

阿里云 文件存储NAS

最佳实践

文档版本：20190809

法律声明

阿里云提醒您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。	 说明： 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 。
<code>courier</code> 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
<code>##</code>	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
<code>[]</code> 或者 <code>[a b]</code>	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
<code>{ }</code> 或者 <code>{a b}</code>	表示必选项，至多选择一个。	<code>swich {stand slave}</code>

目录

法律声明.....	I
通用约定.....	I
1 高性能网站.....	1
1.1 Windows IIS 服务挂载 NAS 共享文件存储.....	1
1.2 Nginx 代理服务器阿里云文件存储 NAS.....	23
2 应用服务器共享存储.....	28
2.1 Windows系统使用NFS协议挂载NAS共享文件存储.....	28
3 远程访问文件系统.....	37
3.1 本地IDC VPN网络访问阿里云文件存储.....	37
3.2 本地 IDC NAT 网关访问阿里云文件存储.....	39
3.3 使用 SFTP 上传下载 NAS 文件系统数据.....	44
4 使用 Windows Server Backup 从 ECS 备份数据到 NAS.....	46
5 通过云服务器ECS (Linux) 访问SMB文件系统.....	57

1 高性能网站

1.1 Windows IIS 服务挂载 NAS 共享文件存储

本文介绍如何结合阿里云 NAS 的 SMB 协议支持 ECS Windows 虚拟机，使用 Windows 内置的互联网信息服务（IIS）来提供 Web 和 FTP 服务。

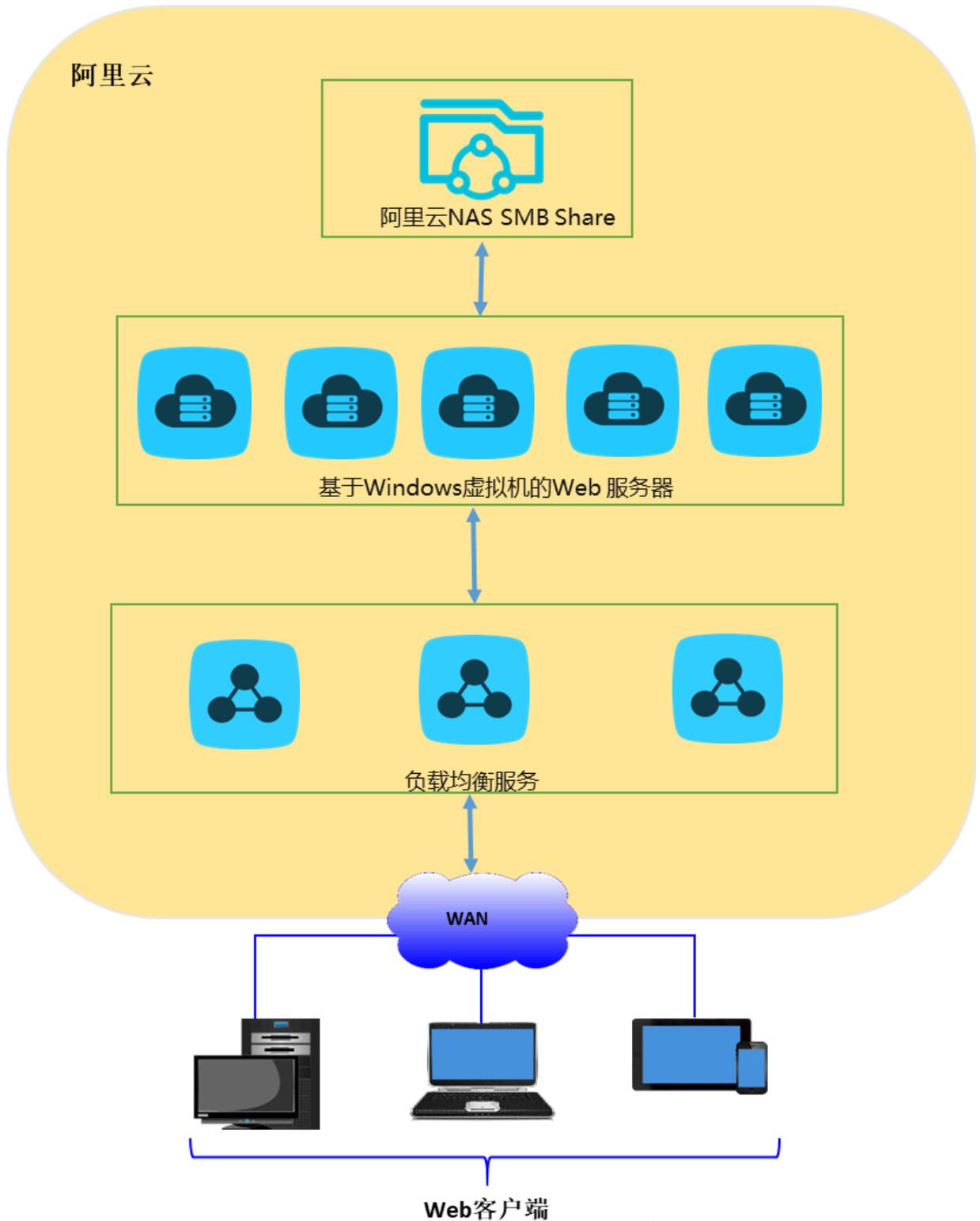
阿里云文件存储服务 NAS 主要面向阿里云 ECS 实例、E-HPC、容器服务、弹性 Web 和 BatchCompute 等计算节点提供文件存储服务。通过标准的文件访问协议 NFS 和 SMB，用户无需对现有应用做任何修改即可在云上使用。

背景和基本信息

与 NFS 相比，SMB 文件系统访问协议更加适合于 Windows 客户端。各个版本的 Windows 对 SMB 协议都能很好的支持，绝大多数 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。因此，阿里云建议应用集中运行在 ECS Windows 实例上的用户优先考虑使用 SMB 文件系统。

阿里云是目前市场上唯一一个全面支持 NFS 和 SMB 协议的公共云厂商。阿里云 NAS 支持 SMB 2.1 及以上的 SMB 协议版本，支持 Windows 7 / Windows Server 2008 R2 及以上的各 Windows 版本，不支持 Windows Vista / Windows Server 2008 及以下的各 Windows 版本。与 SMB 2.1 及以后的版本相比，SMB 1.0 协议设计的巨大差异在性能和功能的上有严重的不足，同时只支持 SMB 1.0 或更早协议版本的 Windows 产品都已经完全退出微软支持的生命周期。如果用户创建新 Windows 实例，建议至少选择 Windows 2008 R2 以上的版本。

Windows Server 目前仍然是非常流行的网站建构平台。到2017年2月止，全球仍然有超过43%站点的 Web Server 采用微软 IIS（来自 Netcraft February 2017 Web Server Survey），很多网站和博客系统也是基于内容管理系统例如WordPress、Joomla 等在 Windows 平台得以实现。在阿里云现有的用户中，有不少用户选择用阿里云 ECS 提供的独享 Windows 虚拟机来提供网站服务。通过将网站内容资源集中存储在一个高可靠、高吞吐、按量付费的阿里云 SMB share 上，IIS 可以像访问本地文件系统一样访问阿里云 NAS 上的数据，从而让用户的网站可以实现存储和计算服务的分离。此外，计算资源和存储资源都可以支持按需弹性扩容，通过阿里云提供的负载均衡服务由多个虚拟机来共同承载一个弹性容错的网站架构。



IIS 提供的 FTP 服务也同样有着非常广泛的需求。例如，很多 Web 站点的管理员通过 FTP 来远程管理 Web 站点的内容，同时还有很多用户希望利用 Windows 虚拟机上的 FTP 服务在广域网和阿里云之间传输和共享文件。

基本设置

我们以 IIS 7.5（Windows Server 2008 R2）的设置为例，展示如何通过阿里云 NAS 在阿里云上提供提供单节点的 Web 和 FTP 服务。其它 Windows 服务器版本如 Windows Server 2012 的安装和部署也类似。用户可以进一步使用阿里云负载均衡服务来建构多服务器节点的弹性容错的站点。

具体方法请参阅[阿里云负载均衡文档](#)。

在公网环境里提供 Web 和 FTP Service 的阿里云 ECS 虚拟机由于服务的开放性容易受到安全攻击。本文档的设置步骤着重说明如何在功能上连接 Web 服务与 NAS 存储，提出某些安全性的考虑，但不能作为完整的安全配置和实现方案。用户需要承担安全方面的所有最终责任，从系统级别（如设置防火墙、ECS 实例安全组和及时安装操作系统补丁）和服务级别（如使用阿里云的各个安全产品）来全面保障自己网站服务和数据的安全性。

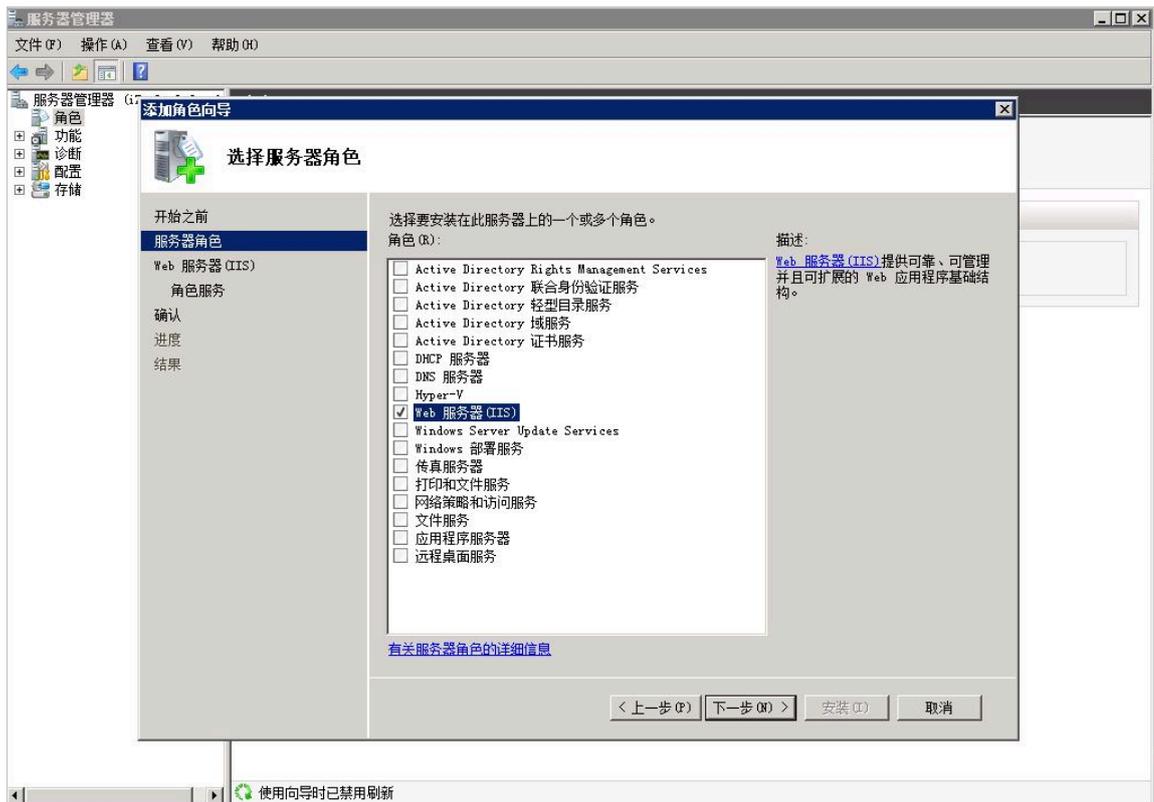
· IIS 安装:

以 Windows Server 2008 R2 为例，通过服务器管理器添加 IIS 角色并安装 IIS 的过程如下图所示。在不同 Windows 操作系统上安装 IIS 的详细过程请参阅下面的微软在线文档:

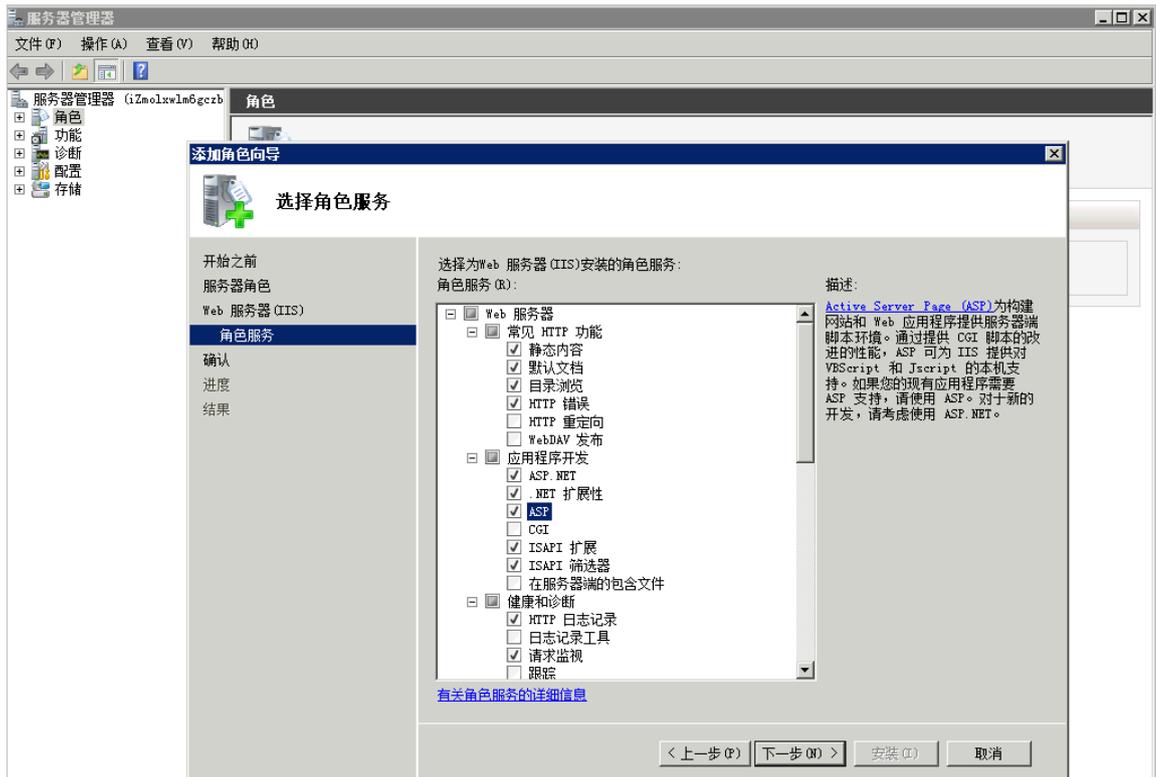
IIS 7 的安装和部署

安装 IIS 和 ASP.NET 模块 (Windows Server 2012 和 Windows Server 2012 R2)

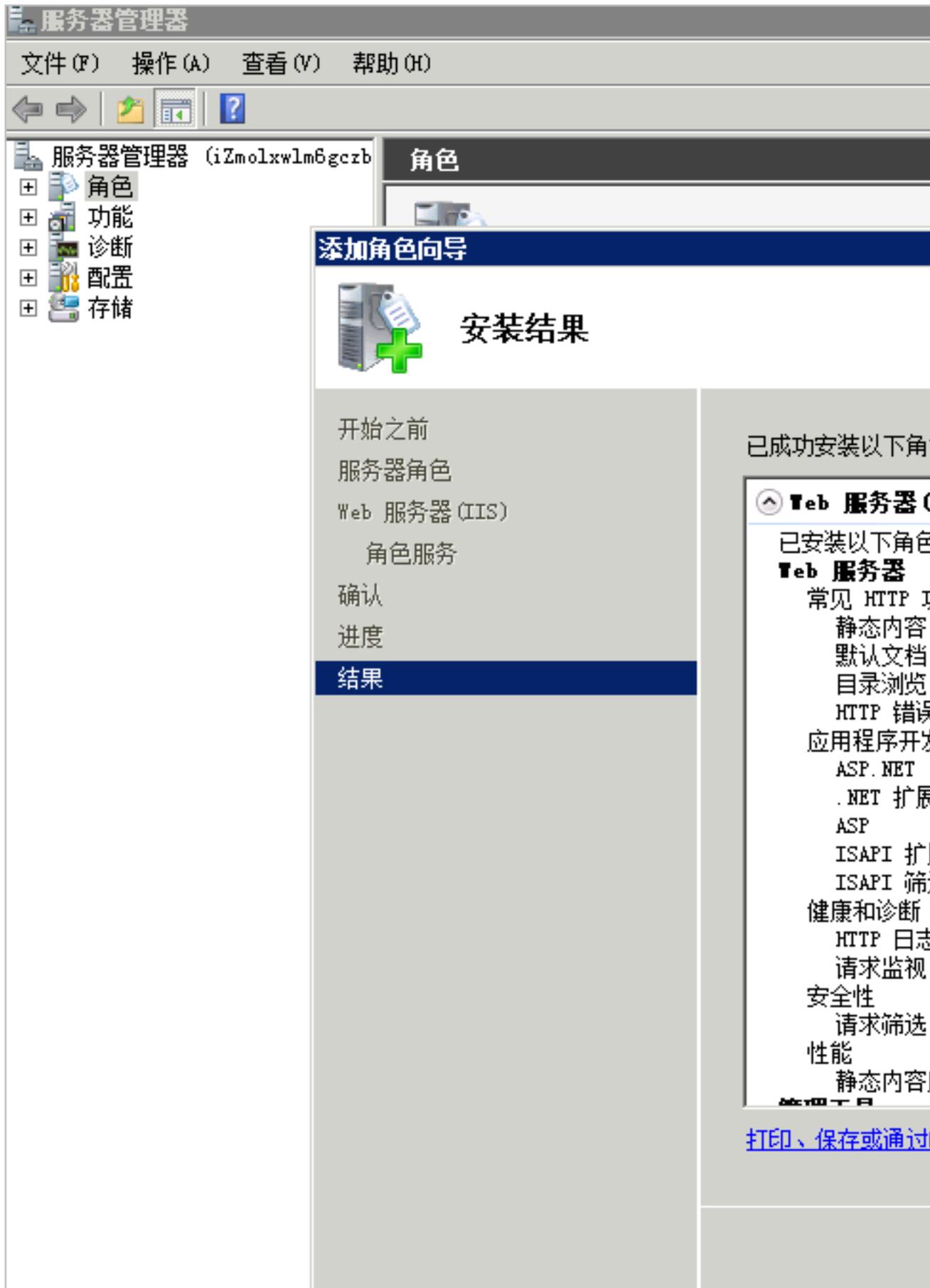
1. 用户在服务器管理器中选择添加 Web 服务器 (IIS) 角色。



2. 用户选择为 Web 服务器安装的角色服务，除基本的 HTTP 功能以外，我们还包括了 FTP 服务及扩展、ASP 服务等，用于 FTP over SSL 服务和演示动态网页脚本的使用。



3. 单击安装，以下是安装成功的提示界面。



- NAS SMB 文件系统的创建和设置：

您的 Web 服务资源及配置文件可以集中存储在阿里云 NAS 的一个 SMB share 上。创建了一个支持 SMB 的阿里云 NAS 文件系统之后，通过设置权限组来保证当前 Web 服务器可以读写访问 SMB share 对应的文件系统。您可以使用 VPC 或者经典网络来连接 NAS 文件系统和 Web 服务器。创建和使用阿里云 NAS SMB 文件系统的具体步骤请参考阿里云博客《[阿里云文件存储 SMB 协议服务及其申请和使用指南](#)》。

创建 SMB 文件系统后，您可以在文件系统的缺省 share > myshare 下创建目录 www 来存储网站文件。本示例中，在 myshare\www 下创建两个文件来说明静态网页 index.html 和动态 ASP 脚本 test.asp 的操作流程。前者显示 Hello World!，后者动态获取并显示当前时间。

Index.html

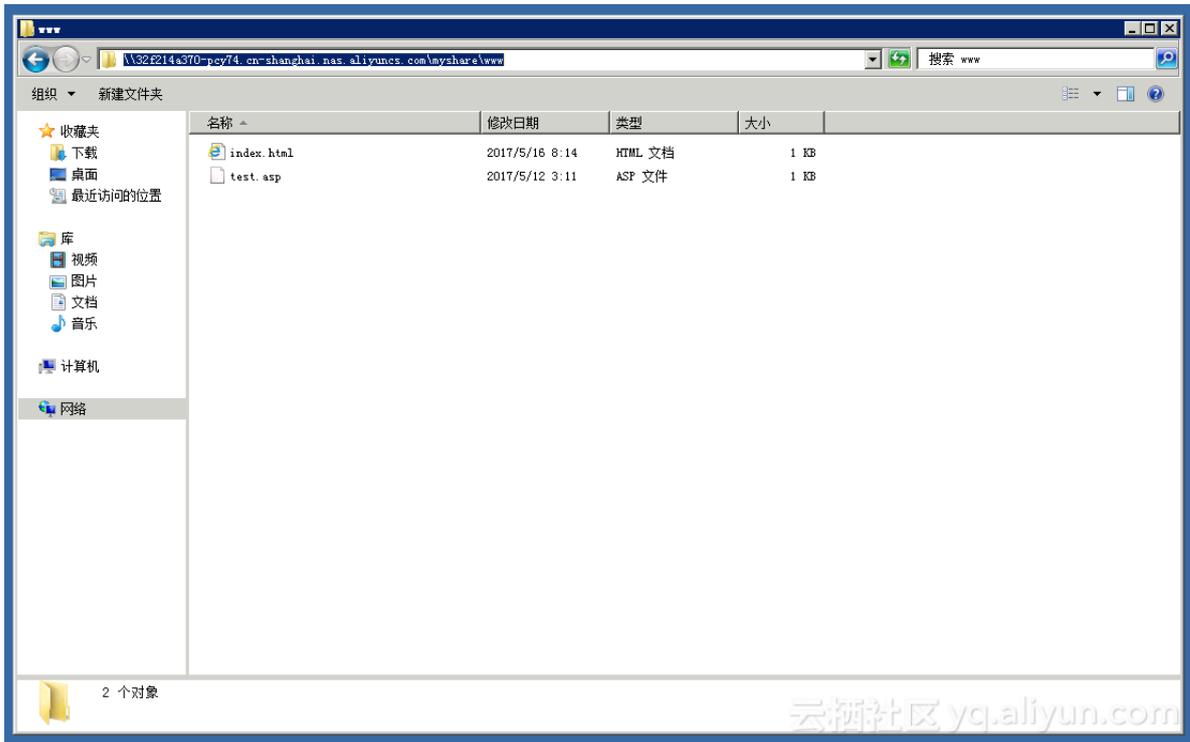
```
<HTML>
  <HEAD>
    <TITLE>Hello World in HTML</TITLE>
  </HEAD>
  <BODY>
    <CENTER><H1>Hello World!</H1></CENTER>
  </BODY>
</HTML>
```

