ALIBABA CLOUD

阿里云

云存储网关

产品简介

文档版本：20220329

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.什么是云存储网关CSG 05
2.云存储网关2.0公测版本 07
3.云存储网关软件版公测 08
4.功能特性 10
5.产品规格 12
6.选型推荐 15
7.使用场景 17
8.服务关联角色 21
9.使用须知 25
10.可靠性和一致性说明 28

1.什么是云存储网关CSG

云存储网关（Cloud Storage Gateway：简称CSG）是一款可以部署在用户本地数据中心和阿里云上的网关产品。它以阿里云对象存储（OSS）为后端存储，为云上和云下应用提供业界标准的文件服务（NFS和SMB）和块存储服务（iSCSI）。

云存储网关目前提供两种形态：

- 文件网关

  文件网关将OSS Bucket的对象结构与NAS文件系统的目录/文件建立映射关系。用户通过标准的NFS和SMB协议即可读写指定OSS Bucket里的对象。并且利用本地存储空间作为热数据缓存，使用户在享受OSS Bucket海量空间的同时，保障数据访问的高性能。文件网关还高度兼容POSIX和第三方备份软件。如果是小文件的备份和共享读写场景，推荐使用标准型或基础型文件网关；如果对性能有一定要求或者同时有多个客户端访问数据的用户，推荐使用增强型/性能型文件网关。

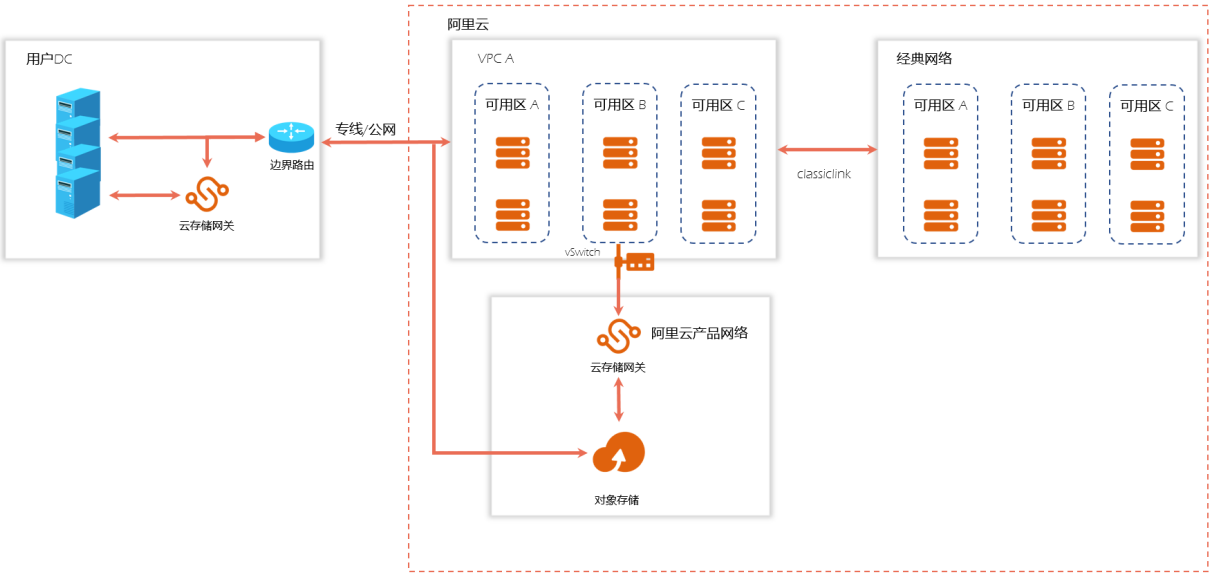
- 块网关

  块网关在OSS中创建存储卷，提供Internet小型计算机系统接口（iSCSI）协议访问。本地应用程序可将这些卷作为iSCSI目标进行访问。块网关提供两种模式：透传模式和缓存模式。透传模式可以将块卷数据切片同步上云，适用于专线等高速链路客户；缓存模式提供本地缓存盘进行读写加速，缓存数据异步上云，适用于期望本地快速访问但是上云链路慢的客户。

产品架构

云存储网关的云上服务和部署在客户数据中心的存储网关实例可以形成存储网关集群。通过这个集群，文件数据可以在云上集群和线下集群之间自由流动，帮助实现数据和业务的协同迁移，典型的场景有文件备份、数据分发和容灾。同时通过集群也可以实现在多个物理机房快速发布数据。

作为一个轻量级的存储网关，可在用户本地的数据中心部署，也可在阿里云上部署。



应用场景

- 文件网关
  - 在本地存储有限的情况下搭建一个海量文件系统的文件存储服务。
  - 将数据以对象形式存储在云端，但希望应用仍然以文件系统的方式访问文件而不需修改代码。
  - 在多个数据中心，通过文件存储服务的方式访问共享文件夹。

