Scalable File Service (SFS)
8.6.0

Service Overview

Issue	01
Date	2025-09-30

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

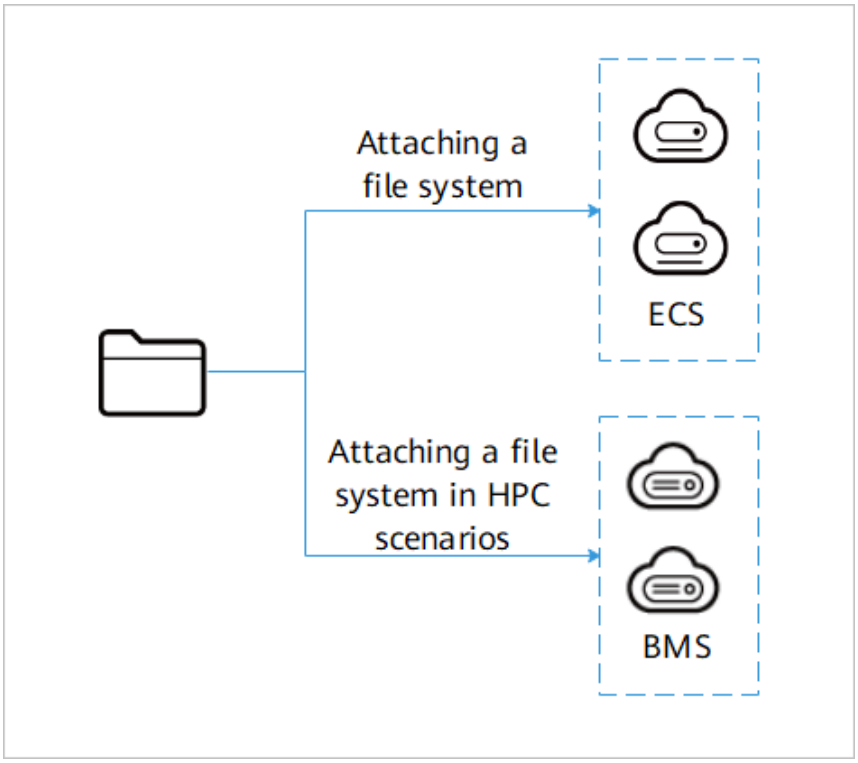
Contents

1 What Is Scalable File Service?

Definition

Scalable File Service (SFS) provides Elastic Cloud Servers (ECSs) and Bare Metal Servers (BMSs) in high-performance computing (HPC) scenarios with a high-performance shared file system that can be scaled on demand. It is compatible with standard file protocols (NFS, CIFS, and DPC) and is scalable to petabytes of capacity to meet the needs of massive amounts of data and bandwidth-intensive applications. **Figure 1-1** describes how to use SFS.

Figure 1-1 SFS function definition



Functions

SFS provides the following functions:

- Creating a file system

  Before using SFS, you must create a file system.
- Attaching a file system

  After a file system is created, you need to attach it to an ECS.
- Managing a file system

  You can manage file systems, including adjusting capacity, viewing, uninstalling, restoring, and deleting file systems.

Comparison Between EVS and SFS

Table 1-1 compares EVS and SFS.

Table 1-1 Comparison between EVS and SFS

Dimension	EVS	SFS
Usage	Provides persistent block storage for compute services such as ECS and BMS. EVS disks feature high availability, high reliability, and low latency. You can format, create file systems on, and persistently store data on EVS disks.	Provides compute services such as ECSs and BMSs (in HPC scenarios) with a high-performance shared file system that supports on-demand elastic scaling. The file system complies with the standard file protocol and delivers scalable performance, supporting mass amount of data and bandwidth-demanding applications.
Data access mode	Data access is limited within the internal network of a data center.	Data access is limited within the internal network of a data center.
Sharing mode	Supports EVS disk sharing. A shared EVS disk can be attached to a maximum of 16 ECSs in the cluster management system.	Supports data sharing. A file system can be mounted to a maximum of 256 ECSs.
Storage capacity	The maximum capacity of a single disk is 64 TB.	The capacity is unlimited. Therefore, advance planning is not required. The file system capacity can be elastically scaled to the PB level.
Storage backend	Supports Huawei SAN storage and Huawei Distributed Block Storage.	OceanStor 9000 files, OceanStor Dorado files, OceanStor files, and OceanStor Pacific files

Dimension	EVS	SFS
Recommended scenarios	Scenarios such as databases, enterprise office applications, and development and testing.	Scenarios such as media processing and file sharing.

