Alibaba Cloud Network Attached Storage

Best Practices

Issue: 20190329

MORE THAN JUST CLOUD | C-J 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 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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.

Generic conventions

Table -1:	Style conv	entions
-----------	------------	---------

Style	Description	Example
•	This warning information 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.
	This warning information 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 restore business.
	This indicates warning informatio n, supplementary instructions, and other content that the user must understand.	• Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
Courier font	It is used for commands.	Run the cd / d C :/ windows command to enter the Windows system folder.
Italics	It is used for parameters and variables.	bae log list instanceid Instance_ID
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	ipconfig [-all -t]

Style	Description	Example
{} or {a b}	It indicates that it is a required value, and only one item can be selected.	<pre>swich {stand slave}</pre>

Contents

Legal disclaimer I
Generic conventions I
1 How to use Alibaba Cloud Network Attached Storage1
2 High-performance website5
2.1 Attach NAS to Windows IIS for data
2.2 Integrate NGINX with NAS 28
3 Application server shared storage
3.1 Mount NAS on Windows
4 Access a file system remotely
4.1 Access NAS from the local IDC through VPN45
4.2 Access NAS from the local IDC through NAT Gateway49
4.3 Use SFTP to upload and download NAS file system data51
4.4 Mount NAS file systems on ECS instances that are located in multiple
VPCs53
4.5 Mount NAS file systems on ECS instances that are owned by multiple
accounts57
5 Back up data from ECS to NAS by using Windows Server
Backup64

1 How to use Alibaba Cloud Network Attached Storage

This section describes Network Attached Storage (NAS) and how it is used.

What is NAS?

In the domain of storage, NAS is the abbreviation for network attached storage, which is referred to as network-based storage. You can share access to a NAS file system by using Network File System (NFS) or Server Message Block (SMB) from multiple servers at the same time. Unlike traditional file storage, NAS is a cloud-based distributed file system that provides scalability, high reliability, high availability, and high performance. Dependent on POXIS-based file APIs, NAS provides numerous benefits, such as compatibility with operating systems, shared access, data consistenc y, exclusive locks, and linear performance with increasing capacity.

A comparison with NAS, EBS, and OSS

Both NAS and Elastic Block Store (EBS) provide computational storage. To access a NAS or EBS file system, you must use POSIX-based APIs and link ECS instances with the file system. The difference between EBS and NAS is the location of each file system . The file system of EBS is integrated with an operating system. However, you can only access the file system of NAS over networks. OSS does not have a dedicated file system. You are only allowed to access OSS by using APIs over networks.



- NAS: As NAS has regulated file systems on a storage system, computational nodes can access NAS in the same way they access a local file system by using POSIX
 -based APIs over networks. NAS supports scalable capacity. You do not need to preserve capacity in advance. Capacity can be scaled based on the amount of actually written data. The file lock mechanism of NAS natively supports shared access. Compared to EBS, NAS has high latency and low IOPS performance due to network issues. Therefore, NAS is mainly applied to shared access scenarios with multiple computational nodes and stateless clusters.
- EBS: EBS is a type of bare disks, which cannot be directly accessed by an operating system. You must expose block storage as volumes by using RAID or LVM. Then, you can access these volumes by formatting the file system to ext3, ext4, and NTFS.
- EBS offers high performance and low latency. EBS is applicable to I/O-intensive , high-performance, and low-latency data stores, such as OLTP data stores and NoSQL data stores. As EBS capacity is not scalable, the maximum size of a single disk is 32 TB. Additionally, due to limited support for shared access, EBS must work with cluster management applications, such as Oracle RAC and WSFC Windows to enable shared access.
- OSS: OSS is a new type of storage. Compared to the directory-based tree hierarchy of NAS, OSS uses a flat file hierarchy.
 - OSS allows access by RESTful APIs and does not support random reading or writing of data. OSS is mainly applied to upload, download, and distribute large amounts of data over the Internet.

NAS scenarios

- · Multiple ECS instances share access to NAS
 - NAS supports shared access to file storage. Each ECS instance can access NAS in the same way it accesses a local file system and retrieves the same data. This

allows data to be automatically synchronized between multiple ECS instances. NAS addresses the issue of data synchronization in clustering mode.



· High-performance websites

The most commonly used architecture for the application platform of a website is a clustering architecture. For each code update, you must deliver the latest version of the website to all clusters. Manually synchronization of code or applicatio ns brings low efficiency, high costs, and low fault-tolerance. However, you can quickly deliver and synchronize code by using the shared storage of NAS.

· Web content management platform

Content management platforms are mostly Web-based applications with a stateless clustering architecture. A content management platform that uses functions such as rsync to synchronize data, images, and files between servers. This allows an image uploaded from server A to be viewed on server B. However, data cannot be fully synchronized in real time. When a spike in business occurs, synchroniz ed data may be inconsistent. NAS is introduced to easily resolve this issue. When cluster servers simultaneously access the same NAS file storage, data will be automatically shared and synchronized.

· Shared storage for both developing and testing environments

With NAS shared storage, you can easily share code between developing and testing environments. You only need to maintain one code base. Note that NAS promotes progress in a developing environment, compiling and uploading to CI for integratio n, and releasing code without the labor-intensive task of copying code. Therefore, NAS shared storage is flexible and quick to meet customer needs.

Container storage

A container is an indispensable component of a micro-service. A container can be preconfigured, is portable, and provides thread isolation. Each time you start a container, you must ensure access to original data and enable a shared file system . In this situation, whichever instance a container runs, the container can connect to the file system. Many data applications require persistent and local storage of a container. Shared file storage is the best option for containers that have a steep growth in demand for persistent storage. NAS supports data sharing between multiple pods. You can switch between containers to ensure high availability. NAS features scalable capacity and can meet the container requirements for business flexibility.

High-performance computing

NAS features high bandwidth and IOPS, which is mainly applied to highperformance computational scenarios.

For example, NAS can be applied to concurrent computing with large-scale computational node-based scenarios, such as High-performance computing (HPC), artificial intelligence (AI) self-driving, simulation, and DNA sequencing. These scenarios require a unified name space and high-performance shared access to file storage.

How to select the appropriate type of NAS

NAS has multiple storage types. For various application models, we recommend that you select the most appropriate storage type to derive the best performance from NAS . The features and scenarios of various NAS types are described as follows.

Туре	Feature	Scenario
NAS Capacity	High capacity, low cost, and scalability. Latency: 3-10ms.	File sharing, content management, and backup.
NAS Performance	High capacity and scalability. Latency: 1-2ms.	File sharing, containers, and big data analysis.

2 High-performance website

2.1 Attach NAS to Windows IIS for data

This document explains how to use the SMB protocol (supported by Alibaba Cloud NAS) and ECS instances in Windows to enable Web and FTP services through Windows built-in Internet Information Service (IIS).

Product implementation

Alibaba Cloud is the only public cloud vendor with a file storage system (NAS) that supports both the Network File System (NFS) protocol (NFSv3 and NFSv4) and the Server Message Block (SMB) protocol (versions 2.0 and later). To ensure IIS works in conjunction with NAS, the following are recommended:

- You must use Windows Vista/Windows Server 2008 or any later Windows version.
 Earlier versions (such as Windows XP or Windows Server 2003) are not supported.
 We strongly recommend using Windows 2008 R2 or later.
- Prioritize use of an SMB file system so that Windows applications can directly access NAS without needing modification.

With centralized resource storage on a highly reliable, high throughput Alibaba Cloud NAS and SMB share, IIS can access data in Alibaba Cloud NAS as though it were accessing a local file system. This allows for the separation of storage and computing services of websites. Additionally, computing resources and storage resources can be re-sized on demand to meet requirements. Furthermore, Alibaba Cloud's Server Load Balancer (SLB) allows multiple instances to support a website architecture, to improve error tolerance and resilience. The following illustration demonstrates a simple architecture example:

Ali	ibaba Cloud NAS SMB Share	
	Web Server based on Windows ECS	
	1	
	Server Load Balancer	
	Web Client	

FTP services provided by IIS are also widely used. Many website administrators remotely manage website content using FTP, and many customers want to transfer and share files between WAN and Alibaba Cloud using the FTP services of Windows instances.

Basic settings

Using IIS 7.5 (Windows Server 2008 R2) as an example, the following explains how to provide single-node Web and FTP service on Alibaba Cloud through Alibaba Cloud NAS. The installation and deployment of other Windows Server versions (for example, Windows Server 2008 and Windows Server 2012) implement a similar setup. For Windows Server 2016, a key difference related to settings are detailed in a following section. Additionally, you can choose to deploy Alibaba Cloud Server Load Balancer to create multi-server-node websites with error tolerance and resilience. For more information, see *What is Server Load Balancer*?.



