ALIBABA CLOUD

Alibaba Cloud

云存储网关

User Guide (On-Premises)

Document Version:

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.

Table of Contents

1.File Gateway 04
1.1. Deploy the local file gateway console 04
1.2. Manage cloud resources 10
1.3. Add disks 11
1.4. Manage cache disks 17
1.5. Manage NFS shares 19
1.6. Manage SMB shares 23
1.7. Access shares 29
1.7.1. Access SMB shares 29
1.7.2. Access NFS shares 31
1.8. Log management 33
1.9. Monitoring 34
1.10. Upgrade 34

1.File Gateway

1.1. Deploy the local file gateway console

This topic describes how to deploy the local file gateway console (a web console) by using an image. The procedure includes: download the image, install the image, configure network settings, and then activate the gateway.

Prerequisites

1. You have registered an Alibaba Cloud account and passed real-name verification. For more information, see Sign up with Alibaba Cloud.

   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. You have activated CSG.
   If this is your first time logging on to the , follow the instructions on the page to activate CSG.
3. You have created an Alibaba Cloud AccessKey pair. You can log on to the User Management console to obtain your AccessKey pair.

Context

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

Note

- OVA images of version 1.0.30 and later can be deployed only on web clients of vCenter version 6.0 and later.
- Images downloaded from the Alibaba Cloud CSG console cannot be imported to ECS instances.

Hardware requirements for virtual machines

The virtual machine where the local file gateway is deployed must meet the following requirements.

- The virtual machine has at least four virtual CPUs.
- The virtual machine has at least 8 GB of memory resources.
- The virtual machine has at least 100 GB of disk space, which is required for installing the CSG image and storing system data.
- We recommend that you use thick-provisioned cache disks on the virtual machine to achieve excellent I/O performance. The capacity of each cache disk must be 40 GB or larger.

Installation methods

The installation methods and installation files vary depending on the hypervisor. You can obtain the installation file when you create a local file gateway.

Hypervisor	Installation method	Installation file format
VMware vSphere	You can import an OVA image to VMware to install the gateway.	OVA
KVM	You can open the virt-manager and use the QCOW2 file to install a gateway.	QCOW2
Hyper-V	You can import a VHD file to Hyper-V to install a gateway.	VHD

Step 1: Download the image

1. Log on to the CSG console.
2. Select the region where you want to create a file gateway.
3. On the **Gateway Clusters** page, select the target gateway cluster, and then click **Create**. If you have not created a gateway cluster, click **Create Gateway Cluster** on the **Overview** page to create a gateway cluster.
4. On the **Basic Information** tab, 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, Chinese characters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter or a Chinese character.
Location	Select where you want to deploy the gateway. In this example, select **On-premise**.
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. Click Next to go to the **Paid Information** tab. Set the following parameters and click **Next**.

Parameter	Description
Billing Method	Supported billing methods include **Pay-as-you-go** and **Subscription**. For more information, see Pricing. If you select **Subscription**, after you create the file gateway, you are redirected to the buy page of CSG to settle the payment. For more information, see Purchase a gateway.
After Expiration	Specify how the the gateway is processed after it expires. You can select **Pay-as-you-go** or **Release After Expiration**.

6. On the **Image Download** tab, download the required image to your local machine.

Step 2: Install the image

After you download the image, you can use it to deploy the file gateway. For more information, see How do I deploy Cloud Storage Gateway instances in on-premises data centers?

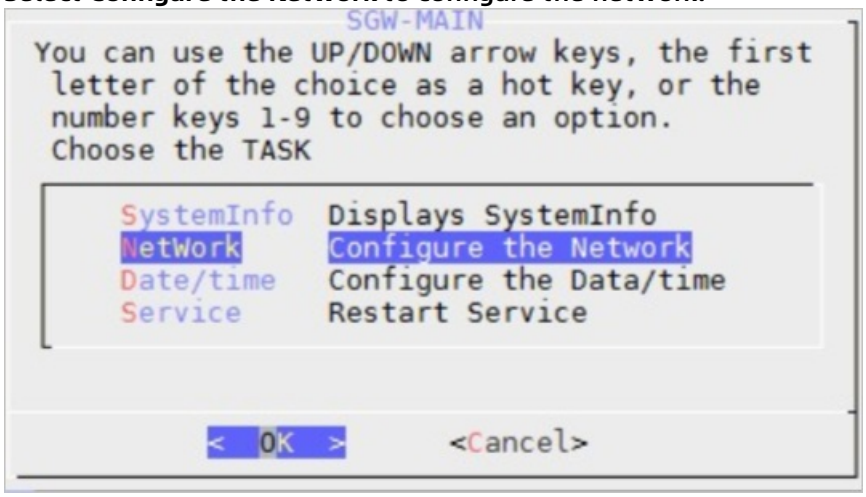
Step 3: Configure network settings

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

1. Start the gateway, and open the Linux terminal of the virtual machine.
2. Enter the user name and password to log on to the gateway CLI.
   The default user name is root and the password is Alibaba#sgw#1030.

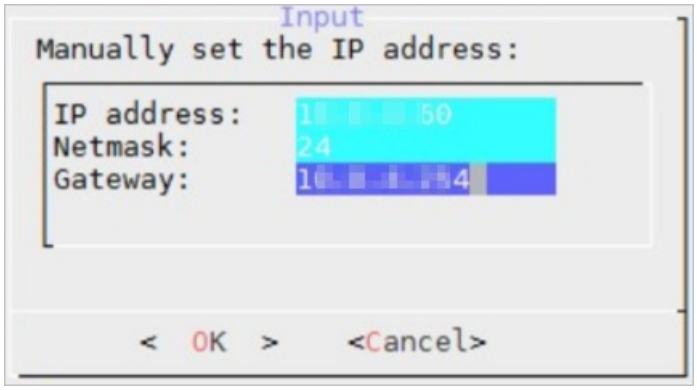
3. Select a language.
   The virtual machine may not support Chinese characters. We recommend that you select English for further configurations.

