CodeArts Pipeline

Service Overview

Issue	01
Date	2024-06-28

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 CodeArts Pipeline

CodeArts Pipeline allows you to visualize and orchestrate CI/CD (continuous integration and continuous delivery) pipelines. It helps enterprises realize continuous, efficient, and automated delivery, shortens the time to market (TTM) of applications, and improves R&D efficiency.

This service is a visualized and automated task scheduling platform. It needs to be used together with automated tasks of services such as CodeArts Build, CodeArts Check, CodeArts TestPlan, and CodeArts Deploy. You can orchestrate these automated tasks based on your requirements, such as application deployment in the development, test, or production environment. A single configuration triggers executions repeatedly to avoid inefficient manual operations.

CodeArts Pipeline provides the following functions:

- Allows you to add, delete, edit, and query pipeline jobs on the Web UI.
- Allows you to assign permissions to different accounts based on their roles.
- Allows you to manage and schedule jobs of building, code check, subpipeline, repositories, deployment, delayed executions, manual reviews, and API tests.
- Allows you to add, delete, and edit pipeline stages.
- Allows you to execute jobs in the same stage in series or parallel.
- Allows you to configure pipeline parameters.
- Allows you to execute specified jobs in a pipeline.
- Allows you to view pipeline execution records.
- Allows you to configure how a pipeline is executed, either triggered by an event (code commit, MR, tag creation) or at a specific time.
- Allows you to configure internal messages and email notifications for pipeline events.
- Allows you to customize extensions.
- Allows you to create rules and policies for pass conditions.
- Supports microservice-based lightweight changes in DevOps.
- Supports dependency analysis for open-source software and vulnerability interception.

Rules/Policies

CodeArts Pipeline allows you to manage pass conditions in pipeline stages through rules and policies. You can create extension-based rules, set the threshold comparison conditions, reference the conditions in policies, and apply them in pass conditions. A policy is a set of rules. You can manage policies by tenant or project.

Extensions

You can use built-in extensions or customize them for task orchestration.

Microservices

Microservices are a software governance architecture. A complex software project consists of one or more microservices. Microservices in the system are loosely coupled. Each microservice is independently developed, verified, deployed, and released. Microservices have the following benefits:

- Specialized: Each microservice focuses on a specific function. It is relatively easy to develop and maintain a single microservice.
- Independently deployable: A microservice is independently deployed and updated without affecting the whole system.
- Diversified technologies: For microservices architectures, different services communicate over RESTful APIs. You can choose the desired technology for each service.

Changes

Changes can be used to meet requirements and fix vulnerabilities. A change belongs to only one microservice.

A change's lifecycle includes developing, to be released, releasing, and released. You can create a change-triggered pipeline to release one or more changes for quick delivery. You can set pass conditions and manual review task to control the quality of changes.

CodeArts Release

CodeArts Release is an E2E solution provided by CodeArts for automated rollout and continuous version delivery. Version compatibility and version quality source tracing ensure version quality. Collaborative release approval and release decision-making ensure the standardization of the release process.

Features:

- Provides solution-oriented baseline management capabilities, supports multi-dimensional version orchestration at the microservice, module, and product levels, and supports multi-cloud version mapping.
- Provides cloud-native microservice release management capabilities, supports gray orchestration and release of microservices, supports blue-green and canary gray release, and implements cross-cloud orchestration based on UCS.

2 Functions

The following table describes the main functions of CodeArts Pipeline.

Function	Description
Orchestrating pipelines	You can manage and schedule jobs of building, code check, subpipeline, repositories, deployment, delayed execution, manual review, and API test.
Adding, deleting, editing, and querying pipelines	You can create, edit, delete pipelines and query execution status on the Web UI. You can go to the job details page to view its logs.
Managing permissions	You can configure project-level permissions for each role. You can configure permissions for each role and user in a pipeline to allow them to view, edit, execute, and delete the pipeline.
Viewing pipeline execution records	You can view the pipeline records in past 31 days.
Configuring notifications	You can configure whether to send internal messages and emails for pipeline events.
Executing specific jobs	You can execute specific jobs in a pipeline.
Configuring parameters	You can add custom parameters and set a value for the parameter when executing a pipeline, so that the job can use the value for execution.
Executing jobs in serial or parallel mode	You can execute jobs in a stage in serial or parallel mode as needed.

