

Scalable File Service

Service Overview

Issue 01
Date 2024-11-25



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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

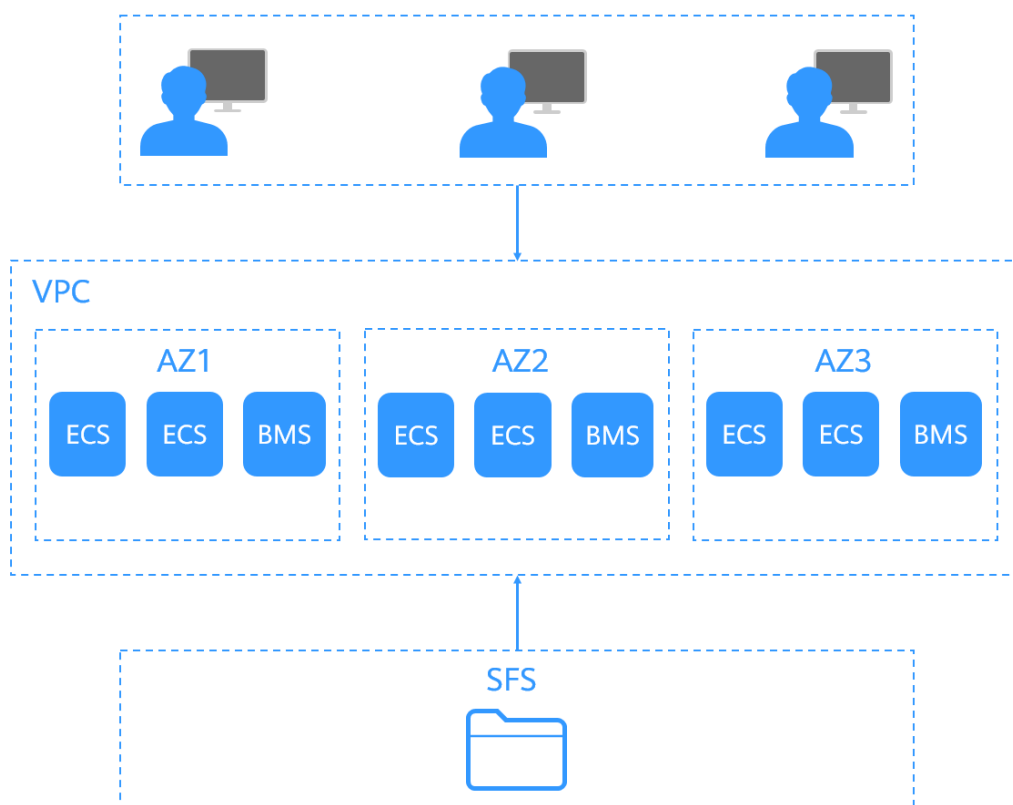
1 What Is SFS?	1
2 Dedicated SFS Turbo	3
3 Application Scenarios	6
4 Functions	8
5 File System Types	11
6 File System Encryption	19
7 Security	20
7.1 Shared Responsibilities	20
7.2 Identity Authentication and Access Control	21
7.2.1 Access Control for SFS	21
7.3 Data Protection	21
7.4 Auditing	22
7.5 Risk Monitoring	22
8 SFS and Other Services	23
9 Basic Concepts	26
9.1 SFS Basic Concepts	26
9.2 Project and Enterprise Project	27
9.3 Region and AZ	27
10 Notes and Constraints	30
11 Billing	35
12 Permissions	40
13 Supported OSs	48

1 What Is SFS?

Overview

Scalable File Service (SFS) provides scalable, high-performance (NAS) file storage. With SFS, you can enjoy shared file access spanning multiple Elastic Cloud Server (ECSs), Bare Metal Servers (BMSs), and containers created on Cloud Container Engine (CCE). See [Figure 1-1](#).

Figure 1-1 Accessing SFS



Compared with traditional file sharing storage, SFS has the following advantages:

- **File sharing**
Cloud servers in multiple availability zones (AZs) of the same region can access the same file system concurrently and share files.
- **Elastic scaling**
Storage can be scaled up or down on demand to dynamically adapt to service changes without interrupting applications. You can complete resizing with a few clicks.
- **Superior performance and reliability**
SFS enables file system performance to increase as capacity grows, and it delivers a high data durability to support rapid service growth.
The backend storage system supports both HDD and SSD storage media. It adopts a distributed architecture and uses full redundant design for modules, which eliminate single-node faults.
- **Seamless integration**
SFS supports Network File System (NFS). With this standard protocol, a broad range of mainstream applications can read and write data in the file system.
- **Easy operation and low costs**
In an intuitive graphical user interface (GUI), you can create and manage file systems with ease. SFS slashes the cost as it is charged on a pay-per-use basis.

Accessing SFS

You can access SFS on the management console or via APIs by sending HTTPS requests.

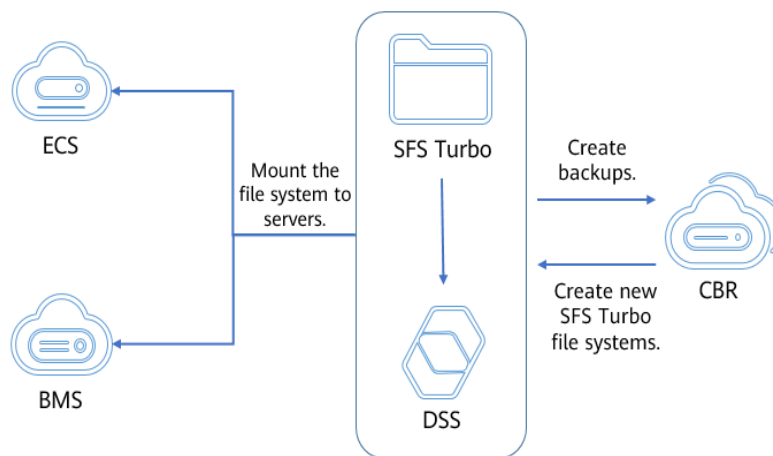
- **APIs**
Use APIs if you need to integrate SFS into a third-party system for secondary development. For detailed operations, see [Scalable File Service API Reference](#).
- **Management console**
Use the console if you prefer a web-based UI to perform operations.

2 Dedicated SFS Turbo

Overview

Dedicated SFS Turbo provides shared file storage for enterprises, governments, and finance institutions based on dedicated compute and storage resource pools. Dedicated resource pools are physically isolated from public pools. The reliable, efficient cloud experience dedicated pools offer can help you meet specific performance, application, and compliance needs.