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

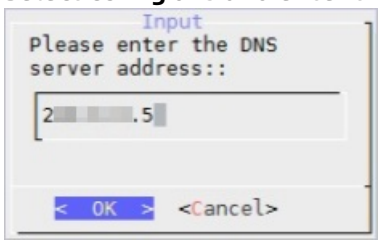


i. Select **use static ip address** and configure the IP address.

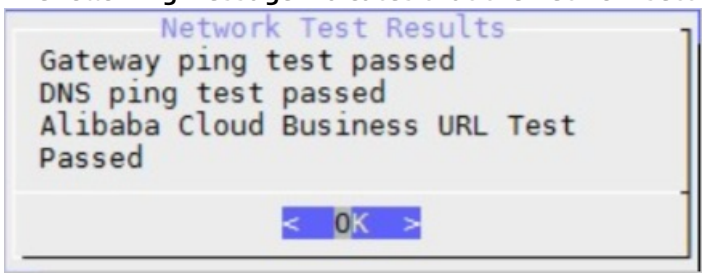
> **Note** Valid values of Netmask: 1 to 32. For example, if the subnet mask is 255.255.255.0, enter 24.



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. The Alibaba Cloud NTP server ntp.aliyun.com is used by default. You can also choose to **specify the 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 gateway.
   - (Recommended) Method 1
     a. Find the target file gateway, and click **Activate Gateway** in the Actions column.
     b. In the **Activate Gateway** dialog box that appears, set the following parameters, and click **Activate**.
        - **Gateway IP address**: Enter the IP address of the 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 the on-premises data center.
          > - The gateway IP address does not require Internet access.

        - **User Name**: Specify the user name used to log on to the local file gateway console.
        - **Password**: Specify the password used to log on to the local file gateway console.
        - **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 connect to the local file gateway console.
     d. In the dialog box that appears, enter the user name and password.

        > **Note** If this is your first time logging on to the gateway console, you must provide 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 target file gateway, and click **Download Certificate** in the Actions column to download the certificate to your local machine.
     b. Open your browser, and enter `https://<IP address of the target file gateway>` in the address bar to connect to the local file gateway console.
     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 user name used to log on to the local file gateway console.
        - **Password**: Specify the password used to log on to the local file gateway console.
        - **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 gateway, log on to the local file gateway console.

Related operations

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

Action	Description
Delete a gateway	Find the target file gateway and choose **More** > **Delete** in the Actions column. **Note** You can only delete pay-as-you-go file gateways.
Rename a gateway	Find the target 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 target 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 a gateway in an on-premises data center, you can reset the password in the local gateway console. To reset the password, find the target 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 the local file gateway console.
2. You have created an Object Storage Service (OSS) bucket. For more information, see Create buckets.

   Note
   - CSG supports Standard, IA, and Archive OSS buckets.
   - If you do not enable the archive feature when you create a share, you must restore archived files before you can read them.

Bind a cloud resource

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

Parameter	Description
Resource Name	Specifies the name of the cloud resource that you want to bind.
Cross-region Binding	○ **Yes**: specifies that you can access the bucket that stays in the different region from the specified gateway. ○ **No**: specifies that you can access only the bucket that stays in the same region as the specified gateway. **Note** The regions of the local file gateway and the OSS bucket must belong to the same time zone.
Region	The region where the target bucket is located.
Bucket Name	The name of the bucket that you want to bind to the gateway.
Use SSL	Specifies whether to access an OSS bucket over SSL. Valid values: **Yes** and **No**.

5. Click **OK**.

Other supported operations

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

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.

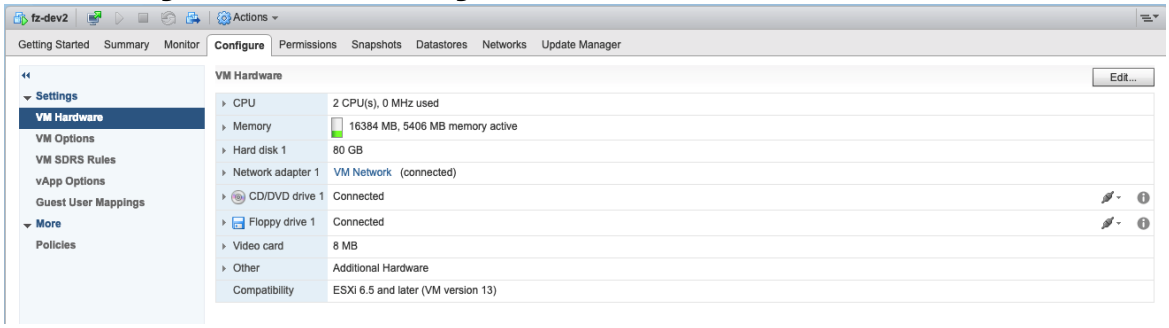
Context

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.