Test.asp

```
<HTML>
  <BODY>
    This page was last refreshed on <%= Now() %>.
  </BODY>
</HTML>
```

如下图所示，当前的 ECS 虚拟机用户可以通过 Windows 文件管理器来验证对 SMB share 的访问。在本示例中，\32f214a370-pcy74.cn-shanghai.nas.aliyuncs.com\myshare

\www是网站资源的物理路径，其中\32f214a370-pcy74.cn-shanghai.nas.aliyuncs.com\myshare为阿里云NAS SMB share。

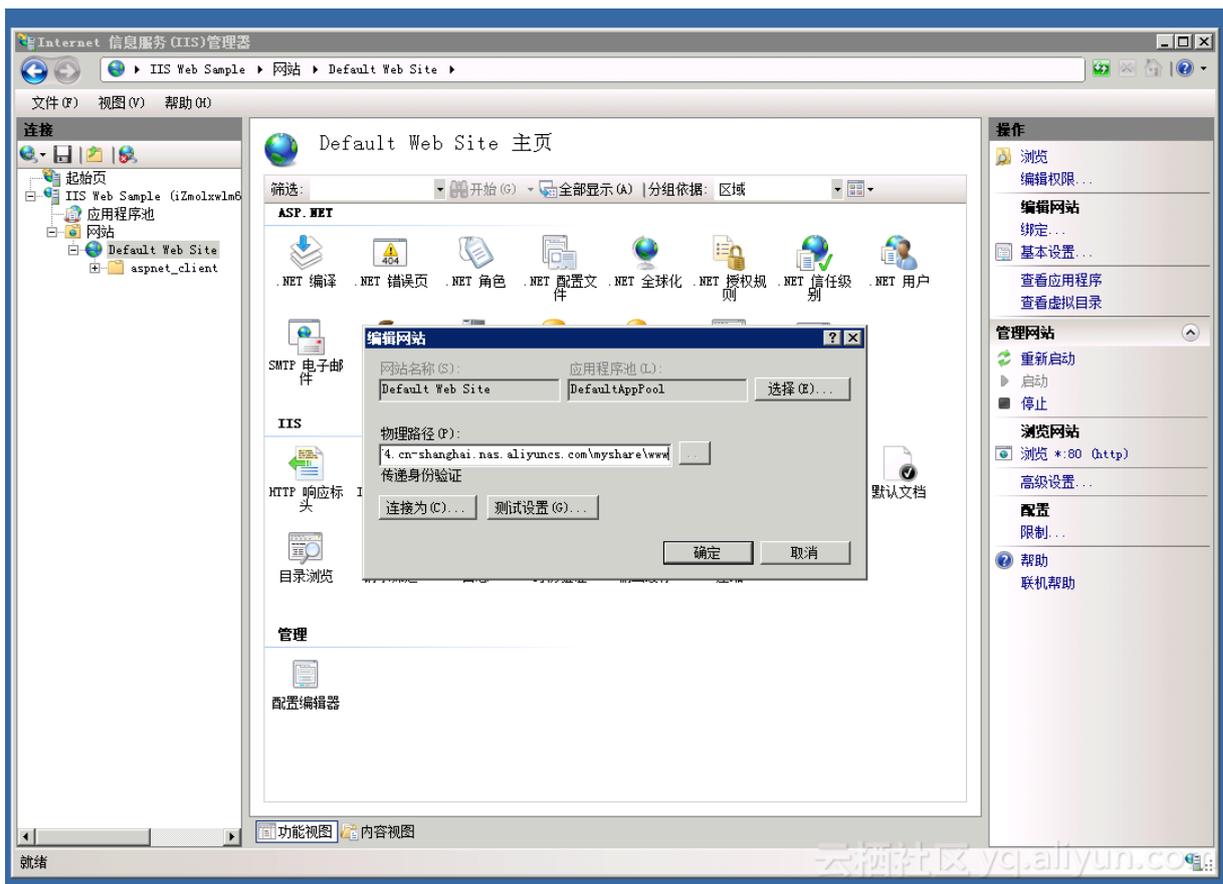


出于安全和管理考虑，我们在系统里还加入了一个新用户 iis_user。在提供 FTP 服务或者在 Windows Server2016 上运行时，我们选择通过该用户而不是系统管理员来进行数据访问。

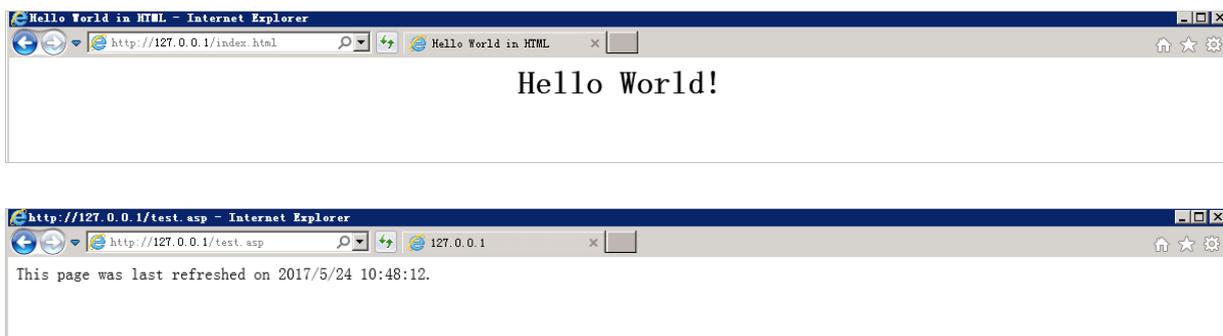
IIS Web 服务的设置

如下图所示，Windows Server2008 R2 的用户打开网站的基本设置，并在编辑网站的交互窗口中将物理路径设置为网站资源在阿里云 NAS 上的存储路径。这里我们输入 UNC 地址\32f214a370-pcy74.cn-shanghai.nas.aliyuncs.com\myshare\www作为网站资源的物理路径。

 **说明:**
由于 IIS 缺省通过 IIS 的应用程序账号和用户组访问，Windows 桌面用户不可直接使用在当前 user session 中映射的网络驱动器如 (Z:\)，否则会出现访问失败的错误。



通过用本地浏览器访问 localhost 或者 127.0.0.1 的 index.html 和 test.asp，我们可以确认 IIS 现在已经可以正常进行 Web 服务了。服务器用户可以进一步设置阿里云安全组和 Windows 防火墙来进行 Web 访问安全的限制。

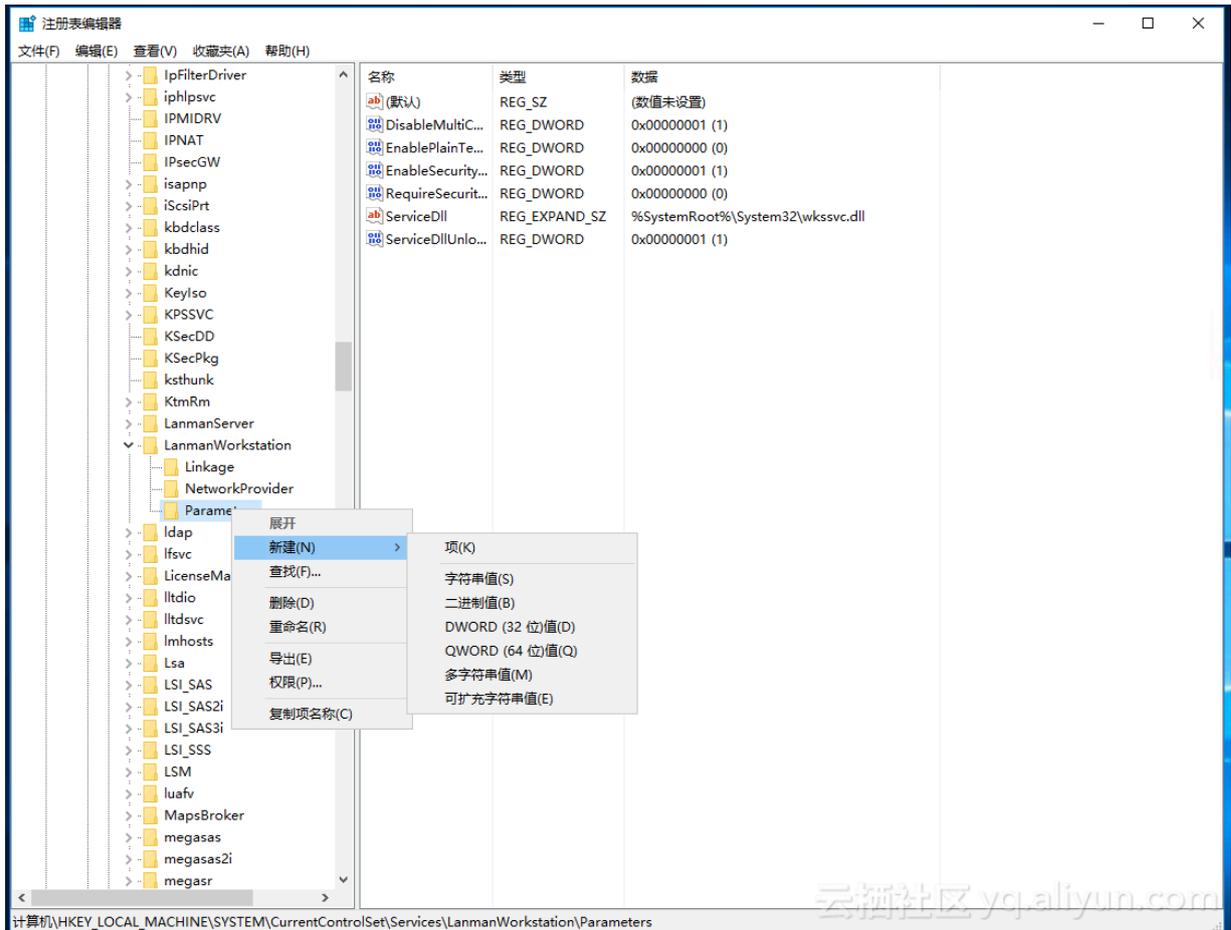


对于Windows Server 2016 的用户来说，由于微软在该产品周期做的几个改动，目前需要通过以下的两个额外设置来让 IIS 和阿里云 NAS 的 SMB 服务正确协同工作。

