CodeArts Artifact

Service Overview

Issue	03
Date	2023-03-23

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.

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 What Is CodeArts Artifact?

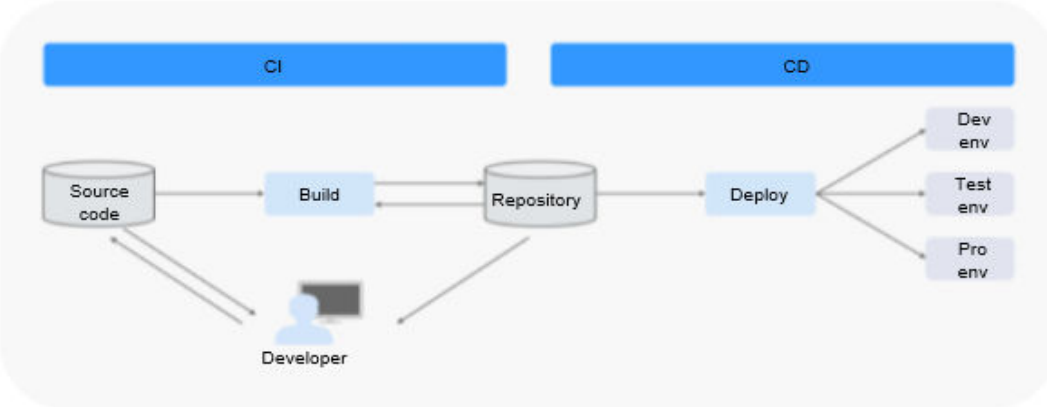
Service Overview

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

CodeArts Artifact 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.

CodeArts Artifact provides the following two types of repositories:

- Release repo

  A release repo 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 vary in the archive format (for example, the Maven component needs to be archived in **GAV** format). CodeArts Artifact manages private development language components and shares them with other developers in an enterprise or team.

What Functions Does CodeArts Artifact Provide?

Table 1-1 Release repo functions

Function	Description
Managing software packages	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 CodeArts Build	The release repo integrates CodeArts Build. Through configuration, all software packages generated by CodeArts Build can be automatically uploaded to the release repo for archiving.
CodeArts Deploy	Software packages stored in the release repo can be used by CodeArts Deploy.
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 CodeArts Build	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 operation permissions of users.

2 Product Advantages

Huawei Cloud CodeArts Artifact enriches artifact repository management in common languages by offering custom agent and virtual repositories, artifact lifecycle management, and efficient viewing and search. It will keep providing customers with comprehensive, efficient, and trusted artifact management.

Self-managed, Secure Artifact Repository with Optimal Performance for Service Continuity

CodeArts Artifact is developed based on the cloud native architecture to resolve service continuity issues caused by external uncontrollable factors. Huawei Cloud CodeArts Artifact has the following features:

– Security: CodeArts Artifact provides multi-dimensional and fine-grained permission control to meet access control requirements of different roles in an enterprise. It uses the cloud native architecture for physical isolation to reduce the risk of malicious artifact theft.

– Traceability: records user operations.

– Reliability: Huawei Cloud CodeArts Artifact supports dual-AZ DR and cross-region DR, API traffic limiting and degradation, service dependency and isolation, and automatic service fault detection. These features allow a 99.99% SLA.

– Ultimate Speed: CodeArts Artifact provides cache acceleration for popular files, incremental upload and download, and full use of cache acceleration advantages for large and small files to improve the build speed, break through the underlying storage bandwidth limit, and implement high-speed concurrent transmission in the same region. Compared with similar open source products, CodeArts Artifact upload performance is improved by 5 times and the download performance by 10 times.

Supporting over 10 Repo Types to Meet Various Needs

Huawei Cloud CodeArts Artifact supports more than 10 mainstream artifact types in Generic, Maven, npm, Go, PyPI, RPM, Debian, Conan, NuGet, and more, meeting the requirements of embedded, web, and mobile application development scenarios. It can seamlessly integrate with on-premises builds, deployment tools,

and CI/CD on the cloud. Huawei Cloud CodeArts Artifact also provides artifact and metadata integrity verification capabilities. It supports fine-grained control and version-based package locking permissions to ensure the integrity of software release tests and comprehensively protect enterprise artifact security.