Figure 2-1 Architecture of Dedicated SFS Turbo



Functions

- A variety of specifications
Various file system types, including Standard, Performance, and HPC (125 MB/s per TiB and 250 MB/s per TiB), are available for diverse application workloads.
- Elastic scaling
File system capacity can be increased on demand, and file system performance improved linearly.
- Reliable and secure
Three-copy redundancy ensures 99.9999999% durability.

Storage pool data encryption protects your data security.

VPC isolation guarantees 100% isolation between tenants.

Physically isolated storage pools provide exclusive resources for tenants.

- Backup and restore

Dedicated SFS Turbo can be backed up using CBR. You can use backups to restore file systems.

- Monitoring

Dedicated SFS Turbo can be interconnected with Cloud Eye, which allows you to view metrics including bandwidth, IOPS, and capacity.

- Auditing

Dedicated SFS Turbo can be audited using CTS. You can view, audit, and backtrack file system operations.

Performance

Table 2-1 Performance

Specifications	Dependent Underlying Resources	Performance
Dedicated SFS Turbo Standard	DCC: C7, C7n, C6, C6s, and C3 instances DSS: high I/O storage pool	Bandwidth = Min. (1 GB/s, Available bandwidth of the DSS storage pool) IOPS = Min. (15,000, Available IOPS of the DSS storage pool)
Dedicated SFS Turbo Performance	DCC: C7, C7n, C6, C6s, and C3 instances DSS: ultra-high I/O storage pool	Bandwidth = Min. (2 GB/s, Available bandwidth of the DSS storage pool) IOPS = Min. (20,000, Available IOPS of the DSS storage pool)
125 MB/s per TiB (Dedicated)	DCC: C6, C7, and C7n instances DSS: ultra-high I/O storage pool	Bandwidth = Min. [125 MB/s/TiB x Storage capacity (TiB), 20 GB/s, Available bandwidth of the DSS storage pool] IOPS = Min. [6,000 x Storage capacity (TiB), Available IOPS of the DSS storage pool]
250 MB/s per TiB (Dedicated)	DCC: C6, C7, and C7n instances DSS: ultra-high I/O storage pool	Bandwidth = Min. [250 MB/s/TiB x Storage capacity (TiB), 20 GB/s, Maximum bandwidth of the DSS storage pool] IOPS = Min. [12,500 x Storage capacity (TiB), Available IOPS of the DSS storage pool]

 **NOTE**

The available bandwidth and IOPS of a storage pool are in direct proportion to the storage capacity. When purchasing Dedicated SFS Turbo and planning DSS resources, reserve enough Dedicated SFS Turbo storage space and performance to prevent affecting the file system performance.

In the **Performance** column, the bandwidth or IOPS value is the smallest value in [] or ().

3 Application Scenarios

Expandable to petabytes, SFS Capacity-Oriented provides fully hosted shared file storage. It features high availability and durability, and seamlessly handles data-intensive and bandwidth-intensive applications. It is suitable for multiple scenarios, including high-performance computing, media processing, file sharing, as well as content management and web services.

- **High-performance computing**
In HPC industries, such as simulation experiments, biopharmacy, gene sequencing, image processing, and weather forecast, SFS provides superb compute and storage capabilities, as well as high bandwidth and low latency.
- **Media processing**
Services of TV stations and new media are more likely to be deployed on cloud platforms than before. Such services include streaming media, archiving, editing, transcoding, content distribution, and video on demand (VoD). In such scenarios, a large number of workstations are involved in the whole program production process. Different operating systems (OSs) may be used by different workstations, requiring file systems to share materials. In addition, HD/4K videos have become a major trend in the broadcasting and TV industry. Taking video editing as an example, to improve audiences' audiovisual experience, HD editing is being transformed to 30- to 40-layer editing. A single editing client may require a file system with a bandwidth up to hundreds of MB per second. Usually, producing a single TV program needs several editing clients to process a lot of video materials concurrently. To meet such requirement, a file storage service with stable, bandwidth-intensive, and latency-sensitive performance is required.
- **Content management and web services**
SFS can be used in various content management systems to store and provide information for websites, home directories, online releases, and archiving.
- **Big data and analytic applications**
SFS delivers an aggregate bandwidth of up to 10 Gbit/s, capable of handling ultra-large data files such as satellite images. In addition, it has robust reliability to prevent service interruptions due to system failures.

SFS Turbo

Expandable to 320 TB, SFS Turbo provides fully hosted shared file storage. It features high availability and durability to support massive small files and applications requiring low latency and high IOPS. SFS Turbo is recommended for various scenarios, including high-performance websites, log storage, compression and decompression, DevOps, enterprise OA, and containerized applications.

- High-performance websites
For I/O-intensive website services, SFS Turbo can provide shared website source code directories for multiple web servers, enabling low-latency and high-IOPS concurrent share access.
- Log storage
SFS Turbo can provide multiple service nodes for shared log output directories, facilitating log collection and management of distributed applications.
- DevOps
The development directory can be shared to multiple VMs or containers, simplifying the configuration process and improving R&D experience.
- Enterprise OA
Office documents of enterprises or organizations can be saved in an SFS Turbo file system for high-performance shared access.

4 Functions

Table 4-1 lists common SFS functions.

Before using SFS, you are advised to learn basic concepts such as NFS and CIFS in **SFS Basic Concepts** to better understand the functions provided by SFS.

- ✓: indicates that the file system type supports this function.
- ×: indicates that the file system type does not support this function.

Table 4-1 Common functions

Function	Description	SFS Capacity - Oriented	SFS Turbo	General Purpose File System
NFS	Network File System (NFS) is a distributed file system protocol that allows different computers and OSs to share data over a network. After the NFS client is installed on multiple ECSs, mount the file system to implement file sharing between ECSs. The NFS protocol is recommended for Linux clients.	✓	✓	✓
CIFS	Common Internet File System (CIFS) is a protocol used for network file access. Using the CIFS protocol, network files can be shared between hosts running Windows. The CIFS protocol is recommended for Windows clients.	✓	×	×

Function	Description	SFS Capacity - Oriented	SFS Turbo	General Purpose File System
Multi-VPC access	Multiple VPCs can be configured for a file system so that ECSs belonging to different VPCs can share the same file system, as long as the VPCs that the ECSs belong to are added to the VPC list of the file system or the ECSs are added to the authorized addresses of the VPCs.	√	√ Implemented through VPC peering connection	√
Multi-account access	If VPC IDs used by other accounts are added to the VPC list of a file system and IP addresses or IP address ranges of ECSs are added to the authorized address list, ECSs of different VPCs and of different accounts can share the same file system.	√	×	×
File system backup	A backup is a complete copy of a file system at a specific time and it records all configuration data and service data at that time. If your file system is faulty or a logical error occurs in the data in the file system, you can use the backup data to restore the data quickly.	×	√	×
File system encryption	SFS enables you to encrypt data on the new file systems as required.	×	√	×
File system monitoring	Cloud Eye is a multi-dimensional resource monitoring service. With Cloud Eye, you can view the file system usage and service running status, and respond to exceptions in a timely manner to ensure smooth running of services.	√	√	√

