Media Processing Center

Service Overview

Issue	01
Date	2024-02-19

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

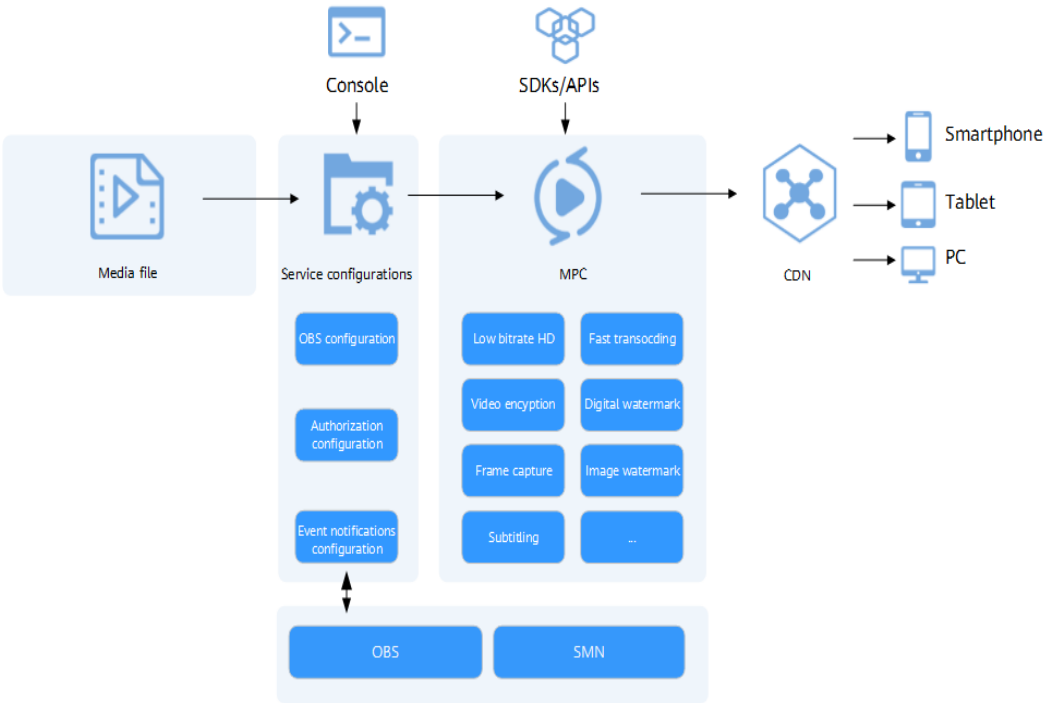
Contents

1 What Is MPC?

Media Processing Center (MPC) efficiently transcodes your media files online, at any scale, and at a low cost. MPC uses object storage and cloud computing to convert your media into the formats you need for playback on devices like smartphones, PCs, and TVs. It also provides functions such as frame capture, and watermarking to meet your diverse requirements.

MPC is built based on Huawei Cloud computing services. There is no need to buy expensive media processing software and to manage them, so you can focus on fast delivery and service rollout. MPC can scale up and down with your business needs, reducing costs and avoiding resource waste.

You can use MPC via the MPC console, SDKs, and APIs, or integrate MPC into your own applications and services.



2 Functions

MPC helps you transcode audio and video files stored in OBS buckets so that the output files can be played on a broad range of devices. It also supports snapshot capturing and watermarking.

Media Transcoding

Media transcoding is to convert an audio or video file into one or more output formats. This involves changing the parameters of the media file such as the format, codec, bitrate, and frame rate.

Parameter	Description
Input format	• Input file formats: MP4, TS, MOV, FLV, MPG, MXF, WMV, ADTS, AVI, MKV, MPEG, GIF, and WAV • Video codecs: H.264, H.265, MPEG-2, MPEG-4, MJPEG, VP6/7/8/9, WMV1/2/3, and ProRes 422 • Audio codecs: AAC, AC3, EAC3, HE-AAC, MP2, MP3, PCM (s161e, s16be, s241e, s24be, DVD), and WMA • Subtitle format: SRT file in UTF-8
Output format	• Output file formats: DASH, HLS, MP4, MP3, and ADTS • Video codecs: H.264 and H.265 • Audio codecs: HE_AAC, AAC, and MP3 • Image file format: GIF
Audio extraction	Extract audio from a video.
Mute video	Remove sound from a video.
Subtitling	Add subtitles to a video.
Watermarking	During transcoding, add static image/text watermarks to videos for copyright protection.

