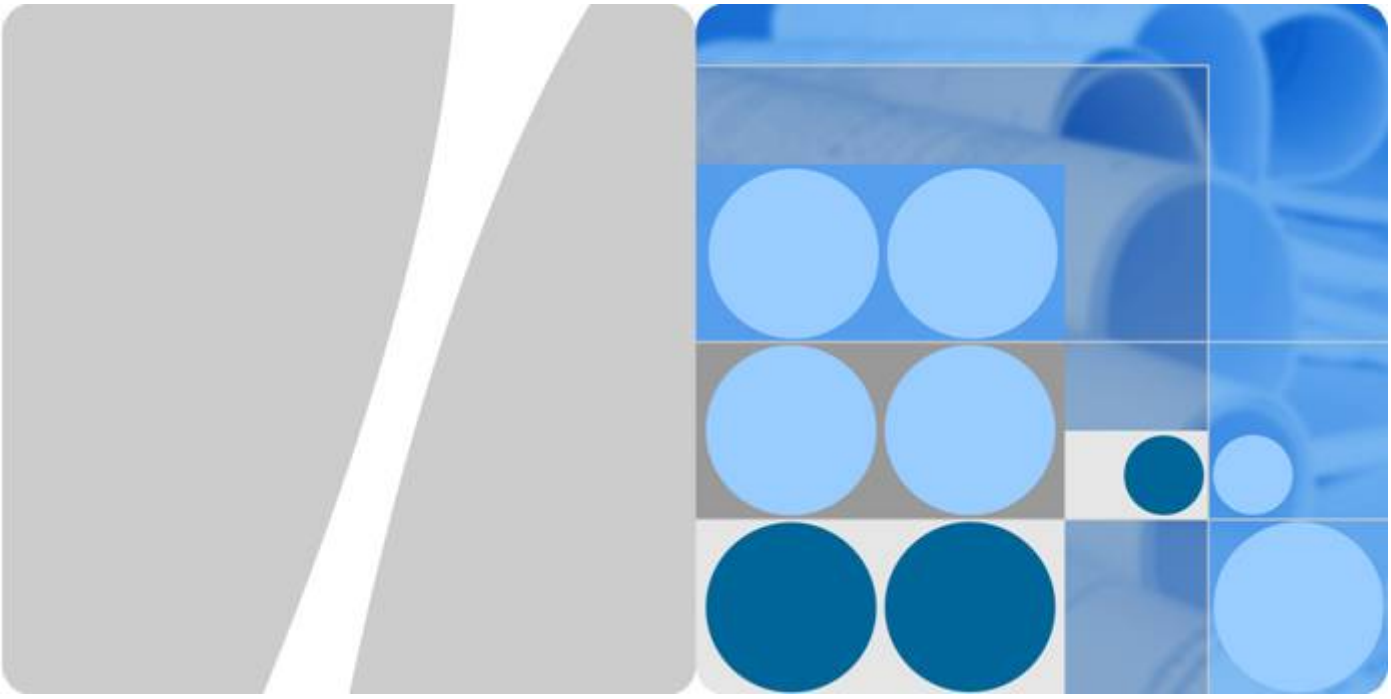


Object Storage Service

Best Practices

Issue 02

Date 2018-11-30

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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.

Contents

1 Overview of OBS Best Practices

This document summarizes operation practices in common application scenarios of Object Storage Service (OBS). Each practice provides detailed solution description and operation guide, helping you easily build your storage services based on OBS.

Table 1-1 OBS best practices

Best Practice	Description
Migrating Local Data to OBS	This section describes how to migrate local data in different sizes from personal computers or on-premises storage servers to OBS.
Using Backup Software to Back Up Local Data to OBS	This section describes the backgrounds of backing up local data to OBS and the backup software supported by OBS. This section uses Commvault as an example to describe how to back up local data to OBS.
Accessing OBS From a Private Network	ECS supports accessing OBS through Internet or the HUAWEI CLOUD private network. To optimize performance and reduce costs, it is recommended that you access OBS through the HUAWEI CLOUD private network. This section describes how to access OBS from ECS over the HUAWEI CLOUD private network.
Using a User-Defined Domain Name to Host a Static Website	This section describes how to use a user-defined domain name to host static websites in OBS. You do not need to set up a website server to quickly publish personal and enterprise static websites.
Enterprise Data Access Control	OBS provides multiple permission control mechanisms to help you manage data stored in OBS. This section uses common data permission control scenarios as examples to describe how to control access to data stored in OBS to ensure data security.

2 Migrating Local Data to OBS

2.1 Overview

Background

Traditional on-premises storage servers cannot meet the demands for massive data storage. The main reasons are as follows:

- The storage capacity is subject to hardware devices. If the storage capacity becomes insufficient, you need to purchase disks and perform manual capacity expansion.
- The initial deployment requires high investment and long construction period, but it quickly lags behind as enterprise services change so fast.
- Network information vulnerabilities, technical vulnerabilities, and misoperations may result in unbearable security risks.

In contrast, OBS provides massive, stable, and secure cloud storage capabilities. With OBS, you do not have to worry about the storage capacity because it can be expanded infinitely. OBS can store unstructured data of any type and size. OBS ensures high stability and security for your data, featuring a multi-level reliability architecture, server-side encryption, log management, and permission control. In terms of the cost, OBS is available upon service subscription, eliminating your investment in physical server deployment and maintenance.

HUAWEI CLOUD provides **migration solutions** to help you migrate data from your on-premises storage servers to OBS in a cost-effective, secure, and efficient manner. You can select a proper migration solution according to your data volume, time arrangement, and budget.

Migration Solutions

Table 2-1 describes the migration solutions provided by HUAWEI CLOUD.

Table 2-1 Migration solutions

Migration Method	Data Volume	Requirement	Time Required	Cost
2.2 Migrating Through OBS Tools	Not larger than 1 TB	Sufficient public network bandwidth; requiring manual operations on clients or scripts to start data upload.	About 10 days for 1 TB data with the bandwidth of 100 Mbit/s	Data transmission is offered for free. Fees are charged only for storage space used in OBS.
2.3 Migrating Through Direct Connect	More than 100 TB data that needs real-time online transmission every month	Private lines need to be deployed.	Depends on the bandwidth of the private line.	Fees are charged based on the distance and bandwidth of the private line. For details, see **Direct Connect Price Details**.

2.2 Migrating Through OBS Tools

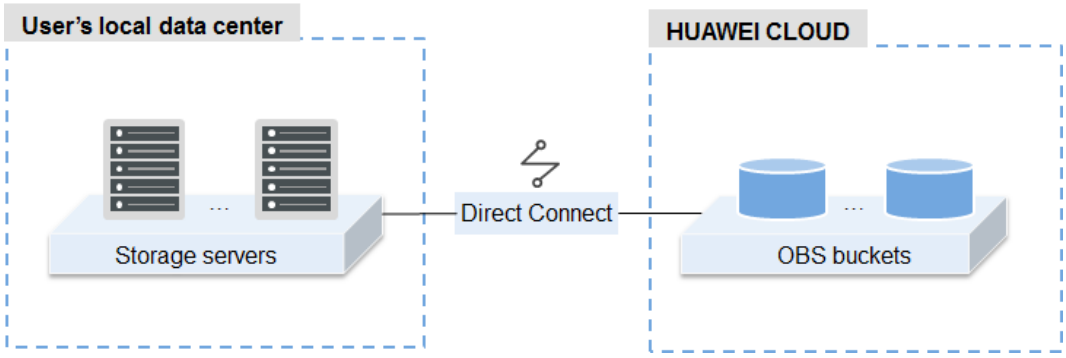
OBS tools are applicable to data migration within the scale of 100 GB. OBS provides various client tools, such as OBS Browser and obsutil, facilitating migration of data from local hosts to OBS. Data upload occupies your public network bandwidth. Therefore, you are advised to upload data during off-peak hours.

For details about the usage scenarios and operation guide of each tool, see **OBS Tools**.

2.3 Migrating Through Direct Connect

Direct Connect connects your data center to HUAWEI CLOUD, so that you can upload local data directly to HUAWEI CLOUD OBS. Direct Connect is recommended when local data needs to be migrated to OBS frequently or in real time. The provided low-latency and high-bandwidth services facilitate uploading data to OBS at any time.

Figure 2-1 Data migration diagram of Direct Connect



1. Creating an OBS bucket

   Log in to OBS Console and create one or more buckets for storing user data.

2. Enabling Direct Connect

   Log in to Direct Connect Console, fill in the application form and submit an order. After the administrator approves the application, you can pay for the order and contact the carrier for physical line connections. Huawei engineers will cooperate with your carrier to configure the connection. For details, see **Creating a Direct Connection**.

3. Starting data transmission

   After Direct Connect is enabled, you can upload local data to OBS using the management console, API, or SDKs.

3 Using Backup Software to Back Up Local Data to OBS

3.1 Overview

In traditional backup and restoration solutions, backup data needs to be written to storage devices such as tapes and then transported to a data center. In this process, data security and integrity are subject to many factors, such as hardware performance and persons. In addition, data center deployment and maintenance pose problems such as complex management and high costs.

Cloud storage is easy-to-use, secure, efficient, and cost-effective, making it an attractive substitute for traditional storage devices such as tapes. OBS is a cloud storage service that provides massive and scalable storage services. All OBS services and storage nodes work in distributed cluster mode to improve OBS scalability. Data redundancy and consistency check functions improve the security and reliability of data stored in OBS. Owing to OBS's pay-per-use billing mode, your cost on OBS is easy to estimate.

Backup software, such as Commvault, CloudBerry Backup, NetBackup, and AnyBackup Cloud, can be connected to OBS for data backup. With such backup software, you can customize backup policies based on your requirements to achieve secure and efficient backup.

3.2 Using Commvault to Back Up Local Data in SAP HANA

SAP HANA is a high-performance real-time data computing platform based on the memory computing technology. Enterprises that need to process a large amount of real-time service data may use SAP HANA. The backup software Commvault is seamlessly integrated with SAP HANA and OBS and supports backup for online databases and logs. When a fault occurs in the SAP HANA system or service migration is required, Commvault can help you quickly and easily restore data, thereby providing enterprise-level data protection for SAP HANA.

Logical Architecture

The following uses Commvault as an example to describe how to back up the SAP HANA deployed on a local single-node system. **Figure 3-1** shows the logical architecture.

