阿里云
文件存储

使用指南

文档版本：20190124

为了无法计算的价值 | 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
	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，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **注意:** 您也可以通过按**Ctrl** + **A**选中全部文件。
>	多级菜单递进。	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。	单击 **确定**。
`courier 字体`	命令。	执行 `cd /d C:/windows` 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。	`swich` *`{stand | slave}`*

目录

1 管理文件系统

您可以在 NAS 控制台上对文件系统进行各类操作，如查看列表、查看文件系统实例详情、删除文件系统等。

前提条件

在对文件系统进行操作前，您需要：

1. 登录文件存储控制台。
2. 创建文件系统，或保证域内有创建完成的文件系统。

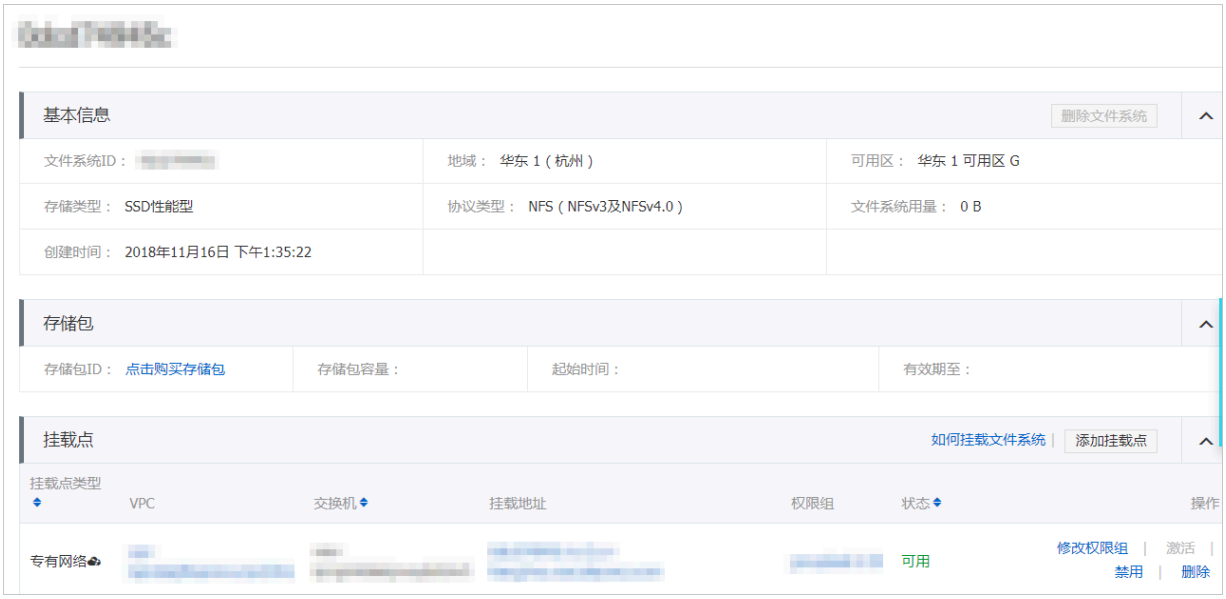
使用文件系统实例列表

单击控制台左侧导航栏的**文件系统列表**即可进入文件系统实例列表页面，如下图。

您可以在文件系统实例列表中对单个实例进行**修改备注名**、**添加挂载点**、**管理**和**删除**操作。

查看文件系统实例详情

单击文件系统实例列表上的**文件系统 ID**或右侧的**管理**可以进入**文件系统详情**页面，如下图。



详情页面分为上下两个部分：

- 上半部分展示了文件系统的基本信息，包括文件系统 ID、地域和可用区、文件系统容量等。
- 下半部分展示了文件系统挂载点列表，用户可以在这里对文件系统的挂载点进行管理。

删除文件系统

您可以单击文件系统实例列表右侧的**删除**删除文件系统。

注意:

- 只有当文件系统的挂载点数目为 0 时，用户才可以删除文件系统实例。
- 文件系统实例一旦删除，数据将不可恢复，请谨慎操作。

2 管理挂载点

您可以在 NAS 控制台上对文件系统实例的挂载点进行各类操作，如查看挂载点列表、删除挂载点、修改挂载点权限组、禁用和激活挂载点等。

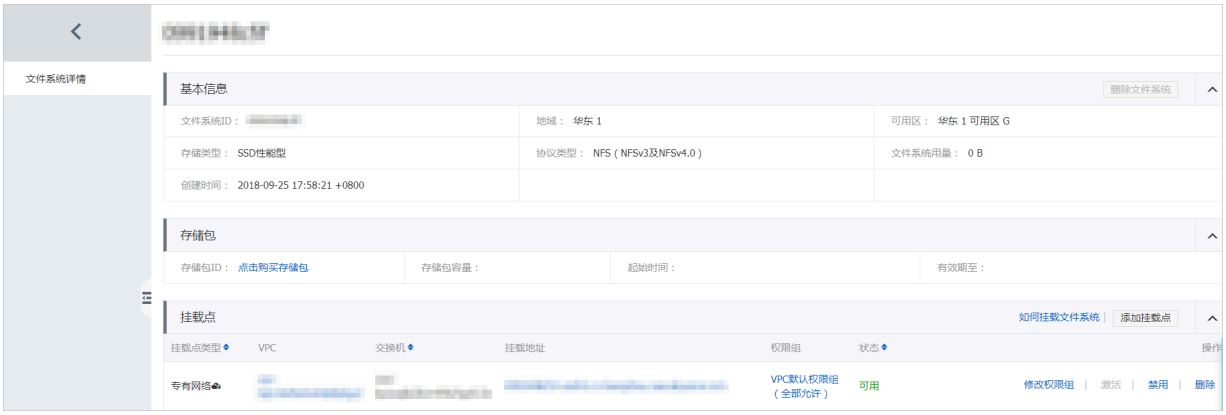
前提条件

在对文件系统的挂载点进行操作前，您需要：

1. 登录文件存储控制台。
2. 创建文件系统，或保证域内有创建完成的文件系统。
3. 添加挂载点，或保证文件系统实例内有添加完成的挂载点。

查看文件系统挂载点列表

在**文件系统列表**页面中单击目标文件系统实例的名称，进入**文件系统详情**页面。页面的下半部分会显示该文件系统实例的挂载点列表，您可以在这里管理挂载点，包括**添加挂载点**、**修改权限组**、**激活**、**禁用**和**删除**等。



添加挂载点

您可以为文件系统添加更多的挂载点，具体操作请参阅添加挂载点。

禁用和激活挂载点

您可以通过单击**禁用**暂时阻止任何客户端对该挂载点的访问，或者单击**激活**重新允许客户端对挂载点的访问。

删除挂载点

您可以单击**删除**来删除挂载点，挂载点删除后无法恢复。

> **注意:**
> 在删除一个 VPC 前，您必须删除 VPC 内的所有挂载点。

修改挂载点权限组

任何挂载点都必须绑定一个权限组，权限组通过指定源 IP 白名单的方式来限制 ECS 实例对挂载点的访问。您可以单击**修改权限组**修改挂载点的权限组。

> **注意:**
> 修改权限组操作生效最多会有 1 分钟延迟。

3 管理文件系统数据访问权限

在 NAS 中，您可以使用权限组管理用户文件系统中的数据访问权限。

权限组简介

在文件存储 NAS 中，权限组是一个白名单机制，通过向权限组添加规则，来允许指定的 IP 或网段访问文件系统，并可以给不同的IP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VPC 默认权限组，该默认权限组允许 VPC 内的任何 IP 以最高权限（读写且不限制 root 用户）访问挂载点。