The following table describes the main functions of policies.

Function	Description
Managing policies	You can manage policies at the tenant and project levels.
Customizing rules	You can customize rules based on extensions.
Using policies	You can use policies as pass conditions during task orchestration.
Copying policies	You can quickly create a policy by copying a tenant-level or project-level policy. In addition, you can copy a tenant-level policy as a project-level policy in a project.
Inheriting policies	You can inherit a tenant-level policy as a project-level policy under the tenant.

The following table describes the main functions of extensions.

Function	Description
System extensions	The extension platform has multiple built-in extensions to meet DevOps requirements.

3 Use Cases

General Software Development

- Challenges: Code check, build, deployment, and test are required during software development. Managing multiple independent activities is complex and costly.
- Solution: CodeArts Pipeline associates and manages multiple activities in the development process and executes multiple activities in parallel or serial mode.

DevOps and Continuous Delivery

- Challenges: The traditional DevOps process (from code change to build, test, and deployment) is complex and cannot keep up with rapid iteration.
- Solution: CodeArts Pipeline connects jobs of test, build, and deployment. Users can configure pass conditions to ensure that only code that passes the automated test can be delivered and deployed.

Cascading Management

- Challenges: Managing applications, projects, and the layered microservice architecture can be time- and labor-consuming.
- Solution: Subpipelines can be mounted to the main pipeline to easily manage complex scenarios such as building and microservice dependency.

4 Security

4.1 Shared Responsibilities

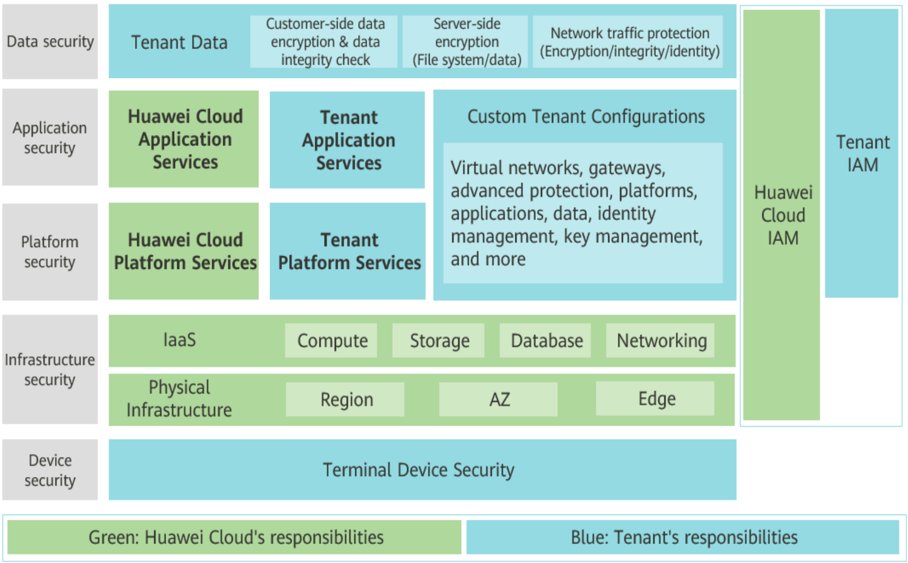
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 4-1 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 4-1 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

4.2 Authentication and Access Control

- Authentication

  You can access CodeArts Pipeline using its UI and APIs. Essentially, your requests are sent through the REST APIs provided by CodeArts Pipeline.

  CodeArts Pipeline APIs can be accessed only after requests are authenticated. CodeArts Pipeline supports two authentication modes:

  - Token: Requests are authenticated using tokens. By default, token authentication is required to access the Pipeline console.
  - AK/SK: Requests are encrypted using an AK (Access Key ID)/SK (Secret Access Key). This method is recommended because it provides higher security than token-based authentication. For operation details, see **AK/SK Signing and Authentication Guide**.

