ALIBABA CLOUD

Alibaba Cloud

云存储网关

User Guide (On-Premises)

Document Version: 20220214

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.File Gateway

1.1. Deploy an on-premises console for a file gateway

This topic describes how to deploy an on-premises console for a file gateway by using an image. You must download and install the image. Then, you must configure network settings and activate the file gateway.

Prerequisites

1. An Alibaba Cloud account is created and real-name verification is complete. For more information, see Create an Alibaba Cloud account.

   > **Note** We recommend that you log on to the CSG console as a RAM user. For more information, see Use RAM to implement account-based access control.

2. CSG is activated.

   When you log on to the for the first time, activate the CSG service as prompted.

3. An Alibaba Cloud AccessKey pair is created. You can log on to the User Management console to obtain your AccessKey pair.

Context

Cloud Storage Gateway (CSG) can be deployed in data centers. You can deploy an on-premises console for a file gateway on the following platforms: VMware vSphere, Hyper-V, and Kernel-based Virtual Machine (KVM). Before the deployment, you can download the corresponding gateway images in the CSG console to your computer.

> **Note**
> - OVA images V1.0.30 and later can be deployed only on web clients of vCenter V6.0 and later.
> - Images downloaded from the CSG console cannot be imported to ECS instances.

Hardware requirements for virtual machines

The virtual machine where the on-premises file gateway is deployed must meet the following requirements:

- The virtual machine has four vCPUs.
- The virtual machine has at least 8 GB of memory resources.
- The virtual machine has at least 100 GB of disk space. The disk space is used to install a CSG image and store system data.
- We recommend that you use thick-provisioned cache disks on the virtual machine to optimize I/O performance. The size of each cache disk must be 40 GB or larger.

Installation methods

Installation methods and installation files vary depending on the hypervisor. You can obtain an installation file when you create an on-premises file gateway.

Hypervisor	Supported installation method	Installation file format
VMware vSphere	Import an OVA image to VMware.	ova
KVM	Open the virt-manager and use the QCOW2 file.	qcow2
Hyper-V	Import a VHD file to Hyper-V.	vhd

Step 1: Download an image

1. Log on to the CSG console.
2. Select the region where you want to create a file gateway.
3. In the left-side navigation pane, click **Gateways**. On the Current Gateway Cluster page, select the gateway cluster and click **Create**.

   If you do not have a gateway cluster, click **Create Gateway Cluster** on the **Overview** page to create a gateway cluster.
4. On the **Basic Information** page, set the following parameters and click **Next**.

Parameter	Description
Name	Specify a name for the gateway. The name must be 1 to 60 characters in length and can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter.
Location	Select a place where you want to deploy the gateway. In this example, select **On-premises**.
Category	Select the category of the gateway. In this example, select **Storage Gateway**.
Type	Select the type of the gateway. In this example, select **File Gateway**.

5. In the **Billing Information** step, set the parameters and click **Next**. The following table describes the parameters.

Parameter	Description
Billing Method	The method that is used by the system to calculate fees for the gateway. Valid values: **Pay-as-you-go** and **Subscription**. For more information, see Billable items and billing methods. If you select **Subscription**, you are redirected to the Cloud Storage Gateway (Subscription) page after you create the file gateway. Complete the payment as prompted. For more information, see Purchase a gateway.
Expiration Policy	Select an expiration policy for the gateway. Valid values: **Switch to Pay-as-you-go** and **Release**.

6. On the **Image Download** tab, download the required image to your on-premises machine.

Step 2: Install the image

After you download the image, you can use it to deploy an on-premises console for the file gateway.

Step 3: Configure network settings

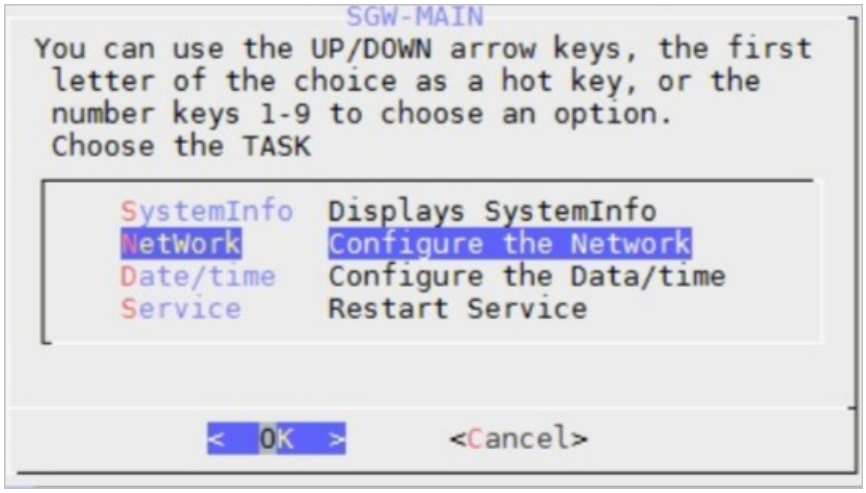
After you install the gateway image, you can configure the gateway IP address in the command-line interface (CLI) of the gateway.

1. Start the on-premises console of the file gateway, and open the Linux terminal of the virtual machine.
2. Enter your username and password to log on to the gateway CLI.

   The default username is root and the default password is Alibaba#sgw#1030.
3. Select a language.

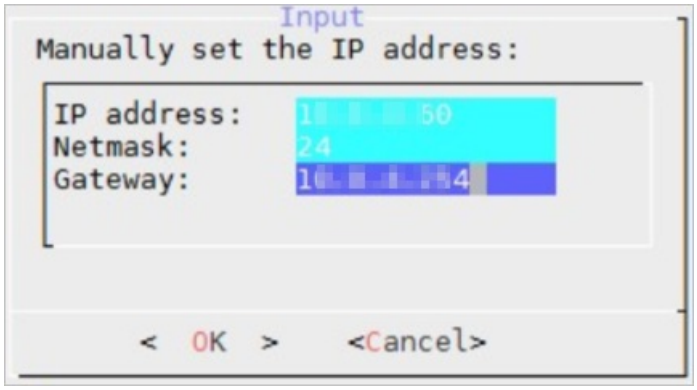
   The virtual machine may not support Chinese characters. We recommend that you select English for further configurations.

4. Select **Configure the Network** to configure network settings.

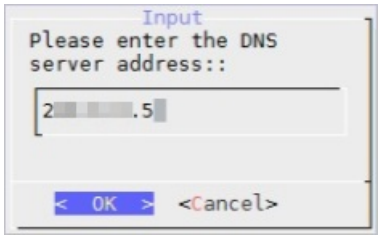


i. Select **use static ip address** and configure the IP address.

> **Note** Valid values of Netmask: 1 to 32. For example, if the subnet mask is 255.255.255.0, enter 24.

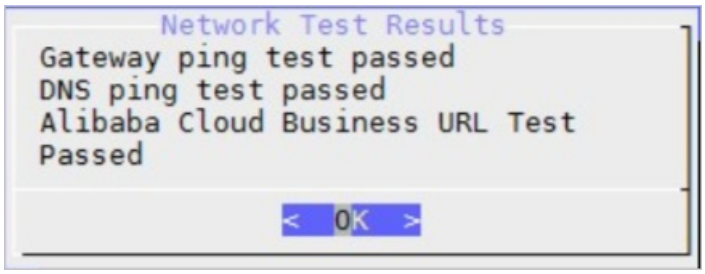


ii. Select **config dns** and enter the Domain Name System (DNS) server IP address.



iii. Select **network test** and check the network configuration result.

The following message indicates that the network settings have been configured.



5. Select **Configure the Date/time** and configure the Network Time Protocol (NTP) server.

   By default, the Alibaba Cloud NTP server at ntp.aliyun.com is used. You can also select **manual input time**. The time must be synchronized with that of Alibaba Cloud.

Step 4: Activate the gateway

1. Log on to the CSG console.
2. Activate the file gateway.

- (Recommended) Method 1
  a. Find the file gateway that you want to activate, and click **Activate Gateway** in the Actions column.
  b. In the **Activate Gateway** dialog box, set the following parameters, and click **Activate**.
     - **Gateway IP address**: Enter the IP address of the file gateway.

       > **Note**
       > - Make sure that your browser can connect to the gateway IP address.
       > - The gateway IP address can be the private IP address of your data center.
       > - The gateway IP address does not require Internet access.

     - **Username**: Specify the username used to log on to the on-premises console of the file gateway.
     - **Password**: Specify the password used to log on to the on-premises console of the file gateway.
     - **Confirm Password**: Confirm the password that you have specified.
  c. Open your browser, and enter `https://<IP address of the target file gateway>` in the address bar to visit the on-premises console of the file gateway.
  d. In the dialog box that appears, enter your username and password.