Function	Description	SFS Capacity - Oriented	SFS Turbo	General Purpose File System
File system auditing	Cloud Trace Service (CTS) records operations of SFS resources, facilitating query, audit, and backtracking.	×	√	×
Enterprise project	An enterprise project manages multiple resource instances by category. Resources and projects in different cloud service regions can be classified into one enterprise project. An enterprise allows you to classify resources based on departments or project groups and put relevant resources into the same enterprise project for management. Resources can be migrated between enterprise projects. If there are more than 20 enterprise projects, SFS Turbo is recommended.	√	√	×
Tag	You can use tags to classify and identify file systems. If you add tags to a file system, service detail records (SDRs) generated for it will be labeled with these tags. You can classify SDRs by tag for cost analysis.	×	√	√

5 File System Types

SFS provides three types of file systems: SFS Capacity-Oriented, General Purpose File System, and SFS Turbo.

The following table describes the features, advantages, and application scenarios of these types of file systems.

Table 5-1 File system types

File System Type	Storage Class	Features	Highlights	Application Scenarios
SFS Capacity-Oriented	-	<ul style="list-style-type: none"> • Maximum bandwidth: 2 GB/s; maximum IOPS: 2,000 • Latency: 3 to 20 ms; maximum capacity: 4 PB • Delivers better performance and suitable for services that require large capacity and high bandwidth. 	Large capacity, high bandwidth, and low cost	Cost-sensitive workloads which require large-capacity scalability, such as media processing, file sharing, high-performance computing, and data backup. For workloads dealing with massive small files, SFS Turbo is recommended.

File System Type	Storage Class	Features	Highlights	Application Scenarios
		<p>NOTE</p> <ul style="list-style-type: none"> • Latency refers to the minimum latency under low workload conditions. It is unstable. • Large files refer to files larger than 10 MB, and large I/Os refer to I/Os larger than 1 MB. • The performance of a file system is related to its capacity. The bandwidth is calculated using the following formula: Bandwidth of a file system = 0.02 MB/s x Capacity of the file system (GB) + 100 MB/s. The maximum bandwidth of a file system with 100 TB capacity is 2 GB/s. If a higher bandwidth is required, purchase a file system with larger capacity. 		

File System Type	Storage Class	Features	Highlights	Application Scenarios
General Purpose File System	-	<ul style="list-style-type: none"> • Maximum bandwidth: 1.25 GB/s; maximum IOPS: million • Latency: about 10 ms; maximum capacity: EB • Delivers better performance and suitable for services that require large capacity and high bandwidth. 	Large capacity, high bandwidth, and low cost	Cost-sensitive workloads which require large-capacity scalability, such as media processing, file sharing, high-performance computing, and data backup. For workloads dealing with massive small files, SFS Turbo is recommended.

File System Type	Storage Class	Features	Highlights	Application Scenarios
SFS Turbo	Standard	<ul style="list-style-type: none"> • Maximum bandwidth: 150 MB/s; maximum IOPS: 5,000 • Latency: 2 to 5 ms; maximum capacity: 32 TB • Suitable for services with massive small files and services that require low latency. <p>NOTE The performance of an SFS Turbo file system depends on the storage class. It is not affected by the file system capacity.</p>	Low latency and tenant exclusive	Workloads dealing with massive small files, such as code storage, log storage, web services, and virtual desktop

File System Type	Storage Class	Features	Highlights	Application Scenarios
	Standard-Enhanced	<ul style="list-style-type: none"> • Maximum bandwidth: 1 GB/s; maximum IOPS: 15,000 • Latency: 2 to 5 ms; maximum capacity: 320 TB • Enhanced bandwidth, IOPS, and capacity 	Low latency, high bandwidth, and tenant exclusive	Workloads dealing with massive small files and those requiring high bandwidth, such as code storage, file sharing, enterprise office automation (OA), and log storage.
	Performance	<ul style="list-style-type: none"> • Maximum bandwidth: 350 MB/s; maximum IOPS: 20,000 • Latency: 1 to 3 ms; maximum capacity: 32 TB • Delivers better performance and suitable for services with massive small files and services that require low latency. 	Low latency, high IOPS, and tenant exclusive	Workloads dealing with massive small files, and random I/O-intensive and latency-sensitive services, such as high-performance websites, file sharing, and content management

File System Type	Storage Class	Features	Highlights	Application Scenarios
	Performance-Enhanced	<ul style="list-style-type: none"> • Maximum bandwidth: 2 GB/s; maximum IOPS: 100,000 • Latency: 1 to 3 ms; maximum capacity: 320 TB • Enhanced bandwidth, IOPS, and capacity 	Low latency, high IOPS, high bandwidth, and tenant exclusive	Workloads dealing with massive small files, and latency-sensitive and bandwidth-demanding workloads, such as image rendering, AI training, and enterprise OA.
	20 MB/s/TiB	<ul style="list-style-type: none"> • Maximum bandwidth: 8 GB/s; maximum IOPS: 250,000 • Latency: 2 to 5 ms; capacity: 3.6 TB to 1 PB 	Large capacity and low cost	Enterprise OA and code repository management
	40 MB/s/TiB	<ul style="list-style-type: none"> • Maximum bandwidth: 8 GB/s; maximum IOPS: 250,000 • Latency: 2 to 5 ms; capacity: 1.2 TB to 1 PB 	Large capacity and low cost	Enterprise OA and code repository management

File System Type	Storage Class	Features	Highlights	Application Scenarios
	125 MB/s/TiB	<ul style="list-style-type: none"> Maximum bandwidth: 20 GB/s; maximum IOPS: 1 million Latency: 1 to 3 ms; capacity: 1.2 TB to 1 PB 	Low latency and cost effectiveness	AI training, EDA simulation, gene analysis, and video rendering
	250 MB/s/TiB	<ul style="list-style-type: none"> Maximum bandwidth: 20 GB/s; maximum IOPS: 1 million Latency: 1 to 3 ms; capacity: 1.2 TB to 1 PB 	Low latency and high bandwidth	AI training, EDA simulation, gene analysis, and video rendering
	500 MB/s/TiB	<ul style="list-style-type: none"> Maximum bandwidth: 80 GB/s; maximum IOPS: 1 million Latency: 1 to 3 ms; capacity: 1.2 TB to 1 PB 	Low latency and high-density performance	Autonomous driving, AI generated content, and EDA in chip design
	1,000 MB/s/TiB	<ul style="list-style-type: none"> Maximum bandwidth: 80 GB/s; maximum IOPS: 1 million Latency: 1 to 3 ms; capacity: 1.2 TB to 1 PB 	Low latency and high-density performance	Autonomous driving, AI generated content, and EDA in chip design

6 File System Encryption

SFS enables you to encrypt data on the new file systems as required.