2 Related Concepts

Availability Zone

Availability Zones (AZs) are geographical zones that use independent power supplies and networks in the same service region. One region has multiple AZs. If one AZ becomes faulty, the other AZs in the region can still provide services. AZs in the same region access each other through the intranet. An ECS can share a file system across AZs in the same region.

NFS

Network File System (NFS) is a distributed file system protocol that allows different computers and operating systems to share data over a network.

CIFS

Common Internet file system (CIFS) is a protocol used for network file access. CIFS is an open SMB protocol version that allows programs to access files on remote computers over Internet and requires the computers to provide services. Through the CIFS protocol, network files can be shared between hosts running Windows.

File System

A file system provides users with shared file storage service through NFS, CIFS, or DPC. It can be used to access network files remotely. After users create shared directories in the management console, the file system can be mounted to multiple ECSs and is accessible through the standard POSIX interface.

File system HyperMetro

A pair of file systems on the active-active storage devices form a HyperMetro pair to process services simultaneously and back up each other. In the event of a storage device fault, the other storage device automatically takes over services, ensuring high data reliability and service continuity.

Storage SLA

A storage Service Level Agreement (SLA) is a group of service capabilities that can be selected when you apply for file storage resources. You can apply for a file system based on the SLA.

VPC

Virtual Private Cloud (VPC) enables you to provision logically isolated, configurable, and manageable virtual networks for ECSs, improving the security of resources in the system and simplifying network deployment.

You can select IP address ranges, create subnets, customize security groups, and configure route tables and gateways in a VPC, which enables you to manage and configure your network conveniently and modify your network securely and rapidly. You can also customize access rules and firewalls to control ECS access within a security group and across different security groups to enhance security of ECSs in the subnet.

In addition, you can create a Virtual Private Network (VPN) between the enterprise data center or private network and the VPC without using an external IP address for port forwarding.

HPC

HPC is a computer cluster system that connects computer systems using interconnection technologies. It relies on the integrated compute capability of all the connected systems to execute computing tasks at scale. For this reason, HPC is also referred to as an HPC cluster.

DPC

Distributed Parallel Client (DPC) runs on compute nodes as a storage client and exchanges data with storage backend nodes over a network protocol.

WORM

In the storage industry, write once read many (WORM) is the most common method used to archive and back up data, ensure secure data access, and prevent data tampering.

3 Product Highlights

- Ease of use

  An easy-to-use operation interface is provided for you to quickly create and manage file systems without worrying about the deployment, expansion, and optimization of file systems.
- File sharing

  Multiple ECSs of different types can concurrently access videos and images.
- Support for mainstream file protocols

  Mainstream NFS, CIFS, and DPC protocols which you are used to are supported in common OS environments.
- On-demand capacity allocation and elastic scaling

  You can configure the initial storage capacity of a file system based on service requirements, and expand or reduce the file storage capacity based on service changes.
- High performance and reliability

  The total bandwidth of a file system can increase with the capacity expansion, which is suitable for high-bandwidth applications. In addition, data durability is ensured to meet service growth requirements.
- Automatic attachment

  After installing the automatic attachment plug-in on a VM, you can select a shared file system on the SFS page and the file system is automatically attached to the VM.