Ensure you take all necessary steps to maintain the security of your data and website services. While Alibaba Cloud strives to maintain the highest data security standards, it is not responsible for protecting against all attacks that may occur. We recommend that you take comprehensive security measures such as setting a firewall and ECS instance security group, and installing updated OS patches as they become available, in order to fully protect your resources.

Install IIS

Using Windows Server 2008 R2 as an example, the procedure for adding an IIS role and installing the IIS through the server console are illustrated as follows: For a detailed procedure of IIS installation on Windows OS, see Microsoft's online documentation.

- Install and deploy of IIS 7
- · Install IIS and ASP.NET module (Windows Server 2012 and 2012 R2)



For a detailed procedure of IIS installation on Windows OS, see Microsoft's online documentation

1. Select the Web Server (IIS) role from the server console.

Add Roles Wizard		×
Select Server Ro	les	
Before You Begin Server Roles Web Server (IIS) Role Services Confirmation Progress Results	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 Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services Application Server DHCP Server DNS Server File Services Hyper-V Network Policy and Access Services Print and Document Services Remote Desktop Services Videb Server (IIS) Windows Deployment Services Windows Server Update Services	Description: Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
	< Previous Next	> Install Cancel

2. Select role services for the Web Server. In this example, in addition to basic HTTP functions, FTP services and extensions, ASP services, and other services are

selected. They are used for FTP over SSL services and dynamic web page scripts.

Then, click Next.

Add Roles Wizard			X
Select Role Servi	ces		
Before You Begin Server Roles Web Server (IIS) Role Services Confirmation Progress Results	Select the role services to install for Web Server (IIS): Role services: Web Server Genumon HTTP Features Static Content Default Document Directory Browsing HTTP Proros HTTP Redirection WebDAV Publishing Application Development Method Publishing Application Development NET Extensibility ASP CGI SAPI Extensions Server Side Includes Health and Diagnostics HTTP Logging Logging Tools Request Monitor Tracina More about role services	AS of arr ba AS inf ap	escription: SP.NET provides a server side object iented programming environment r building Web sites and Web oplications using managed code. SP.NET is not simply a new version ASP. Having been entirely re- chitected to provide a highly roductive programming experience ased on the .NET Framework, SP.NET provides a robust frastructure for building web oplications.
	< Previous	Next >	Install Cancel

3. Click Install.

<mark>} www</mark> G⊖⊽⊽ <mark>]} → myshare (\</mark>	\0b43f4a94d-agy61.cn-hangzhou.nas.aliyuncs.com)	• www • 🗲	Search www	
Organize 👻 New folder		1		i – 🔟 😧
🔆 Favorites	Name ^	Date modified	Туре	Size
Desktop Downloads	index.html test.asp	10/5/2017 2:17 PM 10/5/2017 2:19 PM	HTML Document ASP File	1 KB 1 KB

Create an SMB file system in NAS

You can centralize the storage of your Web service resources and configuration files on an Alibaba Cloud NAS SMB share. After creating an Alibaba Cloud NAS file system that supports SMB, set the permission group so that the current Web server has read and write access to the corresponding file system of the SMB share. You can use VPC or classic network to connect the NAS file system and the Web server.

After creating an SMB file system, create a directory in the file system's default share *myshare*, for example www, to store website files. In this and all following examples, a static file *index*. *html* and a dynamic ASP script file *test*. *asp* are created under *myshare* \ *www*. The former displays Hello World !, and the latter dynamically acquires and displays the current time.

• The index . html file is as follows:

• The test . asp file is as follows:

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

As illustrated in the following figure, users in the current ECS instance can verify access to the SMB share through Windows File Manager. In this example:

- \\ 32f214a370 pcy74 . cn shanghai . nas . aliyuncs . com \ myshare
 \ www is the physical path of the website resources.
- \\ 32f214a370 pcy74 . cn shanghai . nas . aliyuncs . com \ myshare is the Alibaba Cloud NAS SMB share that was created in the preceding step.

Internet Information Services (IIS) Manager							
C Vizw3jvnca	wvsg8Z 🕨 Sites 🕨 Default Web Site 🕨 🔤 🔯 🕼 🕡 🕶						
Connections	Default Web Site Home Filter: Edit Permissions Edit Site						
Default Web Site	Edit Site ? Site name: Application pool: Default Web Site DefaultAppPool Select						
	Physical path: agy61.cn-hangzhou.nas.aliyuncs.com\myshare\www Pass-through authentication Connect as Test Settings						
	OK Cancel						
< Þ	Configure Limits						

For security and management purposes, the user "iis_user" is added to the system . In the following examples, when provisioning the FTP service or running Windows Server 2016, data access is by this user rather than the administrator.

Set up IIS Web services

Open the Basic Settings of the website and go to Edit Website > Physical path to input the storage path for website resources on Alibaba Cloud NAS.

Ť		Registry Editor									
File	Edit	View Fav	orites Help								
		$\begin{array}{c} & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & \\ & & \\ &$	iScsiPrt kbdclass kbdhid kdnic Keylso KPSSVC KSecDD KSecPkg ksthunk KtmRm LanmanServ LanmanWor	er kstatio Provic		Name (Default) DisableMultiCha EnablePlainText DisablePlainText CherDomains RequireSecurity ServiceDII ServiceDIIUnIoa	Ty RE RE RE RE RE RE	pe G_SZ G_DWORD G_DWORD G_DWORD G_MULTI_SZ G_DWORD G_EXPAND_SZ G_DWORD	Data (value 0x0000 0x0000 0x0000 0x0000 %Syst 0x0000	not set) 00001 (1) 00000 (0) 00001 (1) 00000 (0) emRoot% 00001 (1)	\System32\v
			Paramet	ers	Ewr	and	1				
		$\Delta \cdot \Delta \cdot \Delta \cdot \Delta \cdot \Delta \cdot \Delta \cdot \Delta \cdot$	Idap Iltdio Iltdsvc Imhosts Lsa LSI_SAS LSI_SAS2 LSI_SAS3		Exp Ner Fin Del Rer Exp	w d ete name ort missions		Key String Value Binary Value DWORD (32-bit) QWORD (64-bit) Multi-String Valu	Value Value		
<					Co	py Key Name		Expandable String	g Value		

Then, enter the UNC address \\ 32f214a370 - pcy74 . cn - shanghai . nas . aliyuncs . com \ myshare \ www as the physical path of the website resources. (ui) By default, IIS accesses data through user accounts and user groups of IIS applications. If, during the current session, a Windows user maps a network drive (for example, Z:), the network drive cannot be directly used, or the system returns an access failure error.

After accessing the files *index*. *html* and *test*. *asp* at the localhost, or at 127.0.0.1 through a browser, and viewing results similar to the following examples, IIS is ready to provide normal Web services, as shown in the following example:

🧟 Hello Torld in HTEL - Internet Explorer	
🚱 🕞 🗢 🎉 http://127.0.0.1/index.html 🔎 🗹 🍎 🍏 Hello World in HIML 🛛 🗶	ĥ 🖈 🔅
Hello World!	
nerro worrd.	
Ettp://127.0.0.1/test.asp - Internet Explorer	
🚱 🕤 🛡 🖉 http://127.0.0.1/test. asp 🔎 🖌 🍎 🏉 127.0.0.1 🛛 🛛	☆ 🛠
This page was last refreshed on 2017/5/24 10:48:12.	
	1

Additionally, a server user can establish an Alibaba Cloud Security Group and a Windows Firewall to limit web access.

Windows Server 2016

For Windows Server 2016 users, as Microsoft has made several changes in the product cycle of IIS, you must implement the following two additional settings to make sure that IIS works properly with Alibaba Cloud NAS SMB services.

 Modify the following registry key of the SMB client to support access to the SMB share as an anonymous user. You can edit the registry by running the Registry Editor (regedit).