Keys for encrypting file systems are provided by Key Management Service (KMS), which is secure and convenient. You do not need to establish and maintain key management infrastructure. If you want to use your own key material, use the key import function on the KMS console to create a custom key whose key material is empty and import the key material to the custom key. For details, see section "Importing Key Materials" in *Data Encryption Workshop User Guide*.

General Purpose File System does not support file system encryption.

Encryption Key

An SFS Turbo file system does not have a default key. You can use your existing key or create a new key. For details, see [Creating a Custom Key](#) in the *Data Encryption Workshop User Guide*.

7 Security

7.1 Shared Responsibilities

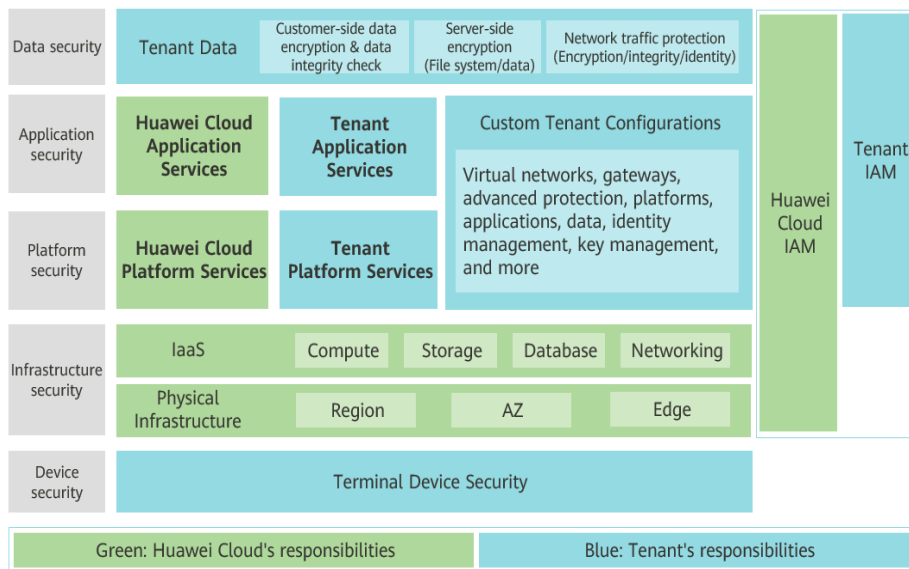
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

[Figure 7-1](#) illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud:** Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant:** Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

[Huawei Cloud Security White Paper](#) elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 7-1 Huawei Cloud shared security responsibility model



7.2 Identity Authentication and Access Control

7.2.1 Access Control for SFS

SFS is interconnected with IAM, so you can assign different permissions to employees to access your SFS resources for fine-grained permissions management. For details, see [SFS Permissions](#).

You can use IAM to securely control access to your SFS resources.

Table 7-1 SFS access control

Method		Description	Reference
Permissions control	IAM permissions	IAM permissions define which actions on your cloud resources are allowed or denied. After creating an IAM user, the administrator needs to add it to a user group and grant the permissions required by SFS to the user group. Then, all users in this group automatically inherit the granted permissions.	Permissions

7.3 Data Protection

Encryption

SFS supports server-side encryption, which allows you to encrypt the data stored in SFS file systems. When data is accessed, SFS automatically decrypts the data and then returns it to you.

To use the encryption function, see [File System Encryption](#).

Backup

A backup is a complete copy of an SFS Turbo file system at a specific time. It records all configuration data and service data at that time. For example, if a file system is faulty or encounters a logical error (accidental deletion, hacker attacks, and virus infection), you can use data backups to restore data quickly.

To use the backup function, see [Backup](#).

7.4 Auditing

Cloud Trace Service (CTS) records operations on the cloud resources in your account. You can use the logs generated by CTS to perform security analysis, track resource changes, audit compliance, and locate faults.

After you enable CTS and configure a tracker, CTS can record management and data traces of SFS for auditing.

For details about how to enable and configure CTS, see [CTS Getting Started](#).

For details about SFS management and data traces that can be tracked by CTS, see section "Supported SFS Operations" in the *Scalable File Service User Guide*.

7.5 Risk Monitoring

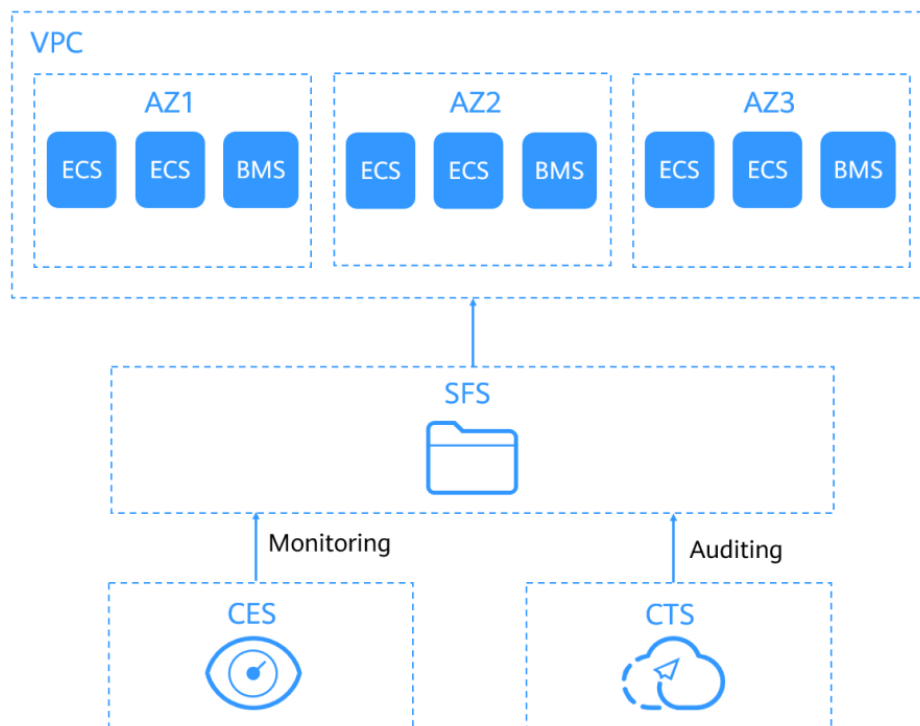
SFS uses Cloud Eye to perform monitoring over resources, helping you monitor your file system usages and receive alarms and notifications in real time. You can monitor the number of client connections, bandwidth, IOPS, and capacity of SFS file systems in real time.

