Scalable File Service

Service Overview

Issue 01

Date 2025-12-17

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/

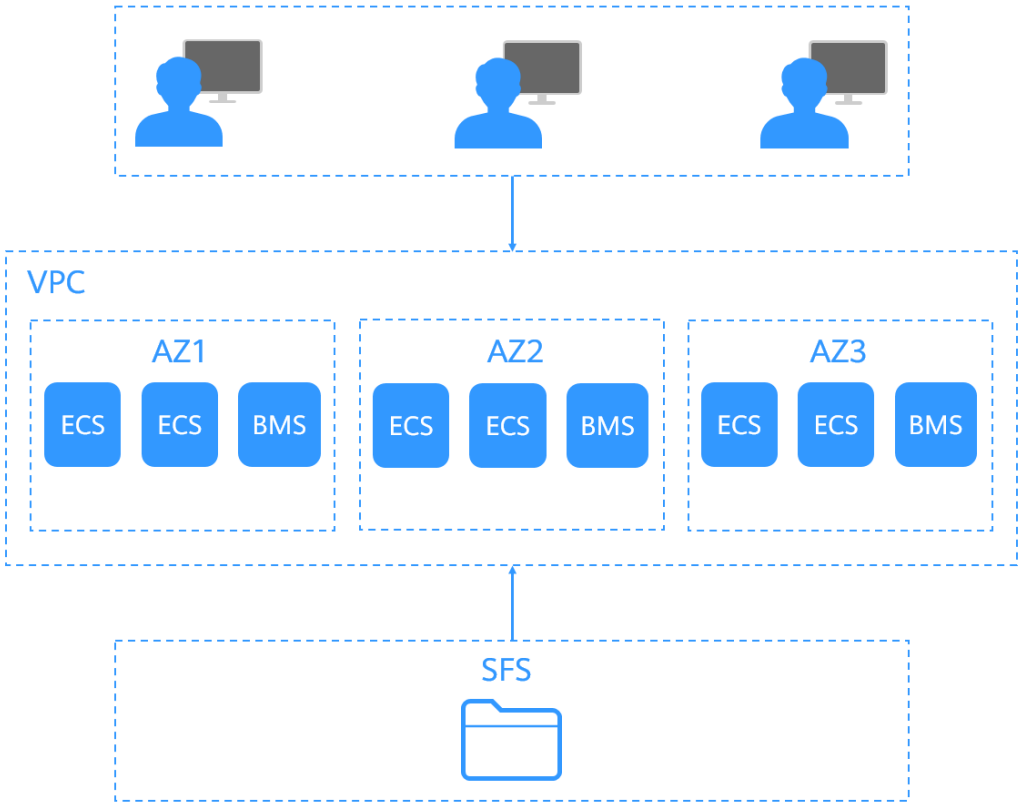
Contents

1 What Is 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). **Figure 1-1** shows the access to SFS.

Figure 1-1 Accessing SFS



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

- File sharing

Cloud servers in multiple availability zones (AZs) of the same region can access the same general-purpose file system and share files.

- Elastic scaling

  The file system 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 background storage system 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

  On an intuitive graphical user interface (GUI), you can create and manage general-purpose 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 console or via application programming interfaces (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**.

- Console

  Use the console if you prefer a web-based UI to perform operations.

2 Application Scenarios

Huawei Cloud General-Purpose File System provides file storage of various specifications. You can select one or more types of file systems based on your service requirements for reliable, secure, and continuous file storage.

General-Purpose File System provides fully hosted shared file storage that can be scaled up to petabytes of capacity and TB/s of bandwidth. Its high availability and durability can provide strong support for data- and bandwidth-intensive applications.

General-Purpose File System is suitable for various workloads, including high-performance computing, media processing, file sharing, content management, and web services. It also supports infrequent access storage.

- 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 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/s. 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.

- File sharing

  For an organization with a large number of staff, SFS allows you to create shared file systems that are accessible to all staff, to facilitate file sharing among staff.