HKEY_LOCAL _MACHINE \ SYSTEM \ CurrentCon trolSet \ Services \
LanmanWork station \ Parameters \ AllowInsec ureGuestAu th

The procedure is as follows:

1. Run the Registry Editor, find

```
HKEY_LOCAL _MACHINE \ SYSTEM \ CurrentCon trolSet \ Services \
LanmanWork station \ Parameters , and right click to select New ( N ) >
DWORD ( 32 ) Value ( D ).
```



2. Edit AllowInsec ureGuestAu th , and set the value to 1.

<u>ش</u>		Registry	/ Editor	_ 0
File Edit View Favor	rites Help iScsiPrt ^ kbdclass kbdhid kdnic Keylso KPSSVC KSecDD KSecPkg ksthunk KtmRm LanmanServer LanmanWorkstatic Linkage NetworkProvic Parameters Idap Itdio Itdsvc Imhosts La	Registry	r Editor Type REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_MULTI_SZ REG_DWORD REG_EXPAND_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD	Data (value not set) 0x0000000 (1) 0x0000000 (0) 0x0000000 (1) 0x00000000 (0) %SystemRoot%\System32\wkssvc.dll 0x00000000 (0) D (32-bit) Value
	Lsa LSI_SAS LSI_SAS2 LSI_SAS3 LSI_SAS3	<	III	O Decimal
Computer\HKEY_LOCAL_I	MACHINE\SYSTEM\Cu	rrentControlSet\Servic	es\LanmanWorkstation	\Parameters

• Specify a local user in the IIS Website Settings to access the website resources on Alibaba Cloud NAS. (ui)Specific steps are illustrated in the following figures. You can select Basic Settings of the website, and then set the specified user by clicking Connect As. In this example, user "iis_user" is selected.(ui)



	?	×
]		
ОК	Cancel	
	OK	? OK Cancel

Set up IIS FTP services

To enable users to share files or release website contents through FTP, you must set the FTP over SSL service (also known as FTP-SSL, S-FTP, or FTP Secure) through IIS.

· Install the SSL certificate

1. Select Server Certificate in the IIS Server section to apply for and manage server certificates.



2. Specify the name of the server certificate.

Create Self	-Signed Certificate	? ×
	Specify Friendly Name	
Specify a for signin	file name for the certificate request. This information can be sent to a certificate authority g:	
Specify a	friendly name for the certificate:	
iis_signed	1	
	QK Cancel	

3. If successful, a certificate displays as follows:

Finternet Information Services (IIS) Manager	
C→ C→ iZw3jvncowvsg8Z →	🔛 🖂 🟠 I 😢 🕶
File View Help	
File View Help Connections Start Page Start Page Start Page ZW3jvncowvsg8Z (Zw Application Pools Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL. Name Issued To Issued By Expiration Date Certificate I Sites Sites	Actions Import Create Certificate Request Complete Certificate Request Create Domain Certificate Create Self-Signed Certificate View Export X Remove Remove Help Online Help
Ready	€∃

· Setting up FTP sites

1. Select Add FTP Site in the IIS Website section.

Similar to Web services, the physical path is the SMB share path in the UNC format. In this example, the *www* directory of the Web services is used. You can select other directories on *myshare* based on your needs, or set multiple FTP sites to access different directories through different ports.

Add FTP Site
Site Information
FTP site name: ftp_siteC
Content Directory
Physical path:
Hd-agy61.cn-hangzhou.nas.aliyuncs.com/myshare/www

2. Bind the IP address that provides the FTP service, and assign a port number.

For security, this example uses port 2222 rather than the standard port 21, to provide the FTP control information channel. We recommended you select

Require SSL certificate to connect to this FTP site, and use the SSL certificate previously created.

Add FTP Site	? ×
Binding and SSL Settings	
Binding IP Address: Port: All Unassigned IP 21	
Enable Virtual Host Names: Virtual Host (example: ftp.contoso.com):	
Start FTP site automatically	
Allow SSL Require SSL	
SSL Certificate: Not Selected View,	
iis_signed Previous Next Finish Can	cel

3. Specify the ID authentication method as Basic, and assign the read and write permission to iis_user. If required, you can select multiple authorized users at this stage.

Add FTP Site	<u>? ×</u>
Authentication and Authorization Information	
Authentication Anonymous Basic	
Authorization Allow access to:	
Ispedned users Iis_user Permissions	
I Read I Write	
Previous Next	Finish Cancel

4. For security, this example limits the port range of the FTP data channel by enabling the server level FTP Firewall Support in IIS console. To do so, click Apply, as follows:



5. Restart the FTP service in the server console, so that the port range can immediately take effect.

📕 Server Manager		
File Action View Help		
🗢 🔿 🔰 📅 🛛		
Server Manager (iZw3jvncowvsg8Z Roles Web Server (IIS) Features Diagnostics Configuration Storage	Web Server (IIS) Provides a reliable, manageable, and scalable Web application infrastructure.	
	Image: 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 Start World Wide Web Publishing Service W3SVC Image: 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.	
	Image: Severity of Title To start a Best Practices Analyzer scan, dick Scan this Role Image: Severity of Title Severity of Title Image: Severity of Title Title Image: Severity of Title Image: Severity of Title	Ŧ
	Last Kerresn: Today at 3:96 PM Configure refresh	_

6. For security, this example limits FTP client access by modifying Alibaba Cloud Security Group settings as follows:

Authorize only one client IP address to access the FTP control and data port range. If needed, you can also authorize multiple IP addresses, or one or more CIDR blocks.

Add Security Group F	Rules	×
NIC:	Intranet 🔹	
Rule Direction:	Inbound \$	
Authorization Policy:	Allow \$	
Protocol Type:	Custom TCP \$	
* Port Range:	2222/2333	
Priority:	1	
Authorization Type:	Address Field Access	
* Authorization Object:	4.15.17.112	 Tutorial
Description:		
	It must contain 2-256 characters and it cannot begin wit http:// or https://	h
		OK Cancel

- 7. The following pictures illustrate how you can access the FTP site through an FTP client WinSCP by selecting FTP over SSL.
 - a. Accept the server certificate. This message appears only when you connect to the FTP site for the first time.

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:
	lssuer: - 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?
	Yes No Cancel Copy Key

b. Set the protocol type, port number, and login information.

🌆 Login	- 🗆 X
 New Site administrator@47.88.35.121 iis_user@139.196.191.56 	Session <u>File protocol: Encryption:</u> FTP TLS/SSL Explicit encryption
	Host name: Port number: 139.196.191.56 2222
	User name: Password: iis_user
Tools Manage	Login Come Meter

c. Click Login. You are prompted to enter a the password of the authorized user on the IIS server.

Password - iis_user@139.196.191.56 X Connecting to 139.196.191.56:2222 TLS connection established. Waiting for welcome message
Connecting to 139.196.191.56:2222 TLS connection established. Waiting for welcome message
Password:

d. Data connection is established. This may take some time.



If successful, the following is displayed, indicating you can upload and download files.



2.2 Integrate NGINX with NAS

Scenarios

NGINX is a powerful high-performance Web server, which can be used as a reverse proxy. It has many excellent features. NGINX is a popular reverse proxy. A proxy server is a go-between or intermediary server that forwards requests for information from multiple clients to different servers across the Internet. A reverse proxy server is a type of proxy server that typically sits behind the firewall in a private network and directs client requests to the appropriate backend server.

Assume that a server is located in a private network cannot be accessed by external networks. In this case, a proxy server is required as an intermediary server, which is located in the same private network as the server and can be accessed by external networks. A server can be both an application server and a proxy server but uses separate ports.
Configure NAS as a reverse proxy to share storage

Configure one NGINX client as a reverse proxy and four NGINX clients as proxy servers. These clients use shared file storage provided by NAS in the background. You can use NAS to store multiple types of proxy server files, such as cache files, back-toorigin files, and static data files uploaded by users. Several proxy servers share access to NAS data to synchronize data. This prevents data inconsistency and frequent back -to-origin requests from occurring because data is not synchronized. The configurat ion is shown in the following figure:



· Deploy an NGINX reverse proxy

1. Install NGINX

[root @ Reverse proxy ~]# yum install nginx

2. Configure a reverse proxy

Configure a reverse proxy and associate it with a backend proxy server

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

You can configure NGINX as follows:

http {

```
upstream web {
    server 192 . 168 . 0 . 105 ;
    server 192 . 168 . 0 . 106 ;
    server 192 . 168 . 0 . 107 ;
    server 192 . 168 . 0 . 108 ;
    }
    server {
        listen 80 ;
        location / {
            proxy_pass http :// web ;
        }
    }
}
```

}

· Create a NAS file system

Create File System		×
* Region :	China North 5 (Huhehaote)	
	File systems and computing nodes in different regions are not connected.	
* Storage Type :	Capacity-type 🔻	
* Protocol Type :	NFS (including NFSv3 and NFSv4) 🔻]
	NFS is recommended in Linux and SMB is recommended in Windows	
* Zone :	China North 5 Zone A	
	File systems and computing nodes in different zones in the same region are connected.	-
Storage Package :	Default No Package	
	Bind an unused storage package	-
		OK Cancel