4 Application Scenario

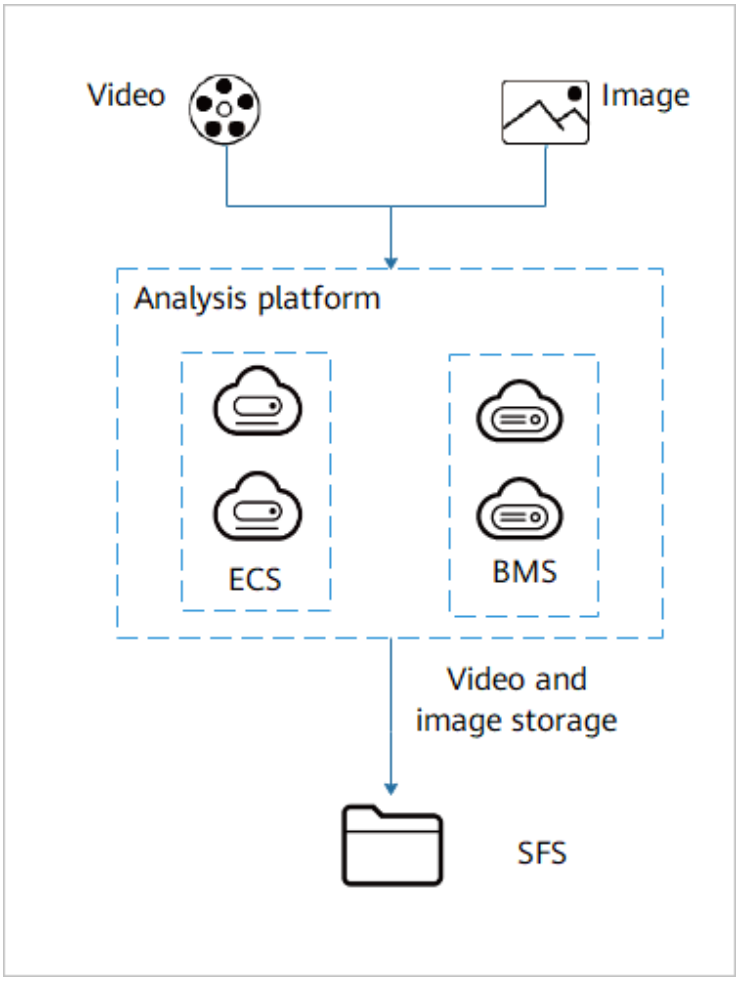
Video Cloud

SFS applies to the video cloud scenario to store video and image files.

Figure 4-1 shows the architecture of the video cloud scenario.

- Video files vary with specific independent software vendors (ISVs). Generally, they are 1 GB to 4 GB large files.
- Images are classified into checkpoint images and analysis images. Generally, they are massive amounts of small images (about 2 billion images in a year) with sizes ranging from 30 KB to 500 KB.

