Object Storage Service

Best Practices

Issue 04
Date 2019-07-06

HUAWEI TECHNOLOGIES CO., LTD.
Copyright © Huawei Technologies Co., Ltd. 2019. All rights reserved.
No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

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................................................................. 1

2 Migrating Local Data to OBS................................................................. 3
  2.1 Overview........................................................................................................ 3
  2.2 Migrating Through OBS Tools................................................................. 4
  2.3 Migrating Through the CDM Service......................................................... 4
  2.4 Migrating Through Disk-Based DES......................................................... 5
  2.5 Migrating Through Teleport-Based DES..................................................... 6
  2.6 Migrating Through Direct Connect............................................................ 7

3 Using Backup Software to Back Up Local Data to OBS........................... 8
  3.1 Overview........................................................................................................ 8
  3.2 Using Commvault to Back Up Local Data in SAP HANA............................. 8

4 Accessing OBS over Intranet................................................................. 11
  4.1 Overview........................................................................................................ 11
  4.2 Accessing OBS over Intranet by Using OBS Browser on a Windows ECS... 13
  4.3 Accessing OBS over Intranet by Using obsutil on a Linux ECS.................... 16

5 Using CDN to Accelerate Access to OBS................................................ 19
  5.1 Overview........................................................................................................ 19
  5.2 Using CDN to Accelerate OBS File Download............................................ 22

6 Using a User-Defined Domain Name to Host a Static Website................... 25
  6.1 Overview........................................................................................................ 25
  6.2 Static Website Hosting................................................................................... 26
  6.3 Updating a Static Website............................................................................. 32

7 Enterprise Data Access Control............................................................... 35
  7.1 Introduction to OBS Access Control............................................................ 35
  7.2 Access Management on Department Public Data........................................ 41
  7.3 Data Sharing Among Departments/Projects............................................... 43
  7.4 Data Isolation from Enterprise Partners..................................................... 49

8 Performance Optimization........................................................................ 51

A Change History......................................................................................... 52
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

<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migrating Local Data to OBS</td>
<td>Describes how to migrate local data from personal computers or on-premises storage servers to OBS.</td>
</tr>
<tr>
<td>Using Backup Software to Back Up Local Data to OBS</td>
<td>Describes the backgrounds of backing up local data to OBS and the backup software supported by OBS. Commvault is used as an example to describe how to back up local data to OBS.</td>
</tr>
<tr>
<td>Accessing OBS over Intranet</td>
<td>Describes how to access OBS from your Elastic Cloud Servers (ECSs) through the HUAWEI CLOUD intranet. To optimize performance and reduce costs, it is recommended that you access OBS over the HUAWEI CLOUD intranet. ECS supports access to OBS through either Internet or the HUAWEI CLOUD intranet.</td>
</tr>
<tr>
<td>Using CDN to Accelerate Access to OBS</td>
<td>Describes how to use the acceleration function of Content Delivery Network (CDN) to quickly obtain data from OBS, with optimal user experience and reduced costs on traffic.</td>
</tr>
<tr>
<td>Using a User-Defined Domain Name to Host a Static Website</td>
<td>Describes how to use a user-defined domain name to host static websites on OBS. You can quickly publish personal and enterprise static websites without setting up a website server.</td>
</tr>
<tr>
<td>Enterprise Data Access Control</td>
<td>OBS provides multiple permission control mechanisms to help you manage data stored on OBS. This section uses common scenarios of data permission control as examples to describe how to control access to data stored on OBS to ensure data security.</td>
</tr>
<tr>
<td>Best Practice</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>8 Performance Optimization</td>
<td>This section describes how to add random prefixes to object names to implement horizontal expansion for access requests, and thus improve the access rate and shorten the access delay.</td>
</tr>
</tbody>
</table>
2 Migrating Local Data to OBS

2.1 Overview

Background

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

- Storage capacity is subject to hardware devices. If the storage capacity becomes insufficient, you need to purchase disks and expand the capacity manually.
- 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 mis-operations may result in unbearable security risks.

In contrast, OBS provides massive, stable, and secure cloud storage capabilities. With OBS, you do not need 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 the need for the 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 suitable 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

<table>
<thead>
<tr>
<th>Migration Method</th>
<th>Data Volume</th>
<th>Requirement</th>
<th>Time Required</th>
<th>Pricing</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2 Migrating Through OBS Tools</td>
<td>Not larger than 1 TB</td>
<td>Sufficient public network bandwidth; requiring manual operations on clients or scripts to start data upload.</td>
<td>About 10 days for 1 TB data with the bandwidth of 100 Mbit/s</td>
<td>Data transmission is offered for free. Fees are charged only for storage space used on OBS.</td>
</tr>
<tr>
<td>2.6 Migrating Through Direct Connect</td>
<td>More than 100 TB data that needs real-time online transmission every month</td>
<td>Private lines need to be deployed.</td>
<td>Depends on the bandwidth of the private line.</td>
<td>Fees are charged based on the distance and bandwidth of the private line. For details, see Direct Connect Pricing Details.</td>
</tr>
</tbody>
</table>

#### 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. Uploading data 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 Guide.

#### 2.3 Migrating Through the CDM Service

**Overview**

Cloud Data Migration (CDM) provides batch data migration services between homogeneous and heterogeneous data sources. By creating scheduled jobs, CDM connects data sources, such as file systems, databases, and object storage on the on-premises storage servers, to HUAWEI CLOUD OBS. In this way, local data can be migrated to OBS periodically and automatically.
Figure 2-1 CDM workflow

1. Creating an OBS bucket
   Create a bucket on OBS Console or OBS Browser to store original user data.

2. Purchasing CDM
   Purchase the CDM service, that is, create a CDM cluster to manage connections and jobs.

3. Configuring connections and jobs
   Create a source connection and a destination connection in the created CDM cluster to respectively connect to the local data source and OBS in the cloud. Then create a CDM job to migrate local data to OBS.

