

Alibaba Cloud

云存储网关 Overview

Document Version: 20220211

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 <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.What is CSG?	05
2.Cloud Storage Gateway V2.0 for public review	07
3.Features	08
4.Specifications	11
5.Gateway models and specifications	15
6.Scenarios	17
7.Service linked roles for CSG	20
8.Usage notes	24
9.Reliability and consistency	28

1. What is CSG?

Cloud Storage Gateway (CSG) is a gateway service that can be deployed at your data center or on Alibaba Cloud. CSG uses Object Storage Service (OSS) buckets as backend storage devices. CSG provides on-premises and cloud applications with standard file services over the Network File System (NFS) and Server Message Block (SMB) protocols. CSG also provides on-premises and cloud applications with block storage services over the Internet Small Computer Systems Interface (iSCSI) protocol.

CSG supports two types of gateways:

- File gateways

File gateways use OSS buckets as backend storage devices, and map the object directory structure of OSS buckets to NAS file systems. You can read and write all objects in a specified OSS bucket over standard NFS and SMB protocols. CSG also uses on-premises storage to cache hot data, and provides high-performance data access in addition to the large storage capacity of OSS buckets. File gateways are compatible with the Portable Operating System Interface (POSIX) and third-party backup software. If you want to back up small files or share small files for reading and writing, we recommend that you use file gateways of the Standard or Basic type. If you have high performance requirements or want to use multiple clients to simultaneously access shared data, we recommend that you use enhanced or advanced types of file gateways.

- Block gateways

Block gateways create storage volumes in OSS and allow you to access OSS by using the iSCSI protocol. On-premises applications can access these volumes as iSCSI targets. Block gateways run in two modes: pass-through and cache. In the pass-through mode, data in iSCSI volumes is sliced and synchronized to the cloud. This mode is applicable when you use high-speed links such as Express Connect circuits. In cache mode, you can create on-premises cache disks to accelerate read and write operations, and transfer data to the cloud in an asynchronous manner. This mode is applicable when you require efficient access to on-premises cached data but have an average performance for uploading data to OSS.

Architecture

You can use cloud gateways and on-premises gateways to build a storage gateway cluster. Then, you can share data between the cloud and your data center. This allows you to migrate data in various business scenarios, such as file backup, data distribution, and disaster recovery. You can also use the clusters to distribute data to multiple data centers.

CSG is a lightweight storage gateway, which can be deployed at your data center and on Alibaba Cloud.

Scenarios

- File gateways

- Build a file storage service for a large file system when local storage is limited.
- Store data as objects in the cloud, and allow applications to access the data in a file system without the need to modify code.
- Access shares in a file storage service among multiple data centers.

- Block gateways

- Back up data to the cloud by using backup software that supports efficient data transfer over iSCSI.

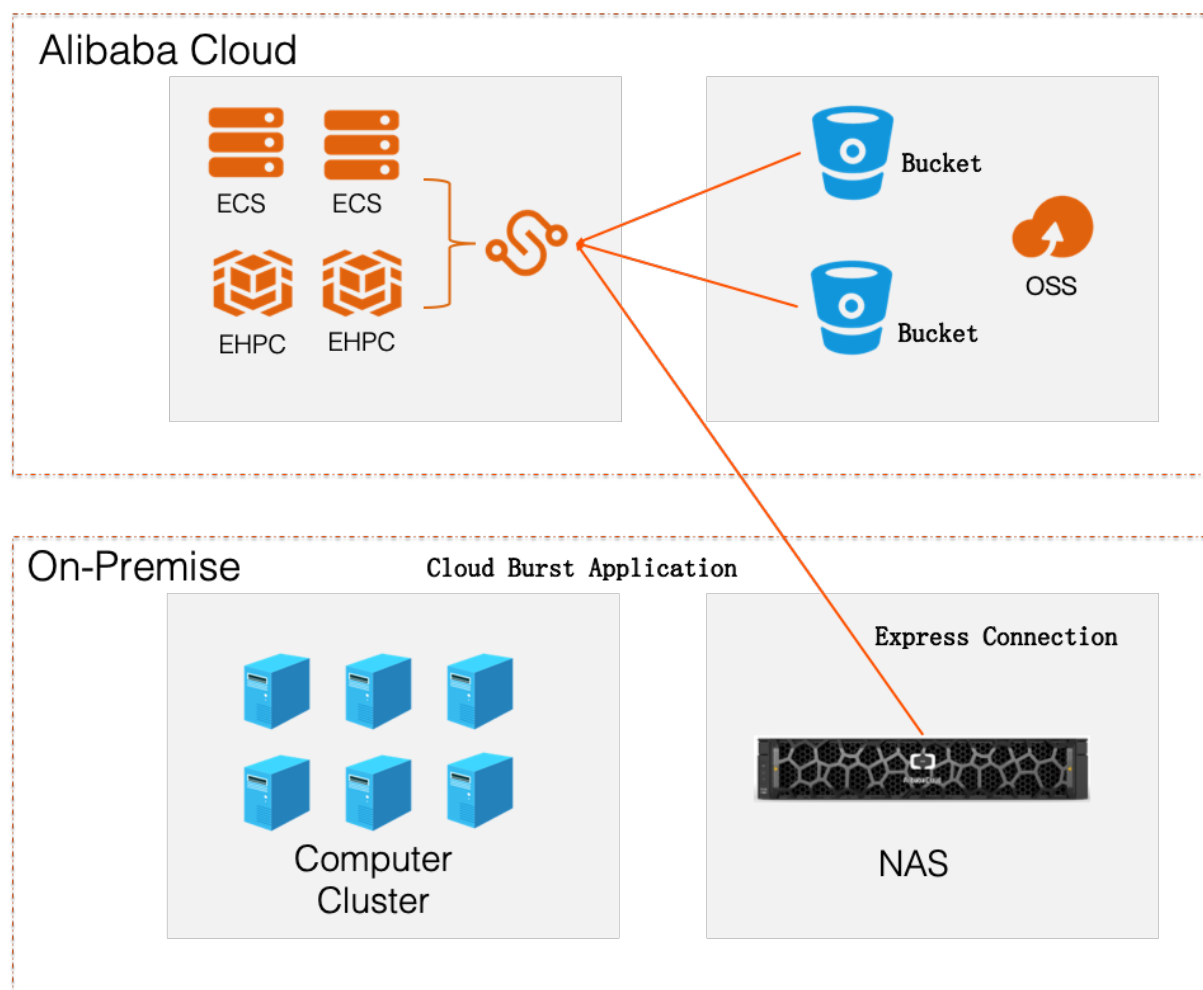
-
- Import video streams to storage volumes over iSCSI to store data in the cloud.

