## 1 Management

1. Permissions Management

1.1 Creating a User and Granting SFS Permissions

1.2 Creating a Custom Policy

1.3 Network Configuration

1.4 Resizing a File System

1.5 Quotas

1.6 Backup

1.7 Monitoring

1.7.1 SFS Metrics

1.7.2 SFS Turbo Metrics

## 2 Typical Applications

2.1 HPC

2.2 Media Processing

2.3 Enterprise Website/App Background

2.4 Log Printing

## 3 Other Operations

3.1 SFS Turbo Performance Test

3.2 Mounting a File System to a Linux ECS as a Non-root User

3.3 Migrating Data to SFS Turbo

3.3.1 Data Migration Using Direct Connect

3.3.2 Data Migration Using the Internet

## A Change History
1.1 Permissions Management

1.1.1 Creating a User and Granting SFS Permissions

This chapter describes how to use IAM to implement fine-grained permissions control for your SFS resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing SFS resources.
- Grant only the permissions required for users to perform a specific task.

If your HUAWEI CLOUD account does not require individual IAM users, skip this section.

This section describes the procedure for granting permissions (see Figure 1-1).

**Prerequisites**

- If you intend to assign permissions using policies such as SFS **ReadOnlyAccess**, enable the policy-based access control function. For more information, see Applying for Policy-based Access Control.
- Learn about the permissions (see **System-defined roles and policies**) supported by SFS and choose policies or roles according to your requirements. For the permissions of other services, see **Permissions Policies**.

**Restrictions**
- All system-defined policies and custom policies are supported in SFS file systems.
- Only the following system-defined policies are supported in SFS Turbo file systems and custom policies are not supported. 
  
  **SFS ReadOnlyAccess**: SFS Turbo file system read-only permission; **SFS Administrator+VPC FullAccess**: creating, modifying, deleting, and querying SFS Turbo file systems.

**Process Flow**

**Figure 1-1** Process for granting SFS permissions

1. **Create a user group and assign permissions** to it.
   Create a user group on the IAM console, and attach the **SFS ReadOnlyAccess** policy to the group.
2. **Create an IAM user**.
   Create a user on the IAM console and add the user to the group created in 1.
3. **Log in** and verify permissions.
   Log in to SFS Console by using the user created in 2, and verify that the user only has read permissions for SFS.
   - Choose **Service List > Scalable File Service**. Click **Create File System** on SFS Console. If a message appears indicating that you have insufficient permissions to perform the operation, the **SFS ReadOnlyAccess** policy has already taken effect.
Choose any other service in the **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **SFS ReadOnlyAccess** policy has already taken effect.

### 1.1.2 Creating a Custom Policy

Custom policies can be created to supplement the system-defined policies of SFS. For the actions that can be added to custom policies, see [Permissions Policies and Supported Actions](#).

You can create custom policies in either of the following two ways:

- **Visual editor**: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- **JSON**: Edit JSON policies from scratch or based on an existing policy.

For details, see [Creating a Custom Policy](#). The following section contains examples of common SFS custom policies.

### Restrictions

The SFS Turbo file system does not support system-defined policies. Therefore, the created SFS custom policies are invalid for the SFS Turbo file system.

### Example Custom Policies

- **Example 1**: Allowing users to create file systems

  ```json
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "sfs:shares:createShare"
      ],
      "Effect": "Allow"
    }
  ]
  ```

- **Example 2**: Denying file system deletion

  A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **SFS FullAccess** policy to a user but also forbid the user from deleting file systems. Create a custom policy for denying file system deletion, and attach both policies to the group to which the user belongs. Then, the user can perform all operations on SFS except deleting file systems. The following is an example of a deny policy:

  ```json
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "sfs:shares:deleteShare"
      ]
    }
  ]
  ```
Example 3: Defining permissions for multiple services in a policy

A custom policy can contain actions of multiple services that are all of the global or project-level type. The following is an example policy containing actions of multiple services:

```json
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sfs:shares:createShare",
        "sfs:shares:deleteShare",
        "sfs:shares:updateShare"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:servers:delete"
      ]
    }
  ]
}
```

1.2 Managing File Systems

Viewing a File System

You can search for file systems by file system name keyword or file system status, and view their basic information.

Procedure

**Step 1** Log in to SFS Console.

**Step 2** In the file system list, view all file systems. Table 1-1 describes the parameters of each file system.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the file system, for example, sfs-name-001</td>
</tr>
<tr>
<td>AZ</td>
<td>Availability zone where the file system is located</td>
</tr>
<tr>
<td>Status</td>
<td>The value can be Available, Unavailable, Frozen, Creating, Deleting.</td>
</tr>
<tr>
<td>Type</td>
<td>File system types</td>
</tr>
<tr>
<td>Share Protocol</td>
<td>NFS protocol is supported.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Used Capacity (GB)       | Used space of the file system for storing data
|                          | NOTE        |
|                          | The space information is refreshed every 15 minutes. |
| Maximum Capacity (GB)    | Maximum capacity of the file system |
| Shared Path              | Shared path of the file system. The format is *File system domain name*/path or *File system IP address*/.  
|                          | NOTE        |
|                          | If the shared path is too long to display completely, expand the column to view the full shared path. |
| Operation                | For an SFS file system, valid operations include capacity adjustment, viewing monitoring indicators, and deletion.  
|                          | For an SFS Turbo file system, valid operations include deletion and viewing monitoring indicators. |

**Step 3** (Optional) Search for and view file systems by file system name keyword, key ID, or file system status.

---End

**Deleting a File System**

After a file system is deleted, data in it cannot be restored. To prevent data loss, before deleting a file system, ensure that files in it have been backed up locally.

**Prerequisites**

Before deleting the file system, unmount it first. For details about how to unmount the file system, see **Unmounting a File System**.

**Procedure**

**Step 1** Log in to SFS Console.

**Step 2** In the file system list, click **Delete** in the row of the file system you want to delete.

**Step 3** In the displayed dialog box, as shown in **Figure 1-2**, confirm the information, enter **Delete** in the text box, and then click **Yes**.

**NOTE**

Only **Available** and **Unavailable** file systems can be deleted.
Figure 1-2 Deleting a file system

Step 4  Check the file system list to confirm that the file system is deleted successfully.

Step 5  (Optional) If you want to delete more than one file system at a time, select the file systems, and then click Delete in the upper left part of the file system list. In the dialog box that is displayed, confirm the information, enter Delete in the text box, and then click Yes. This operation applies only to the SFS file system.

----End

1.3 Network Configuration

1.3.1 Configuring VPCs

VPC provisions an isolated virtual network environment defined and managed by yourself, improving the security of cloud resources and simplifying network deployment. When using SFS, a file system and the associated ECSs need to belong to a same VPC for file sharing.

In addition, VPC can use network access control list (ACL) to implement access control. A network ACL is an access control policy system for one or more subnets. Based on inbound and outbound rules, it determines whether data packets are allowed in or out of any associated subnet. In the VPC list of a file system, each time an authorization address is added and the corresponding permissions are set, a network ACL is created.