     > **Note** If this is your first time to log on to the on-premises console of the file gateway, you must enter the AccessKey pair of your Alibaba Cloud account. You can log on to the User Management console to obtain your AccessKey pair.

- Method 2
  a. Find the file gateway that you want to activate. Click **Download Certificate** in the Actions column to download the certificate to your computer.
  b. Open your browser, and enter `https://<IP address of the target file gateway>` in the address bar to connect to the on-premises console of the file gateway.

c. On the **Cloud Storage Gateway Register** page, set the following parameters, and click **OK**.
   - **Upload Certificate**: Click **Upload Certificate** to select the certificate that you want to upload.
   - **Access Key ID**: Enter the AccessKey ID of your Alibaba Cloud account.
   - **Access Key Secret**: Enter the AccessKey secret of your Alibaba Cloud account.
   - **Username**: Specify the username used to log on to the on-premises console of the file gateway.
   - **Password**: Specify the password used to log on to the on-premises console of the file gateway.
   - **Confirm Password**: Confirm the password that you have specified.

   > **Note** You can log on to the User Management console to obtain your AccessKey pair.

d. After you activate the file gateway, log on to the on-premises console of the file gateway.

Related operations

On the **Gateway Clusters** page of the on-premises console of the file gateway, you can also perform the following operations.

Operation	Description
Delete a gateway	Find the file gateway and choose **More > Delete** in the Actions column. **Note** You can delete only pay-as-you-go file gateways.
Rename a file gateway	Find the file gateway and click **Edit** in the Actions column to rename the gateway.
Switch to subscription	After you create a pay-as-you-go gateway, you can switch the billing method from pay-as-you-go to subscription. Find the file gateway and choose **More > Switch to Subscription** in the Actions column. You are then redirected to the buy page. Select the specification as needed. For more information, see Switch the billing method from pay-as-you-go to subscription.
Reset the password	After you deploy the on-premises console of the file gateway, you can reset the password in the console. To reset the password, find the file gateway and choose **More > Reset password**.

1.2. Manage cloud resources

This topic describes how to manage cloud resources in the local file gateway console, including binding, unbinding, and speed tests.

Prerequisites

1. You have deployed the local file gateway console. For more information, see Deploy an on-premises console for a file gateway.
2. An Object Storage Service (OSS) bucket is created. For more information, see Create buckets.

> **Note**
> - CSG supports Standard, Infrequent Access (IA), and Archive OSS buckets.
> - If you request to read an archived file from a gateway for which the archive feature is disabled, the system sends a request to restore the file at the same time. No error message is returned. However, latency may exist before you can read the archived file.

Bind a cloud resource

1. Open your browser, enter `https://<IP address of the file gateway>` in the address bar, and then press Enter.
2. In the dialog box that appears, enter your username and password, and then click **OK**.
3. On the **Cloud Resources** page, click **Bind**.
4. In the **Bind Cloud Resource** dialog box, set the parameters. The following table describes the parameters.

Parameter	Description
Resource Name	Enter the name of the cloud resource that you want to bind.
Cross-region Binding	Set the parameter. ○ If you select **Yes**, you can access a bucket that resides in a different region from the specified gateway. ○ If you select **No**, you can access only a bucket that resides in the same region as the specified file gateway. **Note** The time zone of the on-premises file gateway must be the same as the time zone of the OSS bucket.
Region	Select a region where the bucket resides.
Bucket Name	Select a bucket that you want to bind to the file gateway.
Use SSL	If you select **Yes**, you can connect to the OSS bucket over SSL.

5. Click **OK**.

Other supported operations

On the **Cloud Resources** page, you can also perform the following operations.

Operation	Description

Operation	Description
Unbind a cloud resource	Find the target cloud resource and click **Unbind**. After the cloud resource is unbound, its data is retained. You can access and delete the data in the Alibaba Cloud Object Storage Service (OOS) console.
Test a cache disk	Find the target cloud resource and click **Speed Test** to test the upload and download speed of cloud resources.

What's next

- Create an NFS share
- Create an SMB share

1.3. Add disks

This topic describes how to add disks to the local file gateway cache on the virtualization platform.

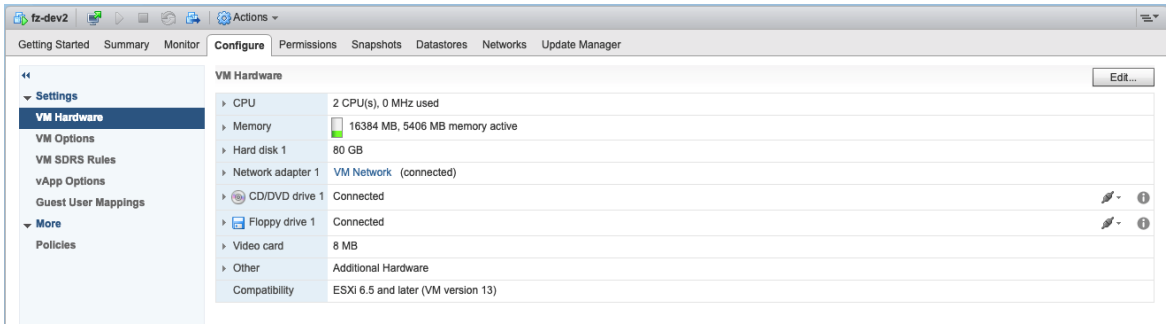
Context

To deploy a local file gateway in the cache mode, you must add a disk to the deployment platforms such as VMware vSphere and Hyper-V. After a disk is added, you can configure available cache disks for the corresponding file gateway in the Cloud Storage Gateway (CSG) console or the local file gateway console.

> **Note** The minimum cache disk capacity supported by the file gateway is 40 GB. Therefore, the new disk capacity cannot be less than 40 GB. Otherwise, the file gateway cannot recognize the new disk.

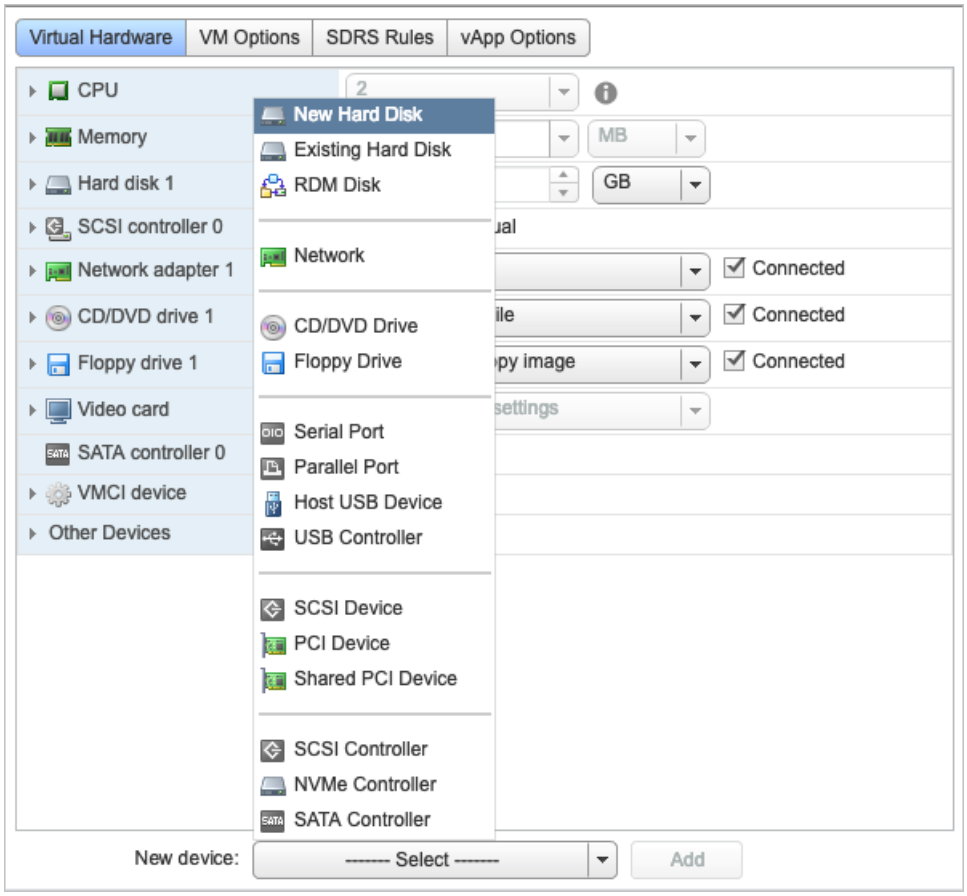
Add disks to VMware vSphere

1. Log on to the VMware vSphere virtualization platform.
2. On the **Configure** tab, choose **Settings > VM Hardware**. Click **Edit**.