2.Cloud Storage Gateway V2.0 for public review

Cloud Storage Gateway (CSG) V2.0 is a gateway service that you can deploy on Alibaba Cloud. The elastic gateway feature is available in CSG V2.0. CSG V2.0 allows you to use Network File System (NFS) clients to mount gateway nodes. CSG V2.0 also allows you to access OSS or NAS data that is virtualized in the same namespace by using standard POSIX APIs.

Architecture

CSG V2.0 uses a distributed architecture that provides symmetric active-active data access and high-performance read/write capabilities. CSG V2.0 allows you to integrate multiple data sources into a unified namespace. This way, you can manage data in an efficient manner. The architecture also allows you to scale up bandwidth and capacity in real time. You can configure and purchase resources based on your business requirements. CSG V2.0 provides a high-performance distributed cache based on the ESSDs and uses OSS as backend storage. This architecture ensures data reliability of up to 99.999999999% (twelve 9s). You can use CSG V2.0 to integrate different data sources into a virtualized file system. You can access the virtualized file system by using a unified API that is provided by CSG V2.0.



3.Features

Cloud Storage Gateway (CSG) provides two types of gateways: file gateway and block gateway. Each type of gateway has multiple specifications. This topic describes the features supported by different specifications of these gateways.

File gateways


File gateways support two network transmission protocols: Network File System (NFS) and Server Message Block (SMB). You can use both protocols to transfer files over LAN.

- NFS allows you to access file systems in UNIX, such as AIX, HP-UX, and other Linux-based operating systems.
- SMB allows you to access file systems in Windows.

Features of file gateways

Feature		Basic	Standard	Enhanced	Advanced	Documentation
Basic features	Cache disks	✓	✓	✓	✓	Manage cache disks
	NFS and CIFS services	✓	✓	✓	✓	Manage shares
	AD and LDAP domains	✓	✓	✓	✓	Configure AD, LDAP, and DNS settings
Operations	Modify gateways	✓	✓	✓	✓	Other supported operations
	Configure tags	✓	✓	✓	✓	Manage tags
	Back up gateways	×	✓	✓	×	Back up file gateways
	Update gateway versions	✓	✓	✓	✓	Upgrade
	Upgrade gateways	✓	✓	✓	✓	Upgrade a file gateway
	Upgrade the network bandwidth	✓	✓	✓	✓	Upgrade the public bandwidth

Feature		Basic	Standard	Enhanced	Advanced	Documentation
	Upload logs	✓	✓	✓	✓	Log management
Advanced features	Associate a share with multiple OSS buckets	×	×	✓	✓	Associate a share with multiple OSS buckets
	Remote sync	✓	✓	✓	✓	Manage shares
	Express synchronization	×	✓	✓	✓	Express synchronization
	Transfer acceleration	✓	✓	✓	✓	Enable transfer acceleration
	Server-side encryption	✓	✓	✓	✓	Create a share
	Gateway-side encryption	×	×	✓	✓	Enable gateway encryption
	Intelligent archiving	×	✓	✓	✓	Manage shares
	Intelligent caching	✓	✓	✓	✓	N/A
	Intelligent replication	✓	✓	✓	✓	Replicate data
	Ignore deletion	✓	✓	✓	✓	Manage shares
	MIME support	✓	✓	✓	✓	N/A


 **Note** In the preceding table, the check sign (✓) indicates that the feature is supported, and the cross sign (×) indicates that the feature is not supported.

Block gateways

Block gateways provide data access services by using the Internet Small Computer System Interface (iSCSI) protocol. iSCSI is a storage technology based on the Internet and SCSI-3 protocols. iSCSI can be used to access Windows and UNIX operating systems.

Features of block gateways

Feature		Basic	Standard	Enhanced	Advanced	Documentation
Basic features	Cache disks	✓	✓	✓	✓	Manage cache disks
	iSCSI service	✓	✓	✓	✓	Manage iSCSI volumes
Operations	Modify gateways	✓	✓	✓	✓	What to do next
	Configure tags	✓	✓	✓	✓	Manage tags
	Update gateway versions	✓	✓	✓	✓	Update gateway versions
	Upgrade gateways	✓	✓	✓	✓	Upgrade a block gateway
	Configure the network bandwidth	✓	✓	✓	✓	Upgrade the public bandwidth
	Upload logs	✓	✓	✓	✓	Log management
Advanced features	CHAP support	✓	✓	✓	✓	Create an iSCSI volume

 **Note** In the preceding table, the check sign (✓) indicates that the feature is supported, and the cross sign (×) indicates that the feature is not supported.

