KooDrive

Service Overview

Issue 01

Date 2024-07-30

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Contents

1 What Is KooDrive?

Introduction

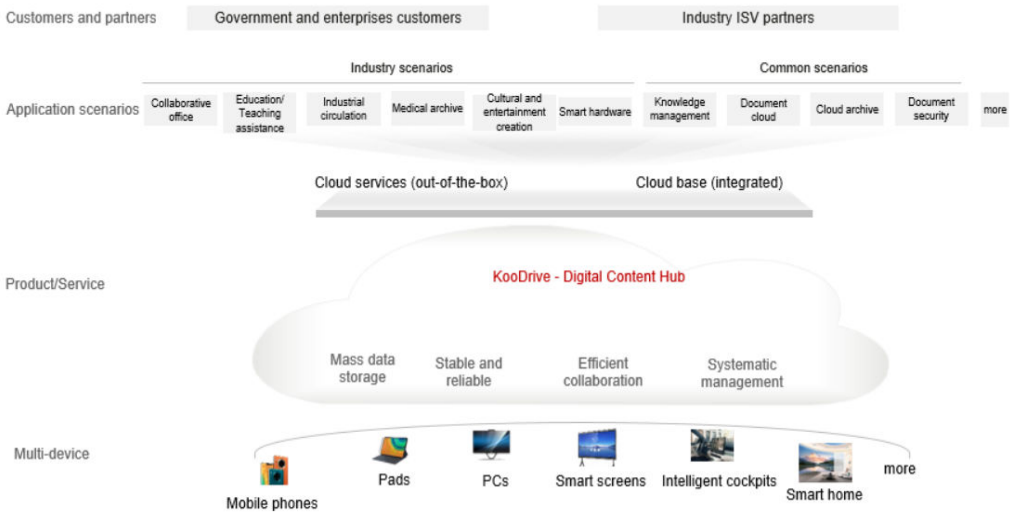
KooDrive is an online service provided by Huawei Cloud for government and enterprise customers. It provides functions such as data storage, access, synchronization, management, and collaboration. It is a one-stop digital content center for enterprises and enables efficient knowledge collaboration.

KooDrive fully utilizes the cloud-cloud synergy advantages of Huawei Cloud and covers multiple terminals to meet digital content storage and collaboration requirements in various application scenarios.

Architecture

Figure 1-1 shows KooDrive architecture.

Figure 1-1 Architecture



Access Mode

KooDrive provides a web-based service management platform. Tenants can access KooDrive through the management console, and users can access KooDrive through web or APIs.

- Using APIs

  If you need to integrate KooDrive into a third-party system for secondary development, access KooDrive using APIs. For details, see the ***API Reference***.

- Web-based console

  Operations other than the secondary development can be performed on the KooDrive console.

If you have registered a Huawei account and subscribed to Huawei Cloud, you can log in to the **console** and select or search for KooDrive on the homepage to access. If you have not registered, register a Huawei account and perform real-name authentication. To register and authenticate an account, perform the following steps:

1. Open the **Huawei Cloud official website**.
2. Click **Sign Up** in the upper right corner and complete the registration as prompt.
3. For details about real-name authentication, see **Enterprise Real-Name Authentication**.

2 Product Advantages

- Mass Storage

  PB-level massive data storage, on-demand scale-out, and file backup are not restricted by offline physical capacity.

- Reliability

  The data durability is up to 12 nines, and the service reliability is 99.99%. The one-stop digital content center of organizations and individuals is protected, enabling more efficient content collaboration in thousands of industries.

- Efficient collaboration

  Supports multi-person, multi-region, and multi-terminal collaboration and mobile office, allowing users to access the latest files at any time, improving collaboration efficiency.

- Systematic warning management

  Supports space and file management based on the enterprise organizational structure, and supports team and personal space.

3 Application Scenarios

- Scenario 1: File Storage and Backup

  Files stored locally are scattered by multiple persons and devices, and digital assets are scattered, disordered, and easy to lose. As digital assets accumulate over time, local storage space cannot meet storage requirements, and self-construction and maintenance costs are high. There is no file management capability that matches the enterprise architecture.