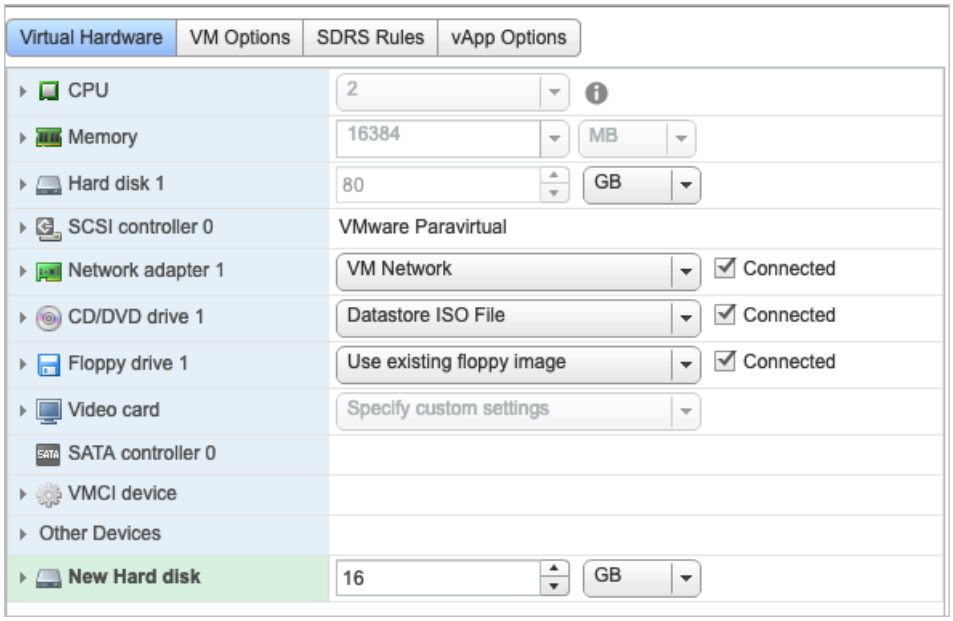
3. On the **Virtual Hardware** tab, from the **New device** list, select **New Hard Disk**. Click **Add**.

   After the disk is added, a **New Hard disk** folder appears.



4. Set the size of the new hard disk.

   We recommend that you use thick provisioning to deploy the disk. Expand the **New hard disk** folder. Set the **Type** to **Thick Provision Lazy Zeroed** or **Thick Provision Eager Zeroed** to achieve better I/O performance.

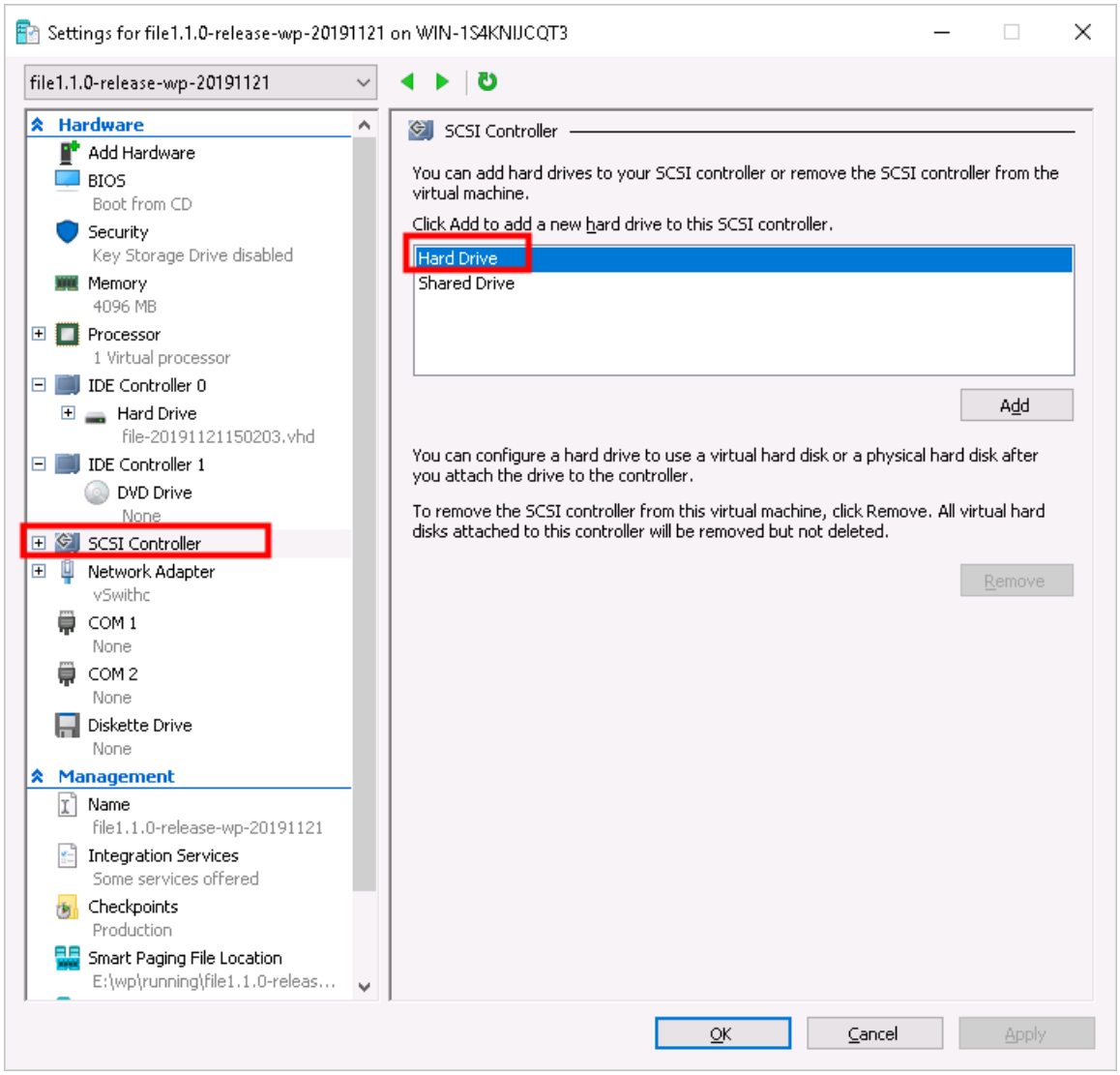


Note In this example, only one hard disk is added. You can add multiple disks based on your needs.