Figure 3-1 Logical architecture

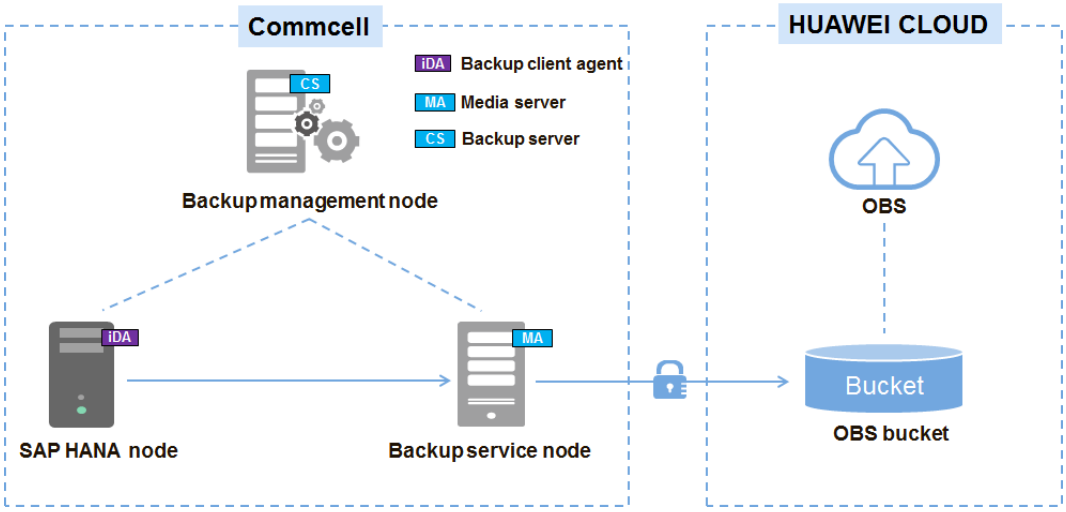


Table 3-1 describes the components in the logical architecture.

Table 3-1 Component description

Component	Description
iDataAgent (iDA)	Backup client agent, which is deployed on the SAP HANA node to obtain data to be backed up from SAP HANA.
CommServe (CS)	Backup server, which is deployed on the backup management node and is responsible for formulating global backup policies and scheduling backup services.
Media Agent (MA)	Backup media, which is deployed on the backup service node and stores backup data to OBS.
OBS	In backup scenarios, OBS stores backup data. Buckets are containers in OBS and data is stored in OBS buckets.

NOTE

A CommCell is a backup management domain and a logical grouping of software components. Such software components obtain, transmit, store, and manage data and information.

Backup Process

1. Installing and preconfiguring the backup software

   When backing up SAP HANA, you need to install and configure the backup server (CommServer), backup media (MediaAgent), and SAP HANA backup client agent (iDataAgent).

2. Creating backup storage space (OBS bucket)

   a. Log in to OBS Console and create a bucket as the backup data storage space. For details about how to create a bucket, see **Creating a Bucket**.

b. Create a cloud repository on CommCell Console. Enter the address, access key, and bucket name of the OBS terminal node to associate the MediaAgent of Commvault with OBS.

NOTE

CommCell Console is a graphical user interface for managing CommCell environments, monitoring and controlling activity jobs, and viewing event-related events.

3. Creating a Commvault backup policy

   Create a backup policy on Commcell Console and specify the backup period, time, and encryption mode.

4. Checking the backup execution status

   During the execution of a backup policy, you can view the backup execution status on Commcell Console.

5. (Optional) Restoring data

   Restore data to the SAP HANA source host.

NOTE

For details about Commvault operations, see **Commvault Official Documentation**.

4 Accessing OBS From a Private Network

4.1 Overview

Scenario Introduction

An enterprise runs basic services on Elastic Cloud Servers (ECSs), but storage capacity of local hard disks becomes insufficient for storing a large number of images and videos. After learning that HUAWEI CLOUD provides massive and elastic cloud storage service, OBS, the enterprise determined to use OBS as a data storage resource pool to reduce the burden on local servers.

From ECS, you can access OBS through the Internet or HUAWEI CLOUD private network. However, for access through the Internet, the network response speed is subject to the network performance, and traffic fees are generated for data reading. To maximize performance and reduce costs, enterprise administrators want to access OBS through the private network.

NOTE

When accessing OBS through the private network, ensure that the OBS resources to be accessed are in the region where the ECS resides. If the OBS resources reside in a different region, access is supported only over the Internet.

Solution

Configure private DNS on the established ECS. The private DNS resolves the OBS domain name so that the ECS can access OBS through the private network. **Figure 4-1** shows the access process.

Figure 4-1 Accessing OBS

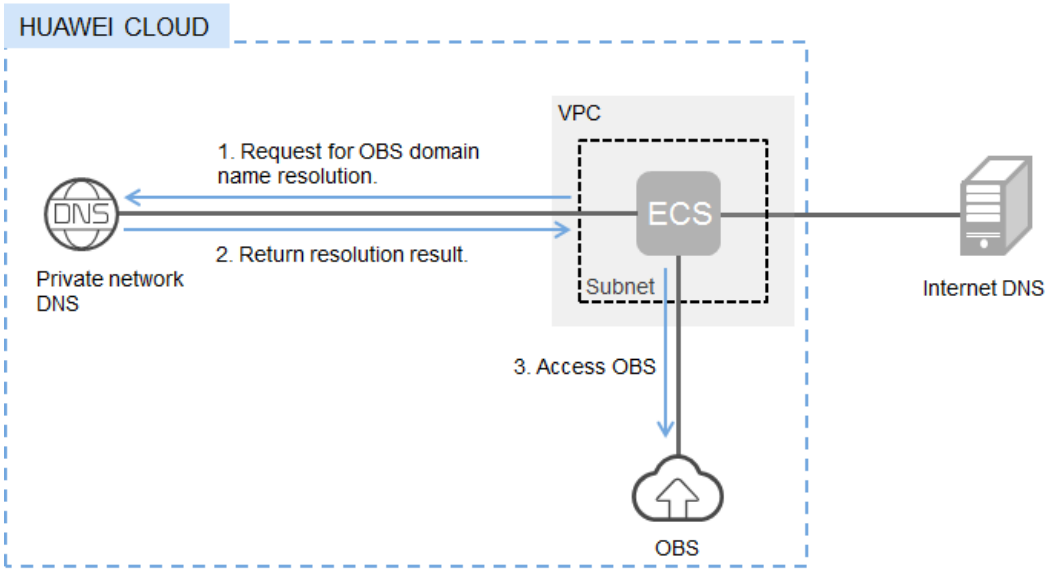


Table 4-1 describes the services in the figure.

Table 4-1 Service description

Service	Description
Virtual Private Cloud (VPC)	VPC enables users to create an isolated virtual network environment defined and managed by themselves, improving security of resources in cloud and simplifying network deployment. A subnet is a network that provides IP address management and DNS services for the ECS in a VPC. The IP addresses of ECSs in a subnet belong to this subnet.
Domain Name Service (DNS)	Internal DNS is provided for resolving internal domain names and OBS domain names. This simplifies the domain name resolution process and reduces the traffic fee for Internet access.

After private network DNS is configured, ECSs can use HUAWEI CLOUD private network to access related cloud services, providing a more stable and reliable network environment for users. You can use either of the following methods to configure private network DNS:

- **Method 1: Changing the VPC Subnet DNS Server Address**

  Private network DNS allows the ECSs in a VPC to use private DNS for resolution, thereby accessing OBS on HUAWEI CLOUD private network. By default, a VPC subnet uses the private network DNS. If this configuration is changed, you need to manually change the subnet DNS address in the VPC.

- **Method 2: Modifying the Local DNS Configuration File**

  To manually modify the local DNS configuration of an ECS, modify the **/etc/resolv.conf** file on a Linux ECS or modify the network configuration on a Windows ECS. When

ECS initiates an OBS access request, local DNS is preferentially used for resolution. If local DNS is not configured, the DNS transparently transmitted by the VPC subnet is used for resolution. If the VPC subnet fails to transparently transmit DNS, you have to modify the local DNS resolution file to enable the OBS access through the private network.

NOTE

The private network DNS configured in method 2 becomes invalid once the ECS is restarted. Therefore, you need to reconfigure the private network DNS after each restart of the ECS.

4.2 Changing the VPC Subnet DNS Server Address

You can perform the following steps to modify the VPC subnet information and add the private network DNS server address to the subnet of an ECS. In this way, when the ECS accesses OBS, the private network DNS server is used for resolution and the OBS is directly accessed within HUAWEI CLOUD intranet.

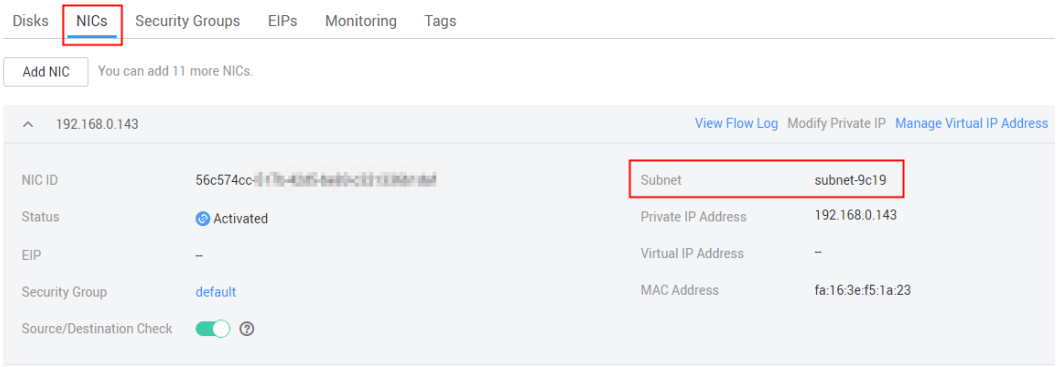
Step 1 Log in to **https://intl.huaweicloud.com/** and click **Console**.

Step 2 Click **Elastic Cloud Server** under **Computing**.

Step 3 Click the target ECS.

Step 4 On the ECS details page, click **NICs** to expand the details and view the subnet name of the ECS. For example, in figure **Figure 4-2**, the subnet name of the ECS is **subnet-9c19**.