4. Starting data transmission
   Run the CDM job to start data transmission. You can view the job progress on the job management page.

Example: Periodically Backing Up Files from an FTP Server to OBS

CDM can periodically upload new files to OBS. You do not need to compile code or manually upload the files. You can also use the massive storage capabilities of OBS on HUAWEI CLOUD to back up files. For details about how to periodically back up files from an FTP server to OBS, see From FTP/SFTP to OBS.

2.4 Migrating Through Disk-Based DES

Disk-based Data Express Service (DES) allows users to deliver data disks (such as USB flash drives and eSATA disks) to a data center of HUAWEI CLOUD, achieving efficient data transmission. Disk-based DES is suitable for TB-scale data migration.
2.5 Migrating Through Teleport-Based DES

Teleport is a storage device specially designed for TB- or PB-scale data migration to OBS. It is dust- and water-proof and resistant to vibration and crush. With multiple security protection mechanisms, such as GPS locking, data encryption, and offline transfer, Teleport can ensure the security of data during delivery.

Figure 2-3 Data migration diagram of Teleport-based DES

1. Creating an OBS bucket
   Create a bucket on OBS Console or OBS Browser to store original user data.

2. Creating a Teleport-based DES order
   Log in to DES Console and create a Teleport-based DES order. Import the provided signature file to a local data disk and send the disk to a HUAWEI CLOUD data center.

3. Starting data transmission
   After receiving the disk, a HUAWEI CLOUD data center administrator mounts the disk to a physical server. Then you will receive an SMS message to notify you of inputting the access keys (AK and SK) to start data uploading. After data transmission is complete, you can view the transmission result on DES Console or OBS Console. The HUAWEI CLOUD data center will send your disk back afterwards.

For details, see Detailed Instructions on Using Disks.
DES provides Teleport-based and disk-based services. Select Teleport-based DES in this scenario.

3. Receiving and importing data to the Teleport
   After the DES order is created successfully, you will receive the Teleport sent by a HUAWEI CLOUD data center. Perform simple configuration to connect the Teleport to your data server, copy the data, and send the Teleport to the HUAWEI CLOUD data center.

4. Starting data transmission
   After the HUAWEI CLOUD data center receives the Teleport, you can input the access keys on DES Console to transmit data from the Teleport to a specified OBS bucket. After data transmission is complete, you can view the transmission result on DES Console or OBS Console.

For details, see [Detailed Instructions on Using Teleport](#).

### 2.6 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.

![Data migration diagram of Direct Connect](image)

**Figure 2-4** 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, APIs, 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 on OBS. Owing to OBS's pay-per-use billing mode, your cost on OBS is easy to estimate.

Backup software, such as Commvault 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.

**NOTE**

Commvault V11 is recommended in this scenario.
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

![Logical Architecture Diagram](image)

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

**Table 3-1** Component description

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

**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 pre-configuring 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 OBS endpoint address, access keys, and the bucket name 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 activity-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 over Intranet

4.1 Overview

Scenario Introduction

An enterprise runs basic services on Elastic Cloud Servers (ECSs), but storage capacity of 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 intranet. 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 intranet.

**NOTE**

When accessing OBS through the intranet, 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 intranet DNS on the established ECS. The intranet DNS resolves the OBS domain name so that the ECS can access OBS through the intranet. **Figure 4-1** shows the access process.
Table 4-1 describes the services in the figure.

**Table 4-1 Service description**

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Private Cloud (VPC)</td>
<td>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.</td>
</tr>
<tr>
<td>Domain Name Service (DNS)</td>
<td>Intranet DNS is provided for resolving intranet domain names and OBS domain names. This simplifies the domain name resolution process and reduces the traffic fee for Internet access.</td>
</tr>
</tbody>
</table>

- For Windows ECSs, you are advised to use OBS Browser to access OBS over intranet. For details, see: [Accessing OBS over Intranet by Using OBS Browser on a Windows ECS](#).
- For Windows ECSs, you are advised to use obsutil to access OBS over intranet. For details, see: [Accessing OBS over Intranet by Using obsutil on a Linux ECS](#).

When accessing OBS through the intranet from your ECS, you can read, back up, and archive data without affecting the public network bandwidth.
4.2 Accessing OBS over Intranet by Using OBS Browser on a Windows ECS

OBS Browser is a graphical interface tool applicable to Windows operating systems. You can configure the intranet DNS server address to access OBS over intranet on a HUAWEI CLOUD Windows ECS. The process and procedure are described as follows.

Process

Figure 4-2 The process of accessing OBS over intranet by using OBS Browser on a Windows ECS
Procedure

Step 1  Log In to the Windows ECS.
1. Log in to HUAWEI CLOUD and click Console.
3. 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 2  Check whether the intranet DNS is configured on the Windows ECS.

On the Windows ECS, you can view the current DNS configuration by using the graphical user interface (GUI) or command line interface (CLI). This section uses the CLI as an example to describe how to view the DNS configuration.

1. After logging in to the ECS, open the CLI.
2. Run the `ipconfig /all` command to check whether DNS server is at the intranet DNS address of the region where the current ECS resides.

**NOTE**

HUAWEI CLOUD provides different intranet DNS server addresses for different regions. For details, see What Are the Private DNS Server Addresses Provided by the DNS Service?

- If no, go to Step 3.
- If yes, go to Step 4.

Step 3  Configure the Intranet DNS.

Change the DNS server address of the ECS to the intranet DNS provided by HUAWEI CLOUD. You can change the DNS address of the VPC subnet or modify the local DNS configuration to achieve this.

- **Methods 1: Changing the DNS server address of the VPC subnet**

  Locate the VPC where the ECS resides and change the DNS server address of the VPC subnet the intranet DNS address. In this manner, ECSs in the VPC can use the intranet DNS for resolution and thereby you can access OBS on HUAWEI CLOUD intranet. For details, see Modifying a Subnet.

