

# Container Guard Service

## Service Overview

**Issue** 02  
**Date** 2021-07-09



**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

---

<b>1 CGS.....</b>	<b>1</b>
<b>2 Functions.....</b>	<b>4</b>
<b>3 Product Advantages.....</b>	<b>8</b>
<b>4 Edition.....</b>	<b>9</b>
<b>5 Scenarios.....</b>	<b>11</b>
<b>6 Billing.....</b>	<b>12</b>
<b>7 Permissions Management.....</b>	<b>14</b>
<b>8 Accessing and Using CGS.....</b>	<b>16</b>
8.1 How to Access CGS.....	16
8.2 How to Use CGS.....	16
<b>9 Related Services.....</b>	<b>17</b>
<b>A Change History.....</b>	<b>19</b>

# 1 CGS

---

Container Guard Service (CGS) scans vulnerabilities and configurations in images, helping enterprises detect the container environment, which cannot be achieved by the traditional security software. CGS also delivers functions such as process whitelist configuration, read-only file protection, and container escape detection to minimize the security risks for a running container.

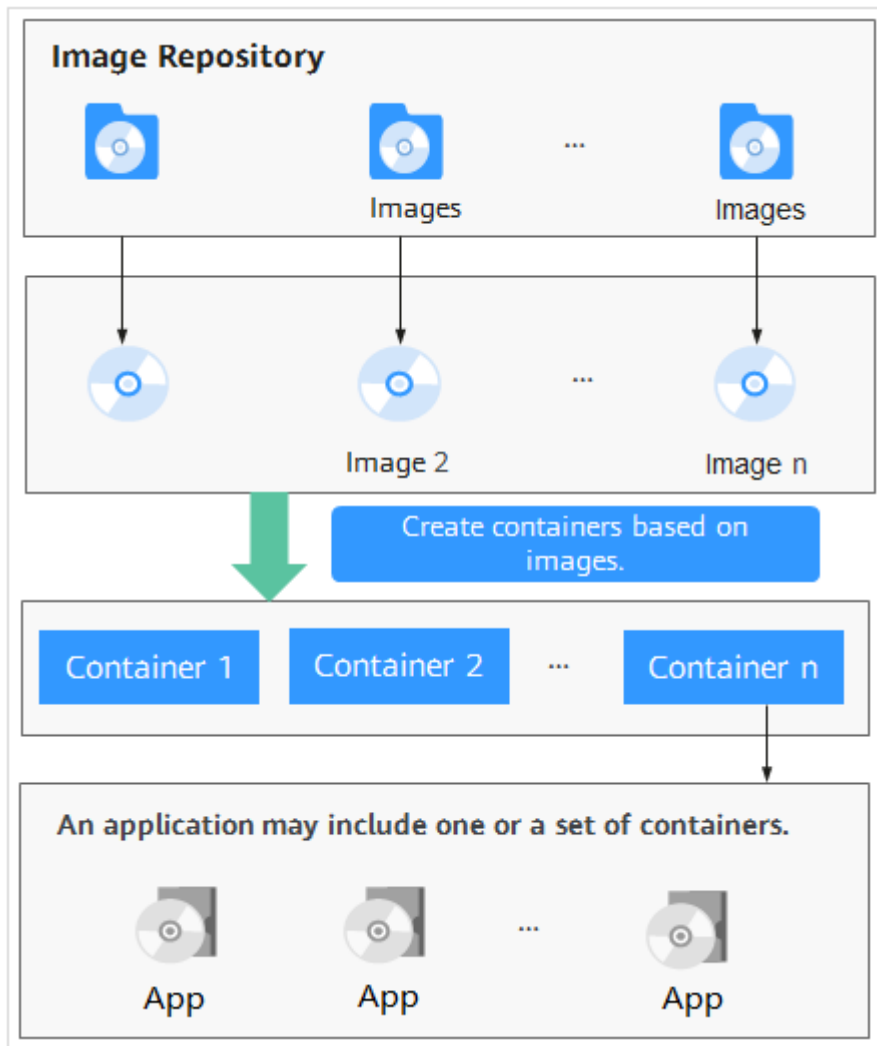
## Concepts

- Image  
An image is a special file system. It provides not only programs, libraries, resources, configuration files but also some configuration parameters required for a running container. An image does not contain any dynamic data, and its content is unchangeable after creation.
- Container  
A container is the instance of an image and can be created, started, stopped, deleted, and suspended.

**Figure 1-1** describes the relationships between images, containers, and applications.

- Multiple containers can be started for an image.
- An application may include one or a set of containers.

