Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.
5. **By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates.** This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. **Please contact Alibaba Cloud directly if you discover any errors in this document.**
# Document conventions

<table>
<thead>
<tr>
<th>Style</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚠️</td>
<td>A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.</td>
<td><strong>Danger:</strong> Resetting will result in the loss of user configuration data.</td>
</tr>
<tr>
<td>⚠️</td>
<td>A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.</td>
<td><strong>Warning:</strong> Restarting will cause business interruption. About 10 minutes are required to restart an instance.</td>
</tr>
<tr>
<td>⚠️</td>
<td>A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.</td>
<td><strong>Notice:</strong> If the weight is set to 0, the server no longer receives new requests.</td>
</tr>
<tr>
<td>📖</td>
<td>A note indicates supplemental instructions, best practices, tips, and other content.</td>
<td><strong>Note:</strong> You can use Ctrl + A to select all files.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Closing angle brackets are used to indicate a multi-level menu cascade.</td>
<td>Click <strong>Settings &gt; Network &gt; Set network type</strong>.</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Bold formatting is used for buttons, menus, page names, and other UI elements.</td>
<td>Click <strong>OK</strong>.</td>
</tr>
<tr>
<td><strong>Courier font</strong></td>
<td>Courier font is used for commands.</td>
<td>Run the <strong>cd /d C:/window</strong> command to enter the Windows system folder.</td>
</tr>
<tr>
<td><strong>Italic</strong></td>
<td>Italic formatting is used for parameters and variables.</td>
<td><strong>bae log list --instanceid</strong> Instance_ID</td>
</tr>
<tr>
<td>[] or [a</td>
<td>b]</td>
<td>This format is used for an optional value, where only one item can be selected.</td>
</tr>
<tr>
<td><strong>Style</strong></td>
<td><strong>Description</strong></td>
<td><strong>Example</strong></td>
</tr>
<tr>
<td>----------</td>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>{} or {a</td>
<td>b}</td>
<td>This format is used for a required value, where only one item can be selected.</td>
</tr>
</tbody>
</table>
Contents

Legal disclaimer................................................................. I
Document conventions.......................................................... I

1 Overview................................................................. 1

2 High-performance website....................................................... 3
  2.1 Use Windows IIS to access Apsara File Storage NAS......................... 3
  2.2 Use NGINX as a proxy for Apsara File Storage NAS............................. 20

3 Application server shared storage............................................. 24
  3.1 Access an NFS file system from a Windows ECS instance...................... 24
  3.2 Use Windows Server Backup to back up data from an ECS instance to Apsara
      File Storage NAS.................................................................................................... 29

4 Access a file system remotely..................................................... 34
  4.1 Access an Apsara File Storage NAS file system from a local data center by using
      VPN Gateway......................................................................................................... 34
  4.2 Access an Apsara File Storage NAS file system from a local IDC by using NAT
      Gateway................................................................................................................ 38
  4.3 Use SFTP to transfer data to and from an Apsara File Storage NAS file system.... 43

5 Access an SMB file system from a Linux ECS instance.................. 46
1 Overview

The best practices for Apsara File Storage NAS consists of many different types of scenarios. These scenarios include remote access, container storage, Windows applications, AI-powered training, Web applications and content management, genetic algorithms and evolutionary computation, and data backup. These best practices allow you to make more efficient use of Apsara File Storage NAS while meeting your business requirements.

Remote access

- #unique_4
- #unique_5
- Access an Apsara File Storage NAS file system from a local data center by using VPN Gateway
- Access an Apsara File Storage NAS file system from a local IDC by using NAT Gateway
- Use SFTP to transfer data to and from an Apsara File Storage NAS file system
- Access an SMB file system from a Linux ECS instance

Container storage

- Solutions by Alibaba Cloud container storage
- Cross-zone high-availability solutions by Alibaba Cloud containers

Windows applications

- Use Windows IIS to access Apsara File Storage NAS
- Access an NFS file system from a Windows ECS instance
- Best practices for integrating IIS and Apsara File Storage NAS
- Use Windows Server Backup to back up data from an ECS instance to Apsara File Storage NAS
- Fix issues such as a failure to access an SMB volume of Apsara File Storage NAS from SQL Server by using the SYSTEM user to mount the volume
- Use VisualSVN Server to manage code based on an Apsara File Storage NAS SMB volume
- Fix issues such as a failure to load SMB volumes for Windows Server 2016 IIS by installing and configuring an Active Directory domain
- Build projects that integrate IIS, WordPress, and MySQL technologies on an Apsara File Storage NAS SMB volume
• Use Visual Studio to debug projects that integrate ASP.NET and SQL Server technologies and deploy these projects to IIS on an Apsara File Storage NAS SMB volume

AI-powered training

• Alibaba Cloud AI solutions
• Best practice for AI inference based on elastic compute

Web applications and content management

• Integrate WordPress websites with Apsara File Storage NAS
• Use Apsara File Storage NAS to build Jenkins continuous integration environments
• Use NAS Extreme to build high-availability GitLab
• Use NGINX as a proxy for Apsara File Storage NAS

Genetic algorithms and evolutionary computation

Best practice for drug screening by using EHPC
2 High-performance website

2.1 Use Windows IIS to access Apsara File Storage NAS

This topic describes how to configure the built-in Internet Information Service (IIS) for Windows-based Elastic Compute Service (ECS) instances and configure Alibaba Cloud Apsara File Storage NAS to provide Web and File Transfer Protocol (FTP) services.

**Context**

Apsara File Storage NAS provides file storage services for Alibaba Cloud ECS instances, E-HPC, Container Service, Elastic Web Hosting, Batch Compute, and other compute nodes. Apsara File Storage NAS is compatible with standard file access protocols, such as Network File System (NFS) and Server Message Block (SMB).

Compared with NFS, the SMB protocol is more compatible with Windows operating systems (OSs). Each different version of Windows OS supports the SMB protocol. Most Windows applications can access Apsara File Storage NAS through the SMB protocol without changing the application code. Therefore, we recommend that you use an SMB-based Apsara File Storage NAS file system when you run applications on Windows-based ECS instances.

Windows Server is a very popular platform for building websites. Many Alibaba Cloud users select Windows-based ECS instances to deliver website services. You can store content resources of your websites on a reliable pay-as-you-go SMB-based Apsara File Storage NAS file system with high throughput. IIS allows you to access the data stored on the file system in the same way that you access local data. In this way, you can separate computing and storage resources for your websites. In addition, you can scale your computing and storage resources based on your business needs.

