Koo Command Line Interface

Service Overview

Issue	01
Date	2022-01-14

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI 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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Privacy Statement....... 1

2 What Is KooCLI?....... 2

3 KooCLI Concepts....... 3

4 Using KooCLI....... 5

5 Security....... 6

5.1 Shared Responsibilities....... 6

5.2 Identity Authentication and Access Control....... 7

5.3 Data Protection....... 8

5.4 Audit and Logs....... 8

5.5 Update Management....... 8

5.6 Certificates....... 8

5.7 Risk Prevention....... 10

1 Privacy Statement

See **Privacy Statement**.

When using Koo Command Line Interface (KooCLI) 3.2.8 or later for the first time, confirm whether to connect it to the Internet and whether to accept the *Privacy Statement*.

In some special scenarios such as KooCLI command execution with automation scripts, run the following command to agree to the privacy statement:

```
hcloud configure set --cli-agree-privacy-statement=true
```

2 What Is KooCLI?

KooCLI, previously named "HCloud CLI", is a command line tool for managing cloud service APIs released on API Explorer. With this tool, you can call open APIs of cloud services to manage and use your cloud service resources.

KooCLI provides a method for calling cloud service APIs through CLI. Before using KooCLI, you need to understand the target APIs. To get help using APIs, contact on-call personnel of the relevant cloud service.

When using KooCLI, you can search for APIs, debug them, and view their documentation on **API Explorer**.

KooCLI is flexible and easy to expand. It has the following features:

- Single executable file, which does not need installation. It can be used right after download and decompression.
- Compatibility with multiple OSs, including Linux, Windows, and macOS.
- High scalability. You can use this tool to encapsulate cloud service APIs for different functions and manage your resources with scripts.

NOTE

For details about how to download KooCLI, see **Getting Started**.

You can also **try out KooCLI** on API Explorer.

NOTICE

When using KooCLI in Windows, do not double-click the **hcloud.exe** file. Instead, go to the directory where this file is located, open a command line tool (such as **cmd.exe**), and then run desired commands.

3 KooCLI Concepts

This topic describes common terms related to KooCLI.

- Command

  Commands are operation instructions provided by KooCLI to configure the working environment or call open APIs of cloud services.

  The format of an API calling command is as follows:

  hcloud [options] <service> <operation> [--param1=paramValue1 --param2=paramValue2 ...]

  The format of a system command is as follows:

  hcloud [options] <systemCommand> <operation> [--param1=paramValue1 --param2=paramValue2 ...]

  In the following command for querying Elastic Cloud Servers (ECSs), *service* is **ECS**, *operation* is **NovaListServers**, and the common information required for calling the API is obtained from the **profile** named **default**:

  ```
  hcloud ECS NovaListServers --cli-profile=default
  ```

- Operation

  A unique name for a cloud service API released on API Explorer. You can query the operation list of a cloud service by using **API Explorer** or by running the **hcloud** *<service>* **--help** command.

- Profile

  Profiles store common information required for calling cloud service APIs. They can be defined by running KooCLI commands. All profiles constitute a configuration file, which is stored on your local host. When calling a cloud service API, you can specify a profile rather than manually inputting the common information.

  The common information that can be set in a profile includes the access key (**AK/SK**), region (**cli-region**), project ID (**cli-project-id**), and account ID (**cli-domain-id**).

- Default profile

  The profile to be used by default if no profile is specified in a command. KooCLI takes the profile that is last added or modified as the default. If the default profile is deleted, the earliest added profile among the remaining ones is used as the new default. You can run the **hcloud configure set --cli-profile=***${profileName}* command to change the default profile.

- Parameter

  Parameters are classified into API parameters and KooCLI system parameters. API parameters are defined in cloud service APIs. System parameters are built-in parameters of KooCLI. The system parameters are used in a fixed mode and have specific meanings. For details, see the **system parameter list**.

- Option

  Options are KooCLI system parameters that can be directly added to commands for calling APIs. Not all system parameters can be used as options. For details, see the **option list**.

- Metadata

  Details about cloud services and their APIs that are obtained by KooCLI during command execution to verify and parse parameters. Remotely obtained metadata is stored locally to reduce network I/O and improve command response. A file that stores metadata is called a metadata cache file. For details, see **Managing Metadata**.

  When using the **offline mode**, KooCLI downloads existing metadata, which is called an "offline metadata package".

4 Using KooCLI

Step 1 Download KooCLI.

