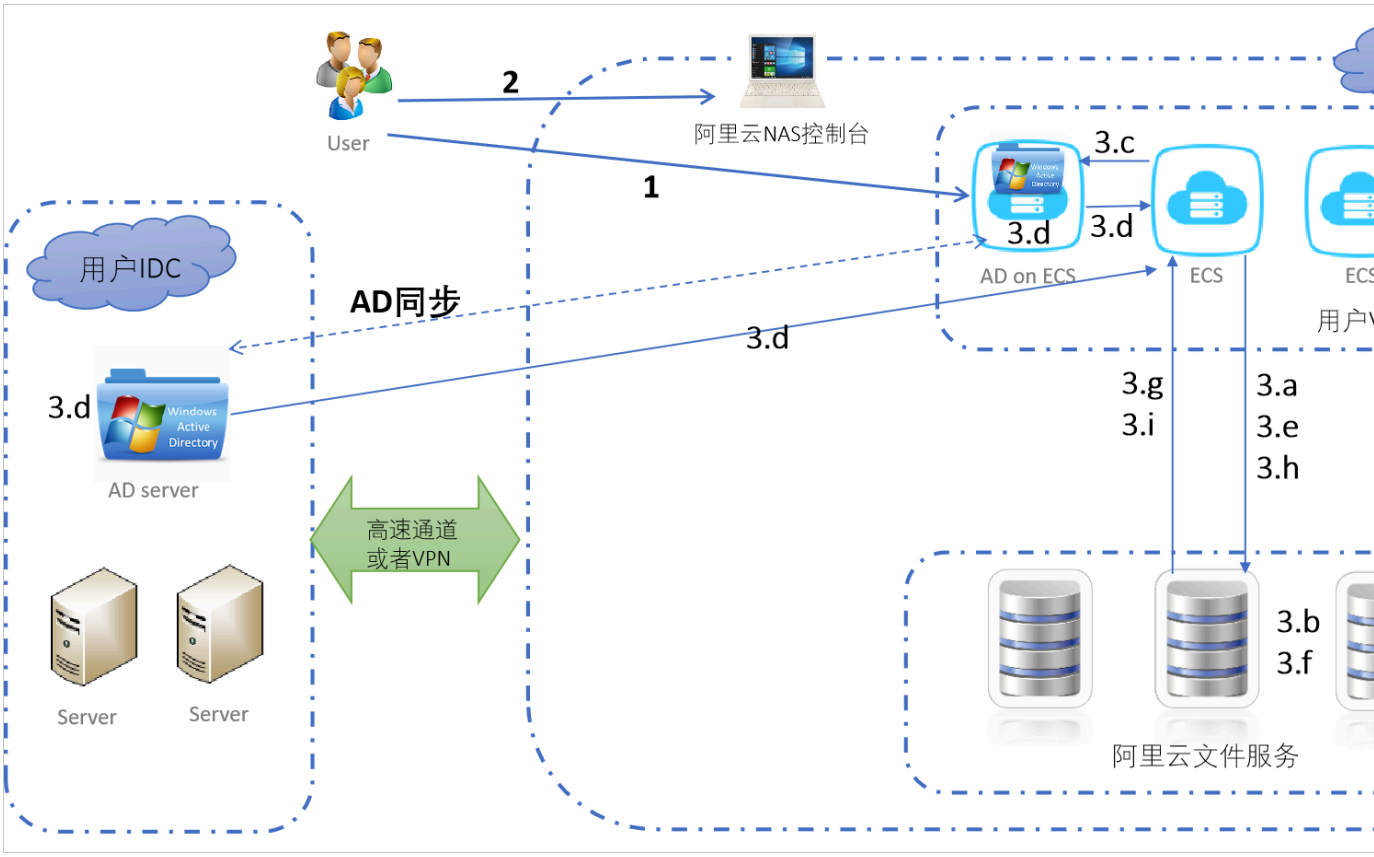
您可以在NAS控制台开启SMB AD ACL功能，如果您有其他问题，请提交工单。

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，详情请参见创建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。

   详情请参见将阿里云SMB协议文件系统挂载点接入AD域。

   a) 创建阿里云NAS文件系统的服务账号。

   b) 注册NAS文件系统挂载点域名。

   c) 为NAS文件系统挂载点服务生成Keytab密钥表文件。

   d) 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。

   a. 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。
   b. 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。
   c. 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。
   d. 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。
   e. 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。
   f. 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。
   g. 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。
   h. 应用向文件系统发出文件系统访问，读写及其它请求。
   i. 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。

1.4.2 将阿里云SMB协议文件系统挂载点接入AD域

本方介绍将阿里云SMB文件系统挂载点接入AD域内，实现以AD域的用户身份对用户身份的认证和文件级别的权限访问控制。

背景信息

在以特定AD域中的用户身份来挂载使用SMB协议的阿里云文件存储NAS文件系统之前，需要先在AD域内为相应的NAS文件系统注册服务，生成并上传Keytab密钥表文件。

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。
- 已创建SMB文件系统，详情请参见创建SMB文件系统。

操作步骤

1. 创建阿里云NAS文件系统在用户AD域内的服务账号。

   使用dsadd命令行工具为NAS在AD域中添加服务账号，比如命名为alinas。使用dsadd工具的Powershell命令模板如下所示。

   ```
   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
   ```

   命令范例如下所示。

   ```
   dsadd user CN=alinas,DC=MYDOMAIN,DC=com -samid alinas -display "Alibaba Cloud NAS Service Account" -pwd tHePaSsWoRd123 -pwdneverexpires yes
   ```

2. 注册NAS文件系统挂载点域名。

   使用setspn命令行工具在NAS服务账号名下为单个NAS文件系统挂载点注册添加服务主体。使用setspn工具的Powershell命令模板如下所示。

   ```
   setspn -S cifs/[SMB协议NAS文件系统挂载点] [AD服务账号名]
   ```

   命令范例如下所示。

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

3. 为NAS文件系统挂载点服务生成Keytab密钥表文件。

   使用ktpass命令行工具为NAS文件系统挂载点服务主体生成Keytab密钥表文件，实现NAS进行用户身份认证。使用ktpass工具的Powershell命令模板如下所示。

   ```
   ktpass
    -princ cifs/[SMB协议NAS文件系统挂载点域名]
    -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]
   ```

   命令范例如下所示。

   ```
   ktpass -princ cifs/nas-mount-target.nas.aliyuncs.com@MYDOMAIN.com -ptype KRB5_NT_PRINCIPAL -crypto All -out c:\nas-mount-target.keytab -pass tHePaSsWoRd123
   ```

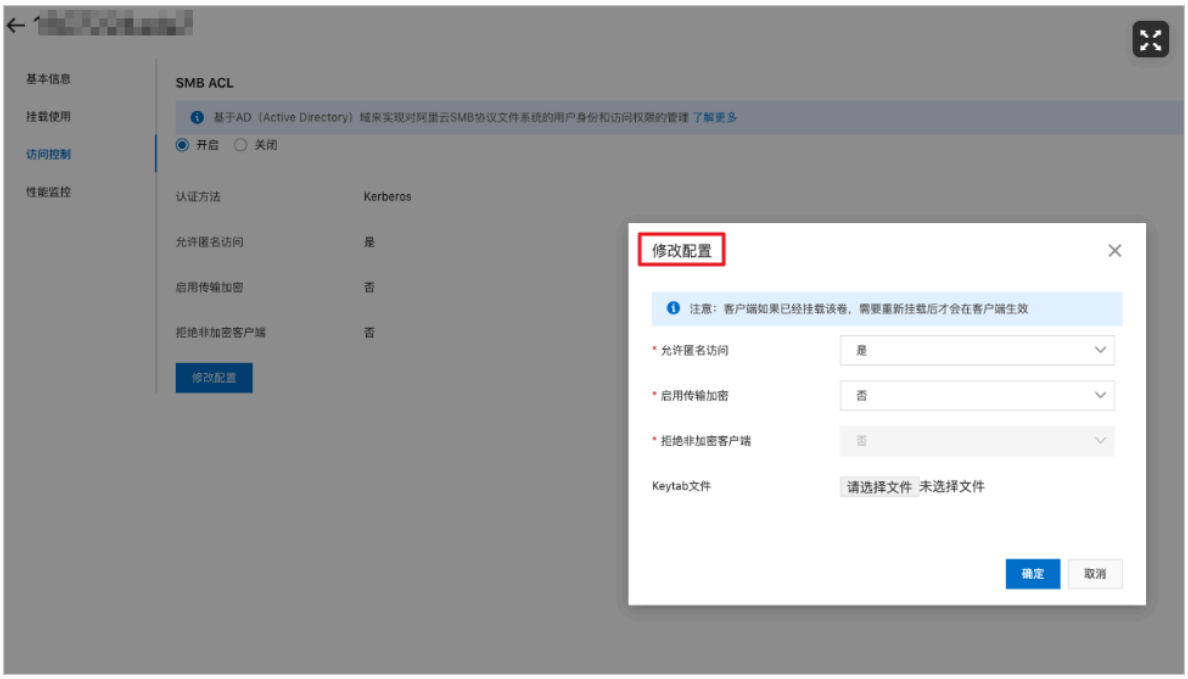
4. 下载阿里云文件系统服务账号的keytab。

   根据**ktpass工具的Powershell命令**中设置的文件路径，下载keytab文件。

5. 上传阿里云文件系统服务账号的Keytab文件。

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**。在**访问控制**区域，单击**开启**，并上传阿里云文件系统服务账号的Keytab文件。

在SMB ACL功能开启之后，当前界面会显示以下参数信息。单击**修改配置**可以对参数进行修改。



参数	是否可修改	描述
认证方式	否	默认值为：Kerberos。
允许匿名访问	是	如果允许匿名访问，则允许任何人以NTLM方式挂载该卷。挂载后身份为Everyone，ACL将继续起作用。 默认值为：否。
启用传输加密	是	是否开启SMB3传输加密功能。 默认值为：否。

参数	是否可修改	描述
拒绝非加密客户端	是	是否拒绝不支持加密的客户端。 启动**传输加密**时才可选择。 默认值为：否。
Keytab文件	是	上传Keytab文件。 单击**修改配置**后才可显示此参数。

说明:

在**修改配置**界面，客户端如果已经挂载该卷，需要重新挂载后才能在客户端生效。

预期结果

阿里云SMB文件系统挂载点接入到了AD域内。在完成AD域接入之后，用户可以开始以AD域用户身份挂载使用阿里云SMB协议文件系统。

1.4.3 将Windows系统服务器加入AD域

本文介绍了如何在Windows服务器配置AD域DNS信息和加入AD域的方法，以便在Windows服务器中使用AD域身份挂载SMB协议文件系统。

背景信息

加入AD域的Windows服务器可以使用AD域完成身份验证挂载SMB文件系统。如果Windows服务器没有加入AD域，而您希望以AD域账号来挂载NAS SMB文件系统，需要修改DNS到AD Server，这样才能找到AD域完成身份验证。

步骤一：设置DNS Server地址

一台Windows机器在加入AD域之前，需要先设置一个记录有AD域控制器地址的DNS服务器地址。一般情况下，AD域控制器也兼有DNS服务器的角色，这种情况下将机器的DNS地址设为AD域服务控制器的IP地址。如果Windows服务器与AD域服务控制器（同一个VPC里）都是阿里云ECS实例，推荐使用ECS实例的内网IP地址。

您可以通过以下Windows系统（以Windows Server 2012版系统为例）路径来设置DNS Server地址：

1. 进入**控制面板** > **网络和Internet** > **网络与共享中心**。
2. 在**网络与共享中心**页面**查看活动网络**区域，单击**以太网**。
3. 在**以太网状态**页面，单击**属性**。

4. 在**以太网属性**页面**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**。
5. 在**Internet协议版本4（TCP/IPv4）属性**页面，选中**使用下面的DNS服务器地址**，设置DNS Server地址为AD域服务控制器的IP地址。

说明：

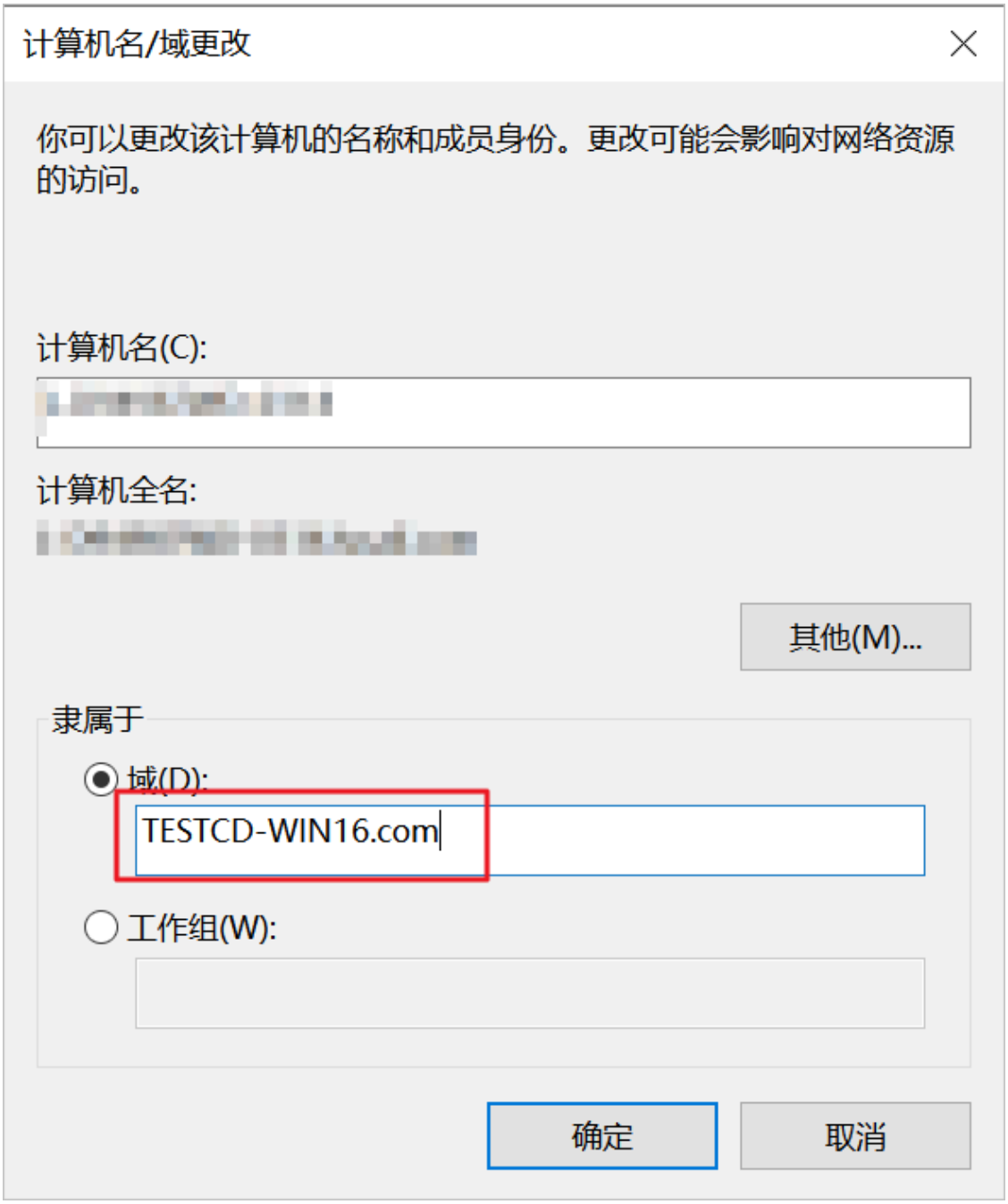
设置DNS后，在新的Windows机器用CMD命令行执行net use z: \\nas-mount-target.nas.aliyuncs.com\myshare /user:MYDOMAIN.com\USERNAME PASSWORD命令，以AD域身份挂载NAS SMB文件系统。

步骤二：加入AD域

在设置完成DNS服务器地址之后，您可以通过以下Windows系统（以Windows Server 2012版系统为例）路径来加入AD域：

1. 进入**控制面板** > **系统和安全** > **系统**。
2. 在**系统**页面**计算机名、域和工作组设置**区域，单击**更改设置**。
3. 在**系统属性**页面的**计算机名**页签，单击**更改**。