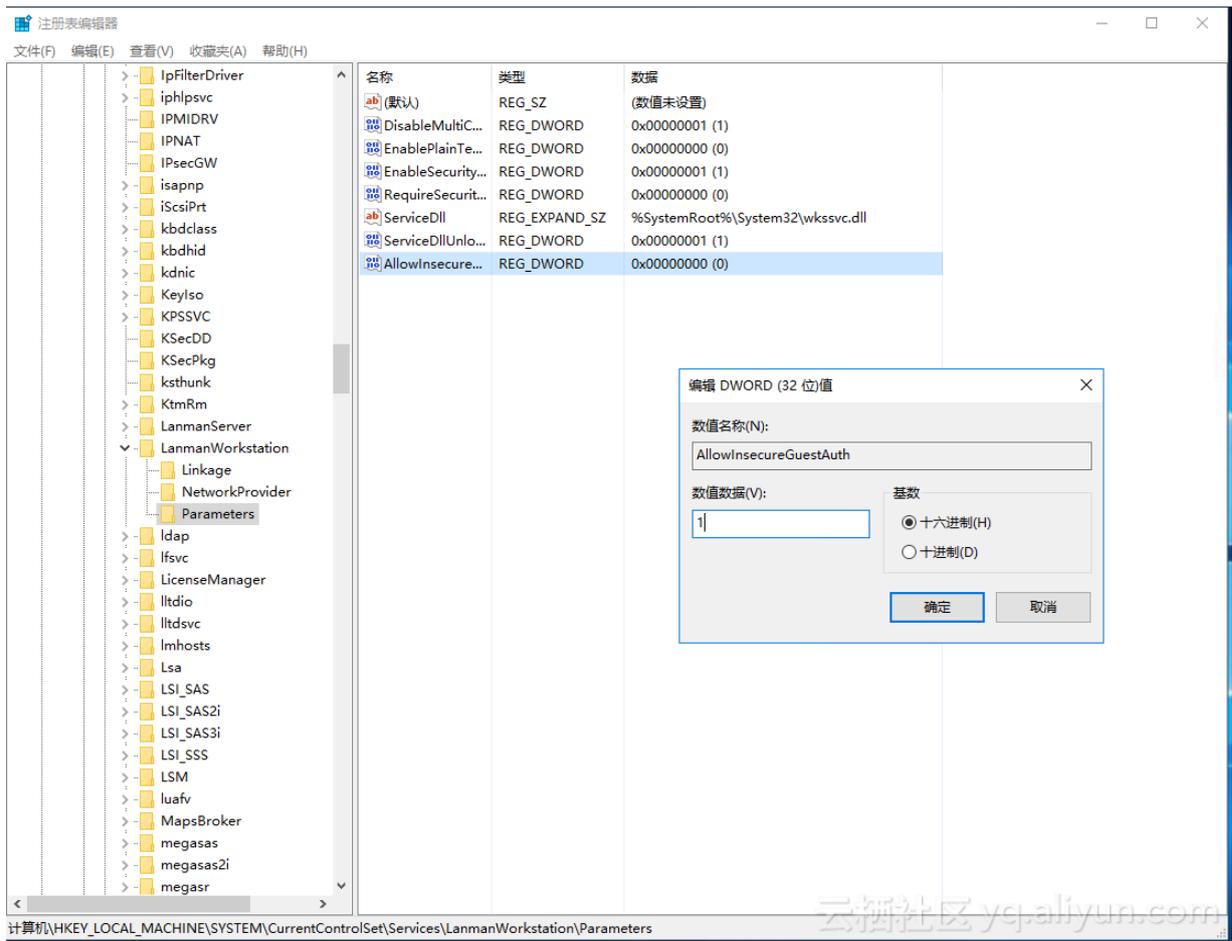
A 用户需要改动 SMB client 的一个注册表项来支持对 SMB share 的匿名访问。如下图所示，用户需要运行注册表编辑器 regedit 来修改下面的注册表值。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters\AllowInsecureGuestAuth
```

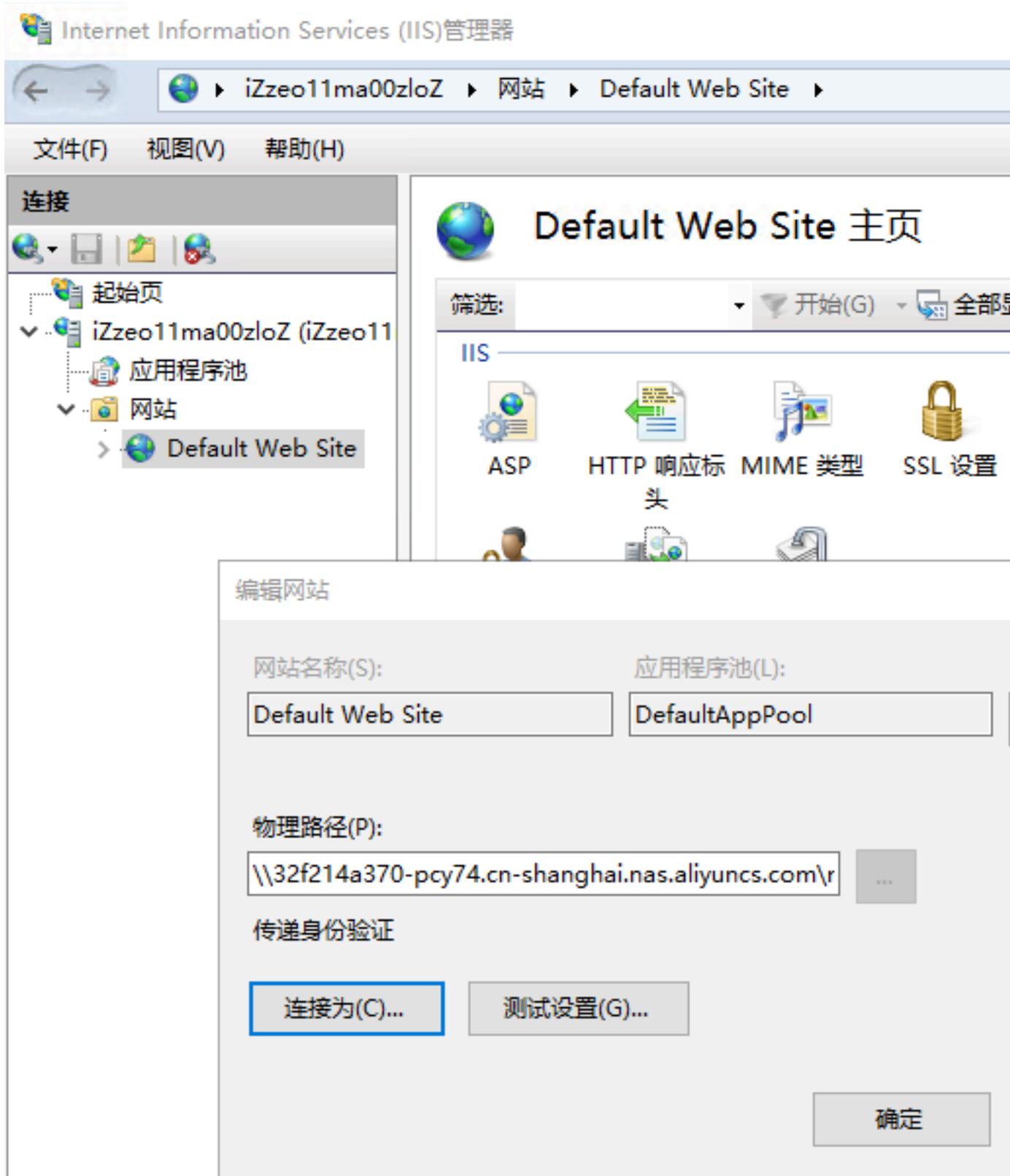
用户打开注册表编辑器之后需要找到 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters`，然后用右键选取新建 DWORD (32 位) 值。



创建并编辑该值 `AllowInsecureGuestAuth` 并将其设置为 1。



除了注册表项外，用户还需要在 IIS 的网站设置中指定一个本地用户来访问网站在阿里云 NAS 上的资源。具体的步骤如下面两图所示，用户选取网站的基本设置，再通过连接为设置特定用户，这里选用前面设置的用户 iis_user。



另外，由于 IIS 使用 SMB share 的方式下访问一个文件时，IIS 后台会有多次访问 SMB share 操作，每次访问的时间不长，但是多次的叠加可能会造成客户端总时间比较长。改进的方式可以参考[SMB2 文档](#)将其中提到的三个注册表项都调大，比如600或者更大。需要注意的是这些注册表项都在注册表`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanWorkstation\Parameters`之下，分别为：

- FileInfoCacheLifetime
- FileNotFoundCacheLifetime
- DirectoryCacheLifetime



说明：

如果找不到以上三个注册表项，则按照 Windows 的字段格式要求进行创建。

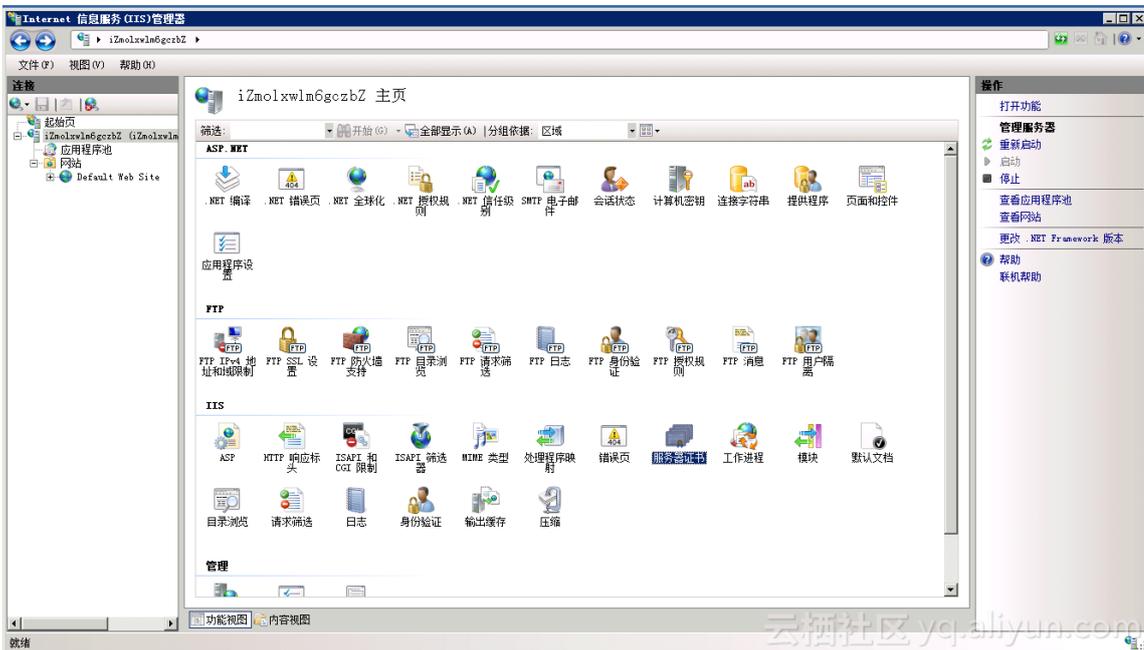
除此之外，建议把 js/css 等网页程序相关的内容放在本地，因为 IIS 访问会非常频繁。

IIS FTP 服务的设置

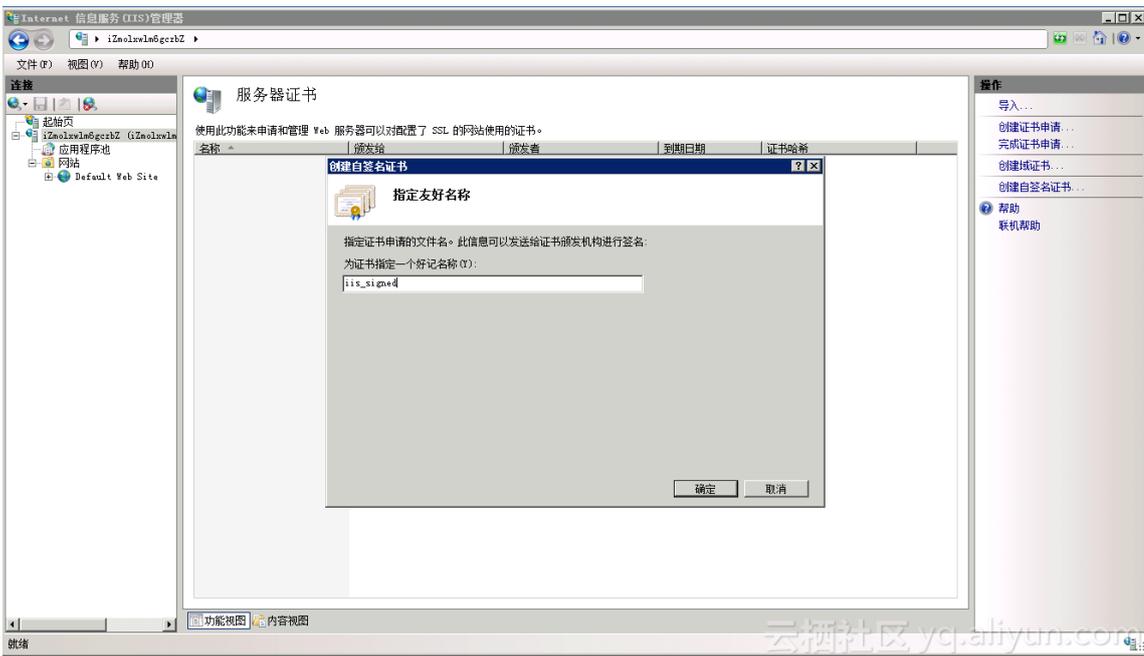
很多 IIS 用户希望用 FTP 来共享文件或进行网站内容发布。在这里我们介绍如何通过 IIS 设置 FTP over SSL 服务（又名 FTP-SSL，S-FTP，FTP Secure）。

· 安装 SSL 证书

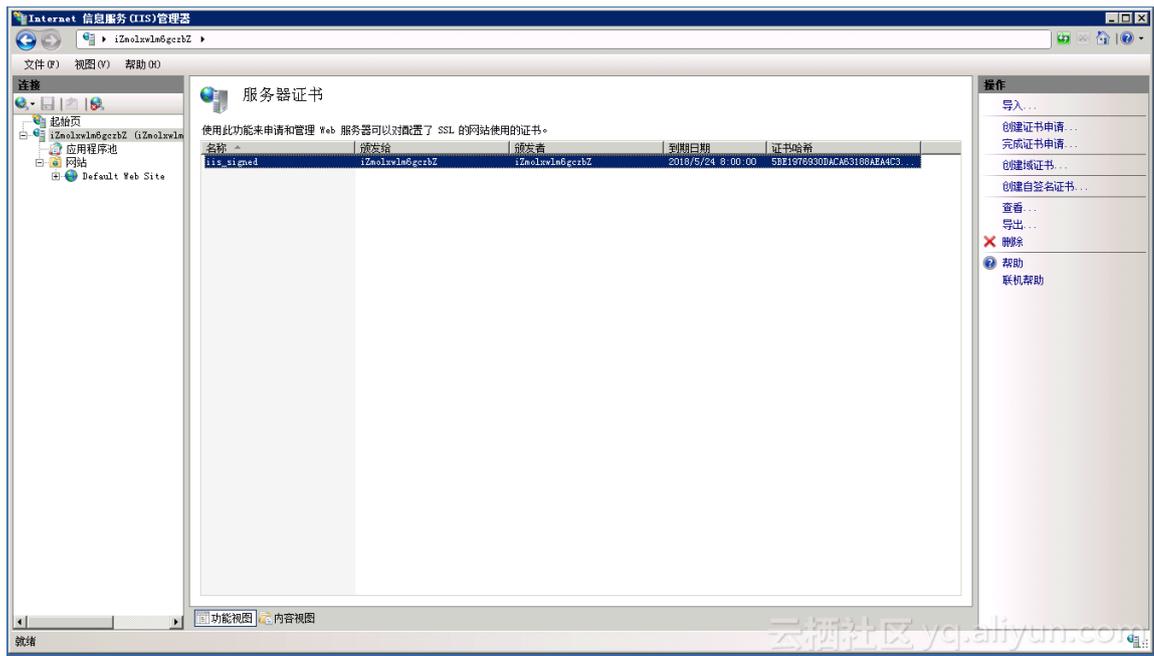
1. 用户在 IIS 的服务器中选择服务器证书，申请和管理服务器证书。



2. 用户指定服务器证书的名称。



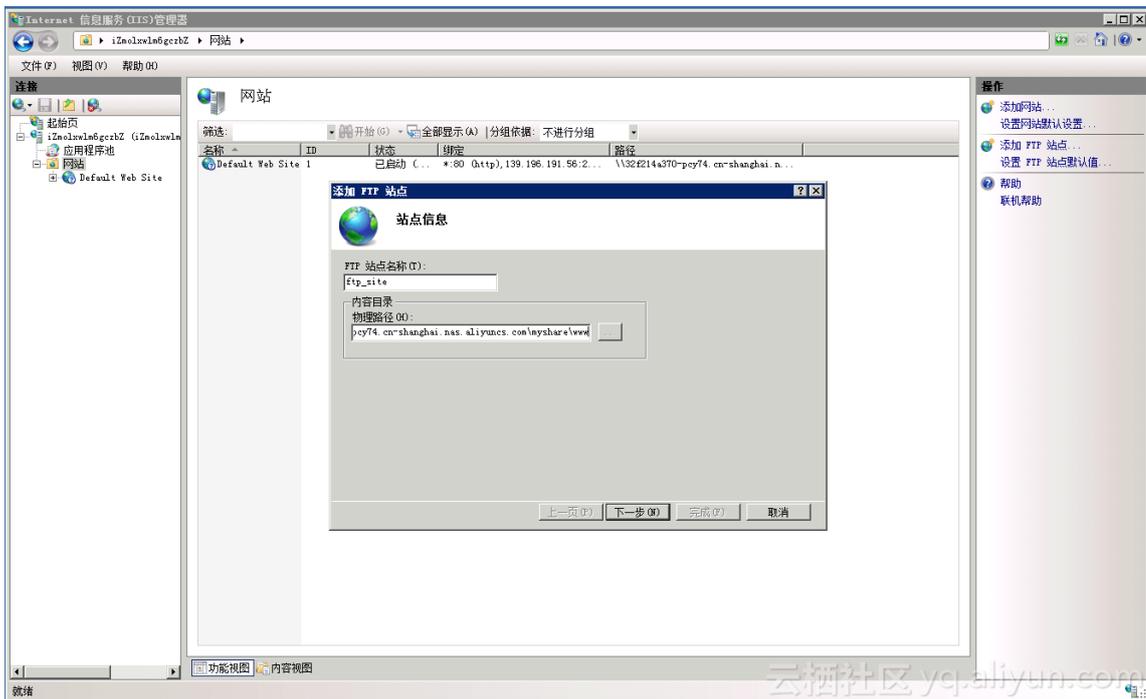
3. 配置和创建 SSL 证书。



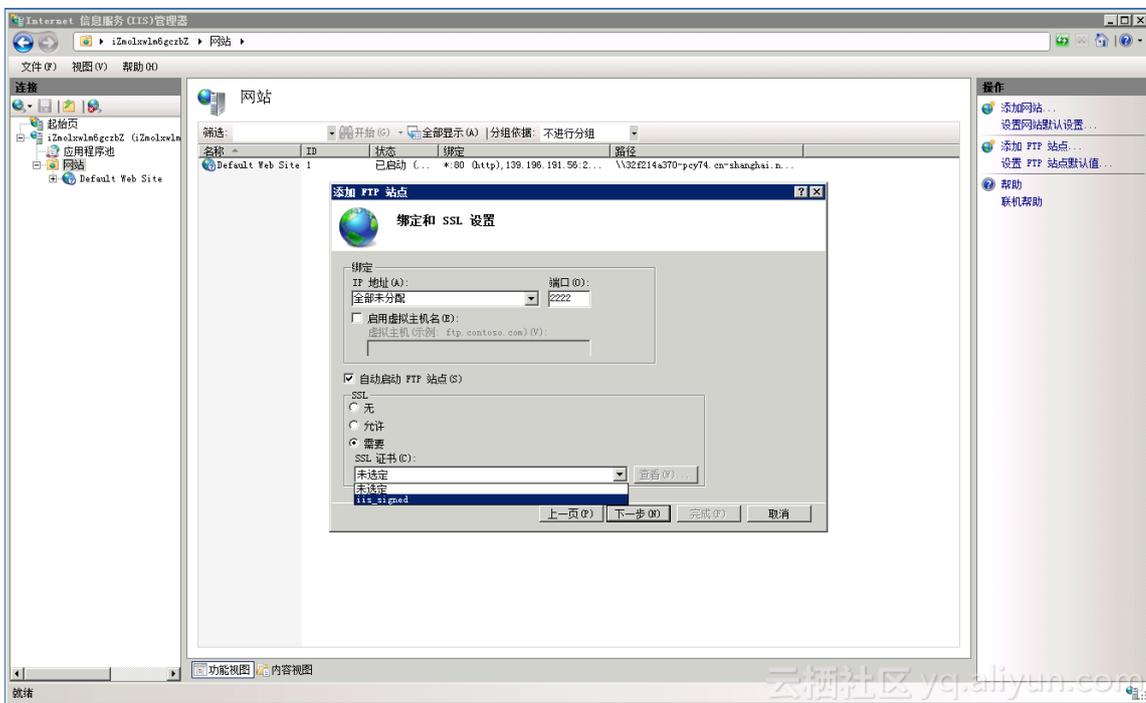
· FTP 站点设置

1. 用户在 IIS 的网站部分选择添加 FTP 站点，和 Web 服务一样，物理路径需要使用 UNC 格式的 SMB share 路径。示例中，我们仍使用前面用过的 Web service 的 www 目录。用户可

根据需求选取 myshare 上其它目录，也可以通过设置多个 FTP 站点利用不同的端口来提供对不同目录的访问。



- 2. 用户绑定提供 FTP 服务的 IP 地址，并分配端口号。这个例子里，我们出于安全的考虑没有使用标准的21端口而是用2222端口来提供 FTP 的控制信息通道。需要格外注意的是，我们选择需要 SSL 证书才能连接这个 FTP 站点，并指定使用前面创建的 SSL 证书。



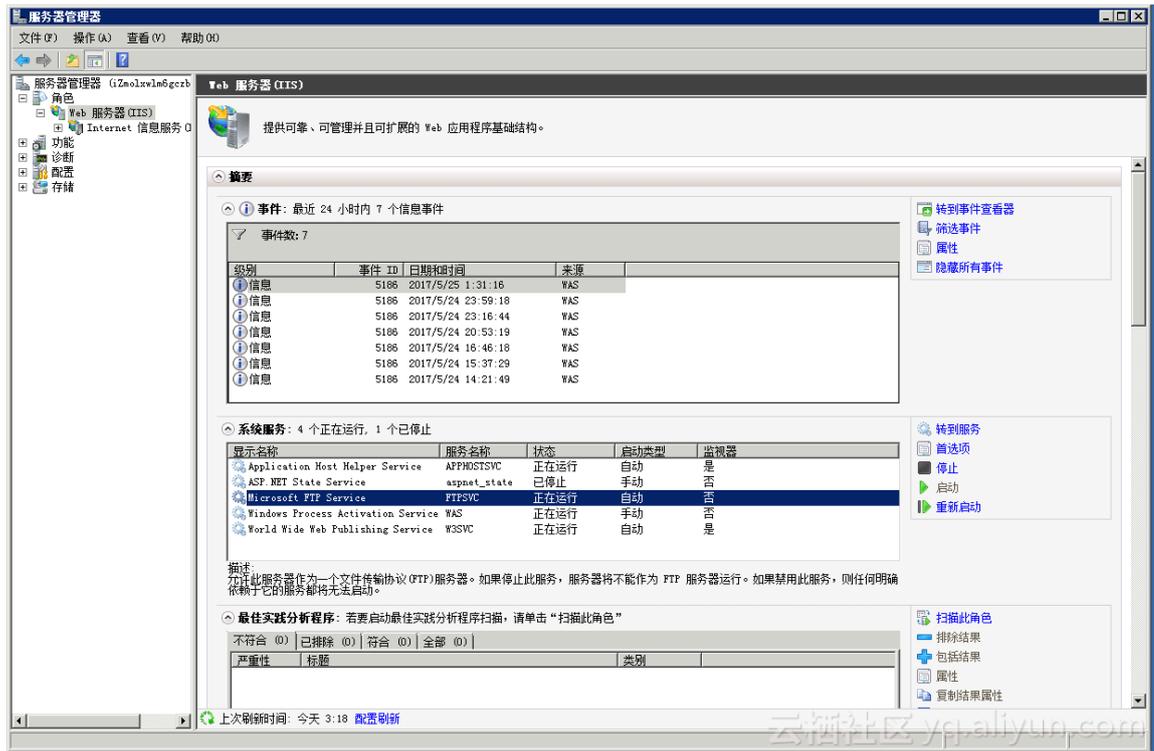
- 3. 用户指定身份验证方式为基本，并授权用户 iis_user 读写权限。您也可以选取更多的授权用户。



4. 出于安全考虑，通过在IIS中打开服务器级别FTP 防火墙支持来限制 FTP 数据通道的端口范围，并选取应用。



5. 为了使该端口范围立即生效，需要在服务器管理器中重启 FTP 服务。



- 出于安全考虑，建议用户通过阿里云的安全组设置来限制 FTP 客户端的访问。在下面的例子里，我们将已经设置的 FTP 控制及数据端口范围只授权给一个客户端 IP 访问。您也可以授权给多个 IP、一个或多个网段。

编辑安全组规则

网卡类型：

规则方向：

授权策略：

协议类型：

* 端口范围： ⓘ

授权类型：

* 授权对象： ⓘ 教我设置

优先级： ⓘ

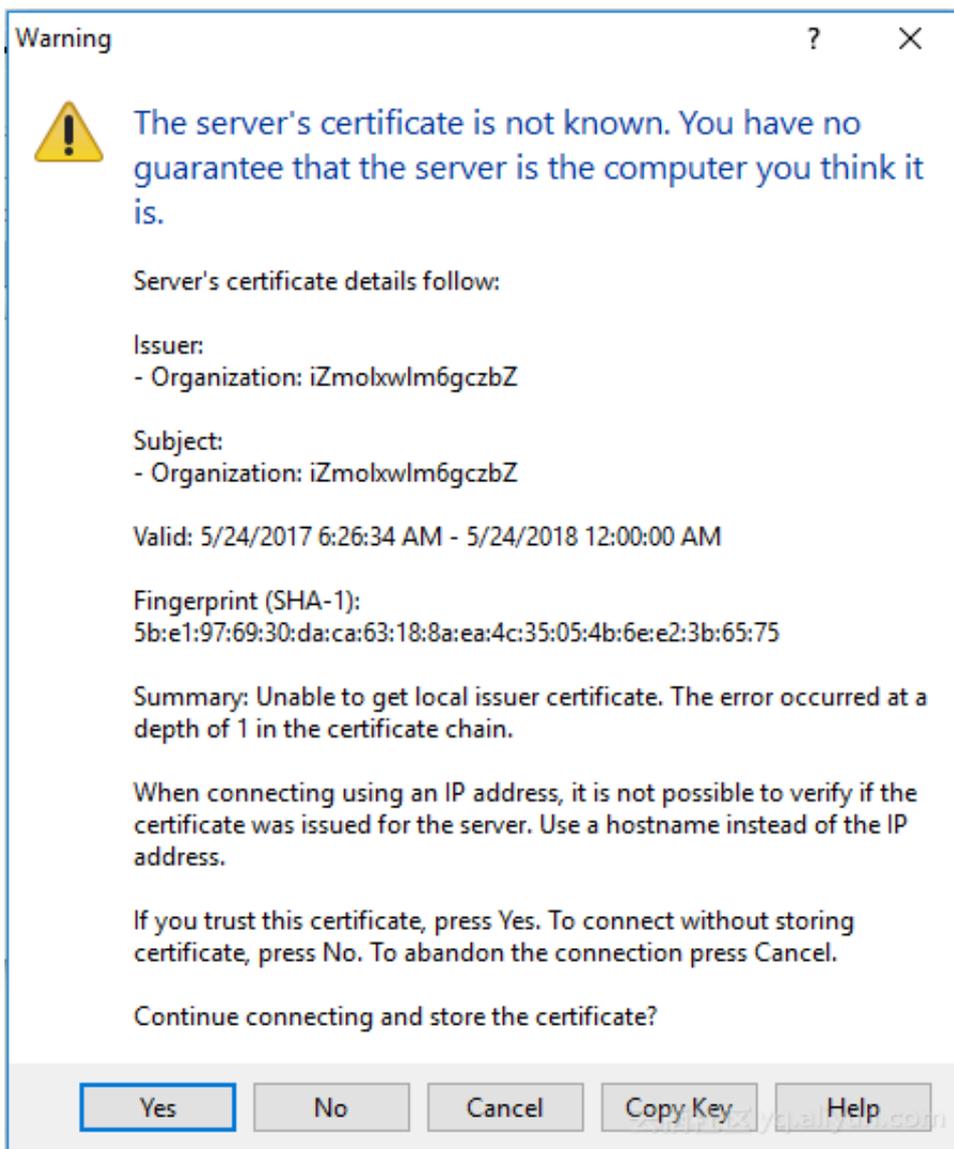
描述：

长度为2-256个字符，不能以http://或https://开头。

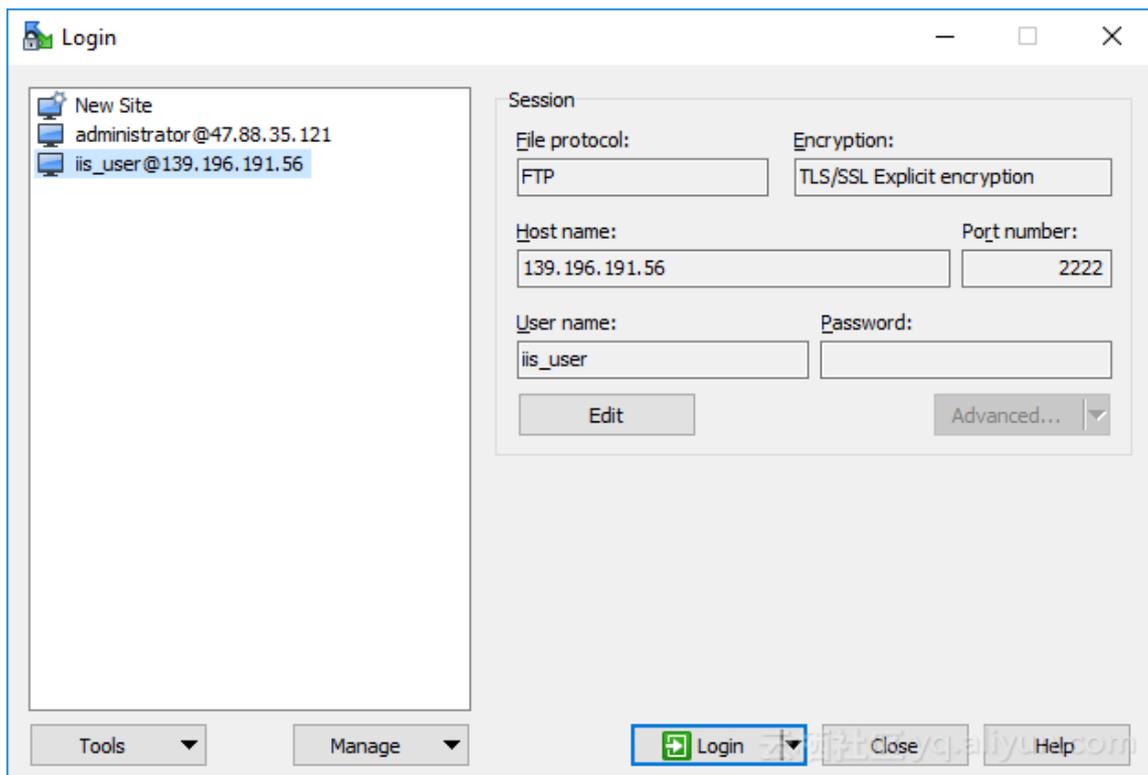
云栖社区 yq.aliyun.com

7. 下面几张图展示了通过FTP客户端 WinSCP 利用 FTP over SSL 来访问我们的 FTP 站点的过程。

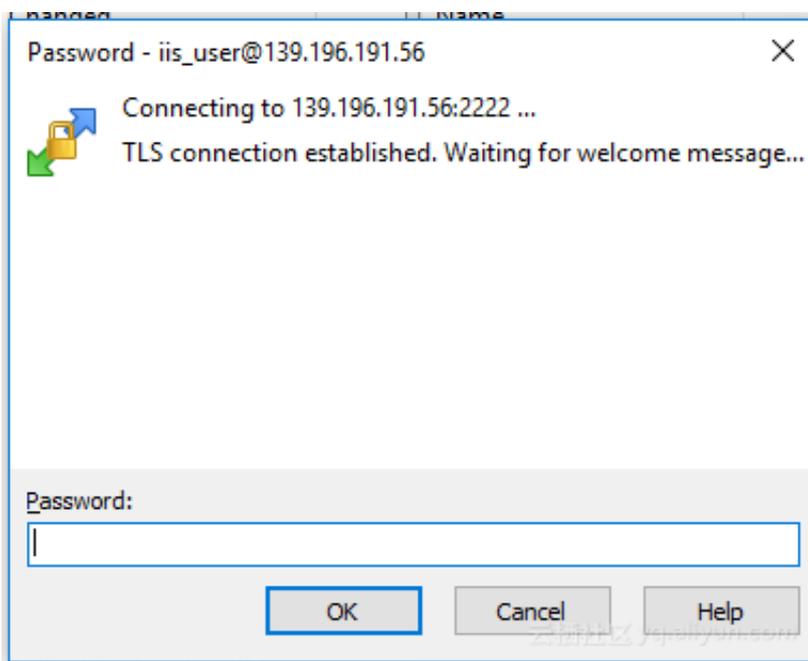
接受服务器证书，只在客户端第一次连接 FTP 站点才发生。



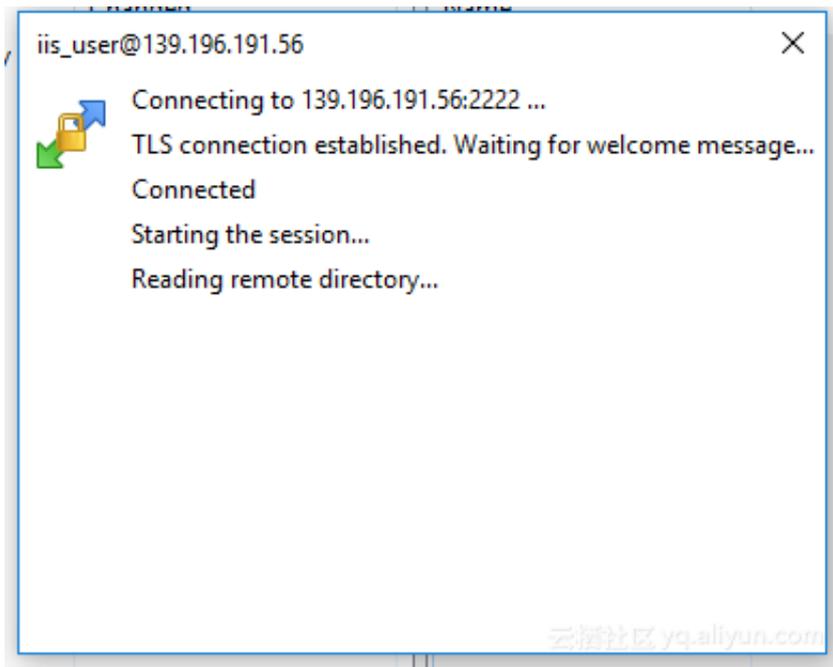
设置协议类型，端口号和登录信息。



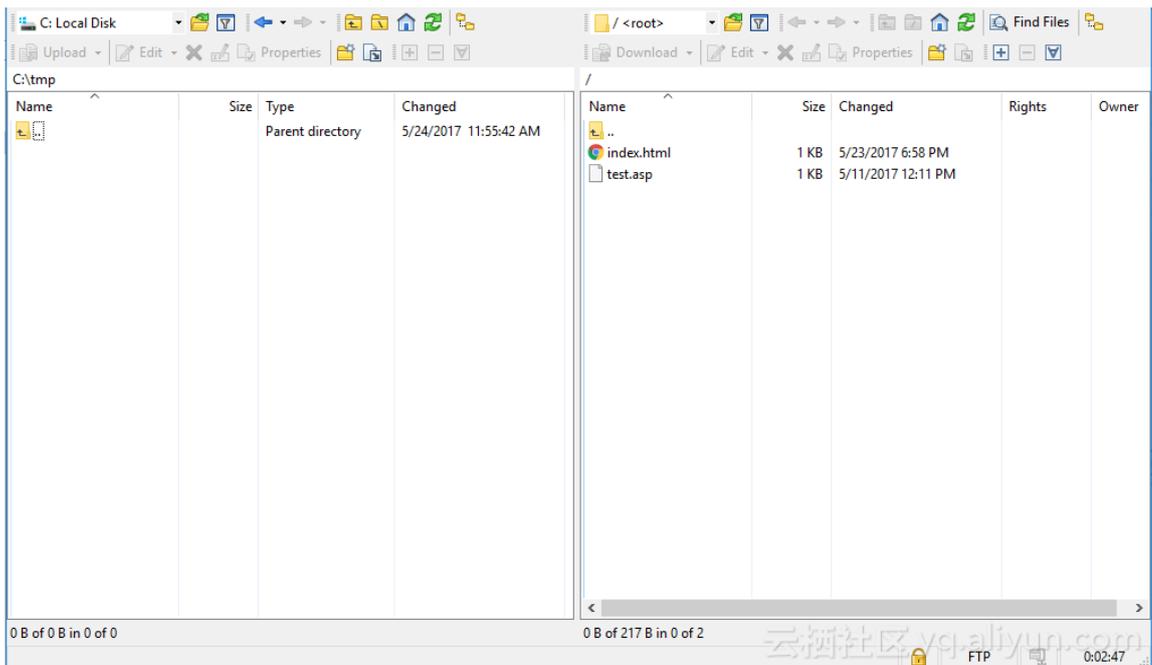
登录后要求输入密码，即授权用户所在 IIS 服务器上的密码。



数据连接建立，服务器读取和传输远程目录信息。



用户完成初步连接，可以进行文件的上传下载。



总结

本文通过例子介绍了如何结合阿里云 NAS 的 SMB 协议支持 ECS Windows 虚拟机，使用 Windows 内置的互联网信息服务（IIS）来提供 Web 和 FTP 服务。阿里云 NAS 服务还在不断发展和演进中，后续会提供更好的协议服务和性能支持。

1.2 Nginx 代理服务器阿里云文件存储 NAS

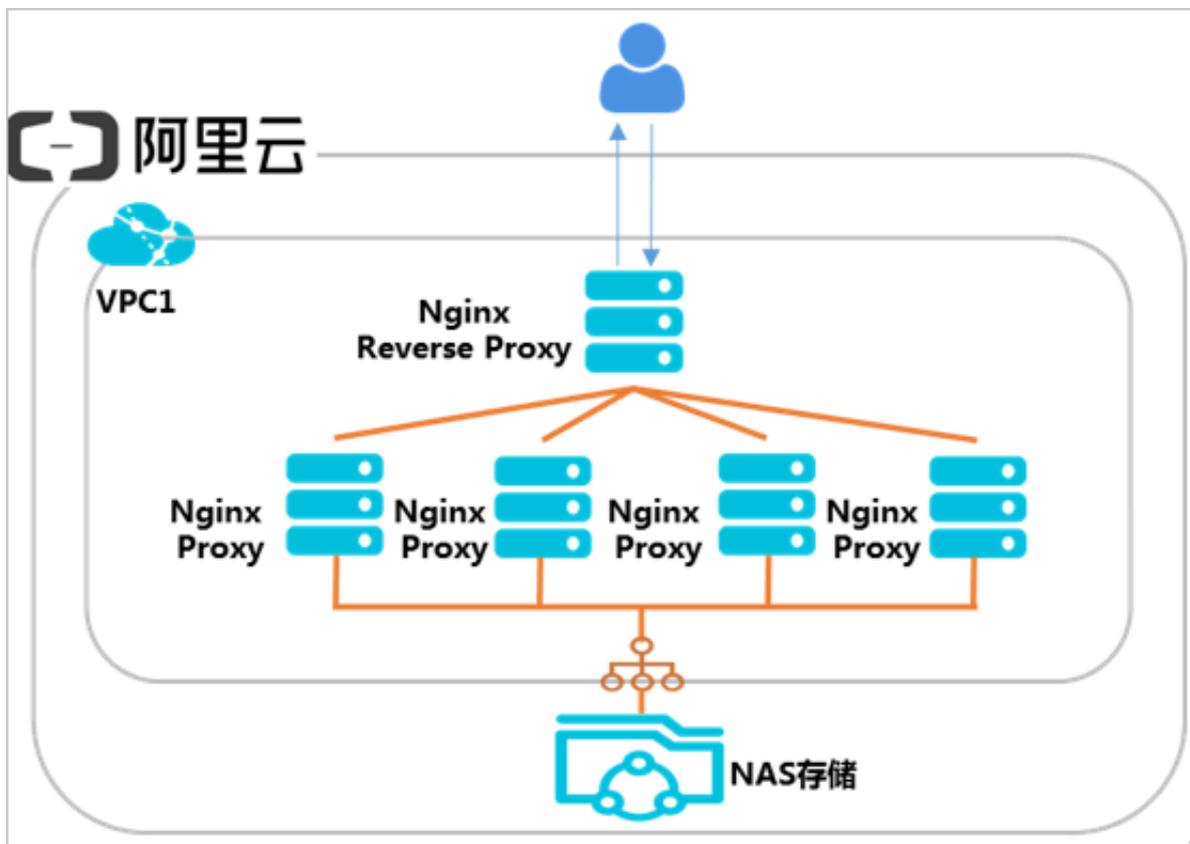
Nginx 应用场景

Nginx 是一个很强大的高性能 Web 和 反向代理服务，它具有很多非常优越的特性。反向代理是 Nginx 一种最常见的应用模式。反向代理 (Reverse Proxy) 是指以代理服务器来接受 internet 上的连接请求，然后将请求转发给内部网络上的服务器，并将从服务器上得到的结果返回给 internet 上请求连接的客户端，此时代理服务器对外就表现为一个反向代理服务器。

简单来说就是真实的服务器不能被外部网络访问，需要一台代理服务器，而代理服务器能被外部网络访问的同时又跟真实服务器在同一个网络环境。或者真实服务器与代理服务器是同一台服务器但端口不同。

配置 NAS 做反向代理共享存储

1 台 Nginx 做反向代理，4 台 Nginx 做代理服务器，后端使用文件共享存储 NAS。文件共享存储 NAS 用于存储 Proxy 代理服务器的缓存文件、镜像回源文件或者用户上传的静态数据文件，不同 Proxy 代理服务器间共享访问 NAS 数据，实现数据同步，避免由于数据不同步导致的数据不一致或者重复镜像回源而浪费带宽。配置组网如下图所示：



· 部署 Nginx 反向代理服务器

1. 安装 Nginx

