CloudArtifact

Overview

Issue	02
Date	2022-11-14

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

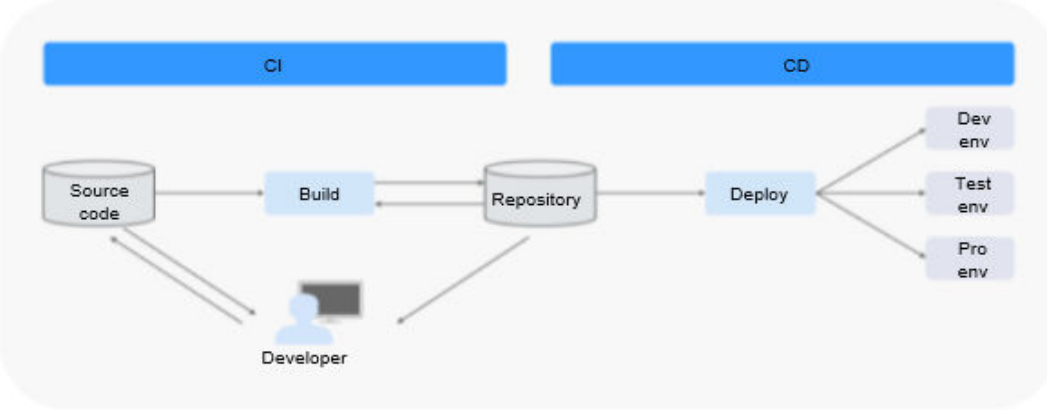
What Is CloudArtifact?

CloudArtifact helps software development enterprises manage the software release process in a standardized, visualized, and traceable way.

CloudArtifact focuses on and manages the staging **software packages** (usually built by or packed from the **source code**) and their lifecycle metadata. The metadata includes basic attributes such as the name and size, repository addresses, build tasks, creators, and build time.

The management of **software packages** and their attributes is the basis of release management. **Figure 1-1** shows the common software development process.

Figure 1-1 Software development process



Repository is a collection of software artifacts and is used to manage software packages generated during software development. It is an important link between continuous integration and delivery. Operations such as release review, tracing, and security control of software packages are usually performed in the repository.

This service provides the following two types of repositories:

- Release repo

  A release repo is a collection of software artifacts. It can store any software packages and tools in any formats.

Build artifacts can be archived to the release repo. You can view and manage the archived software packages and their lifecycle attributes. These software packages are used for deployment.

- Self-hosted repo

  A self-hosted repo manages private component packages (such as Maven) corresponding to various development languages.

  Different development language components have various requirements in the archive format (for example, the Maven component needs to be archived in GAV format). CloudArtifact manages private development language components and share them with other developers in an enterprise or team.

What Functions Does CloudArtifact Provide?

Table 1-1 Release repo functions

Function	Description
Managing software package	You can upload, download, search for, and delete software packages. Folders can also be created for better management.
Querying software package attributes	You can view the software package lifecycle attributes in the release repo. The lifecycle attributes include basic information (such as the name, size, and checksum), build information (such as the build task, build time, and source code repository).
Uploading software packages to the release repo using CloudBuild	The release repo integrates CloudBuild. Through configuration, all software packages generated by CloudBuild can be automatically uploaded to the release repo for archiving.
CloudDeploy	Software packages stored in the release repo can be used by CloudDeploy.
Package view and build view	You can view a software package in the package view (storage directory structure) or build view (build task and pipeline).

Table 1-2 Self-hosted repo functions

Function	Description
Managing private components	You can upload, download, delete, and search for private components.

Function	Description
Releasing components to the self-hosted repo using CloudBuild	In a build task, you can configure build artifacts to be directly released to the self-hosted repo.
Connecting the local development environment	You can generate a configuration file in one click. After the generated file is configured in the local development tool, you can directly connect the local development environment to the private component packages in the self-hosted repo. For example, you can use command lines to upload and download components in the self-hosted repo.
Repository access control	By setting user roles in repositories, administrator can restrict read and write permissions of users.
Accessing SWR	The self-hosted Docker repo uses SWR. You can view and manage private Docker images, and create and manage organizations that archive these images.