4. 在更改页面**隶属于** > **域**区域，填写已有的AD域信息。根据界面提示，单击**确定**完成配置。



5. 重启服务器，并生效配置。

说明:

机器加入AD域之后，您以AD身份登录该机器，就可以直接使用net use z: \\nas-mount-target.nas.aliyuncs.com\myshare，以AD域身份进行挂载，不需要输入 /user:MYDOMAIN.com\USERNAME 。

1.4.4 从Windows以AD域用户身份挂载并使用阿里云SMB协议文件系统

本文介绍了在Windows操作系统下，用户如何以AD域身份挂载阿里云SMB协议文件系统。以及在挂载成功后，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

已将SMB文件系统挂载点接入AD域，详情请参见将阿里云SMB协议文件系统挂载点接入AD域。

背景信息

阿里云SMB文件系统在接入AD域之前，只支持以匿名方式来挂载。以Everyone用户的身份和权限来使用文件系统。当一个SMB文件系统开通AD认证功能之后，用户可以设置是否继续允许匿名挂载访问。

- 如果继续允许匿名访问文件系统，设备可以通过Kerberos认证以域身份使用文件系统，也可以通过NTLM认证以Everyone身份使用文件系统。
- 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设备通过Kerberos认证协议以域用户身份进行挂载。

说明：
请使用Windows系统的命令行工具（cmd）运行本文中提供的命令。

一、用net use命令行工具挂载使用SMB文件系统

使用net use工具进行文件系统挂载的CMD命令模板如下所示。

```
net use [可用的目标盘符] [SMB挂载点域名]
```

命令范例如下所示。

- 已加入AD域的设备可以用以下命令挂载。

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

- 未加入AD域的设备可以用以下命令挂载。

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

NAS用户基于net use命令行工具的挂载命令来挂载文件系统。该模式下，用户可以正常访问文件系统，查看文件或目录的ACL，但不能编辑ACL。

二、用mklink命令行工具使用SMB文件系统

用户可以用mklink命令行工具，在Windows本地盘下，为SMB文件系统挂载点生成符号链接。

说明：

mklink命令无法通过powershell使用，只能用命令提示符。

使用mklink工具进行文件系统映射的CMD命令模板如下所示。

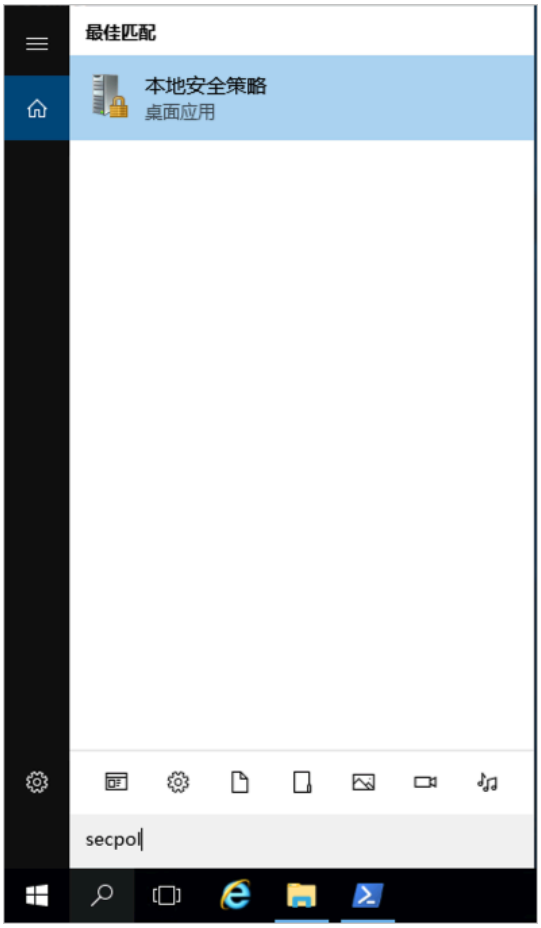
```
mklink /D [符号链接的文件系统路径] [SMB协议NAS文件系统挂载点域名]
```

命令范例如下所示。

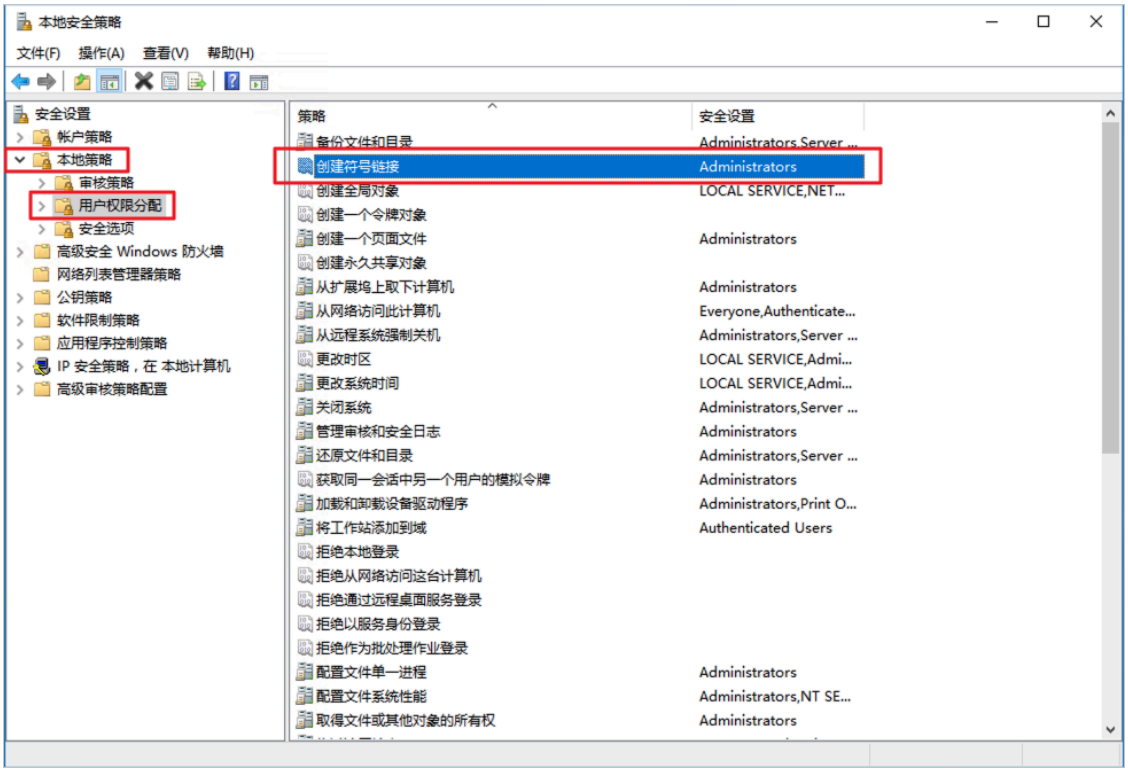
```
mklink /D c:\myshare \\nas-mount-target.nas.aliyuncs.com\myshare
```

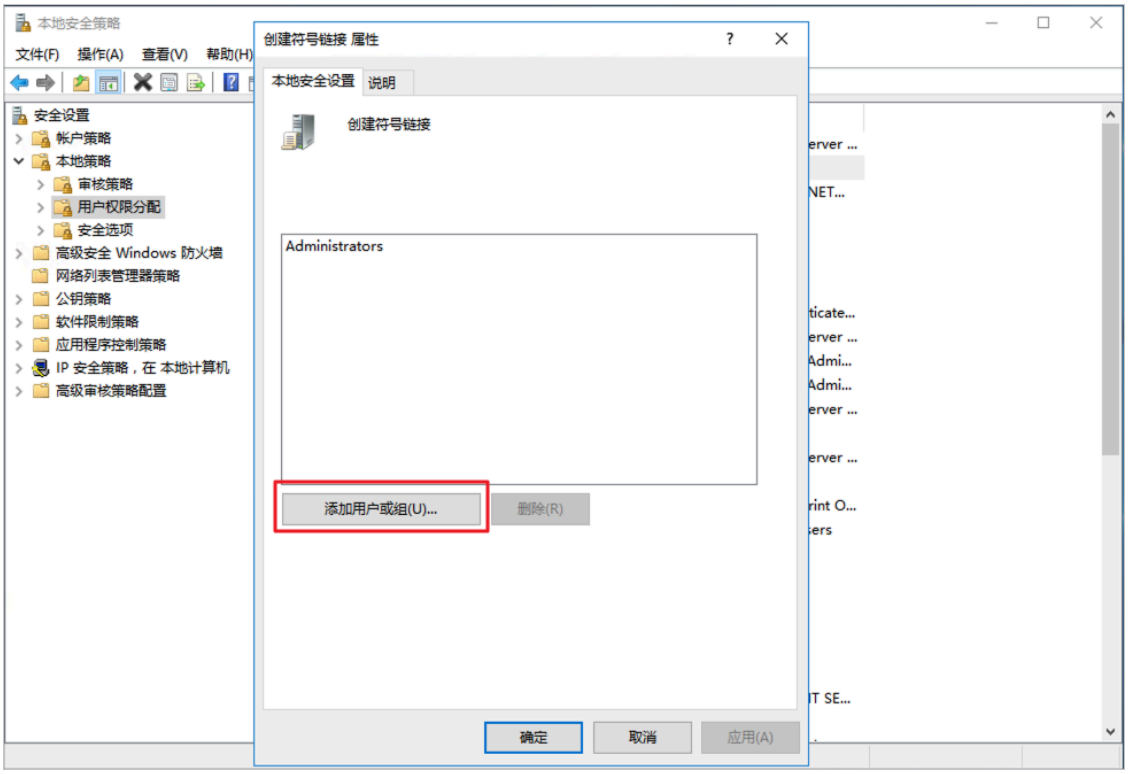
默认情况下，Windows系统只有系统管理员Administrator可以创建符号链接。如果普通用户需要创建符号链接，需要由管理员为该用户添加权限。

1. 以管理员权限搜索并运行secpol.msc。



2. 将指定用户加入**创建符号链接**的权限组中。





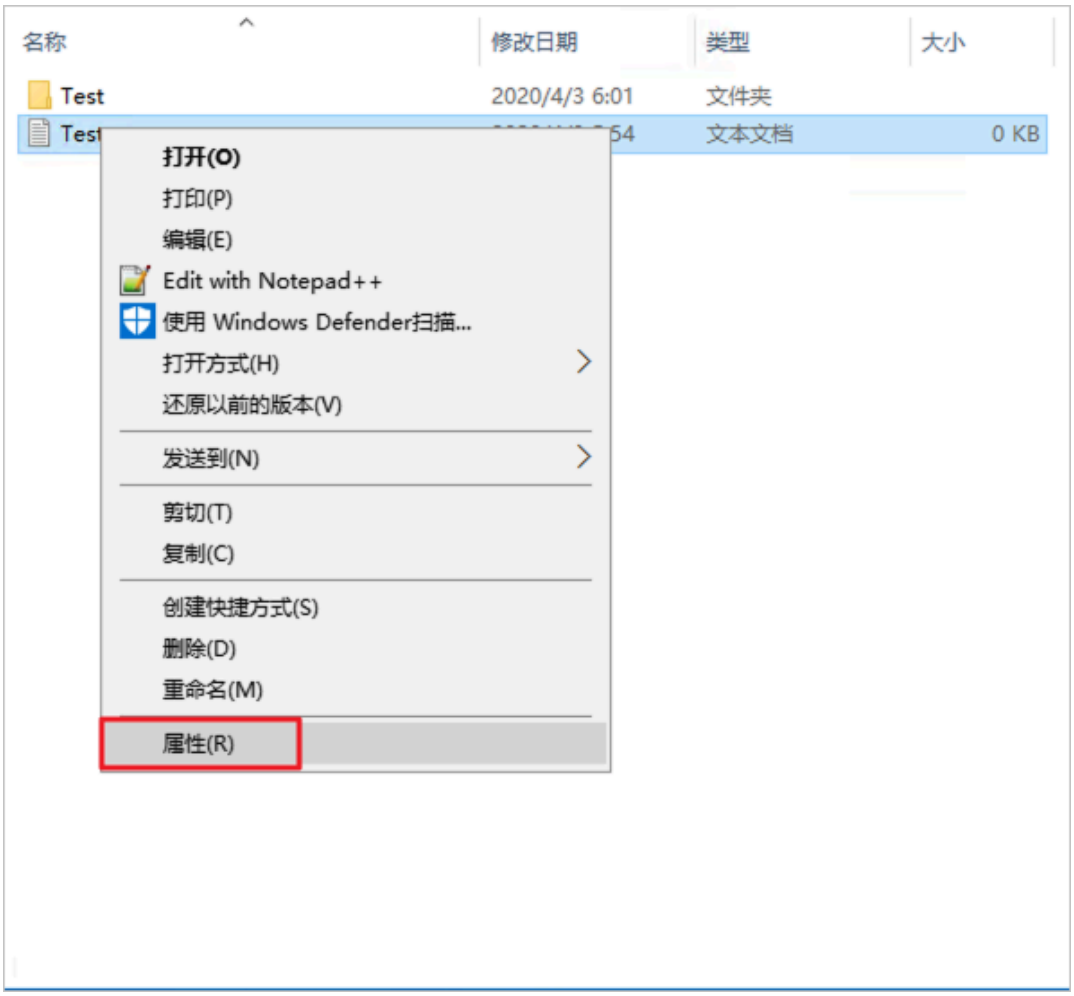
3. 重新登录系统，使创建的符号链接生效。

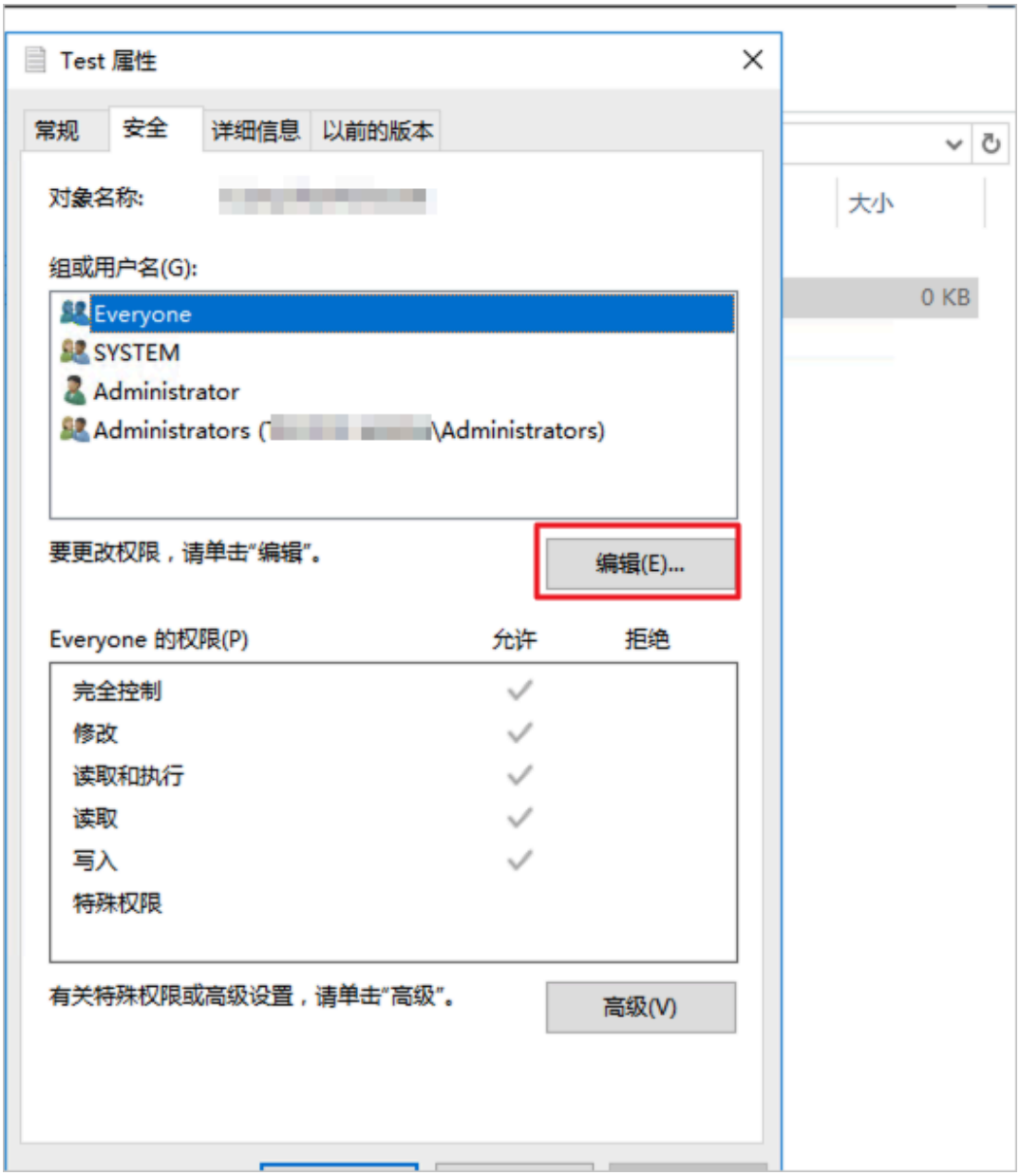
NAS用户为文件系统挂载点在Windows本地盘下生成符号链接，以访问Windows本地盘的子目录的形式来访问NAS文件系统。在该模式下，用户可以正常访问文件系统，也可以查看和编辑文件或目录的ACL。