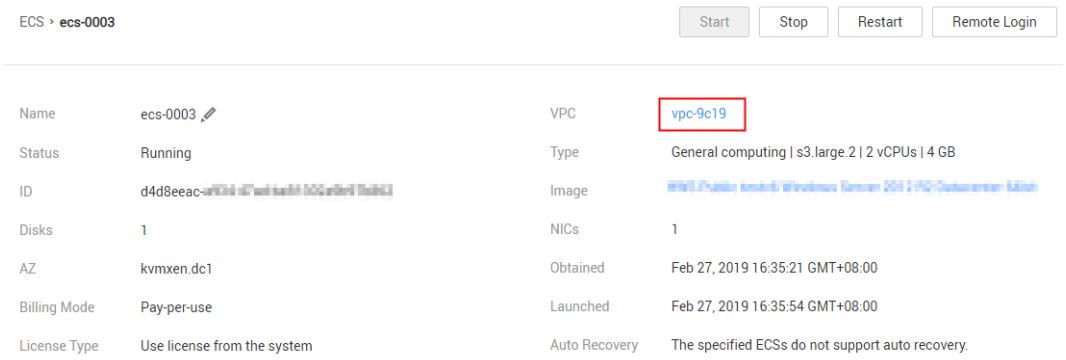
Figure 4-2 NIC details of an ECS



Step 5 On the ECS details page, check the name of the VPC to which the ECS belongs.

For example, in **Figure 4-3**, the name of the VPC is **vpc-9c19**. Click the name of the VPC to go to the **Network Console** page.

Figure 4-3 ECS details



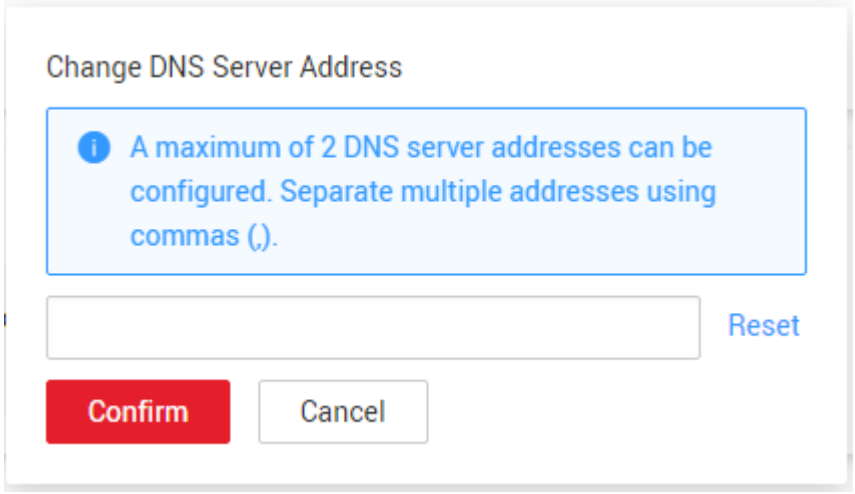
Step 6 Click the VPC name to switch to the **Virtual Private Cloud** page.

Step 7 In the navigation pane on the left, click **Subnet**, and find the subnet in the name of **subnet-9c19**, which is queried in **Step 4**. Click the subnet name. The page with basic information about the subnet is displayed.

Step 8 On the **Gateway and DNS** tab page, click  next to the DNS server address.

Step 9 In the displayed **Change DNS Server Address** dialog box, enter the IP address of the internal DNS server provided by HUAWEI CLOUD and click **Confirm**.

Figure 4-4 Changing DNS server address



NOTE

The IP address of the private DNS server must be configured based on the region where the ECS resides. For details, see **What Are the Private DNS Server Addresses Provided by HUAWEI CLOUD DNS?**.

Step 10 Restart the ECS and then check the local DNS configuration.

- For a Linux ECS, run the **cat** command to check the content of the **/etc/resolv.conf** file and ensure that the address of the private network DNS server is configured before other DNS server addresses.
- For a Windows ECS, open the **Network Properties** dialog box and check that the address of the private network DNS server is the preferred DNS server.

NOTE

- Modifying the subnet information of a VPC subnet will affect all ECSs created using this subnet.
- If the private network DNS of an ECS is not configured successfully, follow instructions in **Modifying the Local DNS Configuration File** to achieve OBS access through HUAWEI CLOUD intranet.

Step 11 After private network DNS is configured, the ECS can access OBS through HUAWEI CLOUD intranet. OBS provides different tools on different operating systems.

- OBS Browser is provided for the Windows OS. For details, see the **Object Storage Service Tools Guide (OBS Browser)**.

  NOTE

  By default, OBS Browser accesses OBS through the Internet. Therefore, when adding an account, select **Other object storage services** for **Service** and enter the endpoint of OBS in this area based on the region where the ECS is located. For details about OBS regions and endpoints, see **Regions and Endpoints**.

- obsutil is provided for the Linux OS. For details about operations, see **Object Storage Service Tools Guide (obsutil)**.

  NOTE

  When configuring the common parameters of obsutil, you need to configure the endpoint of OBS in the region where the ECS is located. For details about OBS regions and endpoints, see **Regions and Endpoints**.

----End

4.3 Modifying the Local DNS Configuration File

Windows and Linux OSs are available for ECS. For different OSs, the configuration methods for accessing OBS through the private network DNS are different. This section describes how to configure internal DNS on two operating systems and how to access OBS after configuration.

Accessing OBS Through the Private Network on a Windows ECS

For different Windows operating systems, the methods of accessing OBS through the private network are slightly different. The following uses an ECS running Windows 7 as an example to describe how to access OBS through the private network.

Step 1 Log in to HUAWEI CLOUD management console. On the home page, choose **Computing** > **Elastic Cloud Server**.

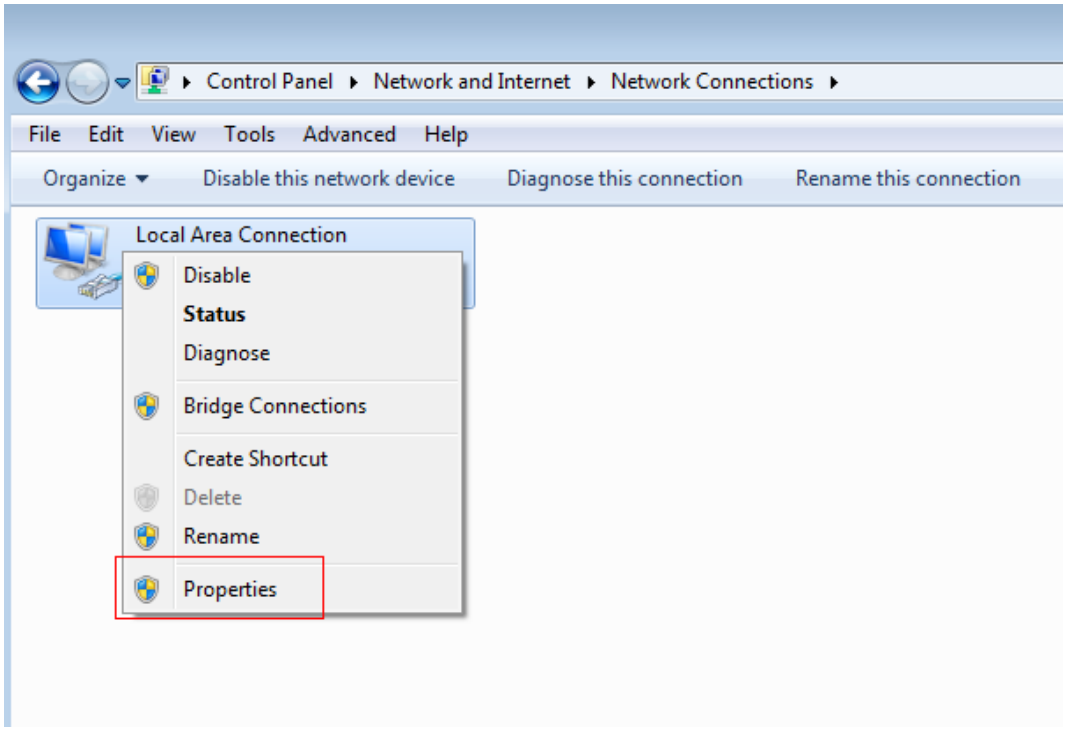
Step 2 Select an ECS and log in to the ECS.

A Windows ECS provides two login modes, VNC remote login and MSTSC. For details, see **Purchasing and Logging In to a Windows ECS**.

Step 3 After logging in to the ECS, open **Network and Sharing Center**.

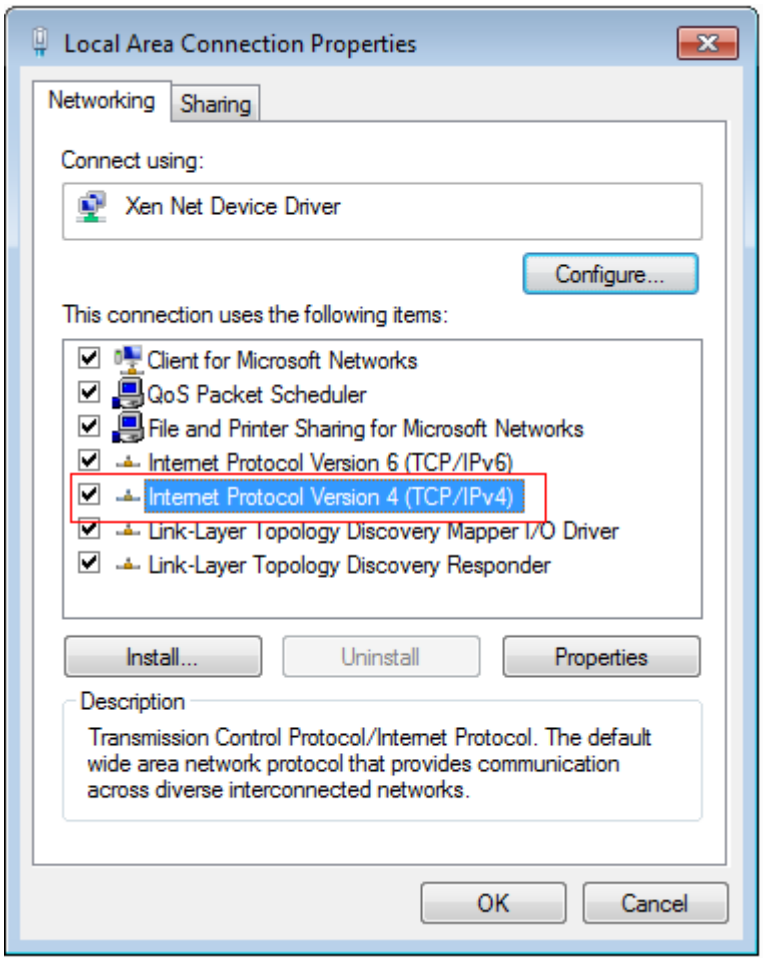
Step 4 Click **Change adapter settings**. On the displayed page, right-click **Local Area Connection** and choose **Properties** from the short cut menu.