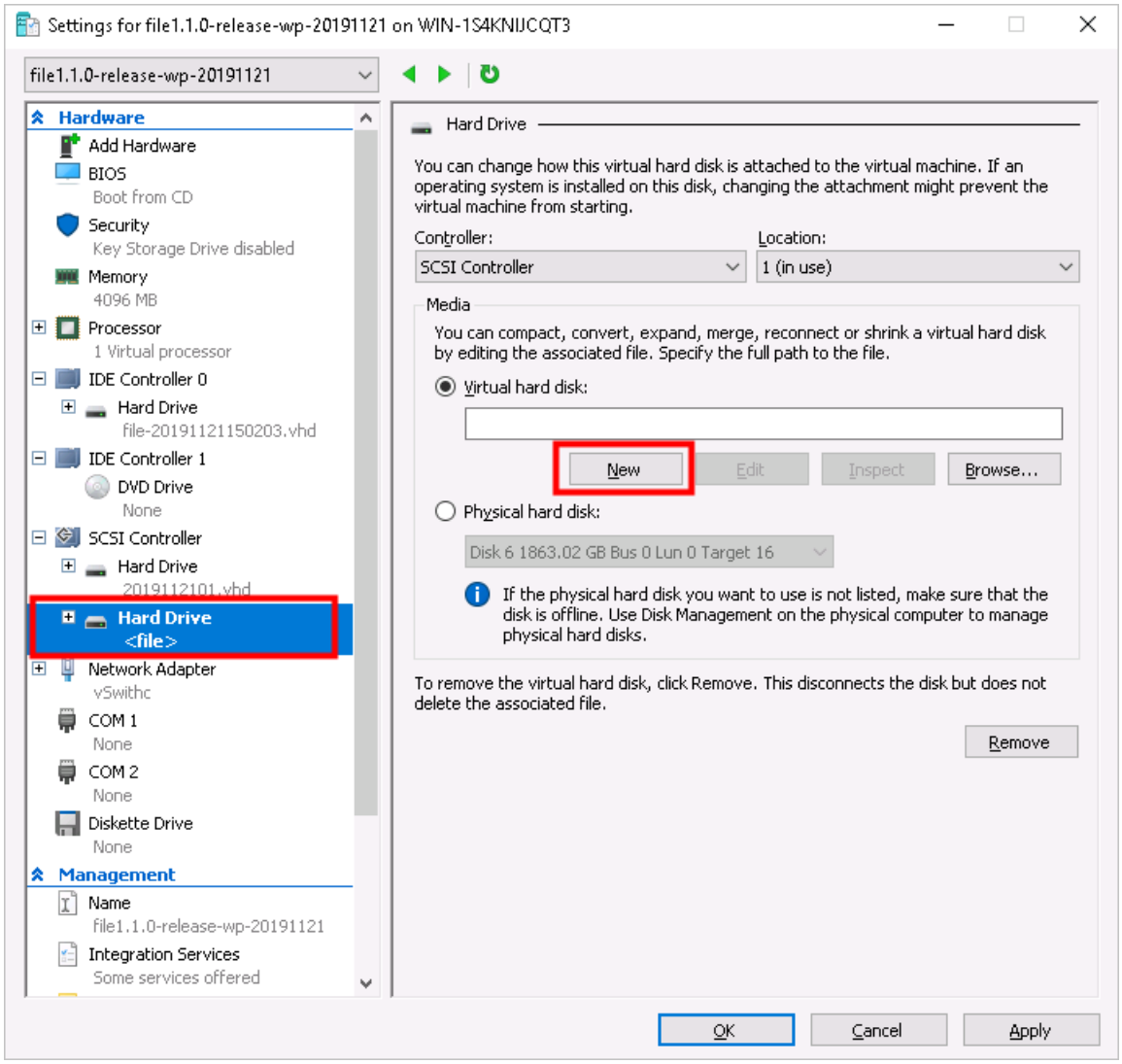
Add disks to Hyper-V

The host must be restarted if you add disks by using an IDE controller. However, you do not need to restart the host if you add disks by using a SCSI controller. We recommend that you use a SCSI controller to add disks.

1. Log on to the Hyper-V virtualization platform.
2. Choose **Hardware > SCSI Controller**, and select **Hard Drive**. Click **Add**.



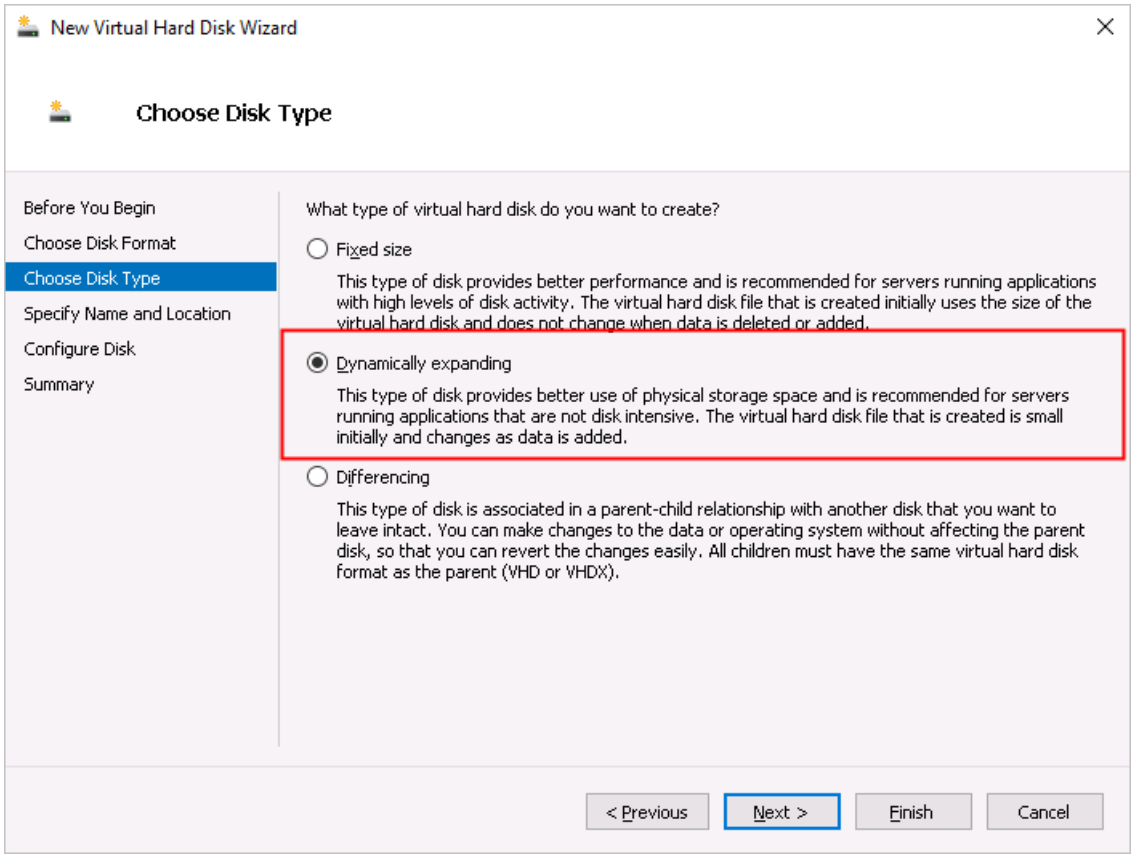
3. On the **Hard Drive** tab, select **Virtual Hard Disk**, and click **New**.



4. Follow the new virtual hard disk wizard to add the hard disk.

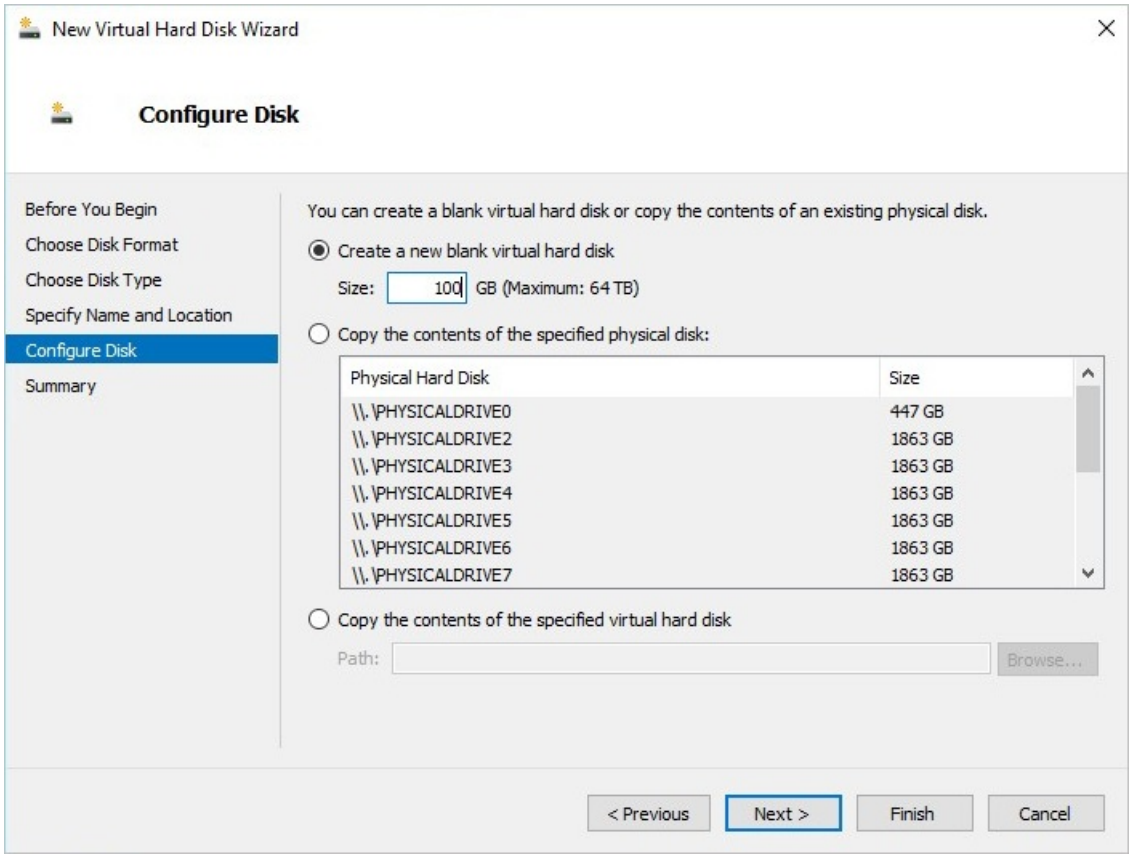
   Note the following settings:

   - On the **Choose Disk Type** tab, select **Dynamically expanding**.



