ALIBABA CLOUD

Alibaba Cloud

Apsara File Storage NAS
Best Practices

Document Version: 20210715

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

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

Table of Contents

1.Web service and content management

Apsara File Storage NAS can be used in various content management systems and web applications to provide efficient storage services for websites and applications. This topic lists the links to the best practices of web services.

- Use NGINX as a proxy for Apsara File Storage NAS
- Use Windows IIS to access Apsara File Storage NAS

2.Windows applications

This topic lists the links to the best practices of building Windows applications on Apsara File Storage NAS.

IIS service

- Use Windows IIS to access Apsara File Storage NAS

Access control

- Authenticate users and control access to files and directories in an SMB file system based on an Active Directory domain
- Join the mount target of an SMB file system to an AD domain
- Use an AD account to mount an SMB file system on a Windows client

Data access

- Upload data to and download data from an SMB file system

Windows tools

- Use Windows Server Backup to back up data from an ECS instance to Apsara File Storage NAS

3.High-performance website

3.1. Use Windows IIS to access Apsara File Storage NAS

Internet Information Service (IIS) can access data in Server Message Block (SMB) file systems in the same way as it accesses data in on-premises disks. IIS provides the web and FTP services to separate website storage from computing. This topic describes how to configure IIS to access a NAS file system.

Prerequisites

- An SMB file system is created and a mount target is created for the file system. For more information, see Manage file systems and Create a mount target.
- WinSCP is installed.

Context

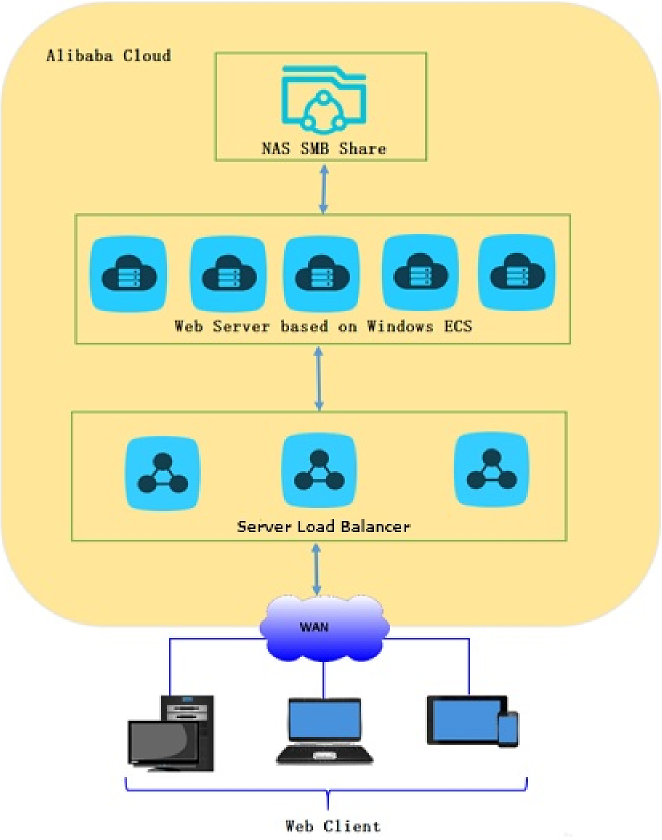
Windows server is a popular platform that is used to build websites. A large number of users build websites on Windows Elastic Compute Service (ECS) instances and store the content resources of the website on a reliable and high-throughput SMB file system. In addition, the computing and storage resources support auto scaling based on specific business requirements.

The FTP service provided by IIS includes a wide range of requirements. A large number of website administrators remotely manage website content by using the FTP service. Meanwhile, a large number of Alibaba Cloud users want to transfer and share files between WANs and Alibaba Cloud by using the FTP service on Windows ECS instances.

In this example, IIS 7.5 (Windows Server 2008 R2) is used to describe how to use NAS to provide both the web service and FTP service for a Windows ECS instance. You can also use Server Load Balancer (SLB) to build a multi-server website that provides error tolerance. For more information, see What is SLB?

Notice

- The topic provides some security suggestions, but they are not a complete security solution. You must devise your own plans to secure your web service and data. For example, you can safeguard your system security by setting up firewalls, configuring security groups for ECS instances, and installing operating system patches. You can also safeguard your service security by using the security services of Alibaba Cloud.
- In this topic, a normal user named iss_user is used. We recommend that you access data as this user instead of the system administrator when you deploy FTP services or run IIS web services on Windows Server 2016.

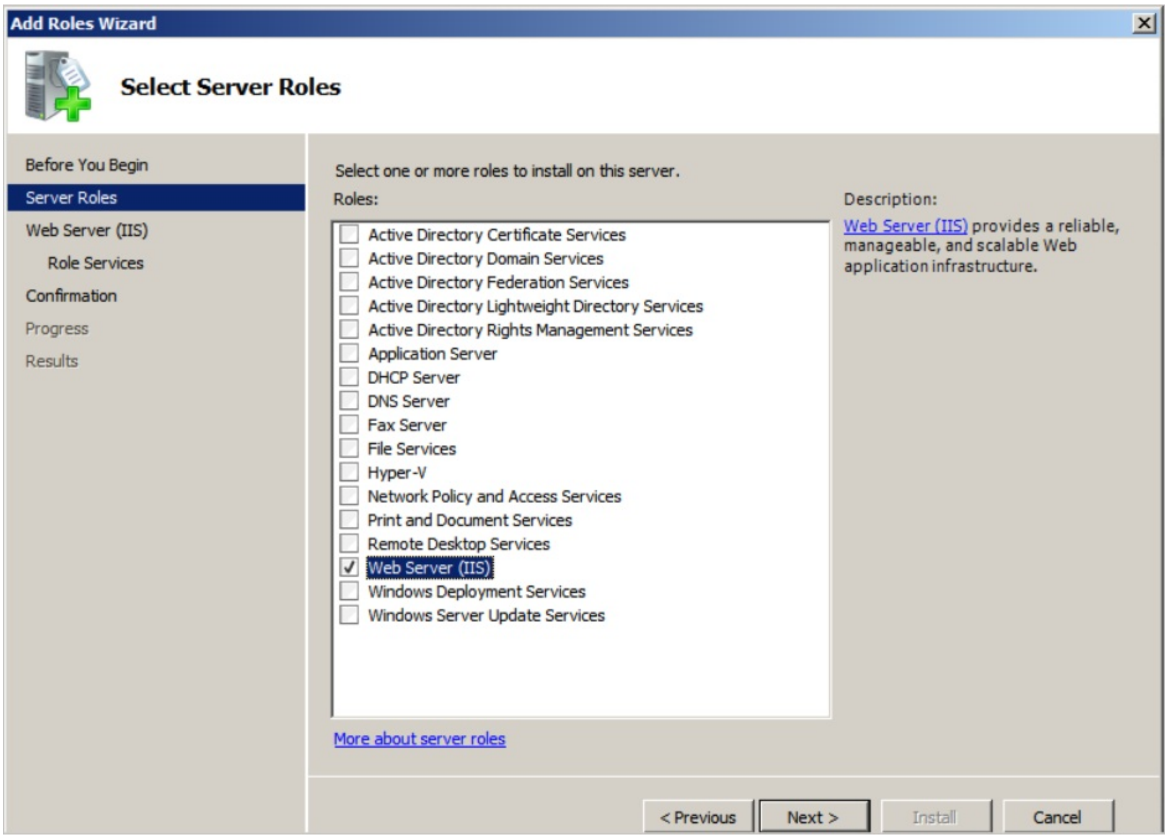


Install Windows IIS

In this example, Windows Server 2008 R2 is used to describe how to add an IIS role and install IIS by using Server Manager.