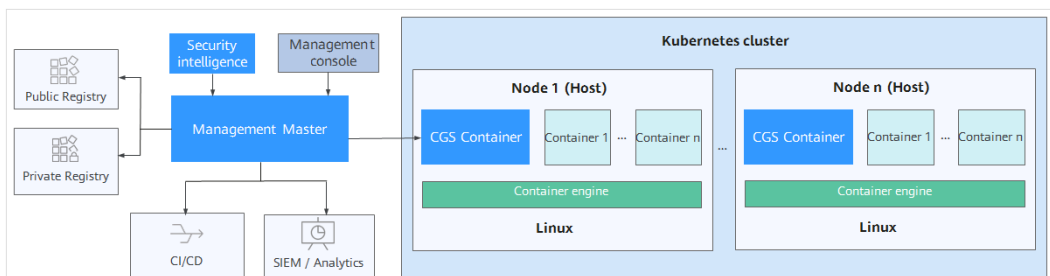
**Figure 1-1** Relationships between images, containers, and applications



## Deployment Architecture

**Figure 1-2** shows the CGS deployment architecture and **Table 1-1** describes its key components.

**Figure 1-2** CGS deployment architecture



**Table 1-1** Key CGS components

<b>Component</b>	<b>Description</b>
CGS Container	Runs on each container node (host) to scan all container images on the node for image vulnerabilities, implement security policies, and collect exceptions.
Management Master	Manages and maintains CGS Containers.
Security Intelligence	Provides a security information knowledge base containing vulnerability and malicious program libraries, as well as big data AI training models.
Management console	Provides a console for users to use CGS.

# 2 Functions

---

CGS provides container image security, security policies, and runtime security functions.

## Container Image Security

CGS scans your images that are running or displayed in your image list, and provides suggestions on how to fix detected vulnerabilities and malicious files.

---

### NOTICE

CGS can scan Linux images.

---

**Table 2-1** Container image check items

Item	Description	Check Frequency
Private image security	<p>Scans private images in SWR for vulnerabilities, unsafe settings, and malicious code.</p> <p>The following items are checked:</p> <ul style="list-style-type: none"> <li>• Vulnerabilities Whether there are CVE or other vulnerabilities in SWR images</li> <li>• Malicious files Whether there are Trojans, worms, adware, or other malicious files in private images</li> <li>• Unsafe settings Non-compliant or insecure settings</li> <li>• Software information Software in private images</li> <li>• File information Files in private images. Software is not included.</li> </ul>	<ul style="list-style-type: none"> <li>• Automatic check in the early morning every day</li> <li>• Manual scan</li> </ul>
Local image vulnerabilities	Checks whether there are CVE or other vulnerabilities in the images running in CCE containers.	Real-time check
Official image vulnerabilities	Periodically scans official Docker images for vulnerabilities.	-

## Container Security Policies

You can configure security policies, whitelist container processes, and set protected files to minimize the permissions required for containers to run, improving system and application security.



**Table 2-2** Container security policies

Item	Description	Check Frequency
Process whitelist	Alarms will be triggered if processes not whitelisted are started, preventing abnormal processes, privilege escalation attacks, and violations.	Real-time check
File protection	Read-only permissions should be configured for critical application directories (such as <b>bin</b> , <b>lib</b> , and <b>usr</b> directories) in the container to prevent hackers from tampering and attacking. If you set these directories to be read-only, CGS will protect them from security incidents such as file tampering.	Real-time check

## Container Runtime Security

CGS scans running containers for malicious programs including miners and ransomware, detects non-compliant security policies, file tampering, and container escape, and provide suggestions.

**Table 2-3** Container runtime security

Item	Description	Check Frequency
Container escape detection	Uses rules and machine learning technologies to accurately detect escape behaviors on servers, including shocker attacks, process privilege escalation, Dirty COW, and brute-force attacks.	Real-time check
High-risk system calls	Detects Linux system calls that were made within containers and could pose security risks.	Real-time check

Item	Description	Check Frequency
Abnormal program detection	Detects the startup of processes that violate security policies and malicious programs such as miners, ransomware, viruses, and Trojans.	Real-time check
Abnormal files	Detects file access that violates security policies. Security O&M personnel can check whether hackers are intruding and tampering with sensitive files.	Real-time check
Container environment	Checks for abnormal container runtime, including abnormal startup and improper configurations.	Real-time check

# 3 Product Advantages

---

With CGS, you can secure your containers and images throughout their lifecycles, detecting and eliminating risks.