- On the **Configure Disk** tab, select **Create a new blank virtual hard disk**, and set the disk size.

We recommend that the size of a single cache disk to be larger than 40 GB for higher I/O throughput. For better local access performance, see File gateways.



5. Return to the **Hard Drive** tab, and click **Apply**.

> **Note** In this example, only one hard disk is added. You can add multiple disks based on your needs.

1.4. Manage cache disks

Cloud Storage Gateway provides a cache disk for each shared path. This topic describes how to manage the cache in the local file gateway console, including adding cache disks, deleting cache disks, and testing the speed of cache disks.

Prerequisites

1. You have deployed the local file gateway console. For more information, see Deploy an on-premises console for a file gateway.
2. You have added cache disks. For more information, see Add disks.

Context

Each file gateway share has a unique cache disk attached to it. To create multiple shares, you must create the same number of cache disks for the shares. You can upload data in a share to an Object Storage Service (OSS) bucket by using a cache disk. You can also download data from OSS buckets to a local device by using a cache disk.

Add a cache disk

1. Open your browser, enter `https://<IP address of the file gateway>` in the address bar, and then press Enter.
2. In the dialog box that appears, enter your username and password, and then click **OK**.
3. In the left-side navigation pane, click **Caches**. On the Caches page, click **Create**.
4. In the **Create Cache** dialog box, set the following parameters:
   - **Disk**: Click **Select**, and then select an available disk in the Select disk dialog box.

     Disks are available only after you add the disks on the deployment platform. For more information, see Add disks.
   - **File System**: This parameter is optional. If you want to reuse data on the cache disk, select this check box. If you delete a share by accident, you can recreate the share and use this feature to restore data.

     > **Note** If you select the File System check box but no file system exists on the cache disk, the cache disk fails to be created.
5. Click **OK**.

Other supported operations

On the **Caches** page, you can also perform the following operations.

Operation	Description
Delete a cache disk	Find the target cache disk, and then click **Delete** to delete the cache disk.
Test a cache disk	Find the target cache disk, and then click **Speed Test** to test the performance of the cache disk, including sequential I/O tests with 1 MB and 4 KB block sizes.

What's next

- Create an NFS share
- Create an SMB share

1.5. Manage NFS shares

This topic describes how to manage Network File System (NFS) shares in the on-premises file gateway console, including how to create, delete, close, and modify NFS shares.

Prerequisites

1. A cache disk is added to the gateway. For more information, see Add a cache disk.
2. Cloud resources are attached to the gateway. For more information, see Bind a cloud resource.

Context

NFS allows computers in a network to share resources over TCP/IP communications. If NFS is used, the local client directly reads files from and writes files to the remote NFS server.

Cloud Storage Gateway (CSG) operates in a similar manner to an NFS server and provides the file sharing service. Before you can use a shared directory, you must create a shared directory on the CSG, specify the users that are allowed to access the shared directory, and configure access permissions.

Install an NFS client

Before you create an NFS share, you must install an NFS client on the client.

1. Log on to the client.
2. Use the following command to install the NFS client.

   This topic describes how to install NFS clients in Ubuntu and CentOS. For more information about how to install NFS clients in other operating systems, see the official NFS documentation.

   - If you are using Ubuntu, run the following command.

     ```
     apt-get install nfs-common
     ```

   - If you are using CentOS, run the following command.

     ```
     yum install -y nfs-utils
     ```

Create an NFS share

1. Open your browser, enter `https://<IP address of the file gateway>` in the address bar, and then press Enter.
2. In the dialog box that appears, enter your username and password, and then click **OK**.
3. Click **NFS**, and click **Create**.
4. In the **Create NFS Share** dialog box, set the parameters and click **OK**. The following table describes the parameters.

Parameter	Description
Share Name	The virtual mount point of the NFS share that you want to create. You can use this share name to mount an NFSv4 share. If you want to mount an NFSv3 share, you must run the `showmount -e <IP address of the gateway>` command to obtain the mount point.
Read/Write Client IPs	The IP address or CIDR block of the client that can read data from or write data to the NFS gateway. Example: 192.168.10.10 or 192.168.0.0/24. You can enter multiple IP addresses or CIDR blocks.
Read-only Client IPs	The IP address or CIDR block of the client that can only read data from the NFS gateway. Example: 192.168.10.10 or 192.168.0.0/24. You can enter multiple IP addresses or CIDR blocks.

Parameter	Description
User Mapping	Maps an NFS client user to an NFS server user. This parameter is available only if you set **Protocol** to **NFS**. ○ none: specifies no mapping relationship between an NFS client user and the nobody user of the NFS server. ○ root_squash: restricts the use of root user permissions. NFS clients that use the root identity are mapped to the nobody user on the NFS server. ○ all_squash: restricts the use of all user permissions. NFS clients are mapped to the nobody user of the NFS server regardless of the identity that is used by the clients. ○ all_anonymous: restricts the use of all user permissions. NFS clients are mapped to the anonymous user of the NFS server regardless of the identity that is used by the clients.
Archive	This parameter is available only if you set the Protocol parameter to NFS and the User Mapping parameter to none. ○ If you select **Yes**, the archive feature is enabled. You can archive and restore files in a share by using the archive management tool. ○ If you select **No**, the archive feature is disabled. You cannot use the archive management tool to manage files. If you request to read data from an archived file, the system sends a request to restore the file at the same time. No error message is returned. However, latency may exist before you can read the archived file. **Note** Basic file gateways do not support the **archive** feature.
Enable	Specify whether to enable the specified NFS share. If you do not want to use the NFS share, you can select **No** to disable the NFS share.
Mode	Valid values: Cache Mode and Replication Mode. ○ **Replication Mode**: In this mode, two backups are created for all data. One backup is stored on the on-premises cache disk and the other backup is stored in the associated OSS bucket. ○ **Cache Mode**: In this mode, the backup that is stored on the on-premises cache disk contains only metadata and the user data that is frequently accessed. The backup that is stored in the OSS bucket contains all data.

Parameter	Description
Reverse Sync	Specifies whether to synchronize metadata that is stored in the OSS bucket to the on-premises cache disk. You can use this feature in scenarios in which disaster recovery, data restoration, and data sharing are required. **Note** In a reverse synchronization process, the system scans all objects in the bucket. If the number of objects exceeds the limit, you are charged when you call the OSS API. For more information, see OSS pricing.
Encrypt	Valid values:**None** and **Server-side Encryption**. If you select **Server-side Encryption**, you must set the **Key ID** parameter. You can create a key in the KMS console. For more information, see Create a CMK. After you enable the OSS server-side encryption feature, you can bring your own key (BYOK). The system supports keys that are imported from Key Management Service (KMS). After you enable the OSS server-side encryption feature, the system uses the imported key to encrypt files that are uploaded to OSS from the shared directory. You can call the GetObject API operation to check whether the specified file is encrypted. If the value of the x-oss-server-side-encryption field is KMS and the value of the x-oss-server-side-encryption-key-id field is the key ID in the response header, the file is encrypted. **Note** ◦ Only the users in the whitelist can use this feature. ◦ If you create a key in the KMS console, you must select the region in which the OSS bucket resides.
Bucket Name	Select an existing bucket.
Subdirectory	Enter a subdirectory of the bucket. The Subdirectory field supports only letters and digits. **Note** In version 1.0.38 and later, you can map the root directory of a file system to a subdirectory of a bucket. This way, you can isolate file access requests. You can specify an existing subdirectory or a subdirectory that does not exist in the bucket. After you create a share, the specified subdirectory serves as the root directory, and stores all related files and directories.