KooCLI is installation-free and can be used right after download and decompression. It can work with Windows 64-bit, Linux AMD64, Linux Arm64, macOS AMD64, and macOS Arm64. **Download** the corresponding version based on the OS you use.

Step 2 Configure KooCLI.

For details, see **Initialize Configurations**.

Step 3 Obtain the commands for calling cloud service APIs.

There are two ways:

- (Recommended) From API Explorer

  View cloud service APIs on **API Explorer**, and enter the required parameters. Then obtain the example command from the **CLI Example** tab page.

- From KooCLI documentation

  To learn how to query cloud service commands, see **View and Run Cloud Service Operation Commands**. The methods of viewing commands in macOS and Linux are similar.

Step 4 Call cloud service APIs by using KooCLI.

Enter a complete API calling command and press **Enter**.

Step 5 (Optional) Integrate KooCLI commands into your custom scripts for automatic management of cloud service resources.

----End

5 Security

5.1 Shared Responsibilities

5.2 Identity Authentication and Access Control

5.3 Data Protection

5.4 Audit and Logs

5.5 Update Management

5.6 Certificates

5.7 Risk Prevention

5.1 Shared Responsibilities

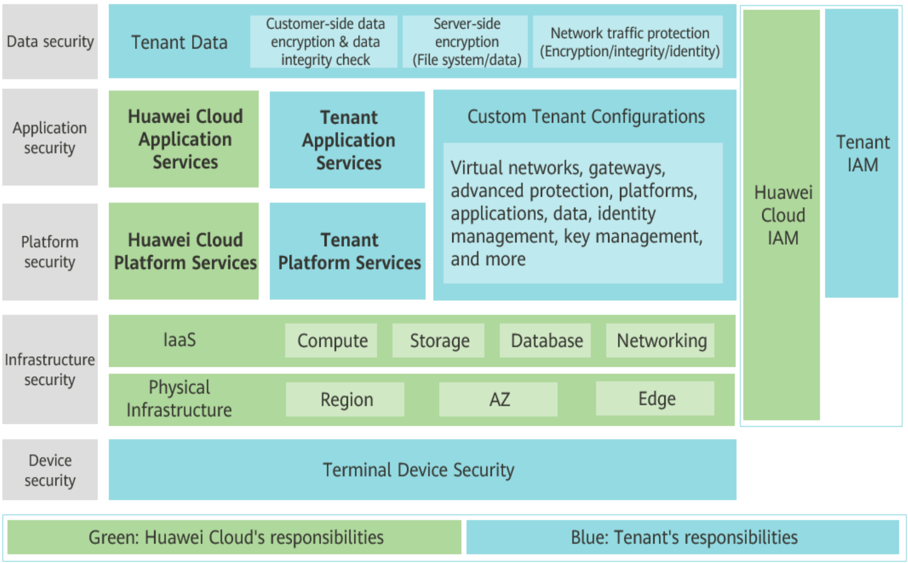
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system 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


Data security
Tenant Data
Customer-side data encryption & data integrity check
Server-side encryption (File system/data)
Network traffic protection (Encryption/integrity/identity)
Application security
Huawei Cloud Application Services
Tenant Application Services
Custom Tenant Configurations
Virtual networks, gateways, advanced protection, platforms, applications, data, identity management, key management, and more
Platform security
Huawei Cloud Platform Services
Tenant Platform Services
Infrastructure security
IaaS
Compute
Storage
Database
Networking
Physical Infrastructure
Region
AZ
Edge
Device security
Terminal Device Security
Huawei Cloud IAM
Tenant IAM
Green: Huawei Cloud's responsibilities
Blue: Tenant's responsibilities

5.2 Identity Authentication and Access Control

KooCLI calls Huawei Cloud's open APIs using API Gateway (APIG). The identity authentication and access control on KooCLI is consistent with that of these open APIs.

Identity Authentication

KooCLI provides two API calling modes: with or without identity authentication. Only APIs that involve identity authentication require IAM identity credentials during calling.

Access Control

- Access control on resources

  Your permissions for debugging and managing resources with KooCLI are the same as those for doing this with SDKs. Your access to specific resources on Huawei Cloud is also consistent with that on the relevant service console.

- Access control on configuration files and run logs

  KooCLI runs on your local PC, so all configuration files and run logs of KooCLI are stored locally. You can control access to these files as required.