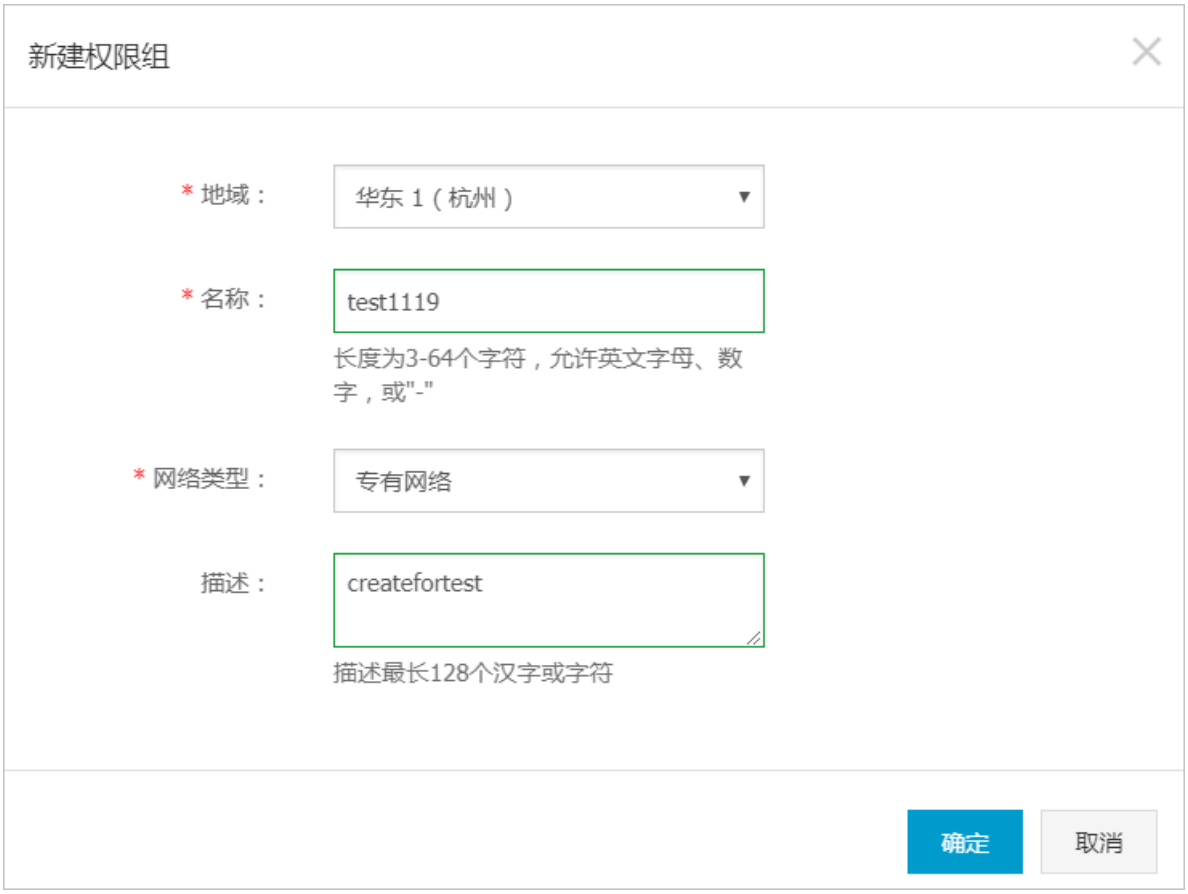
注意:

- 经典网络类型挂载点不提供默认权限组，且经典网络类型权限组规则授权地址只能是单个 IP 而不能是网段。
- 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。

创建权限组

您可以按照以下步骤创建权限组。

1. 登录文件存储控制台。
2. 单击左侧的**权限组**，然后单击右上角的**新建权限组**。
3. 输入权限组名称，即可创建一个新的权限组。



注意:

一个阿里云账号最多可以创建 10 个权限组。

管理权限组规则

您可以按照以下步骤管理权限组规则，包括添加、编辑和删除。

1. 登录文件存储控制台。
2. 单击左侧的**权限组**，在权限组列表中单击**管理规则**。
3. 在权限组规则页面中：
   - 如果您还未创建权限组规则，您可以单击右上角的**添加规则**为权限组添加规则。

权限组规则包含以下四个属性，分别是：

属性	取值	含义
授权地址	单个 IP 地址或网段（经典网络类型只支持单个 IP）	本条规则的授权对象。
读写权限	只读、读写	允许授权对象对文件系统进行只读操作或读写操作。

属性	取值	含义
用户权限	不限制 **root** 用户 **(no_squash)**、限制 **root** 用户 **(root_squash)**、限制所有用户 **(all_squash)**	是否限制授权对象的 Linux 系统用户对文件系统的权限。 在判断文件或目录访问权限时： - 不限制 **root** 用户 **(no_squash)**将允许使用 root 用户访问文件系统。 - 限制 **root** 用户 **(root_squash)**将把 root 用户视为 nobody 处理。 - 限制所有用户 **(all_squash)**将把包括 root 在内的所有用户都视为 nobody。
优先级	1-100，1 为最高优先级	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。

- 如果您已经创建了权限组规则，您可以单击已创建的权限组规则右侧对应的**编辑**或**删除**按钮，对该权限组规则进行编辑或者删除。

4 管理文件系统资源访问权限

您可以使用 RAM 为子用户授权，使其获得文件存储 NAS 的操作权限。为了遵循最佳安全实践，强烈建议您使用子用户来操作文件存储 NAS。

RAM 中可授权的文件存储 NAS 操作

在 RAM 中可以为子用户授予以下 NAS 操作的权限。

操作（**Action**）	说明
DescriptFileSystems	列出文件系统实例
DescriptMountTargets	列出文件系统挂载点
DescriptAccessGroup	列出权限组
DescriptAccessRule	列出权限组规则
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

RAM 中可授权的文件存储 NAS 资源抽象

在 RAM 授权策略中，文件存储 NAS 仅支持以下资源抽象：

资源（**Resource**）	注解
*	表示所有文件存储 NAS 资源

授权策略示例

以下示例中的授权策略允许对文件存储 NAS 所有资源的只读操作。

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

5 NAS备份服务

文件存储NAS备份服务已经开始公测。该服务提供了操作便捷、策略灵活的备份支持。

简介

NAS 备份服务能够接管整个备份流程，帮助您方便地完成整个自动化备份任务，将您从繁琐的人工操作与多版本管理中解放出来。您可以在控制台中快速定义备份任务。

NAS备份服务具有以下特性：

- 支持周期性备份。您可以指定备份间隔，每隔一段时间启动一次新的备份。目前支持的间隔为6/8/12/24小时。
- 支持多备份历史版本保存。每进行一次备份会生成一个新的备份版本。您可以设置需要保留的版本数。保留的版本数目最大为9。
- 支持基于备份的数据恢复。您可以选定特定版本的备份，将其恢复到一个文件系统。为了最大程度避免误操作，恢复目标必须是空文件系统。
- 支持手动触发新的备份任务。您可以手动地、即时地触发一个新的备份任务。这在自动备份的基础上为您提供了更加灵活的备份策略。