The FTP service provided by IIS includes a wide range of requirements. Many website administrators remotely manage website content by using the FTP service. Meanwhile, many Alibaba Cloud users want to transfer and share files between wide area networks (WANs) and Alibaba Cloud by using the FTP service on Windows-based ECS instances.

This topic takes IIS 7.5 (Windows Server 2008 R2) as an example to describe how to use Apsara File Storage NAS to provide both the Web service and FTP service on a single Windows-based ECS instance. The instructions provided in this topic are also applicable for
other versions of Windows OS. You can also use Alibaba Cloud Server Load Balancer (SLB) to construct a multi-server website with higher levels of error tolerance and resilience. For more information, see What is Server Load Balancer?

**Note:**

- The topic provides some security suggestions, but they cannot serve as a complete security solution. You must devise your own plans to secure your Web services and data. For example, you can safeguard your system security by setting up firewalls, configuring security groups for ECS instances, and installing OS patches. You can also safeguard your service security by using Alibaba Cloud security products.
- For improved security and management, a normal user (iss_user) instead of the system administrator is used to access data through the FTP service or through the Web service provided by IIS installed on the Windows Server 2016 OS.
Install Windows IIS

The Windows Server 2008 R2 OS is taken as an example to describe how to add an IIS role and install IIS by using Server Manager.

For more information about how to install IIS on different Windows OSs, see Install IIS and ASP.NET Modules.

1. Open the Server Manager window.
2. Click the Roles node, and click Add Roles to open the Add Roles Wizard.
3. Click the **Server Roles** node, and select **Web Server (IIS)**.
4. Click the **Role Services** node and select role services to be installed for the Web Server (IIS).

In addition to default services, you must also select **FTP Server** and **ASP** to deliver FTP service and demonstrate dynamic Web pages through scripts.

5. After you complete the configuration, click **Install**.

**Create and access an SMB file system**

You can store your Web resources and configuration files in the shared directory (myshare by default) of an SMB-based Apsara File Storage NAS file system. After you create an SMB file system, you can configure a permission group to make sure that the current Web server can read data from and write data to the file system.

1. Create an SMB file system. For more information, see **Create a file system**.

2. Add a mount target for the SMB file system. For more information, see **Add a mount target**.
3. Open the Windows Explorer window and enter `\\xxxx-xxxx.cn-hangzhou.nas.aliyuncs.com\myshare` in the address bar to access the SMB file system.

- `xxxx-xxxx.cn-hangzhou.nas.aliyuncs.com` is the domain name of the mount target for the SMB file system.
- `myshare` is the default shared directory of the SMB file system. You cannot change this directory.

4. Create a subdirectory named `www` under the `myshare` directory of the SMB file system to store Web page files of your website.

The static Web page file `index.html` and the dynamic Web page file `test.asp` are created as an example to describe how to deliver Web services. The static Web page shows `Hello World!` and the dynamic Web page shows the current system time that updates in real time.

- **Index.html**

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

- **Test.asp**

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

**Set up the Windows IIS Web service**

1. Open the **Internet Information Services (IIS) Manager** window.

2. Click localhost, choose **View Sites > Default Web Site**, and then click **Basic Settings**.
3. In the **Edit Site** dialog box that appears, configure **Physical path** and click **OK**.

In the **Physical path** field, enter the storage path of Web resources on Alibaba Cloud Apsara File Storage NAS, for example, `\\xxxx-xxxx-shanghai.nas.aliyuncs.com\myshare` 
`www. xxxx-xxxx-shanghai.nas.aliyuncs.com` is the domain name of the mount target. You must change the domain name based on your business requirements.

**Note:**

- By default, you must use a user account and user group of IIS to access a network drive (for example, Z:\) mapped in the current user session. You cannot directly access the mapped network drive as a Windows user. Otherwise, an access error message is displayed.
- If you are using the Windows Server 2016 OS, you need to complete other operations following the Windows IIS Web service setting to achieve coordination of IIS and Alibaba Cloud Apsara File Storage NAS. For more information, see [FAQ](#).
4. Verify the setting.

Enter the local paths of index.html and test.asp files in the address bar of your local browser to open these files. The pages shown in the following figures are displayed if IIS is running as expected.

You can also configure security groups for your ECS instances and configure Windows Firewall to guarantee Web access security.

Set up the Windows IIS FTP service

1. Open the Internet Information Services (IIS) Manager window.

2. Install the SSL certificate.
   a) On the page of the localhost, double-click Server Certificates.
   b) On the Server Certificates page that appears, click Create Self-Signed Certificate.
   c) Specify a name for the certificate, and click OK.
3. Set up an FTP site.
   a) On the Sites page, click **Add FTP Site**.
   b) In the **Add FTP site** dialog box, configure the relevant information and click **Next**.

   In the **Physical path** field, enter the storage path of Web resources on Alibaba Cloud Apsara File Storage NAS, for example, `\xxxx-xxxx-shanghai.nas.aliyuncs.com\myshare\www.xxxx-xxxx-shanghai.nas.aliyuncs.com` is the domain name.
of the mount target. You must change the domain name based on your business requirements.

You can select another subdirectory under the myshare directory based on your business requirements. You can also set up multiple FTP sites with different ports to access different directories.

c) In the **Binding and SSL Settings** dialog box, configure the relevant information and click **Next**.

- **Port**: The default port number is 21. For security concerns, port number 2222 is used.
- **SSL Certificate**: Select the created SSL certificate.
d) Configure authentication and authorization information, and click Finish.

- **Authentication**: Select Basic.
- **Authorization**: Select a user who is allowed to access Apsara File Storage NAS. iis_user is used as an example.
- **Permissions**: Set read/write permissions for the user.
4. Set up the FTP firewall.

Open the **FTP Firewall Support** dialog box, specify the **Data Channel Port Range**, and then click **Apply**.
5. In the **Server Manager** window, restart the FTP service to make the port range configuration take effect.
6. In the ECS console, configure the security group for the ECS instance to restrict access to or from FTP clients. For more information, see #unique_17.
7. Access the FTP site through the FTP client WinSCP.
   a) Open WinSCP.
   b) Click **Yes** to accept the server certificate.

   When an FTP client accesses an FTP site for the first time, the client must accept the server certificate.

   ![Warning dialog](image)

   The server's certificate is not known. You have no guarantee that the server is the computer you think it is.