The transcoded audio and video specifications can be customized based on your needs. For details, see **Table 2-1**, **Table 2-2**, **Table 2-3**, and **Table 2-4**.

Table 2-1 Video encoding parameters

Parameter	Description
Video Codec	The value can be H.264 or H.265. The default value is H.264.
Resolution (video width and video height)	• H.264 – Video width: [32, 4096] or 0. The unit is px. – Video height: [32, 2880] or 0. The unit is px. • H.265 – Video width: [160, 4096] or 0. The unit is px. – Video height: [96, 2880] or 0. The unit is px. If the video width and height are both set to 0, the transcoded video is produced based on the original resolution. If the video bandwidth or height is set to 0, the corresponding value is adjusted based on the original size.
Bitrate	Video bitrate. The value can be 0 or ranges from 40 to 30,000. The unit is kbit/s. If this parameter is set to 0, an output file is generated at the adaptive bitrate.
Maximum I-Frame Interval	Maximum interval between I frames in a key frame. The value ranges from 2 to 5.
Maximum Consecutive B-Frames	Maximum number of consecutive B-frames in a key frame. The value ranges from 0 to 7.
Profile	Encoding profile. • If the video codec is H.264, BASE, MAIN, and HIGH are available. • If the video codec is H.265, only MAIN is available.
FPS	Video frame rate. The value is 0 or ranges from 5 to 30. If this parameter is set to 0, an output file is generated at the original frame rate.
Maximum Reference Frames	Maximum number of reference frames. • If the video codec is H.264, the value ranges from 1 to 8. • If the video codec is H.265, the value is always 4.

Parameter	Description
Quality	Video encoding level. There are three levels. A larger value indicates higher encoding quality and longer transcoding time.
Black Bar Removal	Automatically detect and remove black bars from your video.

Table 2-2 Video processing parameters

Parameter	Description
Video rotation angle	Rotate a video clockwise. Videos can be simply rotated by 90 degrees, 180 degrees, and 270 degrees.
Adaptive resolution	The following options are available: ● SHORT: Adaptive width ● LONG: Adaptive height ● None: Do not adapt.

Table 2-3 Audio encoding parameters

Parameter	Description
Audio Codec	The available options are AAC, HE_AAC1, HE_AAC2, and MP3. The default value is AAC.
Sampling Rate	The value can be AUTO, 22050 Hz, 32000 Hz, 44100 Hz, 48000 Hz, or 96000 Hz. The default value is AUTO.
Bitrate	Audio bitrate. The value can be 0 or ranges from 8 to 1000. The unit is kbit/s.
Audio Channel	Number of audio channels. The value can be 1 or 2.

Table 2-4 Video processing parameters

Parameter	Description
Volume control	Two methods are supported: ● **auto**: adjusts the volume automatically ● **dynamic**: adjusts the volume manually

Parameter	Description
Volume adjustment amplitude	The value range is [-15, 15], and the unit is dB.

Transcoding Templates

MPC provides plenty of built-in transcoding templates to meet your diverse requirements. You can also create a transcoding template to target your specific scenario.

- Preset templates: You can directly use these templates without any other configuration. There are audio templates, audiovisual templates, and low bitrate HD templates, covering all output formats, encoding formats, and common resolutions and bitrates. Based on the number of output files, preset templates are classified into the following types:
  - One-in one-out transcoding template: Only one file is output.
  - One-in multiple-out transcoding template: A maximum of nine files can be output.
- Custom templates: Set the video and audio parameters based on your needs. A custom template can be one-in one-out or one-in multiple-out. A maximum of six output specifications can be configured for a one-in multiple-out template.

Low Bitrate HD

MPC uses perceptual coding to analyze each scenario, action, content, and texture in a video, achieving lower bitrate and bandwidth usage at a given video quality.

Video Watermark

- You can add both image and text watermarks to videos.
- The input format can be PNG, JPG, or JPEG.
- A maximum of two static images can be overlaid on an output video per frame.
- A maximum of ten static images can be overlaid on each output video.
- The resolution of a watermark is between 8 x 8 and 4096 x 4096. The size of the watermark cannot exceed 10 MB.

Snapshot Capturing

You can capture a snapshot from a video and save it as a JPG file during transcoding or at any other time. The following two capturing methods are supported:

- By interval: Take snapshots at regular intervals. The default interval is 12s.
- At fixed time: Take snapshots at specified time points.