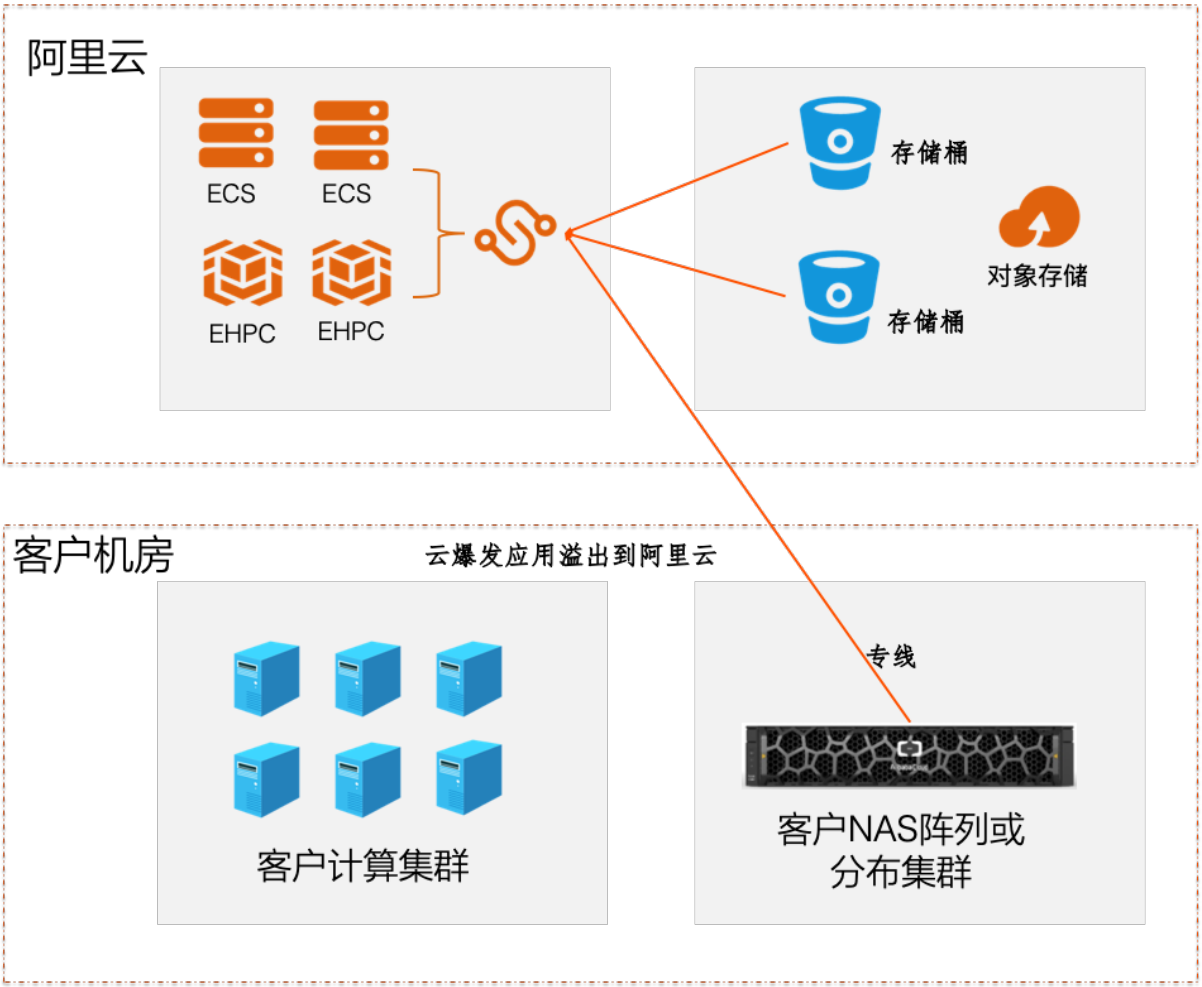
- 块网关
  - 通过备份软件备份数据到云上且备份软件支持iSCSI高效传输。
  - 将视频流数据通过iSCSI访问方式导入存储卷上，实现云上存储。

2.云存储网关2.0公测版本

云存储网关2.0版本（弹性网关）是一款可以部署在阿里云上的网关产品。您可以通过NFS客户端挂载网关节点，通过标准的POSIX接口读写虚拟化在同一个命名空间里的OSS或者NAS的数据。

产品架构

云存储网关2.0采用分布式架构，提供了全对称多活的数据访问和高性能读写的能力，实现多数据源的统一命名空间，方便您数据管理。同时支持带宽和容量动态扩展，方便您按需配置购买资源。云存储网关2.0采用ESSD提供高性能分布式缓存，以阿里云对象存储OSS为后端存储，提供最高99.9999999999%（12个9）的数据可靠性。通过网关2.0可以方便的将多个不同的数据源集成在同一个虚拟文件系统中提供统一的访问接口。



3.云存储网关软件版公测

云存储网关软件版是一款可以安装在阿里云用户ECS上的产品，使用云存储网关软件版可以实现将OSS Bucket挂载到ECS本地以POSIX文件接口进行访问。

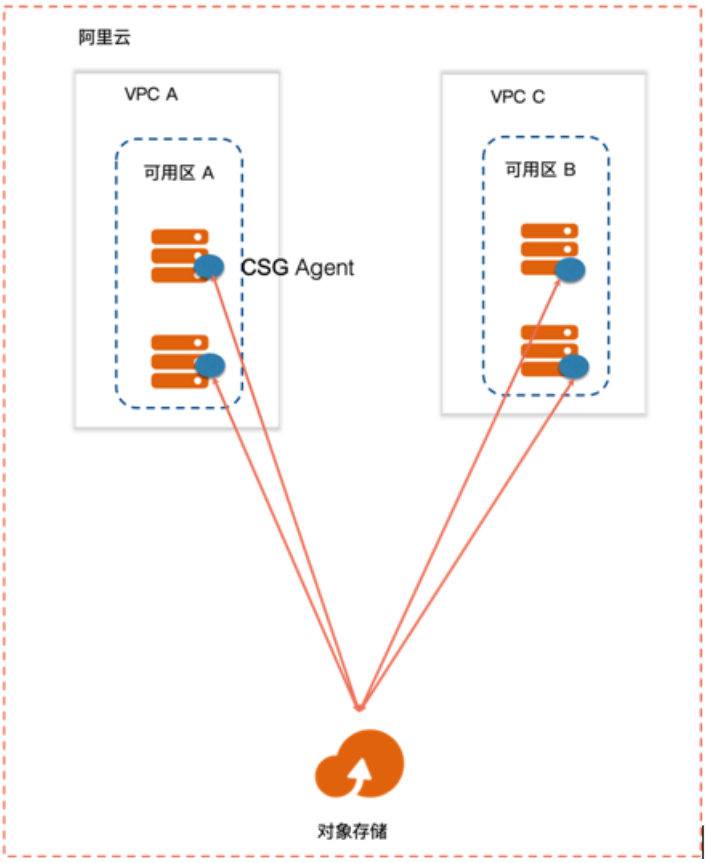
开放地域：华东2（上海）。

支持操作系统：CentOS 7和Alibaba Cloud Linux 2。

产品架构

云存储网关软件版直接部署在客户的ECS上，提供类似ossfs的功能，可以将OSS Bucket挂载到ECS的本地目录，从而可以像操作本地文件一样操作OSS里面的文件。和ossfs相比，稳定性更好并且功能也更丰富，在元数据管理和数据同步机制等多方面均有所优化。