Parameter	Description
Use Metadata	Specifies whether to use metadata disks. If you use metadata disks, data disks are separated from metadata disks, and metadata disks are used to store the metadata of shared directories. ○ If you select **Yes**, you must set the **Metadata** and **Data** parameters. ○ If you select **No**, you must set the **Cache Disk** parameter. **Note** Only the users in the whitelist can use this feature.
Ignore Deletions	If you select Yes, the data that is deleted from the on-premises cache disk is not deleted from the OSS bucket. The OSS bucket retains all data.
NFS V4 Optimization	Specifies whether to improve the upload efficiency of NFSv4 files. If you select Yes, you cannot mount an NFSv3 file system on your on-premises host.
Sync Latency	Specify a synchronization latency to upload modified and closed files. The **Sync Latency** feature prevents OSS file fragments that are caused by frequent on-premises modifications. Default value: 5. Maximum value: 120. Unit: seconds.
Max Write Speed	Specify the maximum write speed. Valid values: 0 to 1280. Unit: MB/s. Default value: 0. The value 0 indicates that the write speed is unlimited.
Max Upload Speed	Specify the maximum upload speed. Valid values: 0 to 1280. Unit: MB/s. Default value: 0. The value 0 indicates that the upload speed is not limited. **Note** When you customize the maximum write speed and upload speed, make sure that the maximum upload speed is greater than or equal to the maximum write speed.
Fragmentation Optimization	Specifies whether to optimize the performance for applications that frequently and randomly read and write small amounts of data. You can enable this feature based on your business requirements.
Upload Optimization	If you select Yes, cached data is cleared in real time. You can enable this feature if you synchronize only backups to the cloud.

5. Click **OK**.

Other supported operations

On the **NFS** page, you can perform the following operations.

Operation	Description

Operation	Description
Disable NFS sharing	On the **NFS** page, you can click the button on the upper-left side of the page to disable NFS sharing. If you want to disable a single NFS share, you can use the following method. On the **NFS** page, find the NFS share that you want to disable. Click **Settings**, and set **Enabled** to **No**.
Delete an NFS share	On the **NFS** page, find the NFS share that you want to delete, and click **Delete** to delete the NFS share. **Note** If the NFS share is mounted on a client, it takes a short period of time for the system to unmount the mount point from the client after the share is deleted. During this period, if you create an NFS share with the same ID, the mount point fails to be unmounted from the client. Therefore, after you delete an NFS share, run the `df -h` command to confirm that the file is successfully unmounted before you perform other operations.
Modify an NFS share	On the **NFS** page, find the NFS share that you want to modify, and click **Settings** or **Advanced Settings** to modify the NFS share.

What's next

Access an NFS share directory

1.6. Manage SMB shares

This topic describes how to manage Server Message Block (SMB) shares in the on-premises file gateway console. You can create, delete, disable, and modify SMB shares. You can also configure AD or LDAP and add SMB users.

Prerequisites

1. A cache disk is added to the gateway. For more information, see Add a cache disk.
2. Cloud resources are bound. For more information, see Bind a cloud resource.

Context

SMB is a network protocol that facilitates network communication between servers and clients or between network nodes. You can use this protocol to share files. SMB requires both a client and a server.

Cloud Storage Gateway (CSG) acts as an SMB server and provides the file sharing service. When you access CSG from a Windows-based client, CSG receives a request from the client and returns a response.

To use the SMB service, you must configure a share directory in the CSG console, create an SMB user, and specify user permissions.

Create an SMB share

1. Open your browser, enter `https://<IP address of the file gateway>` in the address bar, and then press Enter.

2. In the dialog box that appears, enter your username and password, and then click **OK**.
3. On the **SMB** page, click **Create** in the upper-right corner.
4. In the **Create SMB Share** dialog box, set the following parameters.

Parameter	Description
Share Name	The name of the SMB share.
Read-only Users	The list of users who have read-only access to the SMB share.
Read/Write Users	The list of users who have read and write access to the SMB share.
Enable	Specify whether to enable SMB sharing. If you do not want to enable SMB sharing, you can select **No** to disable SMB sharing.
Browsable	Specify whether the SMB share can be discovered by network neighbors.
Mode	Valid values: Cache Mode and Replication Mode. ○ **Replication Mode**: In this mode, two backups of all data are created. One is stored in the on-premises cache disk and the other is stored in the OSS bucket. ○ **Cache Mode**: In this mode, the backup stored in the on-premises cache disk contains only metadata and user data that is frequently accessed. The backup stored in the OSS bucket contains all data.
Reverse Sync	Specify whether to synchronize metadata stored in the OSS bucket to the on-premises cache disk. This feature is suitable for disaster recovery, data restoration, and data sharing scenarios. **Note** During a remote sync process, the system scans all objects in the bucket. If the number of objects is large, you are charged for calling the OSS API. For more information, see Pricing of OSS.

Parameter	Description
Encryption Type	You can select **None** or **Server-side Encryption**. If you select **Server-side Encryption**, you must also set the **ID** parameter. You can log on to the KMS console and create a key. For more information, see Create a CMK. After you enable OSS server-side encryption, you can bring your own key (BYOK). The system supports keys imported from Key Management Service (KMS). After OSS server-side encryption is enabled, the system uses the imported key to encrypt files uploaded to OSS by using a share directory. You can call the GetObject operation to check whether the specified file is encrypted. In the response header, if the x-oss-server-side-encryption field value is KMS and the x-oss-server-side-encryption-key-id field value is the key ID, the file is encrypted. **Note** ○ This feature is available only to selected users. ○ When you create a key in the KMS console, you must select the same region as the OSS bucket.
Bucket Name	Select an existing bucket.
Subdirectory	Specify a subdirectory of the bucket. The subdirectory name can contain only letters and digits. **Note** File gateways V1.0.38 and later allow you to map the root directory of a file system to a subdirectory of a bucket. This enables separate file access between users. You can specify an existing subdirectory or a subdirectory that does not exist in the bucket. After you create a share, the specified subdirectory serves as the root directory, and stores all related files and directories.
Cache Use	Specifies whether to enable metadata disks. If you use metadata disks, data disks are separated from metadata disks, and metadata disks are used to store metadata of share directories. ○ If you select **Yes**, you must set the **Metadata** and **Data** parameters. ○ If you select **No**, you must set the **Cache Disk** parameter. **Note** This feature is available only to selected users.
Ignore Deletion	During the data synchronization process, the OSS bucket ignores all delete operations. The backup stored in the OSS bucket contains all data.

Parameter	Description
Sync Latency	You can specify a synchronization latency to upload files that you have modified and closed. The **Sync Latency** feature avoids OSS file fragmentation caused by frequent on-premises modifications. The default value is 5 seconds and the maximum value is 120 seconds.
Write Speed Limit	Specify the maximum speed of writing data. Valid values: 0 to 1280. Unit: MB/s. Default value: 0, which indicates that the upload rate is not limited.
Upload Speed Limit	Specify the maximum speed of uploading data. Valid values: 0 to 1280. Unit: MB/s. Default value: 0, which indicates that the upload rate is not limited. **Note** When you customize the maximum write speed and upload speed, make sure that the maximum upload speed is not lower than the maximum write speed.
Fragmentation Optimization	Specifies whether to optimize the performance for applications that frequently and randomly read and write small amounts of data. You can enable this feature based on your needs.
Upload Optimization	This feature releases cache in real time. You can enable this feature if you synchronize only backups to the cloud.

AD and LDAP

Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) are standard application protocols used to query and change directory information. Select the AD or LDAP service that you want to join and configure the settings.

- You can join an AD domain only after you complete the DNS settings.
- You can join either an AD or LDAP domain.
- The permissions of the current AD domain user, LDAP user, and on-premises user override each other and whichever configured last takes effect. After you join or leave an AD domain, or connect to or disconnect from an LDAP server, the user permissions configured in the CIFS share are automatically removed.
- The AD feature supports 64-bit Windows Server 2016 Datacenter and Windows Server 2012 R2 Datacenter.
- The LDAP feature supports 64-bit CentOS 7.4 with OpenLDAP 2.4.44.

Configure AD settings

1. Configure the DNS server.
   i. In the on-premises console of file gateways, click **About**.
   ii. In the **Network Configuration** section, click **Update DNS**.

iii. In the **Update DNS** dialog box, enter the IP addresses of DNS servers. Click **OK**.

In the **DNS server** field, specify the IP address of the AD server to resolve the AD domain name.

2. Join an AD domain.
   i. Choose **SMB > AD/LDAP**.
   ii. In the **Windows AD** section, click **Join AD**.
   iii. In the **Join AD** dialog box, set the following parameters. Click **OK**.
   - **Server IP Address**: Enter the IP address of the AD server.
   - **Username**: Enter the username of the administrator.
   - **Password**: Enter the password of the administrator.

   After the connection is established, the status of **Connected** under **Windows Active Directory (AD)** changes to **Yes**.

> **Note** After you join the AD domain, the on-premises user permissions configured in the SMB share are removed.