> **Note** For more information about how to install IIS on different Windows operating systems, see Install IIS and ASP.NET Modules.

1. In the Windows server, choose **Start > Administrative Tools > Server Manager**.
2. In the left-side navigation pane of the **Server Manager** dialog box, click **Roles** and then click **Add Roles**.
3. In the left-side navigation pane of the **Add Roles Wizard**, click **Server Roles** and select **Web Server (IIS)**.



Add Roles Wizard

Select Server Roles

Select one or more roles to install on this server.

Roles:

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Desktop Services
- ☑ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

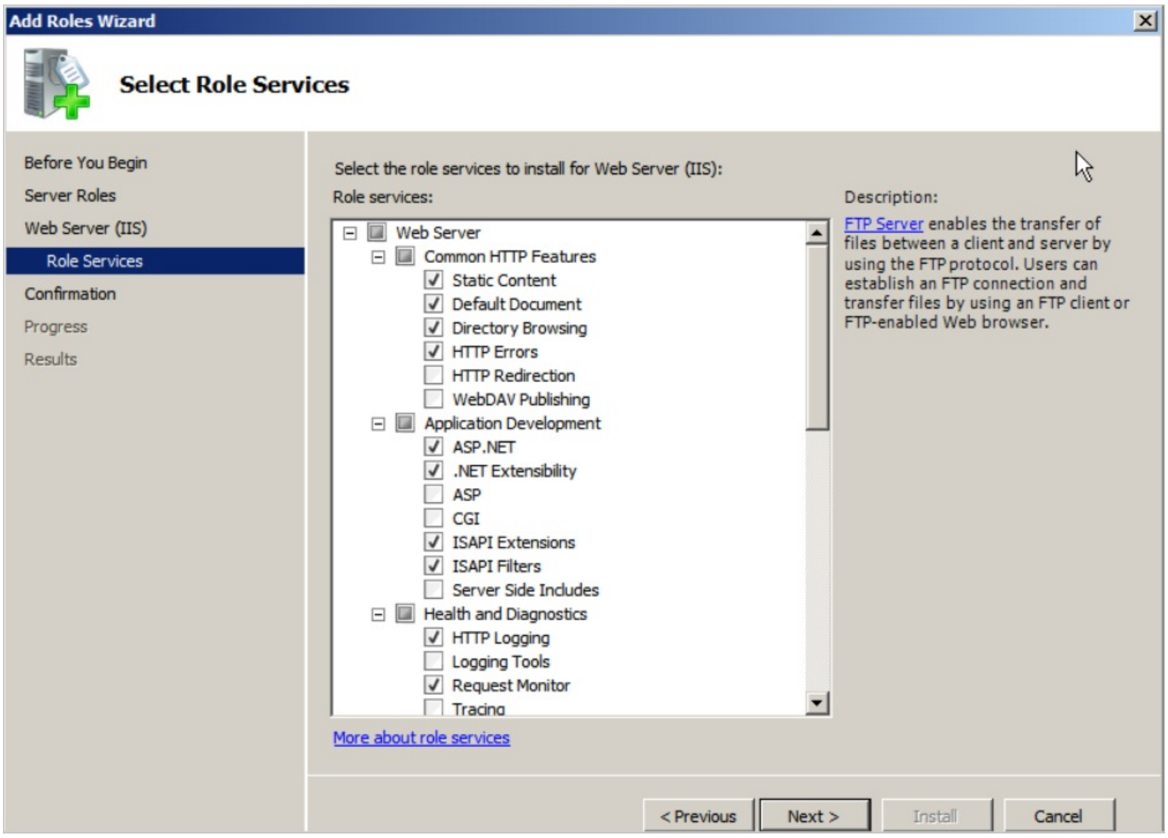
Description:

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

More about server roles

4. In the left-side navigation pane of the **Add Roles Wizard**, click **Role Services**, and select the role services that you want to install for the web server (IIS).

   In addition to the default services, you must also select **ASP** and **FTP Server** to enable FTP services and demonstrate dynamic web pages by using scripts.



Select Role Services

Select the role services to install for Web Server (IIS):

Role services:

- ▣ Web Server
  - ▣ Common HTTP Features
    - ☑ Static Content
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - □ HTTP Redirection
    - □ WebDAV Publishing
  - ▣ Application Development
    - ☑ ASP.NET
    - ☑ .NET Extensibility
    - □ ASP
    - □ CGI
    - ☑ ISAPI Extensions
    - ☑ ISAPI Filters
    - □ Server Side Includes
  - ▣ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Logging Tools
    - ☑ Request Monitor
    - □ Tracing

Description:

FTP Server enables the transfer of files between a client and server by using the FTP protocol. Users can establish an FTP connection and transfer files by using an FTP client or FTP-enabled Web browser.

More about role services

5. Click **Next** and complete the installation as prompted.

Access the SMB file system

You can store your web resources and configuration files in the shared directory (myshare by default) of the SMB file system. You can configure the permission group of the SMB file system to make sure that the web server can read data from and write data to the file system.

1. Open the File Explorer window and enter *\\xxxx-xxxx.cn-hangzhou.nas.aliyuncs.com\myshare* in the address bar to access the SMB file system. where:
   - *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.
2. Create a subdirectory named *www* in the *myshare* directory of the SMB file system to store web page files of your website.

   In this example, the static web page file index.html and the dynamic web page file test.asp are created in the *myshare\www* directory. The following sample code shows how to create the files:

   - Index.html

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

`Hello World!` is displayed in the static web page.

- Test.asp

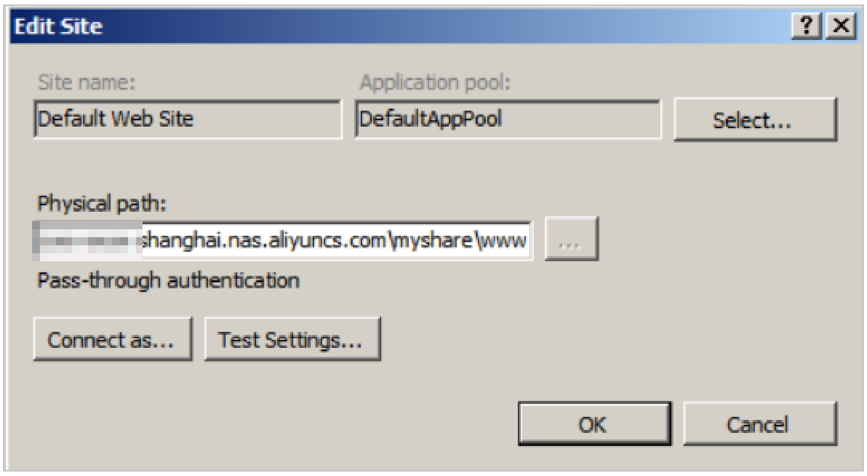
  ```
  <HTML>
   <BODY>
     This page was last refreshed on <%= Now() %>.
   </BODY>
  </HTML>
  ```

  The current system time is displayed on the dynamic web page.

Set up the Windows IIS web service

1. In the Windows server, choose **Start** > **Windows Operating System** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. In the left-side navigation pane, choose **View Sites** > **Default Web Site**, and click **Basic Settings**.
3. In the **Edit Site** dialog box, set **Physical path** and click **OK**.

   In the **Physical path** field, enter the storage path of web resources on 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.