For details about supported SFS metrics and how to create alarm rules, see [Monitoring](#).

8 SFS and Other Services

Figure 8-1 lists the relationship between SFS and other cloud services.

Figure 8-1 Relationships between SFS and other services



Relationships Between SFS and Other Services

Table 8-1 Related services

Function	Related Service	Reference
A file system and the ECSs must belong to the same project. File systems are mounted to shared paths for data sharing.	Elastic Cloud Server (ECS)	Mounting an NFS File System to ECSs (Linux)

Function	Related Service	Reference
<p>CCE is a highly scalable, enterprise-class hosted Kubernetes service for you to run containers and applications. With CCE, you can easily deploy, manage, and scale containerized applications in the cloud.</p> <p>You can use SFS file systems as persistent storage for containers and mount the file systems to containers when creating a workload.</p>	<p>Cloud Container Engine (CCE)</p>	<p>Mounting an NFS File System to ECSs (Linux)</p>
<p>VPC provisions an isolated virtual network environment defined and managed by yourself, improving the security of cloud resources and simplifying network deployment.</p> <p>An ECS cannot access file systems in a different VPC. Before using SFS, assign the file system and the ECSs to the same VPC.</p>	<p>Virtual Private Cloud (VPC)</p>	<p>Creating a File System</p>
<p>VPCEP is a cloud service that provides secure and private channels to connect your VPCs to VPC endpoint services. It allows you to plan networks flexibly without having to use EIPs.</p> <p>General Purpose File System communicates with ECSs through VPC endpoints, so that ECSs can access file systems.</p>	<p>VPC Endpoint (VPCEP)</p>	<p>Configuring a VPC Endpoint</p>
<p>IAM is an enterprise-level self-service cloud resource management system. It provides user identity management and access control functions. When employees in your enterprise need to use SFS, the enterprise administrator can use IAM to create users and control these users' permissions on enterprise resources.</p>	<p>Identity and Access Management (IAM)</p>	<p>Permissions</p>
<p>The encryption feature relies on KMS, which improves the data security of your file systems.</p>	<p>Data Encryption Workshop: Key Management Service (KMS)</p>	<p>Encryption</p>

Function	Related Service	Reference
Once you have subscribed to SFS, you can monitor its performance without installing any plug-ins and view monitored metrics, such as the read bandwidth, write bandwidth, and read and write bandwidth on Cloud Eye.	Cloud Eye	Monitoring
Cloud Trace Service (CTS) allows you to collect, store, and query cloud resource operation records and use these records for security analysis, compliance auditing, resource tracking, and fault locating. With CTS, you can record operations associated with SFS for later query, audit, and backtrack operations.	Cloud Trace Service (CTS)	Auditing
You can use tags to classify and identify file systems.	Tag Management Service (TMS)	Tags

9 Basic Concepts

9.1 SFS Basic Concepts

Before you start, understand the following concepts.

NFS

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

You are advised to use NFS file systems in Linux OS.

CIFS

Common Internet File System (CIFS) is a protocol used for network file access. It is a public or open version of the Server Message Block (SMB) protocol, which is initiated by Microsoft. CIFS allows applications to access files on computers over the Internet and send requests for file services. Using the CIFS protocol, network files can be shared between hosts running Windows.

CIFS file systems cannot be mounted to Linux servers.

You are advised to use CIFS file systems in Windows OS.

File System

A file system provides users with shared file storage service through NFS. It is used for accessing network files remotely. After a user creates a mount point on the management console, the file system can be mounted to multiple servers and is accessible through the standard POSIX.

POSIX

Portable Operating System Interface (POSIX) is a set of interrelated standards specified by Institute of Electrical and Electronics Engineers (IEEE) to define the application programming interface (API) for software compatible with variants of the UNIX operating system. POSIX is intended to achieve software portability at

the source code level. That is, a program written for a POSIX compatible operating system may be compiled and executed on any other POSIX operating system.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a LAN network protocol. The server controls an IP address range, and a client can automatically obtain the IP address and subnet mask allocated by the server when logging in to the server. By default, DHCP is not automatically installed as a service component of Windows Server. Manual installation and configuration are required.

9.2 Project and Enterprise Project

Project

A project is used to group and isolate OpenStack resources, such as compute, storage, and network resources. A project can be a department or a project team. Multiple projects can be created for one account.

Enterprise Project

An enterprise project manages multiple resource instances by category. Resources and projects in different cloud service regions can be classified into one enterprise project. An enterprise can classify resources based on departments or project groups and put relevant resources into one enterprise project for management. Resources can be migrated between enterprise projects.

References

- For details about enterprise projects, see [Applicable Scenarios of Enterprise Projects](#).
- For details about the APIs and actions supported by enterprise projects, see [Supported Actions](#).

9.3 Region and AZ

Concept

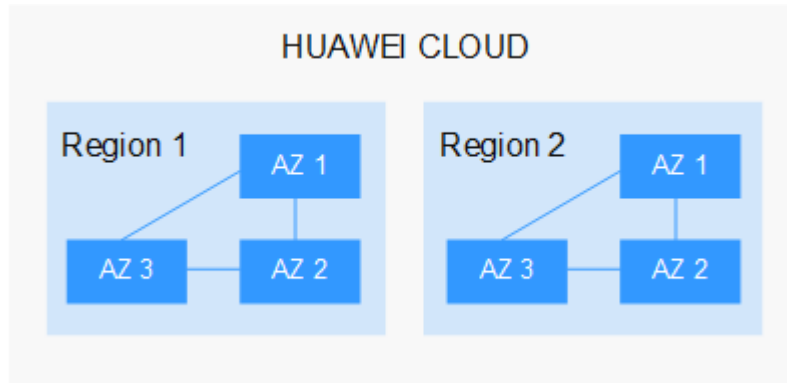
A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are classified based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type or only provides services for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an

AZ, compute, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers, to support cross-AZ high-availability systems.

Figure 9-1 shows the relationship between regions and AZs.

Figure 9-1 Regions and AZs



Huawei Cloud provides services in many regions around the world. You can select a region and an AZ based on requirements. For more information, see [Huawei Cloud Global Regions](#).

Selecting a Region

When selecting a region, consider the following factors:

- Location

It is recommended that you select the closest region for lower network latency and quick access.

- If your target users are in Asia Pacific (excluding the Chinese mainland), select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
- If your target users are in Africa, select the **AF-Johannesburg** region.
- If your target users are in Latin America, select the **LA-Santiago** region.