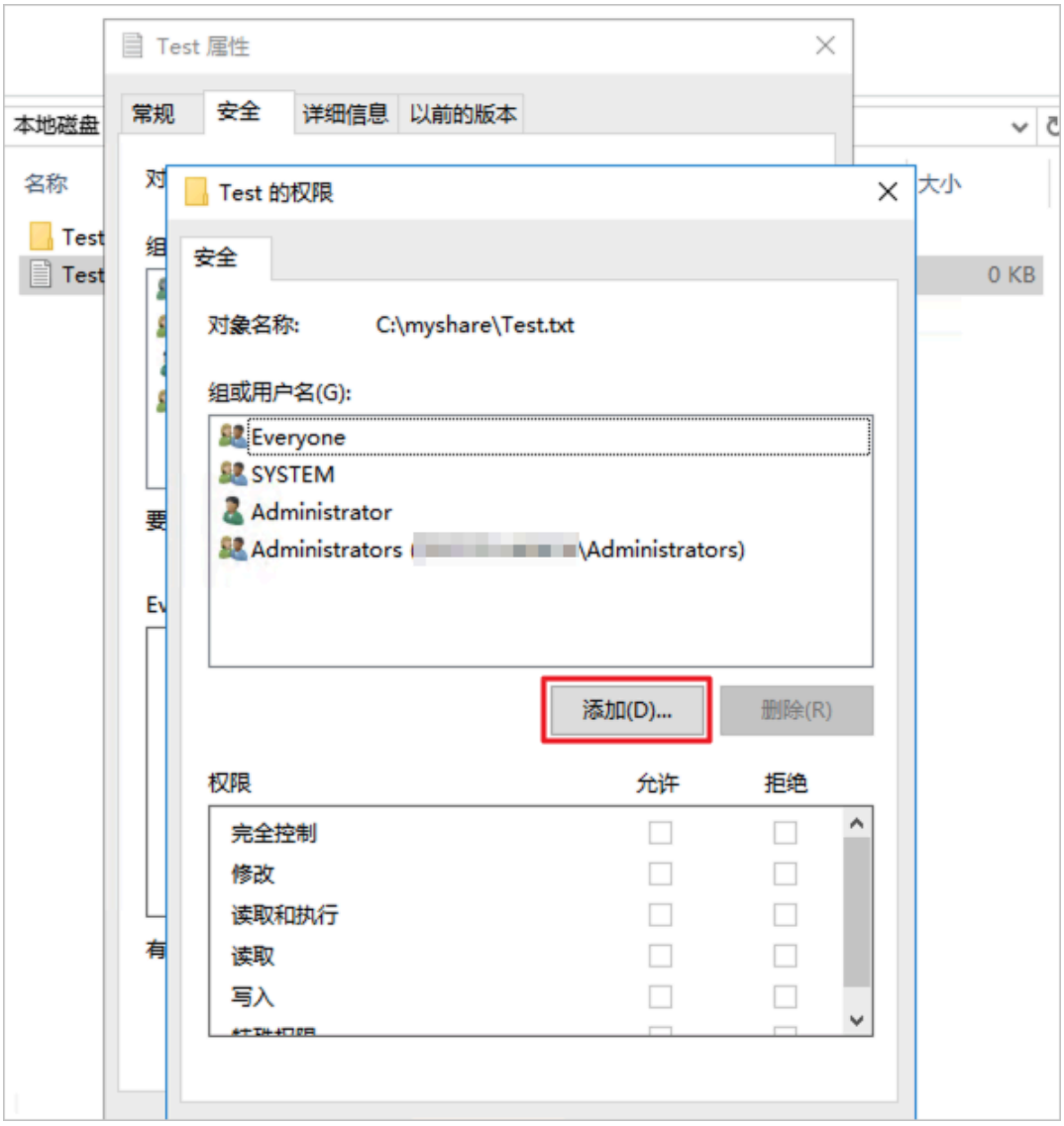
三、用Windows文件资源管理器查看和编辑ACL

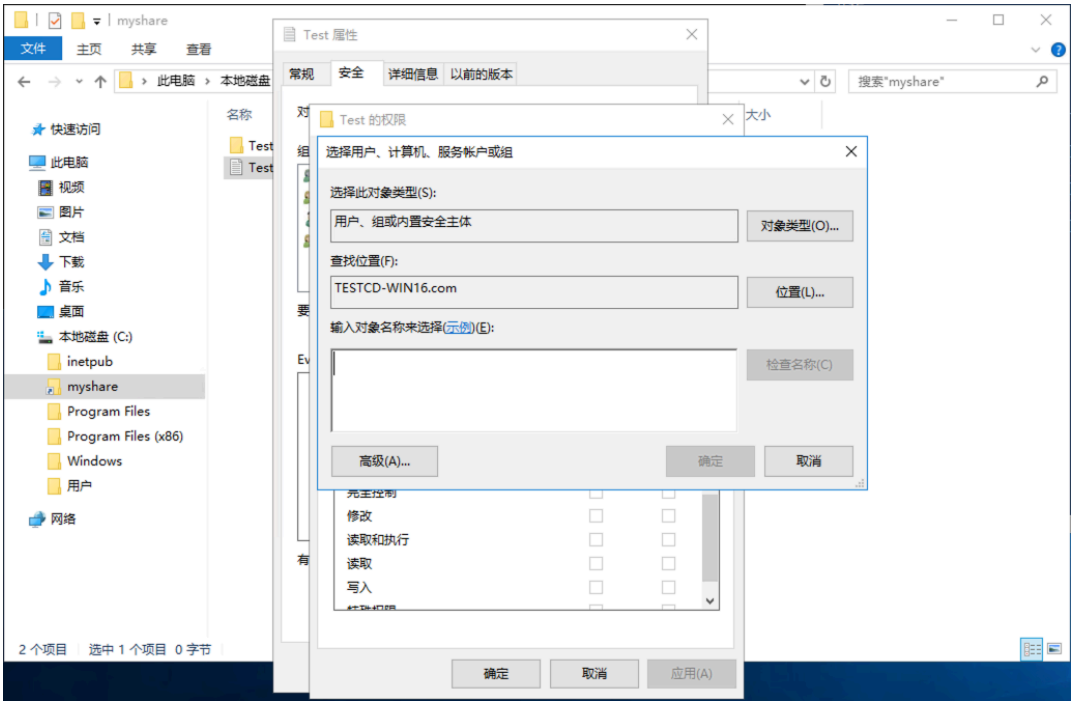
NAS用户为文件系统挂载点在Windows本地盘下生成符号链接后，可以通过Windows的文件资源管理器（File Explorer）查看、编辑文件和目录的ACL。

下图为使用mklink工具在此电脑>本地磁盘下生成符号链接（myshare）的形式挂载使用SMB文件系统后，使用Windows的文件资源管理器（File Explorer）查看NAS文件系统中文件的安全属性（即ACL）的示例。



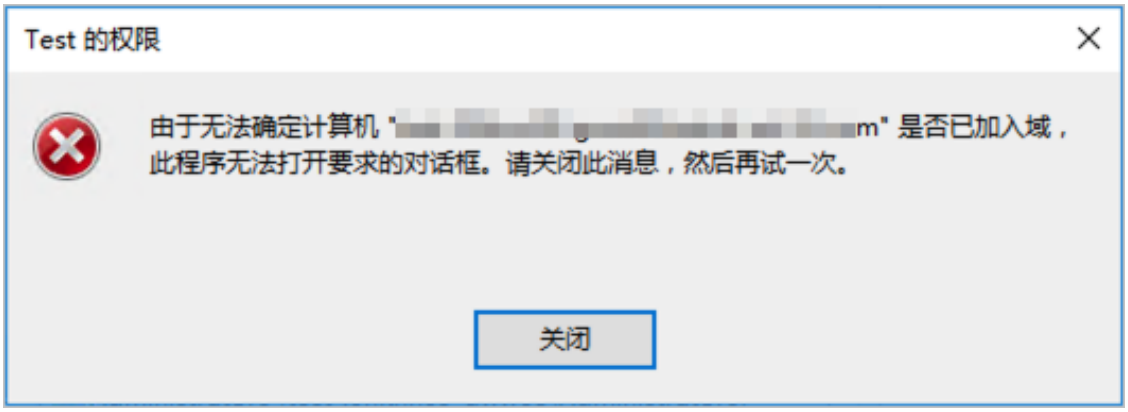

Test 属性
常规
安全
详细信息
以前的版本
对象名称:
组或用户名(G):
Everyone
SYSTEM
Administrator
Administrators (\Administrators)
要更改权限，请单击"编辑"。
编辑(E)...
Everyone 的权限(P)
允许
拒绝
完全控制
修改
读取和执行
读取
写入
特殊权限
有关特殊权限或高级设置，请单击"高级"。
高级(V)
大小
0 KB

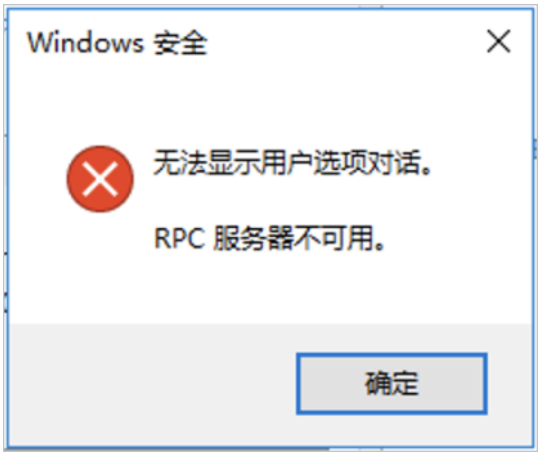

Test 属性
常规
安全
详细信息
以前的版本
本地磁盘
名称
大小
Test
Test
0 KB
Test 的权限
安全
对象名称: C:\myshare\Test.txt
组或用户名(G):
Everyone
SYSTEM
Administrator
Administrators \Administrators)
添加(D)...
删除(R)
权限
允许
拒绝
完全控制
修改
读取和执行
读取
写入


myshare
文件
主页
共享
查看
此电脑 › 本地磁盘
搜索"myshare"
快速访问
此电脑
视频
图片
文档
下载
音乐
桌面
本地磁盘 (C:)
inetpub
myshare
Program Files
Program Files (x86)
Windows
用户
网络
2 个项目
选中 1 个项目 0 字节
Test 属性
常规
安全
详细信息
以前的版本
Test 的权限
选择用户、计算机、服务帐户或组
选择此对象类型(S):
用户、组或内置安全主体
对象类型(O)...
查找位置(F):
TESTCD-WIN16.com
位置(L)...
输入对象名称来选择(示例)(E):
检查名称(C)
高级(A)...
确定
取消
修改
读取和执行
读取
写入
确定
取消
应用(A)

在使用Windows的文件资源管理器查看NAS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。如下图所示。

在用Windows文件资源管理器访问和使用文件系统模式下，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。如下图所示。





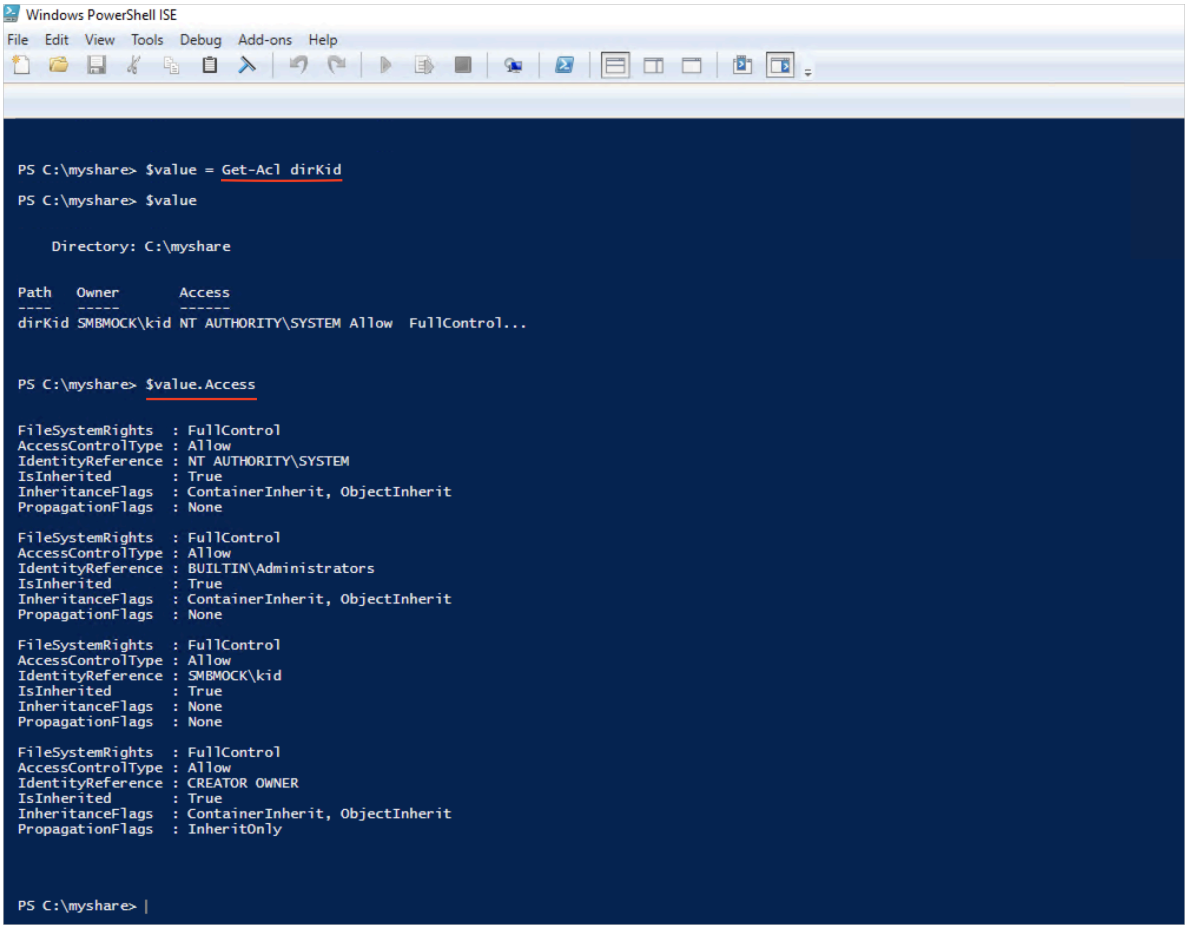
四、通过Get-Acl或Set-Acl Powershell命令查看和编辑ACL