```
[root@Reverse proxy~]#yum install nginx
```

2. 配置反向代理

配置反向代理服务器指向后端代理服务器。

```
[root@Reverse proxy~]#vim /etc/nginx/nginx.conf
```

nginx 配置如下：

```
http {
    upstream web{
        server 192.168.0.105;
        server 192.168.0.106;
        server 192.168.0.107;
        server 192.168.0.108;
    }
    server {
        listen 80;
        location / {
            proxy_pass http://web;
        }
    }
}
```

```
}  
}
```

· 创建文件存储 NAS

1. 创建对应区域的文件系统

创建文件系统

SSD性能型文件系统存储容量上限1PB，容量型文件系统存储容量上限10PB。

* 地域： ▼
不同地域文件系统与计算节点不互通

* 存储类型： ▼

* 协议类型： ▼

* 可用区： ▼
同一地域不同可用区之间文件系统与计算节点互通

存储包： ▼
绑定一个现有空闲存储包，没有则不绑定

2. 创建文件存储 NAS 挂载点

文件系统ID/名称	存储类型	协议类型	存储量	所在可用区	已绑存储包	挂载点数目	
800444b921 800444b921	容量型	NFS	128.00 GB	华北 5 可用区 A	是	1	添加挂载点 管理
8961f4bf03 NFS	SSD性能型	NFS	711.99 GB	华北 5 可用区 A	否	1	添加挂载点 管理

添加挂载点

挂载点是云服务器访问文件系统的入口，当前支持专有网络和经典网络挂载点，每个挂载点必须与一个权限组绑定。

Linux客户端在默认情况下对NFS请求并发数做了限制，若遇到性能较差的情况，可以参考该文档进行配置。

文件系统ID：

* 挂载点类型：

* VPC网络：
[点击前往VPC控制创建VPC网络](#)

* 交换机：

* 权限组：

3. 成功创建 NAS 挂载点后用于后续使用

8961f4bf03

[删除文件系统](#)

文件系统ID： 8961f4bf03	地域： 华北 5	可用区： 华北 5 可用区 A
存储类型： SSD性能型	协议类型： NFS (NFSv3及NFSv4.0)	文件系统的容量： 711.99 GB
创建时间： 2018-09-03 12:16:41 +0800		

存储包

存储包ID： 点击购买存储包	存储包容量：	到期时间：	有效期至：
--------------------------------	--------	-------	-------

挂载点

[如何挂载文件系统](#) | [添加挂载点](#)

挂载点类型	VPC	交换机	挂载地址	权限组	状态	
专有网络	VPC- hp3d4ppqaj1o4fndwz	VSW- hp31o45yh327b42jpeec9k	8961f4bf03-fce21.cn-huhehaote.nas.aliyuncs.com	VPC默认权限组 (全部允许)	可用	修改权限组 删除 管理

部署 Nginx 代理服务器

部署方式如下：

1. 安装 Nginx、NFS客户端

```
[root@proxy~]#yum install nginx
[root@proxy~]#yum install nfs-utils
```

2. 挂载文件共享存储 NAS 到 Nginx 网站目录

```
[root@proxy~]#sudo mount -t nfs -o vers=4.0,挂载点域名:/ /usr/share/nginx/html/
```

3. 编辑 Nginx 主目录文件