- 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

  General-purpose file systems deliver an aggregate bandwidth of up to 10 Gbit/s, capable of handling ultra-large data files such as satellite images. In addition, its robust reliability prevents service interruptions caused by system failures.

3 Functions

This section describes main functions of SFS. You can check if a certain function is available in a region on the console.

NFS Protocol

Network File System (NFS) is a distributed file system protocol that allows different computers and operating systems (OSs) to share data over a network. After the NFS client is installed on each ECS, you can mount the file system to implement file sharing between ECSs. NFS is recommended for Linux clients. For more information, see **Mounting an NFS General-Purpose File System to ECSs (Linux)**.

File System Management

File systems are containers that store files in SFS. You can create, view, and delete SFS file systems. For more information, see **File System Management**.

Multi-VPC Access

You can configure multiple VPCs for a file system so that ECSs in different VPCs can share the same file system, as long as the VPCs that the ECSs belong to are added as authorized VPCs of the file system or the ECSs are added as authorized addresses of the VPCs. For more information, see **Configuring Multi-VPC Access**.

Permissions Management

SFS uses IAM for permissions management. You can control the read and write permissions of file systems by granting IAM users fine-grained SFS permissions using IAM custom policies. For more information, see **Permissions**.

Tag

You can use tags to classify and identify file systems. If you add tags to a file system, the bills generated for this file system will contain these tags. You can classify bills by tag for cost analysis. For more information, see **Managing General-Purpose File System Tags**.

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. For more information, see **Monitoring General-Purpose File System Using Cloud Eye**.

Replicating Settings of Existing File Systems

SFS allows you to replicate settings from an existing general-purpose file system when creating a new one. The following settings can be replicated: region, AZ, protocol, authorization, and tags. For more information, see **Creating a General-Purpose File System**.

Enterprise Project

An enterprise project manages multiple resources by category. Resources and projects in different cloud service regions can be classified into one enterprise project. For example, an enterprise can classify resources based on departments or project groups and then put relevant resources into the same enterprise project for management. Resources cannot be migrated between enterprise projects. For more information, see **Project and Enterprise Project**.

4 General-Purpose File System Types

The following table describes the characteristics, highlights, and application scenarios of general-purpose file systems.

For details about SFS Turbo file system types, see **SFS Turbo File System Types**.

Table 4-1 General-purpose file system

Parameter	Description
Max. bandwidth	1.25 TB/s
Max. IOPS	Million
Latency	10 ms
Max. capacity	EB
Highlights	Large capacity, high bandwidth, and low cost
Use cases	Cost-sensitive workloads which require large-capacity scalability, such as media processing, file sharing, high-performance computing, and data backup.

NOTE

- 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.

5 Security

5.1 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.

Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. For this reason, cloud security cannot be fully ensured by one party. Cloud security requires joint efforts of Huawei Cloud and you, as shown in **Figure 5-1**.

- **Huawei Cloud**: Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.
- **Customer**: As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

Figure 5-1 Huawei Cloud shared security responsibility model

Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. As shown in **Figure 5-1**, customers can select different cloud service types (such as IaaS, PaaS, and SaaS) based on their service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

- In on-premises scenarios, customers have full control over assets such as hardware, software, and data, so tenants are responsible for the security of all components.
- In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.
- In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the PaaS middleware, database, and network access under their control.
- In SaaS scenarios, customers have control over their content, accounts, and permissions. They need to protect their content, and properly configure and protect their accounts and permissions in compliance with laws and regulations.

On-premises (On-Prem): Software and IT infrastructure that are deployed and managed by customers within their own data centers, rather than be deployed by remote cloud service providers.

Infrastructure as a Service (IaaS): Cloud service providers offer compute, network, storage, and more infrastructure services, including **Elastic Cloud Server (ECS)**, **Virtual Private Network (VPN)**, and **Object Storage Service (OBS)**.

Platform as a Service (PaaS): Cloud service providers deliver platforms required for application development and deployment, such as **ModelArts** and **GaussDB**. Customers do not need to maintain the underlying infrastructure.

Software as a Service (SaaS): Cloud service providers offer complete application software, such as **Huawei Cloud Meeting**. Customers use the software directly without the need to install the application, maintain it, or manage its underlying platform or infrastructure.