申请公测

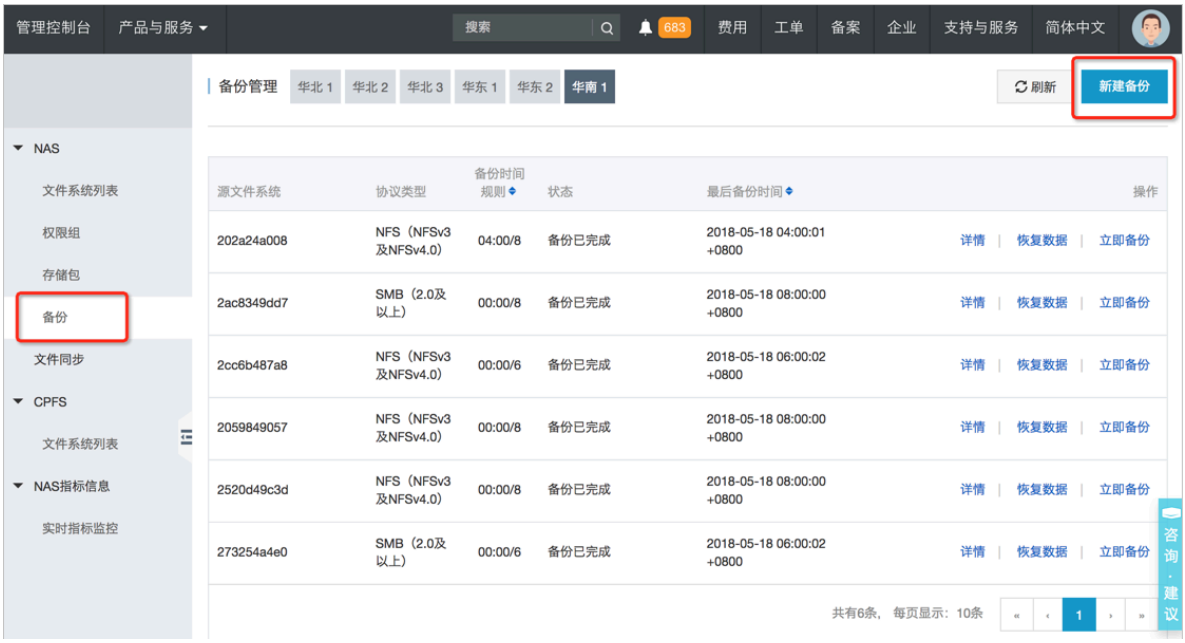
使用NAS备份服务需要申请公测资格，申请界面如下：

您可以登录需要在NAS的控制台主页上进行申请。申请时需要填写公司名称以及需求。申请公测完成并在后端审核通过后，备份页面将被开启，如下图所示：

创建备份任务

获取公测资格后，您可以进行文件系统的备份。创建备份方法如下：

1. 登录文件存储控制台。
2. 单击备份，单击右上角的新建备份，如下图所示：



3. 在弹出的对话框中选择需要备份的源文件系统（即要备份的对象），如下图所示：

创建备份任务中的其他选项描述如下：

- **开始时间**：目前只提供3个时间点供选择，分别是0点8点和16点。
- **备份间隔**：目前可选择6小时、12小时和24小时。一般情况下，推荐选择24小时，并将备份放在业务低峰时间。
- **备份保留份数**：指备份时需要保留最新版本的个数。

4. 创建备份任务完成后，备份服务会根据备份策略自动运行备份任务。

注意:

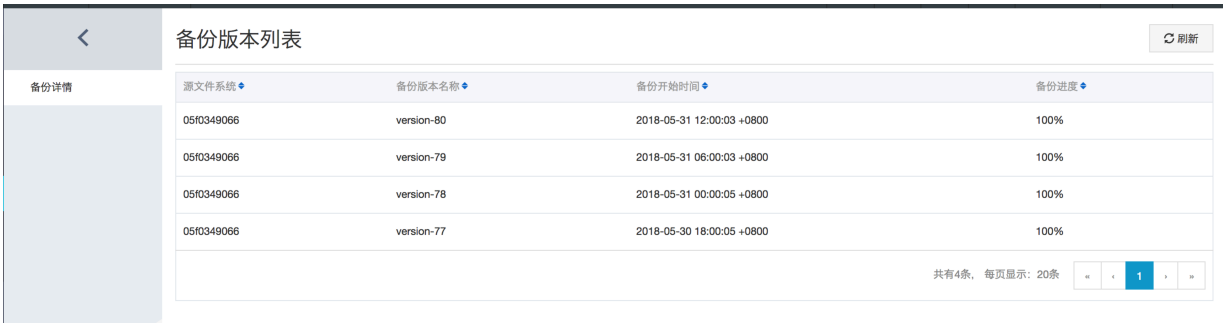
您也可以在**备份**页面中单击源文件系统右侧的**立即备份**，人工触发一次备份，如下图所示：

