

Container Guard Service

User Guide

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

1 Cluster Protection	1
1.1 Service Authorization	1
1.2 Purchasing CGS Quota	2
1.3 Enabling Protection for a Cluster	3
1.4 Enabling Alarm Notification	5
2 (Optional) Configuring Policies	7
3 Image Security	10
3.1 Managing Local Image Vulnerabilities	10
3.2 Managing Private Image Vulnerabilities	13
3.3 Managing Official Image Vulnerabilities	15
3.4 Viewing Malicious File Detection Results	16
3.5 Viewing Unsafe Settings	17
4 Viewing Container Runtime Security Details	19
5 Managing Images	24
5.1 Managing Local Images	24
5.2 Managing Private Images	27
5.3 Managing Official Images	36
6 Viewing Clusters and Quotas	39
7 Disabling Protection for a Cluster	42
8 Auditing	43
8.1 Supported CGS Operations	43
8.2 Viewing Audit Logs	44
9 Managing Permissions	46
9.1 Creating a User and Granting Permissions	46
9.2 CGS Custom Policies	48
9.3 CGS Permissions and Supported Actions	49
A Change History	52

1 Cluster Protection

1.1 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 (with the global Security Administrator permission) 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 & Compliance > Container Guard Service**.

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 system administrator to increase the agency quota.

----End

1.2 Purchasing CGS Quota

CGS provides the enterprise edition.

- The enterprise edition is recommended if you would like to have a comprehensive picture for your asset security on the cloud in a timely manner.

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 alarm and security settings.

The price is calculated based on the number of protected nodes.


This section describes how to purchase enterprise edition CGS.

Constraints

- CGS service authorization has been approved.
- 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 login account and password for logging in to the management console.

Procedure

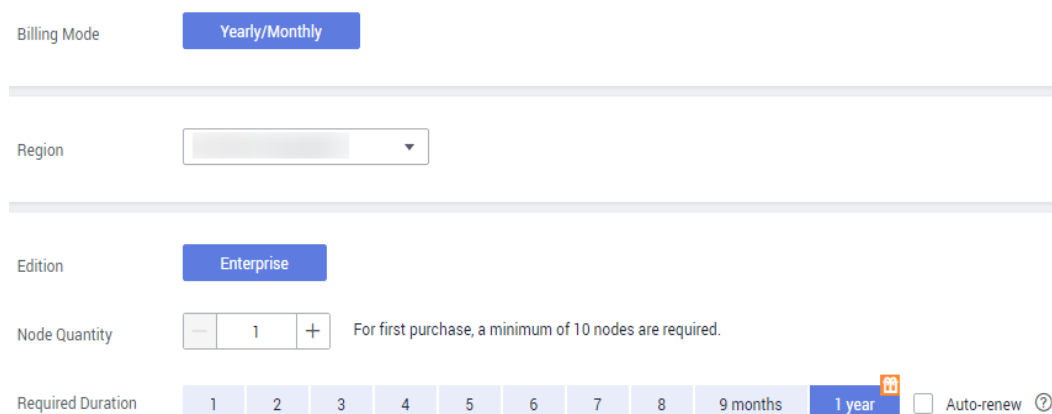
Step 1 [Log in to the management console.](#)

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

Step 3 In the upper right corner, click **Buy CGS.**

Step 4 On the **Buy CGS** page, configure the parameters based on [Figure 1-1](#), as shown in [Table 1-1](#).

Figure 1-1 Buying CGS quota



The screenshot shows the configuration interface for buying CGS quota. It includes the following elements:

- Billing Mode:** A button labeled "Yearly/Monthly".
- Region:** A dropdown menu.
- Edition:** A button labeled "Enterprise".
- Node Quantity:** A numeric input field with a value of "1" and minus/plus buttons. A note states: "For first purchase, a minimum of 10 nodes are required."
- Required Duration:** A row of buttons for durations: "1", "2", "3", "4", "5", "6", "7", "8", "9 months", "1 year" (which is highlighted), and "Auto-renew" (with an unchecked checkbox and a help icon).

Table 1-1 Parameter description

Parameter	Description
Billing Mode	Select Yearly/Monthly .
Region	Select a region from the drop-down list. NOTICE <ul style="list-style-type: none"> 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.
Edition	Enterprise
Node Quantity	Indicates the CGS quota you purchase. NOTE <ul style="list-style-type: none"> The minimum quota in the first purchase is 10. One protection quota can protect a cluster node.
Required Duration	The duration ranges from a month to a year. NOTE The Auto-renew option is optional. If the Auto Renew option is selected, upon expiration of the service, the system automatically renew your service subscription according to the required duration specified here.

Step 5 In the lower right corner of the page, click **Next**.

----End

1.3 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 pod on each compute node in the cluster to monitor and scan the status and events of 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 & Compliance > Container Guard Service.**

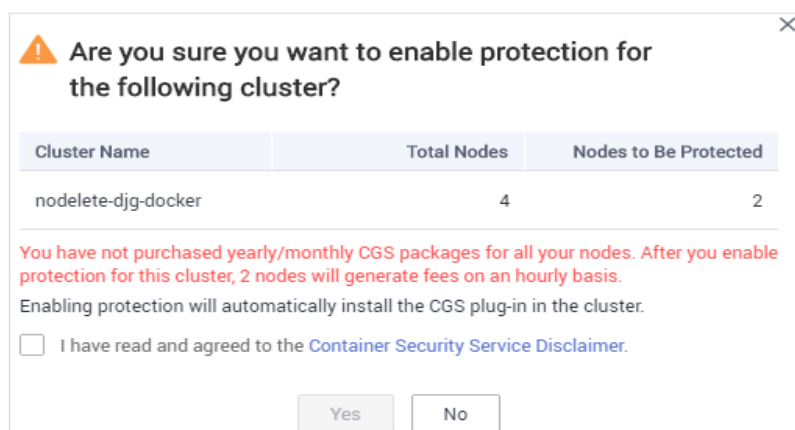
Step 3 Locate the row containing the target cluster and click **Enable Protection** in the **Operation** column.

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 displayed dialog box, read and select **I have read and agreed to the Container Guard Service Disclaimer**, and click **OK.**

Figure 1-2 Enabling protection



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.

NOTE

- If you enable CGS for more nodes than can be protected by the yearly/monthly packages you have purchased, you will be charged on an hourly basis for protection of the excess nodes. For details, see [When and How Will CGS Be Charged Per Use?](#)
- CGS automatically enables protection for a new node in the cluster when the node is added to a cluster with protection enabled.
- Enabling protection will automatically install the CGS plug-in in the cluster.

----End

References

- After enabling CGS, you can define security policies by configuring a process whitelist and file protection list to prevent risks during the running of the container, keeping systems and applications secure. For details about how to configure security policies, see [\(Optional\) Configuring Policies](#).
- To disable cluster protection, follow the instructions provided in [Disabling Protection for a Cluster](#).

- To troubleshoot an offline shield, follow the instructions provided in [What Should I Do If the Shield on a Node Is Offline?](#)


1.4 Enabling Alarm Notification

You can enable alarm notification to get notified of image and container risks via email or SMS. Without this function, you have to log in to the management console to view alarms.