Figure 4-5 Configuring local area connection properties



Step 5 On the **Networking** tab page, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

Figure 4-6 Configuring networking properties

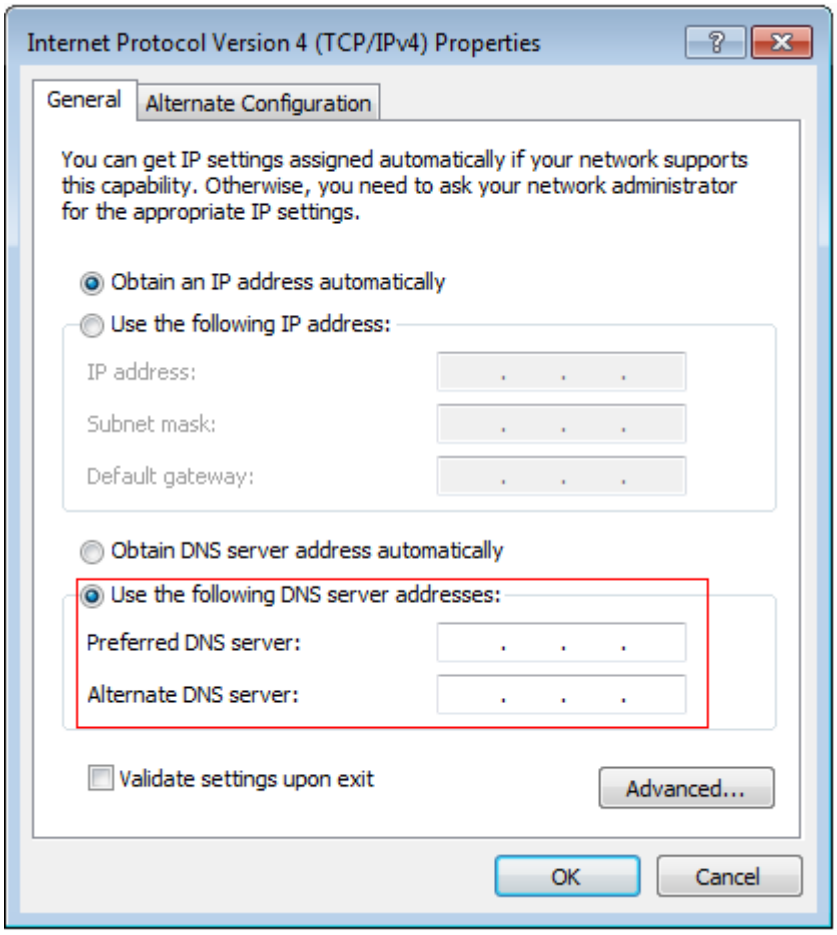


Step 6 On the **General** tab page, select **Use the following DNS server address (E)**. Enter the private DNS server address provided by HUAWEI CLOUD in **Preferred DNS server (P)**, and click **OK**.

NOTE

- The IP address of the private DNS server must be configured based on the region where the ECS resides. For details, see **What Are the Private DNS Server Addresses Provided by HUAWEI CLOUD DNS?**.
- **Alternative DNS server (A)** is the DNS server used when the preferred DNS server is faulty, unavailable, or cannot resolve the requested domain name. Therefore, you can set this parameter to the IP address of a HUAWEI CLOUD private DNS server or the IP address of a public DNS server, or even leave it blank.

Figure 4-7 Configuring DNS server addresses



Step 7 Click **OK**.

NOTE

If you want to switch to the public network access mode, perform **step 1** to **step 5** and change the value of **Preferred DNS server (P)** to the IP address of a public DNS server. See **Figure 4-7**.

Step 8 On the Windows ECS, use OBS Browser to access OBS. For details, see the **Object Storage Service Tools Guide (OBS Browser)**.

NOTE

By default, OBS Browser accesses OBS through the Internet. Therefore, when adding an account, select **Other object storage services** for **Service** and enter the endpoint of OBS in this area based on the region where the ECS is located. For details about OBS regions and endpoints, see **Regions and Endpoints**.

----End

Accessing OBS Through the Private Network on a Linux ECS

The method of accessing OBS through the private network varies for different Linux operating systems. The following uses an ECS running 64-bit CentOS 6.x as an example to describe how to access OBS through the private network.

Step 1 Log in to HUAWEI CLOUD management console. On the home page, choose **Computing** > **Elastic Cloud Server**.

Step 2 Select an ECS and log in to the ECS.

The login mode varies according to the login authentication mode set during ECS purchase. For details about how to log in to the ECS, see **Purchasing and Logging In to a Linux ECS**.

Step 3 After logging in to the ECS, open the command line tool.

Step 4 Run the following command to open the **/etc/resolv.conf** file:

vi /etc/resolv.conf

Step 5 Press **i** to enter the editing mode. In the **/etc/resolv.conf** file, add the internal server address before the original DNS server address in the following format:

```
nameserver DNS server IP address
```

NOTE

- The IP address of the private DNS server must be configured based on the region where the ECS resides. For details, see **What Are the Private DNS Server Addresses Provided by HUAWEI CLOUD DNS?**.
- The IP address of the new DNS must come before all existing DNS IP addresses.
- In Linux, DNS servers are selected in the sequence of nameserver. A new DNS server is selected only when the previous DNS server is faulty, unavailable, or cannot resolve the requested domain name. Therefore, if you want to switch to the public network access mode, you need to add a public DNS server address before the IP address of the private DNS server.

Step 6 Press **ESC** and enter **:wq!** to save the settings and close the file.

NOTE

The configuration takes effect immediately after you save the modification to the **/etc/resolv.conf** file.

Step 7 Use obsutil to access OBS from a Linux ECS. For details about operations, see **Object Storage Service Tools Guide (obsutil)**.

NOTE

When configuring the public parameters of the obsutil, you need to configure the region and the endpoint based on the region where the ECS is located. For details about OBS regions and endpoints, see **Regions and Endpoints**.

----End

5 Using a User-Defined Domain Name to Host a Static Website

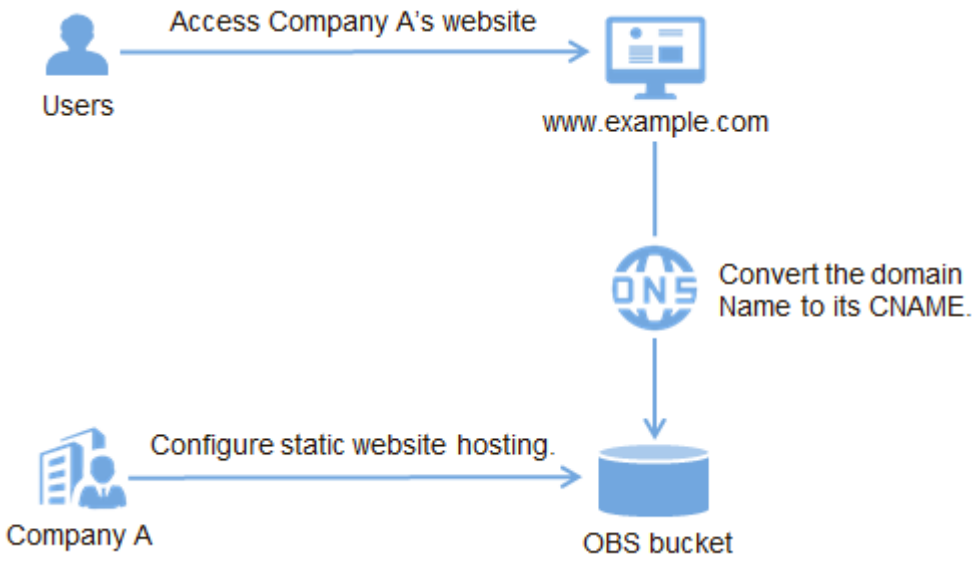
5.1 Overview

OBS allows you to access static websites hosted by OBS using user-defined domain names. This section uses a specific scenario as an example to describe how to use a user-defined domain name to configure static website hosting.

Scenario Introduction

Company A has a large number of files to archive but it does not want to put efforts on storage resources. Therefore, the company subscribes to OBS for hosting static websites and expects that the user names owned by the company can access the static resources through a user-defined domain name. See **Figure 5-1**.

Figure 5-1 Using a user-defined domain name to access hosted static website



Data Planning

Table 5-1 describes the data to be planned before this configuration.

Table 5-1 Data Planning

Item	Description	Example
User-defined domain name	User's own domain name	www.example.com
Bucket name	The bucket name must be consistent with the user-defined domain name.	www.example.com
Static website homepage	Indicates the index page that is returned when you access a static website, that is, the homepage.	index.html
Default 404 Page	When an incorrect static website path is accessed, the 404 error page is returned.	error.html

- The contents of index.html are as follows:

```
<html>
  <head>
      <title>Hello OBS!</title>
      <meta charset="utf-8">
  </head>
  <body>
      <p>Welcome to use OBS static website hosting.</p>
      <p>This is the homepage.</p>
  </body>
</html>
```

- The contents of error.html are as follows:

```
<html>
  <head>
      <title>Hello OBS!</title>
      <meta charset="utf-8">
  </head>
  <body>
      <p>Welcome to use OBS static website hosting.</p>
      <p> This is the 404 error page.</p>
  </body>
</html>
```

5.2 Static Website Hosting

Process of Static Website Hosting

You need to create a bucket named with a user-defined domain name on OBS Console to store static website resources, enable static website hosting for the bucket, and create and configure domain name hosting using the Domain Name Service (DNS). Specific operations are as follows:

1. **Register a domain name.**
2. **Create a bucket.**
3. **Upload static website files.**
4. **Host the static website on OBS.**
5. **Create and configure domain name hosting.**
6. **Verify the configuration.**

Procedure

Step 1 Register a domain name.

If you have a registered domain name, skip this step.

If you do not have a registered domain name, register one with a registrar of your choice. In this scenario, the example domain name **www.example.com** is used. In practice, you need to replace the domain name with the one you actually planned.