数据恢复

备份服务目前支持将备份恢复到一个空的NAS文件系统上，恢复界面如下：

您只需选择目标NAS文件系统及希望恢复的源文件系统备份版本号，即可将特定版本的备份恢复到目标文件系统。

关于希望恢复的源文件系统备份版本号，可在备份详情页中查找，如下图所示：



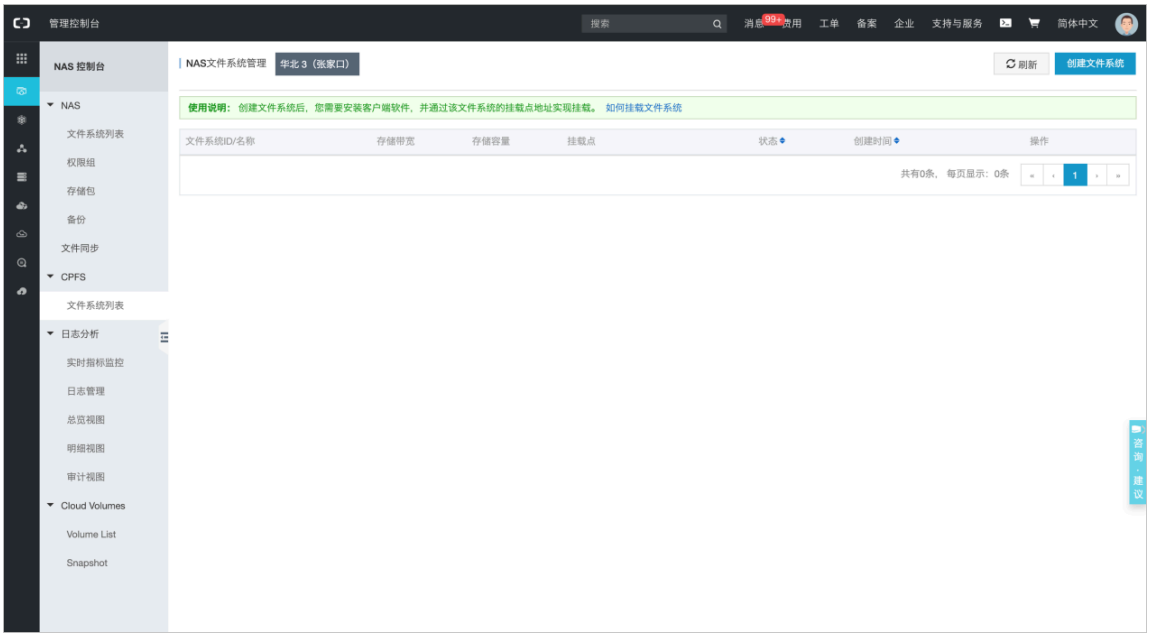
6 CPFS使用指南

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。

使用 CPFS 的操作步骤如下：

1. 创建文件系统

   a. 登录阿里云文件存储控制台，在左侧边栏选择**CPFS**，如下图所示：



   b. 单击右上角创建文件系统按钮，进入购买页面。

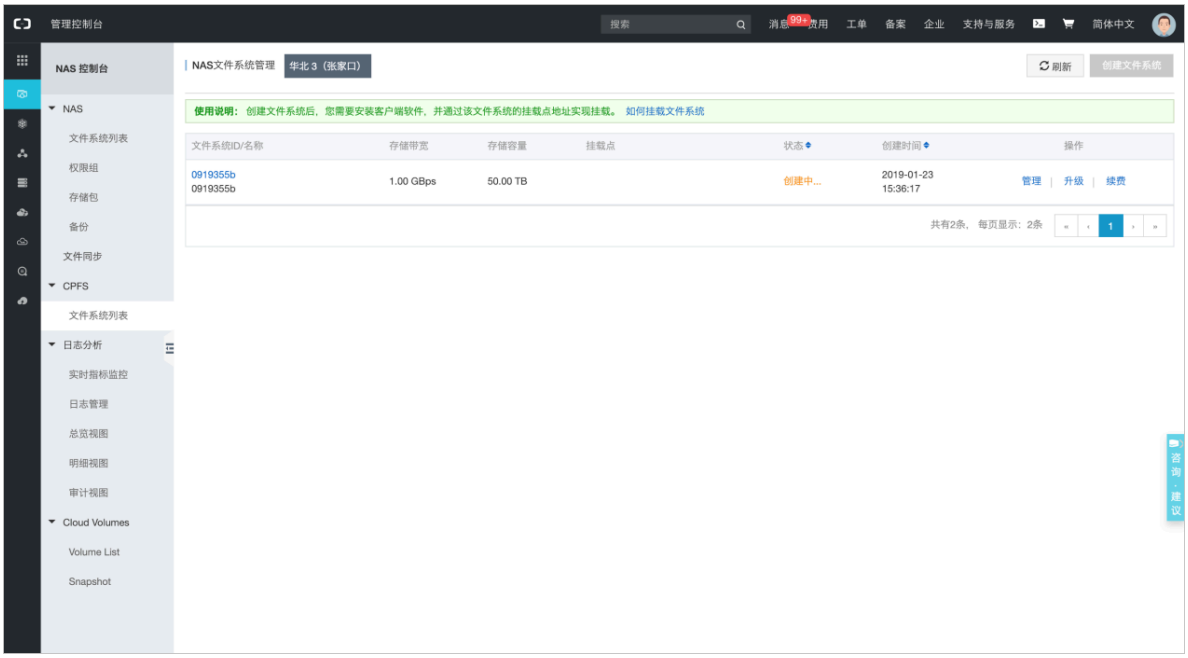
c. 请根据您自身需求进行基本配置、网络配置和购买量的选择。

- 基本配置需要选定地域、可用区和文件系统的容量。
- 网络配置需要选定指定地域内的专有网络和虚拟交换机。若您还未创建，请先前往阿里云专有网络控制台进行相关配置。
- 购买量的选择需要选定文件系统实例数量和服务时长。

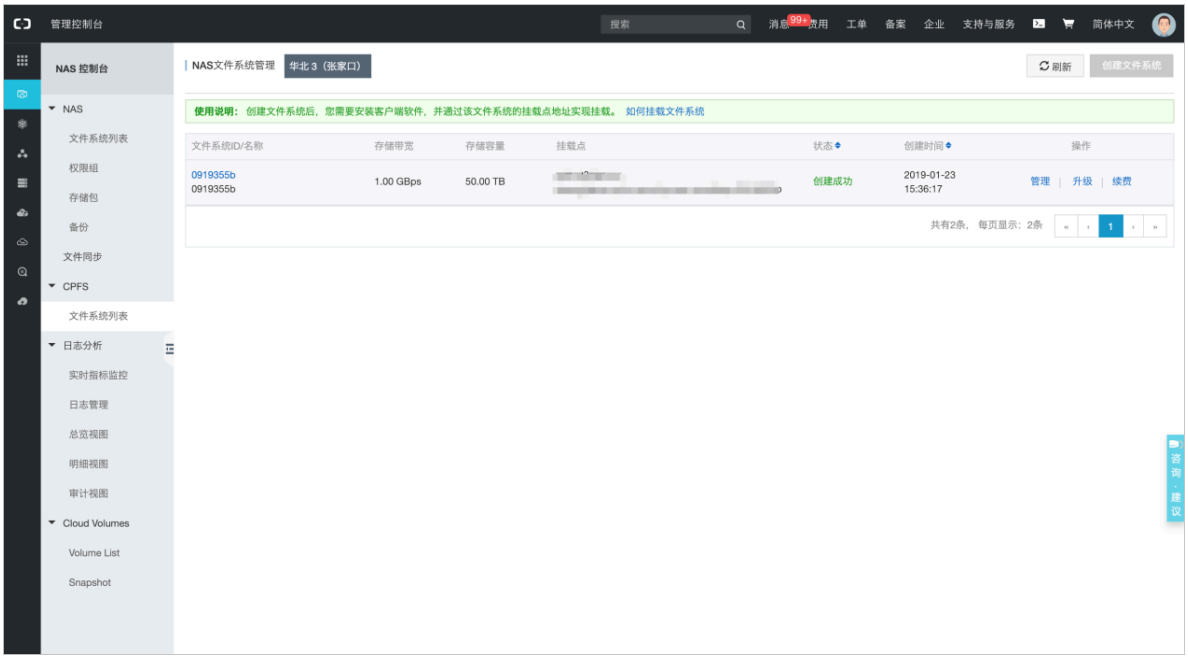
CPFS服务目前采用预付费模式（即包年包月），服务期间您可以根据自身业务增长情况选择升级存储量，服务到期您可以选择续费。

2. 管理文件系统

购买成功后，回到阿里云文件存储控制台，即可看到您的CPFS实例正在创建中。



CPFS实例创建过程大约需要10分钟，创建成功后，如下图所示：



您可以选择单击管理按钮，查看实例详情；单击升级按钮进行容量升级；单击续费按钮进行服务续费。

3. 使用文件系统

   CPFS文件系统创建完成后，在客户端ECS上进行挂载即可使用。

   a. 下载并安装客户端软件包

   b. 配置文件统挂载点

      使用控制台展示的文件系统挂载点进行挂载配置。

   c. 挂载CPFS文件系统

   d. 使用CPFS文件系统

      CPFS文件系统兼容POSIX语义，可以使用Linux的常见操作命令（如`ls`等）进行访问和操作文件系统。

7 数据迁移

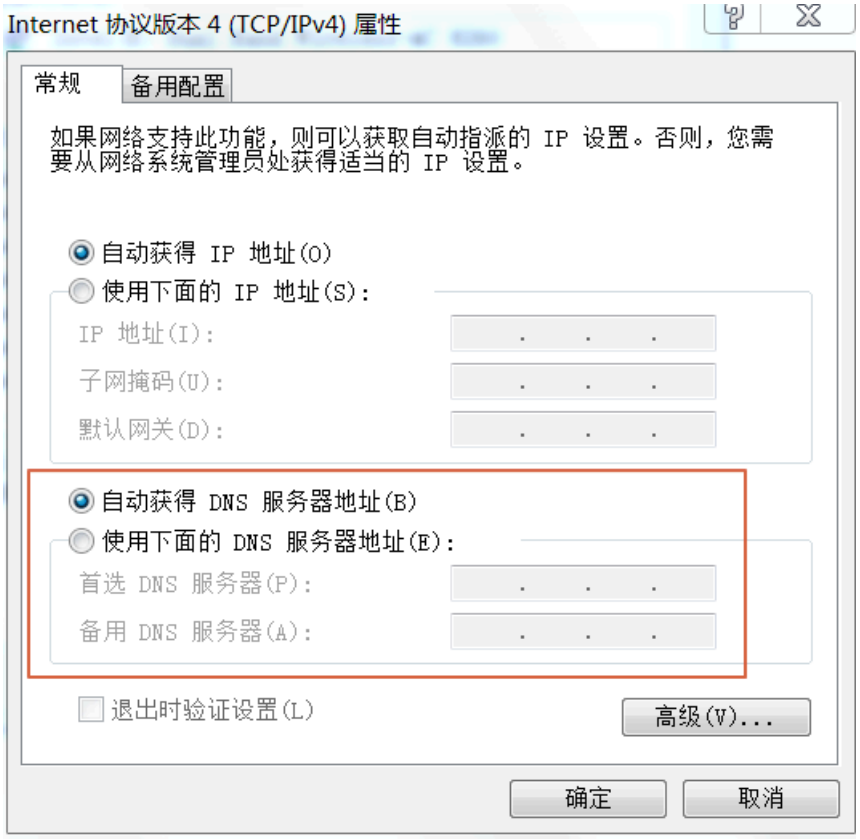
7.1 通过专线网络从线下IDC将数据迁移至阿里云NAS

7.1.1 环境准备

在将数据从线下 IDC 迁移至阿里云NAS前，需要进行必要的准备和配置。

在使用专线网络进行数据迁移前，您需要进行以下准备：

- 根据 IDC 机房所在的地域，在阿里云上选择举例机房最近的区域，创建目标 NAS 文件系统、VPC 和挂载点。
- 申请高速通道服务专线，并接入 NAS 挂载点所在的VPC，具体操作请参见物理专线接入。
- 联系阿里云客服，获取对应区域的内网 DNS 服务 IP 地址。
- 在线下 IDC 的服务器上配置 DNS 服务 IP 地址，并使用ping命令测试网络至挂载点域名的连通性。在不同操作系统中配置 IP 地址的方法如下：
  - 在 Windows 中按照下图配置 IP 地址：



- 在 Linux 中，使用`vi`编辑`/etc/resolve.conf`，增加参数，如下所示：

```
nameserver xx.xx.xx.xx
```