Windows Powershell支持Get-Acl和Set-Acl来查看和编辑ACL。

- Get-Acl示例如下所示。

```
$value = Get-Acl dir
```

```
$value.Access
```



- Set-Acl命令示例如下所示。

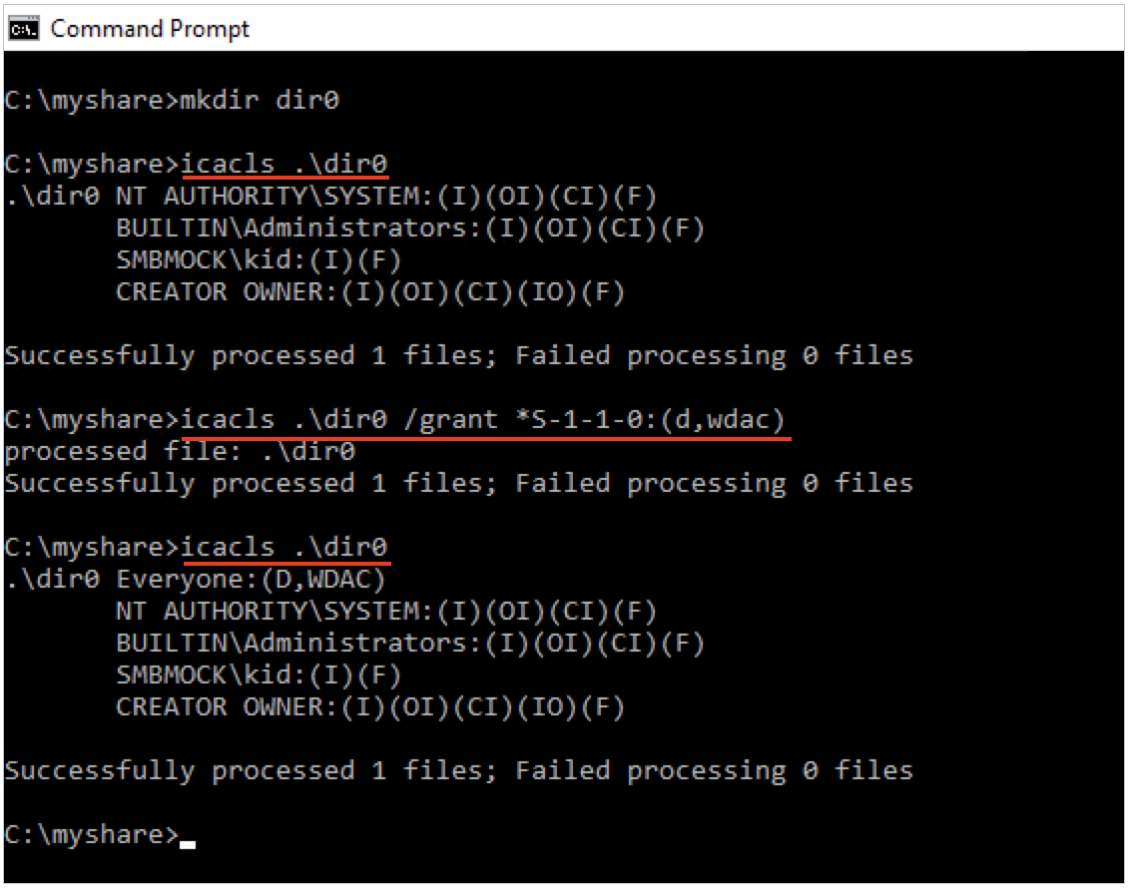
```
Set-Acl .\dirKid2 $value
Get-Acl .\dirKid1 | Set-Acl .\dirKid2
```

五、通过icacls命令查看和编辑ACL

icacls是Windows命令行下的ACL操作标准命令。示例如下所示。

```
icacls .\dir0
icacls .\dir0 /grant *S-1-1-0:(d,wdac)
```

```
icacls .\dir0
```



1.4.5 阿里云NAS SMB ACL特性

本文介绍阿里云NAS SMB ACL相关特性。

背景信息

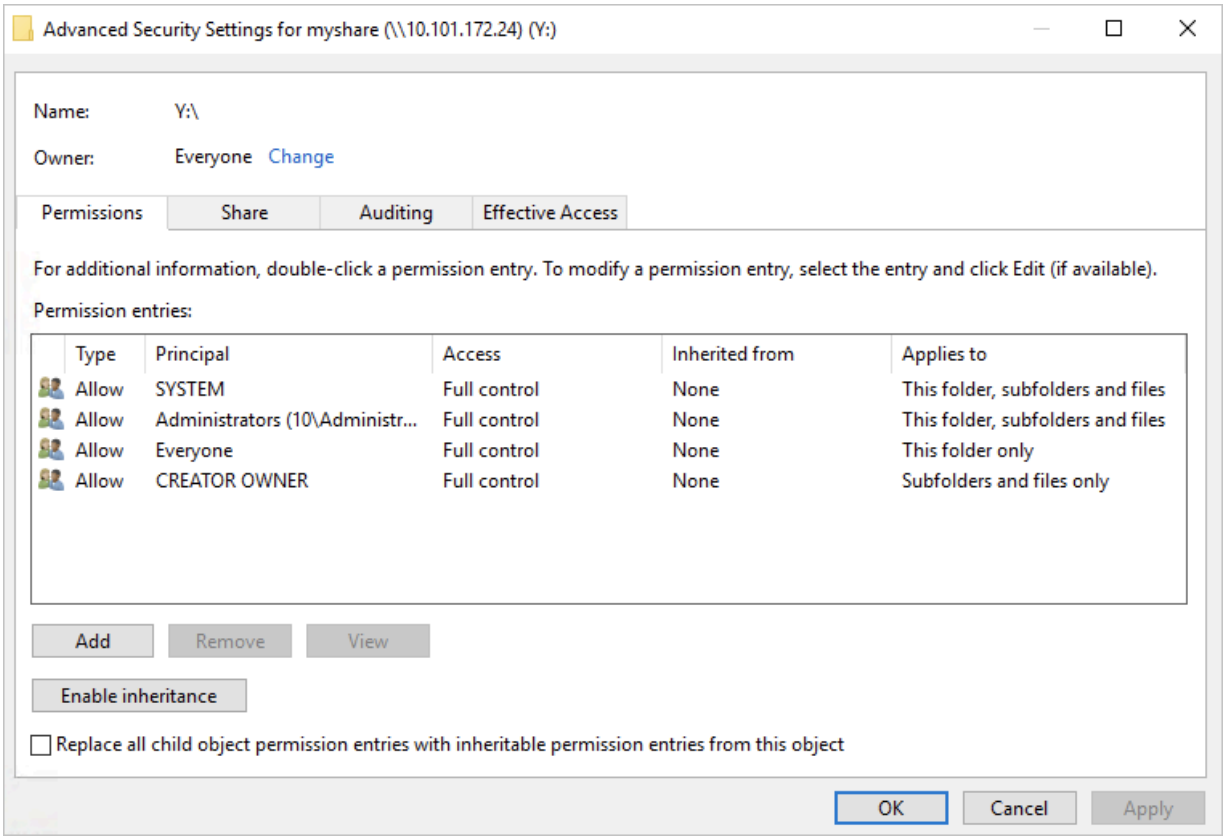
ACL权限控制表是一项重要的企业级特性。在SMB文件系统不连通AD服务时，NAS SMB卷的ACL是只读的，用户登录身份为匿名（Everyone）。目前，阿里云用户可以将自建的AD服务与NAS SMB卷连通，通过AD域身份或者Everyone的方式挂载NAS SMB卷，从而可以对文件、文件夹设置ACL权限。

具体配置AD的方法，请参见将阿里云SMB协议文件系统挂载点接入AD域。

挂载SMB卷的方法，请参见从Windows以AD域用户身份挂载并使用阿里云SMB协议文件系统。

默认值设计

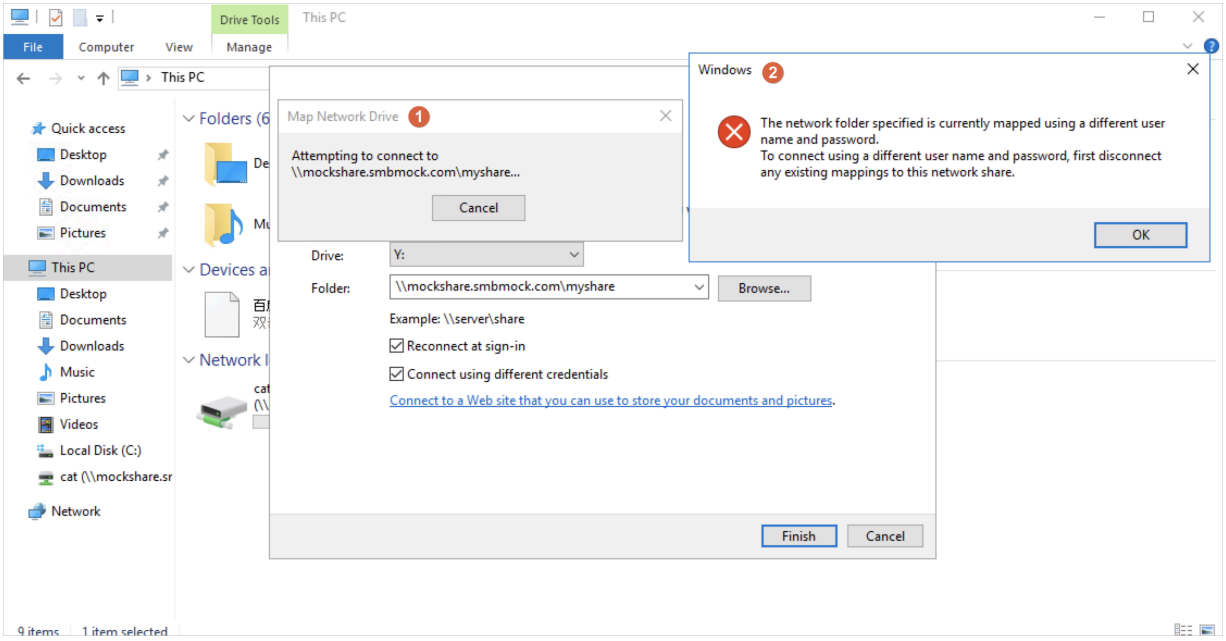
阿里云NAS SMB ACL的卷根目录权限默认值如图所示：



- 默认值设计的原因
  - SYSTEM和Administrators这两个ACE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。
  - 设置Owner为Everyone，让Everyone有根目录的所有权限。这样，没有使用AD的用户也能够以Everyone的身份登录卷，并且在卷上实现创建新文件、文件夹的操作而不受影响。
  - 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。
  - 文件卷根目录权限是锁定的，这可以保障所有用户能够访问根目录。如需隔离，请自行建立子目录并设置隔离权限，让Everyone不能访问。
  - 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：

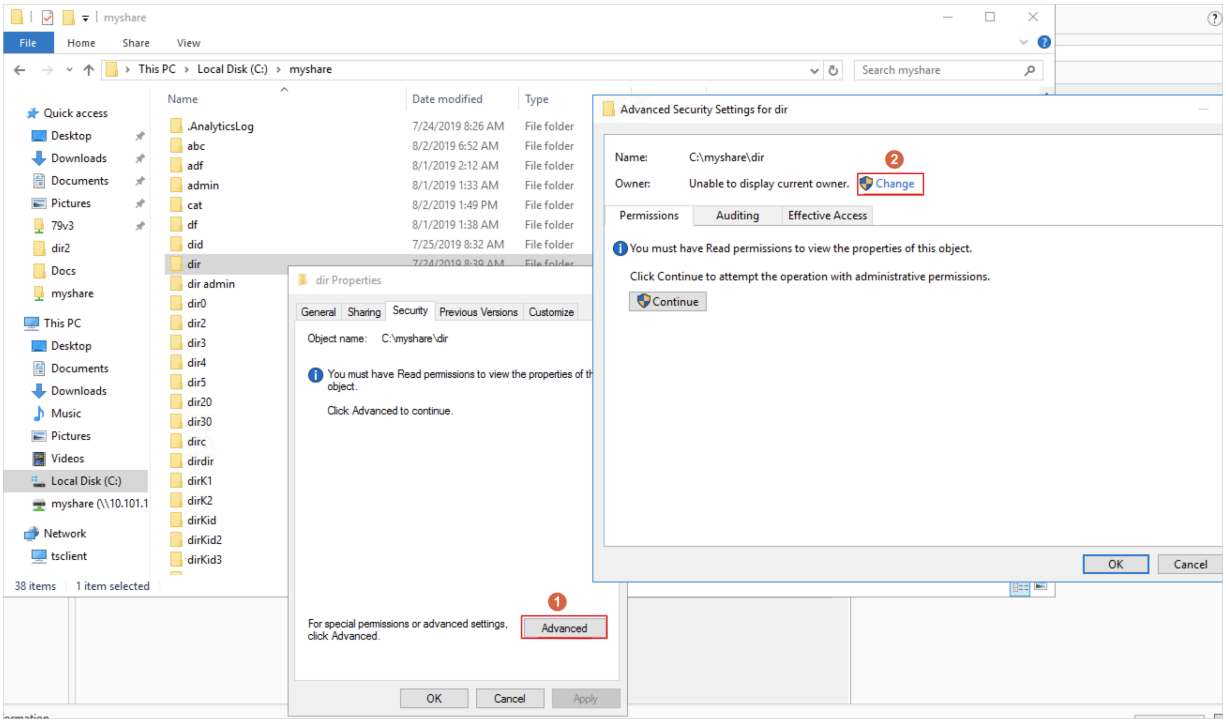


逃逸机制

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文件卷实现了与Windows Server文件卷类似的逃逸机制。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，管理者（Domain Admins，Built-in Administrators）可以在单击确认后作以下操作：

- 将文件夹的拥有者修改为管理者本人或者Everyone。
- 将Deny Everyone的权限项删除并添加合适的Allow权限项。



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

  在Cygwin中使用NAS SMB卷时，建议在Cygwin的/etc/fstab中加入noacl的挂载选项。这样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，用户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。

详情请参见Linux客户端以AD域用户身份挂载使用阿里云SMB协议文件系统。

1.5 NAS NFS ACL

1.5.1 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。

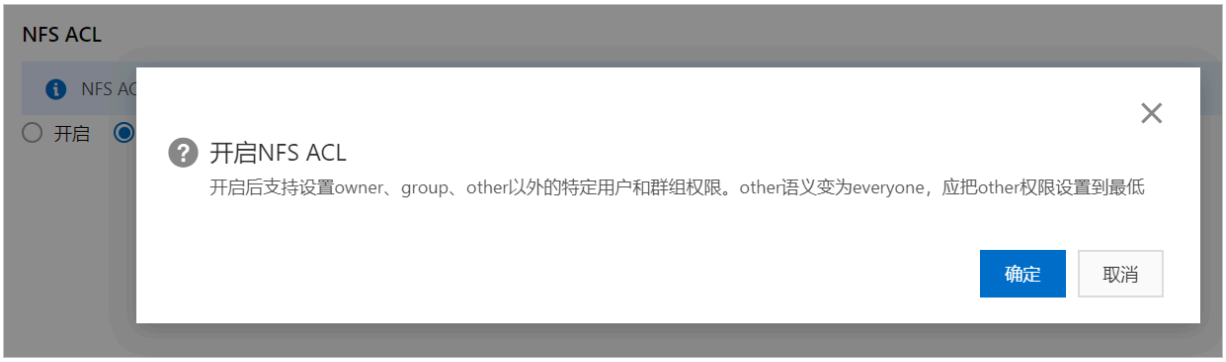
NFS v4 ACL是NFS v4协议能够扩展支持的权限控制协议，提供比POSIX ACL更细粒度的权限控制。详细介绍请参见nfs4_acl - Linux man page。

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NFS4 ACL和POSIX ACL并不完全兼容，加上mode和ACL之间的互操作也无法尽善尽美，另外NAS NFS v3挂载不支持锁，所以建议您在使用NFS ACL功能时尽量只使用NFS v4协议挂载并设置NFS4 ACL，不使用mode和POSIX ACL。相关特性说明请参见特性。