Seamlessly Connecting to Third-party Repos and Providing a Unified Aggregated Repo Address, Improving User Experience and Download Performance

In scenarios where users use multiple image sources or artifact repositories at the same time, CodeArts Artifact provides repository aggregation, allows flexible combination of multiple agent repositories, and provides a unified Artifact homepage to allow users to easily find artifact packages and simplify configurations.

The support for custom agent repositories enables users to create agents for open-source repositories and third-party dependency repositories. After files are downloaded from the agent repositories, they can be cached to CodeArts Artifact, allowing downloading files from third-party dependencies as fast as from the local repositories.

Searching for Artifacts by File Name and Checksum and Precisely Locating Them Among Hundreds of Millions of Artifacts in Seconds

Huawei Cloud CodeArts Artifact has powerful search capabilities by using data engine. In a few seconds, you can search artifacts quickly from tens of billions of artifact files from multiple dimensions.

It covers multiple artifact types, such as Maven, npm, Go, PyPI, RPM, Debian, Conan and NuGet. You can search for and locate artifacts in seconds by file name or hash information (MD5, SHA1, SHA256, and SHA512). Based on this, CodeArts Artifact also supports efficient query associating hundreds of millions of metadata and SBOM to quickly trace artifact files. Compared with similar open-source products, CodeArts Artifact improves the search performance by 20 times.

3 Security

3.1 Shared Responsibilities

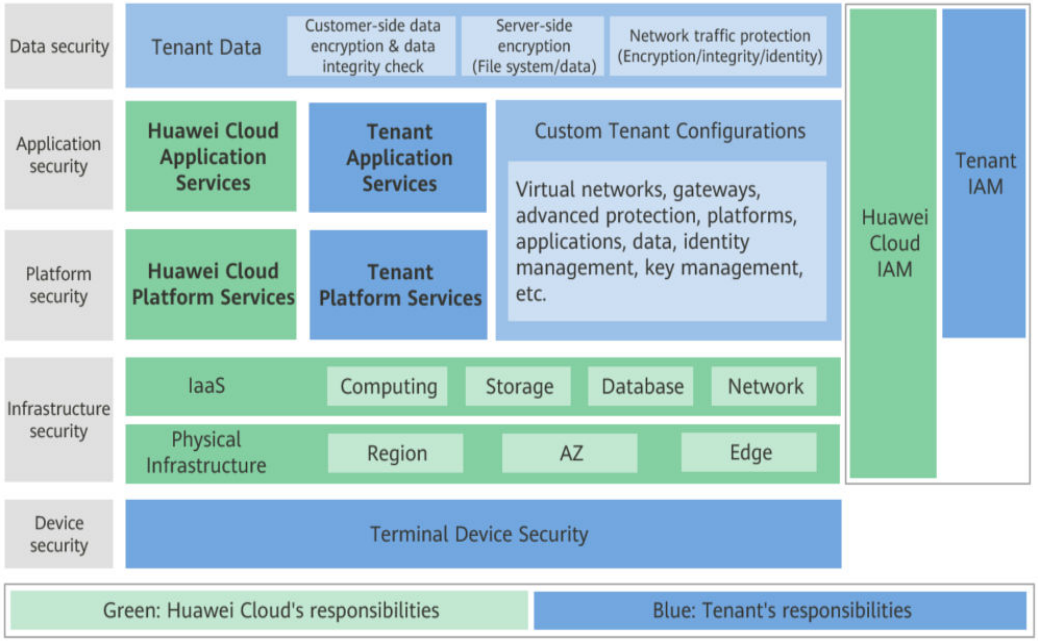
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 3-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Is responsible for providing secure cloud services. Huawei Cloud's security responsibilities include 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 3-1 Huawei Cloud shared security responsibility model



3.2 Identity Authentication and Permission Management

Authentication

You can access CodeArts Artifact 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

CodeArts Artifact has the 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 tenant administrator 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**.

3.3 Data Protection Technologies

CodeArts Artifact takes different methods and features to keep data secure and reliable.

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

3.4 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 Cloud Artifact for auditing.

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

3.5 Service Resilience

CodeArts Artifact 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.