Multiple VPCs can be configured for an SFS 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.

For more information about VPC, see the Virtual Private Cloud.
Restrictions

- You can add a maximum of 20 VPCs for each file system. A maximum of 400 ACL rules for added VPCs can be created. When adding a VPC, the default IP address 0.0.0.0/0 is automatically added.
- If a VPC bound to the file system has been deleted from the VPC console, the IP address/address segment of this VPC in the VPC list of the file system can still be seen as activated. However, this VPC cannot be used any longer and you are advised to delete the VPC from the list.
- SFS Turbo file systems do not support multiple VPCs at the moment.

Procedure

**Step 1** Log in to SFS Console.

**Step 2** In the file system list, click the name of the target file system to go to the VPC authorization page.

**Step 3** If no VPCs are available, apply for one. You can add multiple VPCs for a file system. Click Add VPC and the Add VPC dialog box is displayed. See Figure 1-3.

You can select multiple VPCs from the drop-down list.

**Figure 1-3 Adding VPCs**

![Add Authorized VPC](image)

**Step 4** Click OK. A successfully added VPC is displayed in the list. When adding a VPC, the default IP address 0.0.0.0/0 is automatically added. The default read/write permission is **read/write**, the default user permission is **no_all_squash**, and the default root permission is **no_root_squash**.

**Step 5** View the VPC information in the VPC list. For details about the parameters, see Table 1-2.

**Table 1-2 Parameter description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the added VPC, for example, vpc-4040</td>
</tr>
<tr>
<td>Number of authorized IP addresses</td>
<td>Number of added IP addresses or IP address segments.</td>
</tr>
</tbody>
</table>
### Table 1-3

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>The value can be <strong>Add</strong> or <strong>Delete</strong>. <strong>Add</strong>: Adds an authorized VPC. This operation configures the IP address, read/write permission, user permission, user root permission, and priority. For details, see Table 1-3. <strong>Delete</strong>: Deletes this VPC.</td>
</tr>
</tbody>
</table>

**Step 6** Click on the left of the VPC name to view details about the IP addresses/segments added to this VPC. You can **Add**, **Edit**, and **Delete** IP addresses/segments. In the **Operation** column of the target VPC, click **Add**. The **Add Authorized Address/Segment** dialog box is displayed. See Figure 1-4. Table 1-3 describes the parameters to be added.

**Figure 1-4** Adding an authorized address or segment

![Add Authorized Address/Segment](image_url)
### Table 1-3 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Authorized Address/Segment    | - Only one IPv4 address or address segment can be entered.  
- The entered IPv4 address or address segment must be valid and cannot be an IP address or address segment starting with 0 except 0.0.0.0/0. The value 0.0.0.0/0 indicates any IP address in the VPC. In addition, the IP address or address segment cannot start with 127 or any number from 224 to 255, such as 127.0.0.1, 224.0.0.1, or 255.255.255.255. This is because IP addresses or address segments starting with any number from 224 to 239 are class D addresses and they are reserved for multicast. IP addresses or address segments starting with any number from 240 to 255 are class E addresses and they are reserved for research purposes. If an invalid IP address or address segment is used, the access rule may fail to be added or the added access rule cannot take effect.  
- Multiple addresses separated by commas (,), such as 10.0.1.32,10.5.5.10 are not allowed.  
- An address segment, for example, 192.168.1.0 to 192.168.1.255, needs to be in the mask format like 192.168.1.0/24. Other formats such as 192.168.1.0-255 are not allowed. The number of bits in a subnet mask must be an integer ranging from 0 to 31. The number of bits 0 is valid only in 0.0.0.0/0. |
| Read&Write Permissions        | The value can be **Read&Write** or **Read-only**. The default value is **Read&Write**.                                                                                                                                                                                                                                                   |
| User Permission               | Specifies whether to retain the user identifier (UID) and group identifier (GID) of the shared directory. The default value is **no_all_squash**.  
- **all_squash**: The UID and GID of a shared file are mapped to user **nobody**, which is applicable to public directories.  
- **no_all_squash**: The UID and GID of a shared directory are retained.                                                                                                                                                                                                 |
| User Root Permission          | Specifies whether to allow the root permission of the client. The default value is **no_root_squash**.  
- **root_squash**: Clients cannot access as the root user. When a client accesses as the root user, the user is mapped to the nobody user.  
- **no_root_squash**: Clients are allowed to access as the root user who has full control and access permissions of the root directories.                                                                                                                                                             |
### Parameter and Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>The value must be an integer ranging from 0 to 100. 0 indicates the highest priority, and 100 indicates the lowest priority. In the same VPC, the permission of the IP address or address segment with the highest priority is preferentially used. If some IP addresses or address segments are of the same priority, the permission of the most recently added or modified one prevails. For example, if the IP address for mounting is 10.1.1.32 and both 10.1.1.32 (read/write) with priority 100 and 10.1.1.0/24 (read-only) with priority 50 meet the requirements, the permission of 10.1.1.0/24 (read-only) with priority 50 prevails. That is, if there is no other authorized priority, the permission of all IP addresses in the 10.1.1.0/24 segment, including 10.1.1.32, is read-only.</td>
</tr>
</tbody>
</table>

#### NOTE

For an ECS in VPC A, its IP address can be added to the authorized IP address list of VPC B, but the file system of VPC B cannot be mounted to this ECS. The VPC used by the ECS and the file system must be the same one.

----End

### 1.3.2 Configuring DNS

A DNS server is used to resolve domain names of file systems. For details about DNS server IP addresses, see What Are the Private DNS Server Addresses Provided by the DNS Service?

By default, the IP address of the DNS server used to resolve domain names of file systems is automatically configured on ECSs when creating ECSs. No manual configuration is needed except when the resolution fails due to a change in the DNS server IP address.

Windows 2012 is used as an example in the operation procedures for Windows.

#### Procedure (Linux)

1. **Step 1** Log in to the ECS as user `root`.

2. **Step 2** Run the `vi /etc/resolv.conf` command to edit the `/etc/resolv.conf` file. Add the DNS server IP address above the existing nameserver information. See Figure 1-5.

#### Figure 1-5 Configuring DNS

```
: generated by /sbin/dhclient-script
search openstacklocal
nameserver 114.114.114.114
nameserver 110.110.110.110
```
The format is as follows:
nameserver 100.125.1.250

Step 3  Press Esc, input :wq, and press Enter to save the changes and exit the vi editor.

Step 4  Run the following command to check whether the IP address is successfully added:
        cat /etc/resolv.conf

Step 5  Run the following command to check whether an IP address can be resolved from
        the file system domain name:
        nslookup *File system domain name*

.note

Obtain the file system domain name from the file system shared path.