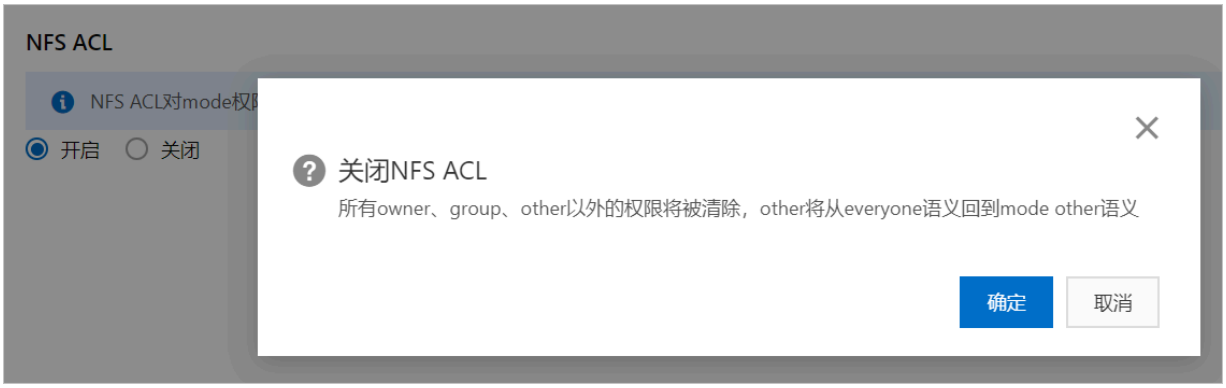
> **说明：**
>
> 目前，NFS ACL功能只支持亚太南部1（孟买）、中国香港（香港）、华东2（上海）、英国（伦敦）、欧洲中部 1（法兰克福）、西南1（成都）、亚太东南 2（悉尼）、亚太东南 5（雅加达）、美国东部1（硅谷）、美国西部1（弗吉尼亚）、华北3（张家口）、华东1（杭州）、华北5（呼和浩特）、华东2（北京）地域。如果您所在的区域还不支持NFS ACL功能，请提交工单。

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**。在**访问控制**区域，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。

1.5.2 特性

本文介绍NFSv4 ACL和POSIX ACL相关的特性。

> **说明:**
>
> 目前，NFS ACL功能只支持亚太南部1（孟买）、中国香港（香港）、华东2（上海）、英国（伦敦）、欧洲中部 1（法兰克福）、西南1（成都）、亚太东南 2（悉尼）、亚太东南 5（雅加达）、美国东部1（硅谷）、美国西部1（弗吉尼亚）、华北3（张家口）、华东1（杭州）、华北5（呼和浩特）、华东2（北京）地域。如果您所在的区域还不支持NFS ACL功能，请提交工单。

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上不起作用。如果需要审计和报警功能，可以在阿里云控制台上进行配置。

- 未设置ACL的文件或目录会呈现与之mode对应的缺省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。

  1. 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
```

  2. 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
```

  3. 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，确保同一个用户名和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=0sAAAABgAAAAAAAAAABYBhwAAAAZPV05FUkAAAAAAAAAAAAAA
ABIAhwAAAAZHUk9VUEAAAAAAAAAAAAAAABIAhwAAAAlFVkVSWU9ORUAAAAAA
AAAAAAAAAAAAAAEAAAAEMTAwMAAAAAAAAALAAAAAwAAAQxMDAwAAAAAAAA
AEAAFgGQAAAABTEwMDAxAAAA
```

- 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。

- 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。

  1. 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::---
```

2. 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/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。

1.5.3 使用POSIX ACL进行权限管理

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

前提条件

已使用NFSv3协议挂载文件系统，详情请参见挂载NFS文件系统。

> **说明：**
>
> 目前，NFS ACL功能只支持亚太南部1（孟买）、中国香港（香港）、华东2（上海）、英国（伦敦）、欧洲中部 1（法兰克福）、西南1（成都）、亚太东南 2（悉尼）、亚太东南 5（雅加达）、美国东部1（硅谷）、美国西部1（弗吉尼亚）、华北3（张家口）、华东1（杭州）、华北5（呼和浩特）、华东2（北京）地域。如果您所在的区域还不支持NFS ACL功能，请提交工单。

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。

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

   ```
   sudo useradd player
   ```

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

2. 对目录和文件设置POSIX ACL实现权限管理。

   本文假设创建目录dir0，针对目录dir0中的所有文件，授予players只读权限，授予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。

   a) 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'
```

   b) 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::---
```

c) 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：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
```

1.5.4 使用NFSv4 ACL进行权限管理

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

前提条件

已使用NFSv4协议挂载文件系统，详情请参见挂载NFS文件系统。

说明:

目前，NFS ACL功能只支持亚太南部1（孟买）、中国香港（香港）、华东2（上海）、英国（伦敦）、欧洲中部 1（法兰克福）、西南1（成都）、亚太东南 2（悉尼）、亚太东南 5（雅加达）、美国东部1（硅谷）、美国西部1（弗吉尼亚）、华北3（张家口）、华东1（杭州）、华北5（呼和浩特）、华东2（北京）地域。如果您所在的区域还不支持NFS ACL功能，请提交工单。

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。

   a) 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'
```

   b) 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
```

c) 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
```

2 管理文件系统

本文介绍如何在NAS控制台上管理文件系统，包括创建文件系统、查看文件系统列表、查看文件系统详情、删除文件系统等操作。

创建文件系统

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**，单击**创建文件系统**。
3. 在**通用型**区域，单击**按量付费**，此处以创建按量付费的通用型NAS文件系统为例进行说明。
   - 如果您要绑定存储包，请选择**购买存储包**。存储包是在按量付费的基础上推出的更加优惠的计费方式，详情请参见#unique_22。
   - 如果您要创建极速型NAS文件系统，请在**极速型**区域，单击**包年包月**或**按量付费**进行创建。
4. 在**通用型NAS（按量付费）**页面，配置相关信息。

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不互通。 每个账号在单个地域内最多可以创建20个文件系统。 地域不同，文件系统支持的存储类型、协议类型不同，更多详情请参见#unique_23。
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，建议和云服务器ECS在同一可用区，避免跨可用区产生的时延。
协议类型	包括**NFS**和**SMB**。 NFS适合Linux ECS文件共享，SMB适合Windows ECS文件共享。
存储类型	包括**性能型**或**容量型**。 性能型文件系统容量上限为1 PB，容量型文件系统容量上限为10 PB。 按实际使用量付费。

参数	说明
加密类型	使用KMS服务托管密钥，对文件系统落盘数据进行加密存储，详情请参见数据加密。 **说明：** • 目前只支持NFS文件系统。 • 针对极速型NAS，如果启用了数据加密功能，则在创建快照时，也会自动加密数据。 • 在读写加密数据时，无需解密。 • 加密类型分为：不加密和静态加密。
网络类型	包括**专有网络**和**经典网络**。 此处为挂载点参数配置，文件存储NAS支持专有网络类型和经典网络两种挂载点。每个文件系统最多可添加两个挂载点，如果您要再创建一个挂载点，请参见添加挂载点。 **说明：** • 目前不支持境外地域添加经典网络挂载点。 • 目前经典网络类型挂载点仅支持ECS实例挂载。
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。 **说明：** 必须与云服务器ECS选择一样的VPC网络和交换机。如果是不同的VPC，则需要先通过云企业网打通网络，才能挂载文件系统，详情请参见#unique_26。
虚拟交换机	选择VPC网络下创建的交换机。

5. 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，请参见修改挂载点的权限组。

查看文件系统列表

在**文件系统列表**页面，可查看当前区域所有的文件系统。在**文件系统列表**中，找到目标文件系统，可修改文件系统的名称。

查看文件系统详情

找到目标文件系统，单击文件系统ID或者**管理**，进入**文件系统详情**页面，可查看文件系统的基本信息、挂载使用和性能监控。

删除文件系统

只有当文件系统的挂载点数目为0时，您才可以删除文件系统实例。

找到目标文件系统，单击**更多**，选择**删除**，即可删除文件系统。

警告:

文件系统实例一旦删除，数据将不可恢复，请谨慎操作。

3 管理挂载点

本文介绍如何在NAS控制台上管理挂载点，包括创建挂载点、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

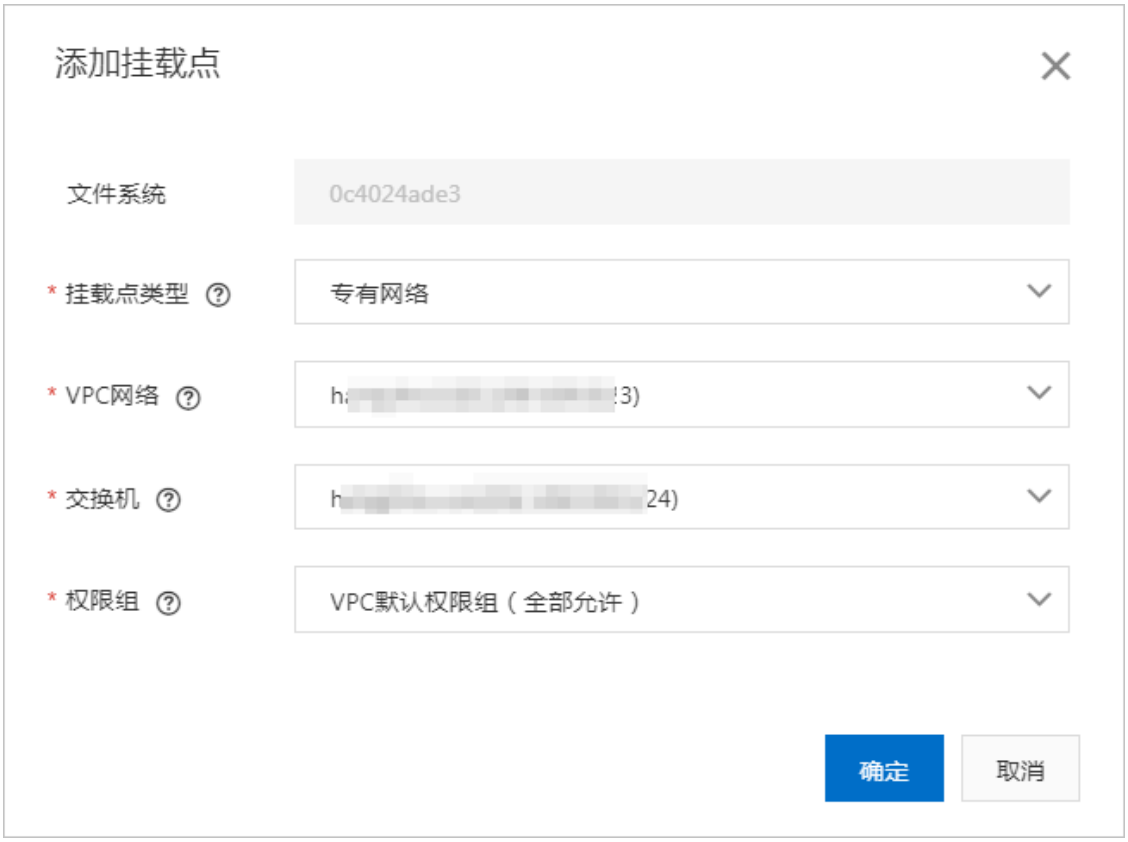
在文件存储NAS中，需要通过挂载点将文件系统挂载至云服务器ECS，添加挂载点的操作如下所示。

说明：

- 通用型NAS支持专有网络类型和经典网络类型两种挂载点，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，每个文件系统只可添加一个挂载点。

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。

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。 **说明：** 必须与云服务器ECS选择一样的VPC网络和交换机。如果是不同的VPC，则需要先通过云企业网打通网络，才能挂载文件系统，详情请参见#unique_26。
交换机	选择VPC网络下创建的交换机。

参数	说明
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环境下的任何IP地址通过该挂载点访问文件系统。如果您要创建权限组，请参见创建权限组和规则。

- 如果您要添加经典网络类型的挂载点，请配置以下参数。

参数	说明
权限组	根据需求选择权限组。 **说明：** - 目前不支持境外地域添加经典网络挂载点。 - 目前经典网络类型挂载点仅支持ECS实例挂载。

5. 配置完成后，单击**确定**。

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**，进入**文件系统详情**页面。在**挂载点**区域，查看挂载点列表。

查看已挂载的客户端列表

单击**已挂载客户端**，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不在此列表中显示。

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

单击**删除**，删除挂载点。

警告：

删除挂载点后，无法恢复，请谨慎操作。

修改挂载点的权限组

单击**修改权限组**，可修改挂载点的权限组。关于权限组的详细信息，请参见管理权限组。

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。

背景信息

由于极速型NAS文件系统有容量限制，当数据写满容量之后，将会导致数据无法写入。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文件系统。

说明：

在扩容极速型NAS时，请注意以下事项：

- 文件系统必须处于正常状态，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90 S。请选择在业务低峰进行扩容，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日之前创建的文件系统为版本1，之后创建的文件系统为版本2。文件系统的详情页可查看版本号。

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

  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，建议使用迁移服务将数据迁移到新规格的文件系统，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。

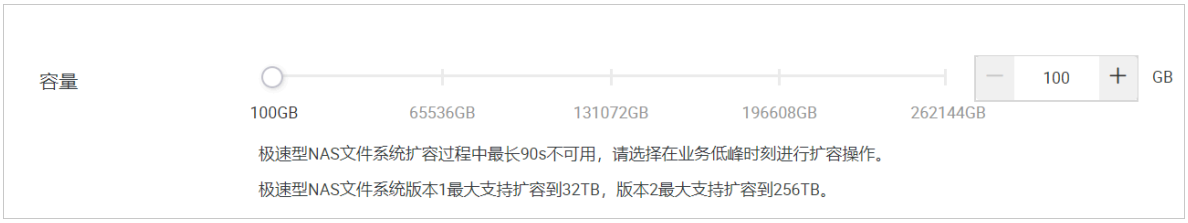
前提条件

已创建极速型NAS文件系统。

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**变配**页面的**容量**区域，滑动按钮调节容量大小。



5. 在**服务协议**区域，选中**极速型NAS（按量付费）服务协议**。
6. 单击**立即购买**，根据页面提示，完成购买。

> **说明:**
>
> 如果是**按量付费**的文件系统，单击**立即购买**后即可。
>
> 如果是**包年包月**的文件系统，请继续以下操作。

7. （可选）在**支付**页面，单击**订购**，完成支付。

5 管理配额

本文介绍如何通过阿里云NAS控制台在NAS文件系统上新建目录配额，并可以对每个目录进行配额管理，包括添加配额、编辑配额和删除配额。

背景信息

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

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

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

使用限制

- 目前，配额管理功能只支持华北 3（张家口）、亚太东南 1（新加坡）地域。
- 对于单个文件系统，最多只能对10个目录设置配额。

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、目录和特殊文件、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是有延迟的（正常情况下5 分钟~15 分钟）。

新建目录配额

1. 登录NAS控制台，选择**文件系统** > **文件系统列表**。
2. 找到目标文件系统，单击文件系统ID或者**管理**，进入**配额管理**区域，单击**新建目录配额**。
3. 在弹出的对话框中，输入**目录路径**（例如： /dir/subdir1），完成目录的添加。

说明：

所添加的目录已经在文件系统中存在。

由于配额是设置在文件系统的某个目录上的，配额路径就是目录在文件系统的全路径。

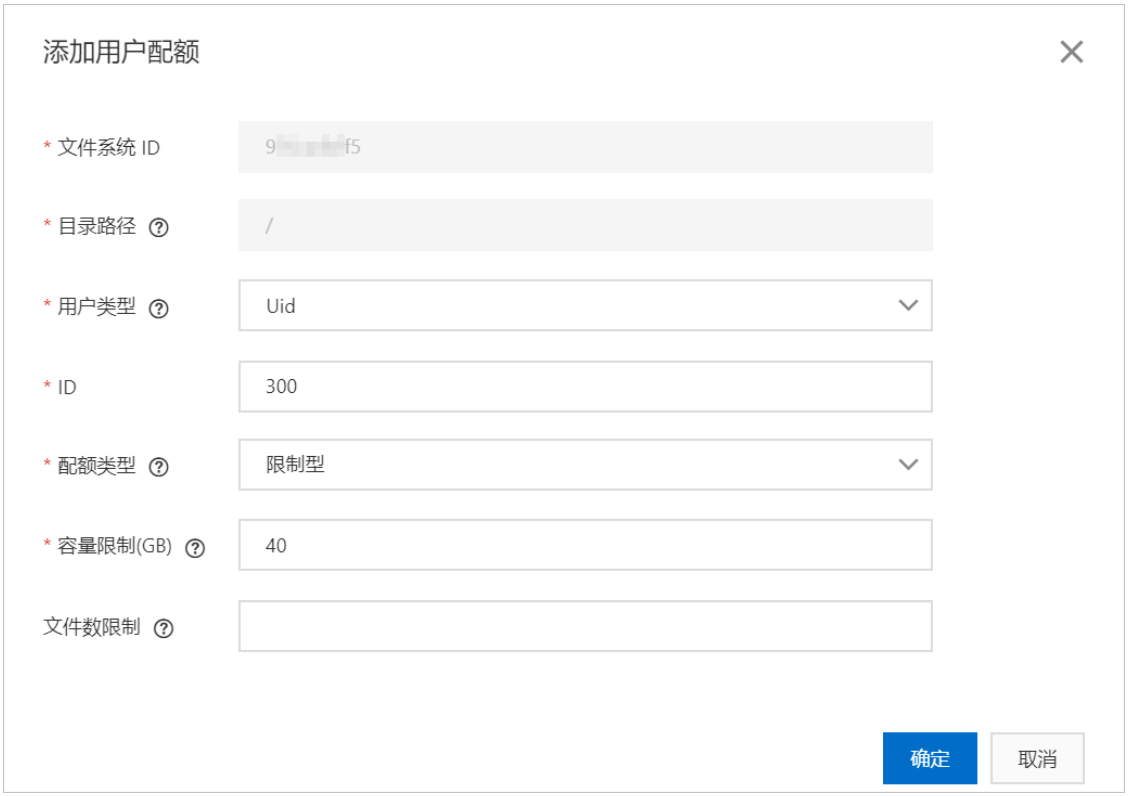
4. 查询目录配额状态。

   新建目录配额后，初次查询时，有个初始化过程，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。

   说明：
   NAS目录配额更新是异步执行的，因此会有一定的延迟。

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。



名称	是否必选	描述
用户类型	是	指定用户ID（UserId）的类型，包括Uid、Gid、AllUsers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。