   Edit Site

   Site name: Default Web Site

   Application pool: DefaultAppPool

   Physical path: [redacted]shanghai.nas.aliyuncs.com\myshare\www

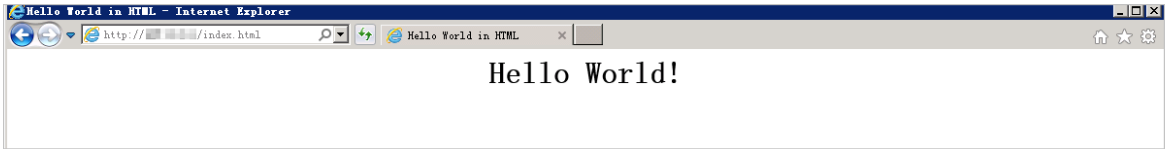
   Pass-through authentication

   Note

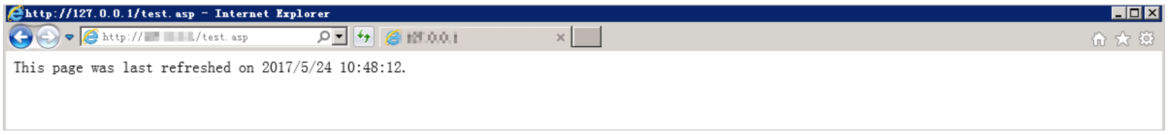
   - By default, you must use a user account and user group of IIS to access a network drive (for example, Z:\) mapped in the user session. You cannot directly access the mapped network drive as a Windows user. Otherwise, an access error may occur.
   - If you are using Windows Server 2016, you must perform other operations to integrate IIS with NAS after you set up the Windows IIS web service. For more information, see How can I integrate IIS with NAS?

4. Verify the setting.

Enter the local paths of the index.html and test.asp files in the address bar of your browser to open these files. If the following figures are displayed, IIS is running as expected. You can also configure security groups for your ECS instances and configure Windows Firewall to guarantee access security.


Hello World in HTML - Internet Explorer
http://[redacted]/index.html
Hello World in HTML

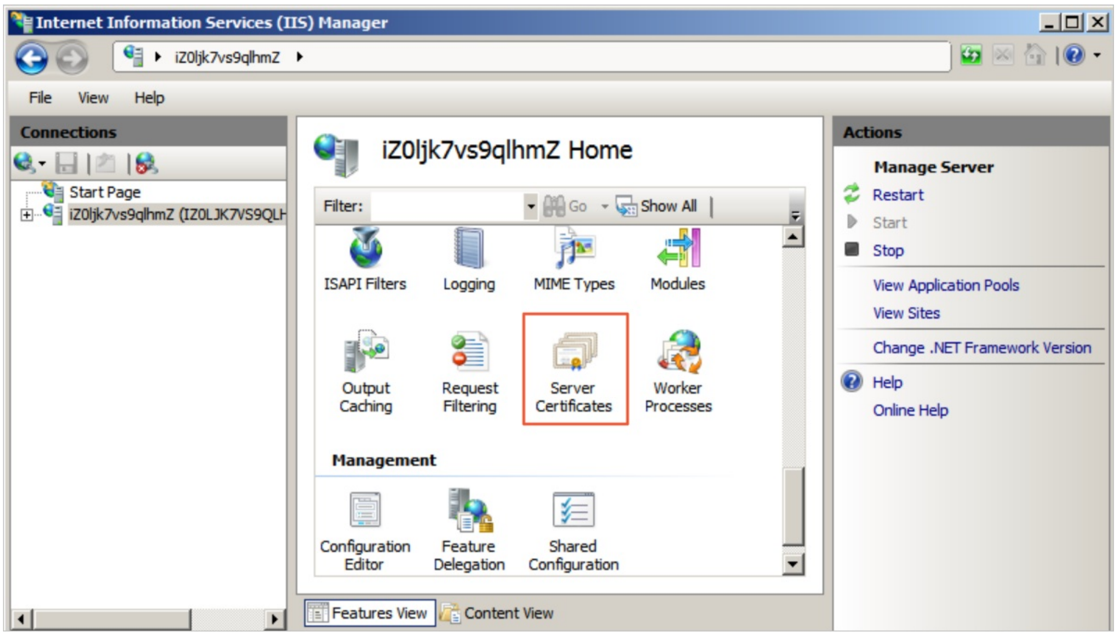
Hello World!


http://127.0.0.1/test.asp - Internet Explorer
http://[redacted]/test.asp
127.0.0.1

This page was last refreshed on 2017/5/24 10:48:12.

Set up the Windows IIS FTP service

1. In the Windows server, choose **Start** > **Windows Operating System** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. Install the SSL certificate.
   i. On the homepage, double-click **Server Certificates**.

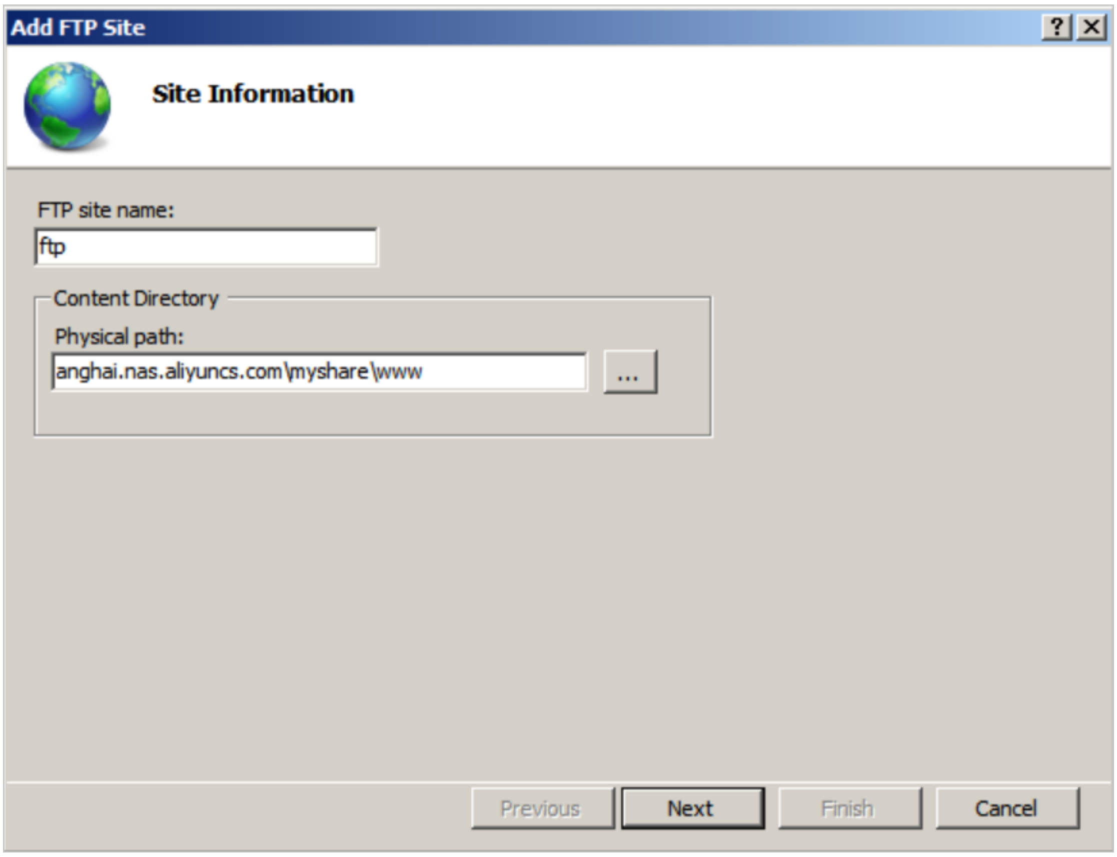


   ii. On the **Server Certificates** page, click **Create Self-Signed Certificate**.
   iii. Specify a name for the certificate, and click **OK**.
3. Set up an FTP site.
   i. In the left-side navigation pane, double-click **Sites**.
   ii. On the **Sites** page, click **Add FTP Site**.

iii. In the **Add FTP site** dialog box, set the relevant parameters and click **Next**.