Step 6  (Optional) In a network environment of the DHCP server, edit the /etc/resolv.conf
        file to prevent the file from being automatically modified upon an ECS startup,
        and prevent the DNS server IP address added in Step 2 from being reset.
1. Run the following command to lock the file:
        chattr +i /etc/resolv.conf

       .note

       Run the chattr -i /etc/resolv.conf command to unlock the file if needed.

2. Run the following command to check whether the editing is successful:
        lsattr /etc/resolv.conf

If a command output similar to Figure 2 is displayed, the file has been locked.

Figure 1-6  A locked file

```
[root@dm011IP-Node-Boot ]# lsattr /etc/resolv.conf
---i--------e- /etc/resolv.conf
```

----End

Procedure (Windows)

Step 1  Go to the ECS console and log in to the ECS running Windows 2012.

Step 2  Click This PC in the lower left corner.

Step 3  On the page that is displayed, right-click Network and choose Properties from
        the drop-down list. The Network and Sharing Center page is displayed, as shown in
        Figure 1-7. Click Local Area Connection.
Figure 1-7 Page for network and sharing center

**Step 4** In the Activity area, select **Properties**. See **Figure 1-8**.

**Figure 1-8** Local area connection

**Step 5** In the Local Area Connection Properties dialog box that is displayed, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. See **Figure 1-9**.
Step 6 In the dialog box that is displayed, select **Use the following DNS server addresses**: and configure DNS, as shown in Figure 1-10. The DNS server IP address is 100.125.1.250. After completing the configuration, click **OK**.

Figure 1-10 Configuring DNS on Windows

---End
1.4 Resizing a File System

You can expand or shrink the capacity of a file system when needed.

SFS Turbo file systems support online capacity expansion. During the capacity expansion, the file system will be unavailable for two to three minutes. Online capacity expansion may not be available for some instances of earlier versions. If capacity expansion is required, click Service Tickets in the upper right corner of the console to submit a service ticket.

Rules for Resizing

- Expanding a file system
  Total capacity of a file system after expansion ≤ (Capacity quota of the cloud account - Total capacity of all the other file systems owned by the cloud account)
  For example, cloud account A has a quota of 500 TB. This account has already created three file systems: SFS1 (350 TB), SFS2 (50 TB), and SFS3 (70 TB). If this account needs to expand SFS2, the new capacity of SFS2 cannot be greater than 80 TB. Otherwise, the system will display a message indicating an insufficient quota and the expansion operation will fail.

- Shrinking a file system
  - When a shrink error or failure occurs on a file system, it takes approximately five minutes for the file system to restore to the available state.
  - After a shrink operation fails, you can only reattempt to shrink the file system storage capacity but cannot expand it directly.
  - Total capacity of a file system after shrinking ≥ Used capacity of the file system
  For example, cloud account B has created a file system, SFS1. The total capacity and used capacity of SFS1 are 50 TB and 10 TB respectively. When shrinking SFS1, the user cannot set the new capacity to be smaller than 10 TB.

Procedure

Step 1 Log in to SFS Console.

Step 2 In the file system list, click Resize in the row of the file system you want to resize. The Resize File System dialog box is displayed.

Step 3 Enter a new maximum capacity of the file system based on service requirements, and click OK. Table 1-4 describes the parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used Capacity (GB)</td>
<td>Used capacity of the current file system</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maximum Capacity (GB)</td>
<td>Maximum capacity of the current file system</td>
</tr>
<tr>
<td>New Maximum Capacity (GB)</td>
<td>Target maximum capacity of the file system after expanding or shrinking.</td>
</tr>
<tr>
<td></td>
<td>The value ranges from 1 GB to 512,000 GB.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
</tr>
<tr>
<td></td>
<td>The new maximum capacity cannot be smaller than the used capacity.</td>
</tr>
</tbody>
</table>

**Step 4** In the dialog box that is displayed, confirm the information and click **Yes**.

**Step 5** In the file system list, check the capacity information after resizing.

----End

### 1.5 Quotas

**What Is Quota?**

Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

**How Do I View My Quotas?**

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose Resources > My Quotas. The Service Quota page is displayed.
4. View the used and total quota of each type of resources on the displayed page.
   If a quota cannot meet service requirements, click Increase Quota to adjust it.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose Resources > My Quotas.
   The Service Quota page is displayed.

3. Click Increase Quota.
4. On the Create Service Ticket page, configure parameters as required.
   In Problem Description area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select I have read and agree to the Tenant Authorization Letter and Privacy Statement and click Submit.
1.6 Backup

Currently, only SFS Turbo file systems provide the file system backup function. The maximum number of backups is 20. You can create backups and backup policies based on service requirements.

Scenarios

A backup is a complete copy of an SFS Turbo file system at a specific time and it records all configuration data and service data at that time. When backing up file systems based on service requirements, you can create a file system backup on the Backup tab page.

For example, if a file system is faulty or encounters a logical error (for example, mis-deletion, hacker attacks, and virus infection), you can use data backups to restore data quickly.

Creating a File System Backup

Ensure that the target file system runs no task. Otherwise, the backup task cannot start. This topic describes how to manually create a file system backup.

**Step 1** Log in to SFS Console.

**Step 2** In the file system list, find the SFS Turbo file system to be backed up and click the name of it. The file system details page is displayed.

**Step 3** On the Backup tab page, click Create Backup. See Figure 1-13.

**Figure 1-13 Creating a backup**

![Create Backup](image)

**Step 4** In the Create Backup dialog box, enter the backup name and description. For details about the parameters, see Table 1-5.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Name</td>
<td>backup-001</td>
</tr>
<tr>
<td>Description</td>
<td>for test</td>
</tr>
</tbody>
</table>
### Table 1-5 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup name</td>
<td>Enter 4 to 64 characters starting with a letter. The name cannot start with the word &quot;auto&quot; and can only contain letters, digits, and hyphens (-).</td>
<td>backup-001</td>
</tr>
<tr>
<td>Backup description</td>
<td>The value contains a maximum of 0 to 64 characters and cannot contain the following special characters: !&quot;&lt;&gt;-=&amp;&quot;</td>
<td>for test</td>
</tr>
</tbody>
</table>

**Step 5** Click **Submit**.

**Step 6** The system automatically backs up the file system.

You can view the backup creation status on the **Backup** tab page. When the **Status** of the backup changes to **Available**, the backup has been successfully created.

---- End

### Setting a Backup Policy

In addition to setting a backup policy when creating an SFS Turbo file system, you can also create a backup policy on the file system details page.

After the automated backup policy is enabled, the system automatically creates backups based on the preset time and period.

**Step 1** Log in to the management console and select **Scalable File Service**.

**Step 2** In the file system list, click the name of the target file system to go to the detail information page.

**Step 3** On the **Backup** tab page, click **Modify Backup Policy**. See **Figure 1-14**.

**Figure 1-14 Setting a backup policy**
Step 4 Slide on the **Automatic Backup** switch.

[Image indicates that the backup policy is enabled and indicates that the backup policy is disabled. For details about parameter settings, see Backup Policy Parameter Description.]

