

CodeCheck

Service Overview

Issue 02
Date 2022-11-15



Copyright © Huawei Technologies Co., Ltd. 2022. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of 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.

Contents

1 What Is CodeCheck?	1
2 CodeCheck Advantages	4
3 Application Scenarios	6
4 Security	7
4.1 Shared Responsibilities	7
4.2 Authentication and Access Control	8
4.3 Data Protection Technologies	9
4.4 Auditing and Logging	9
4.5 Service Resilience	9
4.6 Certificates	10
5 Constraints	12

1 What Is CodeCheck?

What Is CodeCheck?

CodeCheck is a cloud-based management service that checks code quality. Developers can easily perform static code and security checks in multiple languages and obtain comprehensive quality reports. CodeCheck also allows developers to view defects by group and provides suggestions on fixing code defects, effectively securing high quality and helping achieve business success.

CodeCheck has the following features:

- Supports mainstream encoding languages.
Java, C++, Python, JavaScript, TypeScript, , PHP, Go, HTML, and CSS
- Is compatible with mainstream security standards in the industry.
CWE, OWASP TOP 10, SANS TOP 25, MISRA, and CERT
- Is seamlessly integrated into DevCloud process by providing multi-branch and MR checks.
- Provides impact description and fix suggestions for code defects.
- Accurately locates code lines and allows users to view and fix code issues online.
- Focuses on handling new issues to prevent new technical debts.
- Automatic assigns issue owners, which accelerates the closure of quality issues.
- Has more metrics.
Code cyclomatic complexity (built-in risk measurement system) and code repetition rate
- Other aspects
CodeCheck supports scheduled triggering, code commit triggering, and code check result notification.

Code Check Function List

Table 1-1 Code Check function list

Function	Description
Check coding issues	Use rule sets to check issues in your own code.
Check code security	Use rule sets to check code security risks and issues.
Check code style	Use rule sets to check whether your code matches the selected style.
Check code quality	The code quality score is automatically calculated.
Manage issues	Handle issues found in code checks based on issue descriptions, status, check rules, file paths, source code, and fix suggestions.
Measure code cyclomatic complexity	Evaluate code quality risks based on the code cyclomatic complexity report.
Collect code quantity data	Check the code quantity in projects online.
Measure code repetition rate	Evaluate code quality risks based on the code repetition rate report.
Perform scheduled checks	Use the function of scheduling code checks every week and every day to balance rest and coding.
Notify check results	After the check is complete, the messages are sent to notify related personnel of the check results so that they can handle issues in time.
Check Java code	Check the Java code in projects online.
Check JavaScript code	Check the JavaScript code in projects online.
Check CSS code	Check the CSS code in projects online.
Check web code	Check the HTML/JSP code in projects online.
Check C++ code	Check the C++ code in projects online.

Function	Description
Check Python code	Check the Python code in projects online.
Check PHP code	Check the PHP code in projects online.

2 CodeCheck Advantages

Professional

- Provides nearly 2000 typical check rules.
- Provides multi-dimensional quality statistics reports, including quality gates and code health status.

Accurate

- Locates reported defects under fix guidance.
- Enables you to customize check rule sets to target at issues that you pay more attention to.

Comprehensive

- Supports 10 mainstream development languages, such as Java, C++, and JavaScript.
- Supports code guideline, security, code repetition rate, and cyclomatic complexity checks.
- Is compatible with CWE/OWASP TOP 10/SANS TOP 25/MISRA/CERT security standards.

Easy to Use

- Checks code in hybrid languages
- Allows you to run configured tasks by one click, filter issues in batches, and quick handle issues by severity or category.

Supporting Code Security Check

Scenario

- In the software development phase, you can use CodeCheck to automatically check code quality and security issues. It supports built-in security specifications, requirements, and software production workflows, helping enterprises secure software production.
- CodeCheck provides in-depth code security check capabilities to help government cloud operators and large enterprises manage and control ISV software security quality and build a supply chain security system.

Capability

- Analyzes taints and checks across functions and files.
- Checks for top security vulnerabilities, such as injection and access key leakage.
- Supports Huawei Cloud programming specifications and is compatible with CWE, OWASP TOP 10, CERT and SANS TOP 25 checks.