3.6 Update Management

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

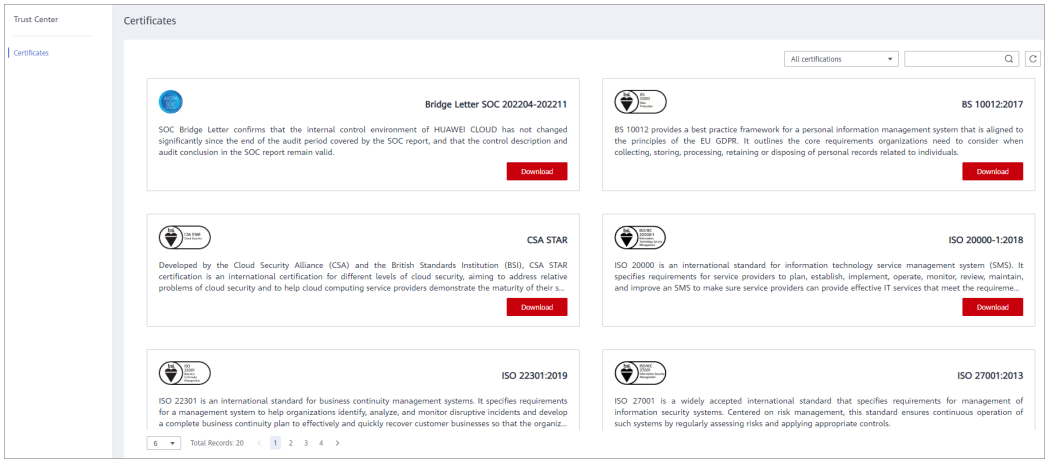
3.7 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International

Organization for Standardization (ISO), System and Organization Controls (SOC), and Payment Card Industry (PCI). You can **download** them from the console.

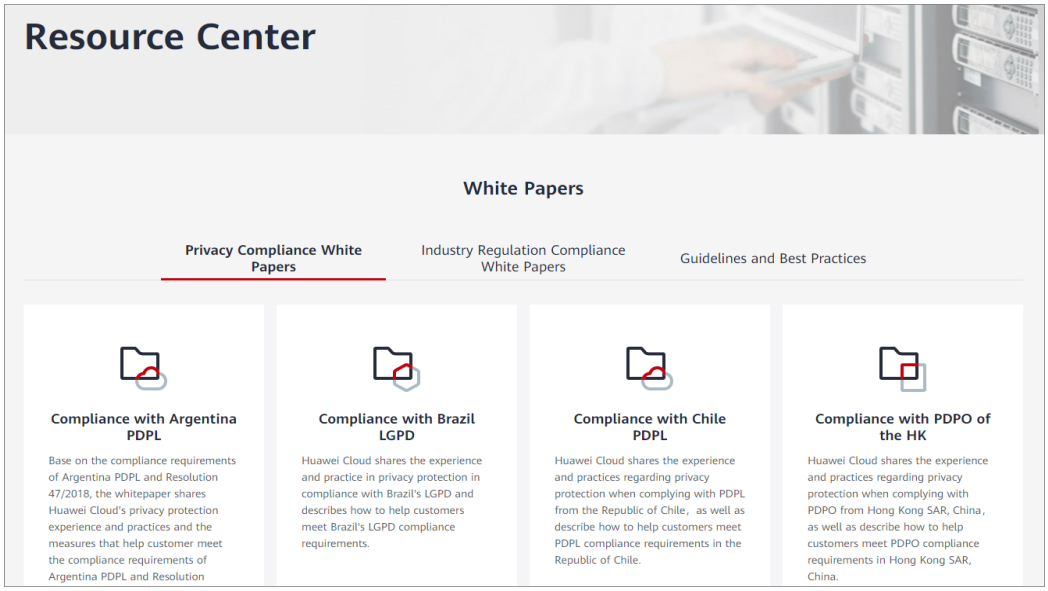
Figure 3-2 Downloading compliance certificates



Resource Center

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

Figure 3-3 Resource center



4 Constraints

Table 4-1 describes the constraints on CodeArts Artifact.

Table 4-1 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
Total storage capacity	Release repos and self-hosted repos	Total capacity: 10 GB
Total download capacity	Traffic of release repos and self-hosted repos	Total traffic: 5 GB/month
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	10 GB

Category	Item	Limit
Constraints on a self-hosted repo	Maximum size of a file uploaded on the console	Maven/npm/PyPI/Go/RPM/Debian/Conan: 100 MB NuGet: 20 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**.
	Repository quantity	• Max. 100 non-Maven repositories • Max. 50 pairs of Maven repositories
	Maximum size of a file uploaded by a build task	2 GB

NOTE

- For details about the specifications of different CodeArts packages, see **Specifications**.
- The current edition is CodeArts Free Edition.