## Centralized Security Management

On a single console, manage the security of containers and images running on all nodes in the CCE cluster.

## Extensive Vulnerability Database

Accurately detect over 100,000 image vulnerabilities.

## Lightweight Agent

The CGS agent runs as a container and generally occupies only 1% of system resources. Peak resource usage is no more than 5%.

## Container Anti-escape

Scan for container escapes based on 100 subcategories of built-in container escape rules under 10 major categories.

## Security Compliance

Meet compliance requirements against intrusions and malicious code.

# 4 Edition

CGS supports the enterprise edition. For more information, see [Table 4-1](#). For more details, see [Functions](#).

- The enterprise edition provides a range of detection and monitoring functions, allowing you to protect your clusters and container runtime, detect and fix vulnerabilities, check for unsafe settings and malicious files, and configure security settings. The enterprise edition will be available if you purchase CGS quotas.

**Table 4-1** Editions

Function	Item	Enterprise (√: supported; ×: not supported)
Cluster protection	Protects your clusters.	√
Local image	Scans for vulnerabilities in local images.	√
Private image	Scans for vulnerabilities in private images.	√
	Scans for malicious files in private images.	√
	Scans software in private images.	√
	Scans files in private images.	√
	Checks the settings of private images.	√
Official image	Scans for vulnerabilities in official images.	√
Runtime security	Detects escapes.	√

Function	Item	Enterprise (√: supported; ×: not supported)
	Detects high-risk system calls.	√
	Detects abnormal programs.	√
	Detects abnormal files.	√
	Checks container environment.	√
Security configurations	Process whitelist	√
	File protection	√

# 5 Scenarios

---

## Checking Container Image Security

Vulnerabilities will probably be introduced to your system through the images downloaded from Docker Hub or through open-source frameworks.

You can use CGS to scan images for risks including image vulnerabilities, unsafe accounts, and malicious files. Receive reminders and suggestions and eliminate the risks accordingly.

## Checking Container Runtime Security

Develop a whitelist of container behaviors to ensure that containers run with the minimum permissions required, securing containers against potential threats.

## Meeting Compliance Requirements

Prevent intrusions and malicious code, making sure your container and system security meet compliance requirements.

# 6 Billing

This section describes CGS billing and renewal.

## Billing Items

CGS is charged based on the edition, number of protected nodes, and duration you use it.

**Table 6-1** CGS billing

Billing Item	Description
Edition	CGS provides the enterprise edition. For details about its functions and how to enable the functions, see <a href="#">Edition</a> .
Node quantity	Number of nodes protected by CGS
Duration	<ul style="list-style-type: none"> <li>Yearly or monthly package</li> <li>Pay-per-use</li> </ul>

## Billing Modes

**Table 6-2** Billing mode

Edition	Billing Mode	Description	Pricing
Enterprise	Yearly/ Monthly package	<ul style="list-style-type: none"> <li>The edition charging in yearly/monthly mode provides a higher discount and more functions than that charging on a per-use basis, and is recommended for long-term users. Yearly/monthly CGS is billed based on the purchase period specified in the order.</li> <li>If you are paying for CGS per use but want change to the yearly/monthly edition, simply purchase the protection quota. The system preferentially uses the yearly/monthly quota you purchased.</li> </ul>	<a href="#">Product Pricing Details</a>

## Renewal

If you do not renew CGS billed in yearly/monthly mode upon its expiration, a retention period will be granted.

CGS stops providing services if its quota expires. To avoid loss caused by security issues, you are advised to renew it in a timely manner. CGS expiration does not affect your other services.

You can renew your resources on the [Renewals](#) page of the management console. For details, see [Renewal Management](#).

## Expiration and Overdue Payment

- Service expiration  
If you do not renew a quota upon its expiration, a retention period is available for you. For details, see [Retention Period](#).
- Overdue payment  
For container and asset security purposes, you are advised to top up your account and repay arrears in a timely manner. For details, see [Making Repayments \(Prepaid Direct Customers\)](#).

## FAQ

For more charging FAQs, see [CGS FAQs](#).



# 7 Permissions Management

---

To assign different access permissions to employees in an enterprise for the CGS resources you purchased on Huawei Cloud, you can use Identity and Access Management (IAM) to perform refined permission management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your Huawei Cloud resources.

With IAM, you can use your Huawei Cloud account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, some software developers in your enterprise need to use CGS resources but must not delete them or perform any high-risk operations. To achieve this, you can create IAM users for the software developers and grant them only the permissions required for using CGS resources.