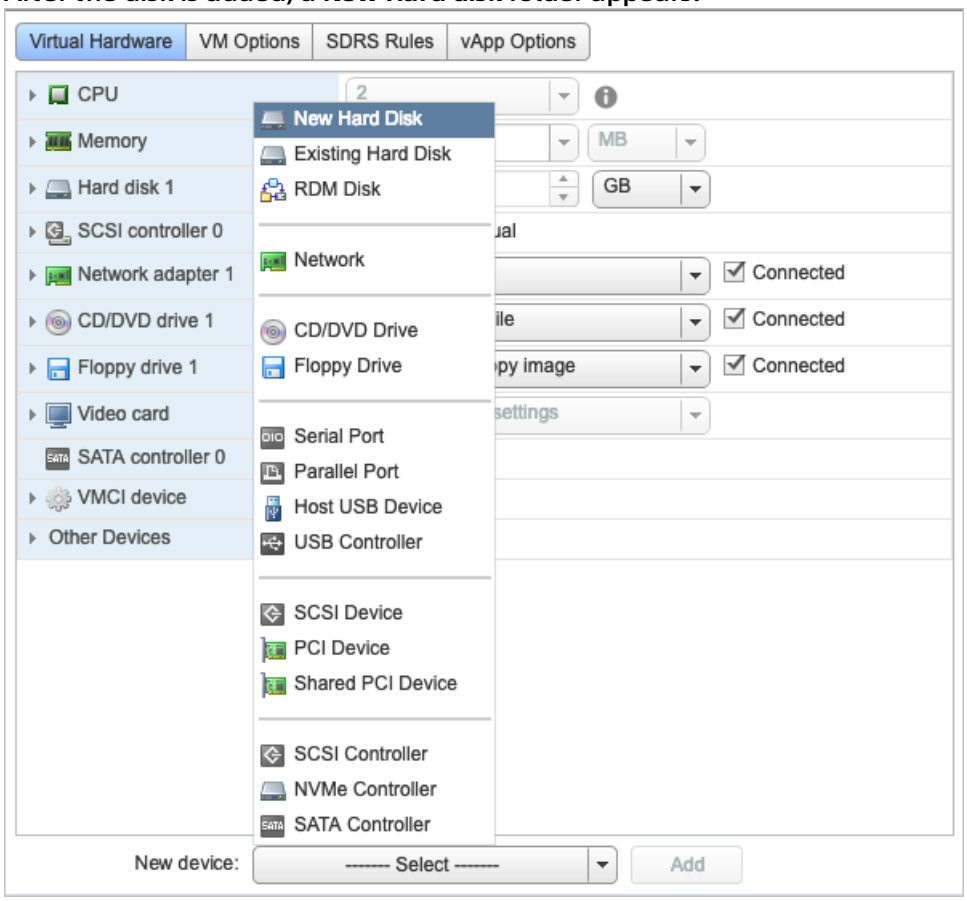
> **Note** The minimum cache disk capacity supported by the file gateway is 40 GB. Therefore, the new disk capacity cannot be less than 40 GB. Otherwise, the file gateway cannot recognize the new disk.

Add disks to VMware vSphere

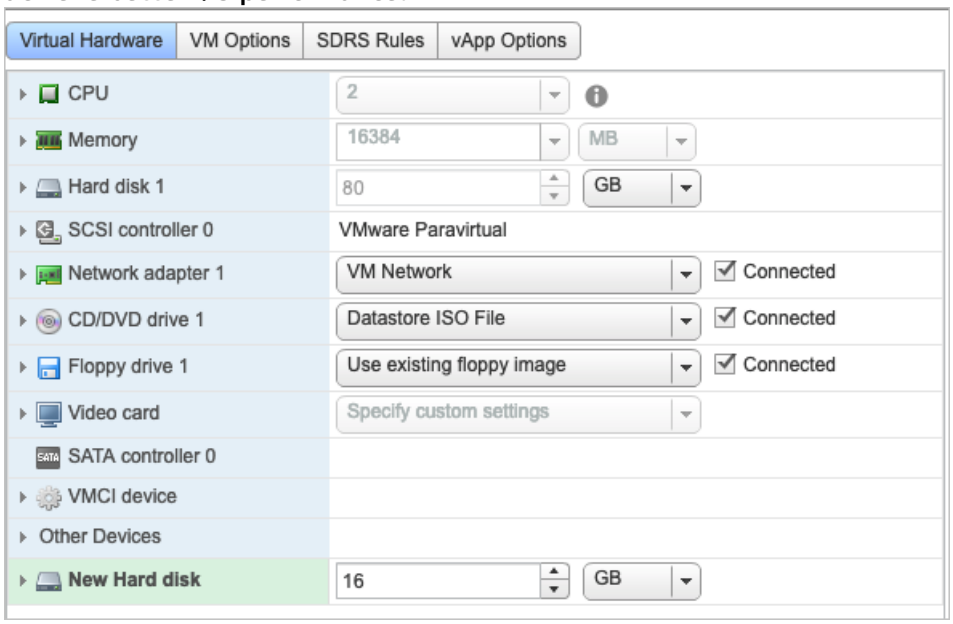
1. Log on to the VMware vSphere virtualization platform.
2. On the **Configure** tab, choose **Settings** > **VM Hardware**. Click **Edit**.



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.