7.1.2 线下IDC使用NAS存储设备时的数据迁移

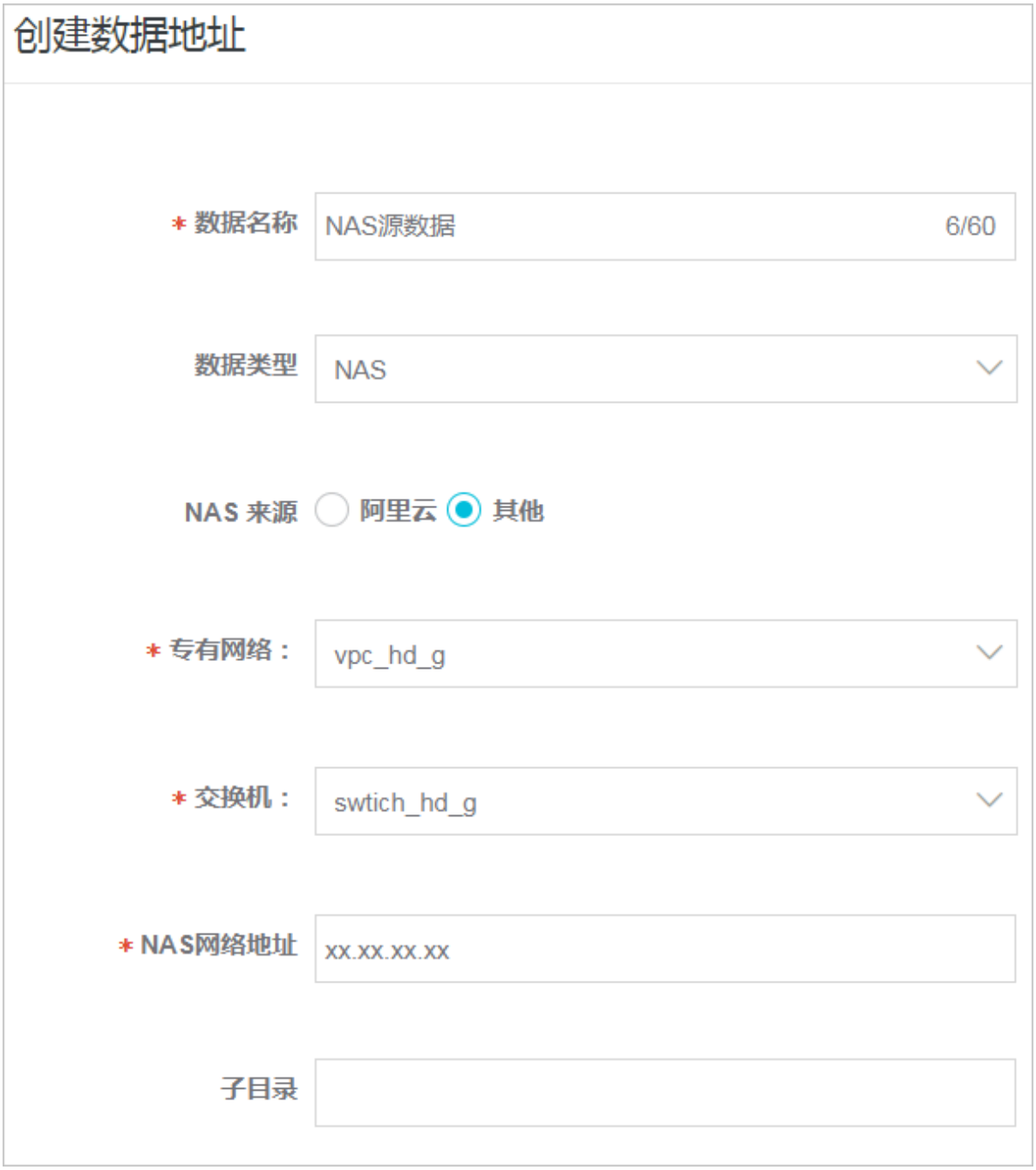
如果线下 IDC 使用 NAS 存储设备，您可以使用 FileSync 服务将文件系统数据从线下的 NAS 设备迁移至阿里云 NAS。

操作步骤

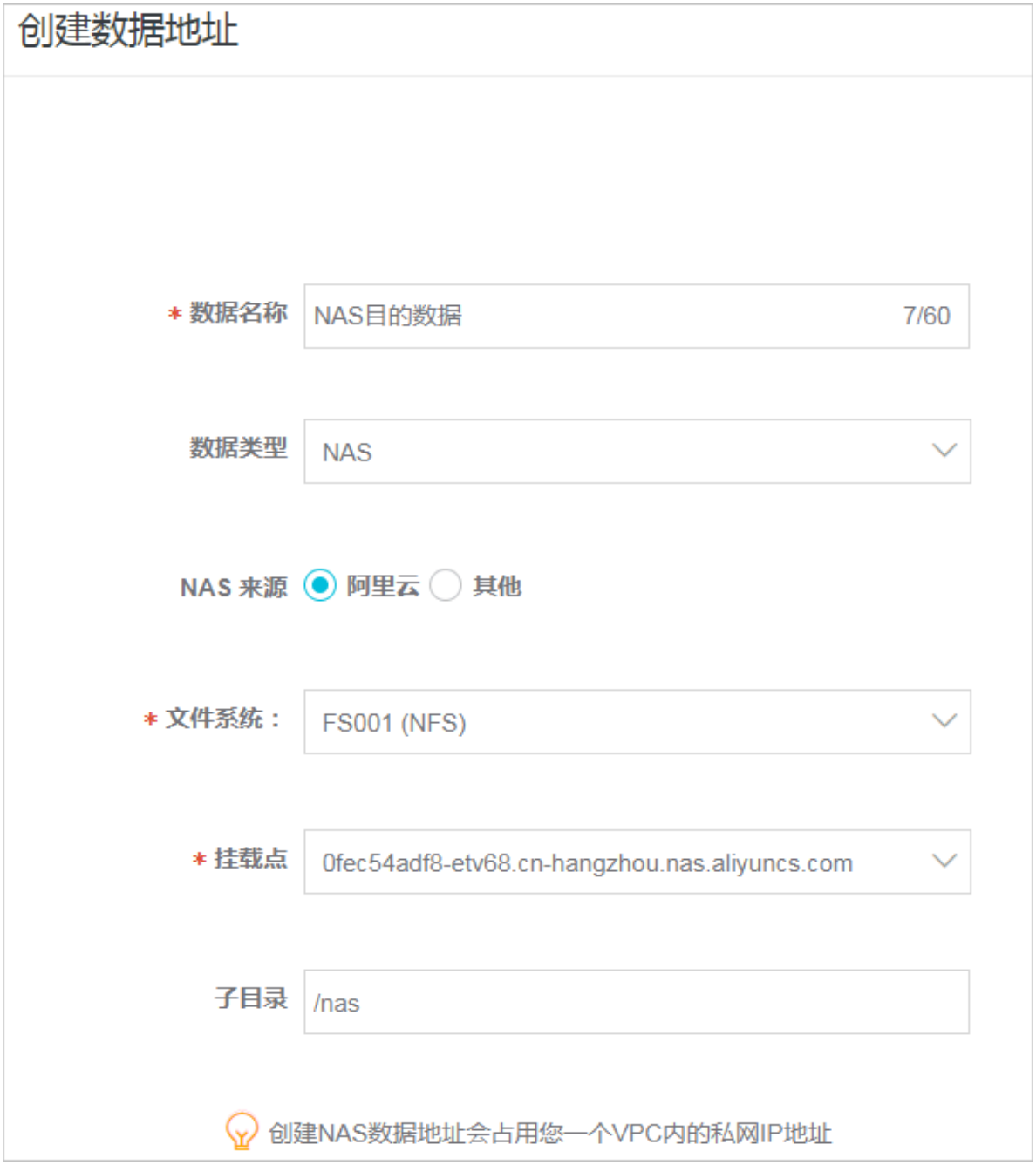
1. 登录文件存储控制台，单击文件同步。

2. 在管理同步任务页面中，单击数据地址。

3. 在管理数据地址页面中，单击创建数据地址，在创建数据地址对话框中，选择其他，将线下 IDC 的 NAS 地址配置为源 NAS 数据地址。



4. 在管理数据地址页面中，单击创建数据地址，在创建数据地址对话框中，选择阿里云，将阿里云 NAS 地址配置为目的 NAS 数据地址。



5. 返回管理同步任务页面，单击创建同步任务。
6. 在创建同步任务对话框中，在源地址中选择线下 IDC 的 NAS 地址，在目的地址中选择阿里云的 NAS 地址，单击确定。