5.2 Identity Authentication and Access Control

5.2.1 Access Control for SFS

You can use IAM to control access to your SFS resources. For details, see **Permissions**.

Table 5-1 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**

5.3 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.

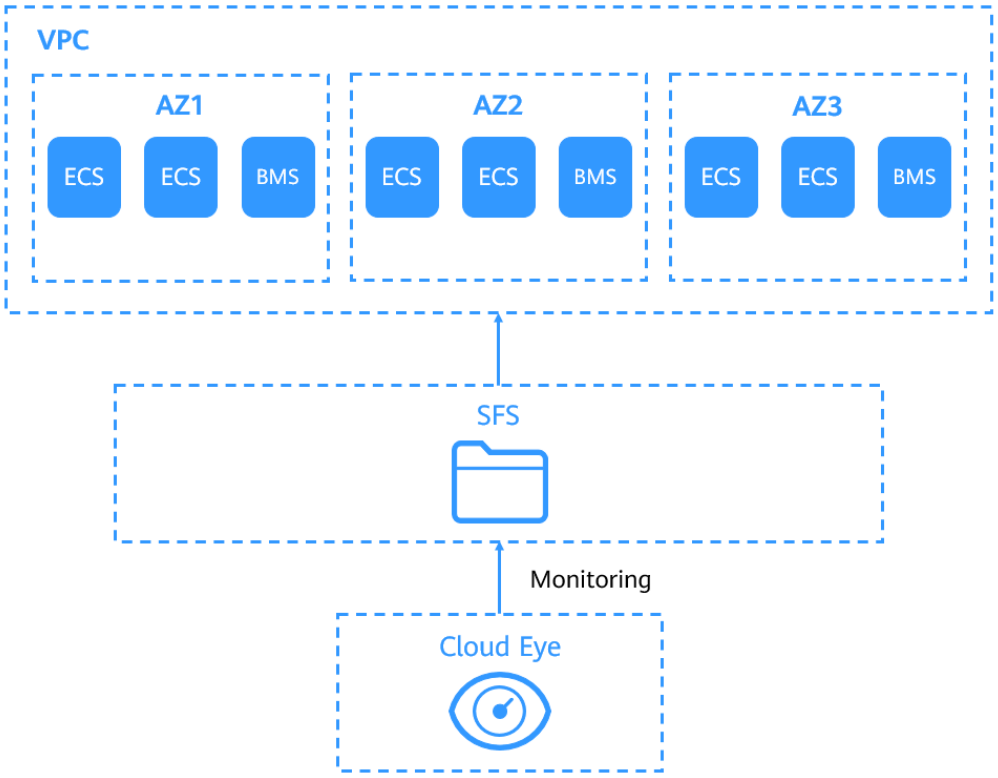
You can monitor the number of client connections, bandwidth, IOPS, and capacity of SFS file systems in real time.

For details about supported SFS metrics and how to create alarm rules, see **Monitoring General-Purpose File Systems Using Cloud Eye**.

6 SFS and Other Services

Figure 6-1 lists the relationship between SFS and other cloud services.

Figure 6-1 Relationships between SFS and other services



Relationships Between SFS and Other Services

Table 6-1 SFS and other services

Function	Related Service	Reference
A general-purpose file system and the ECSs must belong to the same project. File systems are mounted on the ECS local paths for data sharing.	Elastic Cloud Server (ECS)	**Mounting an NFS General-Purpose File System to ECSs (Linux)**
VPC provisions an isolated virtual network environment defined and managed by yourself, improving the security of cloud resources and simplifying network deployment. An ECS cannot access general-purpose file systems in a different VPC. Before using SFS, ensure that the general-purpose file system and the ECSs are in the same VPC.	Virtual Private Cloud (VPC)	**Creating a General-Purpose File System**
VPC Endpoint 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. General-Purpose File System communicates with ECS through VPC endpoints, so that ECSs can access general-purpose file systems.	VPC Endpoint	**Configuring a VPC Endpoint**
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.	Identity and Access Management (IAM)	**Permissions**
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 General-Purpose File System Using Cloud Eye**

Function	Related Service	Reference
You can use tags to classify and identify file systems.	Tag Management Service (TMS)	**Managing General-Purpose File System Tags**

7 Basic Concepts

7.1 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 OSs to share data over a network.