- Alarm notification settings are effective only for the current region. To receive notifications from another region, switch to that region and configure alarm notification.
- Alarm notifications may be mistakenly blocked. If you do not receive any alarm notifications, check whether they have been blocked as spams.
- To set recipients, go to the Message Center and choose **Message Receiving Management > SMS & Email Settings**. In the **Security** area, click **Modify** in the row where **Security event** resides.

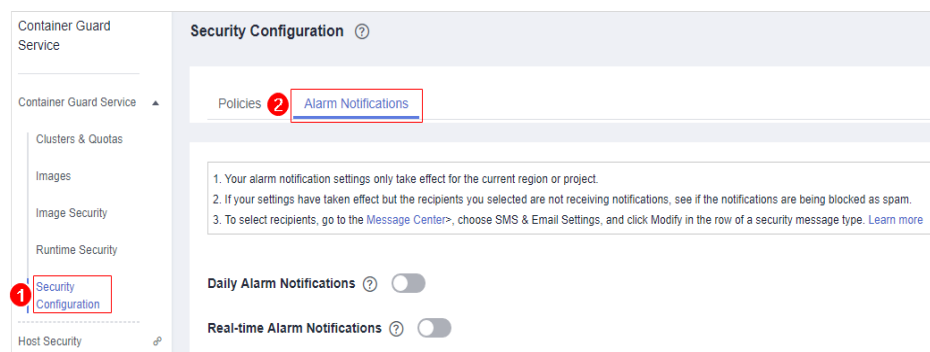
Procedure

Step 1 [Log in to the management console](#).

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

Step 3 On the **Security Configuration** page, click the **Alarm Notifications** tab, as shown in [Figure 1-3](#).

Figure 1-3 Alarm configurations



Step 4 Enable **Daily Alarm Notifications**.

NOTE

Daily alarm notifications are sent once a day. If no alarms have been reported in the last 24 hours, no notifications will be sent.

Step 5 Enable **Real-time Alarm Notifications**.

 **NOTE**

- Real-time alarm notifications are sent immediately when an exception occurs.
- In a region, up to 10 real-time notifications can be sent every day, and the minimum interval between notifications is 5 minutes.

----End

2 (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 & Compliance > Container Guard Service**.

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

Step 4 Click the **Policies** tab. In the upper part of the policy list, click **Add**.

Step 5 On the displayed page, configure the policy. See [Figure 2-1](#). For details, see [Table 2-1](#).

Figure 2-1 Add dialog box

The 'Add' dialog box contains the following elements:

- Policy Name:** A text input field with a red border and placeholder text 'Enter a policy name.'. Below it, a note states: 'Enter a maximum of 24 characters starting with a letter. Only letters, digits, and hyphens (-) are allowed.'
- Process Whitelist:** A large text area for listing paths. Below it, a note states: '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:** A large text area for listing file paths. Below it, a note states: 'You can enter a maximum of 50 complete paths of read-only files in the container. Enter only one path in a line.'
- Buttons:** 'OK' and 'Cancel' buttons at the bottom center.

Table 2-1 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](#).

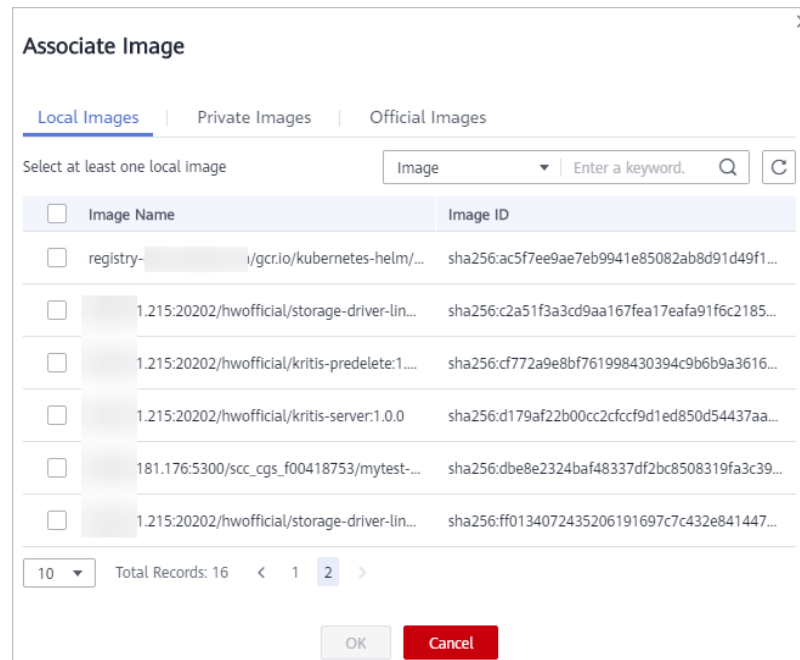
Step 2 In the upper part of the page, select a region, click , and choose **Security & Compliance > Container Guard Service**.

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

Step 4 Click the **Policies** tab. 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 2-2](#).

Figure 2-2 Associate Image dialog box



Step 6 Select an image and click **OK**.

After the image is associated, you can view the monitoring results of malicious files and container exceptions in the image file. For details, see [Viewing Malicious File Detection Results](#) and [Viewing Container Runtime Security Details](#).

----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.

3 Image Security

3.1 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 & Compliance > Container Guard Service**.

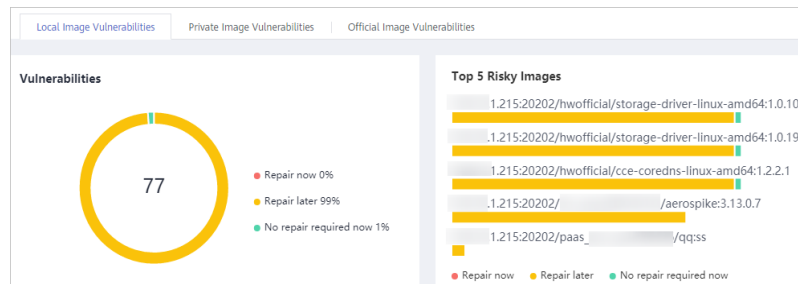
Step 3 In the navigation pane on the left, choose **Image Security**.

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 3-1 Local image vulnerability overview



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. For more information, see [Table 3-1](#).

Table 3-1 Parameter description

Parameter	Description	Operation
Vulnerability Name	-	<ul style="list-style-type: none"> Click to view the details of a vulnerability, including CVE ID, CVSS Score, Disclosed, and Vulnerability Details. Click a vulnerability name 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 3-2](#) and [Figure 3-3](#).