  KooDrive supports centralized storage and management of massive enterprise files, preventing risks caused by file disorder, such as leakage, damage, and loss of important data. KooDrive also supports on-demand scale-out to solve the problem of insufficient local space and does not require self-maintenance. Supports systematic space and file management by enterprise organization and member, and supports team and personal space.

- Scenario 2: Enterprise Team Collaboration

  KooDrive is centered on the file management system and covers multiple collaboration scenarios, improving collaboration efficiency.

  Multi-person collaboration: Multiple teams and multiple persons in a team can access and perform operations at the same time, improving enterprise collaboration efficiency.

  Multi-region collaboration: Cross-region remote office breaks regional collaboration restrictions and implements online file collaboration.

  Multi-terminal collaboration: Supports access from multiple terminals at any time, real-time synchronization between multiple terminals, and mobile office.

4 Functions

The KooDrive service provides enterprise users with enterprise office file services such as file storage and management and collaboration, building a one-stop cloud space for enterprises.

KooDrive provides the functions described in **Table 4-1**.

Table 4-1 KooDrive functions

Function	Description	Region Availability
Organization management	Allows users to create, modify, and delete enterprise departments.	AP-Singapore
User management	Users can be added, modified, disabled, enabled, and deleted.	AP-Singapore
Workspace management	Allows users to manage team spaces and personal spaces, including allocating, modifying, disabling, enabling, and deleting spaces.	AP-Singapore
File storage and management	Allows users to create folders, copy files, view file details, rename, move, dump, search for folders, add folders to favorites, delete folders, permanently delete folders, and restore folders.	AP-Singapore
File transmission	Supports file upload and download. Large files can be uploaded and downloaded through the fragmentation mechanism.	AP-Singapore
File storage	Users can view image thumbnails online.	AP-Singapore
File Sharing and collaboration	Allows enterprise users to share files or folders, and view, download, and save shared files or folders.	AP-Singapore

Function	Description	Region Availability
Tool Center	Manages user groups, including creating, modifying, and deleting groups, and adding and removing group members.	AP-Singapore
Recycle bin management	Files (folders) in the personal recycle bin and team recycle bin can be managed. including restoring and permanently deleting files or folders in the recycle bin and clearing the recycle bin.	AP-Singapore
Open APIs	Opens interfaces for department management, user management, and space management for third parties to perform secondary development.	AP-Singapore

5 Security

5.1 Shared Responsibilities

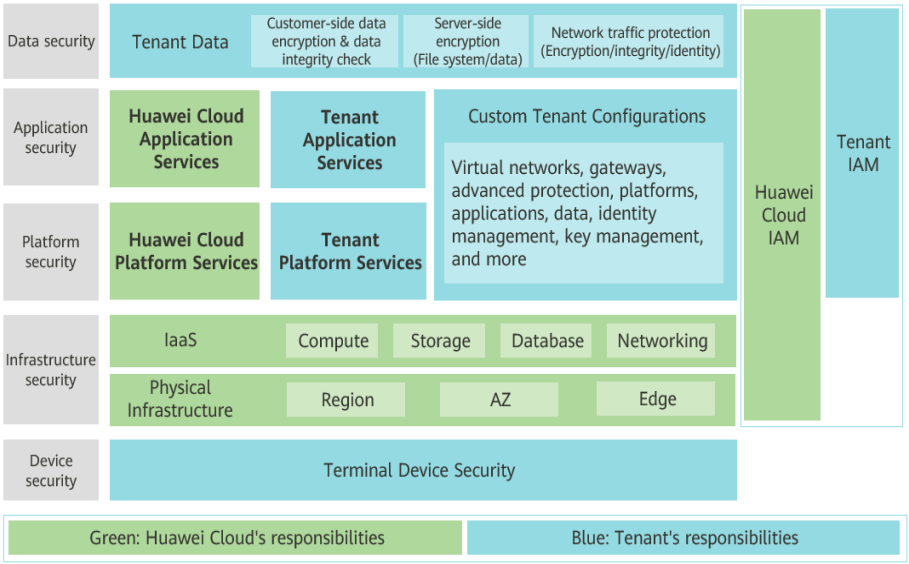
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 5-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide 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 and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 5-1 Huawei Cloud shared security responsibility model



5.2 Authentication and Access Control

Identity Authentication

KooDrive provides two identity authentication login modes. Unauthorized users cannot access KooDrive.