```
[root@proxy~]#echo "This is Testing for Nginx&NAS"> /usr/share/nginx/html/index.html
```

重复配置另外三台 Nginx 代理服务器，均挂载同一个 NAS 文件系统，所有 Nginx 代理服务器都可以访问 index.html 测试文件。

测试配置结果



2 应用服务器共享存储

2.1 Windows系统使用NFS协议挂载NAS共享文件存储

如果您想要使用分布式文件系统，并在多台ECS实例上共享存储，您可以使用NAS服务。NAS服务的地域信息，请以NAS控制台上显示的信息为准。

本文以Windows Server 2012 R2系统为例，描述了如何在一台Windows ECS实例上挂载一个阿里云NAS文件系统。您可以使用类似的方法在其他版本的Windows系统上操作。



说明：

如果您要在一台Linux实例上挂载一个NAS文件系统，请参考[挂载文件系统](#)。

前提条件

在将NAS文件系统挂载到Windows ECS实例之前，您必须先完成以下工作：

- 参考 [创建ECS实例](#) 创建ECS实例。在本示例中，
 - 地域选择华东1。
 - 镜像选择Windows 2012 R2数据中心版本。
 - 网络类型选择VPC（专有网络）。

- 准备NAS文件系统及挂载点：
 1. 开通NAS服务。
 2. 登录NAS控制台。
 3. 按以下步骤购买一个存储包：

- a. 在左侧导航栏中，单击存储包。
- b. 在存储包管理页面，单击购买存储包。



- c. 在NAS存储包页面，选择区域（在本示例中，选择华东1）、容量和购买时长，单击立即购买，并按页面提示完成操作。

NAS存储包

基本配置

区域	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #00a0e3; color: white; padding: 5px;">华东1</td> <td style="padding: 5px;">华北2</td> <td style="padding: 5px;">华东2</td> <td style="padding: 5px;">华南1</td> </tr> <tr> <td style="padding: 5px;">华北1</td> <td style="padding: 5px;">华北5</td> <td style="padding: 5px;">亚太东南 1 (新加坡)</td> <td style="padding: 5px;">华北3</td> </tr> <tr> <td style="padding: 5px;">德国1 (法兰克福)</td> <td style="padding: 5px;">香港</td> <td></td> <td></td> </tr> </table>	华东1	华北2	华东2	华南1	华北1	华北5	亚太东南 1 (新加坡)	华北3	德国1 (法兰克福)	香港		
华东1	华北2	华东2	华南1										
华北1	华北5	亚太东南 1 (新加坡)	华北3										
德国1 (法兰克福)	香港												
文件系统ID	<div style="background-color: #00a0e3; color: white; padding: 5px; display: flex; justify-content: space-between; align-items: center;"> 创建新文件系统并绑定存储包 ▼ </div> <p style="font-size: 0.8em; margin-top: 5px;">存储包必须与一个文件系统绑定，且一个文件系统同一时刻只能绑定一个存储包，您可以在这里选择一个已经存在的文件系统ID或选择【创建新文件系统并绑定存储包】</p>												
存储类型	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">SSD性能型</td> <td style="background-color: #00a0e3; color: white; padding: 5px;">容量型</td> <td style="padding: 5px;">NASPlus智能缓存型</td> </tr> </table> <p style="font-size: 0.8em; margin-top: 5px;">性能型、容量型和NAS Plus智能缓存型之间的区别，请点击查看：【存储类型选择】</p>	SSD性能型	容量型	NASPlus智能缓存型									
SSD性能型	容量型	NASPlus智能缓存型											
协议类型	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #00a0e3; color: white; padding: 5px;">NFS</td> <td style="padding: 5px;">SMB</td> </tr> </table>	NFS	SMB										
NFS	SMB												
容量	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #00a0e3; color: white; padding: 5px;">500GB</td> <td style="padding: 5px;">1TB</td> <td style="padding: 5px;">5TB</td> <td style="padding: 5px;">10TB</td> </tr> <tr> <td style="padding: 5px;">30TB</td> <td style="padding: 5px;">50TB</td> <td style="padding: 5px;">100TB</td> <td style="padding: 5px;">200TB</td> </tr> </table>	500GB	1TB	5TB	10TB	30TB	50TB	100TB	200TB				
500GB	1TB	5TB	10TB										
30TB	50TB	100TB	200TB										
可用区	<div style="background-color: #00a0e3; color: white; padding: 5px;">华东 1 可用区 B</div>												

高级配置

购买时长	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #00a0e3; color: white; padding: 5px;">1个月</td> <td style="padding: 5px;">6个月</td> <td style="padding: 5px;">1年</td> </tr> </table>	1个月	6个月	1年
1个月	6个月	1年		

4. 按以下步骤创建文件系统：

- a. 在NAS控制台的左侧导航栏中，单击文件系统列表。
- b. 选择地域（在本示例中，选择华东1）。
- c. 单击创建文件系统。
- d. 在创建文件系统对话框中，指定文件系统的配置，并绑定已创建的存储包。
- e. 单击确定。

5. `#unique_10`。

挂载点是云服务器访问文件系统的入口，当前支持专有网络和经典网络挂载点，每个挂载点必须与一个权限组绑定。本示例中选择专有网络并选择需要的交换机。

6. 在文件系统列表中，单击文件系统ID进入文件系统详情页，查看新挂载点的挂载地址。

挂载点					
挂载点类型	VPC	交换机	挂载地址	权限组	状态
专有网络	vpc-bp- qoc	vsw- bp- j8	03- 63.cn-hangzhou.nas.aliyuncs.com	VPC默认权限组 (全部允许)	可用

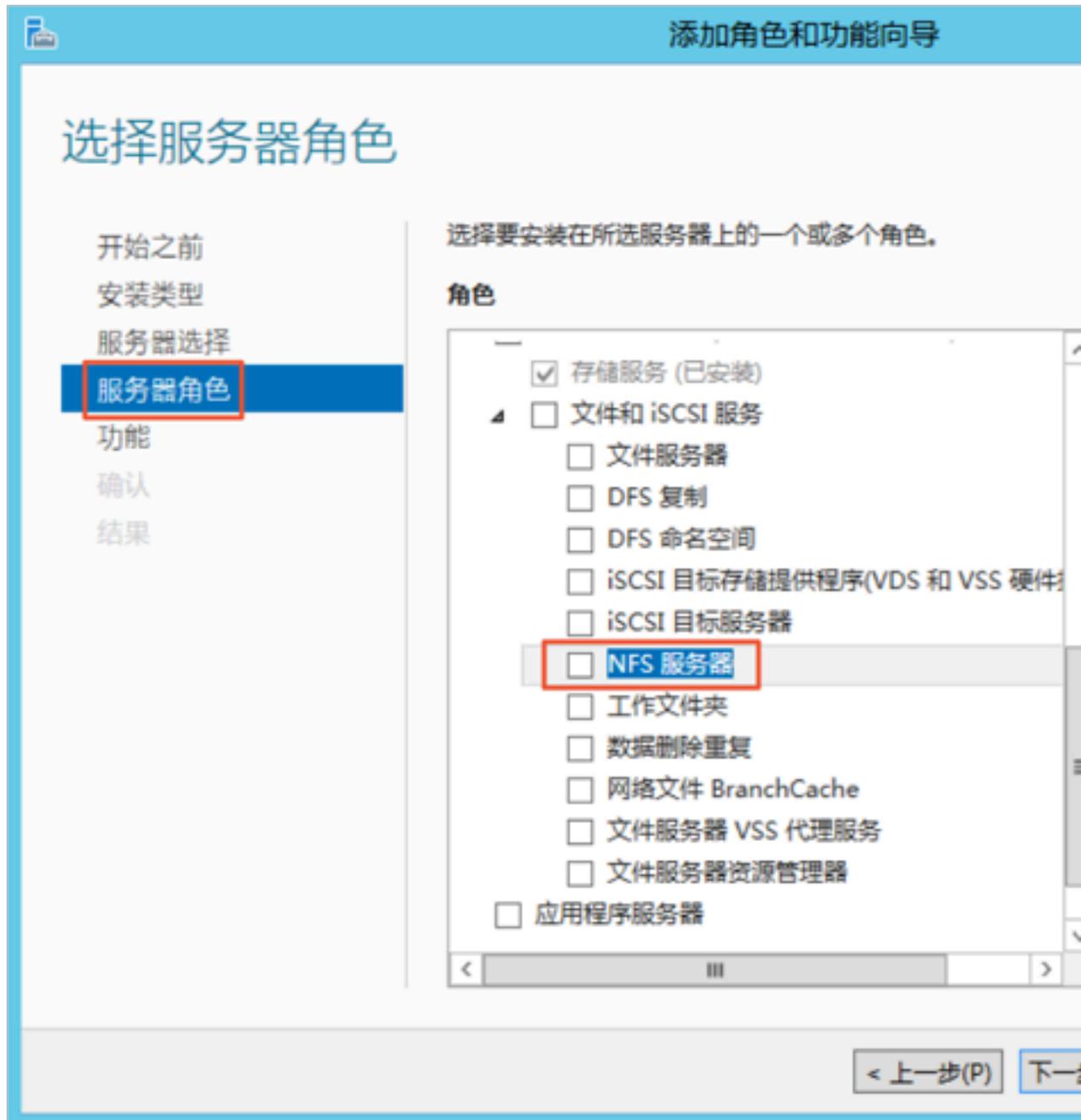
挂载文件系统

本部分描述如何在Windows ECS实例上挂载一个NAS文件系统。本文描述的步骤适用于大部分安装了NFS客户端的Windows ECS实例。

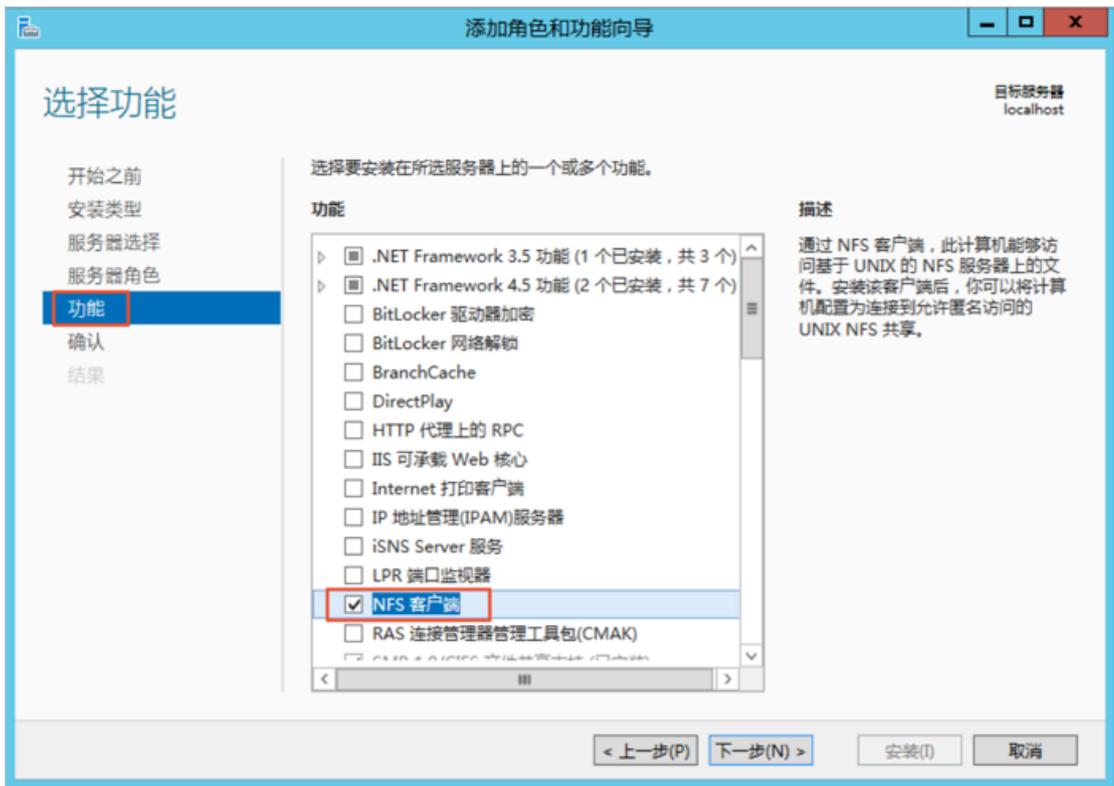
1. #unique_11。

2. 安装NFS客户端。

- a. 打开服务器管理。
- b. 选择管理 > 添加角色和功能。
- c. 按添加角色和功能向导指示安装NFS客户端，注意以下配置：
 - 在服务器角色选项卡下，选择NFS服务器。



- 在功能选项卡下，选择NFS客户端。



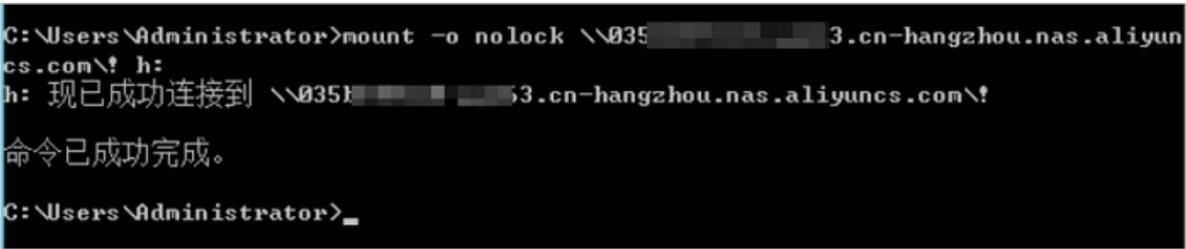
- d. 在实例内部重启。
- e. 启动命令提示符, 运行命令 `mount`。如果返回以下信息, 说明NFS客户端安装成功。



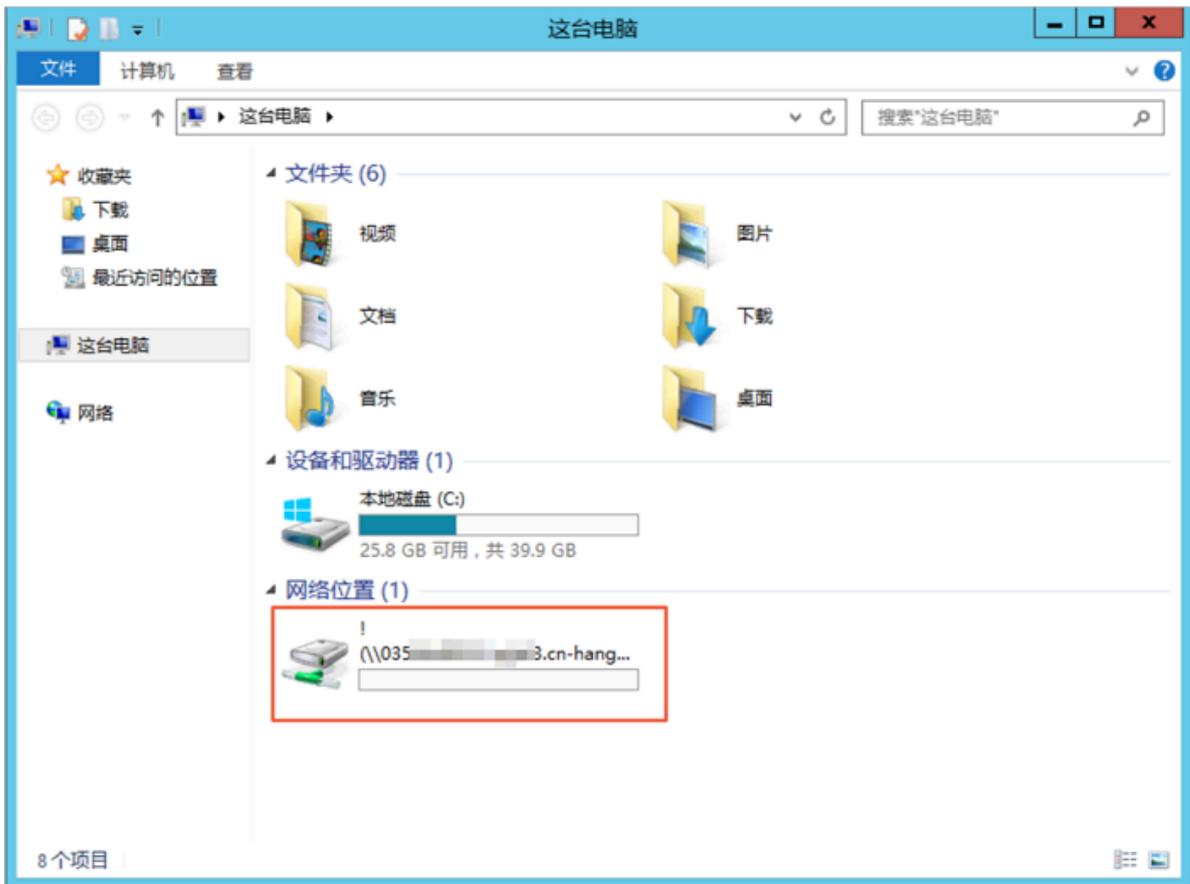
3. 运行以下命令挂载NAS文件系统。

```
mount -o no lock \\035XXXXXX3.cn-hangzhou.nas.aliyuncs.com\! h:
```

其中, `035XXXXXX3.cn-hangzhou.nas.aliyuncs.com\` 是新挂载点的挂载地址。



4. 在这台电脑里查看新的共享文件系统。



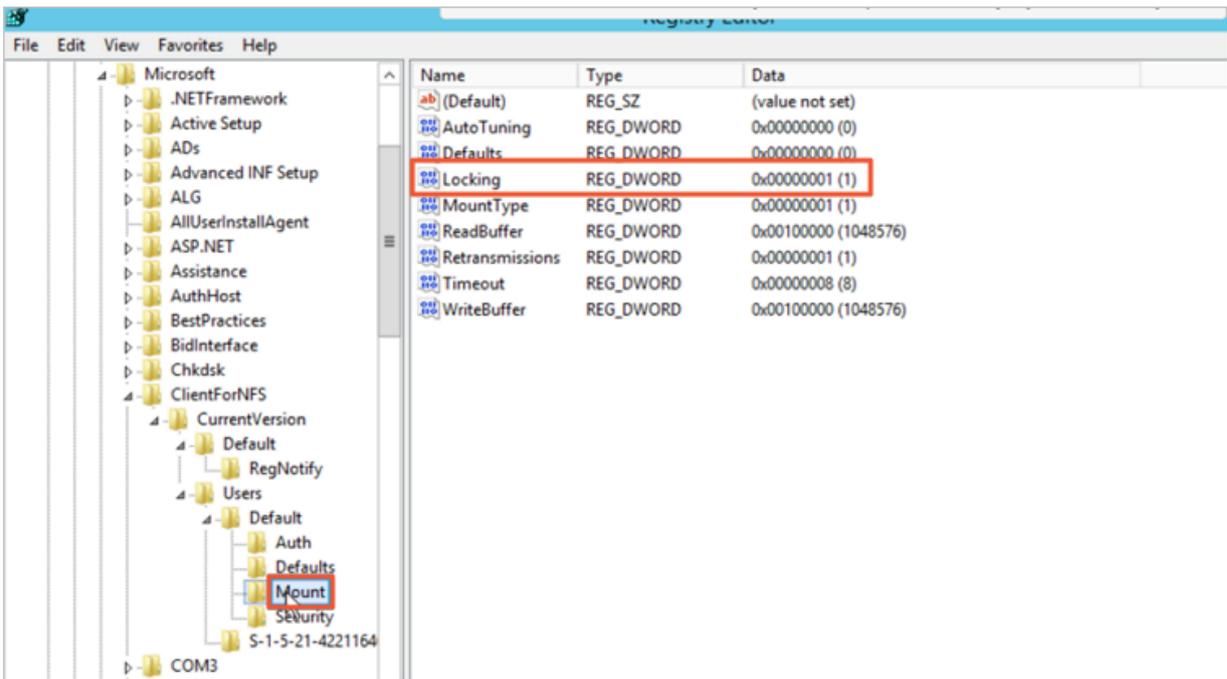
5. 在共享文件系统里新建文件夹和文件，检查是否能正常操作这个文件系统。

常见问题

如果在操作时系统报错 file handle error，您需要确认以下注册表信息：

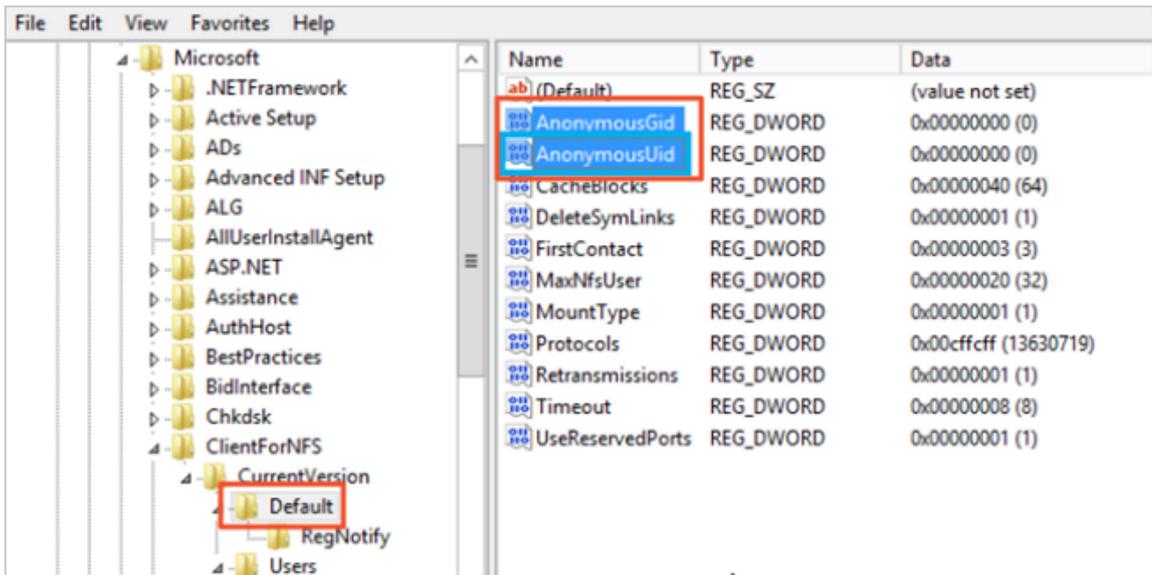
 **说明：**
如果找不到Locking、AnonymousGID、AnonymousUID这三个注册表项，则按照 Windows 的字段格式要求进行创建。

HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > ClientForNFS > CurrentVersion > User > Default > Mount，其中Locking值必须为 1。



您也能创建以下注册表项设置GID和UID：

1. 进入Default注册表项目录：HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > ClientForNFS > CurrentVersion > Default。
2. 右击空白处，选择新建 > DWORD(32位)值，并创建以下两个注册表项：
 - AnonymousGID， 值为0。
 - AnonymousUID， 值为0。



3. 运行 mount 检查新的UID和GID。

```
C:\Users\Administrator>mount
Local      Remote      Properties
-----
h:         \\192.168.1.100\h.~  UID=0, GID=0
                                     rsize=1048576, wsize=1048576
                                     mount=soft, timeout=0.8
                                     retry=1, locking=yes
                                     fileaccess=755, lang=ANSI
                                     casesensitive=no
                                     sec=sys
```

3 远程访问文件系统

3.1 本地IDC VPN网络访问阿里云文件存储

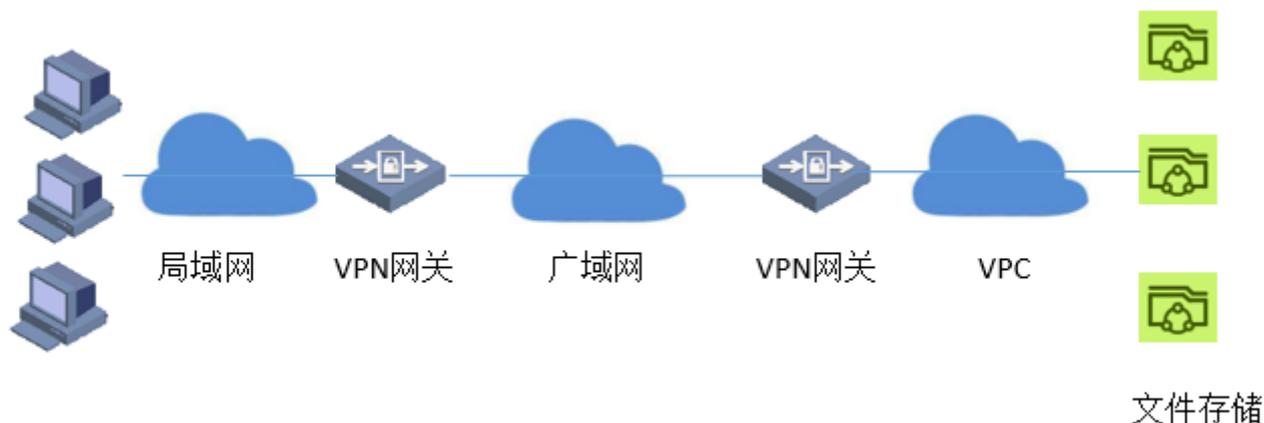
NAS的使用限制

阿里云文件存储服务在使用时有一个限制：对于一个地域（比如华东1）内创建的文件系统（NFS或者SMB），只支持同一地域内的ECS挂载，用户在其他地域（比如华北1）内的ECS，或者用户自己IDC机房的服务器，无法直接挂载；只有通过建立不同VPC间或者IDC和VPC间的高速通道才能实现跨地域或者从IDC服务器挂载文件系统，而部署高速通道带来的高成本将是很多用户面临的一个非常现实的问题。

解决方案

通过阿里云VPN网关服务，用户可以完成IDC到阿里云VPC的访问，以及不同地域的VPC之间的互通。对于阿里云文件存储的用户来说，通过VPN网关服务，现在用户可以部署如下图所示的网络拓扑，实现两种方式的文件系统挂载：

- 从用户IDC内挂载文件系统
- 从ECS跨地域挂载文件系统



从用户IDC内挂载文件系统的操作步骤

1. 登录控制台，创建文件系统，并为文件系统添加VPC挂载点，具体步骤请参见[Linux系统](#)。
2. 登录控制台，创建VPN连接，连接VPC内VPN网关和用户IDC内的VPN网关，具体步骤请参见[建立VPC到本地数据中心的连接](#)。

完成这些配置之后，可以用ping命令验证IDC内服务器和VPC内ECS或者文件系统挂载点的连通性，在确认两端的IP互相可以ping通之后，在用户IDC内VPN网关侧的服务器就可以挂载VPC内的文件系统，挂载的具体步骤请参见[#unique_8](#)。

从ECS跨地域挂载文件系统的操作步骤

从ECS跨地域挂载文件系统有两种方法，方法一需要在VPC2内使用一台ECS服务器搭建VPN网关，适合于已经部署类似网关服务的用户，如果用户没有这样的环境，可以采用方法二。

· 方法一

1. 登录控制台，创建文件系统，并为文件系统添加在VPC1内的VPC挂载点，具体步骤请参见[创建文件系统](#)。
2. 在另一个地域的VPC2内使用一台ECS服务器搭建用户VPN网关作为用户侧网关，注意该ECS需要有公网IP，才能有VPC1内的VPN网关建立连接。



说明：

关于如何试用ECS服务器搭建VPN网关，可以参考互联网上的一些教程，例如[Using StrongSwan for IPSec VPN on CentOS 7](#)。

3. 登录控制台，创建VPN连接，连接VPC1内VPN网关和VPC2内的网关（即，上一步骤中创建的网关），具体步骤请参见[建立VPC到本地数据中心的连接](#)。
4. 在VPC2内的其他ECS添加静态路由，目标网段是VPC1的网段，下一跳节点是VPC2内的网关（即，上一步骤中创建的网关）。

完成这些配置之后，可以用ping命令验证VPC1和VPC2内ECS或者文件系统挂载点的连通性，在确认两端的IP互相可以ping通之后，在VPC2内的其他ECS就可以挂载VPC1内的文件系统，挂载的具体步骤请参见[#unique_8](#)。

- 方法二

1. 登录控制台，创建文件系统，并为文件系统添加在VPC1内的VPC挂载点，具体步骤请参见[Linux系统](#)。
2. 登录控制台，在VPC1内创建VPN网关，具体步骤请参见[建立VPC到本地数据中心的连接](#)。
3. 登录控制台，在另一个地域的VPC2内，也创建VPN网关。
4. 分别以第2步和第3步创建的VPN网关的IP，创建用户网关，具体步骤请参见[建立VPC到本地数据中心的连接](#)。
5. 创建VPN连接第2步和第3步创建的VPN网关，具体步骤请参见[建立VPC到本地数据中心的连接](#)。
6. 分别为两个VPC添加路由，对于VPC1，目标网段是VPC2的内网IP，下一跳节点是VPC1内的网关，对于VPC2，目标网段是VPC1的内网IP，下一跳节点是VPC2内的网关，具体步骤请参见[建立VPC到本地数据中心的连接](#)。

完成这些配置之后，可以用ping命令验证VPC1和VPC2内ECS或者文件系统挂载点的连通性，在确认两端的IP互相可以ping通之后，在VPC2内的其他ECS就可以挂载VPC1内的文件系统，挂载的具体步骤请参见[#unique_8](#)。

使用VPN的优劣势

- 优势：
 - VPN解决了连通性的问题
 - VPN提供安全的访问（通过IPsec实现加密通信）
 - 使用VPN与使用高速通道相比，用户的成本会有明显下降。
- 劣势：通过VPN访问文件系统时的I/O性能将受限于从IDC到VPC或者VPC之间的公网带宽和时延。

3.2 本地 IDC NAT 网关访问阿里云文件存储

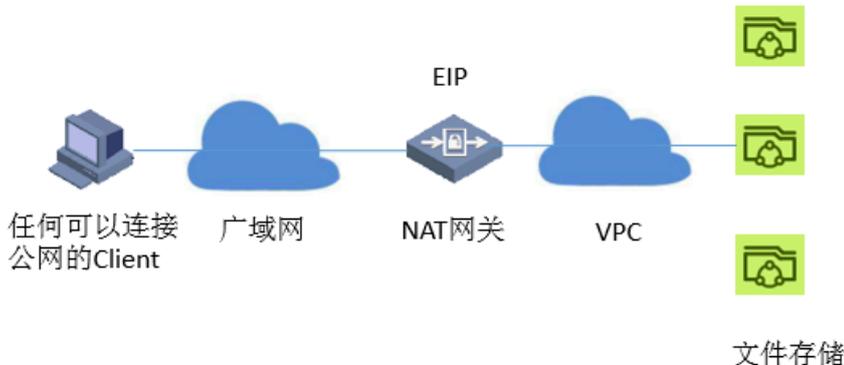
本文主要介绍本地 IDC 通过 NAT 进行跨地域挂载文件系统。

阿里云文件存储服务只支持同一地域内的 ECS 挂载，本地 IDC 或跨地域ECS 无法直接挂载。无法直接挂载时，需要通过建立高速通道进行挂载，但成本往往很高。

对于之前已经在自己机房部署了 VPN 服务的用户，我们推荐使用阿里云的 VPN 网关来实现办公环境或者 IDC 到阿里云 NAS 的互通，具体操作方法请参见[本地IDC VPN网络访问阿里云文件存储](#)。

由于部署 VPN 较为繁琐，而且阿里云 VPN 目前是按月收费的（每月收费从几百到几千不等）。将少量的线下数据上传到阿里云文件存储 NAS 时，使用 VPN 会有很大的浪费？接下来我们就来介绍一个更简单（而且花费更少）的方案：使用 NAT 网关实现从公网访问阿里云 NAS。

使用 NAT 网关从公网访问阿里云 NAS 的网络架构如下图所示：



操作步骤如下：

1. 创建 NAS 文件系统。
2. 为文件系统添加挂载点。
3. 创建 NAT 网关。
4. 为 NAT 网关添加带宽包，获得公网 IP（EIP）。
5. 为 NAT 网关添加 DNAT 转发条目。

通过以上五步，可以在任何一台连接公网的 PC（Windows 或 Linux）挂载 NAS，实现文件的上传和下载。

操作步骤示例如下：

1. 在 NAS 控制台创建文件系统。



2. 为文件系统添加挂载点，且需要创建 VPC 挂载点 (NAT 只支持 VPC)



3. 获得挂载点的 IP

可以在 ECS 中 ping 挂载点地址获得 IP。

