Container Guard Service

User Guide

Issue	02
Date	2021-06-15

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Introduction

1.1 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

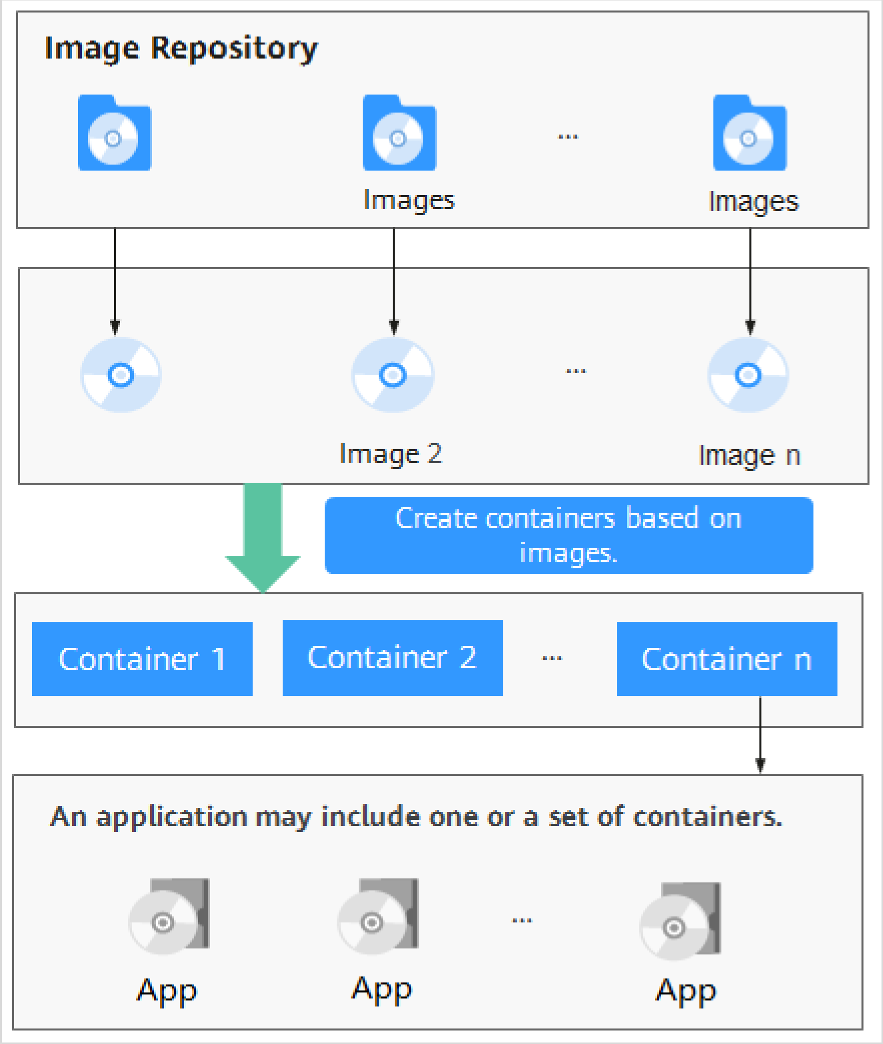
  An image is a special file system. It provides not only programs, libraries, resources, configuration files but also some configuration parameters required for a running container. An image does not contain any dynamic data, and its content is unchangeable after creation.
- Container

  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

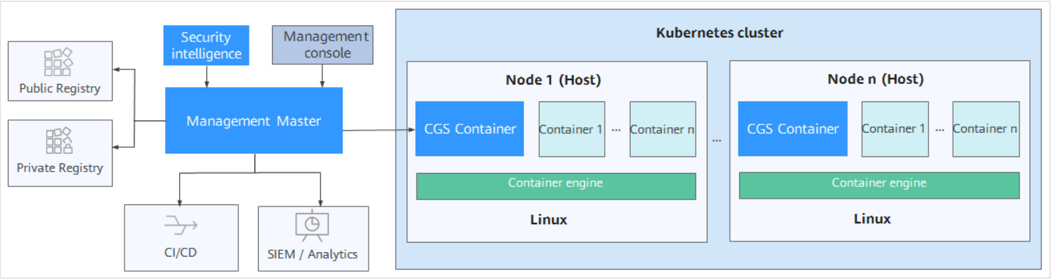


Table 1-1 Key CGS components

Component	Description
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.

1.2 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 1-2 Container image check items

Item	Description	Check Frequency
Private image security	Scans private images in SWR for vulnerabilities, unsafe settings, and malicious code. The following items are checked: ● Vulnerabilities Whether there are CVE or other vulnerabilities in SWR images ● Malicious files Whether there are Trojans, worms, adware, or other malicious files in private images ● Unsafe settings Non-compliant or insecure settings ● Software information Software in private images ● File information Files in private images. Software is not included.	● Automatic check in the early morning every day ● Manual scan
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 1-3 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 **bin**, **lib**, and **usr** 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 1-4 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

1.3 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.

Compliance

Meet compliance requirements against intrusions and malicious code.

1.4 Editions

CGS provides basic and enterprise editions. **Table 1-5** describes the functions of each edition. For details, see **Functions**.

- The basic edition is available for free if you log in to the CGS console and agree to the service authorization.

  In the basic edition, you can only check the details and solutions for vulnerabilities detected in your private and official images.
- 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. To use this edition, agree to the service authorization and enable cluster protection on the console.

Table 1-5 Editions

Function	Item	Basic edition	Enterprise
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.	×	√
	Detects high-risk system calls.	×	√

Function	Item	Basic edition	Enterprise
	Detects abnormal programs.	×	√
	Detects abnormal files.	×	√
	Checks container environment.	×	√
Security configurations	Process whitelist	√	√
	File protection	√	√

1.5 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.

1.6 Permissions Management

To assign different access permissions to employees in an enterprise for the CGS resources you purchased, 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 resources.

With IAM, you can use your 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 account does not need individual IAM users for permissions management, skip over this chapter.

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 ECS 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 1-6 CGS system role

Role/Policy Name	Description	Type	Dependencies
CGS Administrator	CGS administrator, who has all permissions of CGS.	System role	Dependent on the **Tenant Guest** policy, which needs to be assigned in the same project as the **CGS Administrator** policy
CGS FullAccess	All permissions of CGS	System-defined policy	None

Role/ Policy Name	Description	Type	Dependencies
CGS ReadOnlyAccess	Read-only permissions for CGS	System-defined policy	None

1.7 Accessing and Using CGS

1.7.1 How to Access CGS

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

1.7.2 How to Use CGS

Table 1-7 describes how to use CGS.

Table 1-7 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.

1.8 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 1-8 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
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

Operation	Resource Type	Trace Name
Unauthorized access	cgs	registeCgsAgency
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*.

1.9 Common Concepts

Cluster

A cluster consists of one or more ECSs (also known as nodes) in the same subnet. It provides a computing resource pool for running containers.

Node

In CGS, each node corresponds to an Elastic Cloud Server (ECS), and containers run on nodes.

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.

Security Policy

A security policy indicates the security rule that must be followed for a running container. If a container violates a security policy, a container exception is displayed on the **Runtime Security** page of the CGS management console.

2 Service Authorization

CGS requires access permissions for Cloud Container Engine (CCE) to protect its clusters and Software Repository for Container (SWR) to scan its images.

Authorize CGS to access these services the first time you use it.

Constraints

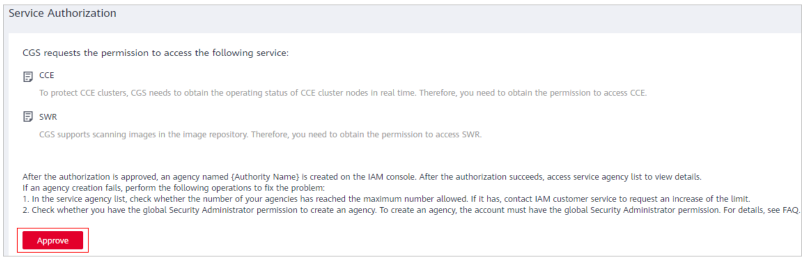
- CGS cannot be used across regions. The images to be scanned and the clusters to be protected must be in the same region as CGS.
- You have obtained the account and password for logging in to the management console.

Procedure

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Figure 2-1 Service authorization



CGS requests the permission to access the following service:

CCE

To protect CCE clusters, CGS needs to obtain the operating status of CCE cluster nodes in real time. Therefore, you need to obtain the permission to access CCE.

SWR

CGS supports scanning images in the image repository. Therefore, you need to obtain the permission to access SWR.

After the authorization is approved, an agency named {Authority Name} is created on the IAM console. After the authorization succeeds, access service agency list to view details.
If an agency creation fails, perform the following operations to fix the problem:
1. In the service agency list, check whether the number of your agencies has reached the maximum number allowed. If it has, contact IAM customer service to request an increase of the limit.
2. Check whether you have the global Security Administrator permission to create an agency. To create an agency, the account must have the global Security Administrator permission. For details, see FAQ.

Step 3 Click **Approve**.

Once service authorization has succeeded, an agency named **cgs_admin_trust** on CGS will be created and you can start to use CGS.

📖 **NOTE**

After authorization, if the agency fails to be created for CGS, it is probably because the number of agencies already reaches the upper limit. In this case, log in to the IAM console and delete unnecessary agencies, or contact the administrator to increase the agency quota.

----End

3 Enabling Protection for a Cluster

Enabling protection will automatically install the CGS shield plug-in in the cluster. The CGS shield is installed as a daemonset, which starts a container on each compute node in the cluster to monitor the status and events of other containers on the node.

CGS automatically enables protection for a new node in the cluster when the node is added to a cluster with protection enabled.

Check Frequency

CGS performs a full check in the early morning every day.

If you enable server protection before the check interval, you can view check results only after the check at 00:00 of the next day is complete.

Prerequisites

- You have created clusters on CCE.
- **Cluster Protection Status** is **Disabled**.

Procedure

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 Locate the row containing the target cluster and click **Enable Protection** in the **Operation** column.