5.3 Data Protection

Encrypted Transmission (HTTPS)

KooCLI communicates with APIG through HTTPS, which prevents data tampering and keeps your data secure. As for the encryption protocols, TLS 1.2 and TLS 1.3 are used because they are considered more secure than others.

Sensitive Data Protection

Both your authentication credentials (AK/SK) configured in KooCLI and custom variables can be encrypted for storage. KooCLI dynamically generates an encryption key when you use it for the first time. This ensures that each user can only use their encryption key to decrypt their own data.

When you query sensitive data with commands, the data is anonymized for display to prevent leakage.

For details, see **Adding or Modifying a Profile**.

5.4 Audit and Logs

The logs of KooCLI can be used for auditing. You need to control access to these logs to prevent tampering. Similar to SDKs, KooCLI parses your commands into HTTPS requests and sends the requests to APIG. The related information recorded by APIG can also be used for auditing.

For details, see **Managing Logs**.

5.5 Update Management

Update of Open-Source Third-Party Software

Built with a trustworthy pipeline, KooCLI has a complete management process for open-source third-party software. The process ensures that the open-source third-party software used in each version does not involve high-risk vulnerabilities.

High-Risk Vulnerability Fixing

If high-risk vulnerabilities are disclosed for involved software, a fixed KooCLI version will be provided for download and update.

For details, see **Upgrading the Version**.

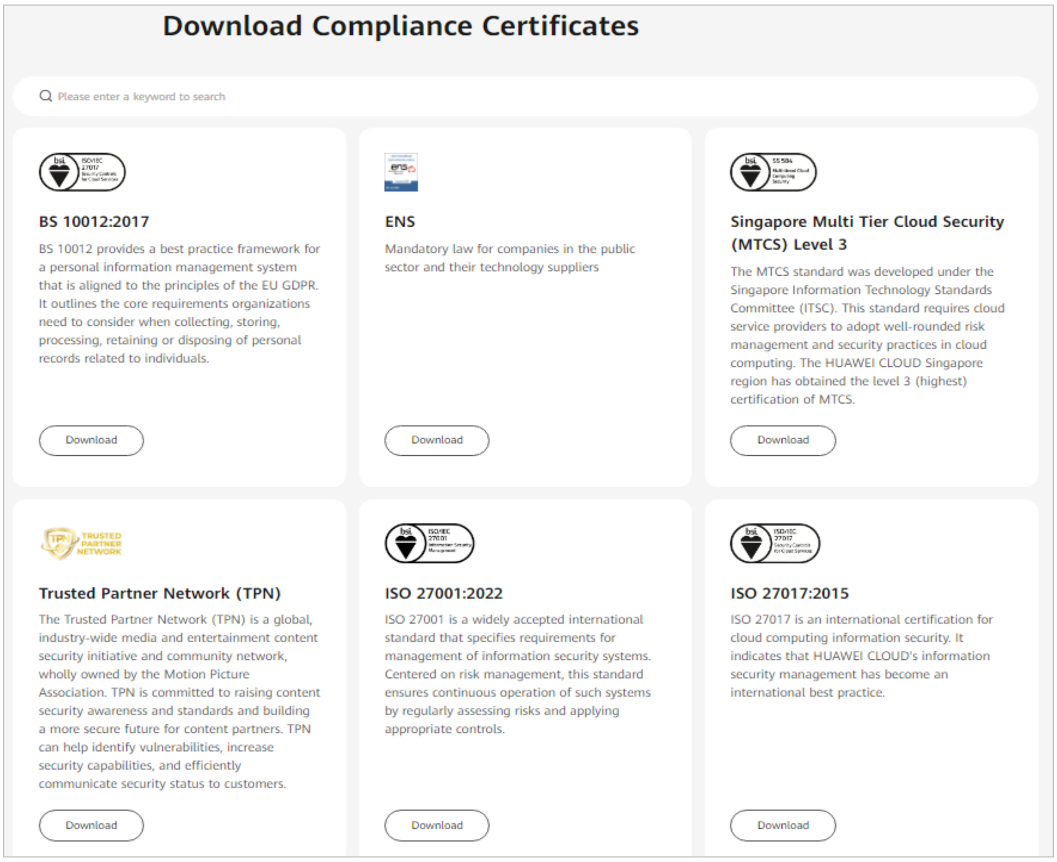
5.6 Certificates

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



Download Compliance Certificates

BS 10012:2017

BS 10012 provides a best practice framework for a personal information management system that is aligned to the principles of the EU GDPR. It outlines the core requirements organizations need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals.