3 Application Scenarios

Web Applications

- Application: Rule sets of web development languages such as Java and JavaScript are used for code review.
- Characteristics: Web services are oriented to the Internet and are vulnerable to DDoS attacks or information leakage.
- Scenario: Accept security levels during Internet service delivery.

Project Quality Control

- Application: Control risks in real time based on the code complexity, repetition rate, and quality score during delivery.
- Characteristics: Project managers agree that they should secure quality from the front end in daily delivery. However, there is often no effective tool platform. Currently, most quality work depends on backend testing.
- Scenario: Project managers control iteration delivery quality.

4 Security

- [4.1 Shared Responsibilities](#)
- [4.2 Authentication and Access Control](#)
- [4.3 Data Protection Technologies](#)
- [4.4 Auditing and Logging](#)
- [4.5 Service Resilience](#)
- [4.6 Certificates](#)

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.

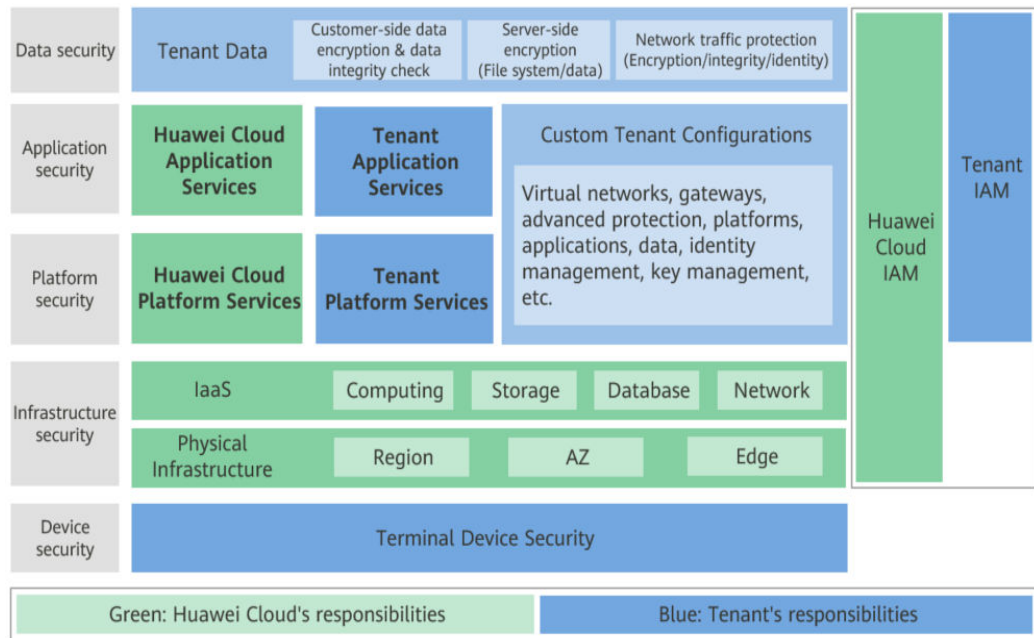
Figure 4-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **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 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 CodeCheck using its UI, APIs, and SDKs. Regardless of the access mode, your requests are sent through REST APIs provided by CodeCheck.

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

Token: Requests are authenticated using tokens. By default, token authentication is required to access the CodeCheck console.

AK/SK: Requests are encrypted using an AK/SK. This method is recommended because it provides higher security than token-based authentication.

For more authentication details and how to obtain tokens and signatures, see [Authentication](#).

Access Control

CodeCheck controls user operations in the following ways:

- **Role permission control:** Roles and permissions are required for adding, deleting, modifying, and querying check tasks and rule sets, viewing rules, creating, importing, and exporting service orders.

- Fine-grained permission control (IAM): Operations such as querying tenant projects, setting project creators, and managing tenant project member lists require fine-grained authorization from IAM.

4.3 Data Protection Technologies

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

Measure	Description	Reference
Transmission encryption (HTTPS)	To secure data transmission, CodeCheck uses HTTPS.	Making an API Request
Personal data protection	ProjectMan controls access to data and records logs for operations performed on the data.	Permission Management
Privacy protection	CodeCheck does not consume or store sensitive user data.	-
Data destruction	When you delete service data or deregister your account: <ul style="list-style-type: none">• Non-key data is physically deleted in real time.• Key data will be marked as soft deleted and then physically deleted seven days later.	-

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 CodeCheck for auditing.