In the **Physical path** field, enter the storage path of web resources on 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 in the *myshare* directory based on your business requirements. You can also set up multiple FTP sites that provide different ports to access different directories.



FTP site name: ftp

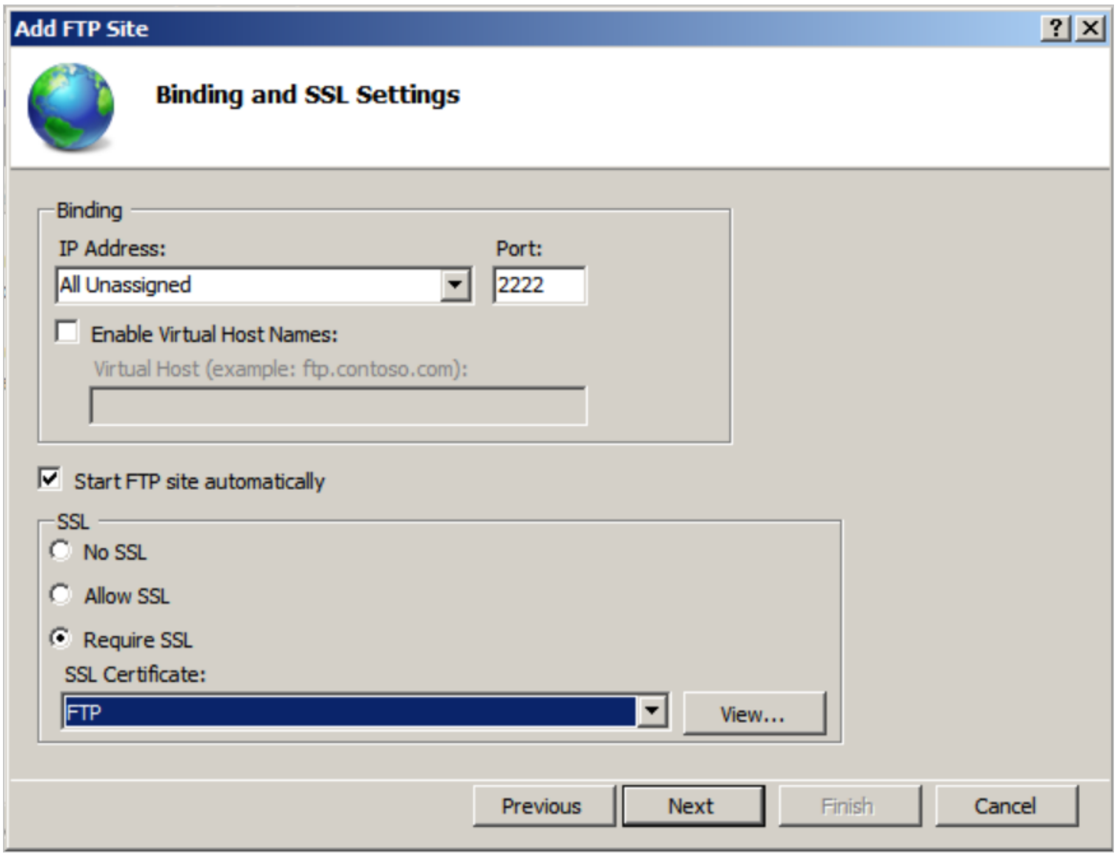
Content Directory

Physical path: anghai.nas.aliyuncs.com\myshare\www

iv. In the **Binding and SSL Settings** dialog box, set the relevant parameters and click **Next**.

Set the following parameters:

- **Port**: The default port number is 21. For security concerns, port 2222 is used.
- **SSL Certificate**: select the created SSL certificate.



Add FTP Site

Binding and SSL Settings

Binding

IP Address: All Unassigned

Port: 2222

□ Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

☑ Start FTP site automatically

SSL

○ No SSL

○ Allow SSL

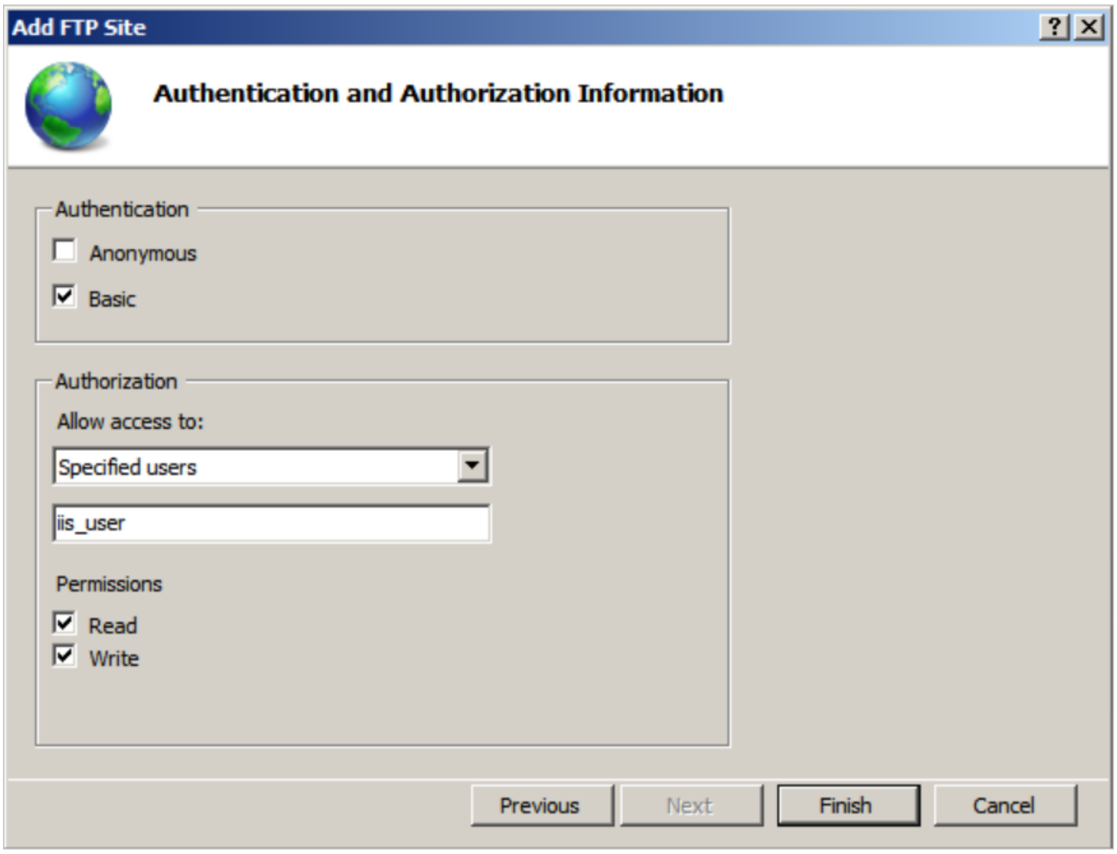
● Require SSL

SSL Certificate: FTP

v. Configure the authentication and authorization information, and click **Finish**.

Set the following parameters:

- **Authentication**: Select **Basic**.
- **Authorization**: Select a user who is allowed to access NAS. In this example, iis_user is used.
- **Permissions**: Grant read and write permissions to the user.