4. Specifications

This topic describes the specifications of in-cloud file gateways, local file gateways, in-cloud block gateways, and local block gateways.

File gateways

File gateways are classified into in-cloud file gateways and local file gateways. [Table 1](#) and [Table 2](#) show the specifications of these file gateways.

Specifications of in-cloud file gateways

Item	Description			
Type	Basic	Standard	Enhanced	Advanced
Storage protocol	Network File System Version 3 (NFSv3), NFSv4, and Server Message Block (SMB)	NFSv3, NFSv4, and SMB	NFSv3, NFSv4, and SMB	NFSv3, NFSv4, and SMB
Maximum number of files transferred between Object Storage Service (OSS)	10 million	50 million	100 million	500 million
Maximum capacity of file sharing systems (recommended)	64 TB	128 TB	256 TB	256 TB
Maximum number of file shares	NFS: 4, SMB: 4	NFS: 8, SMB: 8	NFS: 16, SMB: 16	NFS: 16, SMB: 16
Maximum number of clients concurrently connected to a gateway	NFS: 1,024, SMB: 1,024	NFS: 1,024, SMB: 1,024	NFS: 1,024, SMB: 1,024	NFS: 1,024, SMB: 1,024
Maximum bandwidth for synchronization with OSS	1 Gbit/s	2 Gbit/s	5 Gbit/s	10 Gbit/s
Encrypted transmission to OSS	Yes	Yes	Yes	Yes
Minimum cache capacity	40 GB	40 GB	40 GB	40 GB

Item	Description			
Maximum gateway bandwidth	1 Gbit/s	2 Gbit/s	5 Gbit/s	10 Gbit/s

Specifications of local file gateways

Item	Description			
Recommended configurations for virtual machines	4-core, 8 GB memory	8-core, 16 GB memory	16-core, 32 GB memory	
Storage protocol	NFSv3, NFSv4, and SMB	NFSv3, NFSv4, and SMB	NFSv3, NFSv4, and SMB	
Maximum number of files transferred between Object Storage Service (OSS)	50 million	50 million	50 million	
Maximum capacity of file sharing systems (recommended)	128 TB	128 TB	128 TB	
Maximum number of file shares (recommended)	NFS: 4, SMB: 4	NFS: 8, SMB: 8	NFS: 16, SMB: 16	
Maximum number of file shares	NFS: 16, SMB: 16	NFS: 16, SMB: 16	NFS: 16, SMB: 16	
Maximum number of clients concurrently connected to a gateway	NFS: 1,024, SMB: 1,024	NFS: 1,024, SMB: 1,024	NFS: 1,024, SMB: 1,024	
Maximum bandwidth for synchronization with OSS	10 Gbit/s	10 Gbit/s	10 Gbit/s	
Encrypted transmission to OSS	Yes	Yes	Yes	
Minimum cache capacity	40 GB	40 GB	40 GB	
Image format	OVA, VHD, and QCOW2	OVA, VHD, and QCOW2	OVA, VHD, and QCOW2	

Block gateways

Block gateways are classified into in-cloud block gateways and local block gateways. [Table 3](#) and [Table 4](#) show the specifications of these block gateways.

Specifications of in-cloud block gateways

Item	Description			
Type	Basic	Standard	Enhanced	Advanced
Storage protocol	iSCSI	iSCSI	iSCSI	iSCSI
Maximum number of local data volumes	4	8	16	16
Maximum volume capacity	256 TB	256 TB	256 TB	256 TB
Maximum number of clients concurrently connected to a gateway	Not limited	Not limited	Not limited	Not limited
Maximum bandwidth for synchronization with OSS	1 Gbit/s	2 Gbit/s	5 Gbit/s	10 Gbit/s
Encrypted transmission to OSS	Yes	Yes	Yes	Yes
Cache settings	Write-through and cache	Write-through and cache	Write-through and cache	Write-through and cache
Bandwidth	1 Gbit/s	2 Gbit/s	5 Gbit/s	10 Gbit/s

Specifications of local block gateways

Item	Description		
Recommended VM specifications	4-core, 8 GB memory	8-core, 16 GB memory	16-core, 32 GB memory
Storage protocol	iSCSI	iSCSI	iSCSI
Maximum volume capacity	256 TB	256 TB	256 TB
Recommended number of data volumes	16	64	128
Maximum number of data volumes	128	128	128
Maximum number of clients concurrently connected to a gateway	Not limited	Not limited	Not limited

Item	Description		
Encrypted transmission to OSS	Yes	Yes	Yes
Minimum cache disk capacity	20 GB	20 GB	20 GB
Image format	OVA, VHD, and QCOW2	OVA, VHD, and QCOW2	OVA, VHD, and QCOW2

5. Gateway models and specifications

This topic introduces different gateway models and specifications.

File gateways

- Models and features

The following table lists the features and scenarios supported by different gateway models.