Step 5 Confirm the configuration and click **Submit**.

Step 6 If you want to modify the backup policy, click **Modify Backup Policy** again. The backup policy cannot be deleted. If the backup policy is not required, disable it.

----End

Restoring the File System Using a Backup

To view the backup data of a file system at a certain time, you must use the backup to restore the file system. The backup status must be **Available**.

When a backup is used to restore the file system, the data in the file system is restored to the state at the backup time. Modifications (including new data) after the backup time will be lost. The file system is unavailable during the restoration. Exercise caution when performing this operation.

Step 1 Log in to the management console and select **Scalable File Service**.

Step 2 In the file system list, click the name of the target file system to go to the detail information page.

Step 3 On the **Backup** tab page, click **Restore** in the **Operation** column of the target backup. See **Figure 1-15**.

**Figure 1-15** Restoring a backup

Step 4 After confirming that the restoration information is correct, enter **Restore** in the text box and click **OK**.

Step 5 You can view the backup restoration status in the backup list. When the backup status changes from **Restoring** to **Available**, the restoration is successful.

----End
Deleting a Backup

If you do not need to use the backup or the backup status is **Unavailable**, you can delete the backup. A deleted backup cannot be recovered. Exercise caution when performing this operation.

**Step 1** Log in to the management console and select **Scalable File Service**.

**Step 2** In the file system list, click the name of the target file system to go to the detail information page.

**Step 3** On the **Backup** tab page, click **Delete** in the **Operation** column of the target backup.

**Step 4** After confirming that the deletion information is correct, enter **Delete** in the text box and click **OK**.

**Step 5** Confirm that the backup is deleted successfully by checking the backup list.

----End

1.7 Monitoring

1.7.1 SFS Metrics

**Function**

This topic describes metrics reported by Scalable File Service (SFS) as well as their namespaces and dimensions. You can use the console or **APIs** provided by Cloud Eye to query the metrics generated for SFS.

**Namespace**

SYS.SFS

**Metrics**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Name</th>
<th>Description</th>
<th>Value Range</th>
<th>Monitored Object</th>
<th>Monitoring Period (Original Metric)</th>
</tr>
</thead>
<tbody>
<tr>
<td>read.bandwidth</td>
<td>Read Bandwidth</td>
<td>Read bandwidth of a file system within a monitoring period</td>
<td>≥ 0 bytes/s</td>
<td>SFS file system</td>
<td>4 minutes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: byte/s</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Metric**

<table>
<thead>
<tr>
<th>Metric Name</th>
<th>Description</th>
<th>Value Range</th>
<th>Monitored Object</th>
<th>Monitoring Period (Original Metric)</th>
</tr>
</thead>
<tbody>
<tr>
<td>write_bandwidth</td>
<td>Write bandwidth of a file system within a monitoring period Unit: byte/s</td>
<td>≥ 0 bytes/s</td>
<td>SFS file system</td>
<td>4 minutes</td>
</tr>
<tr>
<td>rw_bandwidth</td>
<td>Read and write bandwidth of a file system within a monitoring period Unit: byte/s</td>
<td>≥ 0 bytes/s</td>
<td>SFS file system</td>
<td>4 minutes</td>
</tr>
</tbody>
</table>

**Dimension**

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>share_id</td>
<td>SFS file system</td>
</tr>
</tbody>
</table>

**Viewing Monitoring Statistics**

**Step 1** Log in to the management console.

**Step 2** View the monitoring graphs using either of the following methods.

- Method 1: Choose **Service List > Storage > Scalable File Service**. In the file system list, click **View Metric** in the **Operation** column of the target file system.

- Method 2: Choose **Management & Deployment > Cloud Eye > Cloud Service Monitoring > Scalable File Service**. In the file system list, click **View Metric** in the **Operation** column of the target file system.

**Step 3** You can view the SFS file system monitoring data by metric or monitored duration.

*Figure 1-16* shows the monitoring graphs. For more information about Cloud Eye, see the *Cloud Eye User Guide*. 
# 1.7.2 SFS Turbo Metrics

## Function

This topic describes metrics reported by Elastic File Service (EFS) to Cloud Eye as well as their namespaces and dimensions. You can use the console or APIs provided by Cloud Eye to query the metrics generated for EFS.

## Namespace

SYS.EFS

## Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Metric Name</th>
<th>Description</th>
<th>Value Range</th>
<th>Monitored Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>client_connection</td>
<td>Client Connections</td>
<td>Number of client connections</td>
<td>≥ 0</td>
<td>SFS Turbo file system</td>
</tr>
<tr>
<td>data_read_io_bytes</td>
<td>Read Bandwidth</td>
<td>Data read I/O load</td>
<td>≥ 0 bytes/s</td>
<td>SFS Turbo file system</td>
</tr>
<tr>
<td>data_write_io_bytes</td>
<td>Write Bandwidth</td>
<td>Data write I/O load</td>
<td>≥ 0 bytes/s</td>
<td>SFS Turbo file system</td>
</tr>
<tr>
<td>metadata_io_bytes</td>
<td>Metadata Read and Write Bandwidth</td>
<td>Metadata read and write I/O load</td>
<td>≥ 0 bytes/s</td>
<td>SFS Turbo file system</td>
</tr>
<tr>
<td>total_io_bytes</td>
<td>Total Bandwidth</td>
<td>Total I/O load</td>
<td>≥ 0 bytes/s</td>
<td>SFS Turbo file system</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric Name</td>
<td>Description</td>
<td>Value Range</td>
<td>Monitored Object</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>--------------------------------------------------</td>
<td>-------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>iops</td>
<td>IOPS</td>
<td>I/O operations per unit time</td>
<td>≥ 0</td>
<td>SFS Turbo file system</td>
</tr>
<tr>
<td>used_capacity</td>
<td>Capacity</td>
<td>Used capacity of a file system</td>
<td>≥ 0 bytes</td>
<td>SFS Turbo file system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: byte</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>capacity</td>
<td>Percentage of used capacity in the total capacity</td>
<td>0% to 100%</td>
<td>SFS Turbo file system</td>
</tr>
<tr>
<td></td>
<td>Usage</td>
<td>Unit: Percent</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Dimension

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>efs_instance_id</td>
<td>Instance</td>
</tr>
</tbody>
</table>

### Viewing Monitoring Statistics

**Step 1** Log in to the management console.

**Step 2** View the monitoring graphs using either of the following methods.

- Method 1: Choose **Service List > Storage > Scalable File Service**. In the file system list, click **View Metric** in the **Operation** column of the target file system.

- Method 2: Choose **Management & Deployment > Cloud Eye > Cloud Service Monitoring > Elastic File Service**. In the file system list, click **View Metric** in the **Operation** column of the target file system.