Authentication

□ Anonymous

☑ Basic

Authorization

Allow access to:

Specified users

iis_user

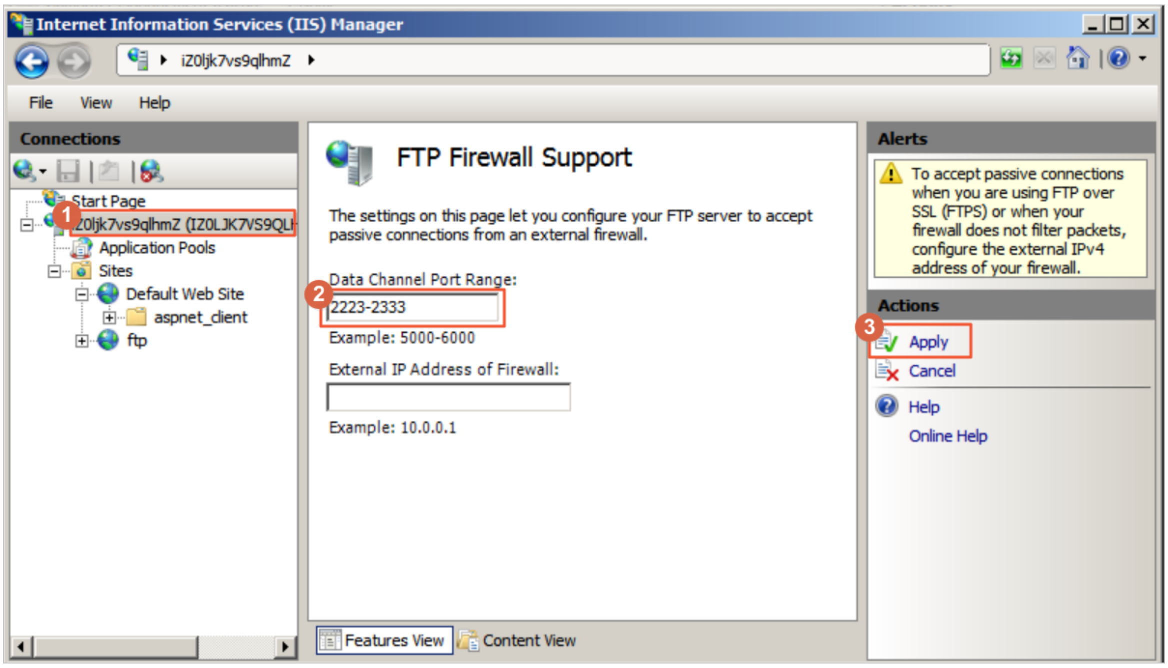
Permissions

☑ Read

☑ Write

4. Set up the FTP firewall.

On the homepage, double-click **FTP Firewall Support** dialog box, specify **Data Channel Port Range**, and then click **Apply**.



FTP Firewall Support

The settings on this page let you configure your FTP server to accept passive connections from an external firewall.

Data Channel Port Range: 2223-2333

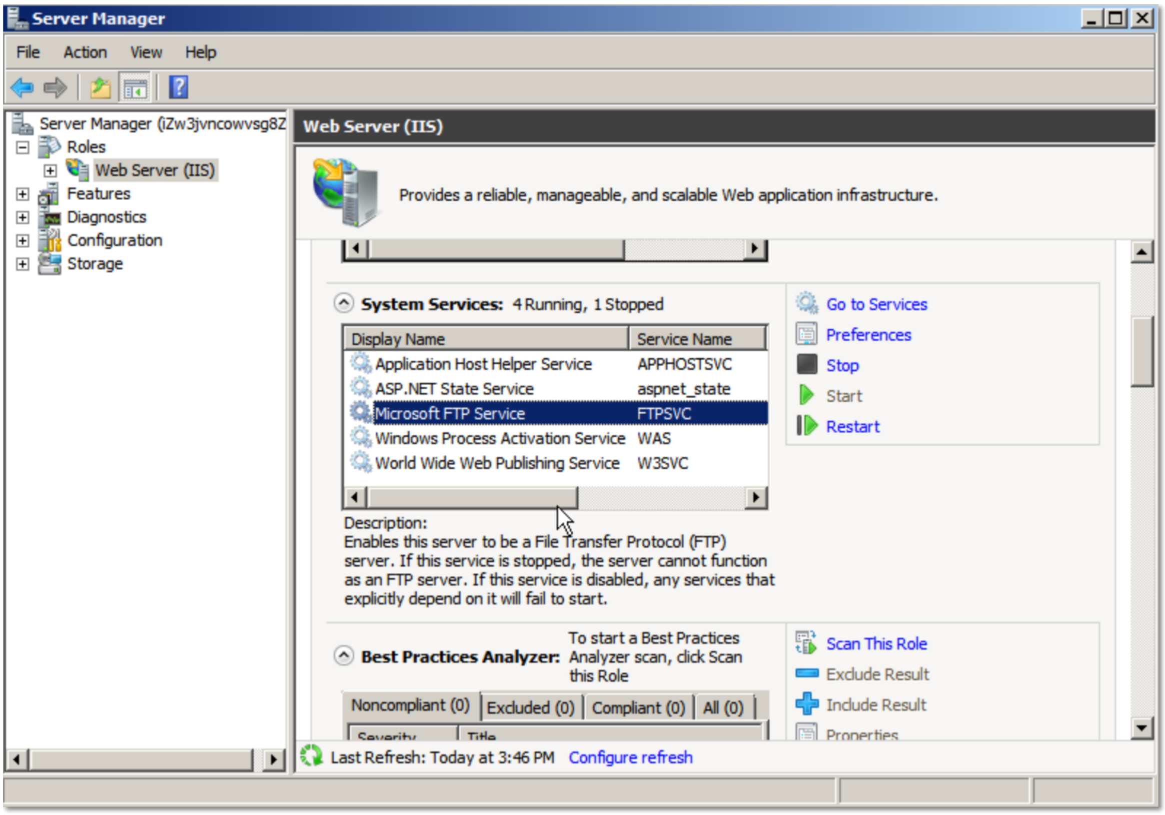
Example: 5000-6000

External IP Address of Firewall:

Example: 10.0.0.1

To accept passive connections when you are using FTP over SSL (FTPS) or when your firewall does not filter packets, configure the external IPv4 address of your firewall.

5. In the **Server Manager** window, restart the FTP service to validate the port range configurations.



Provides a reliable, manageable, and scalable Web application infrastructure.

System Services: 4 Running, 1 Stopped

Display Name	Service Name
Application Host Helper Service	APPHOSTSVC
ASP.NET State Service	aspnet_state
Microsoft FTP Service	FTPSVC
Windows Process Activation Service	WAS
World Wide Web Publishing Service	W3SVC

Description:
Enables this server to be a File Transfer Protocol (FTP) server. If this service is stopped, the server cannot function as an FTP server. If this service is disabled, any services that explicitly depend on it will fail to start.