- 以KV数据库缓存目录结构等元数据信息，执行ls命令等元数据操作更为高效。
- 以切片的方式高效组织并缓存文件数据，按需自动下载和淘汰。
- 以持久化日志的方式记录用户的每次写入删除等操作，并以异步的方式有序回放这些日志，用户操作延迟更低，体验更好。
- 写入数据以Sync IO的方式落盘，如果ECS意外重启，则数据也不会丢失。
- 用户重命名操作保证原子性，在异步回放时，实际是调用copy + delete object的API组合。
- 支持挂载OSS子目录。



云存储网关托管版和软件版对比

和云存储网关托管版相比，云存储网关软件版更加的轻量，在某些场景更加适合。比如云存储网关托管版有不同的规格，每个规格会对应具体的网络带宽，多客户端会共享固定带宽。如果客户端数目比较多的话，存储网关的网络带宽就可能会成为瓶颈，无法匹配所有客户端带宽的总能力。但是使用云存储网关软件版则可以突破这个限制，它安装于客户ECS内部，可以发挥出每个客户ECS带宽的完整能力。

下面分别列出了云存储网关托管版和云存储网关软件版的适用场景。

云存储网关托管版

- 云存储网关托管版支持NFS、SMB和iSCSI标准协议，对这些协议的某些特性有强需求，比如需要访问SMB共享并使用AD服务来鉴权，通过NFS服务指定某些客户端只读功能等。
- 多个客户端想看到统一的目录结构视图并保证操作互斥性，需要使用托管版本来保持唯一的视图，否则各个客户端看到的视图可能会有所不一致，操作也可能会有冲突，比如多个客户端同时修改同一个文件时需要保证顺序性。
- 如果需要在Windows下访问OSS Bucket，建议使用SMB共享以及托管版本的云存储网关，不推荐在Windows上访问NFS共享。
- 云存储网关托管版作为一个整体，阿里云可以提供更为完备的监控和运维能力，比如和云监控的集成。

云存储网关软件版

- 可以接受使用POSIX的文件接口来对OSS Bucket进行访问，主要诉求是读写文件，对于权限之类功能要求不高。
- 允许不同客户端同一时间看到的视图偏差（客户端是异步将操作回放到OSS，所以不同客户端会有偏差），多客户端基本可以认为互不干扰的独立存在。
- 客户端数目比较多，远大于单网关的处理能力，或者总体的带宽需求比较高，在满足前一条件的情况下，可以使用云存储网关软件版，并且可以使用批量挂载功能迅速部署。
- 客户端数目比较少，比如只有一两个客户端需要挂载使用OSS的情况，并且客户端之间的操作没有冲突，推荐使用云存储网关软件版这种轻量的方案。

4.功能特性

阿里云云存储网关提供文件网关和块网关两种类型，各类型网关分为多种规格。本文介绍不同类型规格的网关支持的功能特性。

文件网关

文件网关支持NFS和SMB这两种网络传输协议，两者都是基于局域网的网络文件传输协议。

- NFS协议主要用于Unix操作系统的文件系统访问，例如AIX、HP-UX及各种Linux系统。
- SMB协议主要用于Windows操作系统的文件系统访问。

文件网关功能特性支持列表

文件网关功能特性		基础型	标准型	增强型	性能型	相关文档
基础服务特性	缓存盘配置	√	√	√	√	管理缓存
	NFS/CIFS服务	√	√	√	√	管理共享
	AD/LDAP域	√	√	√	√	配置AD/LDAP/DNS
操作模块	编辑	√	√	√	√	相关操作
	编辑标签	√	√	√	√	管理标签
	备份	×	√	√	×	备份服务
	升级	√	√	√	√	升级
	升配网关	√	√	√	√	升配网关
	升级网络带宽	√	√	√	√	数据公网带宽配置
	上传日志	√	√	√	√	日志管理
高级功能特性	多bucket聚合	×	×	√	√	多Bucket聚合
	反向同步	√	√	√	√	管理共享
	极速同步	×	√	√	√	极速同步
	传输加速	√	√	√	√	传输加速
	服务端加密	√	√	√	√	创建共享
	网关侧加密	×	×	√	√	网关侧加密
	智能归档	×	√	√	√	管理共享

文件网关功能特性		基础型	标准型	增强型	性能型	相关文档
	智能缓存	√	√	√	√	无
	智能复制	√	√	√	√	数据下载
	忽略删除	√	√	√	√	管理共享
	MIME支持	√	√	√	√	无

说明 “√”表示支持，“×”表示不支持。

块网关

块网关主要通过iSCSI协议提供数据接入服务，iSCSI是一种基于因特网及SCSI-3协议下的存储技术。iSCSI可以既可以用于Windows操作系统访问，也可以用于Unix操作系统访问。

块网关功能特性支持列表

块网关功能特性		基础型	标准型	增强型	性能型	相关文档
基础服务特性	缓存盘配置	√	√	√	√	管理缓存
	iSCSI服务	√	√	√	√	管理iSCSI卷
操作模块	编辑	√	√	√	√	相关操作
	编辑标签	√	√	√	√	管理标签
	升级	√	√	√	√	升级
	升配网关	√	√	√	√	升配网关
	数据网络带宽配置	√	√	√	√	数据公网带宽配置
	上传日志	√	√	√	√	日志管理
高级功能特性	chap支持	√	√	√	√	创建iSCSI卷

说明 “√”表示支持，“×”表示不支持。

5.产品规格

本文介绍云上文件网关、本地文件网关、云上块网关、本地块网关的规格及相关信息。

文件网关

文件网关包括云上文件网关和本地文件网关，其产品规格说明如下所示。

云上文件网关规格说明表

网关规格	基础型	标准型	增强型	性能型
存储协议	NFSv3，NFSv4.0；SMB	NFSv3，NFSv4.0；SMB	NFSv3，NFSv4.0；SMB	NFSv3，NFSv4.0；SMB
文件数上限（建议值）	5000万	1亿	5亿	10亿
共享文件系统容量上限（建议值）	128 TB	256 TB	512 TB	1 PB
文件共享数量上限	NFS：4，SMB：4	NFS：8，SMB：8	NFS：15，SMB：15	NFS：15，SMB：15
最大可挂载客户端数	NFS：1024，SMB：1024	NFS：1024，SMB：1024	NFS：1024，SMB：1024	NFS：1024，SMB：1024
最大OSS同步带宽	1 Gbps	2 Gbps	5 Gbps	10 Gbps
是否支持上云传输加密	是	是	是	是
缓存容量区间	40 GB~1 TB	40 GB~2 TB	40 GB~32 TB	40 GB~32 TB
网关最大读带宽	1 Gbps	2.5 Gbps	5 Gbps	10 Gbps
网关最大写带宽	1 Gbps	2 Gbps	3 Gbps	5 Gbps