3 Product Advantages

Cost-effectiveness

Low-bitrate HD reduces the costs by 20% to 30% at a given image quality.

Access from Anywhere

SDKs and open APIs are available for quick access from anywhere you have an internet connection.

Fast Transcoding

Parallel transcoding allows you to transcode a one-hour media file in just 10 minutes.

Scalability

A rich set of media processing functions, including watermarking, snapshots, system presets, and custom templates, are available for you to choose from.

4 Constraints

Before using MPC, understand the following constraints.

Table 4-1 Constraints

Item	Description
Media file storage	• MPC does not store media files. You need to upload a video file to be transcoded to an OBS bucket before using MPC. • The MPC service and the OBS bucket for storing media files must be in the same region, such as the CN North-Beijing4 region.
Video encoding format	Video codecs supported are H.264, H.265, MPEG-2, MPEG-4, MJPEG, VP6/7/8/9, WMV1/2/3, and ProRes 422. If an input file is not in one of these formats, transcoding will fail.
Audio encoding format	The supported audio codecs: AAC, AC3, EAC3, HE-AAC, MP2, MP3, PCM (s161e, s16be, s241e, s24be, DVD), and WMA
Video packaging format	• Supported input formats: MP3, MP4, FLV, and TS • Supported output formats: HLS and MP4
API request throttling	The caps on requests are as follows: • Single tenants: 100 requests/minute • Overall: 1000 requests/minute

5 Related Services

Before using the event notifications, permissions management, and media storage functions, you need to enable the dependent services. See **Table 5-1**.

Table 5-1 Related services

Interactive Function	Service Name	Reference
Selecting an SMN topic when configuring event notifications on the MPC console	Simple Message Notification (SMN)	**Creating a Topic** **Adding a Subscription** **Configuring Topic Policies**
Managing users and user groups using IAM	Identity and Access Management (IAM)	**Create User Groups and Assign Permissions** **Create IAM Users and Log In**
Using OBS to store and manage audio and video files	Object Storage Service (OBS)	**Creating a Bucket** **Uploading an Object**

6 Concepts

OBS

Object Storage Service (OBS) is a stable, secure, efficient, and easy-to-use cloud storage service. MPC uses OBS to manage media files. MPC transcodes the media files stored in input buckets and then saves the transcoded files to output buckets. For more information about OBS, see **OBS Help Center**.

Bucket

Buckets are containers for storing objects. OBS provides flat storage in the form of buckets and objects. Unlike the conventional multi-layer directory structure of file systems, all objects in a bucket are stored at the same logical layer.

SMN

The Simple Message Notification (SMN) service notifies you of your transcoding task status. For more information about SMN, see **SMN Help Center**.

Transcoding Template

A transcoding template is a set of transcoding parameters, such as audio, video, and container parameters. You can select a system template to save a lot of configuration operations. If you have special requirements, you can customize a transcoding template.

Low Bitrate HD

Based on the human visual system model and Huawei's transcoding technology, MPC analyzes each scenario, action, content, and texture in a video to deliver lower bitrate while keeping the bandwidth costs down but without compromising the video quality.

Fast Transcoding

This allows MPC to transcode video segments in parallel, which can be six times faster than standard transcoding. It is perfect for transcoding videos longer than 30 minutes.

One-in Multiple-out

It is a transcoding method. That is, a video file is transcoded into video files of multiple resolutions and bitrates to meet the playback requirements of different devices and different network speeds.

Image Enhancement

The combination of the traditional super-resolution algorithm and AI-powered image enhancement algorithm converts 2K videos to 4K videos, repairs damaged images, and improves the image quality of existing videos.

7 Region and AZ

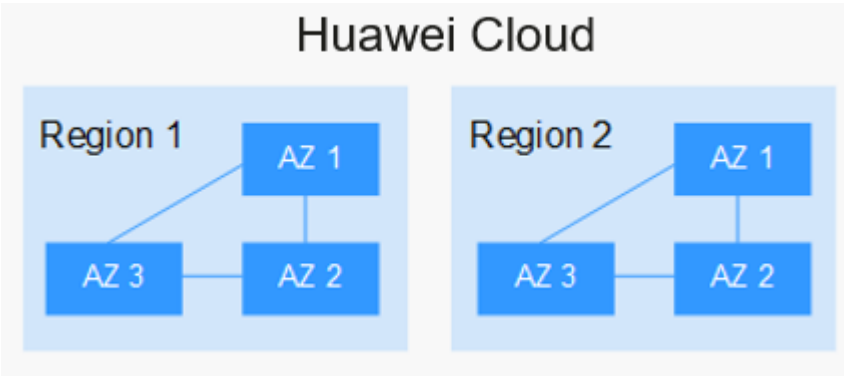
Concepts

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

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or multiple physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