1. Create a file system for the corresponding region

2. Create a NAS mount point

The Linux client imple In the event of poor p	ments a default limitation on the number of concurrent request performance, you can refer to this document to adjust the conf	ts to the NFS. iguration.
File System ID :	0356249afa	nt point is the entry to
* Mount Point Type :	VPC •	
* VPC :	Select a VPC Go to the VPC console to create a VPC	Action Add Mount Point
* VSwitch :	Select a VSwitch	Manage Delete
* Permission Group :	Select the permission group	Add Mount Point Manage Delete
	Click to manage/create a permission group	Add Mount Point Manage Delete
	0	Add Mount Point Cancel Manage Delete

3. The newly created NAS mount point is for future use.

File System Details	Basic	Information					C	Delete File System	^
	File Sy	stem ID: 0356246afa		Region: China East 1 (Hangzhou)			Zone: China East 1 Zone G		
	Storage Type: SSD performance-type			Protocol Type: SMB (2.0 and later)			File System Usage: 0 B		
	Create	d On: Mar 23, 2019, 2:2	3:16 PM						
	Storag	ge Package							^
-	ID: na 035624	aspackage- 49afa-e732a5	Capacity: 500.00 Started At: Mar 23, 2019, 2:30:14 GB Upgrade PM			2:30:14	14 Valid Until: May 24, 2019, 12:00 AM Renew		
	Mount	t Point				How	to mount	Add Mount Point	^
	Mount Point Type 🕈	VPC	VSwitch 🗢		Mount Address	Permission Group	Status 🕈		Action
	VPC 🎝	vpc- bp13mh9fant3quv03f	vsw- bp1e6ds9dh;	zit59efpsqp	0356249afa-laj32.cn- hangshou navaliyuncu cam	VPC default permission group (Available	Modify Permission Activate	n Group Disable Delete

Deploy NGINX proxy servers

You can deploy an NGINX proxy server as follows:

1. Install NGINX and NFS clients

[root @ proxy ~]# yum install nginx

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

2. Mount a shared file storage on the web directory of NGINX

```
[ root @ proxy ~]# sudo mount - t nfs - o vers = 4 . 0 , <
the domain name of the mount point >:/ / usr / share /
nginx / html /
```

3. Modify the file of the NGINX main directory

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

Repeat the preceding procedure for the other three NGINX proxy servers and mount the same NAS file system. At this point, all Nginx proxy servers can access the index. html test file.

Testing results



This is Testing for Nginx&NAS

3 Application server shared storage

3.1 Mount NAS on Windows

NAS is a storage service that offers you a distributed file system and shared storage across multiple ECS instances. This topic describes the process of mounting an NAS file system on Windows Server 2012 R2.

Prerequisites

Before you can mount a NAS file system to a Windows instance, you must complete the following actions:

- Follow Step 2. Create an instance to create a Windows ECS instance. In this example:
 - The region is EU Central 1 (Frankfurt).
 - The image is Windows 2012 R2 Data Centre Edition .
 - The network type must be VPC .

· Create a file system and add a mount point.

- 1. Activate the NAS service.
- 2. Log on to the NAS console.
- 3. Buy a storage package. Follow these steps:
 - a. In the left-side navigation pane, click Storage Package.
 - b. Click Buy Storage Package.

c)	Home Pr	oducts 🗸				۹	\$ 245	Billing Manage	ement	English	9
Ξ			Storage Package Management	China North 1	(Qingdao)	China East 1 (Hangzhou)) China No	rth 2 (Beijing)			
•	▼ NAS			China East 2 (Shanghai)	China South 1 (Shenzhen) EU Cent	ral 1 (Frankfurt)			
5	File Syster	n List		Hong Kong	Asia Pacific	SE 1 (Singapore)		0.0	afrach	Bus Storage	Dackaga
ය	Permission	n Group							circan	buy storage	Гаскаце
4	Storage Pa	ackage							Bound		
۵			ID: •	Type •	Capacity: •	Started At: •	Valid Unt	il: •	To •	Actio	n

c. On the NAS Storage Package page, select the Region (EU Central 1 is selected in this example), Capacity, and the duration of the package.

Region	China East 1 (Hangzhou)	China North 2 (Beijing)	China East 2 (Shanghai)	China South 1 (Shenzhen)	China North 1 (Qingdao)	Asia Pacific SE 1 (Singapore)	Current Selected Region: EU Central 1 (Frankfurt)
File System ID	EU Central 1 (Frankfurt) Create new FS and bin	Hong Kong					File System ID: Create new FS and bind package Storage Type: Capacity-Type Protocol Type: NFS Available Zone: EU Central 1 Zone A
	Storage package must b system ID to bind or sel	and with a file system, act [Create new FS and	and a file system can o I bind package]	only bind with one pack	age at any time. You c	an select an existed file	Capacity: 500GB Order Duratio1month(s)
							Fee
Storage Type	Capacity-Type						Fee
Storage Type Protocol Type	Capacity-Type NFS						Fee \$ (Buy Now
Storage Type Protocol Type Available Zone	Capacity-Type NFS EU Central 1 Zone A						Fee \$ Buy Now
Storage Type Protocol Type Available Zone Capacity	Capacity-Type NFS EU Central 1 Zone A 500GB	178	STB	ТОТВ	30TB	50TB	Fee \$ Buy Now
Storage Type Protocol Type Available Zone Capacity	Capacity-Type NFS EU Central 1 Zone A 500CB 100TB	1TB 200TB	5TB 300TB	10TB 500TB	30TB 1PB	SOTB	Fee \$ Buy Now

- 4. Create a file system. Follow these steps:
 - a. In the NAS console, from the left-side navigation pane, click File System List.
 - b. Select the EU Central 1 (Frankfurt) region.
 - c. Click Create File System.
 - d. Specify the specifications of the file system and bind the storage package to it.

eate File System		
The upper limit of the that of a capacity-typ	storage capacity of an SSD performance-type file system is the file system is 10 petabytes.	1 petabyte, and
· Region:	EU Central 1 (Frankfurt) \$	
	File systems and computing nodes in different regions are not connected.	
* Storage Type:	Capacity-type \$	
Protocol Type:	NFS (including NFSv3 and NFSv4) \$	
Zone:	EU Central 1 Zone A \$	
	File systems and computing nodes in different zones in the same region are connected.	
Storage Package:	Default No Package naspackage-114 Jb54	
	0	K Cancel

- e. Click OK.
- 5. Add a mount point.

In this example, select VPC as the mount point type.

The mount point is th currently supported a permission group.	e entry for the ECS server to visit the file system. The mount point types re classic network and VPC. Each mount point must be bound to a	
The Linux client imple In the event of poor p	ements a default limitation on the number of concurrent requests to the NFS. erformance, you can refer to this document to adjust the configuration.	
File System ID:	11 9	
Mount Point Type:	VPC \$	
· VPC:	vpc-gw mh (19 \$	
	Go to the VPC console to create a VPC	
* VSwitch:	vsw-gw 3h (192.* \$	
Permission Group:	 Select the permission group VPC default permission group (allow all) 	

6. In the file system list, click the file system ID, and view the Mount Address of the new mount point. You will use the mount address to mount the file system on the Windows instance.

ľ	9							
Basic Info	rmation							
File System	1D: 11 9			Region: 6	EU Central 1 (Frankfurt)			
Storage Typ	Storage Type: Capacity-type				Protocol Type: NFS (NFSv3 and NFSv4.0)			
Created On	Feb 06, 2018 10:	47:24 +0000						
Storage P	ackage							
ID: nat		14	Capacity: 500).00 GB Upgrade	Started At: Jan 08, 2	2018 09:29:14 +0000		
Mount Po	int							
Mount Point Type •	VPC		VSwitch •	Mount A	ddress 🕈	Permissi Group		
VPC®	vpc- gv	τh	vsw-	3h 11	9-v 8.eu-central-1.nas.a	VPC defa		

Procedure

You can now mount the mount point on a server with Windows 2012 R2 Data Centre Edition. This solution works for most versions of Windows with NFS Client installed.

1. Connect to a Windows instance.

2. Install the NFS Client on the instance.

- a. Click the Server Manager icon.
- b. From the upper menu, select Manage > Add Roles and Features.
- c. Follow the Add Roles and Features Wizard to finish the installation.
 - Under the Server Roles tab, select Server For NFS.