	Basic	Standard	Enhanced	Advanced
Archive and storage	Not supported	Supported	Supported	Supported
Express sync	Not supported	Supported	Supported	Supported
Bandwidth	1 Gbit/s	2-2.5 Gbit/s	4.5-5 Gbit/s	10 Gbit/s
Capacity	64 TB	128 TB	256 TB	256 TB
Recommended cache disks	Ultra disks	Ultra disks	SSD and Enhanced SSD	SSD and Enhanced SSD
Recommended scenarios	Sharing and storage of a small volume of logs and data. Small websites and user-created FTP sites.	Sharing and storage of logs and data. Sharing data across multiple regions. Shared directories, user-created FTP sites, small-sized websites, data archives, and data warehouses.	Unified storage of data and logs. Archiving of large amounts of data. Data sharing among multiple regions. Medium-sized websites, virtual desktop infrastructure (VDI)-based shared directories, code libraries, and data warehouses.	Unified storage of data and logs. Archiving of large amounts of data. Data sharing among multiple regions. Large-sized websites, VDI-based shared directories, code libraries, and data warehouses.
Recommended number of active clients	≤ 5	≤ 20	≤ 50	≤ 150

- Features and prices

The following table lists the specifications of the express sync and remote sync features. Choose the features based on your actual needs.

	Number of files	Metadata synchronization rate	File change synchronization frequency	Monthly cost
Express sync	> 5,000,000	Maximum synchronization rate: 1,000 incremental files per second.	Less than one second. The maximum update interval is the refresh interval of the NFS/SMB client cache.	Fixed. If the number of API calls is less than 20,000,000, the cost of each month (30 days) is calculated as: $(2 + 0.5 \times \text{number of shares}) \times 30$.
Remote sync	< 5,000,000	The synchronization rate depends on the scanning and matching time.	More than 15 seconds. The maximum update time is two times of the remote sync interval.	Costs are based on the scanning interval and total number of files.

Block gateways

The following table lists the features and scenarios supported by different block gateway models.

	Basic	Standard	Enhanced	Advanced
Bandwidth	1 Gbit/s	2-2.5 Gbit/s	4.5-5 Gbit/s	10 Gbit/s
Recommended cache disks	Ultra Disk	Ultra Disk	SSD and Enhanced SSD	SSD and Enhanced SSD
Recommended scenarios	Large data disks (larger than 32 TB) and data backup volumes	Large data disks (larger than 32 TB), SMB volumes, and user-created FTP sites.	Large data disks (larger than 32 TB), medium-sized websites, DFS volumes, code libraries, and user-created FTP sites.	Large data disks (larger than 32 TB), medium-sized websites, DFS volumes, code libraries, and user-created FTP sites.
Recommended number of active volumes	≤ 2	≤ 4	≤ 8	≤ 16

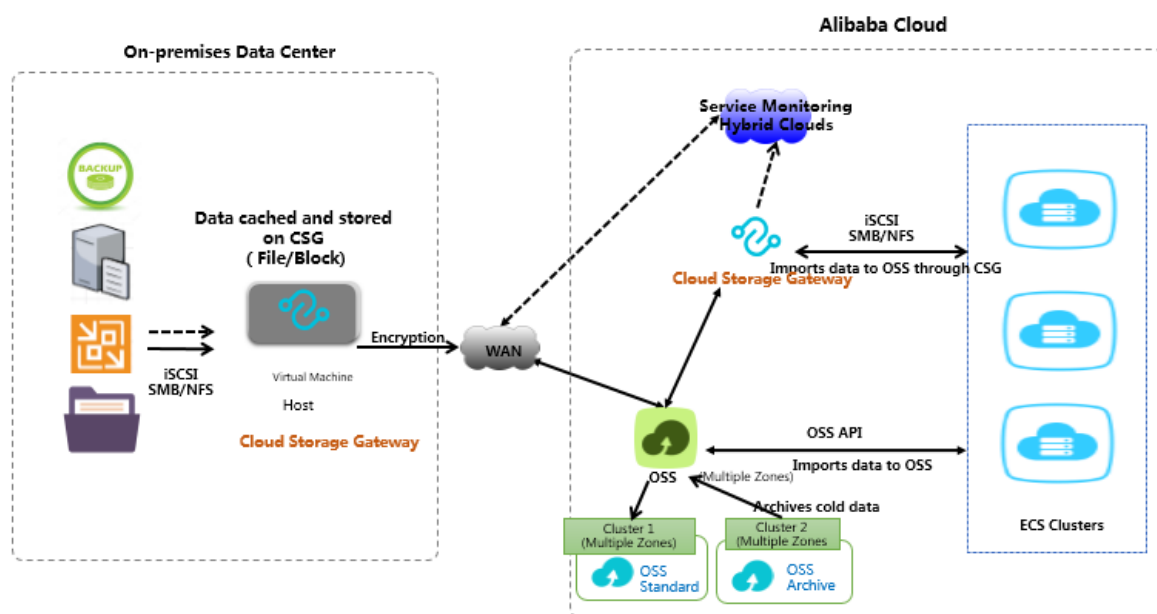
6.Scenarios

This topic describes the common scenarios for which Cloud Storage Gateway (CSG) is used.