File System

A file system provides users with shared file storage through NFS. It is used for accessing network files remotely. After you create a file system on the console, you can mount the file system on multiple servers and access the file system from the servers through 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 APIs for software compatible with UNIX operating systems (OSs). POSIX is intended to achieve software portability at the source code level so that a program written for a POSIX compatible OS can be compiled and executed on any other POSIX OS.

7.2 Project and Enterprise Project

Enterprise Project

An enterprise project is used to manage multiple resource instances. 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.

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**.

7.3 Region and AZ

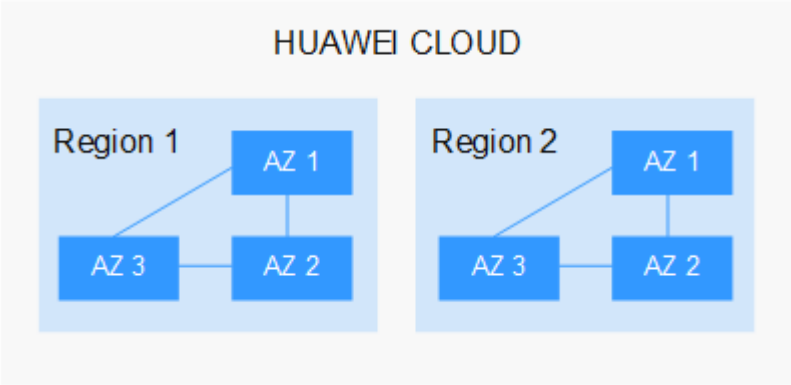
Concept

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 divided 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 into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific 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, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers. This enables users to build cross-AZ high-availability systems.

Figure 7-1 shows the relationship between regions and AZs.

Figure 7-1 Region and AZ



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 Products and Services**.

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.

- 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.

For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more information, see **Table 7-1**.

Table 7-1 Regions and endpoints

Region Name	Region ID	Endpoint	Protocol
CN North-Beijing4	cn-north-4	sfs3.cn-north-4.myhuaweicloud.com	HTTPS
CN East-Shanghai1	cn-east-3	sfs3.cn-east-3.myhuaweicloud.com	HTTPS
CN South-Guangzhou	cn-south-1	sfs3.cn-south-1.myhuaweicloud.com	HTTPS
CN Southwest-Guiyang1	cn-southwest-2	sfs3.cn-southwest-2.myhuaweicloud.com	HTTPS
CN-Hong Kong	ap-southeast-1	sfs3.ap-southeast-1.myhuaweicloud.com	HTTPS

8 Notes and Constraints

Table 8-1 General-purpose file system constraints

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 that a file system allows	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.
Client OS	• Cannot be mounted to 32-bit Linux servers. • Cannot be mounted to Windows servers.
Changing root directory permissions	Not supported

Item	Description
Constraints in the CCE and CCI scenarios	• When general-purpose file systems are 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	You can configure up to 20 lifecycle rules for a file system.
File locking with Flock	Not supported
Tag	• You can add a maximum of 20 tags to a file system. • Tag keys of a file system must be unique.

9 Billing

Billing Items

Pay-per-use billing is preset by default. You can create a general-purpose 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 9-1 General-Purpose File System billing model

Category	Billing Item	Billing Factor	Billing Description	Billing Formula	Billing Mode
Storage	Standard storage	Storage space	Billed based on the used capacity and usage period of the general-purpose file system	Storage price = Unit price per GB x Used capacity x Usage period	Pay-per-use Resource package

Category	Billing Item	Billing Factor	Billing Description	Billing Formula	Billing Mode
	Infrequent access storage	Storage space	Billed based on the used capacity and usage period of the general-purpose file system	Storage price = Unit price per GB x Used capacity x Usage period **NOTE** When calculating the price of a general-purpose file system, if the preset 14 days is used for **Transition to Infrequent Access After (Days)** in the file system lifecycle rule, 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

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

In the Price Calculator, 1 TB equals to 1,024 GB.