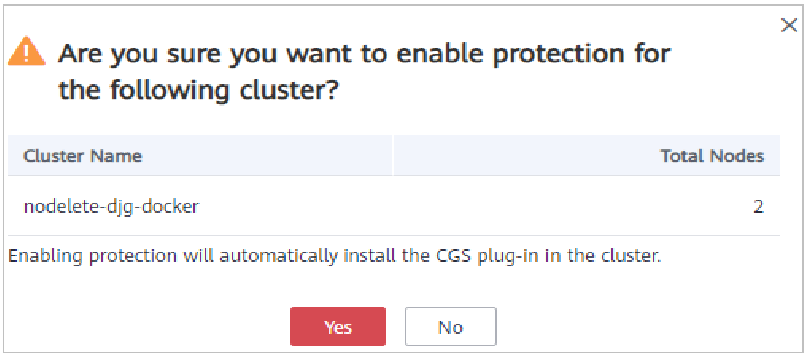
NOTE

Click the name of a cluster to go to the node list page. You can also click **Enable Protection** on the top of the node list.

Step 4 In the dialog box that is displayed, confirm the cluster name and the number of nodes are correct, and click **Yes**.

After protection is enabled, **Cluster Protection Status** of the cluster is **Enabled**, indicating that protection has been enabled for all available nodes in the cluster.

Figure 3-1 Enabling protection



Are you sure you want to enable protection for the following cluster?

Cluster Name	Total Nodes
nodelete-djg-docker	2

Enabling protection will automatically install the CGS plug-in in the cluster.

NOTE

- CGS automatically enables protection for the new node in the cluster when a new node is added to a cluster with protection enabled.
- Enabling protection will automatically install the CGS plug-in in the cluster.

----End

4 (Optional) Configuring Policies

You can customize security policies by configuring a process whitelist (a list of file paths allowed to be executed in the container) and file protection list (a list of the read-only file directories in the container) to prevent risks during the running of the container, and keep systems and applications secure.

Prerequisites

The cluster protection function has been enabled.

Adding a Security Policy

Step 1 Log in to the management console.

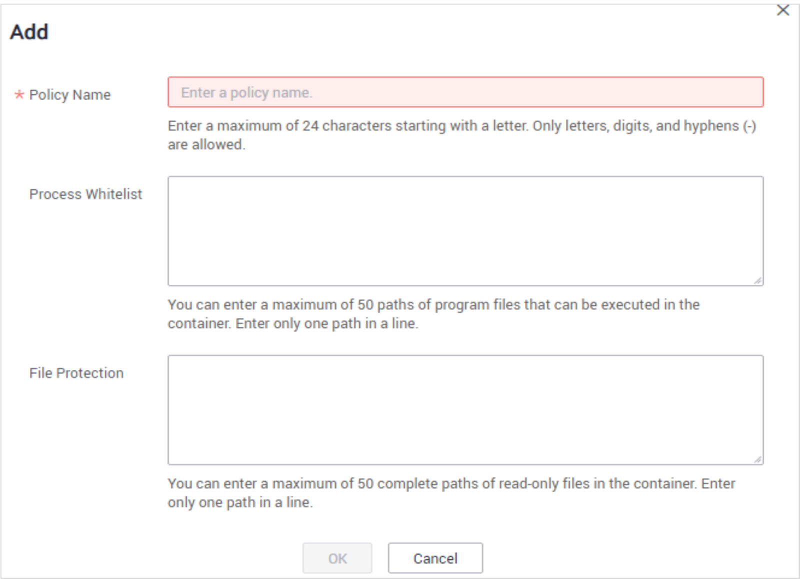
Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the left navigation pane, choose **Security Configurations**.

Step 4 In the upper part of the **Security Policies** page, click **Add**.

Step 5 On the displayed page, configure the policy. See **Figure 4-1**. For details, see **Table 4-1**.

Figure 4-1 Add dialog box



Add

* Policy Name

Enter a policy name.

Enter a maximum of 24 characters starting with a letter. Only letters, digits, and hyphens (-) are allowed.

Process Whitelist

You can enter a maximum of 50 paths of program files that can be executed in the container. Enter only one path in a line.

File Protection

You can enter a maximum of 50 complete paths of read-only files in the container. Enter only one path in a line.

Table 4-1 Parameter description

Parameter	Description
Policy Name	Name of a policy
Process Whitelist	User-defined. Indicates process file paths allowed to be executed in a container. The process whitelist function can effectively prevent security risks, such as abnormal processes, privilege escalation attacks, and violation operations.
File Protection	User-defined. Indicates read-only file directories in a container. Setting the file protection list can effectively prevent security risks such as file tampering.

Step 6 Click **OK**.

----End

Associating an Image

After adding a policy, you can associate an image and apply the policy to the associated image.

Step 1 Log in to the management console.

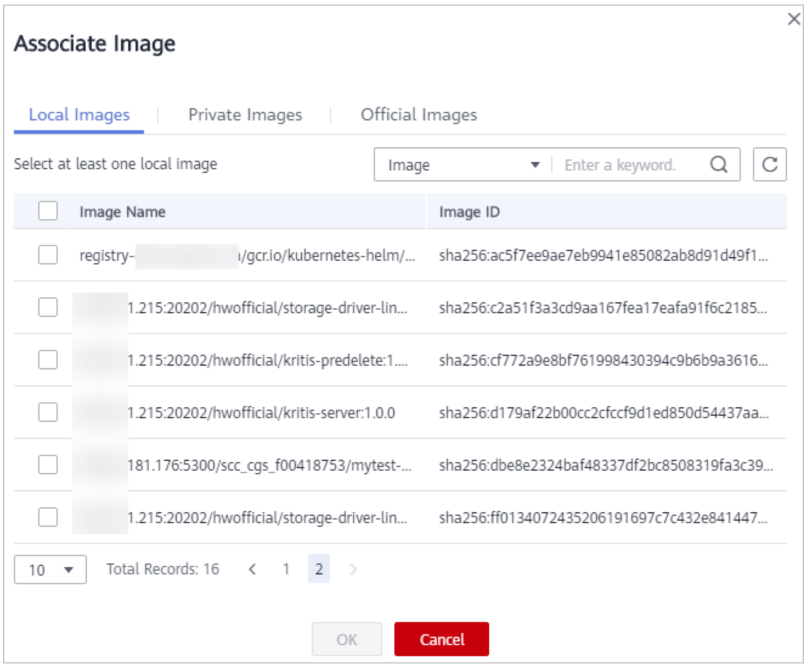
Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the left navigation pane, choose **Security Configurations**.

Step 4 Locate the row that contains the policy which you want to associate an image with, and click **Associate Image** in the **Operation** column.

Step 5 In the **Associate Image** dialog box, select images, as shown in **Figure 4-2**.

Figure 4-2 Associate Image dialog box



Associate Image

Local Images | Private Images | Official Images

Select at least one local image

□	Image Name	Image ID
□	registry-[redacted]/gcr.io/kubernetes-helm/...	sha256:ac5f7ee9ae7eb9941e85082ab8d91d49f1...
□	[redacted]1.215:20202/hwofficial/storage-driver-lin...	sha256:c2a51f3a3cd9aa167fea17eafa91f6c2185...
□	[redacted]1.215:20202/hwofficial/kritis-predelete:1....	sha256:cf772a9e8bf761998430394c9b6b9a3616...
□	[redacted]1.215:20202/hwofficial/kritis-server:1.0.0	sha256:d179af22b00cc2cfccf9d1ed850d54437aa...
□	[redacted]181.176:5300/scc_cgs_f00418753/mytest-...	sha256:dbe8e2324baf48337df2bc8508319fa3c39...
□	[redacted]1.215:20202/hwofficial/storage-driver-lin...	sha256:ff0134072435206191697c7c432e841447...

Step 6 Click **OK**.

----End

Other Operations

- Viewing a policy

  In the policy list, click the name of a policy to view its information.

- Editing a policy

  In the row containing the policy to be modified, click **Edit** in the **Operation** column to modify the policy name, process name, and file protection information.

- Deleting a policy

  In the row containing the policy to be deleted, click **Delete** in the **Operation** column.

5 Image Security

5.1 Managing Local Image Vulnerabilities

This section describes how to check the vulnerabilities on the local image and determine whether to ignore the vulnerabilities.

Check Method

After you enable cluster protection, CGS automatically scans your clusters.

Prerequisites

The cluster protection function has been enabled.

Viewing Vulnerabilities

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

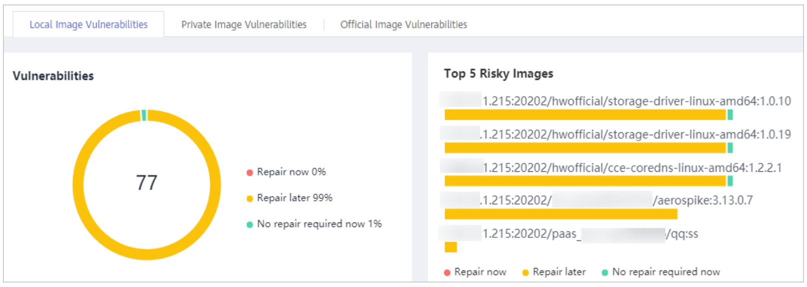
Step 3 In the navigation tree on the left, choose **Image Security**.

Step 4 Click **Image Vulnerabilities** and click **Local Image Vulnerabilities**.

Step 5 View the vulnerability statistics.

- **Vulnerabilities**: Number and percentage of vulnerabilities by the urgency level
- **Top 5 Risky Images**: Top 5 images with the most vulnerabilities and the number of vulnerabilities at each urgency level

Figure 5-1 Local image vulnerability overview


Local Image Vulnerabilities
Private Image Vulnerabilities
Official Image Vulnerabilities
Vulnerabilities
77
Repair now 0%
Repair later 99%
No repair required now 1%
Top 5 Risky Images
1.215:20202/hwofficial/storage-driver-linux-amd64:1.0.10
.1.215:20202/hwofficial/storage-driver-linux-amd64:1.0.19
1.215:20202/hwofficial/cce-coredns-linux-amd64:1.2.2.1
.1.215:20202/ /aerospike:3.13.0.7
1.215:20202/paas_ /qq:ss
Repair now
Repair later
No repair required now

NOTE

Click a risky image to check its vulnerability overview, including the vulnerability name, urgency, status, software information; and choose to fix or ignore the vulnerability.

Step 6 Go to the local image vulnerability page. Table 5-1 describes the parameters.