本地文件网关规格说明表

虚拟机推荐配置	4 Core/8 GB	8 Core/16 GB	16 Core/32 GB
存储协议	NFSv3/NFSv4.0，SMB	NFSv3/NFSv4.0，SMB	NFSv3/NFSv4.0，SMB
文件数上限（建议值）	5000万	5000万	5000万
共享文件系统容量上限（建议值）	128 TB	128 TB	128 TB
文件共享数量上限	NFS：2，SMB：2	NFS：4，SMB：4	NFS：8，SMB：8
最大可挂载客户端数	NFS：1024，SMB：1024	NFS：1024，SMB：1024	NFS：1024，SMB：1024
最大OSS同步带宽	10 Gbps	10 Gbps	10 Gbps

虚拟机推荐配置	4 Core/8 GB	8 Core/16 GB	16 Core/32 GB
上云传输加密	是	是	是
最小缓存盘容量	40 GB	40 GB	40 GB
镜像格式	OVA/VHD/QCOW2	OVA/VHD/QCOW2	OVA/VHD/QCOW2

块网关

块网关包括云上块网关和本地块网关，其产品规格说明如下所示。

云上块网关规格说明表

网关规格	基础型	标准型	增强型	性能型
存储协议	iSCSI	iSCSI	iSCSI	iSCSI
最大支持的本地数据卷数目	4	8	16	16
最大支持数据卷容量	256 TB	256 TB	256 TB	256 TB
并发访问最大客户端数	无限制	无限制	无限制	无限制
最大OSS同步带宽	1 Gbps	2 Gbps	5 Gbps	10 Gbps
上云传输加密	是	是	是	是
缓存配置	透传/缓存	透传/缓存	透传/缓存	透传/缓存
最大缓存容量	1 TB	2 TB	32 TB	32 TB
网关最大读带宽	1 Gbps	2.5 Gbps	5 Gbps	10 Gbps
网关最大写带宽	1 Gbps	2 Gbps	3 Gbps	5 Gbps

本地块网关规格说明表

虚机推荐配置	4 Core/8 GB	8 Core/16 GB	16 Core/32 GB
存储协议	iSCSI	iSCSI	iSCSI
最大支持数据卷容量	256 TB	256 TB	256 TB
推荐数据卷数目	16	64	128
最大数据卷数目	128	128	128
并发访问最大客户端数	无限制	无限制	无限制
上云传输加密	是	是	是

虚机推荐配置	4 Core/8 GB	8 Core/16 GB	16 Core/32 GB
最小缓存盘容量	20 GB	20 GB	20 GB
镜像格式	OVA/VHD/QCOW2	OVA/VHD/QCOW2	OVA/VHD/QCOW2

6.选型推荐

本文介绍在不同应用场景下推荐选择的云存储网关产品类型及特性。

文件网关

- 产品类型

  文件网关各产品规格支持的特性和推荐场景如下表所示。

功能特性	基础型	标准型	增强型	性能型
归档存储	不支持	支持	支持	支持
极速同步	不支持	支持	支持	支持
带宽	1 Gbps	2 Gbps~2.5 Gbps	4.5 Gbps~5 Gbps	10 Gbps
容量	128 TB	256 TB	512 TB	1 PB
推荐缓存	高效云盘/SSD云盘/ESSD云盘	SSD云盘/ESSD云盘	SSD云盘/ESSD云盘	SSD云盘/ESSD云盘
推荐场景	小规模日志/数据共享存储、小型网站、自建FTP	日志/数据共享存储、共享目录、自建FTP、小型网站、数据归档、多地数据共享、备份数据仓库	中型网站，日志/数据统一存储，共享目录（VDI），大规模数据归档，代码库，多地数据共享，备份数据仓库	大型网站，日志/数据统一存储，共享目录（VDI），大规模数据归档，代码库，多地数据共享，备份数据仓库
推荐活跃客户端数	不超过5个	不超过20个	不超过50个	不超过150个

- 产品特性

  文件网关的极速同步和反向同步特性的规格如下表所示，您可以根据情况进行选择。

功能特性	文件规模	元数据同步速率	文件变化同步频率	月成本
极速同步	500 万个以上	同步速率最高可达1,000增量文件/秒。	亚秒级（最大更新间隔为NFS/SMB客户端缓存刷新时间）	成本固定，在API调用小于2,000 万次的情况下，每月（按30天计算）成本计算方式如下：（2+0.5x共享数）x30
反向同步	500 万个以下	同步速率取决于扫描比对的时间，难以估算。	大于15秒（最大更新间隔为反向同步时间间隔的2倍）	成本取决于扫描时间间隔和总文件数，难以估算。

块网关

块网关各产品规格支持的特性和推荐场景如下表所示。

功能特性	基础型	标准型	增强型	性能型
带宽	1 Gbps	2 Gbps~2.5 Gbps	4.5 Gbps~5 Gbps	10 Gbps
推荐缓存	高效云盘/SSD云盘/ESSD云盘	SSD云盘/ESSD云盘	SSD云盘/ESSD	SSD云盘/ESSD
推荐场景	超大数据盘（大于32 TB）、数据备份卷	超大数据盘（大于32 TB）、SMB共享数据卷、自建FTP	超大数据盘（大于32 TB）、中型网站、DFS共享数据卷、代码库、自建FTP	超大数据盘（大于32 TB）、中型网站、DFS共享数据卷、代码库、自建FTP
推荐活跃数据卷	不超过2个	不超过4个	不超过8个	不超过16个