B	Add Roles and Features Wizard	_ _ ×		
Select server roles		DESTINATION SERVER localhost		
Before You Begin Installation Type	Select one or more roles to install on the selected server.	Description		
Server Selection Server Roles	 ▲ ■ File and Storage Services (1 of 12 installed) ▲ □ File and iSCSI Services 	Server for NFS enables this computer to share files with UNIX-		
Features Confirmation	File Server BranchCache for Network Files	based computers and other computers that use the network file system (NFS) protocol.		
Results	Data Deduplication DFS Namespaces DFS Replication			
	File Server Resource Manager File Server VSS Agent Service			
	isCSI Target Server isCSI Target Storage Provider (VDS and VSS			
	Vork Folders Vork Storage Services (Installed)			
	< Previous Next >	Install Cancel		

• Under the Features tab, select Client for NFS.

L	Add Roles and Features Wizard	_ _ X
ES Select features Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Add Roles and Features Wizard Select one or more features to install on the selected server. Features Image: Installed inst	DESTINATION SERVER localhost
	Group Policy Management IIS Hostable Web Core Ink and Handwriting Services	> Install Cancel

- d. Restart the server within the guest operating system.
- e. Start Command Prompt and run mount . If the following result is returned, the Client for NFS has been installed.

C:\Users\Administrator> <mark>mount</mark>					
Local	Remote	Properties			
C:\User	s\Administrator>_				

3. Run the following command to mount the NFS mount point as a drive.

```
mount - o nolock \\ 11xxxxxxx 9 - wxx88 . eu - central - 1 .
nas . aliyuncs . com \! h :
```

Where 11xxxxxxxx 9 - wxx88 . eu - central - 1 . nas . aliyuncs . com is the mount address that we have created.

```
C:\Users\Administrator>
C:\Users\Administrator>mount -o nolock \\11 9-w 8.eu-central-1.nas.aliy
uncs.com\! h:
h: is now successfully connected to \\11 9-w 8.eu-central-1.nas.aliyunc
s.com\!
The command completed successfully.
C:\Users\Administrator>
```



4. Check the shared drive from the This PC of the instance.

_ 🗆 X 🎉 l ⊋ 👪 👳 l New folder Help Home 0 Share View v (e) () ▼ ↑ () (\\11f7e249f29-wyh88.eu-central-1.nas.aliyu... ► New folder Q v C Search New folder . Name Date modified Туре Size 🔆 Favorites 📰 Desktop New Text Document 2/6/2018 10:49 PM Text Document 0 KB Downloads 📃 Recent pla _ 🗆 🗙 New Text Document - Notepad File Edit Format View Help 💻 This PC This is a test file 📬 Network 1 item 1 item

5. Test creation of a folder and a text file inside the newly created folder.

Troubleshooting

If you get a file handle error, check the Registry entries in HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > ClientForNFS > CurrentVersion > User > Default > Mount. The value of Locking must be 1.

3					negistij	Editor
File	Edit	View Favorites Help				
		🖬 - 🐌 Microsoft	^	Name	Туре	Data
		.NETFramework		(Default)	REG_SZ	(value not set)
		Active Setup		8 AutoTuning	REG_DWORD	0x00000000 (0)
		Þ - 퉲 ADs		10 Defaults	REG DWORD	0x00000000 (0)
		Advanced INF Setup		88 Locking	REG_DWORD	0x00000001 (1)
		Þ- 🎍 ALG		88 MountType	REG_DWORD	0x00000001 (1)
		AllUserInstallAgent	_	👪 ReadBuffer	REG_DWORD	0x00100000 (1048576)
		D - ASP.NET	-	B Retransmissions	REG_DWORD	0x00000001 (1)
		Assistance		100 Timeout	REG_DWORD	0x000000x08 (8)
		PartPractices		100 WriteBuffer	REG_DWORD	0x00100000 (1048576)
		P- Bidloterface				
		4 CurrentVersion				
		- Default				
		RegNotify				
		⊿ - 🔐 Users				
		🛛 - 🌺 Default				
		Defaults				
		Mount				
		þ- 퉲 СОМЗ				

You can also set GID and UID by creating the Registry entries:

- 1. Go to HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > ClientForNFS > CurrentVersion > Default.
- 2. Right-click a blank area, and then select New > DWORD(32bit) to add the following Registry entries.
 - AnonymousG ID : Set the value to 0.
 - AnonymousU ID : Set the value to 0.

File Edit View Favorites Help				
⊿ - 🏭 Microsoft	^	Name	Туре	Data
NETFramework		ab (Default)	REG_SZ	(value not set)
Active Setup		🛗 AnonymousGid	REG_DWORD	0x00000000 (0)
Þ. 🎍 ADs		👪 AnonymousUid	REG_DWORD	0x00000000 (0)
Advanced INF Setup		Cacheblocks	REG_DWORD	0x00000040 (64)
⊳ - 🎽 ALG		3 DeleteSymLinks	REG_DWORD	0x00000001 (1)
AllUserInstallAgent	_	100 FirstContact	REG_DWORD	0x0000003 (3)
D ASP.NET	-	38 MaxNfsUser	REG_DWORD	0x00000020 (32)
Assistance		100 MountType	REG_DWORD	0x00000001 (1)
AuthHost		10 Protocols	REG_DWORD	0x00cffcff (13630719)
BestPractices		38 Retransmissions	REG_DWORD	0x00000001 (1)
		10 Timeout	REG_DWORD	0x00000008 (8)
ClientForNES		100 UseReservedPorts	REG_DWORD	0x00000001 (1)
- Default				
RegNotify				
⊿ - 🚻 Users				

3. Start Command Prompt and run mount to check the UID and GID.

C:\Users	:\Users\Administrator}mount				
Local	Remote	Propert			
h:	<pre>\\11f7e249f29-wyh88.eu-central-1.nas.~</pre>	UID=0, rsize=1 mount=s retry=1 fileacc casesen sec=sus			

4 Access a file system remotely

4.1 Access NAS from the local IDC through VPN

Limits

You can use Alibaba Cloud Network Attached Storage (NAS) to mount a file system created within a region on ECS instances only within that same region.

You cannot directly mount a file system on ECS instances in other regions. You also cannot directly mount a file system on the servers in your own data center.

For example, a file system (NFS or SMB) created in the East China 1 region cannot be directly mounted to an ECS instance in the North China 1 region.

To mount a file system on ECS instances in different regions, or on your IDC servers, you can use Express Connect. Using Express Connect, you can connect different VPCs or connect the data center and the VPC. However, deploying Express Connect will incur additional costs.

Solutions

Using the VPN Gateway service of Alibaba Cloud, you can access Alibaba Cloud VPC from your data centers and connect to VPCs in different regions. The VPN Gateway service allows NAS users to deploy the following network topology and mount the file system using two methods:

- $\cdot\,$ Mount the file system on the servers in your IDC
- Mount the file system on ECS instances in different regions



Mount the file system on the servers in your IDC

- 1. Log on to the NAS console, create a file system, and add VPC mount points to the file system.
- 2. Log on to the VPC console, create a VPN connection to connect the VPN Gateway within the VPC and the VPN Gateway within your IDC. For more information, see *Configure a site-to-site connection*.

After completing these configurations, you can verify the connectivity between the IDC server and the ECS instance or the mount point of the file system in VPC by using the ping command. After confirming IP addresses at both ends can be pinged, you can mount the file system within the VPC onto the server at the side of VPN Gateway within your IDC..

Mount the file system on ECS instances in different regions

Two methods are available for mounting the file system on ECS instances in different regions.

For method 1, you must build a VPN Gateway by using an ECS server within VPC2. This method is suitable if you have already deployed similar gateway services. If you do not have such an environment, you may use method 2.

• Method 1

- 1. Log on to the NAS console, create a file system, and add VPC mount points to the file system within VPC1.
- 2. Build a user VPN Gateway as a User Gateway by using an ECS server within VPC2 in another region. This ECS must have an Internet IP address to connect with the VPN Gateway within VPC1.

Note:

If you want to know how to build a VPN Gateway by using an ECS server, you can see tutorials on the Internet, for example, *Using StrongSwan for IPSec VPN on CentOS 7*.

- 3. Log on to the VPC console, create a VPN connection, and connect VPN Gateways within VPC1 and VPC2 (the one created in Step 2). For more information, see *Configure a site-to-site connection*.
- 4. Add a static route for other ECS instances within VPC2, and set the target CDIR block to the same as that of VPC1. Set the net-hop node as the gateway (the one created in Step 2) within VPC2.