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

Figure 7-1 Regions and AZs



HUAWEI CLOUD provides services in many regions around the world. You can select a region and AZ as needed. For more information, see **Huawei Cloud Global Regions**.

How Do I Select a Region?

When selecting a region, consider the following factors:

- Location

  You are advised to select a region close to you or your target users. This reduces the network latency and improves the access speed. Regions within the Chinese mainland provide the same infrastructure, BGP network quality, as well as resource operations and configurations. Therefore, if your target users are in the Chinese mainland, you do not need to consider the network latency differences when selecting a region.

  - If you or your target users are in the Asia Pacific area outside the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your target users are in Africa, select the **AF-Johannesburg** region.
  - If you or your target users are in Europe, select the **EU-Paris** region.
- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

How Do I Select an AZ?

When determining whether to deploy resources in the same AZ, consider your application's requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

Regions and Endpoints

Before using an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

8 Security

8.1 Shared Responsibilities

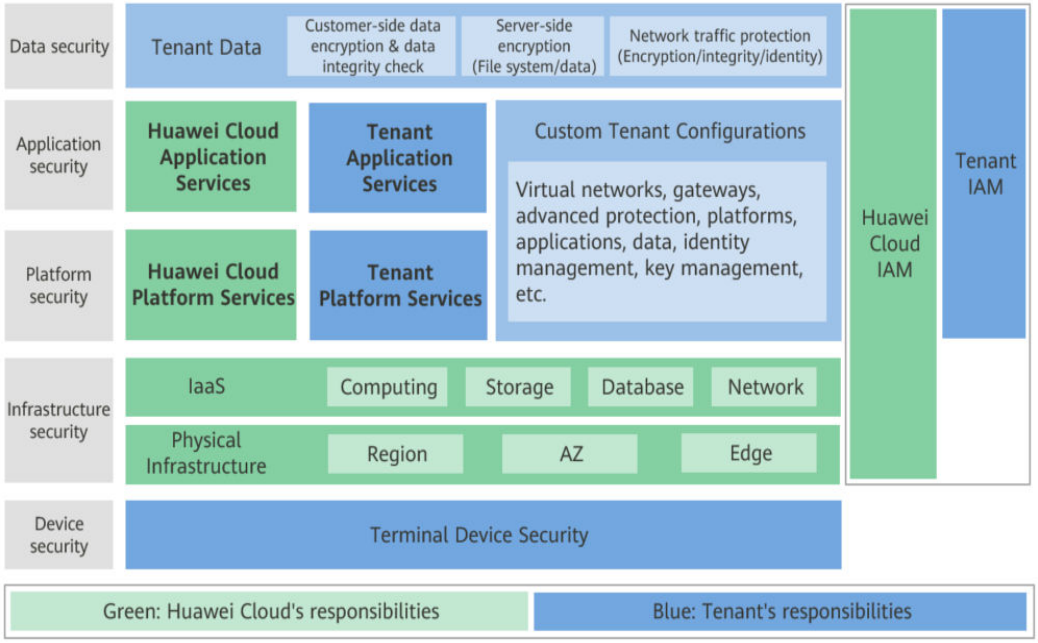
Huawei Cloud guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To tackle emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 8-1 illustrates the responsibilities shared by Huawei Cloud and users.

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

Huawei Cloud Security White Paper introduces in detail the building ideas and measures of Huawei cloud security, including cloud security strategy, responsibility sharing model, compliance and privacy, security organization and personnel, infrastructure security, tenant service and tenant security, engineering security, O&M and operation security, and ecosystem security.

Figure 8-1 Huawei Cloud shared security responsibility model



8.2 Identity Authentication and Access Control1

Identity Authentication

- **Identity credential and its security**

  MPC can be accessed using accounts or IAM users. Both of them support identity authentication using usernames, passwords, access keys, and temporary access keys. As shown in **Table 8-1**, MPC implements security design for each identity credential to protect user data and enable users to access MPC more securely.