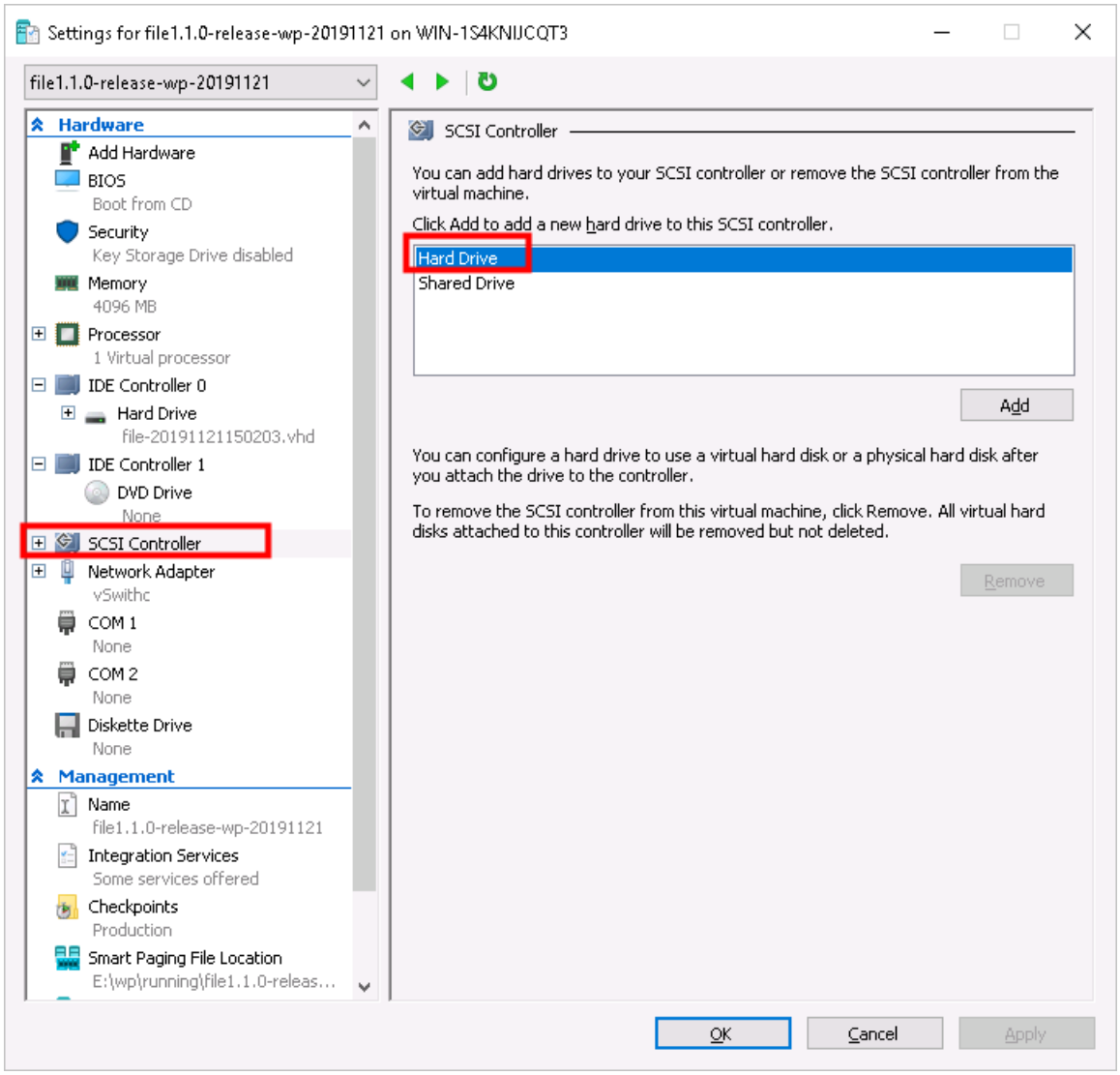


Note In this example, only one hard disk is added. You can add multiple disks based on your needs.