- The tenant administrator can use the Huawei Cloud IAM account and password to log in to the KooDrive console. After the login is successful, the tenant administrator can use the IAM token for authentication. For details about tokens and how to obtain tokens, see **Obtaining a User Token Through Password Authentication**.
- Tenant administrators, department administrators, and common users can use the OrgID account and password to log in to the KooDrive service. After the login is successful, the token generated by the KooDrive service control service is used for authentication.

ACL

- Tenant administrators can set access permissions for employees, set service administrator roles, and add administrators.
- Common users can use the KooDrive service only with the permissions set by the tenant administrator and department administrator.

  For details, see **Permissions Management**.

5.3 Data Protection Controls

KooDrive uses multiple methods and features to ensure data security and reliability when users use KooDrive.

Table 5-1 KooDrive data protection methods and features

Measure	Description
Transmission encryption (HTTPS)	To ensure data transmission security, all interfaces provided by KooDrive use HTTPS (TLS1.2/SSL3.3).
Data storage	Key service data created by users is encrypted for storage. Different tenants use separate DEKs.
Sensitive data protection	The log, diagnostics, debug, and alarm information does not contain sensitive data. Sensitive data is transmitted only through secure channels or after being encrypted.
DR and data protection	Multiple real-time data disaster recovery modes.

5.4 Audit and Logs

Audit

Cloud Trace Service (CTS) is a professional log audit service in Huawei Cloud security solutions. It can record, store and search operation records on the cloud resources in your account to perform security analysis, audit compliance, track resource, and locate faults.

After CTS is enabled, traces can be generated for operations performed on the KooDrive console.

- For details about CTS how to enable and configure CTS, see **Getting Started with CTS**.
- CTS can track KooDrive management traces. For details, see **Auditing**.
- When you enable CTS, the system starts recording operations on KooDrive. You can view operations of the past seven days on the CTS console. For details, see **Querying Real-Time Traces**.

Logs

The KooDrive console provides enterprise tenants with services such as subscribing to (enabling and changing), freezing, and unsubscribing from the KooDrive cloud service. The log system of the KooDrive console is interconnected with the Log Tank Service (LTS) of Huawei Cloud. LTS provides one-stop log collection, log search in seconds, massive log storage, log structuring and transfer. Graphical application O&M, visual analysis of network logs, graded protection compliance, and operation analysis make organization tracking easier.

After you enable LTS, LTS can record operation logs on the KooDrive management side.

- For details about LTS how to enable and configure LTS, see **Getting Started with LTS**.

- When you enable LTS, the system starts recording operations on KooDrive. On the LTS console, click **Log Management** to view the logs reported in real time. (Logs are reported every about 1 minute. In the log message area, you can view the logs reported in real time after waiting for about 1 minute.)

KooDrive records logs about tenant resource access. Customers can use the log management tool provided by WiseCloud to query logs generated in a specified period, analyze the logs, and analyze the access to related service resources in detail.

5.5 Resilience

KooDrive provides a three-level reliability architecture and uses dual-AZ DR, intra-AZ cluster DR, and data DR technologies to ensure service durability and reliability.