Figure 4-1 Architecture of the video cloud scenario

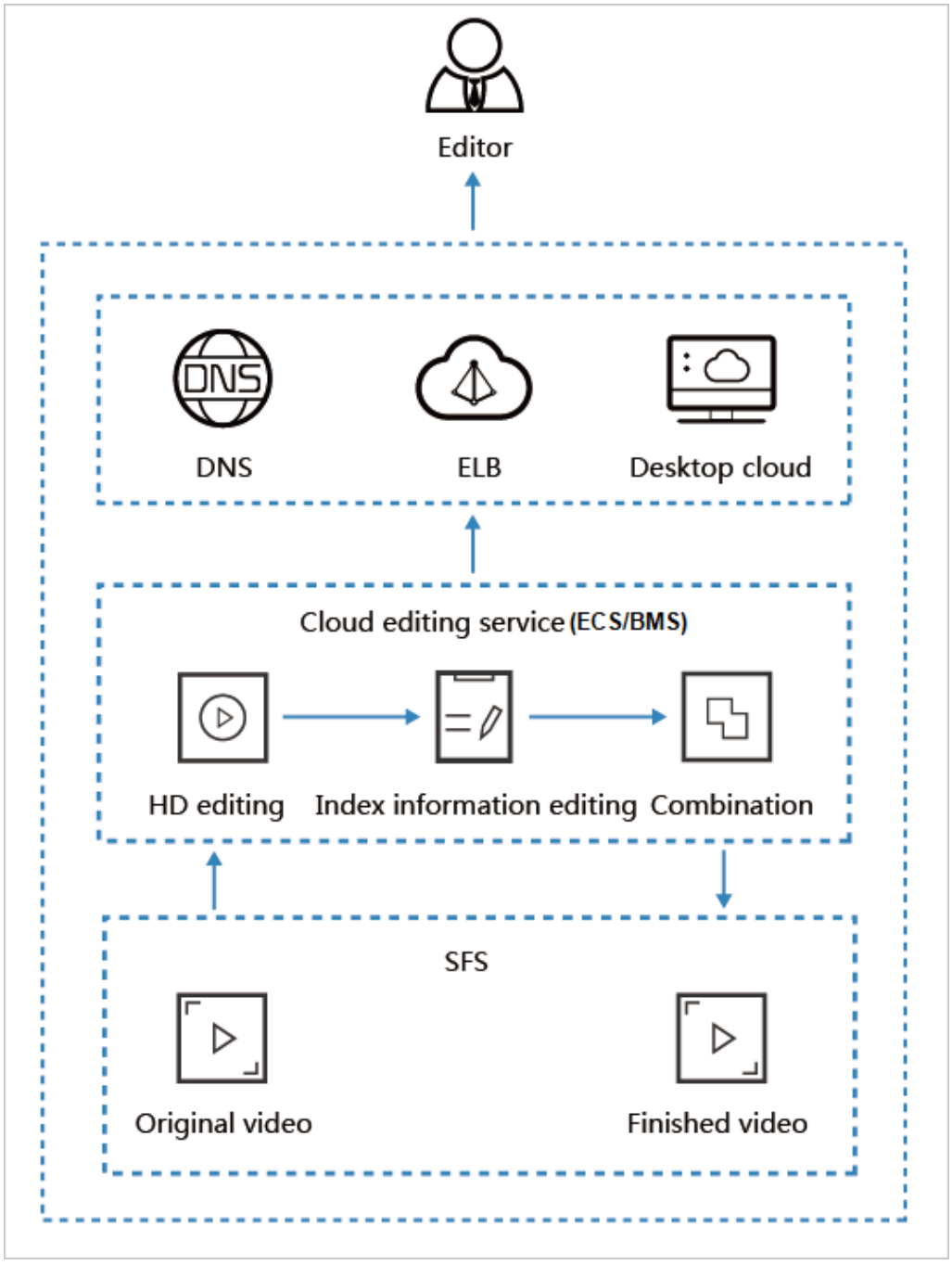


Media Processing

SFS with high bandwidth and large capacity enables shared file storage for video editing, transcoding, composition, high-definition video, and 4K video on demand, satisfying multi-layer HD video and 4K video editing requirements.

Figure 4-2 shows the architecture of the media processing scenario.

Figure 4-2 Architecture of media processing



5 Implementation Principle

Architecture

Figure 5-1 shows the logical architecture of SFS.