After completing these configurations, you can verify the connectivity between VPC1 and the ECS instance or the mount point of the file system in VPC2 by using the ping command. After confirming IP addresses at both ends can be pinged, you can mount the file system within VPC1 onto other ECS instances within VPC2.

· Method 2

- 1. Log on to the NAS console, create a file system, and add VPC mount points to the file system within VPC1.
- 2. Log on to the VPC console, and create a VPN Gateway. For more information, see *Configure a site-to-site connection*.
- 3. Log on to the VPC console, and create a VPN Gateway within VPC2 in another region.
- 4. Create user gateways respectively with IP addresses of VPN Gateways created in Step 2 and Step 3. For more information, see *Configure a site-to-site connection*.
- 5. Create a VPN connection to connect VPN Gateways which were created in Steps 2 and 3. For more information, see *Configure a site-to-site connection*.
- 6. Add routes for the two VPCs. For VPC1, set the target CIDR block as the intranet IP address of VPC2, and the next-hop node as the gateway within VPC1. For VPC2, set the target CIDR block as the intranet IP address of VPC1, and the next-hop node as the gateway within VPC2. For more information, see *Configure a site-to-site connection*.

After completing these configurations, you can verify the connectivity between VPC1 and the ECS instance or the mount point of the file system in VPC2 by using the ping command. After confirming IP addresses at both ends can be pinged, you can mount the file system within VPC1 onto other ECS instances within VPC2.

Benefits

- VPN Gateway service:
 - Solves connectivity issues.
 - Provides secure access (encrypted communication based on IPsec).
 - Greatly reduces user cost in comparison to Express Connect.
- However, when you access the file system through a VPN, the I/O performance is limited. The limitations are based on the Internet bandwidth and latency between the IDC server and VPC or between the different VPCs.

4.2 Access NAS from the local IDC through NAT Gateway

This document introduces how to access NAS using the NAT Gateway for scenarios involving mounting a file system in NAS from your local IDC or VPCs if they are located in different regions.

Background

When using NAS, a file system (NFS) created within a region can only be mounted on ECS instances within the same region. ECS instances in different regions, and servers in your own IDC, are not allowed to mount the file system directly.

To mount a file system on ECS instances in different regions, or on your IDC servers , you can use Express Connect between different VPCs or between the IDC and the VPC. While Express Connect is suitable for long-term connection, deploying Express Connect may be costly for some users.

A more cost-effective solution for uploading small amounts of offline data to NAS is to use the NAT Gateway to access Alibaba Cloud NAS from the Internet.

Limits

- If the EIP and VPC are connected, any user who obtains the EIP can use the mount point corresponding to the EIP without any additional permissions required.
- Each EIP and port can only be mapped to one mount point. Therefore, multiple EIP addresses are required to visit multiple mount points at the same time.

Network architecture

The following figure shows the network architecture of using a NAT Gateway to access Alibaba Cloud NAS from the Internet.

The architecture is implemented as follows:



- 1. Create a NAS file system, and add a mount point for the file system.
- 2. Create a NAT gateway, and add a bandwidth package for the NAT gateway to get an EIP address.
- 3. Add DNAT forwarding entries for the NAT gateway.

Procedure

- 1. Create a file system in the NAS console.
- 2. Add a mount point for the file system. Note that you must create a VPC mount point to support the use of NAT.
- 3. Connect to your ECS instance, and ping the mount point address to get the mount point IP address. An example output is as follows:



- 4. Create a NAT gateway.
- 5. *Bind an EIP* then add the bandwidth package to the NAT gateway.

- 6. Add a DNAT entry to create a DNAT entry.
 - For Public IP, select the EIP created in Step 5.
 - For Private IP, enter the mount point IP address you want to access.
 - For Port Settings, select All ports. You can also select the ports needed by the NFS or SMB protocols.
- 7. Verify the NFS mounting. Configure the DNAT to an NFS mount point. Example outputs are as follows:

DNAT Entry List					
DNAT Entry ID	Public IP	Public Port	Protocol Type	Private IP	Private Port
fwd-bpltys653y8jzn6uhi5xp	114.55.126.64	any	any	192.168.92.36	any
[sudo] passwo Warning: rpc All	ord for qiyi .idmapd appe uids will b	ng.zf: ars not to e mapped to	be running the noboo	g. dy uid.	
<pre>\$mount /dev/sda2 on / ty print of /or /or /or /or /or /or /or /or /or /or</pre>	pe ext3 (rw)	type py gays type ext4 (rw no 1 (rw addr-114 5	atime podirat	ime,delalloc,user	r_xattr,acl)

4.3 Use SFTP to upload and download NAS file system data

This topic describes how to use SFTP to upload and download NAS file system data.

Context

The transmission speed of SFTP depends on the Internet bandwidth of ECS. You can configure an appropriate network bandwidth according to your business needs.

Procedure

- 1. Purchase an ECS instance with CentOS as the operating system in the region where the NAS file system is located.
- 2. Log on to the ECS instance and modify the configuration file / etc / ssh / sshd_confi g as follows:
 - a. Comment out the subsystem line in the configuration file sshd_confi g , and then add a new line Subsystem sftp internal - sftp .

override default of no subsystems
Subsystem sftp / usr / libexec / openssh / sftp server

Subsystem sftp internal - sftp

b. Add the following commands to the end of the file sshd_confi g . / usr /

sftp is the SFTP root directory of the user. The name used in the example is for reference only. You can modify the name according to the actual situation.

X11Forward ing no AllowTcpFo rwarding no ForceComma nd internal-sftp ChrootDire ctory / usr / sftp

- 3. Run the groupadd sftp command to add a user group.
- 4. Run the useradd g sftp s / sbin / nologin M sftp

command to add a user and add it to the SFTP user group.

5. Set the password of the SFTP user.

```
[ root @ localhost ~]#
                        passwd
                                 sftp
Change
         the
               password
                          for
                                 the
                                             SFTP .
                                      user
New password :
Invalid
          password : the
                            password
                                       is
                                            less
                                                    than
                                                           8
characters
              password :
Enter
        new
passwd : All
                authentica
                           tion
                                   tokens
                                            have
                                                    been
successful ly
                 updated .
```

6. Create the root directory and configure the owner and group of the SFTP user, and

then modify the permission of the SFTP user to 755.

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

7. Under the root directory of the SFTP user, create a directory used to mount a NAS file system.

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

8. Run the following command to mount a NAS file system to the / usr / sftp /

file directory.

```
sudo mount - t nfs - o vers = 4 . 0
91fd04a7b7 - cvn49 . cn - zhangjiako u . nas . aliyuncs . com :/ /
usr / sftp / file
```

9. Run the service sshd restart command to restart SFTP.

10 Log on to the SFTP service using the SFTP client with the name and password of the SFTP user you configured in the preceding steps. You can choose a client that supports the SFTP protocol to connect to the SFTP service.

4.4 Mount NAS file systems on ECS instances that are located in multiple VPCs

This section describes how to mount NAS file systems on ECS instances that are located in multiple VPCs.

By default, when you mount a NAS file system on an ECS instance, ensure that the ECS instance and the NAS file system are located in the same VPC network. However , in most deployments, the VPC of an ECS instance is different from the VPC of a NAS mount point. You can connect VPCs by using Cloud Enterprise Network (CEN).

Configure a connection between VPCs

CEN enables connections between instances that are located in multiple VPCs but in the same region. After the connection is established, the ECS instance in VPC1 can directly communicate with the ECS instance and the NAS mount point in VPC2 by using the ping command.



1. Create a CEN instance

- a. Log on to the CEN console.
- b. On the CEN page, click Create CEN Instance.
- c. Configure the CEN instance as shown in the following figure.

[DO NOT TRANSLATE]

Create CEN	Instance	? ×
	Description 🕜	
	0/256	
Attach Ne	twork	
Your Act	count	
(i) No Ad	te: You cannot attach networks that are already attached to the CEN instance ditionally, you cannot attach networks that have Express Connect enabled.	
	• Network Type 🕜	
	Select ~	
	• Region 💿	
	Select ~	
	Networks ?	
	Select ~	
	ОК	Cancel

The options are described as follows:

Option	Description
Name	Enter the name of the CEN instance. The name can be 2 to 128 characters in length and can contain numbers, letters, Chinese characters, hyphens (-), and underscores (_). It must start with a letter or a Chinese character.
Description	Enter the description of the CEN instance. The description can be 2 to 256 characters in length. It cannot start with http://or https://.
Attach a network	You can attach networks in your account or another account to a CEN instance. For more information, see <i>Networks</i> .