  **NOTE**

  The intranet DNS server address must be selected based on the region where the ECS resides. For details, see What Are the Private DNS Server Addresses Provided by the DNS Service?

- **Method 2: Modifying the local DNS configuration**

  The intranet DNS configured in this method becomes invalid once the ECS is restarted. Therefore, you need to reconfigure the intranet DNS after each restart of the ECS. This section uses configuration through CLI as an example to describe how to modify the DNS configuration locally.

  1. Open the CLI.
  2. Run the following command to configure the IP address of the primary DNS server:

     ```
     netsh interface ip set dns name="Local connection" source=static addr=Intranet DNS server address register=primary
     ```
### NOTE

- **Local connection**: NIC name. You need to modify the name according to the actual NIC.
- **Intranet DNS server address**: Select the intranet DNS server address based on the region where the ECS resides. For details, see [What Are the Private DNS Server Addresses Provided by the DNS Service?](#)

3. (Optional) Run the following command to configure the IP address of the backup DNS server:

   ```bash
   netsh interface ip add dns name="Local connection" addr= Alternative DNS server address index=2
   ```

### NOTE

- **Local connection**: NIC name. You need to modify the name according to the actual NIC.
- **Alternative DNS server address**: The DNS server is used when the primary DNS server is faulty, unavailable, or cannot resolve the requested domain name. Therefore, you can set this parameter to the IP address of the HUAWEI CLOUD intranet DNS server. (You need to select the intranet DNS server address based on the region where the ECS resides. For details, see [What Are the Private DNS Server Addresses Provided by the DNS Service?](#)) You can also set this parameter to the IP address of a public DNS server.

**Step 4** Download OBS Browser.

For details, see [Downloading OBS Browser](#).

**Step 5** Log in to OBS Browser.

OBS Browser uses the public network to access OBS by default. Therefore, when you log in to OBS Browser to add an account, set **Service** and **Server Address** as follows:

- **Service**: Select **Other object storage services**.
- **Server Address**: Enter the OBS domain name in the region where your ECS resides and the port number. The HTTPS port number is 443 and the HTTP port number is 80. The HTTPS server is used by default. If you want to use the HTTP server, click in the upper right corner of OBS Browser and click **System Configuration**. In the **System Configuration** dialog box that is displayed, deselect **Enable HTTPS**.

Example: obs.ap-southeast-1.myhuaweicloud.com:443

### NOTE

For details about OBS regions and endpoints, see [Regions and Endpoints](#).

**Step 6** Start to use OBS Browser.

After logging in to OBS Browser, you can access OBS over HUAWEI CLOUD intranet on the Windows ECS to perform basic data access operations and other advanced settings.

For details, see the following topics:

- **Uploading a File or Folder**
- **Downloading a File or Folder**

For details, see the [OBS Browser Overview](#).

--- End
4.3 Accessing OBS over Intranet by Using obsutil on a Linux ECS

obsutil is a command line tool applicable to Windows and Mac operating systems. You can configure the intranet DNS server address to access OBS over intranet on a HUAWEI CLOUD Linux ECS. The process and procedure are described as follows.

Process

Figure 4-3 The process of accessing OBS over intranet by using OBS Browser on a Linux ECS
Procedure

Step 1  Log In to the Linux ECS.

1. Log in to HUAWEI CLOUD and click Console.
3. Select an ECS and log in to the ECS.

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

Step 2  Check whether the intranet DNS is configured on the Linux ECS.

1. Log in to the Linux ECS and open the CLI.
2. Run the `cat /etc/resolv.conf` command to check whether the IP address after `nameserver` in the first line is the intranet DNS address of the region where the current ECS resides.

   **NOTE**
   
   HUAWEI CLOUD provides different intranet DNS server addresses for different regions. For details, see What Are the Private DNS Server Addresses Provided by the DNS Service?
   
   - If no, go to Step 3.
   - If yes, go to Step 4.

Step 3  Configure the Intranet DNS.

Change the DNS server address of the ECS to the intranet DNS provided by HUAWEI CLOUD. You can change the DNS address of the VPC subnet or modify the local DNS configuration to achieve this.

- Methods 1: Changing the DNS server address of the VPC subnet

  Locate the VPC where the ECS resides and change the DNS server address of the VPC subnet the intranet DNS address. In this manner, ECSs in the VPC can use the intranet DNS for resolution and thereby you can access OBS on HUAWEI CLOUD intranet. For details, see Modifying a Subnet.

  **NOTE**
  
  The intranet DNS server address must be selected based on the region where the ECS resides. For details, see What Are the Private DNS Server Addresses Provided by the DNS Service?

- Method 2: Modifying the local DNS configuration

  The following uses an ECS running 64-bit CentOS 6.x as an example to describe how to modify the local DNS configuration.

  a. Open the CLI.
  b. Run the following command to open the `/etc/resolv.conf` file:

    ```bash
    vi /etc/resolv.conf
    ```
  c. Press `i` to enter the editing mode. In the `/etc/resolv.conf` file, add the intranet DNS server address before the existing DNS server address in the following format:

    ```bash
    nameserver Intranet DNS server address
    ```
Intranet DNS server address: Select the intranet DNS server address based on the region where the ECS resides. For details, see What Are the Private DNS Server Addresses Provided by the DNS Service?

The IP address of the new DNS server must come before all existing DNS IP addresses.

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 change the first line of the DNS address to a public DNS server address or add a public DNS server address before the existing DNS server address.

d. Press ESC and enter :wq! to save the settings and close the file.

The modified DNS server address takes effect immediately after you save the modification to the /etc/resolv.conf file.

Step 4 Download obsutil.

For details about the latest version of obsutil and download link, see Downloading obsutil.

Step 5 Configure obsutil.

Before using, you need to configure the interconnection between obsutil and OBS. Parameters include OBS endpoints and access keys (AK and SK). For details, see Initializing the Configuration in the obsutil tool guide.

The OBS endpoint needs to be entered according to the region where the ECS resides. For details about OBS regions and endpoints, see Regions and Endpoints.