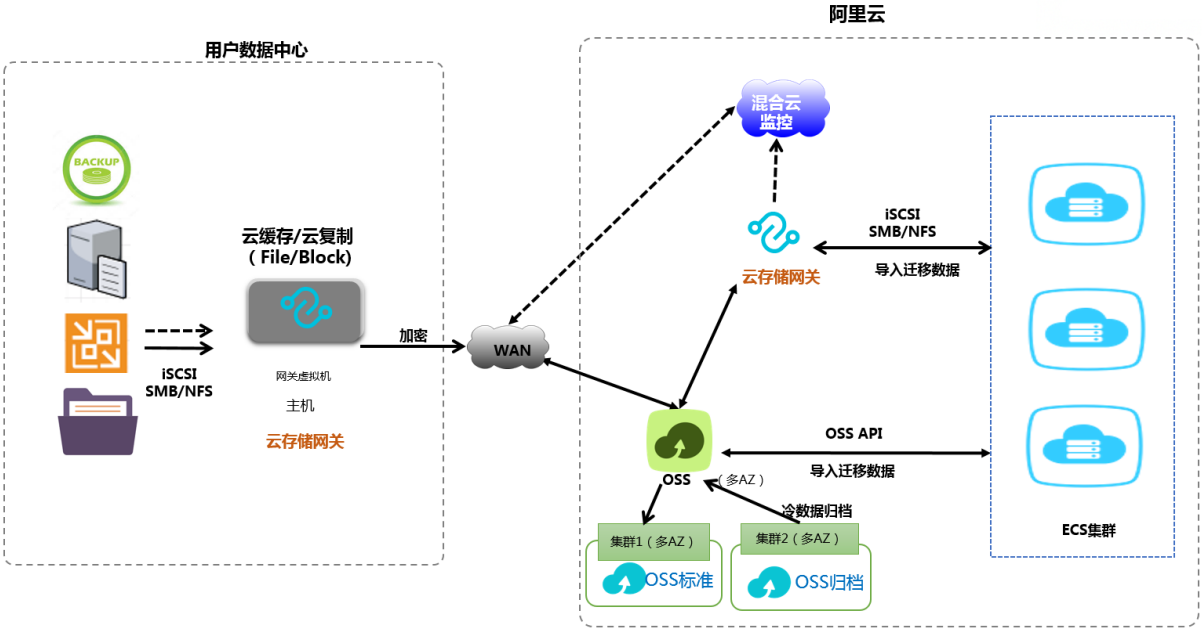
7.使用场景

本文介绍云存储网关的主要应用场景。

云存储扩容和迁移

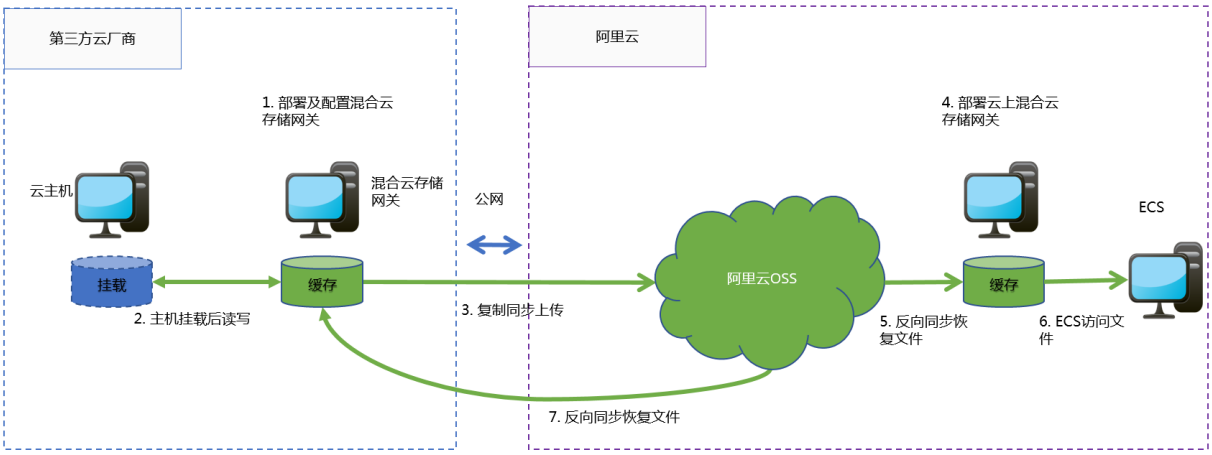
集成智能缓存算法，自动识别冷热数据，将热数据保留在本地缓存，保证数据访问体验，无感知的将海量云存储数据接入本地数据中心，拓展存储空间。同时在云端保留全量数据（冷+热）保证数据的一致性。具体的使用场景如下所示。

- 共享文件池：在不同计算集群之间共享文件和数据。
- 数据备份：通过类似Veaam，NBU等备份软件，将一些应用数据按一定策略通过云存储网关备份到阿里云OSS。
- 冷数据归档：可以将冷数据从本地或者ECS实例中通过云存储网关写入OSS的低频和归档Bucket中，释放本地空间，提高存储的效费比。