Step 2 Create a bucket.

The bucket name must be consistent with the user-defined domain name. Take the **www.example.com** domain name in the data plan as an example. You need to create a bucket named **www.example.com** by performing the following steps:

1. Open **OBS Console** and log in to the console as prompted.
2. Click **Create Bucket** in the upper part of the page.
3. Set the following parameters in the dialog box that is displayed:
   - **Region**: Select a region close to the service according to the proximity principle.
   - **Storage Class**: It is recommended that you select **Standard**.

     NOTE

     You can also select **Low Frequency Access** or **Archive** based on the website access frequency and response speed requirements. For details about storage classes, see **Bucket Storage Classes Overview**.
   - **Bucket Name**: Enter **www.example.com**.
   - **Bucket Policy**: Select **Public Read** to allow any user to access objects in the bucket.
4. Click **Create Now**. The bucket is created.

Step 3 Upload static website files.

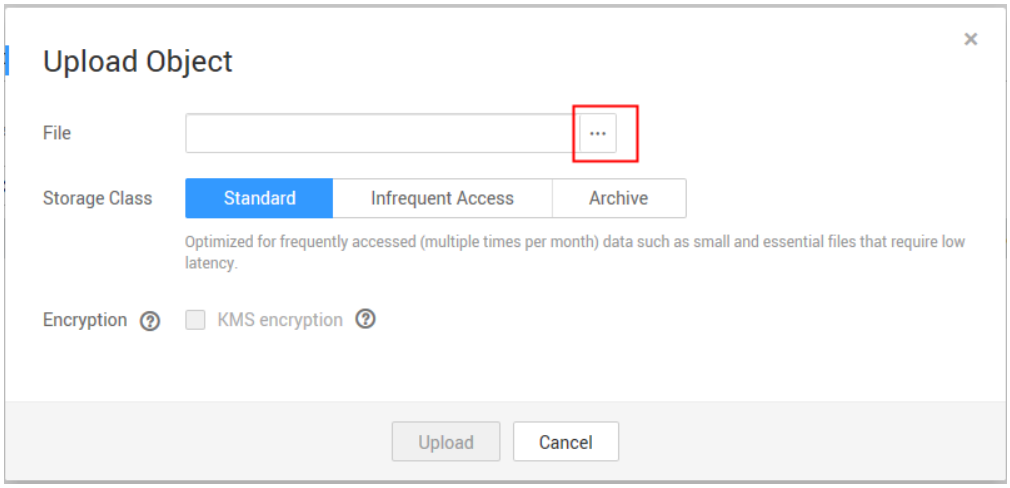
Prepare the static website files to be uploaded and repeat the following steps on OBS Console until all static website files are uploaded to bucket created in **Step 2**.

NOTE

OBS Console does not support uploading folders, uploading a single file larger than 50 MB, or uploading files in batches. If there are a large number of website files, you are advised to use OBS Browser to upload them. For details, see **Uploading a File or Folder**.

1. Click the name of the target bucket to go to the bucket overview page, and then click **Object** in the navigation pane on the left.
2. Click **Upload Object**. A dialog box is displayed. See **Figure 5-2**.

Figure 5-2 Uploading an object



3. Click ... and select the file to be uploaded.

   NOTE

   - The static website files cannot be encrypted for upload.
   - It is recommended that you select **Standard** for the storage class. If the storage class of static website files is **Archive**, you need to restore the files first before accessing it. For details, see **Restoring an Archive File on OBS**.
   - The website homepage file (index.html) and 404 error page (error.html) must be stored in the root directory of the bucket.

4. Click **Upload** to upload the file.

Step 4 Configure static website hosting.

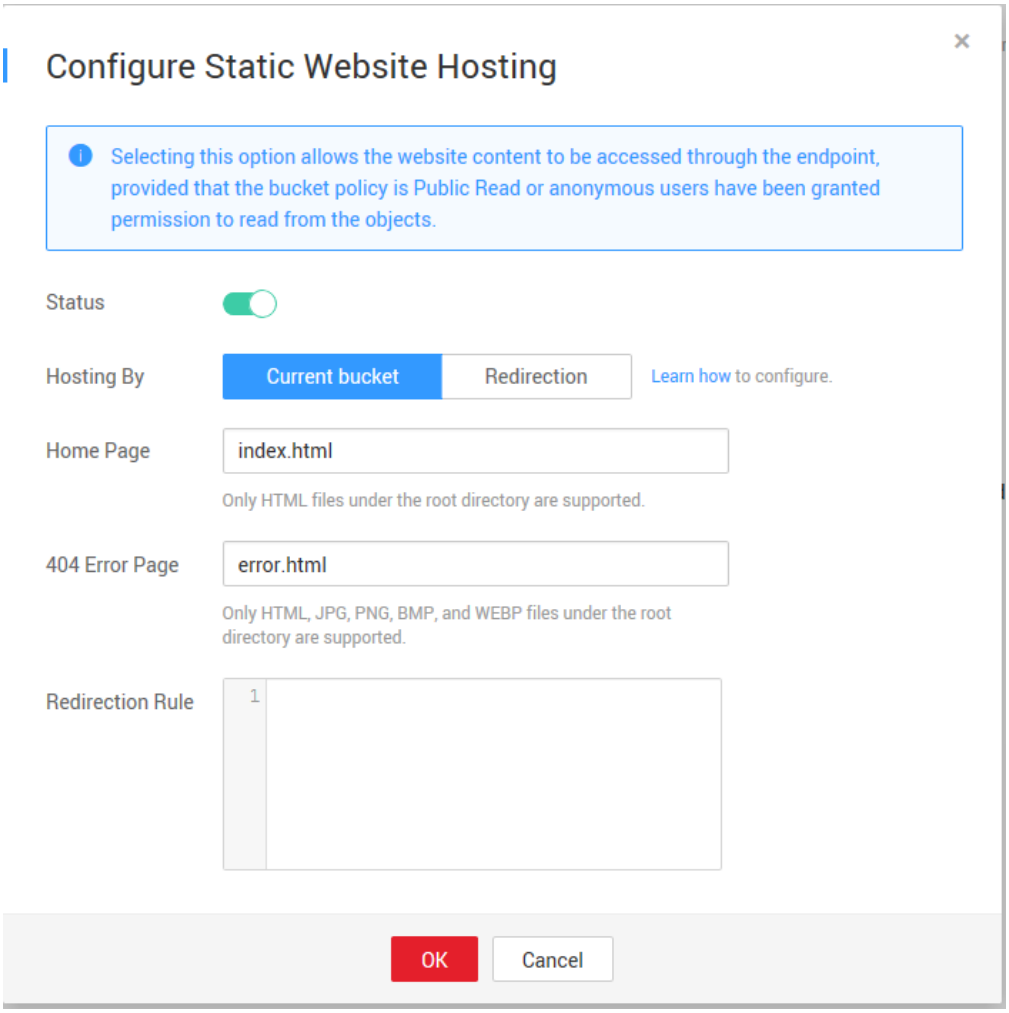
After uploading the static website file, you need to perform the following steps to set the bucket to the static website hosting mode.

NOTE

You can also redirect the entire static website to another bucket or domain name. For details, see **Configuring Redirection**.

1. Click the bucket that you want to configure. On the **Summary** page that is displayed, choose **Basic Configurations** > **Static Website Hosting** on the navigation pane on the left.
2. Click **Configure Static Website Hosting**.
3. In the dialog box that is displayed, select **Use this bucket to host a website**, set **Default Home Page** to index.html in the data plan, and set **Default 404 Error Page** to error.html in the data plan, as shown in **Figure 5-3**.

Figure 5-3 Configuring static website hosting



NOTE

You can also configure redirection rules based on service requirements to implement website content redirection. For details, see **Configuring Static Website Hosting**.

4. Click **OK**.

Step 5 Create and configure domain name hosting.

To facilitate unified management of your user-defined domain names and static websites and implement cloud-based services, you can directly manage your user-defined domain names on DNS. After the hosting is configured, you can perform subsequent management of the domain name on DNS, including managing record sets and PTR records, as well as creating wildcard DNS records.

NOTE

Alternatively, you can add a CNAME record to the DNS at the DNS registrar, mapping to the static website domain name hosted by the bucket. For example: If the region of bucket **www.example.com** is **AP -Hong Kong**, you need to add a CNAME record whose value is **www.example.com CNAME www.example.com.obs-website.ap-southeast-1.myhuaweicloud.com** at your DNS registrar.

To create and configure domain name hosting on DNS, perform the following steps:

1. Add a public zone.

   Use the root domain name **example.com** created in **Step 1** as the name of the public zone to be created. For details, see the description about "Creating a Public Zone" in section "Managing Public Zones" of the *Domain Name Service User Guide*.

2. Add a CNAME record.

   In DNS, add a record set for the sub-domain name **www.example.com** of the hosted domain name, to map the CNAME of the sub-domain name to the static website domain name hosted by OBS. Configure the parameters as follows:

   - **Name**: Enter **www**.
   - **Type**: Select **CNAME-Canonical name**.
   - **Line**: **Default**
   - TTL (s): Retain the default value.
   - **Value**: Domain name mapped to the alias Set this parameter to the static website hosting domain name of the OBS, that is, the access address of the static website.

   For details, see the description about "Adding a Record Set" in section "Managing Record Sets" of the *Domain Name Service User Guide*.

3. Change the DNS server address at your domain name registrar.

   At your domain name registrar, change the DNS server address in the NS record of the root domain name to the cloud DNS server address. The specific address is the NS value of the public zone in DNS.

   For details about how to change the addresses of the DNS servers, see the description about "Updating the NS addresses" in section "Public Zone" of the *Domain Name Service User Guide*.