Table 5-1 Parameter description

Parameter	Description	Operation
Vulnerability Name	-	● Click ⌄ to view the details of a vulnerability, including **CVE ID**, **CVSS Score**, **Disclosure Time**, and **Vulnerability Details**. ● Click the name of a vulnerability to view the images affected by the vulnerability. For details, see Step 7.
Repair Urgency	Shows whether the vulnerability should be repaired immediately.	-
Unprocessed Images	Shows the number of images where the vulnerability is detected but not fixed yet.	-
Historically Affected Images	Shows the number of images that have been affected.	-
Solution	Provides a solution to fix the vulnerability.	Click the link in the **Solution** column to view the solution.

Step 7 Click a vulnerability name to view the basic information about the affected images, as shown in Figure 5-2 and Figure 5-3.

Figure 5-2 Basic information about a vulnerability in local images

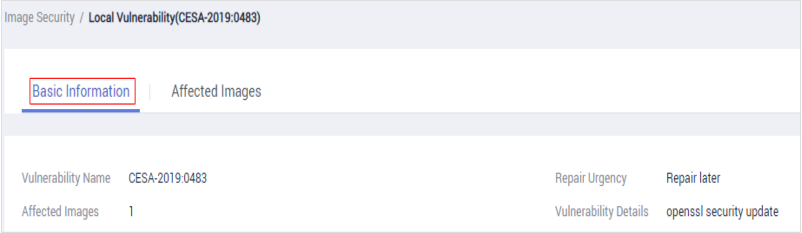


Image Security / Local Vulnerability(CESA-2019:0483)

Basic Information | Affected Images

Vulnerability Name CESA-2019:0483

Affected Images 1

Repair Urgency Repair later

Vulnerability Details openssl security update

Figure 5-3 Affected images

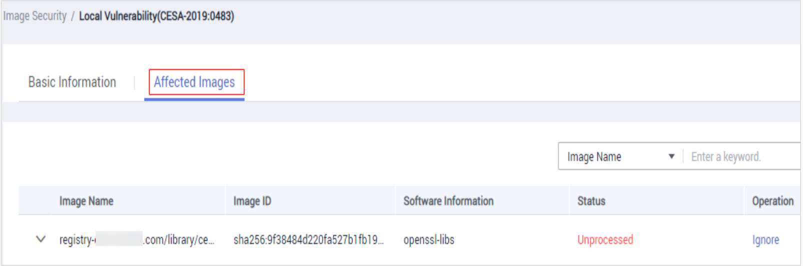


Image Security / Local Vulnerability(CESA-2019:0483)

Basic Information | Affected Images

Image Name ▾ Enter a keyword.

Image Name	Image ID	Software Information	Status	Operation
registry-[redacted].com/library/ce...	sha256:9f38484d220fa527b1fb19...	openssl-libs	Unprocessed	Ignore

----End

Ignoring a Vulnerability

A vulnerability with no risk or small risks can be ignored. After a vulnerability is ignored, the vulnerability is not counted for the image, but it is still in the vulnerability list.

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ≡, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Image Security**.

Step 4 Click **Image Vulnerabilities** and click **Local Image Vulnerabilities**.

Step 5 Ignore the impact of the vulnerability on all images, or ignore the impact of the vulnerability on an image. For details, see **Table 5-2**.

Table 5-2 Ignoring a vulnerability

Operation	Procedure
Ignoring the impact of a vulnerability in all images	1. In the vulnerability list, select a vulnerability to be ignored and click **Ignore** at the upper left corner. 2. In the displayed dialog box, click **OK** to ignore the selected vulnerability.

Operation	Procedure
Ignoring the impact of a vulnerability on an image	● Method 1: 1. In the vulnerability list, click the vulnerability name to view **Images Affected by a Vulnerability**. In the **Operation** column of the image, click **Ignore**. 2. In the displayed dialog box, click **OK** to ignore the vulnerability. ● Method 2: 1. Click the name of the image to view the vulnerability and its processing status. In the **Operation** column of the vulnerability, click **Ignore**. 2. In the displayed dialog box, click **OK** to ignore the vulnerability.

----End

Stopping Ignoring a Vulnerability

- Go to the vulnerability list, select the ignored vulnerability, and click **Cancel Ignorance** in the upper left corner of the vulnerability list to cancel ignoring a vulnerability.
- Go to the list of images affected by a vulnerability. In the **Operation** column of the image, click **Cancel Ignorance** to cancel ignoring a vulnerability.
- Go to the list of vulnerabilities in an image. In the row containing the vulnerability, click **Cancel Ignorance** in the **Operation** column to cancel ignoring a vulnerability.

5.2 Managing Private Image Vulnerabilities

This section describes how to view vulnerabilities in private images and rectify the vulnerabilities based on the suggestions.

Prerequisites

CGS service authorization has been approved.

Viewing Vulnerability List

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Image Security**.

Step 4 Click the **Private Image Vulnerabilities** tab.

Step 5 View the vulnerability percentage.

View the number and percentage of vulnerabilities by the urgency level.

Step 6 Go to the private image vulnerability page. For more information, see **Table 5-3**.

Table 5-3 Parameter description

Parameter	Description	Operation
Vulnerability Name	-	- Click ∨ to view the details of a vulnerability, including **CVE ID**, **CVSS Score**, **Disclosed**, and **Vulnerability Details**. - Click the vulnerability name to view the basic information and images affected by the vulnerability. For details, see **Step 7**.
Repair Urgency	Shows whether the vulnerability should be repaired immediately.	-
Affected Images	Shows the number of images that have been affected before.	-
Solution	Provides a solution to fix the vulnerability.	Click the link in the **Solution** column to view the solution.

Step 7 Click a vulnerability name to view the basic information about the affected images, as shown in **Figure 5-4** and **Figure 5-5**.

Figure 5-4 Basic information about a vulnerability in private images

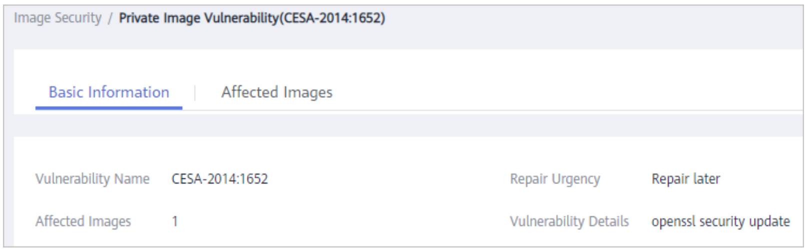


Image Security / Private Image Vulnerability(CESA-2014:1652)

Vulnerability Name CESA-2014:1652

Repair Urgency Repair later

Affected Images 1

Vulnerability Details openssl security update

Figure 5-5 Affected private images

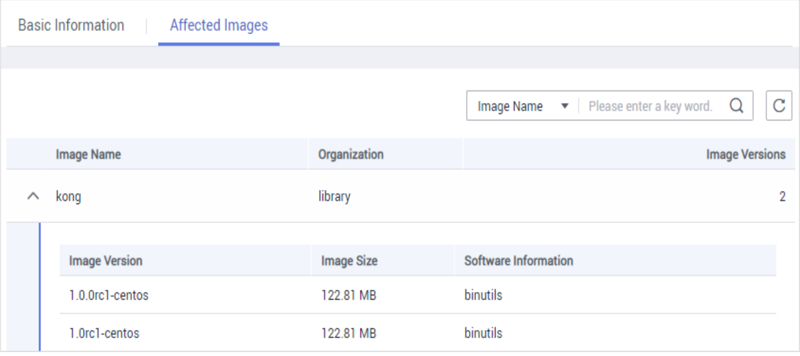


Image Name	Organization	Image Versions
kong	library	2

Image Version	Image Size	Software Information
1.0.0rc1-centos	122.81 MB	binutils
1.0rc1-centos	122.81 MB	binutils

----End

5.3 Managing Official Image Vulnerabilities

This section describes how to view vulnerabilities in official images and rectify the vulnerabilities based on the suggestions.

Prerequisites

CGS service authorization has been approved.

Viewing Vulnerability List

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ≡, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Image Security**.

Step 4 Click the **Official Image Vulnerabilities** tab.

Step 5 View the vulnerability percentage. View the number and percentage of vulnerabilities by the urgency level.

Step 6 Go to the official image vulnerability page. For details, see **Table 5-4**.

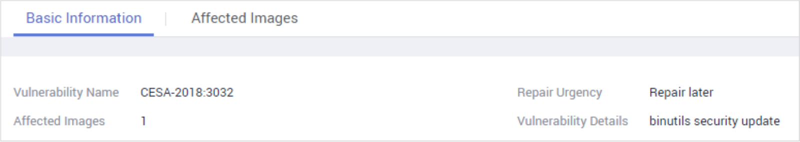
Table 5-4 Parameter description

Parameter	Description	Operation
Vulnerability Name	-	● Click ˅ to view the details of a vulnerability, including **CVE ID**, **CVSS Score**, **Disclosed**, and **Vulnerability Details**. ● Click the vulnerability name to view the basic information and images affected by the vulnerability. For details, see **Step 7**.

Parameter	Description	Operation
Repair Urgency	Shows whether the vulnerability should be repaired immediately.	-
Affected Images	Shows the number of images that have been affected.	-
Solution	Provides a solution to fix the vulnerability.	Click the link in the **Solution** column to view the solution.

Step 7 Click a vulnerability name to view the basic information about the affected images, as shown in **Figure 5-6** and **Figure 5-7**.

Figure 5-6 Basic information of a vulnerability in official images



Vulnerability Name CESA-2018:3032

Affected Images 1

Repair Urgency Repair later

Vulnerability Details binutils security update

Figure 5-7 Affected official images

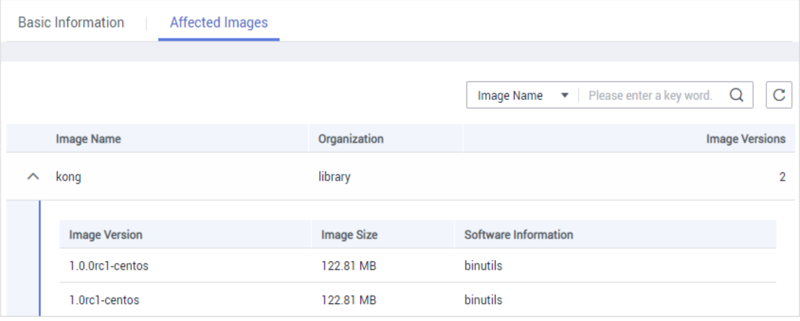


Image Name	Organization	Image Versions
kong	library	2

Image Version	Image Size	Software Information
1.0.0rc1-centos	122.81 MB	binutils
1.0rc1-centos	122.81 MB	binutils

----End

5.4 Viewing Malicious File Detection Results

CGS can automatically detect malicious files in the private images, helping you discover and eliminate the security threats in your assets.