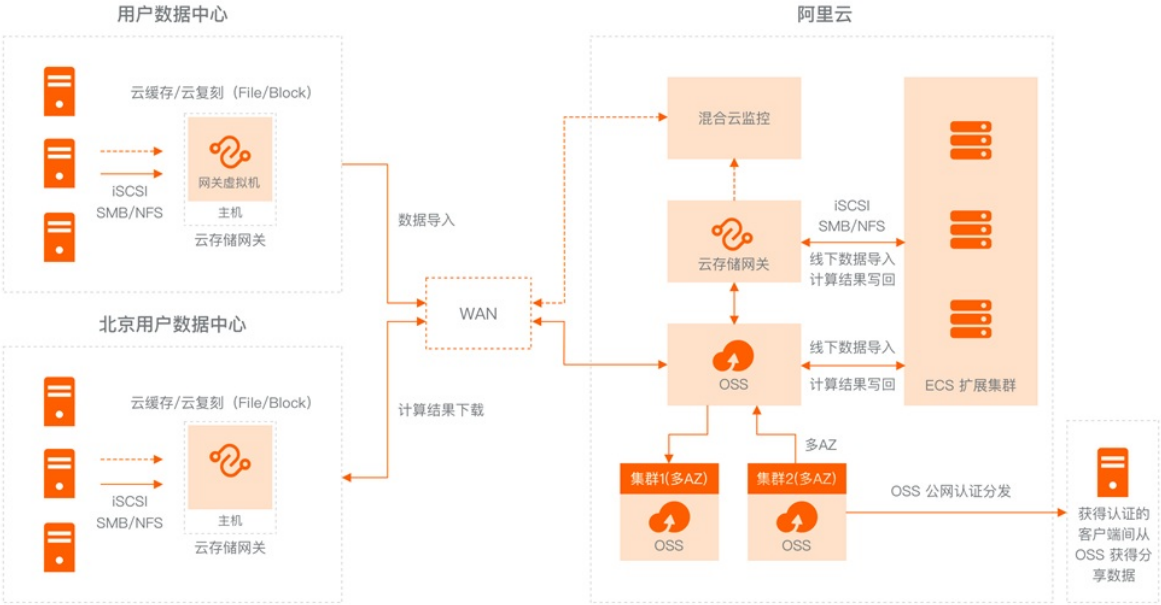
云容灾

随着云计算的普及，越来越多的用户把自己的业务放到了云上。但是随着业务的发展，如何提高业务的可靠性和连续性，跨云容灾是一个比较热门的话题。借助云存储网关对虚拟化的全面支持，可以轻松应对各种第三方云厂商对接阿里云的数据容灾。