```
PING [redacted] nas.aliyuncs.com (192.168.92.38) 56(84) bytes of data:
64 bytes from 192.168.92.38: icmp_seq=1 ttl=64 time=2.53 ms
64 bytes from 192.168.92.38: icmp_seq=2 ttl=64 time=0.877 ms
64 bytes from 192.168.92.38: icmp_seq=3 ttl=64 time=0.864 ms
64 bytes from 192.168.92.38: icmp_seq=4 ttl=64 time=0.835 ms
64 bytes from 192.168.92.38: icmp_seq=5 ttl=64 time=0.869 ms
```

4. 在 NAT 控制台创建 NAT 网关。



5. 为 NAT 网关添加带宽包。



6. 创建 DNAT

- 公网 IP: 创建 EIP 时, 产生公网 IP。
- 私网 IP: 填写需要访问的挂载点的 IP。
- 端口: 推荐选择所有端口, 可以选择安装 NFS 或 SMB 时相应的端口。

ID/名称	专有网络	端口转发规则	SNAT规则	带宽包	规格	状态(全部)	创建时间	操作
ngw-bp1vy0v5rhm15dgv5y4e	vpc-bp1q5jy11xwc9zvbkvm	设置DNAT	设置SNAT	bwp-bp1c3xvstbjhzy0mjsq8	小型	正常	2017-07-28 13:43:30	管理 编辑 删除 强制删除

创建端口转发条目

用于创建端口转发条目的公网IP地址, 将不能用来创建SNAT条目

* 公网IP地址:

私网IP地址:

必需属于本VPC的CIDR范围, 或一个已有的ECS的私网IP地址

端口设置: 所有端口 具体端口

* 公网端口:
源端口; 取值范围: 1~65535

* 私网端口:
目标端口; 取值范围为1~65535

* 协议类型:
IpProtocol类型, 可选TCP|UDP|Any

7. 验证挂载 NFS，将 NAT 映射配置到一个 NFS 的挂载点。

```

$ sudo mount -t nfs4 114.55.126.64:/ /mnt
[sudo] password for qiying.zf:
Warning: rpc.idmapd appears not to be running.
All uids will be mapped to the nobody uid.

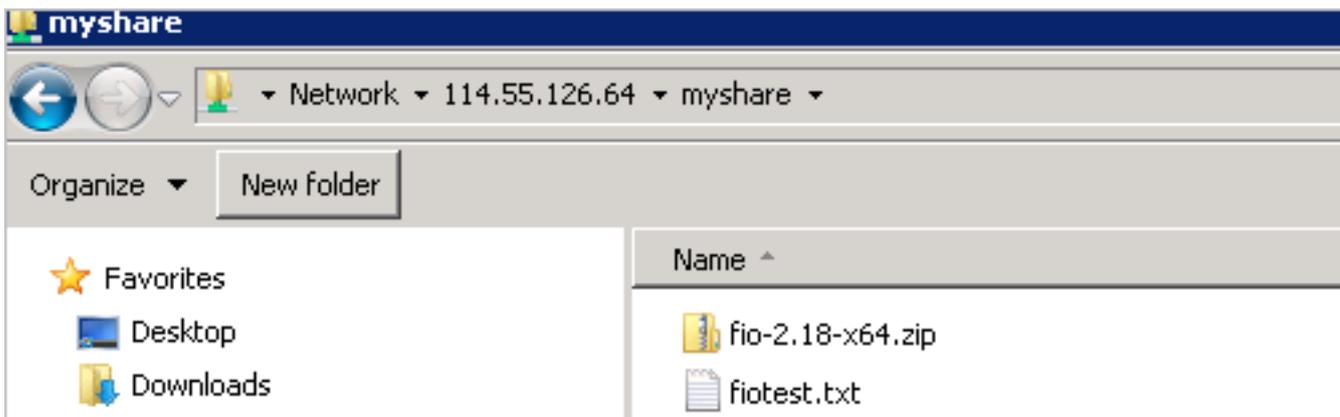
$ mount
/dev/sda2 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
tmpfs on /dev/shm type tmpfs (rw)
/dev/sda1 on /boot type ext4 (rw)
/dev/sda2 on / type ext3 (rw)
/dev/sda3 on /usr type ext4 (rw)
/dev/sda4 on /var type ext4 (rw)
/dev/sda5 on /var/lib/docker type ext4 (rw)
/dev/sda6 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda7 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda8 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda9 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda10 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda11 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda12 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda13 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda14 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda15 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda16 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda17 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda18 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda19 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda20 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda21 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda22 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda23 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda24 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda25 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda26 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda27 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda28 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda29 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda30 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda31 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda32 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda33 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda34 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda35 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda36 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda37 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda38 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda39 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda40 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda41 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda42 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda43 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda44 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda45 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda46 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda47 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda48 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda49 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda50 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda51 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda52 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda53 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda54 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda55 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda56 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda57 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda58 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda59 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda60 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda61 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda62 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda63 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda64 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda65 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda66 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda67 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda68 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda69 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda70 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda71 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda72 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda73 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda74 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda75 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda76 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda77 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda78 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda79 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda80 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda81 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda82 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda83 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda84 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda85 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda86 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda87 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda88 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda89 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda90 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda91 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda92 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda93 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda94 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda95 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda96 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda97 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda98 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda99 on /var/lib/docker/overlay2 type ext4 (rw)
/dev/sda100 on /var/lib/docker/overlay2 type ext4 (rw)
114.55.126.64:/ on /mnt type nfs4 (rw,addr=114.55.126.64)

$ ls /mnt/
阿里  阿里巴巴.jpg

```

8. 验证挂载 SMB，删除原来的 NAT 映射，添加一条映射配置到一个 SMB 的挂载点。

转发条目ID	公网IP地址	公网端口	协议类型	私网IP地址	私网端口	状态
fw-d-bp11s7hg8r4nqa1apva7j	114.55.126.64	any	any	192.168.92.38	any	可用



NAT 的优点为配置简单。

NAT 的缺点为：

- 安全性方面，由于打通了 EIP 和 VPC，任何获得了 EIP 的人都可以挂载 EIP 对应的挂载点。
- 每个 EIP+PORT 只能映射到一个挂载点，同时访问多个挂载点时需要创建多个 EIP。

使用 NAT 与使用 VPN 的优缺点对比如下：

	NAT网关方案	VPN网关方案
配置	简单，完全在阿里云控制台完成	复杂，需要在阿里云控制台配置 VPN 网关，还需要在 IDC 或者 Office 配置用户侧 VPN 网关。
价格	Small 规格：12元/天，EIP带宽包：3.36元/Mbps/天	5Mbps VPN 网关：375元/月
安全性	差	好
灵活性	受限，一个 EIP 只能映射到一个 NAS 挂载点。	好，可以同时访问所有的 NAS 挂载点。
适合场景	临时，少量数据上传下载。	用户线下环境和阿里云NAS长期的连通。

3.3 使用 SFTP 上传下载 NAS 文件系统数据

本文档介绍如何使用 SFTP 上传下载 NAS 文件系统数据。

背景信息

SFTP 的传输速度依赖于 ECS 的外网带宽，可根据业务需求配置适当的网络带宽。

操作步骤

1. 在 NAS 文件系统所在区域购买一台 CentOS 操作系统的 ECS 实例。
2. 登录 ECS 实例并修改配置文件 `/etc/ssh/sshd_config`。
 - a. 将原 `sshd_config` 配置文件中的 `Subsystem` 行注释掉，新增一行 `Subsystem sftp internal-sftp`。

```
# override default of no subsystems
#Subsystem      sftp      /usr/libexec/openssh/sftp-server
Subsystem       sftp      internal-sftp
```

- b. 在 `sshd_config` 文件末尾添加如下内容。其中 `/usr/sftp` 为用户的 sftp 根目录，此处名字仅作为参考，可以根据实际情况修改。

```
X11Forwarding no
AllowTcpForwarding no
ForceCommand internal-sftp
ChrootDirectory /usr/sftp
```

3. 使用命令 `groupadd sftp` 添加用户组。
4. 使用命令 `useradd -g sftp -s /sbin/nologin -M sftp` 添加用户并设置为 SFTP 组。

5. 设置 SFTP 用户密码。

```
[root@localhost ~]# passwd sftp
更改用户 sftp 的密码。
新的密码:
无效的密码: 密码少于 8 个字符
输入密码新的密码:
passwd:所有的身份验证令牌已经成功更新。
```

6. 创建 SFTP 用户的根目录、属主和属组，并修改权限（755）。

```
[root@localhost ~]# cd /usr
[root@localhost usr]# mkdir sftp
[root@localhost usr]# chown root:sftp sftp
[root@localhost usr]# chmod 755 sftp
```

7. 在 SFTP 的目录中创建 NAS 挂载目录。

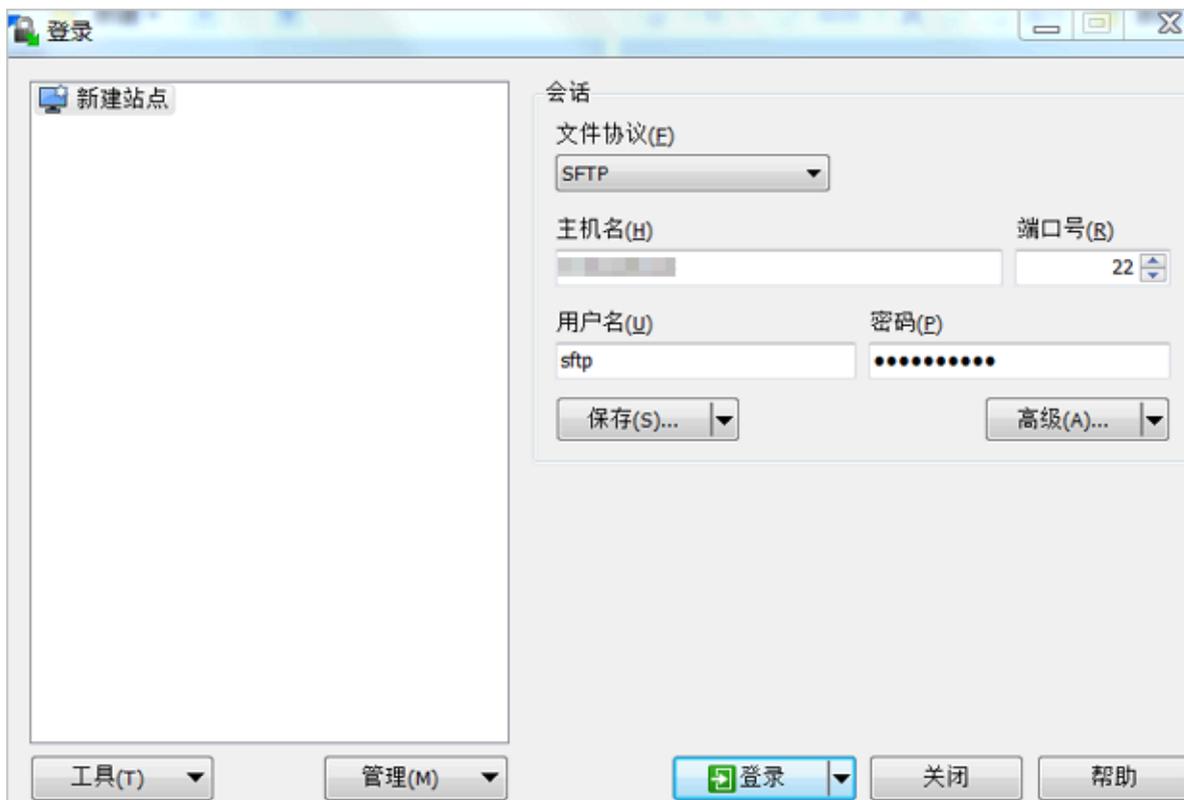
```
[root@localhost usr]# cd sftp/
[root@localhost sftp]# mkdir file
[root@localhost sftp]# chown sftp:sftp file
```

8. 执行以下命名将 NAS 文件系统挂载到 `/usr/sftp/file` 目录。