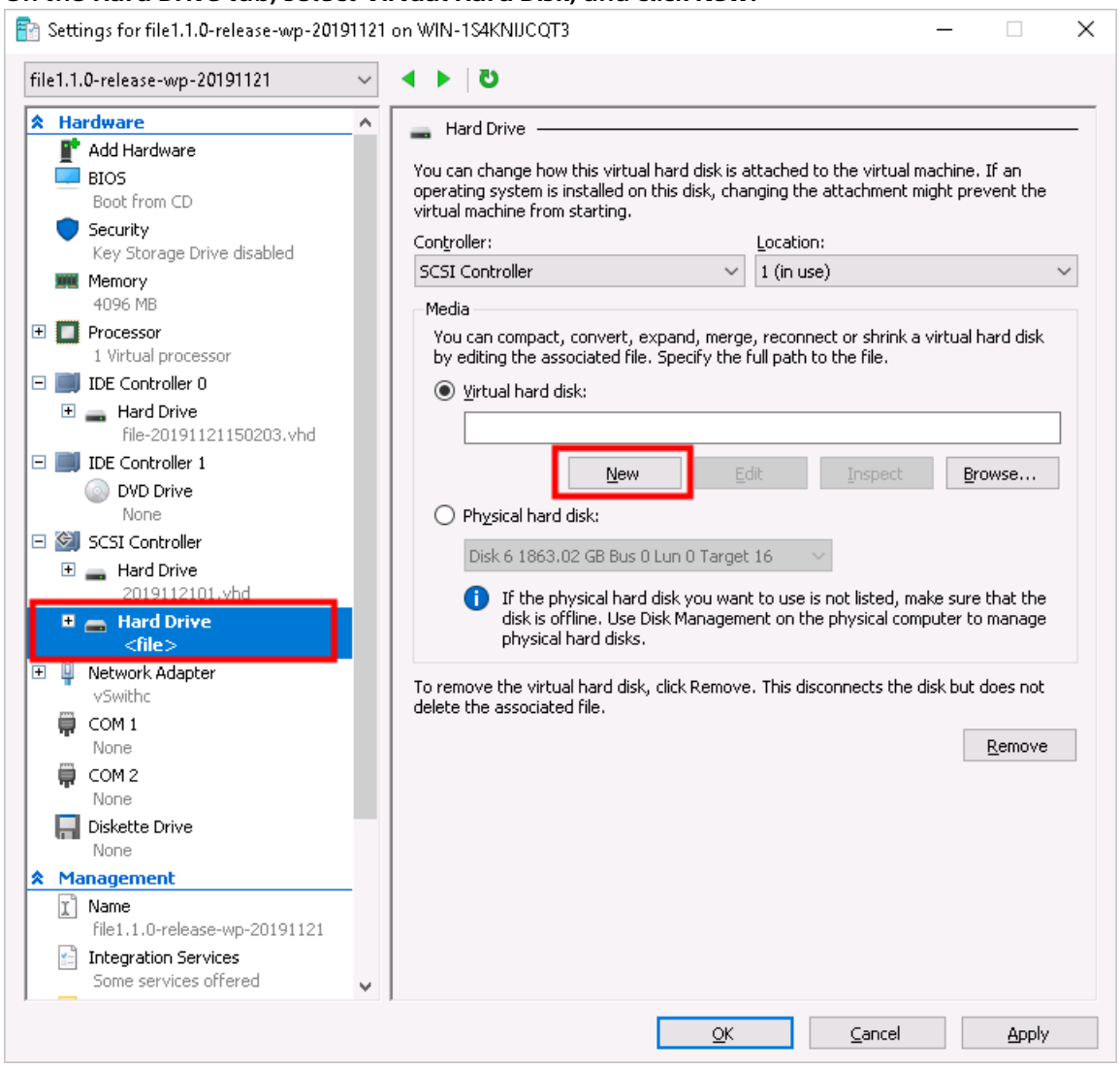
Add disks to Hyper-V

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.**

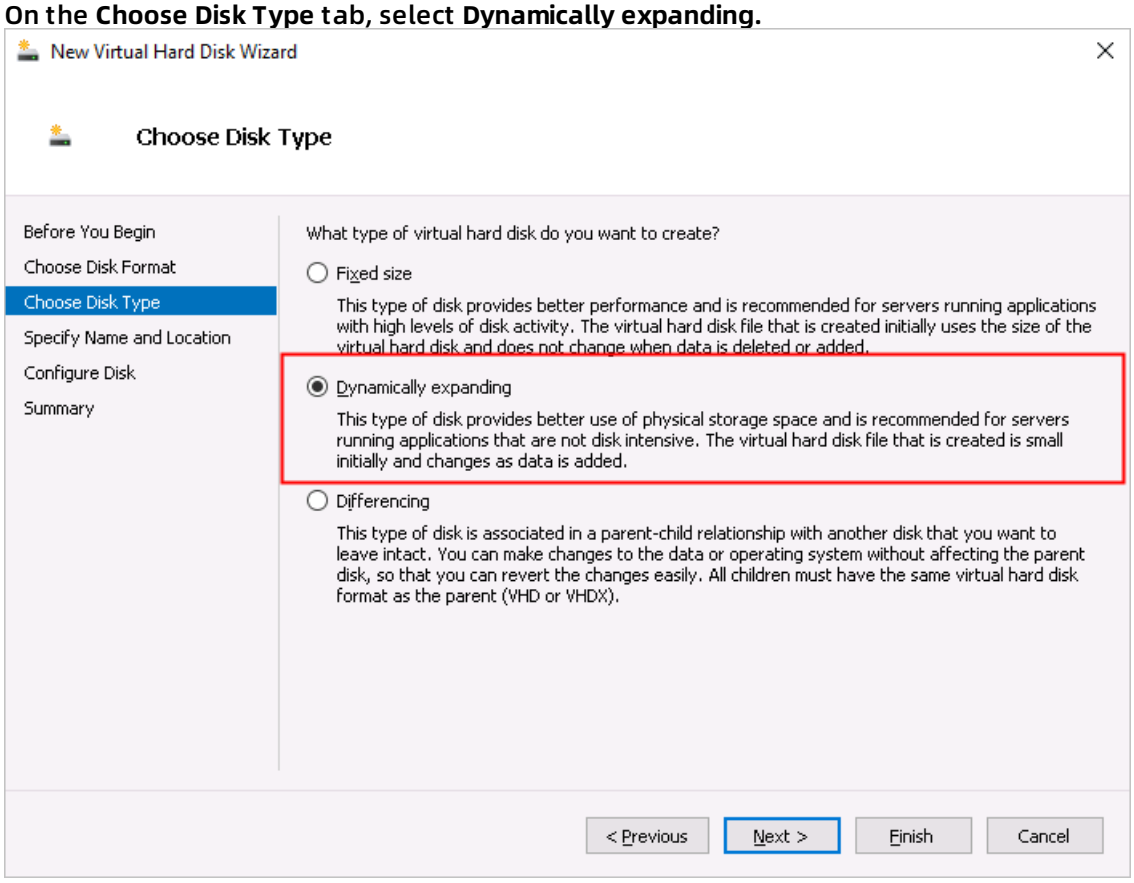


3. On the **Hard Drive** tab, select **Virtual Hard Disk**, and click **New**.



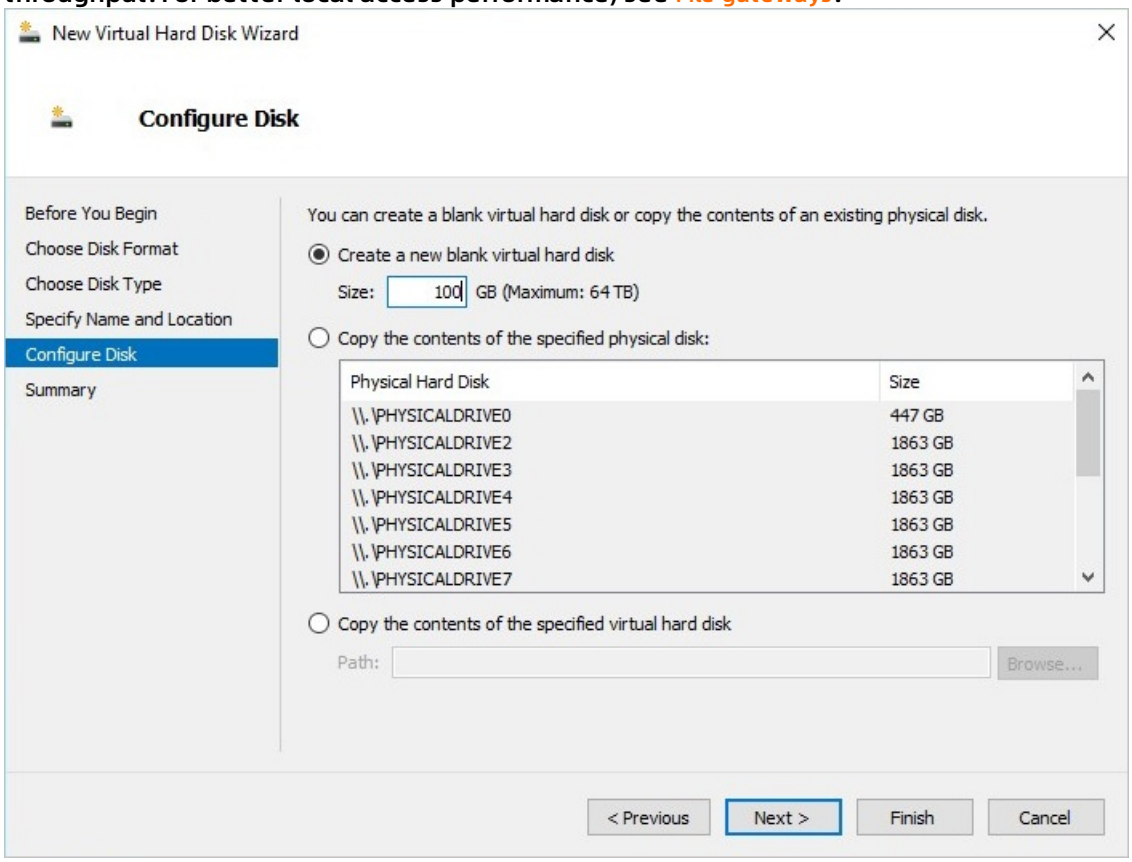
4. Follow the new virtual hard disk wizard to add the hard disk.
   Note the following settings:

- **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 the local file gateway console.
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, and in the address bar, enter `https://<IP address of the target file gateway>` to connect to the local file gateway console.
2. In the dialog box that appears, enter the username and password, and click **OK**.
3. Go to the **Caches** page, and click **Create**.
4. On the **Create Cache** dialog box that appears, set the following parameters:
   - **Disk**: Click **Select**, and in the dialog box that appears, select an available disk. 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. You can select this option to reuse the data in the specified cache disk. If you delete a share by mistake, you can recreate the share and reuse data in the cache disk to restore data.