Step 6 Use obsutil.

After obsutil is successfully configured, you can access OBS over HUAWEI CLOUD intranet on the Linux ECS to perform basic data access operations and other advanced settings.

For details, see the following topics:

● Uploading an Object
● Downloading an Object

For details about operations, see Introduction to obsutil.

---End
5 Using CDN to Accelerate Access to OBS

5.1 Overview

Background

More and more companies in various industries use OBS to store static resource files such as images, videos, and software packages, and use OBS as the storage source for websites, forums, apps, and games. Users can directly request for these static resources from OBS using URLs. Figure 5-1 shows the data request process. OBS can solve the problem of insufficient local storage. Generally, files are stored in only one region. The response speeds for users accessing OBS in different regions are different. In scenarios where frequent access is required, accessing OBS to obtain files consumes a large amount of traffic.

Figure 5-1 Process of obtaining data from OBS

Solution Description

OBS provides low-cost storage, and HUAWEI CLOUD CDN provides website acceleration, file download acceleration, and on-demand acceleration. Storing data on OBS and using CDN
for service acceleration can reduce costs and improve user experience as well. When a user initiates an access request, CDN searches for the CDN node with the fastest response speed and checks whether the content requested by the user is cached on the CDN node.

If the CDN node does not cache the requested data or the cache expires, CDN retrieves the content from OBS. See Figure 5-2.

**Figure 5-2** Accessing OBS using CDN (without cache on the CDN node)

When another user accesses the same data, CDN directly returns the cached data to the user without sending another access request to OBS. **Figure 5-3** shows the process of accessing OBS using CDN when the CDN node caches the desired content.
**Solution Advantages**

- **Low cost**: When data is cached on CDN nodes, subsequent requests are charged based on the downstream traffic consumed by CDN, which reduces OBS costs.
- **High efficiency**: The CDN service on HUAWEI CLOUD has sufficient acceleration resources and widely distributed nodes. It ensures that user requests are precisely scheduled to the optimal edge node to provide effective and stable acceleration effects.

**Application Scenarios**

- Applications or services that provide file download services through OBS. For example, websites, tool download services, game clients, and app stores that use the HTTP file download services.
- Applications or services that provide audio on demand (AOD) or video on demand (VOD) services through OBS. For example, online education websites, online video sharing websites, Internet VOD platforms, and video/audio on-demand apps.

**Constraints and Limitations**

This solution applies only to buckets whose version is 3.0 or later. You can view the bucket version in **Basic Information** area on OBS Console.
5.2 Using CDN to Accelerate OBS File Download

This section uses the game download and update services on a game website as examples to describe how to use CDN on HUAWEI CLOUD to rapidly download game installation packages and update packages from OBS.

Scenario Introduction

A game website has subscribed to OBS and stores a large number of files such as game software packages, pictures, and videos on OBS. As the number of users increases, responses of game download and image loading became slower, especially for users who are far away from the file storage area. To address this issue, the website decided to use the CDN service to accelerate game download at the lowest cost and improve user experience.

Data Preparations

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website domain name</td>
<td>Domain name of the game website. According to China's Internet Management Regulations, this domain name must be licensed by the Ministry of Industry and Information Technology and the license validity does not expire. Otherwise, CDN does not accelerate the domain name.</td>
<td>download.game-apk.com</td>
</tr>
<tr>
<td>OBS Bucket</td>
<td>Bucket for storing static resources such as images and software packages. Set the storage class to Standard and the bucket policy to private.</td>
<td>game-apk</td>
</tr>
</tbody>
</table>

Prerequisites

Static resources, such as images and software packages, have been stored in a bucket on OBS.

**NOTE**

If the required files are not yet uploaded to OBS, you can create buckets and upload files through OBS Console, OBS Browser, or the SDK. For details, see the help documents of each method.

Procedure

**Step 1** Configure CDN file download acceleration.

OBS supports domain name management. After a user-defined domain name is bound to OBS, the OBS can be accessed using this domain name. In addition, CDN acceleration can be enabled during the binding without configuration on the CDN page.

1. Log in to HUAWEI CLOUD console and choose **Service List > Storage > Object Storage Service**. The OBS Console page is displayed.
2. Click the bucket where the software package is stored, for example, bucket `game-apk`.

3. In the navigation tree on the left, choose Domain Name Mgmt and click Bind User Domain Name.

4. In the Bind User Domain Name dialog box, configure the domain name and CDN acceleration information. See Figure 5-4.
   - User Domain Name: Enter the domain name of the game website, for example, `download.game-apk.com`.
   - CDN Acceleration: Enable CDN acceleration.
   - Service Type: Select File download.

   ![Figure 5-4 Binding a user domain name](image)

5. Click OK.

**Step 2** Configure CNAME.

After the CDN acceleration function is enabled when the domain name is bound to OBS, CDN automatically generates a CNAME for the bound domain name. Configure the CNAME record at the domain name service provider so that the acceleration domain name is pointed to its corresponding CNAME in CDN. After the domain name resolution takes effect, all requests for the acceleration domain name will be directed to CDN nodes. For details, see Configuring CNAME.

**Step 3** Enable private bucket retrieval on CDN.

Because the bucket for storing the software package is a private bucket, CDN can retrieve data from the OBS only after the function for private bucket retrieval is enabled on the CDN. For details, see Private Bucket Retrieval.

**Step 4** Configure the file download URL.

Set the URL of the file to be downloaded in the code as follows: Domain name of the game website+Storage path of the file in the OBS bucket+File name.

In the following example, the game website domain name is `download.game-apk.com`, as configured in Step 1, and the `android.apk` file under the `game/3.2.1/` folder in the `game-apk` is used. Then the file download URL is as follows:

https://download.game-apk.com/game/3.2.1/android.apk
**Step 5** Verify the services.

After the game website is redeployed, log in to the game website, browse web pages, and download games.

