Tencent Container Security Service

Operation Guide

Product Documentation

©2013-2022 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Operation Guide
- Security Overview
- Asset Management
  - Overview
  - Container
  - Cluster Asset
  - Processes and Ports
  - Applications and Web Services
- Vulnerability Detection
  - Vulnerability Scan
  - Exploit Prevention
- Image Risk Management
  - Overview
  - Local Image
  - Repository Image
  - Accessing the AWS Image Repository
  - Image Interception Events
- Cluster Risk Management
  - Cluster Check
  - Self-Built Cluster
  - Risk Analysis
- Baseline Management
  - Overview
  - Container
  - Image
  - Docker Server
  - Kubernetes
- Runtime Security
  - Overview
  - Container Escape
  - Virus Scanning
  - Outbound Malware
- Advanced Defense
  - Overview
  - Abnormal Process

©2013-2022 Tencent Cloud. All rights reserved.

Event List
Rule Configuration
File Tampering
Event List
Rule Configuration
High-Risk Syscall
Event List
Allowlist Management
Exceptional Requests of K8s APIs
Policy Management
Container Network Policy
Policy Configuration
Use Cases
Image Interception Policies
Protection Switch
Alarm Settings
Log Analysis
Overview
Querying Log
Configuring Log
Log Shipping
Hybrid Cloud Installation Guide
Overview
Configuring Non-Tencent Cloud Server
Connecting Dedicated VPC
FAQs
Compromised Container Isolation

©2013-2022 Tencent Cloud. All rights reserved.

Operation Guide
Security Overview

Last updated：2024-02-07 09:04:17

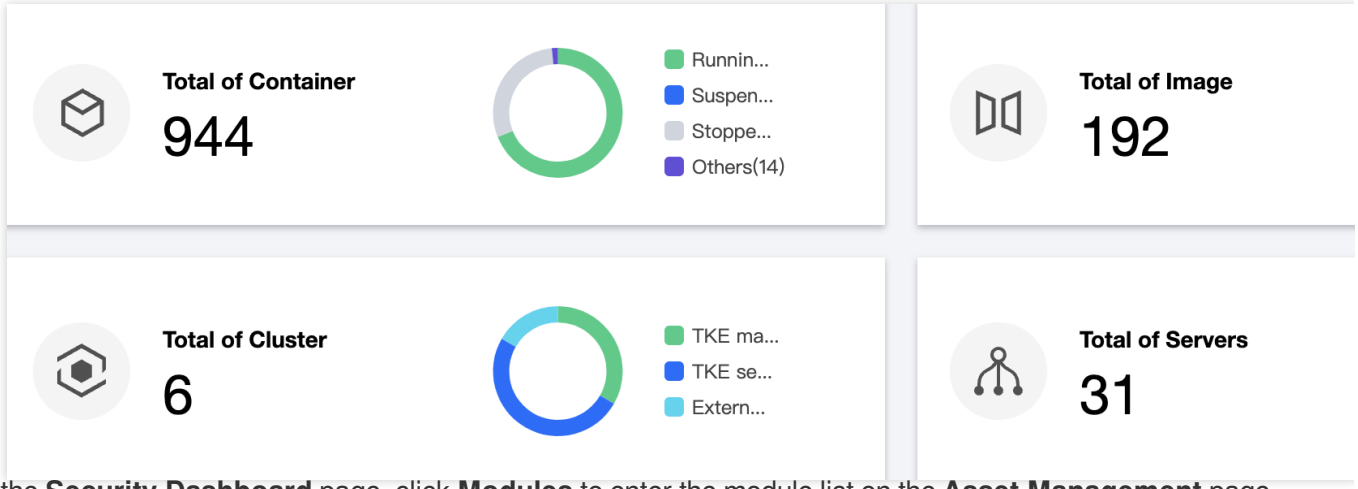
This document describes the security overview of each security module of TCSS.
Displays the overview of container security risks and container security events over time in real time.
Describes TCSS versions and usage, along with upgrade and renewal features.

Key Features

Log in to the TCSS console and select **Security Dashboard** on the left sidebar.

Viewing asset information

1. On the **Security Dashboard** page, the asset information module displays the numbers of containers, images, clusters, and nodes.

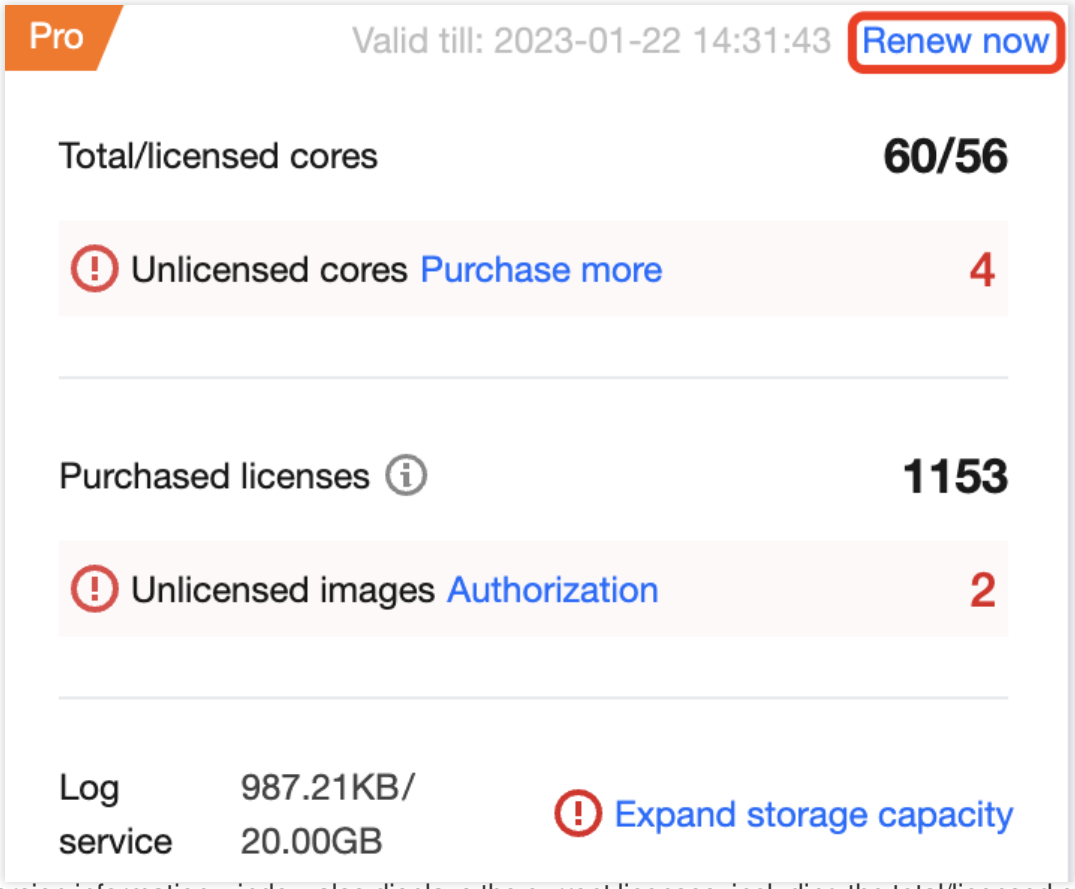


2. On the **Security Dashboard** page, click **Modules** to enter the module list on the **Asset Management** page.

Viewing versions, usage, upgrade, and renewal

On the **Security Dashboard** page, the version information window displays the current TCSS version and its expiration date. The following takes the Pro Edition as an example:
If the current version will expire soon, you will be prompted to renew it. Then, you can click **Renew now**.

©2013-2022 Tencent Cloud. All rights reserved.



The version information window also displays the current licenses, including the total/licensed cores and purchased licenses.

Total/Licensed cores: **Total cores** indicates the total number of virtual cores on the business node, while **Licensed cores** indicates the number of cores enabled in the Pro Edition.

Note:

When licensed cores are fewer than total cores, the required number of cores will be displayed. Then, you can click **Upgrade** to enter the purchase page and purchase licenses.

If you don't purchase the required number of cores, the flexible billing mode will apply, i.e., each excessive core will be charged at 0.25 USD/day.

Purchased licenses: The number of purchased image security scans.

Note:

When there are local images or repository images with image security scan not enabled in the business environment, the required number of image licenses will be displayed. Then, you can click **Purchase** to enter the purchase page and purchase licenses.

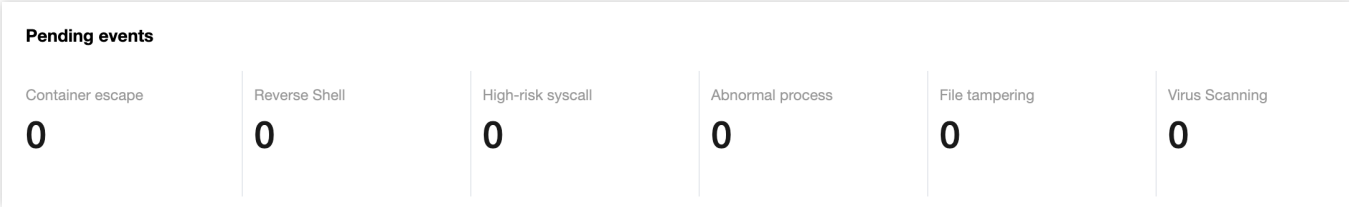
After purchasing the image licenses, go to **Image Security** > **Local Images**/**Repository Images** to configure the licenses. You can customize the images for which to enable image security scan.

Due to product adjustment, the mirror license will be suspended for new purchase from December 29, 2023 to March 31, 2024. Users who have purchased it can still use it normally.

Viewing pending events

©2013-2022 Tencent Cloud. All rights reserved.

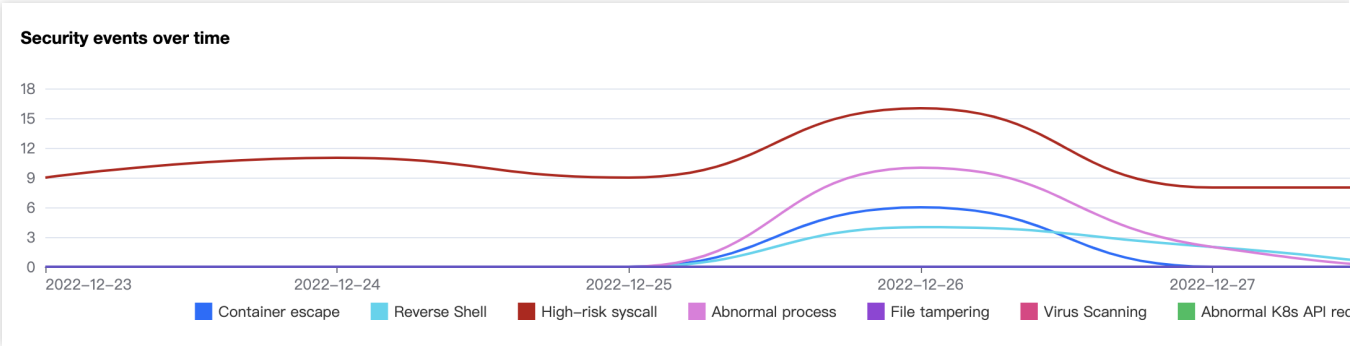
1. On the **Security Dashboard** page, the **Pending events** module displays the number of pending security events.



2. On the **Security Dashboard** page, click **Modules** to enter the security event page to view the details and process the events.

Viewing security events over time

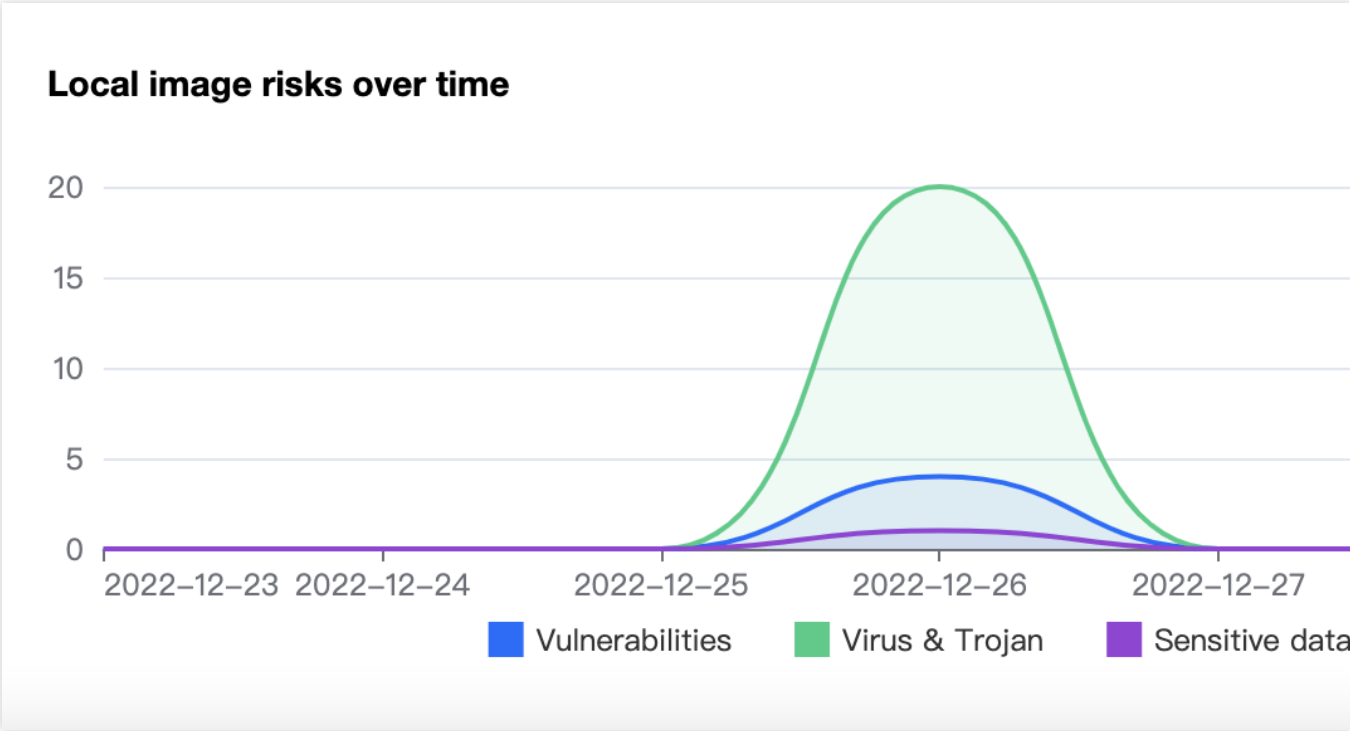
On the **Security Dashboard** page, the **Security events over time** module displays runtime security events over time in the last 7 or 30 days. You can switch between **7 days** and **30 days**.



Viewing local image risks over time

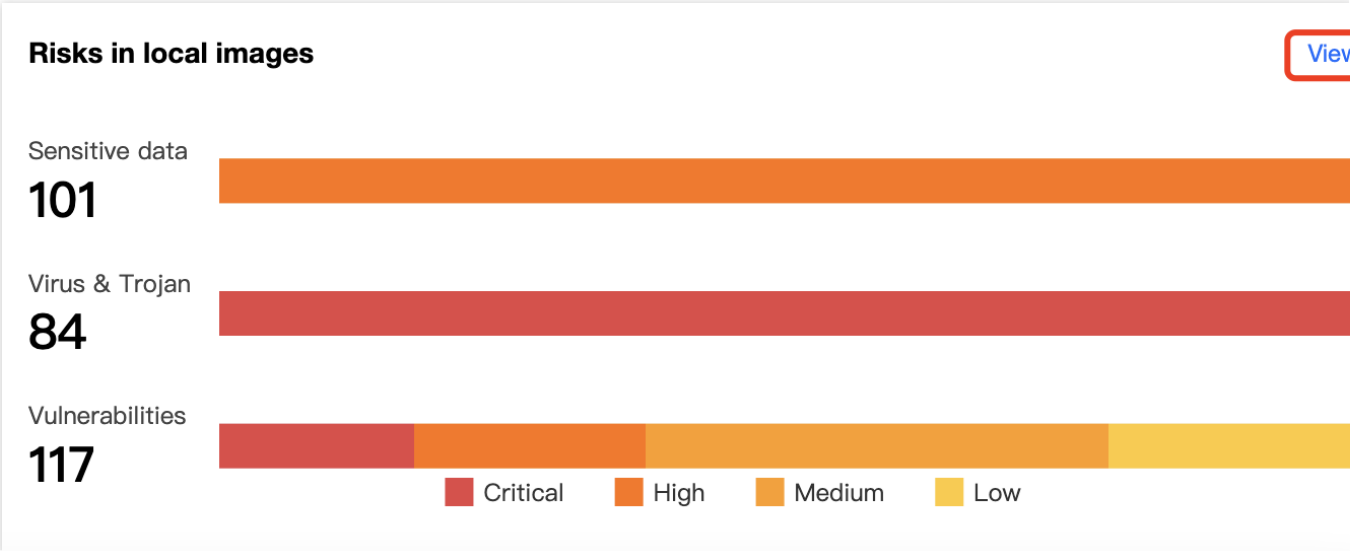
The **Security Dashboard** page displays the trend of vulnerabilities, viruses, trojans, and sensitive data pieces of local images over time in the last 7 or 30 days. You can switch between **7 days** and **30 days**.

©2013-2022 Tencent Cloud. All rights reserved.



Viewing risks in local images

On the **Security Dashboard** page, the **Risks in local images** module displays the total number of risks including sensitive data pieces, viruses, trojans, and vulnerabilities, as well as the severity distribution of the current image. Click **View details** to enter the **Image Security** module to view the details and handle the risks.



©2013-2022 Tencent Cloud. All rights reserved.

Asset Management Overview

Last updated：2024-01-23 15:44:44

This document describes how to use the automatic asset inventory feature of asset management to visualize key assets, such as containers, images, and image repositories.
Asset management data is automatically synced once every 24 hours. Manual sync is supported.
Asset management supports collecting the information of ten types of assets: containers, local images, repository images, clusters, nodes, processes, ports, web services, running applications, and database applications.
Currently, the following assets can be recognized:

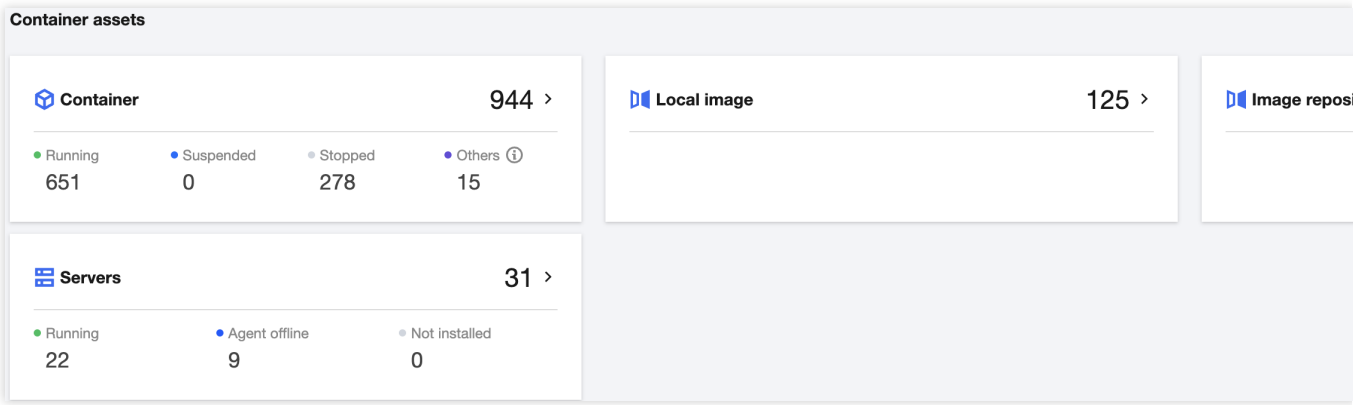
Asset Type	Asset Information
Container	Containers, local images, repository images, clusters, and nodes.
Cluster assets	Clusters, Pods, Services, and Ingresses.
Processes and Ports	Processes and ports.
Applications and Web services	Web services, running applications, and database applications.

©2013-2022 Tencent Cloud. All rights reserved.

Container

Last updated：2024-01-23 15:44:44

This document describes the container module feature and how to view the details of containers, images, and servers.

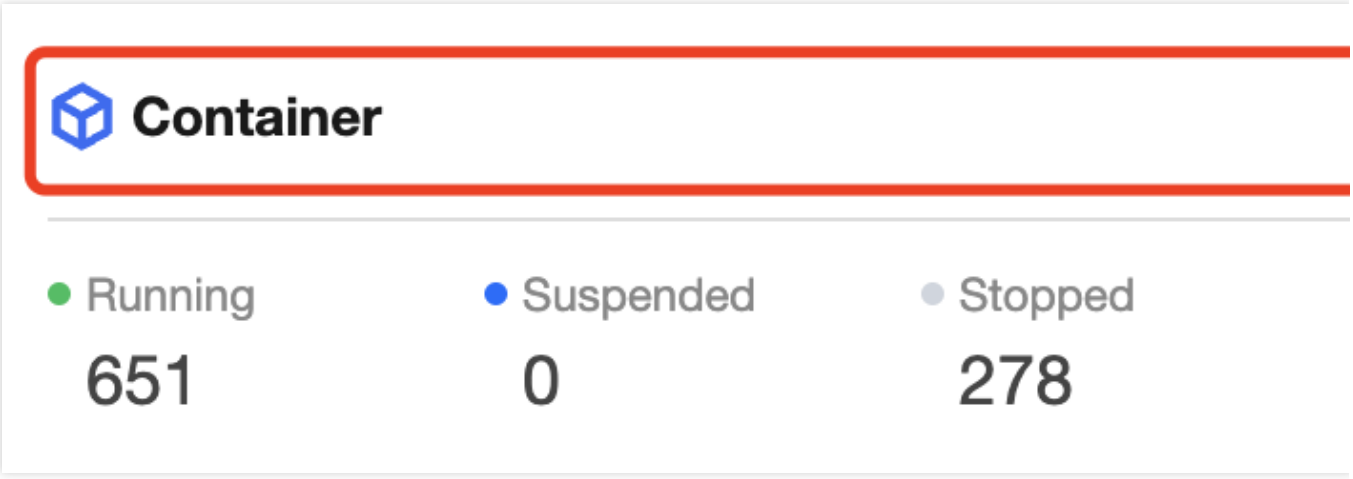


Viewing the Container Module

The container module displays the total number of containers and the numbers of running, suspended, and aborted containers.

Filtering containers

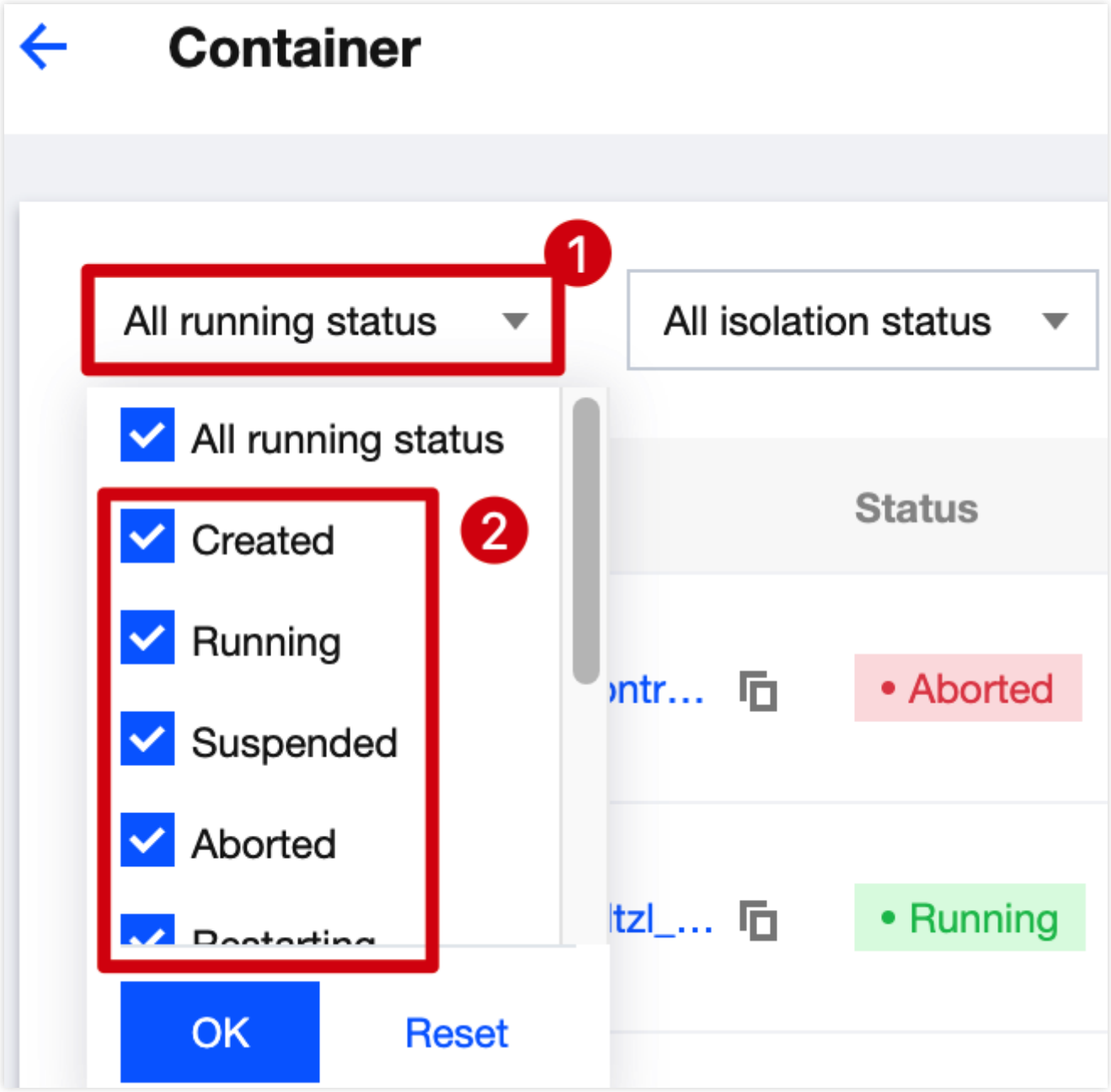
1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Containers** to enter the container list page.



3. On the container list page, filter containers by status or click the search box and search for containers by keyword such as container name/ID, image name, or server IP.

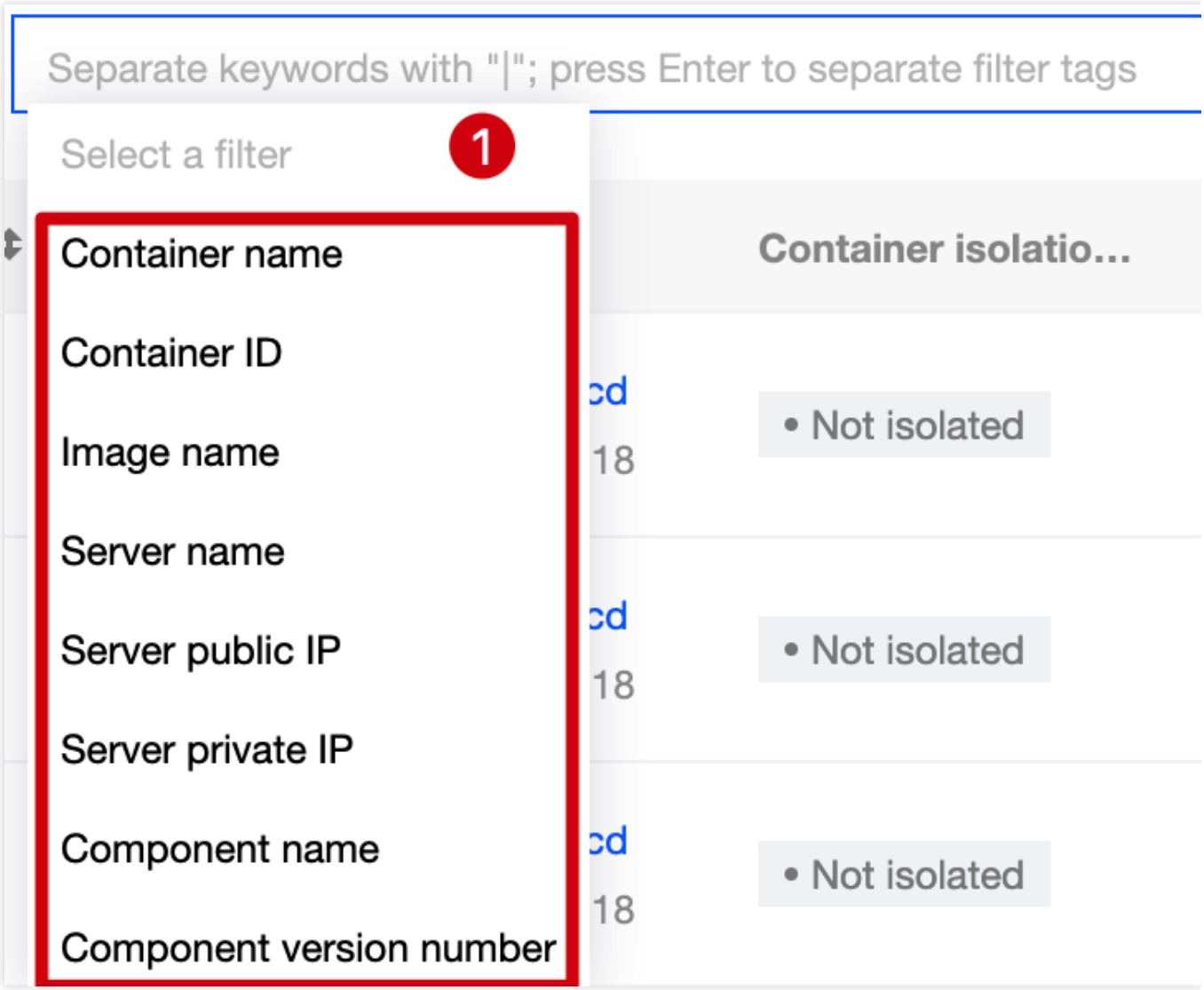
©2013-2022 Tencent Cloud. All rights reserved.

Click the status drop-down list in the top-left corner to filter containers by status.



Click the search box and search for containers by keyword such as container name, container ID, image name, or server IP.

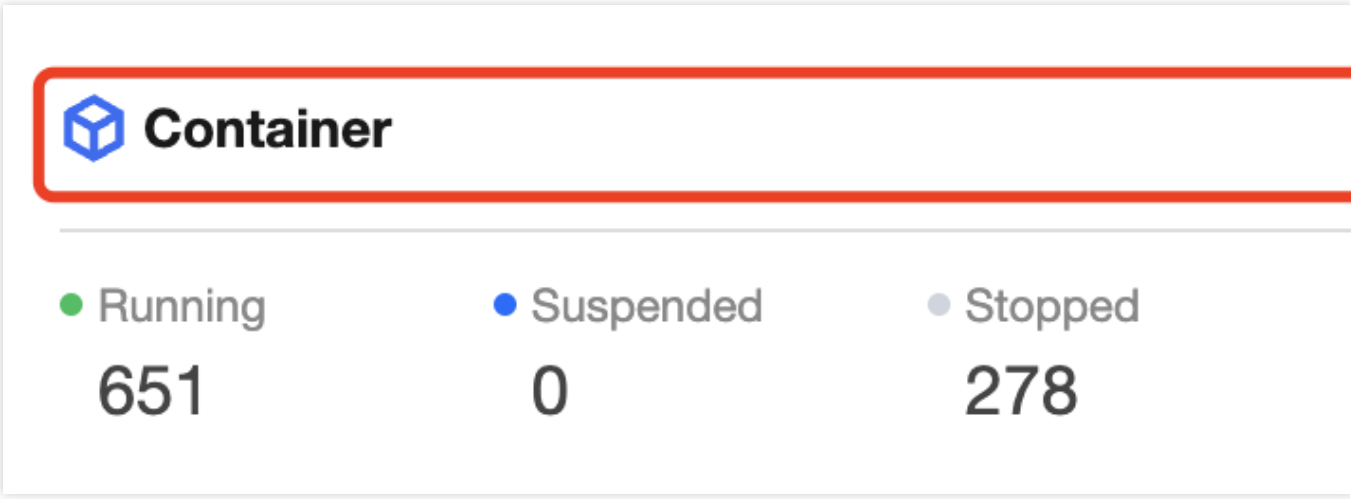
©2013-2022 Tencent Cloud. All rights reserved.



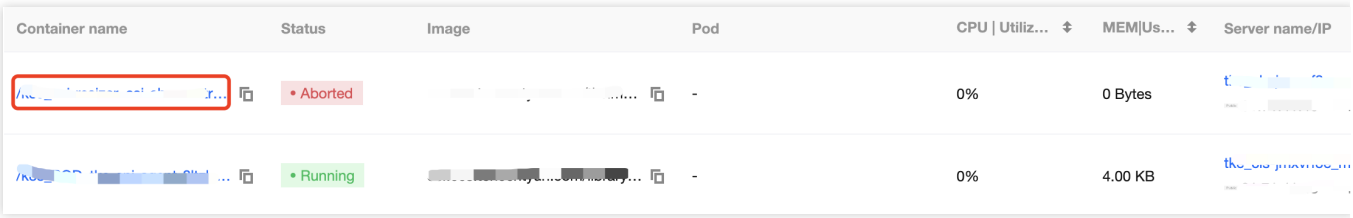
Viewing the list of containers

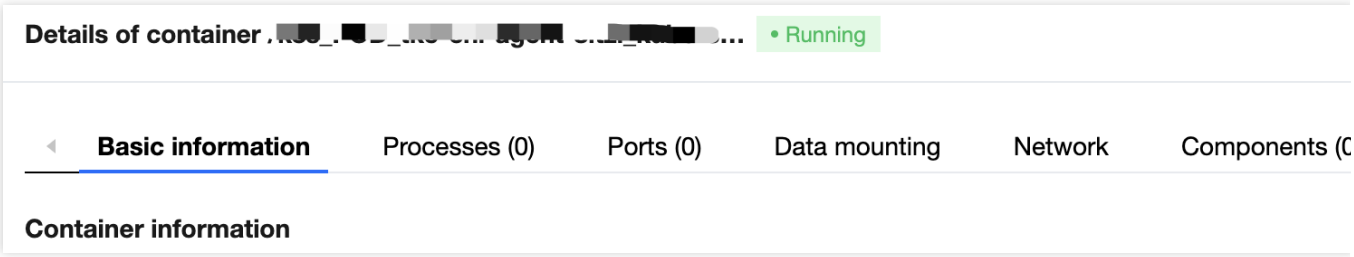
1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Containers** to enter the container list page.

©2013-2022 Tencent Cloud. All rights reserved.



3. On the container list page, click a **Container name** to pop up the drawer on the right, which displays the container details, including the basic container information, process information, and port information.



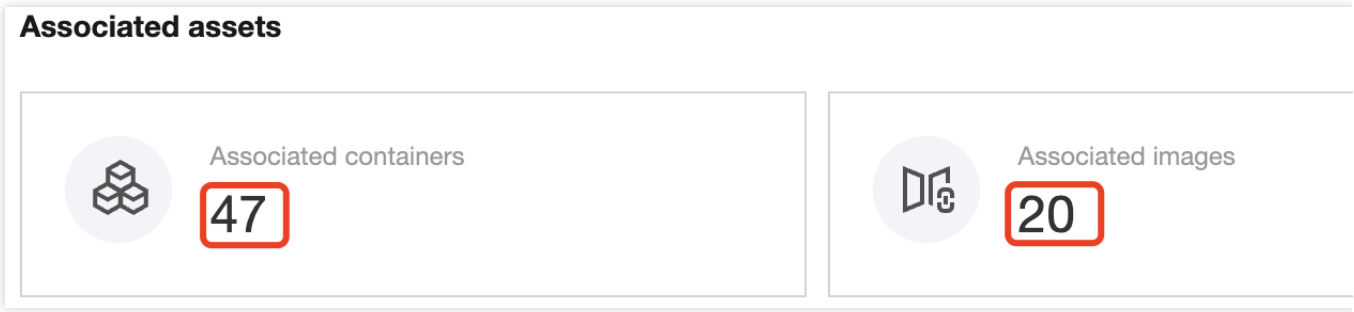


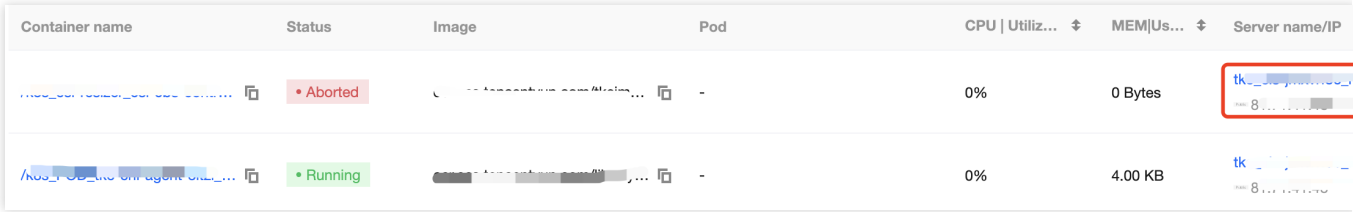
4. On the **Asset Management** page, click a **Server IP** to pop up the drawer on the right, which displays the server details, including the basic server information, Docker information, and the numbers of images and containers.

Note:

In the drawer, click the number to view the numbers of images and containers on the server.

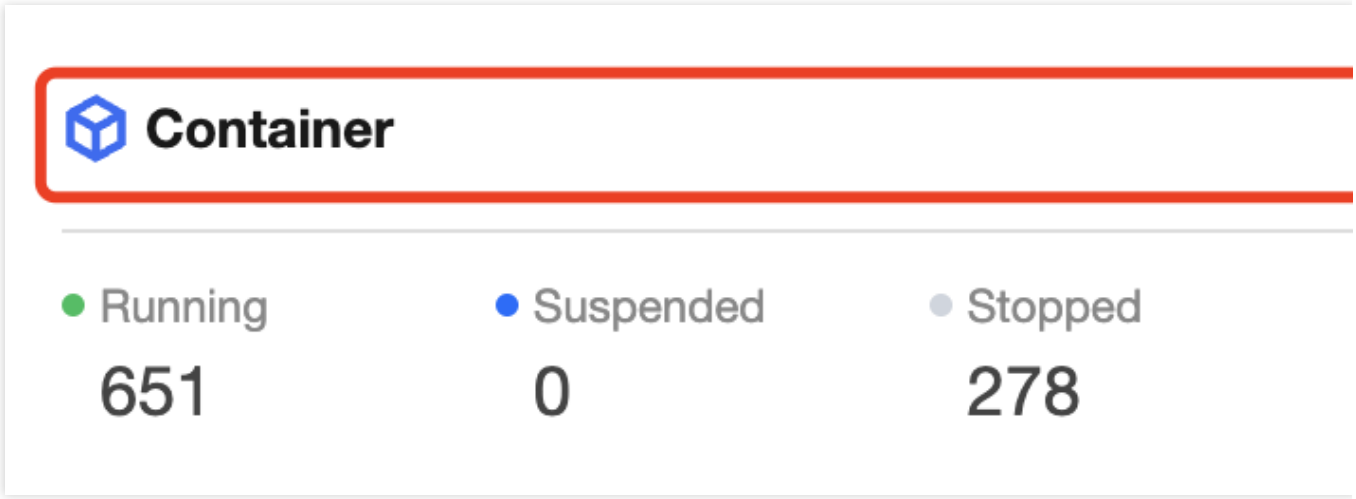
©2013-2022 Tencent Cloud. All rights reserved.





Custom list management

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Containers** to enter the container list page.

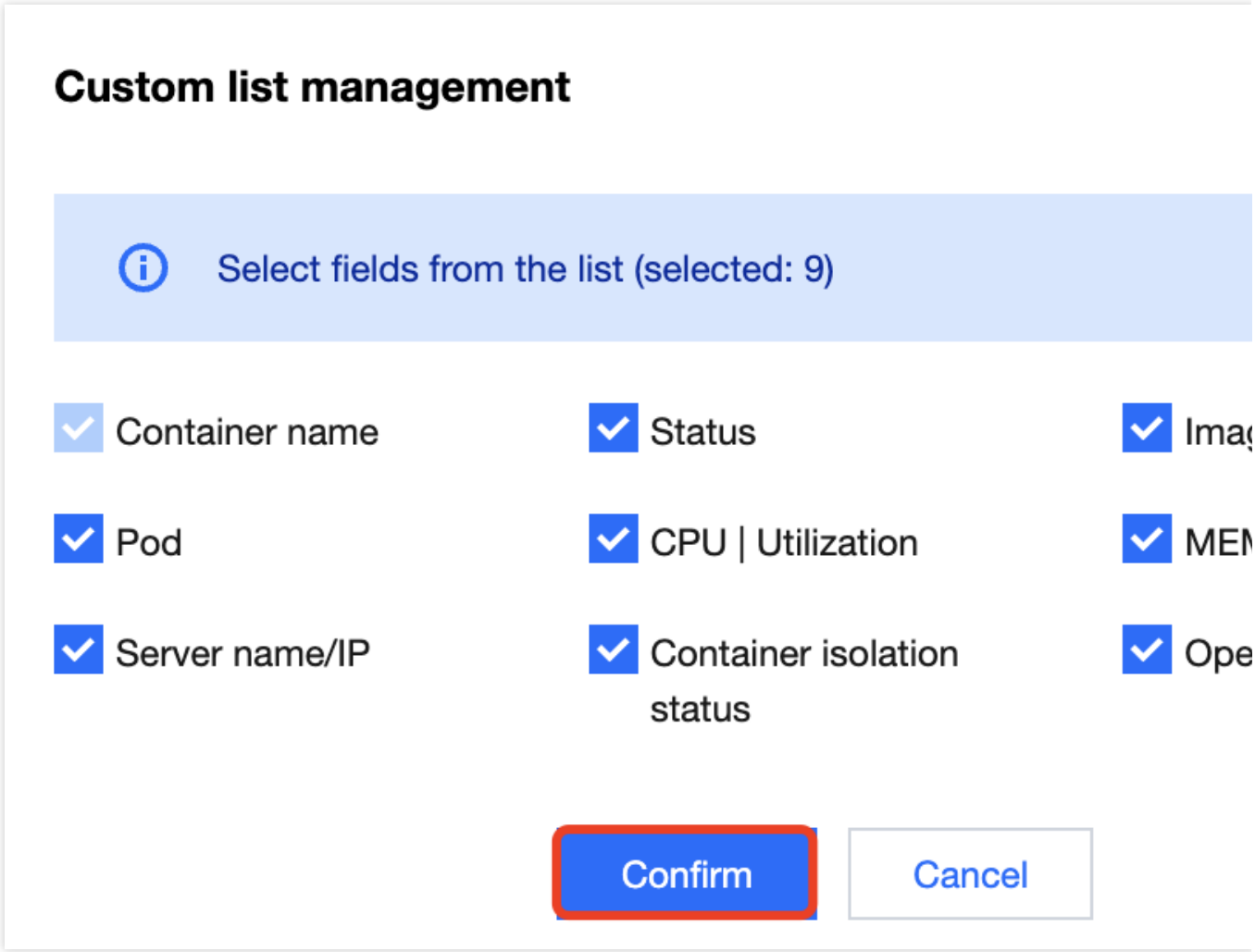


3. On the container list page, click

to pop up the **Custom List Management** window.

4. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Key fields in the list

1. Status: **Running**, **Suspended**, or **Aborted**.
2. Image: Name of the associated image.
3. Pod: Pod of the container.
4. CPU | Utilization: CPU utilization.
5. MEMUsage: Memory utilization.

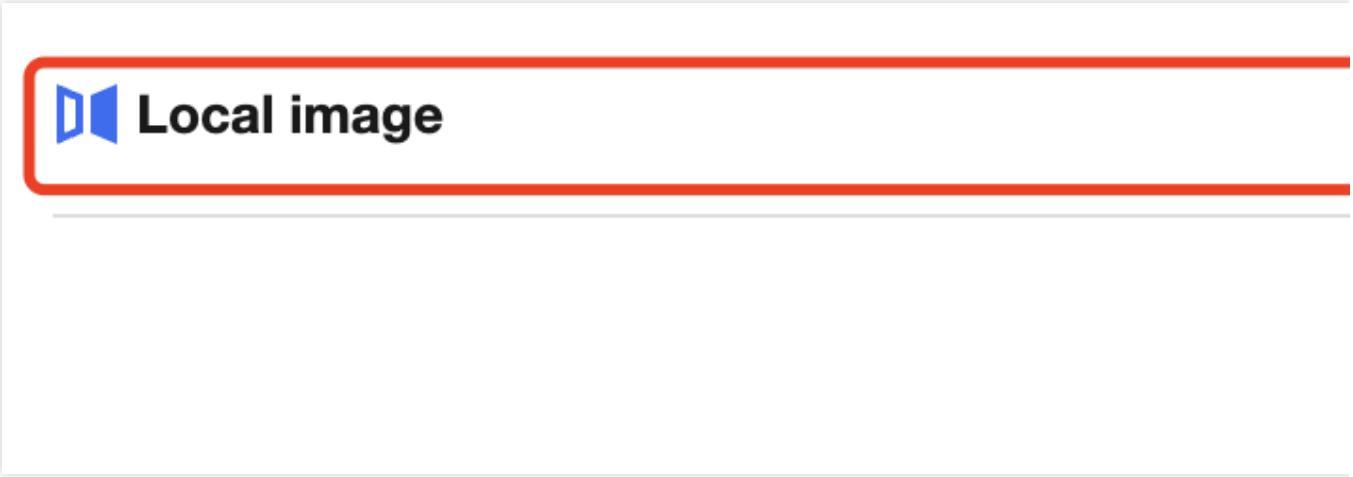
Viewing the Local Image Module

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, the image module displays the total number of images. Click **Images** to enter **Image Security** > **Local Images** and view the details.

Note:

For more information, see Local Image.

©2013-2022 Tencent Cloud. All rights reserved.

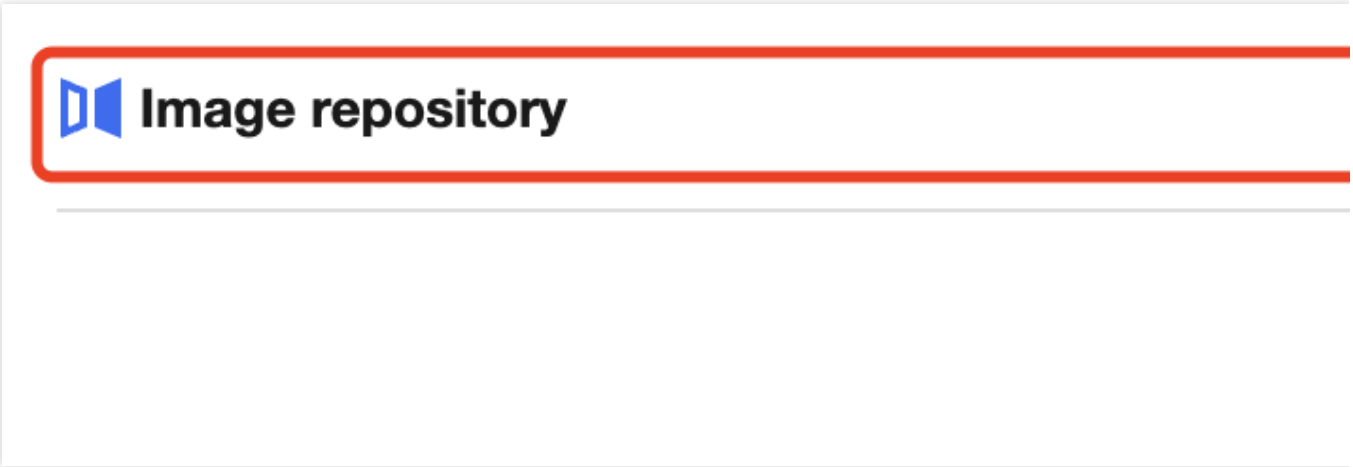


Viewing the Image Repository Module

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, the image repository module displays the total number of image repositories. Click **Image repositories** to enter **Image Security** > **Image repository** and view the details.

Note:

For more information, see Image Repository.



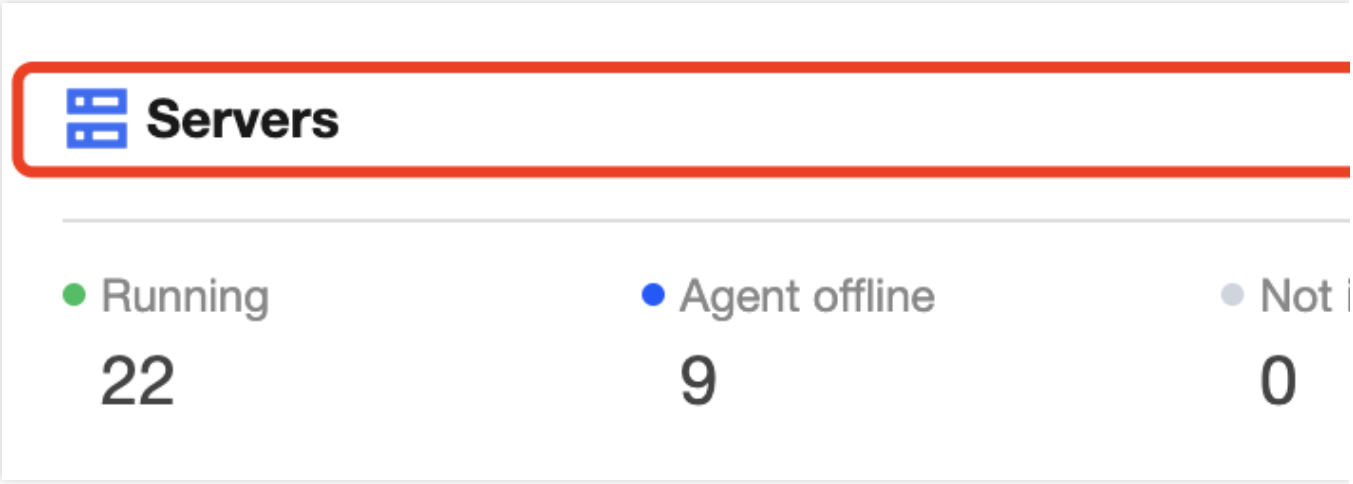
Viewing the Server Module

The server module displays the total number of servers and the numbers of running and offline servers.

Filtering servers

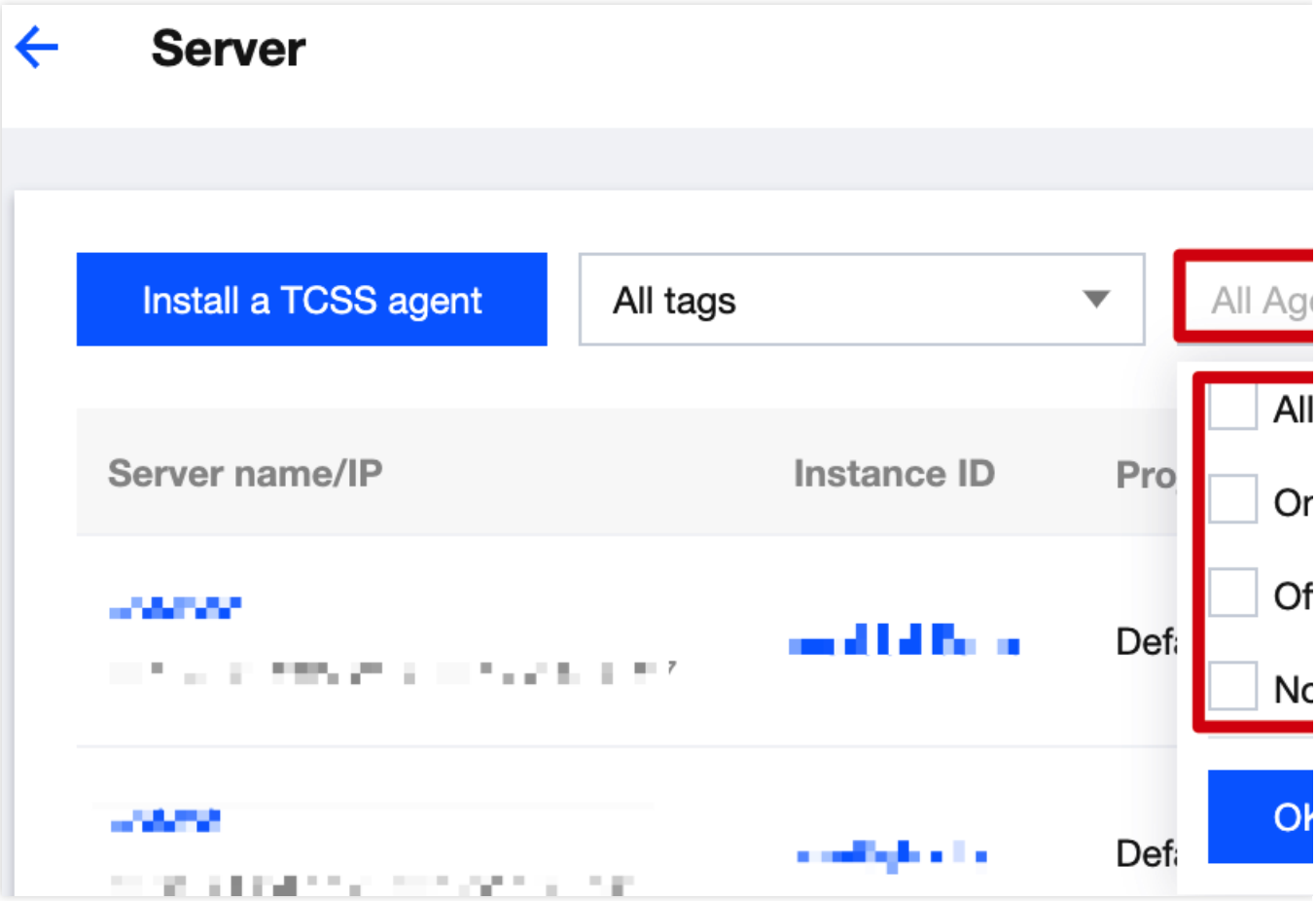
1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Servers** to view the list of all servers.

©2013-2022 Tencent Cloud. All rights reserved.



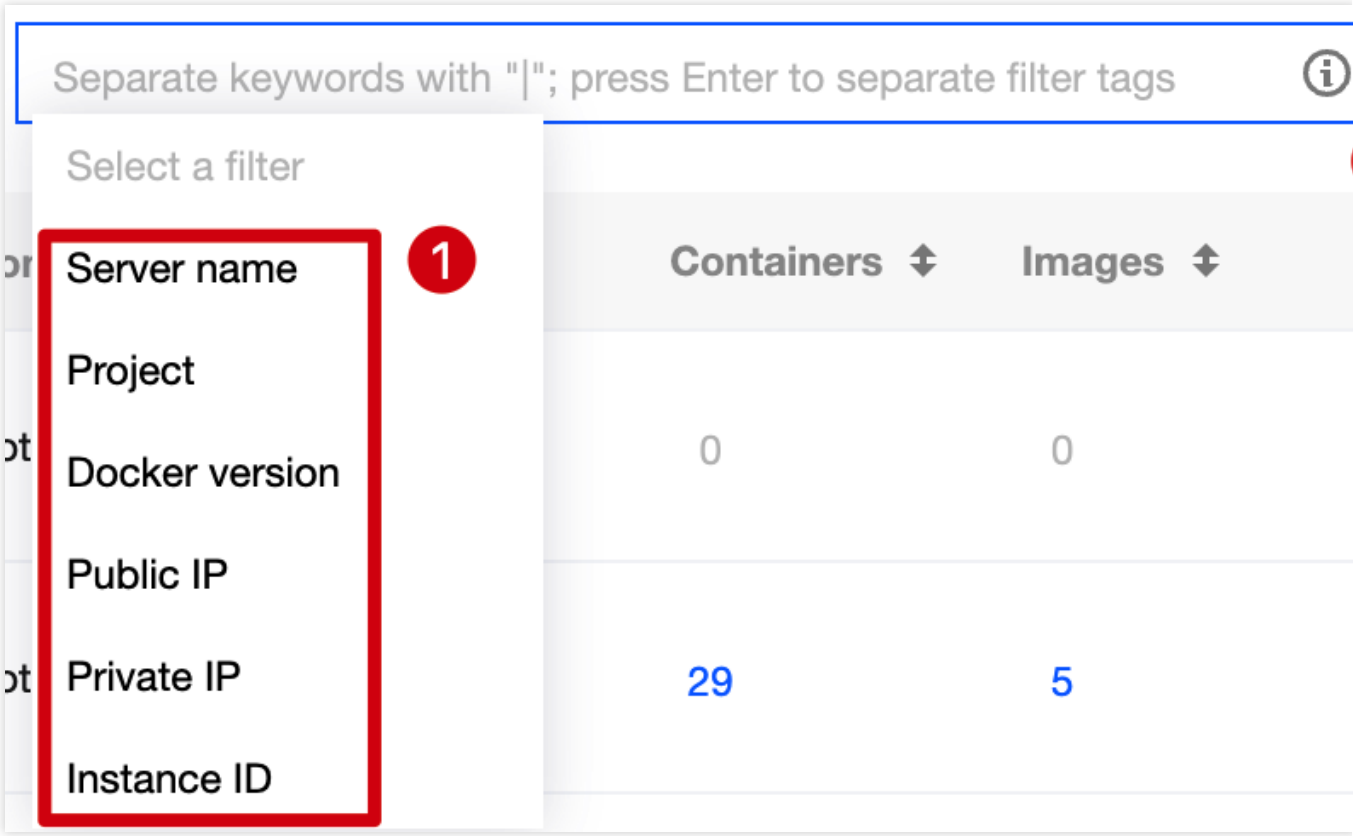
3. On the server list page, filter servers by running status or click the search box and search for servers by keyword such as server name, project, Docker version, or server IP.

Click the status drop-down list in the top-left corner to filter servers by status.



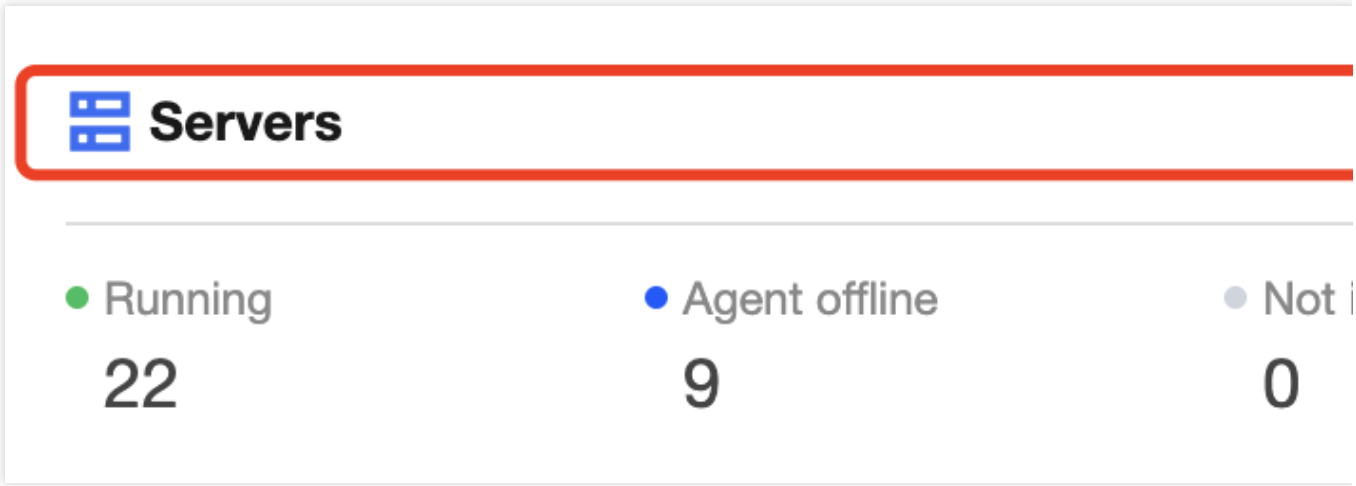
Click the search box and search for servers by keyword such as server name, project, Docker version , or server IP.

©2013-2022 Tencent Cloud. All rights reserved.



Viewing the list of containers

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Servers** to view the list of all servers.

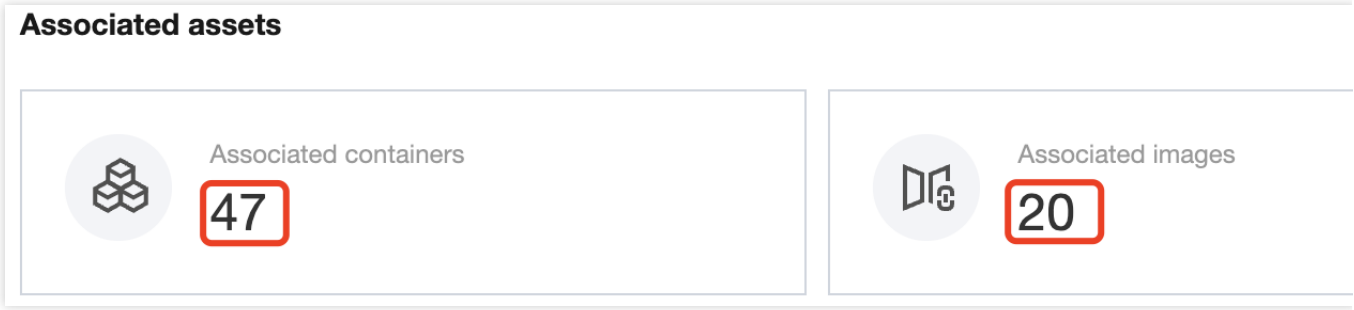


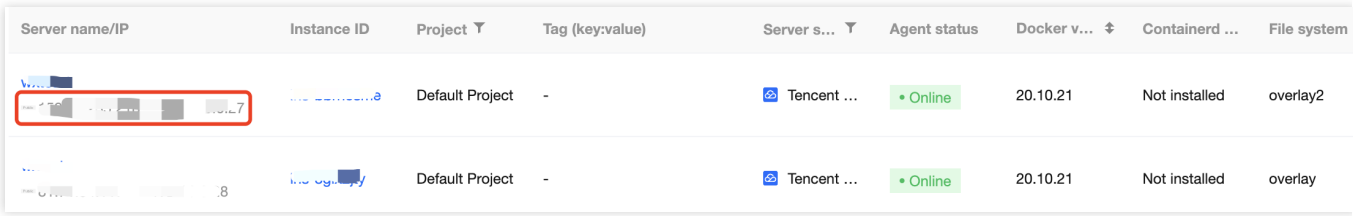
3. On the server list page, click a **Server IP** to pop up the drawer on the right, which displays the server details, including the basic server information, Docker information, and the numbers of images and containers.

Note:

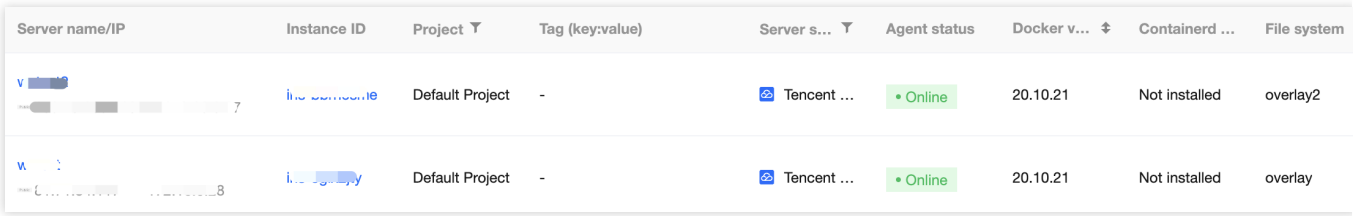
In the drawer, click the number to view the numbers of images and containers on the server.

©2013-2022 Tencent Cloud. All rights reserved.

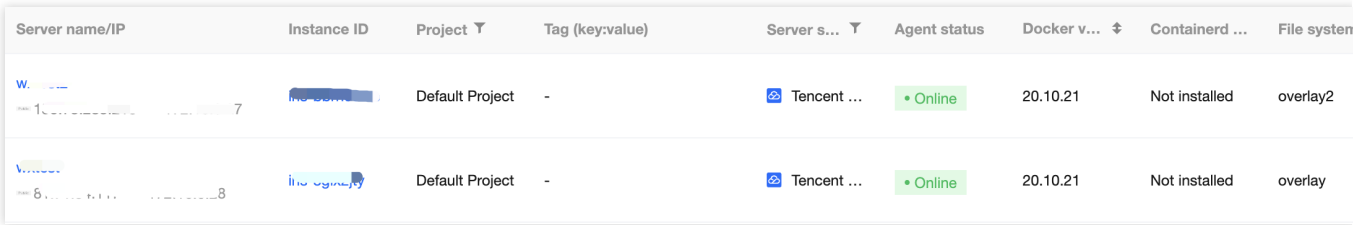




4. On the server list page, click **Images** to view the details of associated images.



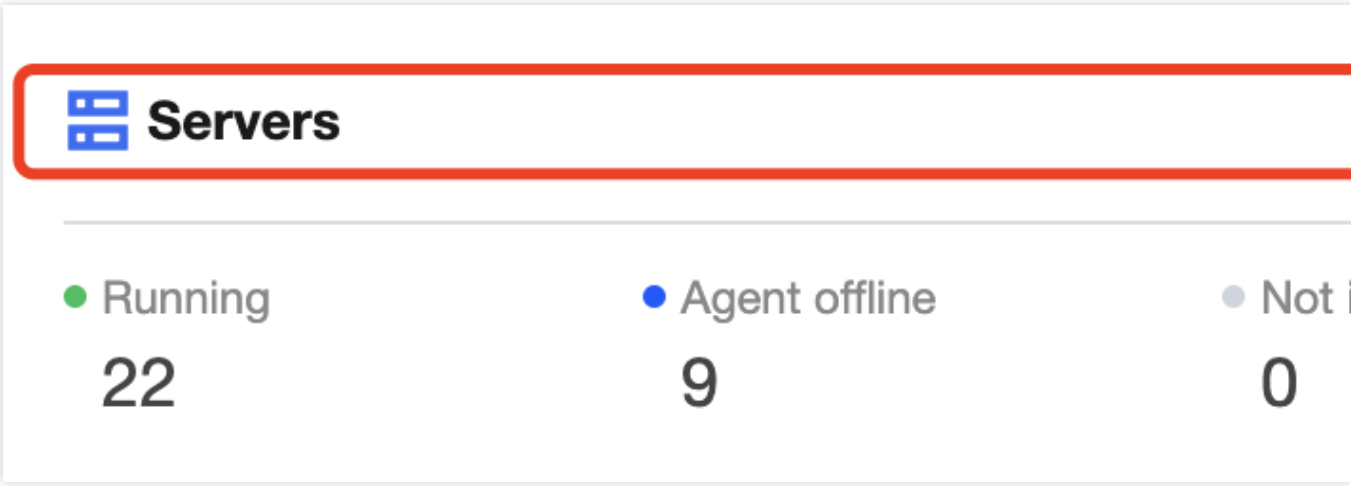
5. On the server list page, click **Containers** to view the details of associated containers.



Custom list management

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Servers** to view the list of all servers.

©2013-2022 Tencent Cloud. All rights reserved.

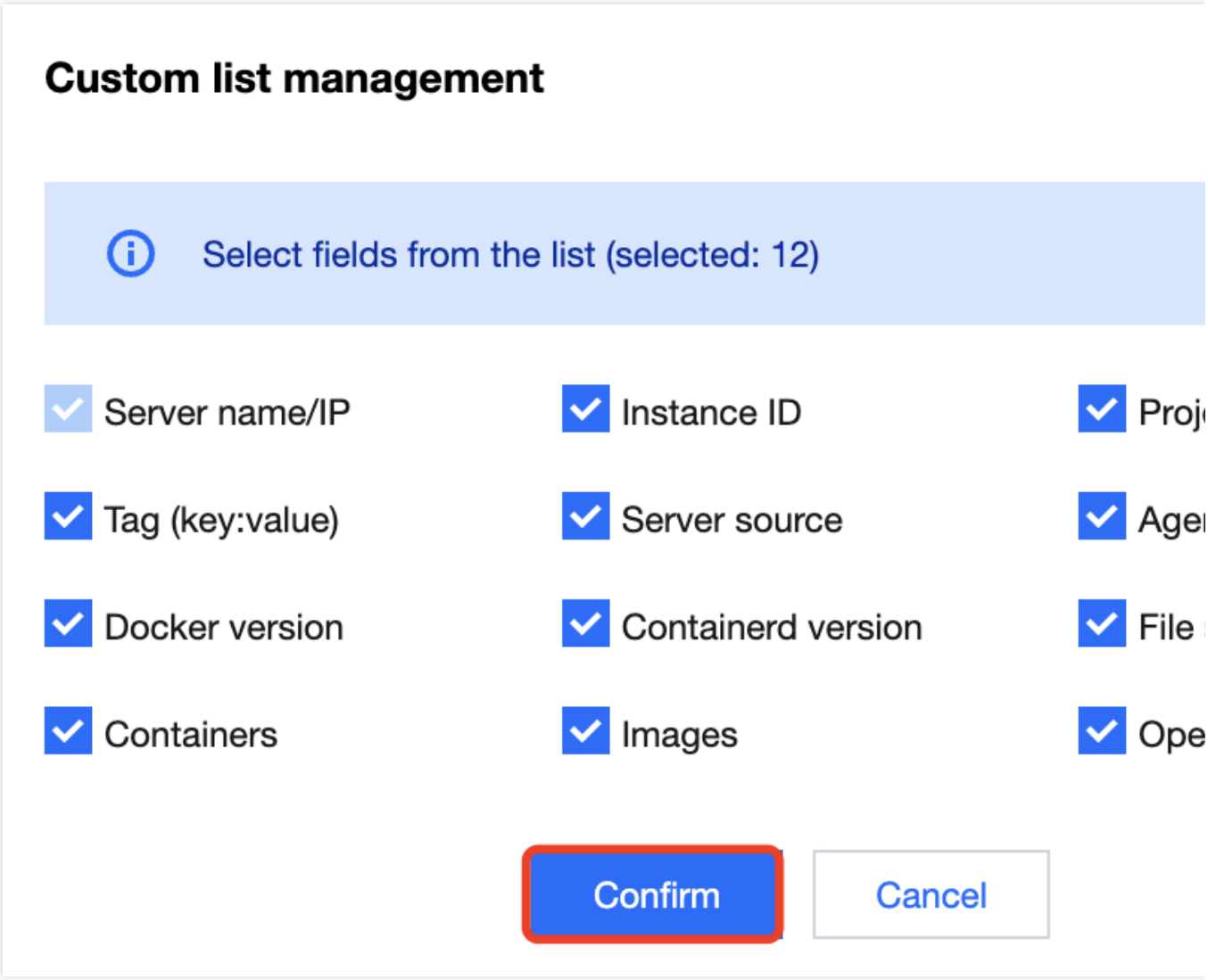


3. On the server list page, click

to pop up the **Custom List Management** window.

4. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Fields in the list

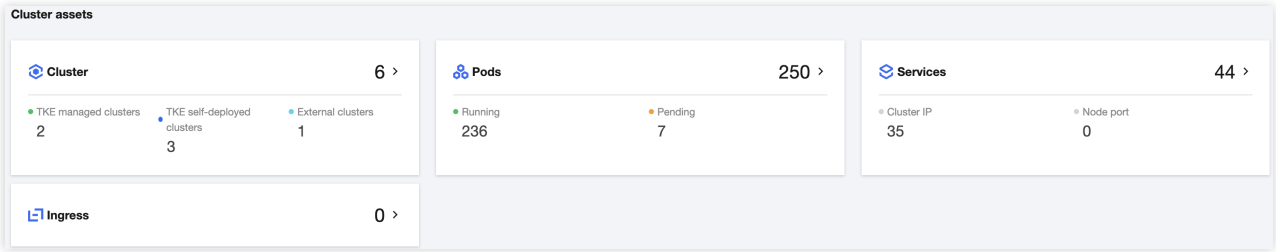
1. Server name: Server name.
2. Server IP: Click a **Server IP** to pop up the drawer on the right, which displays the server details, including the basic server information, Docker information, and the numbers of images and containers.
3. Project: Project name of the server.
4. Docker version: Docker version number. If no Docker version is installed, "Not installed" will be displayed.
5. Docker file system type: Type of the Docker file system.
6. Images: Number of images associated with the server. Click the number to view the details.
7. Containers: Number of containers associated with the server. Click the number to view the details.

©2013-2022 Tencent Cloud. All rights reserved.

Cluster Asset

Last updated：2024-01-23 15:44:44

This document describes the cluster assets feature and how to view the details of clusters, Pods, Services, and Ingresses.

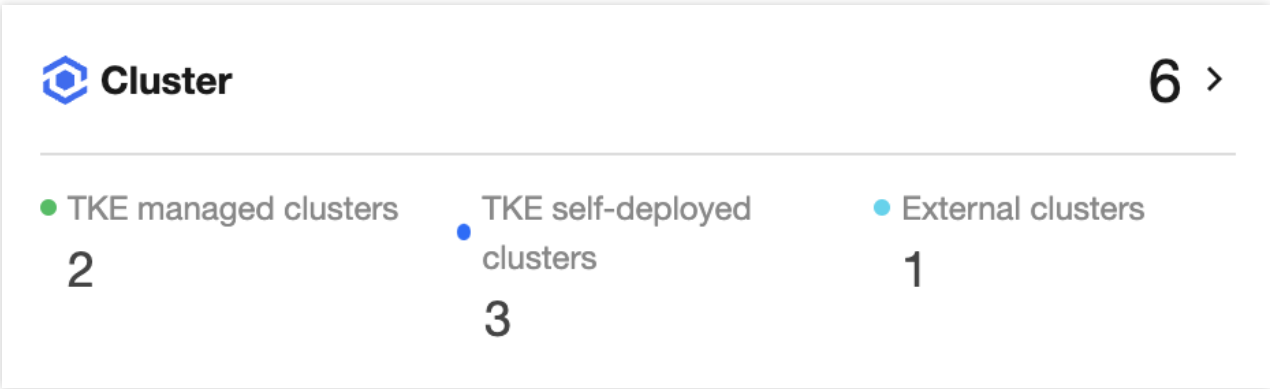


Viewing the Cluster Module

The cluster module displays the total number of clusters and the number of clusters of each type.

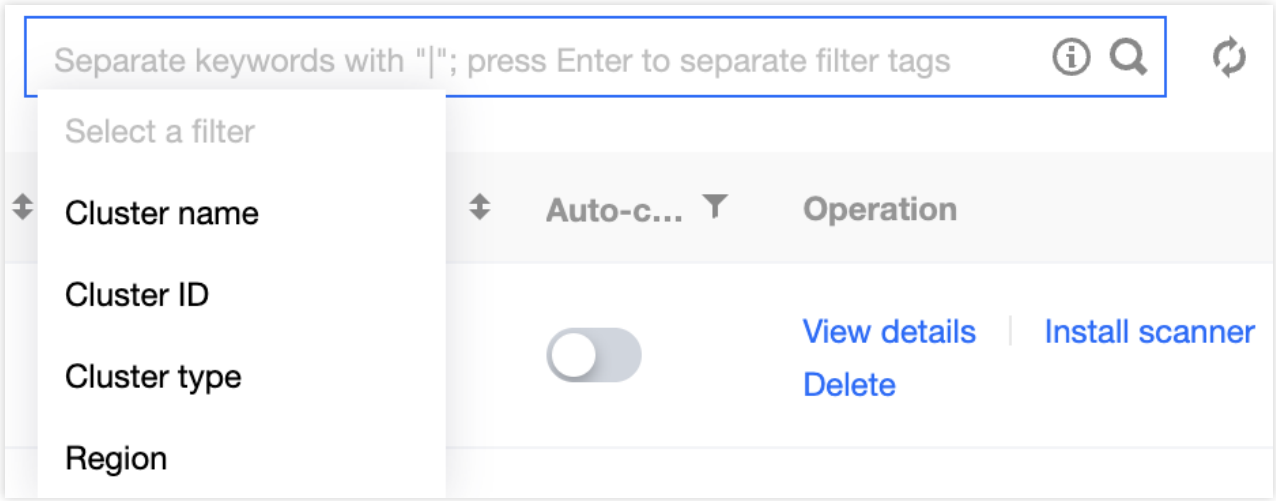
Viewing the list of clusters

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Clusters** to enter the **Security Check** page and view all clusters.



3. On the **Security Check** page, click the search box and search for clusters by keyword such as cluster name, ID, type, and region.

©2013-2022 Tencent Cloud. All rights reserved.



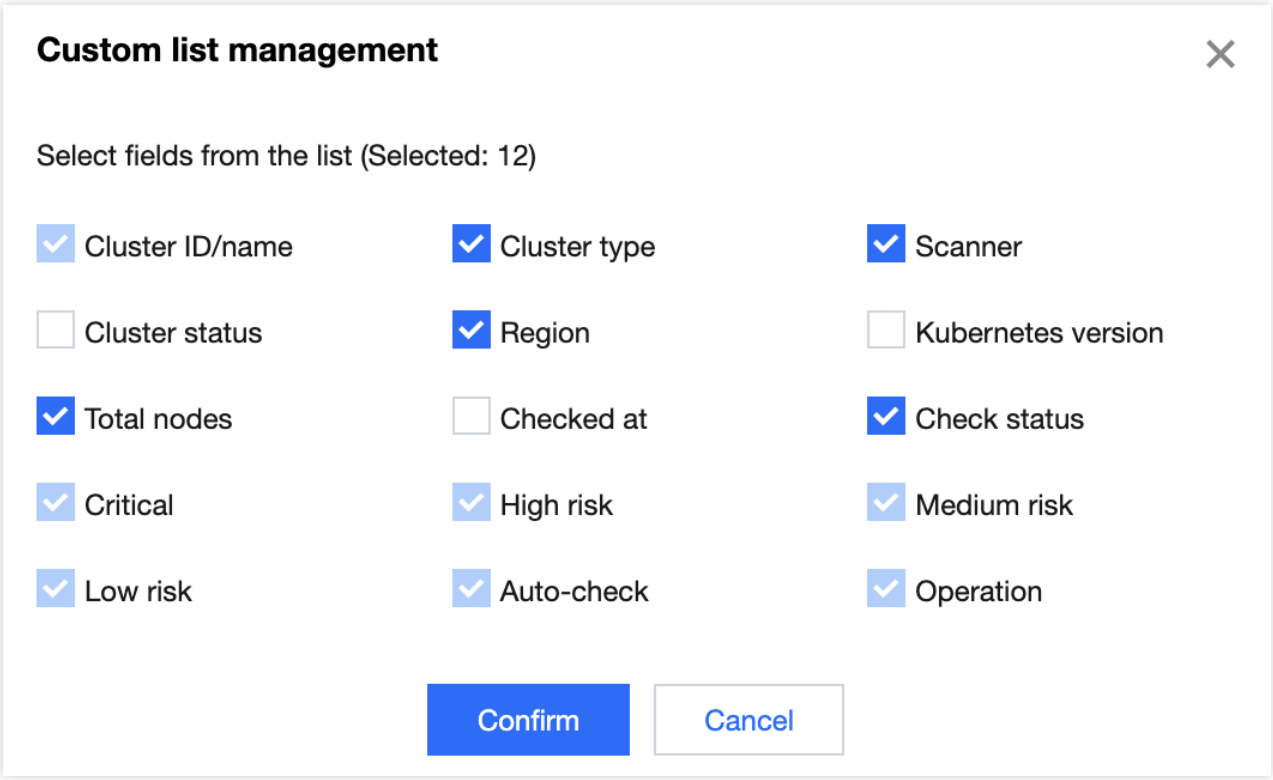
Custom list management

1. On the **Security Check** page, click

to pop up the **Custom List Management** window.

2. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.

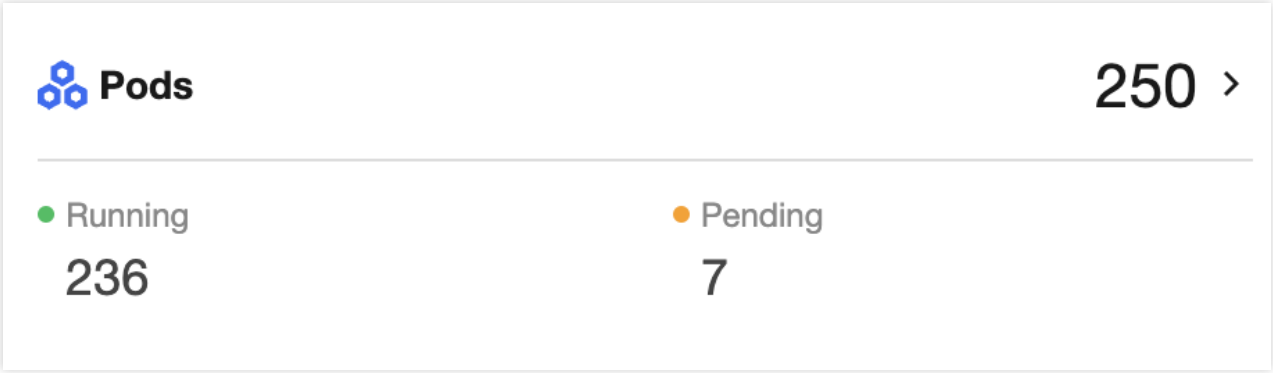


Viewing the Pod Module

The Pod module displays the total number of cluster Pods and the numbers of running and pending Pods.