Figure 5-1 Logical architecture of SFS

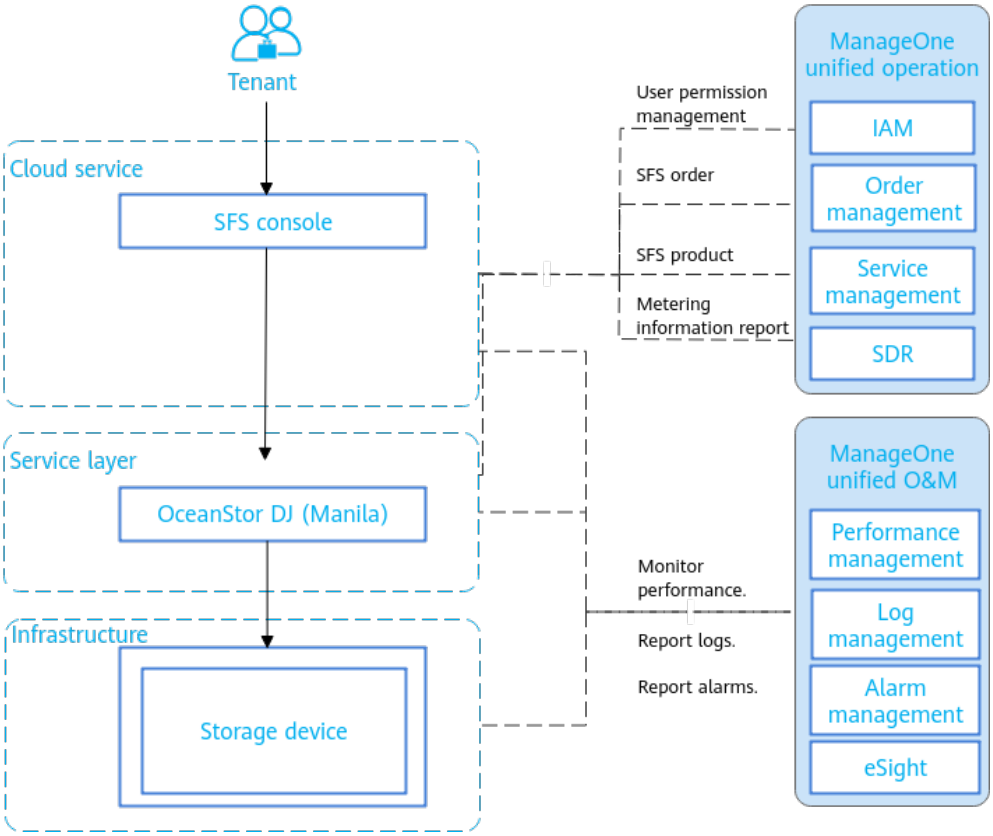


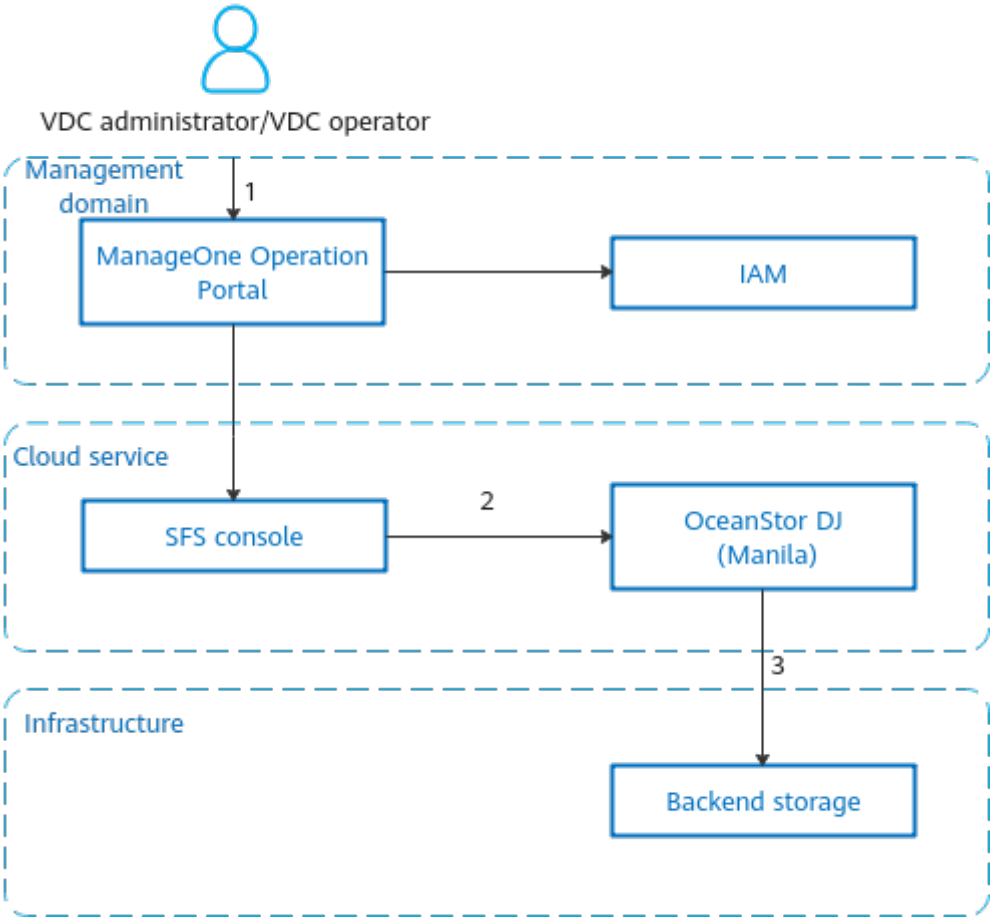
Table 5-1 SFS components

Component Type	Component Name	Description
ManageOne unified operation	IAM	Provides Identity and Access Management (IAM) for SFS.
	Order management	Manages orders submitted by users.
	Service management	Different services are defined based on the registered cloud services, and unified service management is provided.
	SDR	Provides the function of metering and charging resources.
ManageOne unified O&M	Performance management	Monitors performance indicators of infrastructure and analyzes monitoring data.
	Log management	Aggregates and queries the operation and running logs of tenants.
	Alarm management	Receives, stores, and centrally monitors and queries alarm data, helping O&M personnel quickly rectify faults based on alarm information.
	eSight	Provides performance monitoring and alarm generation for the storage device.
Cloud service	SFS console	Provides the SFS management console.
	OceanStor DJ (Manila)	Functions as the SFS server to receive requests from the SFS console.
Infrastructure	Storage device	File storage device that provides file system storage space for the SFS. The following storage devices are supported: OceanStor 9000, OceanStor Dorado, OceanStor, and OceanStor Pacific series.