Configure LDAP

1. In the on-premises console of file gateways, choose **SMB > AD/LDAP**.
2. In the **LDAP** section, click **Join LDAP**.
3. In the **Connect LDAP Server** dialog box, set the following parameters and click **OK**.
   - **Server IP Address**: Enter the IP address of the LDAP server, which is the directory system agent.
   - **TLS Support**: Specify the method used by the system to communicate with the LDAP server.
   - **Base DN**: Specify the LDAP domain, for example, dc=iftdomain, or dc=ift.local.
   - **Root DN**: Specify the root DN, for example, cn=admin, dc=iftdomain, or dc=ift.local.
   - **Password**: Enter the password of the root directory.

   After the connection is established, the status of **Connected** under **Lightweight Directory Access Protocol (LDAP)** becomes **Yes**.

> **Note** After you join the LDAP domain, the on-premises user permissions configured in the SMB share are removed.

Add an SMB user

If you have not joined a domain, you can create an SMB user to access Cloud Storage Gateway.

- If you have joined an AD domain, you can view all AD users on the **SMB Users** page.
- If you have joined an LDAP domain, you can view all LDAP users that have a Samba password on the **SMB Users** page.
- If you have joined an LDAP domain but have not configured a Samba password, click **Create** to add a Samba password for the LDAP users on the **SMB user** page.

  We recommend that you specify the same password for both Samba and LDAP.

1. In the on-premises console of file gateways, choose **SMB > SMB Users**.

2. Click **Create**.
3. In the **Add SMB User** dialog box, set the name and password.
4. Click **OK**.

What to do next

On the **SMB** page, you can also perform the following operations.

Operation	Description
Disable an SMB share	On the **SMB** page, you can disable the toggle on the upper-left side of the page to disable NFS sharing. If you want to disable a single SMB share, you can use the following method. On the **SMB** page, find the NFS share. Click **Settings** and set **Enable** to **No**.
Delete an SMB share	On the **SMB Shares** tab, find the SMB share, and click **Delete**. **Note** After the SMB share is deleted, the Windows mount point or mapped network drive immediately becomes ineffective.
Modify an SMB share	On the **SMB Shares** tab, find the SMB share, and click **Settings** or **Advanced Settings**.
Cache Refresh	On the **SMB Shares** tab, find the SMB share, and click **Cache Refresh**.
Delete an SMB user	On the **SMB Shares** tab, find the SMB user, and click **Delete**.
Disable a connection	On the **AD/LDAP** tab, click **End Connection**.

What's next

Access SMB shares

1.7. Access shares

1.7.1. Access SMB shares

This topic describes how to access a local gateway from a client that is running Windows.

Prerequisites

You have created an Server Message Block (SMB) share. For more information, see Create an SMB share.

Context

To access a local gateway from a client that is running Windows, you must map the share as a network drive first. After you map the share, a network mapping is established between the local directory and the share. You can access the remote share in the same way as you access a local directory.

> **Note**
>
> - You can mount up to 16 SMB shares. The maximum number of SMB shares supported by different types of gateways varies depending on the CPU and memory. For more information, see Specifications.
> - The capacity of the mounted share equals the Object Storage Service (OSS) bucket capacity. The displayed capacity 256 TB is the maximum capacity of the file system. Currently, the capacities of OSS buckets are not limited.
> - For version 1.0.35 and later, if you have not added any users, you can access the SMB share directory as a public user by default. However, if you have added users, you must grant the read/write or read-only permission to a user before the user can access the SMB share directory.
> - After each time you change SMB user permissions, you need to clear the user information saved on the client when you mount the share. You can use the `net use/delete < share path >` command to clear client information in Windows. You do not need to restart the client computer.

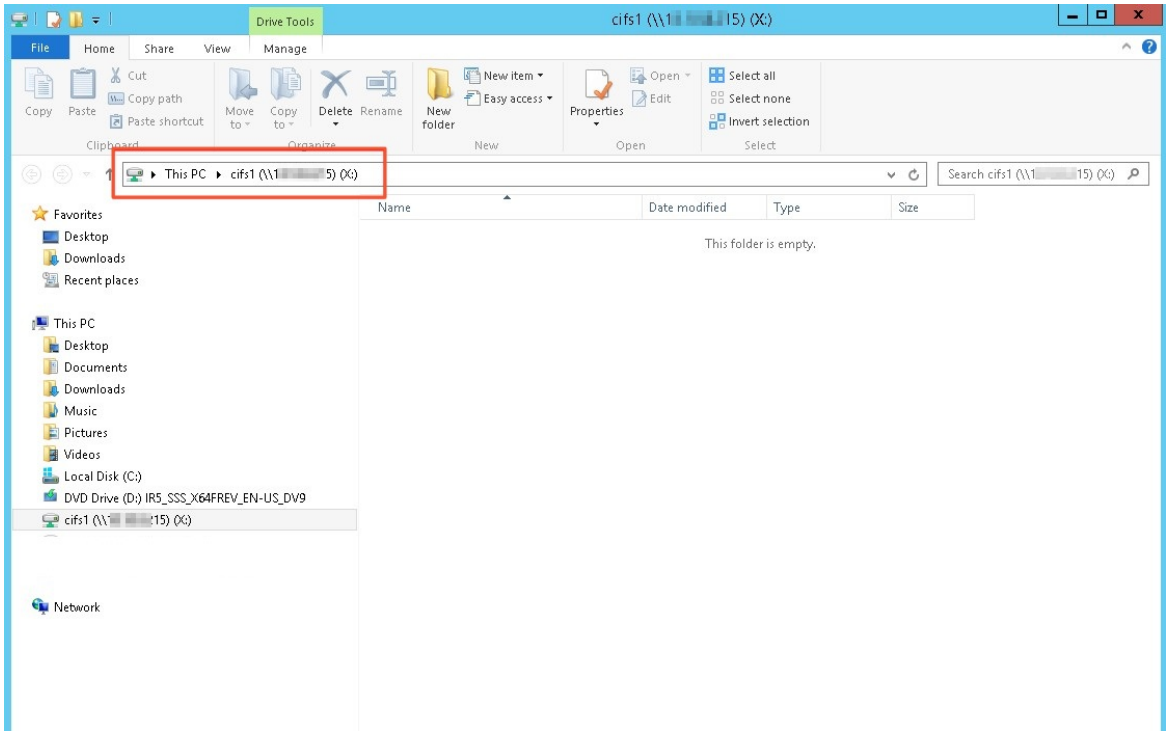
Procedure

1. Log on to the Windows operating system of a local computer.
2. Open **This PC** and select **Map network drive**.
3. Select a drive letter from the drop-down list and enter the mount point into the **Folder** field.

   The mount point includes the IP address of the gateway and the name of the SMB share. Replace them with the actual IP address and share name. To query the mount point, navigate to the **Share** page of the gateway in the Cloud Storage Gateway console.
4. Click **OK** and enter the Common Internet File System (CIFS) username and password.

   If you have joined an Active Directory (AD) domain, add the domain before the username. The format is <domain><username>.
5. After you mount the SMB share, verify the result.

If the following or similar information appears, it indicates that the SMB share is mounted to the local directory.



6. Access the SMB share.

   After the SMB share is mounted to the local directory, you can access the remote share in the same way as you access a local directory. If you have the write permission, you can write data to the SMB share. If you have the read-only permission, then you can only read data from the SMB share.

   > **Note** Shares are synchronized with the associated OSS buckets. Operations performed on shares are synchronized to the associated OSS buckets.

1.7.2. Access an NFS share directory

This topic describes how to access an NFS share directory by using a Cloud Storage Gateway (CSG) agent on a Linux-based client.

Prerequisites

An NFS share is created. For more information, see Install an NFS client.

Context

Before you can access an NFS share from a Linux-based client, you must mount the share on the on-premises file directory of the client. After the share is mounted, directory mappings are established between the share directory and the on-premises directory. You can access the share directory in the same way as you access an on-premises directory.

Procedure

1. Log on to the on-premises Linux-based client.
2. Mount the NFS share to the on-premises directory of the client.

i. Run the following command to mount the share directory:

```
mount.nfs 192.168.0.0:/shares local-directory
```

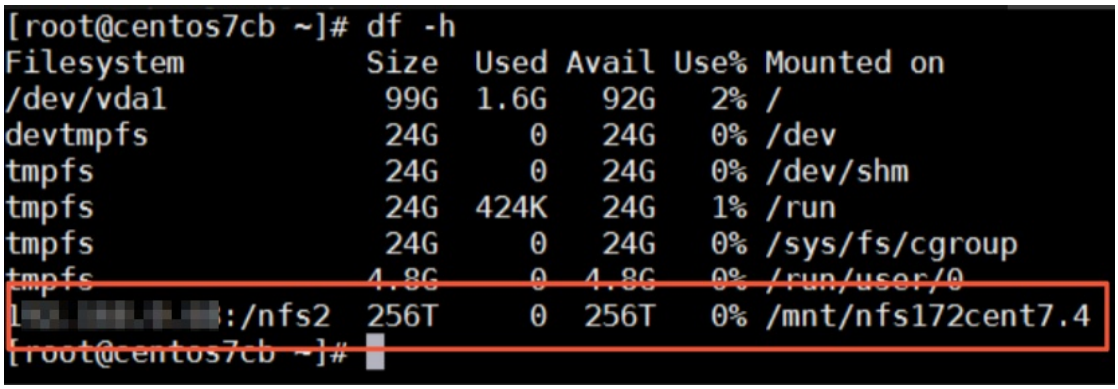
- 192.168.0.0:/shares: the mount target of the gateway, including the IP address and the share directory name. Specify this parameter based on the actual scenario. To check the mount target of the gateway, log on to the CSG console and navigate to the **Share** page of the gateway.
- local-directory: the on-premises directory of the CSG client. Specify a file directory that supports read and write operations. You cannot specify a directory that does not exist.