Table 8-1 MPC identity credential and security design

Access Credential	Security Description	Details
Username and password	You can configure the character type and minimum length of a user key. You can also configure the password validity period policy and minimum password validity period policy.	**Password Policy**
Access key	AK is used together with SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct.	**Access Keys**

Access Credential	Security Description	Details
Temporary access key	In addition to the access key feature, a temporary access key has a validity period that can be customized. After the validity period expires, the temporary access key becomes invalid and you have to obtain a new one.	**Temporary Access Key**

- **Login protection and authentication policies**

  As shown in **Table 8-2**, in addition to requiring users to show their credentials and verify their validity, MPC also provides a login protection mechanism and supports login authentication policies to prevent user information from being stolen.

  Table 8-2 Login protection and authentication policies

Login Protection Method	Description	Details
Login protection	In addition to entering the username and password on the login page (first identity authentication), you also need to enter a verification code on the login verification page (second identity authentication) when logging in to Huawei Cloud. Check whether mobile numbers, email addresses, and virtual MFA devices are supported. For details, see **MFA Authentication**.	**Login Protection**
Login authentication policy	MPC supports the **session timeout policy** (If a user does not log in to the system within a specified period, the user needs to log in again), **account locking policy** (If the number of login failures exceeds the threshold, the account is locked), **account disabling policy** (If a user does not log in to the system for a long time, the account is disabled), and **recent login information** that allows users to view the last login time.	**Login Authentication Policy**

Access Control

MPC supports access control through IAM fine-grained authorization policies.

Table 8-3 MPC access control

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

8.2.1 Identity Authentication and Access Control

Identity Authentication

- **Identity credential and its security**

  MPC can be accessed using accounts or IAM users. Both of them support identity authentication using usernames, passwords, access keys, and temporary access keys. As shown in **Table 8-4**, MPC implements security design for each identity credential to protect user data and enable users to access MPC more securely.

  Table 8-4 MPC identity credential and security design

Access Credential	Security Description	Details
Username and password	You can configure the character type and minimum length of a user key. You can also configure the password validity period policy and minimum password validity period policy.	**Password Policy**
Access key	AK is used together with SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct.	**Access Keys**
Temporary access key	In addition to the access key feature, a temporary access key has a validity period that can be customized. After the validity period expires, the temporary access key becomes invalid and you have to obtain a new one.	**Temporary Access Key**

- **Login protection and authentication policies**

  As shown in **Table 8-5**, in addition to requiring users to show their credentials and verify their validity, MPC also provides a login protection mechanism and

supports login authentication policies to prevent user information from being stolen.

Table 8-5 Login protection and authentication policies

Login Protection Method	Description	Details
Login protection	In addition to entering the username and password on the login page (first identity authentication), you also need to enter a verification code on the login verification page (second identity authentication) when logging in to Huawei Cloud. Check whether mobile numbers, email addresses, and virtual MFA devices are supported. For details, see **MFA Authentication**.	**Login Protection**
Login authentication policy	MPC supports the **session timeout policy** (If a user does not log in to the system within a specified period, the user needs to log in again), **account locking policy** (If the number of login failures exceeds the threshold, the account is locked), **account disabling policy** (If a user does not log in to the system for a long time, the account is disabled), and **recent login information** that allows users to view the last login time.	**Login Authentication Policy**

Access Control

MPC supports access control through IAM fine-grained authorization policies.

Table 8-6 MPC access control

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

8.3 Data Protection

MPC takes different measures to keep data stored in MPC secure and reliable.