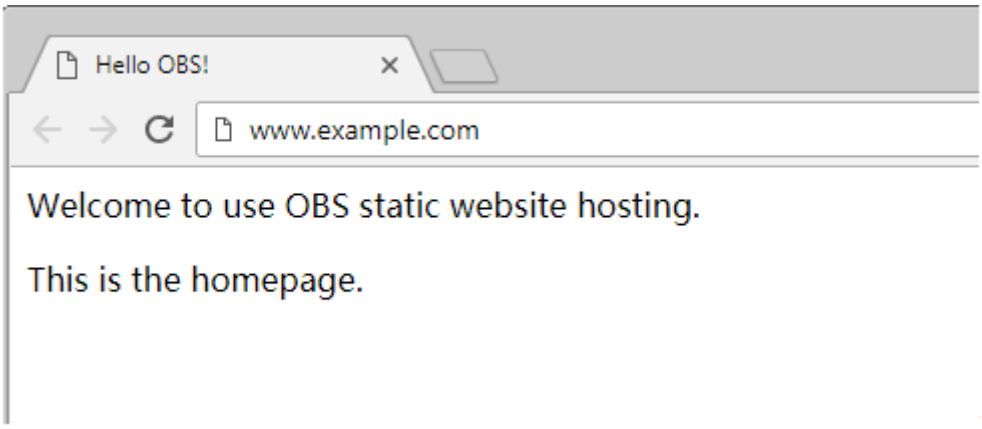
   NOTE

   Generally, the update takes effect within 48 hours, but the time may vary depending on domain name registrars.

Step 6 Verify that the configuration is successful.

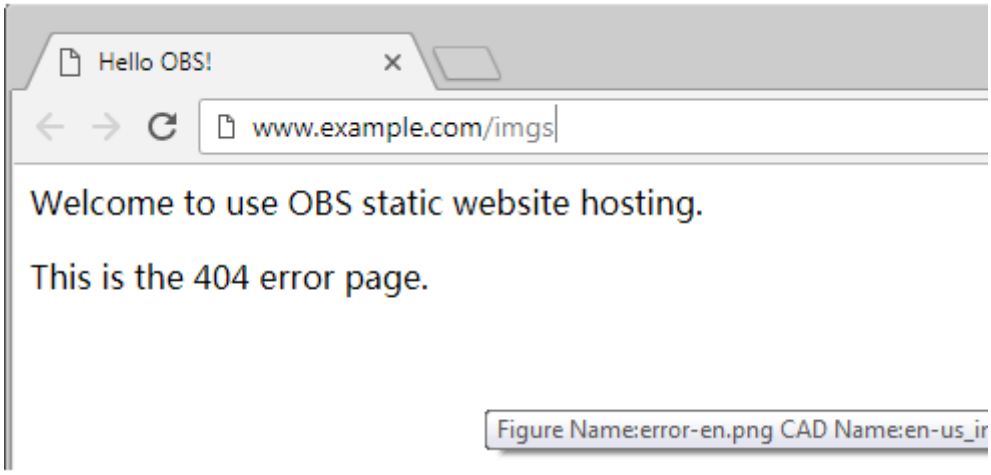
- Enter the **www.example.com** in the address bar of the browser to check whether the default home page can be accessed, as shown in **Figure 5-4**.

  Figure 5-4 Default homepage

- In the web browser, enter a static file access address that does not exist in a bucket. For example: www.example.com/imgs to verify that the 404 error page can be returned, as shown in **Figure 5-5**.

Figure 5-5 Default 404 Page



NOTE

Due to browser cache, you may need to first clear the browser cache to view the expected effect.

----End

5.3 Updating a Static Website

If you need to update a static file (such as a picture, music file, HTML file, or CSS file) on a website, you can upload the static file again. Note that the newly uploaded files in the same path of OBS overwrite the existing files with the same names by default. To avoid file overwriting, you can enable the versioning function of OBS. With versioning enabled, OBS can store multiple versions of a static file. You can quickly search for and restore different versions or restore data in the event of misoperations or application faults.

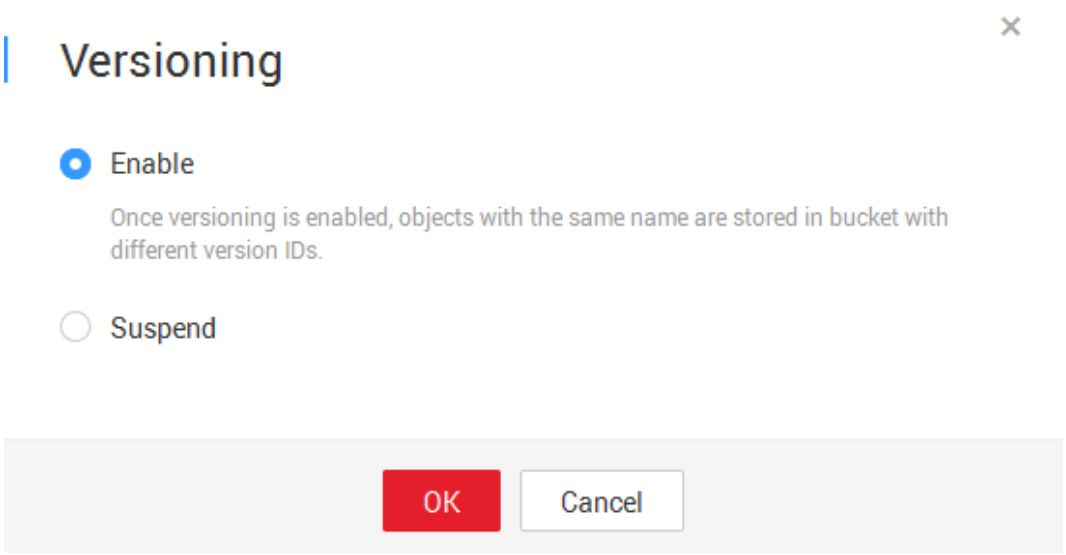
Enabling Versioning

Step 1 Log in to OBS Console.

Step 2 In the bucket list, click the target bucket to go to the **Overview** page.

Step 3 In the **Basic Information** area, locate **Versioning** and click **Edit** to its right.

Figure 5-6 Versioning



Step 4 Select **Enable** and click **OK** to enable versioning for objects in the bucket.

----End

For more information about versioning, see **Versioning**.

Updating Static Files

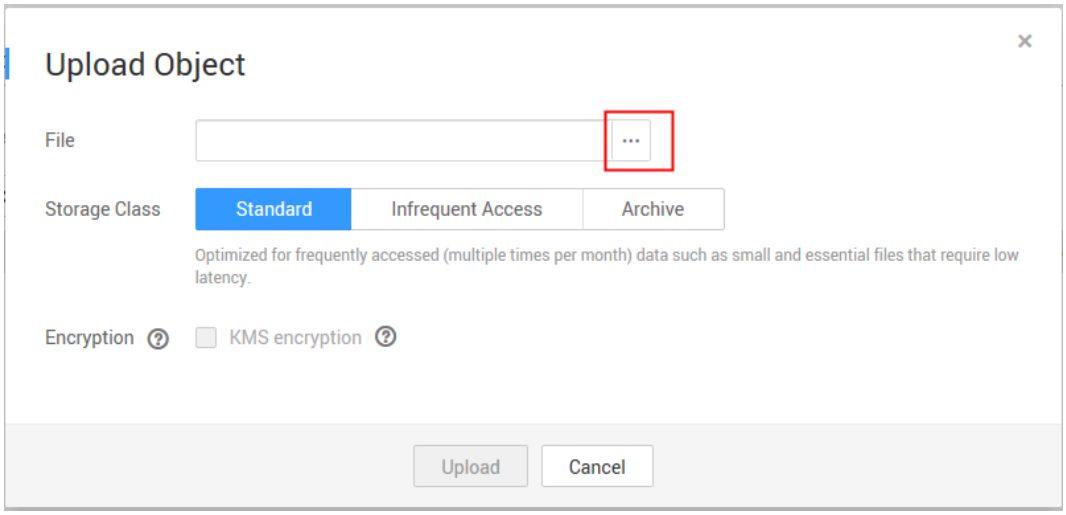
Step 1 Log in to OBS Console.

Step 2 In the bucket list, click the target bucket to go to the **Overview** page.

Step 3 In the navigation tree on the left, click **Object**.

Step 4 Click **Upload Object**, or select the folder where the file to be updated is located and click **Upload Object**. A dialog box is displayed. See **Figure 5-7**.

Figure 5-7 Uploading an object



Step 5 Click and select the file to be uploaded.

NOTE

- The static website files cannot be encrypted for upload.
- It is recommended that you select **Standard** for the storage class. If the storage class of static website files is **Archive**, you need to restore the files first before accessing it. For details, see **Restoring an Archive File on OBS**.

Step 6 Click **OK** to complete the upload.

The newly uploaded file with the same name in the same path is displayed as the latest version in the object list. Each time, only the latest version of the file is accessed. In this way, the static website file can be updated.

----End

6 Enterprise Data Access Control

6.1 Introduction to OBS Access Control

By default, only the resource owner can access OBS resources. Other users do not have the OBS access permission without authorization. OBS offers multiple methods to help you to assign the resource permissions to others. Resource owners can formulate different access control schemes based on service requirements to ensure data security.

OBS Access Control Mechanisms

- **IAM Policy**

  After an IAM user is created, the administrator needs to add the user to a group. IAM can grant the user group required OBS access permissions, and then all users in the group automatically inherit the permissions of the user group.

  For details about OBS permissions controlled by IAM policies, see **User Permissions**.

  IAM policies apply to the following scenarios:

  - Controlling permissions to cloud resources as a whole
  - Controlling permissions to all OBS buckets and objects

- **IAM Agency**

  Delegates other accounts or services to access OBS. A delegated party can manage OBS resources on behalf of the delegating party. This achieves secure and efficient service management.

- **Object ACL**

  Controls access to objects for accounts or user groups. Object owners can configure the object access control list (ACL) to grant basic read and write permissions to specified accounts or user groups.

  By default, an object ACL is created when the object is uploaded. The object owner has full control over the object.

  NOTE

  The owner of an object is the account that uploads the object, who may not be the owner of the bucket to which the object belongs. For example, account **B** is granted the permission to access a bucket of account **A**, and account **B** uploads a file to the bucket. In that case, account **B** is the owner of the object instead of the bucket owner, account **A**.

Object ACLs do not provide fine-grained permission control. Generally, IAM and bucket policies are recommended for permission access control.

- **Bucket ACL**

  Controls access to buckets for accounts or user groups. Bucket owners can configure the bucket ACL to grant basic read and write permissions to specified accounts or user groups.

  By default, a bucket ACL is created upon creation of the bucket. The bucket owner has full control over the object.

  Bucket ACLs do not provide fine-grained permission control. Generally, IAM and bucket policies are recommended for permission access control.

- **Bucket Policy**

  Bucket policies provide centralized access control to OBS resources, and define which operations on which cloud resources are allowed. They are the extension and supplement of ACLs of buckets and objects.