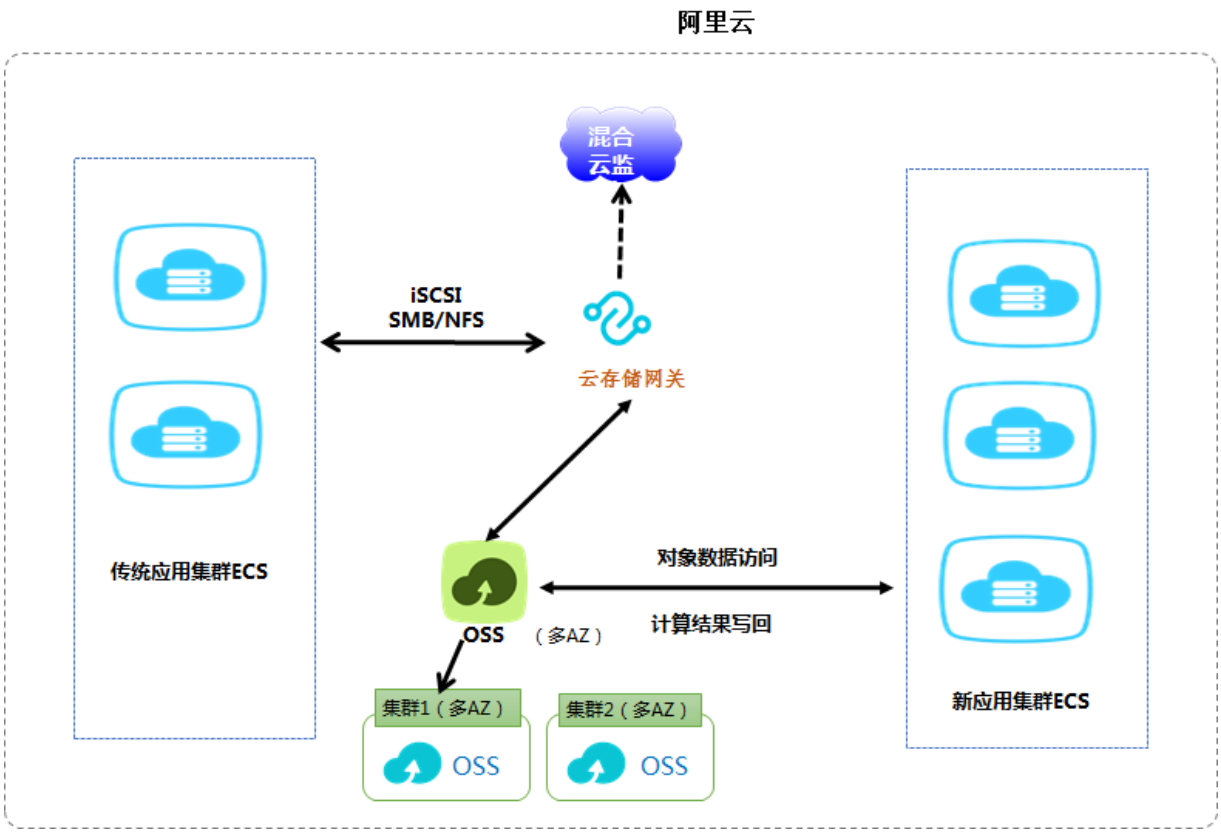
多地数据共享和分发

通过多个异地部署的文件网关实例，对接同一个阿里云OSS Bucket，可以实现快速的异地文件共享和分发，非常适合多个分支机构之间互相同步和共享数据。



适配传统应用

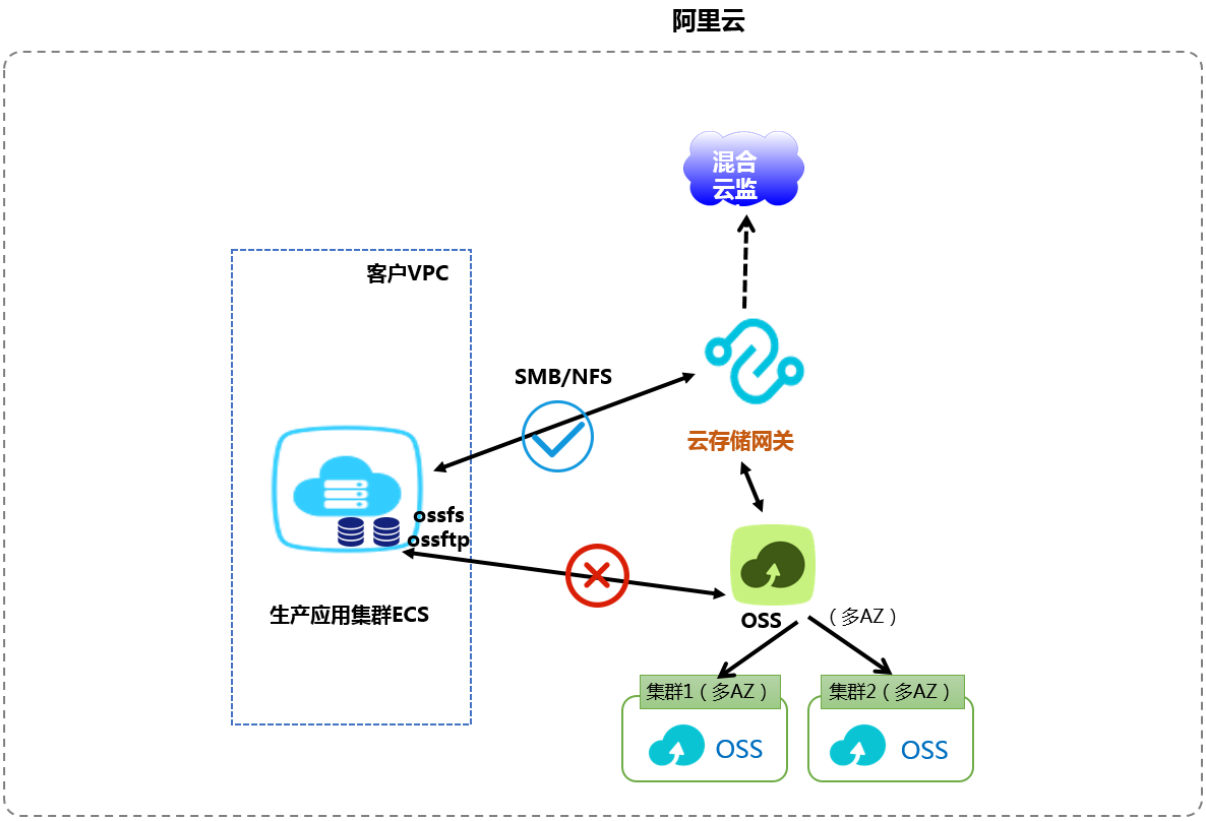
有很多用户在云上的业务是新老业务的结合，老业务是从数据中心迁移过来的使用的是标准的存储协议，例如：NFS，SMB，iSCSI。新的应用往往采用比较新的技术，支持对象访问的协议。如何沟通两种业务之间的数据是一个比较麻烦的事情，云存储网关正好起到一个桥梁的作用，可以便捷的沟通新旧业务，进行数据交换。



替代ossfs和ossftp

ossfs和ossftp都是基于文件协议的开源工具，用户可以通过它们直接上传文件到OSS。但是这两个开源文件都不支持在生产环境使用（POSIX兼容度低），同时挂载在用户的客户端需要额外的配置和缓存资源，对于多个客户端的情况安装配置繁琐。

通过文件网关的服务可以完美替代ossfs和ossftp。通过创建文件网关，用户只需要执行简单的挂载（NFS）和映射（Windows SMB）就可以像使用本地文件系统一样使用OSS。


阿里云
混合
云监
客户VPC
SMB/NFS
云存储网关
ossfs
ossftp
生产应用集群ECS
OSS
（多AZ）
集群1（多AZ）
OSS
集群2（多AZ）
OSS

8.服务关联角色

本文为您介绍什么是云存储网关服务关联角色（AliyunServiceRoleForHCSSGW和AliyunServiceRoleForHCSSGWLogMonitor）以及如何删除服务关联角色。

背景信息

网关服务关联角色（AliyunServiceRoleForHCSSGW和AliyunServiceRoleForHCSSGWLogMonitor）是指在某些情况下，为了完成网关自身的某个功能，需要获取其他云服务的访问权限，从而提供的RAM角色。

网关服务可能需要创建弹性网卡以及消息主题、队列、订阅等对象，使用密钥管理进行数据加密，对OSS数据进行上传下载管理访问等，可通过自动创建的网关服务关联角色（AliyunServiceRoleForHCSSGW）获取访问ECS、VPC、KMS、OSS等资源的权限。

对于日志监控功能，网关服务可能需要获取和推送网关日志，可通过自动创建的网关服务关联角色（AliyunServiceRoleForHCSSGWLogMonitor）获取访问SLS资源的权限。

AliyunServiceRoleForHCSSGW权限说明

> **说明**
>
> RAM用户需具有AliyunHCSSGWFullAccess权限才能创建AliyunServiceRoleForHCSSGW。

AliyunServiceRoleForHCSSGW具备以下云服务的访问权限：

- ECS弹性网卡及安全组相关权限

网关服务需使用弹性网卡（以及相关安全组）来提供挂载协议。

```
{
      "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"
    }
```

- 专有网络VPC的访问权限

网关服务需使用以下权限来访问您的VPC相关资源。

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

- 对象存储OSS的访问权限

网关服务需要使用以下权限对您的数据进行OSS上传，下载及管理。

```
{
      "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"
    }
```