NOTE

The **LA-Santiago** region is located in Chile.

- Resource price

Resource prices may vary in different regions. For details, see [Product Pricing Details](#).

Selecting an AZ

When deploying resources, consider your applications' requirements on network latency.

If your applications require a low network latency between instances, deploy resources in the same AZ.

Regions and Endpoints

Before you call an API to use resources, specify its region and endpoint. For more information, see [Regions and Endpoints](#).

10 Notes and Constraints

SFS Capacity-Oriented

Table 10-1 SFS Capacity-Oriented restrictions

Item	Description
Access method	SFS Capacity-Oriented file systems can only be accessed over the intranet and used on the cloud.
Supported protocols	<ul style="list-style-type: none">• Only NFSv3 is supported (NFSv4 is not supported), and CIFS is supported (SMB 2.0, 2.1, and 3.0 are supported, but SMB 1.0 is not supported).• Export options with NFSv3 include rw, no_root_squash, no_all_squash, and sync. Export options with CIFS include rw and sync.• Encrypted CIFS file systems do not support copychunk.• CIFS file systems cannot be mounted to Linux servers.• A file system can use either the NFS or CIFS protocol. It cannot use both protocols.• SMB file systems provide permission control only on the file systems, but not on files or directories.
Max. number of clients per file system	10,000
Max. capacity per file system	4 PB
Max. size of a single file	240 TB
Multi-VPC access	Supported. You can add a maximum of 20 VPCs for one file system and create a maximum of 400 ACL rules for all added VPCs.

Item	Description
Max. enterprise projects supported	20. If there are more than 20 enterprise projects, SFS Capacity-Oriented file systems may fail to be created. SFS Turbo is recommended.
Replication	Not supported
Cross-region mounting	Not supported
Cross-account mounting	Not supported

 **NOTE**

SFS Capacity-Oriented file systems are now sold out. You can use General Purpose File System or SFS Turbo.

General Purpose File System

Table 10-2 General purpose file system restrictions

Item	Description
Access method	Can only be accessed over the intranet.
Supported protocols	Only NFSv3 is supported (NFSv4 is not supported).
Max. number of clients per file system	10,000
File system encryption	Not supported
Number of files or subdirectories in a file system	Unlimited
Max. number of files or subdirectories in a single directory	1 billion
File system name	Must be globally unique. It cannot be the same as the name of any existing general purpose file system, including one created by the current user or any other user. And it cannot be changed after the file system is created.
File system deletion	If a general purpose file system is deleted, you can only create a general purpose file system with the same name as the deleted one 30 minutes after that file system has been deleted.

Item	Description
Client OS	<ul style="list-style-type: none"> Cannot be mounted to 32-bit Linux servers. Cannot be mounted to Windows servers.
Changing root directory permissions	Not supported
Restrictions in the CCE and CCI scenarios	<ul style="list-style-type: none"> When General Purpose File System is used as the storage backend of CCE or CCI, you need to empty the in-use file systems before you can delete any PVCs or PVs. If you directly delete the PVCs or PVs, the file systems may fail to be deleted. Check whether the file systems are deleted on the General Purpose File System console. Deleting PVCs or PVs takes some time. The billing ends until the corresponding general purpose file systems are deleted.
Lifecycle management	A maximum of 20 lifecycle rules can be configured for a file system.
File locking with Flock	Not supported
Tag	<ul style="list-style-type: none"> A maximum of 20 tags can be added to a file system. Tag keys of a file system must be unique.

SFS Turbo

Table 10-3 SFS Turbo restrictions

Item	General
Access method	VPN, Direct Connect, and Cloud Connect
Max. bandwidth	2 GB/s
Max. IOPS	100,000
Min. latency	1 to 2 ms
Max. capacity per file system	320 TB
Supported protocol	NFSv3
Max. number of clients per file system	500

Item	General
Max. number of authorized VPCs per file system	20
Max. size of a single file	16 TB
Max. number of files or subdirectories per file system	1 billion
Max. number of files or subdirectories in a single directory	20 million NOTE If you need to execute the ls , du , cp , chmod , or chown command on a directory, you are advised to place no more than 500,000 files or subdirectories in that directory. Otherwise, requests may take a long time to complete as the NFS protocol sends a large number of requests to traverse directory files and requests are queueing up.
Max. directory depth (unit: layer)	100
Max. path length (unit: byte)	1,024
Max. soft link length (unit: byte)	1,024
Max. hard link length (unit: byte)	255
Max. number of file systems	32 by default. You can submit a service ticket to increase the quota.
File system backup	Supported
Backup data restoring to the original file system	Not supported NOTE SFS Turbo uses single-AZ deployment. SFS Turbo file systems will fail if their AZ fails.
File locking with Flock	Not supported
Cross-region mounting via domain name	Not supported NOTE <ul style="list-style-type: none"> When you mount a file system using its domain name, cross-region mounting is not supported. To mount a file system across regions, mount the file system using IP address. The file system domain name randomly resolves to a corresponding domain name server IP address, so some domain name servers may have lots of mounts while others have only a few. It is recommended that you use the domain name servers to the maximum extent as uneven mounts may affect the file system performance.
Cache acceleration	Not supported

Item	General
Tag	<ul style="list-style-type: none">• You can add a maximum of 10 tags to a file system.• Tag keys of a file system must be unique.

11 Billing

Billing Items of SFS Capacity-Oriented

Pay-per-use billing is preset by default. You can create a file system for free and pay only for the used storage space based on for how long you use the file system. You will be billed for the file system by the hour, and there is no minimum cost. Any usage period of less than an hour is rounded up to an hour. For details, see [Table 11-1](#).

Table 11-1 Billing model

Billing Item	Billing Description	Billing Formula
Storage space	Billed based on the storage capacity and usage period of the file system	Storage price = Unit price per GB x Storage capacity x Usage period

NOTE

SFS Capacity-Oriented file systems and general purpose file systems can share a resource package.

The price is calculated based on the amount of resources you use and the pricing basis. The price is accurate to two decimal places.

In the price calculator, the 1 TB SFS Capacity-Oriented package equals to 1,000 GB.

Billing Items of General Purpose File System

Pay-per-use billing is preset by default. You can create a file system for free and pay only for the used storage space based on for how long you use the file system. You will be billed for the file system by the hour, and there is no minimum cost. Any usage period of less than an hour is rounded up to an hour.