  Bucket policies apply to the following scenarios:

  - If no IAM policy is used for access permission control and you want to authorize other accounts the permission to access your OBS resources, you can use bucket policies to authorize such permissions.
  - If you want to authorize IAM users different access permissions to different buckets, you can configure different bucket policies for buckets.
  - If you want to authorize other accounts the permission to access your buckets, you can use bucket policies to authorize such permissions.

For details about access control modes when grantees and authorized resources are involved, see **Table 6-1**.

Table 6-1 OBS Access Control Modes

Mode	Grantee	Authorized Resource	Granted Operation	Condition Configuration
IAM user group permissions	IAM users	All OBS resources, but not include specified OBS resources or resource sets	All permissions to access OBS	Not supported
IAM agency	• Accounts • Cloud services	All OBS resources, but not include specified OBS resources or resource sets	All permissions to access OBS	Time limitation configuration (permanent or one-day)

Mode	Grantee	Authorized Resource	Granted Operation	Condition Configuration
Object ACL	● Accounts ● Anonymous users ● Registered user groups	Objects	● Obtains the content and metadata of an object. ● Obtains the content and metadata of a specified object. ● Obtains the ACL for an object. ● Obtains the ACL for an object of a specified version. ● Configures object ACL. ● Configures the ACL for an object of a specified version.	Not supported
Bucket ACL	● Accounts ● Anonymous users ● Registered user groups ● Log delivery user groups	Buckets	● Identifies whether a bucket exists. ● Lists objects in a bucket, and obtains the bucket metadata. ● Lists multi-version objects in a bucket. ● Lists multipart upload tasks. ● Performs PUT upload, POST upload, multipart upload, initialization of uploaded parts, and merging of parts. ● Deletes an object. ● Deletes an object of a specified version. ● Obtains the ACL for a bucket. ● Configures the ACL for a bucket.	No
Bucket policy	● Accounts ● IAM users ● Anonymous users	All OBS resources	All operation permissions on OBS. For details, see **Bucket Policy Action**.	Supported

OBS Access Control Principles

- Least privilege

  Only the minimum permissions required for executing tasks are granted to IAM users or accounts. For example, if an IAM user only needs to upload and download objects to a specified directory, you do not need to assign the user the read and write permissions to the bucket.

- Separation of duties

  You are advised to assign different IAM users under an account to manage different OBS resources and permissions. For example, IAM user A is responsible for assigning permissions, and other IAM users managing OBS resources.

- Restricted conditions

  Configure refined conditions for bucket policies to restrict scenarios where a bucket policy takes effect and enhance the security of resources in a bucket. For example, OBS is configured to accept only access requests from a specific IP address.

How Does Authorization Work When Multiple Access Control Mechanisms Co-Exist?

Based on the least-privilege principle, decisions default to DENY, and an explicit DENY always take precedence over an ALLOW. For example, an IAM policy grants access to an object, a bucket policy denies access to that object, and there is no OBS ACL. Then access will be denied.

if no method specifies an ALLOW, then the request will be denied by default. Only if no method specifies a DENY and one or more methods specify an ALLOW, will the request be allowed.

Figure 6-1 Authorization process

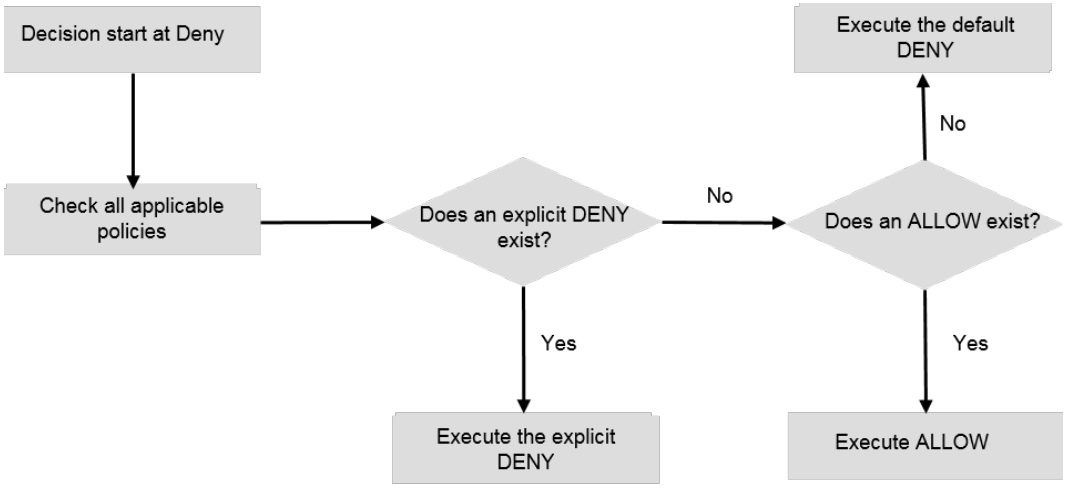


Table 6-2 is a matrix of the IAM policy, bucket policy, and ACL control rules (ALLOW and DENY).

Table 6-2 Matrix of the IAM policy, bucket policy, and ACL control rules (ALLOW and DENY)

Bucket Policy	IAM Policy			ACL
	Deny	Allow	Default Deny	
Deny	Deny			Allow
	Deny			Default Deny
Allow	Deny	Allow		Allow
		Allow		Default Deny
Default Deny	Deny	Allow	Deny	Allow
		Deny		Default Deny

Related Concepts

- Account: An account is automatically created when a user registers with HUAWEI CLOUD. This account has full access permissions for the resources and IAM users under the account.
- Administrator: A user who has the **admin** permission created in IAM and manages IAM users on behalf of the account to ensure security of an account and resources.

  NOTE

  admin is a user group preset on the IAM system and has all operation permissions. An administrator added to the **admin** user group has the same resource management and user management permissions as the account.
- IAM user: A user created by the administrator in IAM. An IAM user uses cloud services and corresponds to an employee, system, or application. IAM users have identity credentials (passwords and access keys) and can log in to the management console or access APIs.

6.2 Access Management on Department Public Data

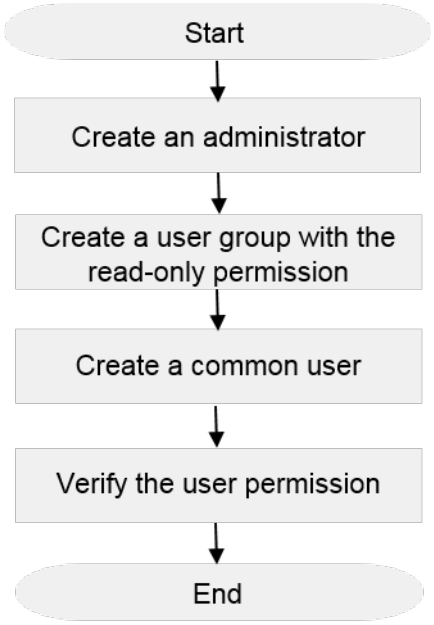
An enterprise has a large number of files to archive but it does not want to put efforts on storage resources. Therefore, this enterprise subscribes to OBS for storing the files, and expects that staff in different departments have different access permissions. By doing so, data access permissions of staff in different departments are isolated.

The enterprise expects that administrators have full permission to department public data stored on OBS, and that common users can only read those data.

Solution and Process

Assign permissions by configuring **IAM user group permissions**. Set the permission of the user group containing common users to **Tenant Guest**, so that common users can access OBS as guests and have only the read permission. **Figure 6-2** shows the process.

Figure 6-2 Flowchart of managing access to department public data



1. **Create an administrator.**

   Create a user on the IAM console and add the user to the **admin** group so that the user has administrator permissions. If an administrator has been created, skip this step.

2. **Create a user group with the read-only permission.**

   Create a user group on the IAM console and grant the **Tenant Guest** permission to the group.

3. **Create a common user.**

   Create a common user on the IAM console and add the user to the group created in **2**.

4. **Verify the user permission.**

   Verify the read-only permission for common users on OBS Console or OBS Browser.

Procedure

Step 1 Create an administrator.

1. On the IAM console, choose **User** in the left navigation tree.
2. On the **User** page, click **Create User**. On the page that is displayed, enter a username and configure the following parameters:
   - Select **Password** for **Credential Type**.
   - Select **admin** from the drop-down list of **User Groups**.
3. Click **Next**. Select **Set manually** for **Password Type**.
4. Enter the email address, mobile number, password, and confirm password.
5. Click **OK**.

Step 2 Create a user group with the read-only permission.

1. On the IAM console, choose **User Group** in the left navigation tree.
2. Click **Create User Group**, and enter a user group name and description.

3. Click **OK**.

   The user group list is displayed, including the newly created user group.

4. Locate the newly created user group, and click **Configure Permission** in the **Operation** column.
5. In the **User Group Permissions** area on the displayed page, select **OBS** and click **Configure Policy**.
6. In the available policy list, select the **Tenant Guest** policy.
7. Click **OK** to save the permission for the user group.

Step 3 Create a common user.

1. On the IAM console, choose **User** in the left navigation tree.
2. On the **User** page, click **Create User**. On the page that is displayed, enter a username and configure the following parameters:
   - Select **Password** for **Credential Type**.
   - Select the user group created in **Step 2** for **User Groups**.
3. Click **Next**. Select **Set manually** for **Password Type**.
4. Enter the email address, mobile number, password, and confirm password.
5. Click **OK**.

Step 4 Verify the user permission.

After the permission is granted, you can verify the permissions of common users using OBS Console, OBS Browser (Windows client tool), and REST APIs. This section takes OBS Console as an example to present how to verify the read-only permission of common users on department public data.

1. Log in to OBS Console as a common user and check whether you have the permission to access the OBS page.
   - If a message indicating that you do not have the permission to access the page is displayed, you cannot read data in the bucket. In this case, check whether the user permission is correctly configured.
   - If a bucket list is displayed, you have the permission to read the bucket list. Go to the next step.
2. Click the name of the target bucket to go to the **Overview** page. You can view objects and lifecycle rules in sequence.
   - If the data cannot be obtained and the message **Access denied** is displayed, you have no permission to read data in the bucket. In this case, check whether the user permission is correctly configured.
   - If the data is displayed, you have the read permission. Go to the next step.
3. On the **Object** page, perform operations including uploading and deleting objects.
   - If an object can be uploaded or deleted, check whether the user permission is correctly configured.
   - If not, the read-only permission for common users is correctly configured.