Check Frequency

CGS automatically performs a comprehensive check in the early morning every day.

Prerequisites

The cluster protection function has been enabled.

Procedure

Step 1 Log in to the management console.

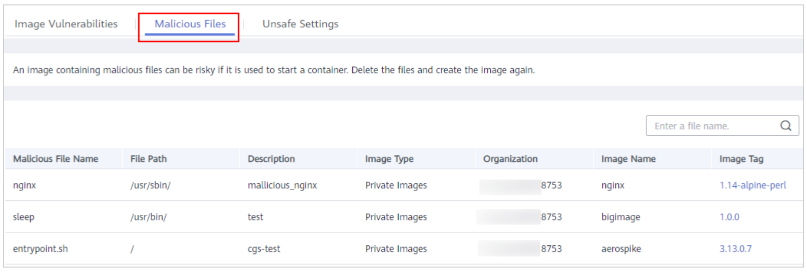
Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Image Security**.

Step 4 Click the **Malicious Files** tab to view details about malicious files in the private image repository, and delete the malicious files or create images again as needed based on the detection result.

- Malicious files include Trojan horses, worms, viruses, and adware.
- In the **Image Tag** column, click an image version to view its vulnerability report.

Figure 5-8 Malicious files



An image containing malicious files can be risky if it is used to start a container. Delete the files and create the image again.

Malicious File Name	File Path	Description	Image Type	Organization	Image Name	Image Tag
nginx	/usr/sbin/	mallicious_nginx	Private Images	[redacted]8753	nginx	1.14-alpine-perl
sleep	/usr/bin/	test	Private Images	[redacted]8753	bigimage	1.0.0
entrypoint.sh	/	cgs-test	Private Images	[redacted]8753	aerospike	3.13.0.7

----End

5.5 Viewing Unsafe Settings

CGS can scan your private image repository for unsafe configurations and provides suggestions for modifying the configurations, helping you fight intrusions and meet compliance requirements.

Check Frequency

CGS automatically performs a comprehensive check in the early morning every day.

Prerequisites

The cluster protection function has been enabled.

Procedure

Step 1 Log in to the management console.

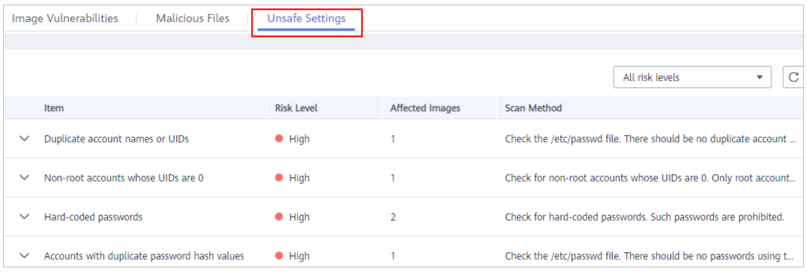
Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Image Security**.

Step 4 Click the **Unsafe Settings** tab and view the detected risks. You can filter risks by level.

In the drop-down list in the upper right corner of the unsafe settings list, select **All risk levels**, **High**, **Medium**, or **Low** to check unsafe settings of the level.

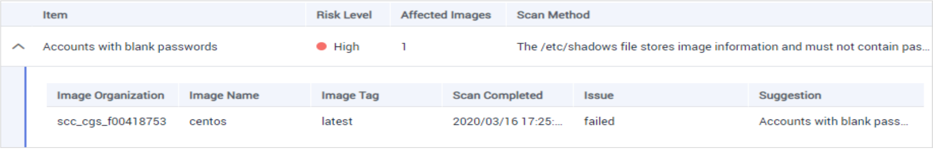
Figure 5-9 Viewing unsafe settings



Item	Risk Level	Affected Images	Scan Method
Duplicate account names or UIDs	● High	1	Check the /etc/passwd file. There should be no duplicate account ...
Non-root accounts whose UIDs are 0	● High	1	Check for non-root accounts whose UIDs are 0. Only root account...
Hard-coded passwords	● High	2	Check for hard-coded passwords. Such passwords are prohibited.
Accounts with duplicate password hash values	● High	1	Check the /etc/passwd file. There should be no passwords using t...

Step 5 Click ⌄ next to a check item to view its details and suggestions, and modify your unsafe settings accordingly.

Figure 5-10 Check item details



Item	Risk Level	Affected Images	Scan Method
Accounts with blank passwords	● High	1	The /etc/shadows file stores image information and must not contain pas...

Image Organization	Image Name	Image Tag	Scan Completed	Issue	Suggestion
scc_cgs_f00418753	centos	latest	2020/03/16 17:25:...	failed	Accounts with blank pass...

----End

6 Viewing Container Runtime Security Details

After you enabled cluster protection, the CGS shield will be installed as a daemonset, monitor container status on cluster nodes, report alarms on abnormal events, and provide solutions.

CGS can detect escapes, high-risk system calls, abnormal processes, abnormal files; and can check the container environment.

Check Frequency

CGS monitors containers running in the container cluster in real time. You can view container exception details at any time.

Prerequisites

Cluster Protection Status is **Enabled**.

Detection Mechanisms

Table 6-1 Runtime vulnerability detection

Check Item	Mechanism
Escapes	● Escape vulnerability attack CGS reports an alarm if it detects container process behavior that matches the behavior of known vulnerabilities (such as Dirty COW, brute-force attack, runC, and shocker). ● Escape file access CGS reports an alarm if it detects that a container process accesses a key file directory (for example, **/etc/shadow** or **/etc/crontab**). Directories that meet the container directory mapping rules can also trigger such alarms.

Check Item	Mechanism
High-risk system calls	CGS reports an alarm if it detects a high-risk call, such as open_by_handle_at, ptrace, setns, or reboot.
Abnormal processes	● Malicious container program CGS monitors container process behavior and process file fingerprints. It reports an alarm if it detects a process whose behavior characteristics match those of a predefined malicious program. ● Abnormal processes If you are sure that only specific processes run in a container, you can add the processes to the whitelist of a policy, and associate the policy with the container. CGS reports an alarm if it detects that a process not in the whitelist is running in the container.
Abnormal files	CGS monitors the container image files associated with file protection policies, and reports an alarm if the files are modified.

Check Item	Mechanism
Container environment	CGS monitors container startups and reports an alarm if it detects that a container with too many permissions is started. This alarm does not indicate an actual attack. Attacks exploiting this risk will trigger other CGS alarms. Container environment check items include: ● Privileged container startup (**privileged:true**) CGS reports an alarm if it detects a container started with the maximum permissions. Settings that can trigger such alarms include the **–privileged=true** parameter in the **docker run** command, and **privileged: true** in the **securityContext** of the container in a Kubernetes pod. The details of such alarms contain **privileged:true**. ● Too many container capabilities (**capability:[xxx]**) In Linux OSs, system permissions are divided into groups before assigned to containers. A container only has a limited number of permissions, and the impact scope of this container is limited in the case of an incident. However, malicious users can grant all the system permissions to a container by modifying its startup configurations. CGS reports an alarm containing **capabilities:[xxx]** if it detects a container started with too many capabilities. ● Seccomp not enabled (**seccomp=unconfined**) Secure computing mode (seccomp) is a Linux kernel feature. It can restrict system calls invoked by processes to reduce the attack surface of the kernel. If **seccomp=unconfined** is configured when a container is started, system calls will not be restricted for the container. CGS reports an alarm containing **seccomp=unconfined** if it detects a container started without enabling seccomp. **NOTE** If seccomp is enabled, permissions will be verified for every system call. The verifications will probably affect services if system calls are frequent. Before you decide whether to enable seccomp, you are advised to test-enable it and analyze the impact on your services. ● Container privilege escalation (**no-new-privileges:false**) CGS reports an alarm if it detects that a process attempts to escalate permissions by running the **sudo** command and using the SUID or SGID bit. If **–no-new-privileges=false** is specified when a container is started, the container can escalate privileges. Such alarms contain **no-new-privileges:false**, indicating that privileges are not restricted for the alarmed containers.

Check Item	Mechanism
	● High-risk directory mapping (**mounts:[...]**) For convenience purposes, when a container is started on a server, the directories of the server can be mapped to the container. In this way, services in the container can directly read and write resources on the server. However, this mapping incurs security risks. If any critical directory in the server OS is mapped to the container, improper operations in the container will probably damage the server OS. CGS reports an alarm if it detects that a critical server path (**/boot**, **/dev**, **/etc**, **/sys**, **/var/run**) is mounted during container startup. Such alarms contain **mounts: [{"source":"xxx","destination":"yyy"...]**. **NOTE** Alarms will not be triggered for the files that need to be frequently accessed by Docker containers, such as **/etc/hosts** and **/etc/resolv.conf**.

Procedure

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation pane, choose **Runtime Security**.

Step 4 Click a tab (**Escapes**, **High-risk System Calls**, **Abnormal Programs**, **Abnormal Files**, or **Container Environment**) to check the container security trends and exceptions.

- The container exception chart displays the exceptions in the past 30 days.
- In the exception list, you can view the exceptions in the past one day, three days, or seven days, and handle them based on the solution provided.

----End

7 Managing Images

7.1 Managing Local Images

Local images are container images that are used and started in the CCE cluster. CGS can scan these images. The local image list displays the basic information and security status of images.

This section describes how to view basic image information and vulnerability reports, and how to manage associated policies.

Prerequisites

- CGS service authorization has been approved.
- The cluster protection function has been enabled.

Viewing Local Images

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ≡, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Local Images** tab.