     > **Note** If no file system exists on the cache, after you enable data reuse, you will fail to create the cache.
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 local file gateway console, including how to create, delete, close, and modify NFS shares.

Prerequisites

1. You have added a cache disk to the gateway. For more information, see Add a cache disk.
2. You have bound the cloud resources. For more information, see Bind a cloud resource.

Context

NFS enables computers in a network to share resources over TCP/IP communications. In a scenario where NFS is applied, the local client directly reads files from and writes files to the remote NFS server.

Cloud Storage Gateway (CSG) operates like 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, set the users that are allowed to access the shared directory, and set 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 for other operating systems, see the official NFS documentation.
   - If you are using Ubuntu, run the following command.
     ```
     sudo 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, and in the address bar, enter `https://<IP address of the target file gatewa y>` to connect to the local file gateway console.
2. In the dialog box that appears, enter the username and password, and click **OK**.
3. Click **NFS**, and click **Create**.
4. In the **Create NFS** dialog box that appears, set the following parameters, and click **OK**.

Parameter	Description

Parameter	Description
Share Name	The virtual mount point of the NFS share that you want to create. You can use this share name to directly mount an NFSv4 share. To mount an NFSv3 share, you must run the `showmount -e <IP address of the target gateway>` command to obtain the mount point.
Read/Write Client IPs	Specifies the IP address or CIDR block of the client that you allow to read from and write to the target NFS gateway, such as 192.168.10.10 or 192.168.0.0/24. You can enter multiple IP addresses or CIDR blocks.
Read-only Client IPs	Specifies the IP address or CIDR block of the client that you allow to only read from the target NFS gateway, such as 192.168.10.10 or 192.168.0.0/24. You can enter multiple IP addresses or CIDR blocks.
User Mapping	Maps an NFS client user to an NFS server user. This parameter is required only when you set the **Protocol** parameter to **NFS**. ○ none: specifies no mapping relationship between an NFS client user and the NFS server user nobody. ○ root_squash: maps only a root user of an NFS client to the NFS server user nobody. ○ all_squash: maps all NFS client users to the NFS server user nobody. ○ all_anonymous: maps all NFS client users to an anonymous NFS server user.
Enabled	Specifies 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.
Data Access Mode	Valid values: Cache Mode and Replication Mode. ○ **Replication Mode**: specifies that all data is stored with two backups. One backup is stored in a local cache and the other is stored in an OSS bucket. ○ **Cache Mode**: specifies that all metadata and frequently accessed user data are stored in the local cache. The OSS bucket retains all data.
Enable Remote Sync	Synchronizes metadata stored in an OSS bucket to the local cache. This feature is applicable to such scenarios as disaster recovery, data restoration, and data sharing. **Note** During remote synchronization, the system scans all objects in the bucket. If a large number of objects exist, you have to pay for corresponding OSS API requests. For more information, see Pricing of OSS.

Parameter	Description
Encryption	Valid values: No Encryption and Server Encryption. If you select Server Encryption, you must set the CMK 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 encryption, you can provide you own key. The system supports the key imported from Key Management Service (KMS). With OSS server encryption enabled, the system automatically uses the imported key to encrypt the files uploaded to OSS through the shared directory. You can call the Get Object API operation to check whether the specified file has been 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, this response indicates that the file has been encrypted. Note ○ Only the users in a whitelist can use this feature. ○ When you create a key in the KMS console, you must select the same region as the target OSS bucket.
Bucket Name	Specifies an existing bucket.
Path Prefix	Specifies a subdirectory of the target bucket in the Path Prefix field. The Path Prefix field supports letters and digits only. Note For version 1.0.38 and later, you can map a root directory of the file system to a subdirectory of a bucket to isolate connections and secure data. You can specify an existing subdirectory or a subdirectory that does not exist in the bucket. After you create the share, the specified subdirectory works as the root directory, and stores all related files and directories in the follow-up management.
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 shared directories. Valid values: Yes and No. ○ 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 a whitelist can use this feature.
Ignore Delete	Ignores file deletion operations during data synchronization to OSS. The OSS bucket retains all data.

Parameter	Description
Sync Delay	Specifies a delay before the system uploads the file that you have modified and closed. The **Sync Delay** feature avoids OSS fragments caused by frequent local modifications. Valid values: 0 to 120. Default value: 5. Unit: seconds.
Max Write Speed	.Specifies the maximum speed of writing data. Valid values: 0 to 1280. Default value: 0. Unit: MB/s. The value 0 specifies that the write speed is not limited
Max Upload Speed	Specifies the maximum speed of uploading data. Valid values: 0 to 1280. Default value: 0. Unit: MB/s. The value 0 specifies that the upload speed is not limited. **Note** The maximum upload speed cannot be lower than the maximum write speed if the speed is limited.
Optimize Fragments	Specifies whether to optimize the performance for some applications that frequently and randomly read and write small amounts of data. You can enable this feature as needed.
Optimize Upload	Releases the cache in real time. You can enable this feature when you only synchronize backups to the cloud.