**Step 3** You can view the SFS Turbo file system monitoring data by metric or monitored duration.

**Figure 1-17** shows the monitoring graphs. For more information about Cloud Eye, see the **Cloud Eye User Guide**.
Figure 1-17 SFS Turbo monitoring graphs

----End
2 Typical Applications

2.1 HPC

Context

HPC is short for high-performance computing. An HPC system or environment is made up of a single computer system with many CPUs, or a cluster of multiple computers clusters. It can handle a large amount of data and perform high-performance computing that would be rather difficult for PCs. HPC has ultra-high capability in floating-point computation and can be used for compute-intensive and data-intensive fields, such as industrial design, bioscience, energy exploration, image rendering, and heterogeneous computing. Different scenarios put different requirements on the file system:

- Industrial design: In automobile manufacturing, CAE and CAD simulation software are widely used. When the software is operating, compute nodes need to communicate with each other closely, which requires high bandwidth and low latency of the file system.
- Bioscience: The file system should have high bandwidth and large storage, and be easy to expand.
  - Bioinformatics: To sequence, stitch and compare genes.
  - Molecular dynamics: To simulate the changes of proteins in molecular and atomic levels.
  - New drug R&D: To complete high-throughput screening (HTS) to shorten the R&D cycle and reduce the investment.
- Energy exploration: Field operations, geologic prospecting, geological data processing and interpretation, and identification of oil and gas reservoirs all require large memory and high bandwidth of the file system.
- Image rendering: Image processing, 3D rendering, and frequent processing of small files require high read/write performance, large capacity, and high bandwidth of file systems.
- Heterogeneous computing: Compute elements may have different instruction set architectures, requiring the file system provide high bandwidth and low latency.

SFS is a shared storage service based on file systems. It features high-speed data sharing, dynamic storage tiering, as well as on-demand, smooth, and online resizing. These outstanding features empower SFS to meet the demanding requirements of HPC on storage capacity, throughput, IOPS, and latency.

A biological company needs to perform plenty of gene sequencing using software. However, due to the trivial steps, slow deployment, complex process, and low efficiency, self-built clusters are reluctant to keep abreast of business development. However, things are getting better since the company resorted to professional HPC service process management software. With massive compute and storage resource of the cloud platform, the initial investment and cost during O&M are greatly reduced, the service rollout time is shortened, and efficiency is boosted.

### Configuration Process

1. Organize the files of DNA sequencing to be uploaded.
2. Log in to SFS Console. Create a file system to store the files of DNA sequencing.
3. Log in to the ECSs that function as the head node and compute node, and mount the file system.
4. On the head node, upload the files to the file system.
5. On the compute node, edit the files.

### Prerequisites

- A VPC has been created.
- ECSs that function as head nodes and compute nodes have been created, and have been assigned to the VPC.
- SFS has been subscribed.

### Example Configuration

**Step 1** Log in to SFS Console.

**Step 2** In the upper right corner of the page, click **Create File System**.

**Step 3** On the **Create File System** page, set parameters as instructed.

**Step 4** After the configuration is complete, click **Create Now**.

For details about how to mount a file system to an ECS running Linux, see **Mounting an NFS File System to ECSs (Linux)**.

**Step 5** Log in to the head node, and upload the files to the file system.
Step 6  Start gene sequencing, and the compute node obtains the gene sequencing file from the mounted file system for calculation.

---End

2.2 Media Processing

Context

Media processing involves uploading, downloading, cataloging, transcoding, and archiving media materials, as well as storing, invoking, and managing audio and video data. Media processing has the following requirements on shared file systems:

- Media materials feature a high video bit rate and a large scale. The capacity of file systems must be large and easy to be expanded.
- Acquisition, editing, and synthesis of audio and video data require stable and low-latency file systems.
- Concurrent editing requires file systems to deliver reliable and easy-to-use data sharing.
- Video rendering and special effects need processing small files frequently. The file systems must offer a high I/O performance.

SFS is a shared storage service based on file systems. It features high-speed data sharing, dynamic storage tiering, as well as on-demand, smooth, and online resizing. The outstanding features empower SFS to meet the demanding requirements of media processing on storage capacity, throughput, IOPS, and latency.

A TV channel has a large amount of audio and video materials to process. The work will be done on multiple editing workstations. The TV channel uses SFS to enable file sharing among the editing workstations. First, a file system is mounted to ECSs that function as upload workstations and editing workstations. Then raw materials are uploaded to the shared file system through the upload workstations. Then, the editing workstations concurrently edit the materials in the shared file system.

Configuration Process

1. Organize the material files that are to be uploaded.
2. Log in to SFS Console. Create a file system to store the material files.
3. Log in to the ECSs that function as upload workstations and editing workstations, and mount the file system.
4. On the upload workstations, upload the material files to the file system.
5. On the editing stations, edit the material files.

Prerequisites

- A VPC has been created.
- ECSs that function as upload workstations and editing workstations have been created, and have been assigned to the VPC.
Example Configuration

Step 1 Log in to SFS Console.
Step 2 In the upper right corner of the page, click Create File System.
Step 3 On the Create File System page, set parameters as instructed.
Step 4 After the configuration is complete, click Create Now.
   For details about how to mount a file system to an ECS running Linux, see Mounting an NFS File System to ECSs (Linux).
Step 5 Log in to the upload workstations, and upload the material files to the file system.
Step 6 Log in to the editing stations, and edit the material files.

2.3 Enterprise Website/App Background

Context

For I/O-intensive website services, SFS Turbo can provide shared website source code directories and storage for multiple web servers, enabling low-latency and high-IOPS concurrent share access. Features of such services are as follows:

- A large number of small files: Static website files need to be stored, including HTML files, JSON files, and static images.
- Read I/O intensive: Scope of data reading is large, and data writing is relatively small.
- Multiple web servers access an SFS Turbo background to achieve high availability of website services.

Configuration Process

1. Sort out the website files.
2. Log in to SFS Console. Create an SFS Turbo file system to store the website files.
3. Log in to the ECS that functions as the compute node and mount the file system.
4. On the head node, upload the files to the file system.
5. Start the web server.

Prerequisites

- A VPC has been created.
- ECSs that function as head nodes and compute nodes have been created, and have been assigned to the VPC.
- SFS Turbo has been enabled.
Example Configuration

Step 1  Log in to SFS Console.
Step 2  In the upper right corner of the page, click Create File System.
Step 3  On the Create File System page, set parameters as instructed.
Step 4  After the configuration is complete, click Create Now.
   For details about how to mount a file system to an ECS running Linux, see Mounting an NFS File System to ECSs (Linux).
Step 5  Log in to the head node and upload the files to the file system.
Step 6  Start the web server.

----End

2.4 Log Printing

Context

SFS Turbo can provide multiple service nodes for shared log output directories, facilitating log collection and management of distributed applications. Features of such services are as follows:

- A shared file system is mounted to multiple service hosts and logs are printed concurrently.
- Large file size and small I/O: The size of a single log file is large, but the I/O of each log writing is small.
- Write I/O intensive: Write I/O of small blocks is the major service.

