CodeArts Pipeline

Service Overview

Issue	01
Date	2024-11-27

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.

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.

The following table describes the features of CodeArts Pipeline.

Table 1-1 CodeArts Pipeline features

Feature	Description
Job orchestration	Manage and schedule jobs of build, code check, sub-pipeline, repository, deployment, delayed execution, manual review, and API test.
Adding, deleting, editing, and checking pipelines	Create, edit, delete pipelines and check execution status on the Web UI. You can go to a job details page to view its logs.
Extensions	Use built-in extensions or customize them for task orchestration.
Parameters	Add custom parameters and set them before executing a pipeline.
Execution plans	Configure event triggers, scheduled tasks, and parallel execution policies for a pipeline.
Permissions	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.

Feature	Description
Notifications	Configure whether to send notifications upon pipeline events.
Executing jobs in serial or parallel mode	Execute jobs in a stage in serial or parallel mode as needed.
Executing specific jobs	Execute specific jobs in a pipeline.
Execution records	Check the pipeline records in past 90 days.
Microservice changes	Pipeline supports microservice-based lightweight changes in DevOps.
Policies	Manage policies at the tenant and project levels.
Pipeline rules	Customize rules based on extensions.
Pass conditions	Create rules and policies for pass conditions.
Release management	Pipeline provides debugging, release orchestration, and automated rollout for continuous delivery.

2 Advantages

Flexible and Efficient

- Multi-step/multi-layer job nesting; pipelines are executable upon code events, upon schedule/changes, manually, or in sub-pipelines.
- Parallel execution of millions of jobs for large-scale build, code check, and testing

Quick Integration

- Low-code, visualized extension development reduces costs and improves efficiency.
- Unified extension access standard quickly develops extensions and adapts to service requirements.

Cost-Effective

- On-demand use of resources greatly reduces the investments in fixed assets during service expansion.
- You can configure auto scaling policies to add or remove instances automatically.
- Multiple billing modes (pay-per-use, yearly/monthly, spot price, etc.) are available for you to choose from.

Fast Delivery

- Consistent software version on the code trunk and live network
- Automated integration and verification of feature branches, one-click rollback and on-demand release
- Automated collaboration of project, work, and branch management flows
- E2E traceability

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: Sub-pipelines can be mounted to the main pipeline to easily manage complex scenarios such as building and microservice dependency.

4 Security

4.1 Shared Responsibilities

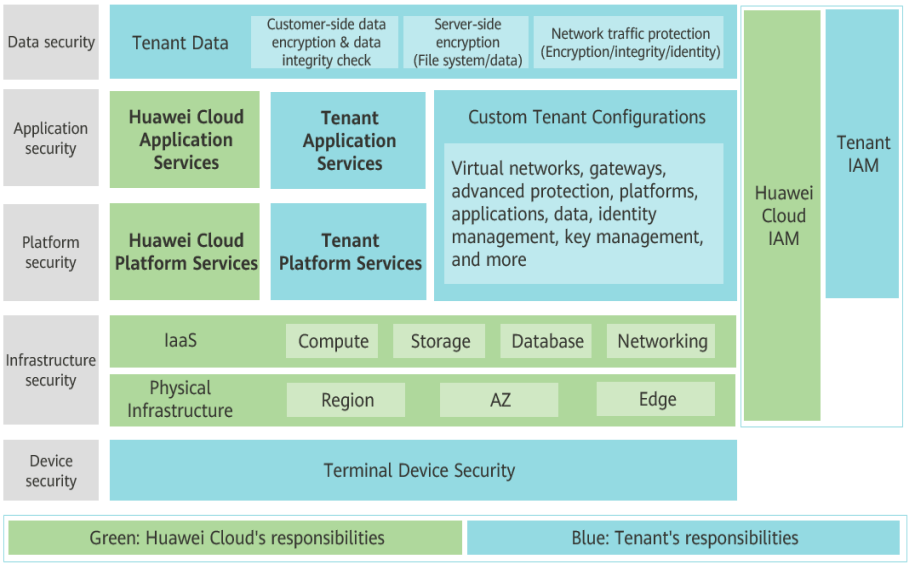
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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