7. 在管理同步任务页面中查看同步任务的状态。

7.1.3 线下IDC使用本地磁盘时的数据迁移

如果线下 IDC 使用本地磁盘作为存储设备，您可以使用 nas_tool 软件将文件系统数据从线下 IDC 迁移至阿里云 NAS。

前提条件

进行迁移前，在计算节点的系统内安装 JAVA JDK 1.7 及以上版本。您可以在Oracle官网进行下载。

操作步骤

1. 在线下 IDC 客户的计算节点上下载 nas_tool 软件，下载链接如下：*https://nasimport.oss-cn-shanghai.aliyuncs.com/nas_tool.zip*。
2. 将*nas_tool.zip*解压缩至工作目录。
3. 将阿里云 NAS 文件系统挂载到线下 IDC 客户的计算节点，具体方式请参见通过VPN网关实现从用户IDC或者跨地域挂载文件系统。
4. 执行迁移脚本，不同操作系统中的操作如下：
   - 在 Windows 系统中，运行`cmd`，执行`cd`命令进入 nas_tool 所在的目录，运行以下命令：
     ```
     copy.bat <src_dir> <dst_dir>
     ```
   - 在 Linux 系统中，打开 terminal， 执行`cd`命令进入 nas_tool 所在的目录，运行以下命令：
     ```
     sh copy.sh <src_dir> <dst_dir>
     ```

7.2 通过公网从线下IDC将数据迁移至阿里云NAS

7.2.1 将线下IDC文件系统数据迁移到OSS

通过公网从线下 IDC 迁移数据到阿里云 NAS 时，需要先使用 ossutil 将数据迁移至阿里云 OSS。

操作步骤

1. 在阿里云创建 OSS 存储空间，并获取对应子账号的 AccessKey。
2. 下载 ossutil。

   各版本的 binary 下载地址如下：
   - [Linux x86 32bit] ：*ossutil32*
   - [Linux x86 64bit] ：*ossutil64*
   - [Windows x86 32bit] ：*ossutil32.zip*

- [Windows x86 64bit] ：*ossutil64.zip*
- [Mac x86 64bit] ：*ossutilmac64*

3. 安装 ossutil。
   - 在 Linux 中，运行下载的 binary 文件。

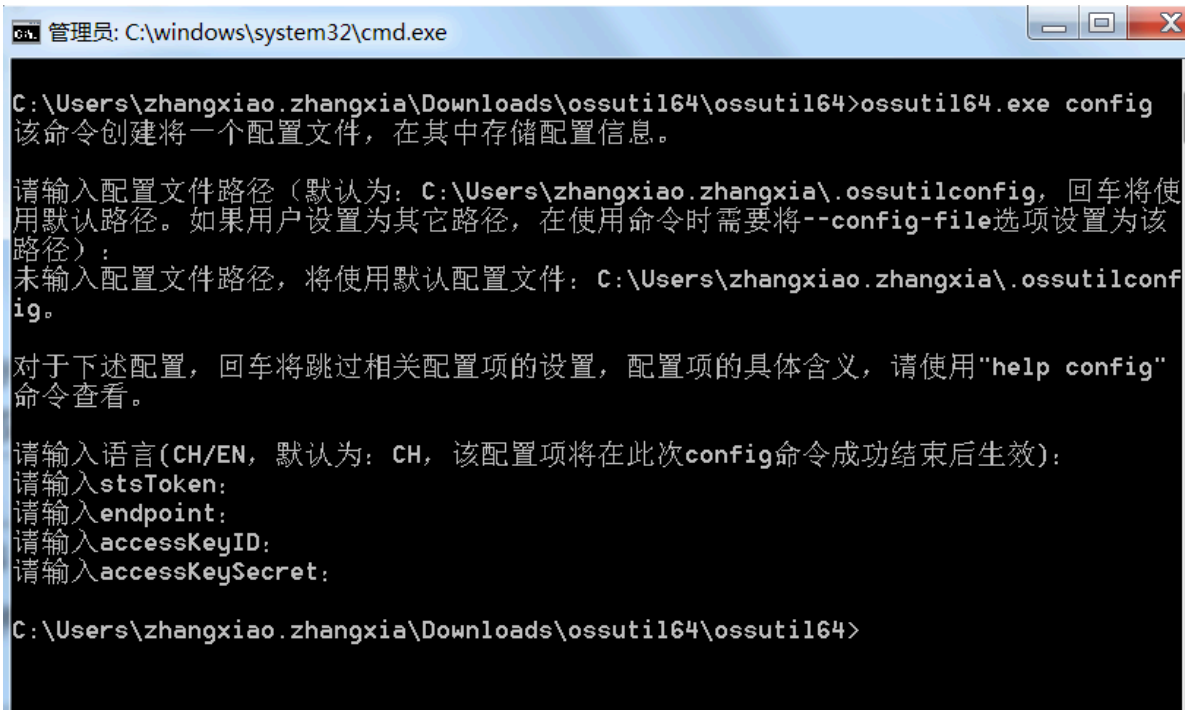
     ```
     ./ossutil config
     ```

     注意:

     如果 binary 为不可执行文件，请运行`chmod 755 ossutil`给 binary 增加可执行权限。
   - 在 Windows 系统中，解压下载的压缩包，双击运行其中的 bat 文件，输入`ossutil64.exe`。
   - 在 Mac OS 中，执行以下命令：

     ```
     ./ossutilmac64 config
     ```

4. 在显示的 ossutil 交互界面中，按照提示输入配置参数。Windows 中的界面如下：



注意:

配置参数中，**accessKeyID** 和 **accessKeySecret** 是必选项。

5. 运行以下命令，启动拷贝。

```
./ossutil cp -r userdir oss://ossutil-test
```

> **注意:**
>
> 命令中*userdir*是用户待上传的目录，*oss://ossutil-test*是用户创建的 OSS 存储空间，请根据实际参数输入。