- Access Control

  CodeArts Pipeline supports access control through IAM permissions.

Table 4-1 Access control

Method		Description	Reference
Permission management	IAM permissions	IAM permissions define which actions on your cloud resources are allowed and which actions are denied, to control access to your resources. By default, new IAM users do not have any permissions assigned. New users must be added to one or more groups, and permissions policies or roles must be attached to these groups.	**What Is IAM?** and **Permissions**

4.3 Data Protection Technologies

CodeArts Pipeline provides different methods and features to keep data secure and reliable.

Table 4-2 CodeArts Pipeline data protection methods and features

Method	Description
Transmission encryption (HTTPS)	All CodeArts Pipeline APIs use HTTPS for transmission.
Personal data protection	CodeArts Pipeline controls access to data and records operations performed on the data.
Privacy protection	CodeArts Pipeline encrypts sensitive data such as database account information of users before storing it.
Data backup	CodeArts Pipeline supports user data backup.

4.4 Auditing and Logging

- 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 CodeArts Pipeline for auditing.

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

- Logs

  After you enable CTS, the system starts recording operations on CodeArts Pipeline. Operation records generated during the last seven days can be viewed on the CTS console.

4.5 Service Resilience

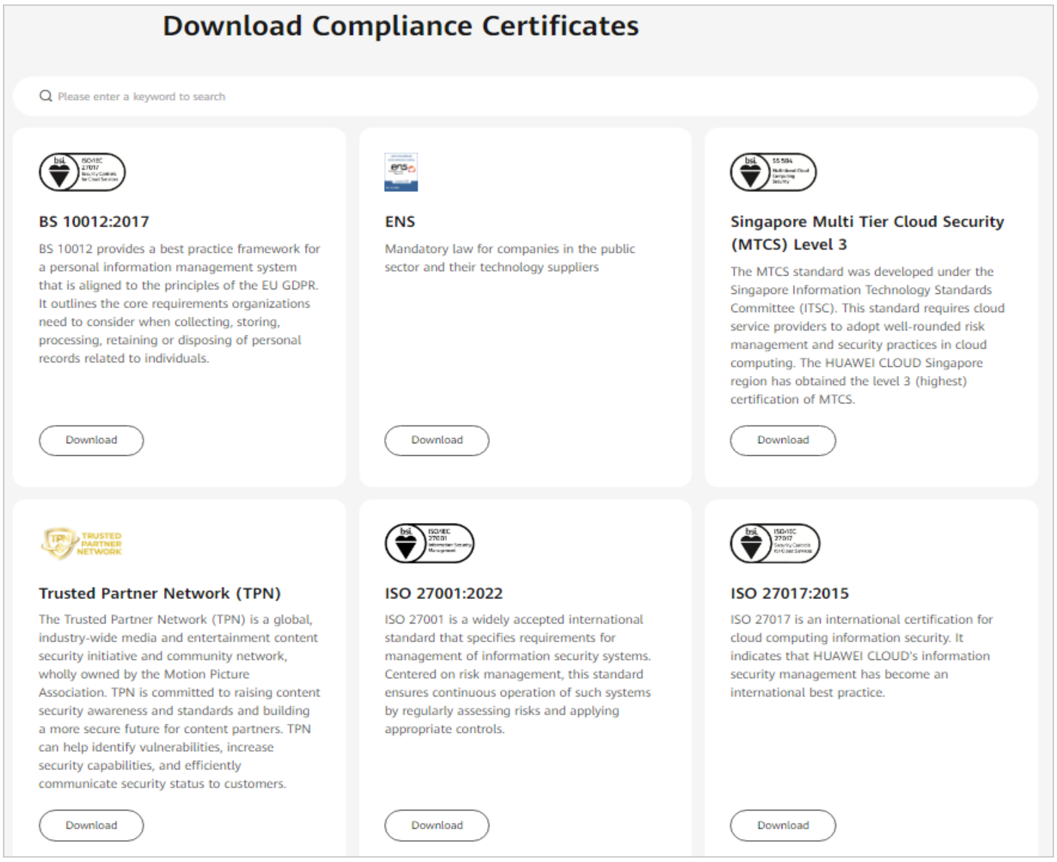
CodeArts Pipeline is deployed in two AZs to ensure service continuity and reliability.