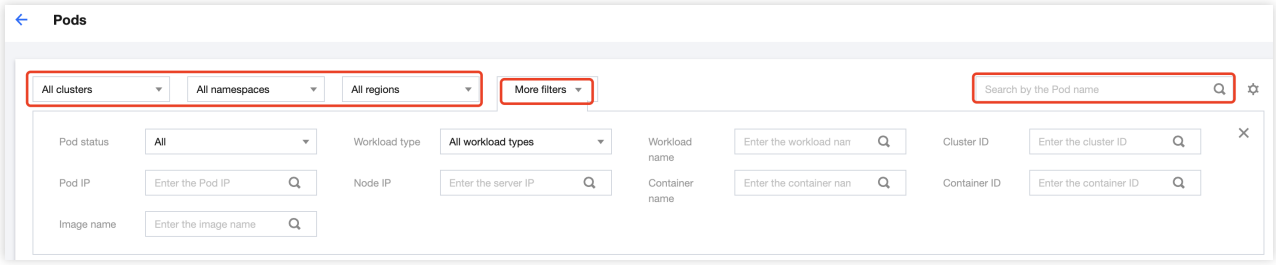
Viewing the list of Pods

1. On the **Asset Management** page, click **Pods** to enter the Pod list page and view all Pods.

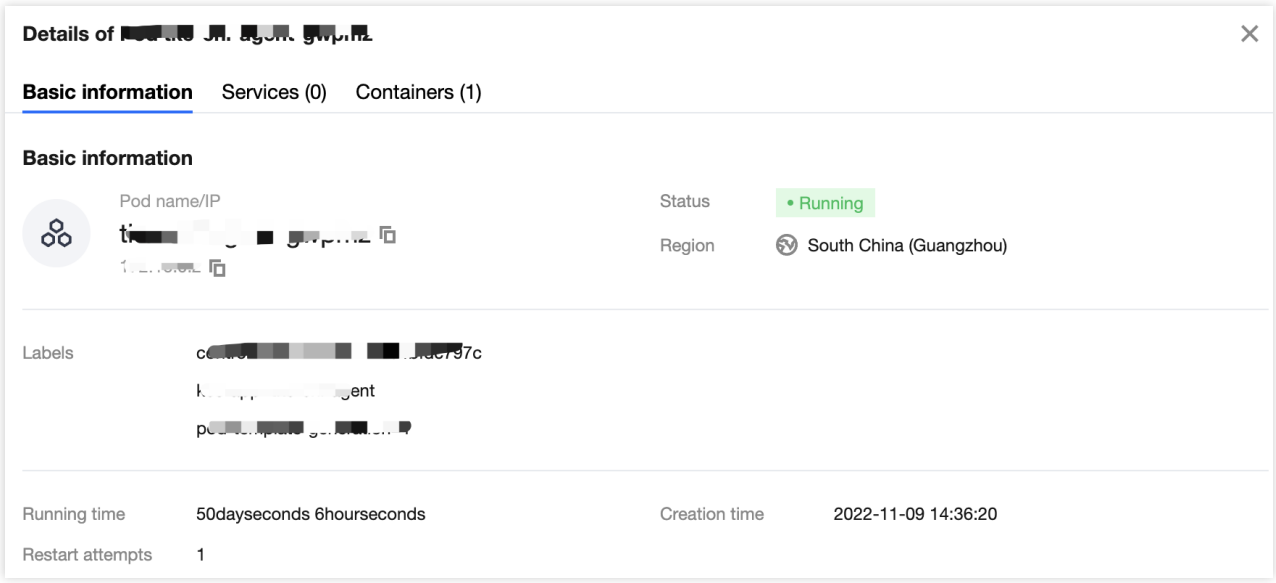


2. On the Pod list page, filter Pods by cluster name, namespace, or region; click **More filters** to filter them by Pod status, workload type, workload name, cluster ID, Pod IP, node IP, container name, container ID, or image name; or click the search box and search for Pods by Pod name.

©2013-2022 Tencent Cloud. All rights reserved.



3. Find the target Pod and click the **Pod name** to pop up the drawer on the right, which displays the Pod details, including the basic Pod information, Service information, and container information.



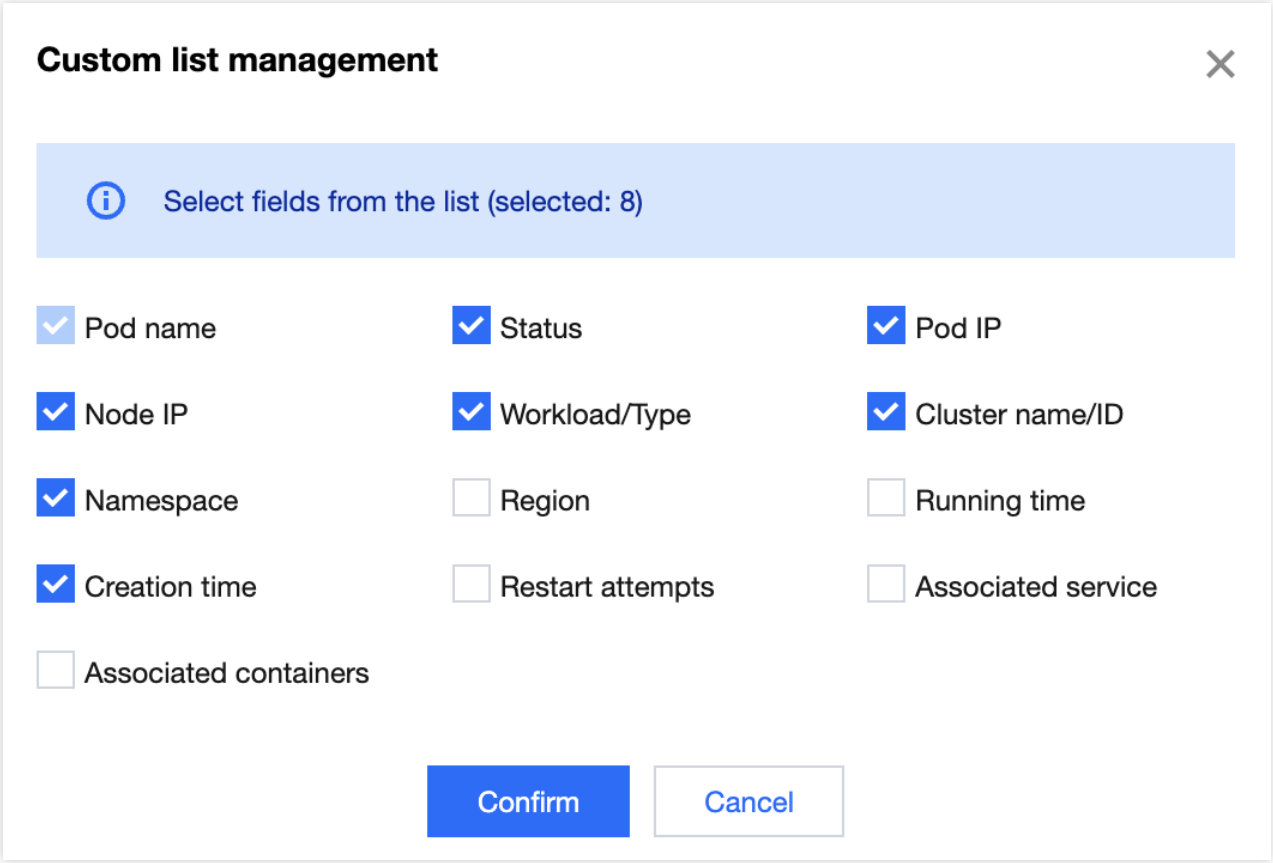
Custom list management

1. On the Pod list page, click

to pop up the **Custom List Management** window.

2. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.

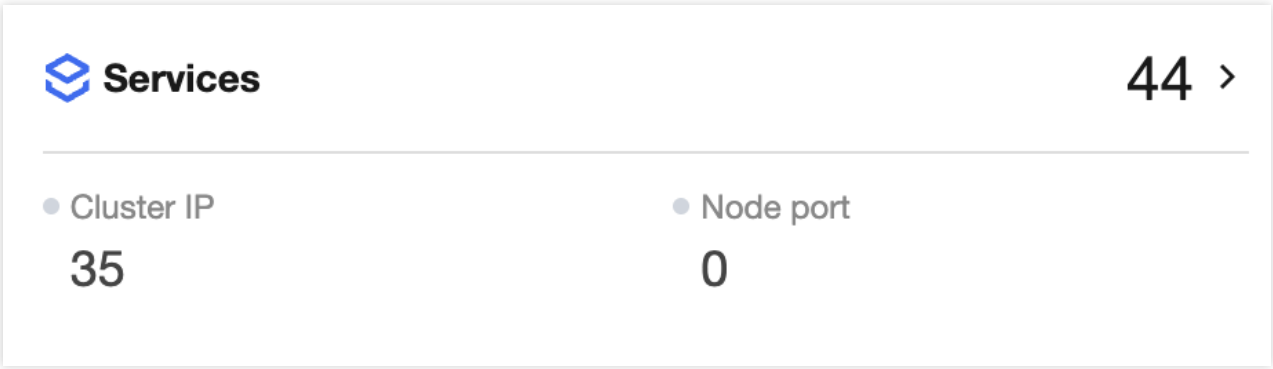


Viewing the Service Module

The Service module displays the total number of cluster Services and the numbers of Services of the ClusterIP and NodePort types.

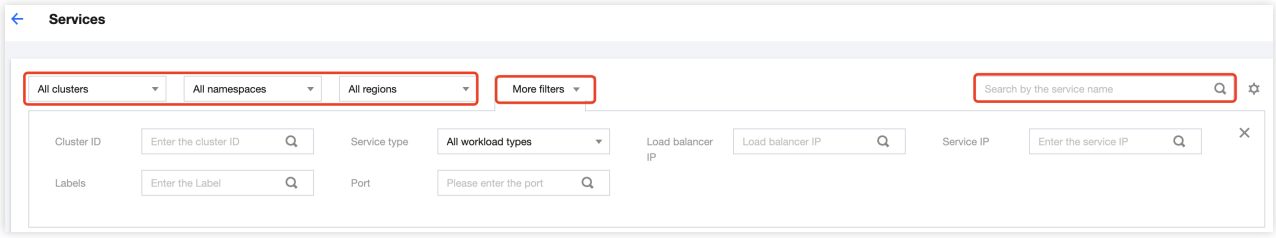
Viewing the list of Services

1. On the **Asset Management** page, click **Services** to enter the Service list page and view all Services.

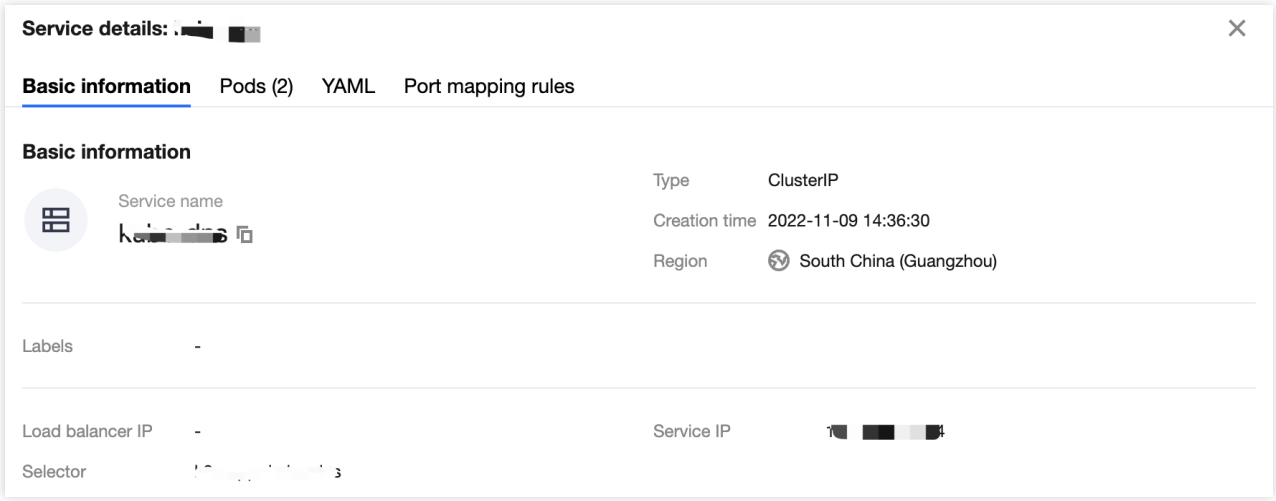


©2013-2022 Tencent Cloud. All rights reserved.

2. On the Service list page, filter Services by cluster name, namespace, or region; click **More filters** to filter them by cluster ID, Service type, load balancer IP, Service IP, label, or port; or click the search box and search for Services by Service name.



3. Find the target Service and click the **Service name** to pop up the drawer on the right, which displays the Service details, including the basic Service information, Pod information, YAML information, and port mapping rules.



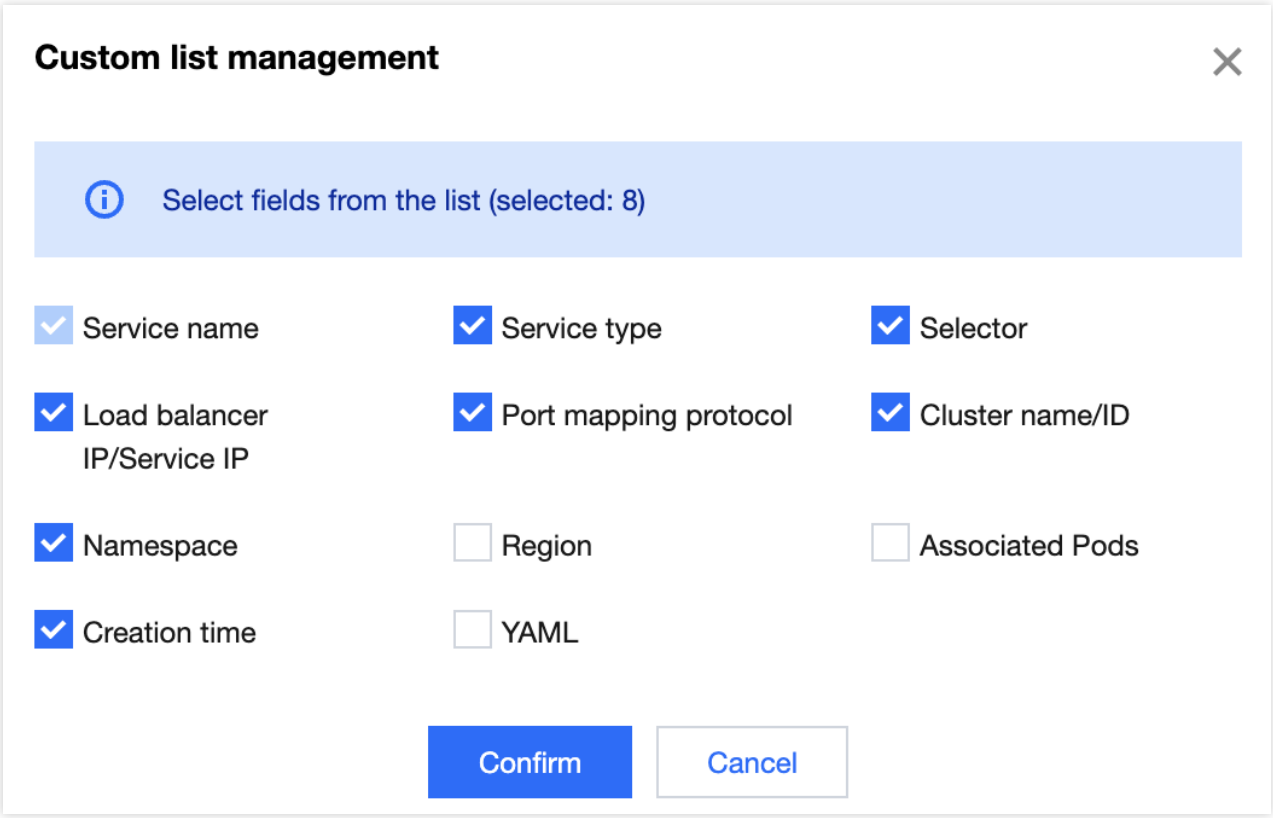
Custom list management

1. On the Service list page, click

to pop up the **Custom List Management** window.

2. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.

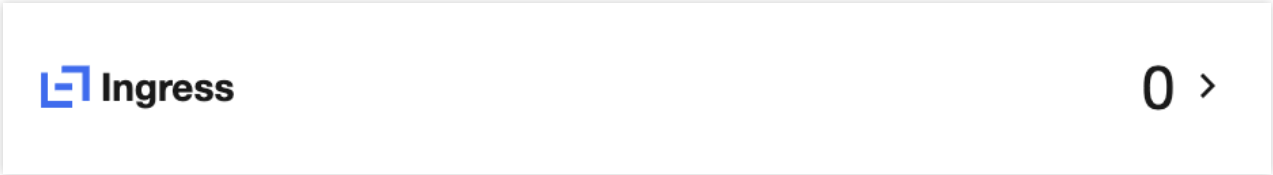


Viewing the Ingress Module

The Ingress module displays the total number of cluster Ingresses.

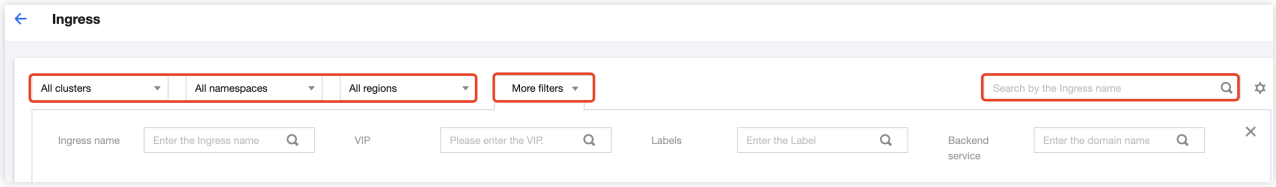
Viewing the list of Ingresses

1. On the **Asset Management** page, click **Ingresses** to enter the Ingress list page and view all Ingresses.

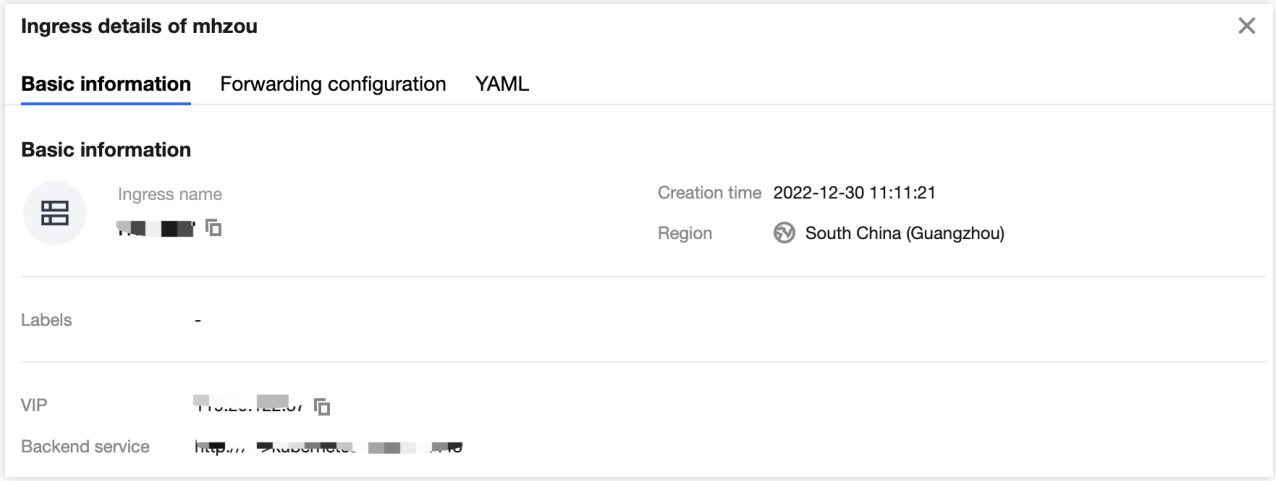


2. On the Ingress list page, filter Ingresses by cluster name, namespace, or region; click **More filters** to filter them by Ingress name, VIP, label, or backend service, or click the search box and search for Ingresses by Ingress name.

©2013-2022 Tencent Cloud. All rights reserved.



3. Find the target Ingress and click the **Ingress name** to pop up the drawer on the right, which displays the Ingress details, including the basic Ingress information, forwarding configuration, and YAML information.



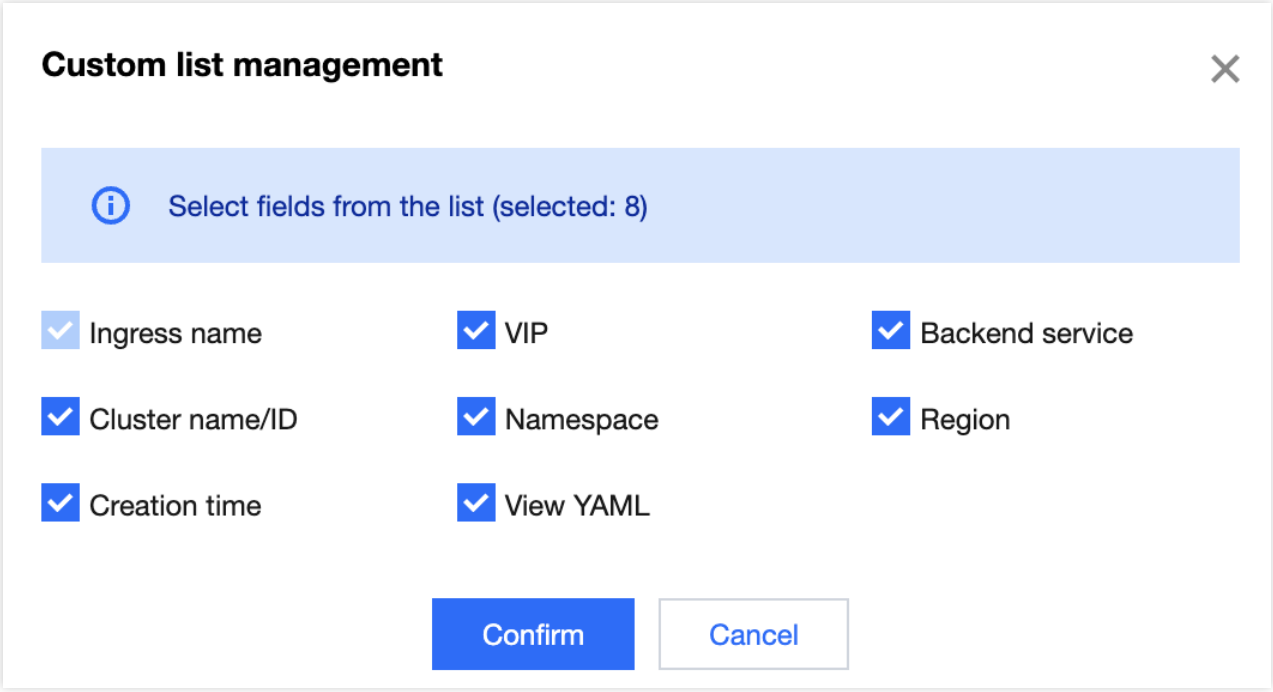
Custom list management

1. On the Ingress list page, click

to pop up the **Custom List Management** window.

2. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.

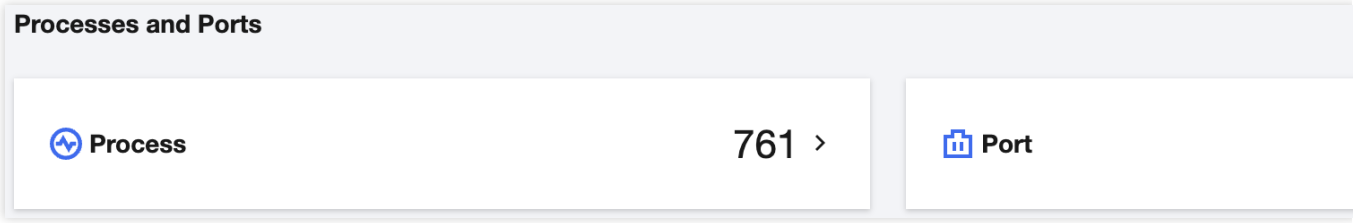


©2013-2022 Tencent Cloud. All rights reserved.

Processes and Ports

Last updated：2024-01-23 15:44:43

This document describes the processes and ports feature and how to view the process and port lists.

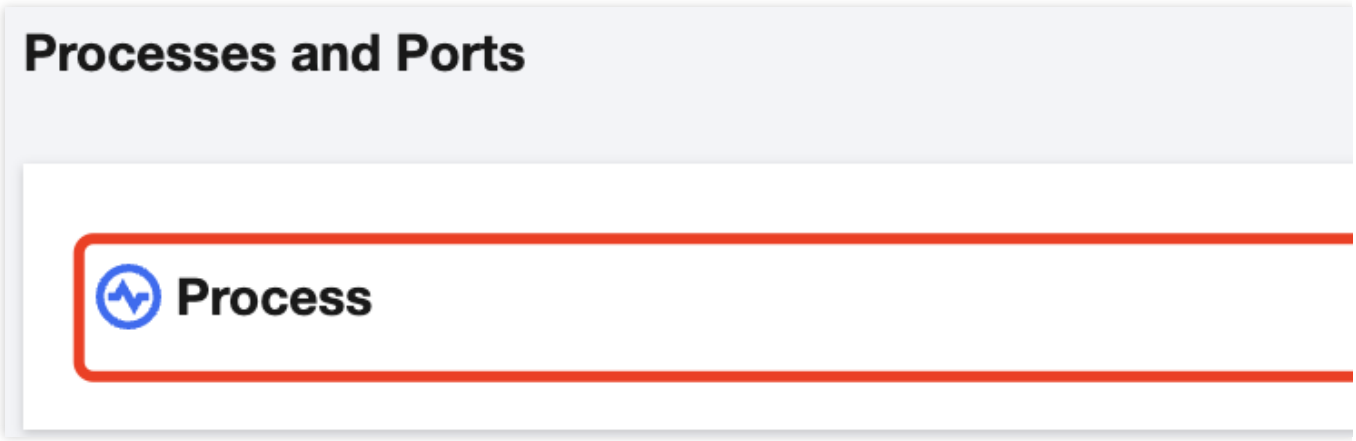


Viewing the Process Module

The process module displays the total number of processes.

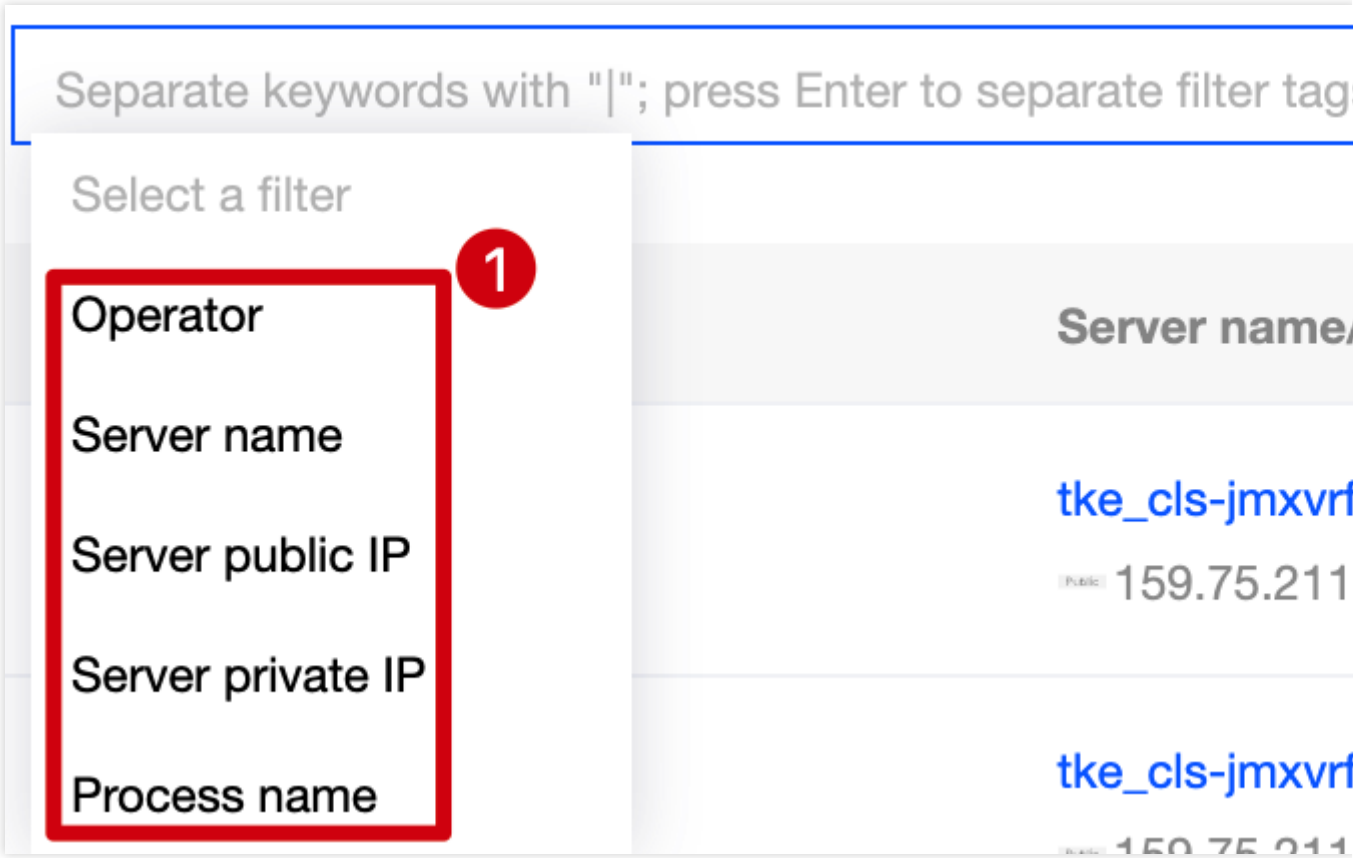
Filtering processes

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Processes** to enter the process list page.



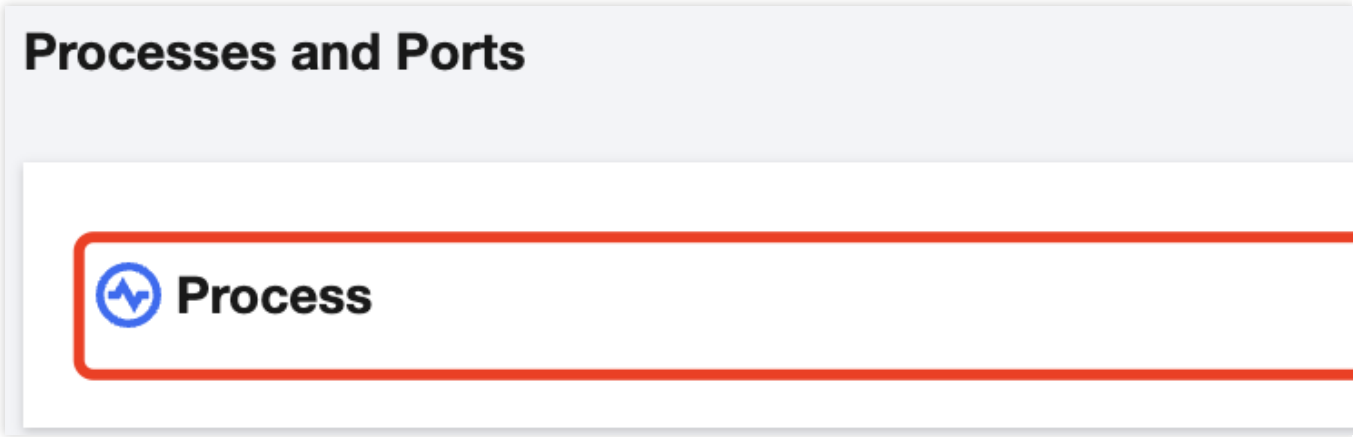
3. On the process list page, click the search box and search for processes by keyword such as initiator, server name, and process name.

©2013-2022 Tencent Cloud. All rights reserved.



Viewing the list of containers

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Processes** to enter the process list page.

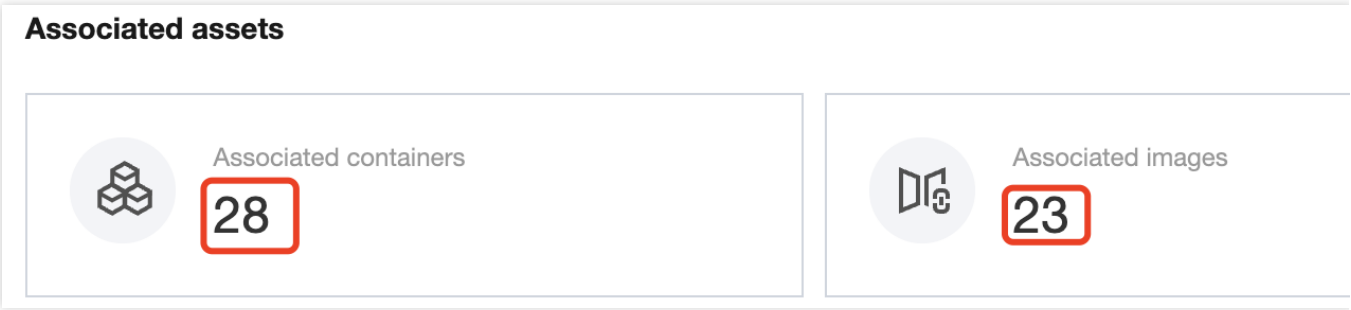


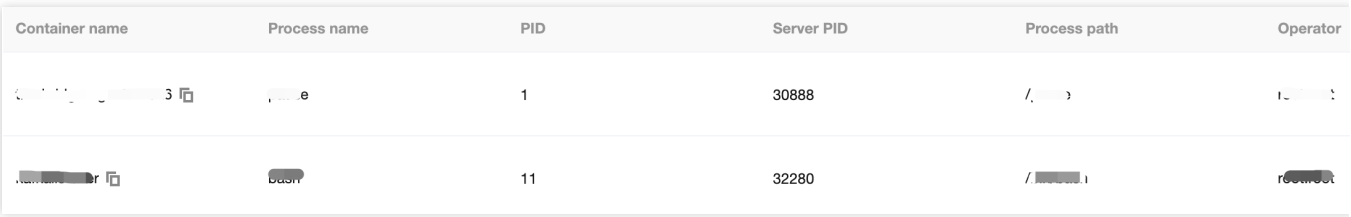
3. On the process list page, click a **Server IP** to pop up the drawer on the right, which displays the server details, including the basic server information, Docker information, and the numbers of images and containers.

Note:

In the drawer, click the number to view the numbers of images and containers on the server.

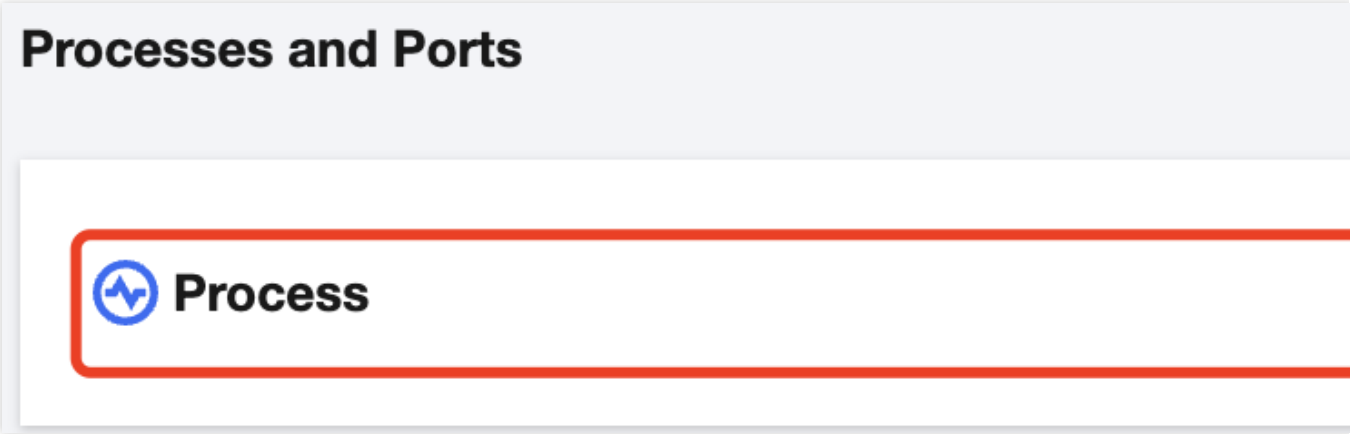
©2013-2022 Tencent Cloud. All rights reserved.





Custom list management

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Processes** to enter the process list page.

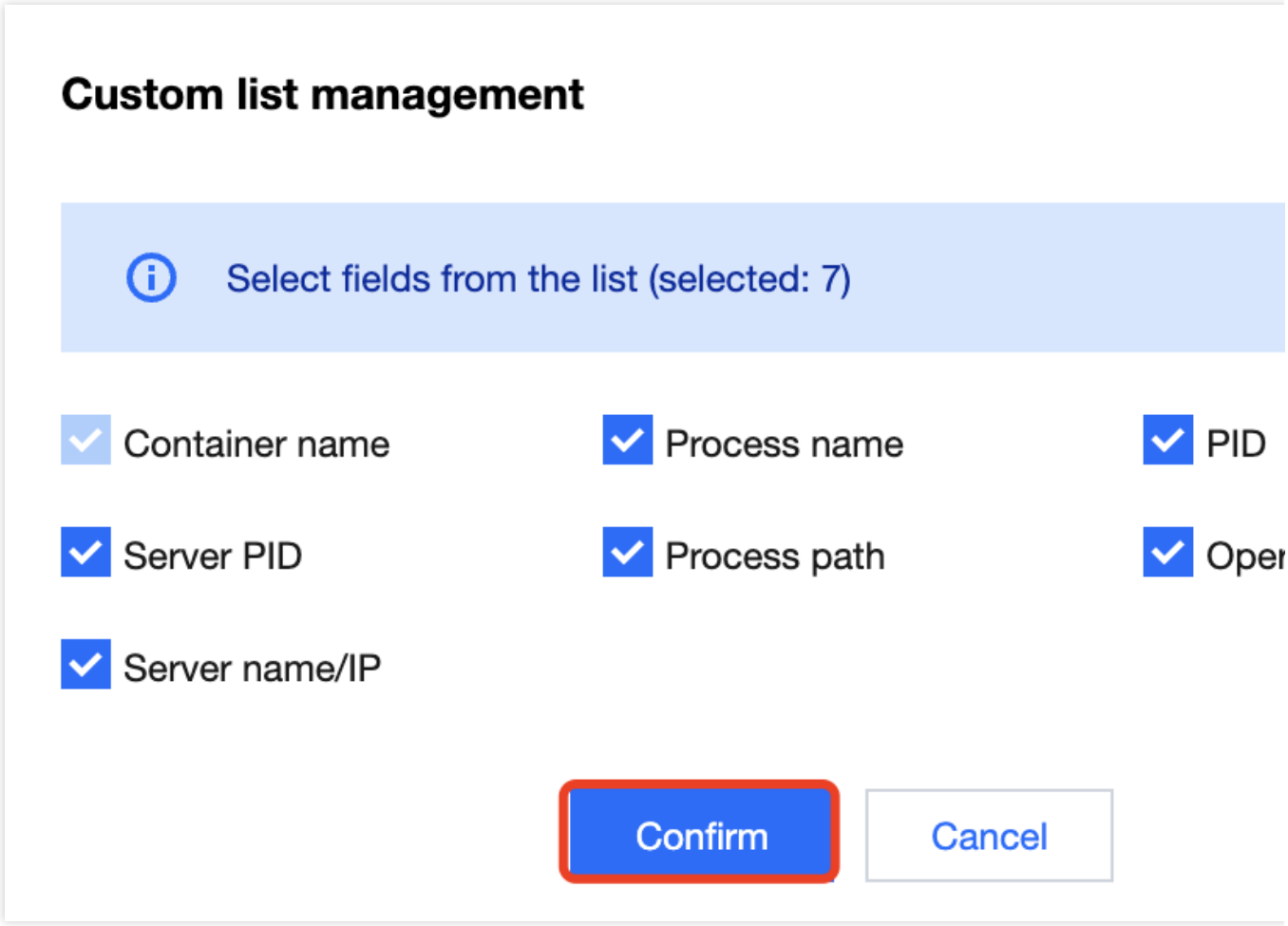


3. On the process list page, click

to pop up the **Custom List Management** window.

4. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.

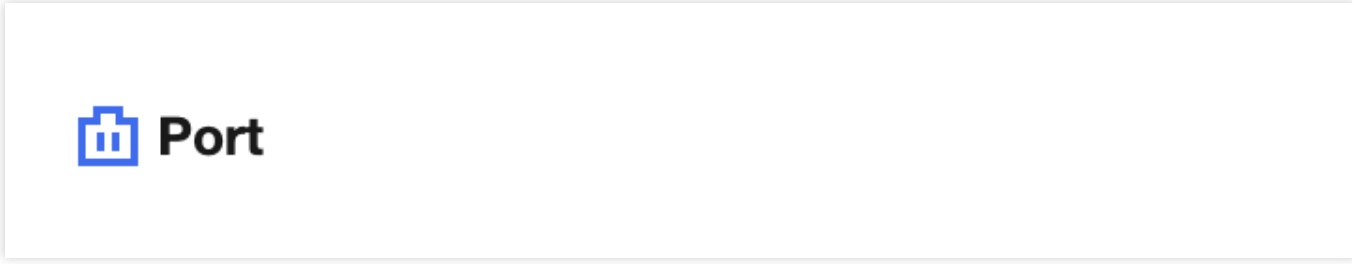


Viewing the Port Module

The port module displays the total number of ports.

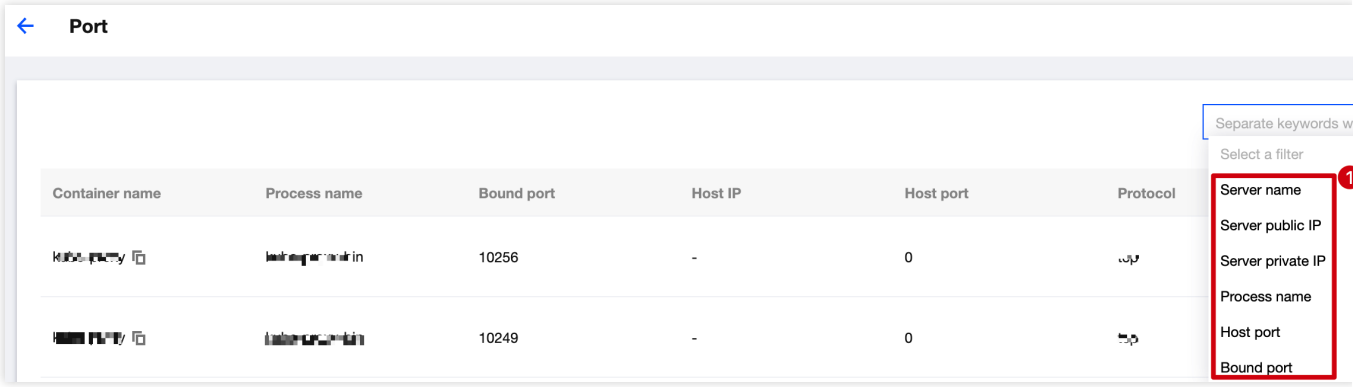
Filtering ports

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Ports** to enter the port list page.



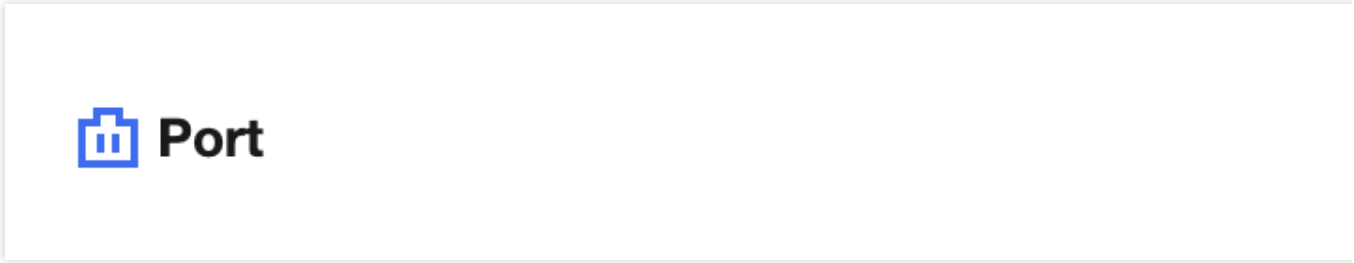
©2013-2022 Tencent Cloud. All rights reserved.

3. On the port list page, click the search box and search for ports by keyword such as server IP, process name, or host port.



Viewing the list of ports

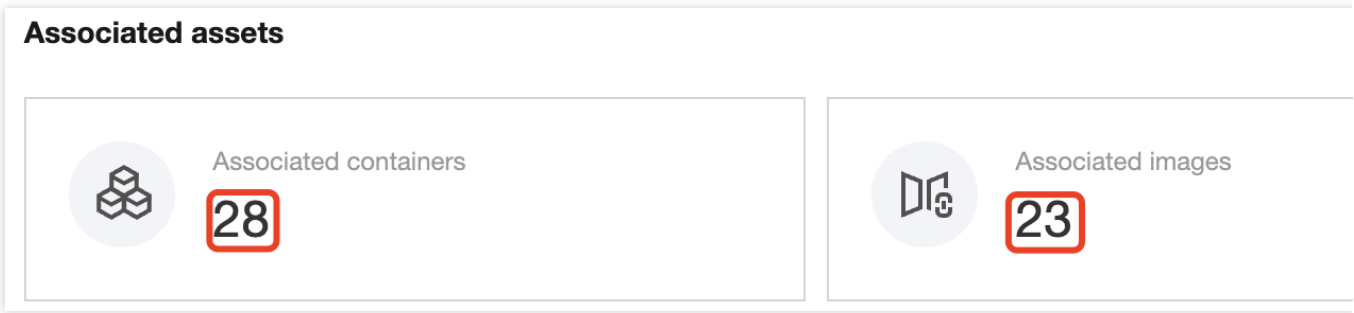
1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Ports** to enter the port list page.



3. On the port list page, click a **Server IP** to pop up the drawer on the right, which displays the server details, including the basic server information, Docker information, and the numbers of images and containers.

Note:

In the drawer, click the number to view the numbers of images and containers on the server.

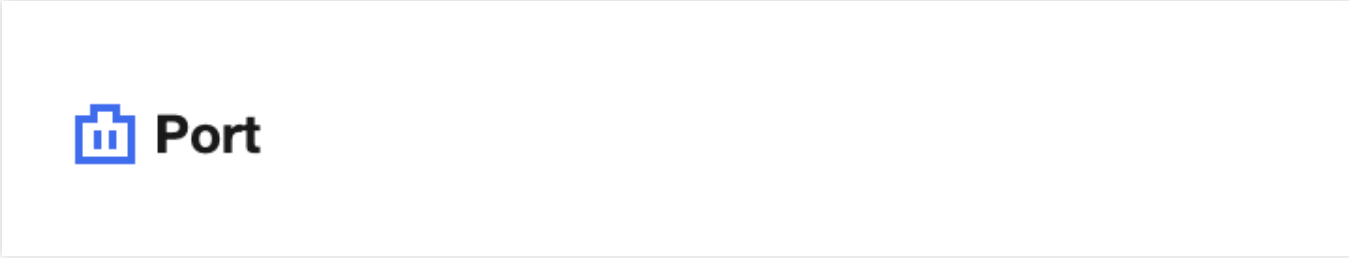


©2013-2022 Tencent Cloud. All rights reserved.

Container name	Process name	Bound port	Host IP	Host port	Protocol	PID
[redacted]	[redacted]	10256	-	0	[redacted]	1
[redacted]	[redacted]	10249	-	0	[redacted]	1

Custom list management

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Ports** to enter the port list page.

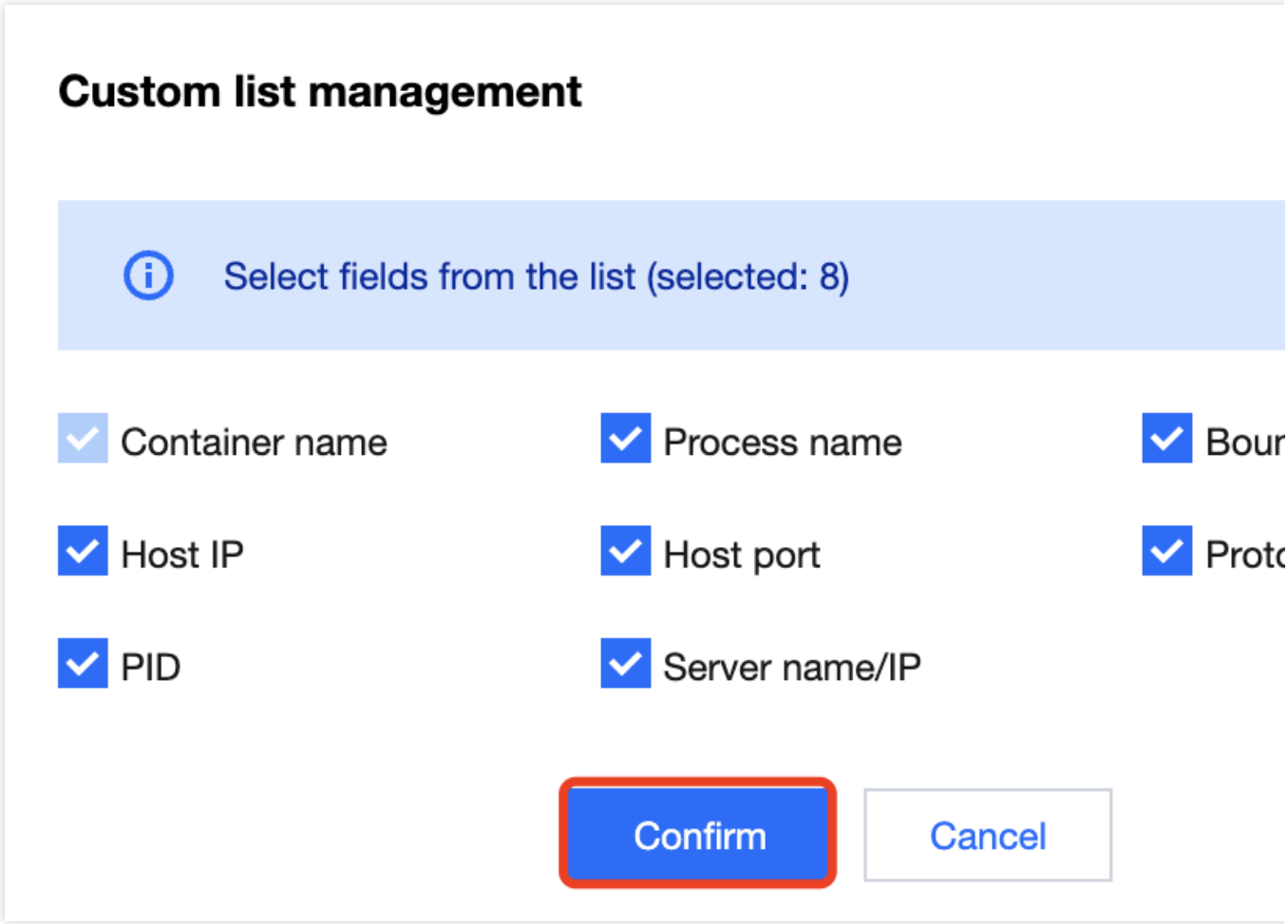


3. On the port list page, click

to pop up the **Custom List Management** window.

4. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.

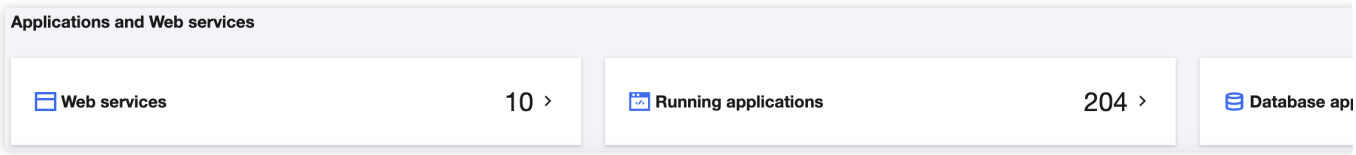


©2013-2022 Tencent Cloud. All rights reserved.

Applications and Web Services

Last updated：2024-01-23 15:44:44

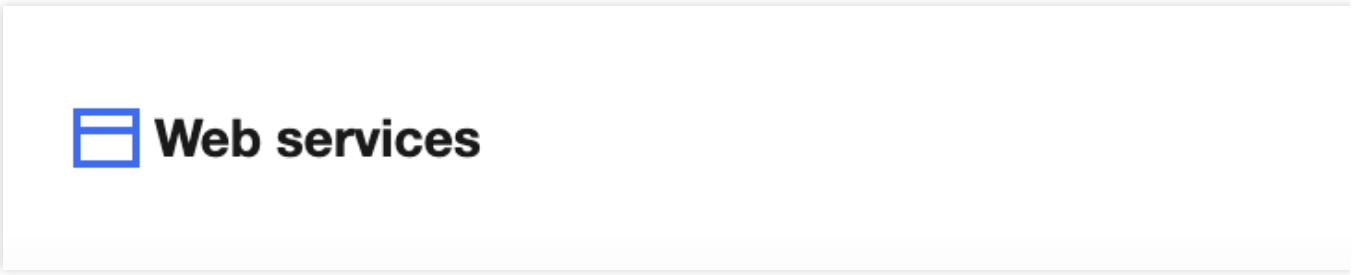
This document describes the applications and web services feature and how to view the numbers of web services, running applications, and database applications.



Viewing Web Services

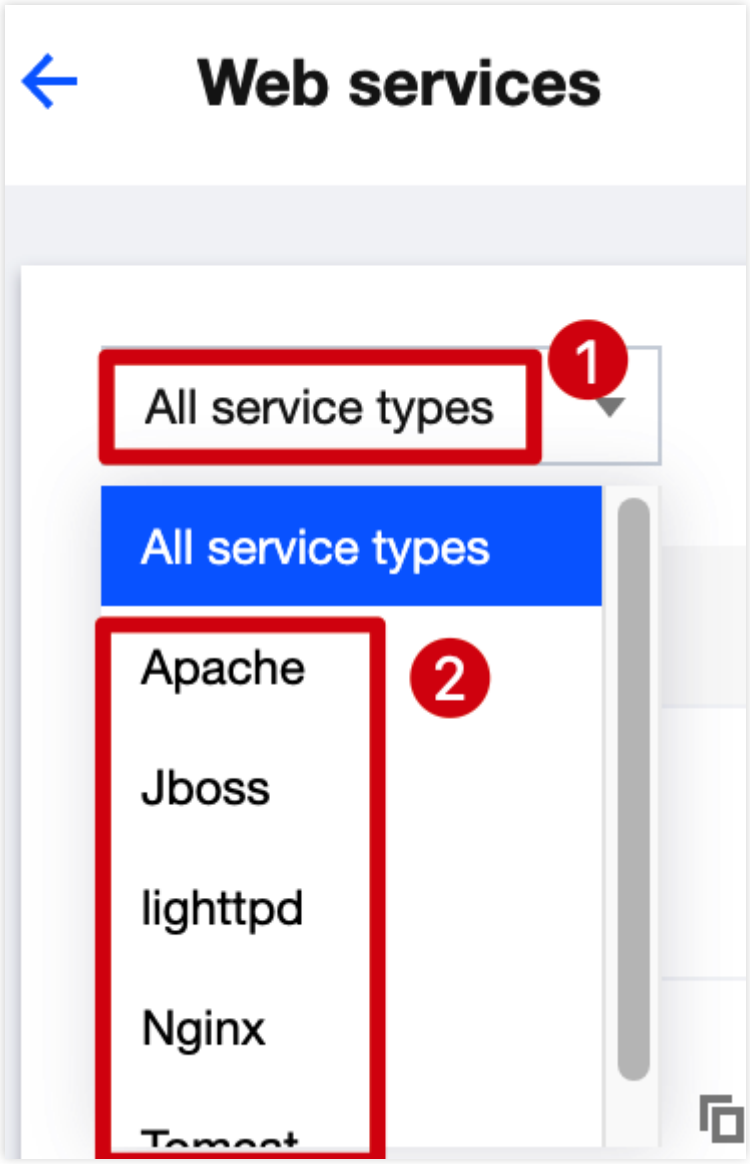
Filtering web services

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Web services** to enter the web service list page.



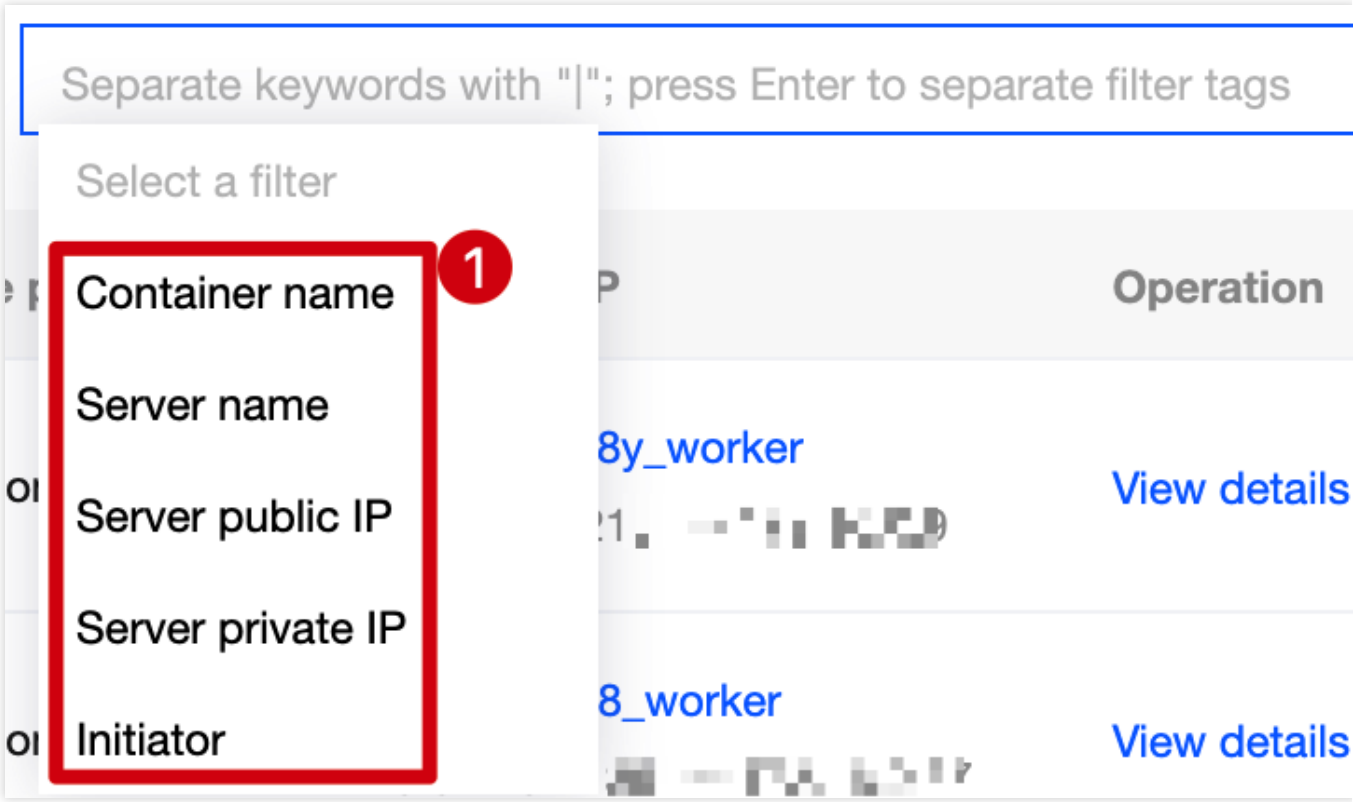
3. On the web service list page, filter web services by type or click the search box and search for web services by keyword such as container name, server name, or initiator.
Click the service type drop-down list in the top-left corner to filter web services by type.

©2013-2022 Tencent Cloud. All rights reserved.



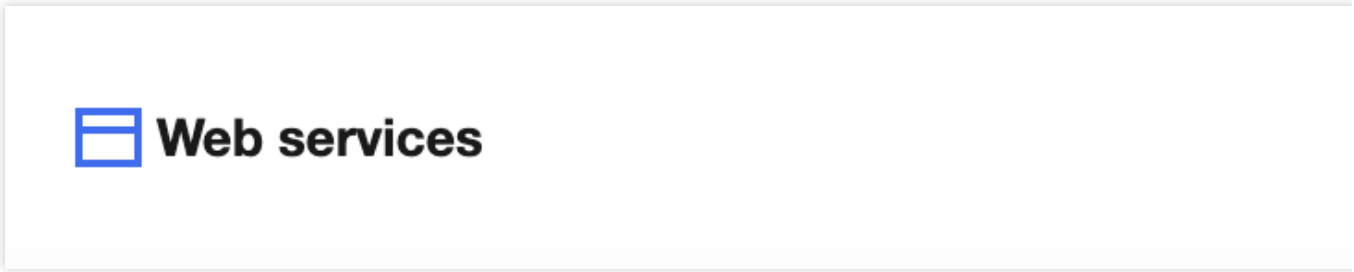
Click the search box and search for web services by keyword such as container name, server name, or initiator.

©2013-2022 Tencent Cloud. All rights reserved.



Viewing the list of web services

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Web services** to enter the web service list page.

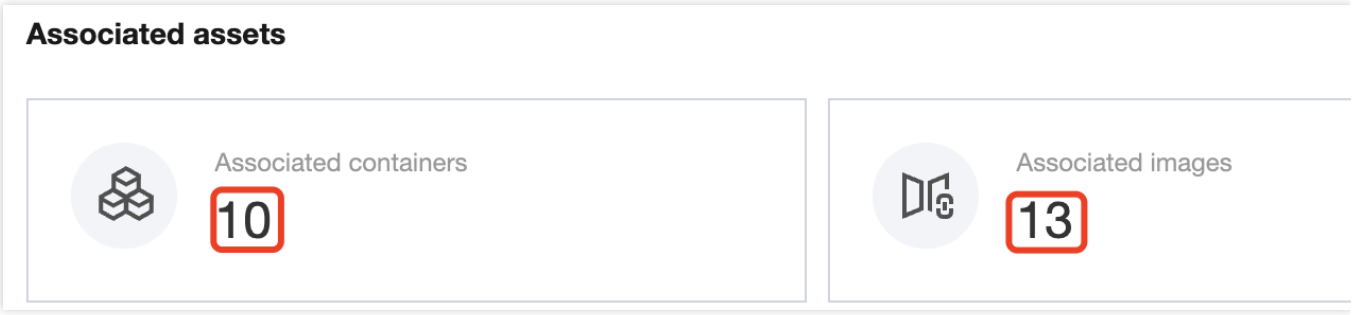


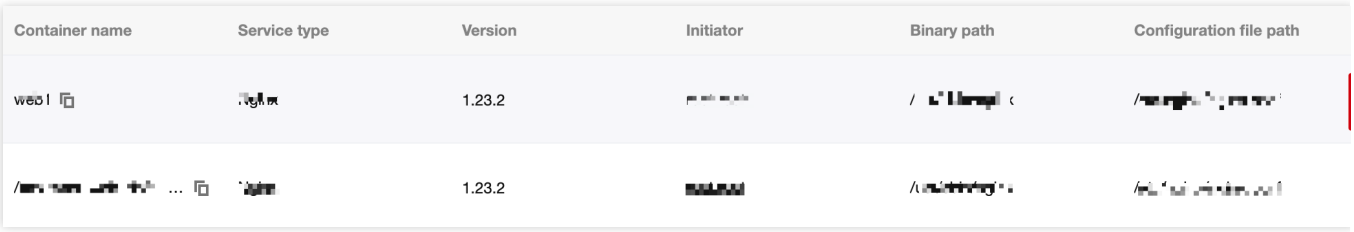
3. On the web service list page, click a **Server IP** to pop up the drawer on the right, which displays the server details, including the basic server information, Docker information, and the numbers of images and containers.

Note:

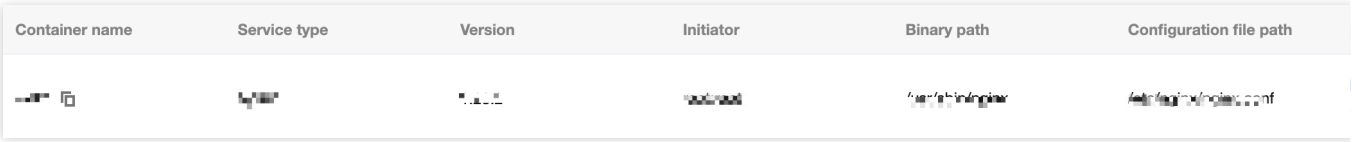
In the drawer, click the number to view the numbers of images and containers on the server.

©2013-2022 Tencent Cloud. All rights reserved.



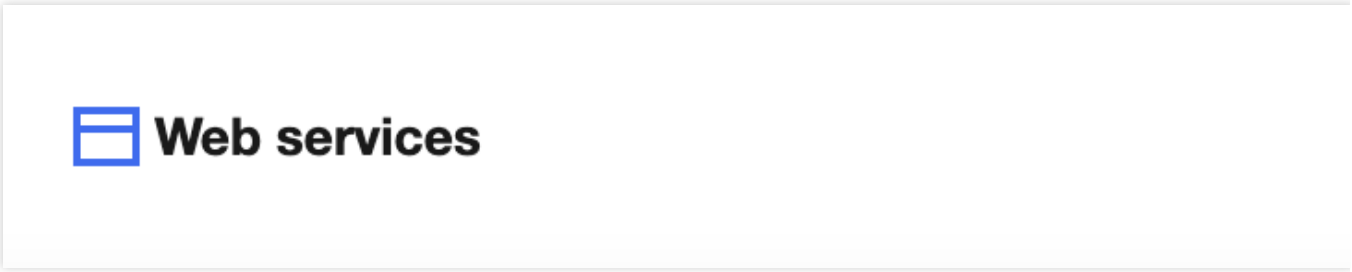


4. On the web service list page, click **View details** to pop up the window, which displays the web service details, including the basic information and list of associated processes.



Custom list management

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Web services** to enter the web service list page.

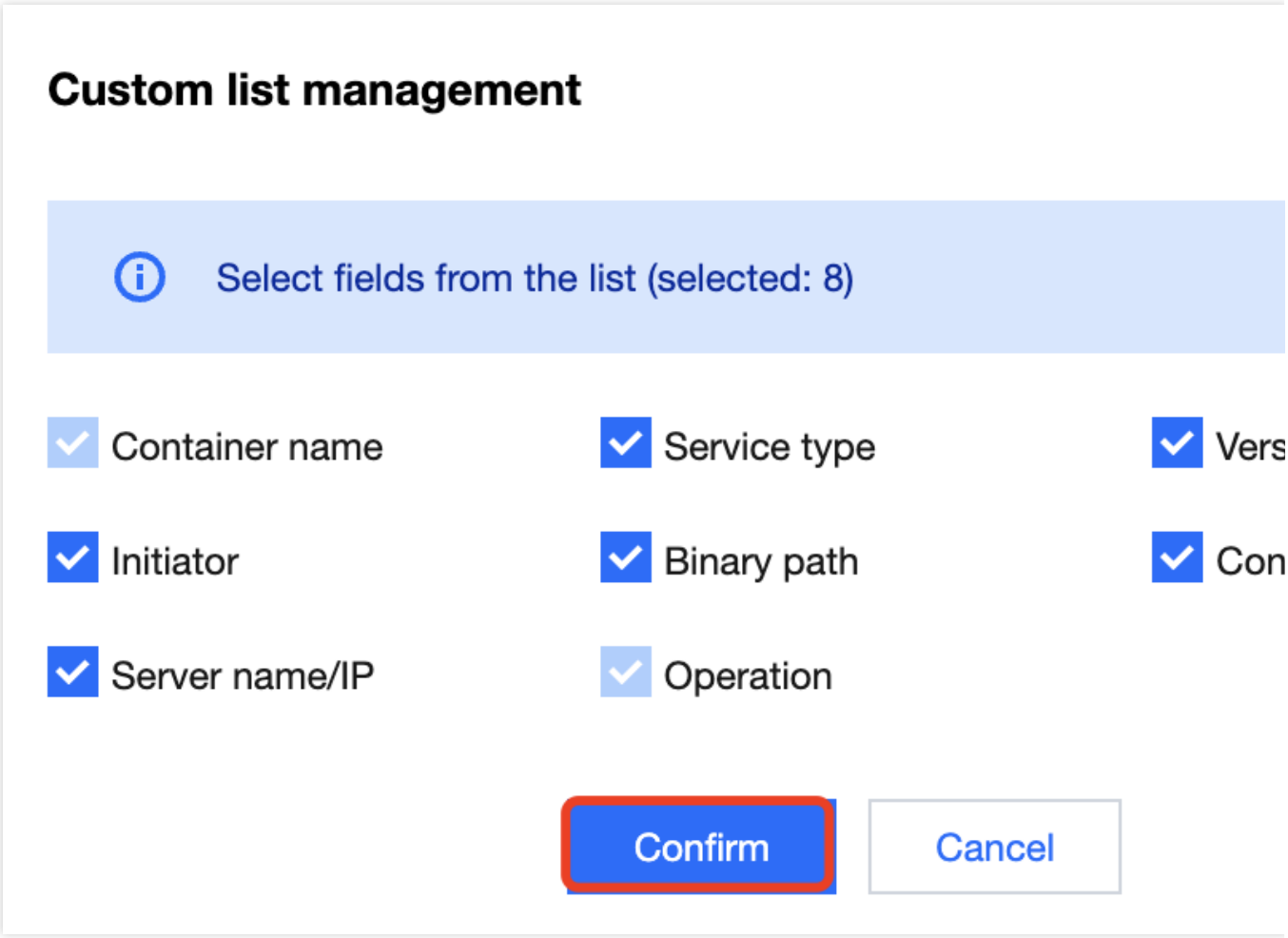


3. On the web service list page, click

to pop up the **Custom List Management** window.

4. In the pop-up window, select the target type and click **OK**.

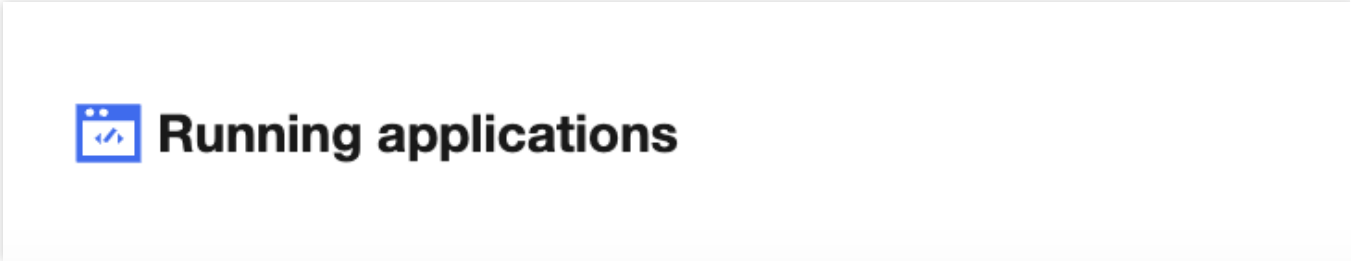
©2013-2022 Tencent Cloud. All rights reserved.



Viewing Running Applications

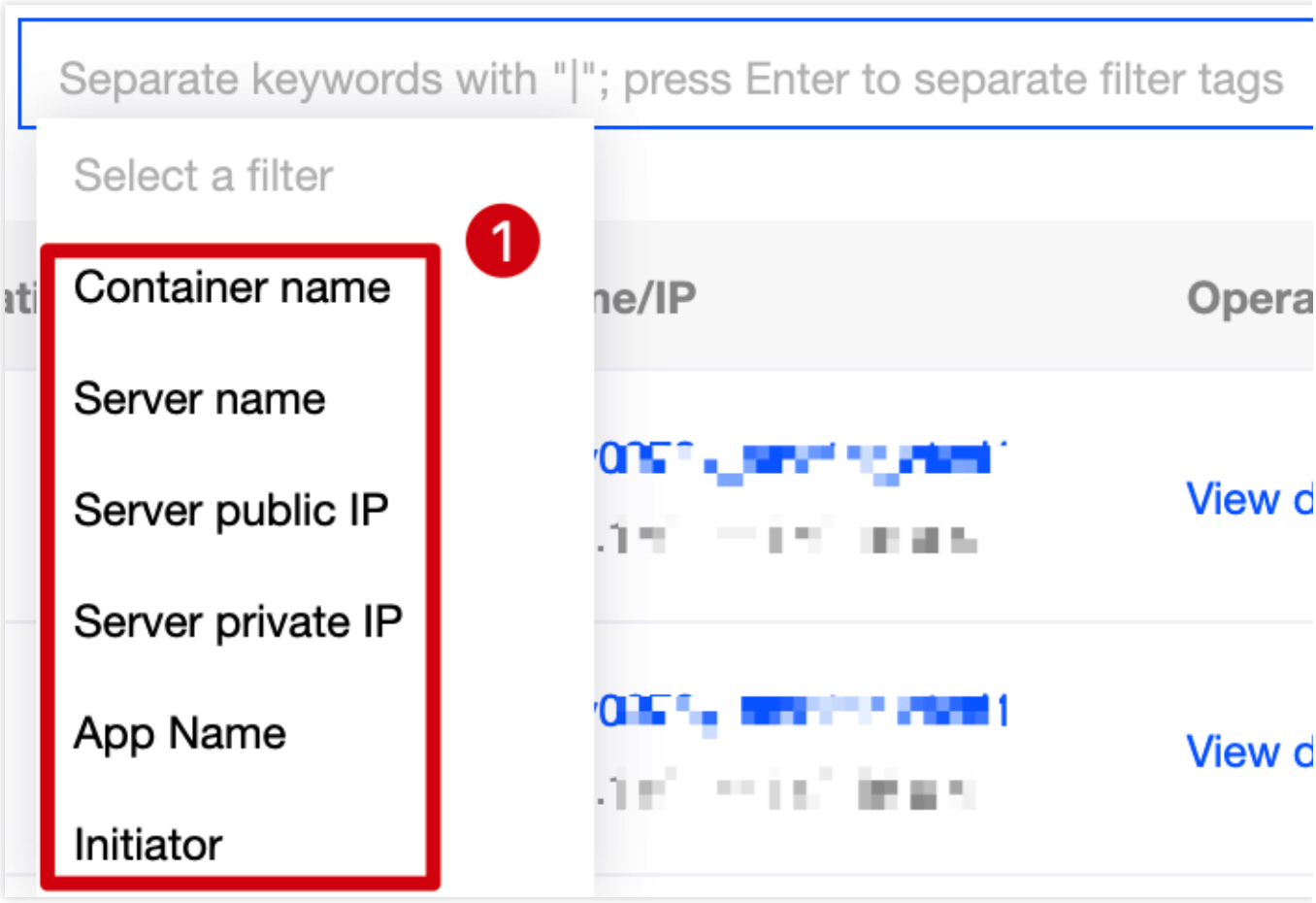
Filtering running applications

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Running applications** to enter the running application list page.



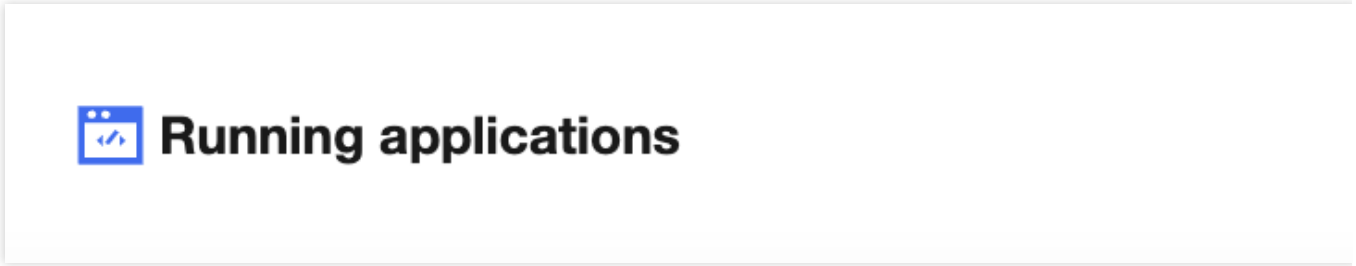
3. On the running application list page, click the search box and search for running applications by keyword such as container name, server IP, or application category.

©2013-2022 Tencent Cloud. All rights reserved.



Viewing the list of running applications

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Running applications** to enter the running application list page.

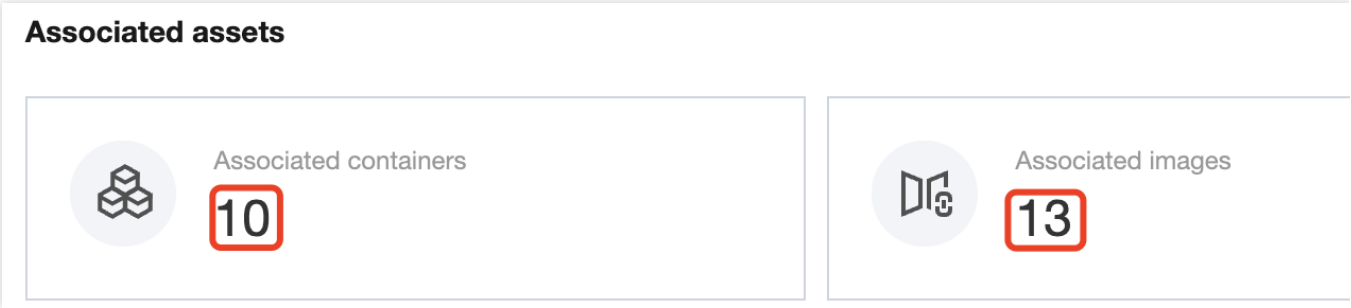


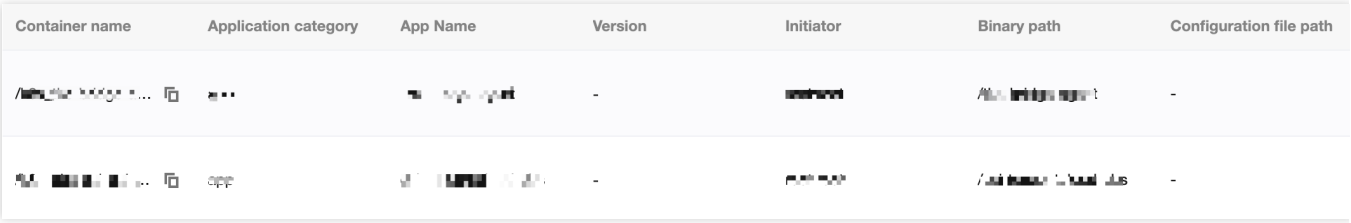
3. On the running application list page, click a **Server IP** to pop up the drawer on the right, which displays the server details, including the basic server information, Docker information, and the numbers of images and containers.

Note:

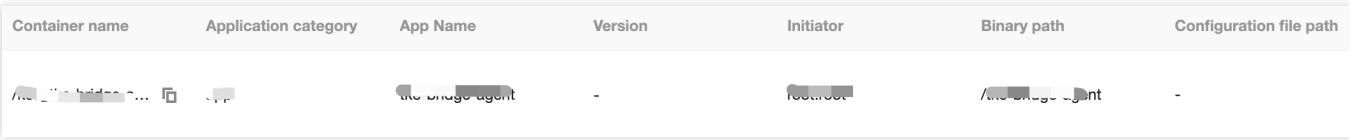
In the drawer, click the number to view the numbers of images and containers on the server.

©2013-2022 Tencent Cloud. All rights reserved.



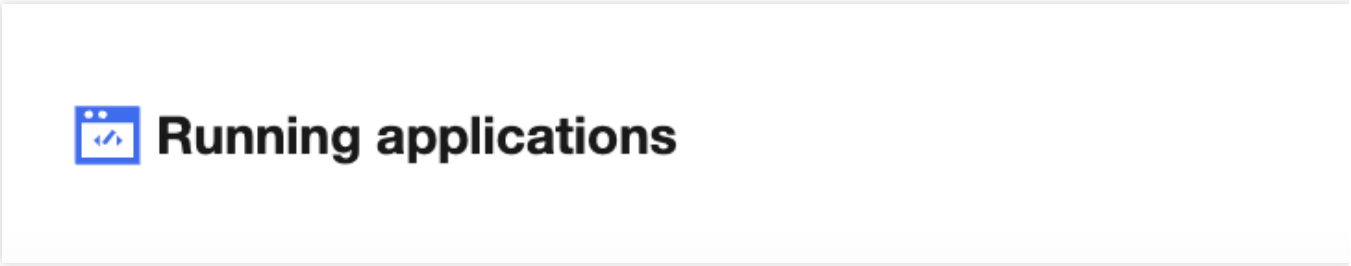


4. On the **Asset Management** page, click **View details** to pop up the window, which displays the list of processes associated with running applications.



Custom list management

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Running applications** to enter the running application list page.

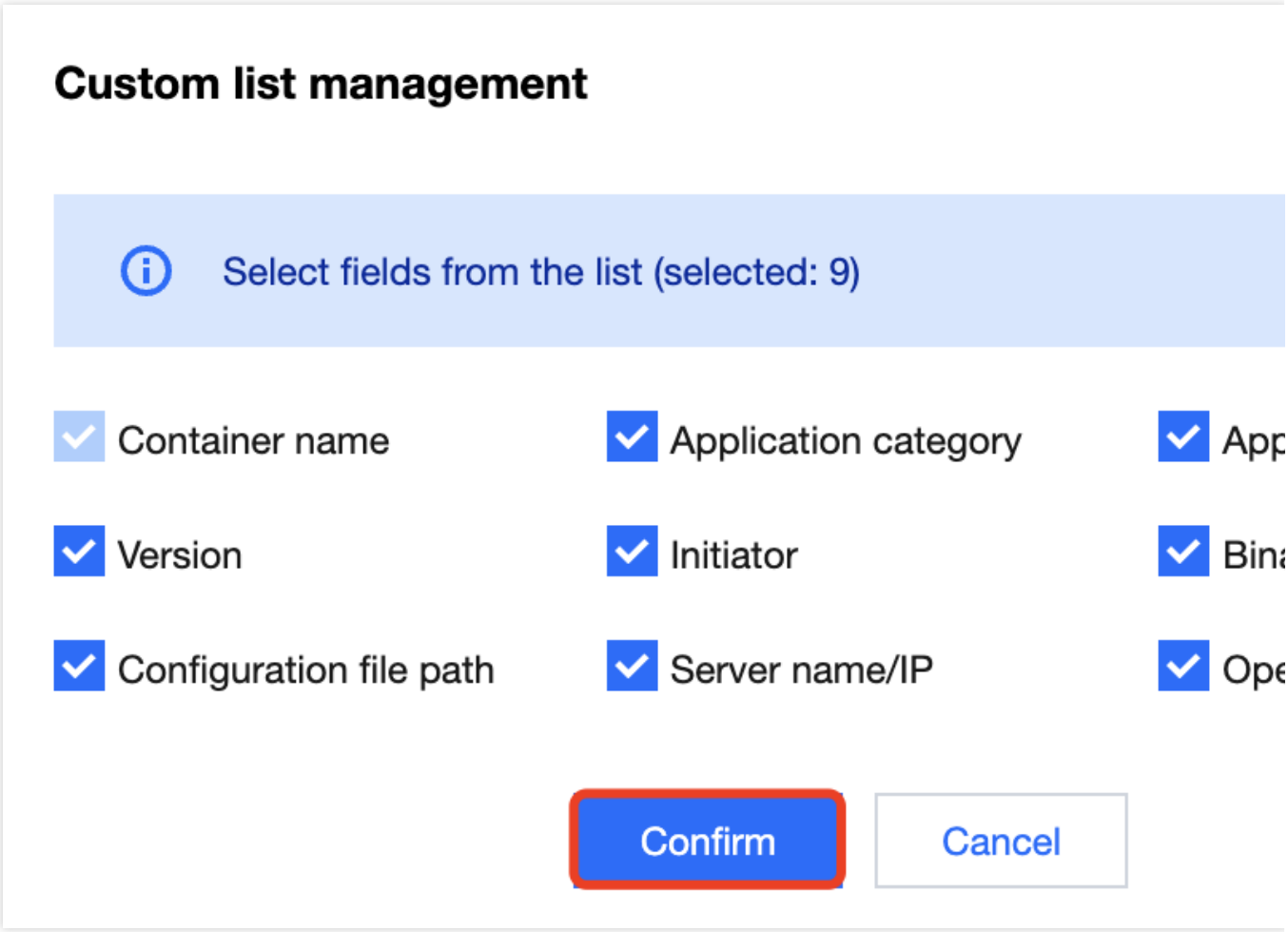


3. On the running application list page, click

to pop up the **Custom List Management** window.