2. Examples

a. On the Instances page, locate the newly created instance and click Manage in the Actions column.

Instances							Get St	arted ⑦ Docume	entation
Create CEN Instance Refresh						CEN Name \vee	Search		Q
Instance ID/Name	Status	Networks	Bandwidth Packages ⑦	Region Connections	De	scription		Actions	
carr-liveFavGpRdykaarfw7cji hjis-test	Ready	1	0	0	-			Manage Delete	

b. On the CEN page, click Attach Network to configure the network as shown in the following figure.

[DO NOT TRANSLATE]

								?
Your	Account	Different Account						
í	Note: You Additionally	cannot attach networks ti y, you cannot attach netw	that are al works that	ready attac have Expr	hed to the	e CEN instan lect enabled.	ice.	
	• Net	work Type 🕜						
	Sele	ect				\sim		
	• Reg	jion ?				\checkmark		
	 Net 	works 🕐						
	Sele	ect				\sim		

Option	Description
Account	Select Your Account.
Network Type	Select the type of network to attach to the instance . You can select one of the following values: VPC , Virtual Border Router (VBR), and CloudConne ctNetwork (CCN). Select VPC.
Region	The region where the network is located. Select China (Qingdao).
Networks	Select a network to attach. Select a VPC network.

The options are described as follows:

Repeat the preceding procedure to attach two VPC networks to the same CEN instance. At this point, the connection between two VPCs is established.

3. Verify the mounting result

Log on to the ECS instance to verify the mounting result.

```
nfs - o
                  mount - t
[ root @ ~]# sudo
                                         vers = 4 . 0 , vpc2 <
                        the
                                       point >:/ / mnt
                               mount
      domain name of
the
[ root @ iZbp18jc3n wxdiy5e1vk kaZ ~]# df - h
Filesystem
                                                 Size
                                                         Used
Avail Use % Mounted
                        on
/ dev / vda1
                                                    40G
                                                           1 . 8G
    36G
           5 % /
devtmpfs
                                                 1.9G
                                                              0
  1 . 9G
           0 % / dev
tmpfs
                                                 1.9G
                                                              0
  1.9G
             0 % / dev / shm
tmpfs
                                                 1.9G
                                                           472K
  1.9G
             1 % / run
tmpfs
                                                 1.9G
                                                              0
             0 % / sys / fs / cgroup
  1.9G
tmpfs
                                                 379M
                                                            0
379M
         0 % / run / user / 0
082e54b989 - ciq13 . cn - hangzhou . nas . aliyuncs . com :/
                                                            1.
         0
             1. OP
                        0 % / mnt
```

4.5 Mount NAS file systems on ECS instances that are owned by multiple accounts

This section describes how to mount NAS file systems on ECS instances that are owned by multiple accounts.

By default, you can only mount NAS file systems on ECS instances that are in the same account. If data transit is required between ECS instances that are owned by multiple UID accounts in an enterprise account and a NAS file system, you only need to establish a connection between the VPC that the ECS instance is located and the VPC that the NAS file system is located. You can connect multiple VPCs by using Cloud Enterprise Network (CEN).

Configure a connection between VPCs

CEN enables connections between VPCs that belong to multiple accounts. After connections between VPCs are established, ECS instances that are in one VPC can access NAS file systems in another VPC, even if the VPCs belong to different accounts.



1. Create a CEN instance using account A

- a. Log on to the CEN console.
- b. On the Instances page, click Create CEN Instance.
- c. Configure the CEN instance as shown in the following figure.

[DO NOT TRANSLATE]

Create CEN	Instance	?	\times
	Description 💿		
	0/256		
	0.200		
Attach Ne	etwork		
	Iditionally, you cannot attach networks that are already attached to the CEN instance.		
	Network Type Select		
	• Region ②		
	Select ~		4
	Networks		
	Select		
	ОК	Cance	

The options are described as follows:

Option	Description
Name	Enter the name of the CEN instance. The name can be 2 to 128 characters in length and can contain numbers, letters, Chinese characters, hyphens (-), and underscores (_). It must start with a letter or a Chinese character.
Description	Enter the description of the CEN instance. The description can be 2 to 256 characters in length. It cannot start with http://or https://.
Attach networks	You can attach networks in your account or another account to a CEN instance. For more information, see <i>Networks</i> .

d. Obtain the ID of the new CEN instance.

In this example, the CEN instance ID is cbn-xxxxxxx4l7.

2. Account B authorizes account A to attach its network instance

On the VPC Details page, you can authorize another account to attach networks that are owned by the current account. Proceed as follows:

1. Log on to the VPC console using account B.

2. In the left-side navigation pane, select VPCs.

3. Click the instance ID of the target VPC.

4. In the CEN cross account authorization information section, click CEN Cross Account Authorization.

In the Attach to CEN dialog box, enter Peer Account UID and Peer Account CEN ID, and then click OK.

Attach to CEN	×
() The account that you have authorized can attach your network to CEN instances and communicate with your network. Use caution performing this operation.	their when
• Peer Account UID	
• Peer Account CEN ID	
ОК	Cancel

3. Attach a network by using account A

After the authorization is complete, you can attach a network as follows.

- a. Log on to the CEN console using account A.
- b. On the Instances page, locate the newly created CEN and click Manage in the Actions column.
- c. On the CEN page, click Attach Network to configure the network.

Your Account	Different Account		
(i) Note: Go router, au attached Connect	to the VPC console, in the prop thorize the related CEN instand to the CEN instance cannot be enabled cannot be attached.	perties page of the VPC or virtual bo ce to attach that network. Networks a attached again. Networks with Expr	rder already ess
• O'	wner Account 🕜		
		0/128	
• No	etwork Type 🕜		
Se	lect	\sim	
• R	egion 🕐		
Se	lect	\sim	
• No	etworks 🕐		
		0/128	

The options are described as follows:

Option	Description
Account	Select Different Account.
Owner Account	Enter a peer account ID. Enter the account ID of account B.

Option	Description
Network Type	Select the type of network to attach to the instance . You can select one of the following values: VPC , Virtual Border Router (VBR), and CloudConne ctNetwork (CCN). Select VPC.
Region	The region where the network is located. Select China (Qingdao).
Networks	Select a network to attach. Select a VPC instance.

4. Verify the mounting result

Log on to the ECS instance to verify the mounting result.

```
vers = 4 . 0 , vpc2 <
point >:/ / mnt
root@~]#sudo mount - t
the domain name of the
[ root @ ~]# sudo
                                            nfs - o
                                            mount
[ root @ iZbp18jc3n wxdiy5e1vk kaZ ~]# df - h
 Filesystem
                                                                       Size
                                                                                  Used
Avail Use % Mounted
/ dev / vda1
                                   on
                                                                           40G
                                                                                     1 . 8G
      36G
                 5 % /
 devtmpfs
                                                                       1 . 9G
                                                                                         0
                  0 % / dev
   1.9G
 tmpfs
                                                                       1 . 9G
                                                                                         0
                  0 % / dev / shm
   1.9G
                                                                       1 . 9G
 tmpfs
                                                                                    472K
                  1 % / run
   1 . 9G
                                                                       1 . 9G
                                                                                         0
 tmpfs
   1 . 9G
                  0 % / sys / fs / cgroup
                                                                       379M
                                                                                      0
 tmpfs

      379M
      0 % / run / user / 0

      082e54b989 - ciq13 . cn - hangzhou . nas . aliyuncs . com :/

      0P
      0 1 . 0P
      0 % / mnt

                                                                                       1.
```

5 Back up data from ECS to NAS by using Windows Server Backup

This topic describes how to back up important data from a folder or the full disk on a Windows ECS instance to Alibaba Cloud NAS in a common method — the Windows Server Backup feature.

Windows Server Backup supports one-time manual data backup and scheduled backup. When necessary, you can conveniently restore data from the backup file.

Background

Alibaba Cloud NAS helps you design a separated compute and storage architecture that backs up persistent data to NAS while retaining computing tasks and memory states on your ECS instance. This way, even if your ECS instance goes down, your business can be quickly fail over to a new ECS instance, which seamlessly and continuously accesses the data stored on NAS. NAS is the best choice for separation of compute and storage with the support for data sharing among multiple ECS instances

In addition to data sharing, you can choose to regularly or occasionally synchronize data from your ECS instance to storage media besides cloud disks. This allows you not only to back up data, but also to recover data in the case of disasters like accidental deletion of the ECS instance and cloud disks. NAS allows you to back up important data as needed. Compared to cloud disk snapshots, which backs up data for the full disk, NAS provides more backup options. For example, you can choose to back up only certain directories rather than the full cloud disk.