> **Note** For example, assume that your file gateway version is earlier than 1.0.35, and you have mounted shares by using the NFSv3 protocol. You must run the `showmount -e <gateway IP address>` command to query the mount path by performing the following steps:
>
> a. Run the following command to query the mount path, for example, 192.168.0.0:/shares.
>
> ```
> showmount -e <gateway IP address>
> ```
>
> b. Run the following command to mount the share directory:
>
> ```
> mount -t nfs -o vers=3,proto=tcp,nolock,noacl,sync 192.168.0.0:/shares local-directory
> ```

ii. Run the `df -h` command to check the result.

If the following information appears, the share directory is mounted on the on-premises directory of the client.

> **Note** The capacity of the mounted share is equal to the capacity of the Object Storage Service (OSS) bucket. The displayed capacity 256 TB is the maximum capacity of the file system. OSS storage capacity is not limited.



3. Access the share directory.

After a share directory is mounted on the on-premises directory of your client, you can access the share directory in the same way as you access an on-premises directory. If you have write permissions, you can write data to the share directory. If you have read-only permissions, you can only read data from the share directory.

> **Note** A share directory is synchronized with its associated OSS bucket. If you perform operations to a share directory, changes occur to the associated OSS bucket too.

Enable automatic mounting of a share directory

If you mount a share directory on an ECS instance, the mount information may be lost after the ECS instance is restarted. To resolve this issue, you can configure the fstab (recommended) file or rc.local file in the /etc/ directory of the instance. This way, you can enable automatic mounting of an NFS share directory when the ECS instance is restarted.

> **Note** Before you enable automatic mounting, make sure that the share directory is mounted on the on-premises directory of your client.

1. Method 1: (Recommended) Open the fstab file in the /etc/ directory and add the mount command.

   > **Note** If your client runs CentOS 6, perform the following steps first:
   >
   > i. Run the `chkconfg netfs on` command to enable NetFS autostartup.
   >
   > ii. Open the netconfig file in the /etc/ directory, and comment out inet6-related information.

   - If you need to mount a share directory over NFSv4, run the following command:

     ```
     192.168.0.0:/shares local-directory nfs defaults 0 0
     ```

   - If you need to mount a share directory over NFSv3, run the following command:

     ```
     192.168.0.0:/shares local-directory nfs vers=3.0 defaults 0 0
     ```

2. Method 2: Open the rc.local file in the /etc/ directory and run the mount command.

   > **Note** Before you configure the rc.local file in the /etc/ directory, make sure that you have execute permissions on the rc.local file in the execute permissions directory and rc.local file in the /etc/rc.d/ directory. For example, in CentOS 7.x, execute permissions are not granted by default. Before you edit the rc.local file in the /etc/ directory, grant execute permissions to the account that you use to log on to the ECS instance.

   i. If you need to mount a share directory over NFSv4, run the following command:

   ```
   sudo mount.nfs 192.168.0.0:/shares local-directory
   ```

   ii. If you need to mount a share directory over NFSv3, run the following command:

   ```
   sudo mount -t nfs -o vers=3,proto=tcp,nolock,noacl,sync 192.168.0.0:/shares local-directory
   ```

   The preceding commands consist of the following parameters:

   - 192.168.0.0:/shares: the mount target of the gateway, including the IP address and the share directory name. Specify this parameter based on the actual scenario. To check the mount target of the gateway, log on to the CSG console and navigate to the **Share** page of the gateway.
   - local-directory: the on-premises directory of the CSG client. Specify a file directory that supports

read and write operations. You cannot specify a directory that does not exist.

-

3. Run the `reboot` command to restart the client.

1.8. Log management

This topic describes how to upload and download logs in the local gateway console.

Context

The local gateway console allows you to upload and download logs. You can click **Download Log** to compress the log information into a gz file and download it to the local client. You can click **Upload Log** to upload logs to the Cloud Storage Gateway (CSG) server. If you encounter an error, you can download the logs or record the paths of uploaded logs. You can then send them to Alibaba Cloud engineers to identify the problem.

Procedure

1. Open your browser, enter `https://<IP address of the file gateway>` in the address bar, and then press Enter.
2. In the dialog box that appears, enter your username and password, and then click **OK**.
3. Click **About** on the left-side navigation pane. The **About** page appears.
4. In the **Log Information** section, click **Download Log** to download logs to your local host.

   If you encounter an error, you can download the logs and submit a ticket to Alibaba Cloud Customer Services. You must provide the log information in the ticket for Alibaba Cloud support engineers to identify the problem.

Upload logs

1. In the local block gateway console, click **About** on the left-side navigation pane. The **About** page appears.
2. In the **Log Information** section, click **Upload Log** to upload logs to the CSG server.

   After the log is uploaded, in the **Log Information** section, the file path of the logs on the CSG server is displayed.

   If you encounter an error, you can upload the logs and submit a ticket to Alibaba Cloud Customer Services. You must provide the log paths in the ticket for Alibaba Cloud support engineers to identify the problem.

   > **Note** The uploaded logs are used for error analysis and system repair only.

1.9. Monitoring

This topic describes how to monitor the CPU, memory, cache IOPS, cache throughput, and network information in the Cloud Storage Gateway (CSG) console.

Procedure

1. Open your browser, enter `https://<IP address of the file gateway>` in the address bar, and

then press Enter.

2. In the dialog box that appears, enter your username and password, and then click **OK**.
3. Click **Monitoring** on the left-side navigation pane. On the **Monitoring** page, you can monitor the CPU, memory, cache IOPS, cache throughput, network, and other information.

1.10. Upgrade

This topic describes the CIDR blocks supported by file gateways deployed on Alibaba Cloud and how to upgrade file gateways in the Cloud Storage Gateway console.

Upgrade notes

- The image of version 1.0.26 is no longer compatible with the local file gateway of version 1.0.30. To upgrade the image to version 1.0.30, download the image again and install the local gateway console. For more information, see Deploy an on-premises console for a file gateway.
- When a new version of the local file gateway is available, an update notification is displayed.
- For version 1.0.32 or later, local file gateways support multiple CIDR blocks that are included in a VPC. The following table lists the CIDR blocks supported by block gateways.

Upgrade path	Supported CIDR block before the upgrade	Supported CIDR block after the upgrade
From version 1.0.30 or 1.0.31 to 1.0.32 and later.	192.168.0.0/16	192.168.0.0/16 172.16.0.0/12
	172.16.0.0/12	192.168.0.0/16 172.16.0.0/12
	10.0.0.0/8	172.16.0.0/12 10.0.0.0/8

Procedure

1. Open your browser, enter `https://<IP address of the file gateway>` in the address bar, and then press Enter.
2. In the dialog box that appears, enter your username and password, and then click **OK**.
3. Click **Click to Upgrade** to upgrade.

> **Note** The console is unresponsive during the update process.

1.11. Modify AccessKey ID and AccessKey secret

Cloud Storage Gateway V1.6.0 and later allows you to modify your AccessKey ID and AccessKey secret in the on-premises gateway console. This topic describes how to modify AccessKey ID and AccessKey secret in the on-premises gateway console.

Procedure

1. Open your browser. Enter `https://<IP address of the gateway>` in the address bar to connect to the on-premises gateway console.
2. In the dialog box that appears, enter your username and password. Click **OK**.
3. Click the profile picture in the upper-right corner of the page, and then click **Modify AK/SK**.
4. In the **Modify AK/SK** dialog box, enter the AccessKey ID and AccessKey secret. Click **OK**.
5. Restart the gateway.

   To restart the gateway, restart the virtual machine on which the gateway is deployed. The new AK and SK take effect after the gateway is restarted.