Storage scale-out and data migration

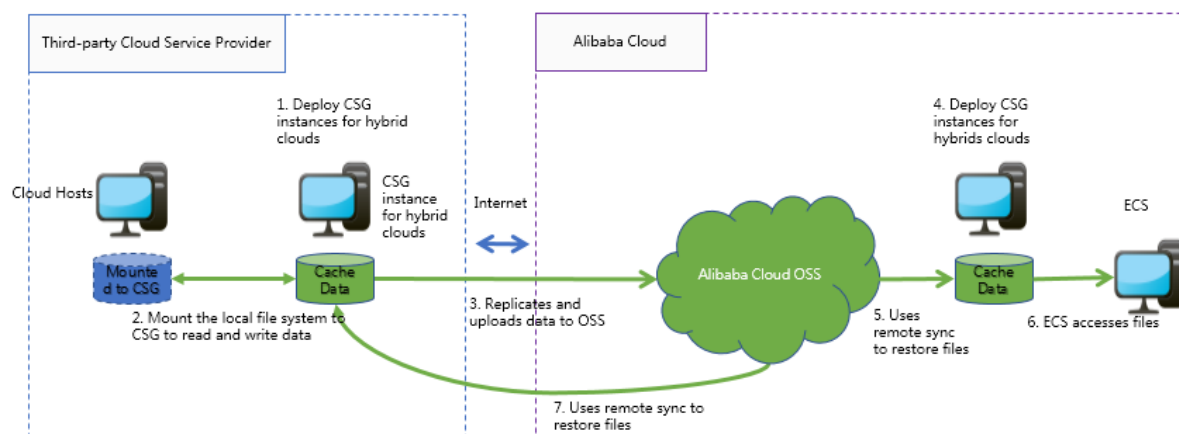
CSG is integrated with intelligent caching algorithms, which automatically distinguish between hot and cold data. This technology allows CSG to store cold data in the cloud and retain hot data in local caches to accelerate data retrieval. You can transfer a large amount of data in the cloud storage to a local center without additional configurations. This way, you can expand your data storage from a data center to the cloud. The cloud also retains a full copy of data. This ensures the integrity of both your hot and cold data. CSG can be used in the following scenarios:

- Share data and files: Files and data are shared among different computing clusters.
- Back up data: Data from applications is synchronized to Alibaba Cloud Object Storage Service (OSS) by using CSG and backup software, such as Veeam and NBU.
- Archive cold data: Cold data is written from local hosts or ECS instances to Infrequent Access (IA) or archive OSS buckets by using CSG. This way, local disk space can be freed up to improve ROI.



Cloud disaster recovery

As cloud computing becomes more widely used, an increasing number of users start to run their workloads in the cloud. Therefore, the reliability and continuity of workloads that are running in the cloud become critical issues. CSG supports virtualization. You can integrate third-party services with Alibaba Cloud services to perform disaster recovery.

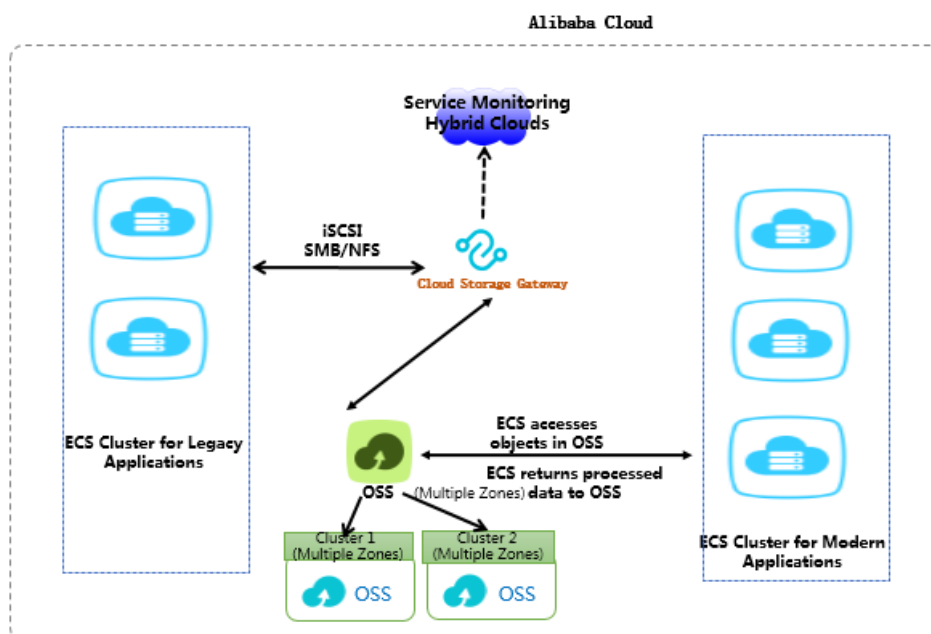


Cross-region data sharing and data distribution

You can deploy CSG instances in multiple regions and associate the CSG instances with the same OSS bucket to quickly share and distribute files across multiple regions. This feature is suitable for branch offices where data needs to be synchronized and shared.

Compatible with legacy applications

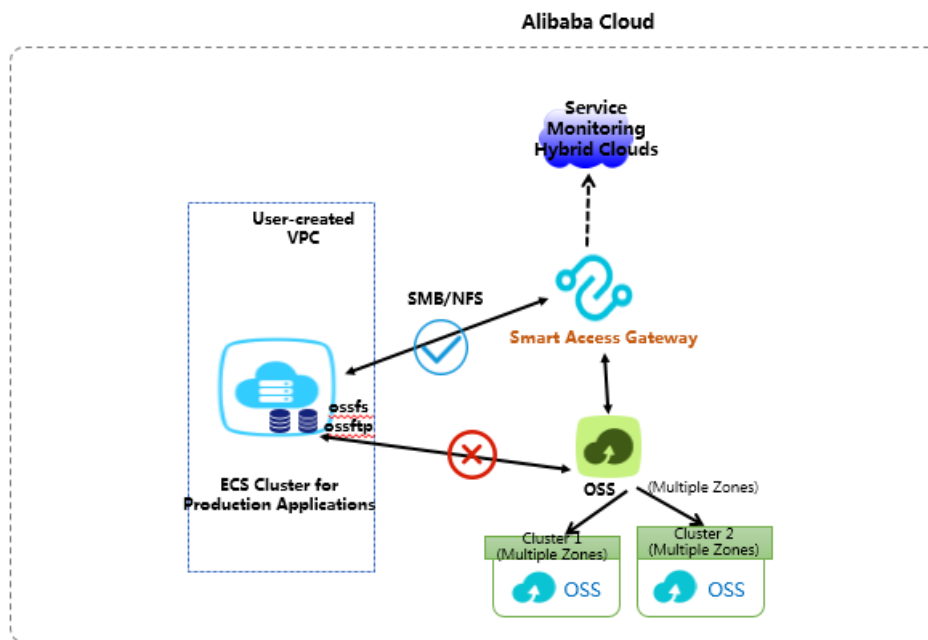
Some users may run both legacy and modern applications in the cloud. In this case, the legacy applications that are migrated from a data center use standard storage protocols, such as NFS, SMB, and iSCSI. In most cases, modern applications are developed based on cutting-edge technologies and support object access protocols. Data communication among applications over different protocols requires complicated operations. As a solution, CSG allows you to establish communications among applications over different protocols and enable data exchange between legacy applications and modern applications.