Windows Server Backup

Windows Server Backup is a native feature of Windows that backs up and restores data for a full disk, folders, or files. According to *Microsoft - Overview of Windows Server Backup*, Windows Server Backup is a feature for your day-to-day backup and recovery needs.

You can use Windows Server Backup to back up a full server (all volumes), selected volumes, system state, or specific files or folders to another device (including other hard disks, tape libraries, or remote shared folders) and to recover the data from the storage media when necessary.
Install Windows Server Backup

Follow these steps to install Windows Server Backup in an Alibaba Cloud Windows image:

- 1. Click Start > Administrative Tools > Server Manager.
- 2. In Server Manager, click Features, and then click Add

Features.

🛼 Server Manager	
File Action View Help	
🗢 🔿 🖄 📅 🛛	
Server Manager (iZtgivl705nl81Z)	Features
Image: Storage Image: Storage	View the status of features installed
	Features Summary
	Seatures: 3 of 42 installed
	Windows PowerShell Integrated Scripting
	Telnet Client
	.NET Framework 3.5.1 Features
	.NET Framework 3.5.1

3. Select Windows Server Backup Features, and then click

Next.	Add Feature	s Wizard			
		Select Features			
	Features		Select (one or more features to install on th	is server.
	Confirmation	1	Feature	35:	
	Progress			SMTP Server	
	Results	1		SNMP Services Storage Manager for SANs Subsystem for UNIX-based Applica Telnet Client (Installed) Telnet Server TFTP Client Windows Biometric Framework Windows Internal Database Windows PowerShell Integrated So Windows Process Activation Servic Windows Server Backup Features Windows Server Migration Tools Windows System Resource Manag Windows TIFF IFilter WinRM IIS Extension WINS Server	itions cripting E ce
				WIREless LAIN Service XPS Viewer	
				A D Honor	
			More at	oout features	
					< Prev

4. Click Install.

After the installation is completed, you can click Start > Administrative Tools > Windows Server Backup to start the feature.

Use Windows Server Backup to back up data

Before using Windows Server Backup to back up data to NAS, you must create an SMB file system instance and mount it to your ECS instance.

Windows Server Backup supports Backup Once and the creation of Backup Schedule for scheduled backups.

Backup Once

With Backup Once, you can manually back up data (on a full disk or in selected folders) to NAS as needed.

1. Start Windows Server Backup, and click Backup Once.

The Backup Once Wizard window is displayed.

🔆 Windows Server Backup	_ 🗆 🗵
File Action View Help	
Windows Server Backup (Local)	Actions
	Windows Server Backup (Local)
	ackup Schedule
A No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup Once Wizard to per	😸 Backup Once
Messages (Activity from last week, double click on the message to see details)	b Recover
Time - Mecrose Description	Configure Performance Settings
I nine * Message Description	Connect To Another Server
	View
	🕜 Help
	_

2. Click Next.

3. On the Select Backup Configuration page, select Full Server or Custom (volumes or files).

If you select Custom, you must click Advanced Settings to set backup types and excluded files in the folders.

🗽 Backup Once Wizard	×
Select Iter	ns for Backup
Backup Options Select Backup Configur Select Items for Backup Specify Destination Type Confirmation Backup Progress	Select the items that you want to back up. Selecting bare metal recovery will provide you with the most options if you need to perform a recovery.

4. On the Specify Destination Type page, select Remote shared folder.

🗽 Backup Once Wizard	×
Specify De	estination Type
Backup Options Select Backup Configur Specify Destination Type Specify Remote Folder Confirmation Backup Progress	Choose the type of storage for the backup: Cucal drives Example: local disk (D:), DVD drive (E:) Remote shared folder Example: \\MyFileServer\SharedFolderName Choosing a storage location
	< Previous Next > Backup Cancel

5. On the Specify Remote Folder page, specify a location under the NAS SMB mount point, such as the backup folder.

🗽 Backup Once Wizard	×
Specify Re	emote Folder
 Backup Options Select Backup Configur Select Items for Backup Specify Destination Type Specify Remote Folder Confirmation Backup Progress 	Location: \\120. \myshare\backup Example: \\MyFileServer\SharedFolderName A folder named 'WindowsImageBackup' will be created inside the specified share to store the backup. Access control Do not inherit This option makes the backup accessible only for the user whose credentials are provided in the next step. Inherit This option makes the backup accessible to everybody who has access to the specified remote shared folder. Inherit The backed up data cannot be securely protected for this destination. More Information
	< Previous Next > Backup Cancel

6. On the Confirmation page, click Backup to start backup and wait for the backup process to be completed.

After backup is completed, you can go to the NAS backup folder and view the backed up content.



Backup Schedule

On the Backup Schedule page, you can configure automatic and regular Backup Once. This process is similar to that of Backup Once, expect that you must specify the backup time.(ui)



In the following procedure, steps that are the same as those in the Backup Once procedure are not described in details. Details for these steps can be found in the Backup Once section.

1. Start Windows Server Backup, and click Backup Schedule.

The Backup Schedule Wizard window is displayed.



2. On the Specify Backup Time page, set the backup frequency and running time.

🍇 Backup Schedule Wizar	d 🛛
Specify Ba	ackup Time
Getting Started Select Backup Configur Select Items for Backup Specify Backup Time Specify Destination Type Confirmation Summary	How often and when do you want to run backups? Once a day Select time of day: 9:00 PM Click an available time and then click Add to add it to the backup schedule. Available time: Scheduled time: 1:30 AM 2:00 AM 2:00 AM 3:00 AM 3:00 AM 3:00 AM 4:00 AM 5:00 AM 5:00 AM 5:00 AM 6:30 AM Learn about more scheduling options
	< Previous Next > Finish Cancel

3. On the Specify Destination Type page, select Back up to a shared network folder.



When you use a remote shared folder as the storage destination for a backup schedule, each backup overwrites the preceding one, so only the latest backup is retained.



4. Start the backup schedule. A backup task automatically runs within the time you specified.

Use Windows Server Backup to recover data

If your data is deleted or a file is overwritten, you can recover files previously backed up to NAS.

1. Start Windows Server Backup, and click Recover.

2. On the Getting Started page, select A backup stored on another location, and type the path of the backup folder configured previously.

😻 Windows Server Ba	ackup			_ 🗆 🗵
File Action View	Help			
🗢 🔿 🗖 🚺	1			
Vindows Serve	r Backup (Local)	<u> </u>	Actions	
You can perf	form a single backup c	r schedule a regular backup using this application	Windows Server Bac	:kup (Local) 🔹
		solicade a regalar backap acing a lo applicadorn	Backup Schedule	
🛕 No backup has be	een configured for this comput	er. Use the Backup Schedule Wizard or the Backup Once Wizard to pe	Backup Once	-
Messages (Activity fro	om last week, double click	on the message to see details)	Recover	
Time 👻	Recovery Wizard		×	ance Settings
3/7/2018 2:55 PM	1			er Server
	Getting Sta	arted		4
Status Last Backup Status: ③ Successi Time: 3/7/201: ③ View details	Getting Started Specify Location Type Select Backup Location Select Backup Date Select Recovery Type Select Items to Recover Specify Recovery Opti Confirmation Recovery Progress	You can use this wizard to recover files, applications, volumes, or the syste backup that was created earlier. Where is the backup stored that you want to use for the recovery? This server (iZtgivl705nl812) A backup stored on another location To continue, click Next.	em state from a	
		More about recovering your server data	Cancel	
		A LICATORS INCAL > INCOMEN		

3. On the Specify Items to Recover page, select one or more files or folders to recover.

4. On the Specify Recovery Options page, type the location on your local device to save the recovered

data.	🗽 Recovery Wizard				
	Specify Re	ecovery Options			
	Getting Started Specify Location Type Specify Remote Folder Select Backup Date Select Recovery Type Select Items to Recover Confirmation Recovery Progress	Recovery destination Original location C:\Users\Administrator\Desktop Browse When this wizard finds items in the backup that are already in Create copies so that you have both versions Overwrite the existing versions with the recovered version Do not recover the items that already exist on the recover Security settings Restore access control list (ACL) permissions to the file or <t< th=""></t<>			

5. On the Confirmation page, click Recover to start data recovery and wait for the process to be completed.