4. In the pop-up window, select the target type and click **OK**.

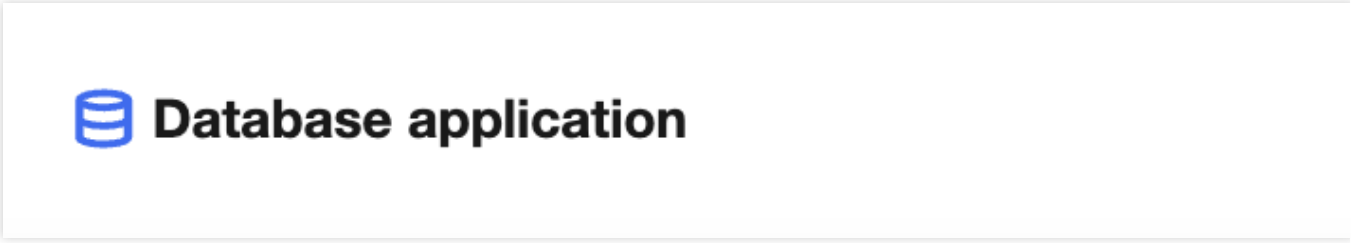
©2013-2022 Tencent Cloud. All rights reserved.



Viewing Database Applications

Filtering database applications

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Database applications** to enter the database application list page.

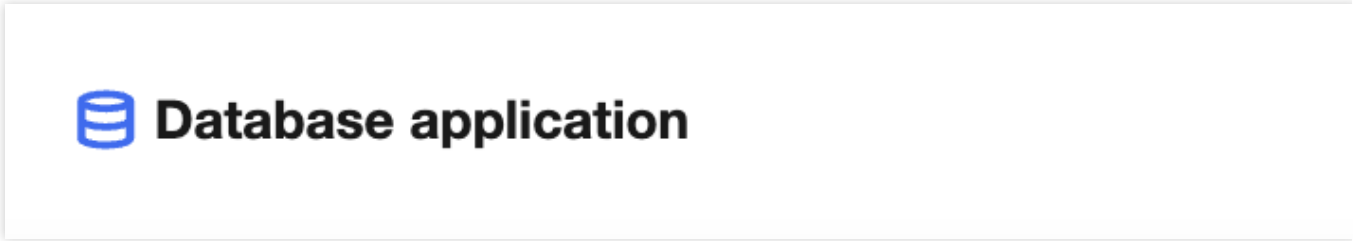


3. On the database application list page, click the search box and search for database applications by keyword such as container name, server IP, or database type.

©2013-2022 Tencent Cloud. All rights reserved.

Viewing the list of database applications

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Database applications** to enter the database application list page.

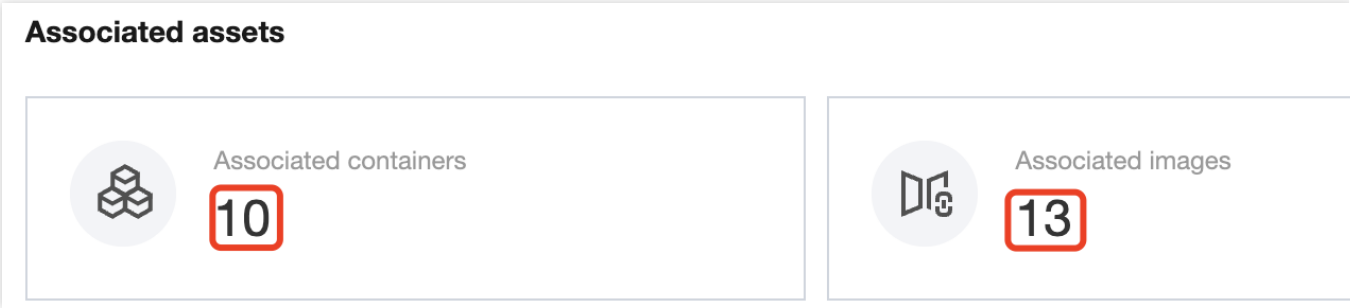


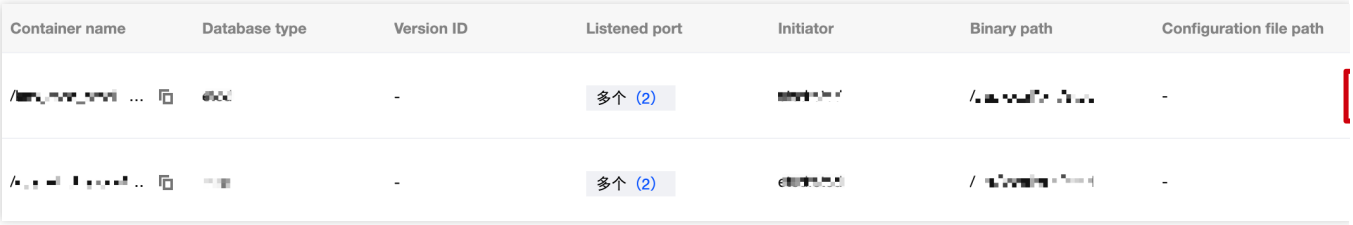
3. On the database application list page, click a **Server IP** to pop up the drawer on the right, which displays the server details, including the basic server information, Docker information, and the numbers of images and containers.

Note:

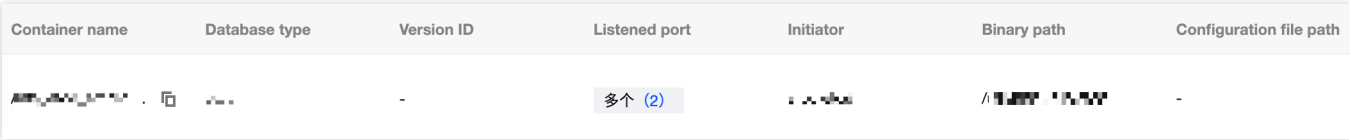
In the drawer, click the number to view the numbers of images and containers on the server.

©2013-2022 Tencent Cloud. All rights reserved.



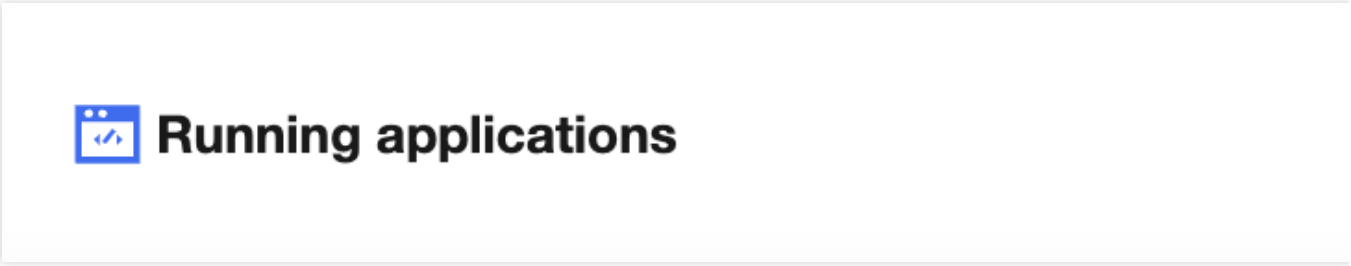


4. On the **Database application** page, click **View details** to pop up the window, which displays the database application details, including the basic information and list of associated processes.



Custom list management

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Running applications** to enter the running application list page.

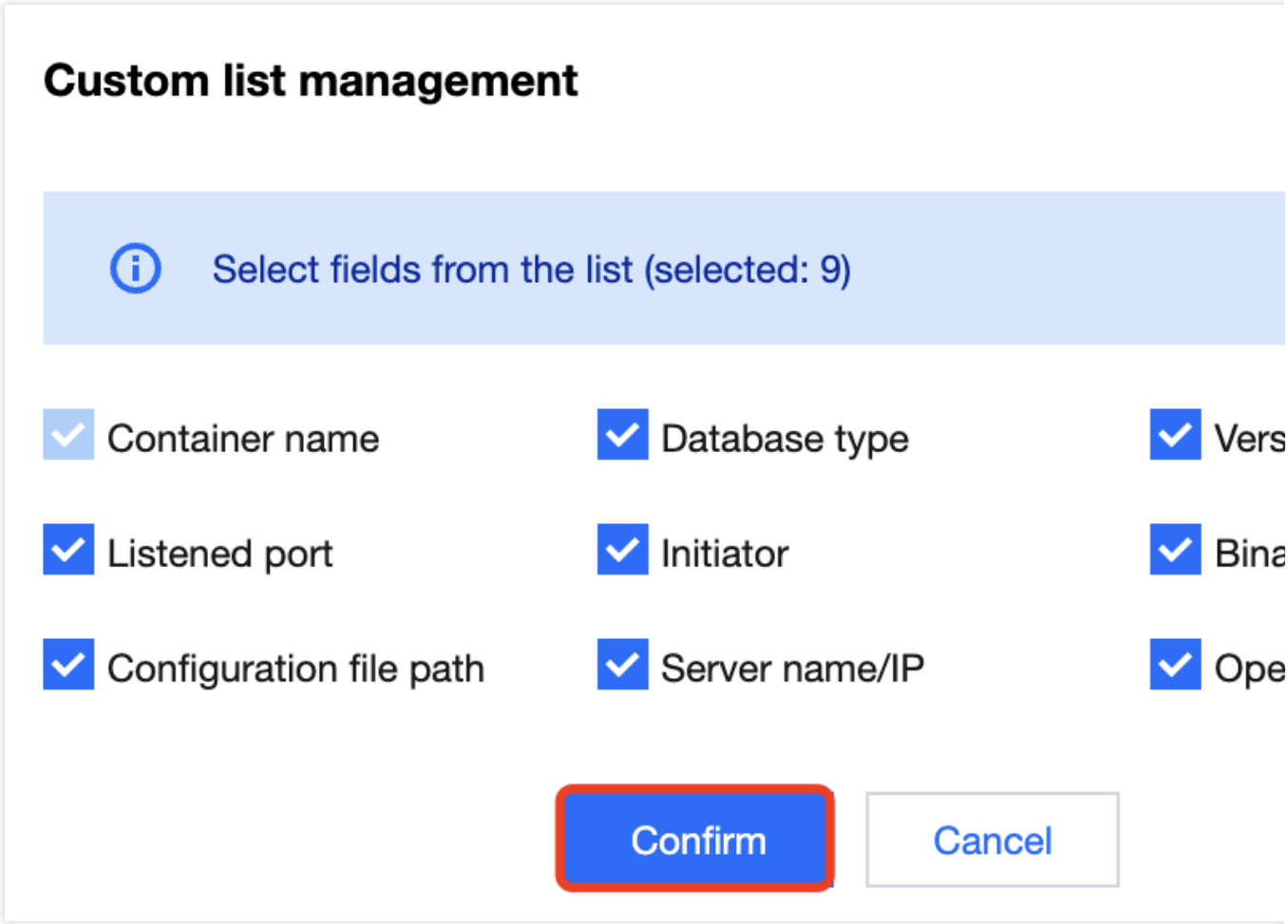


3. On the database application list page, click

to pop up the **Custom List Management** window.

4. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



©2013-2022 Tencent Cloud. All rights reserved.

Vulnerability Detection
Vulnerability Scan

Last updated：2024-01-23 15:44:44

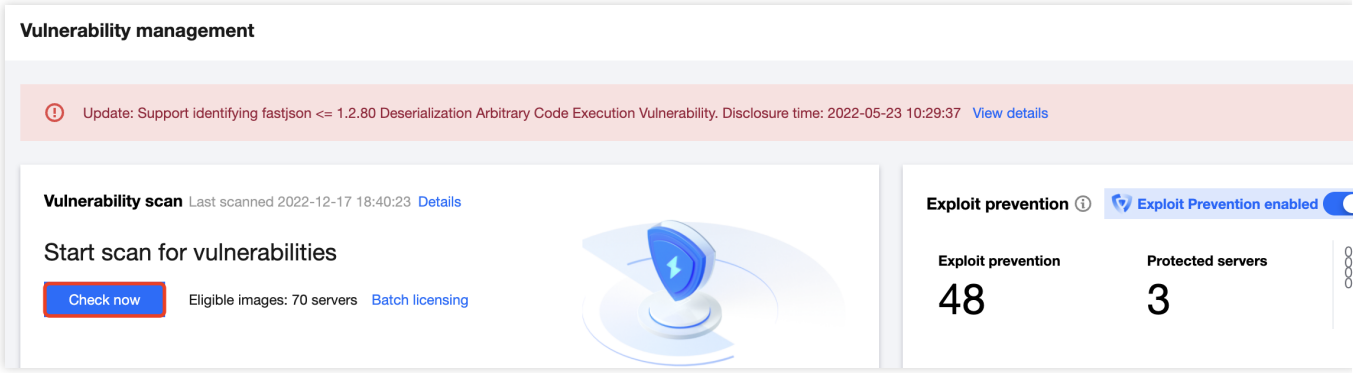
TCSS periodically or promptly scans local and repository images for vulnerabilities. It bases the check on specified images or vulnerability types and allows for ignoring vulnerabilities. It notifies you of vulnerability risks, characteristics, severity, and fix suggestions on visual pages. This helps you better manage vulnerability risks to your images.
This document describes how to use the vulnerability detection feature to manage vulnerability risks to images. The feature supports quickly checking for system vulnerabilities, web application vulnerabilities, and emergency vulnerabilities.

Prerequisites

You have purchased the TCSS Pro Edition.

Vulnerability check

1. Log in to the TCSS console and select **Vulnerability Detection** on the left sidebar.
2. On the **Vulnerability Detection** page, click **Quick check** to check for vulnerabilities and view the result.

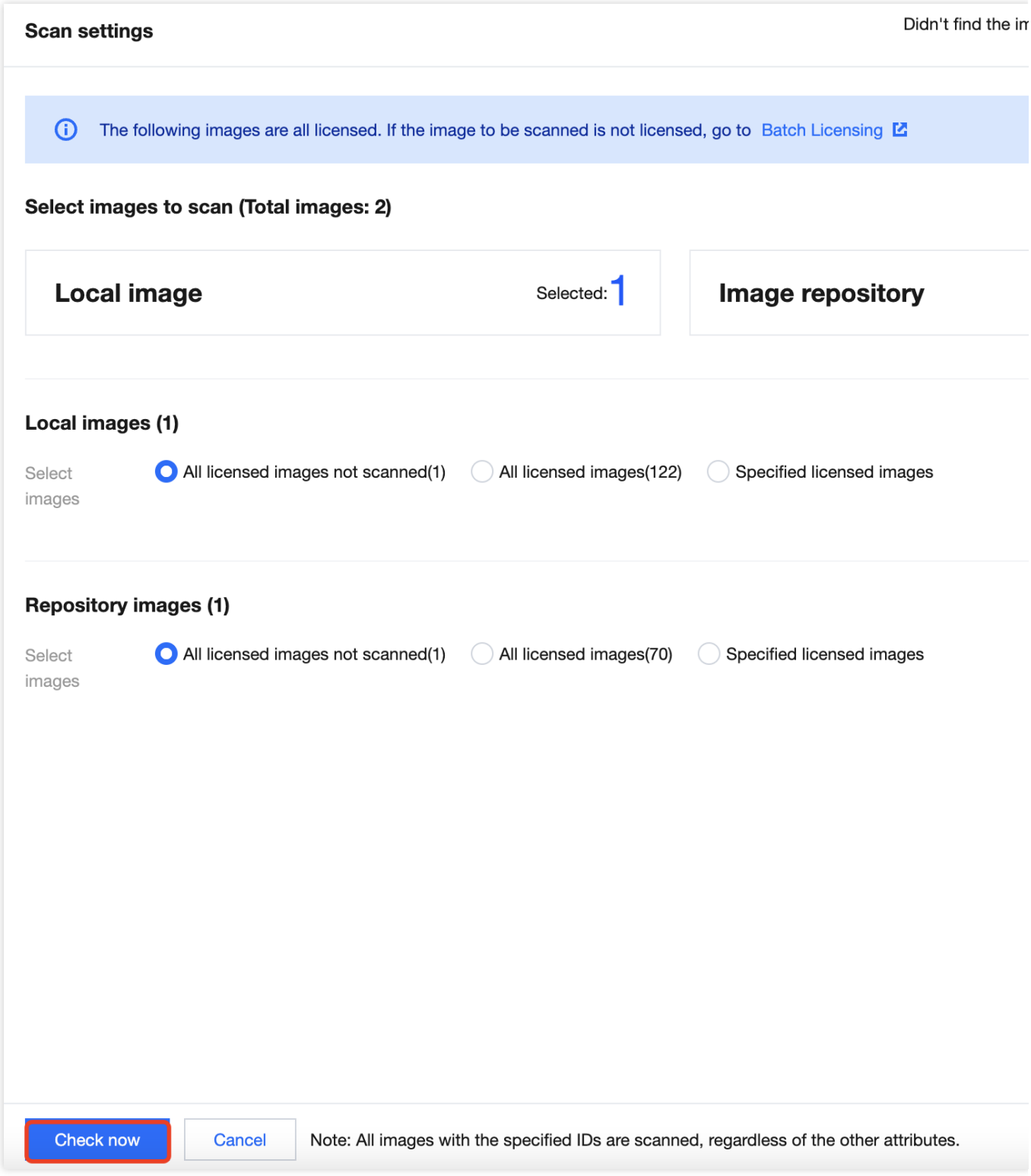


3. In the **Quick check** pop-up window, select the target image and click **Check now**. The result will be visualized as charts on the **Vulnerability Detection** page.

Note:

You need to license the image before the check.
A check generally takes 2–60 minutes, depending on the number of images, image size, and whether it's the first check.

©2013-2022 Tencent Cloud. All rights reserved.

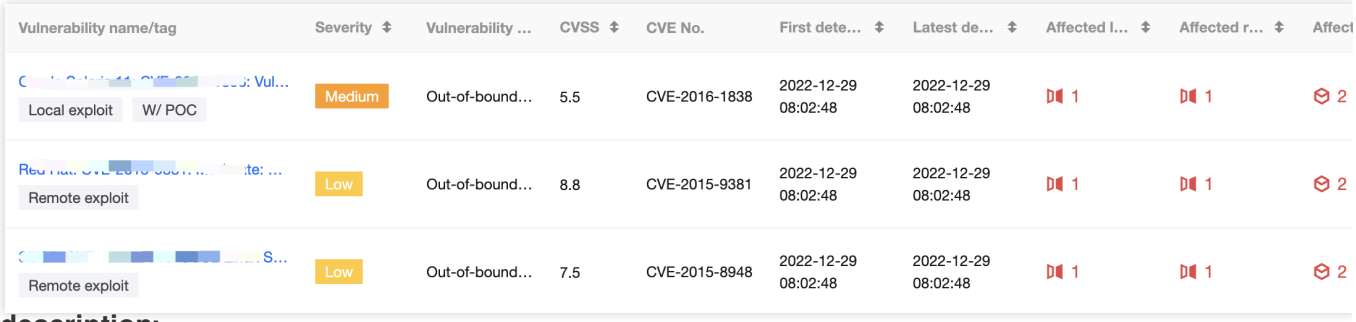


Viewing a vulnerability

1. On the **Vulnerability Detection** page, view the information of the identified system vulnerabilities, web application vulnerabilities, and emergency vulnerabilities in the image. You can also view the affected local images, repository images, running containers, risk statistics, top 5 vulnerabilities, and images affected by critical and high severity vulnerabilities.

©2013-2022 Tencent Cloud. All rights reserved.

Top 5 vulnerabilities: The system ranks the top 5 vulnerabilities based on the CVSS score and dynamic risk level and displays their severity and the numbers of affected images (only those on the latest version) and containers.
Images affected by Critical and High severity vulnerabilities: The system displays the trend of images (on the latest version) with extreme or high-risk vulnerabilities. After the switch to running containers, the system displays the trend of images with extreme or high-risk vulnerabilities and started containers. You can view the trend of the last 7 or 30 days.
2. In the vulnerability list, you can view the vulnerability name, severity, CVE No., first detected time, and latest detected time.



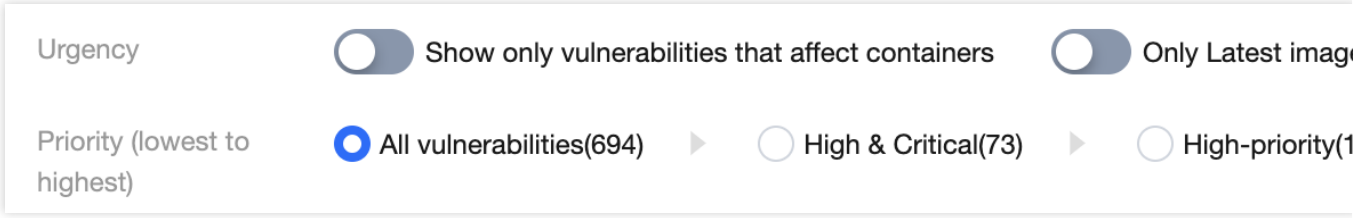
Field description:

Vulnerability name: The publicly known name of the vulnerability.
Severity: **Critical**, **High**, **Medium**, or **Low**, depending on the risk level of the vulnerability.
First detected: The time when the vulnerability is first detected in the image.
Latest detected: The time when the vulnerability is last detected in the image.
Affected local images: Number of local images found to contain the vulnerability, i.e., the number of local images affected by the vulnerability.
Affected repository images: Number of repository images found to contain the vulnerability, i.e., the number of repository images affected by the vulnerability.
Affected containers: Number of running containers found to contain the vulnerability, i.e., the number of running containers affected by the vulnerability.

Note:

The number of affected containers is based on the number of containers started in the affected local images. It is the count at the time of the check and is not subject to the container status change.

3. On the **Vulnerability Detection** page, you can filter vulnerabilities based on their urgency and priority.



Urgency of the impact on the assets

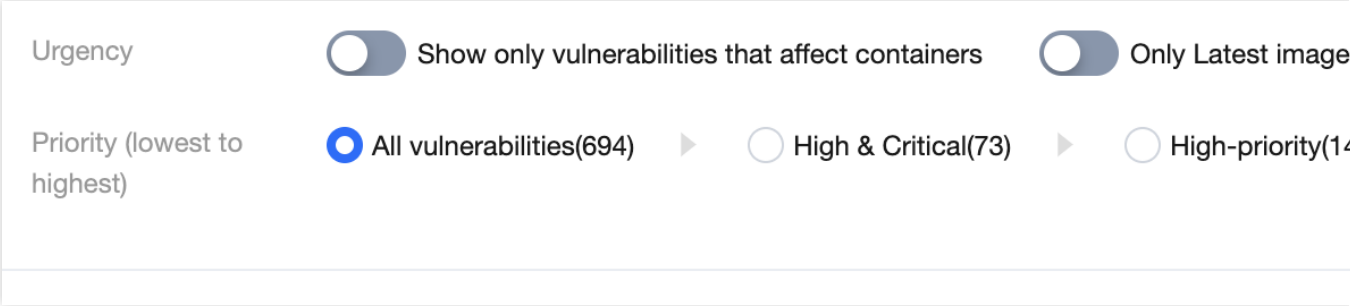
©2013-2022 Tencent Cloud. All rights reserved.

Show only vulnerabilities that affect containers: This option displays the list of vulnerabilities that affect containers.
Only Latest images: This option displays the list of vulnerabilities that affect the latest image tag.
Priority
High & Critical: Vulnerabilities whose severity is extreme or high.
High-priority: High-priority vulnerabilities are vulnerabilities with urgent risks and need to be resolved as soon as possible.
POC/EXP: Vulnerabilities with the risk tag of EXP, POC, or EXP/POC.
Remote EXP: Vulnerabilities with the metric of NetWork (remote exploit) and with EXP.

4. Click **More filters** to search for vulnerabilities by severity, fix possibility, risk tag, CVE No., affected image ID, affected image name, affected container ID, affected container name, affected component version, or affected component name.

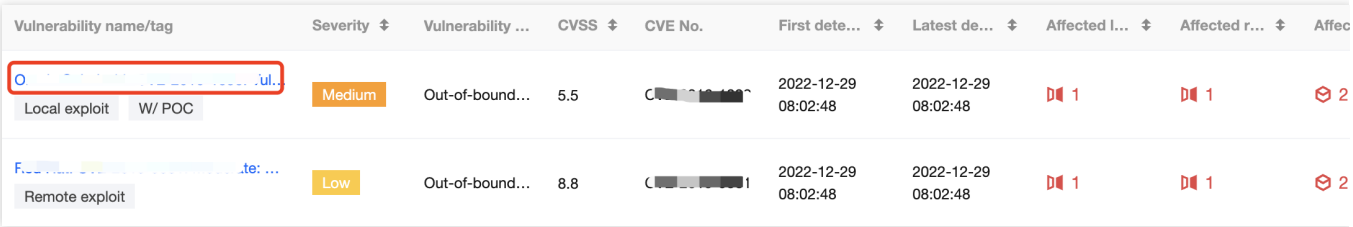
Note:

Vulnerabilities found based on the affected image ID, affected image name, affected container ID, and affected container name are visualized and don't affect the number of affected local images, repository images, or containers.



Viewing vulnerability details

1. At the bottom of the **Vulnerability Detection** page, view the vulnerability overview.
2. On the **Vulnerability Detection** page, click the **Vulnerability name** or **View details** in the **Operation** column of the vulnerability.



3. On the **Vulnerability details** tab, view the vulnerability details, affected local images, affected repository images, and affected containers.

©2013-2022 Tencent Cloud. All rights reserved.

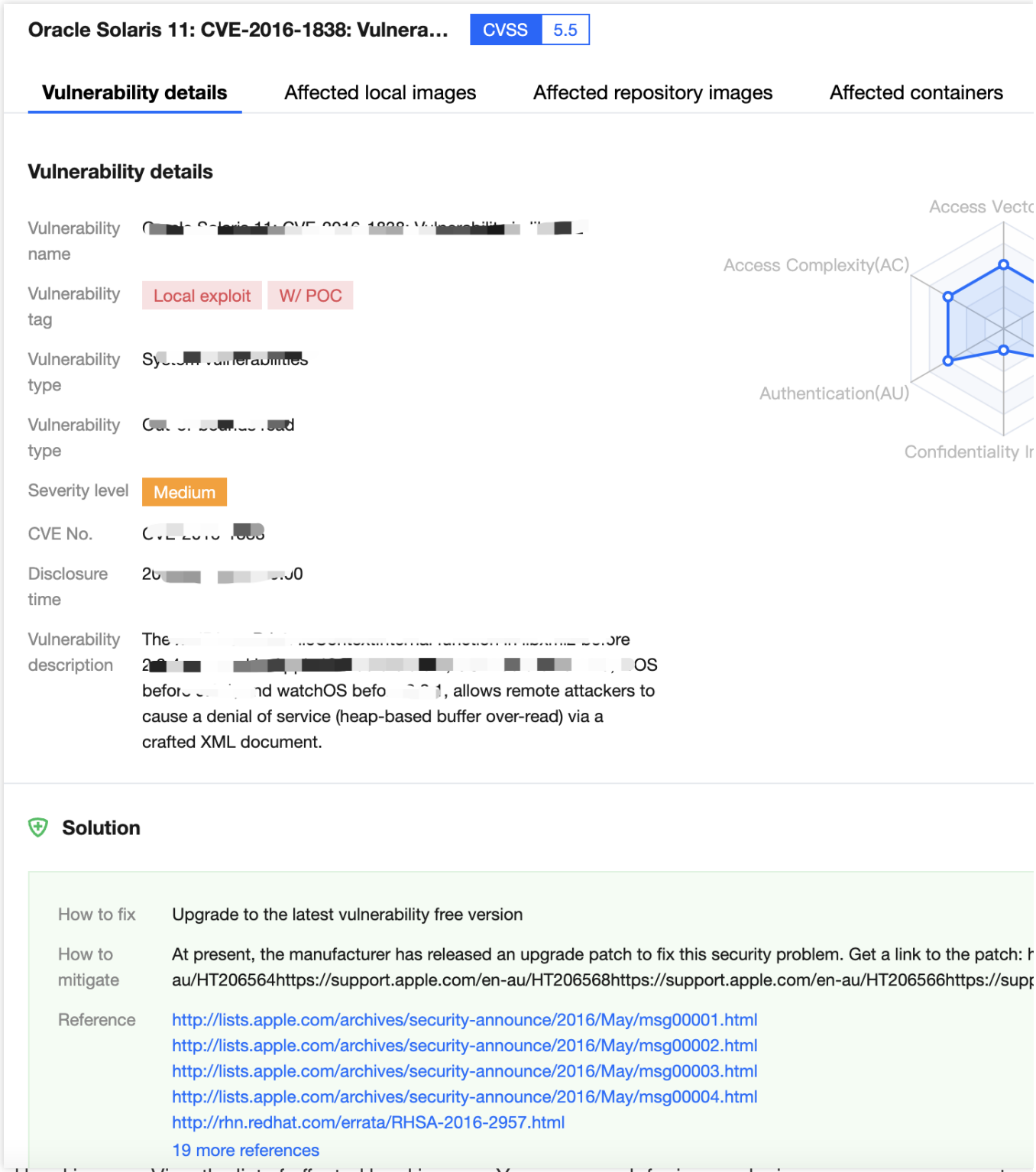
Vulnerability details: Include the description, type, severity level, disclosure time, solution, affected components, and characteristics of the vulnerability.

Note:

Affected components and their versions come from the **Vendor Product** information of the vulnerability CPE in the National Vulnerability Database (NVD) and don't necessarily mean that the components exist in the checked images. The name of an affected component may differ from the actual name in the affected image.

To view the actually affected components in the image, select the **Affected local images** or **Affected repository images** tab and click **Expand** on the left of the image or click **View components** in the **Operation** column.

©2013-2022 Tencent Cloud. All rights reserved.



Affected local images: View the list of affected local images. You can search for images by image name, component name, or IP and view the numbers of associated servers and associated containers of the images.

Affected repository images: View the list of affected repository images. You can search for images by repository name/address.

Affected containers: View the list of affected containers. You can search for containers by container name/ID.

Note:

©2013-2022 Tencent Cloud. All rights reserved.

When the container status changes, the data in the list of affected containers may differ from the number of affected containers in the vulnerability list.

©2013-2022 Tencent Cloud. All rights reserved.

Exploit Prevention

Last updated：2024-01-23 15:44:44

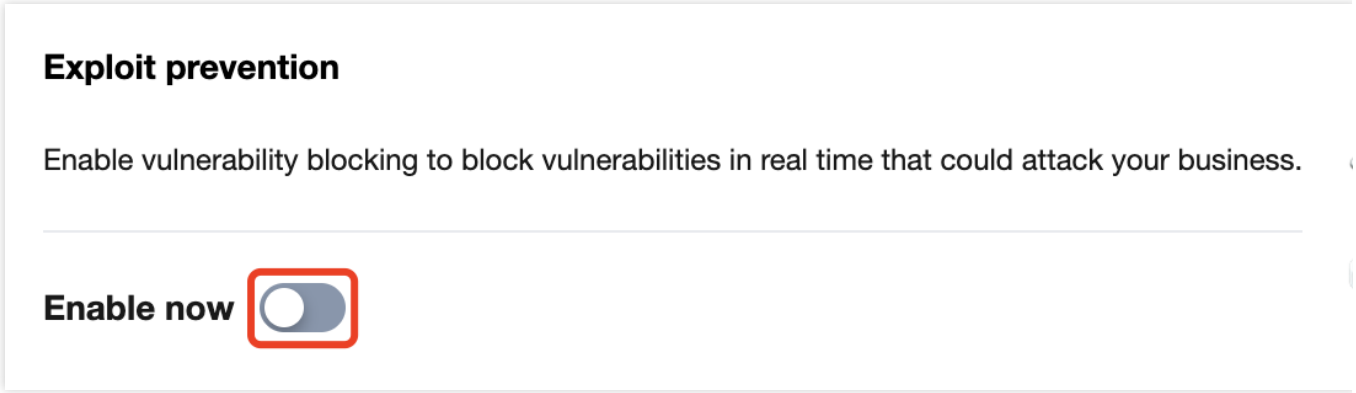
Exploit prevention is a virtual patch-based system developed by the Tencent Cloud security team to defend against frequent 0-day and N-day vulnerabilities. It integrates Tencent's vulnerability mining and real-time high-risk vulnerability alerting technologies to capture and analyze vulnerabilities, generate virtual patches based on Tencent's expertise, and automatically make the patches effective in CVM instances. This helps effectively block hacker attacks and gain more time for vulnerability fix.

Enabling exploit prevention

Enable the exploit prevention feature to block vulnerability exploitation in real time and protect your business from attacks.

1. Log in to the TCSS console and select **Vulnerability Detection** on the left sidebar.
1. On the **Vulnerability Detection** page, toggle on the **Enable now** switch

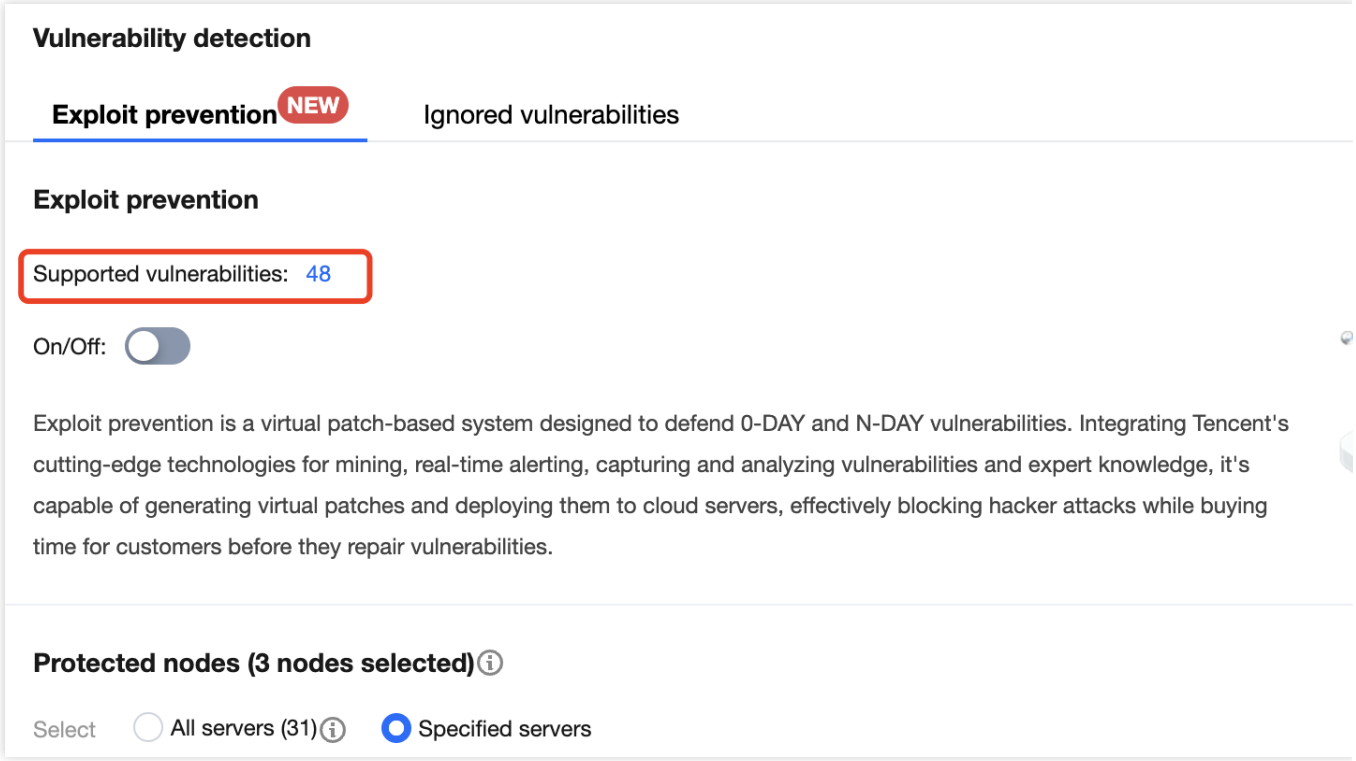
. The drawer on the right will display the configuration page for exploit prevention.



2. On the **Vulnerability Detection** page, click **Vulnerability detection** in the top-right corner.

©2013-2022 Tencent Cloud. All rights reserved.

3. On the **Vulnerability detection** page, click the number of prevented vulnerabilities to view the details.

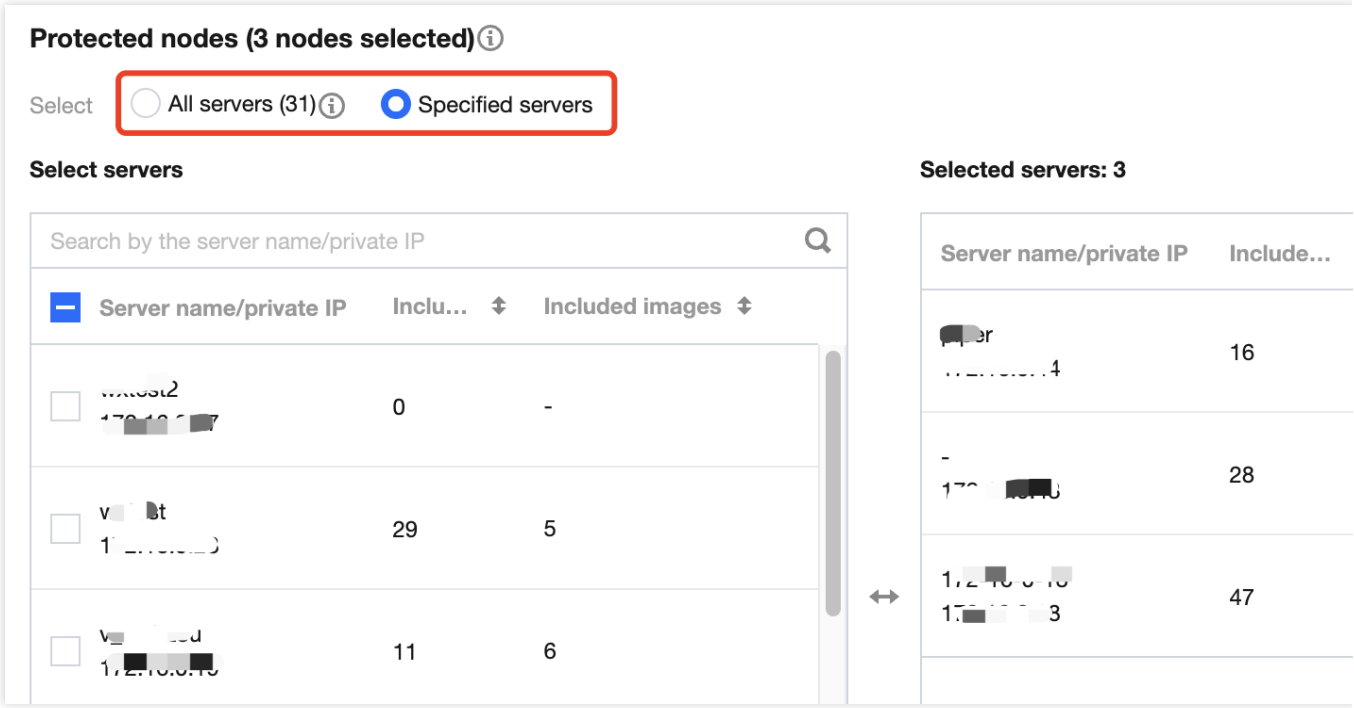


4. On the **Vulnerability detection** page, select **Protected nodes**, click **Implement now** at the bottom of the drawer, and wait for the policy to be distributed. Then, the selected nodes are protected against container vulnerability exploitation.

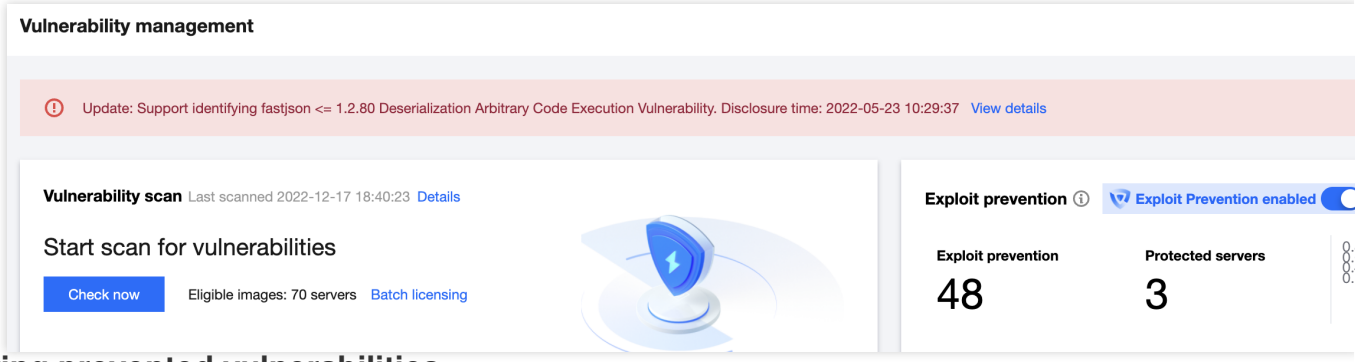
Note:

If you select **All servers** for **Protected nodes**, exploit prevention will be automatically enabled for newly added servers.

©2013-2022 Tencent Cloud. All rights reserved.

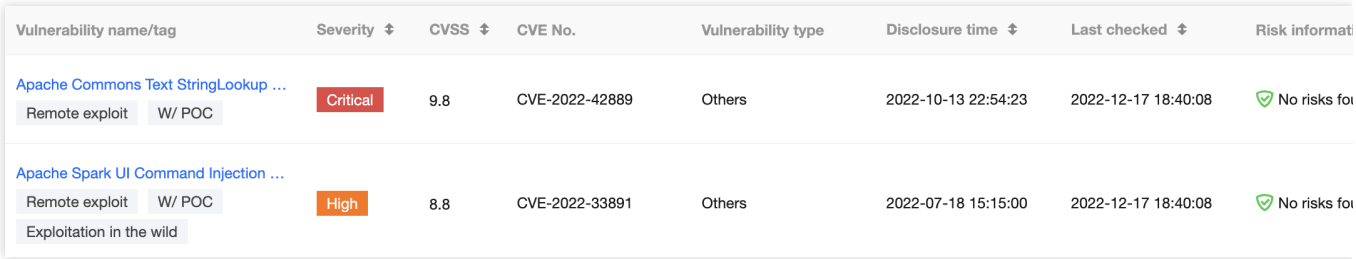


5. On the **Vulnerability Detection** page, click **Protection settings** to view or adjust the status of the exploit prevention switch, adjust the scope of protected nodes, and view the status of the prevention plugin on the node.



Viewing prevented vulnerabilities

1. After exploit prevention is enabled, you can filter vulnerabilities in the **Defending** status on the emergency vulnerabilities, system vulnerabilities, and application vulnerabilities pages to view the details.



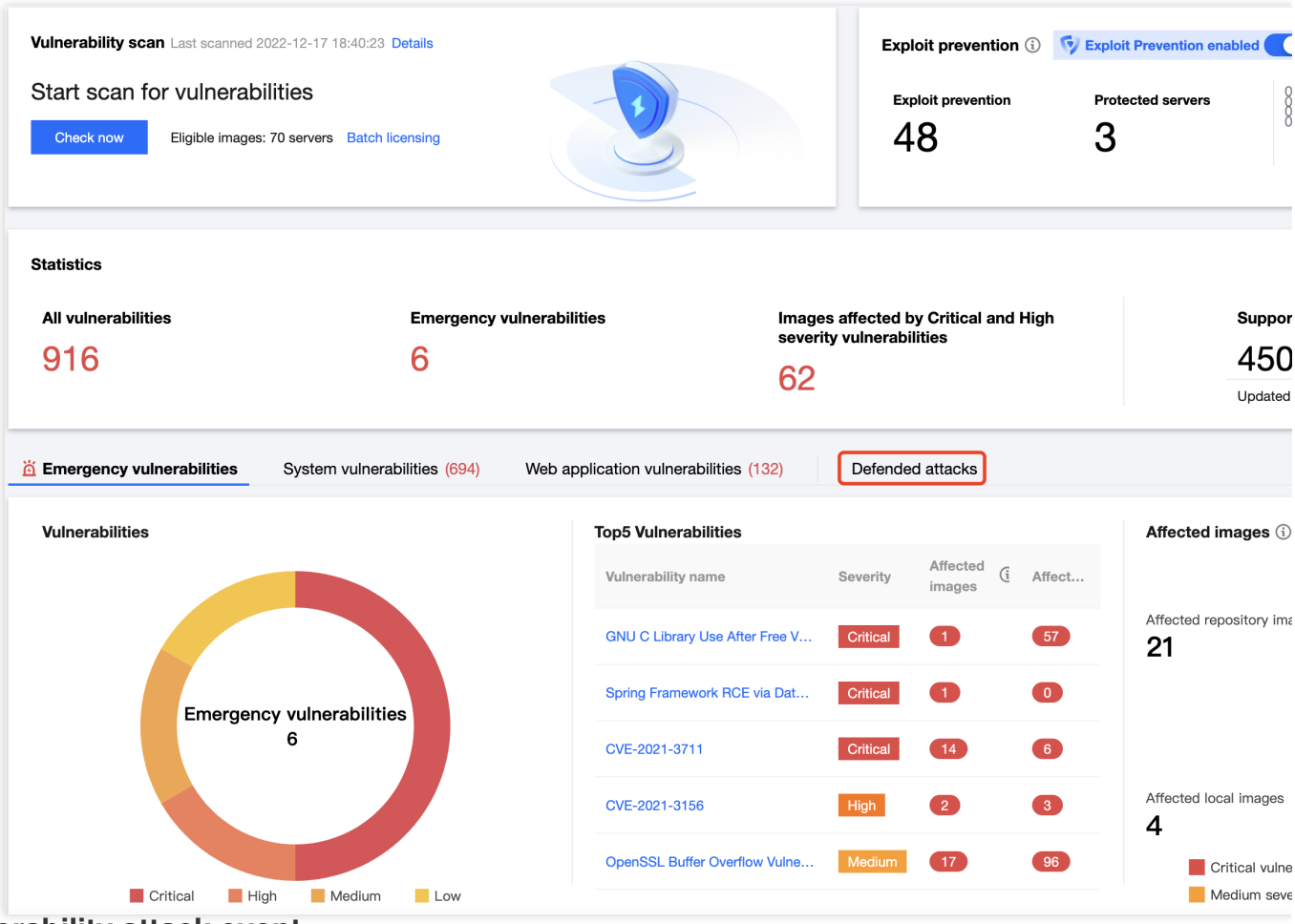
2. Hover over the **Defending** icon to quickly view the numbers of protected nodes and defended attacks. In addition, you can click **Protection settings** to enter the prevention settings drawer and click **Prevented attacks** to enter the

©2013-2022 Tencent Cloud. All rights reserved.

vulnerability attack event page.

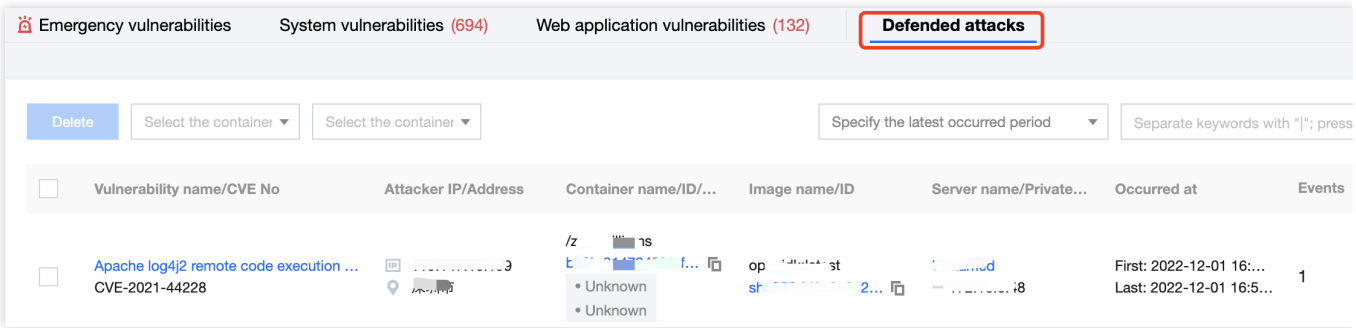
Note:

If exploit prevention is not enabled, you can filter vulnerabilities in the **Undefended** status on the emergency vulnerabilities, system vulnerabilities, and application vulnerabilities pages to view the details.



Vulnerability attack event

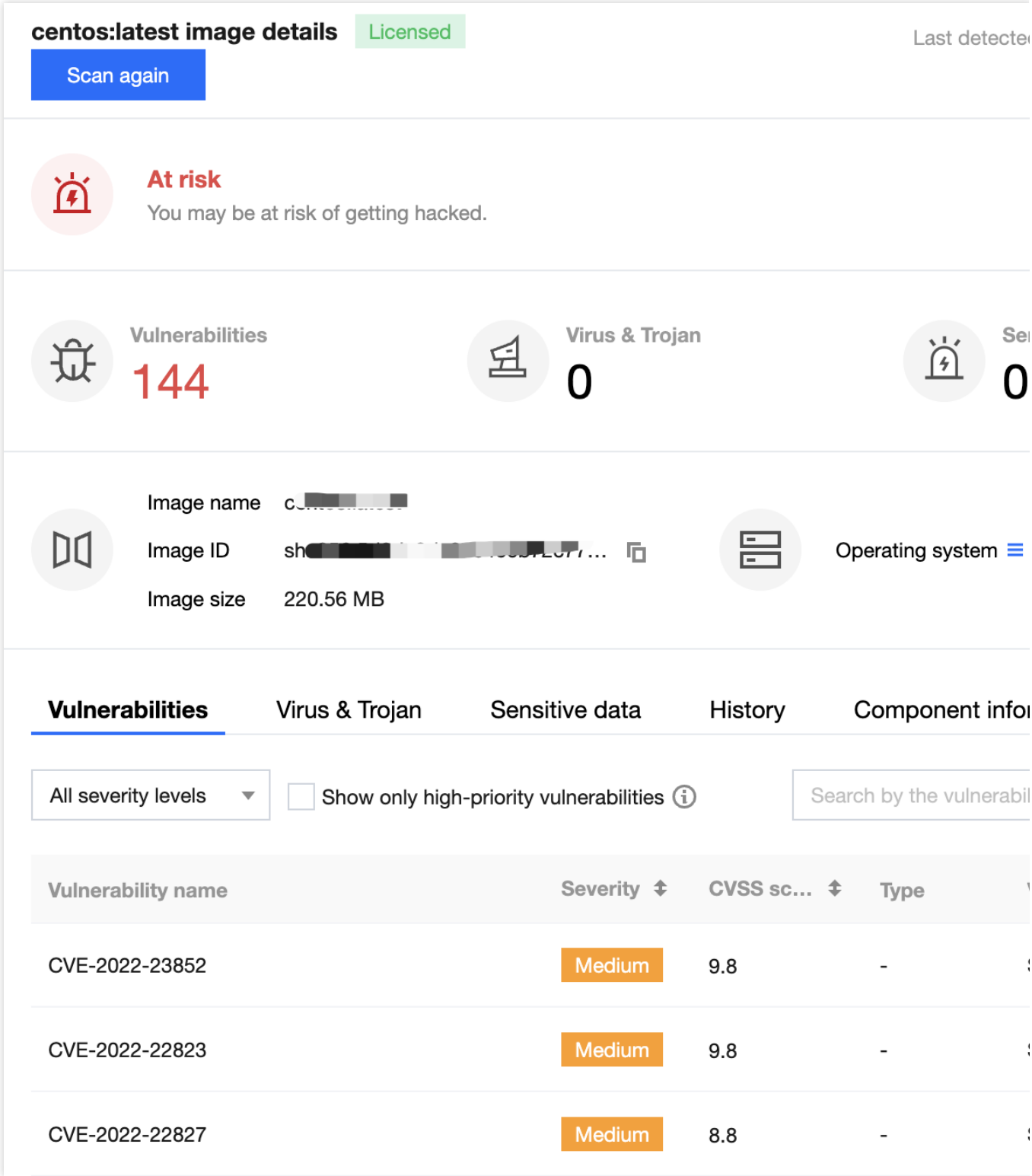
1. On the **Vulnerability Detection** page, click **Vulnerability attack event** to view attacks that have been successfully defended against.



2. Click **View details** to view the attack IP, attack packet, and prevention plugin information. You can also click **Image details** to view the vulnerability details. We recommend you block attack IPs and fix vulnerabilities in business

©2013-2022 Tencent Cloud. All rights reserved.

images.



©2013-2022 Tencent Cloud. All rights reserved.

Image Risk Management Overview

Last updated：2024-01-23 15:44:44

Image security quickly checks local images and repository images for vulnerabilities, trojans, viruses, sensitive data, and more.

Image security risks

An image is a static representation of a container, and its security determines the security of container runtime.
Image security risks originate from the creation process, acquisition source, and acquisition means. An image may be risky in the following cases:
The image contains vulnerabilities or is embedded with malicious scripts, which means that the generated container may contain vulnerabilities or be maliciously exploited.
Note:
For example, an attacker constructs a special compressed image file and triggers the vulnerability during compilation to get the permission to execute arbitrary code.
If `USER` is not specified in the image, the container created from the image will be run by the root user by default. When the container is attacked, the access of the root user to the host may be compromised.
Data may be leaked if the image file storing fixed passwords or other sensitive data is published.
The attack surface will be expanded if unnecessary applications such as SSH and Telnet are added when the image is written.

Repository image security risks

As a tool to set up private image repositories, an image repository is mainly subject to security risks from itself and transfer security risks during image pull.
Repository security: If an image repository, especially a private one, is controlled by a malicious attacker, all its images will be at risk.
Note:
For example, if port 2357 is opened due to improper configuration in a private image repository, the repository will be exposed to the public network, which means that attackers can directly access it and tamper with its content, causing security risks.
Image pull security: Image security also concerns the container image integrity from the image repository to the user end.

©2013-2022 Tencent Cloud. All rights reserved.

Note:

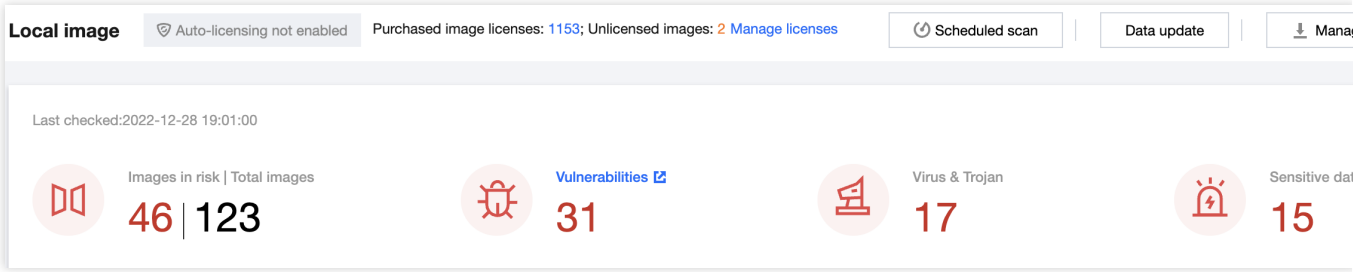
For example, if a user pulls an image in plaintext, the interaction with the image repository will be vulnerable to man-in-the-middle attacks. In this case, the pulled image will be tampered with during transfer, or a malicious image with the same name will be released, causing security risks to the image repository and user.

©2013-2022 Tencent Cloud. All rights reserved.

Local Image

Last updated：2024-01-23 15:44:44

This document describes the local image feature and how to enable data scan and view the local image list.

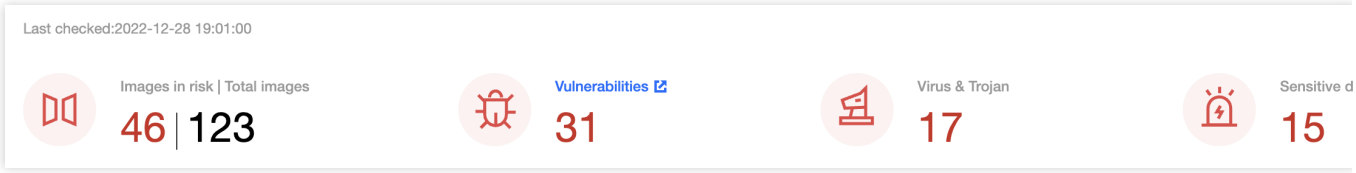


Enabling Data Scan

The data scan module displays the number of images at risk, total number of images, and the numbers of vulnerabilities, viruses, trojans, and sensitive data pieces in the images after the last scan.

Enabling quick scan

1. Log in to the TCSS console and click **Image Risk Control** > **Local Images** on the left sidebar.
2. On the **Local Images** page, click **Scan now** on the right to scan again and get the latest image data or risk information.



3. On the **Scanning settings** page, select the **Risk category** and **Images** as needed.
Risk category: **Vulnerabilities** or **Sensitive data**.
Images: **All images** or **Specified images**. Click

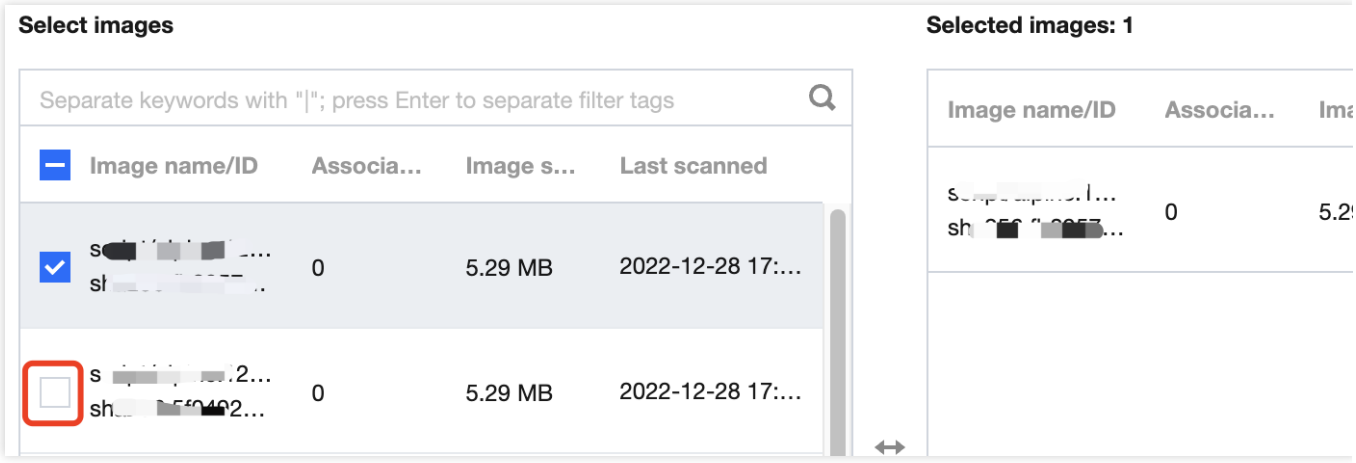
or

to select or delete the target specified image.

©2013-2022 Tencent Cloud. All rights reserved.

Note:

You can press Shift to select multiple ones.



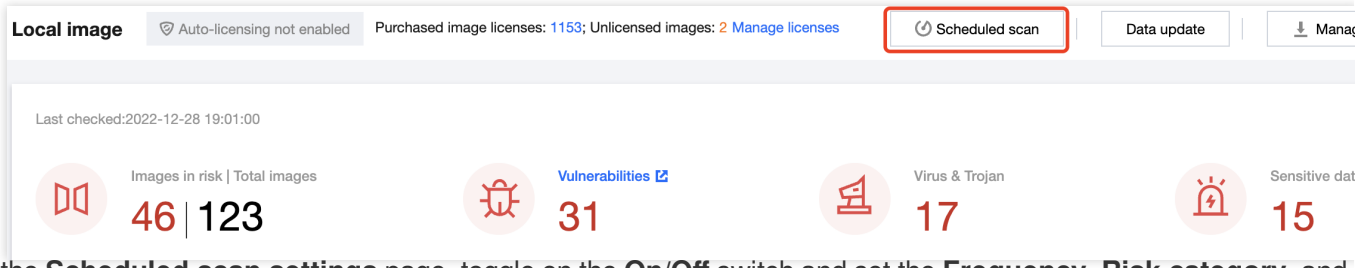
4. After selecting the target content, click **Scan now**.

Note:

After the scan starts, all images with the same ID as the selected image will be scanned at the same time.

Enabling scheduled scan

1. On the **Local Images** page, click **Scheduled scan settings** on the right to specify whether to enable the scheduled scan feature.



2. On the **Scheduled scan settings** page, toggle on the **On/Off** switch and set the **Frequency**, **Risk category**, and **Images** as needed.

Frequency: It can be every day, every 7 days, every 15 days, every 30 days, or a specified time range.

Risk category: Click

to select **Vulnerabilities**, **Sensitive data**, or **Virus & Trojan** as needed.

Images: **All images** or **Specified images**. Click

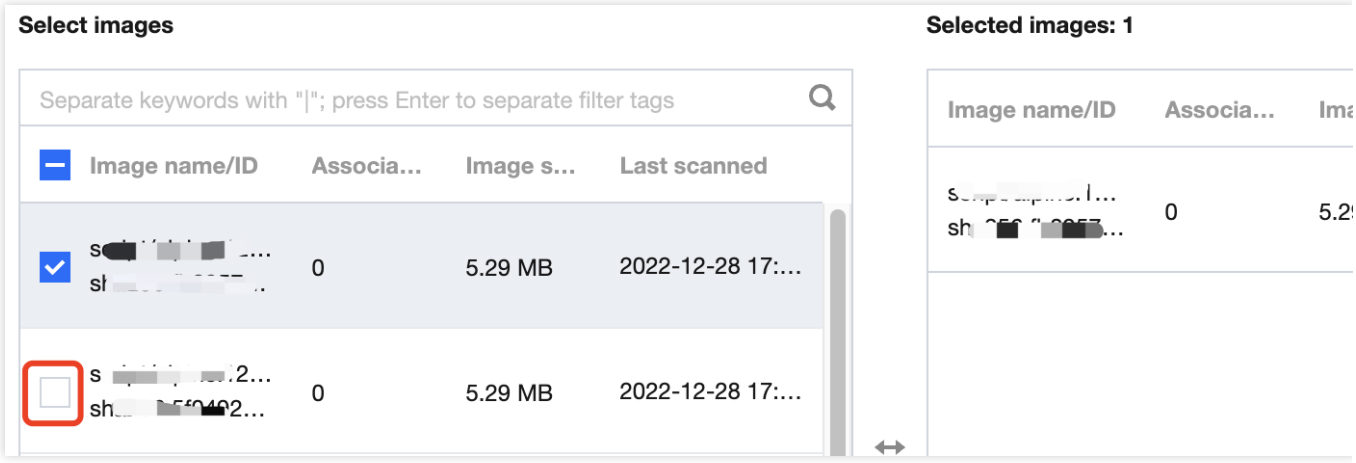
or

©2013-2022 Tencent Cloud. All rights reserved.

to select or delete the target specified image.

Note:

You can press Shift to select multiple ones.



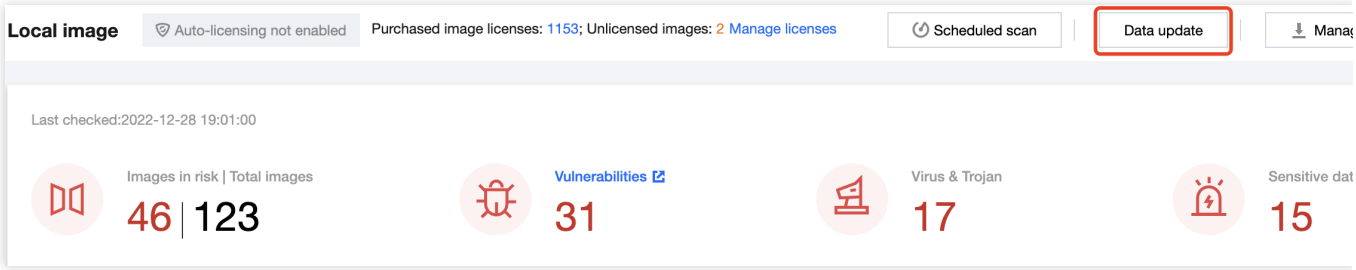
3. After selecting the target content, click **Set** or **Cancel**.

Enabling data update

On the **Local Images** page, click **Data update** > **OK** on the right to immediately update the security information of all images.

Note:

It takes up to one to three minutes.

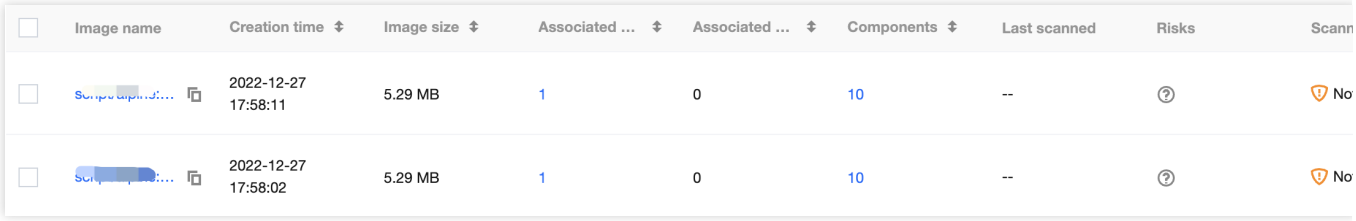


Viewing the List of Local Images

Image licensing event

1. On the **Local Images** page, click **License**.

©2013-2022 Tencent Cloud. All rights reserved.



2. In the pop-up window, click **OK**.

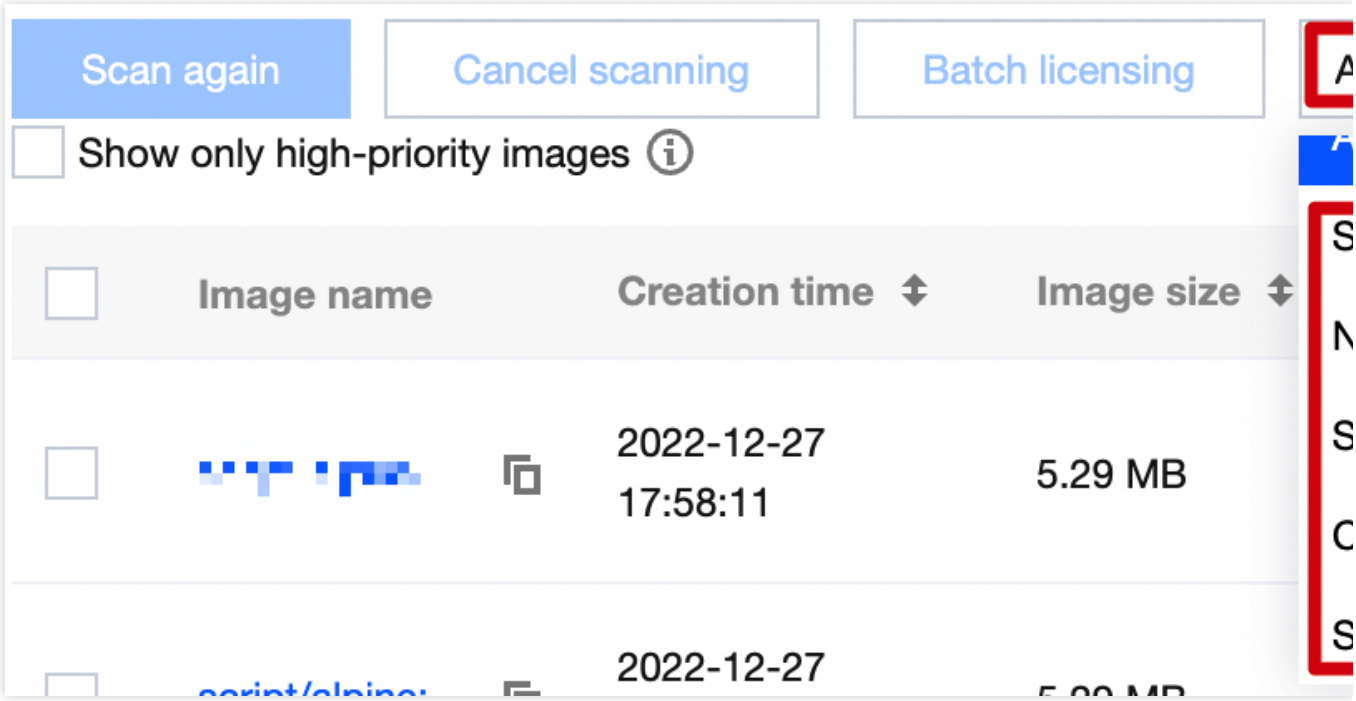
Note:

A license will be assigned to this image.

Filtering images

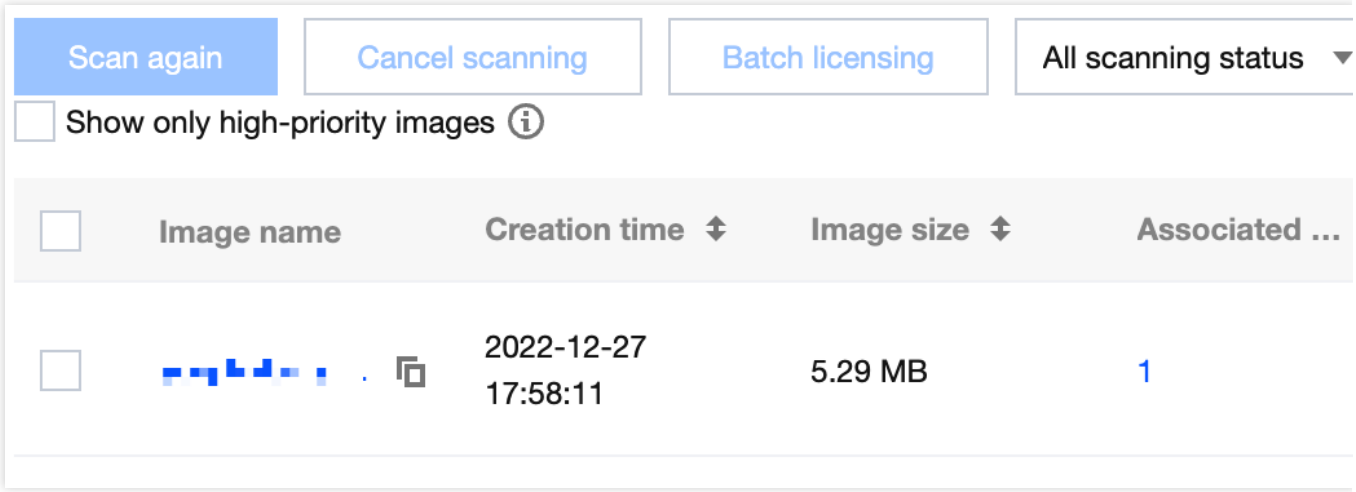
On the **Local Images** page, filter images as follows:

Click the scanning status drop-down list to filter images by scanning status.



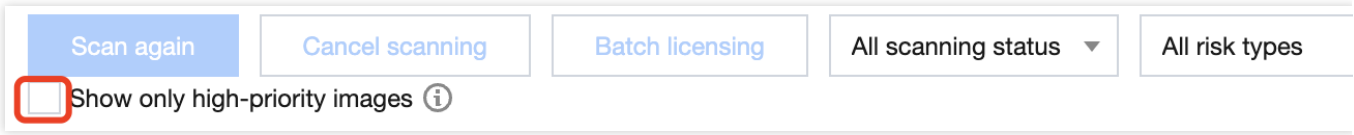
Click the security status drop-down list to filter images by security status.

©2013-2022 Tencent Cloud. All rights reserved.

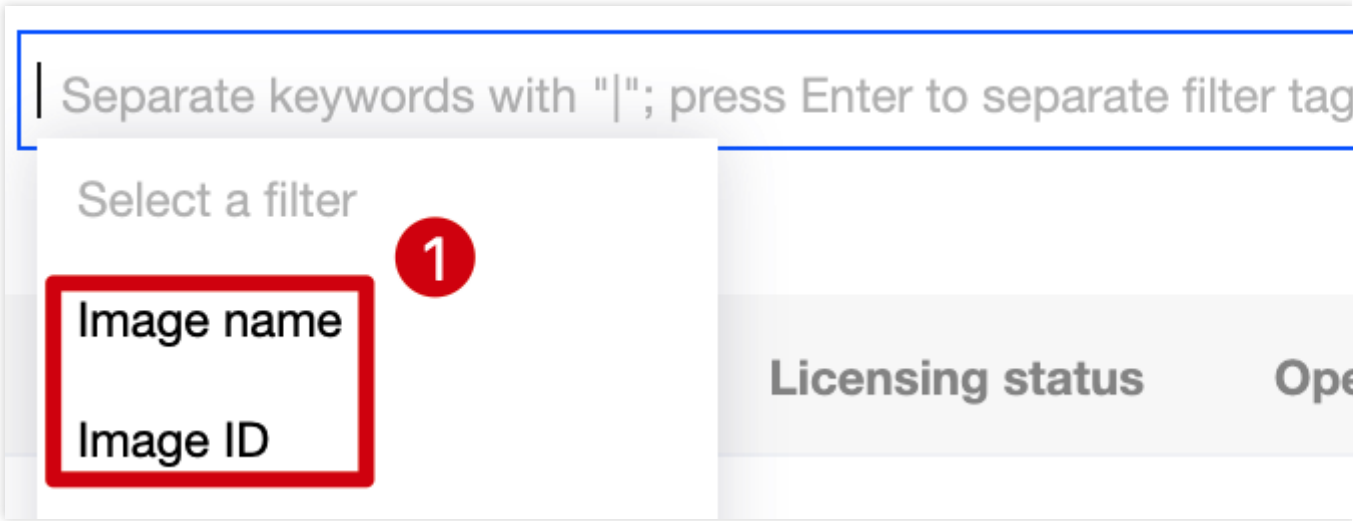


Click

to select **Show only high-priority images** and display the high-priority images based on the risk urgency.



Click the search box and search for images by keyword such as image name or image ID.



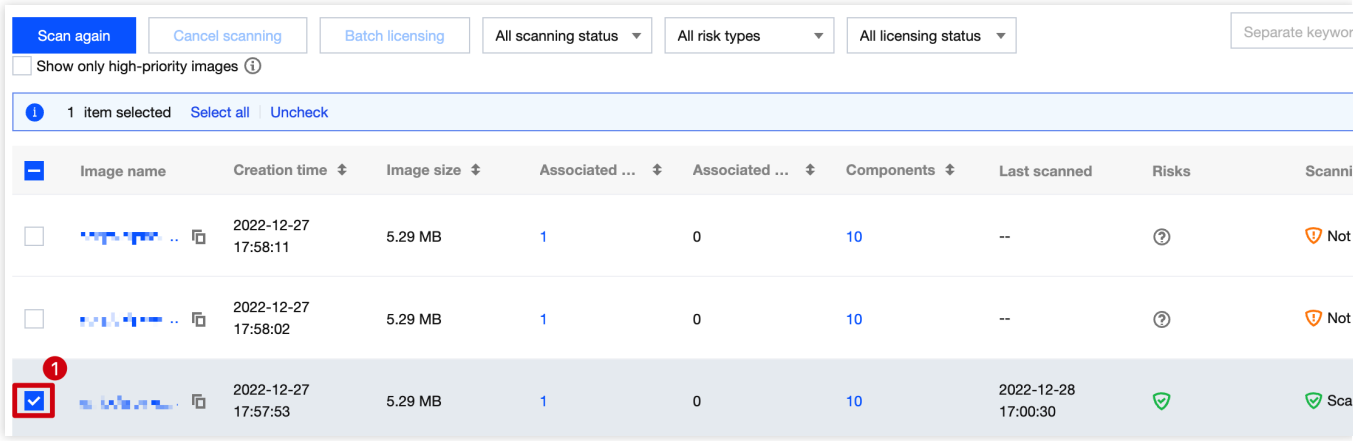
Exporting an image

On the **Local Images** page, click

©2013-2022 Tencent Cloud. All rights reserved.

to select the target local image and click

to export it.



Viewing the list details

1. On the **Local Images** page, click **Image name** to pop up the drawer on the right, which displays the image details.

Note:

Image risk: It indicates whether the image scan is successful and the numbers of vulnerabilities, viruses, trojans, and sensitive data pieces.

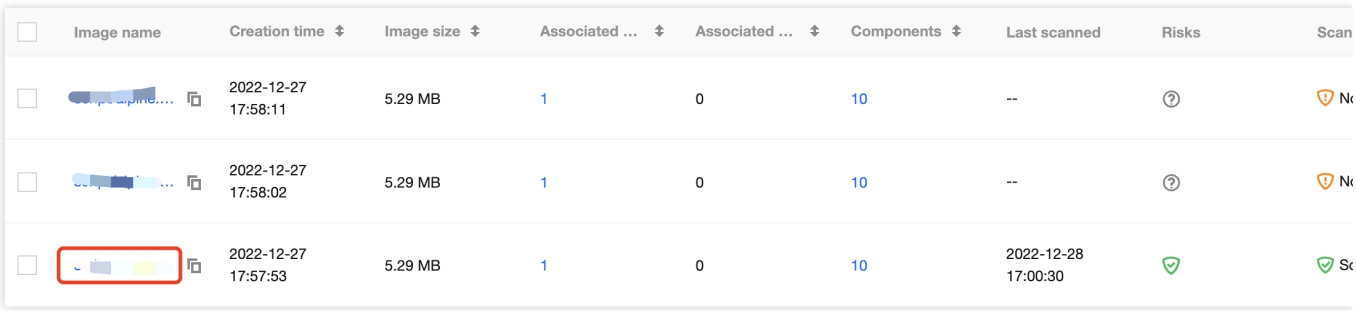
Image details: It includes the image name, image ID, image size, and operating system type.

Vulnerability list: You can filter image security vulnerability events by vulnerability severity or search for them by vulnerability name. Click **View details** to view the vulnerability details and fix suggestion.

Virus and trojan list: You can filter image security events by virus or trojan severity or search for them by filename. Click **View details** to view the virus or trojan details and suggestion.

Sensitive data list: You can filter security events by sensitive data severity, name, or type.

Image build history: It logs the image build history.



©2013-2022 Tencent Cloud. All rights reserved.

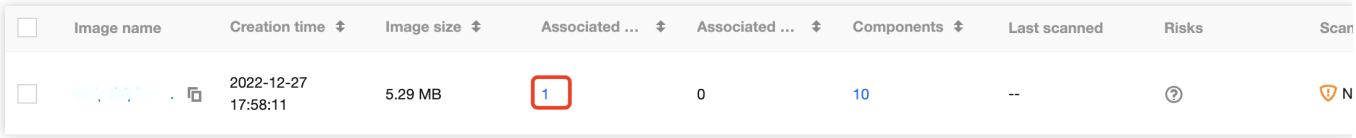
2. On the **Local Images** page, click **Associated servers** to pop up the details window, which displays the server name, server IP, and Docker version.

Note:

If multiple servers are associated, you can filter them as follows:

Click the server status drop-down list to filter servers by status.

Click the search box and search for servers by keyword such as server name, project, or Docker version.



3. On the **Local Images** page, click **Associated containers** to pop up the details window, which displays the container name, container ID, container running status, CMD, and last update time.

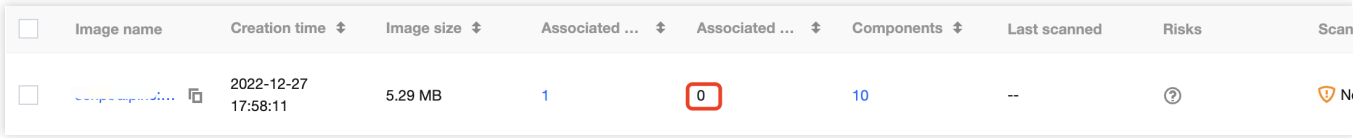
Note:

If multiple containers are associated, you can filter them as follows:

Click the status drop-down list to filter containers by status.

Enter the server name and click

for search.