Billing Modes

SFS supports the following billing modes: pay-per-use and resource package. For details about how to purchase SFS, see **How Do I Purchase SFS?**

For details about the billing standards, see **Product Pricing Details**.

In addition, you can use the **Price Calculator** to quickly calculate an estimated price for the resources or resource packages that you select.

Changing Billing Mode

- Resource packages use a prepaid billing mode. You are billed based on the subscription duration you specify. This mode is ideal when the resource use duration is predictable. A longer subscription often means a lower cost.
- Pay-per-use is a postpaid billing mode. You are billed based on the billing items of specific general-purpose file systems and can purchase or delete file systems at any time. Expenditures are deducted from the account balance.

When using general-purpose file systems, package capacity within the same region is used preferentially. Multiple general-purpose file systems can share a resource package.

Renewal

For more information about renewal, including auto-renewal, exporting the renewal list, and changing subscriptions, see **Renewals**.

Expiration

After a resource package expires, you will be billed for subsequent resource usage on a pay-per-use basis. If you do not pay the amount due timely, the system processes the resource based on **Resource Suspension and Release**. If the resource package is not renewed before the retention period expires, the system automatically deletes the resource. For details about how to repay arrears, see **Making Payments (Postpaid Direct Customers)**.

Overdue Payment

Possible causes of overdue payment:

If the usage of your **expenditure quota** reaches or exceeds 100% and you do not make payments in a timely manner, a grace period starts.

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

Your general-purpose file systems are retained after your account is in arrears and file systems enter a retention period, but you cannot use the file systems. For details about how to repay arrears, see **Making Payments (Postpaid Direct Customers)**. 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**.

10 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 general-purpose file systems 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 for example, **cn-east-1** for **CN East-Shanghai1** 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**.

NOTE

The check mark (√) and cross symbol (x) indicate that an action takes effect or does not take effect for the corresponding type of projects.

Table 10-1 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 10-1 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
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 10-2 lists the common operations supported by system-defined policies for General-Purpose File System.

Table 10-2 Common operations supported by each system-defined policy of General-Purpose File System

Operation	SFS3 FullAccess	SFS3 ReadOnlyAccess
Obtaining file system lifecycle rules	√	√
Obtaining file information	√	√
Querying resources by tag	√	√
Obtaining files	√	√
Obtaining file system information	√	√
Querying tags by project	√	√
Obtaining CORS access rules of a file system	√	√
Querying resource tags	√	√
Querying site configurations	√	√
Obtaining file system limits	√	√
Obtaining file system ACL information	√	√
Querying project configurations	√	√
Obtaining the file system storage usage	√	√
Configuring file system limits	√	×
Creating or updating CORS access rules for a file system	√	×
Deleting project configurations	√	×
Batch adding tags to a resource	√	×
Creating project configurations	√	×
Deleting files	√	×

Operation	SFS3 FullAccess	SFS3 ReadOnlyAccess
Creating file systems	√	×
Deleting file systems	√	×
Batch deleting resource tags	√	×
Uploading files	√	×
Setting or deleting file system lifecycle rules	√	×
Deleting CORS access rules from a file system	√	×
Listing files in a file system	√	√
Listing file systems	√	√
Listing project configurations	√	√
Configuring file system ACLs	√	×
Deleting file system ACLs	√	×

Role/Policy Dependencies of the General-Purpose File System Console

Table 10-3 Role/Policy dependencies of the General-Purpose File System console

Console Function	Dependent Services	Role/Policy Required
Creating general-purpose file systems	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.

Console Function	Dependent Services	Role/Policy Required
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 and Supported Actions**

11 Supported OSs

Table 11-1 lists the OSs that have passed the compatibility test.

Table 11-1 Supported OSs

Type	Version
CentOS	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
EulerOS	EulerOS 2
Fedora	Fedora 24 and 25
openSUSE	openSUSE 42