名称	是否必选	描述
ID	否	如果用户类型（UserType）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	包括统计型（Accounting）和限制型（Enforcement）两种。 • 统计型配额只是配额统计并展示，超出配额后，不对I/O操作限制。 • 限制型配额除了统计和展示外，超出配额后，I/O会被限制。
容量限制(GB)	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接口

管理配额功能提供了以下的API接口：

- #unique_32
- #unique_33
- #unique_34

6 管理快照

极速型NAS支持为文件系统创建快照。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、删除快照、删除快照策略、应用快照策略等操作。

前提条件

已创建文件系统，详情请参见创建文件系统。

背景信息

创建快照是极为重要的操作，是NAS数据在某个时刻的完整拷贝。在有操作风险的场景中，您可以提前创建快照备份数据。当数据丢失时，您可以通过快照将数据恢复到快照某一时间点。您可以为文件系统手动创建快照，也可以通过自动快照策略创建自动快照。

说明：

快照功能只适用于极速型NAS。

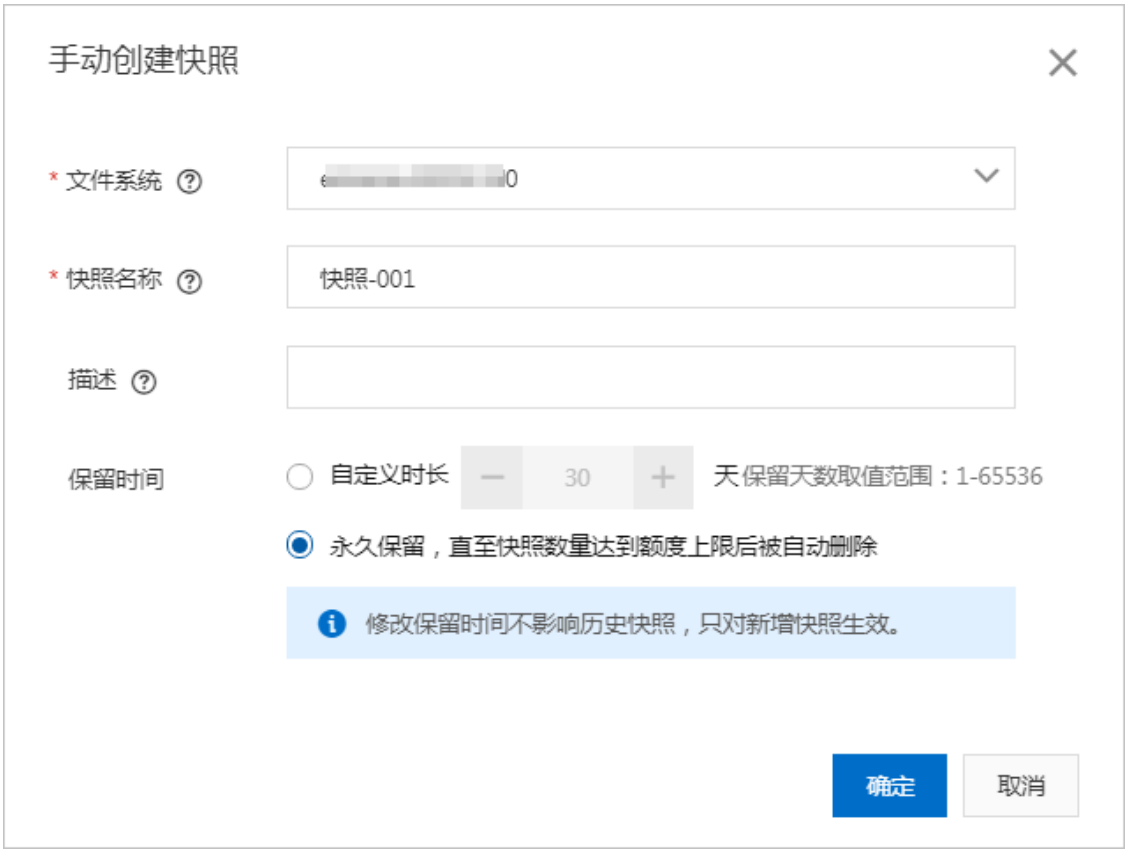
创建快照

1. 登录NAS控制台。
2. 在左侧导航栏，选择**数据服务** > **快照**，在**快照**页签，单击**手动创建快照**。

说明：

- 一个文件系统最多创建128份快照。
- 文件系统实例必须处于正常状态，否则无法创建快照。
- 如果创建快照还未完成，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。
- 创建快照可能会轻微降低文件系统的性能，I/O性能短暂变慢，您需要避开业务高峰期。
- 快照只备份某一时刻的数据，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。
- 手动创建的快照会一直保留，请定期删除不再需要的快照，避免快照容量持续扣费。
- 手动快照可持续保留，直至账户欠费停止服务15天后，会被删除。

3. 在**手动创建快照**对话框中，配置相关参数。



重要参数说明如下所示。

参数	说明
文件系统	选择需要创建快照的极速型NAS文件系统。
保留时间	您可根据需要选择以下保留时间： • 选择**自定义时长**，可指定1天~65536天。 • 选择**永久保留，直至快照数量达到额度上限后被自动删除**，当快照数量达到额度上限后被自动删除。

4. 单击**确定**，创建快照。

创建自动快照

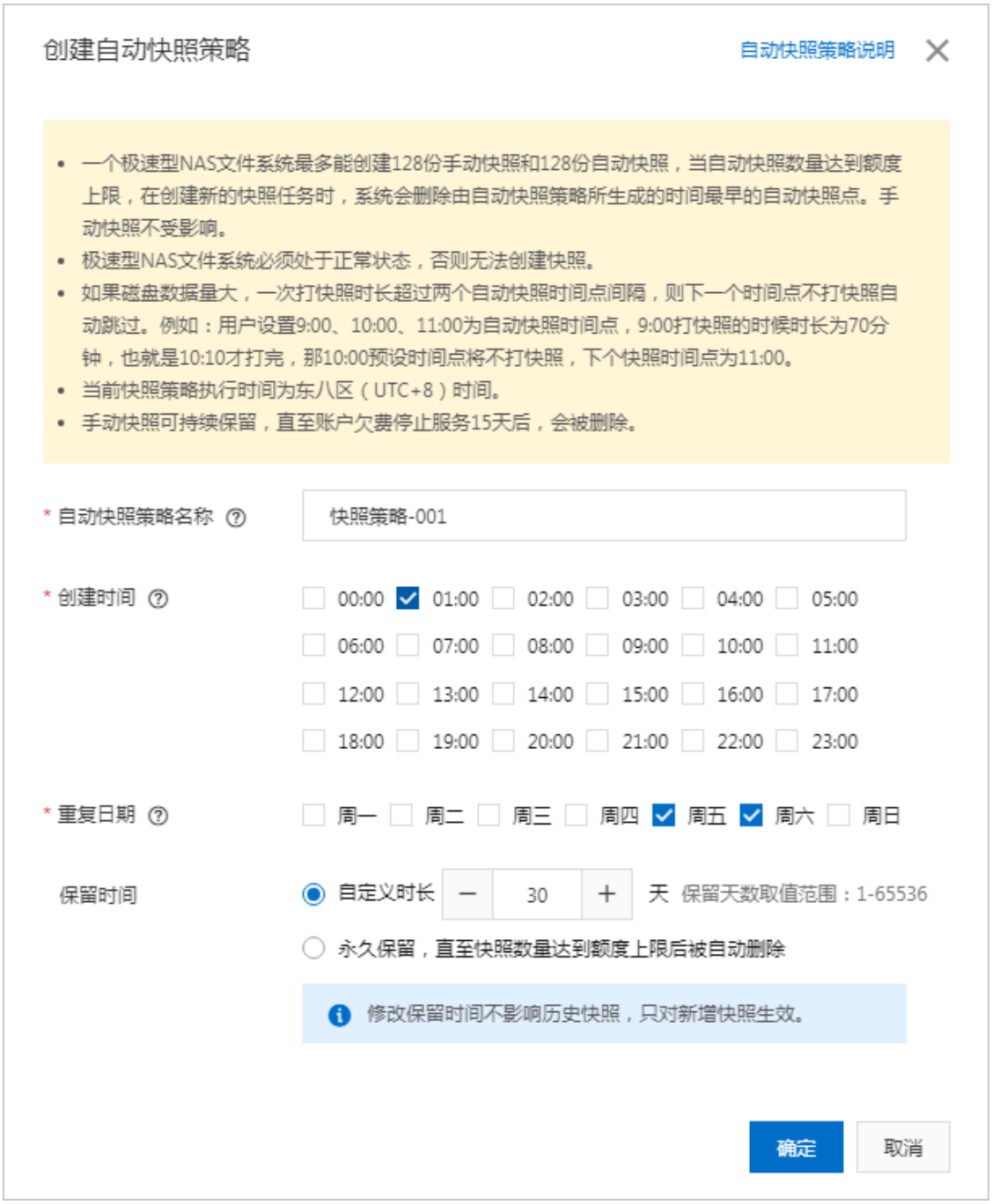
您可以通过自动快照策略创建自动快照。

1. 登录NAS控制台。

2. 创建自动快照策略。

a) 选择**数据服务 > 快照**，在**自动快照策略**页签，单击**创建自动快照策略**。

b) 在**创建自动快照策略**对话框中，配置相关参数。



重要参数说明如下所示。

参数	说明
创建时间	创建自动快照的时间点。从00:00~23:00共24个时间点可选，可选中多个时间点。

参数	说明
重复日期	指定自动快照的重复日期。从周一到周日共7个日期可选，可选中多个日期。
保留时间	• 选择**自定义时长**，可指定1天~65536天。 • 选择**永久保留，直至快照数量达到额度上限后被自动删除**，当直至快照数量达到额度上限后被自动删除。

说明:

- 一个阿里云账户在一个地域最多能创建128条自动快照策略。
- 一条自动快照策略可以应用到多个文件系统上。
- 修改自动快照策略的保留时间时，仅对新增快照生效，历史快照沿用历史保留时间。

c) 单击**确定**，创建自动快照策略。

3. 应用自动快照策略。

a) 找到目标自动快照策略，单击**应用到文件系统**。

b) 在**应用到文件系统**页面**文件系统ID**区域，选中要添加自动快照策略的文件系统，并添加到**应用到文件系统**区域。

说明:

- 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。
- 每个文件系统的自动快照数量总额度128个，达到快照额度上限后，系统会自动删除最早创建的自动快照，手动快照不受影响。
- 手动快照可持续保留，直至账户欠费停止服务15天后，会被删除。
- 修改自动快照策略的保留时间时，仅对新增快照生效，历史快照沿用历史保留时间。
- 正在对某一个文件系统执行自动快照时，您需要等待自动快照完成后，才能手动创建快照。
- 非正常状态的文件系统无法执行自动快照策略。

- 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4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，y表示年、M表示月、d表示天。X表示当日创建的第几份自动快照。

c) 单击**确定**。

应用到文件系统后，将对该文件系统执行自动快照策略，创建自动快照。

通过快照创建文件系统

您还可以调用API，通过快照功能创建文件系统。

1. 安装Python、SDK。

```
pip install aliyun-python-sdk-corepip
pip install aliyun-python-sdk-bssopenapipip
pip install aliyun-python-sdk-nas
```

2. 运行代码创建文件系统。

示例代码中默认创建按量付费的文件系统，如果您要创建包年包月的文件系统请使用包年包月代码。

重要参数说明如下所示，其他参数说明请参见#unique_36。

- accessKeyId和accessSecret：配置您阿里云账号的AccessKeyId和AccessKeySecret，AccessKey信息请参见#unique_37。
- set_parameters：配置为待创建的文件系统的相关参数。

```
#!/usr/bin/env python
# coding=utf-8

from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException
from aliyunsdkbssopenapi.request.v20171214.GetPayAsYouGoPriceRequest import
GetPayAsYouGoPriceRequest
from aliyunsdkbssopenapi.request.v20171214.CreateInstanceRequest import
CreateInstanceRequest
from aliyunsdknas.request.v20170626.DescribeFileSystemsRequest import DescribeFi
leSystemsRequest

client = AcsClient('<accessKeyId>', '<accessSecret>', 'cn-hangzhou')

def Create():
    request = CreateInstanceRequest()
    request.set_accept_format('json')
    request.set_ProductCode("nas")
    # 按量付费
    request.set_SubscriptionType("PayAsYouGo")
    request.set_ProductType("nas_extreme_post")
    # 包年包月
    # request.set_SubscriptionType("Subscription")
```

```
    # request.set_ProductType("nas_extreme")
    # request.set_Period(1) #预付费周期，以月为单位
    request.set_Parameters([
      {
        "Code": "Region",
        "Value": "cn-shanghai"
      },
      {
        "Code": "Zone",
        "Value": "cn-shanghai-g"
      },
      {
        "Code": "ProtocolType",
        "Value": "NFS"
      },
      {
        "Code": "StorageType",
        "Value": "standard"
      },
      {
        "Code": "Size",
        "Value": "100"
      },
      {
        "Code": "Throughput",
        "Value": "150"
      },
      {
        "Code": "SnapshotId",
        "Value": "s-extreme-xxxxxxxxxx"
      }
    ])
    response = client.do_action_with_exception(request)
    print response
if __name__ == '__main__':
    Create()
```

相关操作

操作	说明
取消自动快照策略	相关操作如下所示： **1.** 在**文件系统列表**页面，找到目标文件系统，单击**更多** > **快照** > **设置快照策略**。 **2.** 在**设置快照策略**弹出框，选择**取消**，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。
快照回滚	在**快照**页签，找到目标快照，单击**回滚**，使用文件系统的历史快照回滚至某一阶段的文件系统。
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。

操作	说明
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。

7 数据备份

混合云备份HBR支持备份NAS数据，您可以在NAS控制台上完成数据备份任务，并在数据丢失或受损时及时恢复。

前提条件

您已完成以下操作：

- 已创建用于备份的NFS NAS或SMB NAS文件系统。
- 开通备份服务。您可以登录NAS控制台，在左侧导航栏，选择**数据服务** > **文件备份**。在**欢迎使用NAS备份服务**页面，根据提示开通备份服务。

说明：

- NAS备份服务，不会占用当前文件系统的容量。
- 建议所创建的每个NAS备份任务包含的文件数量不超过5000万，单个目录下的文件及子目录数量之和不超过800万。

创建备份计划

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. 单击**备份文件系统**。
4. 在**备份文件系统**对话框，按照以下说明填写各项参数，然后单击**创建**。

说明：

您可以享受免费备份计划，计划到期日期为创建备份计划之日起60天内。

a) 按以下说明填写基础设置中涉及的各项参数。

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。可不填，默认名字随机分配。
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。

b) 单击**立即转为付费使用**，启用高级设置，并按以下说明填写各项参数。

参数	说明
备份文件路径	输入一个路径，例如：/nas/folder （/代表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。 如果您选择**指定保留时间**来保留备份，则需要指定**备份保留时间**，当前备份保留时间支持的单位为：天、周、月、年。
备份保留时间	选择保留该备份的时间。时间单位：天、周、月、年。