- 密钥管理KMS的权限

网关服务需要使用以下权限对您的数据进行服务端加密（OSS端加密）或客户端加密（网关侧加密）。

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

- 消息MNS的权限

网关服务需要使用以下权限来完成网关极速同步功能的相关配置。

```
{
      "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（交易和账单管理）的权限

网关服务需要使用以下权限来获取展示网关相关价格信息。

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

AliyunServiceRoleForHCSSGWLogMonitor权限说明

> **说明**
>
> RAM用户需具有AliyunHCSSGWFullAccess权限才能创建AliyunServiceRoleForHCSSGWLogMonitor。

AliyunServiceRoleForHCSSGWLogMonitor具备以下云服务的访问权限：

- 日志SLS的权限

网关服务需要使用以下权限来完成网关日志监控功能的相关配置。

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

删除服务关联角色

如果您需要删除网关服务关联角色（AliyunServiceRoleForHCSSGW或AliyunServiceRoleForHCSSGWLogMonitor），您需要先删除网关服务下的所有网关实例。

9.使用须知

为了保证云存储网关实例的正常运行，在使用之前，请您务必认真阅读以下使用须知。

文件网关须知

- 建议不要频繁中断大文件拷贝到NFS或SMB共享文件夹。由于后台的分段上传机制，中断大文件拷贝会造成碎片遗留在OSS。这些碎片会影响OSS的空间统计，造成OSS空间统计略大于看到的文件总量。通过OSS的碎片自动删除策略，可以帮助用户管理碎片，详情请参见管理碎片。
- 文件共享的缓存区估算公式为：本地建议缓存容量=（应用带宽（MB/s）-网关后端带宽（MB/s））×写入时长（s）×1.2。

  如果您需要获得较好的本地访问性能，可以先预估总的热数据容量。取总的热数据容量和本地建议缓存容量的最大值为本地缓存盘容量。
- 如果使用文件网关写入较大的文件，单一文件大小应保持在缓存盘容量的30%以下，且不能多个大文件并发写入，否则容易造成缓存盘写满的情况。
- 1.0.37及之前版本的文件网关支持的最大文件大小是1.2TB。超过该值，文件将无法上传至OSS。1.0.38及之后版本的文件网关支持最大30TB的文件上传。在上传超大文件时（大于2TB），建议用户的公网带宽不低于500MB/s或者采用专线连接阿里云，否则可能出现上传超时的问题。
- 文件网关支持Sparse file。如果上传Sparse file到文件网关失败，请运行以下命令转化。

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

  目前，支持的Sparse File文件大小要求不超过可用缓存盘的大小。
- 文件网关的文件名和目录名必须使用UTF-8编码。文件网关暂不支持非UTF-8编码的文件名或目录名。例如，如果在Windows下挂载文件网关的NFS共享，那么大部分中文文件和中文目录都会创建失败，这时Windows会返回0x8007045D的错误。
- 文件网关中的单个文件超过256 MB的情况下，不建议开启Bucket的多版本功能。否则会出现文件元数据上传超时，影响网关整体性能。
- 文件网关是基于POSIX ACL实现Windows AD的权限访问隔离，不支持跨目录层级的多AD用户授权。例如：目录层级AA/BB/CC，属于用户1。此时仅授予用户2访问（读写/只读）目录CC的权限，用户2无法利用AA/BB/CC全路径直接访问CC下的数据，需要把AA和BB都对用户2授权，才能保证数据对用户2可见。

云上文件网关须知

- 存储网关控制台采用HTTPS协议。NFS或SMB等网络存储协议用到一些特殊的端口，需要通过防火墙或者安全组开通服务。
  - 云存储网关支持AD/LDAP域，新增需配置的端口有：LDAP、AD、DNS、Kerberos。安全组授权包括IP段和安全组授权，具体方法请参见添加安全组规则。

    安全组授权是指在同一VPC和账号下，可以跨安全组授权。例如：将云存储网关所在安全组授权给域服务器所在安全组，另外在域服务器所在安全组中再加上2条规则：TCP 53/636和UDP 53/636即可。

- NFS/SMB所需的端口是在云存储网关入方向的安全组中配置，云上文件网关创建好后安全组默认配置好这些端口，无需手动配置。LDAP/AD是在域服务器所在安全组入方向的端口配置。

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

- 网关同步带宽根据OSS带宽限制制定，目前OSS为每个用户提供的最大访问带宽为10 Gbps。各区域的集群略有差异，请提交工单咨询。
- 创建云上文件网关后，会默认创建一个前缀为Cloud_Storage_Gateway_Usage的安全组，创建ECS时请避免使用此安全组。
- 在OSS文件数超过百万级别后，建议设置比较大的反向同步间隔（>3600s）。
- 从1.0.36版本开始支持按照文件后缀名自动在OSS的对象元数据里设置MIME类型。
- 在反向同步打开的情况下，在一个扫描周期中会出现本地未上云的空目录被反向同步进程删除的情况，再次创建目录即可修复。
- 默认的在线云存储网关只有1 Mb/s的公网带宽上行带宽，在跨地域访问OSS时使用的是公网，不保证传输质量和速度。

本地文件网关须知

- 本地文件网关需在客户端的防火墙中打开以下端口。

协议	端口
HTTPS	443
NFS	111（TCP、UDP），875（TCP、UDP），892（TCP、UDP），2049（TCP、UDP），32887（TCP、UDP），32888（TCP、UDP），32889（TCP、UDP）
SMB	137（UDP），138（UDP），139（TCP），389（TCP），445（TCP），901（TCP）
SSH	22

协议	端口
LDAP	389（UDP，TCP），636（UDP）
AD	445（TCP、UDP）
DNS	53（TCP、UDP）
Kerberos	88（TCP、UDP）

块网关须知

- iSCSI卷缓存区估算格式：本地建议缓存容量=（应用带宽（MB/s）-网关后端带宽（MB/s））×写入时长（s）×1.2

  如果您需要获得较好的本地访问性能，可以先预估总的热数据容量。取总的热数据容量和本地建议缓存容量的最大值为本地缓存盘容量。
- 块网关同步带宽根据OSS带宽限制制定，目前OSS为每个用户提供的最大访问带宽为10Gbps。各区域的集群略有差异，请向各区域OSS客户支持人员查询。
- 缺省配置的IOPS受限于后端云盘的能力。高效云盘的最大带宽为110MB/s，SSD云盘的最大带宽为230MB/s。
- 块网关需在客户端的防火墙中打开以下端口。
  - 云上块网关

协议	端口
iSCSI	860（TCP）、3260（TCP）

  - 本地块网关

协议	端口
HTTPS	443
iSCSI	860（TCP）、3260（TCP）

10.可靠性和一致性说明

本文介绍云存储网关的可靠性和一致性。

可靠性

- 网关缓存模式采用同步IO（Sync IO）落盘，确保掉电不丢失数据。
- 云上网关依托于阿里云云盘的高可靠性，确保了缓存盘的数据持久可靠。
- 本地部署的网关依赖于您虚拟环境后端存储的可靠性，建议您使用RAID存储或高可靠分布式存储作为缓存盘。
- 网关将缓存盘的新数据刷新上传到OSS Bucket，依托OSS数据设计持久性不低于99.9999999999%（12个9）保证了数据的安全可靠，进而确保了数据从进入网关到上传云端整条链路的高可靠性。

一致性

- 网关上传到OSS Bucket的数据执行严格的CRC64校验，经本地计算CRC64值上传到OSS Bucket之后获取OSS服务端计算的CRC64值，比对通过之后即为上传成功。
- 文件网关对于小文件上传会计算整个文件的CRC64值；对于大文件的上传，通过MulitiPart分片上传，会对每个分片执行CRC64校验，从而确保整个文件在本地的CRC64值与OSS Bucket一致。
- 块网关会将整个iSCSI卷按照您指定的存储分配单元进行切分，对上传到OSS Bucket的每个存储单元切片执行CRC64校验，确保云上持久化数据与您写入的数据是一致的。