   Server's certificate details follow:

   **Issuer:**
   - Organization: iZmolxWlm6gcZbZ

   **Subject:**
   - Organization: iZmolxWlm6gcZbZ

   **Valid:** 5/24/2017 6:26:34 AM - 5/24/2018 12:00:00 AM


   **Summary:** Unable to get local issuer certificate. The error occurred at a depth of 1 in the certificate chain.

   When connecting using an IP address, it is not possible to verify if the certificate was issued for the server. Use a hostname instead of the IP address.

   If you trust this certificate, press Yes. To connect without storing certificate, press No. To abandon the connection press Cancel.

   c) Set the protocol type, port number, and logon information.
d) Enter the password of the authorized user (iis_user).

e) Establish a data connection to allow the server to read data from and transfer data with remote directories.
f) After the data connection is established, you can upload and download files.

FAQ

How can I achieve coordination of IIS and Alibaba Cloud Apsara File Storage NAS if I am using the Windows Server 2016 OS?

If you are using the Windows Server 2016 OS, you need to complete other operations following the Windows IIS Web service setting to achieve coordination of IIS and Alibaba Cloud Apsara File Storage NAS. The operations you need to take are as follows:

1. Modify the registry key of the SMB client.
   a) Open the Registry Editor window.
   b) Choose **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > LanmanWorkstation > Parameters > AllowInsecureGuestAuth**, right-click a blank area, and choose **New > DWORD (32-bit) Value**.
   c) Set the value name to **AllowInsecureGuestAuth** and set the value data to **1**.
2. Specify a local user to access Web resources stored on Alibaba Cloud Apsara File Storage NAS.
   a) Open the **Internet Information Services (IIS) Manager** window.
   b) Click localhost, choose **View Sites > Default Web Site**, and then click **Basic Settings**.
   c) In the **Edit Site** dialog box, click **Connect as**.
   d) Select **Specific User** and click **Set**.
   e) Set the username and password, and then click **OK**.
      Set the user to iis_user.

**Note:**
- When you access files stored in the Apsara File Storage NAS shared directory through IIS, the backend of IIS may access the shared directory multiple times. Although each access does not take a long time, multiple accesses may cause a long response time to clients. To avoid this situation, you can choose **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > LanmanWorkstation > Parameters** and specify larger values (for example, 600) for the following three registry keys: **FileInfoCacheLifetime**, **FileNotFoundCacheLifetime**, and **DirectoryCacheLifetime**. For more information, see **SMB2 Client Redirector Caches Explained**.
- If the three registry keys are unavailable, you can create the registry keys by using the field format that is required by your Windows OS.
- IIS accesses the contents of JavaScript (JS), Cascading Style Sheets (CSS), and other Web page programs frequently. We recommend that you select a local directory to store the contents.

### 2.2 Use NGINX as a proxy for Apsara File Storage NAS

This topic describes how to use NGINX as a proxy for Apsara File Storage NAS.

**Context**

NGINX is a light-weight high-performance Web server. It includes many features and can be used as a reverse proxy. One of the most common application modes for NGINX is to serve as a reverse proxy. A proxy server accepts connection requests from clients over the Internet. Then, the proxy server forwards these requests to a server that resides in an internal network and returns responses from the server to these clients. In such cases, when a proxy server acts on behalf of the server, it is called a reverse proxy.
An application server that resides in a private network is not accessible by clients outside the private network. In such cases, a reverse proxy is required to serve as an intermediary between an application server and clients. The reverse proxy resides in the same private network as the application server but is accessible by clients outside the internal network. The reverse proxy and the application server can share the same physical server but use different ports.

The following example uses one NGINX server as a reverse proxy, four NGINX servers as proxy servers, and Apsara File Storage NAS as backend storage. Apsara File Storage NAS stores cache files of proxy servers, and back-to-origin files or static data files uploaded by end-users. Apsara File Storage NAS allows shared access to the same file system from different proxy servers. This enables data to be synchronized between proxy servers and ensures data consistency. This also prevents servers from repeatedly retrieving files from the origin and guarantees efficient use of bandwidth. The following figure shows an example of network topology.

You can create an environment as shown in the preceding topology by following the instructions provided in this topic. This topic takes a CentOS ECS instance as an example.
Step 1: Deploy an NGINX reverse proxy

1. Install NGINX.
   
   ```bash
   yum install nginx
   ``

2. Configure a reverse proxy that points to a proxy server.
   
   a) Use the following command to open the `/etc/nginx/nginx.conf` file.
   
   ```bash
   vim /etc/nginx/nginx.conf
   ```

   b) In the `/etc/nginx/nginx.conf` file, configure the http context. Take the following code as an example.

   ```
   http {
     upstream web{
       server 10.10.0.10;
       server 10.10.0.11;
       server 10.10.0.12;
       server 10.10.0.13;
     }
     server {
       listen 80;
       location / {
         proxy_pass http://web;
       }
     }
   }
   ```

Step 2: Create a file system and mount target

1. Create an NFS file system in a region. For more information, see #unique_18/unique_18_Connect_42_section_5jo_0kj_jn5.

   Note:
   A file system and an ECS instance on which the file system is mounted must reside in the same region.

2. Create a mount target of the VPC type. For more information, see #unique_19/unique_19_Connect_42_section_6xi_a3u_zkq.
Step 3: Deploy an NGINX proxy server

1. Use the following command to install NGINX.

   ```bash
   sudo yum install nginx
   ```

2. Use the following command to install an NFS client.

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

3. Use the following command to mount a file system on a directory of the NGINX website.

   ```bash
   sudo mount -t nfs -o vers=4.0,file-system-id.region.nas.aliyuncs.com:/ /usr/share/nginx/html/
   ```

   In the preceding command, file-system-id.region.nas.aliyuncs.com:/ specifies the domain name of the mount point. You need to replace the domain name based on your business requirements.

4. Edit the NGINX root file.

   ```bash
   echo "This is Testing for Nginx&NAS" > /usr/share/nginx/html/index.html
   ```

5. Repeat the preceding steps to configure the other three NGINX proxy servers and mount the same NFS file system on each proxy server.

6. Verify the configuration result.

   A successful configuration of proxy servers is indicated if each NGINX proxy server can access the index.html root file.

   ![www.test.com](image.png)

   This is Testing for Nginx&NAS
3 Application server shared storage

3.1 Access an NFS file system from a Windows ECS instance

This topic describes how to mount an SMB file system on an Elastic Compute Service (ECS) instance running Linux and perform read/write operations on the file system.

Prerequisites

Before mounting an NFS file system, you must complete the following prerequisites.

1. Apsara File Storage NAS is activated.
   
   When you log on to the Apsara File Storage NAS console for the first time, follow the provided instructions to activate the Apsara File Storage NAS service.

2. A Virtual Private Cloud (VPC) is available in the region where you want to create a file system.
   
   If no VPC is available, we recommend that you create a VPC. For more information, see Create a VPC and VSwitch.

3. An ECS instance is available in the region where you want to create a file system. You must also check whether the ECS instance is attached to the VPC.
   
   If no ECS instance is available, we recommend that you purchase an ECS instance. For more information, see #unique_21.

4. A file system is created.
   
   If no file system is available, we recommend that you create a file system. For more information, see #unique_18/unique_18_Connect_42_section_5jjo_0kj_jn5.

5. A mount target of the VPC type is created for the file system.
   
   If no mount target is available, we recommend that you create a mount target. For more information, see #unique_19/unique_19_Connect_42_section_6xi_a3u_zkq.

Context

If you want to use a distributed file system and allow access to shared storage from multiple ECS instances, we recommend that you use Apsara File Storage NAS.

The topic describes how to mount an NFS file system on a Windows ECS instance that resides in a VPC.
Mount a file system

1. Install an NFS client.
   a) Start **Server Manager**.
   b) Choose **Manage > Add Roles and Features**.
   c) Follow the provided instructions in the **Add Roles and Features Wizard** to install an NFS client.
      - In the **Server Roles** step, choose **File and Storage Services > File and iSCSI Services** and select **Server for NFS**.
      - In the **Features** step, select **Client for NFS**.
   d) Restart the ECS instance.
   e) Start the **command prompt** and run the mount command.

   An NFS client is installed if a result that is similar to the following example is displayed.

   ![Mount command example](image.png)

2. Use the following command to mount the Apsara File Storage NAS file system.

   ```bash
   mount -o nolock -o mtype=hard -o timeout=60 \035XXXXXXX3.cn-hangzhou.nas.aliyuncs.com\! h:
   