参数	说明
备份库配置	您可以**选择已有备份库**。如果您之前没有创建过备份仓库，单击**创建新备份库**，然后输入仓库名称和描述即可创建一个新仓库。仓库名称不得超过64个字节。 **说明：** 备份库是混合云备份的云上存储仓库，用于保存备份的数据。多个客户端可以备份到同一个仓库。备份仓库有地域属性，您仅能选择或者新建当前地域下的仓库。

备份计划创建完成后，将按照指定的备份起始时间、备份执行间隔进行NAS备份任务。您还可以在**备份计划**页签进行如下相关操作：

- 单击**操作**栏下的**立即执行**，开始执行备份任务。
- 单击**操作**栏下的**更多 > 暂停计划**，暂停执行中的备份任务。如需再次启动备份任务，单击**操作**下的**更多 > 继续计划**。
- 单击**操作**栏下的**更多 > 删除计划**，删除执行中的备份任务。备份计划删除后，该备份计划不会继续执行，但仍保留已备份的数据。
- 单击**操作**栏下的**更多 > 备份历史**，您可以查看该文件系统最近3个月或者所有的备份历史。
- 单击**操作**栏下的**编辑**，修改已创建的备份计划。

说明：
您可以在**备份任务**页签查看NAS备份任务进度，待指定的备份任务完成后，您可以将指定的备份源NAS中的备份数据恢复至本NAS或其他指定的NAS文件系统。

其他相关操作

创建恢复任务

#unique_40/unique_40_Connect_42_section_lak_3jr_12s

8 生命周期管理

8.1 生命周期管理功能介绍

本文介绍了阿里云文件存储NAS生命周期管理的工作原理。

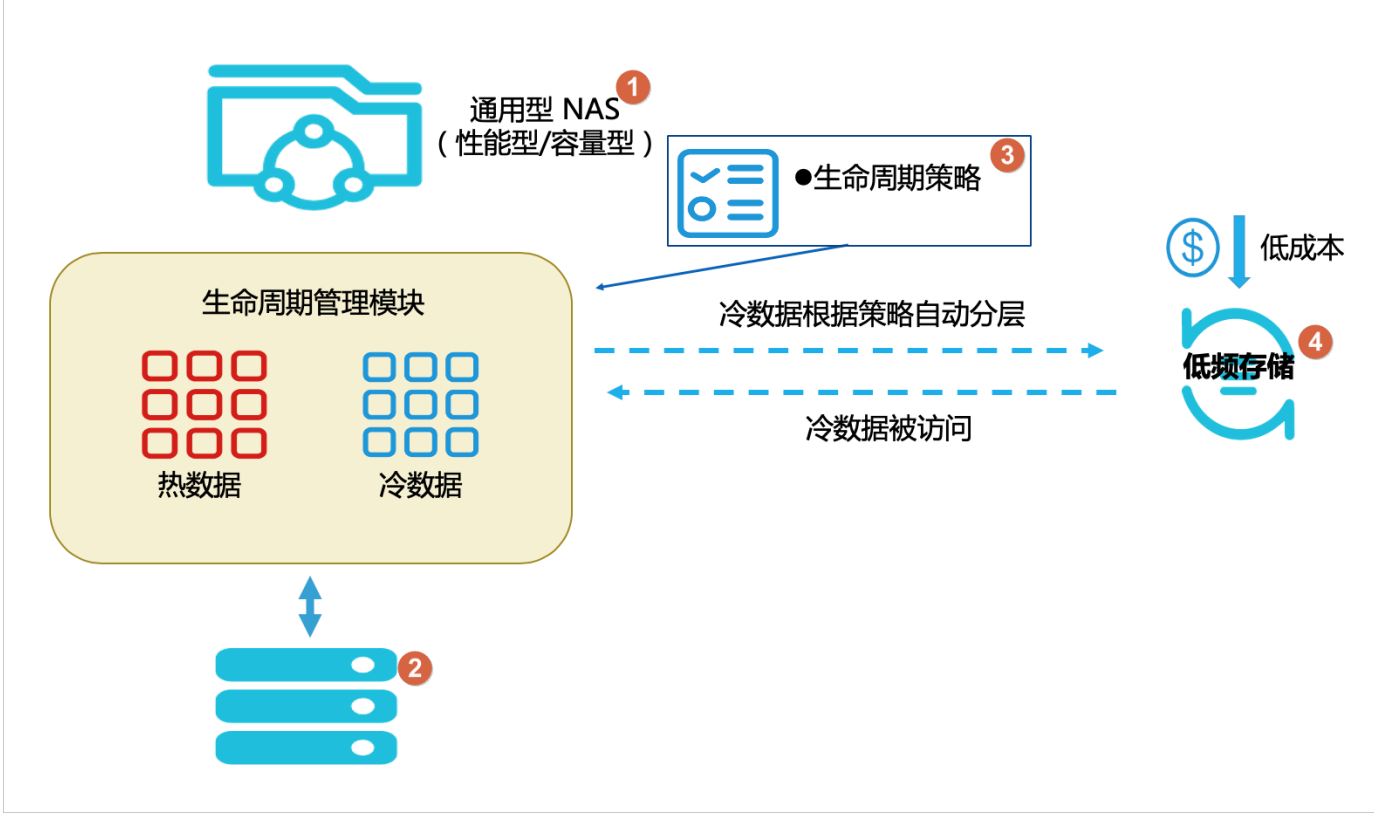
背景信息

阿里云文件存储NAS推出的生命周期管理功能，可以帮助您将低频访问的文件转换到低频存储空间，采用低频计费方式，从而减少用户使用文件系统的费用。

生命周期管理工作流程

如图所示。用户在 NAS控制台上创建和管理文件系统（图示中①）。当用户挂载文件系统写入数据时，数据存储到了NAS通用型存储空间中（图示中②）。当用户访问数据时，数据从NAS通用型存储空间（图示中②）读出返回给用户。

图 8-1: 生命周期管理示意图



通用型NAS配置生命周期管理策略及工作流程包括以下几个部分：

1. 用户在NAS控制台创建生命周期管理策略（图示中③）。

2. 根据创建的生命周期管理策略，定期检查用户策略对应的文件夹是否有冷数据。
3. 如果检查发现冷数据，会根据策略自动分层，把数据转换到低频存储空间（图示中④）。
4. 当用户访问冷数据时，生命周期管理模块会把数据从低频存储空间缓存到通用型存储空间（图示中②）。

   用户第一次访问时会稍有增加数据延迟的时间，之后的访问性能与访问通用型存储空间相同。

使用限制

在使用生命周期管理策略时，请注意以下事项：

- 当数据被划归为冷数据，并且自动分层到低频存储空间之后，这部分数据的计费方式就维持冷数据的计费方式。冷数据的存储费用较热数据的要低很多，但是在被读取时会收取流量费用。详情请参见计量计费。
- 删除生命周期管理策略并不能将该策略下的冷数据转变成热数据。
- 如果想要把冷数据重新变成热数据，需要将冷数据拷贝到新的路径位置。拷贝后的数据将按照热数据的收费方式收费。

生命周期管理策略规则

生命周期管理策略是用户在NAS控制台上配置，绑定了用户名下的一个NAS文件系统中的某个指定目录，根据一定的规则将该指定目录（或其子目录）下的所有符合规则的文件转换为低频存储文件的一种资源实体。

一个文件如果要被转换为低频存储文件，需要满足以下要求：

- 文件所在的目录配置了生命周期管理策略。
- 文件的最近一次访问时间需要超过一定天数。

  按在控制台配置的管理规则，有14天、30天、60天、90天不等，详情请参见创建生命周期管理策略。

案例介绍：

用户对某个NAS文件系统下的目录/DIR配置了生命周期管理策略，设定了**距最近访问14天以上**的管理规则。该目录下有两个文件file_A和file_B，文件信息如下所示。

目录名称	文件名称	最近访问时间
/DIR	file_A	2020年6月1日00:00
	file_B	2020年6月7日00:00

案例分析：

在2020年6月15日，目录/DIR下的文件file_A、file_B，只有file_A被转换为低频存储文件，而文件file_B仍然是NAS标准存储文件。文件file_B没有被转换为低频存储文件的原因是它的最近一次访问时间只过去了8天，不符合距最近访问14天以上的规则。

计量计费

当文件被成功转换为低频存储文件之后，会产生以下两种计费方式：

- 对于该低频文件所占用的容量会按照价格更低的低频存储费率进行计费。
- 对于低频文件的读写操作会按访问数据量收取一定的流量费用。

新的计费方式包含以下三种计费项。

- 标准存储费用：标准存储类型数据，继续保持原来的按量计费的规则，每小时出账。

  说明：
  标准存储是指性能型和容量型NAS中的非低频存储类型。
- 低频存储费用：低频存储类型数据，也是采取按量计费的规则，每小时出账。低频存储单价比标准存储便宜。
- 流量费用：低频存储类型数据读写量，指的是应用对低频存储类型的数据的读写访问量，采取按读写累积量计费的规则，每小时出账。出账后读写量清零，在下一个时间段重新累积。

存储包抵扣

- 如果存储包容量不高于标准存储使用量：
  - 标准存储费用的计费使用量为该文件系统在标准存储类型上的使用量减去存储包的容量。
  - 低频存储费用的计费方式不变。
  - 流量费用的计费方式不变。
- 如果存储包容量高于标准存储使用量：
  - 标准存储费用的计费使用量为零。
  - 低频存储费用的计费使用量=（该文件系统在低频存储使用量-（存储包容量-该文件系统在标准存储上使用量）*系数）。如果计算结果小于零，以零计算。公式中系数跟文件系统类型相关：性能型的系数为12.333，容量型的系数为2.333。

    说明：
    存储包不能用于直接抵扣低频数据读写量。
  - 流量费用的计费方式不变。

计费示例

北京区域的用户A有个性能型文件系统B，在2020年1月1日10:00~11:00文件系统B的使用量大小是1000 GB。其中，200 GB数据存储在标准存储上，800 GB数据转换到了低频存储上。并且在这个小时内对存储在低频存储上的数据的读访问量为1 GB，写访问量为2 GB。

按量计费：

- 标准存储费用：计费使用量=200 GB，费用=1.85（元/GB/月）/24（小时）/30（天）*200（GB）=0.514元。
- 低频存储费用：计费使用量=800 GB，费用=0.15（元/GB/月）/24（小时）/30（天）*800（GB）=0.167元。
- 流量费用：数据读访问量=1 GB，费用=0.06（元/GB）*1（GB）=0.06；数据写访问量为2 GB，费用=0.06（元/GB）*2（GB）=0.12元。
- 总费用=0.514（元）+0.167（元）+0.06（元）+0.12（元）=0.861元。

按存储包（100 GB）抵扣：

- 标准存储费用：计费使用量=200-100=100 GB，费用=1.85（元/GB/月）/24（小时）/30（天）*100（GB）=0.257元。
- 低频存储费用：计费使用量=800 GB，费用=0.15（元/GB/月）/24（小时）/30（天）*800（GB）=0.167元。
- 流量费用：数据读访问量=1 GB，费用=0.06（元/GB）*1（GB）=0.06；数据写访问量为2 GB，费用=0.06（元/GB）*2（GB）=0.12元。
- 总费用=0.257（元）+0.167（元）+0.06（元）+0.12（元）=0.604元。

按存储包（250 GB）抵扣：

- 标准存储费用：费用=0元。

  说明：
  存储包还剩余250-200=50 GB，可以抵扣50*12.333=616.65 GB的低频存储使用量。
- 低频存储费用：计费使用量=800-616.65=183.35 GB，费用=0.15（元/GB/月）/24（小时）/30（天）*183.35（GB）=0.038元。
- 流量费用：数据读访问量=1 GB，费用=0.06（元/GB）*1（GB）=0.06；数据写访问量为2 GB，费用=0.06（元/GB）*2（GB）=0.12元。
- 总费用=0（元）+0.038（元）+0.06（元）+0.12（元）=0.218元。

文件存储NAS的详细价格，请参见文件存储详细价格信息。

8.2 生命周期管理配置操作

本文介绍如何使用阿里云文件存储NAS生命周期管理功能。您可以在NAS控制台上对一个文件系统配置生命周期管理策略、查看文件系统生命周期信息、查看生命周期管理策略、修改生命周期管理策略、删除生命周期管理策略。

背景信息

阿里云文件存储NAS生命周期管理功能可以帮助用户把一定时间内没有访问过的数据转化为低频存储，帮助用户节约成本。

查看生命周期管理策略

1. 登录NAS控制台。
2. 在左侧导航栏，选择**数据服务** > **生命周期管理**，在**生命周期管理**页面，可以查看该区域下所有的生命周期管理策略。

查看某个文件系统的生命周期信息

方式一：在**生命周期管理**页面，在搜索栏里输入文件系统ID，可以找到该文件系统的信息。

方式二：在某个文件系统的详情页，**基本信息**区域，单击**配置策略**，可以转到该文件系统的生命周期信息页面。同时，在详情页可以查询该文件系统的**低频存储用量**。

创建生命周期管理策略

在**生命周期管理**页面，单击**创建策略**。在**创建生命周期管理策略**对话框中，填写相关参数。

参数	是否必填	说明
策略名称	是	长度为3~64个字符，必须以大小写字母开头，可以包含英文字母、数字、下划线（_）或者短划线（-）。
分级存储类型	NA	低频存储：默认把冷数据转储到低频存储空间。
文件系统	是	从文件系统列表，选择一个文件系统。 **说明：** 可以在列表中选择的文件系统必须是在UTC时间2020-06-01 00:00:00以后创建的。
目录路径	是	需要进行生命周期管理的目录路径，以/开始。如果路径上的目录转储了，策略仍然针对转储前的路径，不会跟着目录转储而改变路径。
管理规则	是	系统为您预置了默认的生命周期管理规则： • 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

修改生命周期管理策略

在**生命周期管理**页面，找到目标生命周期管理策略，单击**修改**。只能修改策略的**管理规则**，调整低频时间，不能修改其他策略参数。

删除生命周期管理策略

在**生命周期管理**页面，找到目标生命周期管理策略，单击**删除** > **确认**，策略即被删除。已经转储到低频存储空间的数据会继续保持在低频存储状态。

8.3 计量计费

本文介绍阿里云文件存储NAS引入生命周期管理后的计费方式。

背景信息

文件系统NAS在引入生命周期管理功能后，由于数据需要存到不同的存储介质上，原来的按量计费方式也会发生变化。

按量计费

新的计费方式包含以下三种计费项。

- 计费项一：标准存储类型数据，继续保持原来的按量计费的规则，每小时出账。

  说明：

  标准存储是指性能型和容量型NAS中的非低频存储类型。

- 计费项二：低频存储类型数据，也是采取按量计费的规则，每小时出账。低频存储单价比标准存储便宜。
- 计费项三：低频存储类型数据读写量，指的是应用对低频存储类型的数据的读写访问量，采取按读写累积量计费的规则，每小时出账。出账后读写量清零，在下一个时间段重新累积。

存储包抵扣

- 如果存储包容量不高于标准存储使用量：
  - 计费项一的计费使用量为该文件系统在标准存储类型上的使用量减去存储包的容量。
  - 计费项二的计费方式不变。
  - 计费项三的计费方式不变。

- 如果存储包容量高于标准存储使用量：
  - 计费项一的计费使用量为零。
  - 计费项二的计费使用量=（该文件系统在低频存储使用量-（存储包容量-该文件系统在标准存储上使用量）*系数）。如果计算结果小于零，以零计算。公式中系数跟文件系统类型相关：性能型的系数为12.333，容量型的系数为2.333。
  - 计费项三的计费方式量不变。

说明：

存储包不能用于直接抵扣低频数据读写量。

计费示例

北京区域的用户A有个性能型文件系统B，在2020年1月1日10:00~11:00文件系统B的使用量大小是1000 GB。其中，200 GB数据存储在标准存储上，800 GB数据转换到了低频存储上。并且在这个小时内对存储在低频存储上的数据的读访问量为1 GB，写访问量为2 GB。