4. On the **Local Images** page, click **Details** to display the drawer on the right, which displays the image name.

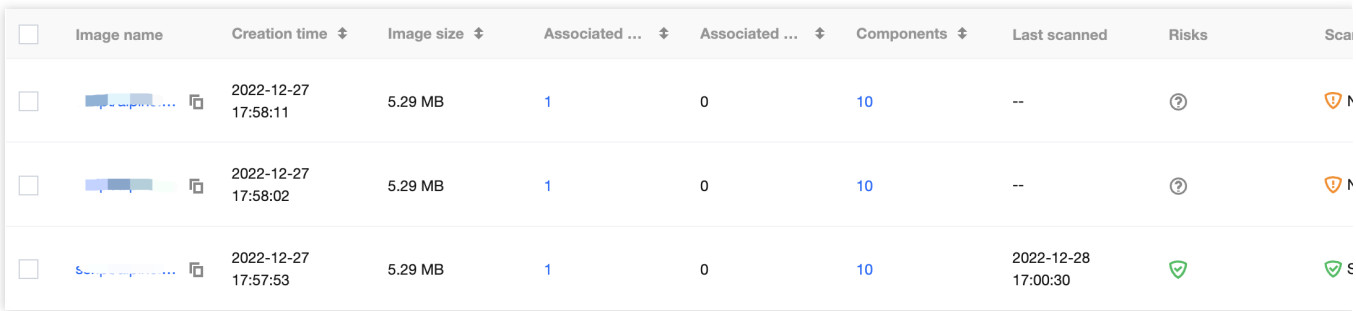
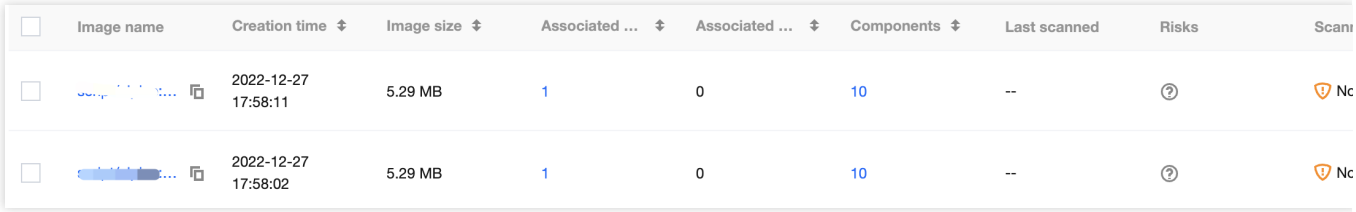


Image scanning

1. On the **Local Images** page, click **Scan now** > **OK** to scan an image in "Not scanned" status.

©2013-2022 Tencent Cloud. All rights reserved.

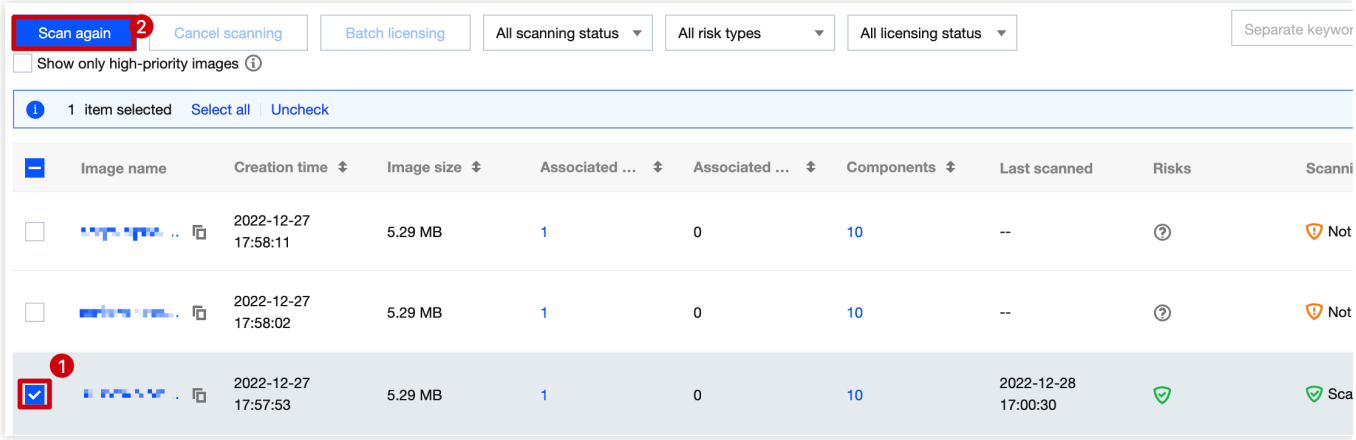


2. On the **Local Images** page, click **Scan again** after the previous scan task ends to scan the image again.

Note:

Click

to select multiple images and click **Scan again** next to ② to batch scan them again.

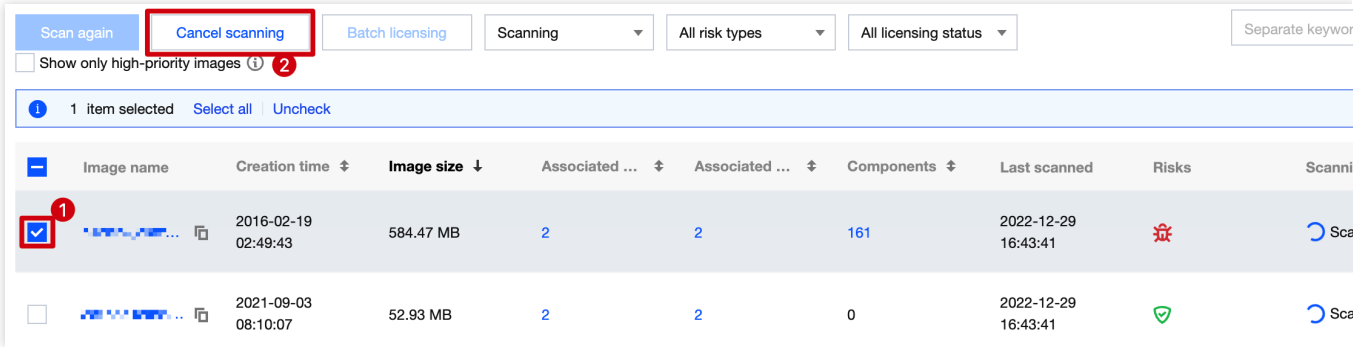


3. On the **Local Images** page, click **Cancel scanning** to cancel scanning an image in "Scanning" status.

Note:

Click

to select multiple images and click **Cancel scanning** next to ② to batch cancel them.



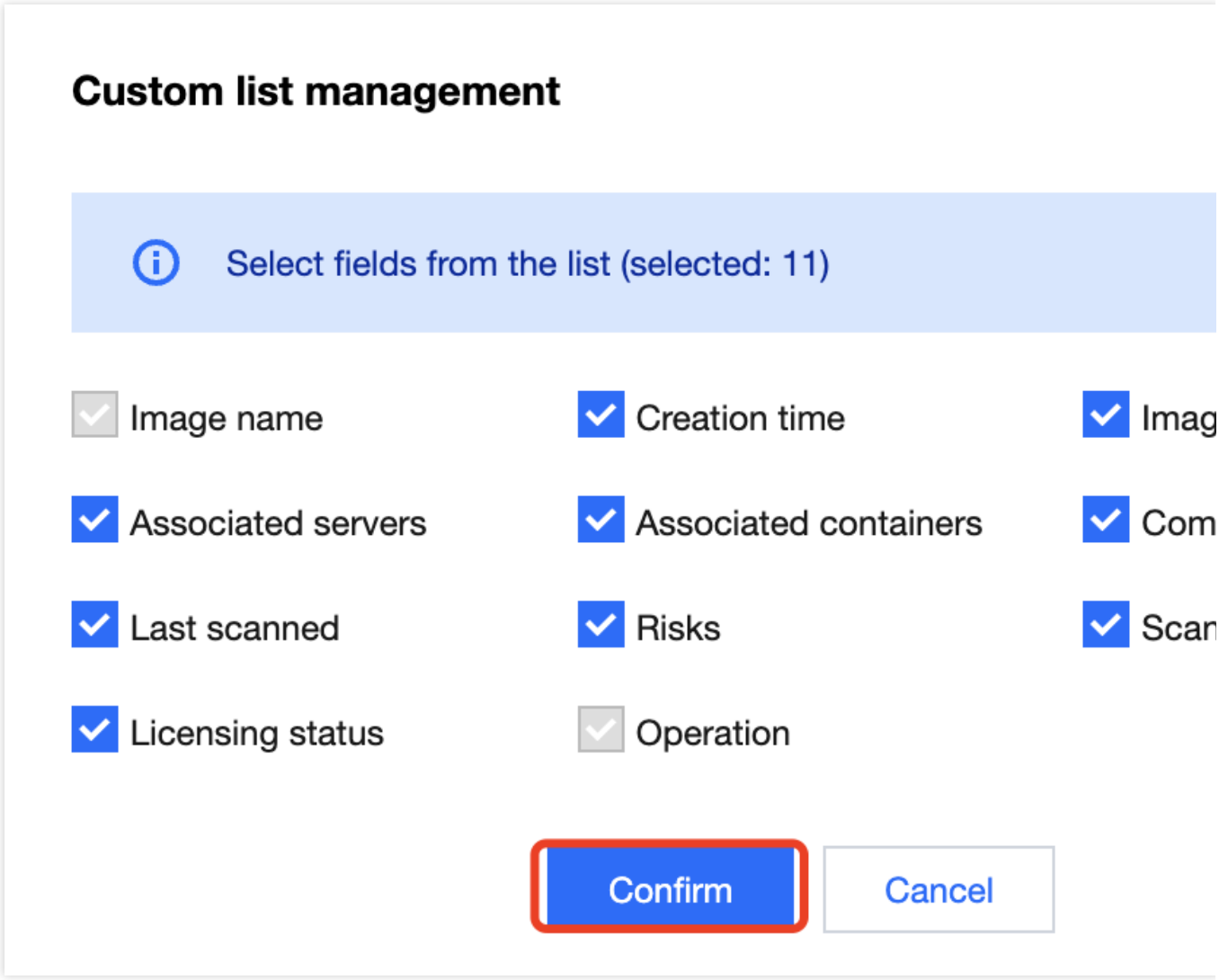
Custom list management

©2013-2022 Tencent Cloud. All rights reserved.

1. On the **Local Images** page, click

to pop up the **Custom List Management** window.

2. In the pop-up window, select the target type and click **OK**.



Key fields in the list

1. Creation time: The time when the image is created.
2. Last scanned: The time of the last scan.
3. Risks: Type of the risks to the container.
4. Status: Container scanning status, which can be **Scanned**, **Not scanned**, **Scanning**, **Cancelled**, or **Scan exception**.

Note:

We recommend you scan again in case of an exception.

©2013-2022 Tencent Cloud. All rights reserved.

Repository Image

Last updated：2024-01-23 15:44:44

This document describes the repository image feature and how to enable data scan and view the repository image list.

Note:

The following image repositories are supported:

TCR/CCR

Third-party Harbor

Prerequisites

You have purchased the value-added feature of TCSS for image security.

Connecting to TCR/CCR

TCSS and TCR/CCR are integrated by default to scan TCR and CCR images.

Note:

By default, TCSS requests TCR repository assets over the public network. If you enable access control for your repository instance, you need to add the service IP range to the allowlist before use or switch the network type. On the **Repository Images** page, click **Operation Guide** at the top to add the IP to the allowlist or switch to VPC as instructed.

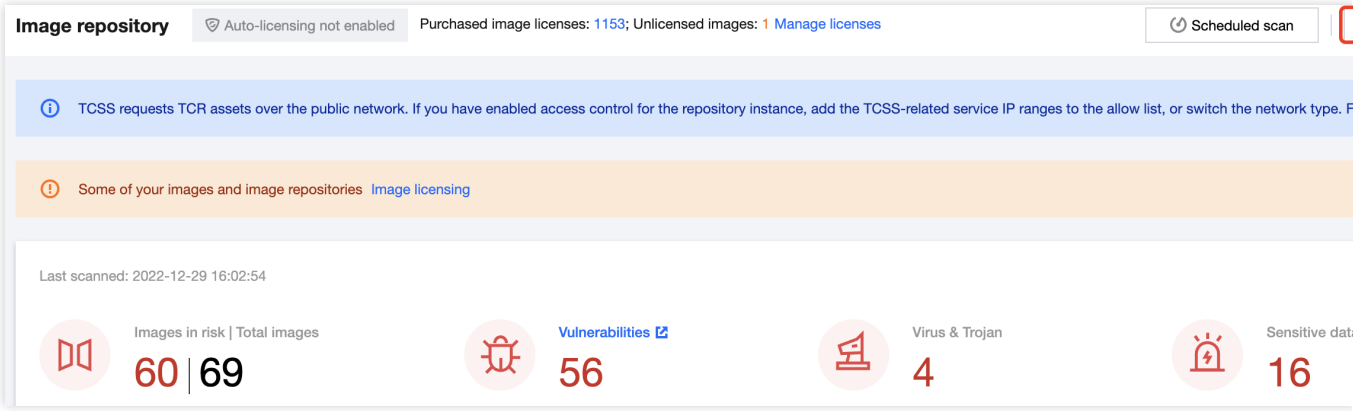
During your first use, you need to manually update the repository image data. On the **Repository Images** page, click **Data update** in the top-right corner to update the data, which may take a long time the first time.

The backend will automatically update the repository image data between 0:00 AM and 3:00 AM every day.

Connecting to Harbor

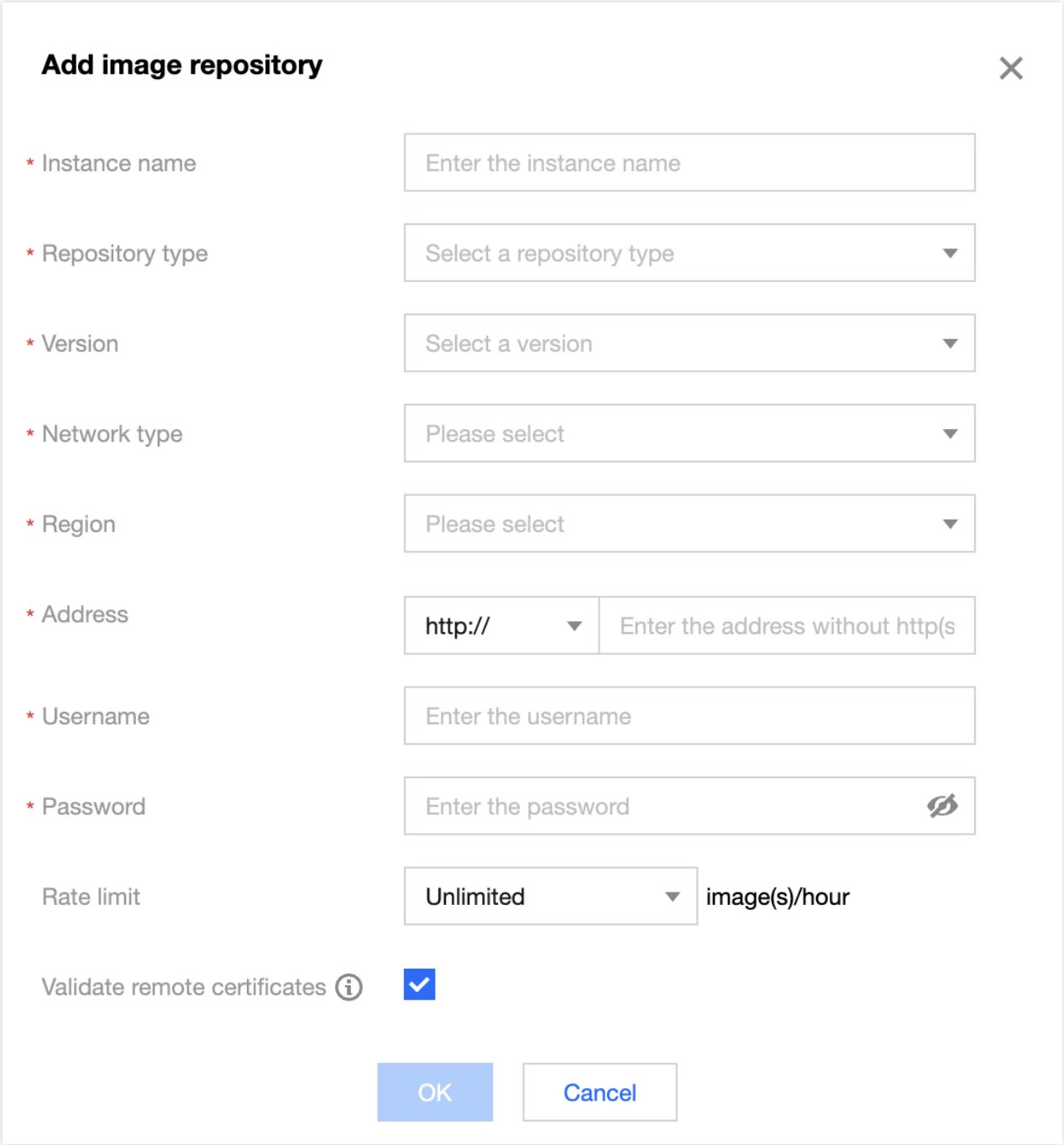
1. Log in to the TCSS console and select **Image Risk Control** > **Repository Images** on the left sidebar.
2. On the **Repository Images** page, click **Image repository management** in the top-right corner.

©2013-2022 Tencent Cloud. All rights reserved.



3. In the image repository list, click **Add image repository**.
4. In the **Add image repository** pop-up window, configure parameters and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Parameters:

Parameter	Description
Instance name	Enter the image repository name, which is unique and cannot be left empty.
Repository type	Select a third-party image repository, which can be Harbor.
Version	Select the third-party image repository version, which can be: V1: The image repository version of 1.X.X. V2: The image repository version of 2.X.X or later.
Network type	Select the network access type of the third-party image repository, which can be Public

©2013-2022 Tencent Cloud. All rights reserved.

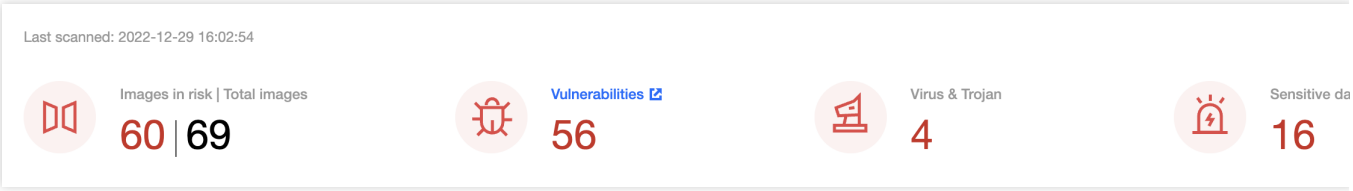
	network.
Region	Select the region of the third-party image repository, which is **Default region** for Harbor.
Address	Enter the access address of the third-party image repository.
Username	Enter the username for accessing the third-party image repository.
Password	Enter the password for accessing the third-party image repository.
Limit	Select the number of images that can be pulled synchronously every hour. Valid values: 5, 10, 20, 50, 100, 500, 1000, unlimited (default).
Validate remote certificates	Specify whether to verify the certificate of the remote image repository for image sync. If the repository uses a self-signed or non-trusted certificate, do not select this option. By default, this option is selected.

Enabling Data Scan

On the **Repository Images** page, the data scan module displays the number of images at risk, total number of images, and the numbers of vulnerabilities, viruses, trojans, and sensitive data pieces in the images after the last scan.

Enabling quick scan

1. On the **Repository Images** page, click **Scan now** on the right to get the latest image data or risk information.



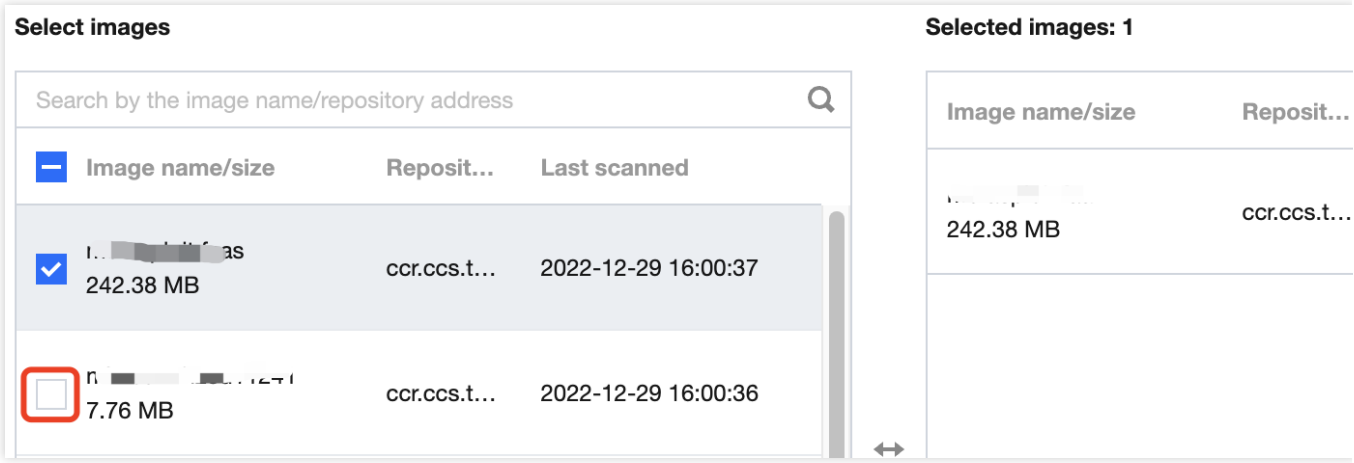
2. On the **Scanning settings** page, select the **Risk category** and **Images** as needed.
Risk category: **Vulnerabilities** or **Sensitive data**.
Images: **All images** or **Specified images**. Click

or

to select or delete the target specified image.

Note:

You can press Shift to select multiple ones.



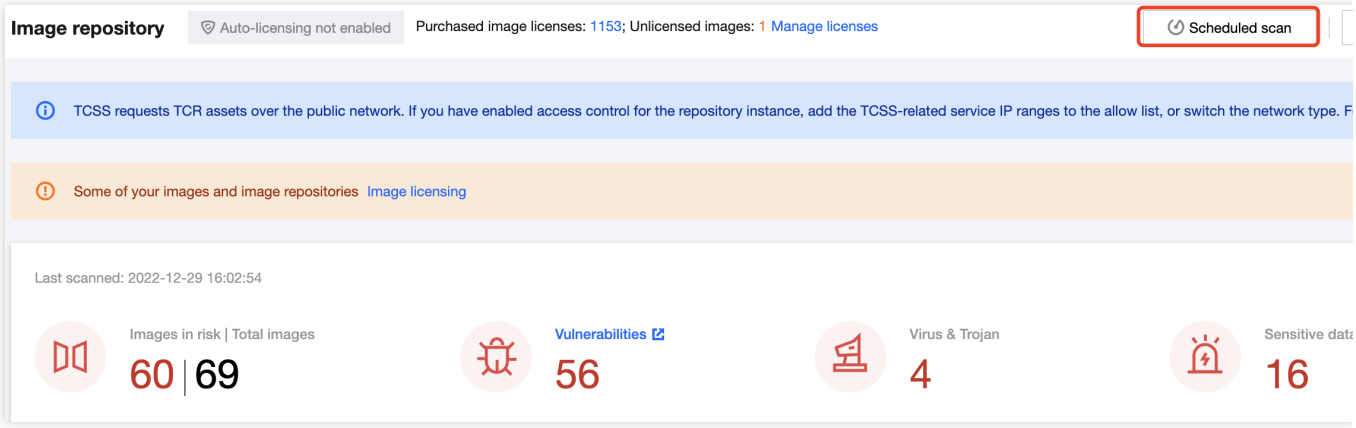
4. After selecting the target content, click **Scan now**.

Note:

After the scan starts, all images with the same ID as the selected image will be scanned at the same time.

Enabling scheduled scan

1. On the **Repository Images** page, click **Scheduled scan settings** on the right to specify whether to enable the scheduled scan feature.



2. On the **Scheduled scan settings** page, toggle on the **On/Off** switch and set the **Frequency**, **Risk category**, and **Images** as needed.

Frequency: It can be every day, every 7 days, every 15 days, every 30 days, or a specified time range.

Risk category: Click

©2013-2022 Tencent Cloud. All rights reserved.

to select **Vulnerabilities**, **Sensitive data**, or **Virus & Trojan** as needed.

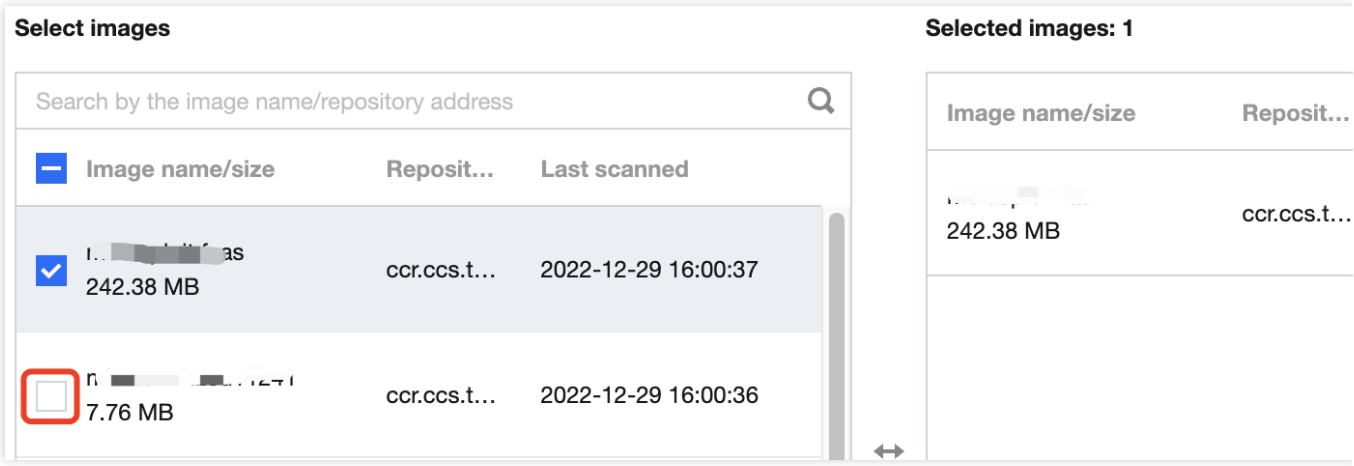
Images: **All images** or **Specified images**. Click

or

to select or delete the target specified image.

Note:

You can press Shift to select multiple ones.



4. After selecting the target content, click **Set** or **Cancel**.

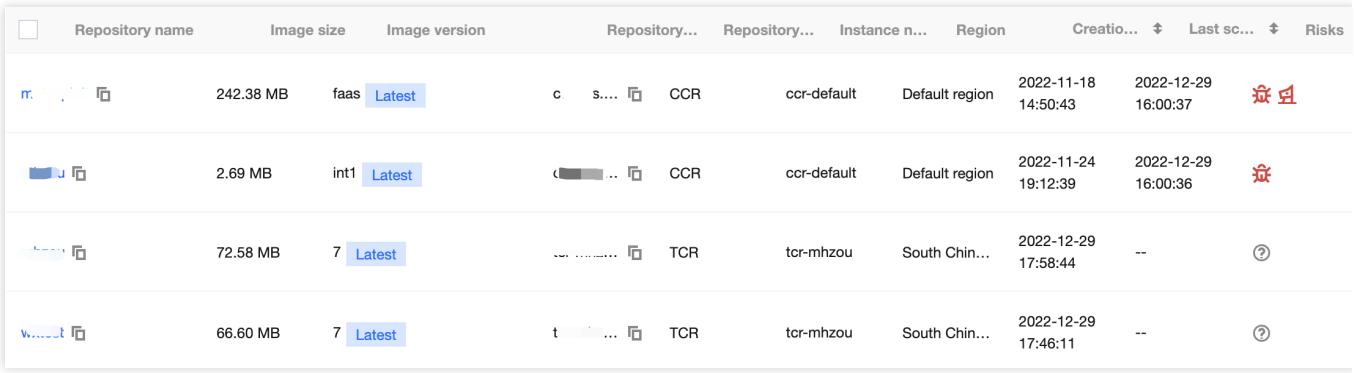
Viewing the List of Repository Images

Log in to the TCSS console and select **Image Risk Control** > **Repository Images** on the left sidebar.

Image licensing event

1. On the **Repository Images** page, click **License**.

©2013-2022 Tencent Cloud. All rights reserved.



2. In the pop-up window, click **OK**.

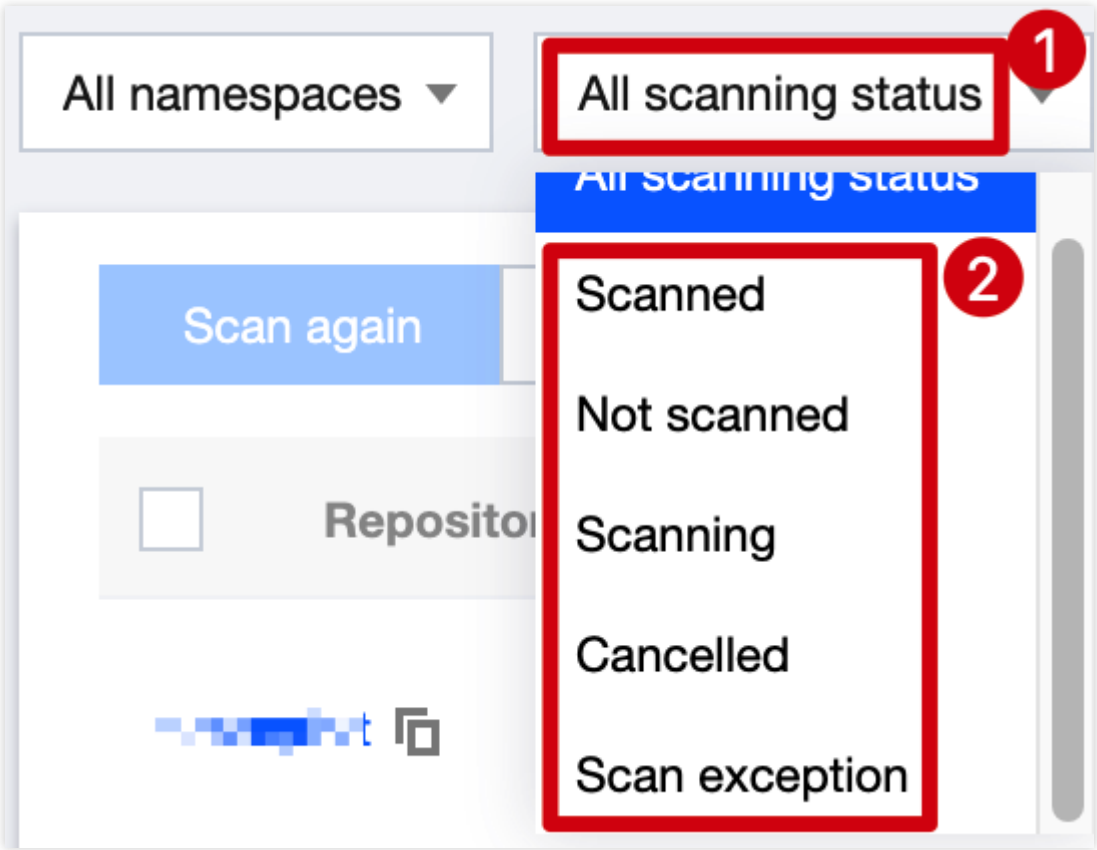
Note:

A license will be assigned to this image.

Filtering images

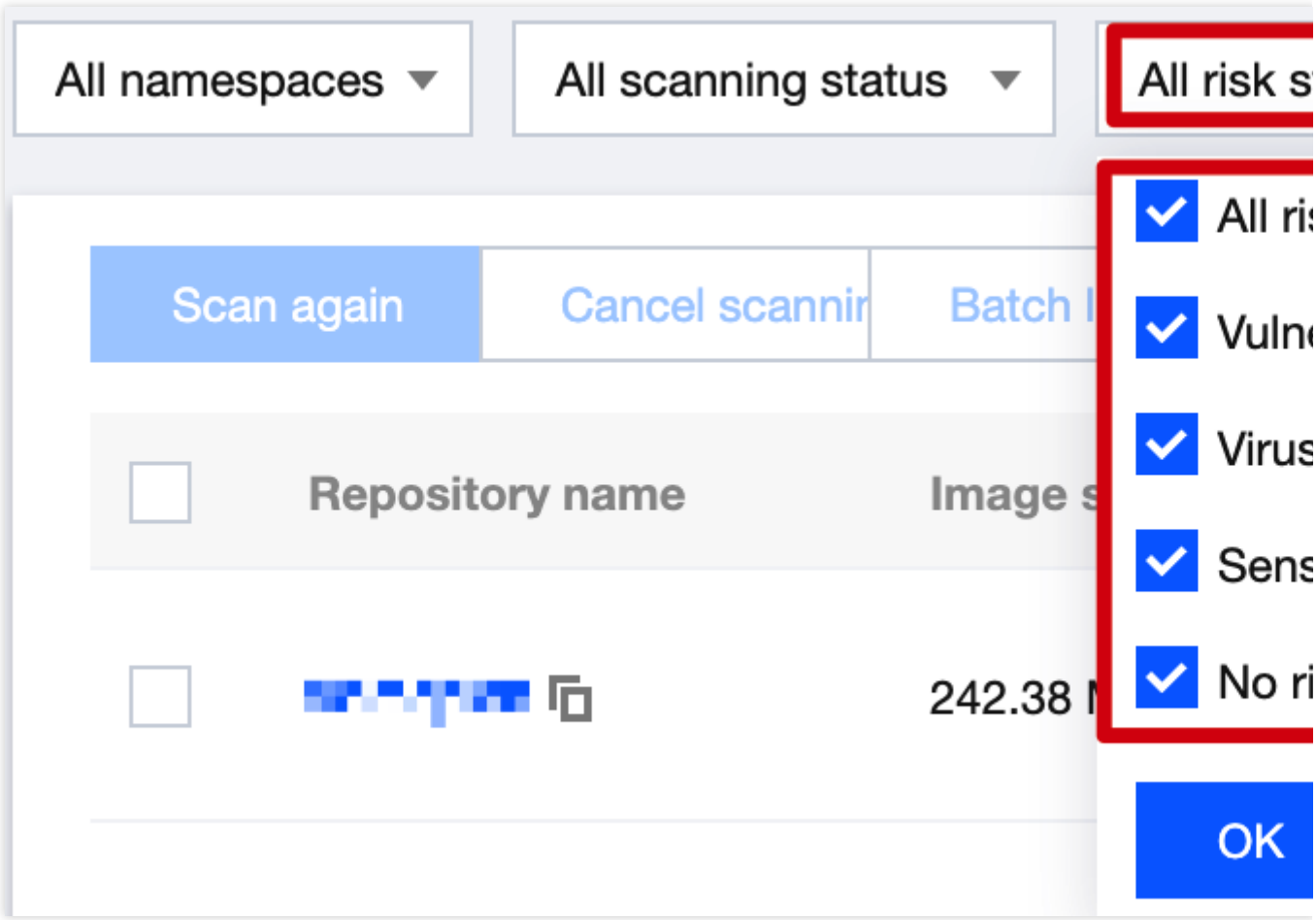
On the **Repository Images** page, filter images as follows:

Click the scanning status drop-down list to filter images by scanning status.

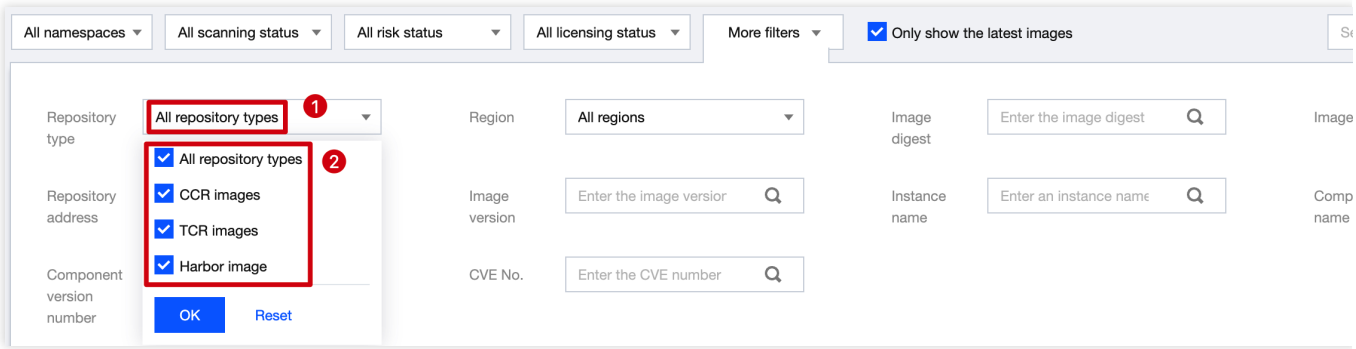


Click the security status drop-down list to filter images by security status.

©2013-2022 Tencent Cloud. All rights reserved.

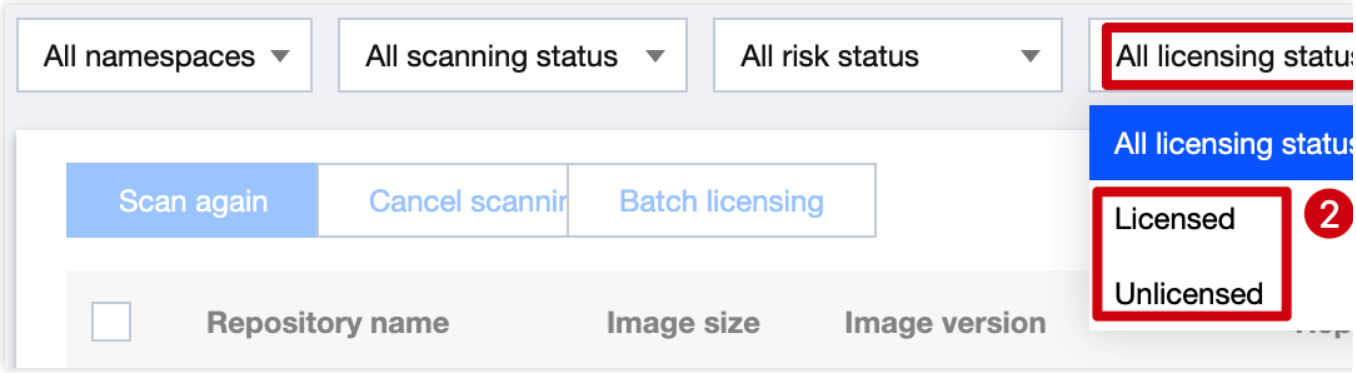


Click the repository type drop-down list to filter images by repository type.

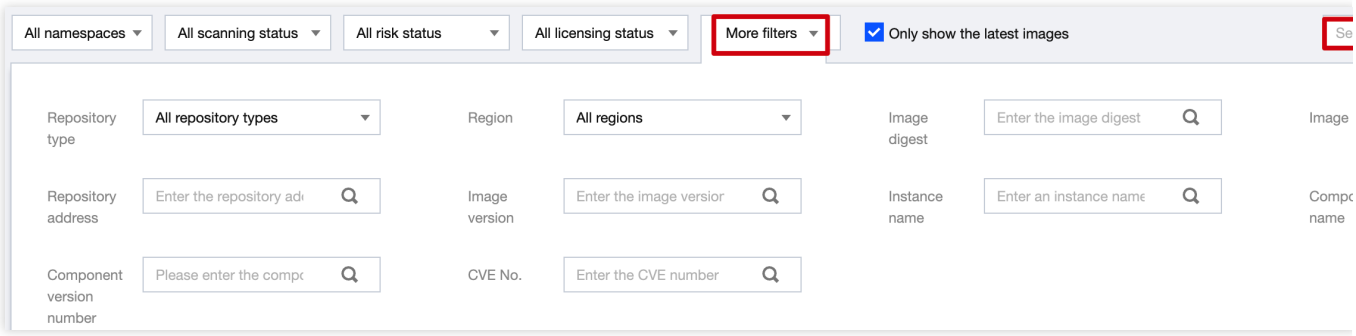


Click the licensing status drop-down list to filter images by licensing status.

©2013-2022 Tencent Cloud. All rights reserved.



Click the search box and search for images by keyword such as image name or image digest.

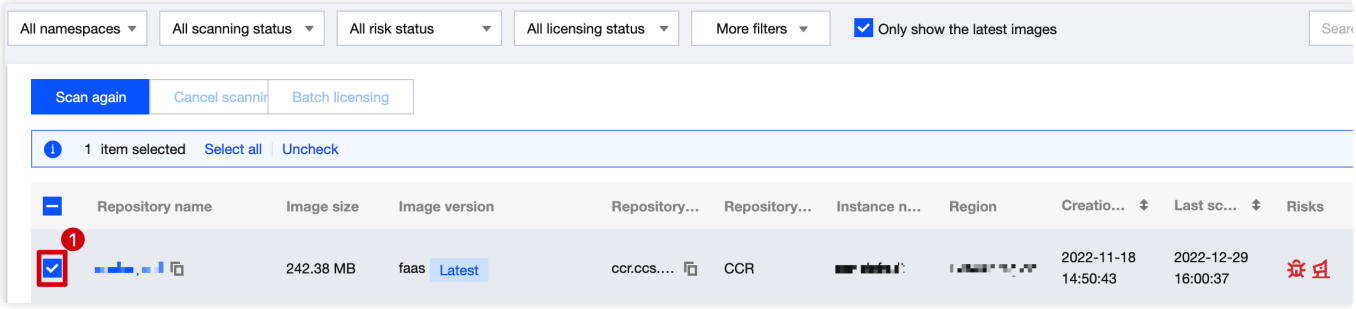


Exporting an image

On the **Repository Images** page, click

to select the target image repository and click

to export it.



Viewing the list details

©2013-2022 Tencent Cloud. All rights reserved.

On the **Repository Images** page, click **Details** to display the drawer on the right, which displays the image risk information, details, and list of vulnerabilities.

Note:

Image risk: It indicates whether the image scan is successful and the numbers of vulnerabilities, viruses, trojans, and sensitive data pieces.

Image details: It includes the image name, image digest, and image size.

Vulnerability list: You can filter image security vulnerability events by vulnerability severity or search for them by vulnerability name. Click **View details** to view the vulnerability details and fix suggestion.

Virus and trojan list: You can filter image security events by virus or trojan severity or search for them by filename. Click **View details** to view the virus or trojan details and suggestion.

Sensitive data list: You can filter security events by sensitive data severity, name, or type.

Image build history: It logs the image build history.

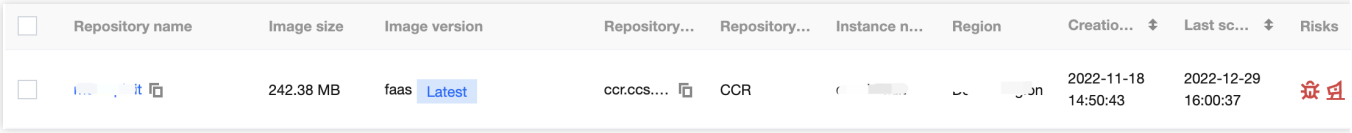
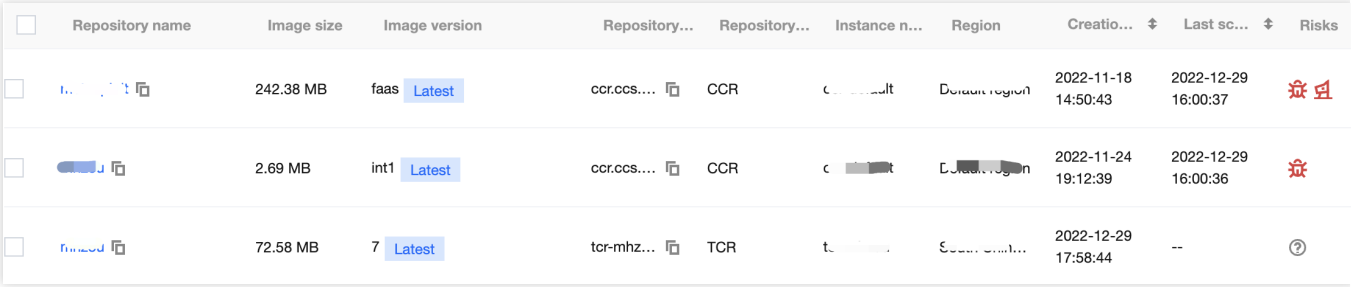


Image scanning

1. On the **Repository Images** page, click **Scan now** > **OK** to scan an image in "Not scanned" status.



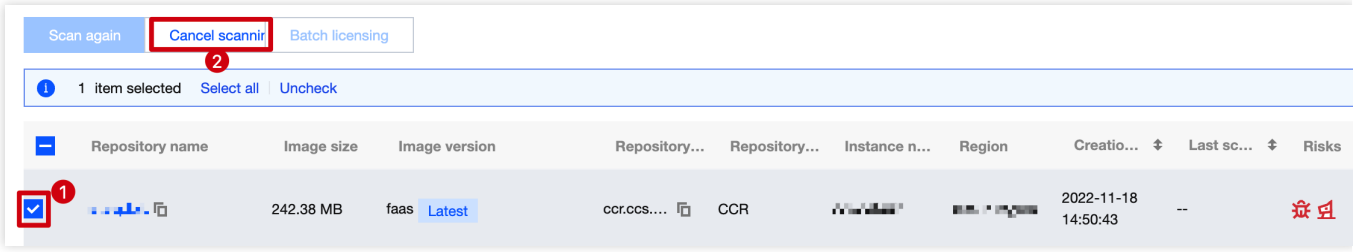
2. On the **Repository Images** page, click **Cancel scanning** to cancel scanning an image in "Scanning" status.

Note:

Click

to select multiple images and click **Cancel scanning** next to ② to batch cancel them.

©2013-2022 Tencent Cloud. All rights reserved.

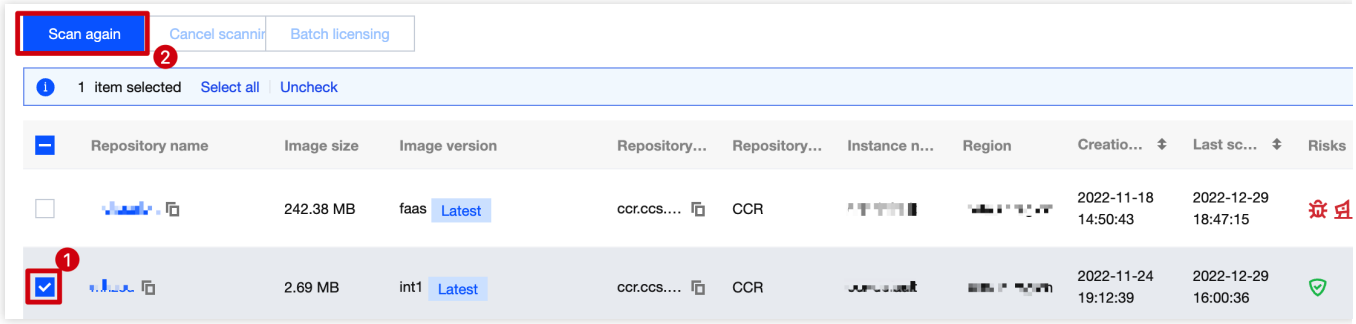


3. On the **Repository Images** page, click **Scan again** after the previous scan task ends to scan the image again.

Note:

Click

to select multiple images and click **Scan again** next to ② to batch scan them again.



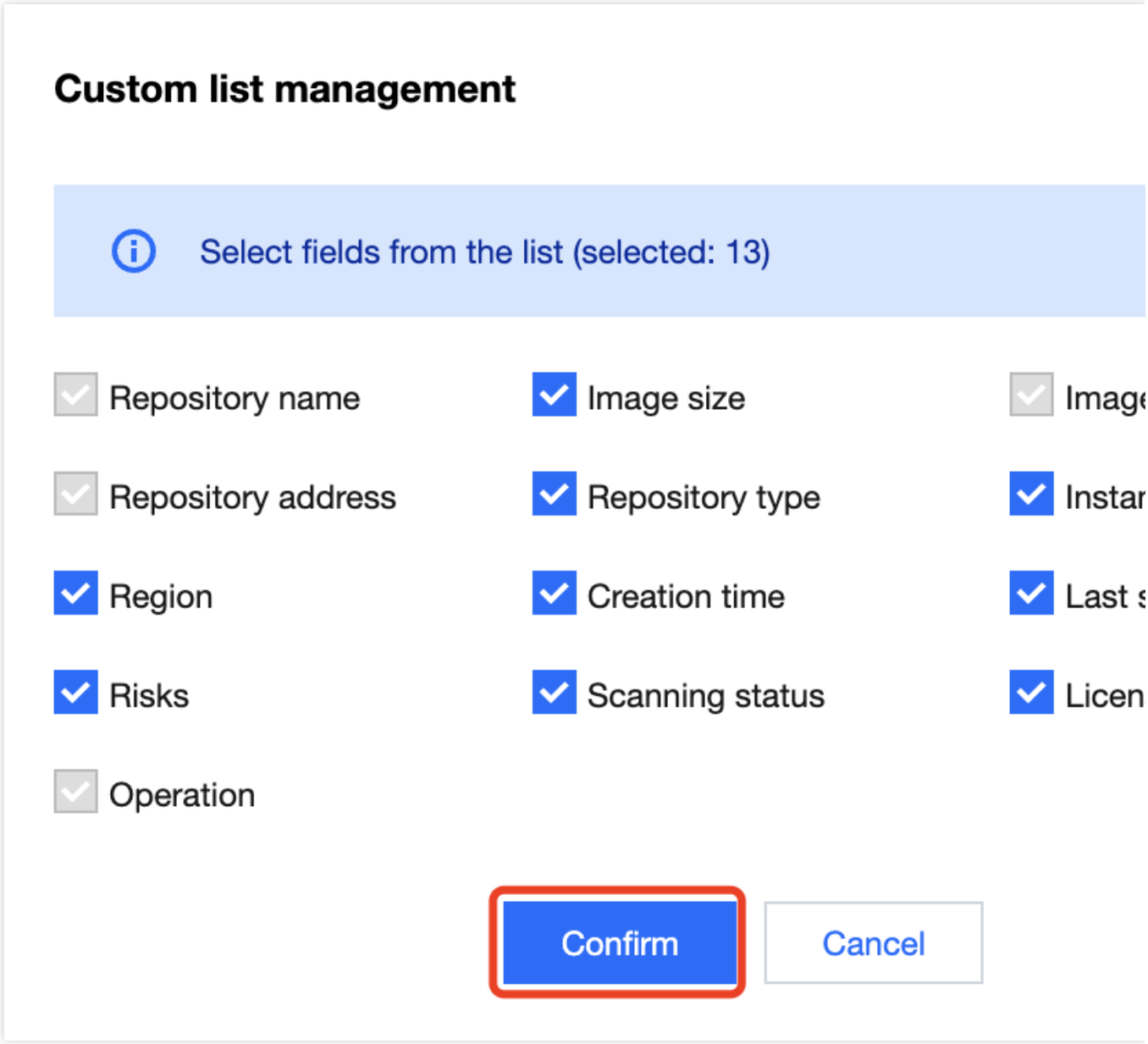
Custom list management

1. On the **Repository Images** page, click

to pop up the **Custom List Management** window.

2. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Fields in the list

1. Image repository address: Source address of the repository image.
2. Repository type: Type of the image repository, which can be TCR or CCR.
3. Image version: Tag of the repository image.
4. Last scanned: The time of the last scan.
5. Risks: Type of the risks to the container.
6. Status: Container scanning status, which can be **Scanned**, **Not scanned**, **Scanning**, **Cancelled**, or **Scan exception**.

Note:

We recommend you scan again in case of an exception.

©2013-2022 Tencent Cloud. All rights reserved.

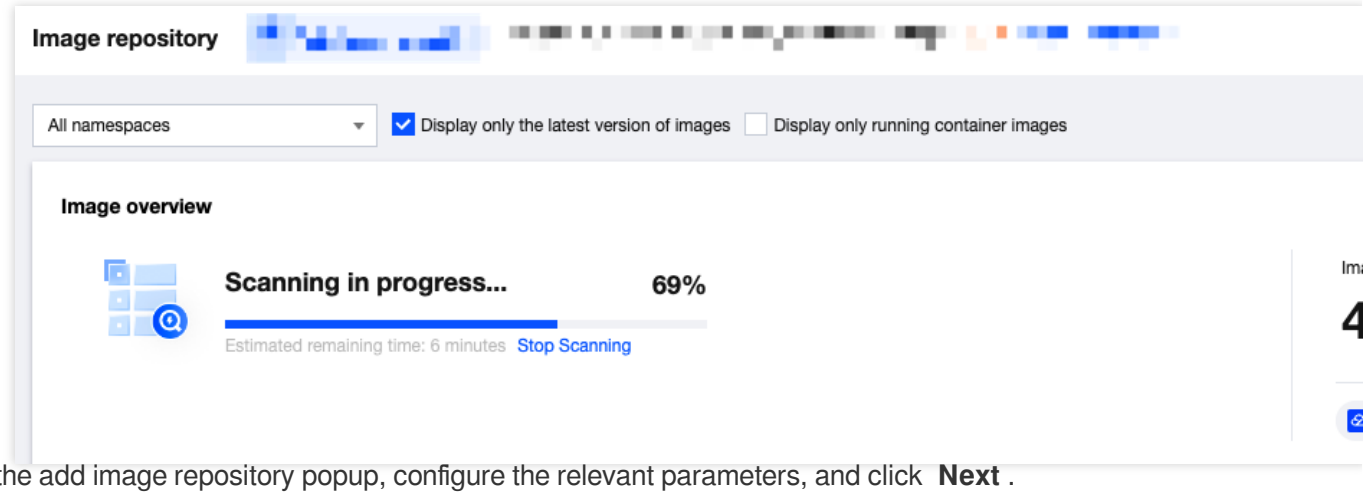
Accessing the AWS Image Repository

Last updated：2024-08-13 17:05:18

When you need to access repository images from your AWS account to the TCSS console for security scanning, you can see this document to access the AWS image repository.

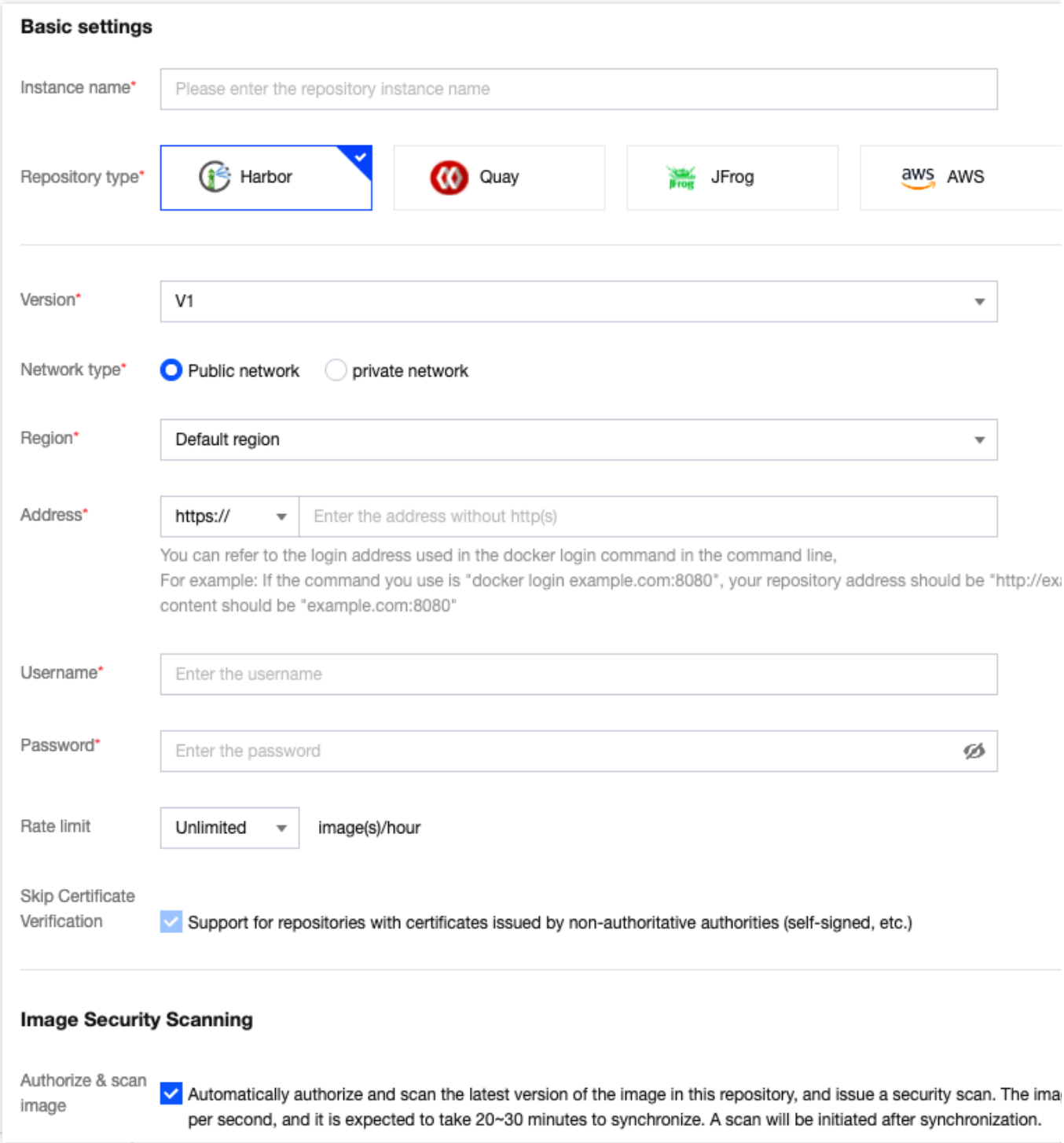
Accessing Repository

1. Log in to the TCSS console. In the left sidebar, click **Image Risk Control** > **Repository Images**.
2. On the image repository page, click **Access Repository**.



3. In the add image repository popup, configure the relevant parameters, and click **Next** .

©2013-2022 Tencent Cloud. All rights reserved.



Parameter Name	Description
Instance Name	Fill in the image repository instance name. The instance name must be unique and not empty.
Repository Type	Select the third-party image repository type. Currently supported options include Harbor, Quay, JFrog, and AWS. When users access AWS repositories, select AWS.
Network Type	Select the network access type for the third-party image repository. AWS repositories only support the public network.

©2013-2022 Tencent Cloud. All rights reserved.

Region	Select the region where the third-party image repository is located. The AWS type defaults to Default Region.
Address	Enter the access address of the third-party image repository. You can see the log-in address used in the docker log-in command on the command line. For example: If your command is docker log-in example.com:8080, your repository address should be http://example.com:8080 and the input content should be example.com:8080.
Username	Enter the username to access the third-party image repository. For details, see how to create an AWS account.
Password	Enter the password to access the third-party image repository. For details, see how to create an AWS account.
Rate Limit	Select the number of images that can be synchronously pulled per hour. The default is unlimited. Optional values are 5, 10, 20, 50, 100, 500, 1,000, and unlimited.
Certificate Verification Skipping	Confirm whether to verify the certificate of the remote image repository instance for image synchronization. If the remote instance uses a self-signed or untrusted certificate, do not check this option. It is checked by default.
Image Authorizing & Scanning	Automatically authorize and scan the latest version of the image in this repository, and issue a security scan. The image synchronization speed is about 20 per second, and it is expected to take 20-30 minutes to synchronize. A scan will be initiated after synchronization.

4. Under the Verify Connection Status, select **Connection method**, and click **Confirm to add**.

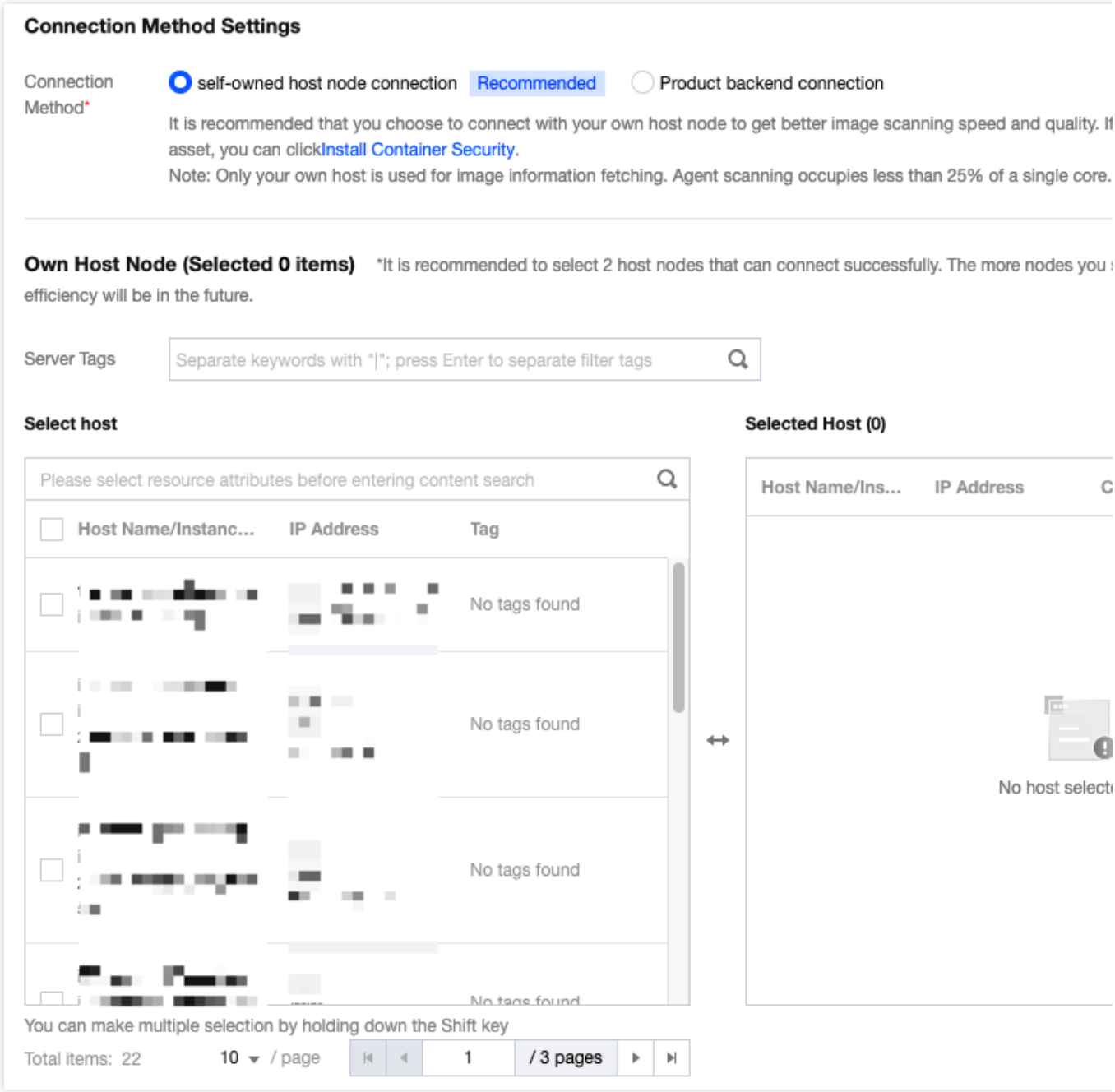
Note:

Verify connection status: You can select **Self-owned Host Node Connection** or **Product Backend Connection**.

Self-owned host node connection: Select your own host node for repository image pulling and scanning. It is recommended to select self-owned host node connection for better image scanning rate.

Product backend connection: Use TCSS product-side backend services for repository image pulling and scanning. The scanning rate is slower and it takes longer time.

©2013-2022 Tencent Cloud. All rights reserved.

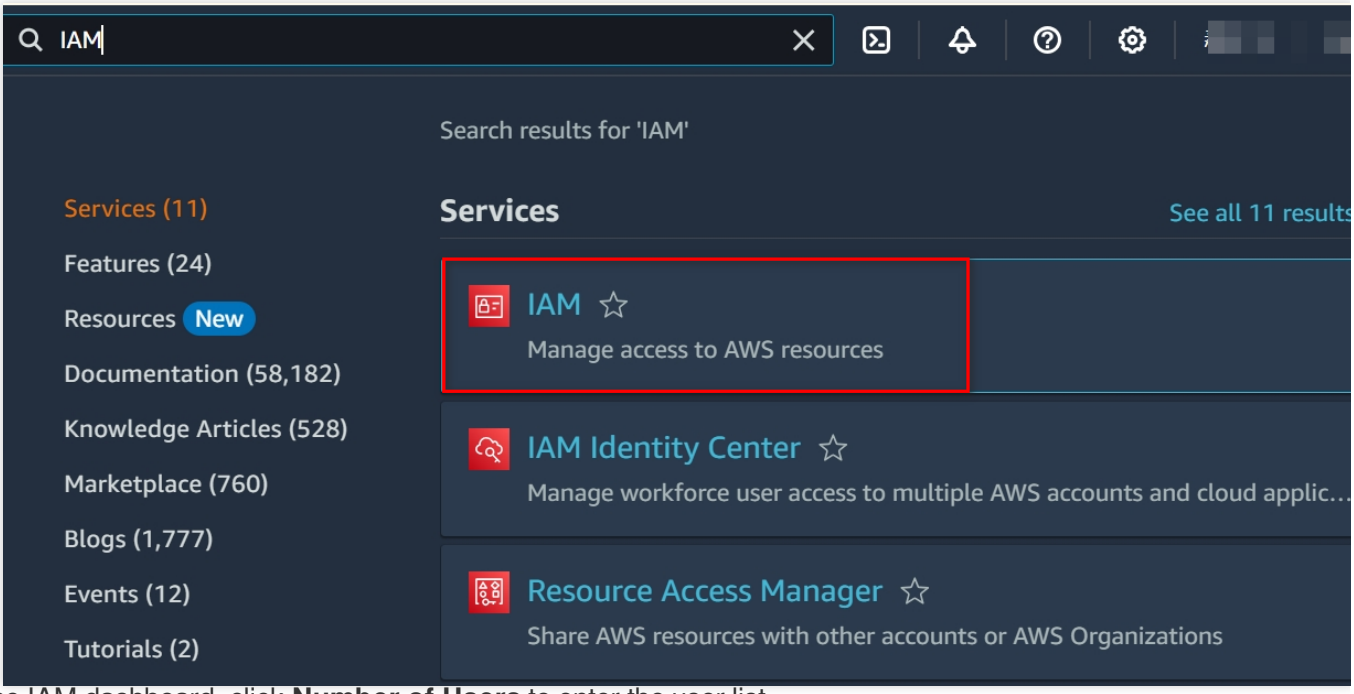


Creating an AWS Account

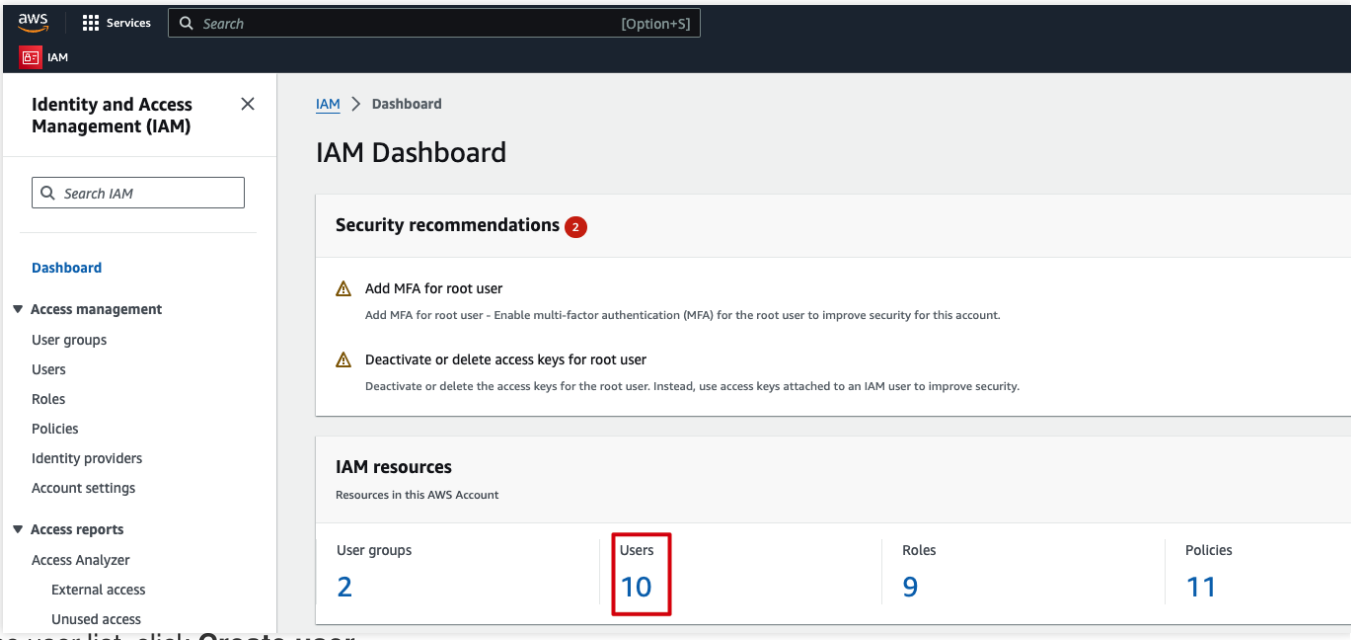
Step 1: Creating an IAM User

1. Log in to the AWS console, and select **IAM** service.

©2013-2022 Tencent Cloud. All rights reserved.

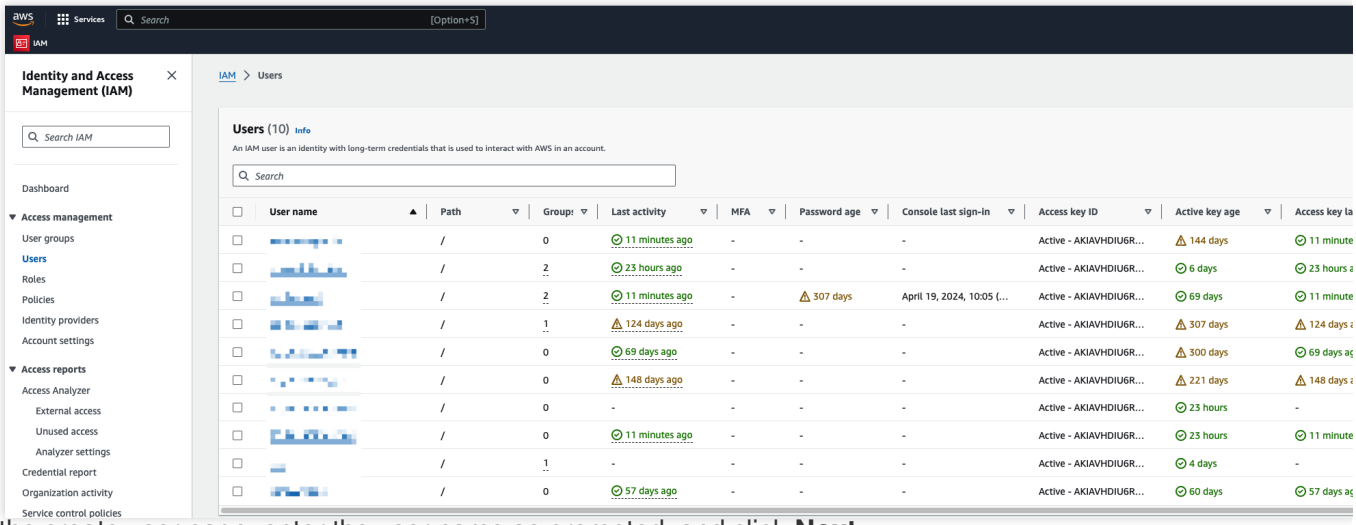


2. In the IAM dashboard, click **Number of Users** to enter the user list.



3. In the user list, click **Create user**.

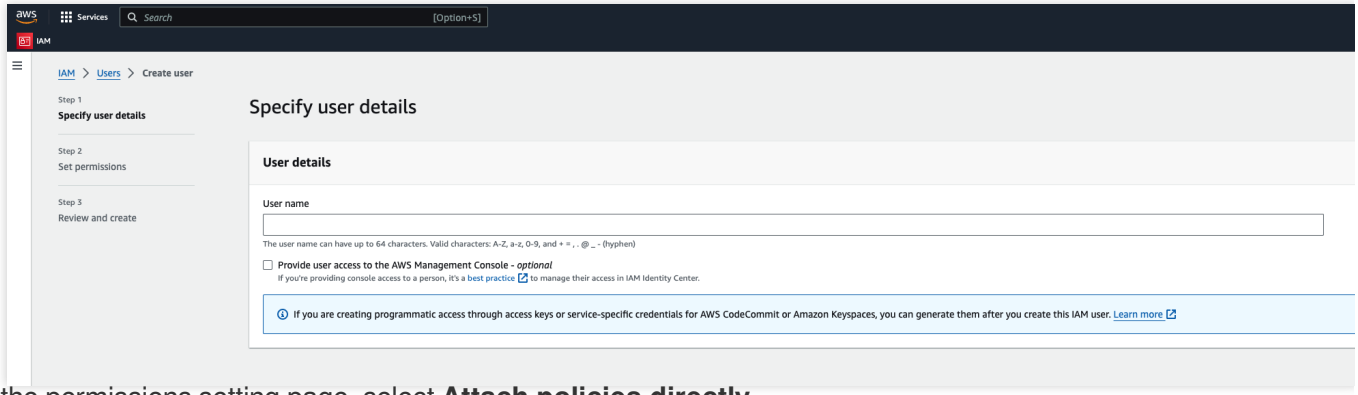
©2013-2022 Tencent Cloud. All rights reserved.



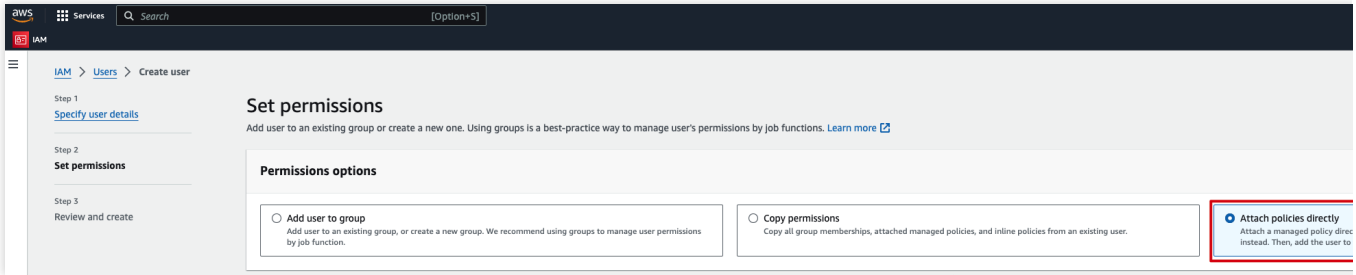
4. On the create user page, enter the user name as prompted, and click **Next.**

Note:

The optional enabling console access can be configured as needed. This guide does not require checking.

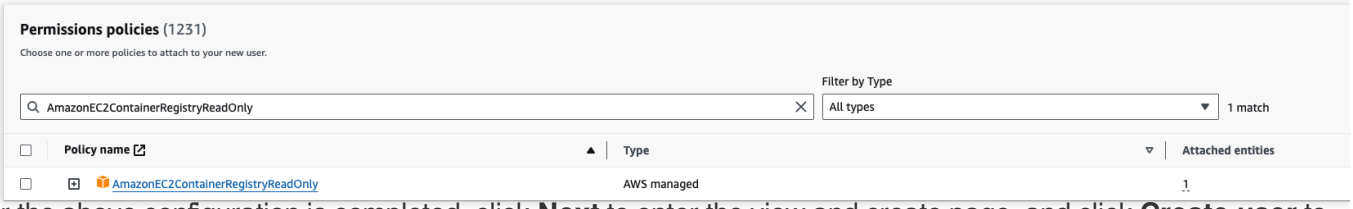


5. On the permissions setting page, select **Attach policies directly**.

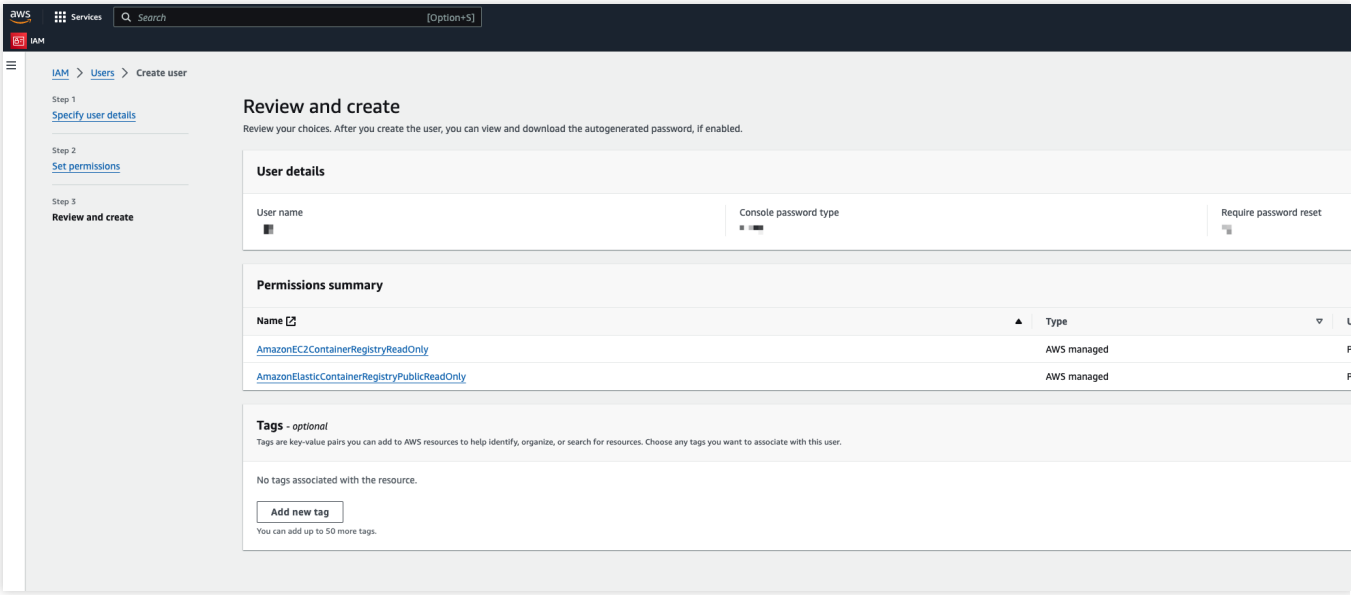


6. When users select permission policies, select the following two policies: AmazonEC2ContainerRegistryReadOnly, and AmazonElasticContainerRegistryPublicReadOnly.

©2013-2022 Tencent Cloud. All rights reserved.

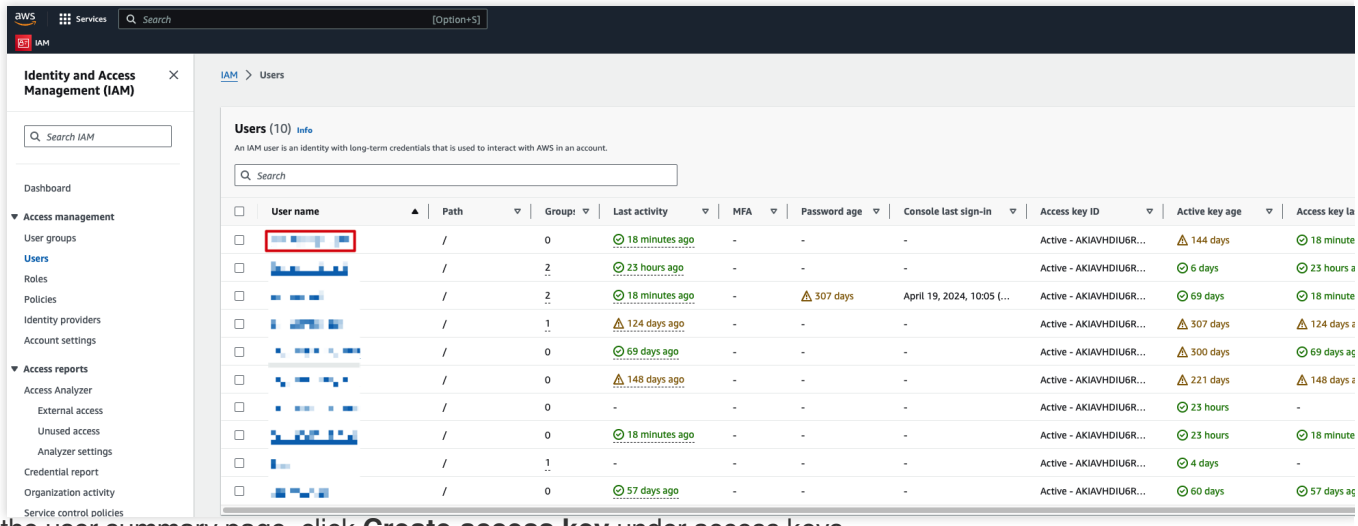


7. After the above configuration is completed, click **Next** to enter the view and create page, and click **Create user** to finish creating an IAM user.