Configuration Process

1. Log in to SFS Console. Create an SFS Turbo file system to store the log files.
2. Log in to the ECS that functions as the compute node and mount the file system.
3. Configure the log directory to the shared file system. It is recommended that each host use different log files.
4. Start applications.

Prerequisites

- A VPC has been created.
- ECSs that function as head nodes and compute nodes have been created, and have been assigned to the VPC.
- SFS Turbo has been enabled.

Example Configuration

Step 1  Log in to SFS Console.
**Step 2** In the upper right corner of the page, click **Create File System**.

**Step 3** On the **Create File System** page, set parameters as instructed.

**Step 4** After the configuration is complete, click **Create Now**.

For details about how to mount a file system to an ECS running Linux, see [Mounting an NFS File System to ECSs (Linux)](https://example.com/mounting-nfs).

**Step 5** Configure the log directory to the shared file system. It is recommended that each host use different log files.

**Step 6** Start applications.

---- End
3 Other Operations

3.1 SFS Turbo Performance Test

fio is an open-source I/O pressure test tool. You can use fio to test the throughput and IOPS of SFS.

Prerequisites

The fio tool has been installed on the ECS. fio can be downloaded from the official website or GitHub.

Note and Description

The test performance depends on the network bandwidth between the client and server, as well as the capacity of the file system.

Installing fio

The following uses the Linux CentOS operating system as an example:

1. Download fio from the official website.
   
   ```bash
   yum install fio
   ```
2. Install the libaio engine.
   
   ```bash
   yum install libaio-devel
   ```
3. Check the fio version.
   
   ```bash
   fio --version
   ```

File System Performance Data

The performance indicators of SFS Turbo file systems include IOPS and throughput. For details, see Table 3-1.
### Table 3-1 Performance data

<table>
<thead>
<tr>
<th>Parameter</th>
<th>SFS Turbo Standard</th>
<th>SFS Turbo Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum capacity</td>
<td>32 TB</td>
<td>32 TB</td>
</tr>
<tr>
<td>Maximum IOPS</td>
<td>5,000</td>
<td>20000</td>
</tr>
<tr>
<td>Maximum throughput</td>
<td>150 MB/s</td>
<td>350 MB/s</td>
</tr>
<tr>
<td>Formula used to calculate the IOPS</td>
<td>IOPS = Min. (5,000, 1,200 + 6 x Capacity)</td>
<td>IOPS = Min. (20,000, 1,500 + 50 x Capacity)</td>
</tr>
</tbody>
</table>

#### Description of the IOPS Calculation Formula

IOPS of a single file system = Min. (Maximum IOPS, Baseline IOPS + IOPS per GB x Capacity)

For example, the maximum IOPS of a single SFS Turbo Performance file system is 20,000.

- If the capacity of an SFS Turbo Performance file system is 100 GB, the IOPS is calculated as follows: IOPS = Min. (20,000, 1,500 + 50 x 100). Compare 20,000 and 6,500 and obtain the smaller value, which is 6,500. Therefore, the IOPS of the file system is 6,500.
- If the capacity of an SFS Turbo Performance file system is 1,000 GB, the IOPS is calculated as follows: IOPS = Min. (20,000, 1,500 + 50 x 1,000). Compare 20,000 and 51,500 and obtain the smaller value, which is 30,000. Therefore, the IOPS of the file system is 20,000.

#### Common Test Configuration Example

This section uses SFS Turbo Performance as an example to describe the specifications of the ECS.

Specifications: General computing-plus | c3.xlarge.4 | 4vCPUs | 16 GB

Image: CentOS 7.5 64-bit

Mixed read/write with the read/write ratio being 7:3

- fio command:

  ```
  fio --randrepeat=1 --ioengine=libaio --name=test -output=output.log --direct=1 --filename=/mnt/nfs/test_fio --bs=4K --iodepth=128 --size=10240M --readwrite=rw --rwmixwrite=30 --fallocate=none
  ```

  **NOTE**

  In the preceding command, `/mnt/nfs/test_fio` indicates the mount path of the target file to be tested. The path must be specific to the file name, that is, the test_fio file in the /mnt/nfs directory. Set it based on the site requirements.
Mixed read/write with the read/write ratio being 3:7

- fio command:
  
fio --randrepeat=1 --ioengine=libaio --name=test -output=output.log --direct=1 --filename=/mnt/nfs/test_fio --bs=4K --iodepth=128 --size=10240M --readwrite=rw --rwmixwrite=70 --fallocate=none

**NOTE**

In the preceding command, `/mnt/nfs/test_fio` indicates the mount path of the target file to be tested. The path must be specific to the file name, that is, the `test_fio` file in the `/mnt/nfs` directory. Set it based on the site requirements.

- fio result:
Read IOPS

- fio command:
  
  ```
  fio --randrepeat=1 --ioengine=libaio --name=test -output=output.log --
  direct=1 --filename=/mnt/sfs-turbo/test_fio --bs=4k --iodepth=128 --
  size=10240M --readwrite=read --fallocate=none
  ```

  **NOTE**
  
  In the preceding command, `/mnt/sfs-turbo/test_fio` indicates the mount path of the target file to be tested. The path must be specific to the file name, that is, the `test_fio` file in the `/mnt/sfs-turbo` directory. Set it based on the site requirements.

- fio result:
Write IOPS

- fio command:
  ```
  fio --randrepeat=1 --ioengine=libaio --name=test --output=output.log --
  direct=1 --filename=/mnt/sfs-turbo/test_fio --bs=4k --iodepth=128 --
  size=10240M --readwrite=write--fallocate=none
  ```

- NOTE

In the preceding command, `/mnt/sfs-turbo/test_fio` indicates the mount path of the target file to be tested. The path must be specific to the file name, that is, the `test_fio` file in the `/mnt/sfs-turbo` directory. Set it based on the site requirements.

- fio result:

```
Run status group 0 (all jobs):
READ: bw=159MB/s (167MB/s), 159MB/s-159MB/s (167MB/s-167MB/s), io=io.008 (10.7GB), run=8
```

---

Read bandwidth
● fio command:
```
fio --randrepeat=1 --ioengine=libaio --name=test -output=output.log --
direct=1 --filename=/mnt/sfs-turbo/test_fio --bs=1M --iodepth=128 --
size=10240M --readwrite=read--fallocate=none
```

**NOTE**

In the preceding command, `/mnt/sfs-turbo/test_fio` indicates the mount path of the target file to be tested. The path must be specific to the file name, that is, the `test_fio` file in the `/mnt/sfs-turbo` directory. Set it based on the site requirements.