按量计费：

- 计费项一：计费使用量=200 GB，费用=1.85（元/GB/月）/24（小时）/30（天）*200（GB）=0.514元。
- 计费项二：计费使用量=800 GB，费用=0.15（元/GB/月）/24（小时）/30（天）*800（GB）=0.167元。
- 计费项三：数据读访问量=1 GB，费用=0.06（元/GB）*1（GB）=0.06元；数据写访问量=2 GB，费用=0.06（元/GB）*2（GB）=0.12元。
- 总费用=0.514（元）+0.167（元）+0.06（元）+0.12（元）=0.861元。

按存储包（100 GB）抵扣：

- 计费项一：计费使用量=200-100=100 GB，费用=1.85（元/GB/月）/24（小时）/30（天）*100（GB）=0.257元。
- 计费项二：计费使用量=800 GB，费用=0.15（元/GB/月）/24（小时）/30（天）*800（GB）=0.167元。
- 计费项三：数据读访问量=1 GB，费用=0.06（元/GB）*1（GB）=0.06；数据写访问量=2 GB，费用=0.06（元/GB）*2（GB）=0.12元。
- 总费用=0.257（元）+0.167（元）+0.06（元）+0.12（元）=0.604元。

按存储包（250 GB）抵扣：

- 计费项一：费用=0元。

  说明：

  存储包还剩余250-200=50 GB，可以抵扣50*12.333=616.65 GB的低频存储使用量。

- 计费项二：计费使用量=800-616.65=183.35 GB，费用=0.15（元/GB/月）/24（小时）/30（天）*183.35（GB）=0.038元。
- 计费项三：数据读访问量=1 GB，费用=0.06（元/GB）*1（GB）=0.06；数据写访问量=2 GB，费用=0.06（元/GB）*2（GB）=0.12元。
- 总费用=0（元）+0.038（元）+0.06（元）+0.12（元）=0.218元。

文件存储NAS的详细价格，请参见文件存储详细价格信息。

8.4 生命周期管理常见问题

本文介绍阿里云文件存储NAS使用生命周期管理功能时的常见问题。

一般问题

- 为什么我的文件系统不能设置生命周期管理？

  NAS生命周期功能发布第一阶段（2020-06-01~2020-09-01）只支持2020-06-01后创建的新NAS实例配置生命周期管理策略。

  NAS生命周期功能发布第二阶段（2020-09-01）将会放开限制，支持用户对所有存量的NAS实例配置生命周期管理策略。

- 如何设置生命周期管理？

  您可以通过NAS控制台或OpenAPI来设置生命周期管理策略。详情请参见NAS生命周期管理使用指南和生命周期管理API：#unique_46、#unique_47、#unique_48、#unique_49。

- 如何选择生命周期策略，如何选择该配置在哪个目录上？

  为了方便选择策略和目录，我们开发了客户端分层策略分析脚本。该脚本可以根据用户想要的分层策略，对指定目录及该目录下的几级子目录进行扫描和排序，将子目录中冷数据量最高的几个目录打印出来。更多详情请参见使用指南。

使用场景与限制

- 所有文件都可以转换为低频存储文件吗?

  一个文件被转换为低频存储文件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。
  - 文件大小需大于或等于64 KB。
  - 文件的最近访问时间需符合策略中的管理规则。

  创建生命周期管理策略时，可以配置管理规则，将距最近访问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
- 一个目录如果配置了几条生命周期管理策略会发生什么?

  如果一个目录被配置了数条策略，目录下的文件只要满足任何一条策略的管理规则就会被转换为低频存储文件。
- 如果一个目录和它的上层目录配置了不同的生命周期管理策略会发生什么?

  目录下文件会同时根据当前目录及上层目录配置的策略来转换低频存储文件。

  例如：当前目录配置了14天未访问转换的策略，其父目录或更上层目录配置了60天未访问转换的策略。那么目录中的14天未访问的文件会被转换为低频存储文件，而父目录或更上层目录策略在扫描当前目录时，会跳过这些已转换文件。
- 文件在策略设置完成后多久会被转换为低频存储文件?

  符合条件的文件最快在2个小时内会被转换为低频存储文件。
- 文件或目录重命名会影响生命周期管理吗?

  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策略管理去转换为低频存储文件。已经转换到低频存储的文件仍将维持其低频存储类型。

  一个文件或目录重命名后如果其新路径配置有生命周期管理策略，则该文件或目录下的文件会受该策略管理，符合条件的文件会被转换为低频存储文件。

- 删除生命周期管理策略会有什么影响？

  被删除策略的关联目录下的文件将不会再被转换为低频存储文件。目录下已经转换到低频存储的文件仍将维持其低频存储类型。

- 策略删除后再重新配置到原来的目录上，会重复转换文件吗？

  重新配置策略后，策略会有机制检查并跳过目录下已经被转换过的低频存储文件，确保不会重复转换。

性能问题

- 低频存储文件可以正常读写吗？

  可以。一个文件系统内的低频存储文件和其他普通文件一样可以被正常读写访问。

- 低频存储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或容量型NAS普通文件的读延时相仿。

  写低频存储文件的延时与一般的性能型或容量型NAS文件相仿。

计费问题

什么是读写流量费？

对于访问低频存储文件的读写数据量单独收取的费用，具体计费规则请参见计量计费。

9 数据迁移

您可以通过数据迁移服务来实现NAS数据迁移。

您可以登录数据迁移服务管理控制台进行数据迁移。

- 如果您要将NAS数据迁移至OSS，详情请参见NAS迁移至OSS教程。
- 如果您要将NAS数据迁移至另一个NAS，详情请参见NAS之间迁移教程
- 如果您要将OSS数据迁移至NAS，详情请参见OSS迁移至NAS教程。

10 数据加密

阿里云NAS支持在创建文件系统时启用静态数据加密。本文介绍加密文件系统的操作步骤及静态加密的工作方式。

加密文件系统

如果您需要静态加密数据和元数据，建议您创建加密的文件系统，操作步骤如下所示。

1. 登录NAS控制台。
2. 在左侧导航栏，选择，单击。
3. 在购买页面，配置**加密类型**，其他参数配置请参见创建文件系统。
4. 单击**立即购买**，根据页面提示，完成购买。

工作方式

NAS使用行业标准AES-256加密算法静态加密数据，为您的文件系统提供落盘存储加密服务，并使用密钥管理服务（KMS）进行密钥管理。

NAS使用用户主密钥（CMK）加密您的文件系统，每一个文件系统有相对应的CMK（目前只支持NAS的服务密钥）和DK，并通过信封加密机制对您的数据进行加密。

在静态加密的文件系统中，在将数据写入到文件系统之前，将自动对其进行加密。同样，在读取数据时，在将其提供给应用程序之前，将自动对其进行解密。这些过程是NAS透明处理的，因此您不必修改您的应用程序。

11 配置监控和报警

本文介绍如何通过云监控管理控制台来实现对NAS文件系统的监控和报警。

前提条件

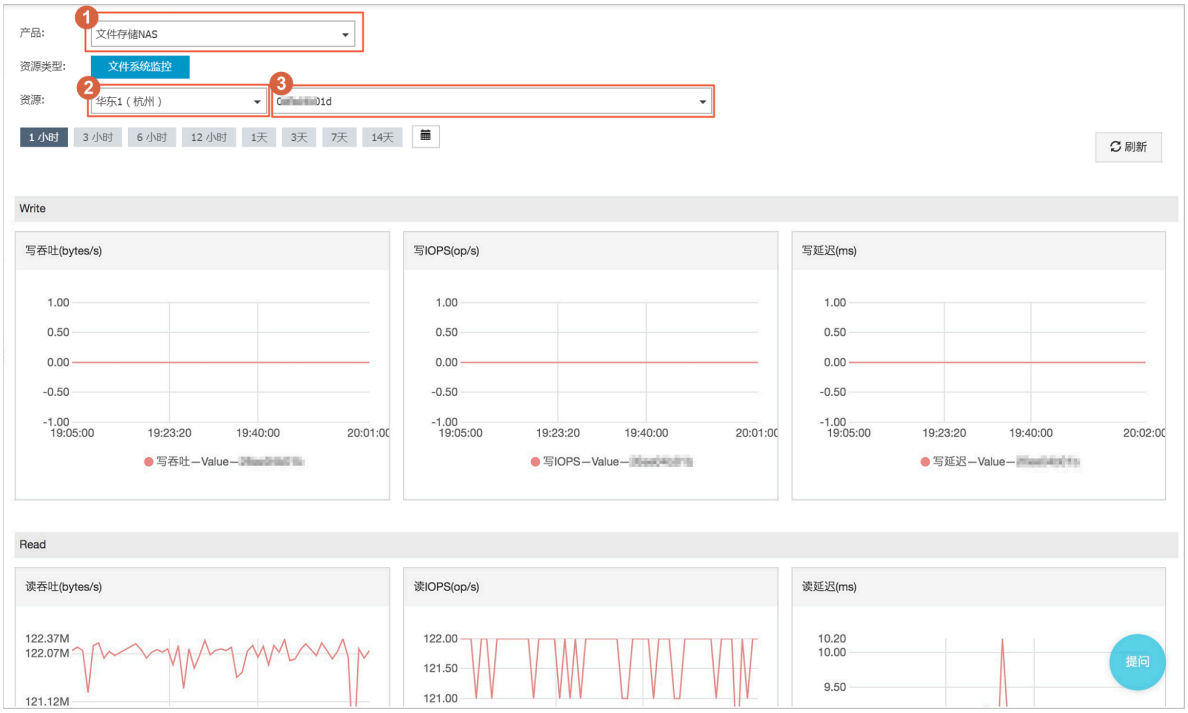
已创建文件系统，详情请参见创建文件系统。

背景信息

您可以使用云监控查看NAS文件系统的性能指标，并且配置相应的报警。目前支持的性能指标包括读写吞吐、IOPS、延时和元数据操作QPS，报警方式包括电话、短信、邮件等。

查看性能指标

1. 登录云监控管理控制台。
2. 在左侧导航栏，选择**Dashboard** > **云产品监控**。
3. 在**云产品监控**页面，选择**文件存储NAS**及对应的地域和文件系统，查看监控图表。



说明:

如果图表显示**无数据**，则说明您选择的文件系统长时间没有向服务端发起任何请求。如果要制造写吞吐监控数据，可以在挂载NAS的ECS上执行fio命令（假设NAS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`。

配置报警规则

1. 登录云监控管理控制台。
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**页面，配置相关信息。

配置项	说明
关联资源	在**关联资源**区域，配置以下参数。 • 在**产品**选项中，选择**文件存储NAS**。 • 在**资源范围**选项中，选择**文件系统**。 • 在**地域**选项中，选择目标文件系统所在地域。 • 在**文件系统**选项中，选择目标文件系统。
设置报警规则	根据需求设置报警规则，可添加多条报警规则，详细参数说明请参见#unique_54。
通知方式	设置报警通知对象及报警等级等信息。 单击**快速创建联系人组**，可创建联系人组，详情请参见创建报警联系人和报警联系组。 **说明:** 如果您要实现电话报警，请参见购买电话报警资源包。根据页面提示完成购买后可选中**电话+短信+邮件+钉钉机器人（Critical）**选项。

4. 单击**确认**，使报警规则设置生效。

   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，帮您及时得知监控数据异常并快速进行处理。

监控多个文件系统

如果您要监控多个文件系统，您可以通过应用分组方式实现。在**应用分组**页面中，设置分组，实现多个文件系统的监控。

1. 登录云监控管理控制台。

2. 设置分组。

   详情请参见#unique_56。

   a) 在左侧导航栏，选择**应用分组**，单击**创建组**。

   b) 在**创建应用分组**页面，配置相关参数。

配置项	说明
创建方式	选择应用分组的创建方式。本文以**标准组创建**为例配置相关参数。
应用分组名称	自定义配置分组名称。
联系人组	选择报警通知对象。 单击**快速创建联系人组**，可创建联系人组，详情请参创建报警联系人和报警联系组。
监控报警	从**选择模板**列表中，选择报警模板。从**通道沉默周期**列表中，选择重复发送报警通知的间隔时间。 启用初始化安装监控插件，系统将会对本组的服务器批量安装上监控插件，以便采集监控数据。
订阅事件通知	选中**订阅事件通知**后，分组内相关资源产生严重和警告级别事件时，将发送报警通知。

   c) 单击**创建应用分组**，完成分组。

3. 添加产品。

   a) 单击已创建的分组，进入详情页面。

   b) 在左侧导航栏，选择**组内资源**，单击**添加产品**。

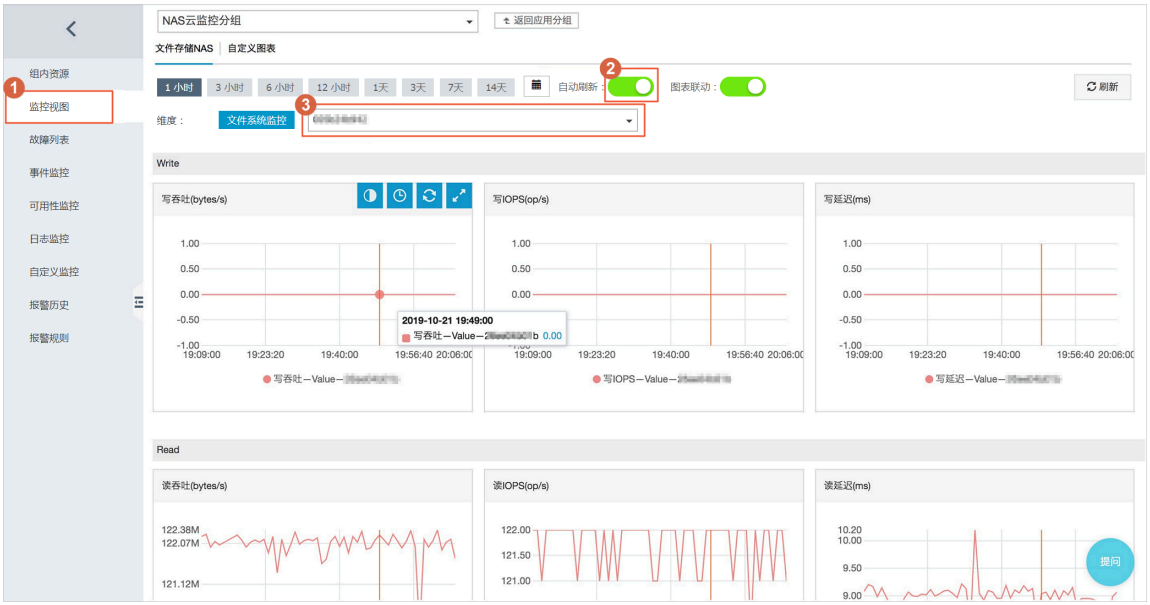
   c) 在**添加资源**页面，选择要监控的产品和实例。

   d) 单击**确认**，完成添加。

4. 查看监控图表。

a) 单击已创建的分组，进入详情页面。

b) 在左侧导航栏，选择**监控视图**，找到对应的文件系统，查看监控图表。



说明：

如果图表显示**无数据**，则说明您选择的文件系统长时间没有向服务端发起任何请求。如果要制造写吞吐监控数据，可以在挂载NAS的ECS上执行fio命令（假设NAS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`。

5. 配置报警规则。

a) 单击已创建的分组，进入详情页面。

b) 在左侧导航栏，选择**报警规则**。在**阈值报警**页签，单击**新建报警规则**。

c) 单击**添加规则**，配置相关信息。配置完成后，单击**确定**。

d) 配置**通道沉默周期**和**联系人组**，单击**添加**。

通过API获取监控数据

NAS的监控数据还可以通过云监控的API查询，主要API如下所示：

- #unique_57： 查询云监控开放的时序类指标监控项描述。
- #unique_58：查询指定时间段内的云产品时序指标监控数据。

- #unique_59：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	值
Namespace	acs_nas
MetricName	IopsRead、IopsWrite、LatencyRead、LatencyWrite、QpsMeta、ThruputRead、ThruputWriteIopsRead
Dimensions	{"userId":"xxxxxx","fileSystemId":"xxxxx"}

12 CPFS使用指南

CPFS是阿里云新上线的并行文件存储服务，专注于提供高性能的文件存储和访问能力。

CPFS支持以下功能和服务：

- #unique_61
- #unique_62
- #unique_63
- #unique_64
- #unique_65