2 Security

2.1 Shared Responsibilities

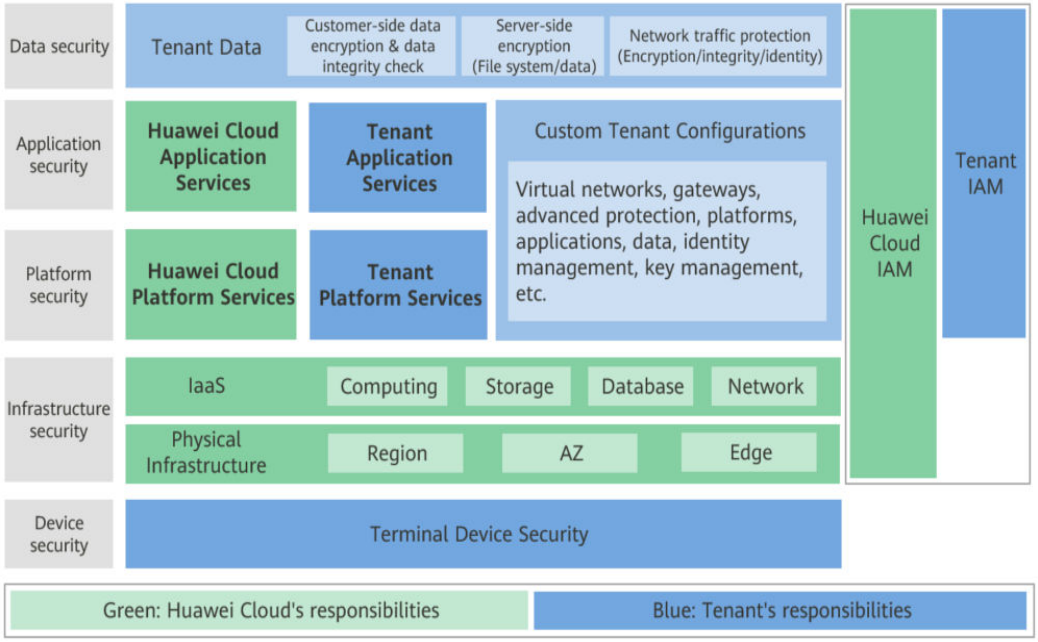
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 2-1 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 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 2-1 Huawei Cloud shared security responsibility model



2.2 Identity Authentication and Permission Management

Authentication

You can access CloudArtifact through the management console or APIs.

Before calling an API, you need to pass the Identity and Access Management (IAM) authentication and obtain the corresponding token to access the API.

Permission Management

CloudArtifact has the software release repo and self-hosted repo.

- Release repo: The permissions can be customized for each role in projects. For details, see **Setting Permissions**.
- Self-hosted repo: The permissions are determined by user roles and repository roles. User roles are essentially IAM permissions. To authorize IAM permissions, an administrator needs to create IAM users, add them to user groups, and assign policies or roles to the user groups. Users in the user groups also obtain the corresponding permissions. The repository role can be assigned by a user with the te_admin user role. For details, see **Managing User Permissions** in **Managing Self-Hosted Repos**. For details about fine-

grained permission management, see the permission list following **Managing User Permissions** in **Managing Self-Hosted Repos**.

2.3 Data Protection Technologies

CloudArtifact takes different methods and features to keep data secure and reliable.

Measure	Description
Transmission encryption (HTTPS)	CloudArtifact uses HTTPS to secure data transmission.
Personal data protection	CloudArtifact records operation logs to prevent personal data leakage and secure personal data.
Privacy protection	CloudArtifact encrypts sensitive data such as repository passwords before storing them.

2.4 Auditing

Cloud Trace Service (CTS) records operations on the cloud resources in your account. You can use the logs generated by CTS to perform security analysis, track resource changes, audit compliance, and locate faults. After you enable CTS and configure a tracker, CTS can record management and data traces of CloudArtifact for auditing.

For details about how to enable and configure CTS, see **Enabling CTS**.

2.5 Service Resilience

CloudArtifact uses multi-active stateless cross-AZ deployment and inter-AZ data disaster recovery (DR) to enable service processes to be quickly started and recovered if a fault occurs, ensuring service continuity and reliability.

2.6 Update Management

CloudArtifact interconnects with CCMS to manage service credentials, ensuring that plaintext valid credentials are not flushed to disks and are rotated periodically.