If images are displayed properly and the game can be downloaded successfully, the acceleration configuration is successful.

---End
6 Using a User-Defined Domain Name to Host a Static Website

6.1 Overview

OBS allows you to access static websites hosted by OBS using user-defined domain names. This section uses a typical scenario as an example to describe how to use a user-defined domain name to configure static website hosting. Before starting the configuration, you may need to learn more about 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 6-1.

Figure 6-1 Using a user-defined domain name to access hosted static website
Data Planning

Table 6-1 describes the data to be planned before this configuration.

Table 6-1 Data Planning

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-defined domain name</td>
<td>User's own domain name</td>
<td><a href="http://www.example.com">www.example.com</a></td>
</tr>
<tr>
<td>Static website homepage</td>
<td>Indicates the index page that is returned when you access a static website, that is, the homepage.</td>
<td>index.html</td>
</tr>
<tr>
<td>Default 404 Page</td>
<td>When an incorrect static website path is accessed, the 404 error page is returned.</td>
<td>error.html</td>
</tr>
</tbody>
</table>

- The contents of index.html are as follows:

```html
<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
<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>
```

6.2 Static Website Hosting

Process of Static Website Hosting

You need to create a bucket on OBS Console to store static website resources, enable static website hosting for the bucket, and bind the user-defined domain name to the newly created bucket using the user-defined domain name binding function provided by OBS. Then, create and configure domain name hosting using Domain Name Service (DNS) so that a user-defined domain name can be used to access the static website hosted on the OBS. 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. **Bind a user-defined domain name.**
6. **Create and configure domain name hosting.**
7. **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.

There is no special requirement for bucket names. You only need to create a bucket for storing static website files as prompted. The following uses creating a bucket named `example` as an example:

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 [Storage Classes Overview](#).

   - **Bucket Name**: Enter `example`.
   - **Bucket Policies**: 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 6-2](#).
3. Click ![FileNotFoundException](image) 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 files.

**Step 4** Configure static website hosting.

After uploading the static website files, 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. See Figure 6-3.
Figure 6-3 Configuring static website hosting

<table>
<thead>
<tr>
<th>Configure Static Website Hosting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
</tr>
<tr>
<td>Hosting By</td>
</tr>
<tr>
<td>Current bucket</td>
</tr>
<tr>
<td>Home Page</td>
</tr>
<tr>
<td>404 Error Page</td>
</tr>
<tr>
<td>Redirection Rule</td>
</tr>
</tbody>
</table>

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 Bind a user-defined domain name.

To bind a user-defined domain name to OBS, perform the following steps:

1. Click the bucket name to go to the Overview page. In the navigation tree on the left, choose Domain Name Management.

2. Click Bind User Domain Name, and enter www.example.com in the User Domain Name text box, as shown in Figure 6-4.
3. (Optional) Configure CDN acceleration.
   After CDN acceleration is enabled, select website acceleration, file download acceleration, or VOD acceleration based on the hosted static website type. CDN acceleration is billable, for details, see CDN Pricing Details.

4. Click OK. The user-defined domain name is bound to the bucket domain name.

5. (Optional) If CDN acceleration is enabled, perform the following steps to configure CDN origin information:
   a. In the Operation column of the user-defined domain name that has been bound, click Manage CDN Acceleration.
   b. On the CDN Console page that is displayed, click the domain name. The page with basic information and settings of the domain name is displayed.
   c. In the Origin Server Setting area, click Edit, the Modify Origin Server dialog box is displayed. In the Primary Origin Server area, select Domain name for Type and enter the website hosting domain name in the Origin Server text box.

   **NOTE**
   Perform the following operations to obtain the website hosting domain name. On OBS Console, enter the bucket for website hosting, select Static Website Hosting from Basic Configurations in the navigation pane on the left. On the displayed page, the value of Endpoint is the website hosting domain name.
   d. Click OK.

**Step 6** 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 HUAWEI CLOUD 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**
- If CDN acceleration is disabled when a user-defined domain name is bound, the added CNAME record must point to the access domain name of 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 "Create a Public Zone" in Hosting Public Domain Names.

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: Select Default.
   - TTL (s): Retain the default value.
   - Value: Domain name mapped to the CNAME. If CDN acceleration is disabled when a user-defined domain name is bound, enter the bucket access domain name. If CDN acceleration is enabled, set this parameter to the acceleration domain name (CNAME) provided by CDN.
   For details, see Adding a CNAME Record Set.

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 IP address of the DNS server, see section "Change the DNS Servers of the Domain Name" in Hosting Public Domain Names.

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

**Step 7** Verify that the configuration is successful.

- Enter www.example.com in the address bar of the browser to check whether the default home page can be accessed. See Figure 6-5.

**Figure 6-5** Default homepage

[Image of a web browser showing the homepage of www.example.com]

Welcome to use OBS static website hosting.

This is the 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. See Figure 6-6.
6.3 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 mis-operations 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. See Figure 6-7.
Step 4 Select Enable and click OK to enable versioning for objects in the bucket.

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 6-8.

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 **Upload** 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
7 Enterprise Data Access Control

7.1 Introduction to OBS Access Control

By default, only the resource owner can access OBS resources. Without authorization, other users cannot access OBS. 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

OBS provides multiple permission control mechanisms, including IAM policies, IAM agencies, object access restriction, object ACL, bucket ACL, and bucket policies. Table 7-1 describes the mechanisms and application scenarios.