5. Click **OK**.

Other supported operations

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

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 target NFS share. Click **Settings**, and set **Enabled** to **No**.
Delete an NFS share	On the **NFS** page, find the target NFS share, and click **Delete** to delete the NFS share. **Note** If the NFS share has been previously mounted to a client, it takes some time for the mount point to be unmounted from the client after the share is deleted. During this period, if you create an NFS share with the same ID, the mount point will not 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 target NFS share, and click **Settings** or **Advanced Settings** to modify the NFS share.

What's next

Access NFS shares

1.6. Manage SMB shares

This topic describes how to manage Server Message Block (SMB) shares in the local file gateway console, including creating, deleting, disabling, and modifying SMB shares, configuring AD/LDAP, and adding SMB users.

Prerequisites

1. You have added a cache disk to the gateway. For more information, see Add a cache disk.
2. You have bound cloud resources. 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) operates like an SMB server and provides the file sharing service. When you access CSG from a Windows client, CSG receives a request from the client and returns a response.

To use the SMB services, you must configure a shared file directory in the Cloud Storage Gateway console, create an SMB user, and specify user permissions.

Create an SMB share

1. Open your browser, and in the address bar, enter `https://<IP address of the target file gateway>` to connect to the local file gateway console.
2. In the dialog box that appears, enter the username and password, and click **OK**.
3. On the **SMB** page, click **Create** in the upper-right corner.
4. In the **Create SMB Share** dialog box, configure 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/write access to the SMB share.
Enabled	Specifies whether to enable SMB sharing. If you do not want to enable SMB sharing, you can select **No** to disable SMB sharing.
Discoverable	Specifies whether the SMB share can be discovered by network neighbors.
Data Access Mode	Cache Mode and Replication Mode are available. ○ **Replication Mode**: In this mode, two backups of all data are created. One is stored in the local cache disk and the other one is stored in the OSS bucket. ○ **Cache Mode**: In this mode, the backup stored in the local cache disk only contains the metadata and frequently accessed user data. The backup stored in the OSS bucket contains all data.

Parameter	Description
Enable Remote Sync	Specifies whether to synchronize metadata of the local cache disk with metadata stored in the OSS bucket This feature can be applied in disaster recovery, data restoration, and data sharing scenarios. Note During remote synchronization, the system scans all objects in the bucket. If the number of objects is large, fees incurred from making OSS API requests may be high. For more information, see OSS Pricing.
Encryption	No Encryption and Server Encryption are available. If you select Server Encryption, you must set the CMK 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 encryption, you can provide your own key. The system supports the key imported from Key Management Service (KMS). With OSS server encryption enabled, the system automatically uses the imported key to encrypt the files uploaded to OSS through the shared directory. You can call the GetObject operation to check whether the specified file has been 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, this response indicates that the file has been encrypted. Note ○ Only whitelisted users can use this feature. ○ When you create a key in the KMS console, you must select the same region as the target OSS bucket.
Cloud Resource	Select an existing bucket.
Path Prefix	Specifies a subdirectory of the target bucket. The path field supports letters and digits only. Note For version 1.0.38 and later, you can map a root directory of the file system to a subdirectory of a bucket to allow separate file access between users. You can specify an existing subdirectory or a subdirectory that does not exist in the bucket. After you create the share, the specified subdirectory works as the root directory, and stores all related files and directories.

Parameter	Description
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 shared directories. ○ If you select **Yes**, you must configure the corresponding **Metadata** and **Data** parameters. ○ If you select **No**, you must set the **Cache Disk** parameter. **Note** Only whitelisted users can use this feature.
Ignore Delete	During the data synchronization process, the OSS buckets ignore all data deletion operations. The backup stored in the OSS bucket contains all data.
Sync Delay	Specifies a delay before the system uploads the file that you have modified and closed. The **Sync Delay** feature avoids OSS file fragmentation caused by frequent local modifications. The default value is 5 seconds and the maximum is 120 seconds.
Max Write Speed	Specifies the maximum speed of writing data. Valid values: 0 to 1280. Unit: MB/s. The default value is 0. which indicates that the write speed is not limited.
Max Upload Speed	Specifies the maximum speed of uploading data. Valid values: 0 to 1280. Unit: MB/s. The default value is 0, which indicates that the upload rate is not limited. **Note** When you customize the maximum write and upload rates, make sure that the maximum upload rate is not lower than the maximum write rate.
Fragment Optimization	Specifies whether to optimize the performance for some applications that frequently and randomly read and write small amounts of data. You can enable this feature based on your needs.
Direct_IO	Releases the cache in real time. You can enable this feature when you only synchronize backups to the cloud.

AD/LADP

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 service, but not both.
- The permissions of the current AD domain user, LDAP user, and local 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.
- Currently, the AD feature supports 64-bit Windows Server 2016 Datacenter and Windows Server 2012 R2 Datacenter.
- Currently, 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 local gateway console, click **About**.
   ii. In the **Network Configuration** section, click **Update DNS**.
   iii. In the **Update DNS** dialog box that appears, enter the IP addresses of DNS servers, and click **OK**.
   In the **DNS server** text box, 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 that appears, configure the following parameters, and click **OK**.
   - **Server IP**: Enter the IP address of the AD server.
   - **User Name**: Enter the administrator username.
   - **Password**: Enter the administrator password.

   After the connection is established, the status of **Joined** under **AD** becomes **Yes**.

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

Configure LDAP

1. In the local gateway console, choose **SMB > AD/LDAP**.
2. In the **LDAP** section, click **Join LDAP**.
3. In the **Connect LDAP** dialog box that appears, set the following parameters and click **OK**.
   - **Server IP**: Enter the IP address of the LDAP server, which is the directory system agent.
   - **Support TLS**: 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 **Joined** under **LDAP** becomes **Yes**.

> Note After you join the LDAP domain, the local user permissions configured in the SMB share are removed.

Add an SMB user

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

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

1. In the local gateway console, choose **SMB > SMB Users**.
2. Click **Create**.
3. In the **Add SMB user** dialog box, set the name and password.
4. Click **OK**.