7.2.2 将数据从OSS迁移到NAS

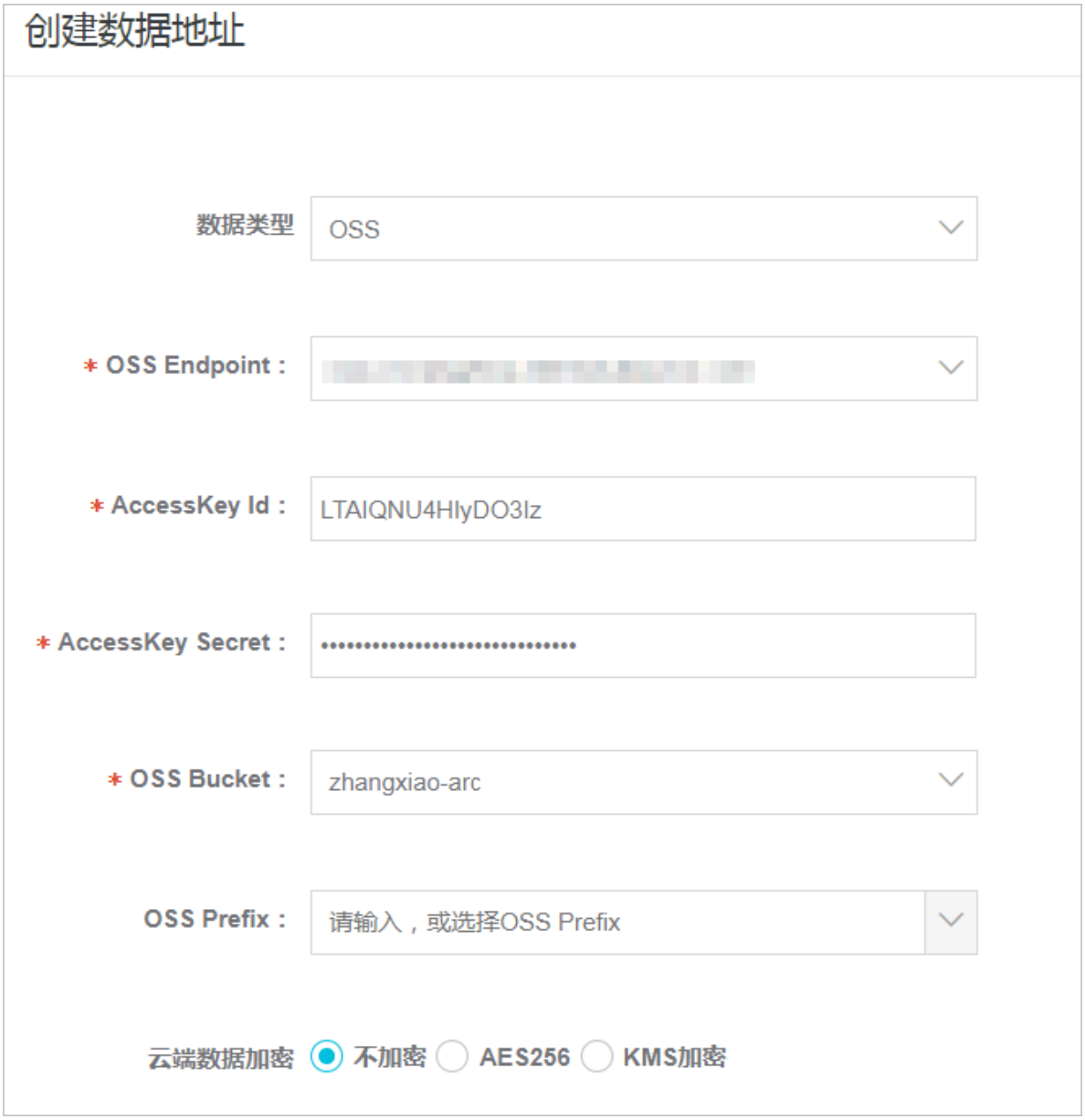
将线下 IDC 文件系统数据迁移至 OSS 后，您可以使用 FileSync 服务将文件系统数据从 OSS 迁移至 NAS。

操作步骤

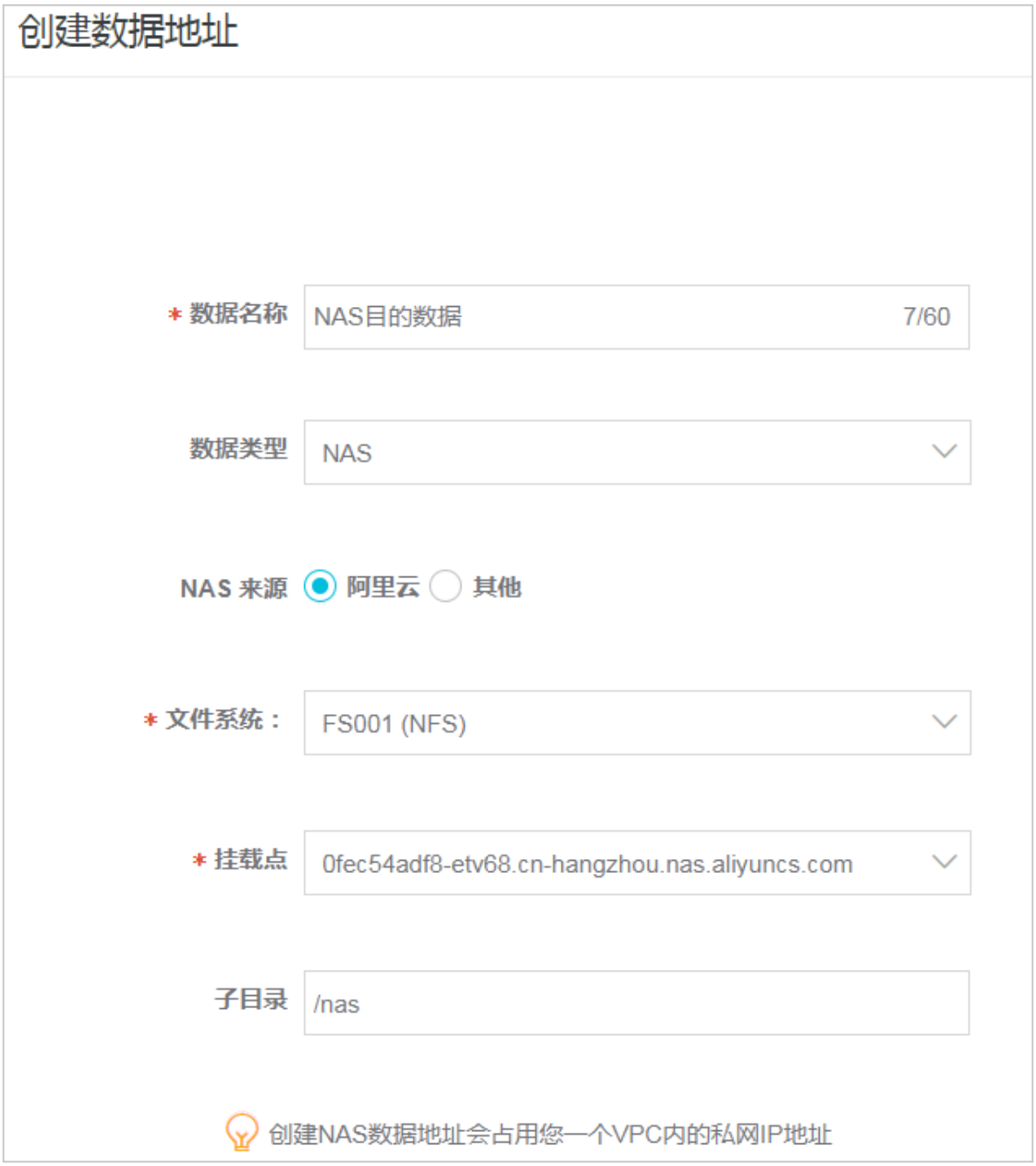
1. 登录文件存储控制台，单击文件同步。

2. 在管理同步任务页面中，单击数据地址。

3. 在管理数据地址页面中，单击创建数据地址，在创建数据地址对话框中，数据类型选择**OSS**，将 OSS 的地址配置为源数据地址。



4. 在管理数据地址页面中，单击创建数据地址，在创建数据地址对话框中，数据类型选择**NAS**，**NAS**来源选择阿里云，将 NAS 地址配置为目的 NAS 数据地址。



5. 返回管理同步任务页面，单击创建同步任务。
6. 在创建同步任务对话框中，在源地址中选择 OSS 地址，在目的地址中选择 NAS 地址，单击确定。

7. 在管理同步任务页面中查看同步任务的状态。

8 数据安全

8.1 NAS NFS传输加密

8.1.1 NAS NFS传输加密公测资格申请

NAS NFSv4 的传输加密功能已在华北1区的容量型 NAS 产品中开始公测。您可以在 NAS 控制台申请公测资格。

背景信息

在申请公测资格并使用前，您需要了解以下内容：

- 与非传输加密版本相比，NAS NFS 传输加密版本的延迟及IOPS会有约10%的损耗。
- NFS 传输加密会在客户端使用 stunnel 进行 TLS 加密代理。对于吞吐型应用，stunnel 会消耗大量 CPU 资源用于加密与解密。在较为极端的场景下，单个挂载点可能会消耗 100% 的 CPU 资源。这种情况下，应用的吞吐也会受到限制。