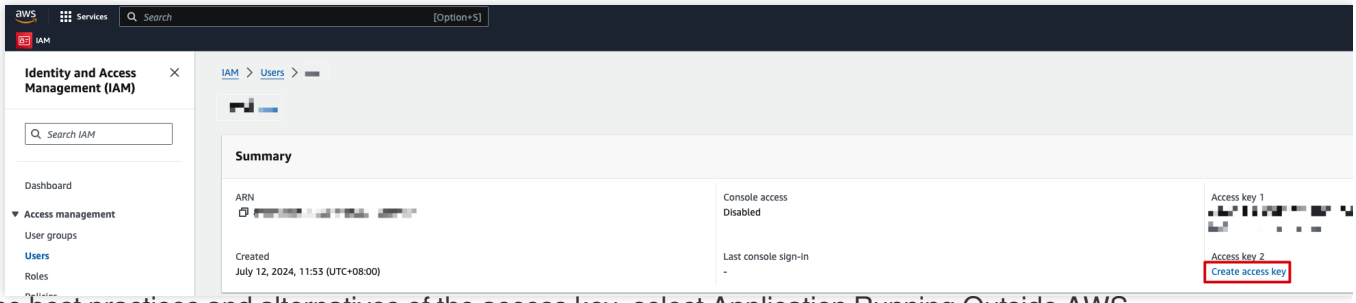
Step 2: Creating AK/SK

1. In the user list, click **User name** to enter the user summary page.

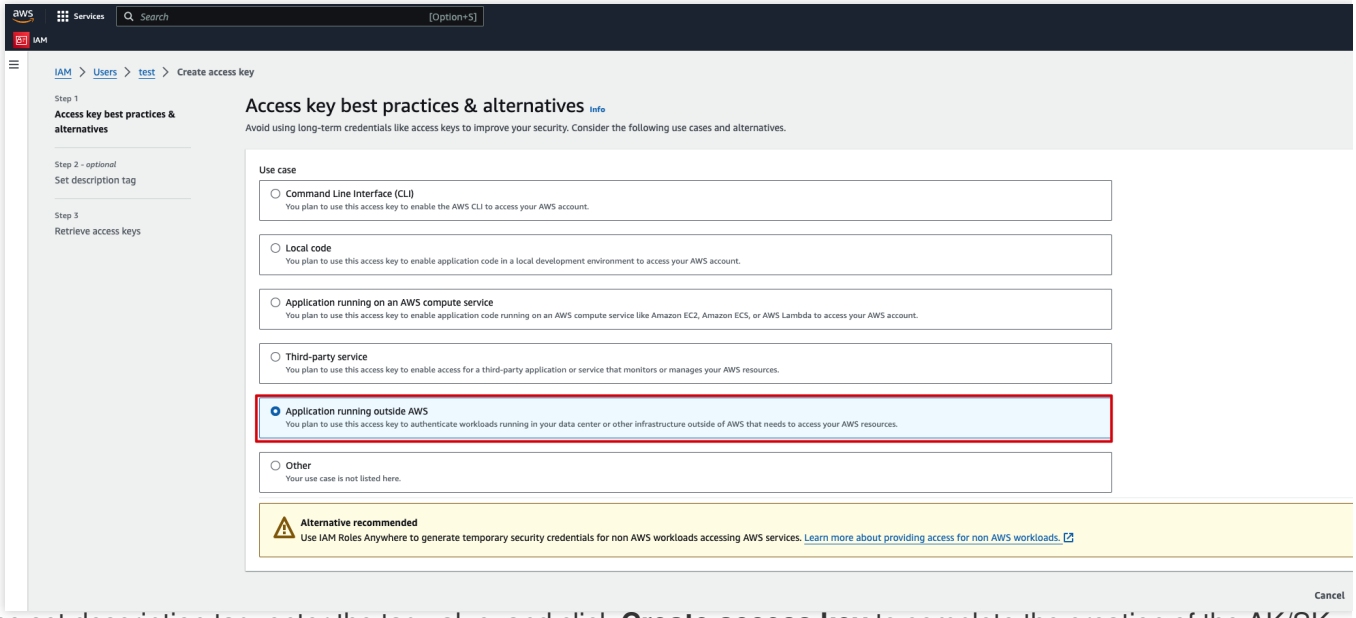


2. On the user summary page, click **Create access key** under access keys.

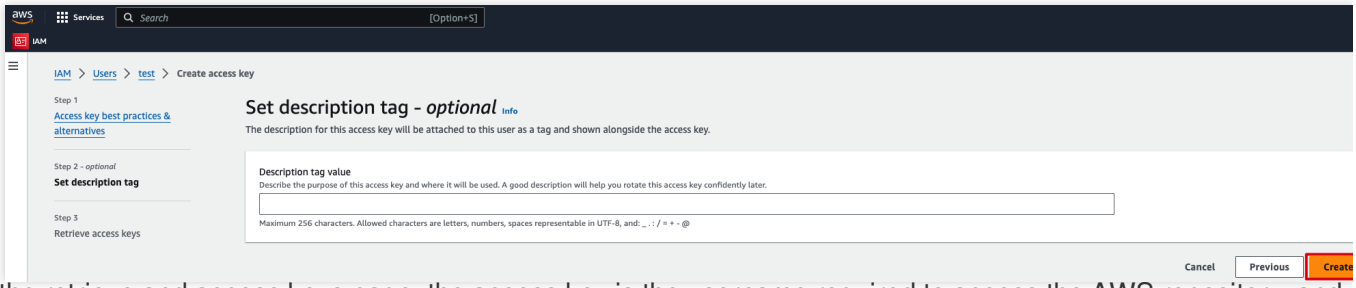
©2013-2022 Tencent Cloud. All rights reserved.



3. In the best practices and alternatives of the access key, select Application Running Outside AWS.

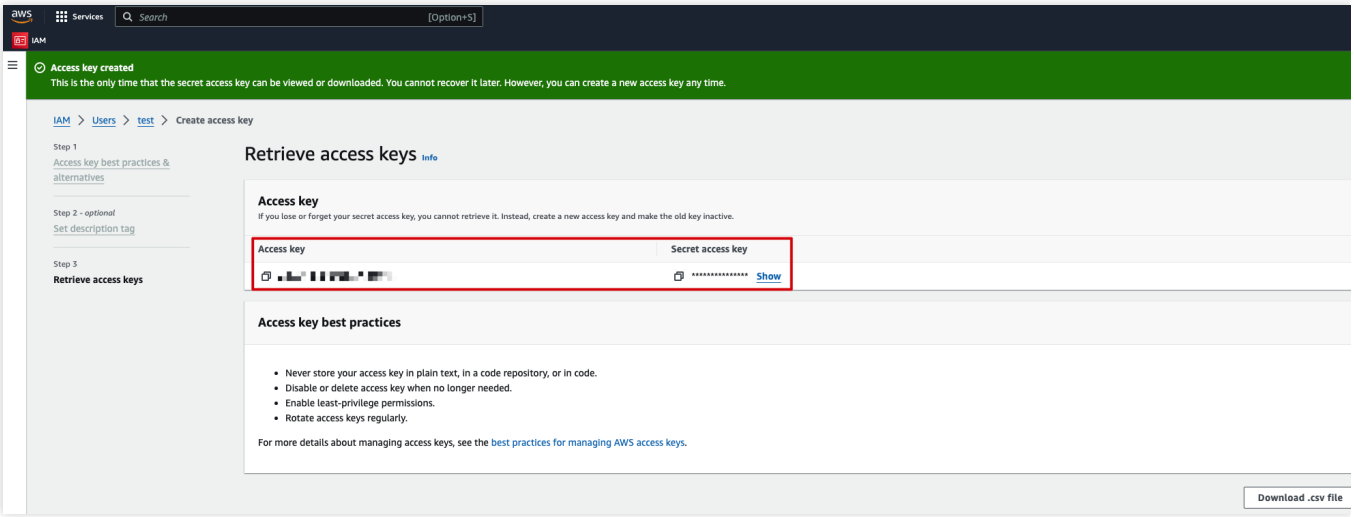


4. In the set description tag, enter the tag value, and click **Create access key** to complete the creation of the AK/SK access key.



5. On the retrieve and access keys page, the access key is the username required to access the AWS repository, and the secret access key is the password required to access the AWS repository.

©2013-2022 Tencent Cloud. All rights reserved.

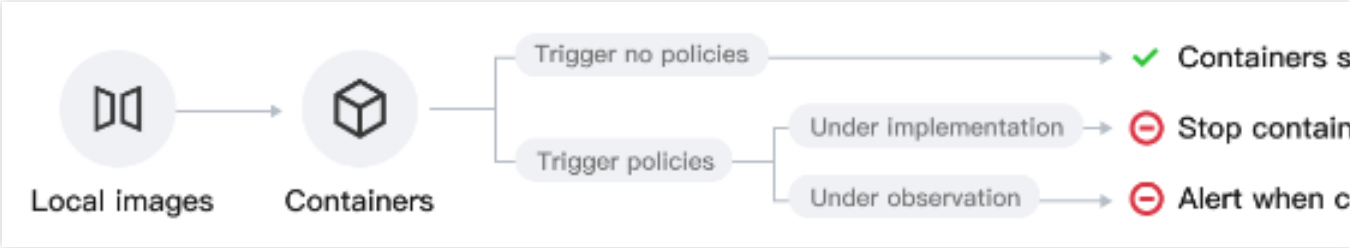


©2013-2022 Tencent Cloud. All rights reserved.

Image Interception Events

Last updated：2024-08-13 17:06:43

Users can configure alarms and interception policies on the image interception policies page. The image interception policy allows you to intercept the startup of containers for images that have critical security issues, thereby preventing malicious images from running container services.

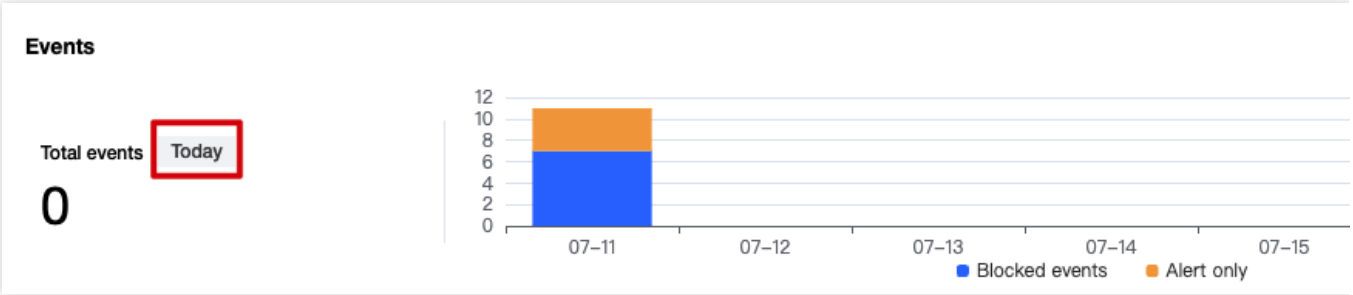


After you create and activate an interception policy, it will take effect in about 3-5 minutes. Once it is activated, if a hit risk image attempts to start a container, the system will alarm or intercept the container startup and report the interception records, based on the configured policy's alarm and interception requirements.
Currently supported intercepted image types: Images with critical and high-risk vulnerabilities, Trojan viruses, and sensitive information risks, as well as privileged images.
Privileged image interception supports only one rule configured. To modify the range of intercepted images, you can edit the configured rule.

Event Overview

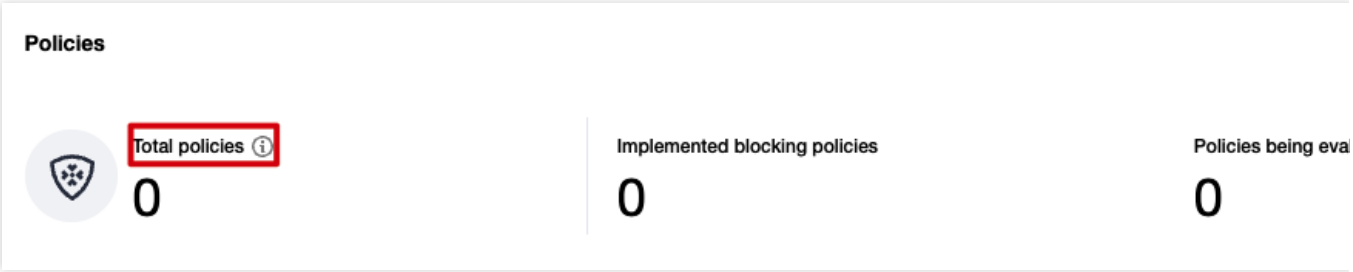
Once the user configures the image startup interception policy and sets it to take immediate effect, attempts to start containers using targeted risky images will be intercepted in real-time, with the image startup actions reported and recorded. If the policy includes an observation period, during which only alarms are issued without interception, attempts to start containers using targeted risky images will trigger real-time reporting of the image startup actions. In both scenarios, event logs will be generated.
In the image interception events > **Events**, daily statistics will be provided for both image startup interception events and events where only alarms were triggered. Trend charts for both types of events over the past 7 days and the current total number of events will be displayed.

©2013-2022 Tencent Cloud. All rights reserved.



Policy Overview

On the image interception policy page, after you have configured the alarm and interception policies, the system will count the total number of enabled policies, as well as the number of included effective interception policies and observation period policies. In the image interception events > **Policies**, click **View policy details** to jump to **Policy Management** > **Image Blocking Policies** page to view the details of the image interception policies.



Event List

In the image interception events > **Event List**, the recorded are the image startup interception events generated by effective interception policies and the image startup alarm events generated by observation period policies. Users can filter events by type, executed action, or latest creation time, and perform keyword searches, such as the hit policy, image name, image ID, name of the node hosting the image, private IP of the node, and public IP of the node.
Event type: Risky image interception, where the image contains certain vulnerabilities, Trojans, or sensitive information needs interception. Privileged image interception, where the image is intercepted when a container is started in privileged mode.
Executed action: Interception successful, indicating image startup interception events generated by effective interception policies. Alarm, indicating image startup alarm events generated by observation period policies.
Users can click **Details** in the action bar to view event details, including event details, hit policy, impact, risk description, and solution.
Event details: The system will aggregate the same interception or alarm events for the same image, with the aggregation time being the current day. This section shows the event type, number of events, and time period of interception or interception events.

©2013-2022 Tencent Cloud. All rights reserved.

Hit policy: Displays the name, type, startup status, policy status, interception start time, policy description, and policy interception content of effective interception policies or observation period policies. Users can click **Details** next to the policy name/policy type to view the policy details associated with this event.
Impact: Displays details of the targeted images requiring interception, including the image name, image ID, and the name and IP address of the node hosting the image.
Risk description: Displays the reasons behind the interception events or alarm events, such as interception due to the presence of critical vulnerabilities or hitting the interception policy. Additionally, it provides detailed parameters of the image startup process.
Solution: It is recommended that users repair images with vulnerabilities, Trojan viruses, or sensitive information to avoid impacting the business.

©2013-2022 Tencent Cloud. All rights reserved.

Cluster Risk Management
Cluster Check

Last updated：2024-01-23 15:44:44

The security check feature provides the security checklist, cluster risk statistics, security check details, and check item management. It allows installing the scanner for specified clusters, performing risk checks, and viewing cluster risk details.

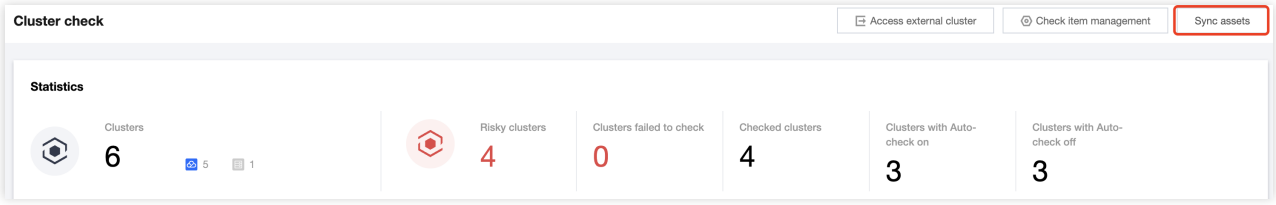
Installing the Scanner

1. Log in to the TCSS console and click **Cluster Risk Management** > **Security Check** on the left sidebar.
2. The **Security Check** page presets a scheduled cluster sync every hour. Click **Sync assets** to manually sync clusters.

Note:

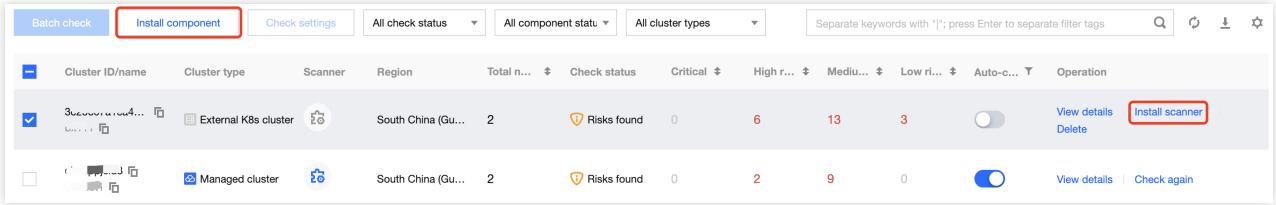
Currently, the security checklist applies to the sync of TKE managed and self-deployed clusters.

During your first use of cluster security, you need to manually "sync the assets" once, and the system will then automatically sync them.



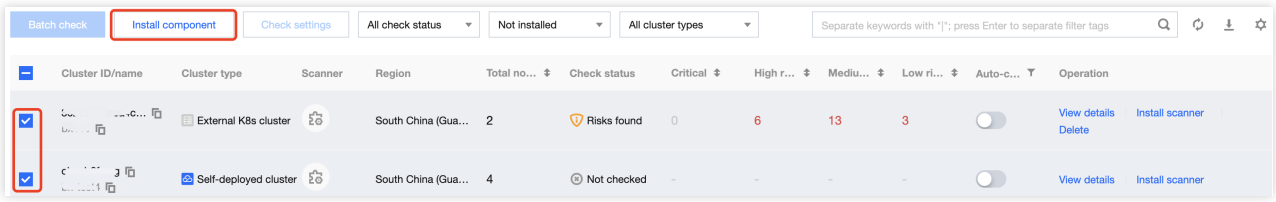
3. On the **Security Check** page, install the component for a single or multiple clusters.

Single: Select the target **Cluster ID** and click **Install scanner** or **Install component**.



Multiple: Select the target **Cluster IDs** and click **Install component**.

©2013-2022 Tencent Cloud. All rights reserved.



3. In the pop-up window, click **OK**.

4. After the confirmation, the system will deploy the DaemonSet component on all nodes in the cluster. The scanner will be in the **Running** status after the installation.

Note:

When the scanner is installed, the `cluster-security-defender` DaemonSet workload will be installed in the `kube-system` namespace of the cluster. To execute a cluster security check, make sure that the DaemonSet workload runs normally.

DaemonSet doesn't affect cluster running or performance. It is subject to the following resource limits:

CPU: 100–250 MB

MEM: 100–250 MiB

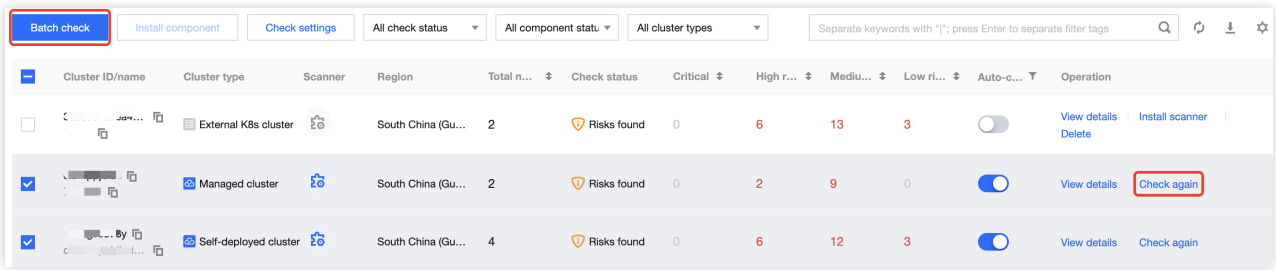
To delete the scanner, log in to the TKE console, click **Workload** on the **Cluster details** page, select **DaemonSet**, select **cluster-security-defender** in the `kube-system` namespace, and click **More** > **Delete** in the **Operation** column.

Performing a Security Check

On the **Security Check** page, the system will automatically perform a check after the scanner is installed successfully. You can specify a cluster and click **Check again**, or specify multiple clusters and click **Batch check**.

Note:

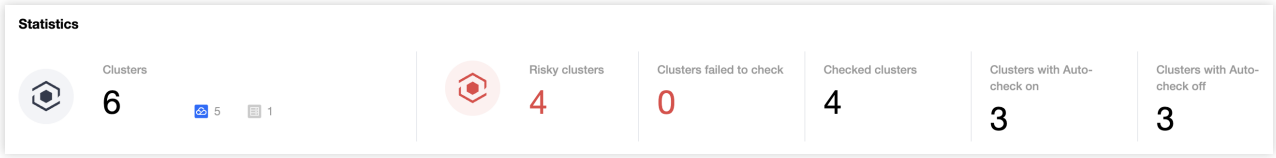
The scanner is not installed by default and needs to be installed before a scan is performed.



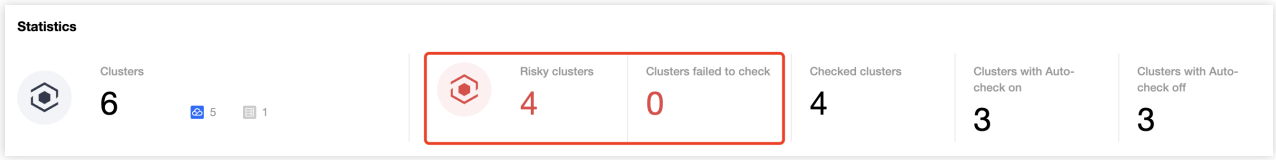
Viewing the Security Check Result

1. On the **Security Check** page, the **Statistics** card displays the total number of clusters and the numbers of clusters involving no risks and those not checked.

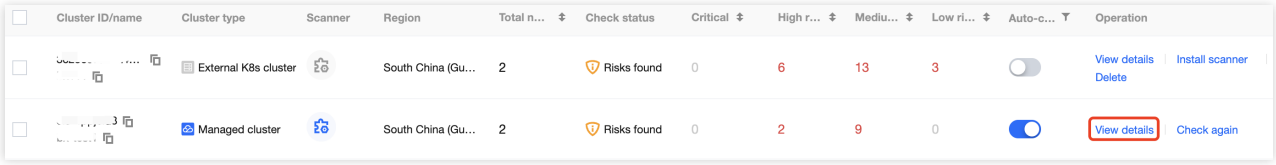
©2013-2022 Tencent Cloud. All rights reserved.



2. The **Cluster risks** card displays the numbers of risky clusters and clusters involving critical risks, high risks, medium risks, and low risks.

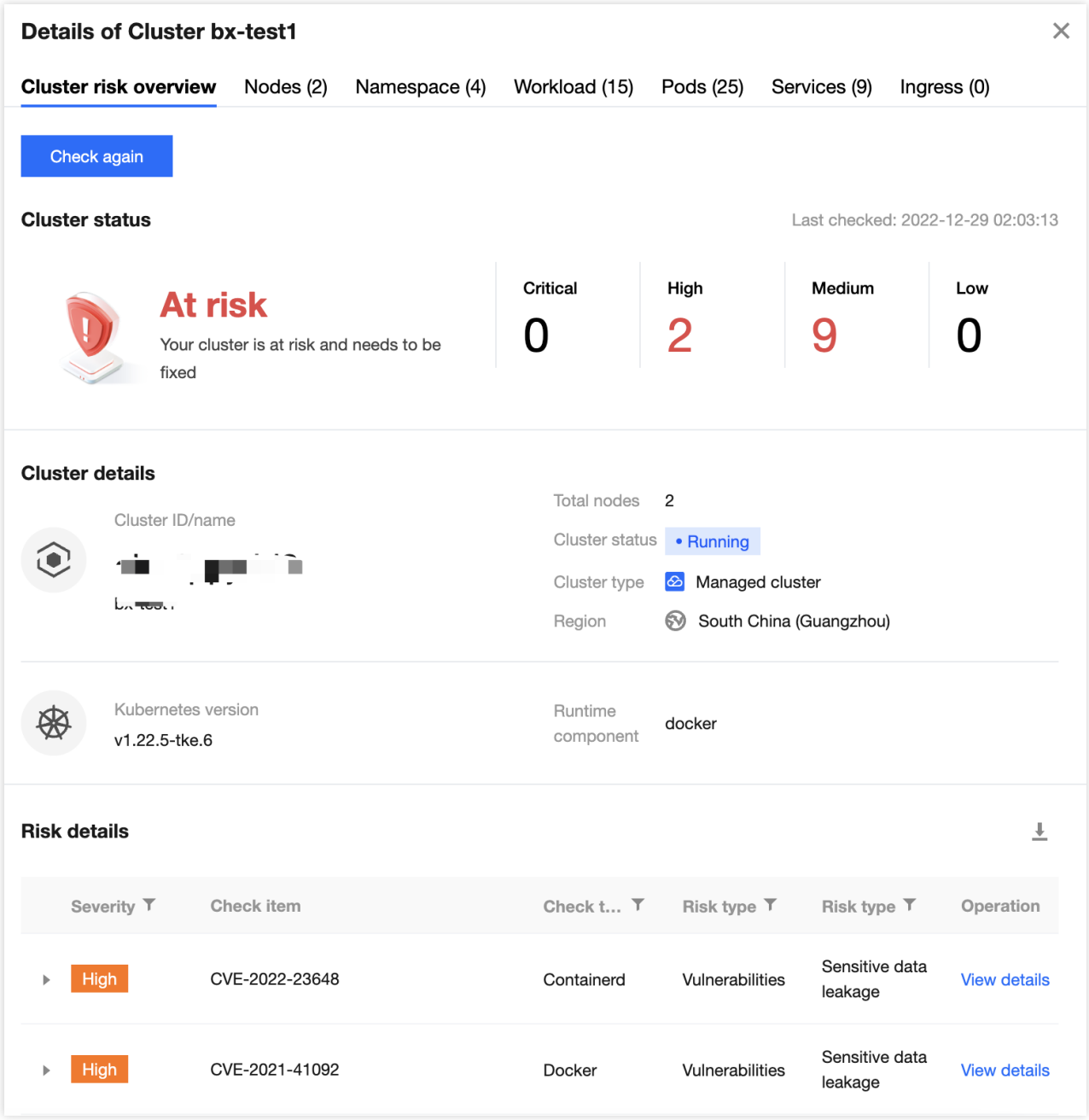


3. On the **Security Check** page, click **View details** in the **Operation** column of the cluster list to enter the **Cluster risk details** page.



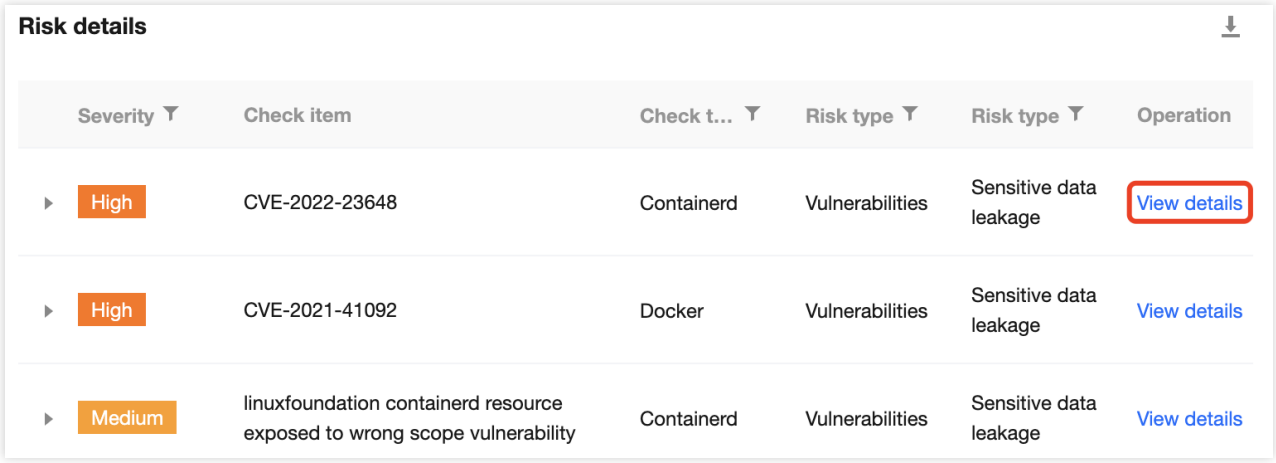
4. The **Cluster risk details** page displays all identified cluster risks, cluster details, and risk details of the current cluster.

©2013-2022 Tencent Cloud. All rights reserved.



5. On the risk details list, select the target check item and click **View details** to enter the **Risk check item details** page.

©2013-2022 Tencent Cloud. All rights reserved.



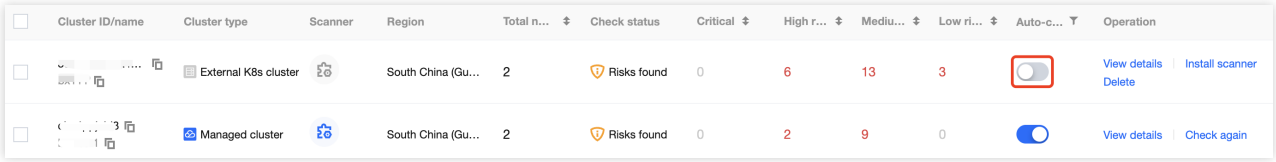
6. The **Risk check item details** page displays the risk details, description, solution, and affected assets in the current cluster.

Enabling Automatic Check

Enabling automatic check for a single cluster

1. On the **Security Check** page, select the target cluster and toggle on

.



2. In the pop-up window, click **OK**.

Note:

After the confirmation, automatic check will be enabled and performed as follows:

Nodes newly added to the cluster will be automatically checked.

The cluster will be checked across every midnight.

Enabling automatic check for multiple clusters

On the **Security Check** page, select multiple clusters and click **Batch check**.

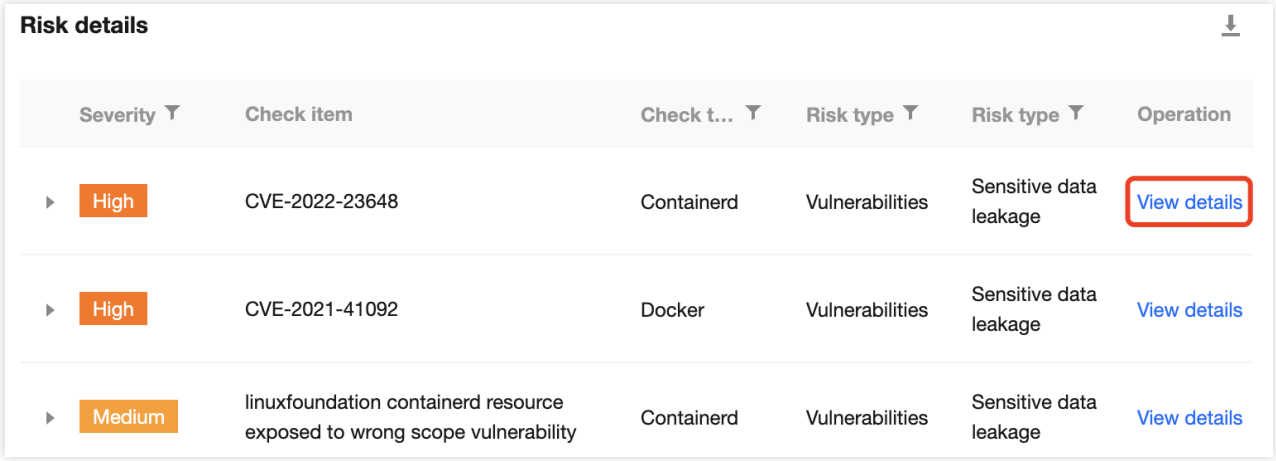
Note:

©2013-2022 Tencent Cloud. All rights reserved.

Automatic security check is disabled by default and can be enabled for the following check items:
Nodes newly added to the cluster will be automatically checked.
The cluster will be checked across every midnight.

Managing Security Check Items

1. On the **Security Check** page, click **Check item management** in the top-right corner.
2. On the check item settings page, the list of check items displays all check items of a security check performed by the system. Click **View details** to view the check item details.



©2013-2022 Tencent Cloud. All rights reserved.

Self-Built Cluster

Last updated：2024-08-13 17:22:21

This document describes how to access an external cluster for unified management and risk check.

Note：

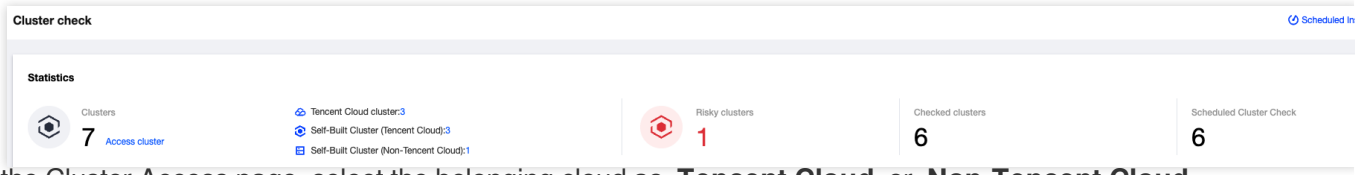
Supports Kubernetes (K8s) cluster versions 1.13 and later.

Limits

You can access an external cluster with up to 500 nodes.

Directions

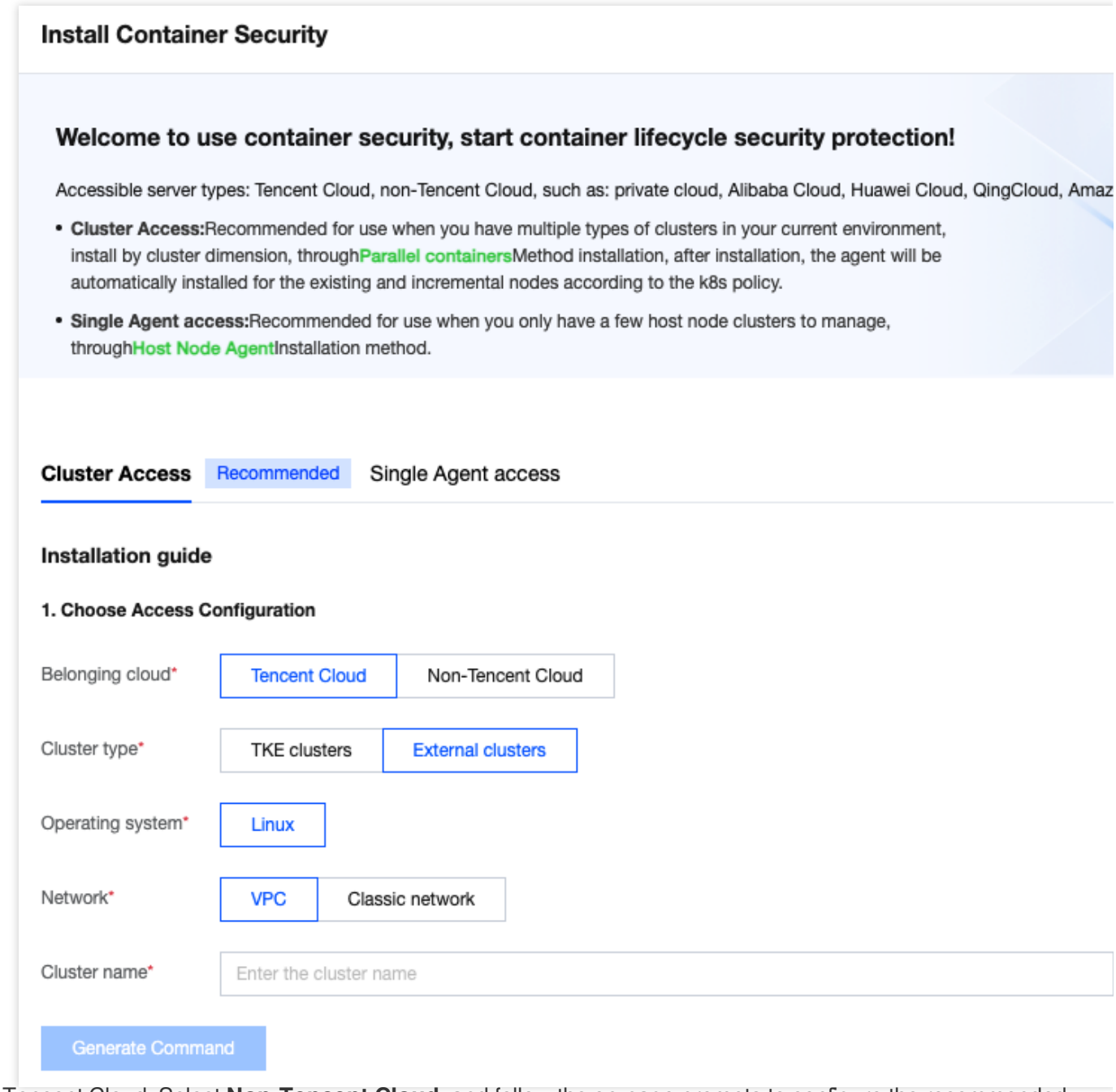
1. Log in to the TCSS console and click **Cluster Security** > **Security Check** on the left sidebar.
2. On the Security Check page, click **Access cluster**.



3. On the Cluster Access page, select the belonging cloud as **Tencent Cloud** or **Non-Tencent Cloud**.

Tencent Cloud: the CVM resources of a self-built cluster come from Tencent Cloud, follow the on-page prompts to select the recommended installation method and the cluster name.

©2013-2022 Tencent Cloud. All rights reserved.

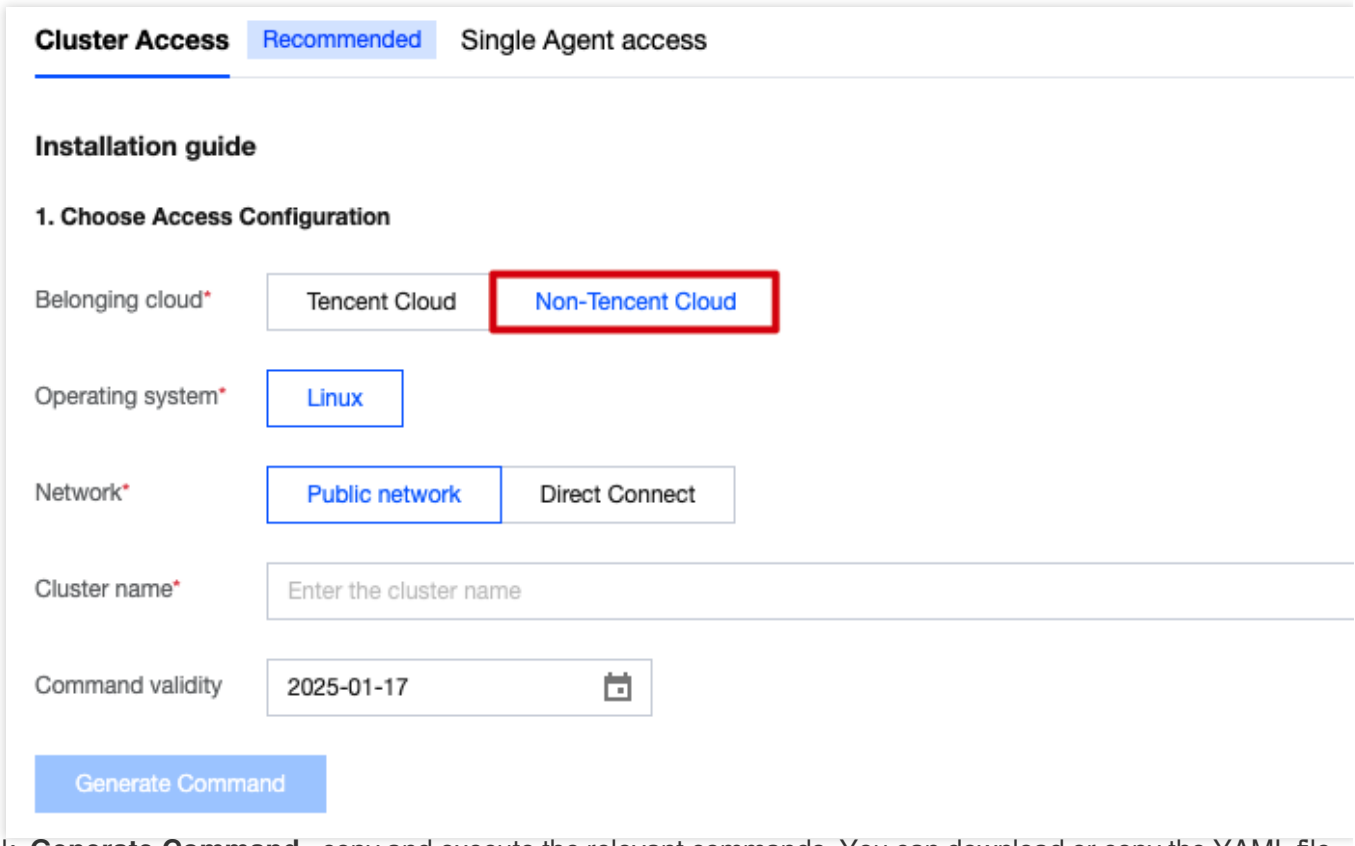


Non-Tencent Cloud: Select **Non-Tencent Cloud**, and follow the on-page prompts to configure the recommended scheme, cluster name, and command validity period.

Note：

The CVM resources of the connected cluster come from other clouds, including self-built clusters, standalone clusters, and managed clusters hosted by other clouds.

©2013-2022 Tencent Cloud. All rights reserved.



4. Click **Generate Command** , copy and execute the relevant commands. You can download or copy the YAML file content below and install it by the following two methods.

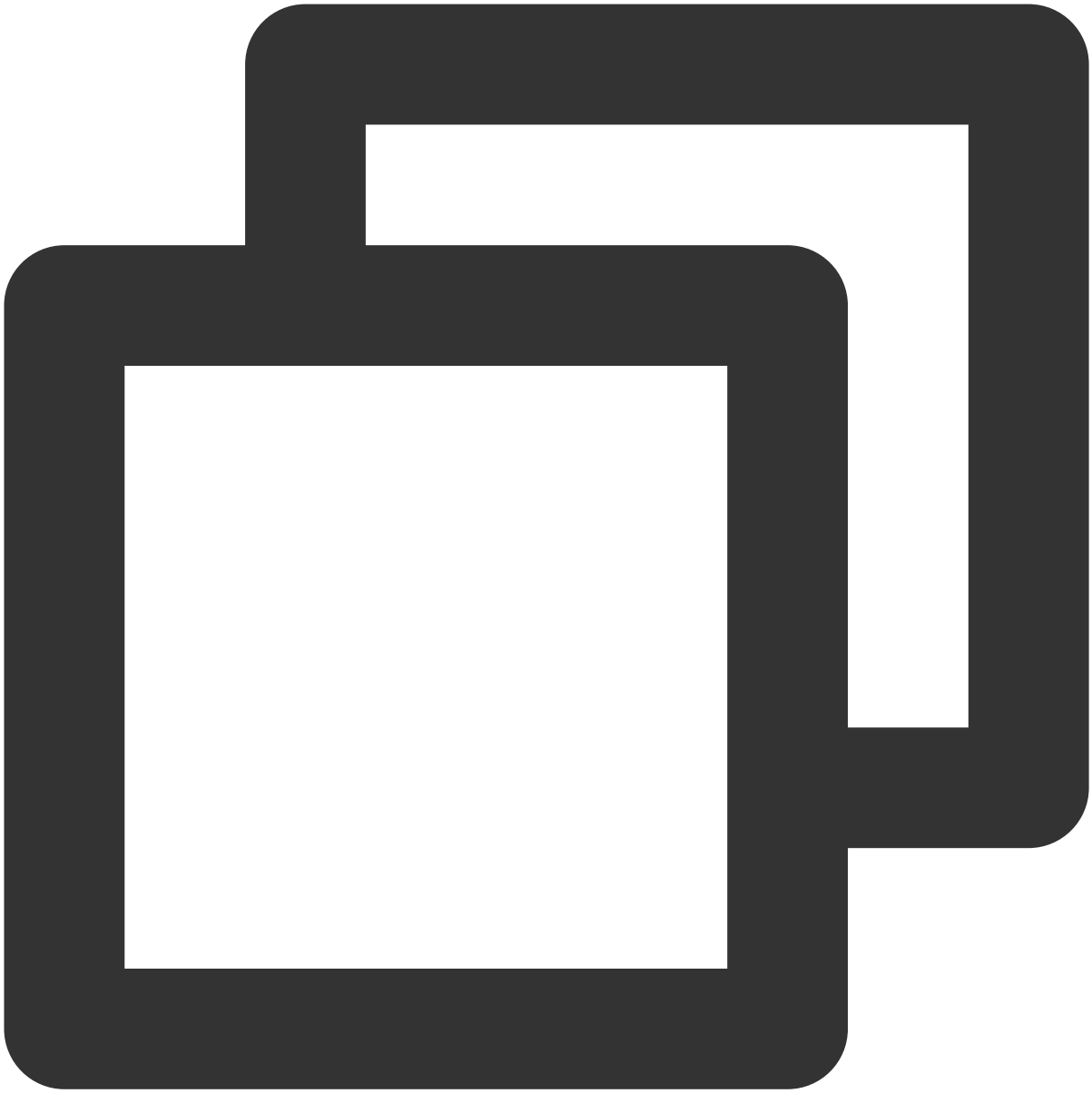
Note：

It is recommended that you generate a separate connection command for each cluster to avoid duplicate cluster names.

Method 1: Click **Copy Command Link** , then paste and execute the command on a machine capable of running k8s commands. Alternatively, you may first download the YAML file below, copy it to the machine, and execute `kubectl apply -f tcss.yaml` .

Method 2: Go to the TKE console - cluster details page, and use the Create Resources with YAML File option to copy the command content.

©2013-2022 Tencent Cloud. All rights reserved.



```
---
apiVersion: v1
kind: Namespace
metadata:
name: tcss

---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
namespace: tcss
```

©2013-2022 Tencent Cloud. All rights reserved.

```
name: tcss-admin
rules:
- apiGroups: ["extensions", "apps", ""]
resources: ["*"]
verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]

---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
name: tcss-admin-rb
namespace: tcss
subjects:
- kind: ServiceAccount
name: tcss-agent
namespace: tcss
apiGroup: ""
roleRef:
kind: Role
name: tcss-admin
apiGroup: rbac.authorization.k8s.io


---
apiVersion: v1
kind: ServiceAccount
metadata:
name: tcss-agent
namespace: tcss

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
name: security-clusterrole
rules:
- apiGroups: ["", "v1"]
resources: ["namespaces", "pods", "nodes", "services", "serviceaccounts", "configma
verbs: ["get", "list", "watch"]
- apiGroups: ["apps","batch","extensions","rbac.authorization.k8s.io","networking.k
resources: ["*"]
verbs: ["get", "list","watch"]
- apiGroups: ["networking.k8s.io"]
resources: ["networkpolicies"]
verbs: ["get", "list", "watch", "create", "update", "patch", "delete"]
- apiGroups: ["apiextensions.k8s.io"]
resources: ["customresourcedefinitions"]
```

©2013-2022 Tencent Cloud. All rights reserved.

```
verbs: ["list", "get","create"]
- apiGroups: ["apiextensions.k8s.io"]
resourceNames: ["tracingpolicies.cilium.io", "tracingpoliciesnamespaced.cilium.io"]
resources: ["customresourcedefinitions"]
verbs: ["list", "get", "update"]

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
name: security-clusterrolebinding
roleRef:
apiGroup: rbac.authorization.k8s.io
kind: ClusterRole
name: security-clusterrole
subjects:
- kind: ServiceAccount
name: tcss-agent
namespace: tcss
- kind: User
name: tcss
apiGroup: rbac.authorization.k8s.io


---
apiVersion: v1
kind: Secret
metadata:
name: tcss-agent-secret
namespace: tcss
annotations:
kubernetes.io/service-account.name: tcss-agent
type: kubernetes.io/service-account-token


---
apiVersion: batch/v1
kind: Job
metadata:
name: init-tcss-agent
namespace: tcss
spec:
template:
spec:
serviceAccountName: tcss-agent
containers:
- image: ccr.ccs.tencentyun.com/yunjing_agent/agent:latest
```

©2013-2022 Tencent Cloud. All rights reserved.

```
imagePullPolicy: Always
name: init-tcss-agent
command: ["/home/work/yunjing-agent"]
args: ["-token","","-vip","",'-cc']
resources:
limits:
cpu: 100m
memory: 512Mi
requests:
cpu: 100m
memory: 128Mi
env:
- name: user_tags
value: "default"
- name: k8s_name
value: "11"
- name: appid
value: "1256299843"
securityContext:
privileged: true
volumeMounts:
- mountPath: /run/secrets/kubernetes.io/tcss-agent
name: token-projection
securityContext: {}
hostPID: true
restartPolicy: Never
volumes:
- name: token-projection
secret:
secretName: tcss-agent-secret
backoffLimit: 5

---
apiVersion: apps/v1
kind: DaemonSet
metadata:
labels:
k8s-app: yunjing-agent
name: yunjing-agent
namespace: kube-system
annotations:
config.kubernetes.io/depends-on: batch/v1/namespaces/tcss/jobs/init-tcss-secrets
spec:
selector:
matchLabels:
k8s-app: yunjing-agent
template:
```

©2013-2022 Tencent Cloud. All rights reserved.

```
metadata:
annotations:
eks.tke.cloud.tencent.com/ds-injection: "true"
labels:
k8s-app: yunjing-agent
spec:
tolerations:
- operator: Exists
containers:
- image: ccr.ccs.tencentyun.com/yunjing_agent/agent:latest
imagePullPolicy: Always
name: yunjing-agent
command: ["/home/work/yunjing-agent"]
args: ["-d","-token",'',"-vip",'']
resources:
limits:
cpu: 250m
memory: 512Mi
requests:
cpu: 100m
memory: 128Mi
securityContext:
privileged: true
terminationMessagePath: /dev/termination-log
terminationMessagePolicy: File
dnsPolicy: ClusterFirst
restartPolicy: Always
schedulerName: default-scheduler
securityContext: {}
terminationGracePeriodSeconds: 30
hostNetwork: true
hostPID: true


---
apiVersion: apps/v1
kind: Deployment
metadata:
labels:
k8s-app: tcss-asset
name: tcss-asset
namespace: tcss
spec:
selector:
matchLabels:
k8s-app: tcss-asset
replicas: 1
```

©2013-2022 Tencent Cloud. All rights reserved.

```
template:
metadata:
labels:
k8s-app: tcss-asset
annotations:
eks.tke.cloud.tencent.com/ds-injection: "true"
spec:
serviceAccountName: tcss-agent
tolerations:
- operator: Exists
containers:
- image: ccr.ccs.tencentyun.com/yunjing_agent/agent:latest
imagePullPolicy: Always
name: tcss-asset
command: ["/home/work/yunjing-agent"]
args: ["-asset"]
resources:
limits:
cpu: 100m
memory: 256Mi
requests:
cpu: 50m
memory: 64Mi
securityContext:
privileged: true
terminationMessagePath: /dev/termination-log
terminationMessagePolicy: File
dnsPolicy: ClusterFirst
restartPolicy: Always
schedulerName: default-scheduler
securityContext: {}
terminationGracePeriodSeconds: 30
hostPID: true
```

5. After installation, check if it is successful. Upon the cluster's connection, a namespace named tcss will be created within the cluster, along with the creation of the following workload resources. Ensure that the following three workloads are running properly:

Install a Job-type workload named init-tcss-agent under the tcss namespace.

Install a Deployment-type workload named tcss-asset under the tcss namespace.

Install a DaemonSet-type workload named yunjing-agent under the kube-system namespace.

5.1 Check if the Job workload is deployed successfully.

To check if the Job is created successfully, run the command: `kubectl get jobs -n tcss` .

©2013-2022 Tencent Cloud. All rights reserved.

```
[root@VM-0-17-tencentos ~]# kubectl get jobs -n tcss
NAME              COMPLETIONS   DURATION   AGE
init-tcss-agent   1/1           8s         9m27s
[root@VM-0-17-tencentos ~]#
```

To check if the Job is deployed successfully, run the command: `kubectl get pods -n tcss | grep init-tcss-agent` .

```
[root@VM-0-17-tencentos ~]# kubectl get pods -n tcss | grep init-tcss-ag
init-tcss-agent-8jpkp          0/1     Completed   0          7m17s
[root@VM-0-17-tencentos ~]#
```

5.2 Check if the DaemonSet is deployed successfully.

To check if the DaemonSet is created successfully, run the command: `kubectl get daemonset -A -l k8s-app=yunjing-agent` .

```
[root@VM-0-17-tencentos ~]# kubectl get daemonset -A -l k8s-app=yunjing-agent
NAMESPACE     NAME             DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE
kube-system   yunjing-agent    1         1         1       1            1
[root@VM-0-17-tencentos ~]#
```

To check if the DaemonSet is deployed successfully, run the command: `kubectl get pods -A -l k8s-app=yunjing-agent` .

```
[root@VM-0-17-tencentos ~]# kubectl get pods -A -l k8s-app=yunjing-agent
NAMESPACE     NAME                   READY   STATUS    RESTARTS   AGE
kube-system   yunjing-agent-bl4w7    1/1     Running   0          30d
[root@VM-0-17-tencentos ~]#
```

5.3 Check if the Deployment workload is deployed successfully.

To check if the Deployment is created successfully, run the command: `kubectl get deployment -n tcss`

```
[root@VM-0-17-tencentos ~]# kubectl get deployment -n tcss
NAME         READY   UP-TO-DATE   AVAILABLE   AGE
tcss-asset   1/1     1            1           15m
[root@VM-0-17-tencentos ~]#
```

To check if the Deployment is deployed successfully, run the command: `kubectl get pods -n tcss | grep tcss-asset`

```
[root@VM-0-17-tencentos ~]# kubectl get pods -n tcss | grep tcss-asset
tcss-asset-79c5c77756-zc5x8   1/1     Running   0          16m
[root@VM-0-17-tencentos ~]#
```

©2013-2022 Tencent Cloud. All rights reserved.

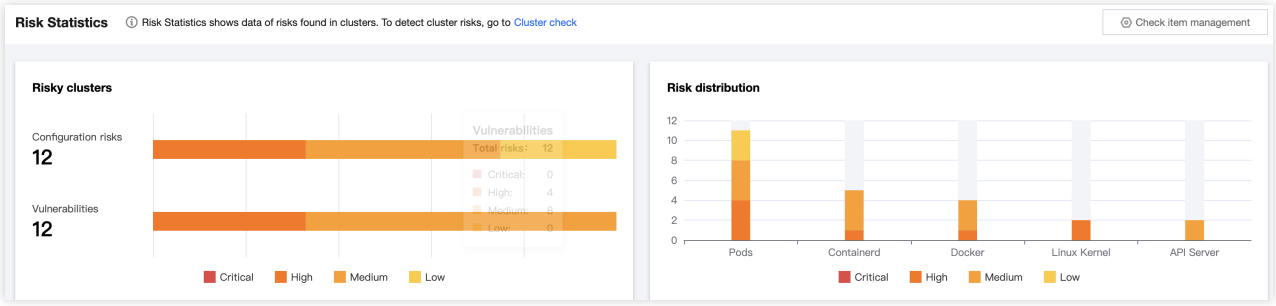
Risk Analysis

Last updated：2024-01-23 15:44:43

The risk statistics feature displays the risk statistics of all checked clusters, including the trend of risky nodes and the information of risk items.

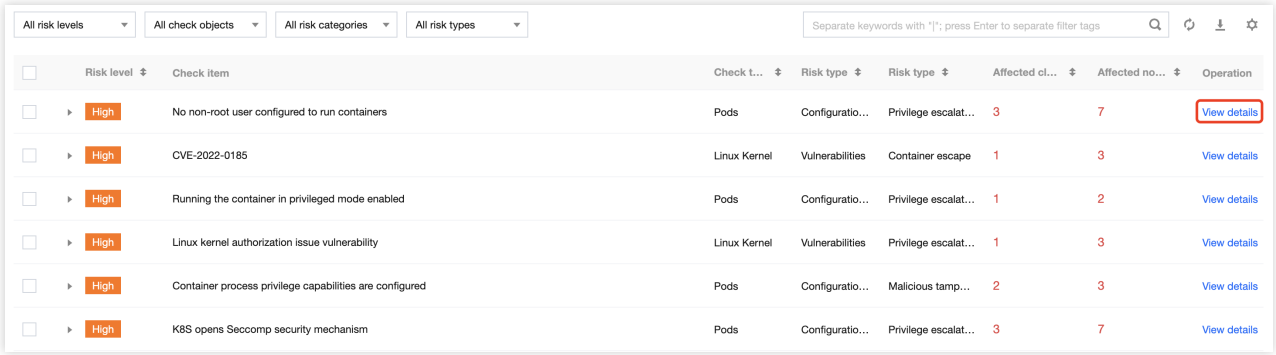
Viewing the statistics of risky nodes

1. Log in to the TCSS console and click **Cluster Risk Management** > **Risk Statistics** on the left sidebar.
2. The risky node statistics card displays the number of risky nodes identified during the security check and the trend in the past seven days, including the numbers and trends of nodes involving critical risks, high risks, medium risks, and low risks.



Viewing the information of risk items

On the **Risk Statistics** page, the list of risk items displays all risk items identified during the security check. The information of risk items includes the risk level, check item information, check target, risk category, risk type, number of affected clusters, and number of affected nodes. Click **View details** to pop up the risk item details window, which displays the risk details, description, solution, and impact.



©2013-2022 Tencent Cloud. All rights reserved.

Baseline Management Overview

Last updated：2024-01-23 15:44:44

The security baseline combines CIS Benchmarks and Yunding Lab's best baseline configuration practices for containers, images, servers, and Kubernetes assets, displays multidimensional baseline compliance of container assets, and helps set up optimal baseline configurations in the container running environment to reduce the attack surface.

©2013-2022 Tencent Cloud. All rights reserved.

Container

Last updated：2024-01-23 15:44:44

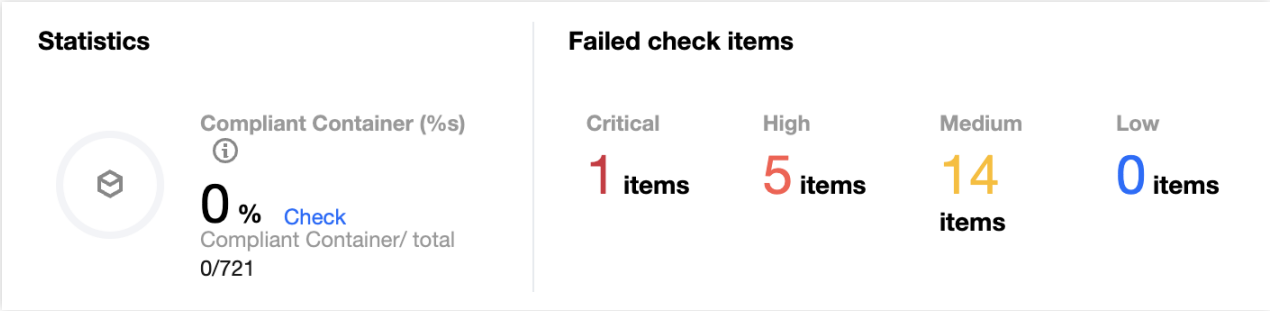
The **Container** page displays the baseline compliance details of containers, including statistics, check information, and the list of check results.

Viewing the Container Overview

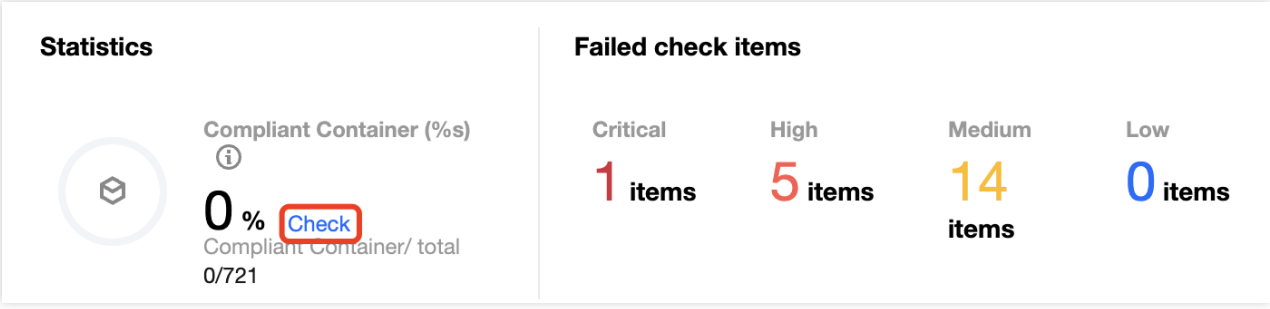
1. Log in to the TCSS console and click **Baseline Management** > **Container** on the left sidebar.
2. On the **Container** page, the **Statistics** window displays the percentage of compliant containers and the numbers of check items at the critical, high, medium, and low severity levels.

Note:

The percentage of compliant containers is calculated as the number of compliant containers/the total number of containers (including those that failed the check).

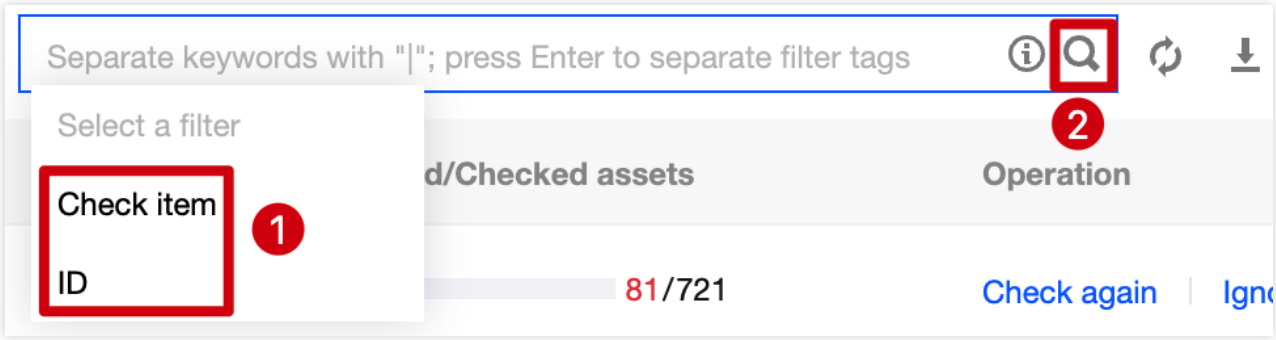


3. On the **Container** page, click **View** next to the proportion to pop up the container drawer, which displays the list of check results.



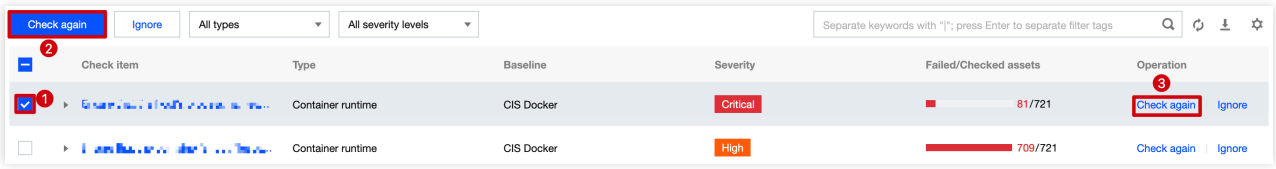
©2013-2022 Tencent Cloud. All rights reserved.

4. In the container drawer, click the search box and search for container check results by check item or ID.

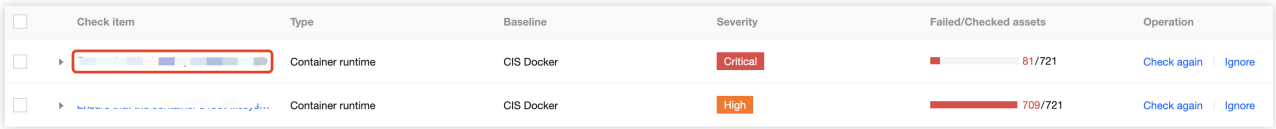


5. In the container drawer, click

to select the target container check item and click **Check again** > **OK** to check it again.



6. In the container drawer, click a check item to view the check results of a specified container.

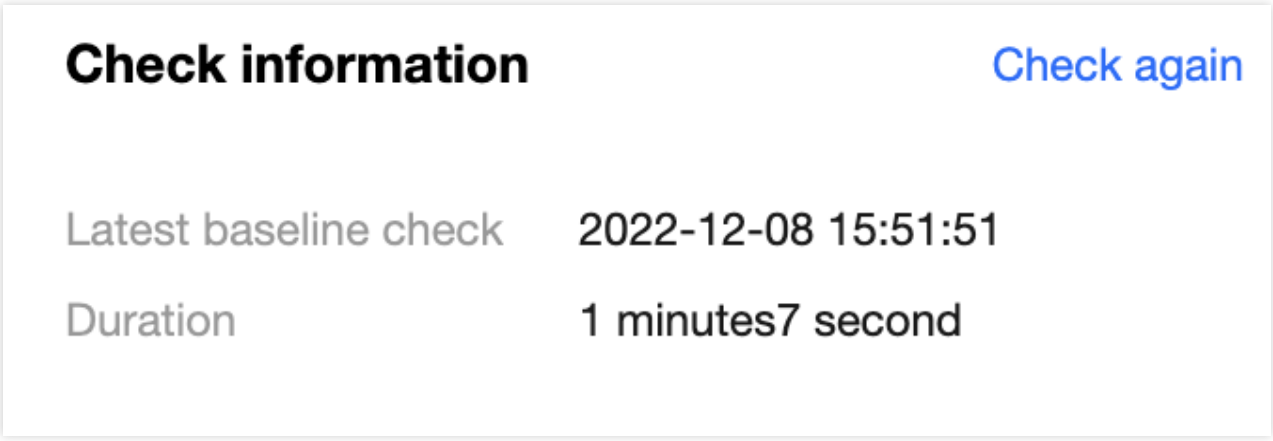


Viewing the Check Information

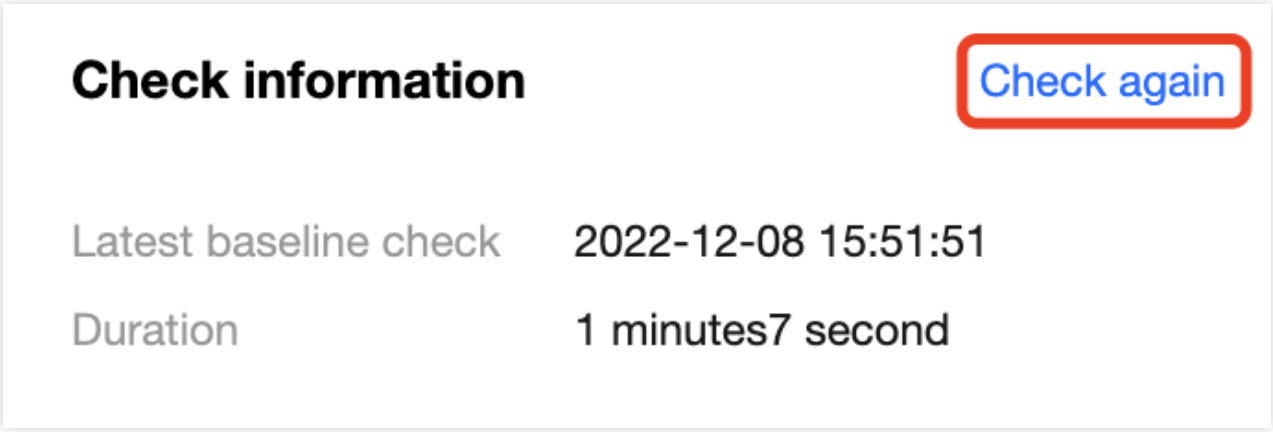
1. Log in to the TCSS console and click **Baseline Management** > **Container** on the left sidebar.

©2013-2022 Tencent Cloud. All rights reserved.

2. On the **Container** page, the **Check information** window displays the last baseline check time, check duration, and configured automatic check schedule.

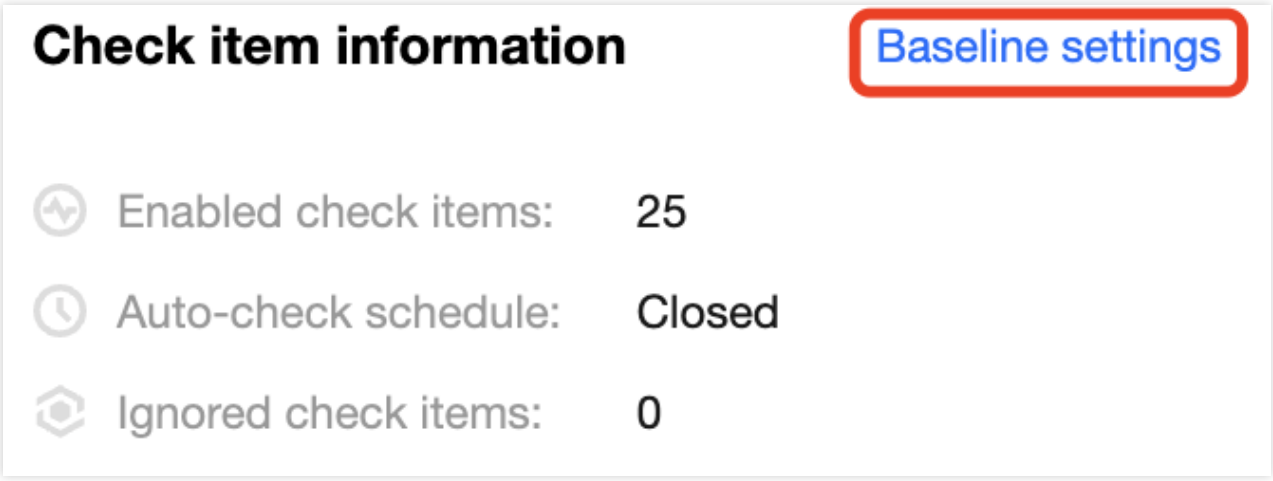


3. On the **Container** page, click **Check again** to perform a baseline check on the container.



4. On the **Container** page, click **Baseline settings** to set the baseline policy and baseline ignored list.

©2013-2022 Tencent Cloud. All rights reserved.

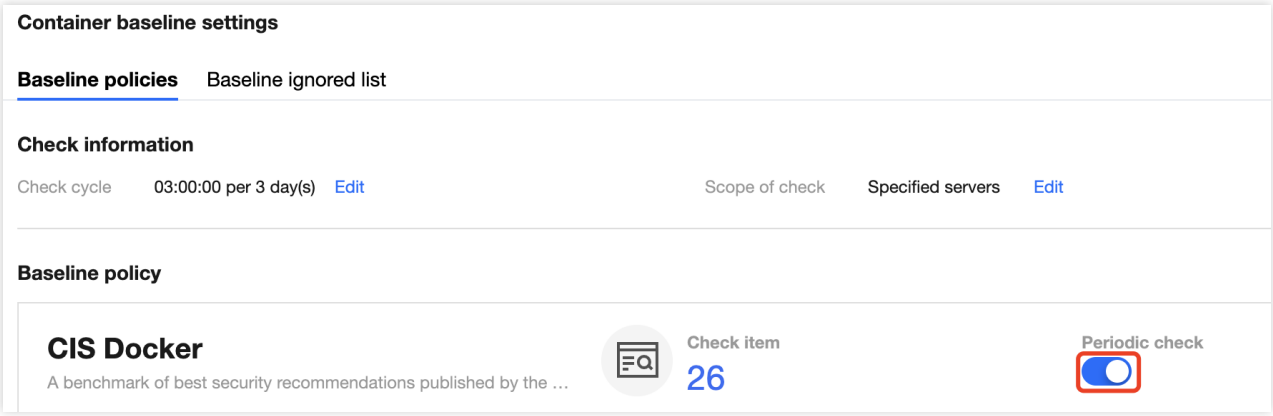


Setting the baseline policy

The **Baseline policies** tab displays the baseline for the current asset check and the number of check items.

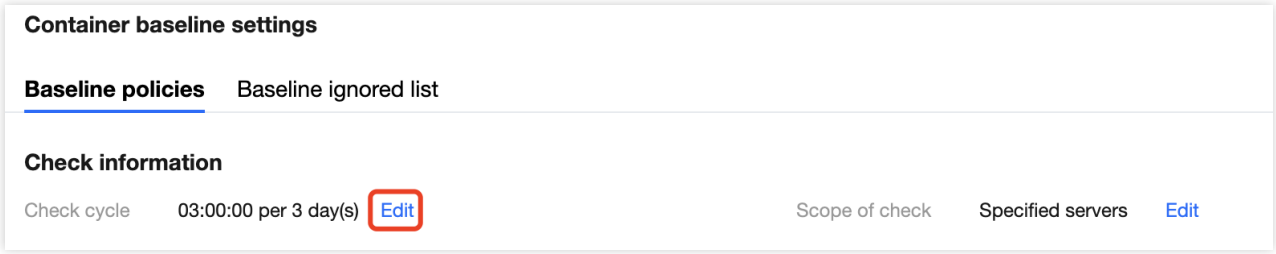
1. On the **Baseline policies** tab, toggle on or off

to enable or disable the periodic check against the current baseline.

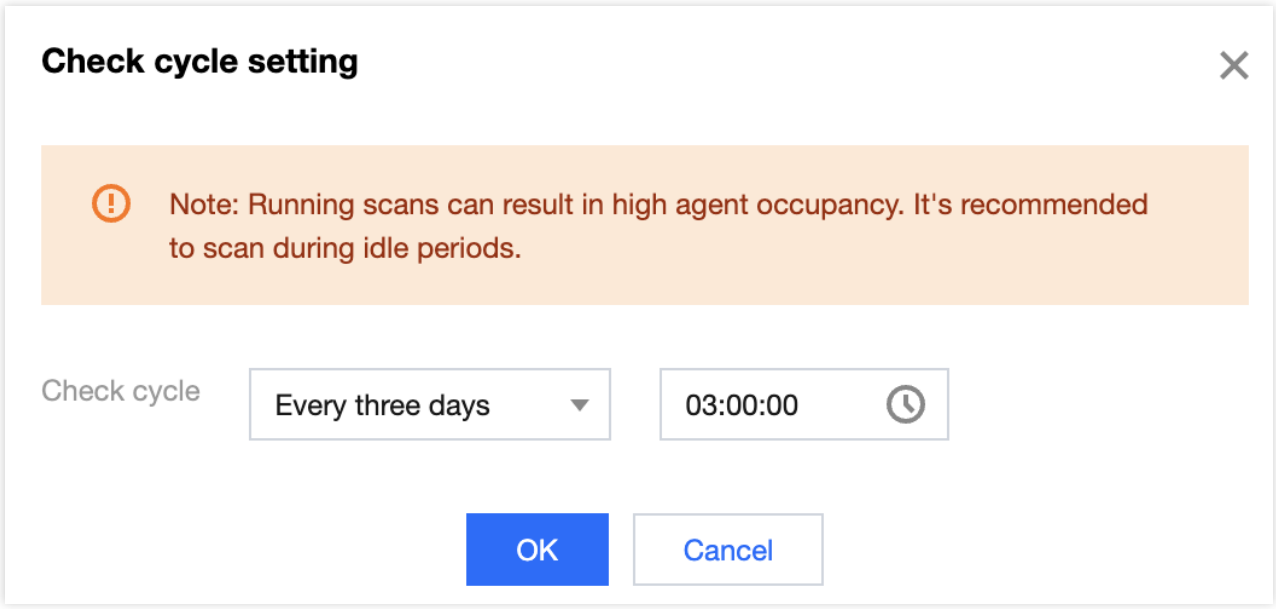


2. On the **Baseline policies** tab, click **Check cycle settings**.

©2013-2022 Tencent Cloud. All rights reserved.



3. In the pop-up window, set the check cycle to every day, every 3 days, every 7 days, or a specified time range.



4. Click **OK**.

Baseline ignored list

The **Baseline ignored list** tab displays the ignored check items of the container.

1. On the **Baseline ignored list** tab, click the search box and search for container check items by check item.

©2013-2022 Tencent Cloud. All rights reserved.

2. On the **Baseline ignored list** tab, click

to select the target check item and click **Unignore** to unignore it.

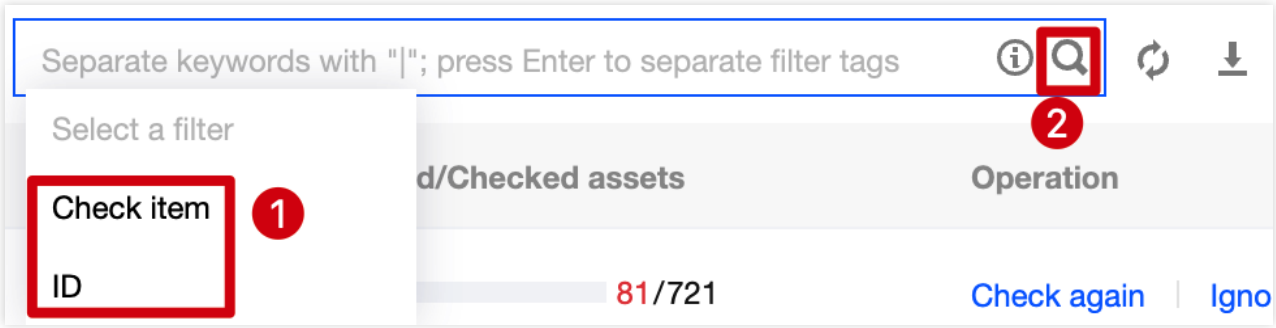
Note:

After a check item is unignored, it will be considered as normal.

Viewing the List of Check Results

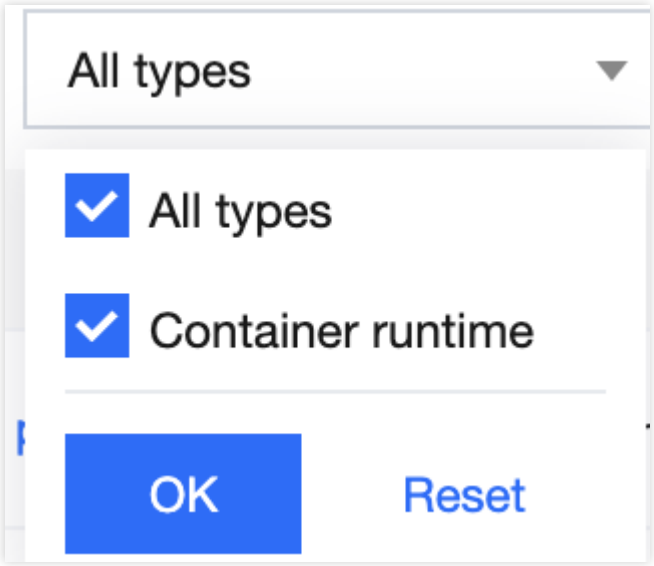
Filtering and refreshing check items

1. Log in to the TCSS console and click **Baseline Management** > **Container** on the left sidebar.
2. On the **Container** page, click the search box and search for check items by container check item or ID.

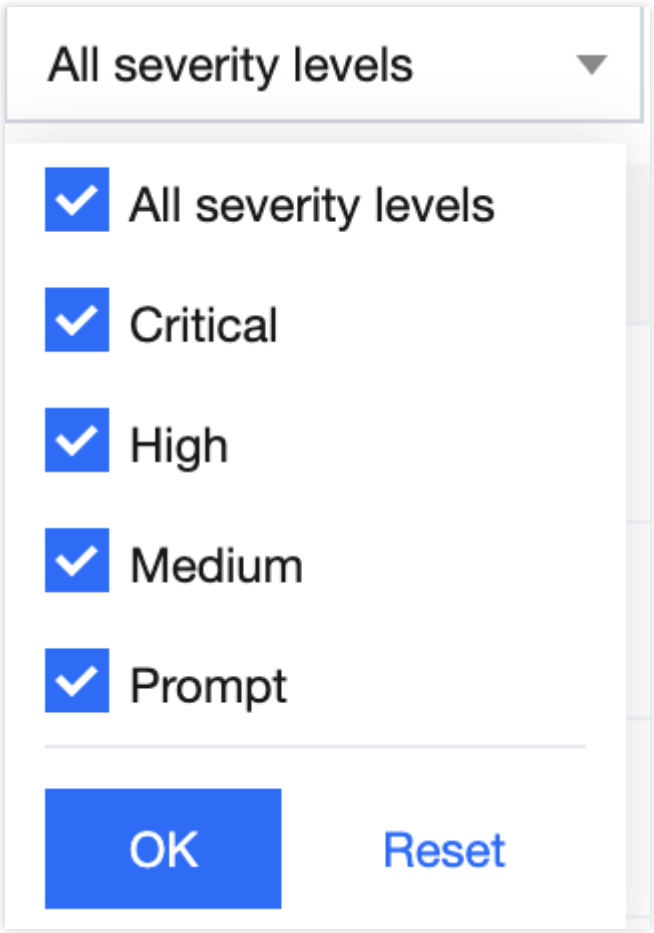


3. On the **Container** page, click the type drop-down list in the top-left corner and filter container check items by type.

©2013-2022 Tencent Cloud. All rights reserved.



4. On the **Container** page, click the severity drop-down list in the top-left corner and filter container check items by severity.



5. On the **Container** page, click

©2013-2022 Tencent Cloud. All rights reserved.

on the right of the **Operation** column to refresh the container check items.

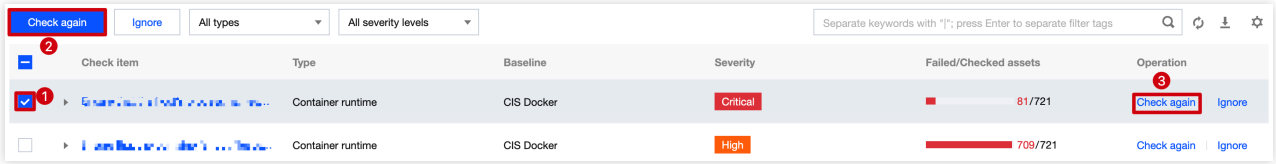
Checking a check item again

1. Log in to the TCSS console and click **Baseline Management** > **Container** on the left sidebar.
2. On the **Container** page, click

to select the target container check item and click **Check again** > **OK** to check it again.

Note:

You can batch check container check items again by selecting them and clicking **Check again** next to ②.



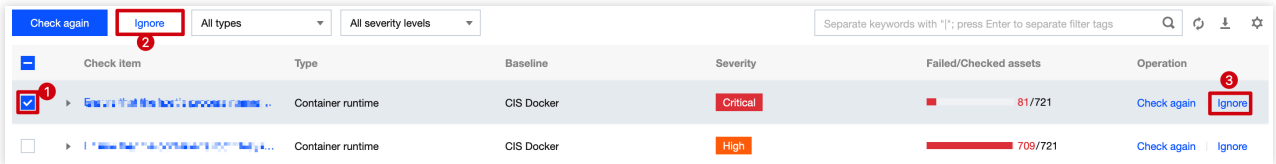
Ignoring a check item

1. Log in to the TCSS console and click **Baseline Management** > **Container** on the left sidebar.
2. On the **Container** page, click

to select the target check item and click **Ignore** > **OK** to ignore it.

Note:

You can batch ignore check items by selecting them and clicking **Ignore** next to ②.



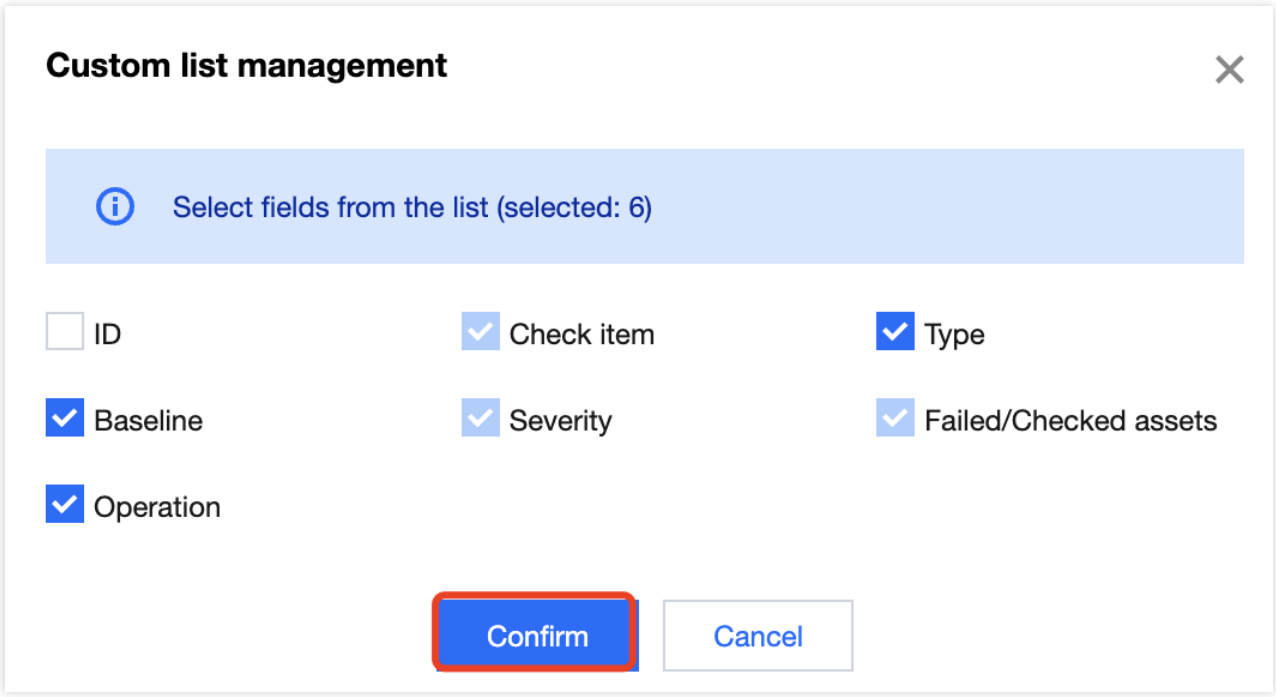
©2013-2022 Tencent Cloud. All rights reserved.