Figure 3-2 Basic information about a vulnerability in local images

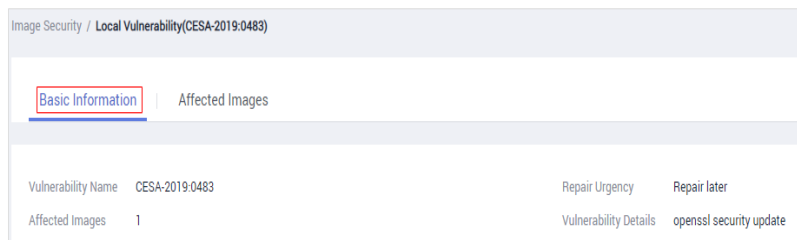
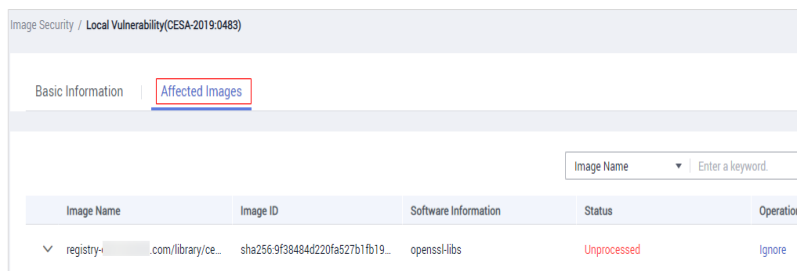


Figure 3-3 Affected images



----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 & Compliance > Container Guard Service**.
- Step 3** In the navigation pane 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 3-2](#).

Table 3-2 Ignoring a vulnerability

Operation	Procedure
Ignoring the impact of a vulnerability on all images	<ol style="list-style-type: none"> In the vulnerability list, select a vulnerability to be ignored and click Ignore at the upper left corner. In the displayed dialog box, click OK to ignore the selected vulnerability.

Operation	Procedure
Ignoring the impact of a vulnerability on an image	<ul style="list-style-type: none"> • Method 1: <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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.

3.2 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 & Compliance > Container Guard Service**.

Step 3 In the navigation pane 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 3-3](#).

Table 3-3 Parameter description

Parameter	Description	Operation
Vulnerability Name	-	<ul style="list-style-type: none"> Click  to view the details of a vulnerability, including CVE ID, CVSS Score, Disclosed, and Vulnerability Details. Click a 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.	-
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 3-4](#) and [Figure 3-5](#).

Figure 3-4 Basic information about a vulnerability in private images

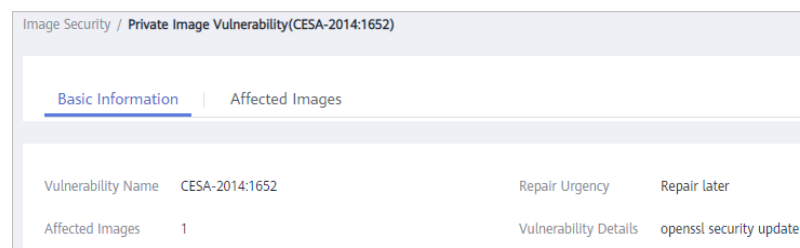


Figure 3-5 Affected private images

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

3.3 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 & Compliance > Container Guard Service.**
- Step 3** In the navigation pane 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 3-4.](#)

Table 3-4 Parameter description

Parameter	Description	Operation
Vulnerability Name	-	<ul style="list-style-type: none"> • Click  to view the details of a vulnerability, including CVE ID, CVSS Score, Disclosed, and Vulnerability Details. • Click a 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 3-6](#) and [Figure 3-7](#).

Figure 3-6 Basic information about a vulnerability in official images

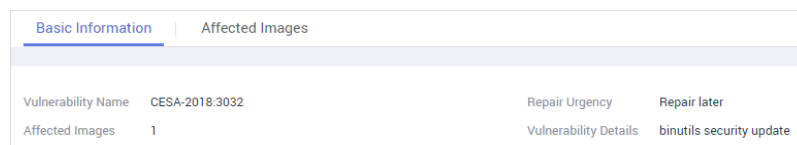
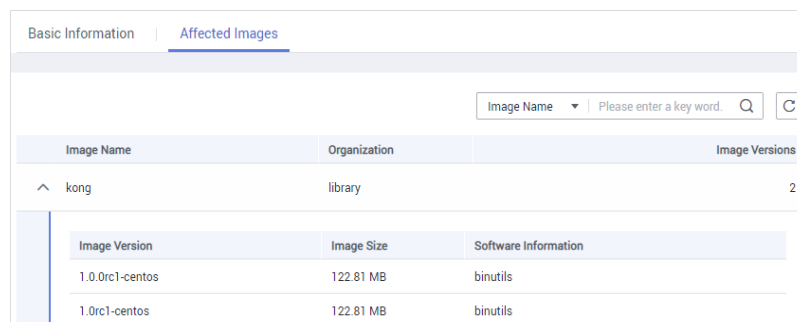


Figure 3-7 Affected official images



----End

3.4 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.](#)

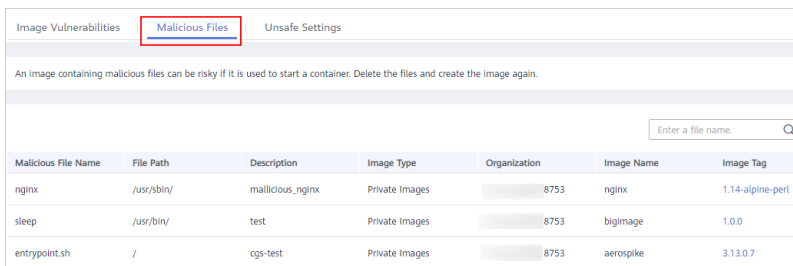
Step 2 In the upper part of the page, select a region, click , and choose **Security & Compliance > Container Guard Service.**

Step 3 In the navigation pane 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 3-8 Malicious files



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

----End

3.5 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.

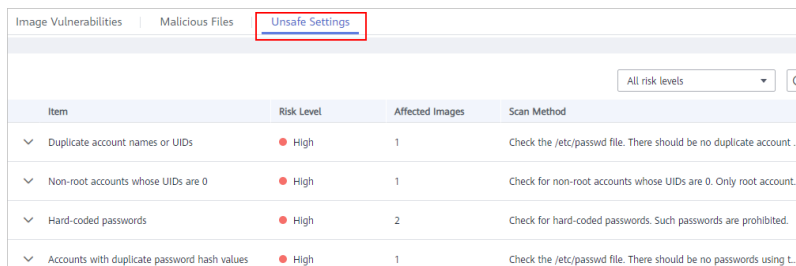
Procedure

Step 1 [Log in to the management console.](#)

- Step 2** In the upper part of the page, select a region, click , and choose **Security & Compliance > Container Guard Service**.
- Step 3** In the navigation pane 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 3-9 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 L...


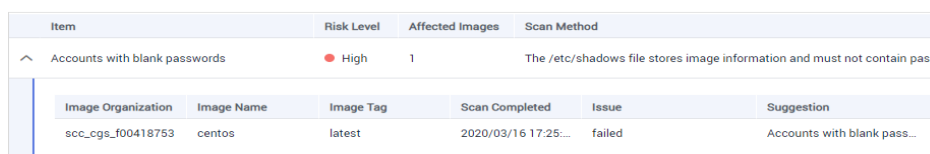
- Step 5** Click  next to a check item to view its details and suggestions, and modify your unsafe settings accordingly.