● fio result:

```
<table>
<thead>
<tr>
<th>bw (Kib/s)</th>
<th>min: 18, max: 33581, per: 68.77%, avg: 156090.01, stdev: 41255.43, samples: 427</th>
</tr>
</thead>
<tbody>
<tr>
<td>lat (msec)</td>
<td>50-0.34%, 100-0.31%, 250-47.97%, 500-42.73%, 750-0.85%</td>
</tr>
<tr>
<td>cpu</td>
<td>usr: 0.06%, sys: 4.02%, ctx: 10235, majf: 0, minf: 623</td>
</tr>
<tr>
<td>depths</td>
<td>1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.2%, 32=0.3%, 64=99.4%</td>
</tr>
<tr>
<td>submit</td>
<td>0.0%, 0.0%, 0.0%, 0.0%, 0.0%, 0.0%, 0.0%, 0.0%, 0.0%, 0.0%</td>
</tr>
<tr>
<td>complete</td>
<td>0.0%, 0.0%, 0.0%, 0.0%, 0.0%, 0.0%, 0.0%, 0.0%, 0.0%, 0.0%</td>
</tr>
<tr>
<td>issued r/w</td>
<td>total:10240/0, short:0/0, dropped:0/0, latency:0/0</td>
</tr>
<tr>
<td>latency</td>
<td>target:0, window:0, percentile:100.00%, depth:128</td>
</tr>
</tbody>
</table>
```

**Write bandwidth**

● fio command:
```
fio --randrepeat=1 --ioengine=libaio --name=test -output=output.log --
direct=1 --filename=/mnt/sfs-turbo/test_fio --bs=1M --iodepth=128 --
size=10240M --readwrite=write--fallocate=none
```

**NOTE**

In the preceding command, `/mnt/sfs-turbo/test_fio` indicates the mount path of the target file to be tested. The path must be specific to the file name, that is, the `test_fio` file in the `/mnt/sfs-turbo` directory. Set it based on the site requirements.

● fio result:
3.2 Mounting a File System to a Linux ECS as a Non-root User

Description
By default, a Linux ECS allows only the root user to run the `mount` command for mounting a file system. However, if the root permission is assigned to other common users, such users can also run the `mount` command for file system mounting. The following describes how to mount a file system to a Linux ECS as a common user. The EulerOS is used as an example.

Prerequisites
- A non-root user has been created on the ECS.
- A file system has been created and can be mounted to the ECS by the root user.
- You have obtained the shared path of the file system.

Procedure

**Step 1** Log in to the ECS as user **root**.

**Step 2** Assign the root permission to the non-root user.
1. Run the `chmod 777 /etc/sudoers` command to change the `sudoers` file to be editable.
2. Run the `vi /etc/resolv.conf` command to edit the `sudoers` file.
3. Add a common user under the root account. In the following figure, user **Mike** is added.
4. Press **Esc**, input `.wq`, and press **Enter** to save and exit.

5. Run the `chmod 440 /etc/sudoers` command to change the **sudoers** file to be read-only.

**Step 3** Log in to the ECS as user **Mike**.

**Step 4** Run the following command to mount the file system: For details about the mounting parameters, see **Table 3-2**.

```bash
mount -t nfs -o vers=3,timeo=600,noresvport,nolock Shared path Local path
```

**Table 3-2** Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Path</td>
<td>The format for an SFS file system is <code>File system domain name/Path</code>. For example, <code>example.com:/share-xxx</code>. The format for an SFS Turbo file system is <code>File system IP address/</code>. For example, <code>192.168.0.0/</code>.</td>
</tr>
<tr>
<td>Local path</td>
<td>Local path on the ECS, used to mount the file system. For example, <code>/local_path</code></td>
</tr>
</tbody>
</table>

**Step 5** Run the following command to view the mounted file system.

```bash
mount -l
```

If the command output contains the following information, the file system is mounted successfully.
3.3 Migrating Data to SFS Turbo

3.3.1 Data Migration Using Direct Connect

Context

Users can migrate data from local NAS devices to SFS Turbo using Direct Connect for cloud service expansion.

In this solution, a Linux ECS is created to enable the connection between a local NAS device and SFS Turbo and to migrate data from the NAS device to the cloud.

You can also refer to this solution to migrate data from the NAS in the cloud to SFS Turbo. For details, see Migrating Data from Cloud NAS to SFS Turbo.

Limitations and Constraints

- Only ECSs running Linux can be used for data migration.
- The UID and GID of a file are no longer consistent after synchronization.
- The file access modes are no longer consistent after synchronization.

Prerequisites

- You have enabled and configured Direct Connect. For details, see Direct Connect User Guide.
- You have obtained a Linux ECS.
- You have created an SFS Turbo file system and have obtained the shared path of the file system.
- You have obtained the shared path of the local NAS device.

Procedure

Step 1 Log in to the management console and switch to the ECS console.

Step 2 Log in to the created Linux ECS to access the local NAS device and the SFS Turbo file system.

Step 3 Run the following mount command to access the local NAS storage device:

```
mount -t nfs -o vers=3,timeo=600,nolock Shared path of the local NAS device /mnt/src
```

Step 4 Run the following mount command to access the SFS Turbo file system:

```
mount -t nfs -o vers=3,timeo=600,nolock Shared path of the SFS Turbo file system /mnt/dst
```

Step 5 Run the following command on the Linux ECS to install the rclone tool:

```
wget https://downloads.rclone.org/rclone-current-linux-amd64.zip --no-check-certificateunzip rclone-current-linux-amd64.zip
chmod 0755 ./rclone-*
cp ./rclone-* /usr/bin/
rm -rf ./rclone-*
```
Step 6 Run the following command to synchronize data:
```
rcplane copy /mnt/src /mnt/dst -P --transfers 32 --checkers 64
```

**NOTE**

The parameters are described as follows. Set *transfers* and *checkers* based on the system specifications.
- **transfers**: number of files that can be transferred concurrently
- **checkers**: number of local files that can be scanned concurrently
- **P**: data copy progress

After data synchronization is complete, go to the target SFS Turbo file system to check whether the migration is successful.

----End

**Migrating Data from Cloud NAS to SFS Turbo**

You can migrate data from the NAS in the cloud to SFS Turbo by configuring the cloud NAS and SFS Turbo in the same VPC or by configuring the network using Cloud Connect.

For details about how to configure Cloud Connect, see *Direct Connect User Guide*.

**3.3.2 Data Migration Using the Internet**

**Context**

Users can migrate data from local NAS devices to SFS Turbo using the Internet for cloud service expansion.

In this solution, a Linux server is created in the cloud and on-premises respectively for data migration from the local NAS devices to the cloud. The inbound and outbound directions of port 22 on these two servers are accessible. The on-premises server is used to access the local NAS devices, and the ECS is used to access SFS Turbo.

You can also refer to this solution to migrate data from the NAS in the cloud to SFS Turbo. For details, see *Migrating Data from Cloud NAS to SFS Turbo*.

**Limitations and Constraints**

- Only ECSs running Linux can be used for data migration.
- The UID and GID of a file are no longer consistent after synchronization.
- The file access modes are no longer consistent after synchronization.
- The inbound and outbound directions of port 22 are accessible.