   035XXXXXXX3.cn-hangzhou.nas.aliyuncs.com\ specifies the domain name of the new mount target.
   ```
3. Use the mount command to verify the mount result.

After the mount is complete, the result shows that the value of mount is hard, the value of locking is no, and the value of timeout is greater than or equal to 10. Otherwise, the mount has failed.

4. In the **Computer** window, you can view the new shared file system.

You can check whether you can manage the new shared file system by creating files and folders in the file system.
Possible issues

If a message showing "file handle error" is displayed during operations, you need to check the following registry keys.

**Note:**
If you cannot find the **Locking**, **AnonymousGID**, and **AnonymousUID** registry keys, you need to follow the format required by the Windows registry to create these keys.

Choose **HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > ClientForNFS > CurrentVersion > Users > Default > Mount**, create a key named **Locking**, and set the value of this key to 1.

Create the following registry keys to configure the GID and UID.

1. Navigate to the **Default** path as follows: **HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > ClientForNFS > CurrentVersion > Default**.
2. Right-click a blank area on the right side of the Registry Editor window, choose **New > DWORD (32-bit) Value**, and create the following registry keys.

- **AnonymousGID**. Set the value of the key to 0.
- **AnonymousUID**. Set the value of the key to 0.

3. Restart the instance.

4. Run the following command to mount a NAS file system.

   ```
   mount -o nolock -o mtype=hard -o timeout=60 \035XXXXXXX3.cn-hangzhou.nas.aliyuncs.com\! h:
   ```

   \035XXXXXXX3.cn-hangzhou.nas.aliyuncs.com\ specifies the domain name of the new mount target.

5. Run the `mount` command to check the UID and GID.

   After the mount is complete, the result shows that the value of mount is hard, the value of locking is no, and the value of timeout is greater than or equal to 10. Otherwise, the mount has failed.

   ```
   C:\Users\Administrator>mount
   Local    Remote        Properties
   mnt:  \035XXXXXXX3.cn-hangzhou.nas.aliyuncs.com\!
   ```
3.2 Use Windows Server Backup to back up data from an ECS instance to Apsara File Storage NAS

This topic describes how to back up data from a Windows ECS instance to Apsara File Storage NAS. You can use a Windows built-in tool named Windows Server Backup to back up data from disks to Apsara File Storage NAS.

Prerequisites

An SMB file system is created and mounted on a Windows ECS instance. For more information, see Quick Start.

Note:

Only the Windows Server 2008 operating system is supported.

Context

With Windows Server Backup, you can perform a full backup to back up all data at a time. You can also schedule backup tasks to run automatically at regular intervals. You can restore data from these backups at any time.

Apsara File Storage NAS helps you achieve compute-storage separation. You can store temporary data for computing tasks and dynamic memory on ECS instances and store permanent data on Apsara File Storage NAS. If no response is returned from one ECS instance, you can switch to another ECS instance to access data stored on Apsara File Storage NAS. Apsara File Storage NAS allows multiple ECS instances to access a file system.

You can manually synchronize data stored on an ECS instance to Apsara File Storage NAS or schedule synchronization plans on a regular basis. This helps you preserve data and restore data in the event of data loss. Each disk snapshot is a copy of an entire disk. However, Apsara File Storage NAS is more flexible for data storage. Instead of backing up an entire disk, you can back up one or more directories at a time.

Windows Server Backup is a Windows built-in tool for data backup and restoration. With the tool, you can back up or restore a file, a directory, or an entire disk. For more information, see Overview of Windows Server Backup. With Windows Server Backup, you can back up an entire server (all volumes), selected volumes, the system state, specific files and folders, or devices. These devices include disks, tape libraries, and remote shared folders. You can also restore data from these devices based on your business requirements.
Install Windows Server Backup

Perform the following steps to install and start Windows Server Backup on a Windows ECS instance.

1. Open the Server Manager.
2. Choose Server Manager > Features and click Add Features.
4. Click Install to install Windows Server Backup.
5. After the installation is complete, choose Start > Administrative Tools and click Windows Server Backup to start the service.

Manual backup task

In Windows Server Backup, you can select the Backup Once option to back up the required data to Apsara File Storage NAS. The data includes the copy of an entire disk or specific folders.

1. In the Windows Server Backup window, click Backup Once to open the Backup Once Wizard dialog box.
2. In the Backup Options step, configure the required settings and click Next.
3. In the **Select Backup Configuration** step, select items to back up and click **Next**.

   You can select **Full Server** to back up the entire server. You can also select **Custom** to back up specific folders.

4. In the **Select Items for Backup** step, click **Add Items** to configure the required settings.

   If you select **Custom** in Step 3, you need to configure the required settings in the **Select Items for Backup** step.

   a) Click **Add Items**, select folders to back up, and click **OK**.

   b) Click **Advanced Settings** to configure settings, such as the backup type and files to skip during backup. Then click **OK**.

5. In the **Specify Destination Type** step, select **Remote shared folder**, and click **Next**.

6. In the **Specify Remote Folder** step, specify the location of a remote folder, and click **Next**.

   In the **Location** field, you must specify a directory that resides in an Apsara File Storage NAS file system, for example, `\file-system-id.region.nas.aliyuncs.com\myshare\backup`.

7. Click **Backup** to start a backup task.

   After the backup task is complete, you can view the backup data in the backup directory of the Apsara File Storage NAS file system.

---

**Scheduled backup task**

You can create backup schedule tasks to enable automatic backup.

1. In the **Windows Server Backup** window, click **Backup Schedule** to open the **Backup Schedule Wizard** dialog box.

2. In the **Getting Started** step, click **Next**.
3. In the **Select Backup Configuration** step, select items to back up and click **Next**.

You can select **Full Server** to back up the entire server. You can also select **Custom** to back up specific folders.

4. In the **Select Items for Backup** step, click **Add Items** to configure the required settings.