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

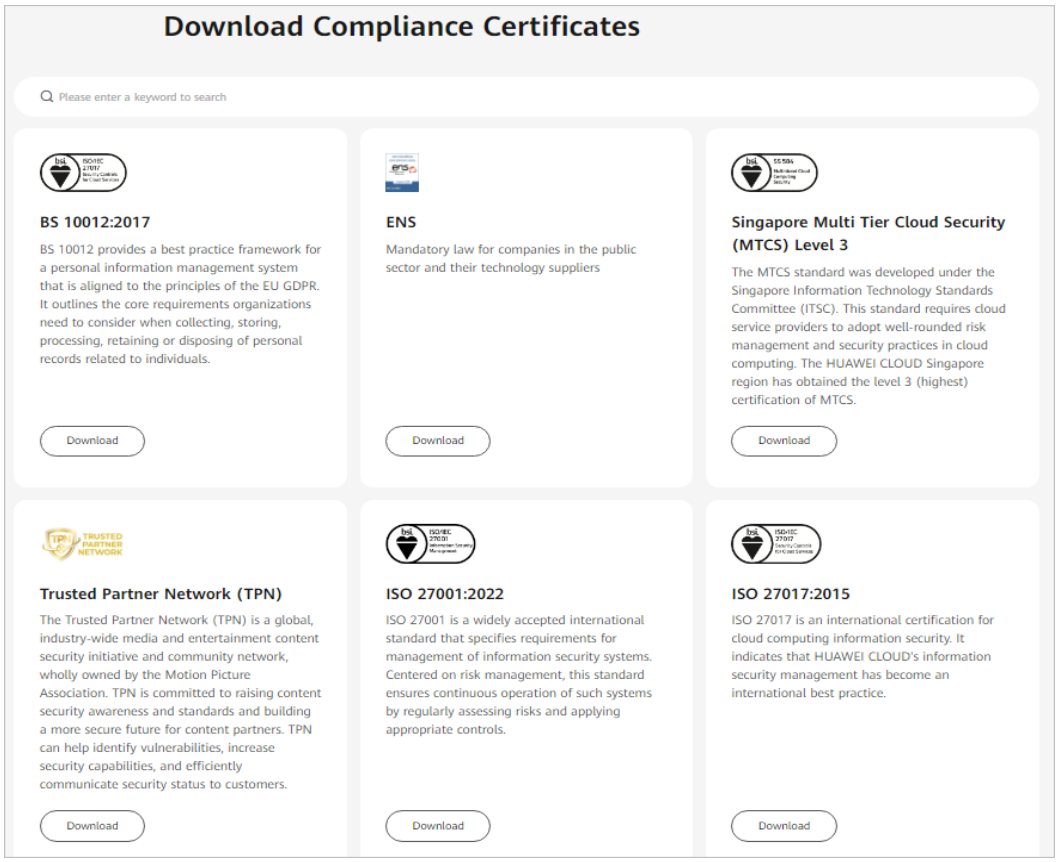
CodeArts Pipeline is deployed in two AZs to ensure service continuity and reliability.

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.