Other supported operations

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 target NFS share. Click **Settings** and set **Enabled** to **No**.
Delete an SMB share	On the **SMB Shares** tab, find the target SMB share, and click **Delete** to delete the SMB share. **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 target SMB share, and click **Settings** or **Advanced Settings** to modify an SMB share.
Cache Refresh	On the **SMB Shares** tab, find the target SMB share, and click **Cache Refresh** to refresh the cache.
Delete an SMB user	On the **SMB Shares** tab, find the target SMB user, and click **Delete** to delete the SMB user.
Disable a connection	On the **AD/LDAP** tab, click **Disconnect** to disable the AD or LDAP 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

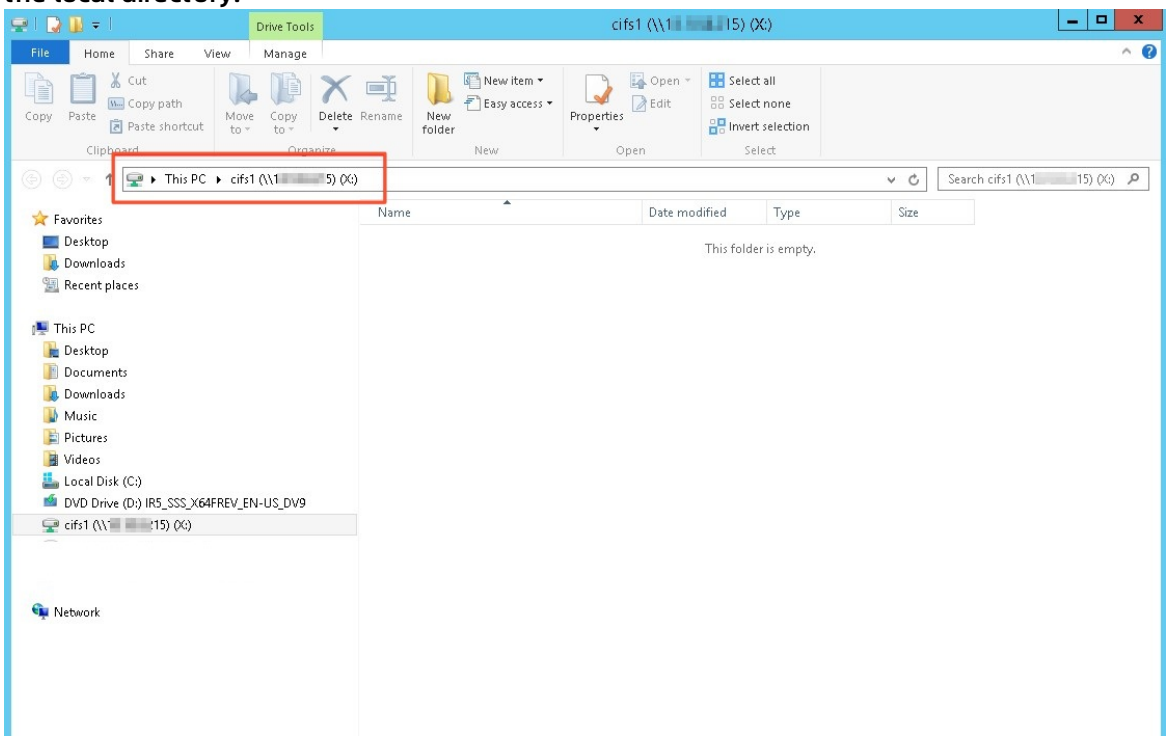
To access a local gateway from a client that is running Windows, you must map the share as a network drive first. After you map the share, a network mapping is established between the local directory and the share. You can access the remote share in the same way as you access a local directory.

> **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 NFS shares

This topic describes how to access local gateways from a client that is running Linux.

Prerequisites

You have created a Network File System (NFS) share. For more information, see Install an NFS client.

Context

To access a gateway from a client that is running Linux, you must mount the NFS share to a local file directory. After the share is mounted, directory mappings are established between the share and the local directory. You can access the remote share in the same way as you access a local directory.

Procedure

1. Log on to a local Linux client.
2. Mount the NFS share to the local directory where the client belongs.
   i. Run the following command to mount the NFS share:

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

   - 192.168.0.0:/shares: the mount point of the file gateway, including the gateway IP address and the share name. Replace them with the actual IP address and share name. On the **Share** page of the gateway in the Cloud Storage Gateway console, you can view the mount points.
   - local-directory: the local file directory. Specify any file directory that supports read and write operations. You cannot specify a directory that does not exist.

> **Note** If your file gateway version is earlier than 1.0.35, and you have mounted shares by using the NFSv3 protocol, then you must run the `showmount -e <The IP address of the file gateway>` command to query the mount path. The procedure is as follows.
>
> a. Run the following command to query the mount path, for example, 192.168.0.0:/shares.
>
> ```
> showmount -e <The IP address of the file gateway>
> ```
>
> b. Run the following command to mount the share to the local 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 verify the result.
   If the following or similar information appears, it indicates that the share is mounted to the local directory.

> **Note** 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.

```
[root@centos7cb ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda1        99G  1.6G   92G   2% /
devtmpfs         24G     0   24G   0% /dev
tmpfs            24G     0   24G   0% /dev/shm
tmpfs            24G  424K   24G   1% /run
tmpfs            24G     0   24G   0% /sys/fs/cgroup
tmpfs           4.8G     0  4.8G   0% /run/user/0
[redacted]:/nfs2  256T     0  256T   0% /mnt/nfs172cent7.4
[root@centos7cb ~]#
```

3. Access the NFS share.
   After the NFS 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 NFS share. If you have the read-only permission, then you can only read data from the NFS share.

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

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, and in the address bar, enter `https://<IP address of the target file gatewa y>` to connect to the local file gateway console.
2. In the dialog box that appears, enter the username and password, and 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, and in the address bar, enter `https://<IP address of the target file gateway>` to connect to the local file gateway console.
2. In the dialog box that appears, enter the username and password, and 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 the local file gateway console.
- 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, and in the address bar, enter `https://<IP address of the target file gateway>` to connect to the local file gateway console.
2. In the dialog box that appears, enter the username and password, and click **OK**.
3. Click **Click to Upgrade** to upgrade.

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