Table 7-1 Local image parameters

Parameter	Description	Operation
Image Name	Image name	Click ⌄ before the name of an image to view the versions of the image.
Image ID	ID of an image	-
Scan Status	Status of the image scan	-

Parameter	Description	Operation
Number of Vulnerabilities	Number of vulnerabilities detected in the image	-
Associated Policies	Number of policies applied in an image	-

----End

Viewing the Basic Information About a Local Image

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Local Image** tab and click the name of an image to view its basic information.

Step 5 View the basic information about the image version, as shown in **Figure 7-1**.

Figure 7-1 Basic information about a local image

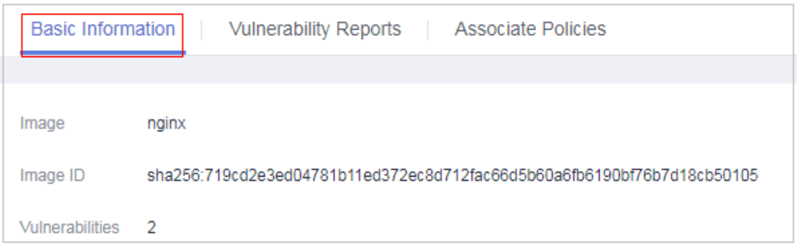


Image nginx

Image ID sha256:719cd2e3ed04781b11ed372ec8d712fac66d5b60a6fb6190bf76b7d18cb50105

Vulnerabilities 2

----End

Viewing Vulnerabilities in Local Images

After the scanning is complete, you can view the vulnerability report.

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Local Images** tab. In the row containing the image whose vulnerability report you want to view, click **View Report** in the **Operation** column.

Step 5 On the **Vulnerability Reports** tab, check the detected image vulnerabilities.

You can perform the following operations:

- Check the number and percentage of vulnerabilities of each urgency level.

  You can check the total number of vulnerabilities and the numbers of urgent and minor vulnerabilities.

- View vulnerabilities

  You can view the vulnerability name, urgency, software information, vulnerability location, and solution.

- Search for vulnerabilities

  In the upper part of the vulnerability list, you can select an urgency level (**Repair now**, **Repair later**, **No repair required now**) to filter vulnerabilities. You can also search for a vulnerability by its name or software information.

  NOTE

  Both vulnerability and software names support fuzzy search.

- Viewing basic information about a vulnerability and the images affected by the vulnerability

  Click a vulnerability name to go to the basic information page. Here you can view more details and the images affected by the vulnerability.

----End

Applying a Policy to a Local Image

You can apply a policy to a local image.

Step 1 Log in to the management console.

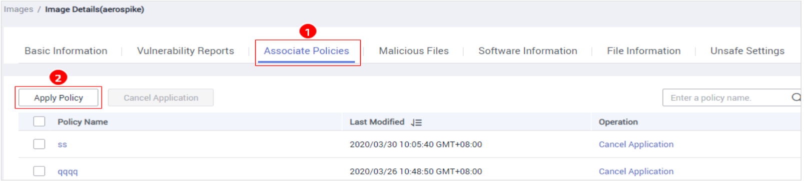
Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Local Images** tab and click the image name. The **Basic Information** page is displayed.

Step 5 Click the **Associate Policies** tab and click **Apply Policy**. See **Figure 7-2**.

Figure 7-2 Applying a policy



	Policy Name	Last Modified	Operation
□	ss	2020/03/30 10:05:40 GMT+08:00	Cancel Application
□	qqqq	2020/03/26 10:48:50 GMT+08:00	Cancel Application

Step 6 In the displayed dialog box, select the policy to be applied and click **OK**.

To cancel application of a policy, click **Cancel Application** in the **Operation** column of the policy.

----End

7.2 Managing Private Images

The images in the private image repository are from SWR. CGS can scan these images, and provide vulnerability reports and solutions. You can also check malicious file information, software information, file information, and baseline settings.

NOTE

After you agree to service authorization, you can scan private images for vulnerabilities free of charge. To check information about your software, files, and malicious files, or to check for unsafe settings, enable cluster protection first.

Precautions

- CGS service authorization has been approved.

Viewing the Private Image List

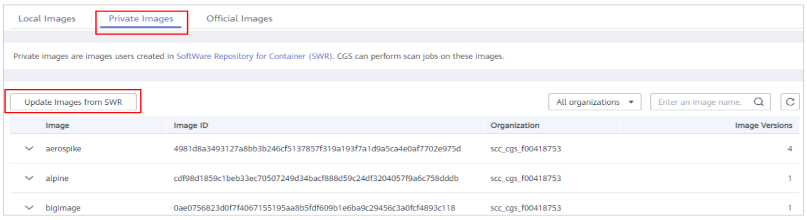
Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Private Images** tab, as shown in **Figure 7-3**.

Figure 7-3 Private images



Private images are images users created in SoftWare Repository for Container (SWR). CGS can perform scan jobs on these images.

Image	Image ID	Organization	Image Versions
aerospike	4981d8a3493127a8bb3b246cf5137857f319a193f7a1d9a5ca4e0af7702e975d	scc_cgs_f00418753	4
alpine	cdf98d1859c1beb33ec70507249d34bacf888d59c24df3204057f9a6c758dddb	scc_cgs_f00418753	1
bigimage	0ae0756823d0f7f4067155195aa8b5fdf609b1e6ba9c29456c3a0fcf4893c118	scc_cgs_f00418753	1

NOTE

You can click **Update Images from SWR** to update self-owned images from SWR.

Table 7-2 Parameters description

Parameter	Description	Operation
Image	Image name	Click ⌄ before the name of an image to view the versions of the image.
Image ID	Image ID	-

Parameter	Description	Operation
Organization	Name of the organization to which the image belongs. The image organization is managed by SWR.	-
Image Versions	Number of image versions	-

----End

Viewing Basic Information About a Private Image

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Private Images** tab and click ⌄ next to the image name to expand the image version list.

Step 5 View the basic information about the image version, as shown in **Figure 7-4**.

Figure 7-4 Basic information about the private image

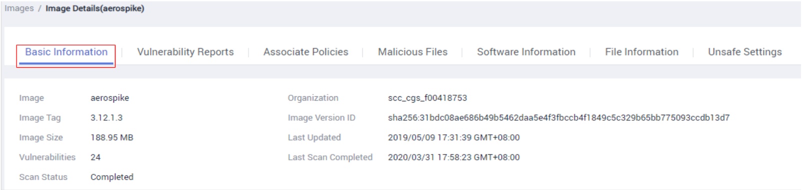


Image aerospike
Image Tag 3.12.1.3
Image Size 188.95 MB
Vulnerabilities 24
Scan Status Completed
Organization scc_cgs_f00418753
Image Version ID sha256:31bdc08ae686b49b5462daa5e4f3fbccb4f1849c5c329b65bb775093ccdb13d7
Last Updated 2019/05/09 17:31:39 GMT+08:00
Last Scan Completed 2020/03/31 17:58:23 GMT+08:00

----End

Scanning a Private Image

CGS automatically scans all private images in the early morning every day. You can also choose an image to scan.

The duration of a security scan depends on the scanned image size. Generally, an image can be completely scanned within 3 minutes.

After the scanning is complete, click **View Report** to check the vulnerability report. This section describes how to scan images.

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Private Images** tab and click ∨ next to the image name to expand the image list.

Step 5 Click **Scan** in the **Operation** column of the image version list.

Figure 7-5 Security scan

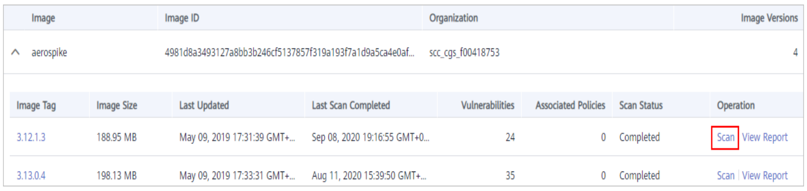


Image	Image ID	Organization	Image Versions
^ aerospike	4981d8a3493127a8bb3b246cf5137857f319a193f7a1d9a5ca4e0af...	scc_cgs_f00418753	4

Image Tag	Image Size	Last Updated	Last Scan Completed	Vulnerabilities	Associated Policies	Scan Status	Operation
3.12.1.3	188.95 MB	May 09, 2019 17:31:39 GMT+...	Sep 08, 2020 19:16:55 GMT+0...	24	0	Completed	Scan View Report
3.13.0.4	198.13 MB	May 09, 2019 17:33:31 GMT+...	Aug 11, 2020 15:39:50 GMT+...	35	0	Completed	Scan | View Report

Step 6 In the displayed dialog box, click **OK** to start the scan job.

----End

Viewing Vulnerabilities in Private Images

After the scanning is complete, you can view the vulnerability report.

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Private Images** tab and click ∨ next to the image name to expand the image list.

Step 5 Click **View Report** in the **Operation** column.

Figure 7-6 Private Images tab

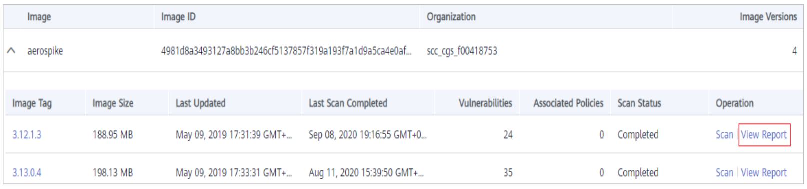


Image	Image ID	Organization	Image Versions
^ aerospike	4981d8a3493127a8bb3b246cf5137857f319a193f7a1d9a5ca4e0af...	scc_cgs_f00418753	4

Image Tag	Image Size	Last Updated	Last Scan Completed	Vulnerabilities	Associated Policies	Scan Status	Operation
3.12.1.3	188.95 MB	May 09, 2019 17:31:39 GMT+...	Sep 08, 2020 19:16:55 GMT+0...	24	0	Completed	Scan | View Report
3.13.0.4	198.13 MB	May 09, 2019 17:33:31 GMT+...	Aug 11, 2020 15:39:50 GMT+...	35	0	Completed	Scan | View Report

Step 6 Check the vulnerability overview of the image version.