Custom list management

1. Log in to the TCSS console and click **Baseline Management** > **Container** on the left sidebar.
2. On the **Container** page, click

to pop up the **Custom List Management** window.

3. In the pop-up window, select the target type and click **OK**.



Key fields in the list

1. Check item: Click a check item to view the details.
1. Failed check items: Number of failed check items.
2. Result: **Failed** if there are failed check items or **Passed** if all items are passed.
3. Last checked: The time of the last check.

©2013-2022 Tencent Cloud. All rights reserved.

Image

Last updated：2024-01-23 15:44:44

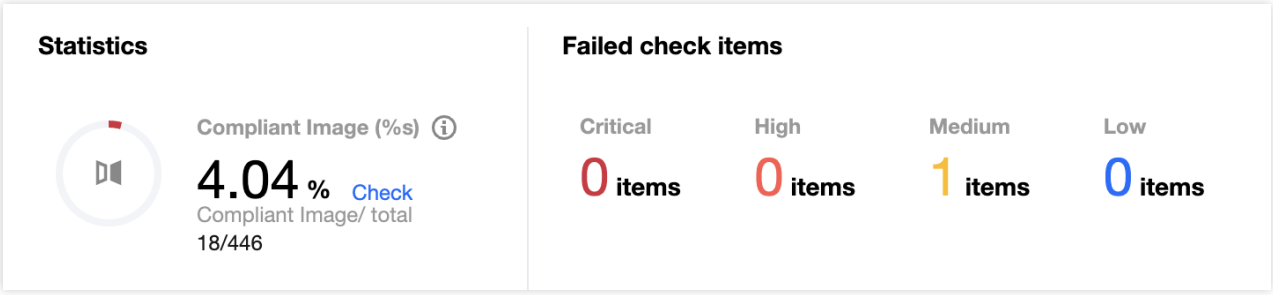
The **Image** page displays the baseline compliance details of images, including statistics, check information, and the list of check results.

Viewing the Image Overview

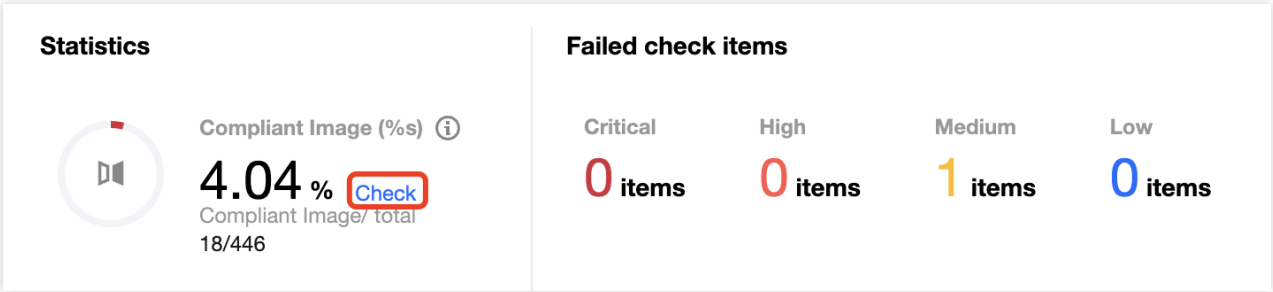
1. Log in to the TCSS console and click **Baseline Management** > **Image** on the left sidebar.
2. On the **Image** page, the **Statistics** window displays the percentage of compliant images and the numbers of check items at the critical, high, medium, and low severity levels.

Note:

The percentage of compliant images is calculated as the number of compliant images/the total number of images (including those that failed the check).



3. On the **Image** page, click **View** next to the proportion to pop up the image drawer, which displays the list of check results.



4. In the image drawer, click the search box and search for image check results by check item or ID.

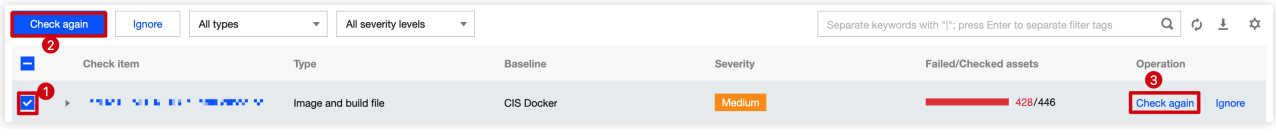
©2013-2022 Tencent Cloud. All rights reserved.

5. In the image drawer, click

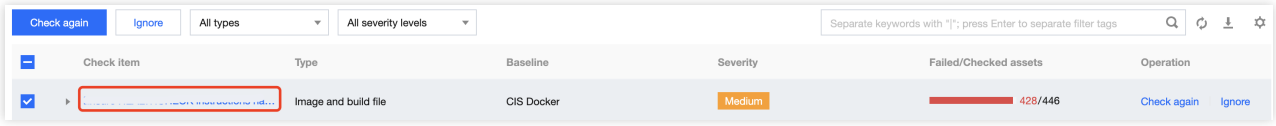
to select the target check item and click **Check again** > **OK** to check it again.

Note:

You can batch check image check items again by selecting them and clicking **Check again** next to ②.



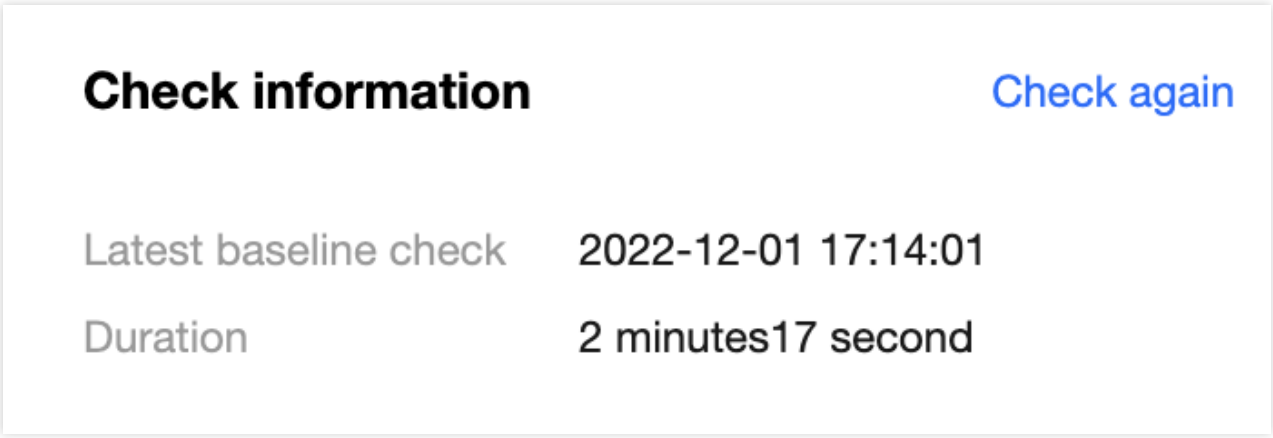
6. In the image drawer, click a check item to view the check results of a specified image.



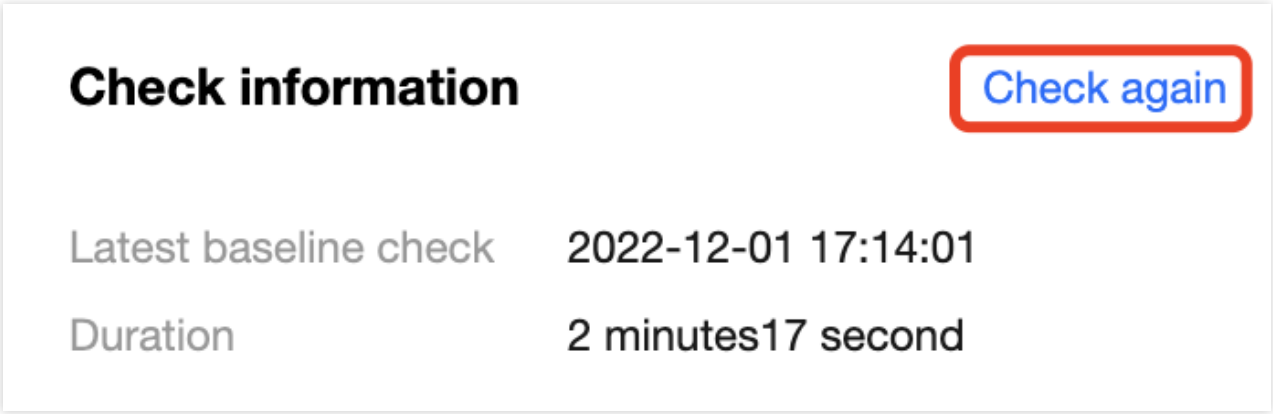
Viewing the Check Information

1. Log in to the TCSS console and click **Baseline Management** > **Image** on the left sidebar.
2. On the **Image** page, the **Check information** window displays the last baseline check time, check duration, and configured automatic check schedule.

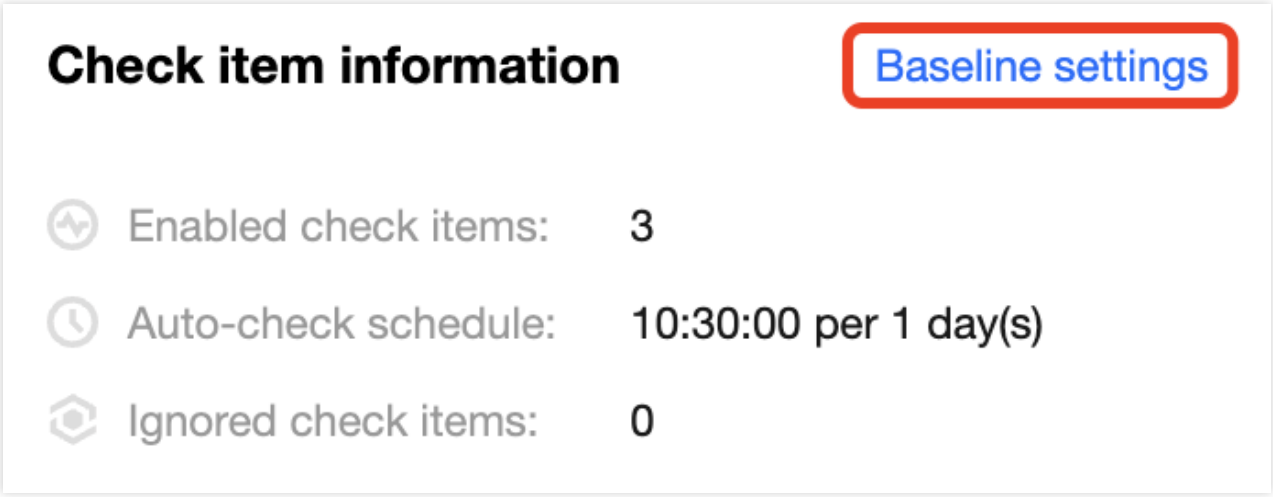
©2013-2022 Tencent Cloud. All rights reserved.



3. On the **Image** page, click **Check again** to perform a baseline check on the image.



4. On the **Image** page, click **Baseline settings** to set the baseline policy and baseline ignored list.



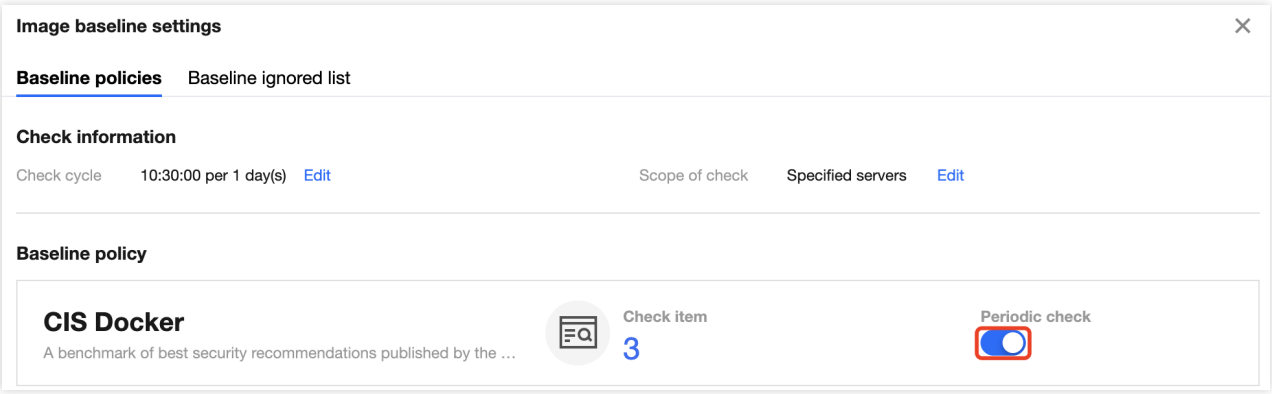
Setting the baseline policy

©2013-2022 Tencent Cloud. All rights reserved.

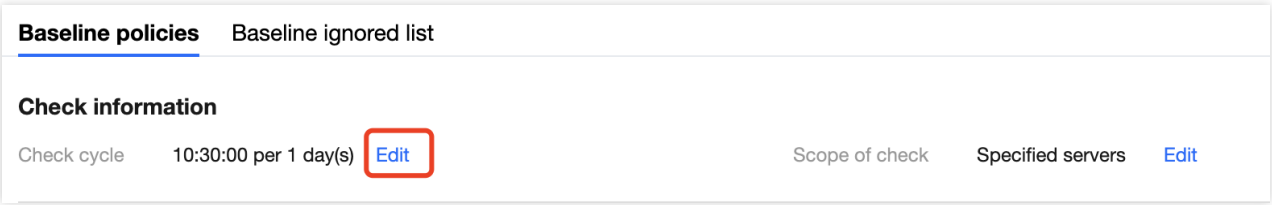
The **Baseline policies** tab displays the baseline for the current asset check and the number of check items.

1. On the **Baseline policies** tab, toggle on or off

to enable or disable the periodic check against the current baseline.

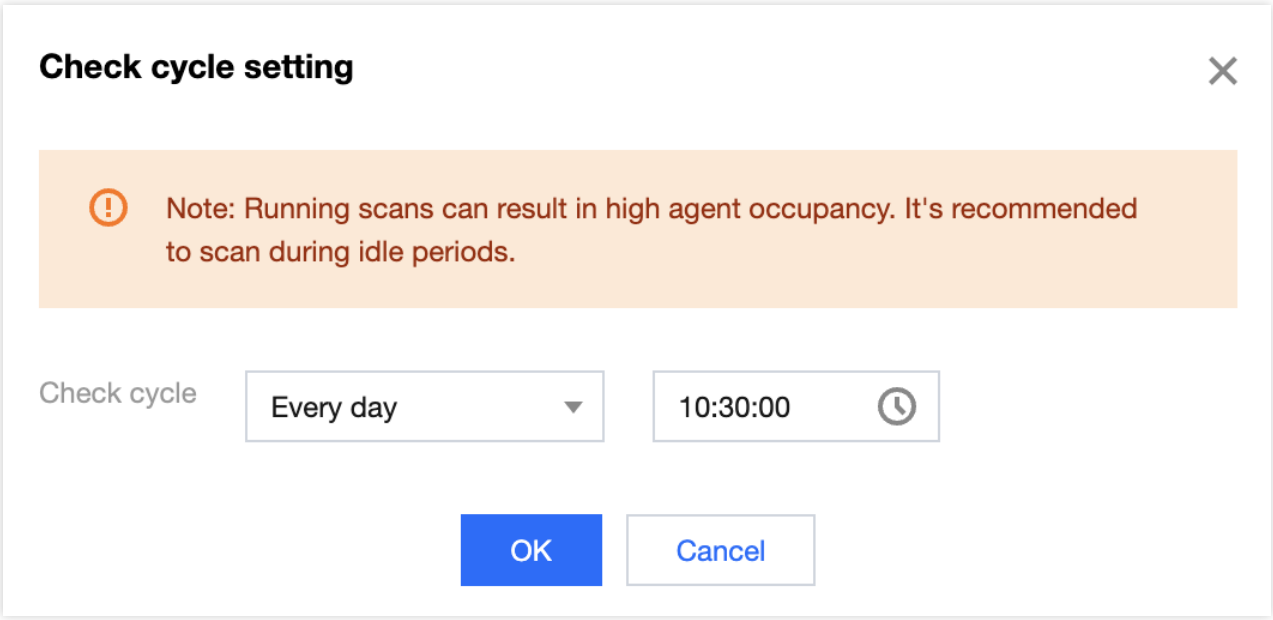


2. On the **Baseline policies** tab, click **Check cycle settings**.



3. In the pop-up window, set the check cycle to every day, every 3 days, every 7 days, or a specified time range.

©2013-2022 Tencent Cloud. All rights reserved.

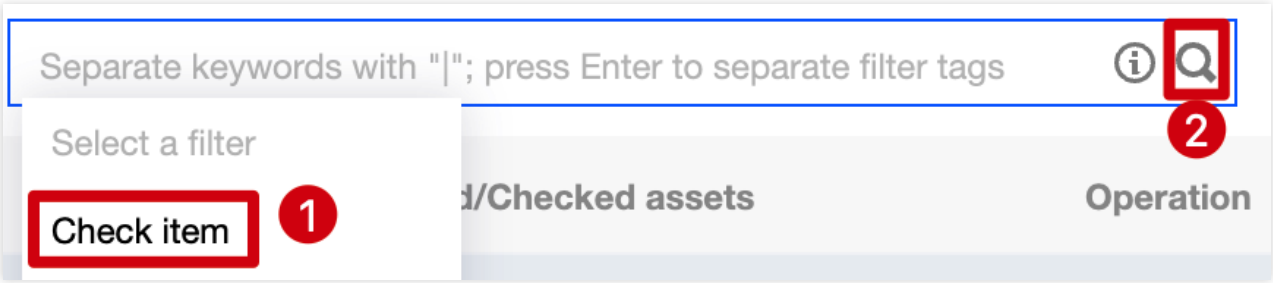


4. Click **OK**.

Baseline ignored list

The **Baseline ignored list** tab displays the ignored check items of the image.

1. On the **Baseline ignored list** tab, click the search box and search for image check items by check item.



2. On the **Baseline ignored list** tab, click

to select the target check item and click **Unignore** to unignore it.

Note:

After a check item is unignored, it will be considered as normal.

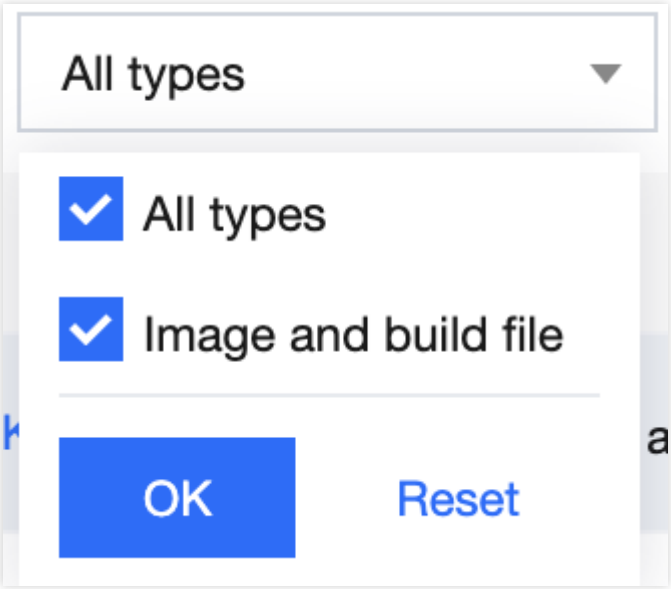
©2013-2022 Tencent Cloud. All rights reserved.

Viewing the List of Check Results

Filtering and refreshing check items

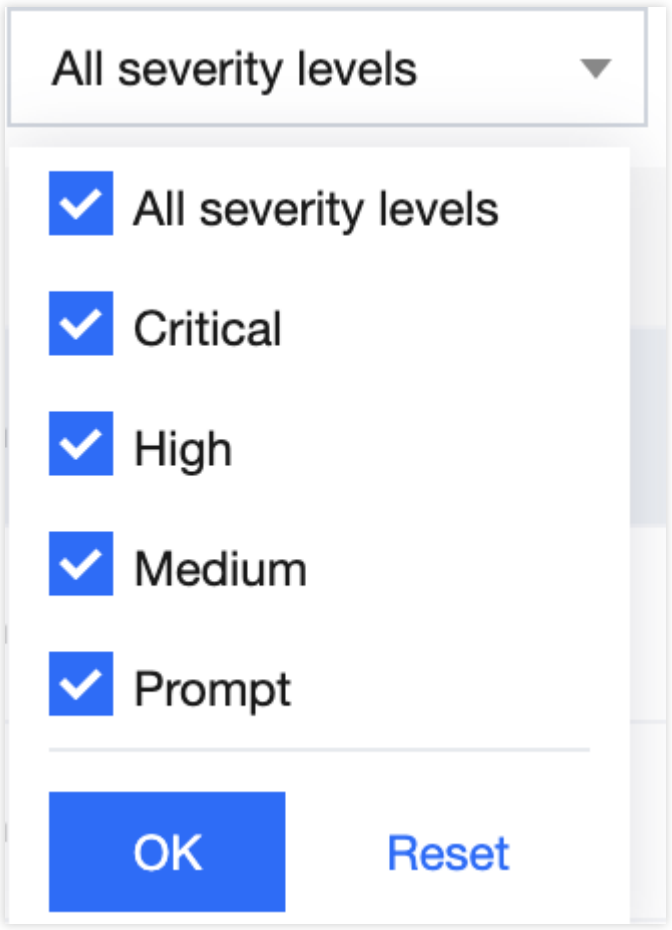
1. Log in to the TCSS console and click **Baseline Management** > **Image** on the left sidebar.
2. On the **Image** page, click the search box and search for image check items by check item or ID.

3. On the **Image** page, click the type drop-down list in the top-left corner and filter image check items by type.



4. On the **Image** page, click the severity drop-down list in the top-left corner and filter image check items by severity.

©2013-2022 Tencent Cloud. All rights reserved.



5. On the **Image** page, click

on the right of the **Operation** column to refresh the baseline check results.

Checking a check item again

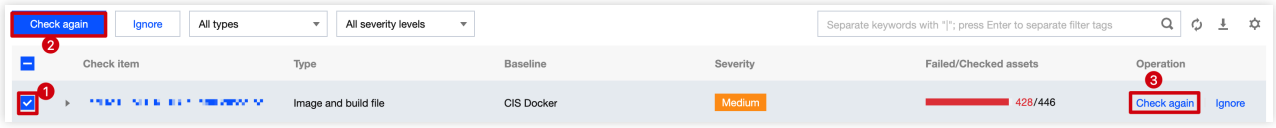
1. Log in to the TCSS console and click **Baseline Management** > **Image** on the left sidebar.
2. On the **Image** page, click

to select the target image check item and click **Check again** > **OK** to check it again.

Note:

You can batch check image check items again by selecting them and clicking **Check again** next to ②.

©2013-2022 Tencent Cloud. All rights reserved.



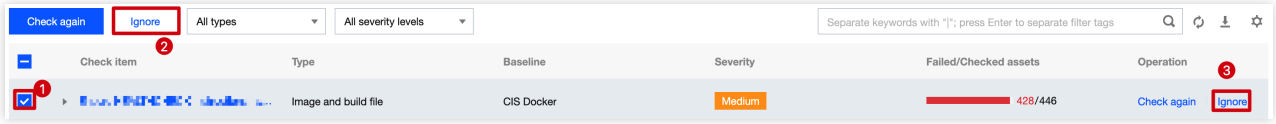
Ignoring a check item

1. Log in to the TCSS console and click **Baseline Management** > **Image** on the left sidebar.
2. On the **Image** page, click

to select the target check item and click **Ignore** > **OK** to ignore it.

Note:

You can batch ignore check items by selecting them and clicking **Ignore** next to ②.



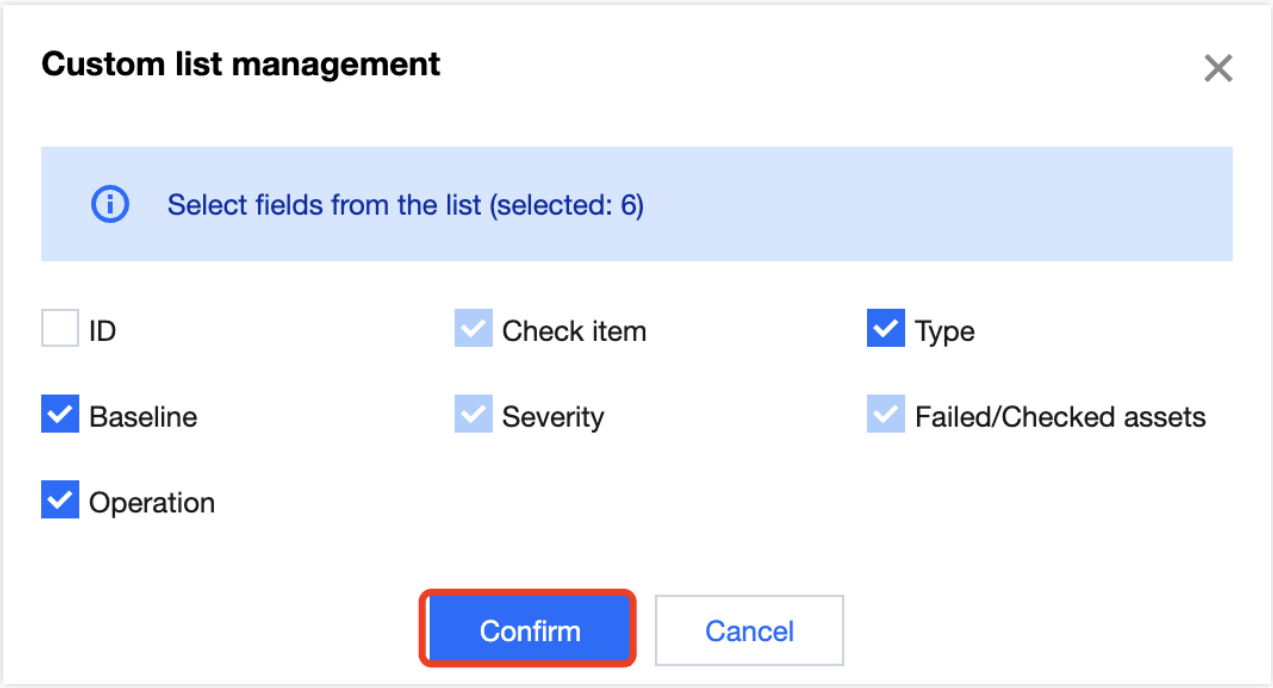
Custom list management

1. Log in to the TCSS console and click **Baseline Management** > **Image** on the left sidebar.
2. On the **Image** page, click

to pop up the **Custom List Management** window.

3. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Key fields in the list

1. ID: ID of the check item, which is globally unique.
2. Check item: Check content. You can click a check item to view the details.
3. Type: Type of the check item.
4. Baseline standard: Baseline standard of the check item.
5. Severity: Severity of the check item, which can be **Critical**, **High**, **Medium**, **Low**, or **Prompt**.
6. Result: Numbers of passed and failed assets for the current check item.
7. Operation: **Check again** or **Ignore**.

©2013-2022 Tencent Cloud. All rights reserved.

Docker Server

Last updated：2024-01-23 15:44:44

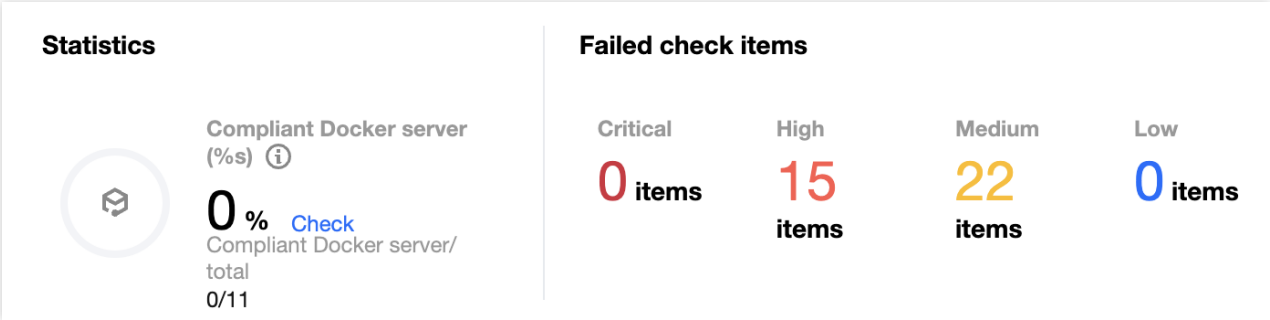
The **Docker server** page displays the baseline compliance details of servers, including statistics, check information, and the list of check results.

Viewing the Docker Server Overview

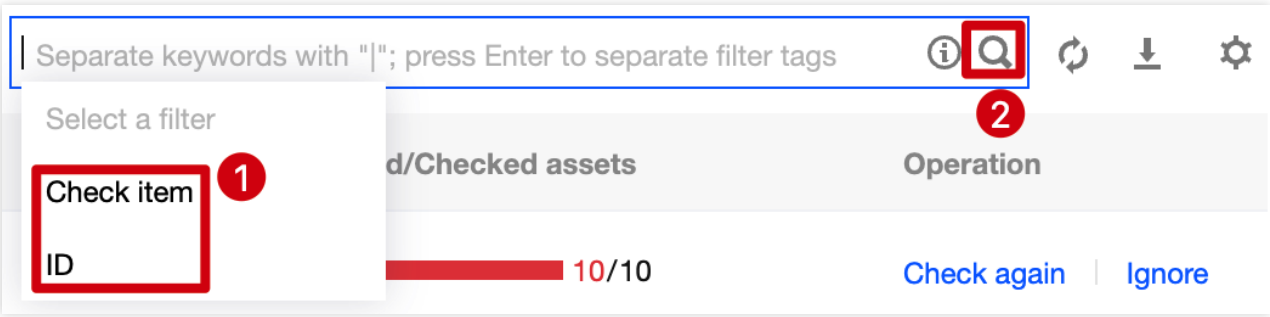
1. Log in to the TCSS console and click **Baseline Management** > **Docker server** on the left sidebar.
2. On the **Docker server** page, the **Statistics** window displays the percentage of compliant servers and the numbers of check items at the critical, high, medium, and low severity levels.

Note:

The percentage of compliant Docker servers is calculated as the number of compliant Docker servers/the total number of Docker servers (including those that failed the check).



3. On the **Docker server** page, click **View** next to the proportion to pop up the server drawer, which displays the list of check results.
4. In the Docker server drawer, click the search box and search for server check results by check item or ID.



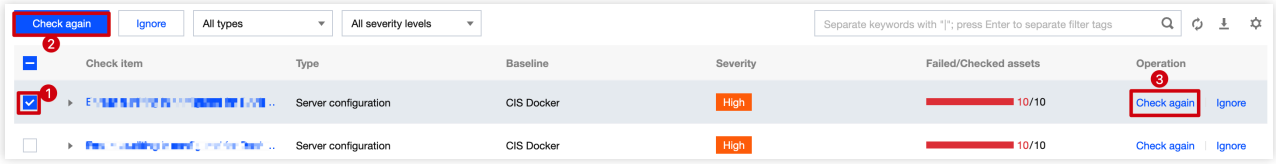
©2013-2022 Tencent Cloud. All rights reserved.

5. In the Docker server drawer, click

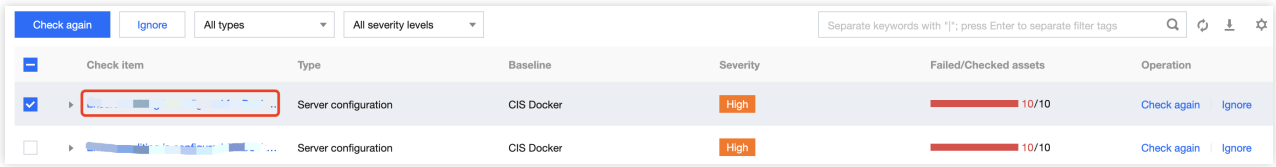
to select the target check item and click **Check again** > **OK** to check it again.

Note:

You can batch check server check items again by selecting them and clicking **Check again** next to ②.



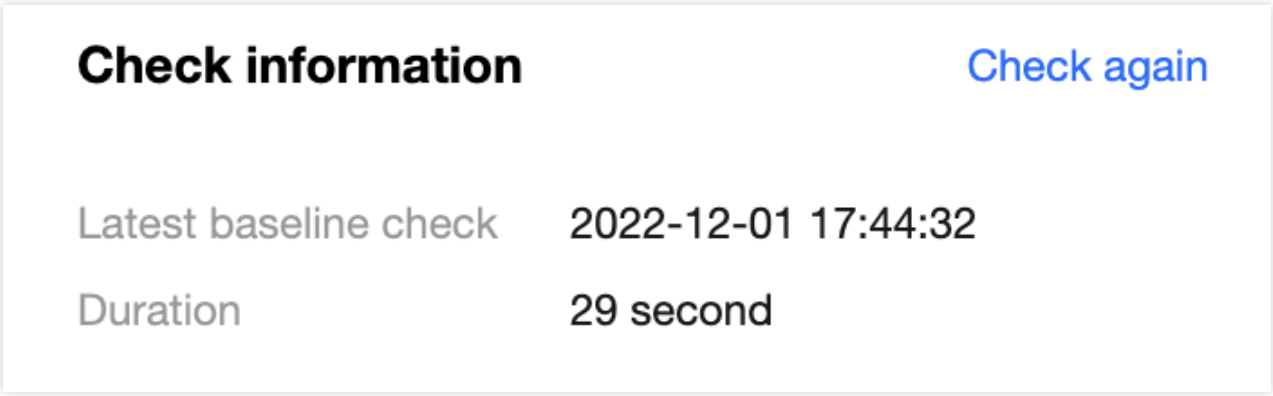
6. In the Docker server drawer, click a check item to view the baseline check results of a specified Docker server.



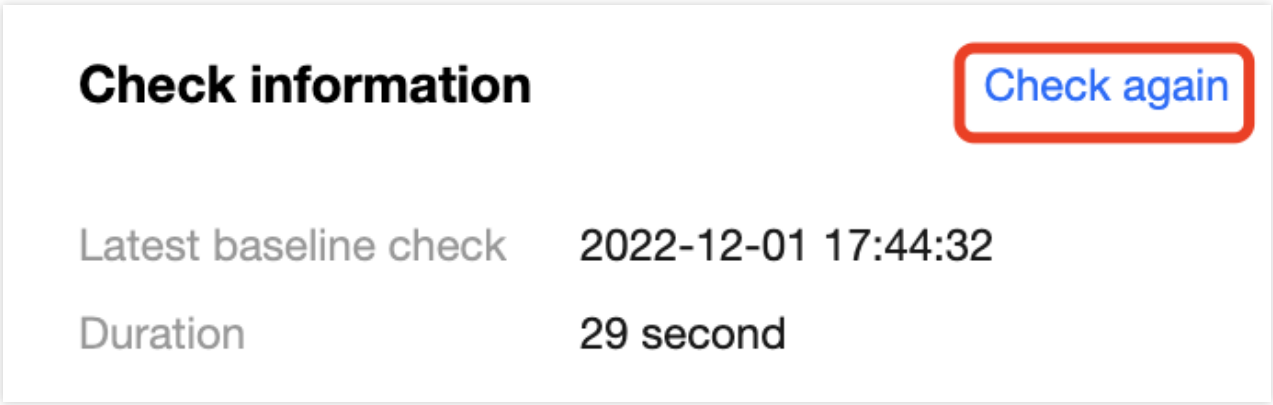
Viewing the Check Information

1. On the **Docker server** page, the **Check information** window displays the last baseline check time, check duration, and configured automatic check schedule.

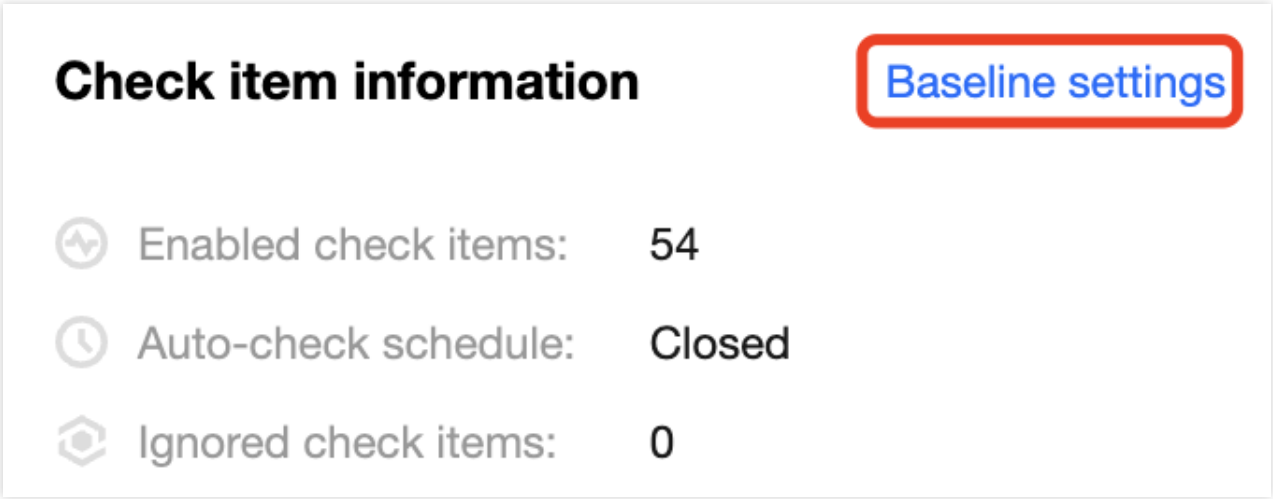
©2013-2022 Tencent Cloud. All rights reserved.



2. On the **Docker server** page, click **Check again** to perform a baseline check on the server.



3. On the **Docker server** page, click **Baseline settings** to set the baseline policy and baseline ignored list.



Setting the baseline policy

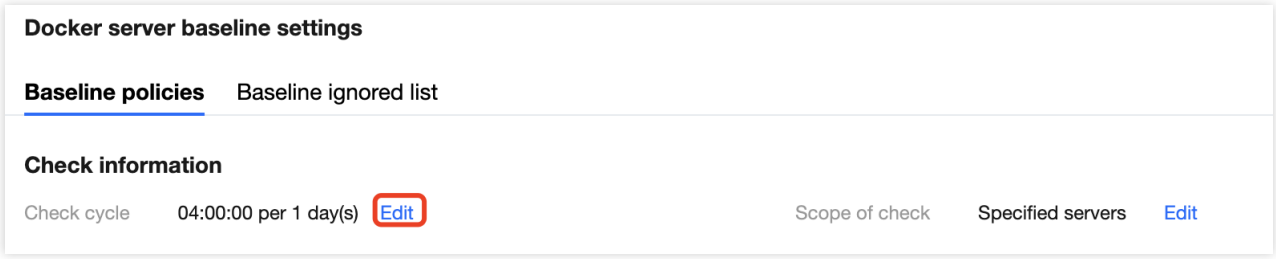
©2013-2022 Tencent Cloud. All rights reserved.

The **Baseline policies** tab displays the baseline for the current asset check and the number of check items.

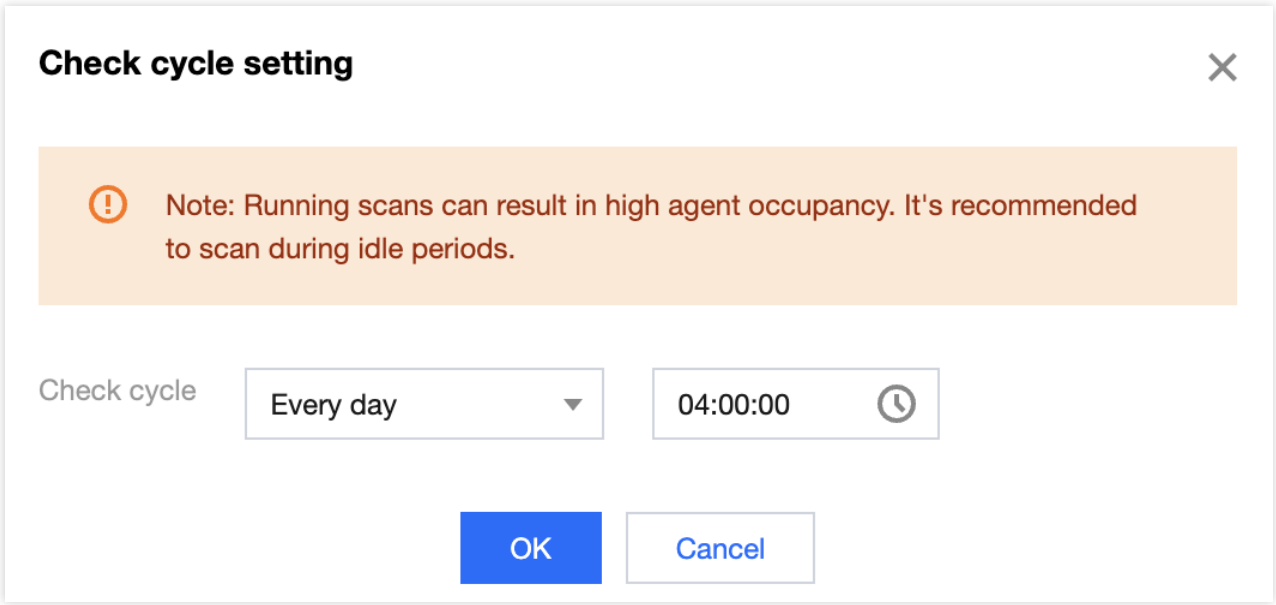
1. On the **Baseline policies** tab, toggle on or off

to enable or disable the periodic check against the current baseline.

2. On the **Baseline policies** tab, click **Edit** next to the check cycle to pop up the **Check cycle setting** window.



3. In the pop-up window, set the check cycle to every day, every 3 days, every 7 days, or a specified time range.



4. Click **OK**.

Baseline ignored list

The **Baseline ignored list** tab displays the ignored check items of the server.

1. On the **Baseline ignored list** tab, click the search box and search for check items by check item or server name/IP.

©2013-2022 Tencent Cloud. All rights reserved.

2. On the **Baseline ignored list** tab, click

to select the target server check item and click **Unignore** to unignore it.

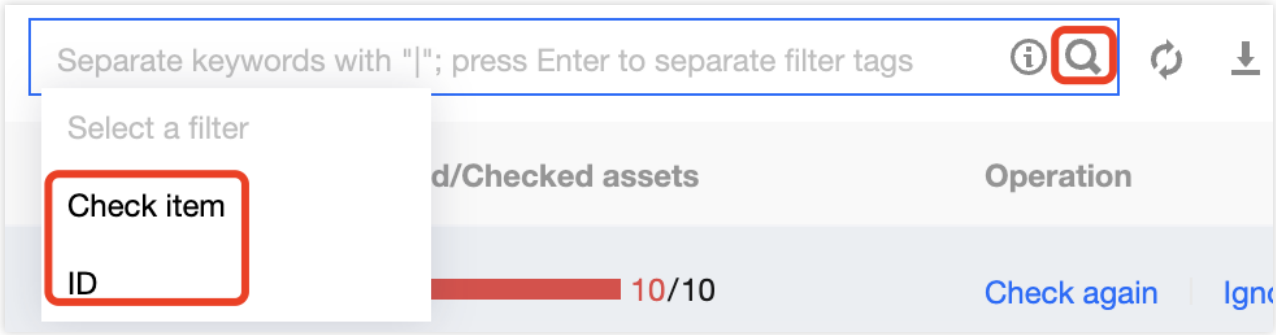
Note:

After a check item is unignored, it will be considered as normal.

Viewing the List of Check Results

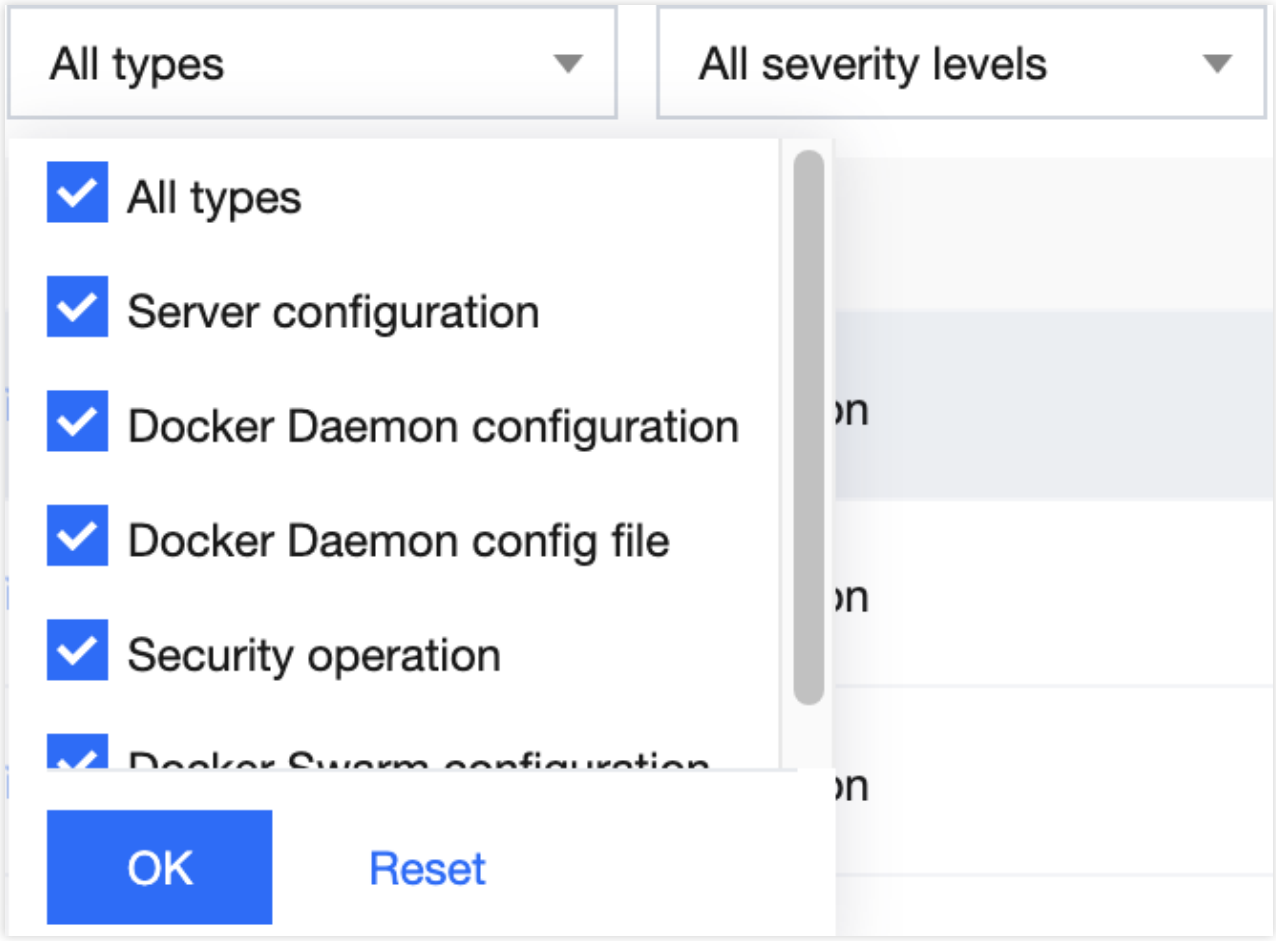
Filtering and refreshing check items

1. On the **Docker server** page, click the search box and search for Docker server check items by check item or ID.



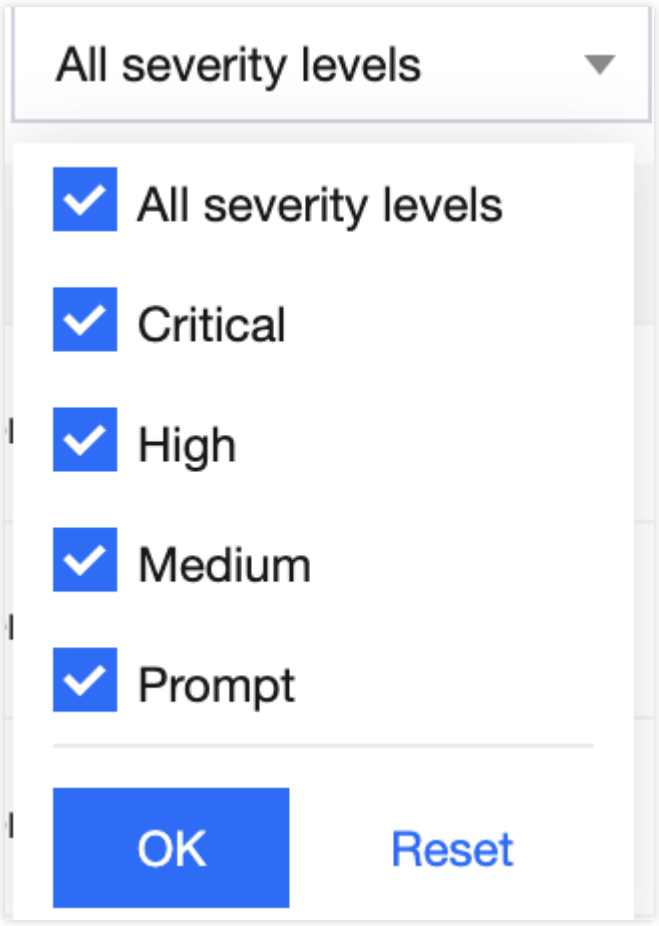
2. On the **Docker server** page, click the type drop-down list in the top-left corner and filter check items by type.

©2013-2022 Tencent Cloud. All rights reserved.



3. On the **Docker server** page, click the severity drop-down list in the top-left corner and filter check items by severity.

©2013-2022 Tencent Cloud. All rights reserved.



4. On the **Docker server** page, click

on the right of the **Operation** column to refresh the baseline check results.

Checking a check item again

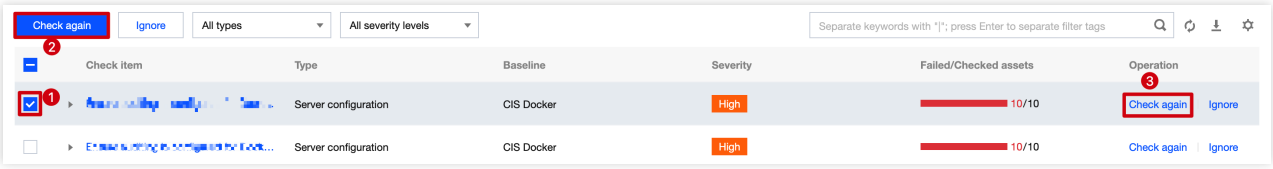
On the **Docker server** page, click

to select the target Docker server check item and click **Check again** > **OK** to check it again.

Note:

You can batch check server check items again by selecting them and clicking **Check again** next to ②.

©2013-2022 Tencent Cloud. All rights reserved.



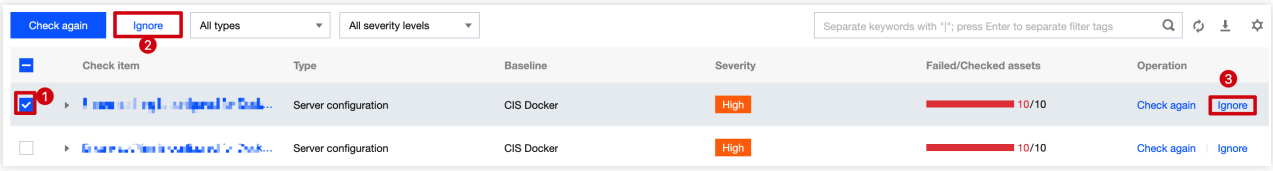
Ignoring a check item

On the **Docker server** page, click

to select the target check item and click **Ignore** > **OK** to ignore it.

Note:

You can batch ignore check items by selecting them and clicking **Ignore** next to ②.



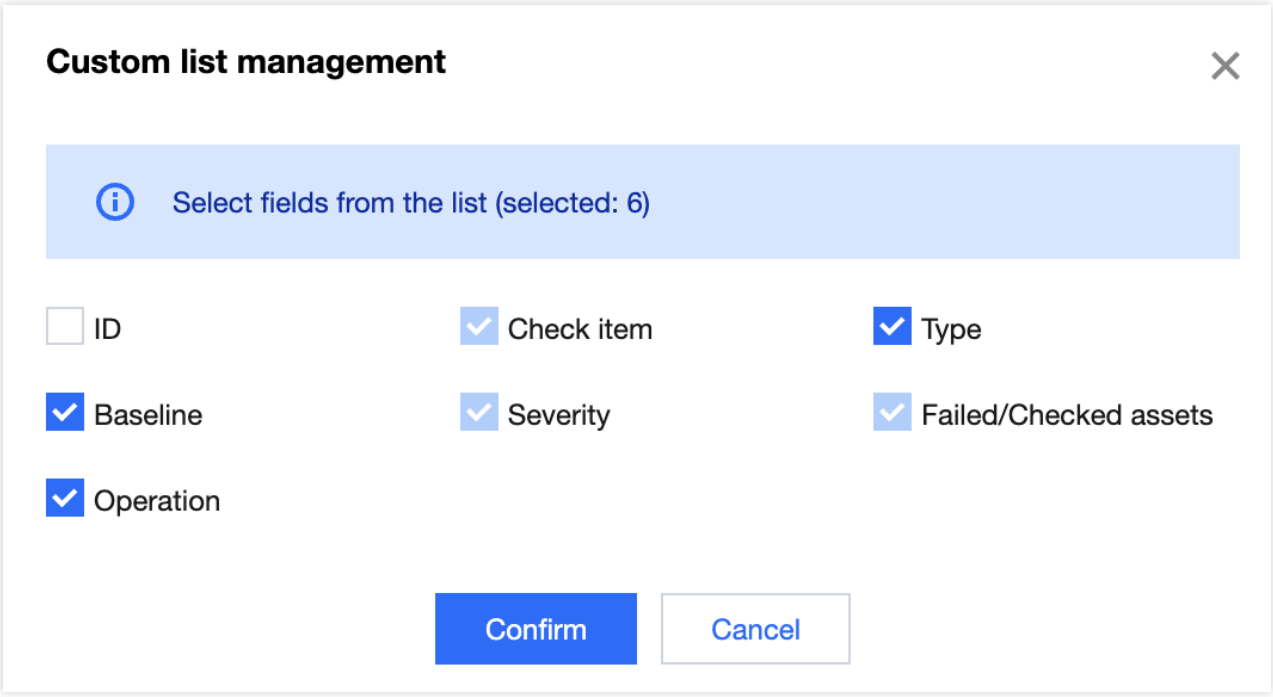
Custom list management

1. On the **Docker server** page, click

to pop up the **Custom List Management** window.

2. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Key fields in the list

1. ID: ID of the check item, which is globally unique.
2. Check item: Check content. You can click a check item to view the details.
3. Type: Type of the check item.
4. Baseline standard: Baseline standard of the check item.
5. Severity: Severity of the check item, which can be **Critical**, **High**, **Medium**, **Low**, or **Prompt**.
6. Result: Numbers of passed and failed assets for the current check item.
7. Operation: **Check again** or **Ignore**.

©2013-2022 Tencent Cloud. All rights reserved.

Kubernetes

Last updated：2024-01-23 15:44:44

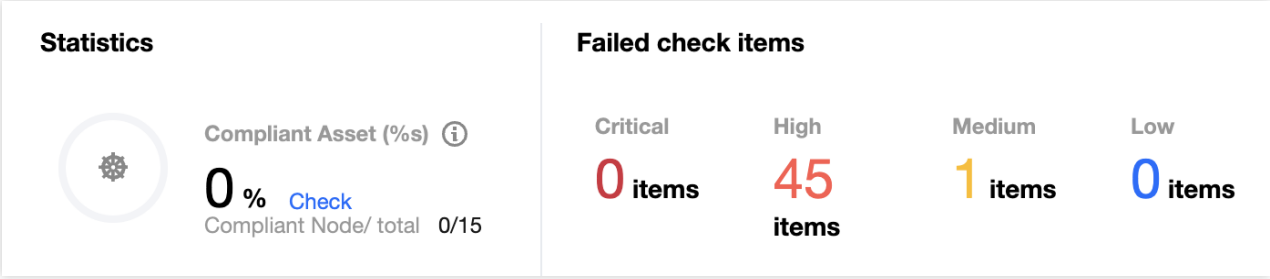
The **Kubernetes** page displays the baseline compliance details of Kubernetes assets against CIS Benchmarks, including statistics, check information, and the list of check results.

Viewing the Kubernetes Overview

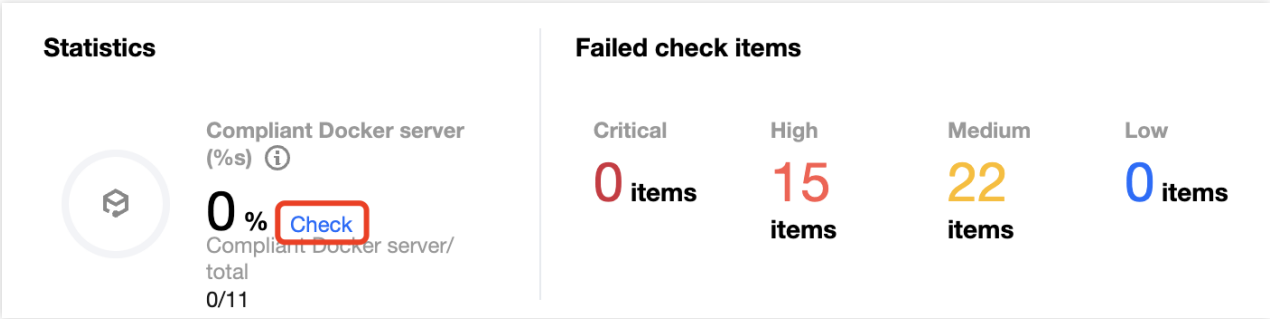
1. Log in to the TCSS console and click **Baseline Management** > **Kubernetes** on the left sidebar.
2. On the **Kubernetes** page, the **Statistics** window displays the check pass rate and the numbers of check items at the critical, high, medium, and low severity levels.

Note:

The check pass rate is calculated as the number of passed check items/the total number of check items.

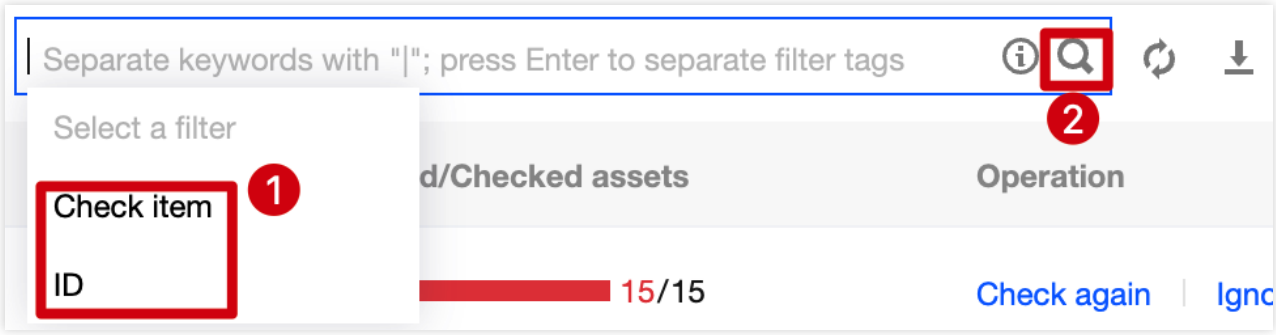


3. On the **Kubernetes** page, click **View** next to the proportion to pop up the drawer, which displays the list of check results.



4. On the **Kubernetes** page, click the search box and search for check results by check item or ID.

©2013-2022 Tencent Cloud. All rights reserved.

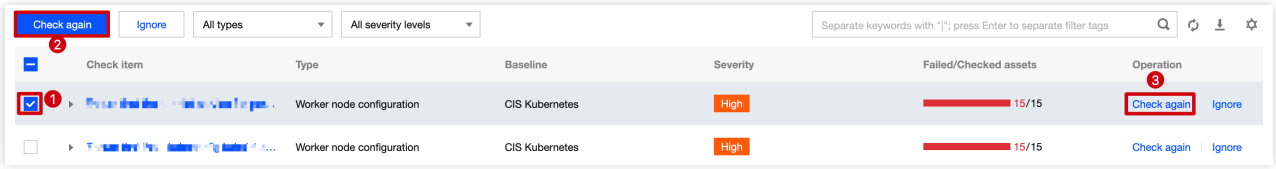


5. On the **Kubernetes** page, click

to select the target check item and click **Check again** > **OK** to check it again.

Note:

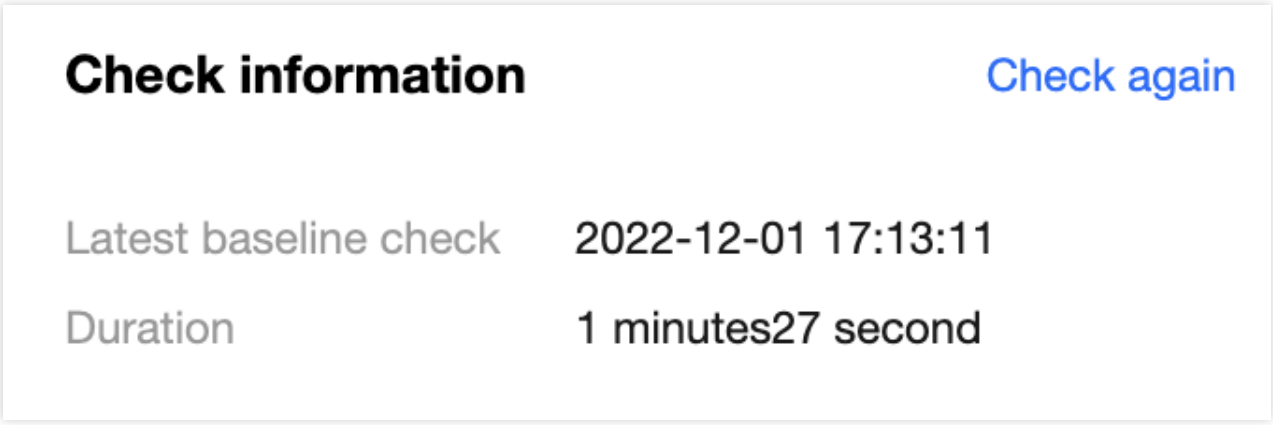
You can batch check Kubernetes check items again by selecting them and clicking **Check again** next to ②.



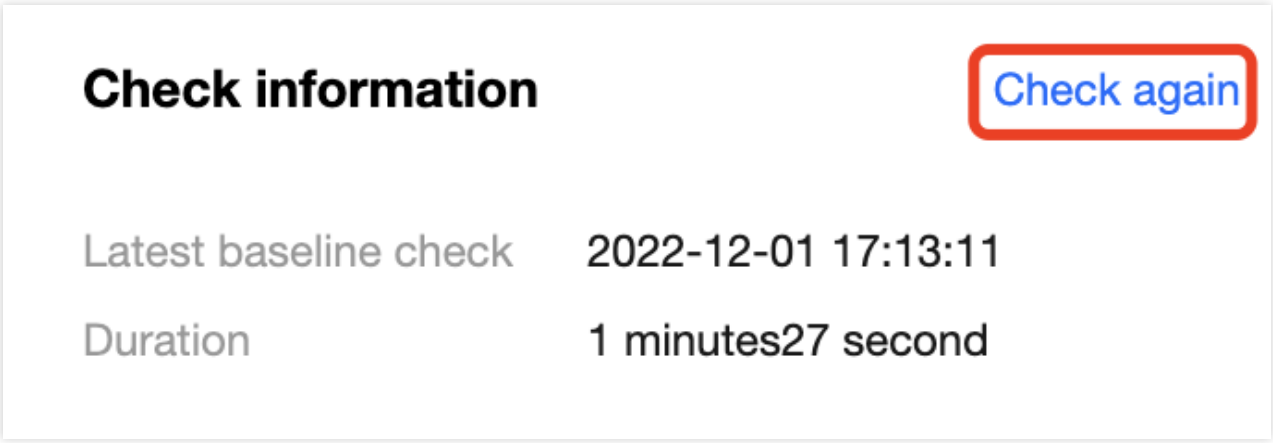
Viewing the Check Information

1. Log in to the TCSS console and click **Baseline Management** > **Kubernetes** on the left sidebar.
2. On the **Kubernetes** page, the **Check information** window displays the last baseline check time, check duration, and configured automatic check schedule.

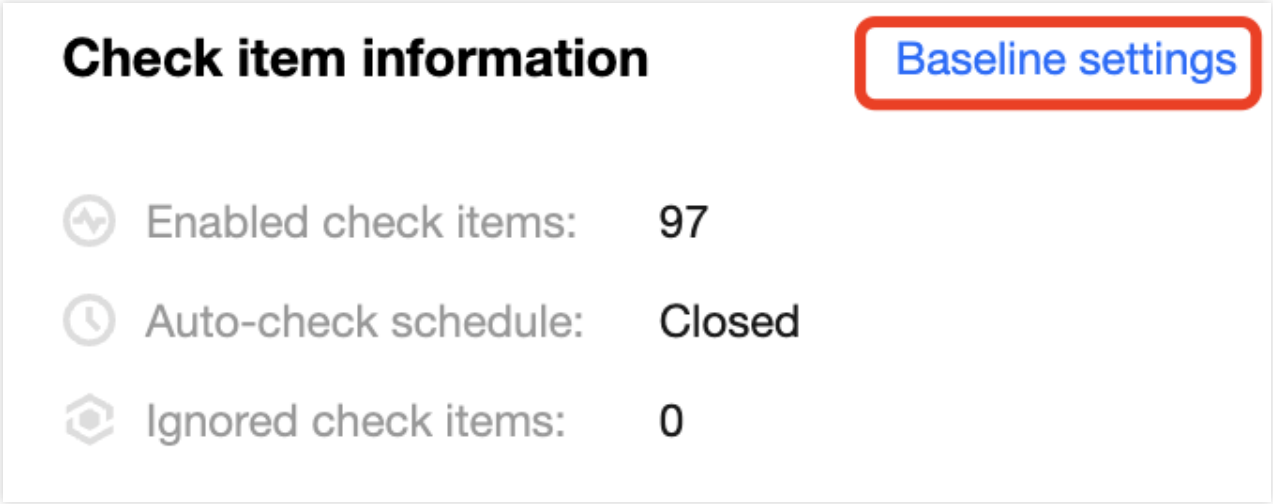
©2013-2022 Tencent Cloud. All rights reserved.



3. On the **Kubernetes** page, click **Check again** to perform a baseline check on the Kubernetes asset.



4. On the **Kubernetes** page, click **Baseline settings** to set the baseline policy and baseline ignored list.



©2013-2022 Tencent Cloud. All rights reserved.

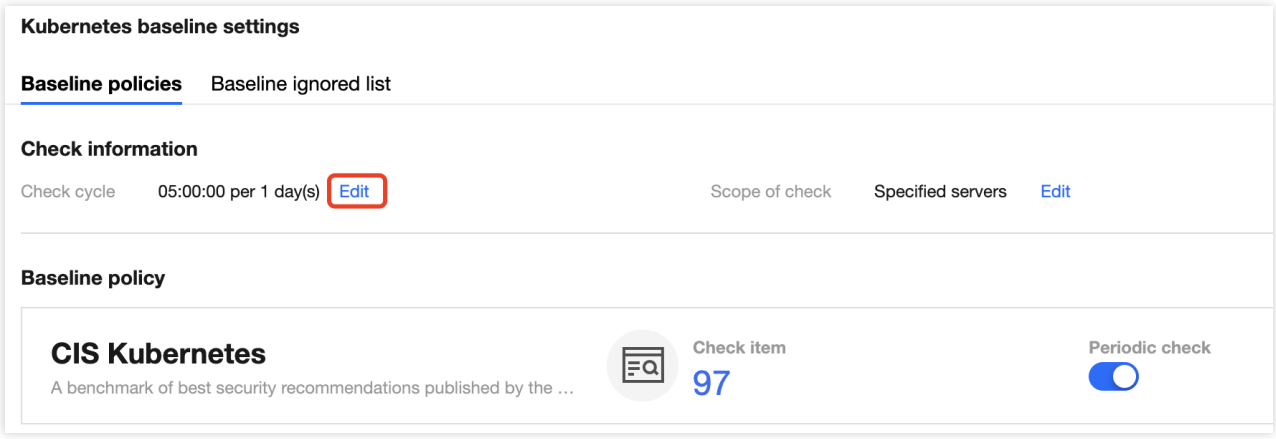
Setting the baseline policy

The **Baseline policies** tab displays the baseline for the current asset check and the number of check items.

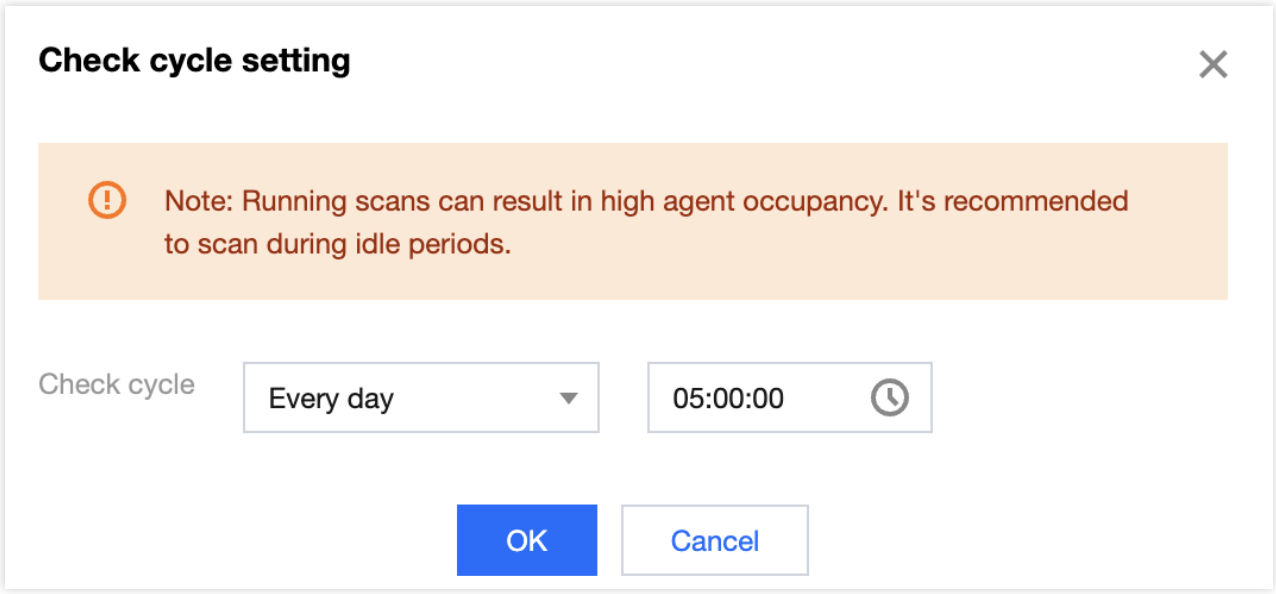
1. On the **Baseline policies** tab, toggle on or off

to enable or disable the periodic check against the current baseline.

2. On the **Baseline policies** tab, click **Edit** next to the check cycle to pop up the **Check cycle setting** window.



3. In the pop-up window, set the check cycle to every day, every 3 days, every 7 days, or a specified time range.



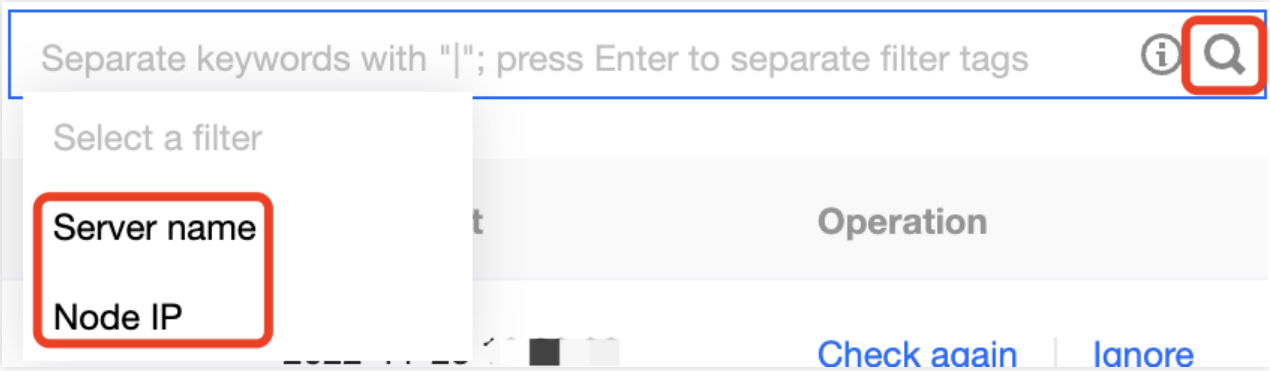
4. Click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.

Baseline ignored list

The **Baseline ignored list** tab displays the ignored check items of the container.

1. On the **Baseline ignored list** tab, click the search box and search for Kubernetes check items by check item, server name, or server IP.



2. On the **Baseline ignored list** tab, click

to select the target Kubernetes check item and click **Unignore** to unignore it.

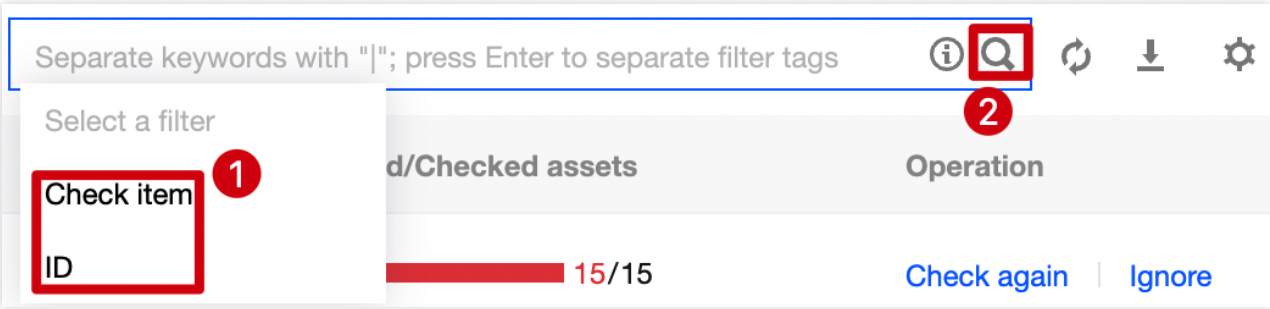
Note:

After a check item is unignored, it will be considered as normal.

Viewing the List of Check Results

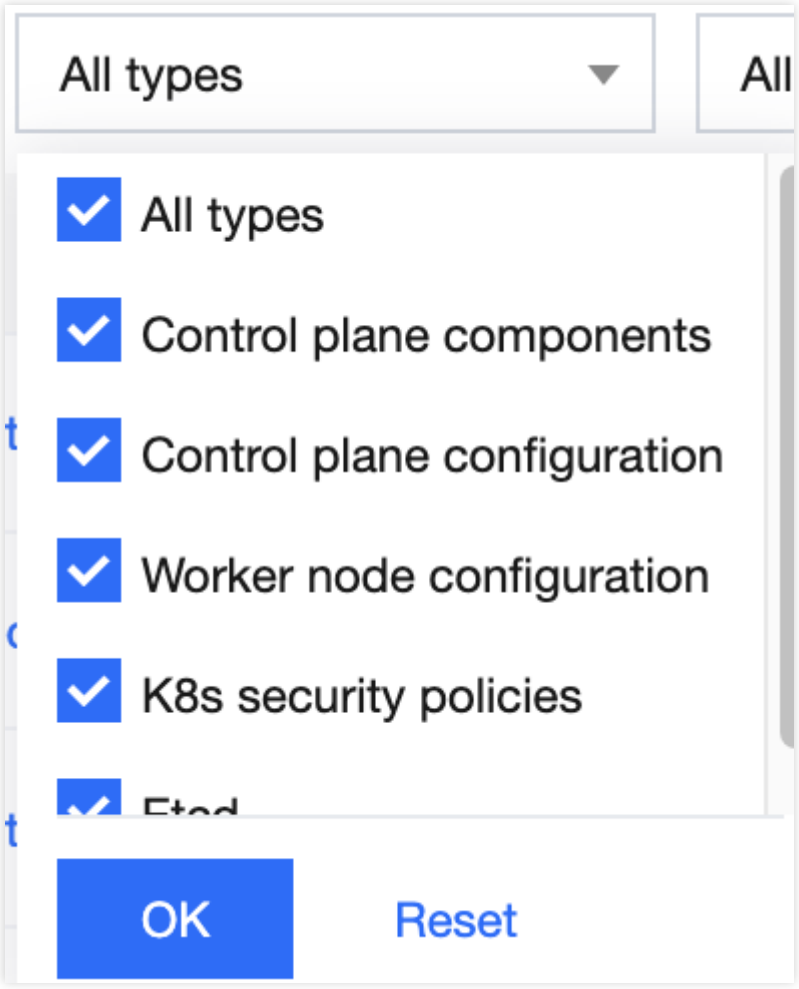
Filtering and refreshing check items

1. Log in to the TCSS console and click **Baseline Management** > **Kubernetes** on the left sidebar.
2. On the **Kubernetes** page, click the search box and search for Kubernetes check items by check item.



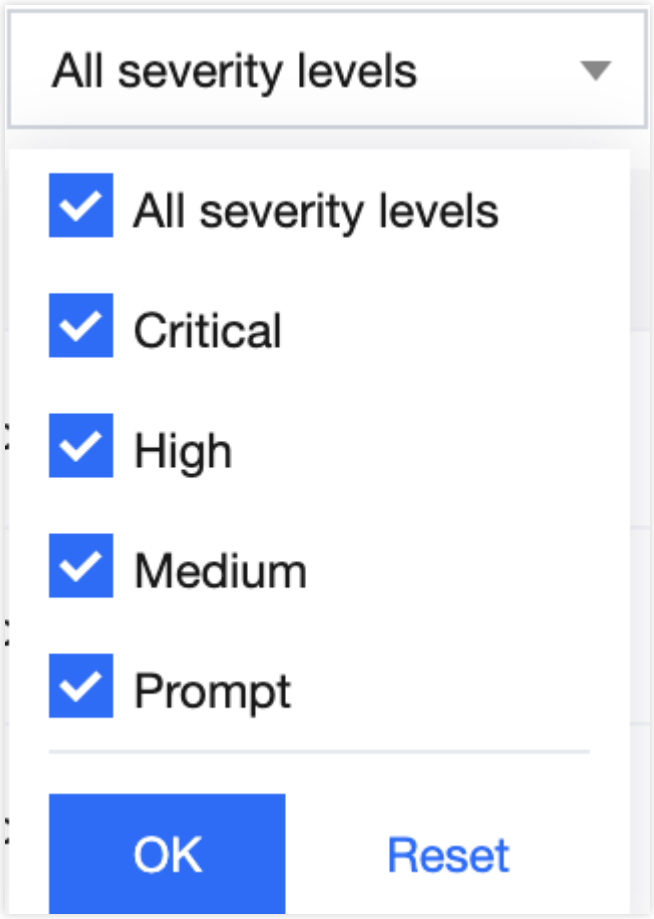
©2013-2022 Tencent Cloud. All rights reserved.

3. On the **Kubernetes** page, click the type drop-down list in the top-left corner and filter Kubernetes check items by type.



4. On the **Kubernetes** page, click the severity drop-down list in the top-left corner and filter Kubernetes check items by severity.

©2013-2022 Tencent Cloud. All rights reserved.



5. On the **Kubernetes** page, click

on the right of the **Operation** column to refresh the Kubernetes check items.

Checking a check item again

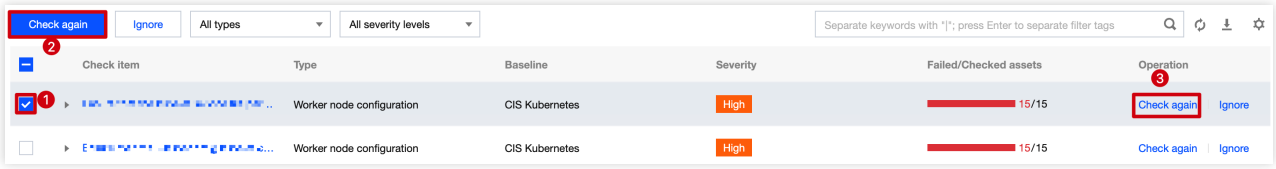
1. Log in to the TCSS console and click **Baseline Management** > **Kubernetes** on the left sidebar.
2. On the **Kubernetes** page, click

to select the target check item and click **Check again** > **OK** to check it again.

Note:

You can batch check Kubernetes check items again by selecting them and clicking **Check again** next to ②.

©2013-2022 Tencent Cloud. All rights reserved.