If your Huawei Cloud account does not need individual IAM users for permissions management, skip over this chapter.

IAM can be used free of charge. You pay only for the resources in your account. For more information about IAM, see [What Is IAM](#).

## CGS Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from their owning groups and can perform specified operations on cloud services based on the permissions.

To assign CGS permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing CGS, the users need to switch to a region where they have been authorized to use cloud services.

You can grant users permissions by using roles and policies.

- **Roles:** A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. This mechanism provides only a limited number of service-level roles for authorization. When using roles to grant permissions, you also need to assign other roles that the permissions depend on to take effect. However, roles are not an ideal choice for fine-grained authorization and secure access control.

- **Policies:** A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, you can grant CGS users only the permissions for managing a certain type of ECSs. For details about the actions supported by CGS, see [CGS Permissions and Supported Actions](#).

**Table 7-1** CGS system role


Role/ Policy Name	Descrip tion	Type	Dependencies
CGS Adminis trator	CGS system adminis trator, who has all permiss ions of CGS.	System role	Dependent on the <b>Tenant Guest</b> policy, which needs to be assigned in the same project as the <b>CGS Administrator</b> policy
CGS FullAcce ss	All permiss ions of CGS	System- defined policy	None
CGS ReadOn lyAccess	Read- only permiss ions for CGS	System- defined policy	None

## References

- [IAM Service Overview](#)
- [Creating a User Group, a User, and Granting CGS Permissions](#)
- [CGS Permissions and Supported Actions](#)

# 8 Accessing and Using CGS

## 8.1 How to Access CGS

You can access CGS on the management console. If you have registered, log in to the management console, click , and choose **Security & Compliance > Container Guard Service**.

## 8.2 How to Use CGS

[Table 8-1](#) describes how to use CGS.

**Table 8-1** Procedure of using CGS

No.	Step	Description
1	Enabling cluster protection	After protection is enabled, images and running containers on all nodes in a cluster can be checked in real time.
2	(Optional) Configuring security policies	Configuring security policies and applying the policies to an image can effectively prevent security risks in a running container.
3	Viewing vulnerabilities	Check the vulnerabilities on the image and determine whether to ignore the vulnerabilities.
	Checking container runtime security details	View exceptions during the running of the container.

# 9 Related Services

## CCE

Cloud Container Engine (CCE) rapidly builds a highly reliable container cluster based on the cloud server and adds nodes in the cluster. CGS installs shields on a cluster to protect container applications on nodes in a cluster.

### NOTE

CCE is a high-performance, high-reliability service through which enterprises can manage containerized applications. CCE supports native Kubernetes applications and tools, allowing you to easily set up a container runtime environment on the cloud. For more information, see the *Cloud Container Engine User Guide*.

## CTS

Cloud Trace Service (CTS) provides you with a history of CGS operations. After enabling CTS, you can view all generated traces to review and audit performed CGS operations. For details, see the *Cloud Trace Service User Guide*.

**Table 9-1** CGS operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Enabling cluster protection	cgs	openClusterProtect
Disabling cluster protection	cgs	closeClusterProtect
Adding a policy	cgs	addPolicy
Editing a policy	cgs	modifyPolicy
Deleting a policy	cgs	deletePolicy
Applying a policy to an image	cgs	imageApplyPolicy

Operation	Resource Type	Trace Name
Ignoring all images affected by the vulnerability	cgs	ignoreVul
Restoring all images affected by the vulnerability	cgs	cancelIgnoreVul
Ignoring images affected by the vulnerability	cgs	ignoreImageVul
Unignoring of images affected by the vulnerability	cgs	cancelIgnoreImageVul
Unauthorized access	cgs	registerCgsAgency
Manually scanning images	cgs	scanPrivateImage
Obtaining and scanning images from Software Repository for Container (SWR)	cgs	syncSwrPrivateImage

## SWR

Software Repository for Container (SWR) provides easy, secure, and reliable management over container images throughout their lifecycles, facilitating the deployment of containerized services. For more information, see the *Software Repository for Container User Guide*. CGS scans vulnerabilities and configurations in container images to help enterprises detect the container environment that cannot be achieved by traditional security software.

## IAM

Identity and Access Management (IAM) provides the permission management for CGS. Only users granted with CGS Administrator permissions can use CGS. To obtain the permissions, contact users who have Security Administrator permissions. For details, see *Identity and Access Management User Guide*.

---

# A Change History

---

Released On	Description
2021-07-09	This is the second official release. Updated the service entry.
2021-01-26	This is the first official release.