Figure 3-10 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

4 Viewing Container Runtime Security Details

After you enabled cluster protection, the CGS shield will be installed as a daemonset to monitor container status on cluster nodes, report alarms on abnormal events, and to 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 4-1 Runtime vulnerability detection

Check Item	Mechanism
Escapes	<ul style="list-style-type: none"> 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 <code>open_by_handle_at</code> , <code>ptrace</code> , <code>setns</code> , or <code>reboot</code> .
Abnormal processes	<ul style="list-style-type: none"> <li data-bbox="660 389 1425 555">● 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. <li data-bbox="660 566 1425 775">● Abnormal processes To allow only specific processes to 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
<p>Container environment</p>	<p>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.</p> <p>Container environment check items include:</p> <ul style="list-style-type: none"> ● Privileged container startup (<code>privileged:true</code>) CGS reports an alarm if it detects a container started with the maximum permissions. Settings that can trigger such alarms include the <code>-privileged=true</code> parameter in the docker run command, and <code>privileged: true</code> in the securityContext of the container in a Kubernetes pod. The details of such alarms contain privileged:true. ● Too many container capabilities (<code>capability:[xxx]</code>) Linux 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 (<code>seccomp=unconfined</code>) 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. <p>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.</p> <ul style="list-style-type: none"> ● Container privilege escalation (<code>no-new-privileges:false</code>) 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 <code>-no-new-privileges=false</code> 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. ● High-risk directory mapping (<code>mounts:[...]</code>)

Check Item	Mechanism
	<p>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.</p> <p>CGS reports an alarm if it detects that a critical server path (/boot, /dev, /etc, /sys, /var/run) is mounted during container startup.</p> <p>Such alarms contain mounts: [{"source":"xxx","destination":"yyy" ...}].</p> <p>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.</p>

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 & Compliance > Container Guard Service**.
- Step 3** In the navigation pane on the left, 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.

Figure 4-1 Container exception trend

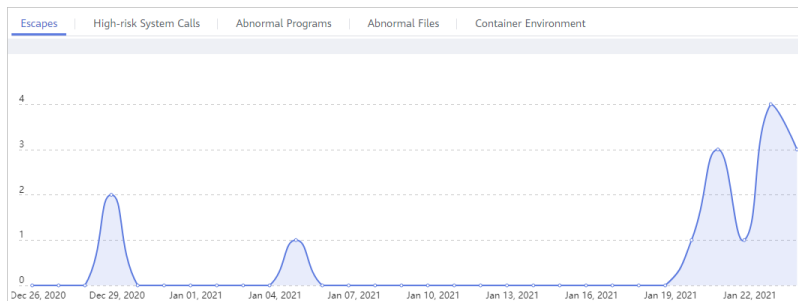


Figure 4-2 Abnormal container event list

Container In...	Image Name	Node Name	Cluster	Exception Type	Exception Descript...	Triggered	Solution
/mysql-test-dirtyco...	100.95.181.176:530...	cgs-test-cluster-19...	cgs-test-cluster	Escape vulnerabilit...	Privilege-Escalation...	Jan 25, 2021 02:02:...	Kill the attacking p...

- 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

5 Managing Images

5.1 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 & Compliance > Container Guard Service**.

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

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

Table 5-1 Local image parameters


Parameter	Description	Operation
Image Name	Image name	Click  next to the name of an image to view its versions.
Image ID	Image ID	-
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 Basic Information About a Local Image

Step 1 [Log in to the management console.](#)

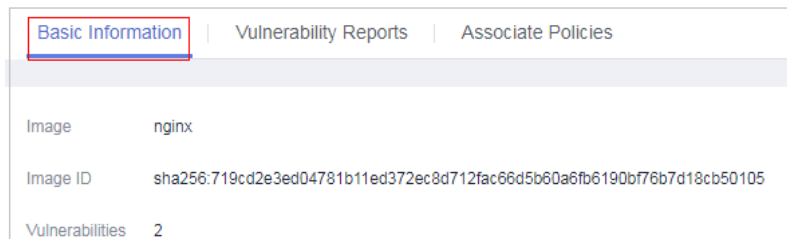
Step 2 In the upper part of the page, select a region, click , and choose **Security & Compliance > Container Guard Service.**

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

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

Step 5 View the basic information about the image version, as shown in [Figure 5-1.](#)

Figure 5-1 Basic information about a local image




----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 & Compliance > Container Guard Service.**

Step 3 In the navigation pane 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.

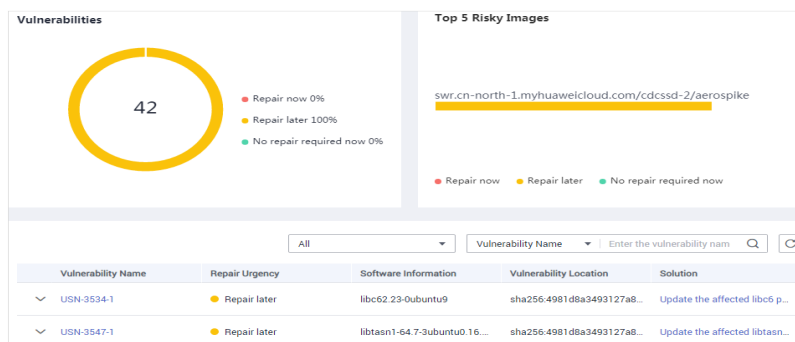
You can perform the following operations:

- 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.

Figure 5-2 Vulnerability report




----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.](#)

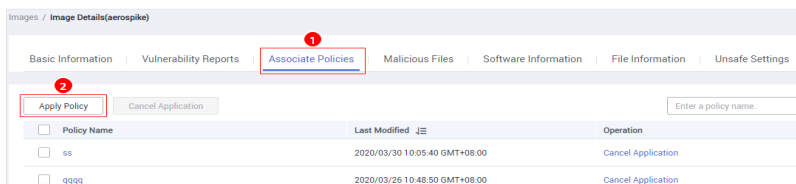
Step 2 In the upper part of the page, select a region, click , and choose **Security & Compliance > Container Guard Service**.

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

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

Step 5 Click the **Associate Policies** tab and click **Apply Policy**.

Figure 5-3 Applying a policy



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

5.2 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 & Compliance > Container Guard Service**.

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

Step 4 Click the **Private Images** tab, as shown in [Figure 5-4](#).

NOTE

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

Figure 5-4 Private images

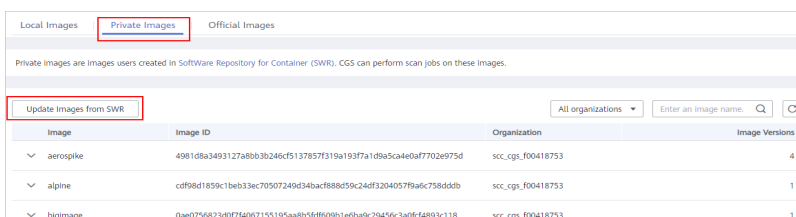




Table 5-2 Parameters description

Parameter	Description	Operation
Image	Image name	Click  next to the name of an image to view its versions.
Image ID	Image ID	-
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 & Compliance > Container Guard Service.**


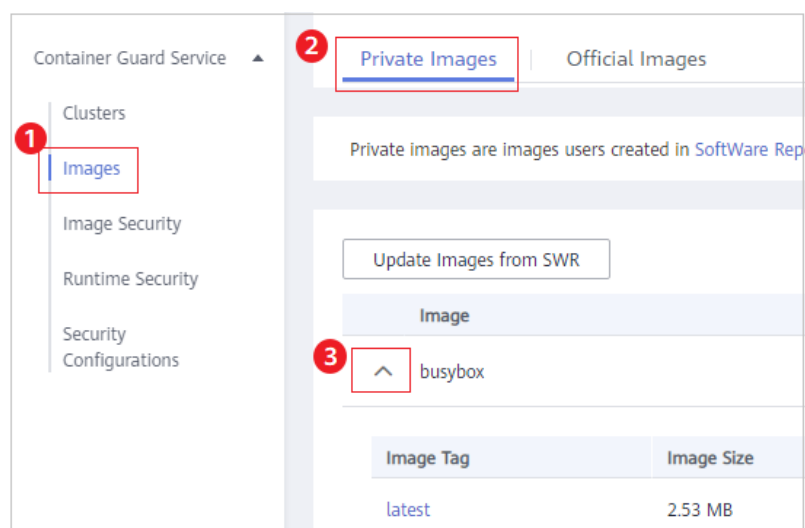
Step 3 In the navigation pane on the left, choose **Images**. Click the **Private Images** tab and click  next to the image name to expand the image version list.