Best Practices Analyzer: To start a Best Practices Analyzer scan, click Scan this Role

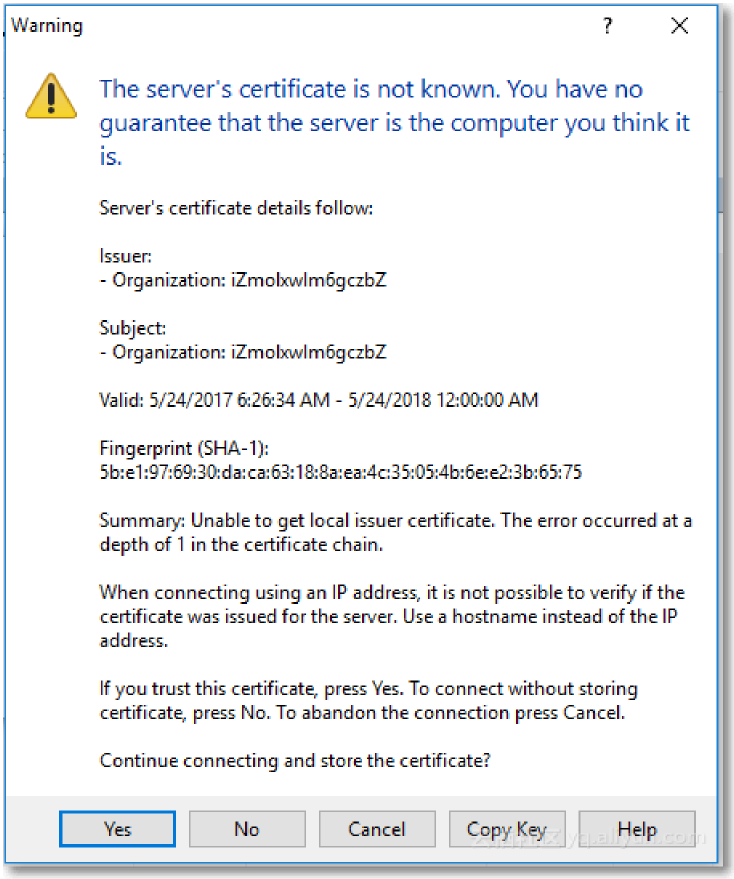
Last Refresh: Today at 3:46 PM

6. In the ECS console, configure the security group for the ECS instance to restrict the access of FTP clients. For more information, see Create a security group.

7. Access the FTP site through the FTP client WinSCP.

   i. Open WinSCP.

ii. Click **Yes** to accept the server certificate.



Warning

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

Fingerprint (SHA-1):
5b:e1:97:69:30:da:ca:63:18:8a:ea:4c:35:05:4b:6e:e2:3b:65:75

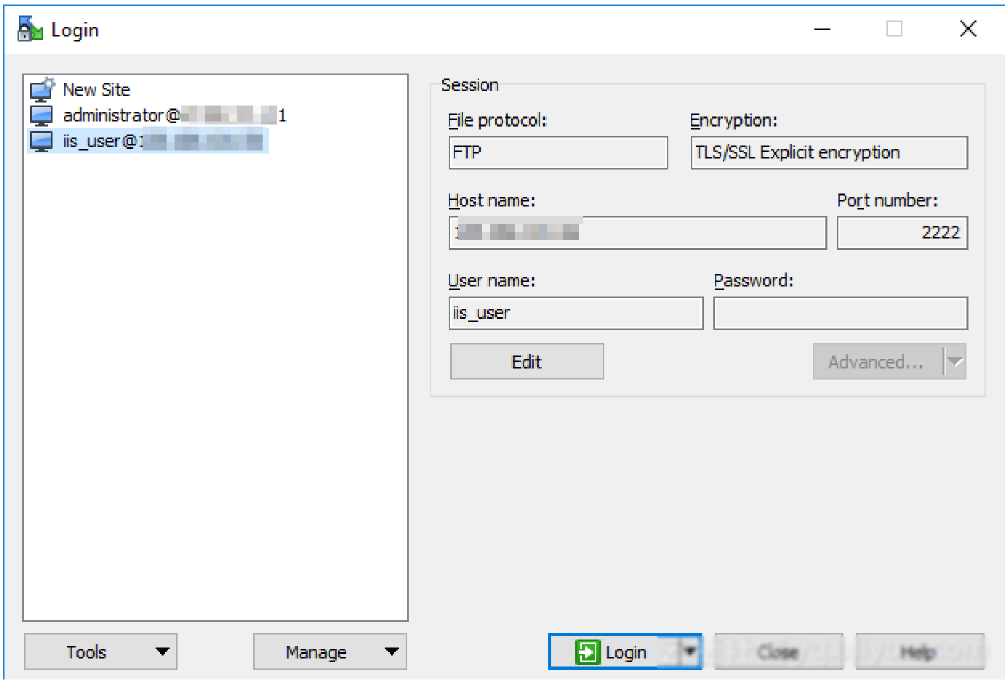
Summary: Unable to get local issuer certificate. The error occurred at a depth of 1 in the certificate chain.

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.

Continue connecting and store the certificate?

iii. Set the protocol type, port number, and logon information.



Login

New Site
administrator@[redacted]
iis_user@[redacted]

Session

File protocol: FTP

Encryption: TLS/SSL Explicit encryption

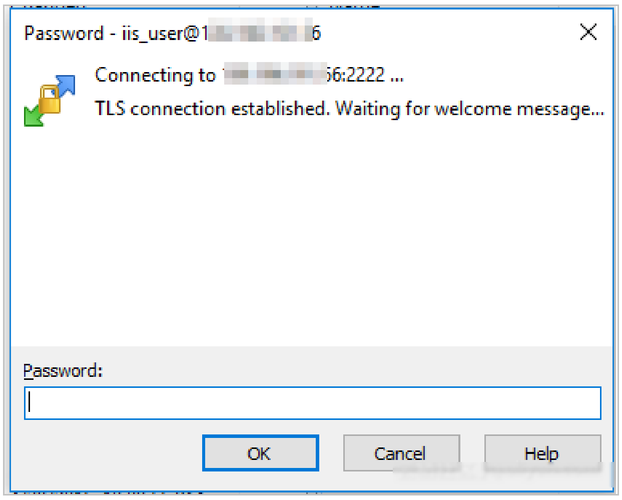
Host name: [redacted]

Port number: 2222

User name: iis_user

Password:

iv. Enter the password of the authorized user (iis_user).



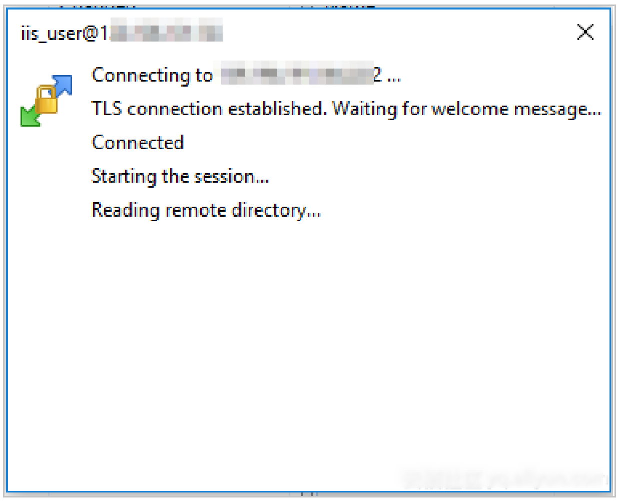
Password - iis_user@1[redacted]6

Connecting to [redacted]6:2222 ...

TLS connection established. Waiting for welcome message...

Password:

v. Establish a data connection to allow the server to read data from and write data to remote directories.



iis_user@1[redacted]

Connecting to [redacted]2 ...

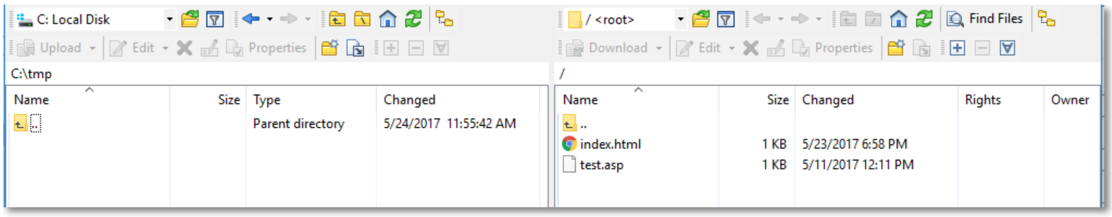
TLS connection established. Waiting for welcome message...

Connected

Starting the session...

Reading remote directory...

vi. After the connection is created, you can upload and download files.