Table 11-2 General Purpose File System billing model

Category	Billing Item	Billing Factor	Billing Description	Billing Formula	Billing Mode
Storage	Capacity	Storage space	Billed based on the used capacity and usage period of the file system	Storage price = Unit price per GB x Used capacity x Usage period	Pay-per-use Yearly/ Monthly
	Infrequent Access	Storage space	Billed based on the used capacity and usage period of the file system	Storage price = Unit price per GB x Used capacity x Usage period NOTE In a lifecycle rule of a general purpose file system, the system presets Transition to Infrequent Access After to 14 days . In this case, you will be billed for 14 days based on the standard storage billing. For the usage after 14 days, you will be billed based on the infrequent access storage billing.	Pay-per-use
Traffic	Infrequent Access	Write traffic	Billed based on the volume of the write traffic	Write traffic price = Unit price per GB x Write traffic volume	Pay-per-use
		Read traffic	Billed based on the volume of the read traffic	Read traffic price = Unit price per GB x Read traffic volume	Pay-per-use

 **NOTE**

SFS Capacity-Oriented file systems and general purpose file systems can share a resource package.

Billing Items of SFS Turbo

Pay-per-use billing is preset by default. You are billed based on the storage capacity that you select (instead of the used capacity) and the amount of time that you use the capacity. Usage period is calculated at the top of every hour. Any usage period of less than an hour is rounded up to an hour. For details, see [Table 11-3](#).

Table 11-3 SFS Turbo billing model

Category	Billing Item	Billing Factor	Billing Description	Billing Formula	Billing Mode
Storage	Standard, Standard-Enhanced, Performance, Performance-Enhanced, 20 MB/s/TiB, 40 MB/s/TiB, 125 MB/s/TiB, 250 MB/s/TiB, 500 MB/s/TiB, 1,000 MB/s/TiB	Storage space	Billed based on the purchased capacity and usage period of the file system	Storage price = Unit price per GB x Purchased capacity x Usage period	Pay-per-use Yearly/ Monthly

Billing Modes

SFS supports the following billing modes: pay-per-use and yearly/monthly. For details about how to purchase SFS, see [How Do I Purchase SFS?](#)

For details about the billing, see [Product Pricing Details](#).

In addition, you can use the [Price Calculator](#) to quickly calculate an estimated price for the resources that you select.

Changing Billing Mode

- Yearly/monthly is a prepaid billing mode. You will be billed based on the subscription duration you specify. This mode provides a favorable price and is ideal when the resource use duration is predictable.
- Pay-per-use is a postpaid billing mode. You will be billed based on the billing items of specific file systems and can purchase or delete file systems at any time. Expenditures are deducted from the account balance.

In some regions, you can change the billing mode of an SFS Capacity-Oriented or a general purpose file system or an SFS Turbo file system from pay-per-use to yearly/monthly. For details, see [Yearly/Monthly Subscription](#). Currently, the billing mode cannot be changed from yearly/monthly to pay-per-use.

The purchased SFS Capacity-Oriented resource packages cannot be viewed on the SFS console. To view the resource packages, see [How Do I Check the Usage of a](#)

Resource Package? The resource package capacity is preferentially used when you use SFS Capacity-Oriented and general purpose file systems, and multiple file systems can share one resource package.

Renewal

For more information about renewal, including auto-renewal, exporting the renewal list, and changing subscriptions, see [Renewal Management](#).

Expiration

After a yearly/monthly SFS Capacity-Oriented or general purpose file system (or resource package) expires, you will be billed for subsequently used resources on a pay-per-use basis. If your account is in arrears, you need to pay off the arrears timely. For details about how to repay the arrears, see [Making Repayments](#). If you do not pay off the arrears timely, the system processes the resource based on [Release Suspension and Release](#). If the resource package is not renewed before the retention period expires, the system automatically deletes the resource.

After a yearly/monthly SFS Turbo file system expires, the system will not automatically change it to pay-per-use billing, but processes it based on the rules specified in [Resource Suspension and Release](#). If the file system is not renewed before the retention period expires, it will be deleted.

Overdue Payment

Possible causes of overdue payment:

- You have purchased an SFS Capacity-Oriented or General Purpose File System resource package, but your file systems have used up the package capacity. In addition, your account balance is not enough to pay for the pay-per-use charges generated afterward.
- You have purchased an SFS Capacity-Oriented or General Purpose File System resource package but created a pay-per-use SFS Turbo file system. Your account balance is not enough to pay for the generated pay-per-use charges.
- You have created a yearly/monthly SFS Turbo file system and a pay-per-use SFS Capacity-Oriented file system. Your account balance is not enough to pay for the generated pay-per-use charges.
- You do not have any SFS Capacity-Oriented or General Purpose File System resource package and created such a pay-per-use file system. Your account balance is not enough to pay for the generated pay-per-use charges.
- You have created a pay-per-use SFS Turbo file system and your account balance is not enough to pay for the generated pay-per-use charges.

Service status and operation restrictions when an account is in arrears:

Your file systems are retained after your account is in arrears and file systems enter the retention period, but you cannot use the file systems. For details about how to repay arrears, see [Topping Up an Account](#). If the outstanding payment is not cleared before the retention period ends, data stored in the file systems will be deleted and cannot be recovered.

For details about the retention period, see [Service Suspension and Resource Release](#).

12 Permissions

If you need to assign different permissions to employees in your enterprise to access your SFS resources on Huawei Cloud, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you to securely access your Huawei Cloud resources.

With IAM, you can use your Huawei Cloud account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, some software developers in your enterprise need to use SFS resources but should not be allowed to delete the resources or perform any other high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the permissions required for using SFS resources.

If your Huawei Cloud account does not require individual IAM users for permissions management, skip this section.

IAM can be used free of charge. You pay only for the resources in your account. For more information about IAM, see [IAM Service Overview](#).

SFS Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

SFS is a project-level service deployed and accessed in specific physical regions. To assign SFS permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing SFS, the users need to switch to a region where they have been authorized to use this service.

You can grant users permissions by using roles and policies.

- **Roles:** A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. This mechanism provides only a limited number of service-level roles for authorization. When using roles to grant permissions, you need to also assign other roles on which the

permissions depend to take effect. However, roles are not an ideal choice for fine-grained authorization and secure 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 allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, you can grant ECS users only the permissions for managing a certain type of ECSs. Most policies define permissions based on APIs. For the API actions supported by SFS, see [Permissions Policies and Supported Actions](#).

Table 12-1 lists all the system-defined roles and policies supported by SFS.

Table 12-1 System permissions for SFS Capacity-Oriented

Role/Policy Name	Description	Type	Dependency
SFS FullAccess	Administrator permissions for SFS. Users granted these permissions can perform all operations on file systems.	System-defined policy	None
SFS ReadOnlyAccess	Read-only permissions. Users granted these permissions can only view file system data.	System-defined policy	None

Role/Policy Name	Description	Type	Dependency
SFS Administrator	Permissions include: <ul style="list-style-type: none"> • Creating, deleting, querying, and modifying file systems • Adding, modifying, and deleting access rules of file systems • Creating, querying, and deleting file system tags • Expanding and shrinking the capacity of a file system • Querying availability zones • Read-only permissions on all cloud services if the Tenant Guest policy is assigned 	System-defined role	Tenant Guest role needs to be assigned in the same project.