If you select **Custom** in Step 3, you need to configure the required settings in the **Select Items for Backup** step.

   a) Click **Add Items**, select folders to back up, and click **OK**.

   b) Click **Advanced Settings** to configure settings, such as the backup type and files to skip during backup, and click **OK**.

5. In the **Specify Backup Time** step, configure the backup interval and backup time, and click **Next**.

6. In the **Specify Destination Type** step, select **Back up to a shared network folder**, and click **Next**.

   **Note:**
   When you store the scheduled backups in a remote folder, the latest backup will overwrite all of the previous backups.

7. In the **Specify Remote Shared Folder** step, specify the location of a remote folder and click **Next**.

In the **Location** field, you must specify a directory that resides in an Apsara File Storage NAS file system, for example, `\file-system-id.region.nas.aliyuncs.com\myshare \backup`. 
8. Click **Finish** to start a scheduled backup task.

   The scheduled backup task automatically runs at the specified time. After the backup task is complete, you can view the backup data in the backup directory of the Apsara File Storage NAS file system.

**Restore data**

If your file is deleted or overwritten, you can restore data from a backup that is stored in an Apsara File Storage NAS file system.

1. In the **Windows Server Backup** window, click **Recover** to open the **Recovery Wizard** dialog box.

2. In the **Getting Started** step, select **A backup stored in another location** and click **Next**.

3. In the **Specify Location Type** step, select **Remote shared folder** and click **Next**.

4. In the **Specify Remote Folder** step, specify the location of a remote folder and click **Next**.

   In the **Location** field, you must specify a directory where a backup is stored in an Apsara File Storage NAS file system, for example, `\file-system-id.region.nas.aliyuncs.com\myshare\backup`.

5. In the **Select Backup Date** step, select the date of a backup to be restored and click **Next**.

6. In the **Select Recovery Type** step, select **Files and folders** and click **Next**.

7. In the **Select Items to Recover** step, select items to restore, such as files and folders, and click **Next**.

8. In the **Specify Recovery Options** step, specify the location of a directory to which you want to restore data and click **Next**.

9. Click **Recover** to restore data.
4 Access a file system remotely

4.1 Access an Apsara File Storage NAS file system from a local data center by using VPN Gateway

This topic describes how to access an Apsara File Storage NAS file system from a local data center by configuring a VPN gateway.

Context

You can only mount a file system on an ECS instance that resides in the same region as the file system. For example, an NFS or SMB file system that you create in China (Hangzhou) can only be mounted on an ECS instance that resides in China (Hangzhou). You cannot mount a file system that resides in China (Hangzhou) on a local data center or on an ECS instance that resides in a different region such as China (Qingdao). To resolve these issues, you can establish a connection over an Express Connect circuit. To enable a file system mount on a local data center, you can establish the connection between the data center and the Virtual Private Cloud (VPC) where the file system resides. To enable a cross-region file system mount, you can establish the connection between the VPC where the ECS instance resides and the VPC where the file system resides. However, high costs incur for establishing the connection.

Instead, we recommend that you use VPN Gateway to enable communication between a local data center and a VPC or between VPCs that reside in different regions. With VPN Gateway, you can mount a file system on the following target instances:

• A server that resides in a local data center
• An ECS instance that resides in a different region different from the region of the file system

If you have created a VPN gateway on an ECS instance in one VPC, you need to create another VPN gateway in the other VPC. Then, you need to establish a connection between the two VPN gateways. For more information about detailed operations, see Enable a cross-region mount (one VPN gateway available). If no VPN gateway exists in your environment, we recommend that you create VPN gateways in the two VPCs and connect the gateways. For more information about detailed operations, see Enable a cross-region mount (no VPN gateway available).
The following figure shows the topology that is adopted when VPN gateways are used.

![Topology Diagram]

The advantages and disadvantages are listed as follows:

- **Advantages**
  - Fixes all connectivity issues.
  - Provides secure access by using IPsec to encrypt data in transit.
  - Compared with Express Connect, VPN Gateway helps you reduce a large number of costs.

- **Disadvantages**
  The Internet bandwidth and latency between a local data center and a VPC or between VPCs restrict I/O performance of a file system over a VPN connection.

**Mount a file system on a server that resides in a local data center**

1. Create a file system and mount target.
   a) Log on to the Apsara File Storage NAS console.
   b) Create a file system. For more information, see #unique_18/unique_18_Connect_42_section_5jo_0kj_jn5.
   c) Create a mount target of the VPC type. For more information, see #unique_19/unique_19_Connect_42_section_6xi_a3u_zkq.
2. Create a connection between the VPC and your local data center. For more information, see #unique_23.
3. Verify the connection between a server that resides in the local data center and an ECS instance or a mount target that resides in the VPC.

Log on to an ECS instance that does not have an Internet IP address. On the ECS instance, use the `ping` command to `ping` the internal IP address of a server that resides in the local data center and verify the connection.

4. After you confirm the connection by using the ping command, you can mount a file system that resides in the VPC on a server that resides in the local data center. For more information, see `Mount a file system`.

Enable a cross-region mount (one VPN gateway available)

The following example shows a practical scenario of two VPCs named VPC 1 and VPC 2 that reside in different regions.

1. Create a file system and mount target.
   a) Log on to the Apsara File Storage NAS console.
   b) Create a file system. For more information, see `unique_18/unique_18_Connect_42_section_5jo_0kj_jn5`.
   c) Create a mount target of the VPC type. For more information, see `unique_19/unique_19_Connect_42_section_6xi_a3u_zkq`.

   Create a mount target in VPC 1.

2. In VPC 2, create a VPN gateway on an ECS instance as a customer gateway.

   Note:
   - You must specify an Internet IP address for the ECS instance to connect to the VPN gateway that resides in VPC 1.