- **Vulnerabilities**: number and percentage of vulnerabilities by the urgency level
- **Vulnerability Distribution by Severity**: number of vulnerabilities by the urgency level
- Vulnerability list: list of vulnerability details and solutions

----End

Applying a Policy to a Private Image

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

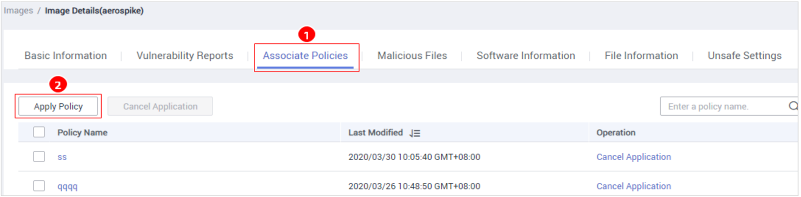
Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Private Images** tab and click ⌄ next to the image name to expand the image list.

Step 5 Click the image version.

Step 6 Click the **Associate Policies** tab and click **Apply Policy**, as shown in **Figure 7-7**.

Figure 7-7 Applying a policy



□	Policy Name	Last Modified	Operation
□	ss	2020/03/30 10:05:40 GMT+08:00	Cancel Application
□	qqqq	2020/03/26 10:48:50 GMT+08:00	Cancel Application

Step 7 In the displayed dialog box, select the policy to be applied and click **OK**.

To cancel application of a policy, click **Cancel Application** in the **Operation** column of the policy.

----End

Viewing Malicious Files on Private Images

After images are scanned, you can view malicious files on them. This section describes how to view malicious files in an image version.

For details about how to view malicious files in global private images, see **Viewing Malicious File Detection Results**.

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Private Images** tab and click ⌄ next to the image name to expand the image list.

Step 5 Click the image version.

Step 6 Click the **Malicious Files** tab to view malicious files on the image.

Figure 7-8 Malicious file in private images

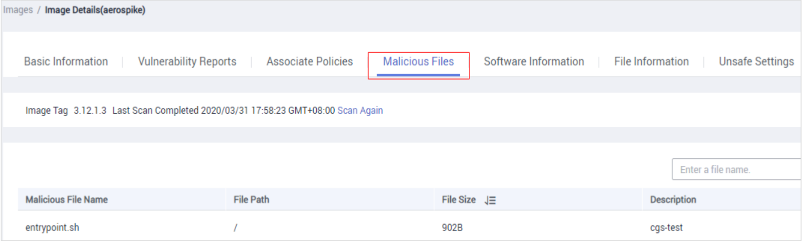


Image Tag 3.12.1.3 Last Scan Completed 2020/03/31 17:58:23 GMT+08:00 Scan Again

Malicious File Name	File Path	File Size	Description
entrypoint.sh	/	902B	cgs-test

----End

Viewing Software Information About a Private Image

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Private Images** tab and click ∨ next to the image name to expand the image list.

Step 5 Click the image version.

Step 6 Click the **Software Information** tab to view the software contained in the image version, software type, and number of vulnerabilities in the software.

Figure 7-9 Software information

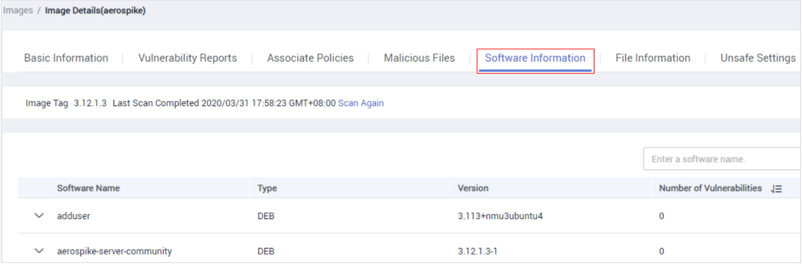


Image Tag 3.12.1.3 Last Scan Completed 2020/03/31 17:58:23 GMT+08:00 Scan Again

Software Name	Type	Version	Number of Vulnerabilities
∨ adduser	DEB	3.113+nmu3ubuntu4	0
∨ aerospike-server-community	DEB	3.12.1.3-1	0

Step 7 Click ∨ next to a software name to view the software vulnerability name, repair urgency, and solution.

----End

Viewing File Information About a Private Image

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Private Images** tab and click ∨ next to the image name to expand the image list.

Step 5 Click the image version.

Step 6 Click the **File Information** tab to view the file information about the image.

Quantities and sizes of software packages and non-attributable files, and top 50 non-attributable files are displayed.

Figure 7-10 File information

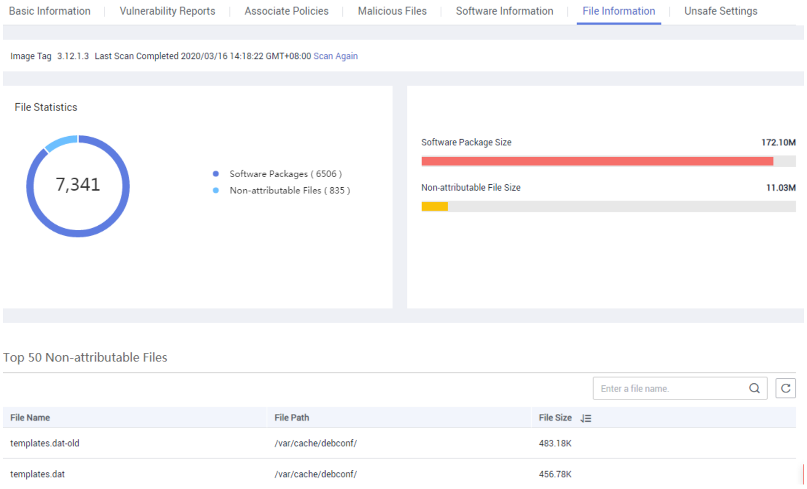


Image Tag 3.12.1.3 Last Scan Completed 2020/03/16 14:18:22 GMT+08:00

- Software Packages (6506)
- Non-attributable Files (835)

Software Package Size 172.10M

Non-attributable File Size 11.03M

Top 50 Non-attributable Files

File Name	File Path	File Size
templates.dat-old	/var/cache/debconf/	483.18K
templates.dat	/var/cache/debconf/	456.78K

----End

Viewing the Unsafe Settings of a Private Image

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Private Images** tab and click ⌄ next to the image name to expand the image list.

Step 5 Click the image version.

Step 6 Click the **Unsafe Settings** tab to view unsafe settings and modify configurations based on suggestions provided.

Figure 7-11 Unsafe settings of a private image

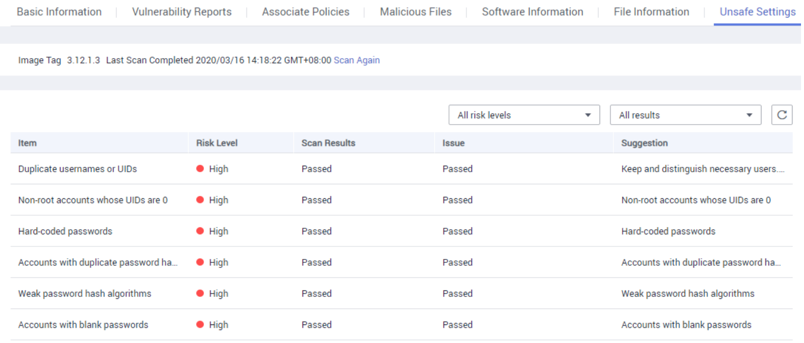


Image Tag 3.12.1.3 Last Scan Completed 2020/03/16 14:18:22 GMT+08:00 Scan Again

Item	Risk Level	Scan Results	Issue	Suggestion
Duplicate usernames or UIDs	● High	Passed	Passed	Keep and distinguish necessary users....
Non-root accounts whose UIDs are 0	● High	Passed	Passed	Non-root accounts whose UIDs are 0
Hard-coded passwords	● High	Passed	Passed	Hard-coded passwords
Accounts with duplicate password ha...	● High	Passed	Passed	Accounts with duplicate password ha...
Weak password hash algorithms	● High	Passed	Passed	Weak password hash algorithms
Accounts with blank passwords	● High	Passed	Passed	Accounts with blank passwords

----End

7.3 Managing Official Images

The images in the official image repository are from SWR. CGS can scan these images.

This section describes how to view the official image list, basic information about an image version, and image vulnerabilities; and the policies for managing official images.

NOTE

After you agree to service authorization, you can scan official images for vulnerabilities free of charge. CGS automatically performs the scan.

Viewing the Official Image List

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Official Images** tab.

----End

Viewing the Basic Information About an Official Image

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Official Images** tab and click ˅ next to the image name to expand the image version list.

Step 5 View its basic information. See **Figure 7-12**.

Figure 7-12 Basic information about an official image

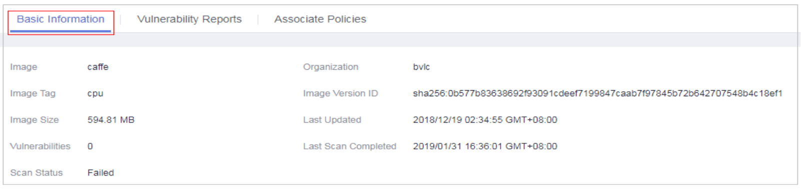


Image	caffe	Organization	bvlc
Image Tag	cpu	Image Version ID	sha256:0b577b83638692f93091cdeef7199847caab7f97845b72b642707548b4c18ef1
Image Size	594.81 MB	Last Updated	2018/12/19 02:34:55 GMT+08:00
Vulnerabilities	0	Last Scan Completed	2019/01/31 16:36:01 GMT+08:00
Scan Status	Failed		

----End

Viewing Vulnerabilities in Official Images

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

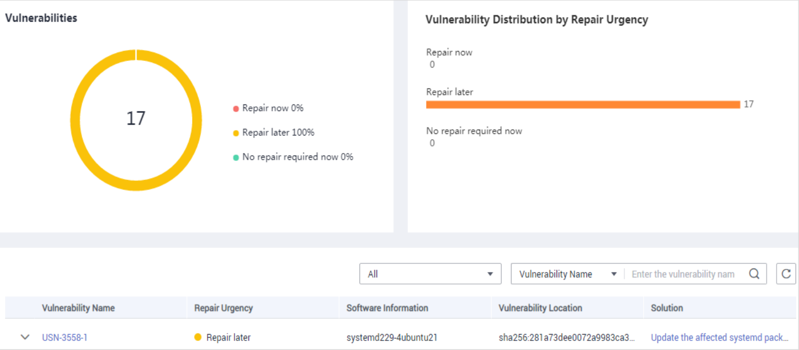
Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Official Images** tab and click ⌄ next to the image name to expand the image version list.