Table 5-2 KooDrive reliability architecture

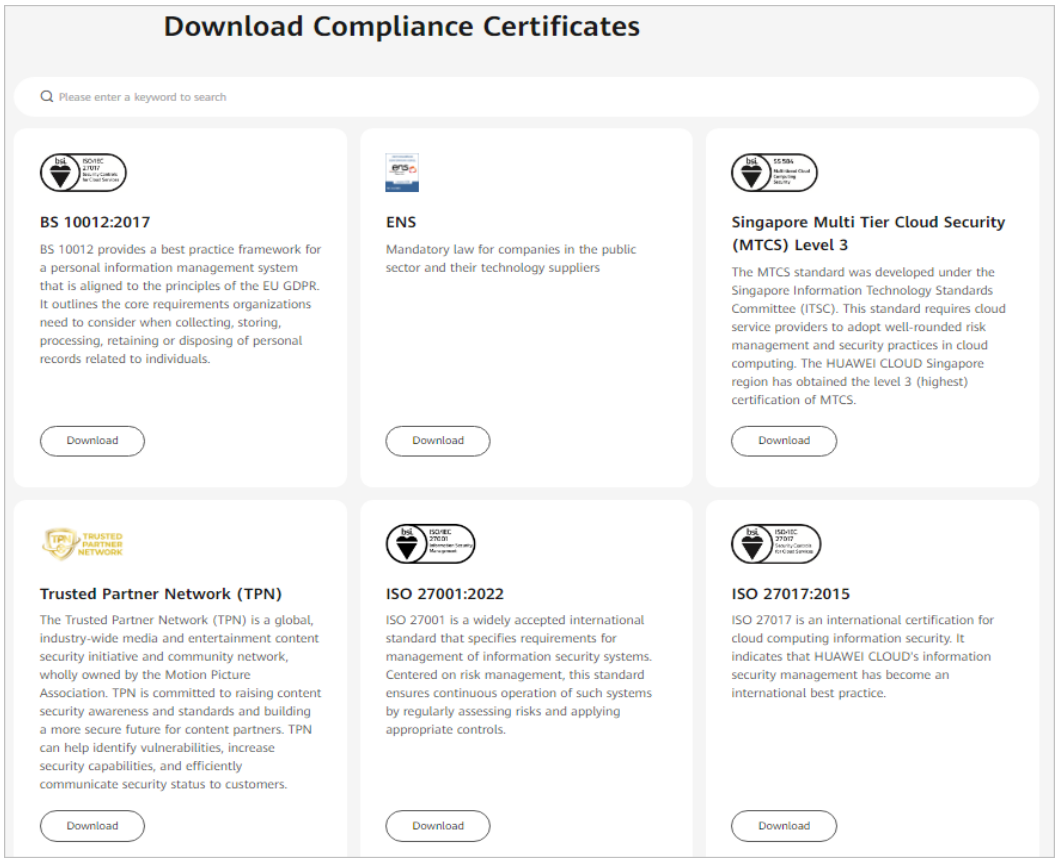
Reliability Solution	Description
Dual-AZ DR	KooDrive implements two AZs in active-active mode. When one AZ is abnormal, cloud services can still provide services.
Intra-AZ cluster DR	KooDrive provides services through clusters. Each microservice in a cluster has multiple instances. When one or some instances are abnormal, other instances can continuously provide services.
Data DR	KooDrive data is stored in RDS and DCS. RDS and DCS implement the AZ DR solution. Data is continuously synchronized to the DR site. When the RDS at the production site is faulty, the DR site can take over services, ensures continuous running of cloud services.

5.6 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can **download** them from the console.

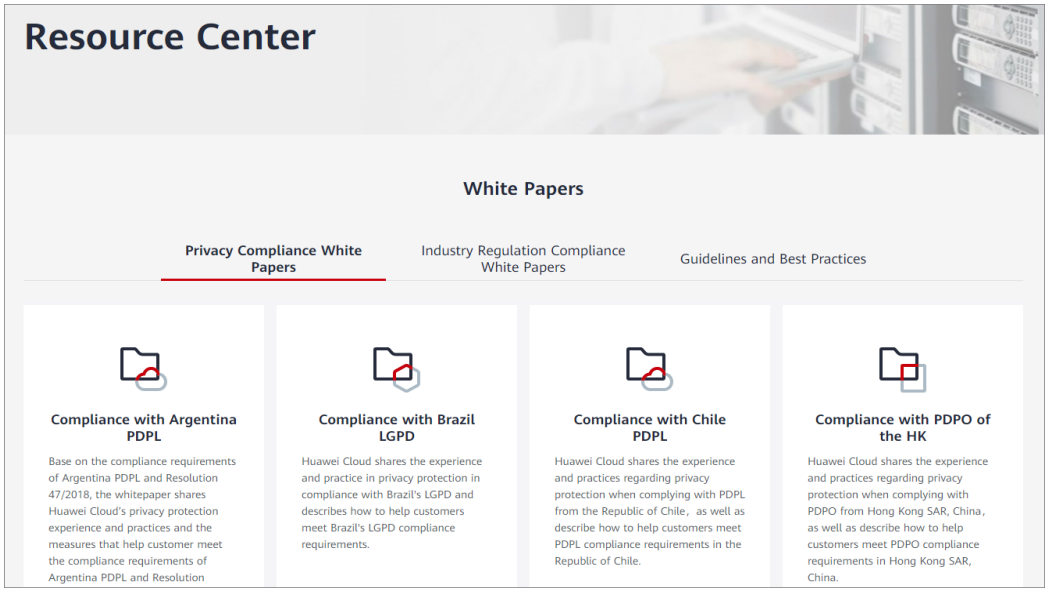
Figure 5-2 Downloading compliance certificates