   - For more information about how to create a VPN gateway on an ECS instance, see tutorials such as `Using StrongSwan for IPsec VPN on CentOS 7`.

3. Establish a connection between VPN gateways that reside in VPC 1 and VPC 2, respectively.
   a) Log on to the VPC console.
   b) Create a VPN connection to enable communication between VPN gateways that resides in VPC 1 and VPC 2, which you created in Step 2. For more information, see `Create an IPsec connection`.  


4. Configure static routes on other ECS instances that reside in VPC 2. For more information, see Configure routes on a VPN gateway. The required settings are described as follows.

**Destination CIDR Block** specifies the private classless inter-domain routing (CIDR) Block of VPC 1. **Next Hop** specifies the customer gateway that resides in VPC 2.

5. Verify the connection between VPC 1 and an ECS instance (or mount target) that resides in VPC 2.

Log on to an ECS instance that resides in VPC 1, use the **ping** command to ping the IP address of an ECS instance that resides in VPC 2, and verify the connection.

6. After you confirm the connection by using the ping command, you can mount a file system that resides in VPC 1 on an ECS instance that resides in VPC 2. For more information, see Mount a file system.

**Enable a cross-region mount (no VPN gateway available)**

The following example shows a practical scenario of two VPCs named VPC 1 and VPC 2 that reside in different regions.

1. Create a file system and mount target.

   a) Log on to the Apsara File Storage NAS console.

   b) Create a file system. For more information, see #unique_18/unique_18_Connect_42_section_5jo_0kj_in5.

   c) Create a mount target of the VPC type. For more information, see #unique_19/unique_19_Connect_42_section_6xi_a3u_zkq.

Create a mount target in VPC 1.
2. Establish a connection between VPN gateways that reside in VPC 1 and VPC 2, respectively.
   a) Log on to the VPC console.
   b) Create VPN gateways in VPC 1 and VPC 2, respectively. For more information, see Create a VPN gateway.
   c) Create customer gateways in VPC 1 and VPC 2, respectively. For more information, see Create a customer gateway. The required settings are described as follows.
      - **IP Address** specifies an IP address for the VPN gateway that resides in VPC 1 and a different IP address for the VPN gateway that resides in VPC 2.
   d) Configure routes for VPN gateways that reside in VPC 1 and VPC 2, respectively. For more information, see Configure routes for a VPN gateway.
      - The following information is important when you configure routes for the VPN gateway that resides in VPC 1. **Destination CIDR Block** specifies the private CIDR block for VPC 2. **Next Hop** specifies the name of the customer gateway that resides in VPC 1.
      - The following information is important when you configure routes for the VPN gateway that resides in VPC 2. **Destination CIDR Block** specifies the private CIDR block for VPC 1. **Next Hop** specifies the name of the customer gateway that resides in VPC 2.

3. Verify the connection between VPC 1 and an ECS instance (or mount target) that resides in VPC 2.
   Log on to an ECS instance that resides in VPC 1, use the ping command to ping the IP address of an ECS instance that resides in VPC 2, and verify the connection.

4. After you confirm the connection by using the ping command, you can mount a file system that resides in VPC 1 on an ECS instance that resides in VPC 2. For more information, see Mount a file system.

4.2 Access an Apsara File Storage NAS file system from a local IDC by using NAT Gateway

This topic describes how to access an Apsara File Storage NAS file system from a local IDC by using an NAT gateway.

**Context**
You can directly mount a file system only on an ECS instance that resides in the same region as the file system. For example, an NFS or SMB file system that you create in China (Hangzhou) can only be mounted on an ECS instance that resides in China (Hangzhou). You cannot directly mount the file system on an ECS instance that resides in a different region such as China (Qingdao) or on a local server. To enable such a mount, you can use Express Connect to establish a connection. For a mount on a local server, you can establish a connection between the local IDC and the Virtual Private Cloud (VPC) where the file system resides. For a cross-region mount, you can establish a connection between the VPC where the ECS instance resides and the VPC where the file system resides. However, high costs incur for establishing the connection.

If you have deployed a VPN gateway in your local IDC, we recommend that you use Alibaba Cloud VPN Gateway to connect your local IDC to Apsara File Storage NAS. For more information, see Access an Apsara File Storage NAS file system from a local data center by using VPN Gateway.

If you only need to upload a small amount of data from your local IDC to Apsara File Storage NAS, we recommend that you use NAT Gateway to establish a connection.

The following figure shows the network topology that is adopted when NAT Gateway is used to establish a connection between a local IDC and Apsara File Storage NAS.

- Advantage: easy to configure
Network Attached Storage

Best Practices / 4 Access a file system remotely

- Disadvantage:
  - In terms of security, any user who has an Elastic IP address (EIP) can create a mount target that relates to the EIP because connections are established between EIPs and VPCs.
  - Each combination of an EIP and port applies only to a mount target. If you want to create multiple mount targets, you must create multiple EIPs.

Create a file system and a mount target

1. Log on to the Apsara File Storage NAS console.
2. Create a file system. For more information, see #unique_18/unique_18_Connect_42_section_5jo_0kj_jn5.
3. Create a mount target in a VPC. For more information, see #unique_19/unique_19_Connect_42_section_6xi_a3u_zkq.

Configure an NAT gateway

You can follow these steps to mount an Apsara File Storage NAS file system on a Windows or Linux local host that is connected to the Internet. After the file system is mounted, you can use your local host to upload files to or download files from the file system.

1. Log on to the VPC console.
2. Create an NAT gateway. For more information, see #unique_25.

- Note:
  You must select the VPC where the Apsara File Storage NAS file system resides.
3. Attach an EIP to the NAT gateway. For more information, see #unique_26.
4. Create a destination network address translation (DNAT) entry. For more information, see #unique_27.

The required settings are described as follows:

- **Public IP Address**: specifies the public IP address that is generated when you create an EIP.
- **Private IP Address**: specifies the IP address of the mount target for the file system.

You can use an ECS instance to ping the endpoint of the mount target to retrieve the IP address.