```
sudo mount -t nfs -o vers=4.0
91fd04a7b7-cvn49.cn-zhangjiakou.nas.aliyuncs.com:/ /usr/sftp/file
```

9. 执行 `service sshd restart` 命令重启 `sshd` 服务。

10.使用 SFTP 客户端登录 SFTP 服务，账号密码为前面配置 SFTP 的账号密码。下图使用的是 `winscp` 工具，可根据实际情况使用支持 SFTP 协议的客户端连接。



4 使用 Windows Server Backup 从 ECS 备份数据到 NAS

背景

本文介绍了一种从 Windows ECS 备份数据到 NAS 的常用方法，即使用 Windows 服务器系统自带的 Windows Server Backup 工具，将云盘上指定文件夹或者整盘的重要数据备份到阿里云 NAS。

Windows Server Backup 支持手动一次性备份数据，和制定备份计划周期性备份数据；在需要时，您可以方便地从备份中恢复数据。

阿里云 NAS 帮助您实现计算和存储分离的架构设计：您可以将计算任务以及内存态数据保留在 ECS 上，而将需要持久化的数据保存到 NAS 上。这样，即使在 ECS 宕机时，您的业务也可以快速切换到其他 ECS 上，并且使用新的 ECS 无缝、持续地访问保存在 NAS 上的数据。NAS 是多 ECS 共享数据，以及实现计算存储分离的最佳工具。

除了数据共享外，您也可以选择把 ECS 上的数据定期或者不定期地同步到云盘之外的存储；这样不仅可以保留历史数据，而且当发生灾难性事件（比如误删除 ECS 及云盘）时，也可以用作数据恢复。NAS 能够帮助您灵活地保存重要数据：相比于云盘快照基于整盘来保存历史数据，备份历史数据到 NAS 提供更灵活的选择，比如您可以选择备份某一个或者几个目录，而不是整块云盘。

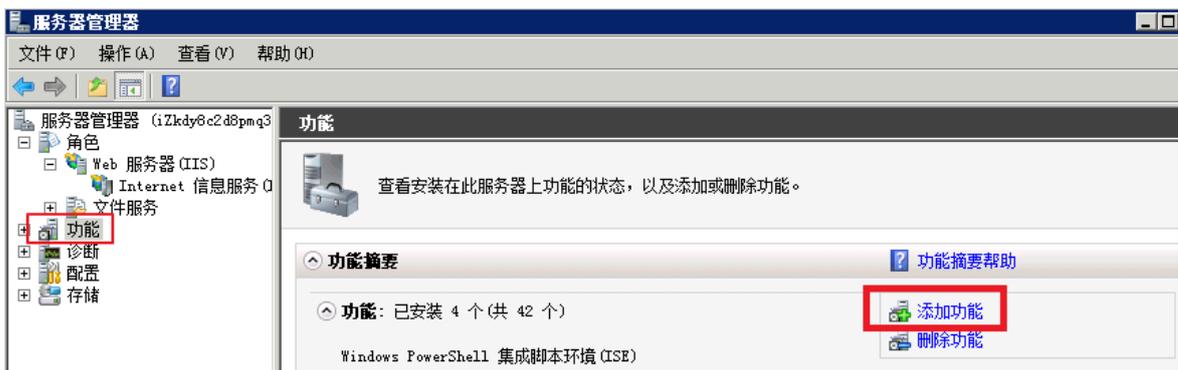
Windows Server Backup

Windows Server Backup 是一个 Windows 原生的数据（整盘、文件夹或者文件）备份和恢复的工具。根据微软官网的介绍（[Windows Server Backup 概述](#)），Windows Server Backup 是一个日常备份和恢复工具。通过 Windows Server Backup 可以备份整个服务器（所有卷）、选定卷、系统状态或者特定的文件或文件夹，到其他设备（包括其他硬盘、磁带库或者远程共享文件夹），并且可以在需要的时候从其他硬盘、磁带库或者远程共享文件夹进行数据的恢复。

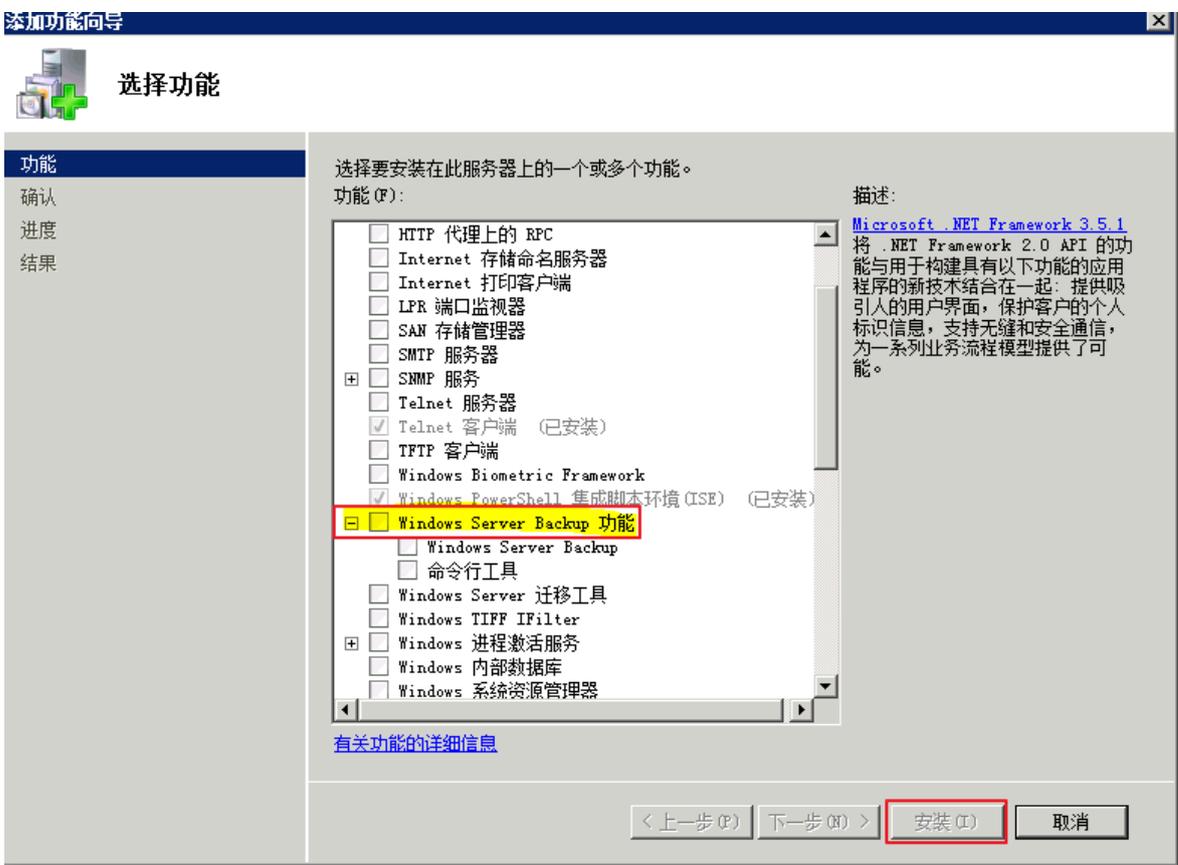
安装 Windows Server Backup

参照以下步骤，在阿里云的 Windows 镜像中安装运行 Windows Server Backup。

1. 打开服务器管理器 > 功能，单击添加功能。



2. 勾选Windows Server Backup 功能，并单击安装。



安装完成之后，你可以在管理工具中单击Windows Server Backup 来启动它。



使用 Windows Server Backup 备份数据

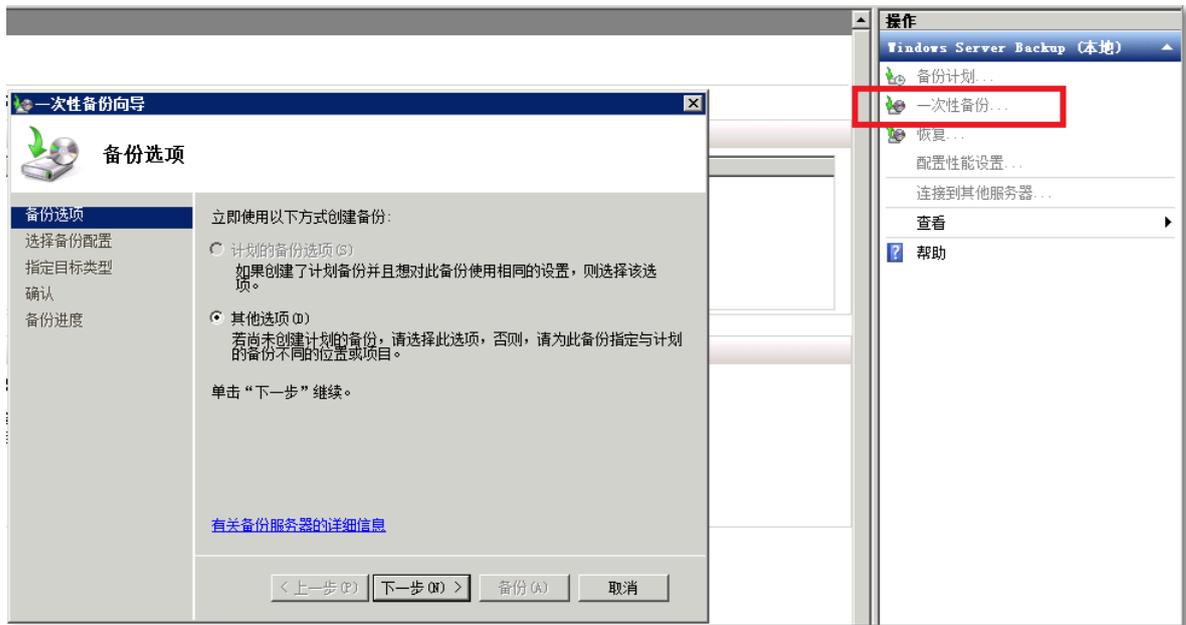
在使用 Windows Server Backup 备份数据到 NAS 前，您需要创建一个 SMB 文件系统实例并将其挂载到 ECS 上，具体操作可以参考 [阿里云文件存储 SMB 协议服务及其申请和使用指南](#)。

Windows Server Backup 支持一次性备份和创建备份计划进行周期性持续备份，以下分别对其进行介绍。

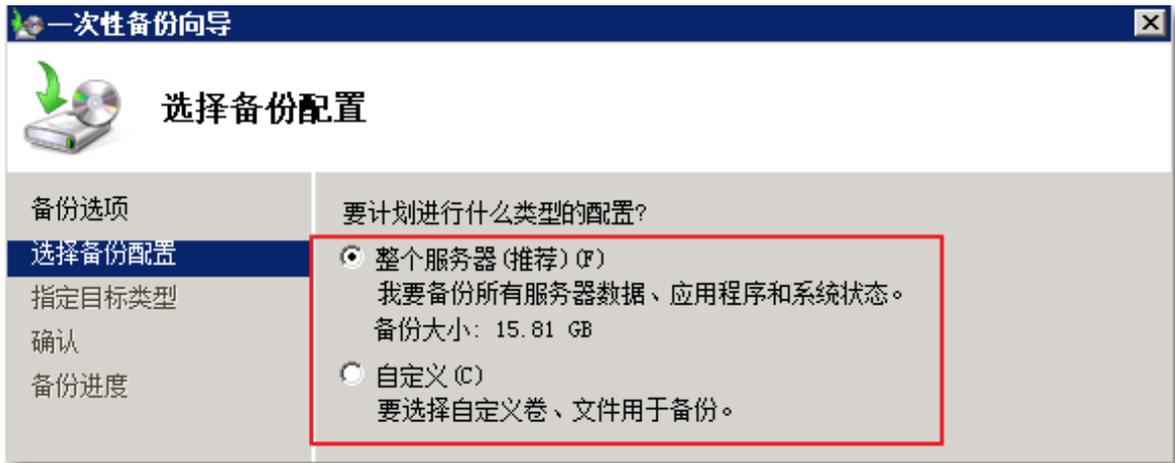
一次性备份

使用一次性备份，您可以按需手动地将数据（整盘或者目录）备份到 NAS。

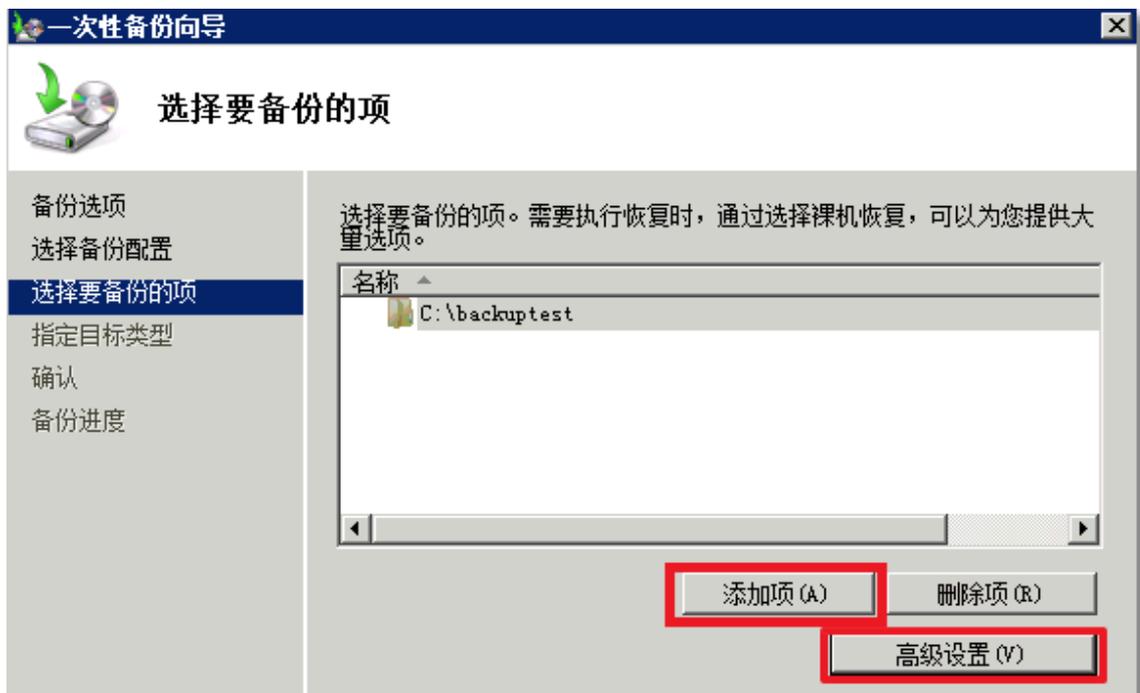
1. 打开Windows Server Backup, 在其右侧操作栏单击一次性备份 启动一次性备份向导。



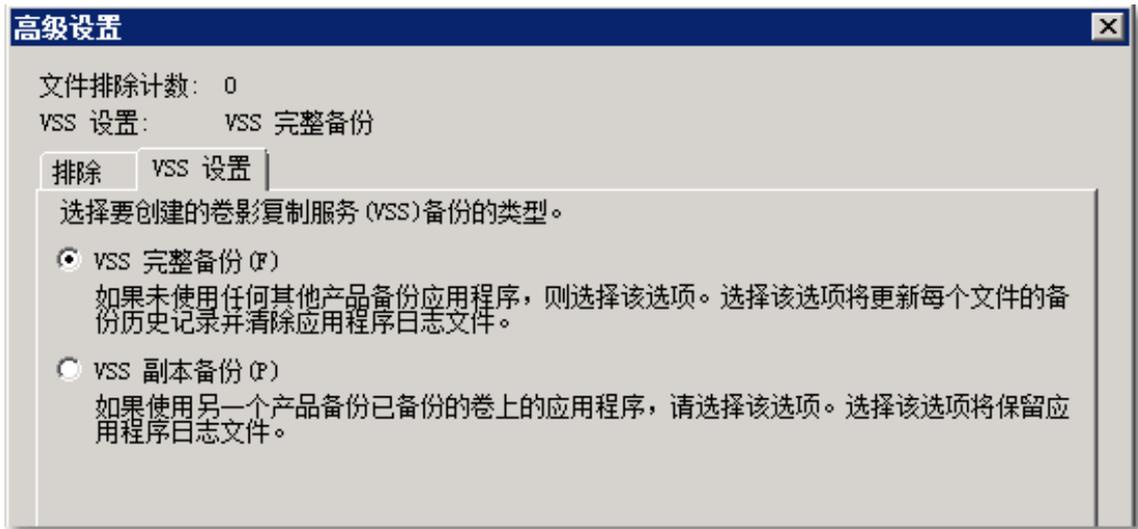
2. 在选择备份配置中按需选择要备份的对象：整个服务器或自定义（卷或文件）。



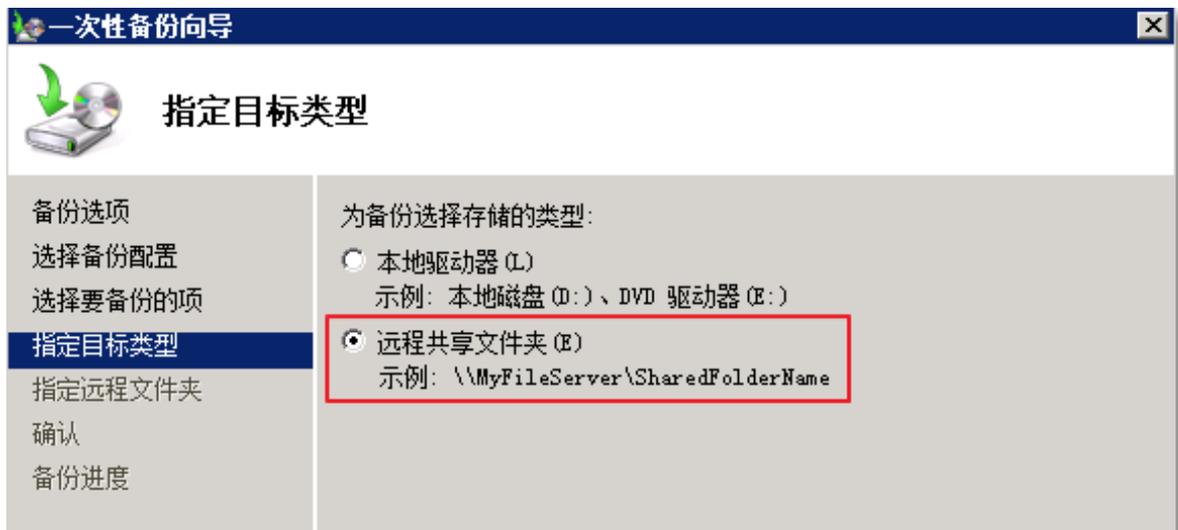
- 当选择自定义时，需要进一步选择要备份的项，单击添加项来完成。



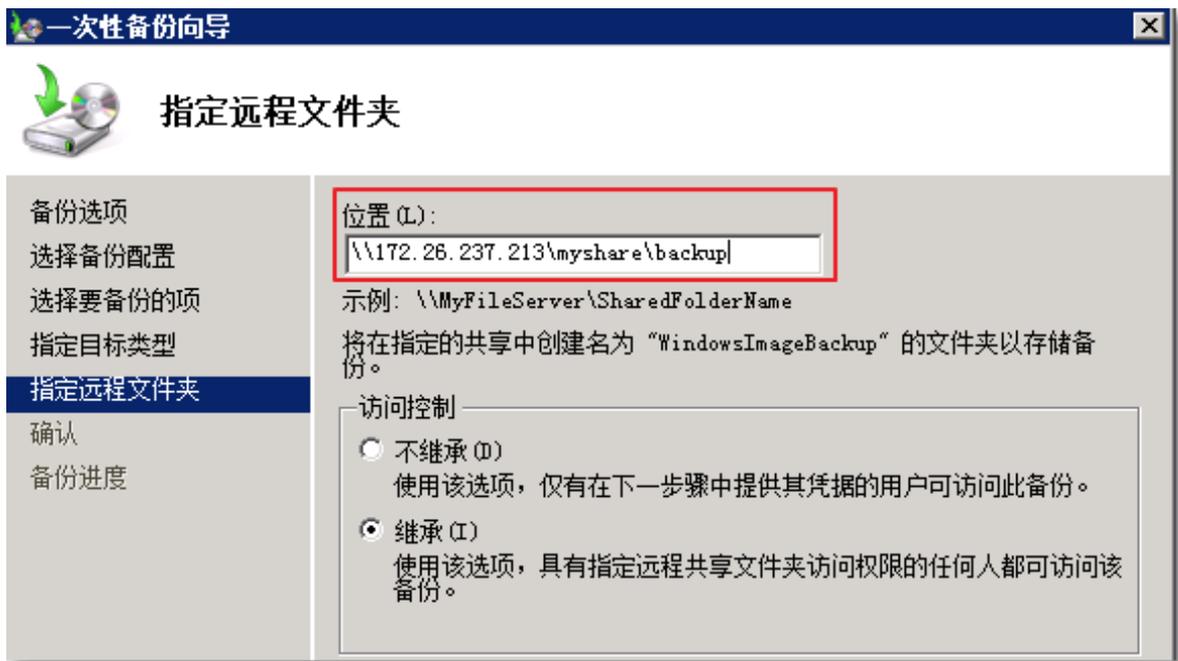
- 在选择要备份的项中，打开高级设置，可以设置备份类型，以及备份中跳过目录中特定的文件等。



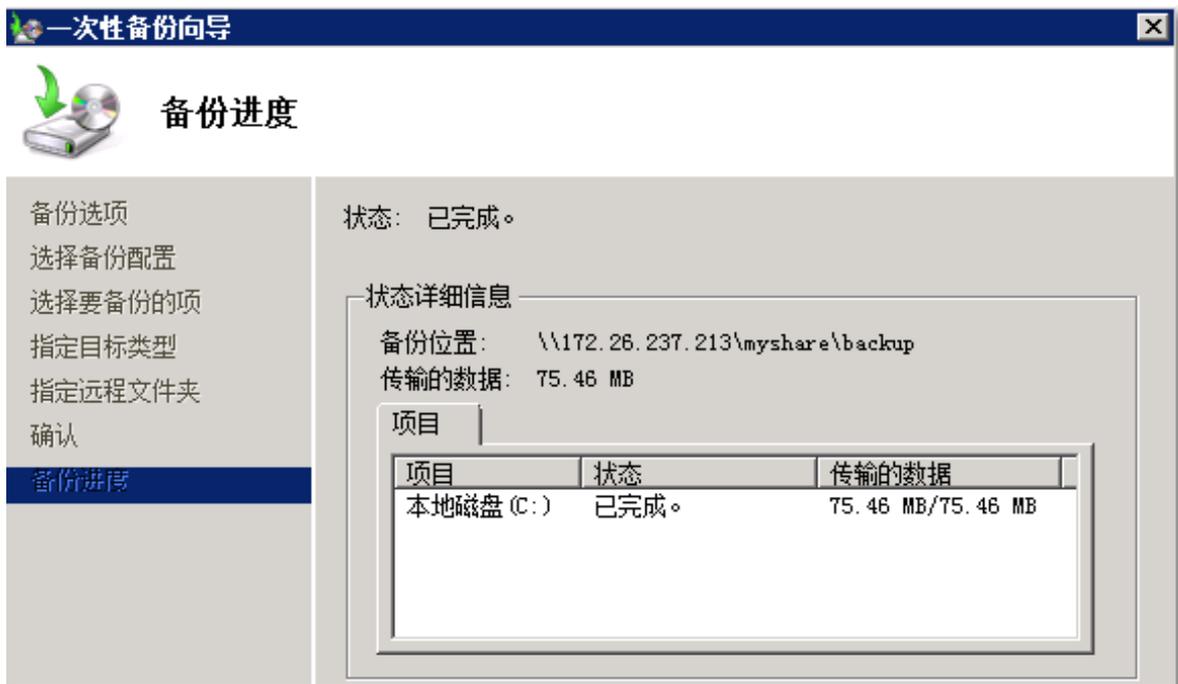
3. 在指定目标类型中选择存储位置，勾选远程共享文件夹。



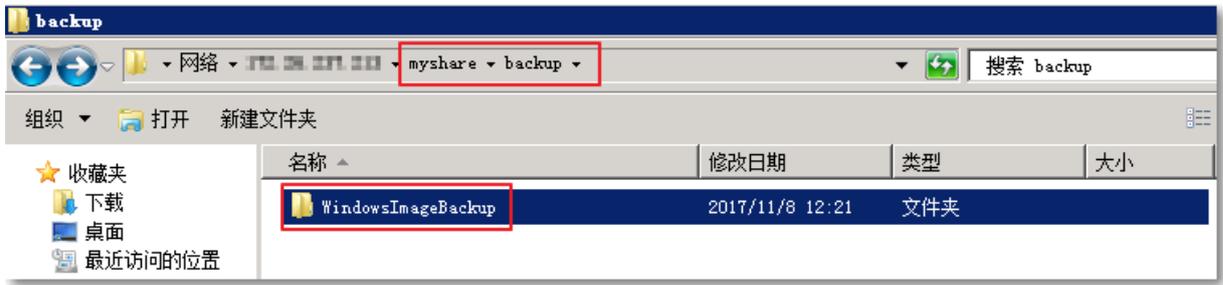
4. 在指定远程文件夹中，指定 NAS SMB 挂载点下的一个位置，比如“backup”目录。



5. 启动备份，等待备份完成。



备份完成后，您可以在 NAS 上“backup”目录下，查看已备份的内容。



备份计划

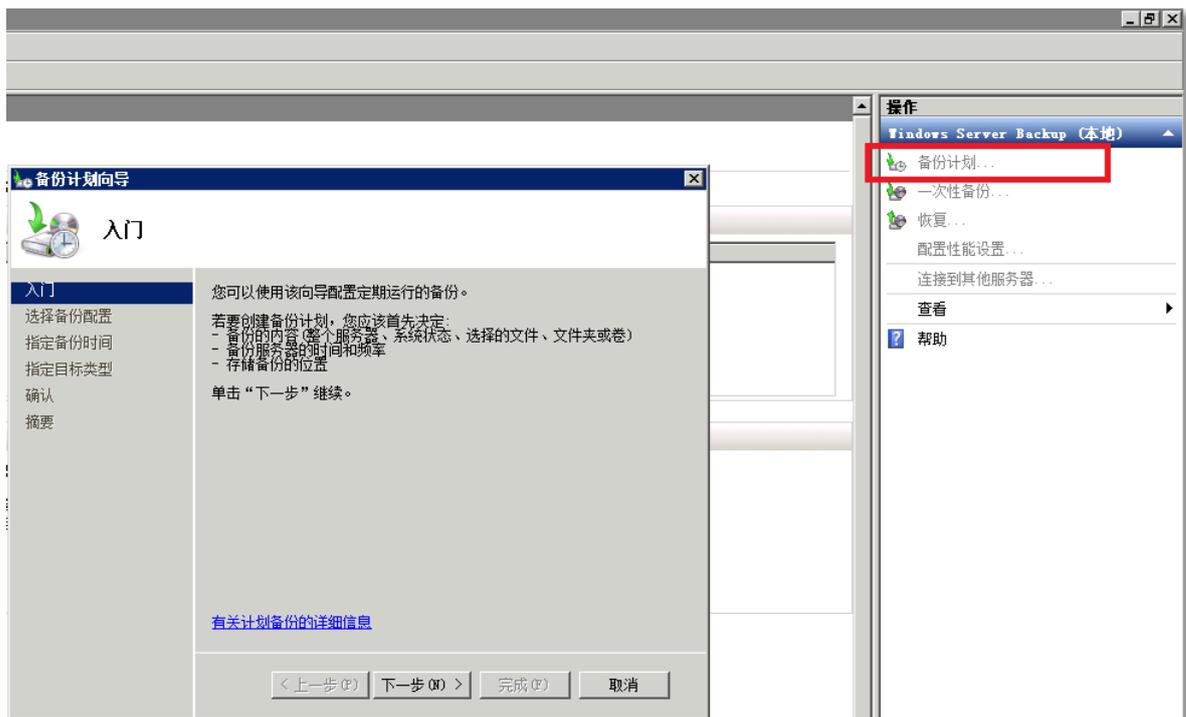
备份计划中可以配置定期自动进行一次性备份。其操作流程与一次性备份类似，主要区别是需要制定备份的时间。



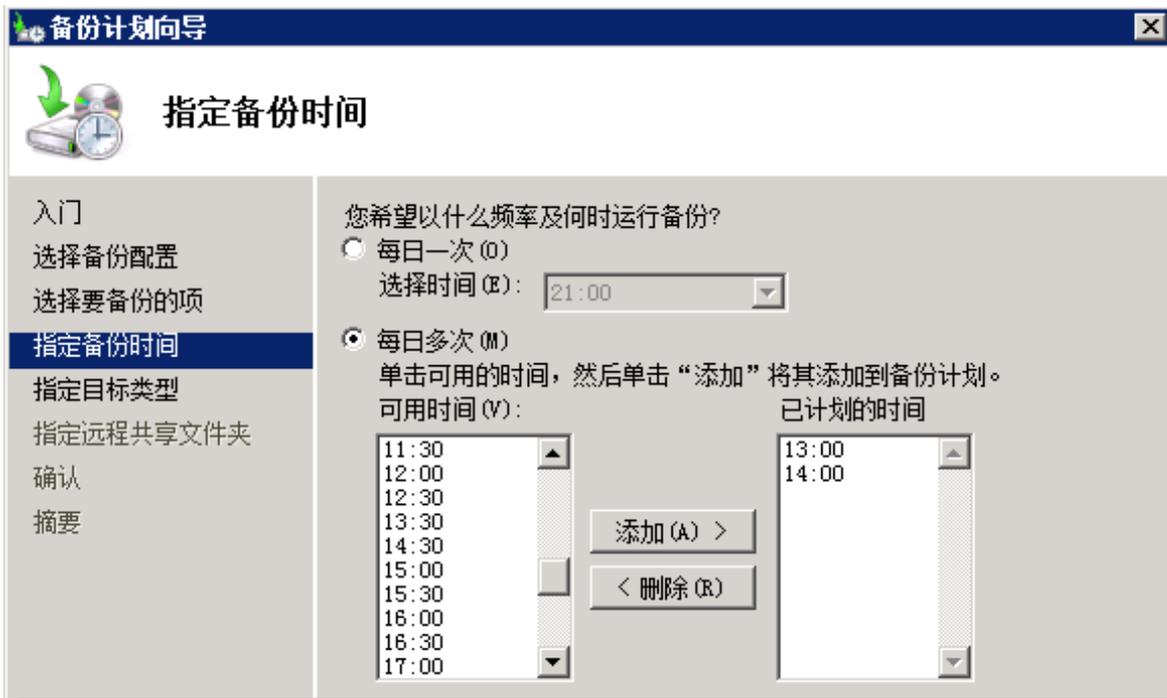
说明:

下述操作步骤中，与一次性备份类似的步骤不作赘述。

1. 打开Windows Server Backup，在其右侧操作栏单击备份计划 启动备份计划向导。

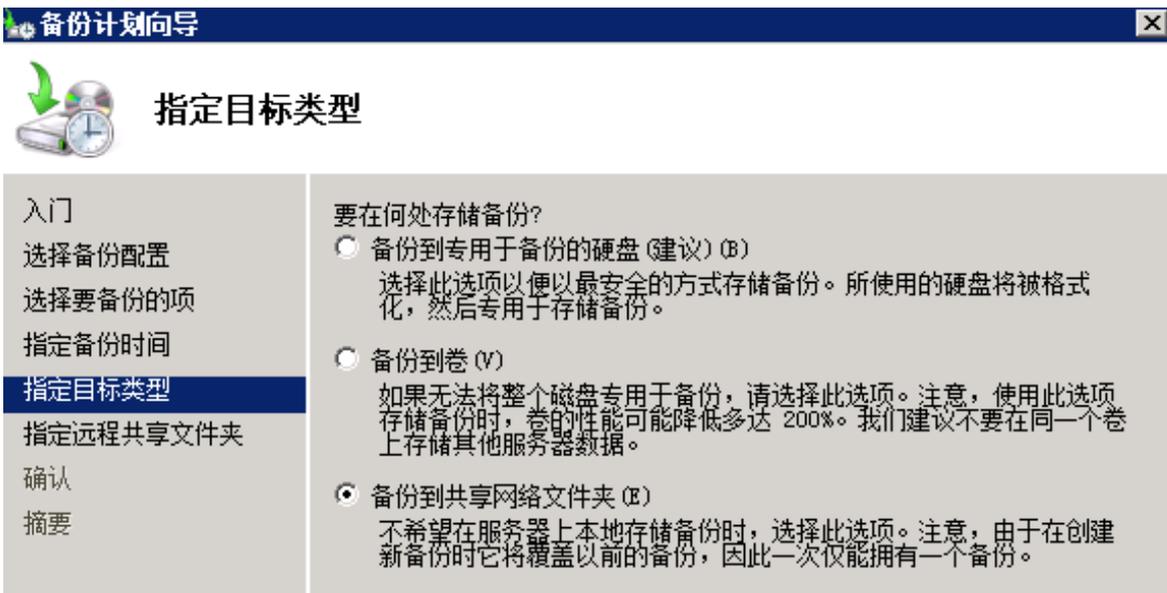


2. 在指定备份时间中设置备份的频率和运行时间。



3. 在指定目标类型中，勾选 备份到共享网络文件夹。

 **说明:**
当将远程共享文件夹用作计划备份的存储目标时，各备份会擦除前面的备份，只保留最新的备份。

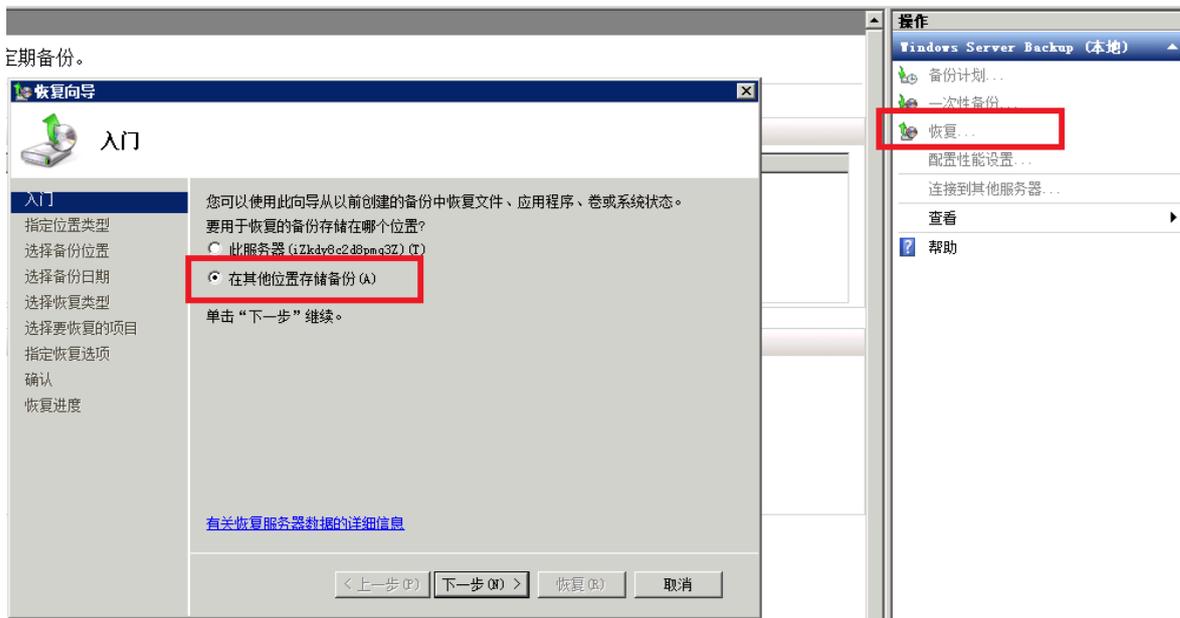


4. 启动备份计划，备份任务会在您指定的时间内自动运行。

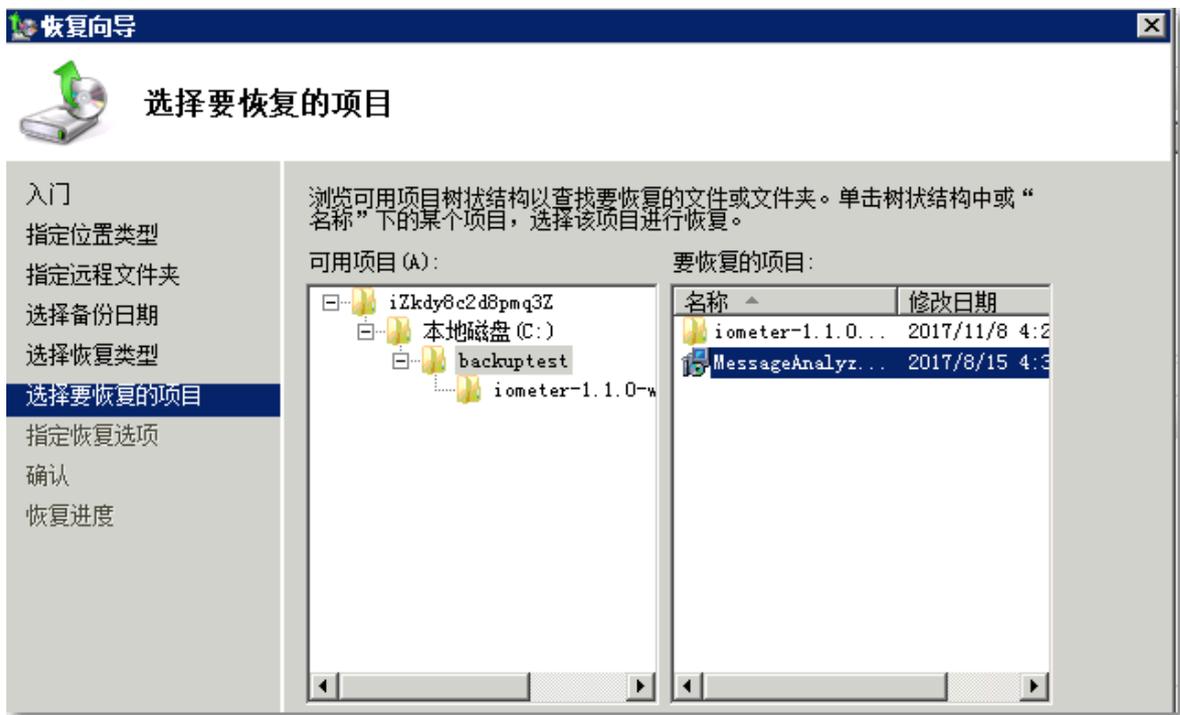
使用 Windows Server Backup 恢复数据

在发生误删除，或者文件被覆盖等情况，您可以从之前备份到 NAS 的数据中恢复文件。

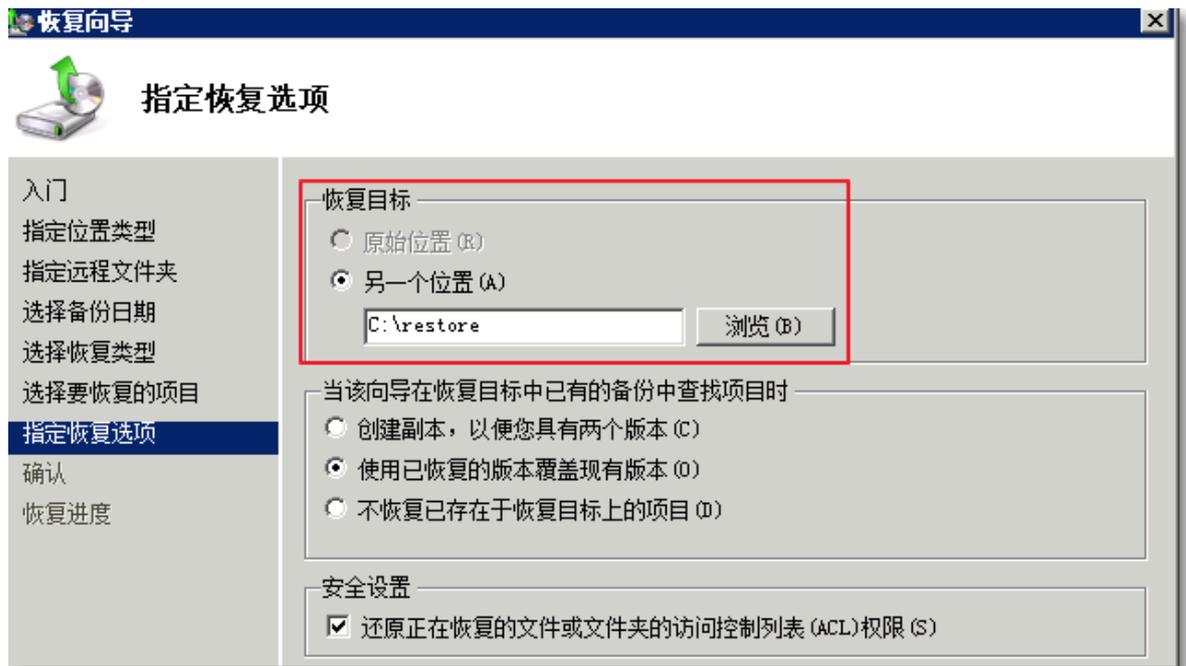
1. 打开 Windows Server Backup，在其右侧操作栏单击 恢复 启动 恢复向导。
2. 在 入门 中，指定备份数据的来源。勾选 在其他位置存储备份，并配置之前用作备份的目录。



3. 在 选择要恢复的项目 中，选择备份中的一个或者某几个文件或者子文件夹进行恢复。



4. 在指定恢复选项中，指定恢复数据保存到本地的位置。



5. 启动数据恢复，等待恢复完成。

5 通过云服务器ECS (Linux) 访问SMB文件系统

本文主要介绍如何将SMB文件系统挂载至云服务器ECS (Linux) 并进行读写操作。

前提条件

- 在需要创建文件系统的地域，已有可用的云服务器ECS (Linux)。

SMB文件系统现在官方支持如下的Linux分发版本，本文中，如果没有特别声明，也只针对以下几个Linux分发版本。

- CentOS 7.6 64bit (3.10.0-957.5.1.el7.x86_64)
- Ubuntu 18.04 64bit (4.15.0-48-generic)
- Debian 9.9 64bit (4.9.0-9-amd64)
- Suse Enterprise Server 12 SP2 64bit (4.4.74-92.35-default)
- OpenSUSE 42.3 64bit (4.4.90-28-default)
- Aliyun Linux (4.19.34-11.al7.x86_64)
- CoreOS (4.19.43-coreos VersionID=2079.4.0)



说明:

由于Linux一些早期版本的SMB内核客户端在某些关键场景有缺陷，用户如果使用非官方支持的Linux分发版本，阿里云不能保证该SMB文件系统的可靠性。

- 网络连通
 - 云服务器ECS (Linux) 需要和SMB文件系统在可连通的同一个用户网络中（比如在同一个VPC）。
 - 检查文件系统白名单，确保云服务器ECS (Linux) 已经被授权访问该SMB文件系统。
 - 确保端口445处于打开状态，SMB通过TCP端口445通信。
如果端口445未打开，请在目标ECS实例的安全组中添加关于端口445的安全组规则，详情请参见[添加安全组规则](#)。
- 已创建SMB文件系统，详情请参见[创建文件系统](#)。
- 已添加挂载点，详情请参见[添加挂载点](#)。

- 软件要求

Linux分发版本都预装了内核客户端，您还需安装cifs-util工具包。

- 如果您使用Ubuntu、Debian操作系统，使用apt-get包管理器进行安装