An alternative to ossfs and ossftp

ossfs and ossftp are open source tools based on file protocols. You can use ossfs and ossftp to directly upload files to OSS. However, ossfs and ossftp are not supported in the production environment due to their low compatibility with POSIX. Using ossfs and ossftp to mount file systems to a client also requires additional configurations and caches. In scenarios in which you need to use ossfs and ossftp to mount file systems on multiple clients, the configuration process may require a long period of time.

CSG is an excellent alternative to ossfs and ossftp. To accelerate access to data that is stored in OSS, create a CSG instance, then mount an NFS share on your local client, or map a Windows SMB share to a network drive. Then, you can manage data in the remote OSS bucket in the same way that you manage data in a local file system.



7. Service linked roles for CSG

This topic describes the following service linked roles of Cloud Storage Gateway (CSG): `AliyunServiceRoleForHCSSGW` and `AliyunServiceRoleForHCSSGWLogMonitor`. It also describes how to delete the roles.

Background information

Resource Access Management (RAM) provides the following service linked roles for CSG: `AliyunServiceRoleForHCSSGW` and `AliyunServiceRoleForHCSSGWLogMonitor`. These roles allow CSG to access the resources of other cloud resources.

In some scenarios, you may need to use CSG to create an elastic network interface, topics, queues, or subscriptions and use Key Management Service (KMS) to encrypt data. You may also need to use CSG to access, upload, download, and manage data in Object Storage Service (OSS) buckets. To do so, you can use the `AliyunServiceRoleForHCSSGW` service linked role to authorize CSG to access ECS resources, virtual private cloud (VPC) resources, KMS resources, and OSS resources.

In some scenarios, you may need to use CSG to obtain and push gateway logs. To do so, you can use the `AliyunServiceRoleForHCSSGWLogMonitor` service linked role to authorize CSG to access Log Service resources.

AliyunServiceRoleForHCSSGW

Note

`AliyunServiceRoleForHCSSGW` can be assigned only to a RAM user that has the `AliyunHCSSGWFullAccess` permission.

`AliyunServiceRoleForHCSSGW` can access the following cloud service:

- Elastic Network Interface and the relevant security groups

CSG must have the following permissions to provide a mount protocol by using ENI and the relevant permission groups:

```
{
  "Action": [
    "ecs:CreateNetworkInterface",
    "ecs:DeleteNetworkInterface",
    "ecs:DescribeNetworkInterfaces",
    "ecs:CreateNetworkInterfacePermission",
    "ecs:DescribeNetworkInterfacePermissions",
    "ecs:DeleteNetworkInterfacePermission",
    "ecs:CreateSecurityGroup",
    "ecs:DescribeSecurityGroups",
    "ecs:AuthorizeSecurityGroup",
    "ecs:DeleteSecurityGroup",
    "ecs:JoinSecurityGroup"
  ],
  "Resource": "*",
  "Effect": "Allow"
}
```

- VPC

CSG must have the following permissions to access your VPC resources:

```
{
  "Action": [
    "vpc:DescribeVpcs",
    "vpc:DescribeVSwitches"
  ],
  "Resource": "*",
  "Effect": "Allow"
}
```

- OSS

CSG must have the following permissions to upload, download, and manage OSS resources:

```
{
  "Action": [
    "oss:ListBuckets",
    "oss:ListObjects",
    "oss:GetObject",
    "oss:PutObject",
    "oss:DeleteObject",
    "oss:HeadObject",
    "oss:CopyObject",
    "oss:InitiateMultipartUpload",
    "oss:UploadPart",
    "oss:UploadPartCopy",
    "oss:CompleteMultipartUpload",
    "oss:AbortMultipartUpload",
    "oss:ListMultipartUploads",
    "oss:ListParts",
    "oss:GetBucketStat",
    "oss:GetBucketWebsite",
    "oss:GetBucketInfo",
    "oss:GetBucketEncryption",
    "oss:PutBucketEncryption",
    "oss:DeleteBucketEncryption",
    "oss:RestoreObject",
    "oss:PutObjectTagging",
    "oss:GetObjectTagging",
    "oss:DeleteObjectTagging"
  ],
  "Resource": "*",
  "Effect": "Allow"
}
```

- KMS

CSG must have the following permissions to perform server-side encryption or client-side encryption on data:

```
{
  "Action": [
    "kms:DescribeKey",
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": "*",
  "Effect": "Allow"
}
```