操作步骤

1. 登录文件存储控制台。
2. 选择区域**华北1**，然后在 NAS NFS 传输加密公测信息右侧单击**申请**。

3. 在提交申请对话框中，输入联系方式、邮箱地址、公司名称和使用场景，然后单击提交。

4. 在控制台首页的 NAS NFS 传输加密公测信息右侧，单击**查询申请状态**。

5. 在**查询申请状态**对话框中查看申请审核是否通过。

   如显示如下信息，表示审核已经通过，您可以开始试用 NAS NFS 传输加密功能。

8.1.2 下载安装NFS传输加密客户端

公测资格申请通过后，您需要下载并安装 NFS 传输加密客户端以使用传输加密功能。

背景信息

NFS 传输加密客户端支持以下操作系统：

- Aliyun Linux 17.1
- Red Hat Enterprise Linux (以及衍生版 CentOS) version 7 及以上
- Ubuntu 16.04 LTS及以上
- Debian 8及以上

NFS 传输加密客户端依赖以下内容，这些内容会在安装工具时自动安装。

- NFS client (nfs-utils 包或 nfs-common 包)
- Stunnel (版本4.56或者以上)
- Python (版本2.7或者以上)
- OpenSSL (版本1.0.2或者更新)

操作步骤

1. 登录文件存储控制台。
2. 选择区域**华北1**，选择一个类型为容量型，支持协议为 NFS 的文件系统，单击其名称。

> **注意:**
> 如果在当前区域没有符合条件的文件系统，您可以新建一个类型为容量型，支持协议为 NFS 的文件系统。有关新建文件系统的详细步骤，请参阅创建文件系统。

3. 在文件系统的详情页面，单击客户端工具下载。

4. 按照提示下载 rpm 或 deb 格式的安装包。
5. 运行命令，安装 NFS 传输加密客户端。各系统中的安装命令如下：

- Aliyun Linux/CentOS 7+：

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

- Red Hat 7+：

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

- Ubuntu 16+/Debian 8+：

```
sudo apt update
sudo dpkg -i aliyun-alinas-utils-*.deb（该步骤会报错，请忽略，直接执行下一步）
sudo apt-get install -f
```

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

6. 运行`man mount.alinas`命令，检查安装是否完成。

   如果运行上述命令后能显示帮助文档，则说明客户端安装成功。

8.1.3 使用NFS传输加密客户端挂载文件系统

下载安装 NFS 传输加密客户端后，您可以使用该客户端加密挂载 NAS 文件系统。

背景信息

NFS 传输加密客户端能够通过 TLS 方式挂载文件系统，并在挂载时使用阿里云 NAS 推荐的挂载选项。同时，该客户端还提供了日志功能，便于在挂载出错时定位错误原因。

NFS 传输加密客户端定义了一个新的网络文件类型：*`alinas`*。该文件类型能够与标准的 `mount` 命令无缝兼容。客户端还支持在系统启动时自动挂载文件系统，您可以在*`/etc/fstab`*文件中添加相关参数完成。使用NFS 传输加密客户端进行 TLS 挂载时，工具会启动一个 stunnel 进程和一个监控进程 aliyun-alinas-mount-watchdog. stunnel 进程会对应用与 NAS 间的读写进行 TLS 加密并转发给 NAS 服务器。

操作步骤

1. 登录文件存储控制台。
2. 创建一个新的挂载点，详细步骤请参阅添加挂载点。

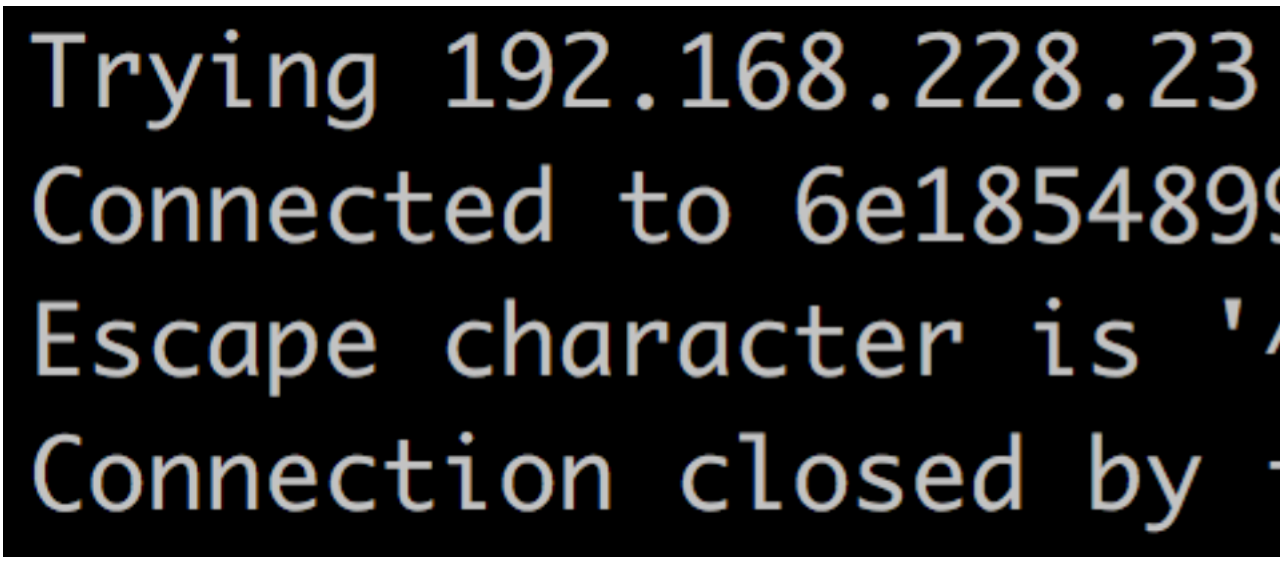
   注意:

   文件系统中原有的挂载点不支持通过 TLS 方式挂载文件系统，因此必须要创建一个新的挂载点。

3. 运行以下命令，检查新建的挂载点是否支持传输加密。

```
telnet 6e1854899b-rvp48.cn-qingdao.nas.aliyuncs.com 12049
```

如果出现以下界面，则表示挂载点支持传输加密。其中`6e1854899b-rvp48.cn-qingdao.nas.aliyuncs.com`为新建的挂载点的名称。



4. 运行以下命令，挂载文件系统。

```
sudo mount -t alinas -o tls file-system-mountpoint alinas-mount-point/
```

示例：`sudo mount -t alinas -o tls 6062949200-xxxx.cn-qingdao.nas.aliyuncs.co /mnt`

5. 运行以下命令，添加其他挂载参数。

```
sudo mount -t alinas -o tls,noresvport 6062949200-xxxx.cn-qingdao.nas.aliyuncs.com /mnt
```

注意:

NFS 传输加密工具默认使用以下选项挂载文件系统：

- vers=4.0
- rsize=1048576
- wsize=1048576
- hard
- timeo=600
- retrans=2

6. 在*/etc/fstab*中添加以下 entry，开启自动挂载：

```
file-system-mountpoint local-mount-point alinas _netdev,tls 0 0
```

示例：`6062949200-xxxx.cn-qingdao.nas.aliyuncs.com /mnt alinas _netdev,tls 0 0`

8.1.4 日志功能

NFS 传输加密工具支持日志记录功能，便于您在挂载失败时定位错误。

NFS 传输加密工具记录的日志保存在*/var/log/aliyun/alinas/*目录中。您可以更改日志配置文件*/etc/aliyun/alinas/alinas-utils.conf*来自定义日志记录功能。

 注意:

NFS 传输加密工具在执行挂载时，会使用 127.0.1.1 - 127.0.255.254 中可用的 IP 作为 stunnel 的 IP 地址，并使用端口60001。在进行配置之前，请确保该 IP 地址段和端口在您的机器上可用，否则传输加密工具无法正常使用。

配置文件中的配置项及说明如下：

配置项	说明
logging_level	日志级别
logging_max_bytes/logging_file_count	日志文件的最大容量以及数量，客户端会自动对日志进行rolling。
stunnel_debug_enabled	是否记录 stunnel debug 日志，默认为关闭。开启时，会显著占用磁盘空间
stunnel_check_cert_hostname	检查证书域名，不支持所有 stunnel 版本。默认关闭。
stunnel_check_cert_validity	检查证书合法性，不支持所有 stunnel 版本。默认关闭。
mount-watchdog相关配置	不建议改动。

 注意:

更新日志配置后，需要 umount 文件系统并重新 mount 后才能使配置生效。