Step 5 Click **View Report** in the **Operation** column.

Step 6 Check the vulnerabilities in the image.

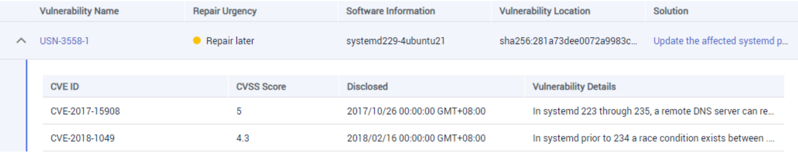
Figure 7-13 Official image vulnerabilities



Vulnerability Name	Repair Urgency	Software Information	Vulnerability Location	Solution
USN-3558-1	● Repair later	systemd229-4ubuntu21	sha256:281a73dee0072a9983ca3...	Update the affected systemd pack...

Step 7 Click ⌄ next to the **Vulnerability Name** to view the details.

Figure 7-14 Vulnerability details



Vulnerability Name	Repair Urgency	Software Information	Vulnerability Location	Solution
USN-3558-1	● Repair later	systemd229-4ubuntu21	sha256:281a73dee0072a9983c...	Update the affected systemd p...

CVE ID	CVSS Score	Disclosed	Vulnerability Details
CVE-2017-15908	5	2017/10/26 00:00:00 GMT+08:00	In systemd 223 through 235, a remote DNS server can re...
CVE-2018-1049	4.3	2018/02/16 00:00:00 GMT+08:00	In systemd prior to 234 a race condition exists between ....

----End

Applying a Policy to an Official Image

You can apply a policy to an official image.

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

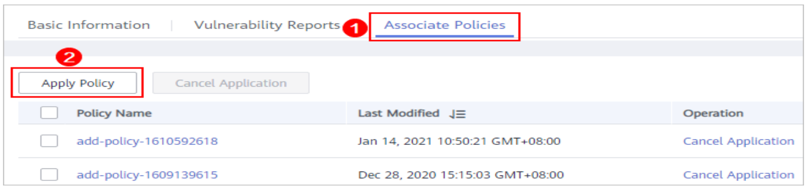
Step 3 In the navigation tree on the left, choose **Images**.

Step 4 Click the **Official Images** tab and click ∨ next to the image name to expand the image version list.

Step 5 Click the image version.

Step 6 Click the **Associate Policies** tab and click **Apply Policy**. See **Figure 7-15**.

Figure 7-15 Applying a policy



☐	Policy Name	Last Modified	Operation
☐	add-policy-1610592618	Jan 14, 2021 10:50:21 GMT+08:00	Cancel Application
☐	add-policy-1609139615	Dec 28, 2020 15:15:03 GMT+08:00	Cancel Application

Step 7 In the displayed dialog box, select the policy to be applied and click **OK**.

To cancel application of a policy, click **Cancel Application** in the **Operation** column of the policy.

----End

8 Viewing Clusters and Quotas

The cluster list displays the security protection status of clusters in CCE. You can obtain the basic information about a cluster and a node from the cluster list and node list.

Prerequisites

CGS service authorization has been approved.

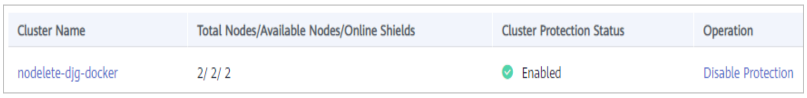
Viewing Clusters

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 Check cluster protection information. **Table 8-1** describes cluster parameters.

Figure 8-1 Clusters



Cluster Name	Total Nodes/Available Nodes/Online Shields	Cluster Protection Status	Operation
nodelete-djg-docker	2/ 2/ 2	● Enabled	Disable Protection

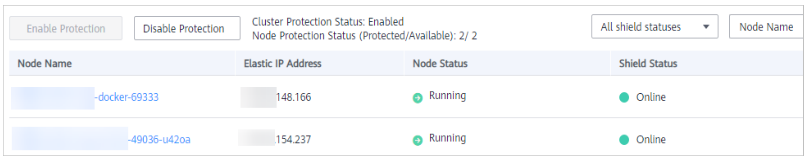
Table 8-1 Cluster parameters

Parameter	Description
Cluster Name	Name of a cluster **NOTE** Click the name of a cluster and the node list is displayed.
Total Nodes/Available Nodes/Online Shields	● **Total Nodes**: Total number of nodes in a cluster ● **Available Nodes**: Number of nodes whose **Node Status** is **Running** ● **Online Shields**: Number of nodes whose **Shield Status** is **Online**

Parameter	Description
Cluster Protection Status	Protection status of a cluster. The options are: ● **Disabled** ● **Enabled**

Step 4 Click the name of a cluster, and the node list is displayed, as shown in **Figure 8-2**.

Figure 8-2 Nodes



Cluster Protection Status: Enabled
Node Protection Status (Protected/Available): 2/ 2

Node Name	Elastic IP Address	Node Status	Shield Status
[redacted]-docker-69333	[redacted]148.166	Running	● Online
[redacted]-49036-u42oa	[redacted].154.237	Running	● Online

Step 5 Check the node list. It contains the following information:

- **Node Status**: **Running** or **Unavailable**
- **Shield Status**: **Unregistered**, **Online**, or **Offline**

----End

9 Disabling Protection for a Cluster

If CGS is not required, disable protection for a cluster by referring to this section.

Disabling the protection will automatically uninstall the CGS plug-in from the cluster.

Prerequisites

- CGS service authorization has been approved.
- **Cluster Protection Status** is **Enabled**.

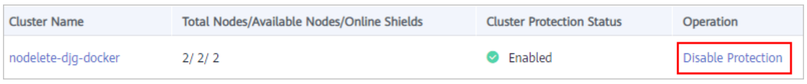
Procedure

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 Locate the row containing the target cluster and click **Disable Protection** in the **Operation** column.

Figure 9-1 Disabling protection



Cluster Name	Total Nodes/Available Nodes/Online Shields	Cluster Protection Status	Operation
nodelete-djg-docker	2/ 2/ 2	● Enabled	Disable Protection

NOTE

Click the name of a cluster to go to the node list page. You can also click **Disable Protection** on the top of the node list.

Step 4 In the displayed dialog box, click **Yes**.

After protection is disabled, **Cluster Protection Status** of the cluster is **Disabled**, indicating that protection has been disabled for all available nodes in the cluster.

📖 NOTE

Disabling protection will automatically uninstall the CGS plug-in from the cluster.

----End

10 Auditing

10.1 Supported CGS Operations

Cloud Trace Service (CTS) records all cloud service operations on CGS, including requests initiated from the management console and responses to the requests, for tenants to query, audit, and trace.

Table 10-1 lists CGS operations supported by CTS.

Table 10-1 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
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

Operation	Resource Type	Trace Name
Unignoring of images affected by the vulnerability	cgs	cancelIgnoreImageVul
Unauthorized access	cgs	registeCgsAgency
Manually scanning images	cgs	scanPrivateImage
Obtaining and scanning images from Software Repository for Container (SWR)	cgs	syncSwrPrivateImage

10.2 Viewing Audit Logs

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

Viewing a CGS Trace on the CTS Console

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, click ☰ and choose **Management & Deployment** > **Cloud Trace Service**.

Step 3 Choose **Trace List** in the navigation pane on the left.

Step 4 Specify the filters used for querying traces. You can select one or more of the following filters to query your traces:

- **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**.

  Select the desired filter criterion from the drop-down list.

  – Set **Trace Type** to **Management**.

  – Set **Trace Source** to **CGS**.

  – When you select **Trace name** for **Search By**, you also need to select a specific trace name. When you select **Resource ID** for **Search By**, you also need to select or enter a specific resource ID. When you select **Resource name** for **Search By**, you also need to select or enter a specific resource name.

- **Operator**: Select a specific operator (a user rather than tenant).

- **Trace Status**: Available options include **All trace statuses**, **normal**, **warning**, and **incident**. You can only select one of them.

- **Time Range**: In the upper right corner of the page, you can query traces in the last 1 hour, last 1 day, last 1 week, or within a customized period.

Step 5 Click **Query**.

Step 6 Click ⌄ on the left of a trace to expand its details.

Step 7 Click **View Trace** in the **Operation** column. In the displayed **View Trace** dialog box, the trace structure details are displayed.

----End

11 Managing Permissions

11.1 CGS Custom Policies

Custom policies can be created to supplement the system-defined policies of CGS. For the actions that can be added to custom policies, see **Permissions and Supported Actions**.