Table 8-7 MPC data protection methods and features

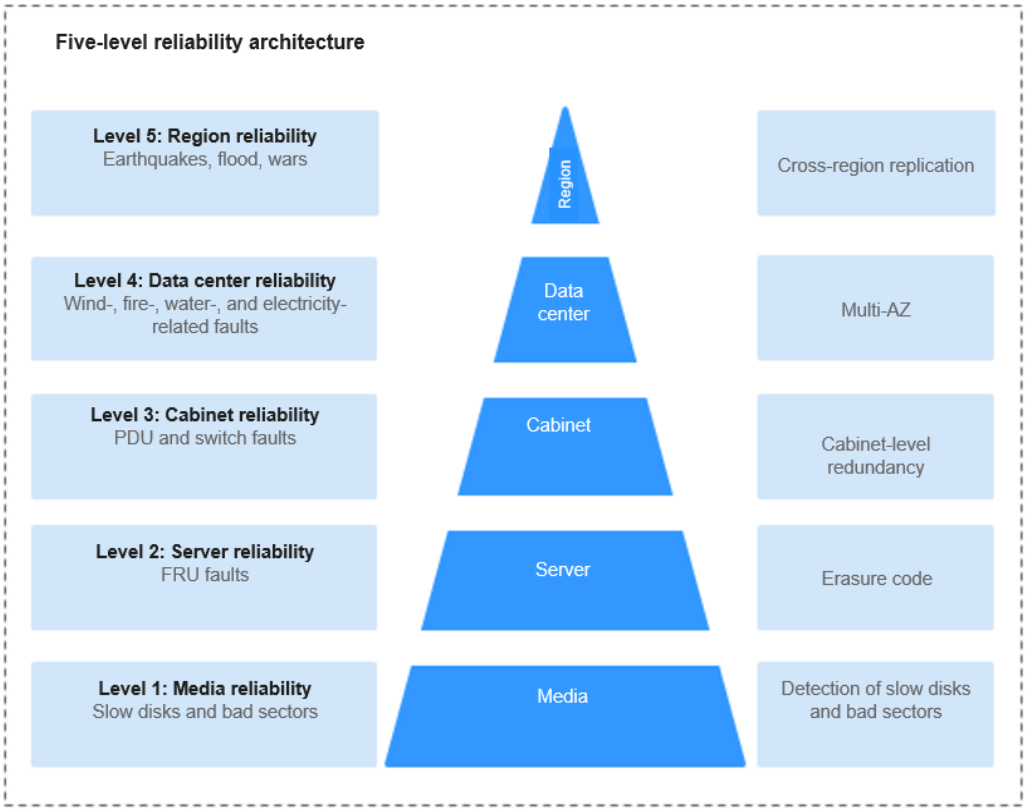
Measure	Description	Details
Transmission encryption (HTTPS)	MPC supports HTTP and HTTPS, but HTTPS is recommended to enhance the security of data transmission.	**Making an API Request**
Data redundancy	OBS uses the Erasure Code (EC) algorithm, instead of multiple copies, to ensure data redundancy. EC delivers a higher storage space utilization than the multi-copy redundancy while maintaining the same reliability level. When creating a bucket on OBS, you can choose a data redundancy policy. Choosing the multi-AZ storage will make your data redundantly stored in multiple AZs in the same region. If one AZ becomes unavailable, data can still be properly accessed from the other AZs. The multi-AZ storage is ideal when high reliability is required.	**Creating a Bucket**
Data integrity verification (MD5)	During object uploads or downloads, data may become inconsistent due to causes such as network hijacking and caching. MPC verifies data consistency by calculating the MD5 value when data is uploaded or downloaded.	**Data Consistency Check**
Cross-region replication	You can configure cross-region replication rules to automatically, asynchronously replicate data from a source bucket to a destination bucket in another region. This provides you with the capability for disaster recovery across regions, catering to your needs for remote backup.	**Cross-Region Replication**

Measure	Description	Details
Critical operation protection	With this function enabled, the system authenticates user's identity when they perform any risky operation like deleting a media file. This enhances the protection for your data and configuration.	**Critical Operation Protection**
Sensitive user data protection	MPC encrypts and stores the required sensitive personal information within the service to prevent disclosure.	-

8.4 Resilience

MPC offers a five-level reliability architecture. It ensures data durability and reliability by leveraging cross-region replication, disaster recovery across AZs, device and data redundancy in an AZ, and detection of slow disks and bad sectors.