Resource Center

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

Figure 5-3 Resource center



6 Permissions Management

If you need to set different access permissions for employees in an enterprise to isolate permissions of different employees, you can set different authorization policies when creating or modifying departments or individual cloud space in KooDrive. KooDrive provides identity authentication, permissions management, and access control, helping you efficiently manage access to your cloud resources.

With the business control service, you can create KooDrive accounts for employees and authorize employees to control their access to resources. For example, if your employee is a department administrator and you want the employee to have all permissions on the department space, such as uploading files to, downloading files from, and deleting files from the team space, you can set the role of the employee to department administrator. For another example, if your employee is a common user of a department and you want the employee to view files in the department space but not to perform other operations, such as deleting files, you can set the role of the employee to a common user.

For an individual space, the owner has all the permissions on the space.

KooDrive Permissions

An enterprise tenant who enables KooDrive on the Huawei Cloud console uses a Huawei Cloud account. After the KooDrive service is enabled, KooDrive creates a system administrator account using the Huawei Cloud account. After the account is used to log in to the KooDrive service application, organizations (departments and users) and space management can be performed. After a user is created by the system administrator, the user needs to be assigned a role so that the user can obtain the corresponding permission. This process is called authorization. After authorization, the user can perform operations on KooDrive resources based on the granted permissions.

KooDrive uses the role-based access control policy for permission management. Permissions are associated with roles. Users can obtain the permissions assigned to a role by becoming members of the role. Currently, KooDrive presets three system roles: system administrator, department administrator, and common user. For details about the permissions assigned to each role, see **Table 6-1**. Currently, roles cannot be customized.

Table 6-1 KooDrive system-defined roles

Role Name	Permissions Assigned	Role Type
System administrator	The system administrator can perform operations on all KooDrive resources except the files in the personal space of other users. The detailed permission list is as follows: 1. Organization management: Creates, queries, modifies, and deletes all departments in an organization. 2. User management: Creates, queries, modifies, and deletes users in all departments of an organization. 3. Space management: Creates, queries, modifies, and deletes all departments or individual spaces in an organization. 4. Team space: Has all permissions over the files in all department space of the organization, such as creating files/directories, and copying and deleting files. 5. Individual space: Operates the files in the individual space. 6. Recycle bin: Has the permission to operate the personal recycle bin and all team recycle bins.	System-defined role

Role Name	Permissions Assigned	Role Type
Department administrator	Department administrator. Users with this permission can perform operations in their own departments, such as managing department spaces and personal spaces of department members. The detailed permission list is as follows: 1. Organization management: Queries the list and information of all departments under the organization. 2. User management: Manages all users in the department, such as querying users and their details, and adding, deleting, and disabling users. 3. Space management: Queries all department space of the organization and individual space of member in the current department, and allocates, modifies, disables, enables, and deletes the current department space and individual space of members in the current department. 4. Team space: Has all permissions over the files in all department space of the organization, such as creating files/directories, and copying and deleting files. 5. Individual space: Operates the files in the individual space. 6. Recycle bin: Has all permissions over the individual and team recycle bins.	System-defined role
Common user	Common users have all operation permissions on files in their individual spaces and restricted operation permissions on their department spaces. The detailed permission list is as follows: 1. Individual space: Operates the files in the individual space. 2. Team space: Has all the permissions (excluding deletion) over the files in the team space. 3. Recycle bin: Has all permissions over the individual recycle bin but does not have permissions over the team recycle bin.	System-defined role

7 Constraints

When a Huawei Cloud account is restricted or frozen or cloud space resources enter the retention period, the use of KooDrive cloud space will be restricted (including but not limited to user sign-in, organization management, and file management). Users must understand and handle the restrictions in advance to avoid impact on services.

8 Change History

Release Date	Change History
2024-07-30	This issue is the first official release.