Figure 5-5 Expanding image details



Step 4 Click an image name to go to its basic information page.

Figure 5-6 Selecting an image

Image Tag	Image Size	Last Updated	Last Scan Completed	Vulnerabilities	Associated Policies	Scan Status	Operation
latest	2.53 MB	2021/06/29 16:49:03 GMT+08...	2021/08/25 10:21:32 GMT+08...	0	1	Completed	Scan View Report

Step 5 View the basic information about the image version, as shown in [Figure 5-7](#).

Figure 5-7 Basic information about the private image

Images / Image Details(aerospike)			
Basic Information		Vulnerability Reports	Associate Policies
Image	aerospike	Organization	scc_cgs_f00418753
Image Tag	3.12.1.3	Image Version ID	sha256-31bd08ae686b49b5462daa5e4f3fbcbb4f1849c5c329b65bb775093ccdb13d7
Image Size	188.95 MB	Last Updated	2019/05/09 17:31:39 GMT+08:00
Vulnerabilities	24	Last Scan Completed	2020/03/31 17:58:23 GMT+08:00
Scan Status	Completed		

----End

Scanning a Private Image

You can also click an image to scan it.

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 & Compliance > Container Guard Service**.


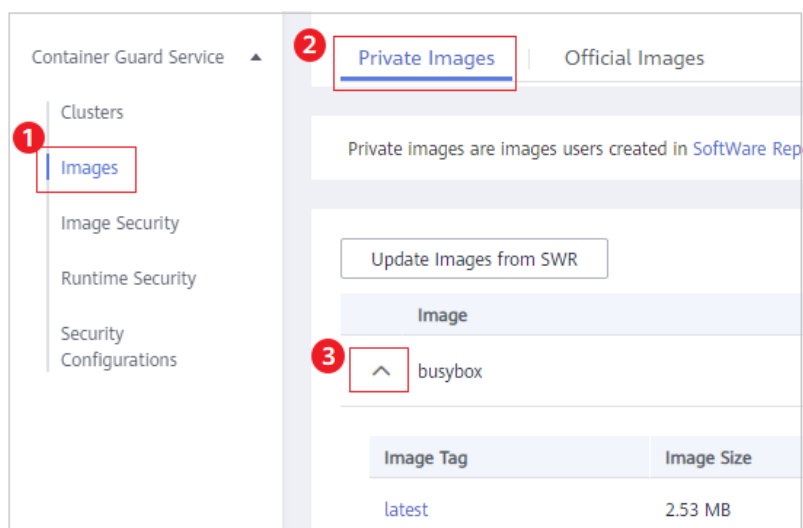
Step 3 In the navigation pane on the left, choose **Images**. Click the **Private Images** tab and click  next to the image name to expand the image version list.

Figure 5-8 Expanding image details



Step 4 Click **Scan** in the **Operation** column of the image version list.

Figure 5-9 Security scan

Image	Image ID	Organization				Image Versions	
^ aerospike	4981d8a3493127a8b63b246cf5137857f319a193f7a1d9a5ca4e0af...	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 5 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 & Compliance > Container Guard Service.**


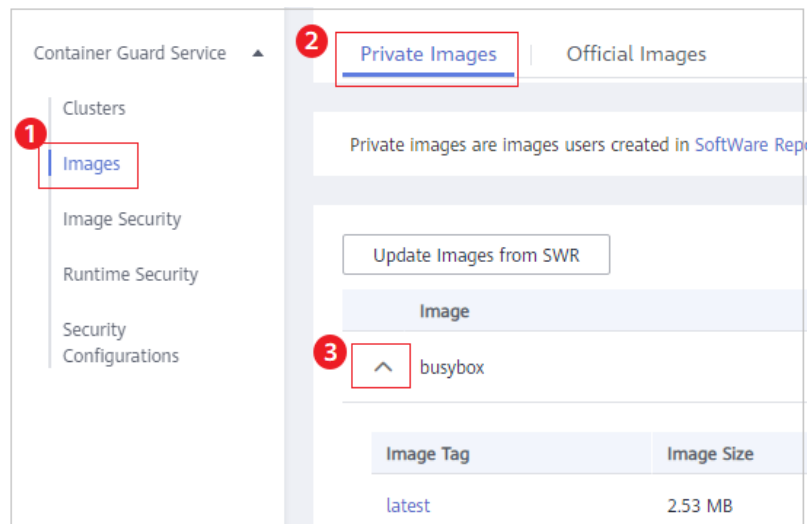
Step 3 In the navigation pane on the left, choose **Images**. Click the **Private Images** tab and click  next to the image name to expand the image version list.

Figure 5-10 Expanding image details



Step 4 Click **View Report** in the **Operation** column.

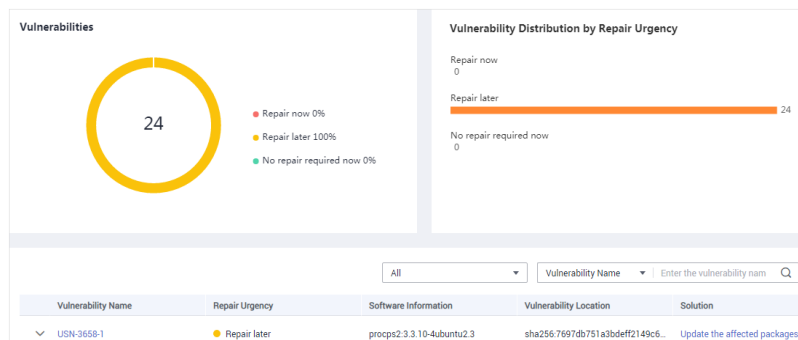
Figure 5-11 Viewing a vulnerability report

Image	Image ID	Organization				Image Versions	
^ aerospike	4981d8a3493127a8b63b246cf5137857f319a193f7a1d9a5ca4e0af...	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 5 Check image vulnerabilities in the vulnerability report.