Workflow

Figure 5-2 shows the SFS workflow.

Figure 5-2 SFS workflow



1. A user applies for file storage resources on the SFS console.
2. The SFS console invokes the API of OceanStor DJ (Manila) to deliver the request to the storage device.
3. OceanStor DJ (Manila) invokes the storage device API to create or manage file systems.

6 Relationships with Other Cloud Services

Figure 6-1 and Table 6-1 list the relationships between SFS and other cloud services.

Figure 6-1 Relationships between SFS and other cloud services

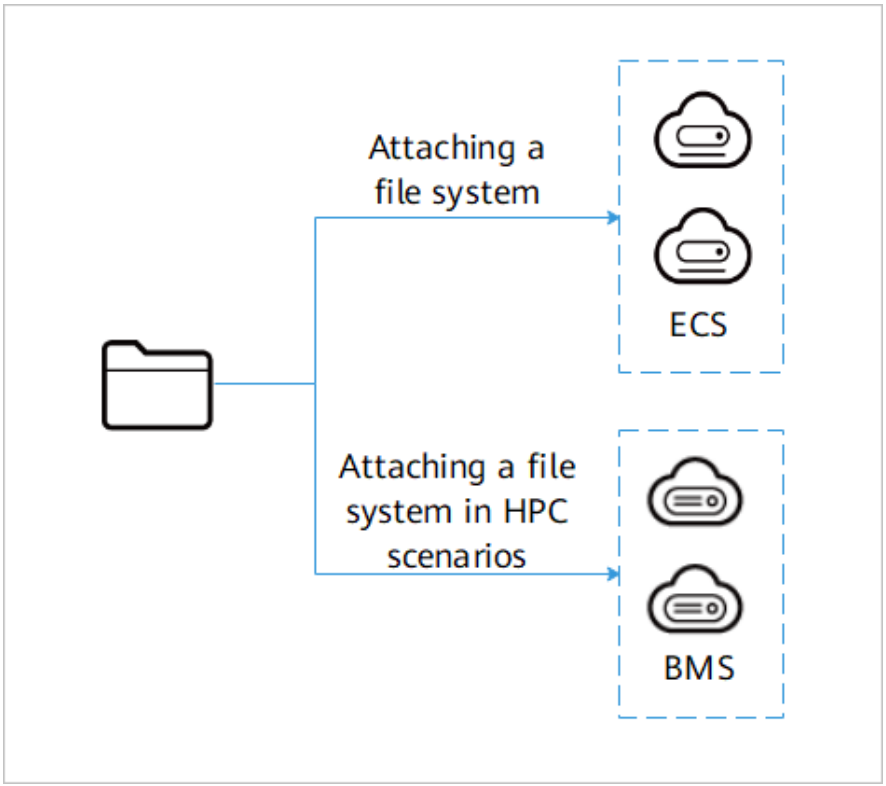


Table 6-1 Relationships between SFS and other cloud services

Cloud Service Name	Description
ECS	File systems can be mounted to ECSs for data sharing.

Cloud Service Name	Description
BMS	In HPC scenarios, file systems can be mounted to BMSs for data sharing.

7 Billing

File System Billing Items

By default, you are charged based on the actual capacity applied for. With this billing mode, your service account is only billed for the amount of time (hours) resources applied for. There is no minimum billing threshold. Any usage period of less than an hour is rounded up to an hour. **Table 7-1** describes billing models.

Table 7-1 Billing models

Billing Item	Billing	Mode	Formula
SFS - sharing	Billing factors: purchased duration and capacity of storage space occupied by SFS	Hourly and monthly	SFS fee=SFS unit price × Capacity × Usage duration

Billing Item	Billing	Mode	Formula
SFS - snapshot	Billing factors: purchased duration and capacity of storage space occupied by SFS snapshots	Hourly and monthly	SFS snapshot fee=SFS snapshot unit price × Capacity (maximum of the maximum snapshot capacity and the shared real-time capacity protected by secure snapshots or secure snapshot schedules) × Usage duration **NOTE** • Maximum snapshot capacity: indicates snapshot with the largest capacity among the file system snapshots of the current file system. • Real-time shared capacity protected by secure snapshots or secure snapshot schedules: indicates the real-time capacity of a file system when the file system is protected by secure snapshots or secure snapshot schedules. If the file system is not protected by them, the value is 0.