- Message Service

CSG must have the following permissions to configure express synchronization for gateways:

```
{
  "Action": [
    "mns:SendMessage",
    "mns:ReceiveMessage",
    "mns:PublishMessage",
    "mns>DeleteMessage",
    "mns:GetQueueAttributes",
    "mns:GetTopicAttributes",
    "mns:CreateTopic",
    "mns>DeleteTopic",
    "mns:CreateQueue",
    "mns>DeleteQueue",
    "mns:PutEventNotifications",
    "mns>DeleteEventNotifications",
    "mns:UpdateEventNotifications",
    "mns:GetEvent",
    "mns:Subscribe",
    "mns:Unsubscribe",
    "mns:ListTopic",
    "mns:ListQueue",
    "mns:ListSubscriptionByTopic"
  ],
  "Resource": "*",
  "Effect": "Allow"
}
```

- BSS

CSG must have the following permissions to collect and display the billing information of gateways:

```
{
  "Action": [
    "bss:DescribePrice"
  ],
  "Resource": "*",
  "Effect": "Allow"
}
```

AliyunServiceRoleForHCSSGWLogMonitor

Note

AliyunServiceRoleForHCSSGWLogMonitor can be assigned only to a RAM user that has the AliyunHCSSGWFullAccess permission.

AliyunServiceRoleForHCSSGWLogMonitor can access the following cloud services:

- Log Service

CSG must have the following permissions to configure log monitoring for gateways:

```
{
  "Action": [
    "log:PostLogStoreLogs",
    "log:GetLogStore"
  ],
  "Resource": "*",
  "Effect": "Allow"
}
```

Delete the service linked roles

Before you delete the AAliyunServiceRoleForHCSSGW or AliyunServiceRoleForHCSSGWLogMonitor service linked role, you must delete all gateways in the CSG console.

8.Usage notes

Before you run Cloud Storage Gateway (CSG) instances, read the following usage notes.

File gateways

- We recommend that you do not frequently interrupt the upload of large files to Network File System (NFS) or Server Message Block (SMB) shares. The system uploads files by using multipart uploads. If you interrupt the upload of large files, file fragments are generated in the associated Object Storage Service (OSS) bucket. These fragments occupy the capacity of the OSS bucket. Therefore, the storage usage of the OSS bucket is slightly higher than the total file size. You can use the automatic fragment deletion policy supported by OSS to manage file fragments. For more information, see [Manage parts](#).
- The cache capacity for file sharing is calculated based on the following formula: Recommended local cache capacity = [Application bandwidth (MB/s) - Backend bandwidth of a gateway (MB/s)] × Write duration (seconds) × 1.2.

To ensure a high I/O throughput when you use an on-premises cache disk, you can estimate the total amount of hot data. Compare the total amount of hot data with the recommended on-premises cache capacity, and select the higher value as the capacity of the on-premises cache disk.

- To write large files by using a file gateway, the size of each file must be smaller than 30% of the cache disk capacity. You cannot write multiple large files at the same time. Otherwise, the cache disk space will be exhausted.
- File gateways version 1.0.37 and earlier support files of up to 1.2 TB. Files larger than 1.2 TB cannot be uploaded to OSS. File gateways version 1.0.38 and later support files of up to 30 TB. If you upload a file larger than 2 TB, we recommend that you use an Internet bandwidth of 500 MB/s or higher, or connect to Alibaba Cloud over an Express Connect circuit. Otherwise, a timeout error may occur.
- File gateways support sparse files. If a sparse file fails to be uploaded to a file gateway, run the following command to convert the format of the sparse file:

```
dd if=<sparse file name> of=<sparse file name> conv=notrunc bs=1M
```

The size of the sparse file cannot exceed the available capacity of the cache disk.

- The names of file gateways and directories must be encoded in UTF-8. File gateways support only file names and directory names that are encoded in UTF-8. Other formats are not supported. For example, if you mount an NFS share of a file gateway on a Windows-based CSG agent, the files and directories that have Chinese names cannot be created. In this case, a 0x8007045D error is reported.
- If the size of a file in a file gateway exceeds 256 MB, we recommend that you disable versioning for the associated OSS bucket. Otherwise, a timeout error may occur when the gateway uploads metadata to the associated bucket. This degrades the performance of the gateway.
- File gateways implement permission isolation on Windows Active Directory (AD) based on POSIX Access Control Lists (ACLs). File gateways do not allow you to authorize multiple AD users across directories. Assume that the AA/BB/CC directory belongs to User 1. If you authorize User 2 to access only the CC directory, User 2 cannot access the data in the CC directory by using the AA/BB/CC directory. You must authorize User 2 to access the AA and BB directories.
- If you rename a file after you enable the ignore deletions feature for a file gateway, a copy of the file is generated in the OSS bucket. The copy has the new name. Both the file and the copy exist in the OSS bucket. This is because the rename operation in OSS is divided into the copy operation and the delete operation. If you enable the ignore deletions feature, all delete operations are prohibited.

File gateways deployed on Alibaba Cloud

- The CSG console uses the HTTPS protocol. Network storage protocols such as NFS and SMB require special ports. Therefore, you must configure a firewall or security group rules for the CSG console to support these ports.
 - CSG supports AD and LDAP domains. Therefore, you must configure specific ports to support the following protocols: Lightweight Directory Access Protocol (LDAP), AD, Domain Name System (DNS), and Kerberos. To configure security group rules, you must specify CIDR blocks and security groups. For more information, see [Add security group rules](#).

In a virtual private cloud (VPC) network, if a gateway and a domain server belong to different security groups of an Alibaba Cloud account, you can configure security group rules. For example, you can authorize connections between these two security groups. Then, you must add TCP 53/636 and UDP 53/636 as rules to the security group of the domain server.