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Description</th>
<th>Application Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM policy</td>
<td>IAM policies define the actions that can be performed on your cloud resources. In other words, an IAM policy specifies what actions are allowed or denied. 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.</td>
<td>• Controlling permissions to cloud resources as a whole • Controlling permissions to all OBS buckets and objects</td>
</tr>
<tr>
<td>Mechanism</td>
<td>Description</td>
<td>Application Scenario</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IAM agency</td>
<td>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.</td>
<td>Reading data in private OBS buckets using other cloud services, for example, private bucket retrieval</td>
</tr>
</tbody>
</table>
| Time-limited access to objects | Provides a URL that is accessible within a specified period of time. In this way, anonymous users can download software from objects only within the specified period. For details, see Sharing a Folder. | • Granting a third party the temporary permission to download objects without user authentication  
• Granting permissions to other HUAWEI CLOUD accounts or users for only temporary access |
| 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. | • Object-level access control is required. A bucket policy can control access permissions for an object or a set of objects. If you want to further specify an access permission for an object in the set of objects for which a bucket policy has been configured, then the object ACL is recommended for easier access control over single objects.  
• Object is accessed through a URL. Generally, if you want to grant anonymous users the permission to read an object through a URL, use object ACL. |

**NOTE**
- By default, an object ACL is created when the object is uploaded. The object owner has full control over the object.
- 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, instead of the bucket owner account A, account B is the owner of the object.
<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Description</th>
<th>Application Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bucket ACL</td>
<td>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. NOTE: By default, a bucket ACL is created upon the creation of the bucket. The bucket owner has full control over the bucket. Bucket ACLs do not provide fine-grained permission control. Generally, IAM and bucket policies are recommended for permission access control.</td>
<td>Granting the log delivery user with the write access to the target bucket, so that access logs can be delivered to the target bucket. Grant an account with the read and write access to a bucket, so that bucket data can be shared or external buckets can be added.</td>
</tr>
<tr>
<td>Bucket policy</td>
<td>Bucket policies provide centralized access control on OBS resources, and define which operations on which cloud resources are allowed. They are the extension and supplement of ACLs of buckets and objects.</td>
<td>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.</td>
</tr>
<tr>
<td>Object policy</td>
<td>An object policy is also a part of a bucket policy. A bucket policy can be applied to multiple or all objects in a bucket. An object policy applies to specified objects. Only actions and conditions related to the object can be configured in an object policy.</td>
<td>Configuring for a single object. For example, you can directly configure a policy for the object after an object is uploaded.</td>
</tr>
</tbody>
</table>

For details about access control mechanisms when grantees and authorized resources are involved, see Table 7-2.
## Table 7-2 OBS access control mechanisms

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Grantee</th>
<th>Authorized Resource</th>
<th>Granted Operation</th>
<th>Condition Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAM policy</td>
<td>IAM users</td>
<td>All OBS resources except specified OBS resources or resource sets</td>
<td>All permissions to access OBS</td>
<td>Not supported</td>
</tr>
<tr>
<td>IAM agency</td>
<td>Accounts</td>
<td>All OBS resources except specified OBS resources or resource sets</td>
<td>All permissions to access OBS</td>
<td>Time limitation configuration (permanent or one-day)</td>
</tr>
<tr>
<td></td>
<td>Cloud services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time-limited access to objects</td>
<td>Anonymous users</td>
<td>Objects</td>
<td>Obtains the content and metadata of an object.</td>
<td>Time limitation configuration</td>
</tr>
<tr>
<td>Object ACL</td>
<td>Accounts</td>
<td>Objects</td>
<td>• Obtains the content and metadata of an object.</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>Anonymously</td>
<td></td>
<td>• Obtains the content and metadata of a specified object.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>registered user groups</td>
<td></td>
<td>• Obtains the ACL for an object.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Obtains the ACL for an object of a specified version.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Configures object ACL.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Configures the ACL for an object of a specified version.</td>
<td></td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Grantee</th>
<th>Authorized Resource</th>
<th>Granted Operation</th>
<th>Condition Configuration</th>
</tr>
</thead>
</table>
| 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. | Not supported |
| Bucket policy | Accounts, IAM users, Anonymous users | All OBS resources | All operation permissions on OBS. For details, see [Actions](#). | Supported |
| Object policy | Accounts, IAM users, Anonymous users | Specified objects | Operations on objects. For details, see [Actions > Actions Related to Objects](#). | Supported |
- Restricted conditions
  
  Configure refined conditions for bucket policies to restrict scenarios where a bucket policy takes effect, in order to 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 7-1 Authorization process**

![Authorization process diagram]

**Figure 7-2** is a matrix of the IAM policy, bucket policy, and ACL (ALLOW and DENY effects).

**Figure 7-2 Matrix of the IAM policy, bucket policy, and ACL (ALLOW and DENY effects)**

<table>
<thead>
<tr>
<th>Bucket Policy</th>
<th>IAM Policy</th>
<th>ACL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny</td>
<td>Deny</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default Deny</td>
</tr>
<tr>
<td>Allow</td>
<td>Deny</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default Deny</td>
</tr>
<tr>
<td>Default Deny</td>
<td>Allow</td>
<td>Deny</td>
</tr>
<tr>
<td></td>
<td>Deny</td>
<td>Default Deny</td>
</tr>
</tbody>
</table>
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.

### 7.2 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 the full control permission to department public data stored on OBS, and that common users can only read those data. Figure 7-3 shows the logical relationships.

#### Figure 7-3 Logical diagram

![Logical diagram](image)

#### Solution and Process

In this scenario, you can assign permissions by configuring an **IAM Policy**. 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 7-4 shows the process.
**Figure 7-4** Flowchart of managing access to department public data

![Flowchart](image)

**Procedure**

**Step 1  Create an administrator.**

1. Log in to the HUAWEI CLOUD console using the enterprise account.
2. On the console homepage, choose **Service List > Management & Deployment > Identity and Access Management** to access the IAM console.
3. On the IAM console, choose **User** in the left navigation tree.
4. 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**.
5. Click **Next**. Select **Set manually** for **Password Type**.
6. Enter the email address, mobile number, password, and confirm password.
7. 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 using OBS Console, OBS Browser, APIs, and SDKs. 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 bucket to be operated. On the **Summary** page that is displayed, click **Objects** to view the list of objects.
   - 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 **Objects** page, perform operations including uploading and deleting objects.
   - If the write and delete operations can be performed, it indicates the read-only permission fails to be granted. Check whether the user permission configuration is correct.
   - If not, the read-only permission for common users is correctly configured.