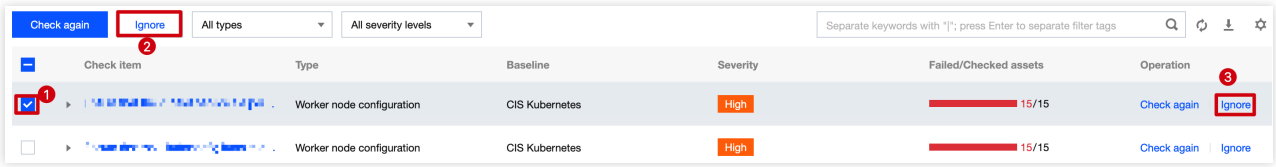
Ignoring a check item

1. Log in to the TCSS console and click **Baseline Management** > **Kubernetes** on the left sidebar.
2. On the **Kubernetes** page, click

to select the target Kubernetes check item and click **Ignore** > **OK** to ignore it.

Note:

You can batch ignore Kubernetes check items by selecting them and clicking **Ignore** next to ②.



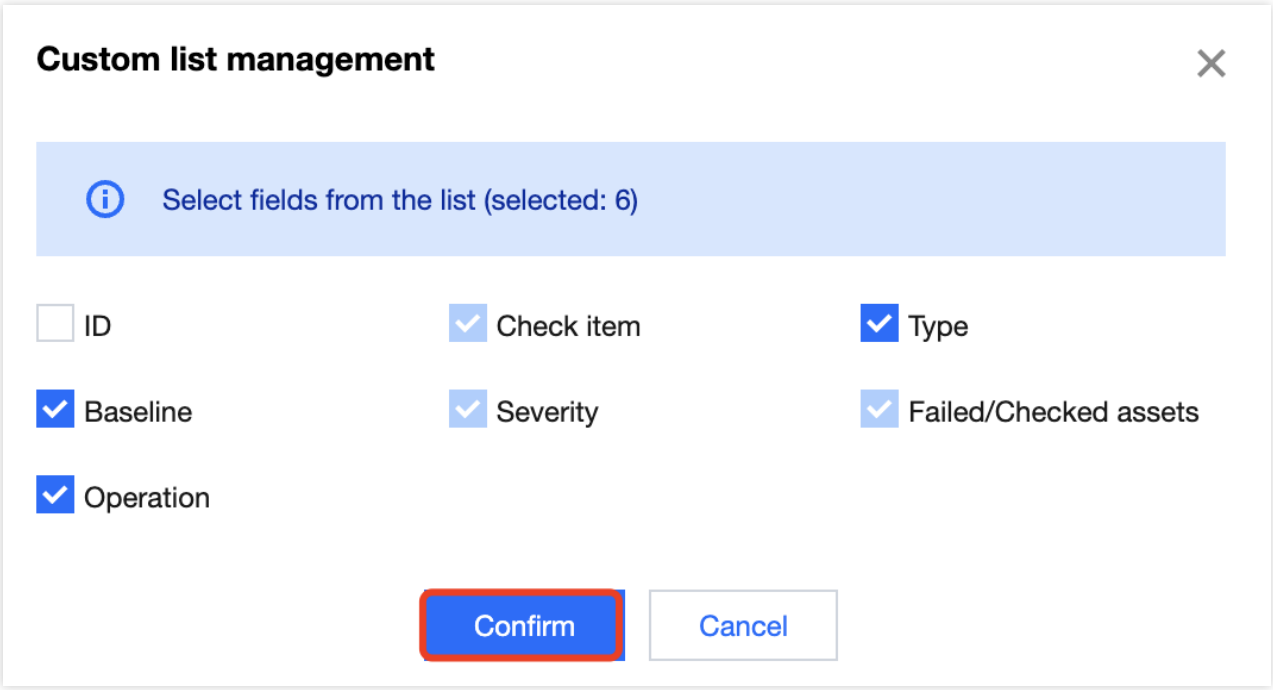
Custom list management

1. Log in to the TCSS console and click **Baseline Management** > **Kubernetes** on the left sidebar.
2. On the **Kubernetes** page, click

to pop up the **Custom List Management** window.

3. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Key fields in the list

1. ID: ID of the check item, which is globally unique.
2. Check item: Check content. You can click a check item to view the details.
3. Type: Type of the check item.
4. Baseline standard: Baseline standard of the check item.
5. Severity: Severity of the check item, which can be **Critical**, **High**, **Medium**, **Low**, or **Prompt**.
6. Result: Numbers of passed and failed assets for the current check item.
7. Operation: **Check again** or **Ignore**.

©2013-2022 Tencent Cloud. All rights reserved.

Runtime Security Overview

Last updated：2024-01-23 15:44:44

Runtime security identifies hacker attacks adaptively, monitors and protects container runtime security in real time, and utilizes diversified security features, including container escape, reverse shell, and virus scanning.

Container escape: A container escapes from its permissions and accesses the host and other containers on the host by exploiting system vulnerabilities. As containers share the operating system kernel with the host, to prevent them from getting the host's root privileges, they are usually not allowed to run in privileged mode. TCSS categorizes risk events into three types based on the sequence of container escapes performed by intruders: container in risk, program privilege escalation, and container escape.

Containers in risk: Risks are found in the current container, such as sensitive path mount and privileged container, which may cause privilege escalation or escape.

Program privilege escalation: Privilege escalation events are detected on the container.

Container escape: The current container has escaped. In this case, you should immediately respond to the risky event with the recommended solution.

Reverse shell: Based on Tencent Cloud security technologies and multidimensional means, it recognizes and records reverse shell connections for real-time monitoring in the runtime container.

Virus scanning: It checks for risky files called by running containers in real time. You can also manually trigger a quick scan to check for malicious viruses, trojans, and web shells in the container.

©2013-2022 Tencent Cloud. All rights reserved.

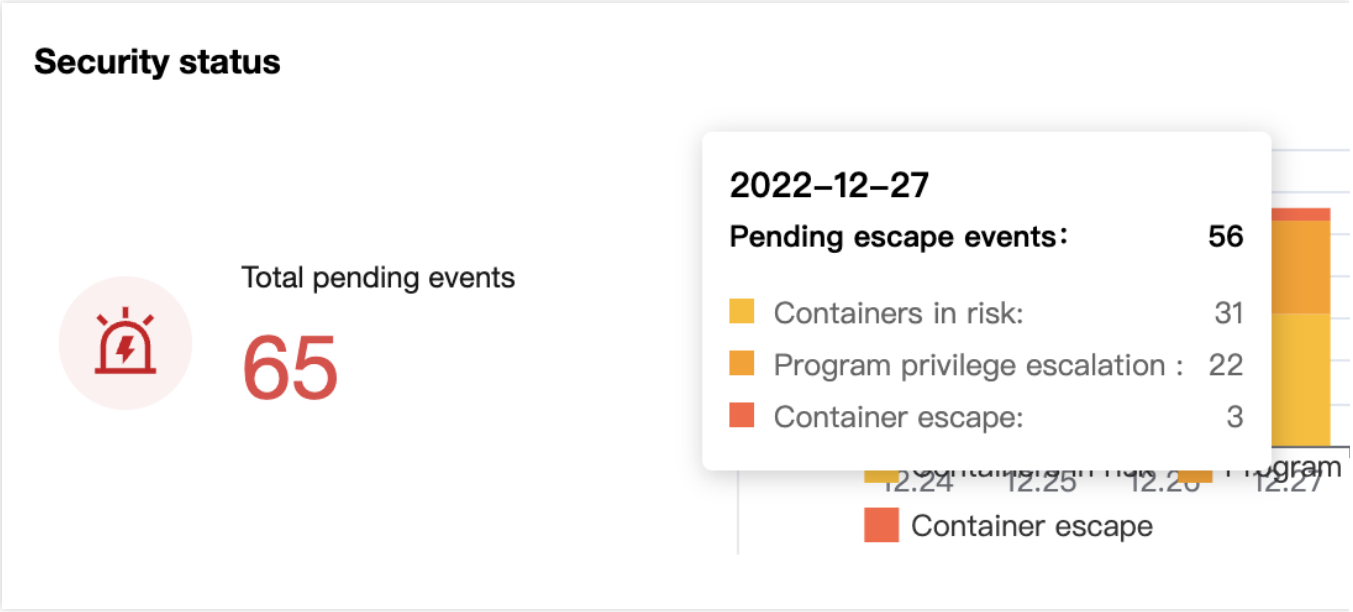
Container Escape

Last updated：2024-01-23 15:44:44

Event List

Viewing the set status

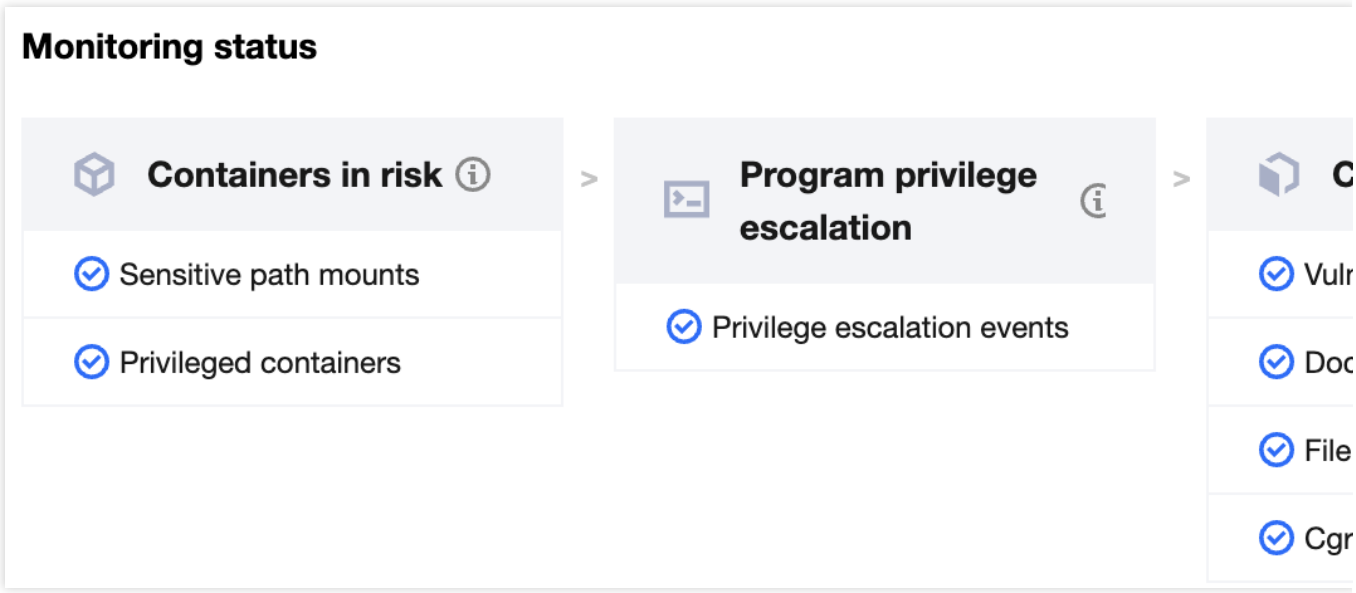
1. Log in to the TCSS console and click **Runtime Security** > **Container Escape** on the left sidebar.
2. On the **Container Escape** page, the security status module displays whether a container escape event exists, and if so, we recommend you process it immediately.



3. On the **Container Escape** page, the monitoring status module displays the container escape event types that can be checked by the system. Toggle on

to customize the monitoring status.

©2013-2022 Tencent Cloud. All rights reserved.



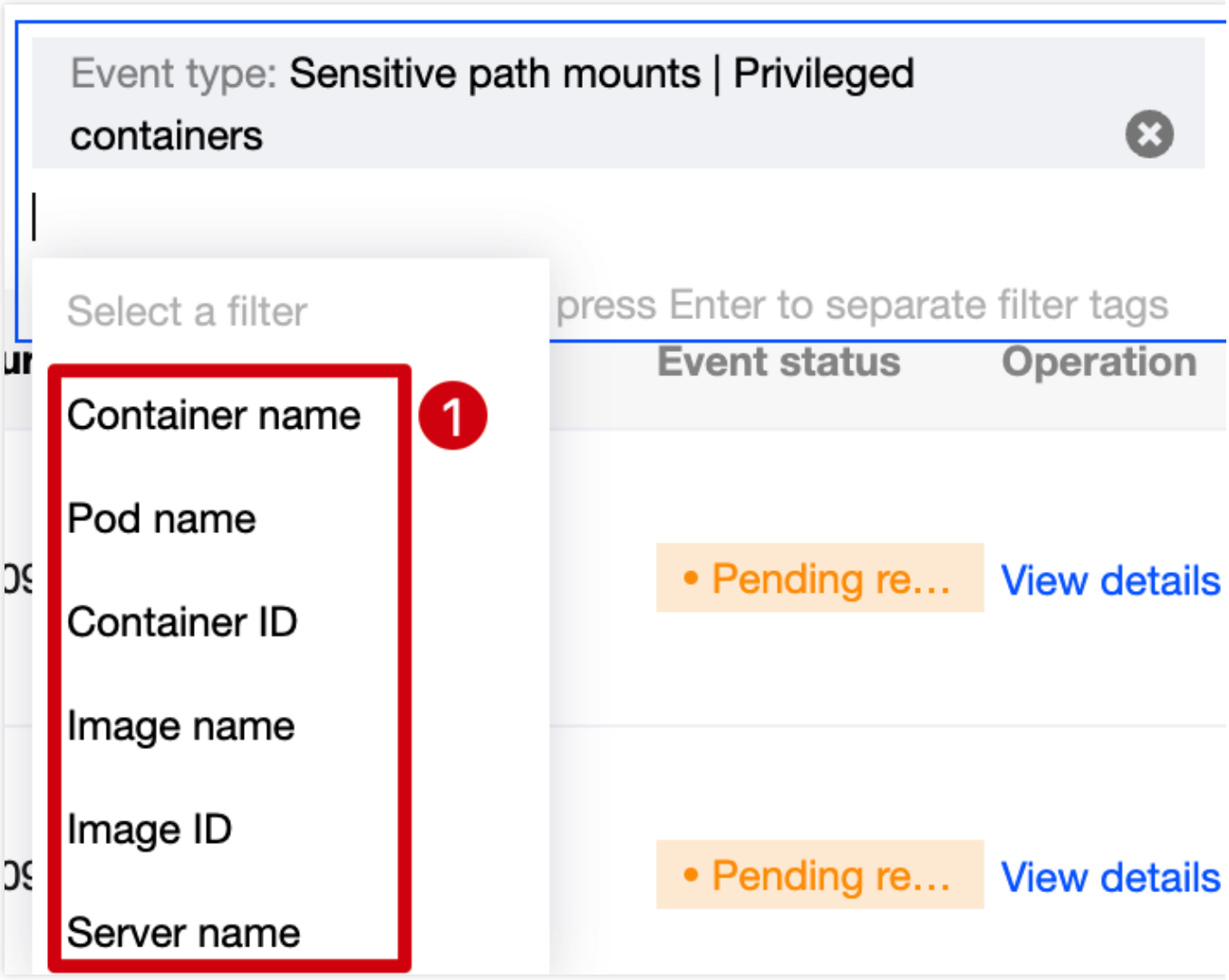
Viewing the list of container escapes

Log in to the TCSS console and click **Runtime Security** > **Container Escape** on the left sidebar.

Filtering and refreshing container escapes

1. On the **Container Escape** page, click the search box and search for container escape events by keyword such as container name, image name, or server name.

©2013-2022 Tencent Cloud. All rights reserved.



2. On the **Container Escape** page, click

on the right of the **Operation** column to refresh the container escape events.

Exporting a container escape

On the **Container Escape** page, click

to select the target container escape event and click

to export it.

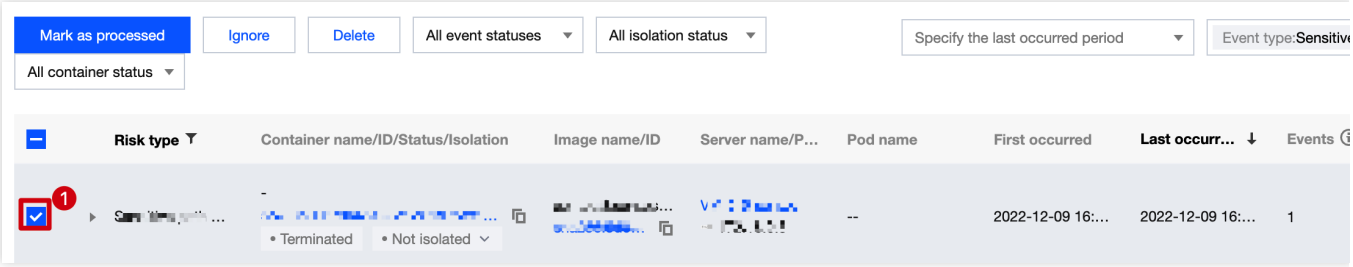
Note:

©2013-2022 Tencent Cloud. All rights reserved.

You can click

to select multiple events and click

to batch export them.



Event status processing

On the **Container Escape** page, you can mark a container escape event as processed or ignore or delete it.

Mark as processed: Click

to select the target container escape event and click **Mark as processed** > **OK**.

Note:

It's recommended to handle the event by following "Solution" in the event details and mark it as processed.

Ignore: Click

to select the target container escape event and click **Ignore** > **OK**.

Note:

Only the selected events are ignored. Alerts will be triggered when the same events occur again.

Delete: Click

to select the target container escape event and click **Delete** > **OK**.

Note:

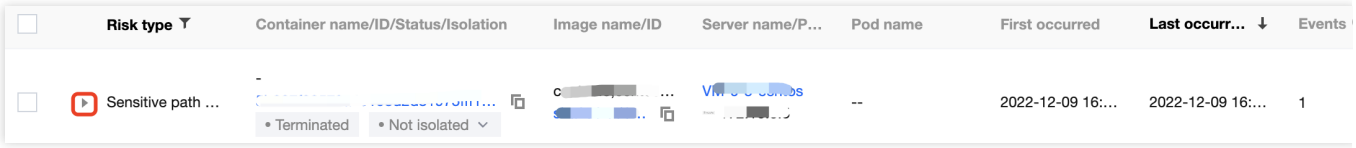
The selected event record will no longer be displayed in the console and cannot be recovered once deleted. Proceed with caution.

©2013-2022 Tencent Cloud. All rights reserved.

Viewing list details

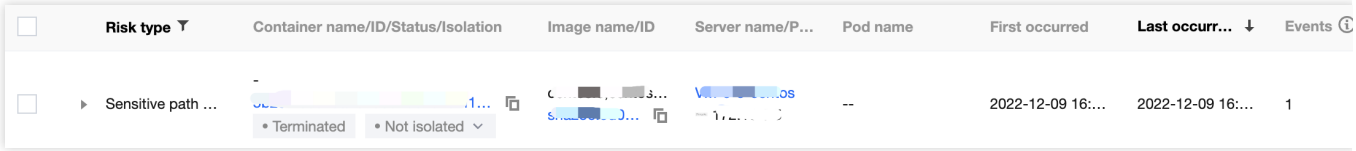
1. On the **Container Escape** page, click

on the left of **Event type** to view the event description.



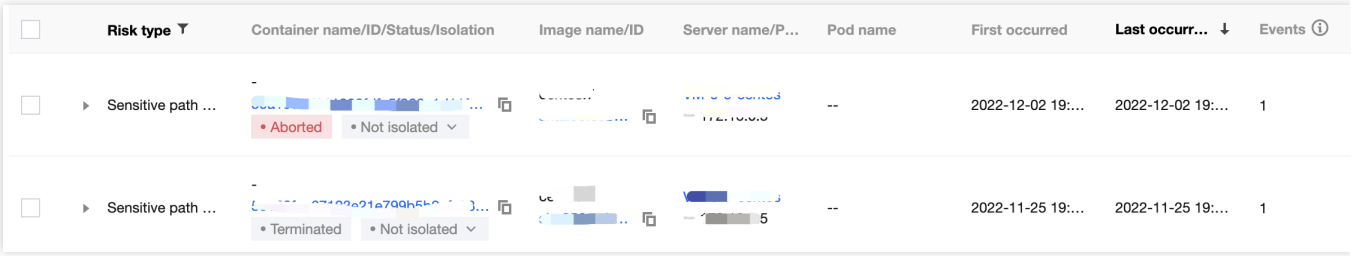
2. On the **Container Escape** page, click the **Container name/ID** or **Image name/ID** to enter the asset management list.

3. On the **Container Escape** page, click **View details** to pop up the drawer on the right, which displays the event details, process information, and event description.

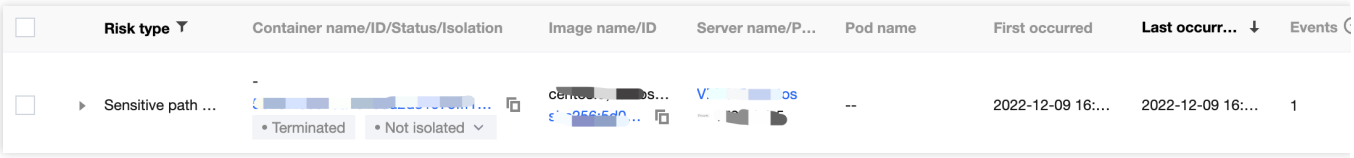


4. On the **Container Escape** page, the event status can be **Processed**, **Ignored**, or **Pending resolved**. You can manipulate events in different statuses as follows:
Processed: Click **Delete** and click **OK** in the pop-up window.
Note:
The event record will no longer be displayed in the console and cannot be recovered once deleted. Proceed with caution.

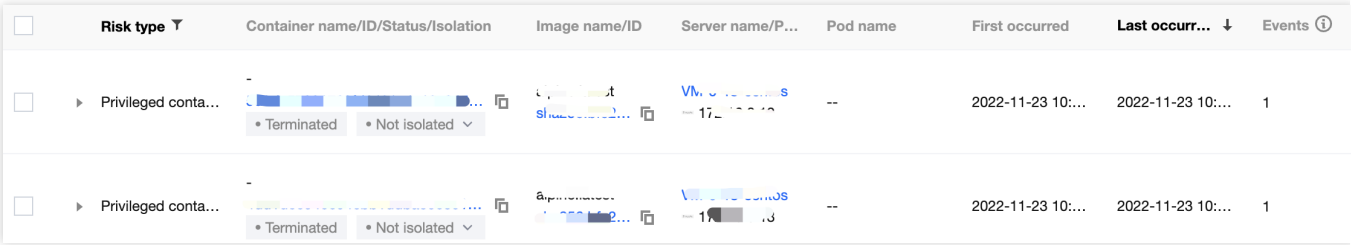
©2013-2022 Tencent Cloud. All rights reserved.



Pending resolved: Click **Process now** to mark the event as processed or ignore or delete it. For detailed directions, see Event status processing.



Ignored: Click **Unignore** or **Delete** to turn the event into the **Pending resolved** status or delete it.



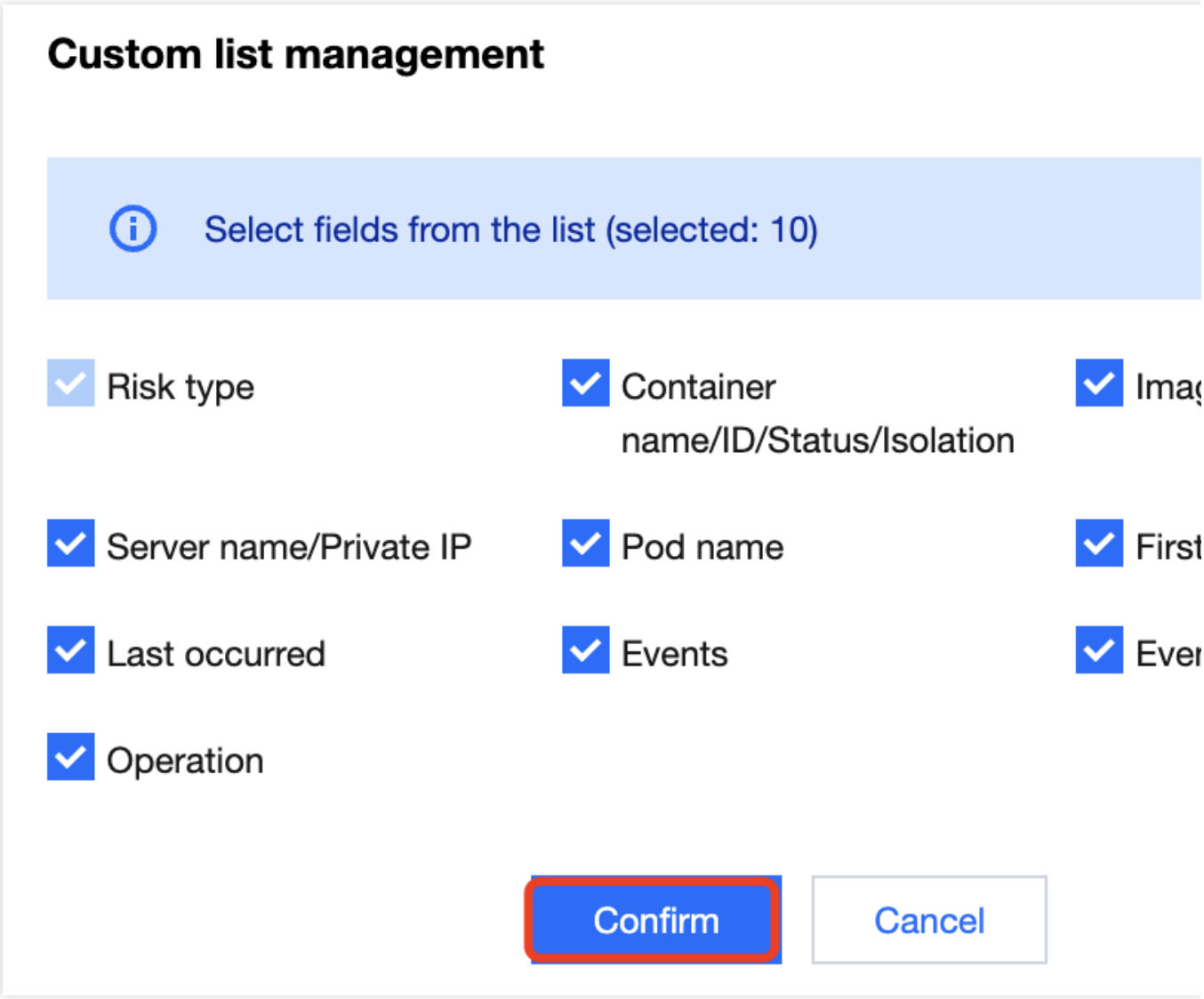
Custom list management

1. On the **Container Escape** page, click

to pop up the **Custom List Management** window.

2. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Fields in the list

1. Event type: Type of the container escape event, which can be host file access escape, mount namespace escape, program privilege escalation, privileged container startup escape, sensitive path mounts, or syscall escape.
2. First occurred: The time when an alert is first triggered by the escape event.

Note:

By default, the system aggregates the same escape events not processed.

3. Last occurred: The time when an alert is last triggered by the aggregated alert events. You can click the sort button on the right to sort the events in the list in chronological or reverse chronological order.
4. Events: Total number of alerts triggered by the escape event within the aggregation period.
5. Status: **Processed**, **Ignored**, **Pending resolved**, or **Allowed**. You can quickly filter events in the list by status.

Escape Allowlist

©2013-2022 Tencent Cloud. All rights reserved.

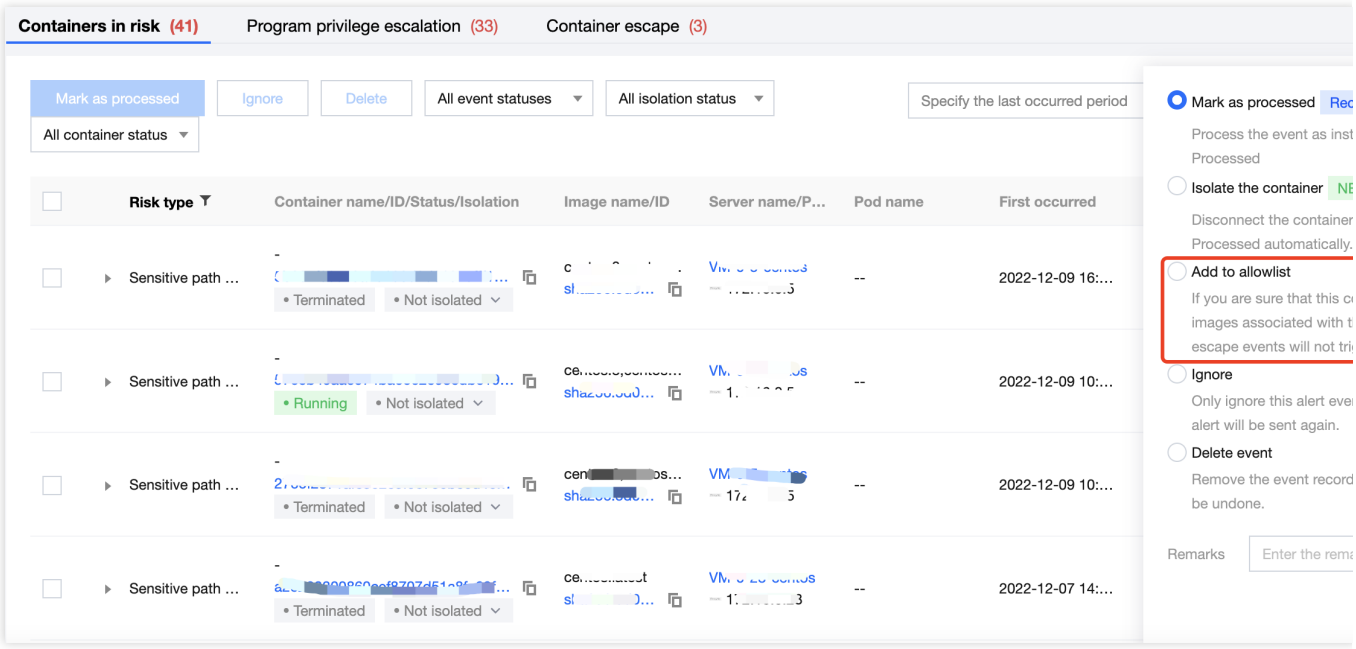
When troubleshooting a container escape alert, for example, if a business container requires startup in privileged mode, sensitive path mounting, or other configuration that will trigger an escape alert, you can add the alert event to the allowlist or create an allowlist on the **Allowlist policies** tab.

Adding an alert event to the allowlist

1. On the **Container Escape** page, click **Process**, select **Add to allowlist**, and click **OK** to allow an alert event.

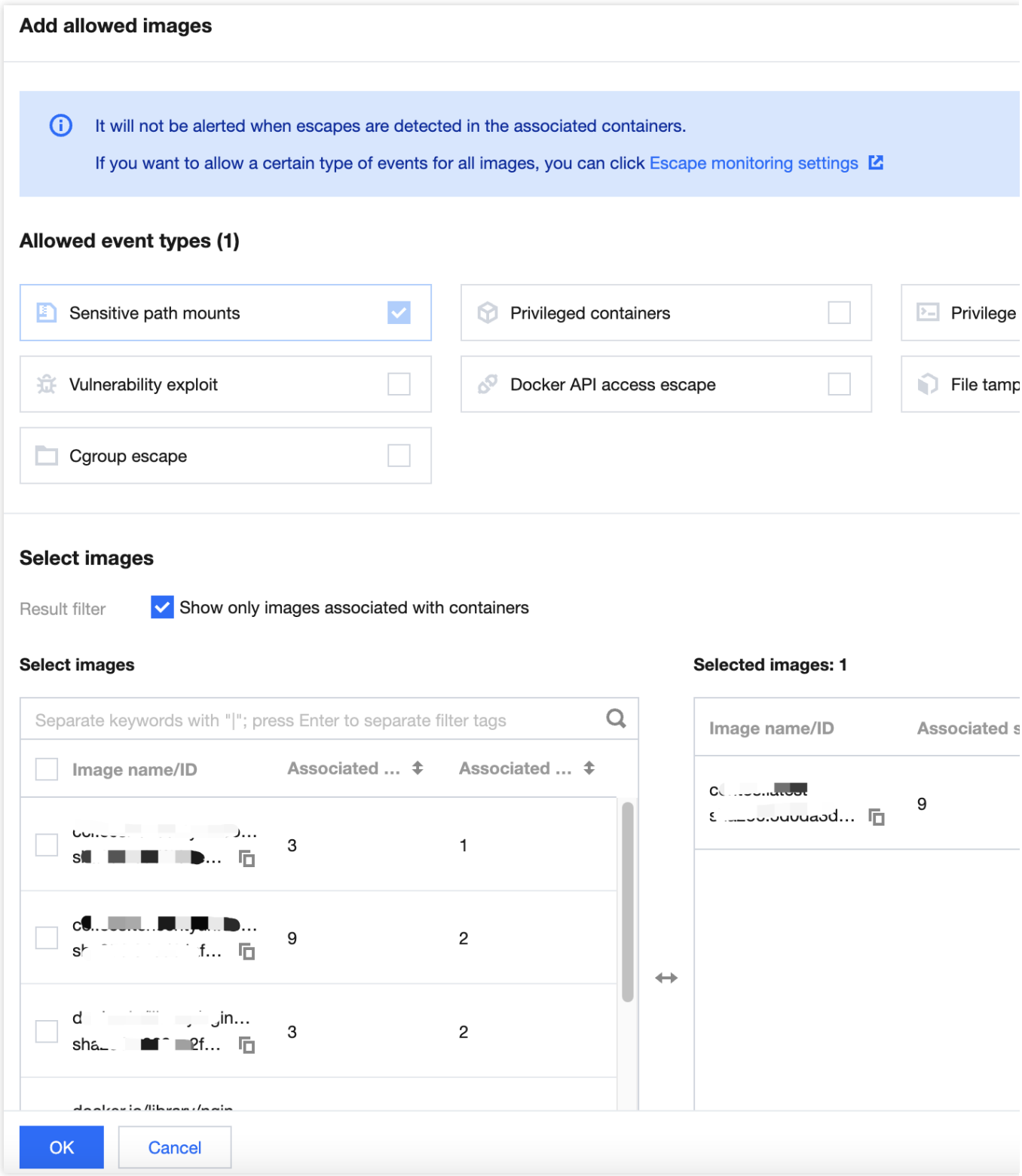
Note:

If you are sure that this container escape event is normal, add the images associated with the container to the allowlist. **This kind of escape events will not trigger alerts any more**.



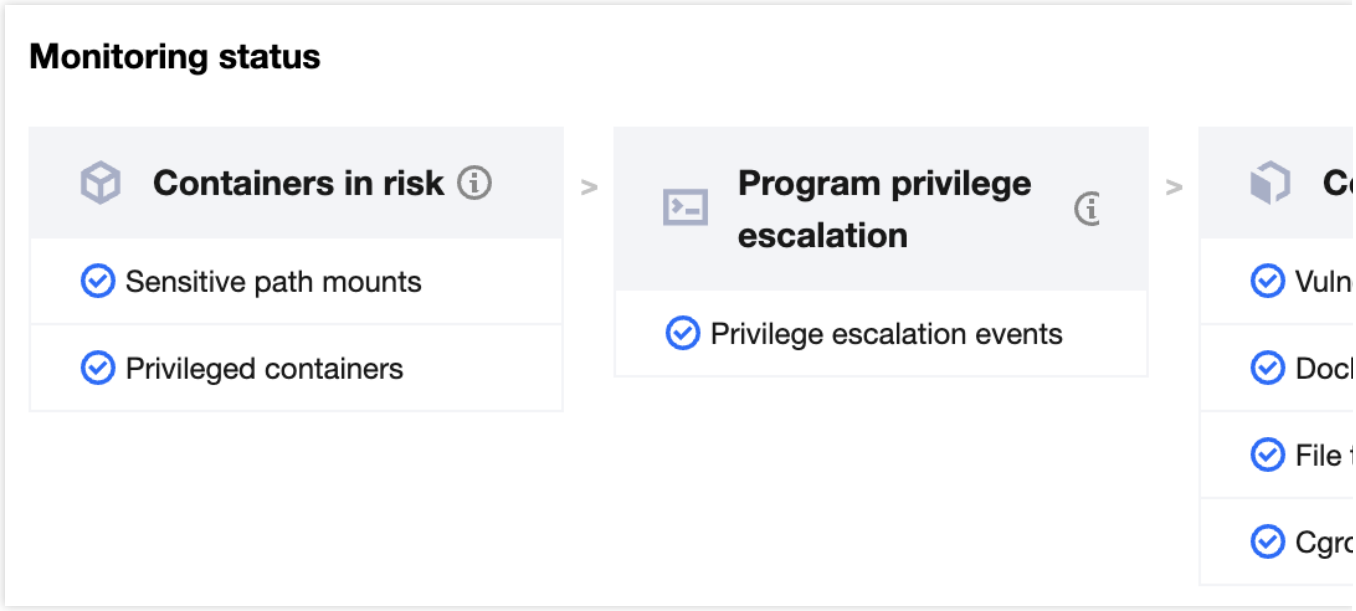
2. On the **Add allowed images** page, the escape alert type and source image associated with the alert event are selected by default. You can add allowed event types and images to be added to the allowlist and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



3. To add all images to the allowlist for an event type, click **Monitoring settings** on the right of the **Monitoring status** and adjust the event type with monitoring enabled.

©2013-2022 Tencent Cloud. All rights reserved.

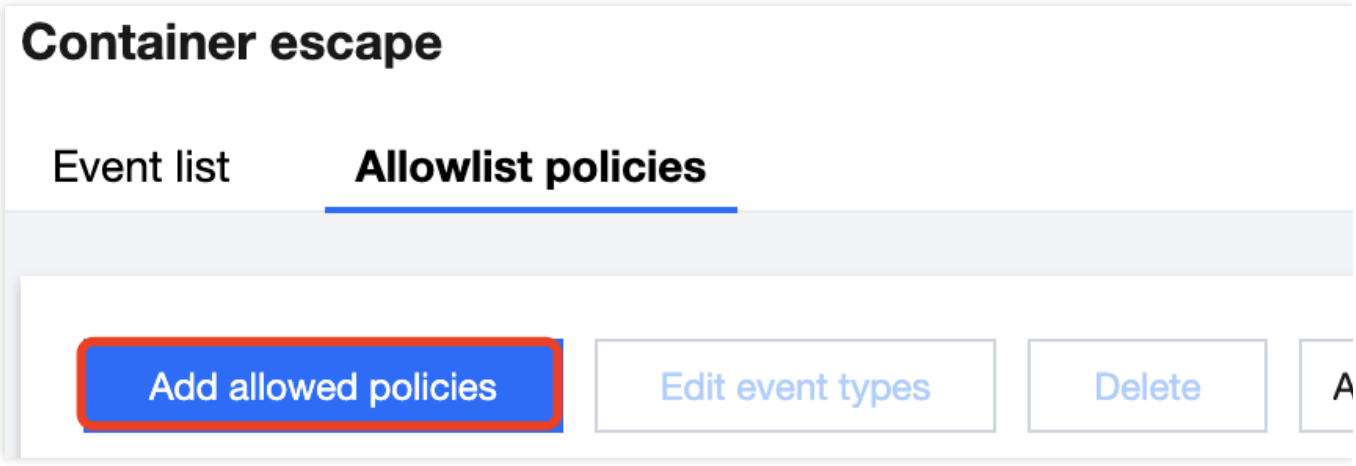


Allowlist policies

You can batch add images to the allowlist on the **Allowlist policies** tab to avoid further alerts.

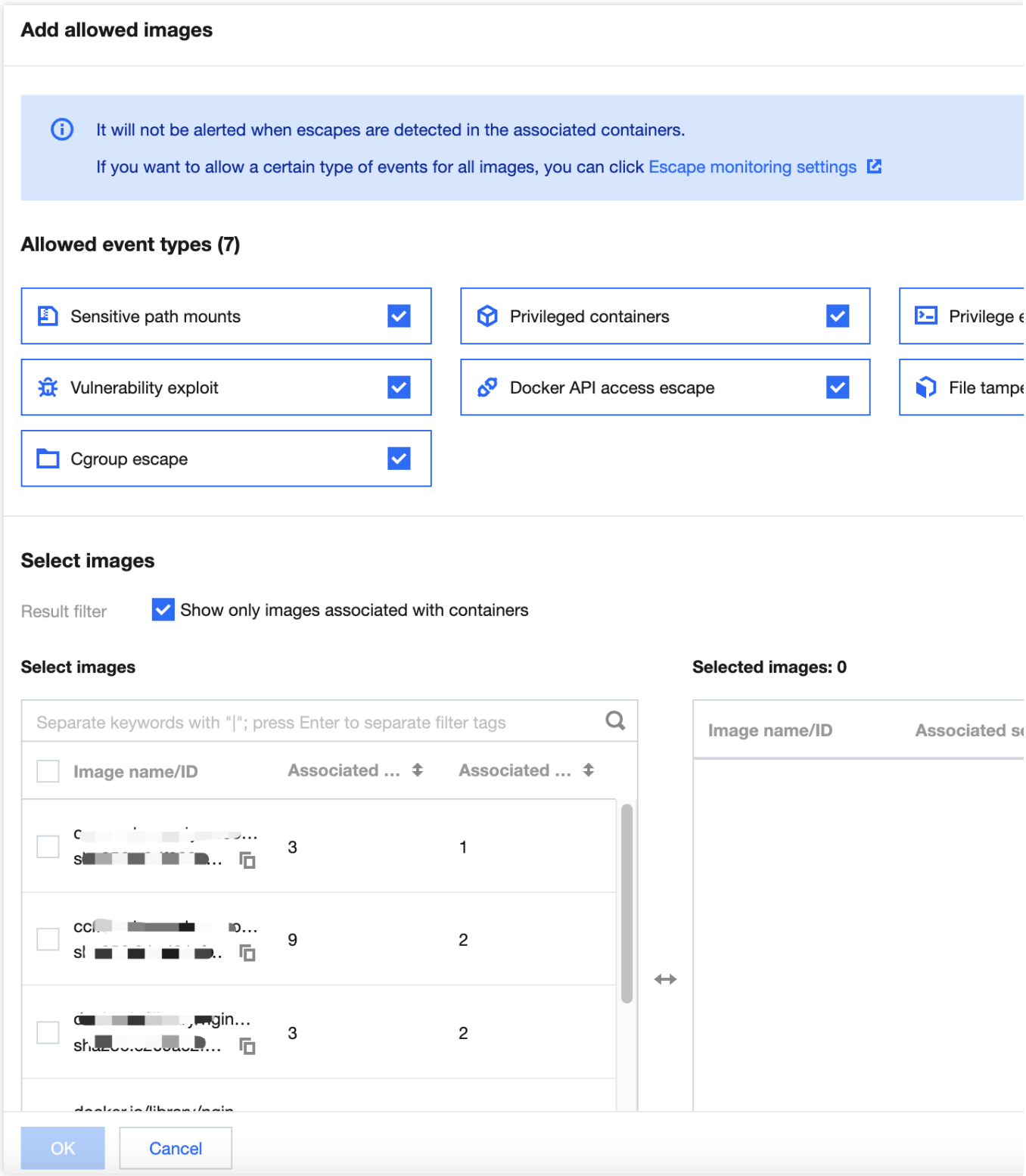
Adding to the allowlist

1. On the **Container Escape** > **Allowlist policies** page, click **Add allowed policies**.



2. On the **Add allowed images** page, select allowed event types and images and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



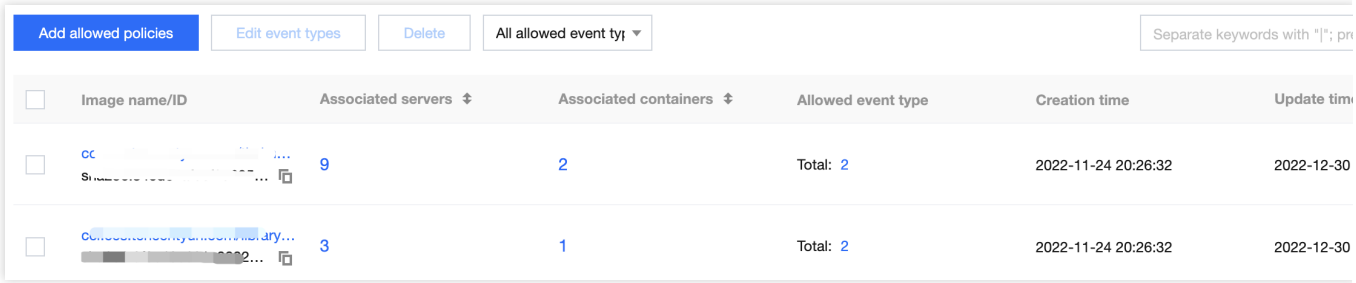
3. The list of allowlist policies can be managed based on the image ID. It displays the allowed event types of each image. For example, if three images are added to the allowlist, their records will be updated in the list.

Editing the allowlist

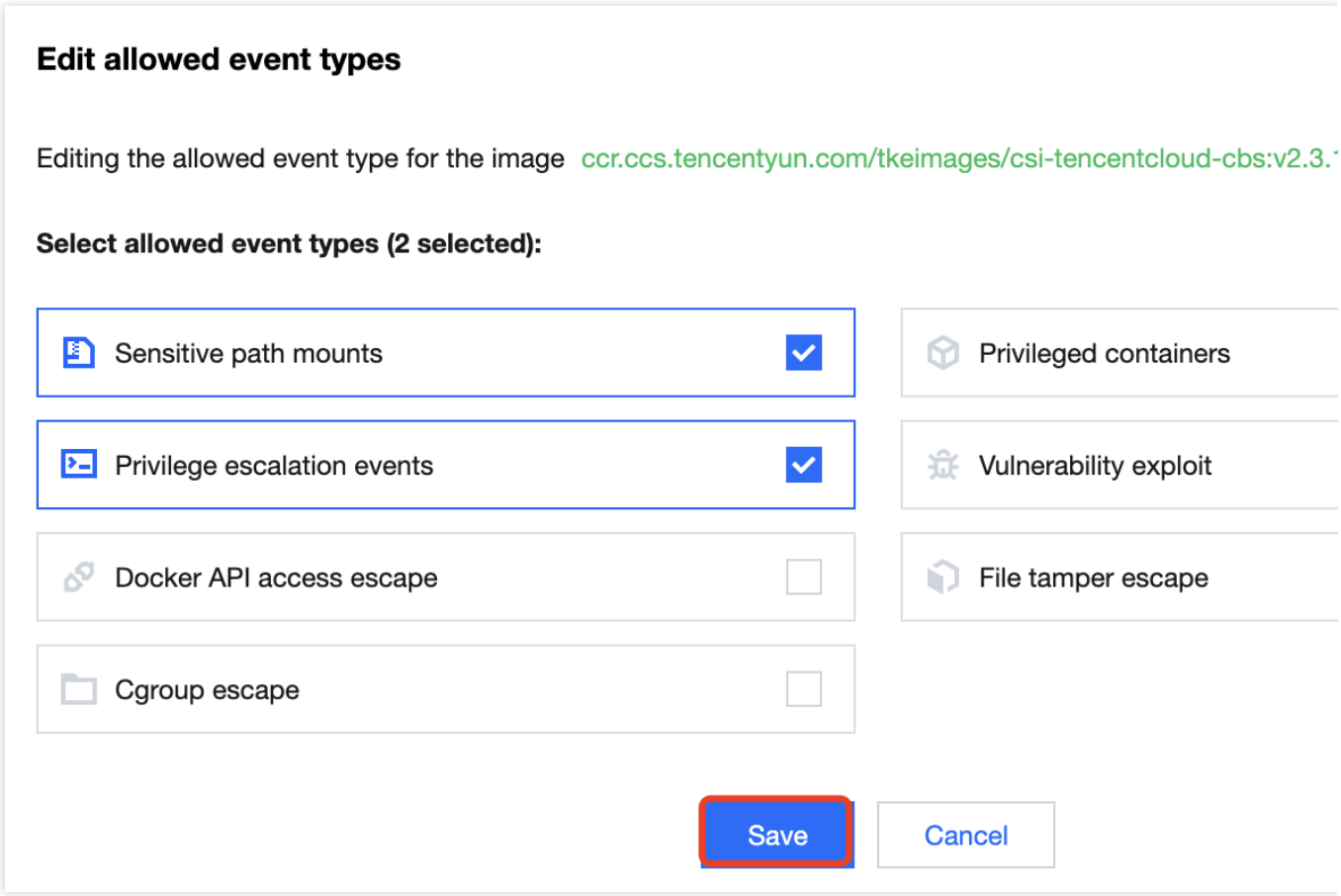
Edit the allowlist for an image

©2013-2022 Tencent Cloud. All rights reserved.

1.1 On the **Container Escape** > **Allowlist policies** page, click the **Edit allowed types** in the **Operation** column of the target image.



1.2 In the **Edit allowed event types** pop-up window, change the allowed event types and click **Save**.

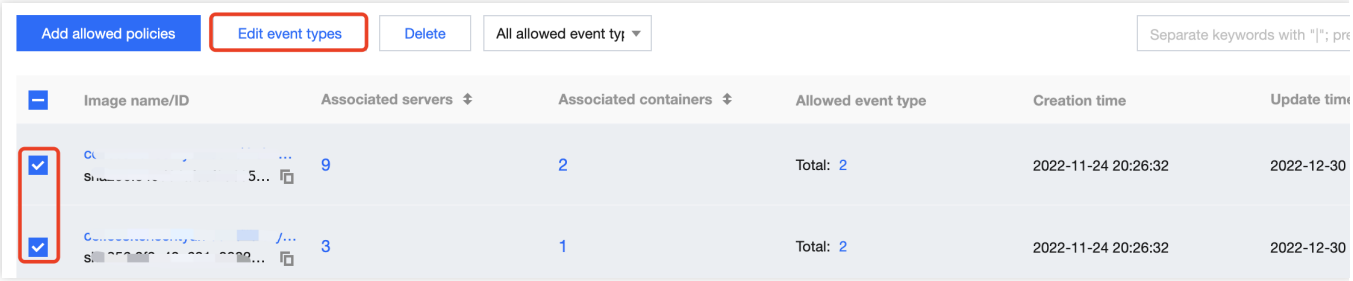


Edit the allowlist for multiple images

To change the allowed event types **to the same types** for multiple images, take the following steps:

1.1 On the **Container Escape** > **Allowlist policies** page, select one or multiple images and click **Edit allowed types** in the top-left corner.

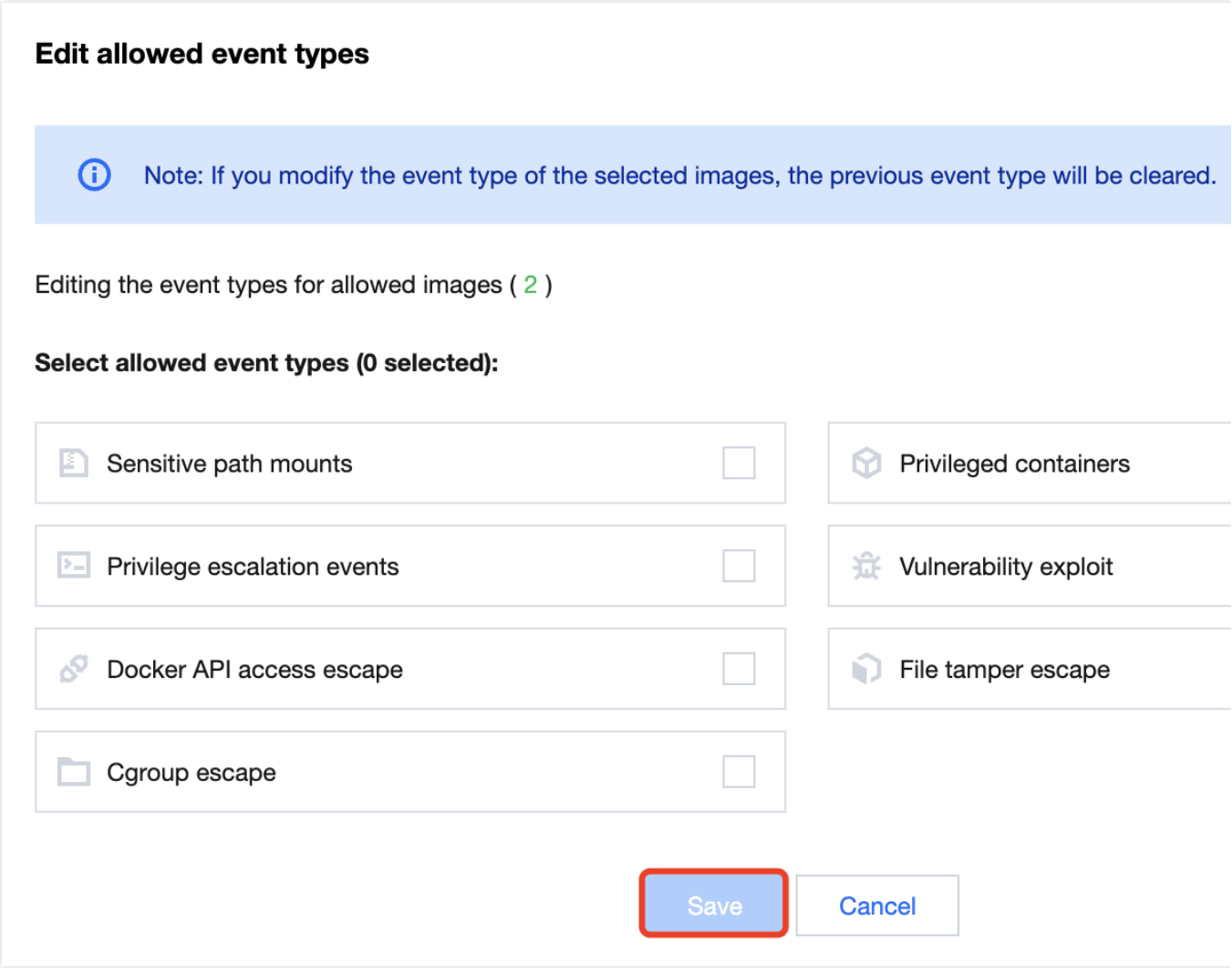
©2013-2022 Tencent Cloud. All rights reserved.



1.2 In the **Edit allowed event types** pop-up window, change the allowed event types and click **Save**.

Note:

After the event type is changed for the selected images, the previously set event type will be cleared.

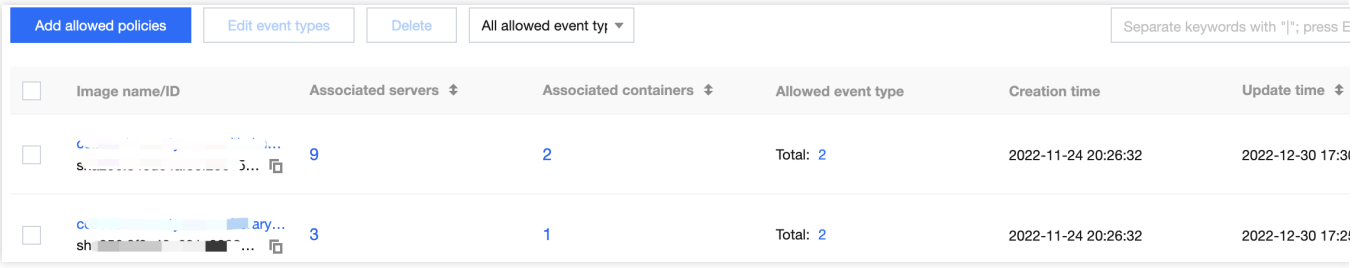


Deleting an image from the allowlist

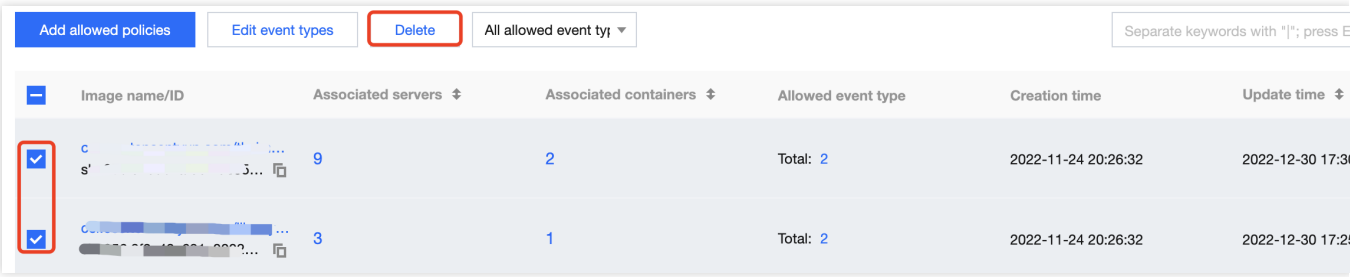
1. On the **Container Escape** > **Allowlist policies** page, delete one or multiple allowed images.

Deleting an allowed image: Select the target image and click **Delete** in the **Operation** column.

©2013-2022 Tencent Cloud. All rights reserved.



Batch deleting allowed images: Select one or multiple images and click **Delete** in the top-left corner.



2. In the pop-up window, click **OK**.

Note:

Alerts will be triggered when this kind of escape events occur again.

©2013-2022 Tencent Cloud. All rights reserved.

Virus Scanning

Last updated：2024-01-23 15:44:44

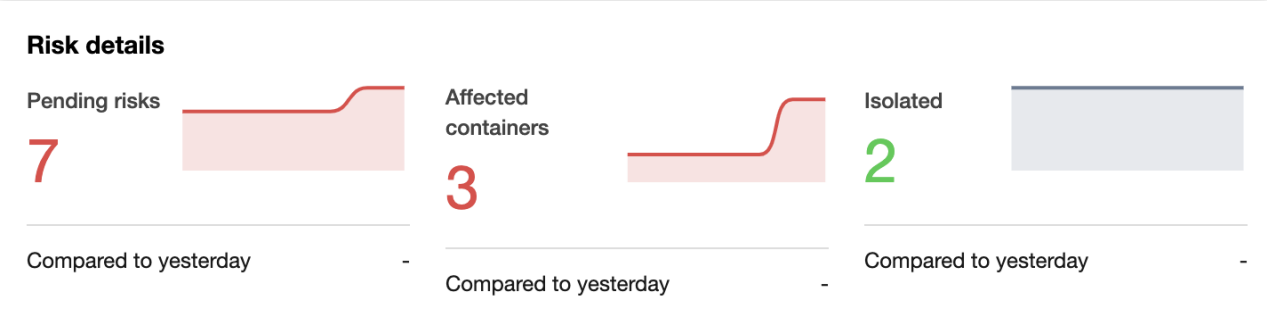
The virus scanning feature scans files in the container for viruses and trojans in real time or on schedule.

Viewing the Risk Trend

1. Log in to the TCSS console and click **Runtime Security** > **Virus Scanning** on the left sidebar.
2. The **Virus Scanning** page displays the pending risks, number of affected containers, and trend.

Pending risks: It displays the trend of pending risks in the last 7 days and the comparison with the previous day. Hover over the trend to display the number of pending risks of a certain day.

Affected containers: It displays the trend of affected containers in the last 7 days and the comparison with the previous day. Hover over the trend to display the number of affected containers of a certain day.



Setting the Risk Check

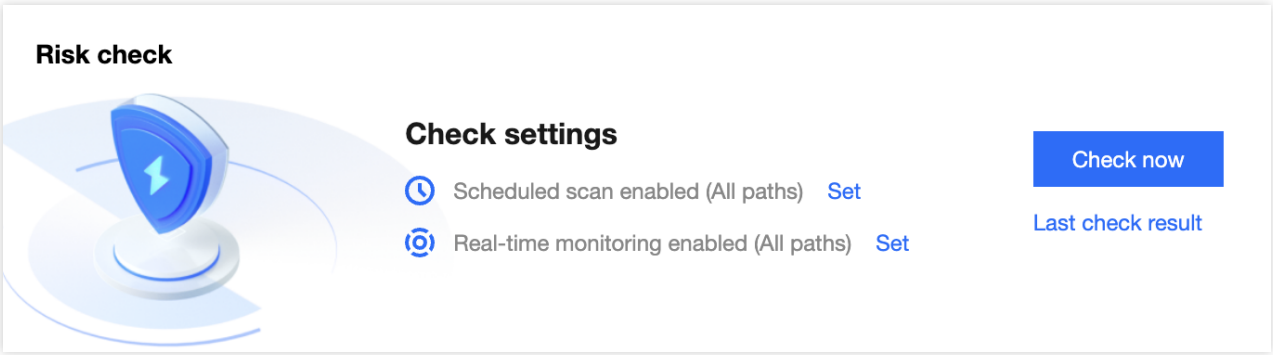
On the **Virus Scanning** page, the risk check module allows you to set the scheduled check and real-time monitoring.

Note:

Real-time monitoring applies to the incremental files in the configured path.

Scheduled check applies to all files in the configured path.

©2013-2022 Tencent Cloud. All rights reserved.



Setting scheduled check

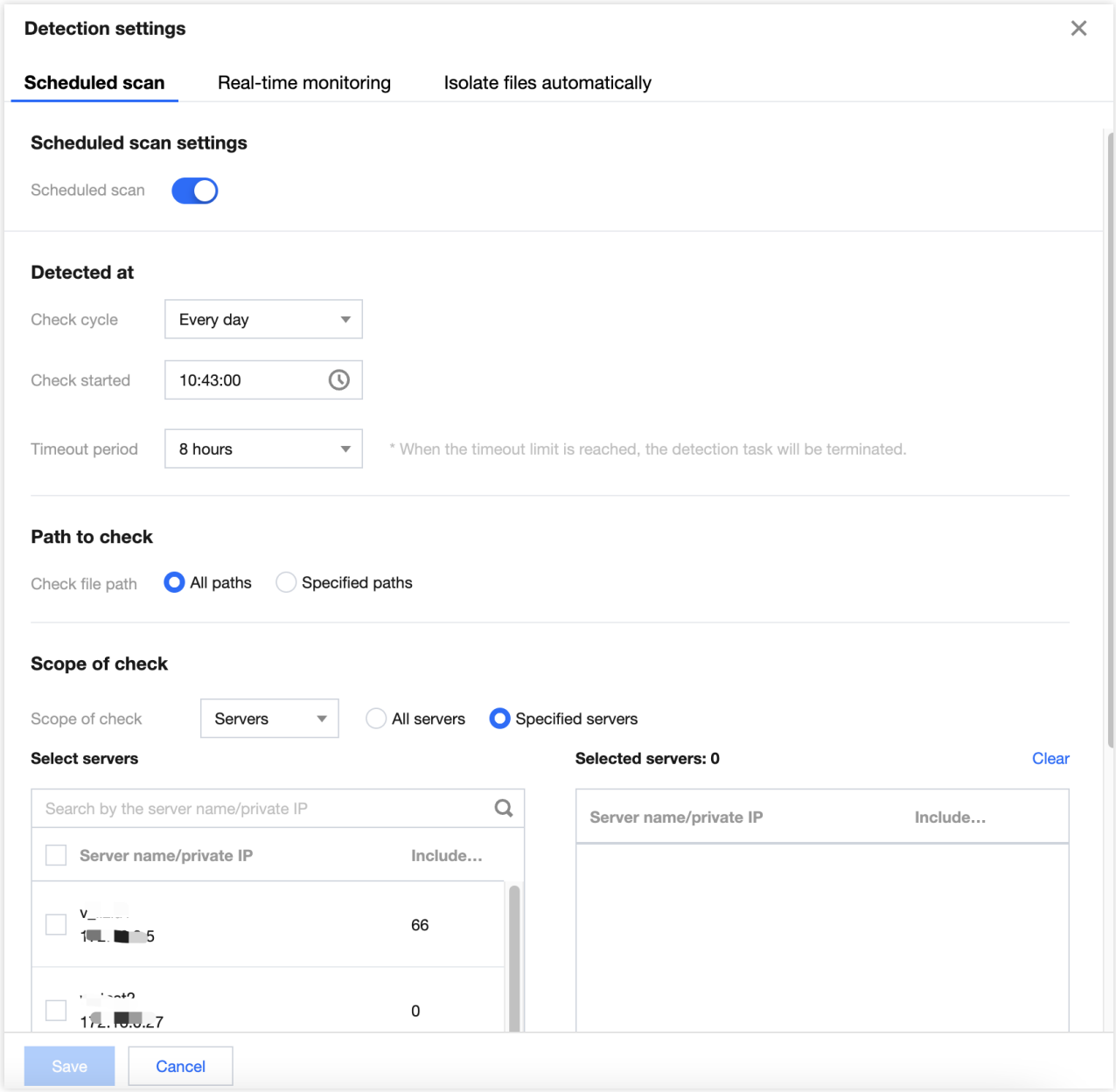
1. In the risk check module, click

on the right of **Scheduled check**.

2. On the **Scheduled check settings** page, click

to enable scheduled check and set the check time, path to check, and scope of check.

©2013-2022 Tencent Cloud. All rights reserved.



Parameter description:

Scheduled check: Toggle on or off the switch to enable or disable the feature.

Checked at

Check cycle: It can be **Every day**, **Every 3 days**, or **Every 7 days**.

Check start time: Configure when to start the scheduled check task.

Timeout period: When the time consumed reaches the timeout period, the check task will end. The default value is five hours.

Path to check

All paths: Check all file paths in the container.

Specified paths: Check specified file paths in the container.

Scope of check

©2013-2022 Tencent Cloud. All rights reserved.

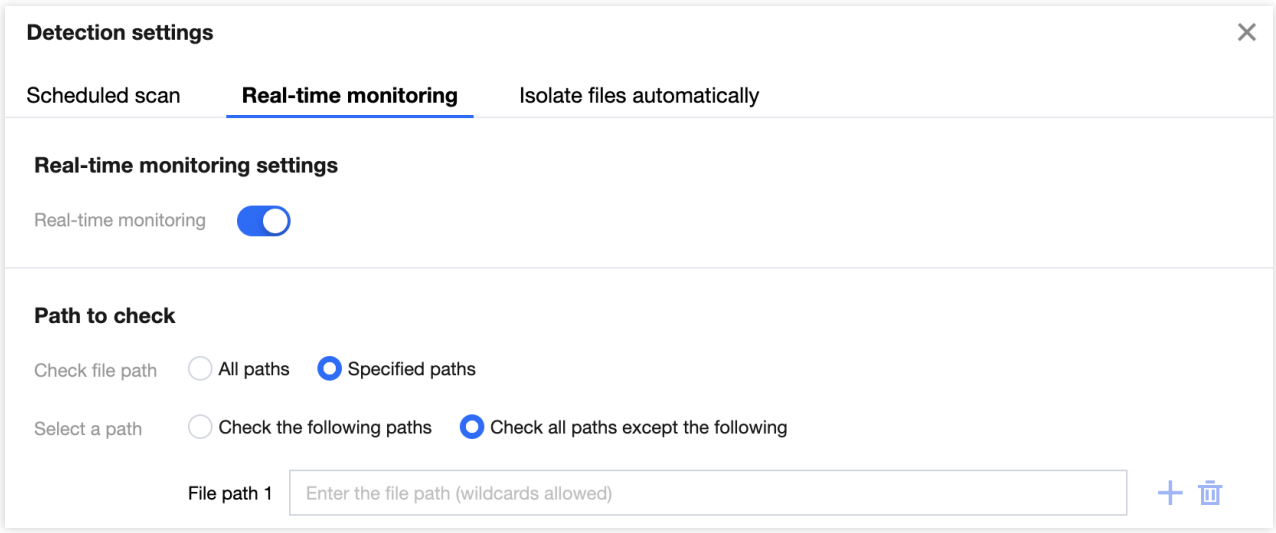
Nodes: You can select **All servers** or **Specified servers**. The latter option allows you to filter servers by server name/IP for scheduled scan.
Containers: You can select **All containers** or **Specified containers**. The latter option allows you to filter containers by container name/ID for scheduled scan.
3. Click **Save settings**.

Setting real-time monitoring

1. In the risk check module, click

on the right of **Real-time monitoring**.
2. On the **Real-time monitoring settings** page, click

to enable real-time monitoring and configure parameters.



Parameter description:

Real-time monitoring: Click

©2013-2022 Tencent Cloud. All rights reserved.

or

to enable or disable the feature.

Path to check

All paths: Check all file paths in the container.

Specified paths: Check specified file paths in the container.

Select a path: Select **Check the following paths** or **Check all paths except the following** as needed. Click

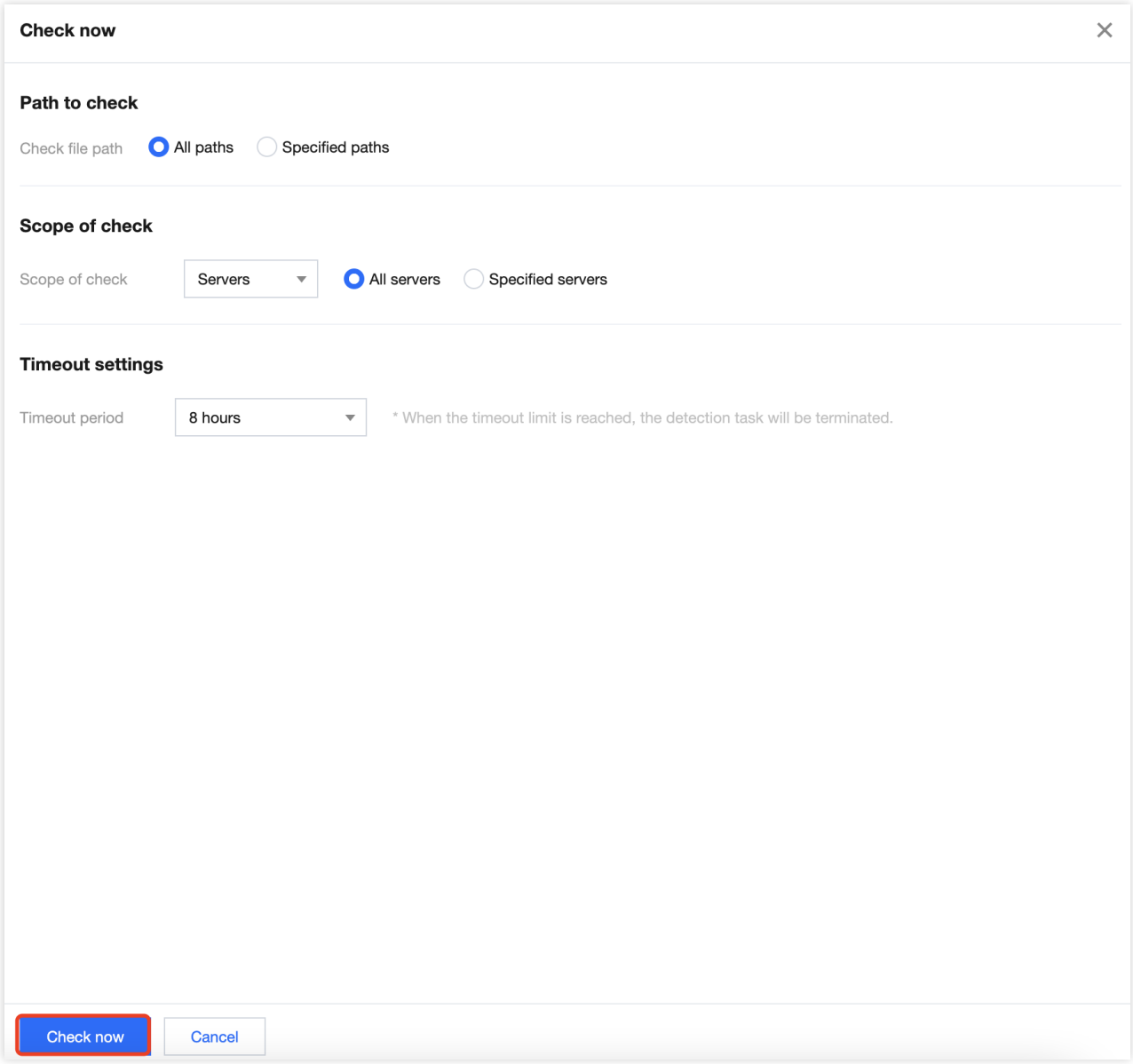
to add up to 30 paths.

3. Click **Save settings**.

Setting quick check

1. In the risk check module, click **Quick check**.
2. On the **Quick check** page, select the path to check and scope of check and set the timeout period.

©2013-2022 Tencent Cloud. All rights reserved.



Parameter description:

Path to check:

All paths: Check all file paths in the container.

Specified paths: Check specified file paths in the container.

Scope of check:

Nodes: You can select **All servers** or **Specified servers**. The latter option allows you to filter servers by server name/IP for scheduled scan.

Containers: You can select **All containers** or **Specified containers**. The latter option allows you to filter containers by container name/ID for scheduled scan.

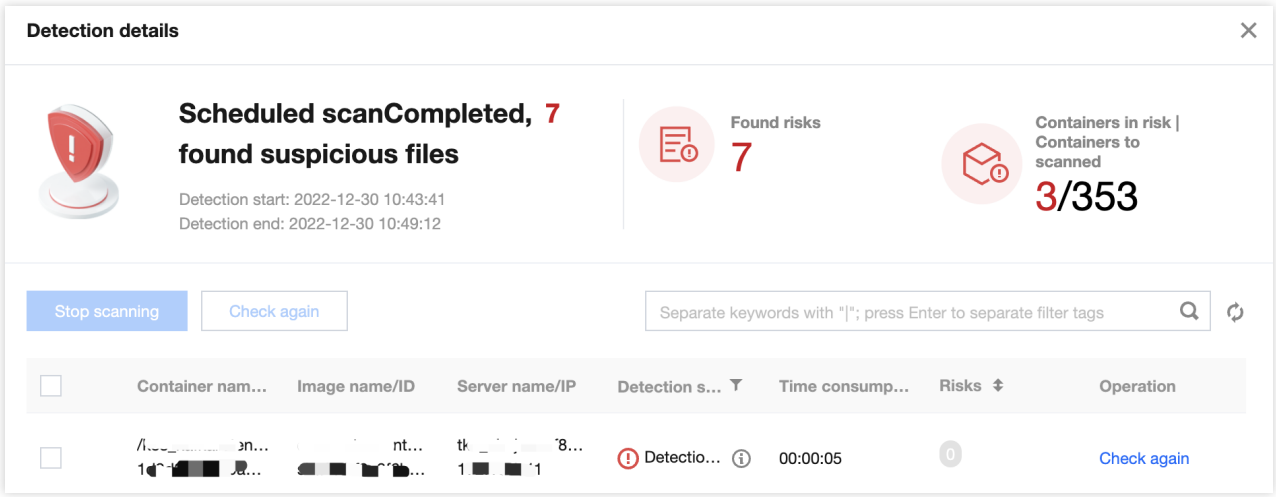
Timeout settings: When the time consumed reaches the timeout period, the check task will end. The default value is five hours.

3. Click **Start check**.

©2013-2022 Tencent Cloud. All rights reserved.

Viewing the last check result

In the risk check module, click **Last check result** to view the details.



Check details:

Overview

Numbers of suspicious files, containers in risk, and scanned containers if suspicious files are found in the last scan.

Start time and end time of the last scan task.

Check details list: Displays the overview of suspicious files found in the last scan and aggregates them by container. The fields in the list include the container name/ID, image name/ID, node name/IP, check status, time consumption, number of risks, and operation items.

You can check again or stop a running task.

You can search by server name/IP, container name/ID, or image name/ID.

Click

to view the name and path of the suspicious file, the virus name, and the **View details** button. Click **View details** to view the details of the suspicious file.

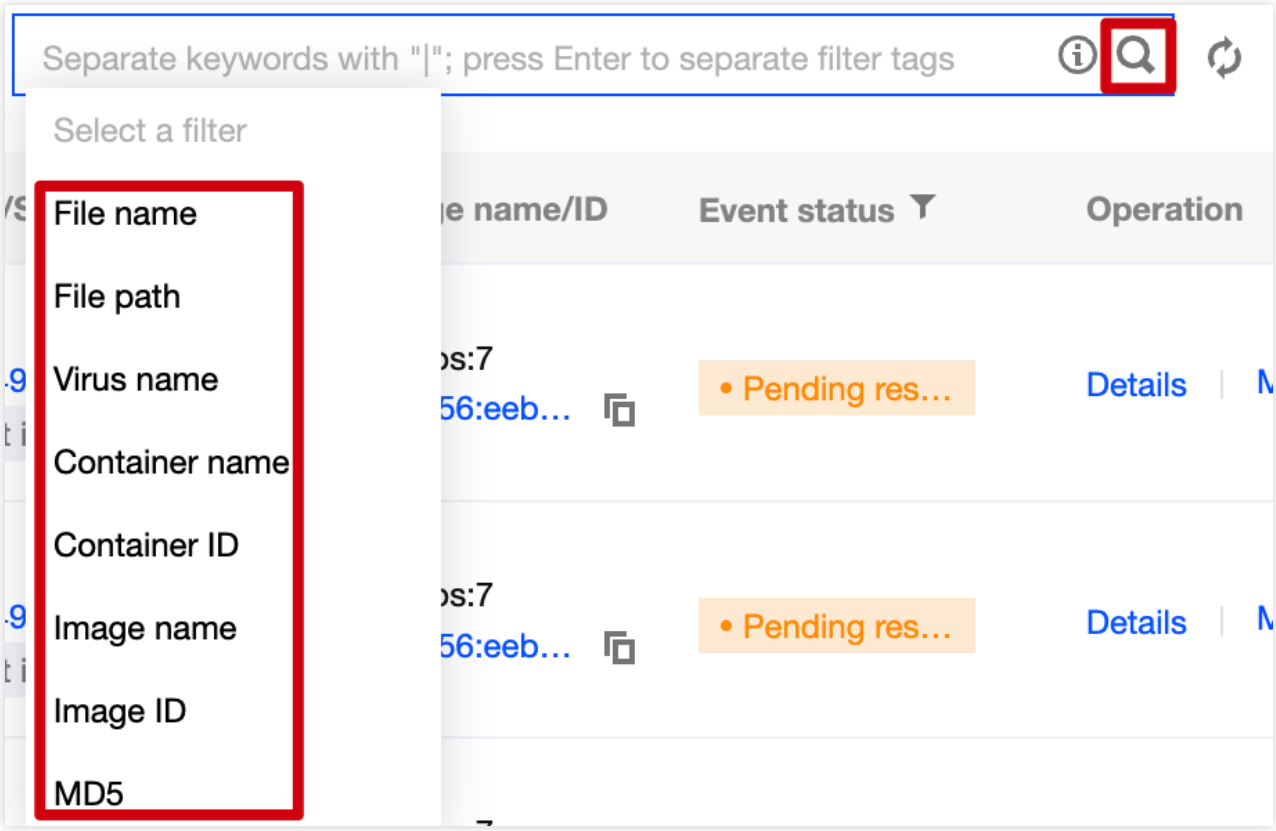
Viewing the Event List

On the **Virus Scanning** page, the event list module displays the virus and trojan check results.

Filtering events

©2013-2022 Tencent Cloud. All rights reserved.

In the event list module, filter events in either of the following methods:
Click the search box and search for virus and trojan events by keyword such as filename, file path, virus name, or container name.



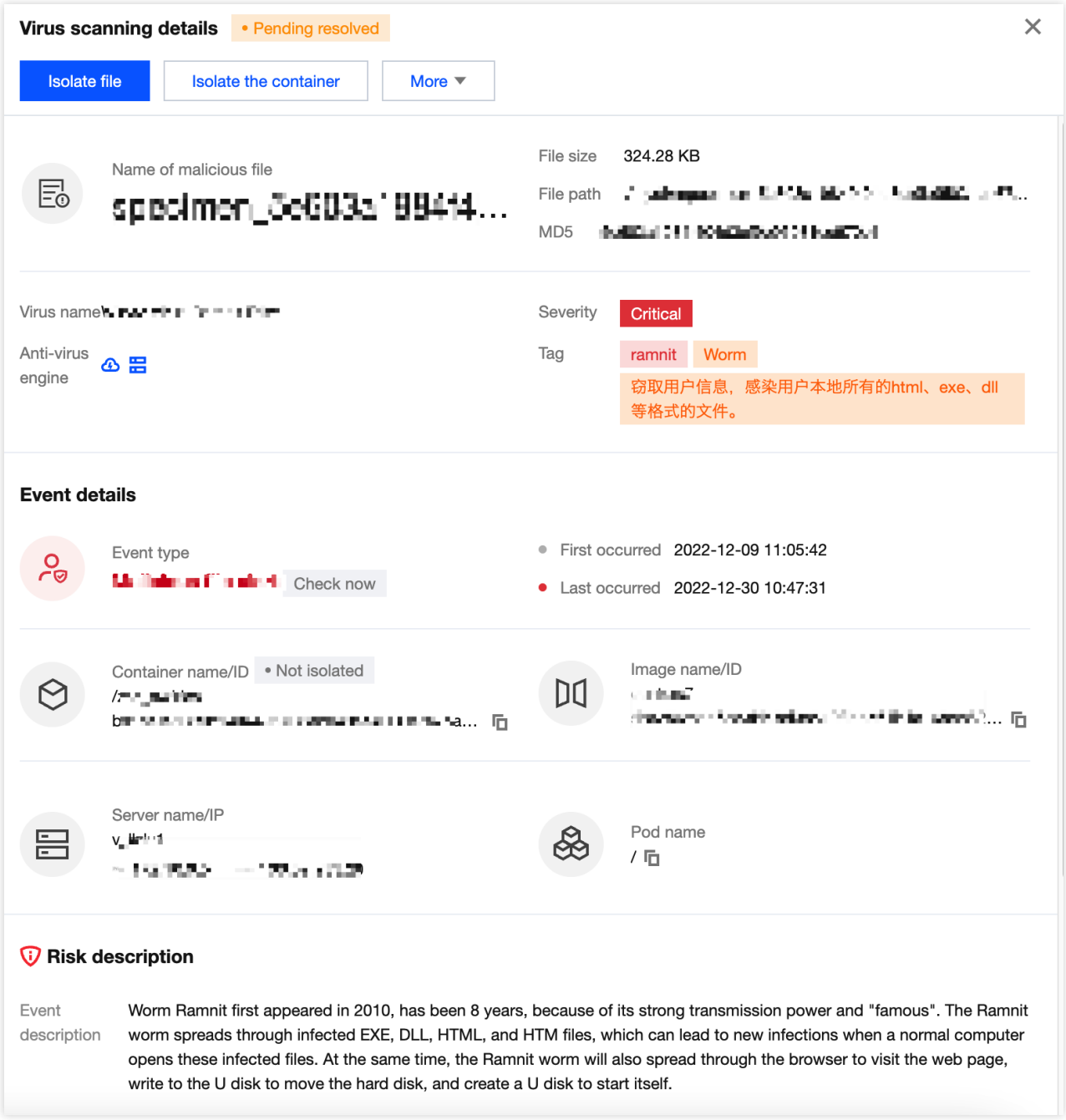
Click **Container status** or

on the right to search for virus and trojan events by container status or event status.