Example Custom Policies

- Example 1: Allowing users to query the cluster list

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cgs:cluster:list"
            ]
        }
    ]
}
```

- Example 2: Preventing users from modifying configurations

  A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the policies assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

  The following method can be used if you need to assign permissions of the **CGS FullAccess** policy to a user but also forbid the user from modifying CGS configurations. Create a custom policy to disallow configuration modification and assign both policies to the group the user belongs to. Then the user can perform all operations on CGS except modifying configurations. The following is an example of a deny policy:

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Action": [
                                "cgs:configuration:operate"
                        ],
                        "Effect": "Deny"
                }
```

```
    ]
}
```

- Example 3: Defining permissions for multiple services in a policy

  A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cgs:cluster:list",
                "cgs:quota:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "hss:accountCracks:unblock",
                "hss:commonIPs:set"
            ]
        }
    ]
}
```

11.2 CGS Permissions and Supported Actions

This section describes fine-grained permissions management for your CGS resources. If your account does not need individual IAM users, you can skip this section.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies to these groups. Users inherit permissions from their groups and can perform operations on cloud services as allowed by the permissions.

You can grant users permissions by using roles and policies. Roles are a type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Policies define API-based permissions for operations on specific resources under certain conditions, allowing for more fine-grained, secure access control of cloud resources.

Supported Actions

CGS provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- Permission: a statement in a policy that allows or denies certain operations.
- Actions: added to a custom policy to control permissions for specific operations

Permission	Action	Related Action
Obtain CGS quota statistics.	cgs:quota:get	-
Query system process information.	cgs:cluster:list	● cce:addonInstance:* ● cce:node:list ● cce:cluster:list
Enable or disable protection for a container cluster.	cgs:cluster:operate	● cce:addonInstance:*
Query the image list.	cgs:images:list	-
Synchronize and scan images.	cgs:images:operate	-
Query container image information.	cgs:images:get	-
Query configurations.	cgs:configuration:list	-
Modify configurations.	cgs:configuration:operate	-
Query image security information.	cgs:imageSecure:list	-
Handle image security events.	cgs:imageSecure:operate	-
Obtain image scanning results.	cgs:imageSecure:get	-
Obtain the runtime event list.	cgs:runtimeSecure:list	-
Obtain runtime monitoring information.	cgs:runtimeSecure:get	-
Handle runtime monitoring events.	cgs:runtimeSecure:operate	-
Handle security agency authorization for CGS.	cgs:privilege:operate	-
Query CGS authorization.	cgs:privilege:get	-

12 FAQs

12.1 How Do I Enable Cluster Protection?

Perform the following steps to enable protection, which will automatically install the CGS plug-in in the cluster.

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ≡, and choose **Security** > **Container Guard Service**.

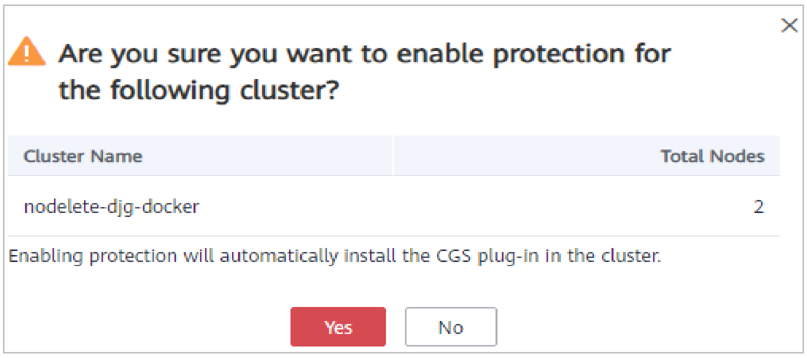
Step 3 Locate the row containing the target cluster and click **Enable Protection** in the **Operation** column.

> NOTE
>
> Click the name of a cluster to go to the node list page. You can also click **Enable Protection** on the top of the node list.

Step 4 In the dialog box that is displayed, confirm the cluster name and the number of nodes are correct, and click **Yes**.

After protection is enabled, **Cluster Protection Status** of the cluster is **Enabled**, indicating that protection has been enabled for all available nodes in the cluster.

Figure 12-1 Enabling protection



Are you sure you want to enable protection for the following cluster?

Cluster Name	Total Nodes
nodelete-djg-docker	2

Enabling protection will automatically install the CGS plug-in in the cluster.

NOTE

- CGS automatically enables protection for the new node in the cluster when a new node is added to a cluster with protection enabled.
- Enabling protection will automatically install the CGS plug-in in the cluster.

----End

12.2 How Do I Disable Cluster Protection?

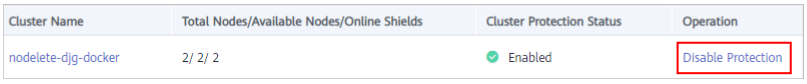
Perform the following steps to disable protection, which will automatically uninstall the CGS plug-in from the cluster.

Step 1 Log in to the management console.

Step 2 In the upper part of the page, select a region, click ☰, and choose **Security** > **Container Guard Service**.

Step 3 Locate the row containing the target cluster and click **Disable Protection** in the **Operation** column.

Figure 12-2 Disabling protection



Cluster Name	Total Nodes/Available Nodes/Online Shields	Cluster Protection Status	Operation
nodelete-djg-docker	2/ 2/ 2	● Enabled	Disable Protection

NOTE

Click the name of a cluster to go to the node list page. You can also click **Disable Protection** on the top of the node list.

Step 4 In the displayed dialog box, click **Yes**.

After protection is disabled, **Cluster Protection Status** of the cluster is **Disabled**, indicating that protection has been disabled for all available nodes in the cluster.

NOTE

Disabling protection will automatically uninstall the CGS plug-in from the cluster.

----End

12.3 What Should I Do If the Shield on a Node Is Offline?

If the shield on a node is offline, check the following items:

- Whether the CGS plug-in has been installed in the cluster

  CGS automatically installs the shield on a cluster when you enable protection for the cluster on the CGS console, and uninstalls it when you disable protection. If protection is not enabled for a cluster, the shield is offline.
- Whether cluster node status is normal

The shield will be online only if node where you installed it is running. If the node status is abnormal, go to CCE to fix it.

- After the shield is installed for the first time, it takes a maximum of 5 minutes for the shield status to change to **Online**. After you enable protection, wait for a while before checking the shield status.

12.4 What Should I Do If I Have No Service Authorization Permissions or Fail to Create an Agency as an IAM User?

If you log in to the CGS console as an IAM user and find the **Authorize** button grayed out, it indicates that the IAM user does not have the required permissions. In this case, contact the administrator with the **Security Administrator** permission to grant the permissions or use the IAM account to apply for and obtain the permissions.

If the number of agencies in your account has reached the maximum, an agency will fail to be created.

After authorization, if the agency fails to be created for CGS, it is probably because the number of agencies already reaches the upper limit. In this case, log in to the IAM console and delete unnecessary agencies, or contact IAM technical support to increase the agency quota.

12.5 When Does CGS Update and Back Up Logs?

CGS updates logs in its log file every 10 minutes. If the file exceeds 30 MB, CGS will back up the latest 30 MB logs to a backup file and clear the content of the log file.

The name of the backup log file is the name of the log file plus the extension **.last**. For example, the backup file of **shield.log** is **shield.log.last**.

12.6 Where Can I Find My CGS Logs?

CGS logs are stored in the **/var/log/shield** directory of the server where CGS is deployed.

Log files include:

- **shield.log**: CGS run logs and error logs
- **message.log**: communication between the CGS agent and server, such as policy delivery and alarm reporting
- **defender_audit.log**: audit system logs. This file stores audit messages triggered by the audit rules that you manually configured but not used for CGS (if any).

12.7 Does the Shield Plug-in of CGS Affect My Services?

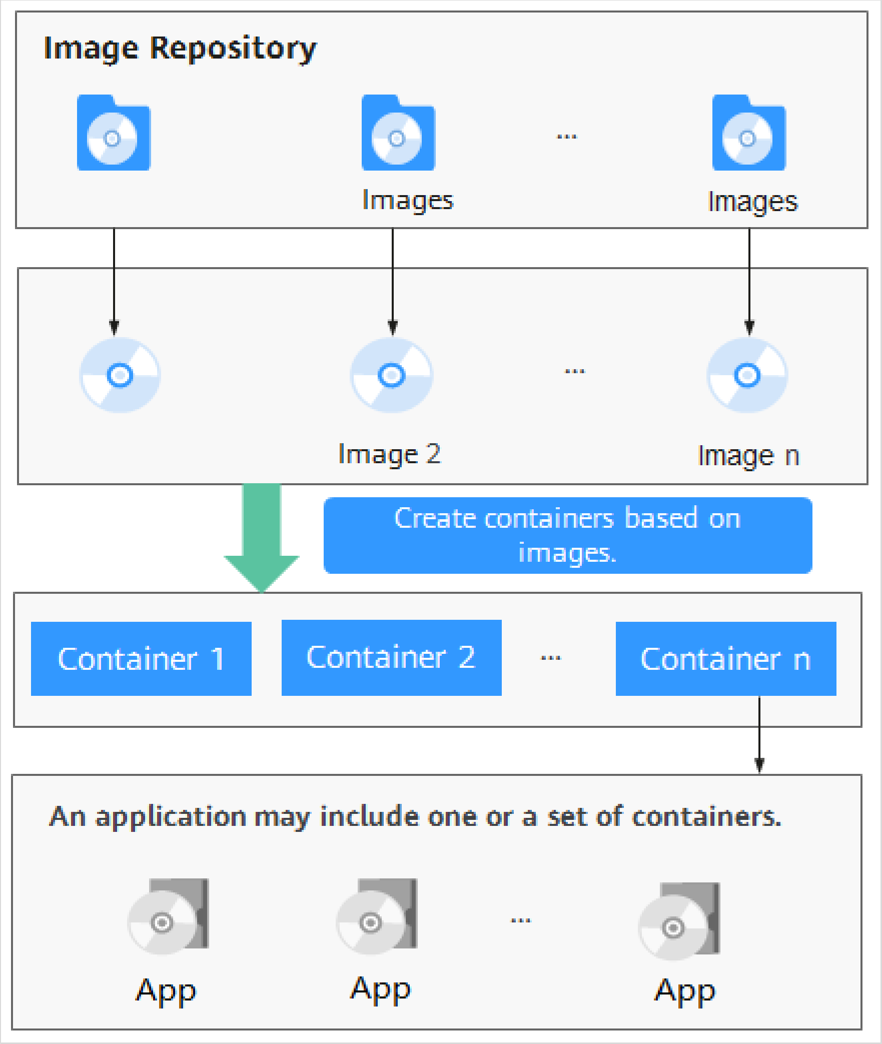
No. The CGS shield is installed as a daemonset plug-in and runs on each node of a cluster in container mode. When the shield plug-in is started, it requests a fixed amount of resources (0.3 vCPU and 300 MB memory). After the shield plug-in is started, it monitors started containers without affecting your services.

12.8 What Are the Relationships Between Images, Containers, and Applications?

- An image is a special file system. It provides programs, libraries, resources, configuration files and other files required for a running container. An image also contains some configuration parameters (such as anonymous volumes, environment variables, and users) prepared for a running container. An image does not contain any dynamic data, and its content is unchangeable after creation.
- A container is to an image what an instance is to a class in computer programming. An image is static, and a container is the entity for a running image. A container can be created, started, stopped, deleted, and suspended.
- Multiple containers can be started for an image.
- An application may include one or a set of containers.

Figure 12-3 shows the relationships between images, containers, and applications.

Figure 12-3 Relationships between images, containers, and applications



A Change History

Released On	Description
2021-06-15	This is the second official release. Added section "Permissions Management".
2021-01-27	This is the first official release.