```
sudo apt-get update
```

```
sudo apt-get install cifs-util
```

- 如果您使用RHEL、CentOS、Aliyun Linux操作系统，使用yum包管理器进行安装

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

- 如果您使用OpenSUSE、SLES12-SP2操作系统，使用zypper或者yast工具进行安装

```
sudo zypper install cifs-utils
```

```
sudo yast2 -> Software -> Software Management, 然后安装cifs-utils
```

- 如果您使用阿里云支持的CoreOS分发版本，通过以下方法进行安装

1. 配置SELINUX

```
sed -i 's/SELINUXTYPE=mcs/SELINUXTYPE=targeted/' /etc/selinux/  
config
```

2. 在CoresOS上自行编译cifs-utils

您可以执行以下命令启动一个Fedora容器用以编译cifs-utils客户端工具或者下载阿里云官方提供使用的CoreOS版本的cifs-utils工具，并拷贝至/tmp/或者/bin目录。

```
$ docker run -t -i -v /tmp:/cifs fedora /bin/bash  
  
fedora # yum groupinstall -y "Development Tools" "Development  
Libraries"  
  
fedora # yum install -y bzip2  
  
fedora # curl https://download.samba.org/pub/linux-cifs/cifs-  
utils/cifs-utils-  
6.9.tar.bz2 --output cifs-utils-6.9.tar.bz2;  
  
fedora # bunzip cifs-utils-6.9.tar.bz2; && tar xvf cifs-utils-6  
.9.tar  
  
fedora # cd cifs-utils-6.9; ./configure && make  
  
fedora # cp mount.cifs /cifs/  
  
fedora # exit
```

挂载文件系统

1. 使用root用户或者sudo enabled客户端管理员用户，登录云服务器ECS (Linux)。

2. 执行以下命令，挂载文件系统。

```
mount -t cifs //xxx-crf23.eu-west-1.nas.aliyuncs.com/myshare /mnt -o  
vers=2.1,guest,uid=0,gid=0,dir_mode=0755,file_mode=0755,mfsymlinks,  
cache=strict,rsize=1048576,wsiz=1048576
```

挂载命令格式：`mount -t cifs //<挂载点域名>/myshare <挂载目录> -o <挂载选项>`

参数	说明
文件系统类型	SMB文件系统，必须使用-t cifs。
挂载点域名	创建文件系统挂载点时，自动生成的挂载点域名，请根据实际值替换。挂载点详情请参见 ../DNnas1882233/ZH-CN_TP_18694_V10.dita#task_27531_zh 。
myshare	SMB的share名称，不允许变更。
挂载目录	您要挂载的目标目录，如/mnt/sharepath。

参数	说明
挂载选项 (option)	<p>通过 <code>-o</code> 指定挂载选项</p> <ul style="list-style-type: none"> · (必选) <code>vers</code>: 支持2.1 和 3.0协议版本。 · (必选) <code>guest</code>: 在认证方面, 现在只支持基于ntlm认证协议的<code>guest</code>挂载。即使用<code>username=guest</code>、<code>password=guest</code>或者<code>guest</code>。 <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p> 说明: 服务器支持ntlm, ntlmv2和ntlmssp。缺省时, SMB客户端和服务器会协商一个可接受的ntlm认证协议; 或者您在挂载时, 通过"sec" option可以选择一个自己期望的值 (ntlm, ntlmv2 或者ntlmssp)。</p> </div> <ul style="list-style-type: none"> · (可选) <code>uid</code>: 挂载成功后, 文件所属的用户。如果未设置<code>uid</code>, 则默认<code>uid=0</code>。 · (可选) <code>gid</code>: 挂载成功后, 文件所属的用户组。如果未设置<code>gid</code>, 则默认<code>gid=0</code>。 · (可选) <code>dir_mode</code>: 向用户授予目录的读取、写入和执行权限。必须以0开头, 如0755、0644等。如果未设置<code>dir_mode</code>, 则默认<code>dir_mode=0755</code>。 · (可选) <code>file_mode</code>: 向用户授予普通文件的读取、写入和执行权限。必须以0开头, 如0755、0644等。如果未设置<code>file_mode</code>, 则默认<code>file_mode=0755</code>。 · (可选) <code>mfsymlinks</code>: 需要用以支持symbol link功能。 · (可选) <code>cache</code>: <ul style="list-style-type: none"> - <code>cache=strict</code>: 设置SMB客户端使用客户端缓存。如果未设置<code>cache</code>, 则默认<code>cache=strict</code>。 - <code>cache=none</code>: 设置SMB客户端不使用客户端缓存。 · (可选) <code>rsize</code>: 用来设置读数据包的最大限制。一般不需要设置, 使用缺省值1048576即可。 · (可选) <code>wsize</code>: 用来设置内写数据包的最大限制, 一般不需要设置, 使用缺省值1048576即可。 · (可选) <code>atime relatime</code>: 如果您的业务不是对文件的访问时间极为敏感请不要在挂载时使用<code>atime</code>选项, 缺省时会使用<code>relatime</code>方式挂载。 <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p> 说明:</p> <ul style="list-style-type: none"> · 被授权的云服务器 (Linux) 管理员拥有对SMB文件系统的绝对控制权。 · 您可以使<code>mount grep cifs</code>命令查询自己的挂载点信息。 · 如果您使用非官方支持的Linux分发版本, 强烈建议使用内核在3.10.0-514以上的版本。如果Linux kernel版本小于等于3.7, 一定要在挂载选项中显示设置<code>cache=strict</code>参数。您可以使<code>uname -a</code>命令检查当前内核版本。 </div>

3. 执行mount -l命令，查看挂载结果。

如果回显包含如下类似信息，说明挂载成功。

```
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw,relatime)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=808920k,mode=700)
cn-hangzhou.nas.aliyuncs.com/myshare on /mnt type cifs (rw,relatime,vers=2.1,sec=none,cache=strict,domain=,uid=0,noforceuid,gid=0,noforcegid,addr=,file_mode=0755,dir_mode=0755,soft,nounix,serverino,mapposix,rsize=1048576,wsz=1048576,echo_interval=60,actimeo=1)
```

4. 挂载成功后，您可以在ECS (Linux) 上访问NAS文件系统，执行读取或写入操作。

您可以把NAS文件系统当作一个普通的目录来访问和使用，例子如下：

```
[root@i7n5c6owi-q421d4p0f16qz ~]# mkdir /mnt/dir1
[root@i7n5c6owi-q421d4p0f16qz ~]# mkdir /mnt/dir2
[root@i7n5c6owi-q421d4p0f16qz ~]# touch /mnt/file1
[root@i7n5c6owi-q421d4p0f16qz ~]# echo 'some file content' > /mnt/file2
[root@i7n5c6owi-q421d4p0f16qz ~]# ls /mnt
dir1 dir2 file1 file2 tmp
```

经典使用场景

不同使用场景，可选择不同的挂载选项，比较经典的使用场景及挂载选项配置如下所示。

- 云服务器ECS (Linux) 共享访问场景

在多个云服务器ECS (Linux) 中需要共享访问文件系统数据，但没有用户权限控制要求，被授权的云服务器ECS (Linux) 管理员可以使用如下方法在各个云服务器ECS (Linux) 上执行挂载。

```
mount -t cifs //smbfs.hangzhou-g.aliyun.com/myshare /mnt/sharepath
-o vers=2.1,guest,mfsymlinks
```

- 多用户Home Directory场景

在多个云服务器ECS (Linux) 中需要共享访问文件系统数据时，如果有权限控制需求，可以通过挂载时指定uid、gid、dir_mode、file_mode来满足要求。

- 云服务器ECS (Linux) WebServer共享访问场景

在多个云服务器ECS (Linux) 上安装WebServer(如apache)，并且SMB文件系统做共享文件存储。



说明：

- SMB文件系统主要特点是共享访问、横向扩展、高可用，和本地硬盘由于实现机理不同，某些场景的小文件访问性能上会稍微有一些差距。对于WebServer场景，如果想要达到极致性能，可以考虑只将需要共享的文件放在SMB文件系统上，而将不需要共享访问的WebServer程序等放在本地硬盘。

- WebServer应用通常网络协议通讯负载较大，我们为这个场景做了专门的WebServer加速功能，您可以联系阿里云NAS团队申请开通。

· 云服务器ECS (Windows) 和云服务器ECS (Linux) 共享访问

如果您需要同时从云服务器ECS (Windows) 和云服务器ECS (Linux) 访问SMB文件系统的内容。这个场景下，云服务器ECS (Linux) 挂载时一定要使用客户端缓存，即设置cache=strict或者缺省方式挂载。

如果您在使用中遇到问题，请参见[通过云服务器ECS \(Linux\) 访问SMB文件系统的问题排查](#)。