NOTE

After the price is calculated based on the usage duration (times or quantity) multiplied by the unit price, the prices are accurate to two decimal places.

8 Permission Management

New users do not have any permissions assigned by default. You need to first add them to one or more groups and then attach policies or roles to these groups. After that, users can perform operations on cloud services.

You can grant permissions to a role or by creating a policy.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Only a limited number of service-level roles are available for authorization. When using roles to grant permissions, you need to also assign other roles which the permissions depend on to take effect. Roles are not ideal for finer authorization and access control.
- Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism enables more flexible authorization and meets secure access control requirements.

Table 8-1 lists all the system-defined roles and policies supported by SFS.

Table 8-1 System-defined policies supported by SFS

Policy Name	Description	Type	Dependency
SFS FullAccess	Full permissions for SFS, including permissions to create, query, and delete file resources.	System policy	None
SFS ReadOnlyAccess	Users with this permission can access and perform read-only operations on SFS.	System policy	None
SFS Administrator	Permissions for managing all SFS resources.	System role	None

Table 8-2 lists the common operations supported by each system-defined policy of file systems. Select the policies as required.

Table 8-2 Common operations supported by each system policy of file systems

Operation	SFS FullAccess	SFS ReadOnlyAccess	SFS Administrator
Creating a file share	√	x	√
Querying shared information	√	√	√
Querying the share list	√	√	√
Updating a file share (scale-out/in, renaming, adding/deleting remote replication relationships, and adding/deleting HyperMetro relationships)	√	x	√
Soft deleting a file share	√	x	√
Restoring soft deletion	√	x	√
Deleting a file share	√	x	√
Modifying a share access rule	√	x	√
Creating a snapshot for a file share	√	x	√
Querying snapshot information about a file share	√	√	√
Querying the snapshot list of a file share	√	√	√

Operation	SFS FullAccess	SFS ReadOnlyAccess	SFS Administrator
Updating a file share snapshot	√	x	√
Restoring a file share snapshot	√	x	√
Deleting a file share snapshot	√	x	√
Managing share tags in batches	√	x	√
Querying the shared tag list	√	√	√
Updating a share tag	√	x	√
Deleting a tag from a share	√	x	√
Checking the virtual interface	√	x	√

9 Key Indicators

Table 9-1 lists the key indicators of SFS.

Table 9-1 Key indicators of SFS

Item	Specifications
Maximum number of file systems that a tenant can create (Region)	2000
Maximum number of file systems that a tenant can create in one batch (Region)	20
Maximum number of VPCs added to a file system	20
Maximum number of authorized IP addresses in the VPCs added to a file system	400

10 Constraints and Limitations

SFS Constraints and Restrictions

Table 10-1 Constraints and Limitations

Item	Constraint and Limitation
Capacity adjustment	• A file system with unlimited capacity does not support capacity expansion. • You can adjust the capacity only when the file system is in the **Available** state. • If you adjust the capacity of a newly created file system, an error will be reported. In this case, wait for 5 to 10 minutes and then adjust the capacity again. • After the capacity of a file system protected by the asynchronous replication disaster recovery (DR) scales in or out, synchronize resources from the primary end to the secondary end to ensure resource data consistency between the primary and secondary ends. For details, see "Operation Help Center" > "Storage" > "Scalable File Service" > "API Reference".
Supported protocols	• Currently, SFS supports NFS, CIFS, DPC, and NFS&DPC protocols. OceanStor 9000: NFSv3 and NFSv4 OceanStor Dorado and OceanStor: NFSv3, NFSv4, and NFSv4.1 OceanStor Pacific: NFSv3 and NFSv4.1 • File systems can be attached to all ECSs that support NFS and CIFS protocols. For optimal performance, however, you are advised to use the OSs that have passed the compatibility test. • The DPC protocol can only be used in the attachment to BMSs.