Figure 8-2 Five-level reliability architecture

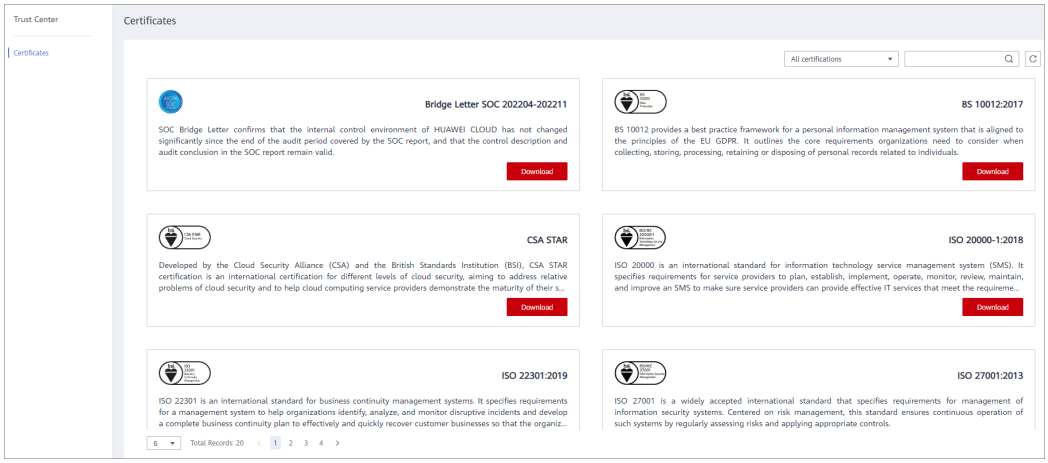


8.5 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained security compliance certificates of multiple authoritative organizations (such as ISO, SOC, and PCI) inside and outside China. You can **apply for and download** compliance certificates.

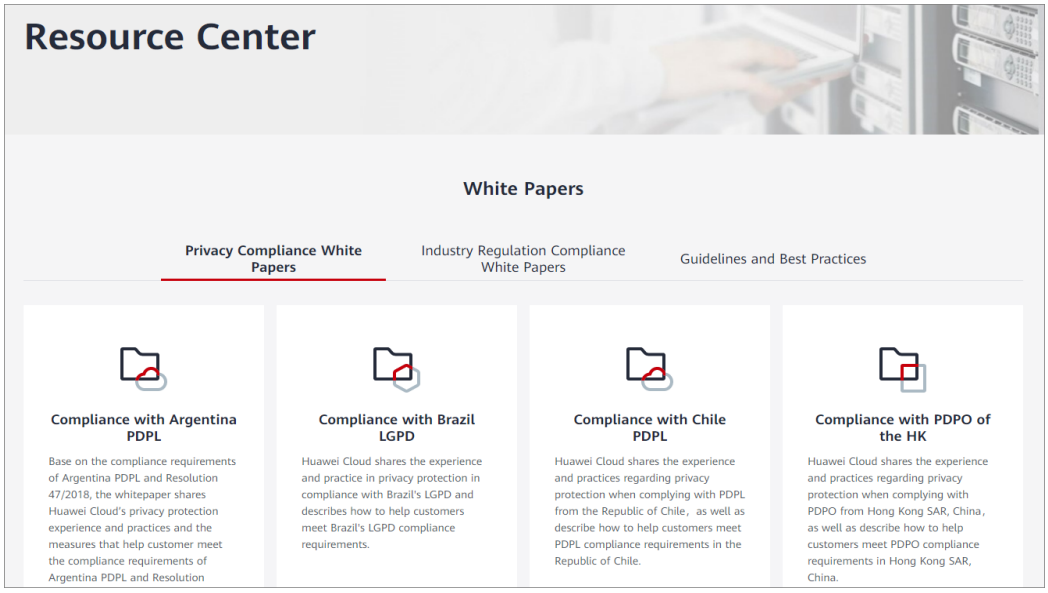
Figure 8-3 Compliance certificate download



Resource Center

Huawei Cloud also provides the following resources to help you meet compliance requirements. For details, see **Resource Center**.

Figure 8-4 Resource Center



9 Personal Data

Personal Data Use Scenario	Transcoded and packaged media files	After you deliver a snapshot capturing task, the screenshot is stored in your OBS bucket.
Collected Personal Data	Media files for media processing	Snapshot capturing
Collection Source and Method	MPC collects data when you process a media file.	During media processing, MPC obtains data from the video file.
Purpose and Security Measure	A video file is transcoded and stored in your OBS bucket. The transcoded file is stored in your OBS bucket. You can process the transcoded file and configure the security mechanism of the OBS bucket.	The screenshot is stored in your OBS bucket. You can process the screenshot and configure the security mechanism of the OBS bucket.
Retention Period and Policy	The system cache can be retained for a maximum of 24 hours in abnormal scenarios.	The system cache can be retained for a maximum of 24 hours in abnormal scenarios.
Destruction Method	The cache is automatically deleted.	The cache is automatically deleted.
Export Method	You can export and download the data from OBS buckets.	You can export and download the data from OBS buckets.
Export Guide	**OBS User Guide**	**OBS User Guide**