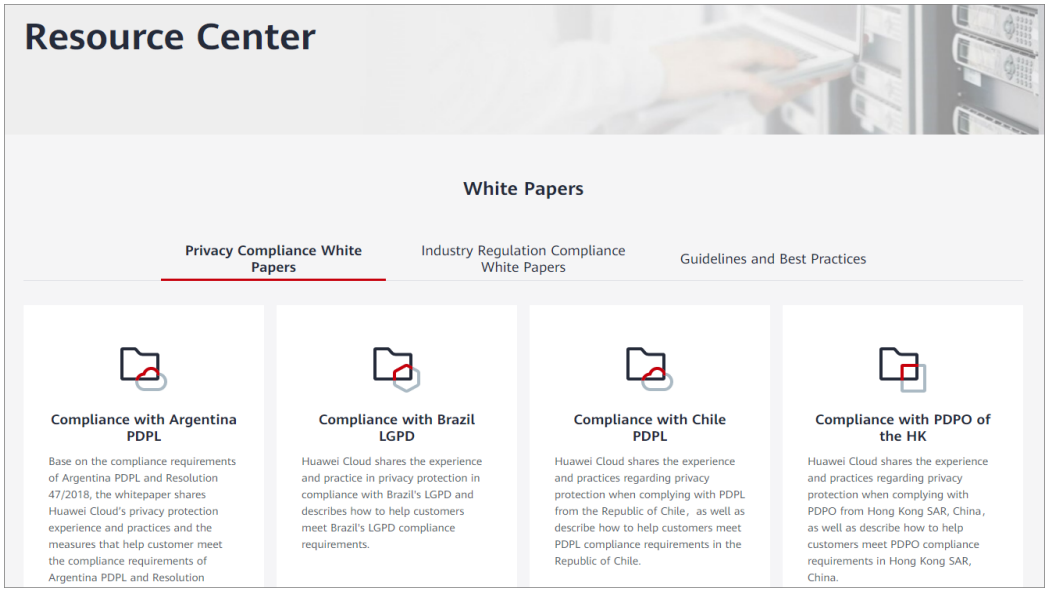
Figure 4-2 Downloading compliance certificates



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



5 Constraints

Naming

Table 5-1 CodeArts Pipeline naming conventions

Item	Description
Pipeline name	• Supports only letters, digits, hyphens (-), and underscores (_) • 1 to 128 characters allowed
Rule name	• Supports only letters, digits, hyphens (-), and underscores (_) • 1 to 128 characters allowed
Policy name	• Supports only letters, digits, hyphens (-), and underscores (_) • 1 to 128 characters allowed
Extension name	• Supports only spaces, letters, digits, hyphens (-), underscores (_), and periods (.) • 1 to 50 characters allowed
Parameter name	• Supports only letters, digits, and underscores (_) • 1 to 128 characters allowed

Specifications

Table 5-2 CodeArts Pipeline specifications

Category	Item	Limit
CodeArts Pipeline	Max. pipelines per tenant	5,000
	Max. parallel executions per tenant	5
Single pipeline	Max. stages	16
	Max. jobs	256

Category	Item	Limit
	Max. jobs per stage	100
	Max. steps	512
	Max. steps per job	16
	Max. custom parameters	100
	Max. source code repositories	1
	Max. reviewers per review task	10
	Max. times for delayed execution	3
	Max. days for execution records	90
	Max. scheduled tasks	10
	Max. lawfully listened branch conditions	32
	Max. lawfully listened path conditions	32

Table 5-3 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 5-4 Policy constraints

Category	Item	Limit
Policy management	Max. custom rules per tenant	2,000
	Max. project-level policies per tenant	1,000
	Max. custom policies per tenant	100
	Max. custom policies per project	100
	Max. custom rules per policy	20

Table 5-5 Microservice constraints

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

Table 5-6 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

6 Concepts

Table 6-1 Basic concepts

Term	Definition
Task orchestration	You can orchestrate stages and jobs when you create, clone, or edit a pipeline.
Stage	A stage is a basic part of a pipeline. Jobs of build, code check, API test, and deployment can be orchestrated and managed in different stages. Closely associated jobs can be managed in one stage for intuitive workflows.
Job	A job is the minimum manageable execution unit in a pipeline. Jobs can be orchestrated in serial and parallel mode in a stage. Job types include build, code check, API test, deployment, and so on.
Execution plan	Execution plans are used to automatically trigger pipelines. By configuring an execution plan, you can make the pipeline run more flexibly.
Pass conditions	Pass conditions are quality thresholds used for a pipeline stage. You can configure policies for pass conditions to control whether a pipeline can proceed to the next stage.
Pipeline template	The template for creating a pipeline.