---End

### 7.3 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.

In this document, department A shares data in the bucket **example-bucket** to users in department B for download. This section describes how to perform permission control on
shared data based on the principle of least privilege. Figure 7-5 shows the logical relationships among administrators, users, and buckets for data sharing of the two departments in this scenario.

**Figure 7-5 Logical diagram**

![Logical diagram showing the relationships among administrators, users, and buckets for data sharing.](image)

**Solution and Process**

In this scenario, department A administrator can use the bucket policy to implement permission control to users in department B so that they can download but cannot modify or delete the shared data. Figure 7-6 illustrates the configuration process.
Figure 7-6 Process for configuring permission settings that allows data sharing

Prerequisites

Administrators and common users of departments A and B have been created by the account in IAM. For details about how to create an IAM user, see Creating a User.

**NOTE**

Department A administrator needs to perform operations such as creating buckets and configuring bucket policies. Therefore, when creating an administrator, the user group to which the administrator belongs must be granted at least the Tenant Administrator policy of OBS.

Procedure

**Step 1  Create a bucket.**

1. Log in to the HUAWEI CLOUD console as an administrator of department A.
2. On the console homepage, choose Service List > Storage > Object Storage Service to access OBS Console.
3. On OBS Console, click Create Bucket in the upper right corner.
4. Select a region, storage class, and bucket policy, and then enter the bucket name.

**NOTE**
To ensure data security, set Bucket Policies to Private and set other parameters as prompted.
5. Click Create Now. The bucket is created.

**Step 2** Authorize the users with the permission to upload data for sharing.

If the OBS policy for the user group to which users of department A belong is Tenant Administrator, skip this step and go to step 3. If the OBS policy is not configured or the policy is set to OBS Buckets Viewer or Tenant Guest, an administrator of department A needs to perform the following steps to grant the permission to upload data to be shared to users in department A.

1. On OBS Console, click the name of the bucket that stores the shared data to go to the Summary page.
2. In the left navigation tree, choose Permissions. On the page that is displayed, click the Bucket Policies tab.
3. Click Create Bucket Policy under Custom Bucket Policies.
4. Create a custom bucket policy by referring to Table 7-3.

**Table 7-3** Parameters for creating a policy to allow upload

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Mode</td>
<td>Select Read-only.</td>
</tr>
<tr>
<td>Principal</td>
<td>Select Include and Current account, and then select an authorized user from the drop-down list. Select users of department A who can upload data for sharing.</td>
</tr>
<tr>
<td>Resources</td>
<td>Select Include and enter the resource name based on the scope of the shared data.</td>
</tr>
<tr>
<td></td>
<td>- If all objects in the current bucket need to be shared, enter *.</td>
</tr>
<tr>
<td></td>
<td>- If a folder or a type of objects in the bucket needs to be shared, enter the name of the folder (for example, example-folder/) or an object set with a wildcard character (for example, *.doc). You can also enter multiple resource names, separating them using commas (,).</td>
</tr>
</tbody>
</table>

5. Click OK. If a message similar to Bucket policy created successfully is displayed, it indicates that the permission is successfully configured.

**Step 3** Authorize the users with the permission to download the shared data.

If the policy for the user group to which users of department B belong is Tenant Administrator or Tenant Guest, skip this step and go to step 2. If the OBS policy is not configured or the policy is set to OBS Buckets Viewer, an administrator of department A needs to perform the following steps to grant the permission to download shared data to users in department B.
1. On OBS Console, click the name of the bucket that stores the shared data to go to the Summary page.
2. In the left navigation tree, choose Permissions. On the page that is displayed, click the Bucket Policies tab.
3. Click Create Bucket Policy under Custom Bucket Policies.
4. Create a custom bucket policy by referring to Table 7-4.

Table 7-4 Parameters for creating a policy to allow download

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Mode</td>
<td>Select Customized.</td>
</tr>
<tr>
<td>Effect</td>
<td>Select Allow.</td>
</tr>
<tr>
<td>Principal</td>
<td>Select Include and Current account, and then select an authorized user from the drop-down list. Select users of department B who can download the shared data.</td>
</tr>
</tbody>
</table>
| Resources       | Select Include and enter the resource name based on the scope of the shared data.  
|                 | - If all objects in the current bucket need to be shared, leave the resource name blank.  
|                 | - If a folder or a type of objects in the bucket needs to be shared, enter the name of the folder (for example, example-folder/) or an object set with a wildcard character (for example, *.doc). You can also enter multiple resource names, separating them using commas (,). |
| Actions         | Select Include, and select Get* and List* under General in Action Name. |

5. Click OK. If a message similar to Bucket policy created successfully is displayed, it indicates that the permission is successfully configured.

**Step 4** Prevent the users from modifying and deleting the shared data.

1. On OBS Console, click the name of the bucket that stores the shared data to go to the Summary page.
2. In the left navigation tree, choose Permissions. On the page that is displayed, click the Bucket Policies tab.
3. Click Create Bucket Policy under Custom Bucket Policies.
4. Create a custom bucket policy by referring to Table 7-5.

Table 7-5 Parameters for creating a policy to prevent write and deletion

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Mode</td>
<td>Select Customized.</td>
</tr>
<tr>
<td>Effect</td>
<td>Select Deny.</td>
</tr>
</tbody>
</table>
### Parameter | Configuration
---|---
Principal | Select Include and Current account, and then select an authorized user from the drop-down list. Select users of department B who cannot modify or delete data.
Resources | Select Include and enter the resource name based on the scope of the shared data.  
- If all objects in the current bucket need to be shared, enter *.
- If a folder or a type of objects in the bucket needs to be shared, enter the name of the folder (for example, example-folder/) or an object set with a wildcard character (for example, *.doc). You can also enter multiple resource names, separating them using commas (,).
Actions | Select Include and select the following six actions under Object from the drop-down list of Action Name.  
- PutObject  
- PutObjectAcl  
- PutObjectVersionAcl  
- DeleteObject  
- DeleteObjectVersion  
- AbortMultipartUpload

5. Click OK. If a message similar to Bucket policy created successfully is displayed, it indicates that the permission is successfully configured.