```bash
ping file-system-id.region.nas.aliyuncs.com
```

- **Port**: We recommend that you select **All Ports**. You can also select a port for your NFS or SMB file system.

5. Mount the file system on your local host.

**Note:**

- To mount an NFS file system, you must first install an NFS client. For more information, see #unique_28/unique_28_Connect_42_section_kvj_d02_szj.
- Before mounting an SMB file system, you must enable Workstation and TCP/IP NetBIOS Helper services. For more information, see #unique_29/unique_29_Connect_42_section_zlq_3j1_dfb.
- Run the following command to mount an NFS file system.

```bash
mount -t nfs4 10.10.10.1:/ /mnt
```

- 10.10.10.1 is the public IP address generated when you create an EIP. Replace the IP address as needed.
- /mnt is the mount directory. Replace the directory as needed.
- Run the following command to mount an SMB file system.

```bash
net use D: \\10.10.10.1\myshare
```

- D: is the target drive letter on which you need to mount a file system. Replace the drive letter as needed.
- 10.10.10.1 is the public IP address generated when you create an EIP. Replace the IP address as needed.
- myshare is the name of the shared SMB directory. You cannot change the name.
6. Verify the mount result.

- **NFS file system**

  The mount is successful if the following result is displayed after you run the `mount` command. You can read data from and write data to the files of the NFS file system.

- **SMB file system**

  The mount is successful if you can access the SMB file system from your local Windows Explorer. You can read data from and write data to the files of the SMB file system.

---

**Differences between the NAT Gateway solution and the VPN Gateway solution**

The following table illustrates the differences between the two solutions.

<table>
<thead>
<tr>
<th>Item</th>
<th>NAT Gateway</th>
<th>VPN Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Easy: You can configure all settings in the Alibaba Cloud console.</td>
<td>Complex: You must configure a VPN gateway in the Alibaba Cloud console and configure a client-side VPN gateway in a local IDC.</td>
</tr>
<tr>
<td>Security</td>
<td>Poor</td>
<td>Excellent</td>
</tr>
<tr>
<td>Flexibility</td>
<td>Restricted: Each EIP can only map one mount target.</td>
<td>You can access all Apsara File Storage NAS mount targets without the need of EIPs.</td>
</tr>
<tr>
<td>Scenarios</td>
<td>Establish temporary connections to transfer a small amount of data.</td>
<td>Establish a long-term connection that is required between a local IDC and Apsara File Storage NAS.</td>
</tr>
</tbody>
</table>
4.3 Use SFTP to transfer data to and from an Apsara File Storage NAS file system

This topic describes how to use the Secure File Transfer Protocol (SFTP) to transfer data to and from an Apsara File Storage NAS file system.

Prerequisites

In a region where an Apsara File Storage NAS file system resides, you have purchased an Elastic Compute Service (ECS) instance. The following takes CentOS as an example. For more information, see #unique_21.

Context

The transmission speed for SFTP is based on the Internet bandwidth of an ECS instance that runs the SFTP service. We recommend that you configure a suitable Internet bandwidth based on your business requirements.

Procedure

1. Log on to the ECS console.
2. Modify the /etc/ssh/sshd_config configuration file.
   a) In the sshd_config configuration file, annotate the line that starts with Subsystem, create a line, and add Subsystem sftp internal-sftp to the line.

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

   b) Add the following code at the end of the sshd_config configuration file.

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

3. Grant permissions.

   a) Use the following command to create a group named sftp.

      ```bash
      groupadd sftp
      ```

   b) Use the following command create a user account named sftp and add the user account to the new group.

      ```bash
      useradd -g sftp -s /sbin/nologin -M sftp
      ```

   c) Use the following command to specify a password for the sftp user account.

      ```bash
      passwd sftp
      ```

   d) Use the following commands to create a workspace for the user account, change the owner to root, change the owner group to sftp, and change the access permissions for the sftp directory to 755.

      ```bash
      cd /usr
      mkdir sftp
      chown root:sftp sftp
      chmod 755 sftp
      ```

4. In the sftp directory, create a mount directory named file for the Apsara File Storage NAS file system.

   ```bash
   cd sftp/
   mkdir file
   chown sftp:sftp file
   ```

5. Use the following command to mount the Apsara File Storage NAS file system on the /usr/sftp/file directory.

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

6. Use the following command to restart the sshd service.

   ```bash
   service sshd restart
   ```

7. Log on to the SFTP service to transfer files.
Enter the username and password that you have specified in Step 3. The following takes WinSCP client as an example. You can connect to the SFTP service by using a client that supports SFTP based on your business requirements.
5 Access an SMB file system from a Linux ECS instance

This topic describes how to mount an SMB file system on a Linux ECS instance and perform read/write operations on the file system.

Prerequisites

- At least one ECS instance is available in the region where you need to create a file system.

SMB file systems provide native support for the following Linux distribution versions. In this topic, unless otherwise specified, any Linux distribution mentioned refers to one of these versions:

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

Note:

If you use an unsupported version of Linux, errors may occur in the SMB module of the Linux kernel due to internal defects. In this case, Alibaba Cloud cannot ensure the reliability of SMB file systems.

- Networking

- The Linux ECS instance on which you need to mount an SMB file system resides in the same network (such as the same VPC) as that of the SMB file system.
- The Linux ECS instance is in the whitelist of the SMB file system so that the instance is authorized to access the SMB file system.
- The port 445 is open for the SMB client to establish TCP connections.

If the port 445 is not open, we recommend that you add rules to a security group of the ECS instance for the port. For more information, see #unique_30.
• An SMB file system is created. For more information, see #unique_18/unique_18_Connect_42_section_5/jo_0kj_jn5.
• A mount target is added for the file system. For more information, see #unique_19/unique_19_Connect_42_section_6xi_a3u_zkq.

• Software requirements

The SMB kernel module is pre-installed on each supported Linux distribution. In addition, you must install the cifs-utils package.

- If you are using Ubuntu or Debian, you can use the apt-get package management utility to install the cifs-utils package.