ENS

Mandatory law for companies in the public sector and their technology suppliers

Singapore Multi Tier Cloud Security (MTCS) Level 3

The MTCS standard was developed under the Singapore Information Technology Standards Committee (ITSC). This standard requires cloud service providers to adopt well-rounded risk management and security practices in cloud computing. The HUAWEI CLOUD Singapore region has obtained the level 3 (highest) certification of MTCS.

Trusted Partner Network (TPN)

The Trusted Partner Network (TPN) is a global, industry-wide media and entertainment content security initiative and community network, wholly owned by the Motion Picture Association. TPN is committed to raising content security awareness and standards and building a more secure future for content partners. TPN can help identify vulnerabilities, increase security capabilities, and efficiently communicate security status to customers.

ISO 27001:2022

ISO 27001 is a widely accepted international standard that specifies requirements for management of information security systems. Centered on risk management, this standard ensures continuous operation of such systems by regularly assessing risks and applying appropriate controls.

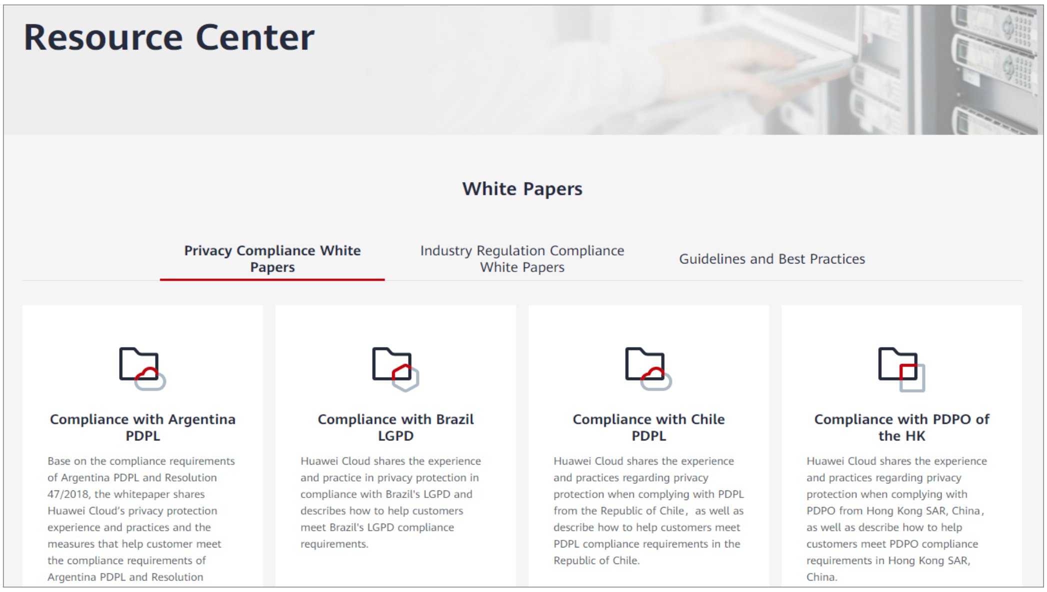
ISO 27017:2015

ISO 27017 is an international certification for cloud computing information security. It indicates that HUAWEI CLOUD's information security management has become an international best practice.

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



Resource Center

White Papers

Privacy Compliance White Papers
Industry Regulation Compliance White Papers
Guidelines and Best Practices

Compliance with Argentina PDPL

Base on the compliance requirements of Argentina PDPL and Resolution 47/2018, the whitepaper shares Huawei Cloud's privacy protection experience and practices and the measures that help customer meet the compliance requirements of Argentina PDPL and Resolution

Compliance with Brazil LGPD

Huawei Cloud shares the experience and practice in privacy protection in compliance with Brazil's LGPD and describes how to help customers meet Brazil's LGPD compliance requirements.

Compliance with Chile PDPL

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPL from the Republic of Chile，as well as describe how to help customers meet PDPL compliance requirements in the Republic of Chile.

Compliance with PDPO of the HK

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPO from Hong Kong SAR, China，as well as describe how to help customers meet PDPO compliance requirements in Hong Kong SAR, China.

5.7 Risk Prevention

You are strongly recommended to:

- Configure proper file system permissions on the **.hcloud** directory and its subdirectories and files to limit access only to authorized users.
- Encrypt the values of sensitive variables to prevent information leakage.
- Use temporary authentication credentials whenever possible to reduce risks that may be caused by credential leakage.