**Prerequisites**

- A Linux server has been created on the cloud and on-premises respectively.
- The elastic IP addresses have been configured for the servers to ensure that the two servers can communicate with each other.
You have created an SFS Turbo file system and have obtained the shared path of the file system.

You have obtained the shared path of the local NAS device.

Procedure

Step 1 Log in to the management console and switch to the ECS console.

Step 2 A Linux server has been created on the cloud and on-premises respectively. For example, the on-premises server client1 and ECS client2.

Step 3 Log in to client1 and run the following command to access the local NAS device:
```
mount -t nfs -o vers=3,timeo=600,noresvport,nolock Shared path of the local NAS device /mnt/src
```

Step 4 Log in to client2 and run the following command to access the SFS Turbo file system:
```
mount -t nfs -o vers=3,timeo=600,noresvport,nolock Shared path of the SFS Turbo file system /mnt/dst
```

Step 5 Run the following command on client1 to install the rclone tool:
```
wget https://downloads.rclone.org/rclone-current-linux-amd64.zip --no-check-certificate
unzip rclone-current-linux-amd64.zip
chmod 0755 ./rclone-*
cp ./rclone-* /usr/bin/
rm -rf ./rclone-*
```

Step 6 Run the following command on client1 to configure the environment:
```
rclone config
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n
name> remote name (New name)
Type of storage to configure.
Enter a string value. Press Enter for the default (".").
Choose a number from below, or type in your own value
Storage> 24 (SSH/SFTP Connection)
24 / SSH/SFTP Connection
  sftp
Storage> 24 (Select the SSH/SFTP number)
SSH host to connect to
Enter a string value. Press Enter for the default (".").
Choose a number from below, or type in your own value
host> ip address (IP address of client2)
SSH username, leave blank for current username, root
Enter a string value. Press Enter for the default (".").
user> user name (Username of client2)
SSH port, leave blank to use default (22)
Enter a string value. Press Enter for the default (".").
port> 22
SSH password, leave blank to use ssh-agent.
y) Yes type in my own password
g) Generate random password
n) No leave this optional password blank
y/g/n> y
Enter the password:
password: (Password for logging in to client2)
Confirm the password:
password: (Confirm the password for logging in to client2)
Path to PEM-encoded private key file, leave blank or set key-use-agent to use ssh-agent.
Enter a string value. Press Enter for the default (".").
key_file> (Press Enter)
The passphrase to decrypt the PEM-encoded private key file.
```
Only PEM encrypted key files (old OpenSSH format) are supported. Encrypted keys in the new OpenSSH format can't be used.

1) Yes type in my own password
2) Generate random password
3) No leave this optional password blank

**y/g/n> n**

When set forces the usage of the ssh-agent.

> When key-file is also set, the ".pub" file of the specified key-file is read and only the associated key is requested from the ssh-agent. This allows to avoid "Too many authentication failures for *username*" errors when the ssh-agent contains many keys.

Enter a boolean value (true or false). Press Enter for the default ("false").

**key_use_agent> (Press Enter)**

Enable the use of the aes128-cbc cipher. This cipher is insecure and may allow plaintext data to be recovered by an attacker.

Enter a boolean value (true or false). Press Enter for the default ("false").

**use_insecure_cipher> (Press Enter)**

Disable the execution of SSH commands to determine if remote file hashing is available.

Leave blank or set to false to enable hashing (recommended), set to true to disable hashing.

Enter a boolean value (true or false). Press Enter for the default ("false").

**disable_hashcheck>**

Edit advanced config? (y/n)

1) Yes

2) No

**y/n> n**

Remote config

-------------

[remote_name]
type = sftp
host=(client2 ip)
user=(client2 user name)
port = 22
pass = *** ENCRYPTED ***
key_file_pass = *** ENCRYPTED ***
-------------

**y) Yes this is OK**
**e) Edit this remote**
**d) Delete this remote**

**y/e/d> y**

Current remotes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote_name</td>
<td>sftp</td>
</tr>
</tbody>
</table>

**e) Edit existing remote**
**n) New remote**
**d) Delete remote**
**r) Rename remote**
**c) Copy remote**
**s) Set configuration password**
**q) Quit config**

**e/n/d/r/c/s/q> q**

**Step 7** Run the following command to view the rclone.conf file in /root/.config/rclone/

**rclone.conf:**

```
cat /root/.config/rclone/rclone.conf
[remote_name]
type = sftp
host=(client2 ip)
user=(client2 user name)
port = 22
pass = ***
key_file_pass = ***
```
**Step 8** Run the following command on **client1** to synchronize data:
```
rcclone copy /mnt/src remote_name:/mnt/dst -P --transfers 32 --checkers 64
```

- Replace `remote_name` in the command with the actual remote name.
- The parameters are described as follows. Set `transfers` and `checkers` based on the system specifications.
  - `transfers`: number of files that can be transferred concurrently
  - `checkers`: number of local files that can be scanned concurrently
  - `P`: data copy progress

After data synchronization is complete, go to the target SFS Turbo file system to check whether the migration is successful.

----End

**Migrating Data from Cloud NAS to SFS Turbo**

To migrate data from the cloud NAS to SFS Turbo using the Internet, perform the preceding steps.
<table>
<thead>
<tr>
<th>Release Date</th>
<th>What's New</th>
</tr>
</thead>
</table>
| 2019-05-30   | This issue is the sixth official release. Updated the following content:  
  ● Added the description of the SFS Turbo file system.  
  ● Added section "SFS Turbo Performance Test."  
  ● Added section "Mounting a File System as a Non-root User."  
  ● Added the description of managing file system's VPCs. |
| 2019-02-15   | This issue is the fifth official release. Updated the following content:  
  ● Added the "Quotas" section.  
  ● Changed the "Troubleshooting" section to "Scalable File Service Troubleshooting" for separate publishing. |
| 2018-11-15   | This issue is the fourth official release. Updated the following content:  
  Split the document into several parts for release. |
| 2018-01-30   | This issue is the third official release. Updated the following content:  
  ● Updated section "Configuring DNS", and changed the IP addresses of the DNS server for resolving domain names of file systems.  
  ● Updated section "Limitations and Constraints", and added the sentence "You can mount file systems to all Elastic Cloud Servers (ECSs) that support the NFSv3 protocol."  
  ● Deleted "Can a File System Be Mounted to a Windows-based ECS" in FAQs.  
  ● Added "Does the Security Group of VPC Affect SFS" in FAQs.  
  ● Added section "How to Purchase SFS." |
<table>
<thead>
<tr>
<th>Release Date</th>
<th>What's New</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-01-11</td>
<td>This issue is the second official release. Updated the following content: ● Updated section &quot;SFS&quot; and section &quot;Deleting a File System.&quot; ● Updated section &quot;Application Scenarios&quot; and section &quot;Limitations and Constraints.&quot;</td>
</tr>
<tr>
<td>2017-12-31</td>
<td>This issue is the first official release.</td>
</tr>
</tbody>
</table>