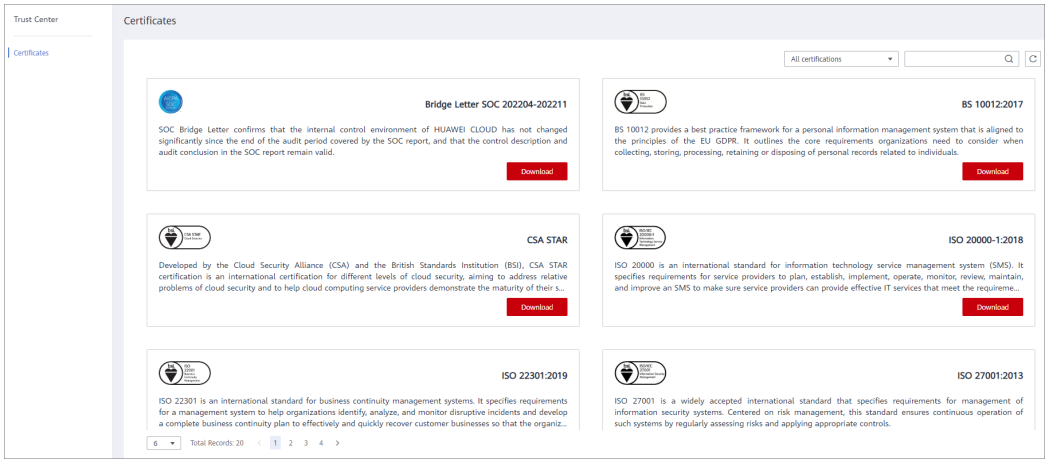
2.7 Certificates

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.

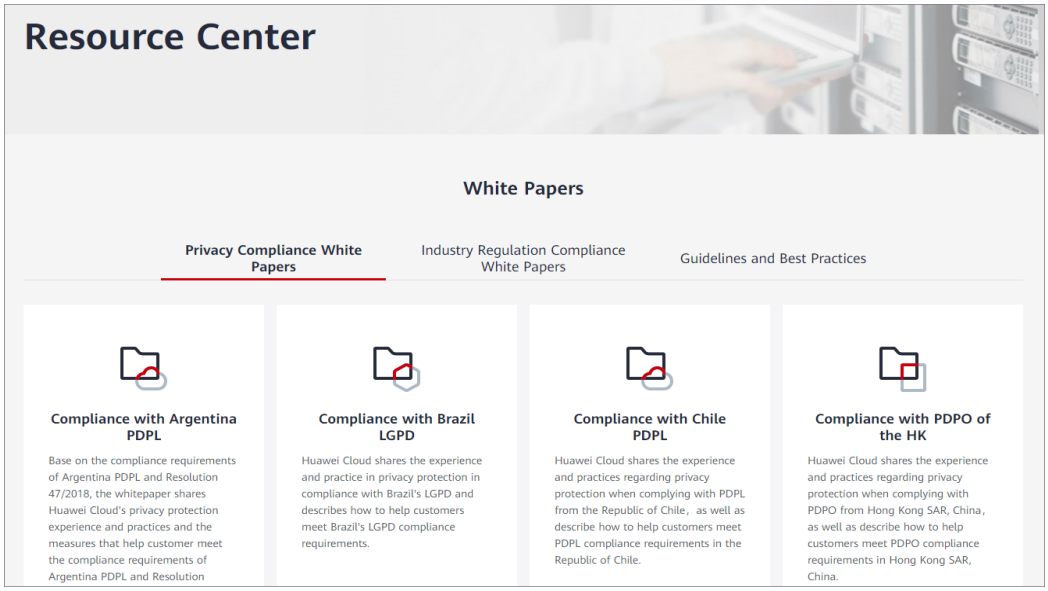
Figure 2-2 Downloading compliance certificates



Resource Center

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

Figure 2-3 Resource center



3 Constraints

Table 3-1 describes the constraints on CloudArtifact.

Table 3-1 Constraints

Category	Item	Limit
Browser	Type	The following browsers are supported: • Chrome: The latest three stable versions are supported and tested. • Firefox: The latest three stable versions are supported and tested. • Microsoft Edge: Windows 10 uses Microsoft Edge by default. The latest three stable versions are supported and tested. • Internet Explorer is no longer supported and tested. **Chrome and Firefox are recommended.**
Resolution	Resolution	(Recommended) 1280 x 1024 or higher
Constraints on a release repo	Maximum size of a file uploaded on the console	2 GB
	Maximum size of a file uploaded by a build task	1 GB
Constraints on a self-hosted repo	Total storage capacity	1 TB

Category	Item	Limit
	Maximum size of a file uploaded on the console	100 MB **NOTE** The maximum size of a file uploaded to the self-hosted repo is for non-Docker repositories. For details about quota for Docker repositories, see **SWR Quotas**.
	Maximum size of a file uploaded by a build task	300 MB
	Access control	The self-hosted repo manages private component packages. Repository types such as Maven, npm, Go, PyPI, and RPM are supported. You can access private components only after being granted permissions by the administrator.