- **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


Figure 5-12 Vulnerability report



----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 & Compliance > Container Guard Service.**


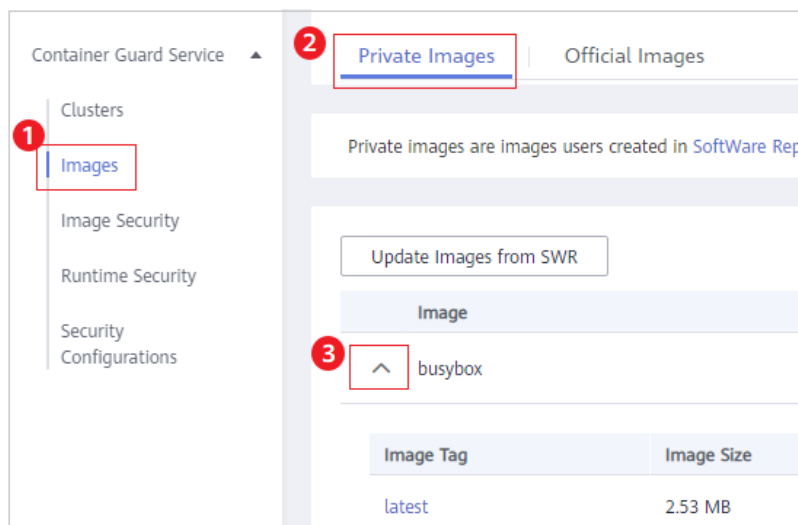
Step 3 In the navigation pane on the left, choose **Images**. Click the **Private Images** tab and click  next to the image name to expand the image version list.

Figure 5-13 Expanding image details



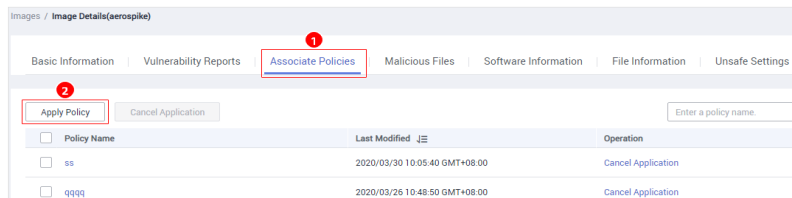
Step 4 Click an image name. Go to the basic image information page.

Figure 5-14 Selecting a target image

Image	Image ID	Organization	Image Versions				
^ busybox	a7d768c7d845545460315d89d6f18806d4734903c3c09f8a2a25956950b	g42	1				
Image Tag	Image Size	Last Updated	Last Scan Completed	Vulnerabilities	Associated Policies	Scan Status	Operation
latest	2.53 MB	2021/06/29 16:49:03 GMT+08:00	2021/08/25 10:21:32 GMT+08:00	0	1	Completed	Scan View Report

Step 5 Click the **Associate Policies** tab and click **Apply Policy**, as shown in [Figure 5-15](#).

Figure 5-15 Applying a policy



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

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 & Compliance > Container Guard Service**.


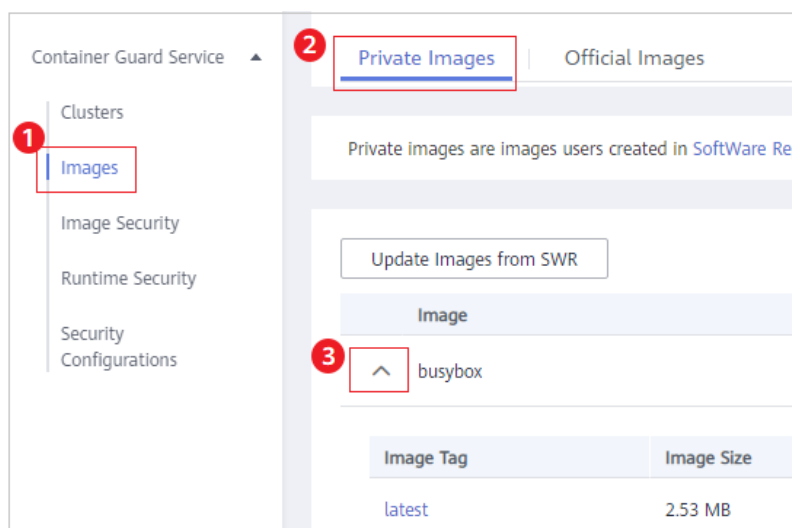
Step 3 In the navigation pane on the left, choose **Images**. Click the **Private Images** tab and click  next to the image name to expand the image version list.

Figure 5-16 Expanding image details



Step 4 Click an image name. Go to the basic image information page.

Figure 5-17 Selecting a target image

Image	Image ID	Organization	Image Versions				
^ busybox	47f18b7c7b4554548315896d18806d17848033c09f8a2c2555020b	g42	1				
Image Tag	Image Size	Last Updated	Last Scan Completed	Vulnerabilities	Associated Policies	Scan Status	Operation
latest	2.53 MB	2021/06/29 16:49:03 GMT+08:00	2021/06/29 10:21:32 GMT+08:00	0		1 Completed	Scan View Report

Step 5 Click the **Malicious Files** tab to view malicious files on the image.

Figure 5-18 Malicious file in private images

Images / Image Details(aerospike)

Basic Information | Vulnerability Reports | Associate Policies | **Malicious Files** | Software Information | File Information | Unsafe Settings

Image Tag 3.12.1.3 Last Scan Completed 2020/03/31 17:58:23 GMT+08:00 [Scan Again](#)


Enter a file name

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 & Compliance > Container Guard Service**.


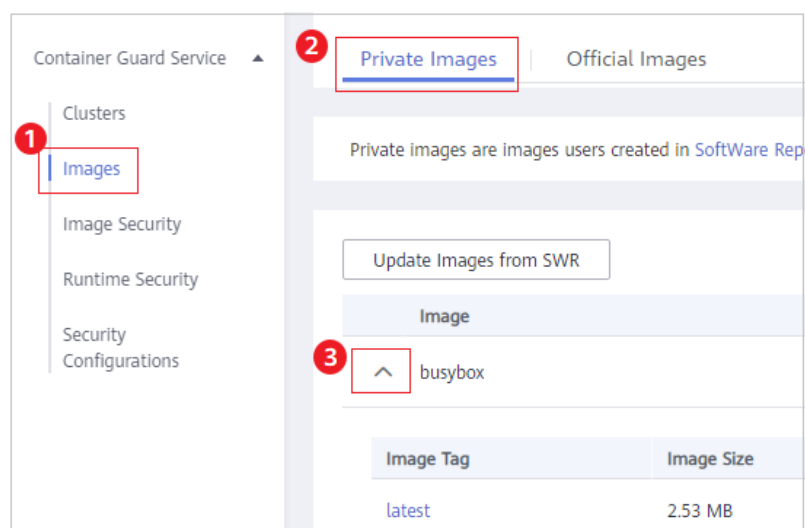
Step 3 In the navigation pane on the left, choose **Images**. Click the **Private Images** tab and click  next to the image name to expand the image version list.

Figure 5-19 Expanding image details



Step 4 Click an image name to go to its basic information page.


Figure 5-20 Selecting an image

Image Tag	Image Size	Last Updated	Last Scan Completed	Vulnerabilities	Associated Policies	Scan Status	Operation
latest	2.53 MB	2021/06/29 16:49:03 GMT+08...	2021/08/25 10:21:32 GMT+08...	0	1	Completed	Scan View Report

Step 5 Click the **Software Information** tab to view the software contained in the image version, software type, and number of vulnerabilities in the software.