```bash
sudo apt-get update
dsudo apt-get install cifs-utils
```

- If you are using RHEL, CentOS, or Aliyun Linux, you can use the yum package management utility to install the cifs-utils package.

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

- If you are using OpenSUSE or SLES12-SP2, you can use the zypper or yast tool to install the cifs-utils package.

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

Run the `sudo yast2` command, choose Software > Software Management, and then install the cifs-utils package.

- If you are using a supported CoreOS distribution, perform the following steps to install the cifs-utils package:

  1. Configure SELinux settings.

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

  2. Compile and install the cifs-utils package on CoreOS.

     You can use the following command to run a Fedora-based Docker container to compile and install the cifs-utils package. You can also download the cifs-utils package from Alibaba Cloud and copy the package to the /tmp or /bin folder.

     ```bash
     $ 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-
     ```
Mount a file system

1. Log on to a Linux ECS instance by using the root account. You can also use a client administrator account that has been authorized with the sudo command.

2. Run the following command to mount the file system.

```
mount -t cifs //xxx-crf23.eu-west-1.nas.aliyuncs.com/myshare /mnt -o vers=2.0,guest ,uid=0,gid=0,dir_mode=0755,file_mode=0755,mfsymlinks,cache=strict,rsize=1048576, wsize=1048576
```

The syntax of a mount command: mount -t cifs //<The domain name of a mount target >/myshare <A mount directory> -o <Mount options>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File system type</td>
<td>For an SMB file system, you must specify -t cifs.</td>
</tr>
<tr>
<td>Domain name of a mount target</td>
<td>When you create a mount target for a file system, the domain name of the mount target is generated. You must replace the domain name based on your requirements. For more information about mount targets, see #unique_19.</td>
</tr>
<tr>
<td>myshare</td>
<td>The name of an SMB share. The name cannot be changed.</td>
</tr>
<tr>
<td>Mount directory</td>
<td>The target mount directory, such as /mnt/sharepath.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mount options</td>
<td>You can use the <code>-o</code> parameter to specify mount options.</td>
</tr>
<tr>
<td></td>
<td>• vers: required. Specifies the version of the SMB protocol. You can specify 2.0 for the option.</td>
</tr>
<tr>
<td></td>
<td>• guest: required. Specifies a user account that you use to mount the file system. You must use a guest user account that can be authenticated by NT LAN Manager (NTLM). You can specify one of the following statements for the option: username=guest, password=guest, or guest.</td>
</tr>
</tbody>
</table>

**Note:**

The NTLM, NTLMv2, and NTLMSSP protocols are applicable. By default, the SMB client negotiates an NTLM protocol with Apsara File Storage NAS to mount a file system. You can specify a protocol by setting the sec option to ntlm, ntlmv2, or ntlmssp.

- uid: optional. Specifies the user to which the files stored on the file system belong after a successful mount. The default value of uid is 0.
- gid: optional. Specifies the user group to which the files stored on the file system belong after a successful mount. The default value of gid is 0. The default value of gid is 0.
- dir_mode: optional. Specifies the permissions granted to the user on a directory. The permissions include read, write, and execute. The value must start with zero, such as 0755 and 0644. The default value of dir_mode is 0755.
- file_mode: optional. Specifies the permissions granted to the user on a file. The permissions include read, write, and execute. The value must start with zero, such as 0755 and 0644. The default value of file_mode is 0755.
- mfsymlinks: optional. Specifies whether symbol links are supported.
- cache: optional.
  - If the cache option is set to strict, caching is enabled for the SMB client. The cache option is set to strict by default.
  - If the cache option is set to none, caching is disabled for the SMB client.
- rsize: optional. Specifies the maximum number of bytes of data that the SMB client can read from the file system. The default value is 1048576.
- wsize: optional. Specifies the maximum number of bytes of data that the SMB client can write to the file system. The default value is 1048576.
- atime|relatime: optional. If your business is not sensitive to access time for files, we recommend that you do not use the atime option. The default option is relatime.
3. Use the mount -l command to view the mount result.

The following figure shows an example of a successful mount.

![Example of a successful mount](image)

4. After you mount a file system, you can perform read/write operations on the Apsara File Storage NAS file system from the ECS instance running Linux.

You can access the Apsara File Storage NAS file system in the same way you access a local directory. The following figure shows a code example.

```
[root@i7-5500u-421d6-9f16aZ ~]# mkdir /mnt/dir1
[root@i7-5500u-421d6-9f16aZ ~]# mkdir /mnt/dir2
[root@i7-5500u-421d6-9f16aZ ~]# touch /mnt/file1
[root@i7-5500u-421d6-9f16aZ ~]# echo 'some file content' > /mnt/file2
[root@i7-5500u-421d6-9f16aZ ~]# ls /mnt
dir1  dir2  file1  file2  tmp
```

**Scenarios**

You can specify different mount options for different scenarios. This section describes typical scenarios and corresponding mount options.

- **Shared access to a file system from multiple Linux ECS instances**

  Multiple Linux ECS instances share access to a file system and you have no access control requirements. You can use an authorized administrator account of each ECS instance to mount a file system on these ECS instances. An example mount command is as follows.

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

- **Shared access to a file system from multiple Linux ECS instances with access control**

  Multiple Linux ECS instances share access to a file system and you need to control access from users by using permissions. You can configure the uid, gid, dir_mode, and file_mode options in the mount command to manage permissions.
• Shared access to a file system from multiple Linux ECS instances that function as web servers

You can install web server applications such as Apache HTTP Server on multiple Linux ECS instances and use an SMB file system as shared file storage.

Note:

- SMB file systems allow shared access and ensure high scalability and availability. In some scenarios such as when you access a large number of small files on an SMB file system, the performance of the SMB file system may be slightly compromised. This occurs because the implementation scheme of SMB file systems is different from that of local disks. For web server scenarios, we recommend that you store shared files on an SMB file system and exclusive files on local disks to achieve high performance.
- Web server applications require high bandwidth for communication. Apsara File Storage NAS supports an acceleration feature for these applications. You can contact Alibaba Cloud Technical Support to enable the feature.

• Shared access to a file system from both Windows ECS instances and Linux ECS instances

Windows ECS instances and Linux ECS instances can share access to an SMB file system. In this scenario, you must set the cache option to strict or use the default value of this option in the mount command when mounting a file system on a Linux ECS instance.

For information about how to troubleshoot issues that you may encounter when mounting a file system, see #unique_31.