C:\tmp

Name	Size	Type	Changed
..		Parent directory	5/24/2017 11:55:42 AM

/

Name	Size	Changed	Rights	Owner
..				
index.html	1 KB	5/23/2017 6:58 PM		
test.asp	1 KB	5/11/2017 12:11 PM		

How can I achieve coordination of IIS and NAS in Windows Server 2016?

If you are using Windows Server 2016, you must perform the following operations to achieve coordination of IIS and NAS after you set up the Windows IIS web service:

1. Modify the registry key of the SMB client.

   i. On the Windows server, choose **Start > Administrative Tools > Registry Editor**.

   ii. In the left-side navigation pane of **Registry Editor**, choose **HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > LanmanWorkstation > Parameters > AllowInsecureGuestAuth**, right-click a blank area, and then choose **New > DWORD (32-bit) Value**.

   iii. Set the value name to **AllowInsecureGuestAuth**, set the value data to **1**, and then click **OK**.

2. Specify a local user to access the web resources stored on NAS.

   i. In the Windows server, choose **Start > Windows Operating System > Administrative Tools > Internet Information Services (IIS) Manager**.

   ii. In the left-side navigation pane, choose **View Sites > Default Web Site**, and click **Basic Settings**.

   iii. In the **Edit Site** dialog box, click **Connect as**.

   iv. Select **Specific User** and click **Set**.

   v. Set the username and password, and then click **OK**.

   In this example, the iis_user user is used.

> ? Note
>
> - When IIS accesses a file in the shared directory of the NAS file system, the backend of IIS may access the shared directory for multiple times. Although each access request does not take a long time, the client may take a long time to respond if multiple access requests are sent. For more information, see How to improve performance when using IIS to access NAS?
> - We recommend that you store the web-related files such as JS and CSS files to local disks if these files are frequently accessed by IIS.
> - If a write failure still occurs after you perform the preceding operations, see Install and configure the AD domain to resolve the access failure from IIS in Windows Server 2016 to SMB file systems, or.

How can I achieve coordination of IIS and NAS in Windows Server 2019?

If you are using Windows Server 2019, you must follow the steps in How can I achieve coordination of IIS and NAS in Windows Server 2016? to modify the registry key and add the iis_user. You must also run the *New-SmbGlobalMapping* command in PowerShell to mount the file system and resolve the load failure of DLL. The following code is an example:

```
# Define clear text string for username and password
[string]$userName = 'WORKGROUP\administrator'
[string]$userPassword = '****'
# Convert to SecureString
[securestring]$secStringPassword = ConvertTo-SecureString $userPassword -AsPlainText -Force
[pscredential]$credObject = New-Object System.Management.Automation.PSCredential ($userName, $secS
tringPassword)
New-SmbGlobalMapping -LocalPath z: -RemotePath \\file-system-id.region.nas.aliyuncs.com\myshare -Persi
stent $true -Credential $credObject
```

`****` is the logon password of the administrator.

3.2. Use NGINX as a proxy for Apsara File Storage NAS

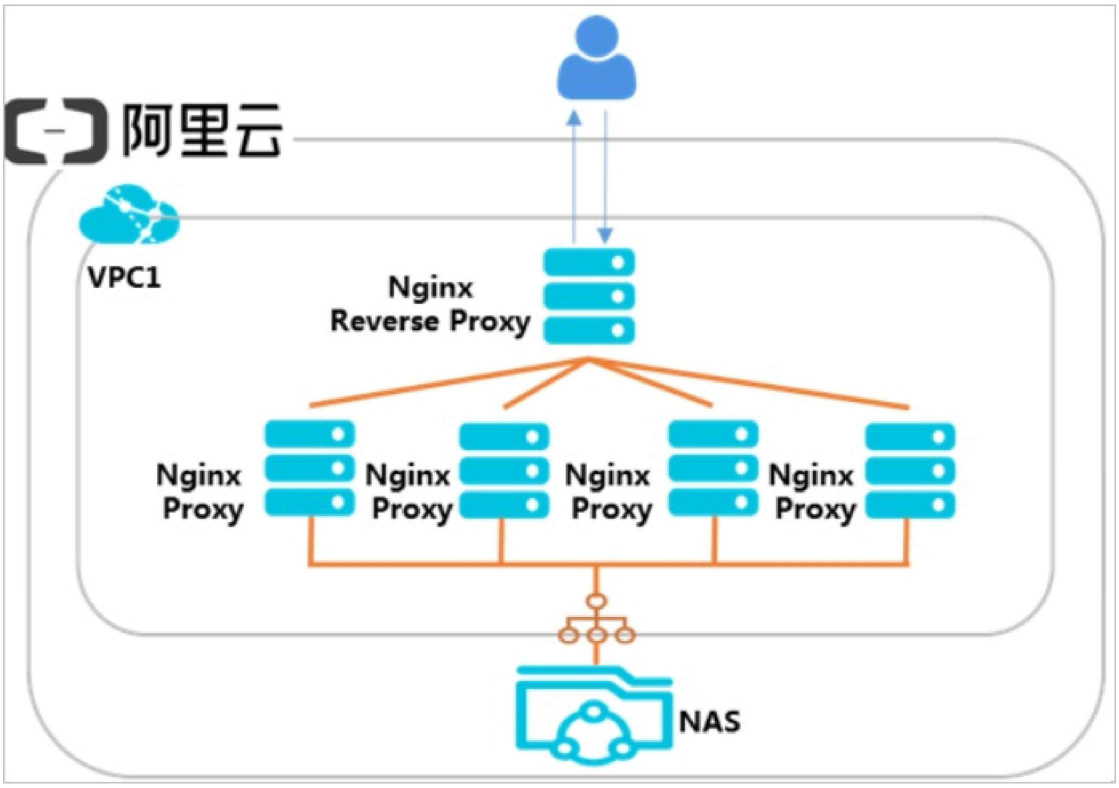
This topic describes how to use NGINX as a proxy for Apsara File Storage NAS.

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.

   ```
   yum install nginx
   ```

2. Configure a reverse proxy that points to a proxy server.

   i. Use the following command to open the */etc/nginx/nginx.conf* file.

   ```
   vim /etc/nginx/nginx.conf
   ```

   ii. 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 Create a General-purpose NAS file system in the NAS console.

   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 Create a mount target.

Step 3: Deploy an NGINX proxy server

1. Use the following command to install NGINX.

   ```
   sudo yum install nginx
   ```

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

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

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

   ```
   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.

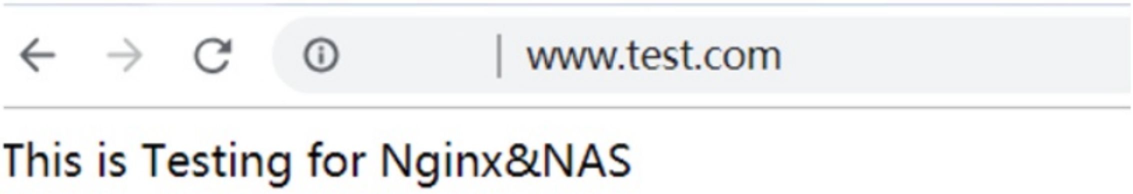
4. Edit the NGINX root file.

```
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

This is Testing for Nginx&NAS

4.Application server shared storage

4.1. 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 Mount an SMB file system on Windows .

> ? **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.