Figure 5-21 Software information


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

Step 6 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 & Compliance > Container Guard Service.**


Step 3 In the navigation pane on the left, choose **Images**. Click the **Private Images** tab and click  next to the image name to expand the image version list.

Figure 5-22 Expanding image details

Image Tag	Image Size
latest	2.53 MB

Step 4 Click an image name to go to its basic information page.

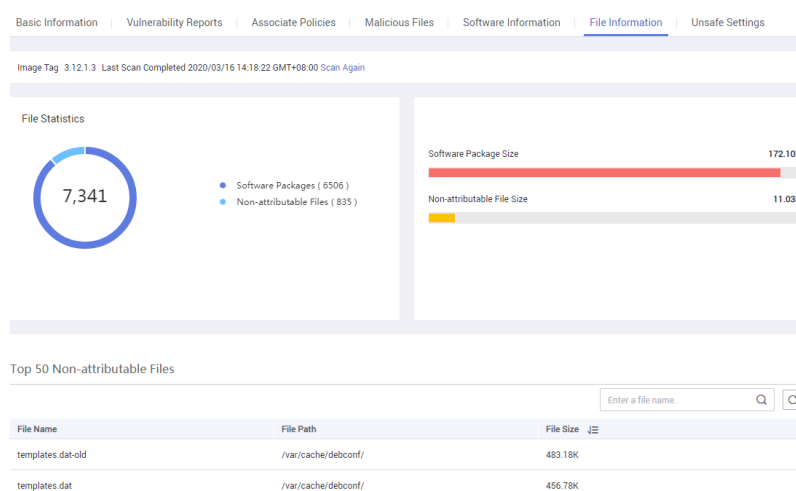
Figure 5-23 Selecting an image

Image Tag	Image Size	Last Updated	Last Scan Completed	Vulnerabilities	Associated Policies	Scan Status	Operation
latest	2.53 MB	2021/06/29 16:49:03 GMT+08...	2021/08/25 10:21:32 GMT+08...	0	1	Completed	Scan View Report

Step 5 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 5-24 File information



----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 & Compliance > Container Guard Service**.


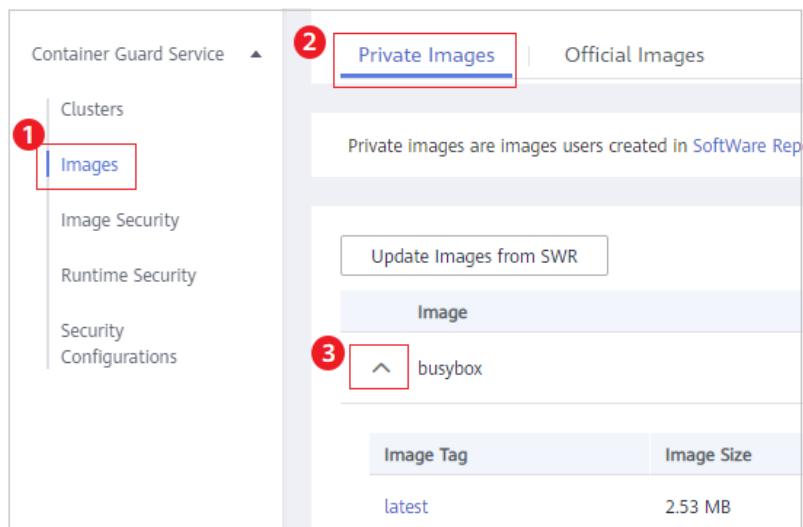
Step 3 In the navigation pane on the left, choose **Images**. Click the **Private Images** tab and click  next to the image name to expand the image version list.

Figure 5-25 Expanding image details



Step 4 Click an image name to go to its basic information page.

Figure 5-26 Selecting an image

Image Tag	Image Size	Last Updated	Last Scan Completed	Vulnerabilities	Associated Policies	Scan Status	Operation
latest	2.53 MB	2021/06/29 16:49:03 GMT+08...	2021/08/25 10:21:32 GMT+08...	0	1	Completed	Scan View Report

Step 5 Click the **Unsafe Settings** tab to view unsafe settings and modify configurations based on suggestions provided.

Figure 5-27 Unsafe settings of a private image

Basic Information | Vulnerability Reports | Associate Policies | Malicious Files | Software Information | File Information | **Unsafe Settings**

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

All risk levels: [v] All results: [v] [C]

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

5.3 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 & Compliance > Container Guard Service.**


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


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

----End

Viewing 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 & Compliance > Container Guard Service.**

Step 3 In the navigation pane on the left, choose **Images.** Click the **Official Images** tab and click  next to the image name to expand the image version list.

Step 4 Click an image name to go to its basic information page.

Step 5 View its basic information. See [Figure 5-28.](#)


Figure 5-28 Basic information about an official image


Basic Information		Vulnerability Reports		Associate Policies	
Image	caffe	Organization	bvlc		
Image Tag	cpu	Image Version ID	sha256:0b577b83638692f93091cd0ef7199847caab7f97845b72b642707548b4c18ef1		
Image Size	594.81 MB	Last Updated	2019/12/19 02:34:55 GMT+08:00		
Vulnerabilities	0	Last Scan Completed	2019/01/31 16:38:01 GMT+08:00		
Scan Status	Failed				

----End

Viewing Vulnerabilities in Official Images

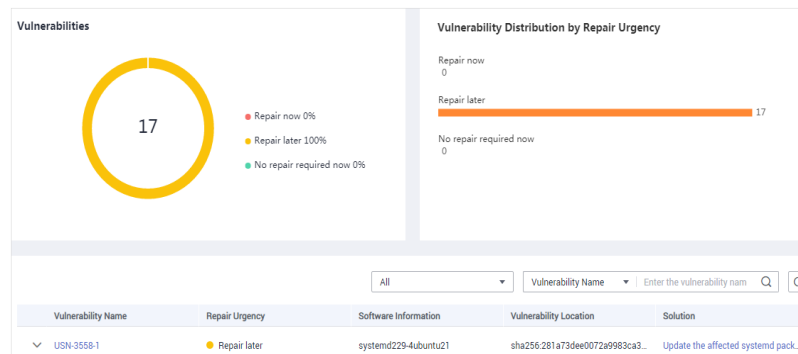
Step 1 [Log in to the management console.](#)

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

Step 3 In the navigation pane on the left, choose **Images.** Click the **Official Images** tab and click  next to the image name to expand the image version list.

Step 4 Click **View Report.** Check image vulnerabilities.

Figure 5-29 Official image vulnerabilities



Step 5 Click  next to the **Vulnerability Name** to view the details.

Figure 5-30 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 & Compliance > Container Guard Service.**

Step 3 In the navigation pane on the left, choose **Images**. Click the **Official Images** tab and click  next to the image name to expand the image version list.

Step 4 Click an image name to go to its basic information page.

Step 5 Click the **Associate Policies** tab and click **Apply Policy**.

Figure 5-31 Applying a policy



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


6 Viewing Clusters and Quotas

Prerequisites

CGS service authorization has been approved.

Viewing the Protection Information

Step 1 [Log in to the management console.](#)


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

Step 3 View the protection information.