4.6 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 4-2 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.

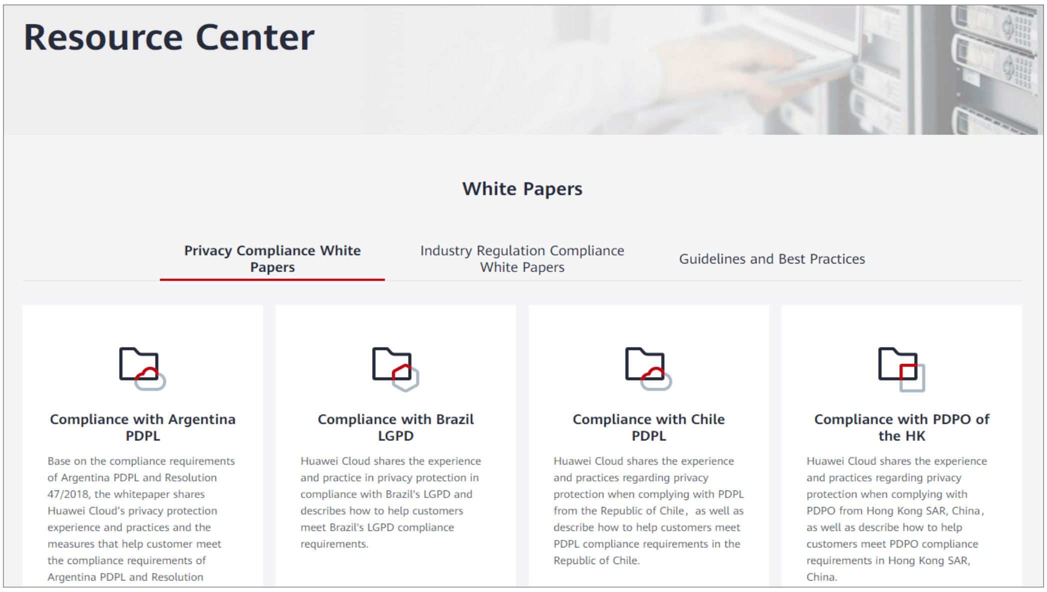
ISO 27017:2015

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 4-3 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 Constraints

The following table describes the constraints on CodeArts Pipeline.

Table 5-1 CodeArts Pipeline constraints

Category	Item	Limit
CodeArts Pipeline	Max. pipelines per tenant	5,000
Single pipeline	Max. stages	16
	Max. jobs	256
	Max. jobs per stage	100
	Max. steps	512
	Max. steps per job	16
	Max. custom parameters	20
	Max. source code repositories	1
	Max. reviewers per review task	10
	Max. times for delayed execution	3
	Max. parallel executions	5
	Max. days for retained execution records	90
	Max. scheduled tasks	10
	Max. lawfully listened branch conditions	32
	Max. lawfully listened path conditions	32

Table 5-2 CodeArts Release constraints (limited free trial)

Category	Item	Limit
Cloud native release	Max. environments per project	50
	Max. policies per environment	5
	Max. tasks per policy	10
	Max. custom environment variables per environment	50
	Max. historical versions of custom variables per environment	20

Table 5-3 Policy constraints

Category	Item	Limit
Policy management	Max. custom rules per tenant	2,000
	Max. project-level rule sets per tenant	1,000
	Max. custom rule sets per tenant	100
	Max. custom rule sets per project	100
	Max. custom rules per rule set	100

Table 5-4 Microservice constraints

Category	Item	Limit
Microservice	Max. microservices per tenant	500
	Max. microservices per project	50

Table 5-5 Change constraints

Category	Item	Limit
Change	Max. changes per microservice (including changes in the developing, to-be-released, and releasing states)	50
	Max. work items associated with a change	10
	Max. changes per release pipeline	10