**Step 5** **Upload data.**

Users in department A can upload data using OBS console, OBS Browser, APIs and SDKs. This section takes the operations on OBS console as an example to describe how to upload data.

1. Log in to OBS Console as a user of department A.
2. In the OBS bucket list, click the name of the bucket that stores the shared data.
3. In the navigation tree on the left, click Objects and then Upload Object.
4. In the displayed Upload Object dialog box, select the upload mode, storage class, and data to be uploaded as prompted.
5. Click Upload.

You can click Task Management in the lower part of the page to view the upload progress and result.

**Step 6** **Verify the permission.**

After the permission is configured, users in department B can verify the permissions using OBS Console, OBS Browser, APIs, and SDKs. This section takes OBS Console as an example to present how to verify that users in department B can only read the shared data.

1. Log in to OBS Console as an IAM user of department B.
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 public data record is located.
   - If the download fails, the download permission fails to be granted. Check whether the user group permission configuration is correct.
   - If the download is successful, the download permission is granted successfully. Go to the next step.
5. Click Upload Object, select a file, and click Upload.
   - If the upload is successful, the permission configuration for preventing write and deletion by users of other departments fails. Check whether the bucket policy is correctly configured.
   - If the upload fails, the permission configuration succeeded. Go to the next step.
6. Click Delete in the row where a public data record is located.
   - If the deletion is successful, the permission configuration for preventing write and deletion by users of other departments fails. Check whether the bucket policy is correctly configured.
   - If the deletion fails, the permission configuration succeeded.

---End

7.4 Data Isolation from Enterprise Partners

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

Prerequisites

An account ID of the partner has been obtained.

Procedure

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

Step 1 Log in to the HUAWEI CLOUD console as an account or an enterprise administrator (an IAM user whose user group is admin).

Step 2 On the homepage of the HUAWEI CLOUD console, choose Service List > Storage > Object Storage Service.

Step 3 In the OBS bucket list, click the name of the target bucket.

Step 4 In the left navigation tree, choose Permissions. On the page that is displayed, click the Bucket Policies tab.

Step 5 Click Create Bucket Policy under Custom Bucket Policies.

Step 6 Create a custom bucket policy based on the following parameter settings.
   - Select Customized for Policy Mode.
   - Select Allow for Effect.
Select **Include** and **Other account** for **Principal**, and enter the account ID of the partner.

- For **Resources**, enter *, which indicates that this bucket policy applies to all the objects in the current bucket.
- For **Actions**, select * under **General** from the drop-down list, which indicates that all actions related to the object can be performed.

**NOTE**
You can also configure one or more specified actions by referring to **Actions > Actions Related to Buckets**

**Step 7** Click **OK** to create the policy.

**Step 8** Verify the permission.

After the permission is granted, partner users can use OBS Browser 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 added and the action configured in **Step 6** can be properly performed, the permission is granted successfully.

----End
OBS manages partitions based on the UTF-8 code range of object names and implements horizontal expansion and dynamic load balancing accordingly. If you use sequential prefixes (such as timestamps or alphabetical order) in object naming, object access requests may be concentrated in a specific partition, causing access hotspots. The request rate in a hotspot partition is limited, as a result, access delay increases.

**Random prefixes for object naming are recommended so that requests are evenly distributed across partitions, allowing horizontal expansion.**

Example:

In a typical scenario of log archiving, the names of objects to be uploaded are as follows:

```plaintext
yourbucket/obslog/20190610-01.log.tar.gz
yourbucket/obslog/20190610-02.log.tar.gz
yourbucket/obslog/20190610-03.log.tar.gz
yourbucket/obslog/20190610-04.log.tar.gz
...
yourbucket/obslog/20190611-01.log.tar.gz
yourbucket/obslog/20190611-02.log.tar.gz
yourbucket/obslog/20190611-03.log.tar.gz
yourbucket/obslog/20190611-04.log.tar.gz
```

You are advised to add a hexadecimal hash prefix with three or more digits to the object name.

```plaintext
yourbucket/6ac-obslog/20140610-01.log.tar.gz
yourbucket/b42-obslog/20140610-02.log.tar.gz
yourbucket/17f-obslog/20140610-03.log.tar.gz
yourbucket/ac9-obslog/20140610-04.log.tar.gz
...
yourbucket/95d-obslog/20140611-01.log.tar.gz
yourbucket/4a5-obslog/20140611-02.log.tar.gz
yourbucket/ea2-obslog/20140611-03.log.tar.gz
yourbucket/ba3-obslog/20140611-04.log.tar.gz
```
## Change History

<table>
<thead>
<tr>
<th>Release Date</th>
<th>What's New</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-07-06</td>
<td>This issue is the fourth official release.</td>
</tr>
<tr>
<td></td>
<td>This issue incorporates the following change:</td>
</tr>
<tr>
<td></td>
<td>• Added the section &quot;Performance Optimization&quot;.</td>
</tr>
<tr>
<td>2019-05-20</td>
<td>This issue is the third official release.</td>
</tr>
<tr>
<td></td>
<td>This issue incorporates the following change:</td>
</tr>
<tr>
<td></td>
<td>• Added the section &quot;Using CDN to Accelerate Access to OBS.&quot;</td>
</tr>
<tr>
<td>2018-11-30</td>
<td>This issue is the second official release.</td>
</tr>
<tr>
<td></td>
<td>This issue incorporates the following change:</td>
</tr>
<tr>
<td></td>
<td>• Added the section &quot;Overview of OBS Best Practices.&quot;</td>
</tr>
<tr>
<td>2018-09-30</td>
<td>This issue is the first official release.</td>
</tr>
</tbody>
</table>