- **Cluster Protection Statistics:** numbers of protected and unprotected clusters
- **Protected Nodes:** number of protected nodes
- **My Protection Quota:** numbers of normal, expired, and frozen quotas

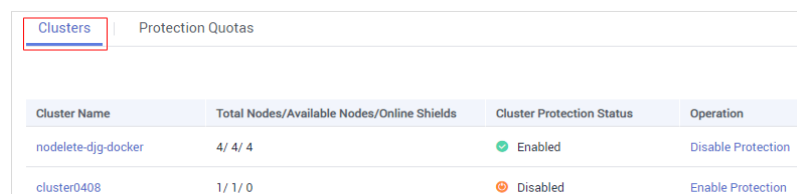
----End

Viewing Clusters

Step 1 In the upper part of the page, select a region, click , and choose **Security & Compliance > Container Guard Service.**

Step 2 On the **Clusters & Quotas** page, click the **Clusters** tab to check protection information, as shown in [Figure 6-1](#). For more information, see [Table 6-1](#).

Figure 6-1 Clusters



Cluster Name	Total Nodes/Available Nodes/Online Shields	Cluster Protection Status	Operation
nodelete-djg-docker	4/ 4/ 4	Enabled	Disable Protection
cluster0408	1/ 1/ 0	Disabled	Enable Protection

Table 6-1 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	<ul style="list-style-type: none"> ● 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
Cluster Protection Status	Protection status of a cluster. The options are: <ul style="list-style-type: none"> ● Disabled ● Enabled NOTE <ul style="list-style-type: none"> - Enabling protection will automatically install the CGS plug-in in the cluster. To enable cluster protection, follow the instructions provided in Enabling Protection for a Cluster. - Disabling protection will automatically uninstall the CGS plug-in from the cluster. To disable cluster protection, follow the instructions provided in Disabling Protection for a Cluster.

Step 3 Click the name of a cluster, and the node list is displayed, as shown in [Figure 6-2](#).

Figure 6-2 Nodes

Node Name	Elastic IP Address	Node Status	Shield Status
nodelete-djg-docker-69333	.148.166	Running	Online
nodelete-djg-docker-master-6tcq0	--	Running	Offline

Step 4 Check the node list. It contains the following information:

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

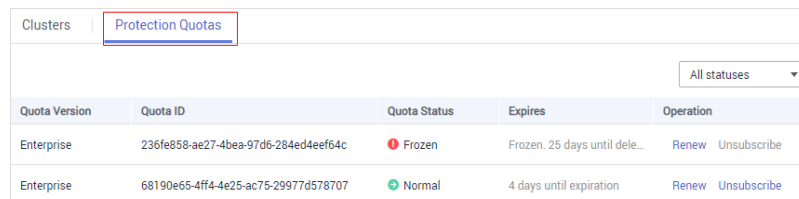
An offline shield fails to communicate with the server. To troubleshoot it, follow the instructions provided in [What Should I Do If the Shield on a Node Is Offline?](#)

----End

Viewing Protection Quotas

On the **Clusters & Quotas** page, click **Protection Quotas** to view quota details, as shown in [Figure 6-3](#).

Figure 6-3 Protection quotas



Quota Version	Quota ID	Quota Status	Expires	Operation
Enterprise	236fe858-ae27-4bea-97d6-284ed4eef64c	● Frozen	Frozen. 25 days until dele...	Renew Unsubscribe
Enterprise	68190e65-4ff4-4e25-ac75-29977d578707	● Normal	4 days until expiration	Renew Unsubscribe

The details page contains the following information:

- **Quota Status:** **Normal**, **Expired**, or **Frozen**
- **Expires:** time before a CGS quota expires
- **Operation:** **Renew** or **Unsubscribe** from a quota

7 Disabling Protection for a Cluster


If CGS is not required, disable protection for a cluster by referring to this section. Disabling 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 & Compliance > Container Guard Service.**

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

Figure 7-1 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

8 Auditing

8.1 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 8-1 lists CGS operations supported by CTS.

Table 8-1 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	registerCgsAgency
Manually scanning images	cgs	scanPrivateImage
Obtaining and scanning images from Software Repository for Container (SWR)	cgs	syncSwrPrivateImage

8.2 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 & Governance > 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

9 Managing Permissions

9.1 Creating a User and Granting Permissions

This chapter describes IAM's fine-grained permissions management for your CGS. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to CGS resources.
- Grant only the permissions required for users to perform a task.
- Entrust a HUAWEI CLOUD account or cloud service to perform professional and efficient O&M on your CGS resources.

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

This section describes how to authorize users.

Prerequisites

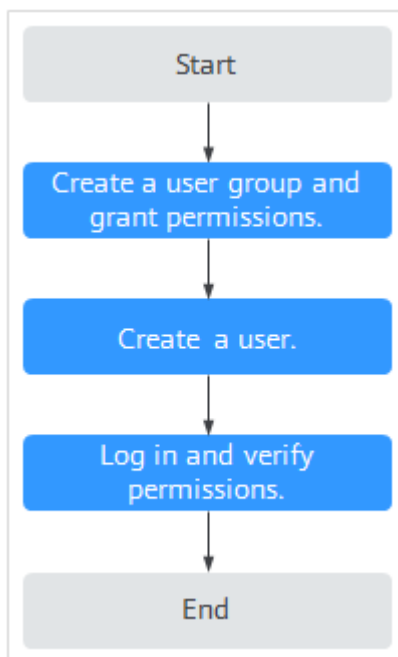
Learn about the permissions (see [Table 9-1](#)) supported by CGS and choose policies or roles according to your requirements.

Table 9-1 CGS system role

Role/ Policy Name	Descrip tion	Type	Dependencies
CGS Adminis trator	CGS system adminis trator, who has all permis sions 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 FullAcce ss	All permis sions of CGS	System- defined policy	None
CGS ReadOn lyAccess	Read- only permis sions for CGS	System- defined policy	None

Authorization Process

Figure 9-1 Process for granting permissions



1. **Create a user group and assign permissions.**
Create a user group on the IAM console and grant the user group the **CGS ReadOnlyAccess** permission for CGS.
2. **Create an IAM user.**
Create a user on the IAM console and add the user to the user group created in **1**.
3. **Log in** and verify permissions.
Log in to the CGS console by using the newly created user, and verify that the user only has read permissions for CGS.
Verification method: Assume you are granted only the **CGS ReadOnlyAccess** permission. Click **Service List** and choose **Container Guard Service**. On the CGS console, click **Buy CGS** and try purchasing CGS quota. If the purchase fails, the permission setting has already taken effect.

9.2 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](#).

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For more information, see [Creating a Custom Policy](#). The following section contains examples of common CGS custom policies.

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"
      ]
    }
  ]
}
```

9.3 CGS Permissions and Supported Actions

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

By default, new IAM users do not have 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	-
Obtain the yearly/monthly quota list.	cgs:quota:list	-
Subscribe to yearly/monthly CGS quota.	cgs:quota:operate	-
Query system process information.	cgs:cluster:list	<ul style="list-style-type: none"> • cce:addonInstance:* • cce:node:list • cce:cluster:list
Enable or disable protection for a container cluster.	cgs:cluster:operate	<ul style="list-style-type: none"> • 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	-

Permission	Action	Related Action
Query CGS authorization.	cgs:privilege:get	-

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.