- To support NFS and SMB, configure the corresponding service ports listed in the following table in the inbound rule of the security group of CSG. After you create a file gateway in the CSG console, these ports are configured for the security group by default. Configure ports for LDAP and AD in the inbound rules of the security group on the domain server.

Protocol	Port
HTTPS	443 and 8080
NFS	111 (UDP and TCP), 875 (UDP and TCP), 892 (UDP and TCP), 2049 (UDP and TCP), 32887 (UDP and TCP), 32888 (UDP and TCP), and 32889 (UDP and TCP)
SMB	137 (UDP), 138 (UDP), 139 (TCP), 389 (TCP), 445 (TCP), and 901 (TCP)
SSH	22
LDAP	389 (UDP and TCP) and 636 (UDP)
AD	445 (UDP and TCP)
DNS	53 (UDP and TCP)
Kerberos	88 (UDP and TCP)

- The synchronization bandwidth of a file gateway is determined by the OSS bandwidth. OSS provides an access bandwidth of up to 10 Gbit/s for a single user. The bandwidth slightly varies among clusters in different regions. For more information, contact the technical support of OSS in the region where your OSS buckets reside.
- After you create a file gateway on Alibaba Cloud, the gateway has a security group prefixed with Cloud_Storage_Gateway_Usage configured by default. Do not use this security group when you create ECS instances.
- When OSS stores more than one million files, we recommend that you set the interval of remote sync to longer than 3,600 seconds.
- A Multipurpose Internet Mail Extensions (MIME) is automatically specified in the OSS metadata based on the file suffix for file gateways version 1.0.36 and later.

- If remote sync is enabled, empty on-premises directories that are not uploaded to Alibaba Cloud may be deleted by remote sync during a scan cycle. You can create the directories again to address this issue.
- By default, the upload bandwidth of gateways deployed on Alibaba Cloud is 1 Mbit/s. These gateways access OSS buckets across regions over the Internet. As a result, the data transmission performance may be unstable.

On-premises file gateways

- To use file gateways deployed in data centers, you must open the following ports in the firewall of your CSG agent.

Protocol	Port
HTTPS	443
NFS	111 (UDP and TCP), 875 (UDP and TCP), 892 (UDP and TCP), 2049 (UDP and TCP), 32887 (UDP and TCP), 32888 (UDP and TCP), and 32889 (UDP and TCP)
SMB	137 (UDP), 138 (UDP), 139 (TCP), 389 (TCP), 445 (TCP), and 901 (TCP)
SSH	22
LDAP	389 (UDP and TCP) and 636 (UDP)
AD	445 (UDP and TCP)
DNS	53 (UDP and TCP)
Kerberos	88 (UDP and TCP)

Block gateways

- The cache capacity of Internet Small Computer Systems Interface (iSCSI) volumes is calculated based on the following formula: Recommended on-premises cache capacity = [Application bandwidth (MB/s) - Backend bandwidth of the gateway (MB/s)] × Write duration (seconds) × 1.2.

To ensure a high I/O throughput when you use an on-premises cache disk, you can estimate the total amount of hot data. Compare the total amount of hot data with the recommended on-premises cache capacity, and select the higher value as the capacity of the on-premises cache disk.

- The synchronization bandwidth of a block gateway is determined by the OSS bandwidth. OSS supports a maximum bandwidth of 10 Gbit/s. The bandwidth slightly varies among clusters in different regions. For more information, contact the technical support of OSS in the region where your OSS buckets reside.
- The default input/output operations per second (IOPS) are determined by the backend disk capacity. An ultra disk supports a maximum bandwidth of 110 MB/s. An SSD disk supports a maximum bandwidth of 230 MB/s.
- To use block gateways, you must open the following ports in the firewall of your CSG agent.

- Block gateways deployed on Alibaba Cloud

Protocol	Port
iSCSI	860 (TCP) and 3260 (TCP)

- Block gateways deployed in data centers

Protocol	Port
HTTPS	443
iSCSI	860 (TCP) and 3260 (TCP)

9. Reliability and consistency

This topic describes the reliability and consistency of Cloud Storage Gateway (CSG).

Reliability

- In the cache mode, data is written to a disk by using synchronous I/O to prevent data loss due to power failures.
- CSG ensures the durability and reliability of data in the local cache disks by using Alibaba Cloud disks.
- On-premises gateways depend on the reliability of the backend storage in your virtual environment. We recommend that you use Redundant Array of Independent Disks (RAID) storage or a distributed storage system as local cache disks.
- CSG refreshes and uploads data in the local cache disks to an OSS bucket. Alibaba Cloud OSS guarantees 99.999999999% reliability. This ensures data security and reliability when you transfer data from the gateway to Alibaba Cloud.

Consistency

- A 64-bit cyclic redundancy check (CRC-64) is implemented on the data that is uploaded to an OSS bucket from the gateway. If you send data from your data center to an OSS bucket, a checksum is generated and sent along with the data. Another checksum is generated by OSS and compared with the checksum that is received by OSS. If the two are equal, the uploading process is complete.
- If you upload a small file to an OSS bucket, the file gateway generates a checksum of the file. If you upload a large file in multiple parts to an OSS bucket, the file gateway implements CRC-64 on each part. This ensures consistency between the two checksums that are generated in your data center and the OSS bucket.
- A block gateway splits iSCSI volumes into storage allocation units. If you upload data in multiple units to an OSS bucket, the block gateway implements CRC-64 on the data in each unit. This ensures that the persistent data in the cloud is consistent with the data you write.