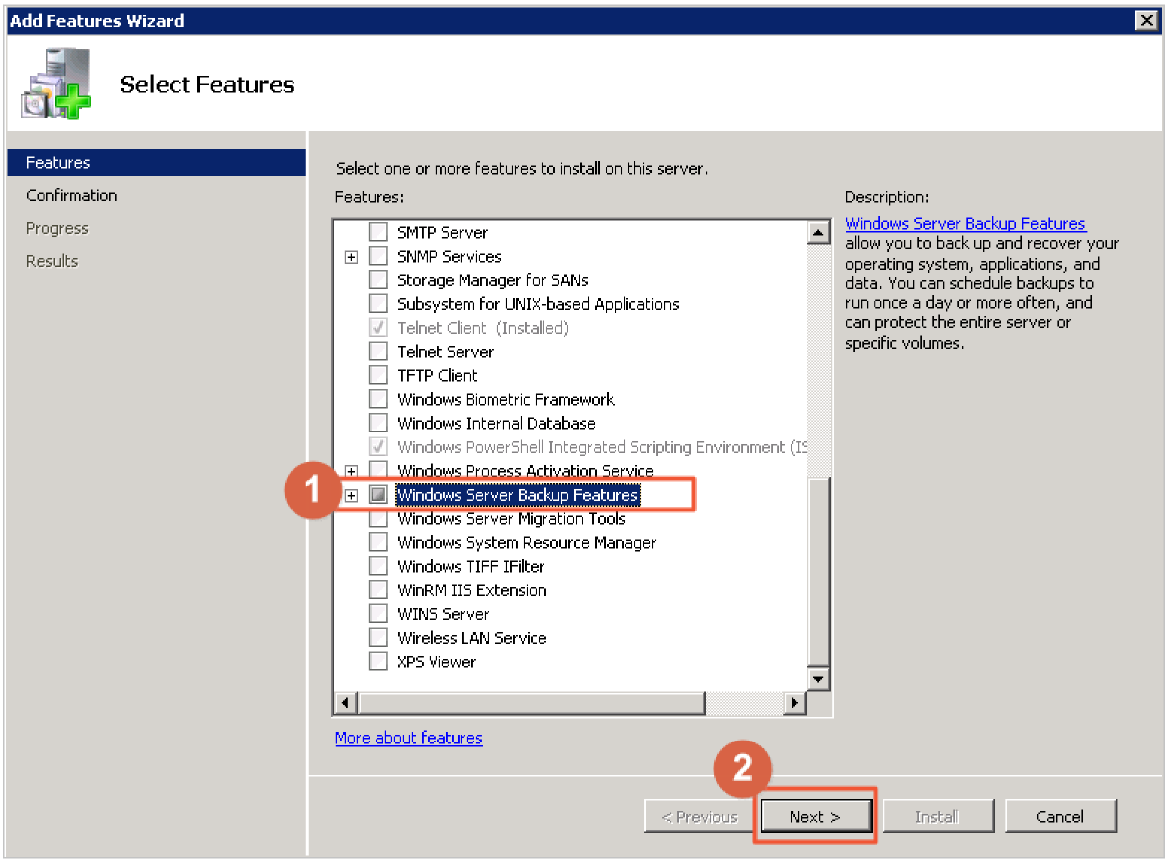
You can manually synchronize data stored on an ECS instance to Apsara File Storage NAS or schedule synchronization plans on a regular basis. This helps you preserve data and restore data in the event of data loss. Each disk snapshot is a copy of an entire disk. However, Apsara File Storage NAS is more 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**.
3. Select **Windows Server Backup Features** and click **Next**.


Add Features Wizard
Select Features
Features
Confirmation
Progress
Results
Select one or more features to install on this server.
Features:
□ SMTP Server
□ SNMP Services
□ Storage Manager for SANs
□ Subsystem for UNIX-based Applications
☑ Telnet Client (Installed)
□ Telnet Server
□ TFTP Client
□ Windows Biometric Framework
□ Windows Internal Database
☑ Windows PowerShell Integrated Scripting Environment (IS
□ Windows Process Activation Service
■ Windows Server Backup Features
□ Windows Server Migration Tools
□ Windows System Resource Manager
□ Windows TIFF IFilter
□ WinRM IIS Extension
□ WINS Server
□ Wireless LAN Service
□ XPS Viewer
Description:
Windows Server Backup Features allow you to back up and recover your operating system, applications, and data. You can schedule backups to run once a day or more often, and can protect the entire server or specific volumes.
More about features
1
2
< Previous
Next >
Install
Cancel

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.

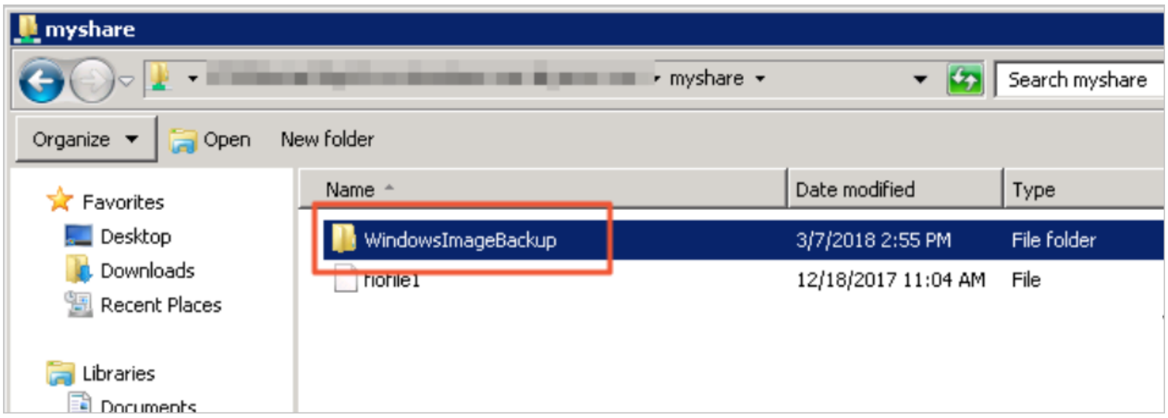
   i. Click **Add Items**, select folders to back up, and click **OK**.

   ii. 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.



Name	Date modified	Type
WindowsImageBackup	3/7/2018 2:55 PM	File folder
nofile1	12/18/2017 11:04 AM	File

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.

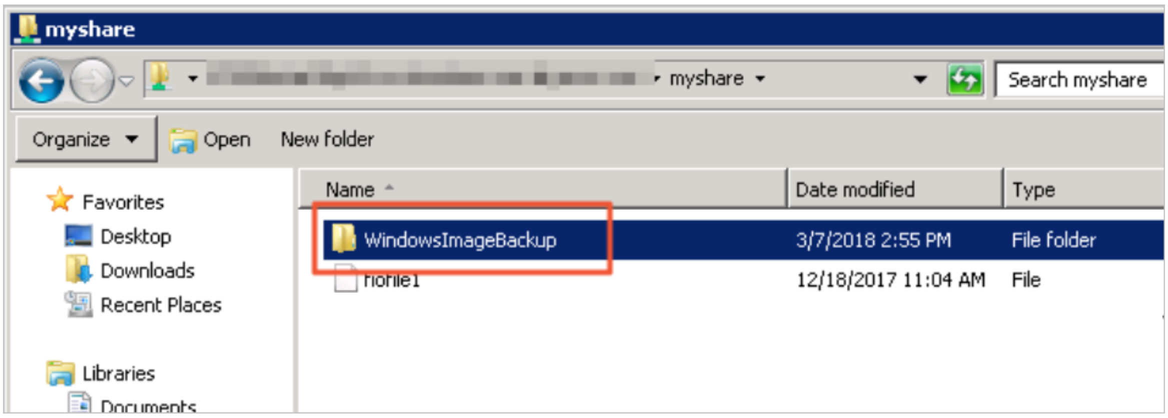
   i. Click **Add Items**, select folders to back up, and click **OK**.

   ii. 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.



Name	Date modified	Type
WindowsImageBackup	3/7/2018 2:55 PM	File folder
nofile1	12/18/2017 11:04 AM	File

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.