Table 12-2 lists the common operations supported by system-defined policies for SFS Capacity-Oriented.

Table 12-2 Common operations supported by each system-defined policy of SFS Capacity-Oriented

Operation	SFS FullAccess	SFS ReadOnlyAccess	SFS Administrator
Creating a file system	√	x	√
Querying a file system	√	√	√

Operation	SFS FullAccess	SFS ReadOnlyAccess	SFS Administrator
Modifying a file system	√	x	√
Deleting a file system	√	x	√
Adding an access rule of a file system (Adding a VPC or adding an authorized address to a file system)	√	x	√
Modifying an access rule of a file system (Modifying the VPC or authorized address of a file system).	√	x	√
Deleting an access rule of a file system (Deleting the VPC or authorized address of a file system).	√	x	√
Expanding the capacity of a file system	√	x	√
Shrinking the capacity of a file system	√	x	√
Creating file system tags	√	x	√
Querying file system tags	√	√	√
Deleting file system tags	√	x	√
Querying availability zones	√	√	√

Table 12-3 lists all the system-defined roles and policies supported by SFS Turbo.

Table 12-3 System-defined roles and policies supported by SFS Turbo

Role/Policy Name	Description	Type	Dependency
SFS Turbo FullAccess	Administrator permissions for SFS Turbo. Users granted these permissions can perform all operations on SFS Turbo file systems.	System-defined policy	None
SFS Turbo ReadOnlyAccess	Read-only permissions for SFS Turbo. Users granted these permissions can only view SFS Turbo file system data.	System-defined policy	None

Table 12-4 lists all the system-defined roles and policies supported by General Purpose File System.

 **NOTE**

Due to data caching, a role and policy involving General Purpose File System actions will take effect 10 to 15 minutes after it is attached to a user, an enterprise project, or a user group.

Table 12-4 System-defined roles and policies supported by General Purpose File System

Role/Policy Name	Description	Type	Dependency
SFS3 FullAccess	Administrator permissions for General Purpose File System. Users granted these permissions can perform all operations on general purpose file systems.	System-defined policy	None

Role/Policy Name	Description	Type	Dependency
SFS3 ReadOnlyAccess	Read-only permissions for General Purpose File System. Users granted these permissions can only view data in general purpose file systems.	System-defined policy	None

Table 12-5 lists the common operations supported by system-defined policies for General Purpose File System.

Table 12-5 Common operations supported by each system-defined policy of General Purpose File System

Operation	SFS3 FullAccess	SFS3 ReadOnlyAccess
Obtaining file system lifecycle rules	√	√
Querying resources by tag	√	√
Obtaining file system information	√	√
Querying tags by project	√	√
Querying tags of a resource	√	√
Obtaining file system limits	√	√
Obtaining file system ACL information	√	√
Obtaining the file system storage usage	√	√
Configuring file system limits	√	×
Batch Adding tags to a resource	√	×
Creating a file system	√	×
Deleting a file system	√	×
Batch deleting tags from a resource	√	×

Operation	SFS3 FullAccess	SFS3 ReadOnlyAccess
Setting/Deleting the file system lifecycle rules	√	×
Querying file systems	√	√
Configuring a file system ACL	√	×
Deleting a file system ACL	√	×

Role/Policy Dependencies of the SFS Turbo Console

Table 12-6 Role/Policy dependencies of the SFS Turbo console

Console Function	Dependent Services	Role/Policy Required
Creating a file system	VPC Billing Center DSS ECS	<ul style="list-style-type: none"> The permissions of the SFS Turbo FullAccess policy already include the permissions of VPC FullAccess, which are required for creating file systems. An IAM user assigned the SFS Turbo Full Access policy does not need to have the VPC FullAccess policy assigned explicitly. To create yearly/monthly file systems, the BSS Administrator policy is required. To create file systems in dedicated projects, the DSS FullAccess and ECS FullAccess policies are required.
Querying file system details	VPC	<ul style="list-style-type: none"> The permissions of the SFS Turbo ReadOnlyAccess policy already include the permissions of VPC ReadOnlyAccess, which are required for querying file system details. An IAM user assigned the SFS Turbo ReadOnlyAccess policy does not need to have the VPC ReadOnlyAccess policy assigned explicitly.
Creating a vault at the OBS backend	OBS	<ul style="list-style-type: none"> To create vaults at the OBS backend, the OBS Administrator policy is required.

Role/Policy Dependencies of the General Purpose File System Console

Table 12-7 Role/Policy dependencies of the General Purpose File System console

Console Function	Dependent Services	Role/Policy Required
Creating a general purpose file system	VPC	The permissions of the SFS3 FullAccess policy already include the permissions of VPC ReadOnlyAccess , which are required for creating general purpose file systems. An IAM user assigned the SFS3 FullAccess policy does not need to have the VPC ReadOnlyAccess policy assigned explicitly.
Querying general purpose file system details	VPC	The permissions of the SFS3 ReadOnlyAccess policy already include the permissions of VPC ReadOnlyAccess , which are required for querying general purpose file system details. An IAM user assigned the SFS3 ReadOnlyAccess policy does not need to have the VPC ReadOnlyAccess policy assigned explicitly.

Helpful Links

- [IAM Service Overview](#)
- [Creating a User and Granting SFS Permissions](#)
- [Permissions Policies and Supported Actions](#)

13 Supported OSs

Table 13-1 lists the OSs that have passed the compatibility test.

Table 13-1 Supported OSs

Type	Version	SFS Capacity-Oriented	General Purpose File System	SFS Turbo
Cent OS	CentOS 5, 6, and 7 for x86	√	√	√
Debian	Debian GNU/Linux 6, 7, 8, and 9 for x86	√	√	√
Oracle	Oracle Enterprise Linux 5, 6, and 7 for x86	√	√	√
Red Hat	Red Hat Enterprise Linux 5, 6, and 7 for x86	√	√	√
SUSE	SUSE Linux Enterprise Server 10, 11, and 12 for x86	√	√	√
Ubuntu	Ubuntu 14.04 and later	√	√	√
Euler OS	EulerOS 2	√	√	√
Fedora	Fedora 24 and 25	√	√	√
Open SUSE	OpenSUSE 42	√	√	√
Windows	Windows Server 2008, 2008 r2, 2012, 2012 r2, and 2016 for x64 Windows 7, 8, and 10	√	×	×