----End

6.3 Data Sharing Among Departments/Projects

An enterprise has data that needs to be shared among different departments and projects. These data can be downloaded but cannot be modified or deleted by users in other departments, which reduces the risk of mistaken deletion and data tampering.

Prerequisites

Users in other departments must have at least one of the permissions listed in **Table 6-3**. For details about how to view user permissions, see **Viewing and Modifying User Group Information**.

Table 6-3 OBS user permissions

Permission	Description
Tenant Administrator	Users with this permission can perform any operation on OBS resources.
Tenant Guest	Users with this permission can query the usage of OBS resources. Specifically, a user with this permission can only read OBS resources.
OBS Buckets Viewer	Users with this permission can obtain lists of buckets and objects, and query metadata and location information of buckets.

Procedure

Configure a bucket policy for buckets that store shared data to prevent users in other departments from writing or deleting data.

Step 1 On the homepage of HUAWEI CLOUD console, choose **All Services** > **Storage** > **Object Storage Service**.

Step 2 In the OBS bucket list, click the name of the target bucket.

Step 3 In the left navigation tree, choose **Permissions**. On the page that is displayed, click the **Bucket Policy** tab.

Step 4 Click **Create Bucket Policy** under **Custom Bucket Policy**.

Step 5 Create a customized bucket policy based on the following parameter settings. See **Figure 6-3**.

- Select **Customized** for **Policy Mode**.
- Select **Deny** for **Effect**.
- Select **Include** > **Current account** for **Principal**, and click the drop-down list box to select an authorized user.
- In the text bar next to **Resource**, enter the wildcard * which indicates all objects in the current bucket.

NOTE

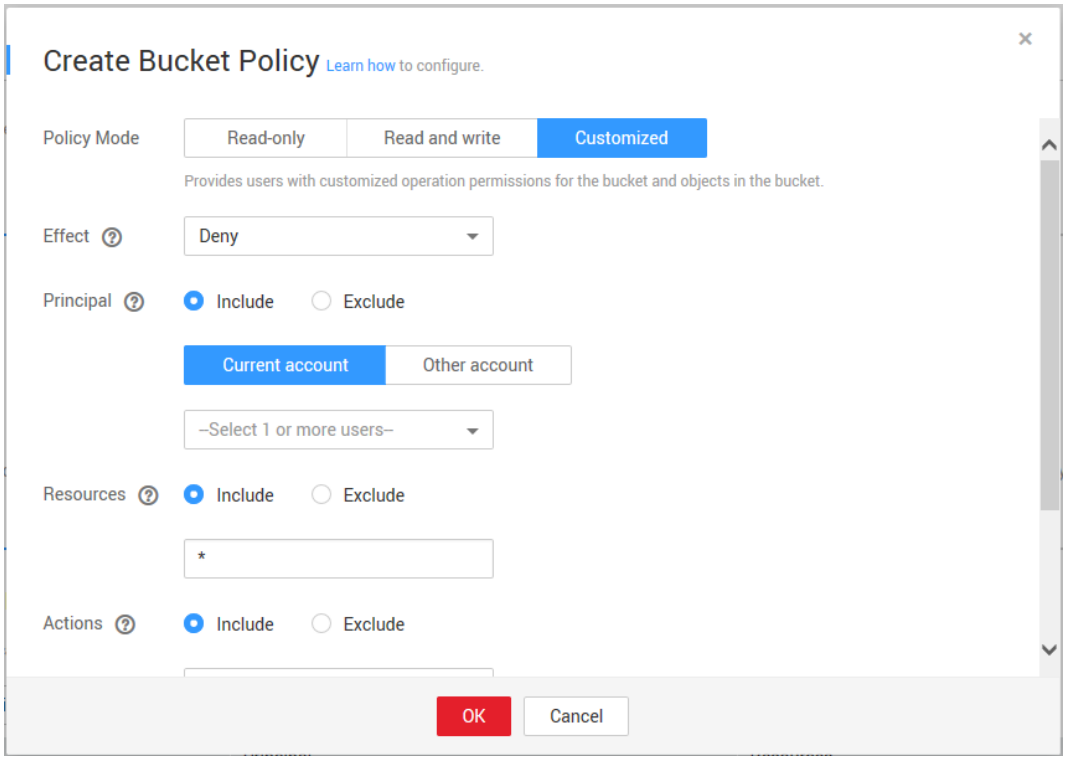
If the written and deletion prohibition is required only on some data, for example, a folder or a type of objects, fill in the text bar by referring to the following examples:

- example/
- example*

You can also enter multiple resources. Use commas (,) to separate multiple resources.

- Select **Include** for **Action**, and select **PutObject**, **GetObjectAcl**, **GetObjectVersionAcl**, **PutObjectAcl**, **PutObjectVersionAcl**, **DeleteObject**, **DeleteObjectVersion**, **ListMultipartUploadParts**, and **AbortMultipartUpload** from the drop-down list.

Figure 6-3 Creating a custom bucket policy



Step 6 Click **OK**.

Step 7 Verify the permission.

After the permission is granted, you can verify the permissions of users in other departments using OBS Console, OBS Browser (Windows client tool), and REST APIs. This section takes OBS Console as an example to present how to verify that users in other departments can only read the data shared among departments and projects.

1. Log in to OBS console as a common user.
2. In the OBS bucket list, click the name of the target bucket.
3. In the left navigation tree, click **Objects**. The object list is displayed.
4. Click **Download** in the row where a common data record is located, or click **More** > **Download As**.
   - If the download fails, check the user permission configuration by referring to **Prerequisites**.

- If the download is successful, go to the next step.

5. Click **Upload File**, select a file, and click **OK**.
   - If the upload is successful, check whether the bucket policy is correctly configured.
   - If the upload fails, go to the next step.
6. Click **Delete** in the row where a public data record is located.
   - If the deletion is successful, check whether the bucket policy is correctly configured.
   - If the deletion fails, the permission is granted successfully.

----End

6.4 Data Isolation from Enterprise Partners

An enterprise expects to isolate internal data from partner data. That is, partners can view only authorized buckets.

Prerequisites

A partner user has been created by an enterprise account. The user is not added to any user group or is added to a user group without the OBS permission. For details, see **Creating Users**.

Procedure

Configure a bucket policy for buckets that store partner data to allow partner users to access the buckets.

Step 1 On the homepage of HUAWEI CLOUD console, choose **All Services** > **Storage** > **Object Storage Service**.

Step 2 In the OBS bucket list, click the name of the target bucket.

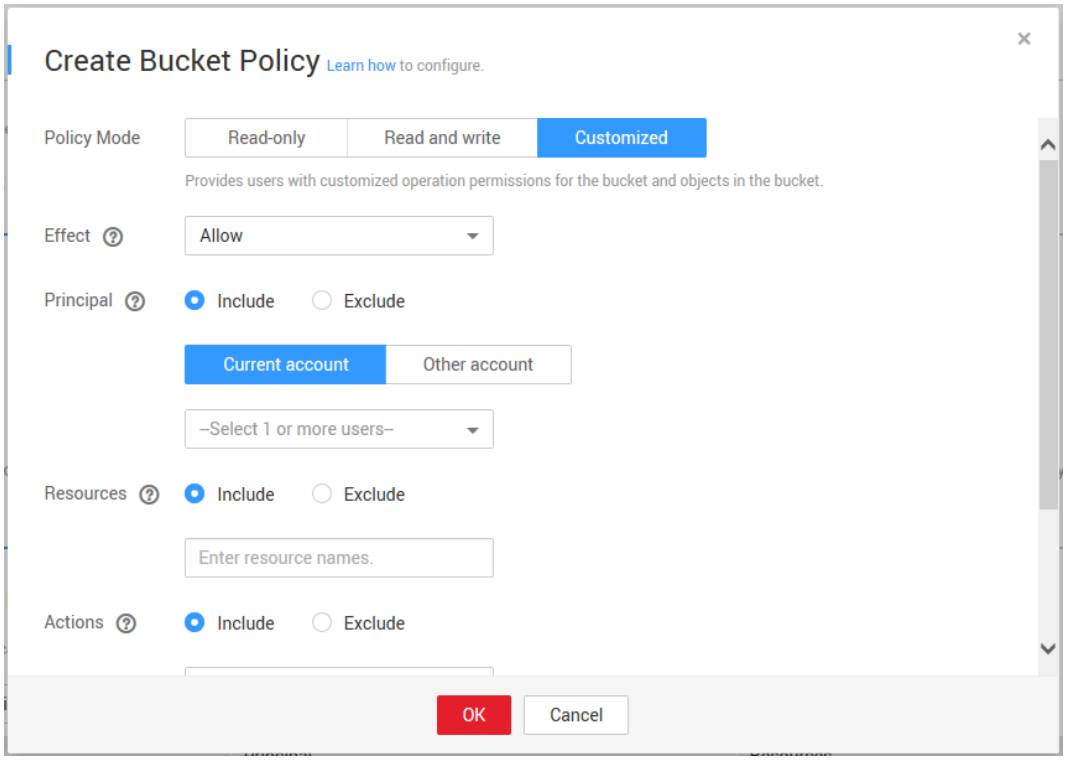
Step 3 In the left navigation tree, choose **Permissions**. On the page that is displayed, click the **Bucket Policy** tab.

Step 4 Click **Create Bucket Policy** under **Custom Bucket Policy**.

Step 5 Create a customized bucket policy based on the following parameter settings. See **Figure 6-4**.

- Select **Customized** for **Policy Mode**.
- Select **Allow** for **Effect**.
- Select **Include** > **Current account** for **Principal**, and click the drop-down list box to select the partner user.
- Select **Include** for **Resource** and leave the text bar blank, which indicates that this bucket policy applies to the entire bucket.
- In the text bar next to **Action**, select ***** below **General** from the drop-down list.

Figure 6-4 Creating a custom bucket policy



Step 6 Click **OK**.

Step 7 Verify the permission.

After the permission is granted, partner users can use OBS Browser (Windows client tool) to add external buckets for permission verification.

1. Log in to OBS Browser as a partner user.
2. Click **Add Bucket**. In the **Add Bucket** dialog box, select **Add External Bucket** and enter the name of an authorized bucket.
3. Click **OK**.

   If the bucket is successfully mounted and can be accessed, the permission is granted successfully.

----End

A Change History

Release Date	What's New
2018-11-30	This issue is the second official release. This issue incorporates the following change: ● Added the section "Overview of OBS Best Practices."
2018-09-30	This issue is the first official release.