Item	Constraint and Limitation
File system deletion	• Before deleting a file system, ensure that the file system has been successfully detached from the ECS. • By default, a file system is soft deleted and moved to the recycle bin. The file system still occupies the quota. You can restore or permanently delete the file system from the recycle bin. • A file system removed to the recycle bin has a frozen period of 24 hours by default. The file system cannot be permanently deleted within the frozen period. • If you delete a newly created file system, an error will be reported. In this case, wait 5 to 10 minutes and then delete the file system again.
File system attachment	• To use the automatic attachment function of the SFS, install the cloudMountShareAgent plug-in first. • In the internal public network overlay scenario, file systems can be automatically attached only over the NFS protocol and a single share path. In the internal public network scenario, OceanStor 9000 supports automatic file system attachment over the NFS and CIFS protocols, while other storage devices only over the NFS protocol and a single share path. • After the installation, do not uninstall the plug-in. Otherwise, the file systems may fail to be automatically attached. • After the OS of an ECS is reinstalled or switched, the automatic attachment function becomes invalid. If you want to continue to use this function, reinstall the plug-in.
File system management	Currently, orders can be executed only in one region for synchronous active-active file systems. If orders are executed in both regions for the same HyperMetro file system at the same time, the orders in one region will fail to be executed.
File system authorization	• A file system supports a maximum of 20 VPCs in the same AZ and Resource Spaces. The total number of authorized IP address segments and IP addresses in the added VPCs cannot exceed 400. • In the internal public network scenario, users or user groups can be manually created for OceanStor Pacific file systems created in HCS 8.2.1 or earlier. In the internal public network overlay scenario, users or user groups can be manually created for OceanStor/OceanStor Dorado file shares created in HCS 8.2.1 or earlier. The automatic creation of users or user groups is not supported in theses scenarios.

Constraints on Frozen Tenants

When the status of a tenant is **Frozen**, cloud services will restrict operations of this tenant based on the restriction policy. **Table 10-2** lists the operations prohibited for frozen tenants except querying and tagging.

Table 10-2 Restrictions on frozen tenants

Operation Category	Operation	Restriction Policy	Description
Subscription/ creation	Applying for a file system	Forbidden	-
Operations	Renaming a file system	Forbidden	-
Specification changes	Adding a protocol to a file system	Forbidden	-
Specification changes	Adjusting the capacity of a file system	Forbidden	-
Operations	File system authorization	Forbidden	-
Subscription/ creation	Applying for a snapshot	Forbidden	-
Operations	Adding a snapshot description	Forbidden	-
Subscription/ creation	Rolling back a disk from a snapshot	Forbidden	-
Subscription/ creation	Adding an access key for an object user	Forbidden	-
Subscription/ creation	Creating an object user mapping	Forbidden	-
Operations	Modifying an object user mapping	Forbidden	-
Subscription/ creation	Creating a UNIX user	Forbidden	-
Operations	Modifying the UNIX user	Forbidden	-
Subscription/ creation	Creating a UNIX user group	Forbidden	-

Operation Category	Operation	Restriction Policy	Description
Operations	Modifying the UNIX user group	Forbidden	-
Subscription/ creation	Creating a secure snapshot	Forbidden	-
Subscription/ creation	Rolling back a secure snapshot	Forbidden	-
Operations	Modifying secure snapshots	Forbidden	-
Subscription/ creation	Creating a secure snapshot schedule	Forbidden	-
Operations	Modifying the secure snapshot schedule	Forbidden	-
Specification changes	Adding a file system using a secure snapshot schedule	Forbidden	-
Subscription/ creation	Creating a user	Forbidden	-
Operations	Modifying a user	Forbidden	-
Operations	Resetting the password	Forbidden	-
Subscription/ creation	Performing synchronization	Forbidden	-
Subscription/ creation	Performing a planned migration	Forbidden	-
Subscription/ creation	Continuing planned migration	Forbidden	-
Subscription/ creation	Rectifying a fault	Forbidden	-
Subscription/ creation	Performing reprotection	Forbidden	-
Operations	Modifying a protection policy	Forbidden	-
Operations	Canceling the remote replication	Forbidden	-
Subscription/ creation	Enabling remote replication	Forbidden	-

Operation Category	Operation	Restriction Policy	Description
Subscription/ creation	Creating a HyperMetro relationship	Forbidden	-
Operations	Canceling a HyperMetro relationship	Forbidden	-
Operations	Modifying WORM	Forbidden	-

11 Accessing and Using SFS

Two methods are available:

- Web UI

  Log in to ManageOne Operation Portal (ManageOne Operation Portal for Tenants in B2B scenarios) as a tenant, click  in the upper left corner of the page, select a region, and select the cloud service.
- API

  If you want to integrate the cloud service into a third-party system for secondary development, you can access the cloud service using APIs. For details, see **Operation Help Center** > **Storage** > **Scalable File Service** > **API Reference**.