For details about how to enable and configure CTS, see [Enabling CTS](#).

4.5 Service Resilience

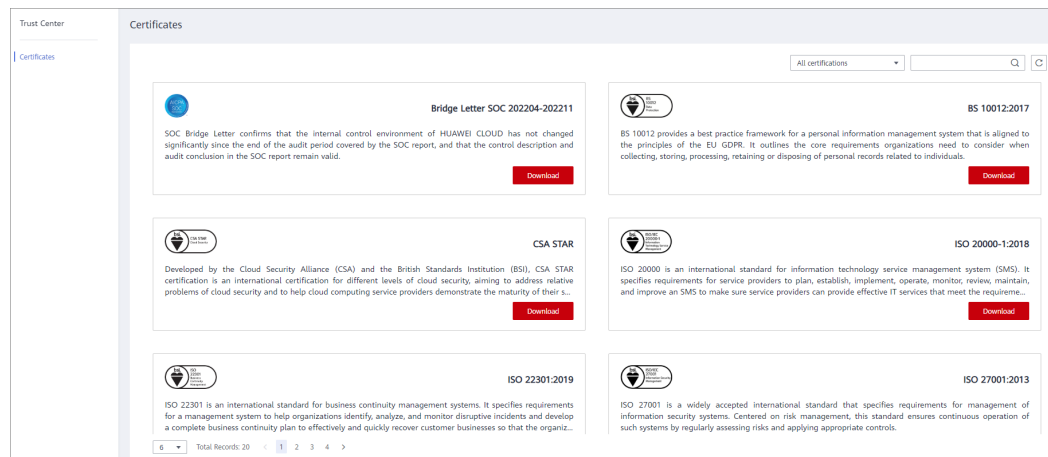
CodeCheck uses multi-active stateless cross-AZ deployment and inter-AZ data disaster recovery (DR) to enable service processes to be quickly started and recovered if a fault occurs, ensuring service reliability.

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.

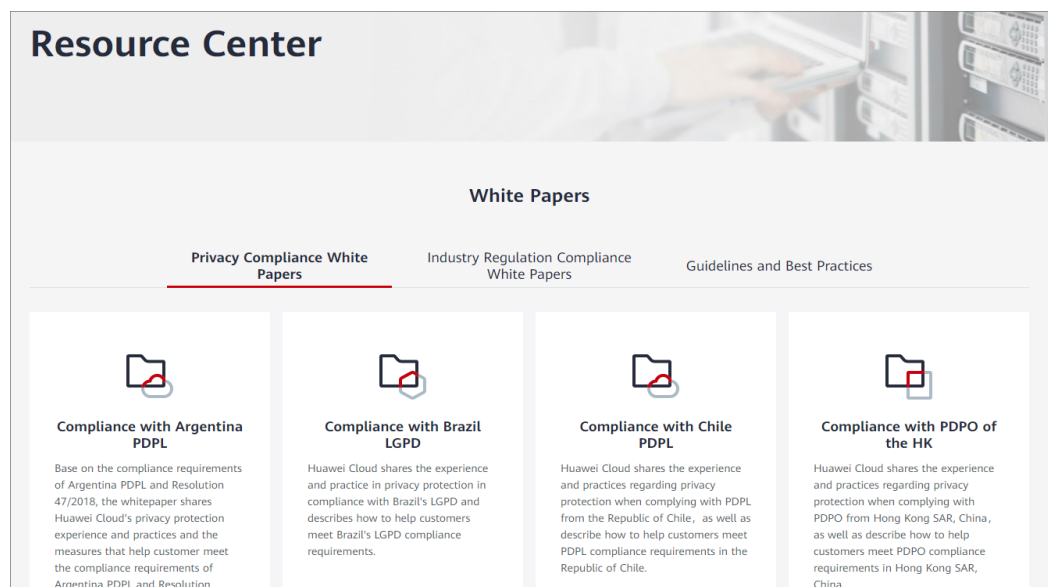
Figure 4-2 Downloading compliance certificates



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

CodeCheck

This section describes the restrictions on CodeCheck, as shown in [Table 5-1](#).

Table 5-1 CodeCheck constraints

Scenario	Constraint
Maximum number of custom rule sets per tenant	1000
Maximum number of code check tasks that can be created per tenant	5000
Maximum code check duration (minutes)	90