Viewing details

In the event list module, click **View details** to pop up the drawer on the right, which displays the basic information of the virus file, event details, event description, and process information. The process information is displayed only in the details of events reported by the real-time monitoring feature.

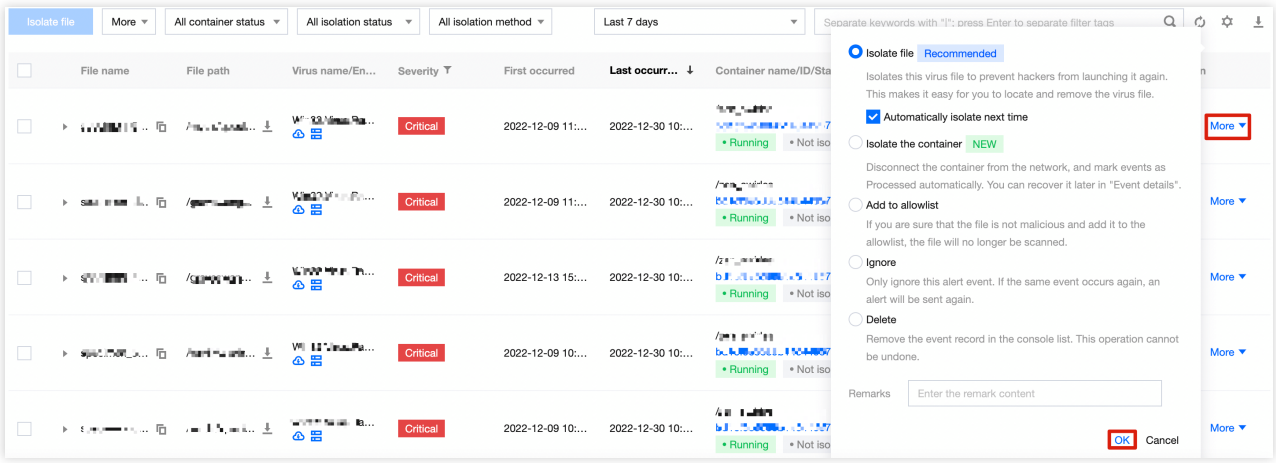
©2013-2022 Tencent Cloud. All rights reserved.



Processing an event

In the event list module, click **Process now** to add an event to the allowlist or isolate (recommended), ignore, or delete it and then click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Parameter description:

Add to allowlist: If you are sure that the file is not malicious and add it to the allowlist, **the file will no longer be checked**.

Isolate (recommended): An isolated virus file cannot be launched again by a hacker. This makes it easy for you to locate and remove the virus file.

Ignore: Only ignore this alert event. If the same event occurs again, an alert will be sent again.

Delete: The event record will no longer be displayed in the console and cannot be recovered once deleted. Proceed with caution.

Automatic File Isolation

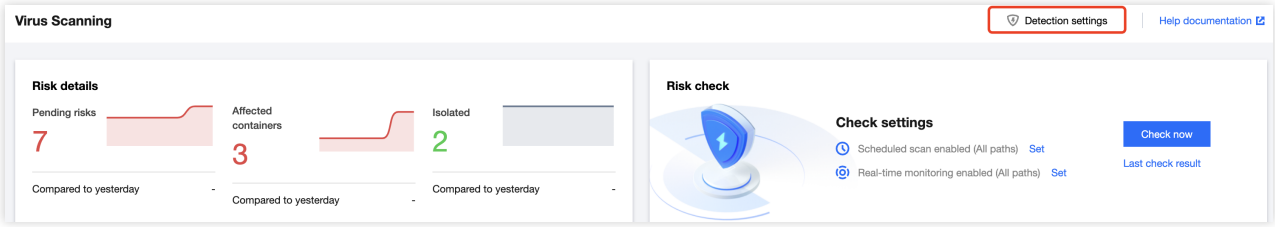
TCSS adds the automatic trojan isolation feature, which automatically isolates files found to be in the system blocklist and custom malicious files.

Automatic file isolation

TCSS automatically isolates files found to be in the system blocklist. Some malicious files still need to be manually confirmed and isolated. We recommend you check all the security events in the virus scanning list to ensure that all files are processed. You can recover the files isolated by mistake from the list of isolated files.

1. Log in to the TCSS console and click **Runtime Security** > **Virus Scanning** on the left sidebar.
2. On the **Virus Scanning** page, click **Detection settings** in the top-right corner.

©2013-2022 Tencent Cloud. All rights reserved.



3. In the **Detection settings** pop-up window, click **Isolate files automatically**.
4. In the automatic file isolation module, click

to enable or disable automatic isolation. You can also isolate and end processes involving malicious files.

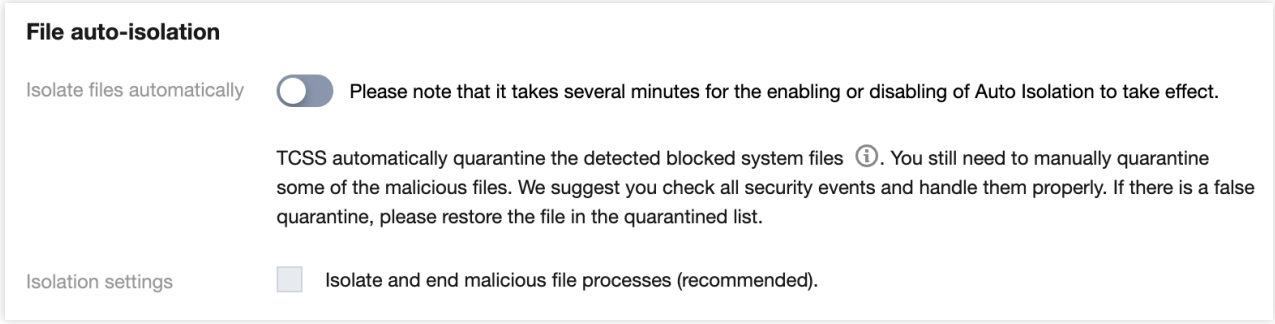
Note:

Blocked system files: This list is provided by Tencent Cloud security experts. Files in the list are automatically isolated.

The **Auto isolation** switch is toggled off by default and can be toggled on as needed. When enabling automatic isolation, you can specify whether to isolate and end processes involving malicious files.

When automatic isolation is enabled, it takes effect for both the system blocklist and custom blocklist.

When automatic isolation is disabled, it takes effect for both the system blocklist and custom blocklist, and malicious files associated with the alert will not be automatically isolated.

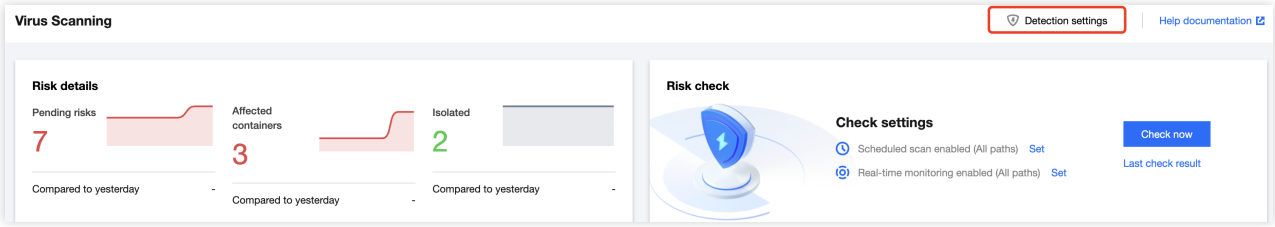


Custom isolated files

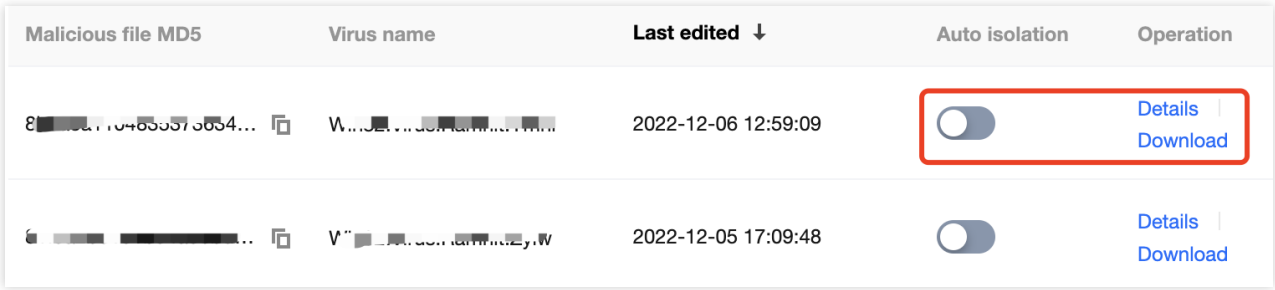
You can customize and view the list of custom isolated files and enable or disable automatic isolation for the files.

1. Log in to the TCSS console and click **Runtime Security** > **Virus Scanning** on the left sidebar.
2. On the **Virus Scanning** page, click **Detection settings** in the top-right corner.

©2013-2022 Tencent Cloud. All rights reserved.



3. In the **Detection settings** pop-up window, click **Isolate files automatically**.
4. In the **Custom isolated files** module, toggle on or off the **Auto isolation** switch, view the details, and download the files.

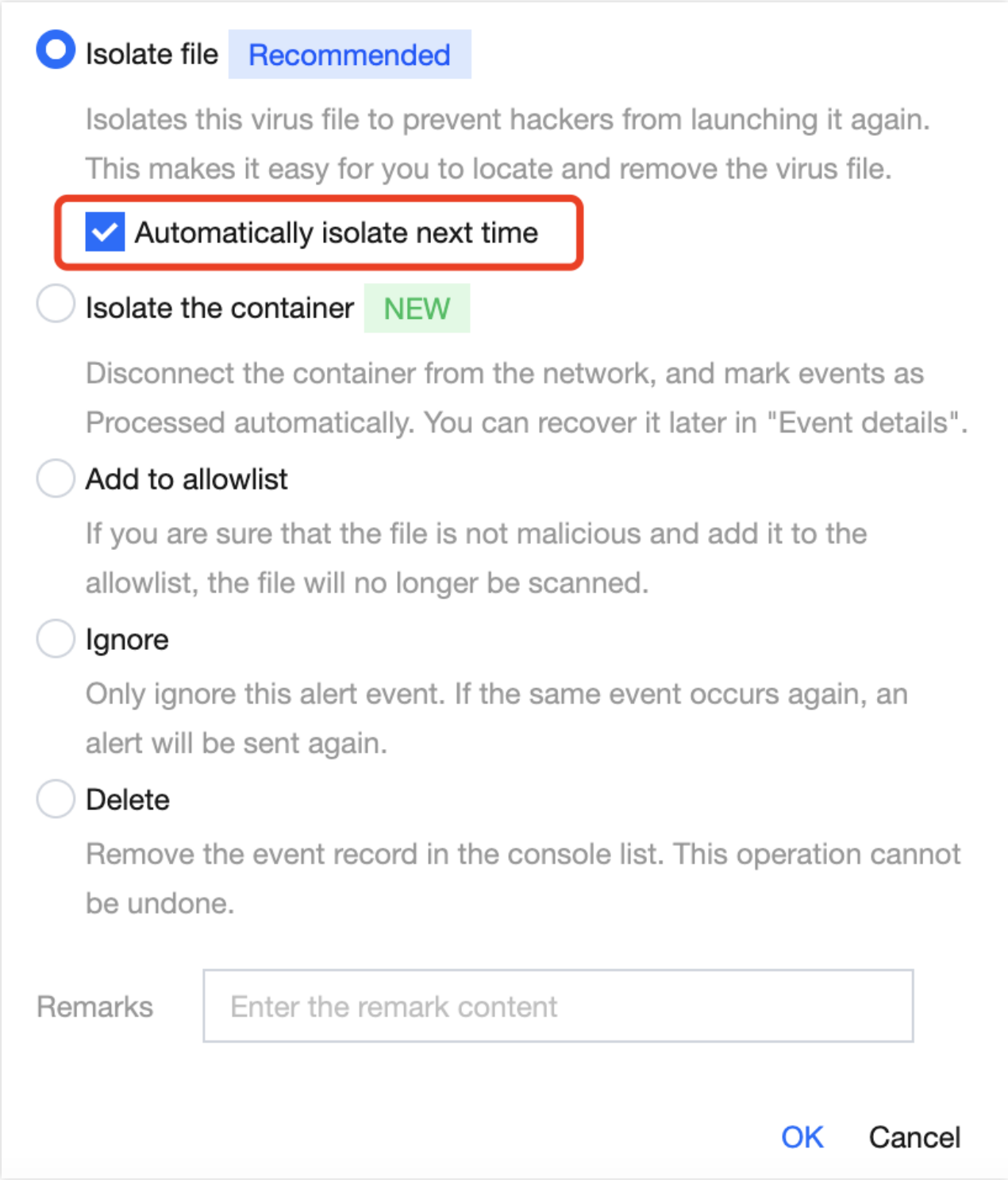


Instructions:
Toggle on or off the **Auto isolation** switch to enable or disable the feature.
Click **Details** to view the basic information of the malicious file, description, and fix suggestion.
Click **Download** to download the malicious file.

List of isolated files

In the event list on the **Virus Scanning** page, when you manually isolate a malicious file and select "Automatically isolate next time", the MD5 value of the file will be recorded in the list of custom isolated files, and the **Auto isolation** switch will be on. Then, the system will automatically isolate similar files. When the option is deselected, the record will be deleted from the list, and automatic isolation will no longer take effect.

©2013-2022 Tencent Cloud. All rights reserved.



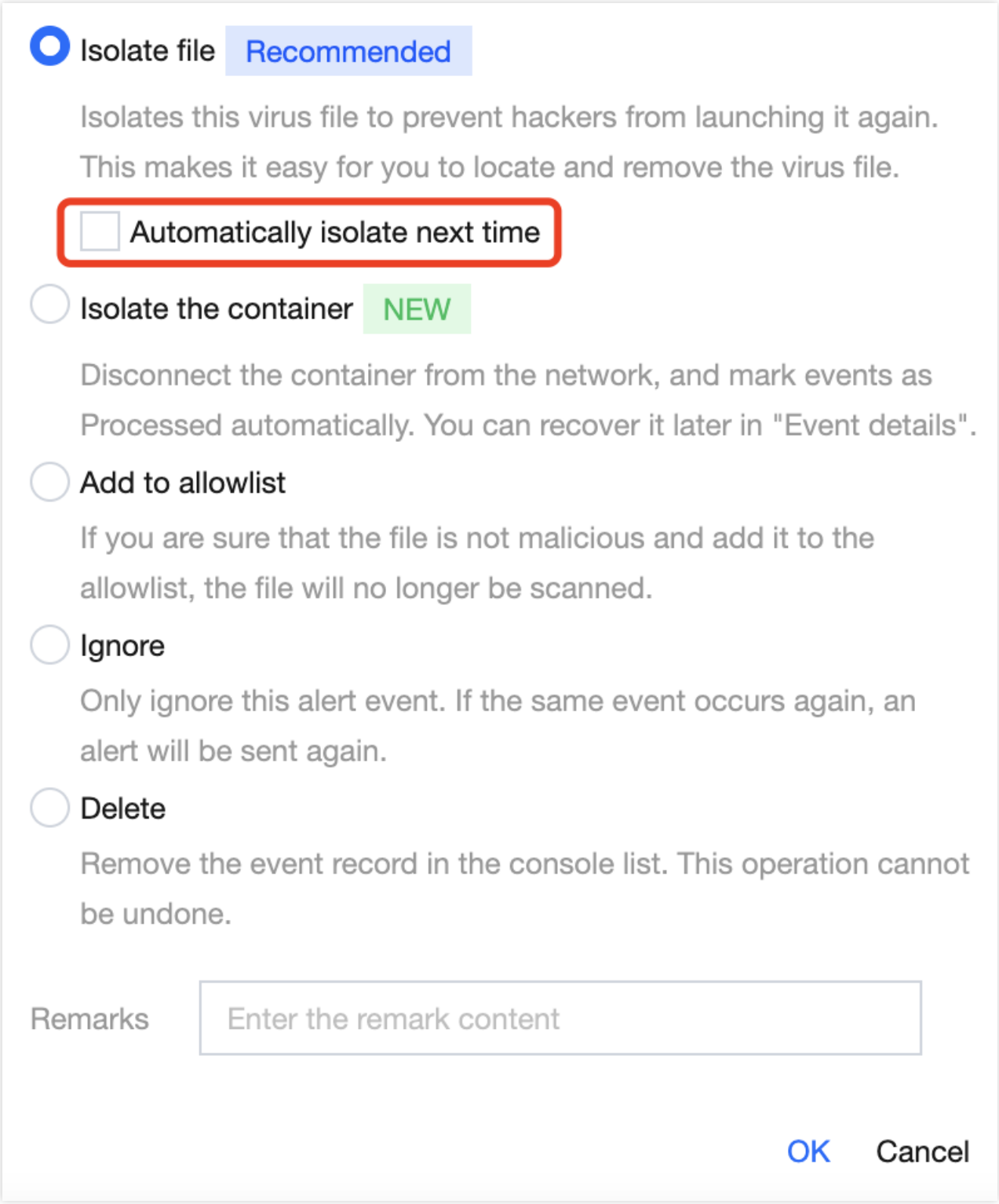
In the event list on the **Virus Scanning** page, when you manually isolate a malicious file and don't select "Automatically isolate next time", the MD5 value of the file will be recorded in the list of custom isolated files, and the **Auto isolation** switch will be off.

Note:

To make the automatic isolation of custom isolated files effective, you need to toggle on the **Auto isolation** switch; otherwise, no automatic isolation will be performed even if you have selected "Automatically isolate next time" when

©2013-2022 Tencent Cloud. All rights reserved.

processing security events.



©2013-2022 Tencent Cloud. All rights reserved.

Outbound Malware

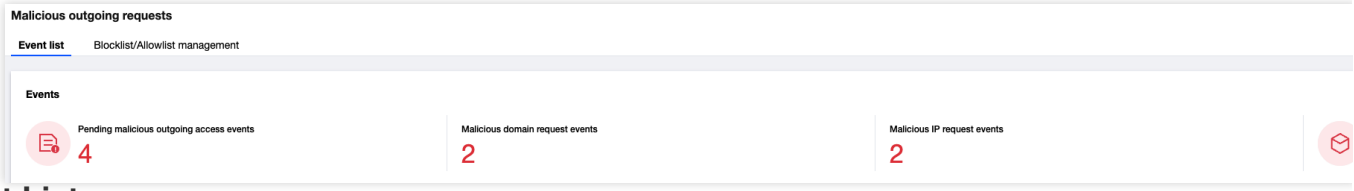
Last updated：2024-08-13 17:08:45

When a container initiates an outbound request to a malicious domain name or IP, TCSS will detect such behavior and provide you with real-time alarms. If it is discovered that the container is accessing a malicious domain name/IP, your container may have already been compromised, as the malicious domain name/IP could be a hacker's remote control server, malicious software download source, and mining pool address. You need to promptly troubleshoot as the following:
1. Check the malicious processes and illegal ports within the container, and delete suspicious startup items and scheduled tasks.
2. Troubleshoot the risks existing in the container, such as performing vulnerability scans and Trojan scans.
3. Harden the images used by the container and replace the running containers.

Event List

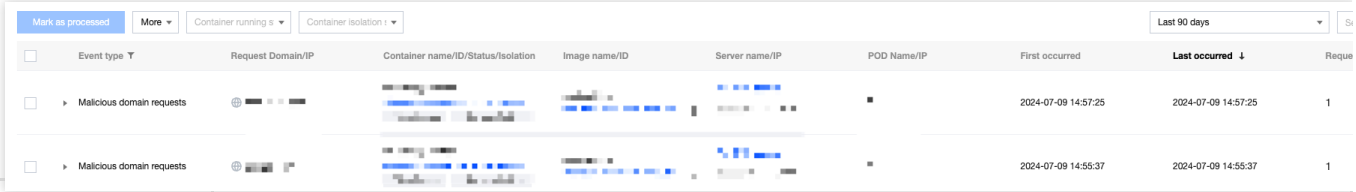
Event Overview

1. Log in to the TCSS console. In the left sidebar, click **Runtime Security** > **Outbound Malware** to enter the event list page by default.
2. In the event overview on the event list page , the number of pending outbound malware events and the affected containers will be reported in real-time based on the security events reported by the system.



Event List

In the event list, the outbound malware events from the last 7 days are displayed by default. To view more events, you can adjust the query duration. The fields displayed in the list are as shown in the table below.



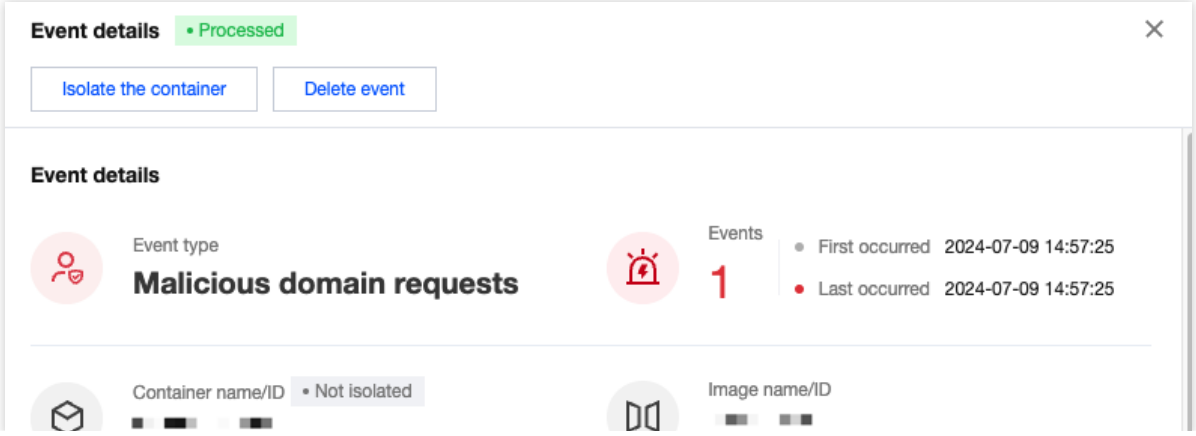
Field Name	Field Details
Event Type	Malicious Domain Requests

©2013-2022 Tencent Cloud. All rights reserved.

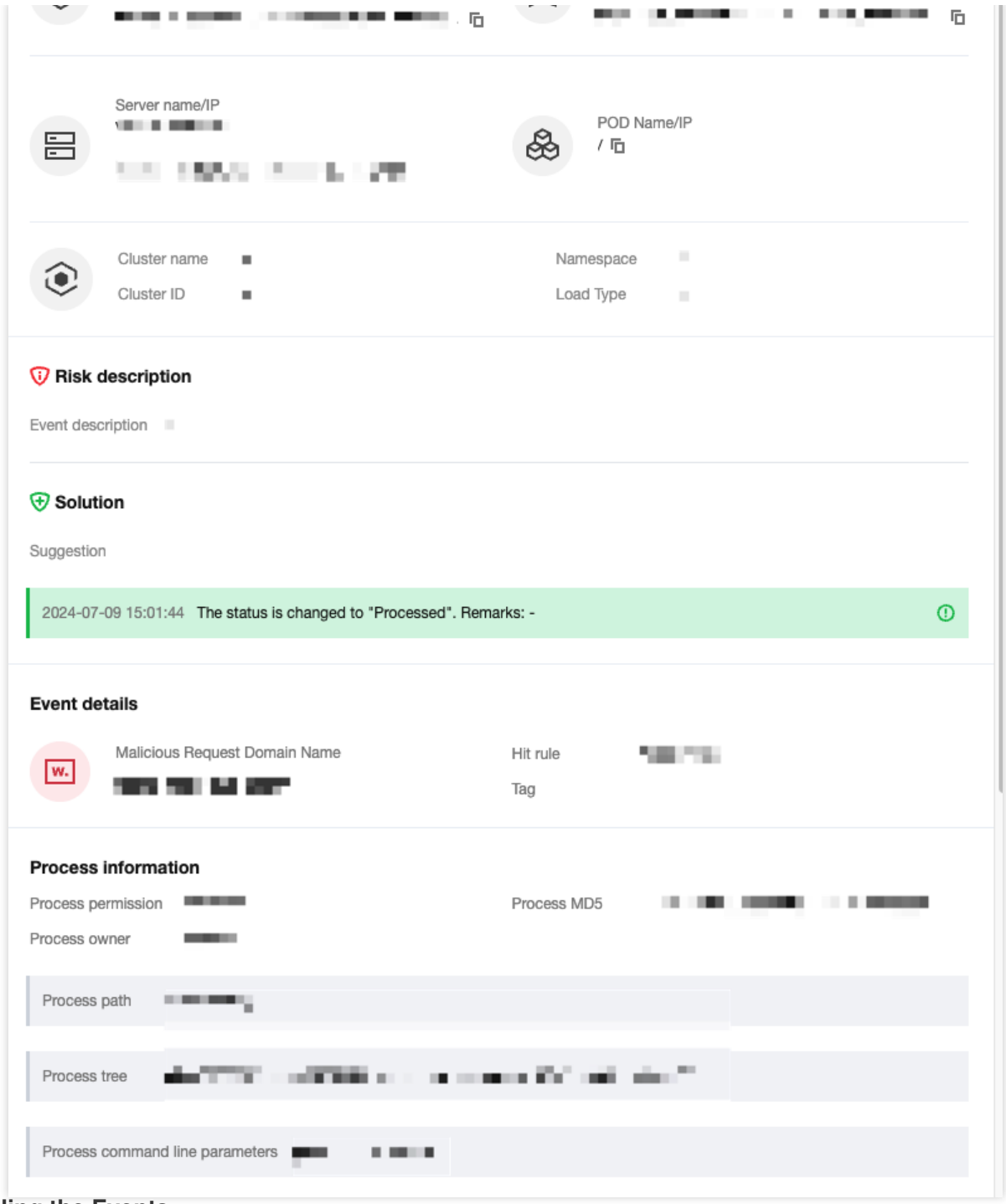
Request Domain/IP	Domain Details of the Triggered Security Event
Container Name/ID/Running Status/Isolation	Displays information related to container assets such as name, ID, and running status. If the customer believes that the security event is valid, meaning the container may have been compromised, they can click to isolate the container to prevent the risk from spreading within the private network.
Image Name/ID	The source mirror of the container that triggered the security event can be viewed by clicking **Image ID** for details such as image security risks, component information, and build history.
Host Name/IP	The CVM node where the container that triggered the security event is located. Displays the node's name and private/public IP address information.
First Occurred	The time when this security event first occurred.
Last Occurred	The time when this security event most recently occurred.
Requests	The system aggregates and displays pending security events by container ID, domain name, process path, and process startup user. The aggregation cycle is every day.
Status	Including pending, processed, ignored, and allowlisted.
Operation	Click **Details** to view event details. Details include event details, asset information (such as associated container, image, and host), risk description, solution, requested domain name details, and Layer-3 process information. Click **Process** to process security events. This includes adding to allowlist, marking as processed, isolating the container, ignoring, and deleting records.

Viewing Details

In the event list, click **Details** to enter the event details. This page displays event details, associating assets (such as container, image, and host), risk description, solution, requested domain name details, and Layer-3 process information.



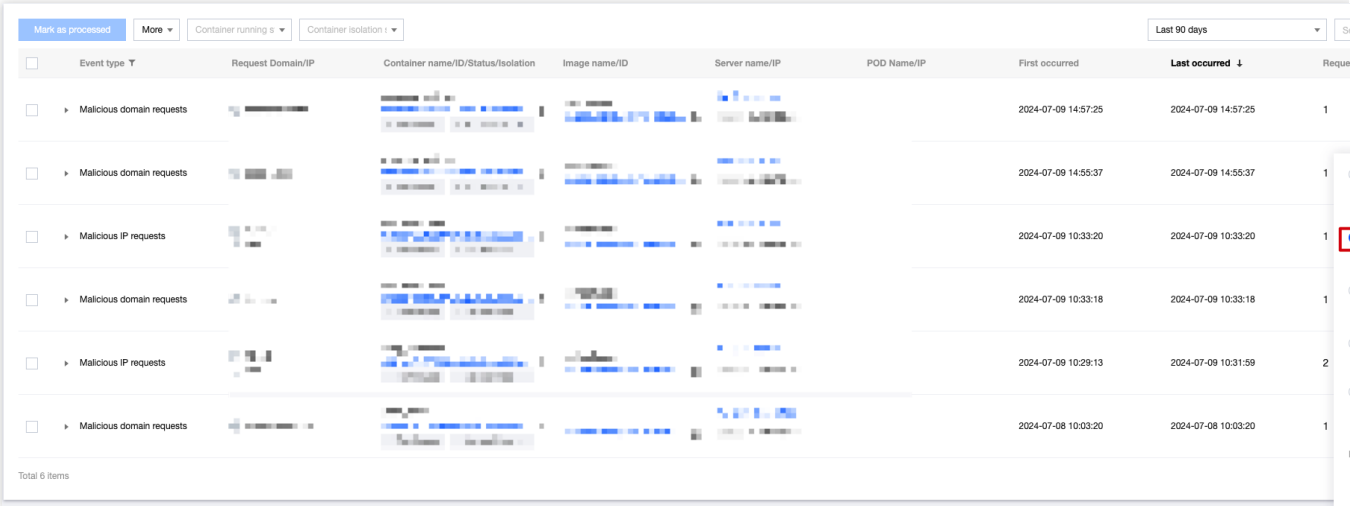
©2013-2022 Tencent Cloud. All rights reserved.



Handling the Events

1. In the event list, click **Process** to select actions like adding to allowlist, marking as processed, isolating the container, ignoring, and deleting records. Click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



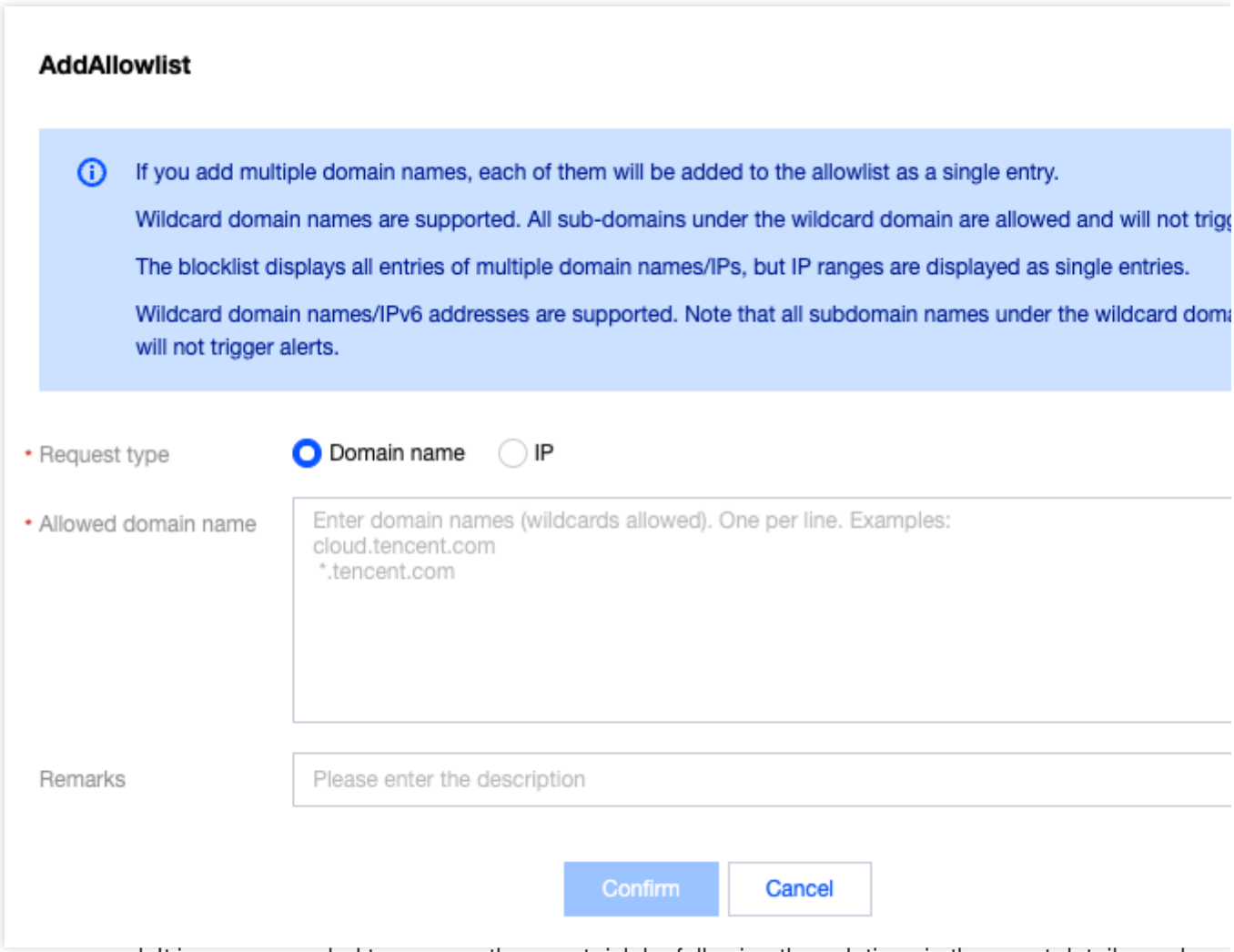
2. In the secondary confirmation window, perform the following operations:

Add to allowlist: Enter the allowlist domain name and remarks, and click **Confirm**. When users add to the allowlist, the system automatically fills in the requested domain name based on the allowlisted source event. If necessary, it can be manually adjusted to the parent domain name. At the same time, you can check Batch Process Similar Events (batch allowlist events triggered by the same domain name). After you have checked and confirmed, the system will batch allowlist security events generated by the same domain name.

Note:

If you confirm that the domain name request is a normal behavior, you can add the domain name to the allowlist allow rules. When the same domain name request appears again, **it will be allowed directly without interception/alert. Proceed with caution.**

©2013-2022 Tencent Cloud. All rights reserved.



Mark as processed: It is recommended to process the event risk by following the solutions in the event details, and click **Confirm**. After processing, you can mark the event as processed.
Isolate the container: If you confirm to isolate the container, the system will disable its network communication and mark the event as processed. Proceed with caution. Click **Confirm** to isolate. After isolation, you can remove the isolation from more operations or the container asset list.
Ignore: Click **Confirm** to ignore only this alarm event. If the same event occurs again, an alarm will still be triggered.
Delete: Click **Delete** to delete the selected event record. It will no longer be displayed in the console and cannot be recovered. Proceed with caution.

Allowlist/Blocklist Management

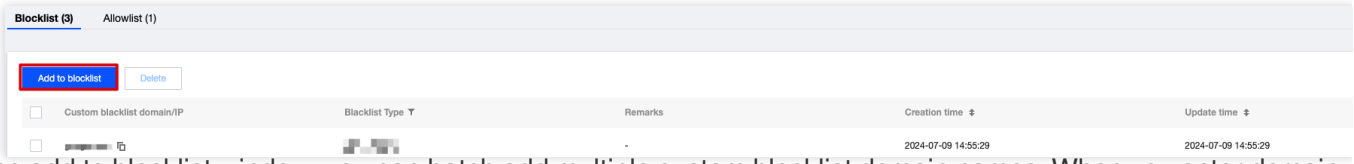
Aside from the system blocklist provided by the TCSS products, customers can also have their custom domain name blocklist and domain name allowlist. The priority of effectiveness is: **allowlist > blocklist.**
Blocklist: When the container initiates an outbound request to a domain name on the list, the system will determine it as the outbound malware, generating a real-time alarm. You can view it in the event list.

©2013-2022 Tencent Cloud. All rights reserved.

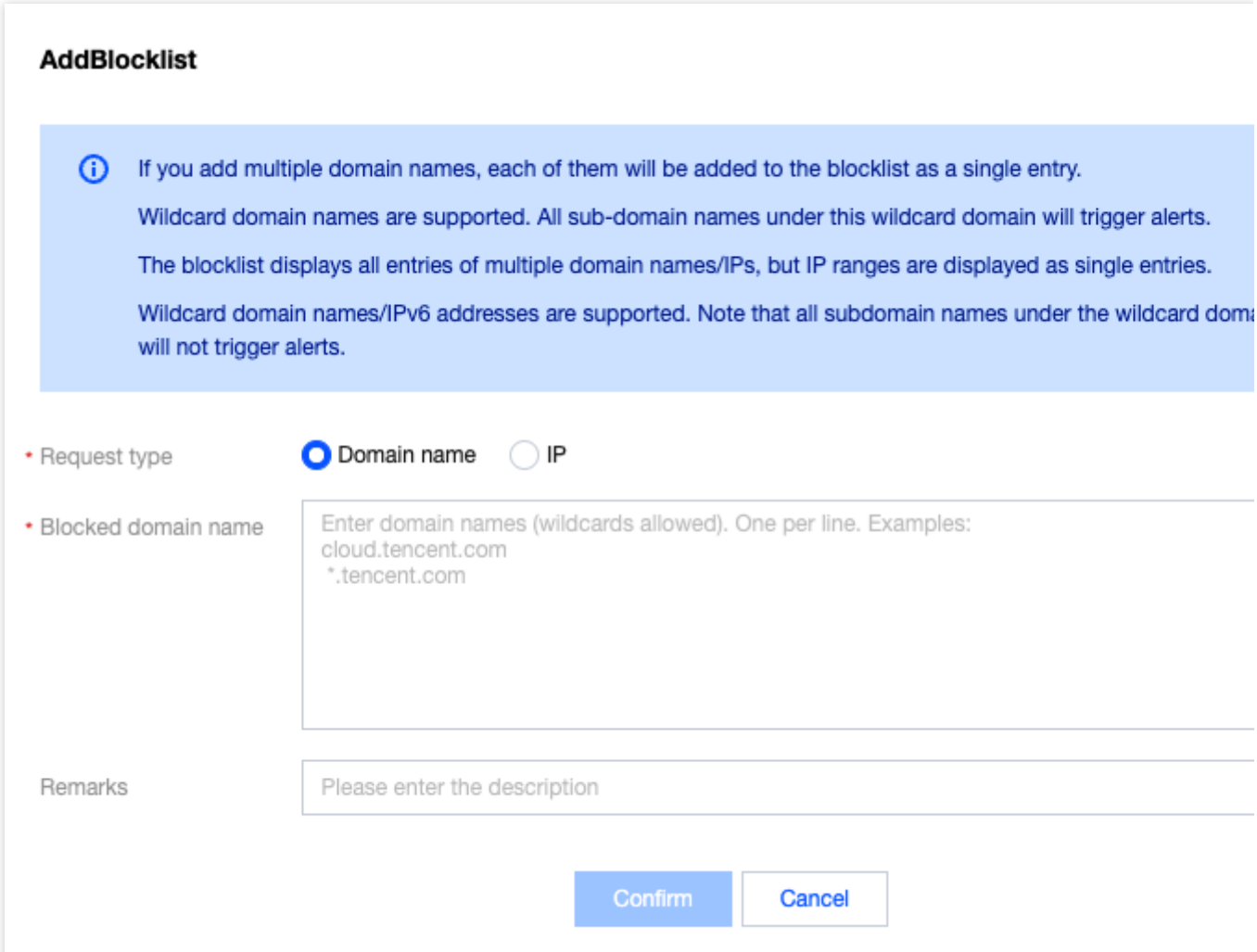
Allowlist: When the container initiates an outbound request to a domain name on the allowlist, the system will allow it directly without triggering an alarm.

Blocklist Management

1. Log in to the TCSS console. In the left sidebar, click **Runtime Security** > **Outbound Malware** > **Blocklist/Allowlist management**.
2. On the blocklist tab, click **Add to blocklist.**



3. In the add to blocklist window, you can batch add multiple custom blocklist domain names. When you enter domain names, wildcard domain names with empty prefixes are supported, e.g., `*.tencent.com;` . All subdomain names under a wildcard domain name will trigger alarms.

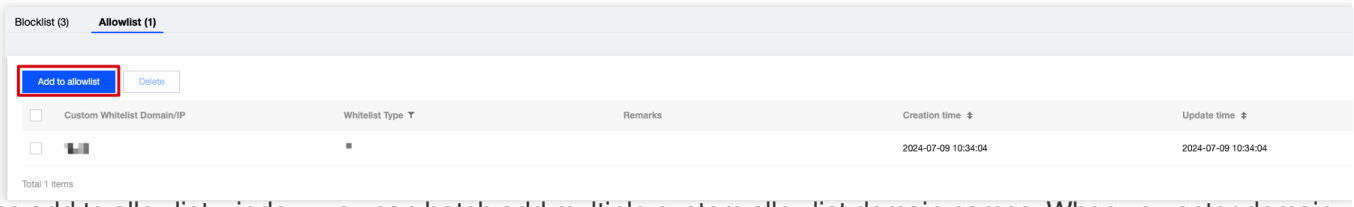


4. Click **Confirm**, and the list will generate records based on the entered domain names. If multiple domain names are entered, multiple records will be generated.

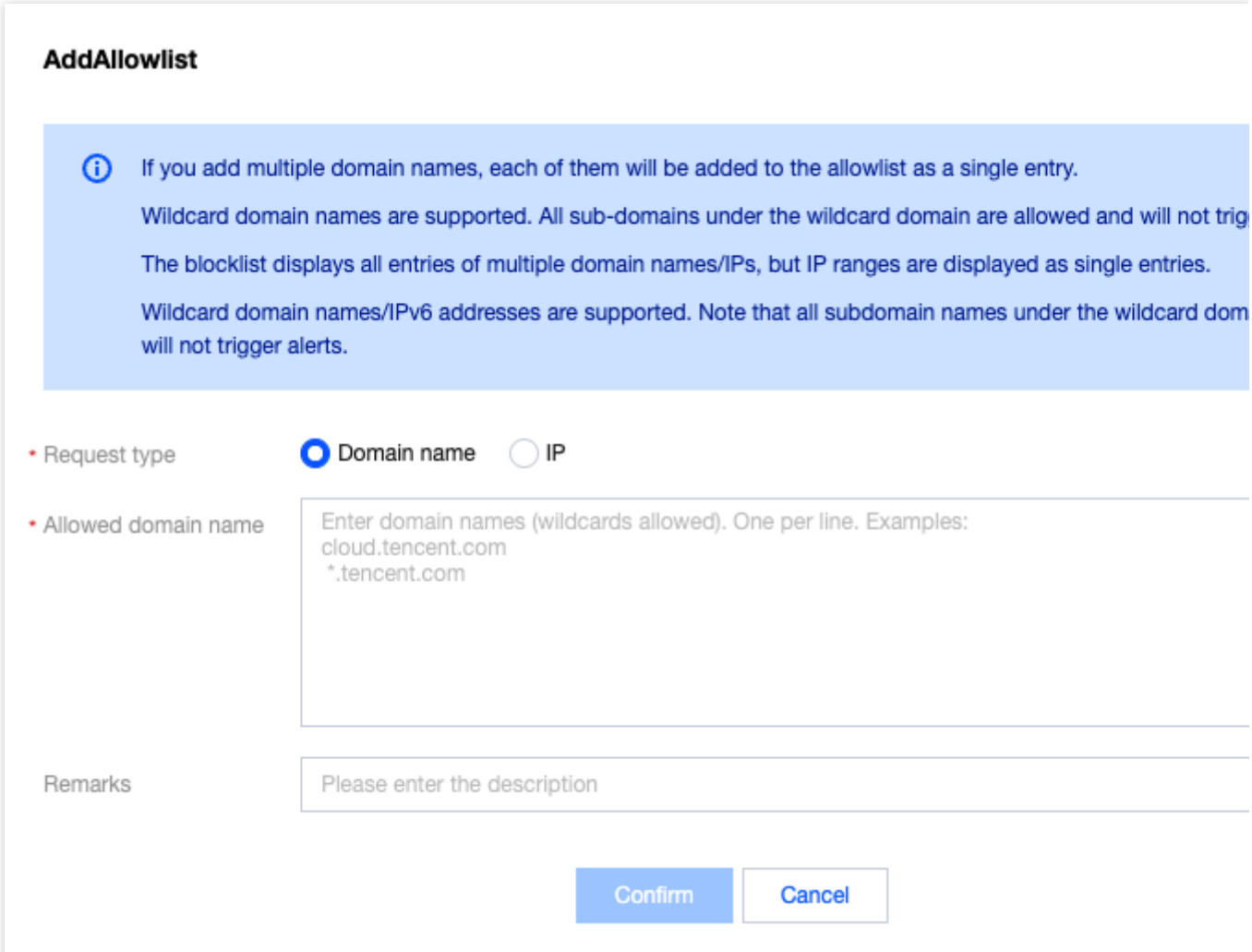
©2013-2022 Tencent Cloud. All rights reserved.

Allowlist Management

1. Log in to the TCSS console. In the left sidebar, click **Runtime Security** > **Outbound Malware** > **Blocklist/Allowlist management**.
2. On the allowlist tab, click **Add to allowlist**.



3. In the add to allowlist window, you can batch add multiple custom allowlist domain names. When you enter domain names, wildcard domain names with empty prefixes are supported, e.g., `*.tencent.com;` . All subdomain names under a wildcard domain name will be allowed and will not trigger alarms.



4. Click **Confirm**, and the list will generate records based on the entered domain names. If multiple domain names are entered, multiple records will be generated.

©2013-2022 Tencent Cloud. All rights reserved.

Advanced Defense Overview

Last updated：2024-01-23 15:44:44

Advanced prevention identifies hacker attacks adaptively, monitors and protects container runtime security in real time, and utilizes diversified security features, including abnormal process, file tampering, and high-risk syscall.
Abnormal process: It applies preset rules and custom check rules to monitor abnormal process startups in real time and then trigger alerts or block the exceptions. The system monitoring policy covers proxy software, lateral movements, malicious commands, reverse shells, fileless execution, high-risk commands, and unusual start found in the child process of the sensitive service.
File tampering: It applies preset rules and custom check rules to monitor abnormal file access behaviors that modify core files in real time and then trigger alerts or block the exceptions. The system monitoring policy covers rules for tampering with scheduled tasks, system programs, and user configurations.
High-risk syscall: It leverages Tencent Cloud's adaptive learning technologies in security protection to audit Linux syscalls initiated in the container that may cause security risks in real time.

©2013-2022 Tencent Cloud. All rights reserved.

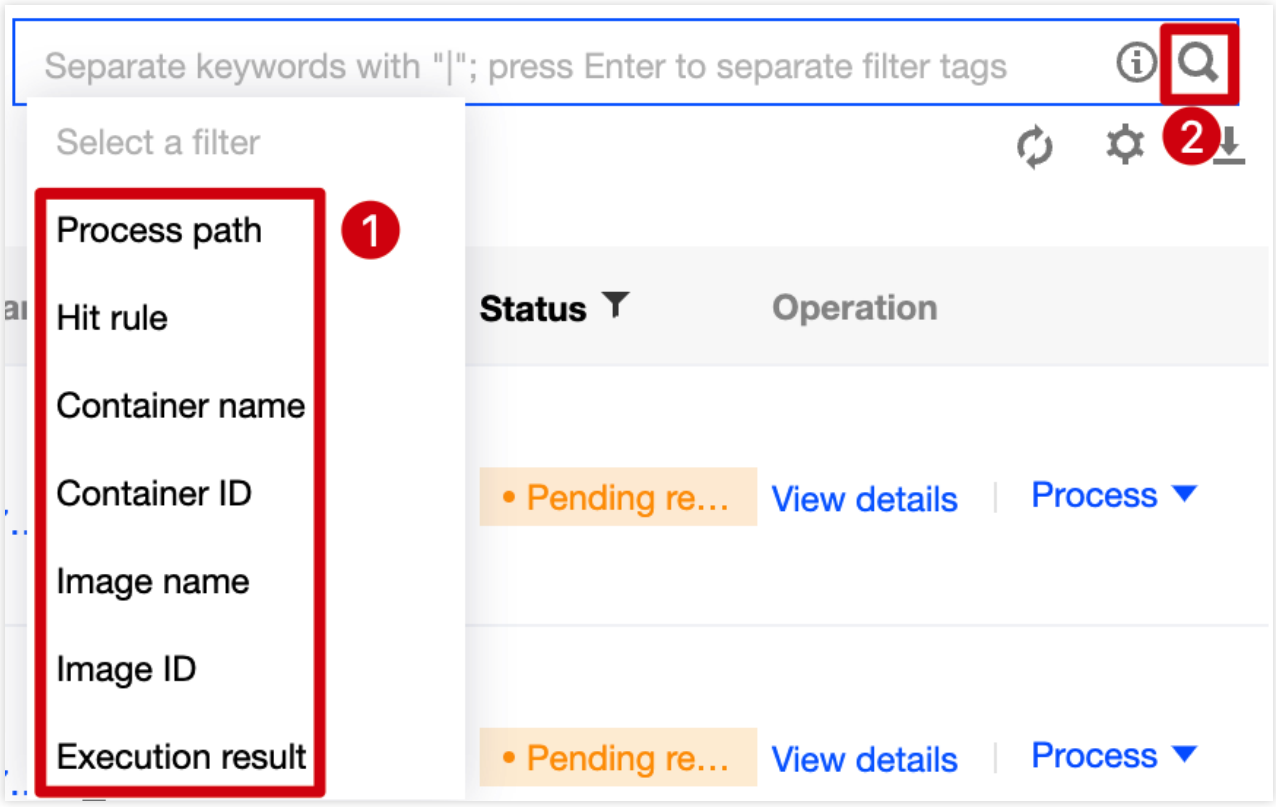
Abnormal Process Event List

Last updated：2024-01-23 15:44:44

Based on adaptive learning technologies, the abnormal process feature applies preset rules and custom check rules to monitor abnormal process startups and then trigger alerts or block the exceptions in real time. It consists of the event list and rule configuration modules. This document describes the event list feature of advanced prevention.

Filtering and Refreshing Events

1. Log in to the TCSS console and click **Advanced Prevention** > **Abnormal Processes** > **Event list** on the left sidebar.
2. On the **Event list** page, click the search box and search for events by connection process.



3. On the **Event list** page, click

©2013-2022 Tencent Cloud. All rights reserved.

on the right of the **Operation** column to refresh the event list.

Exporting the Event List

1. Log in to the TCSS console and click **Advanced Prevention** > **Abnormal Processes** > **Event list** on the left sidebar.
2. On the **Event list** page, click

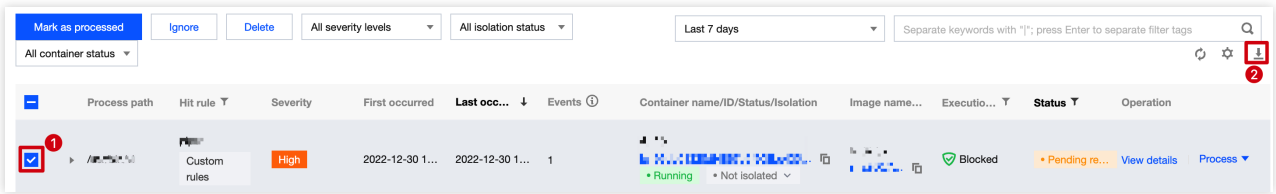
to select the target abnormal process event and click

to export it.

Note:

Click

in the **Operation** column to select multiple ones.



Event Status Processing

©2013-2022 Tencent Cloud. All rights reserved.

Log in to the TCSS console and click **Advanced Prevention** > **Abnormal Processes** > **Event list** on the left sidebar.

Method 1

On the **Event list** page, you can mark an abnormal process event as processed or ignore or delete it.
Mark as processed: Click

to select the target abnormal process event and click **Mark as processed** > **OK**.
Note:
It's recommended to handle the event by following "Solution" in the event details and mark it as processed.
Ignore: Click

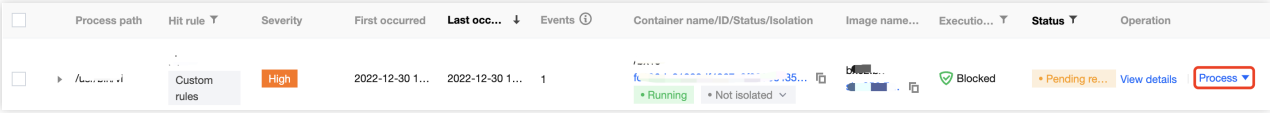
to select the target abnormal process event and click **Ignore** > **OK**.
Note:
Only the selected events are ignored. Alerts will be triggered when the same events occur again.
Delete: Click

to select the target abnormal process event and click **Delete** > **OK**.
Note:
The selected event record will no longer be displayed in the console and cannot be recovered once deleted. Proceed with caution.

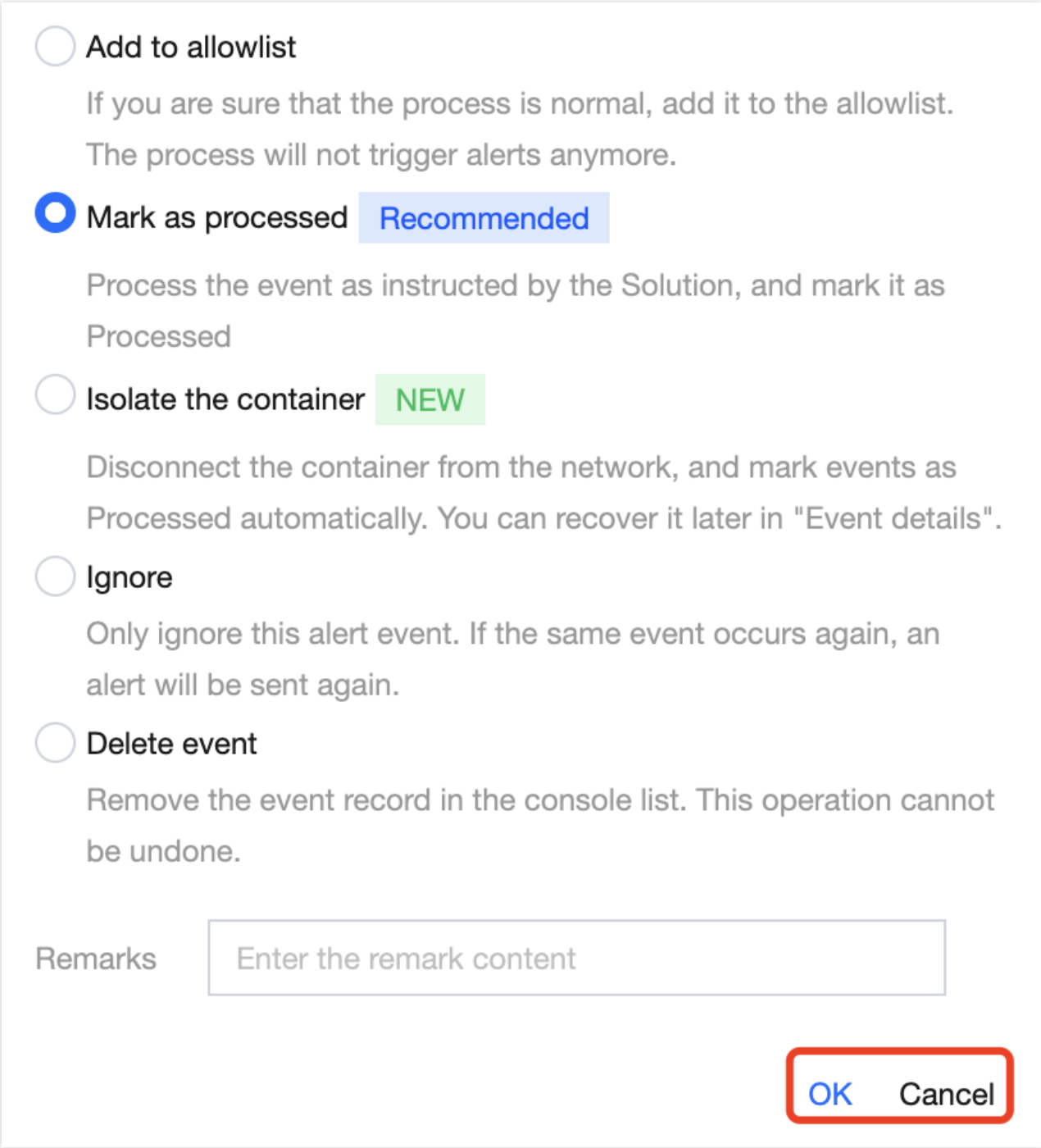
Method 2

1. On the **Event list** page, click **Process now** to add events in the **Pending resolved** status to the allowlist, mark them as processed, or ignore them.

©2013-2022 Tencent Cloud. All rights reserved.



2. Click **OK** or **Cancel**.



3. On the **Event list** page, click **Unignore** or **Delete** to unignore or delete events in the **Ignored** status.

©2013-2022 Tencent Cloud. All rights reserved.

Note:

As an event will be in the **Pending resolved** status once unignored, you need to click **OK** for confirmation.

The event record will no longer be displayed in the console and cannot be recovered once deleted. Proceed with caution.

4. On the **Event list** page, click **Delete** to delete events in the **Processed** status.

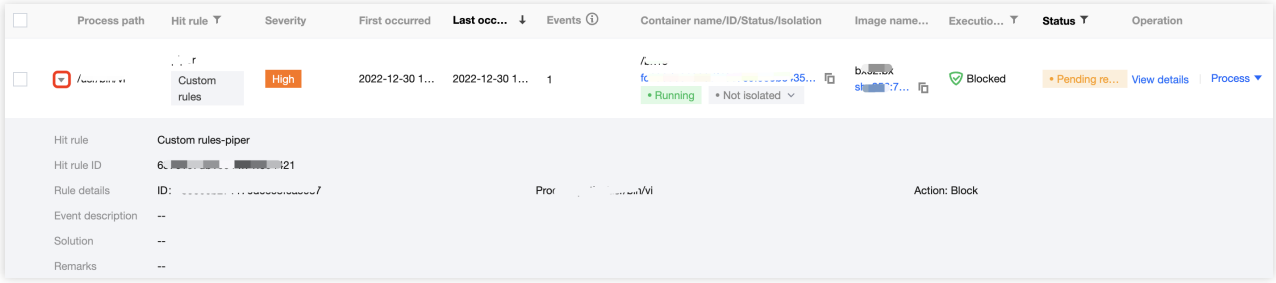
Note:

The event record will no longer be displayed in the console and cannot be recovered once deleted. Proceed with caution.

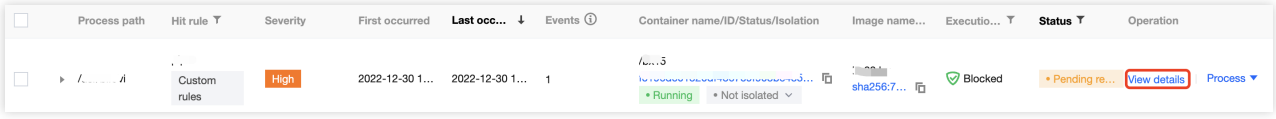
Viewing Event Details

1. Log in to the TCSS console and click **Advanced Prevention** > **Abnormal Processes** > **Event list** on the left sidebar.
2. On the **Event list** page, click

on the left of the **Process path** to view the event description.



3. On the **Event list** page, click **View details**.



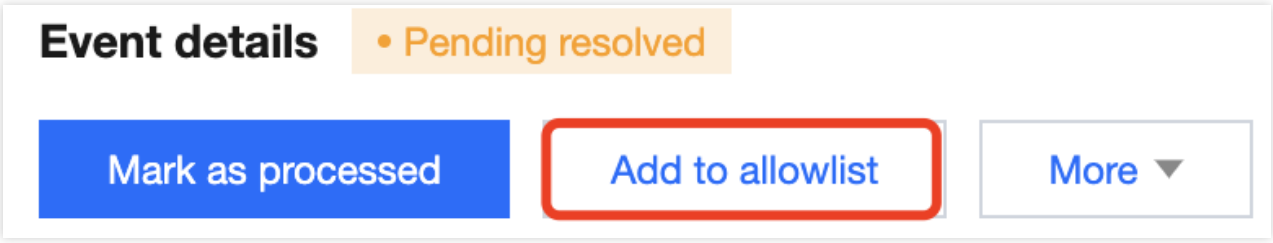
4. The **Event details** page displays the event details, process information, parent process information, and event description. You can mark the event as processed, ignore it, or add it to the allowlist.

Note:

For detailed directions on how to mark an event as processed or ignore or delete it, see Event Status Processing.

©2013-2022 Tencent Cloud. All rights reserved.

5. On the **Event details** page, click **Add to allowlist** to enter the **Copy rule** page, where you need to configure the basic information and rules and specify the scope.

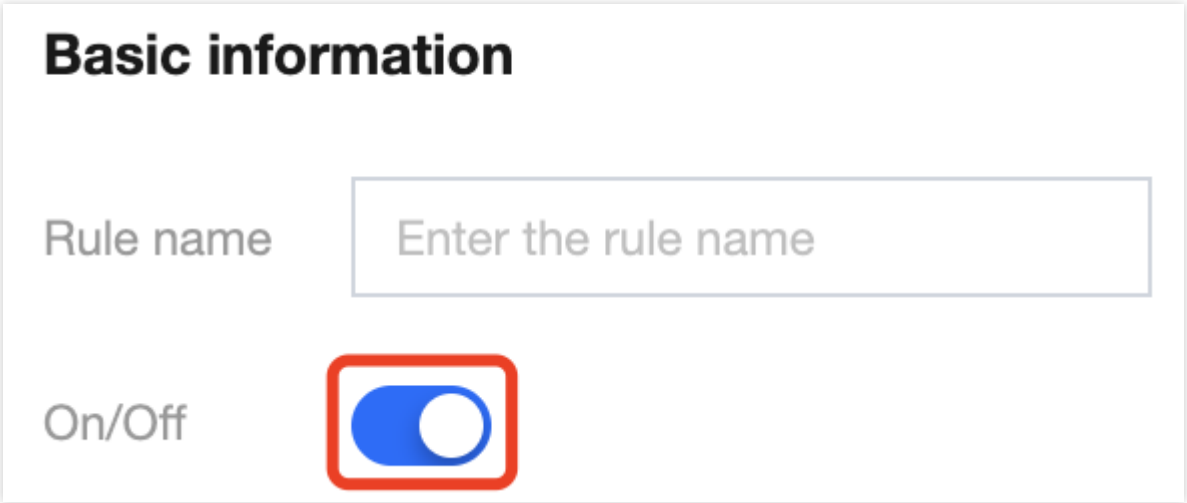


Basic information: Enter the rule name of the event. Toggle on or off

to enable or disable rule check.

Note:

This rule will no longer be executed once disabled.



Configure rules: Enter the process path and select the action. Click **Add** or **Delete** to add or delete a rule.

Images: **All images** or **Specified images**. Click

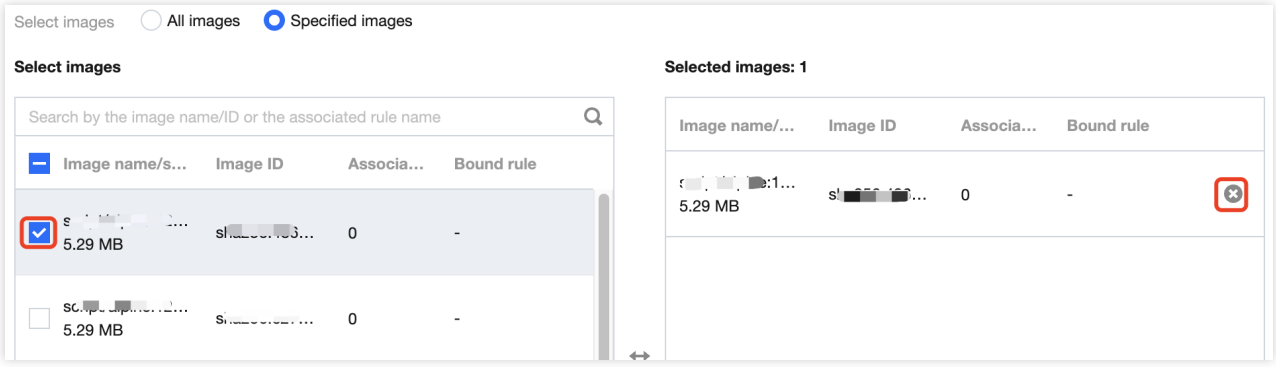
or

©2013-2022 Tencent Cloud. All rights reserved.

to select or delete the target specified image.

Note:

You can press Shift to select multiple ones.



6. After selecting the target content, click **Set** or **Cancel**.

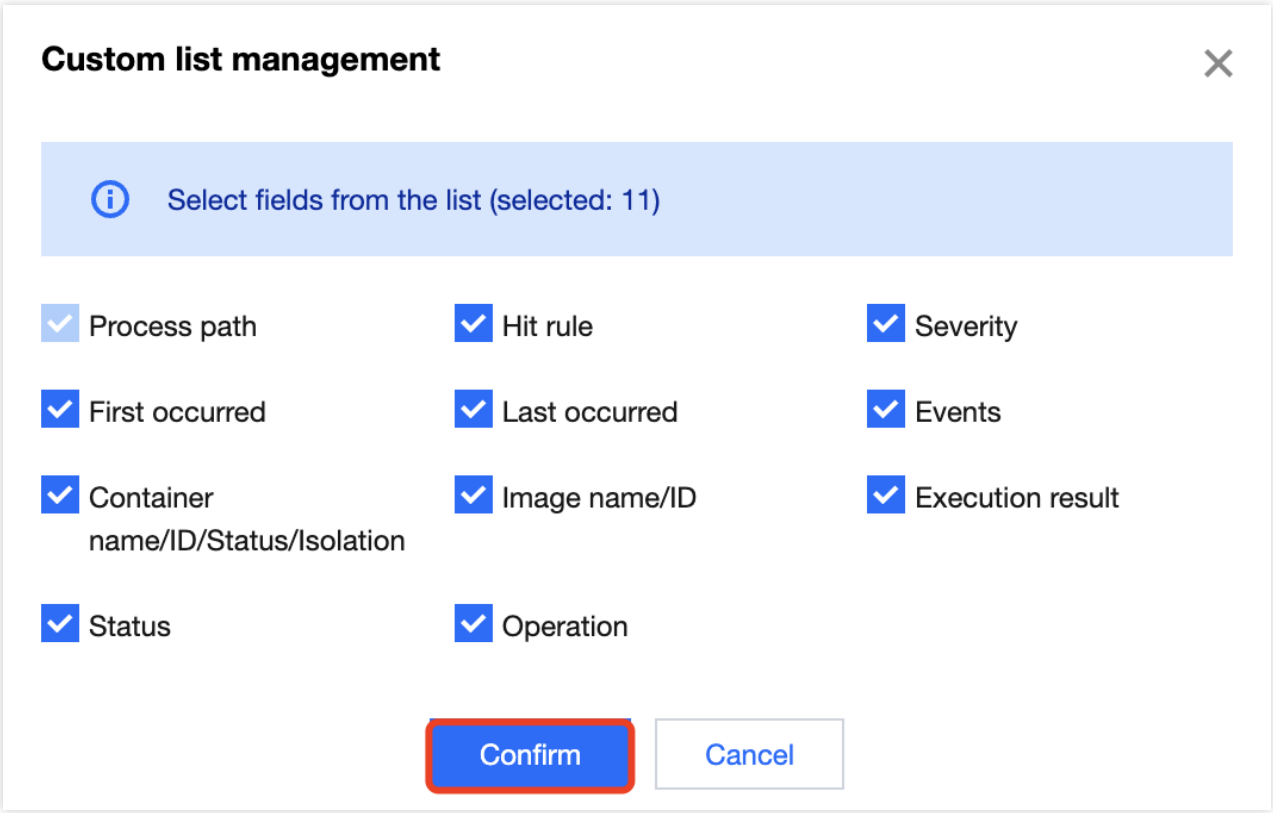
Custom List Management

1. Log in to the TCSS console and click **Advanced Prevention** > **Abnormal Processes** > **Event list** on the left sidebar.
2. On the **Event list** page, click

to pop up the **Custom List Management** window.

3. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Key fields in the list

1. First occurred: The time when an alert is first triggered by the abnormal process event. By default, the system aggregates the same alert events not processed.
2. Last occurred: The time when an alert is last triggered by the aggregated alert events. You can click the sort button on the right to sort the events in the list in chronological or reverse chronological order.
3. Events: Total number of alerts triggered by the abnormal process event within the aggregation period.
4. Execution result: **Blocked successfully**, **Failed to block**, **Allowed**, or **Alert**. You can quickly filter events in the list by action execution result.
5. Status: **Processed**, **Ignored**, **Pending resolved**, or **Allowed**. You can quickly filter events in the list by status.

©2013-2022 Tencent Cloud. All rights reserved.

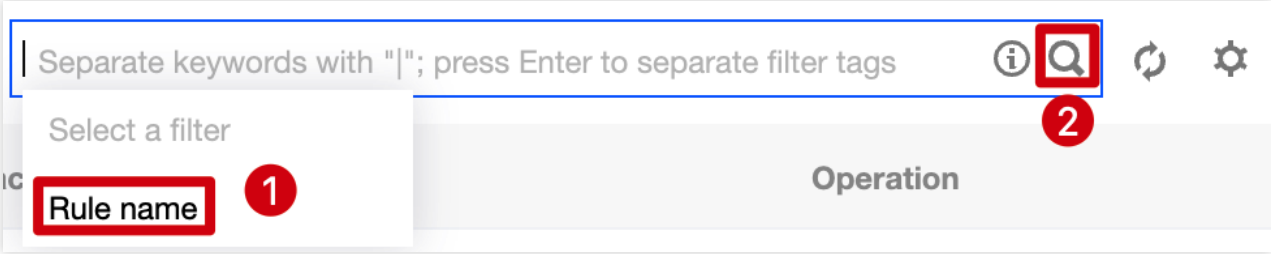
Rule Configuration

Last updated：2024-01-23 15:44:44

Based on adaptive learning technologies, the abnormal process feature applies preset rules and custom check rules to monitor abnormal process startups and then trigger alerts or block the exceptions in real time. It consists of the event list and rule configuration modules. This document describes the rule configuration feature of advanced prevention.

Filtering and Refreshing Rules

1. Log in to the TCSS console and click **Advanced Prevention** > **Abnormal Processes** > **Rule configuration** on the left sidebar.
2. On the **Rule configuration** page, click the search box and search for configured rules by rule name.



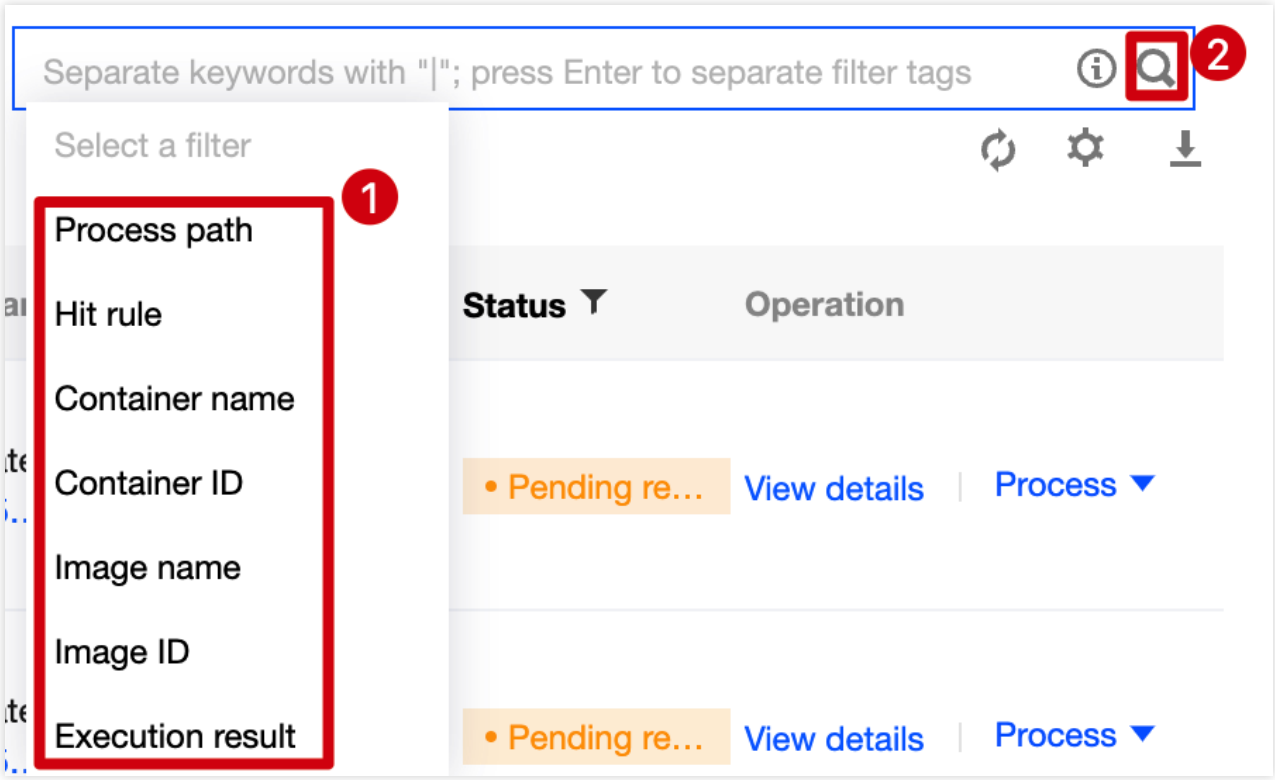
3. On the **Rule configuration** page, click

on the right of the **Operation** column to refresh the rule list.

Adding a Rule

1. Log in to the TCSS console and click **Advanced Prevention** > **Abnormal Processes** > **Rule configuration** on the left sidebar.
2. On the **Rule configuration** page, click **Create rule**.

©2013-2022 Tencent Cloud. All rights reserved.



3. On the **Add rule** page, configure the basic information and rules and specify the scope.

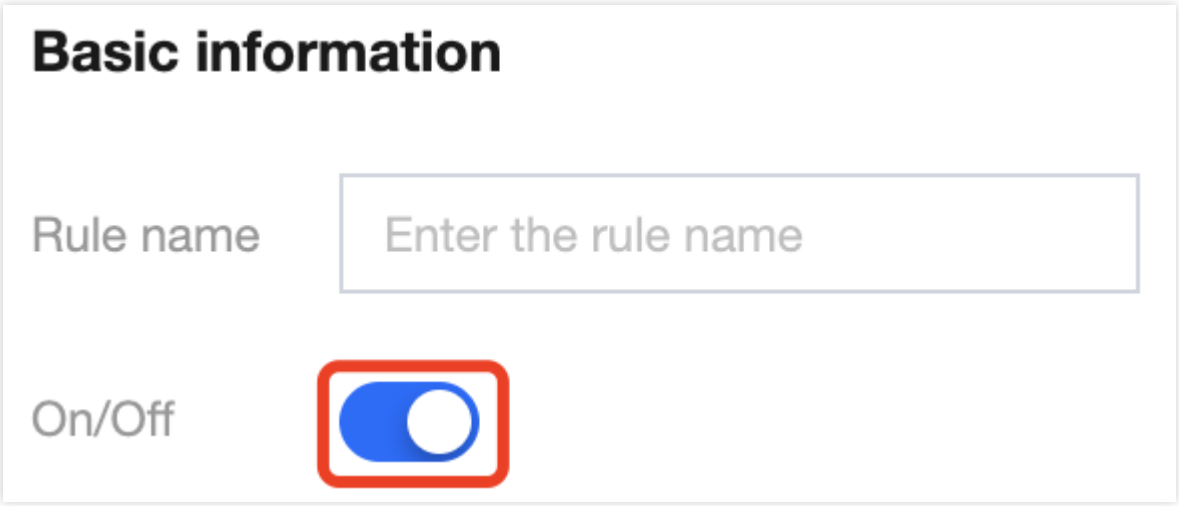
Basic information: Enter the rule name of the event. Toggle on or off

to enable or disable rule check.

Note:

This rule will no longer be executed once disabled.

©2013-2022 Tencent Cloud. All rights reserved.



Configure rules: Enter the process path and select the action. Click **Add** or **Delete** to add or delete a rule.

Note:

You can configure up to 30 rules.

Actions to be executed include:

Block: Once a rule is hit, the process will be blocked and the event details will be recorded.

Alert: Trigger alerts about the event, allow running of the process and log the event details.

Allow: When a rule is hit, the process will be automatically allowed without being recorded.

Images: **All images** or **Specified images**. Click

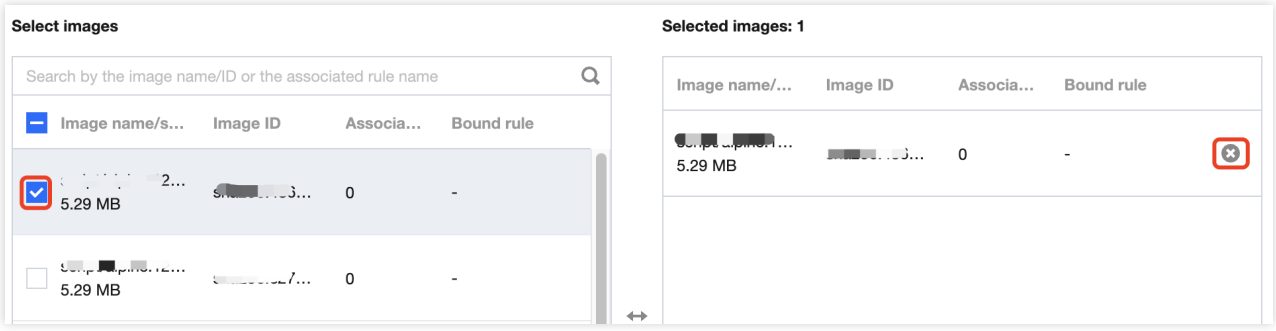
or

to select or delete the target specified image.

Note:

You can press Shift to select multiple ones.

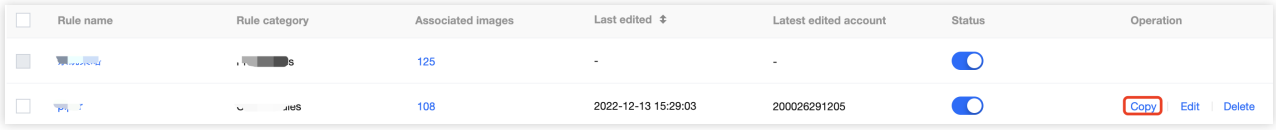
©2013-2022 Tencent Cloud. All rights reserved.



4. After selecting the target content, click **Set** or **Cancel**.

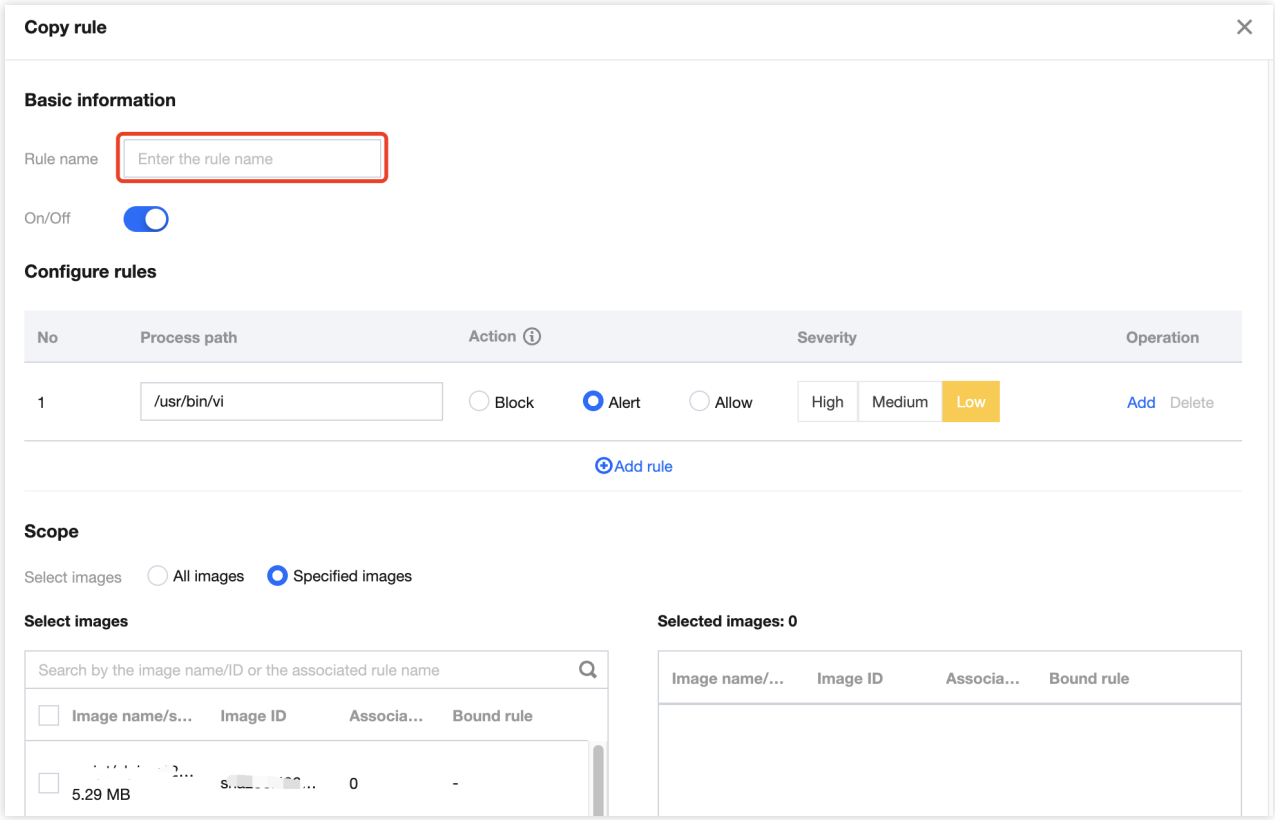
Copying a Rule

1. Log in to the TCSS console and click **Advanced Prevention** > **Abnormal Processes** > **Rule configuration** on the left sidebar.
2. On the **Rule configuration** page, click **Copy** on the right.



3. On the **Copy rule** page, enter the rule name, toggle **On**/**Off**, configure rules, and specify the scope.

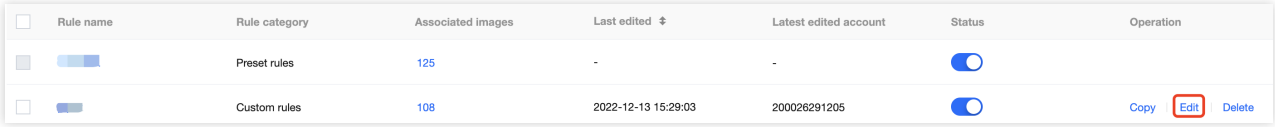
©2013-2022 Tencent Cloud. All rights reserved.



4. After selecting the target content, click **OK** or **Cancel**.

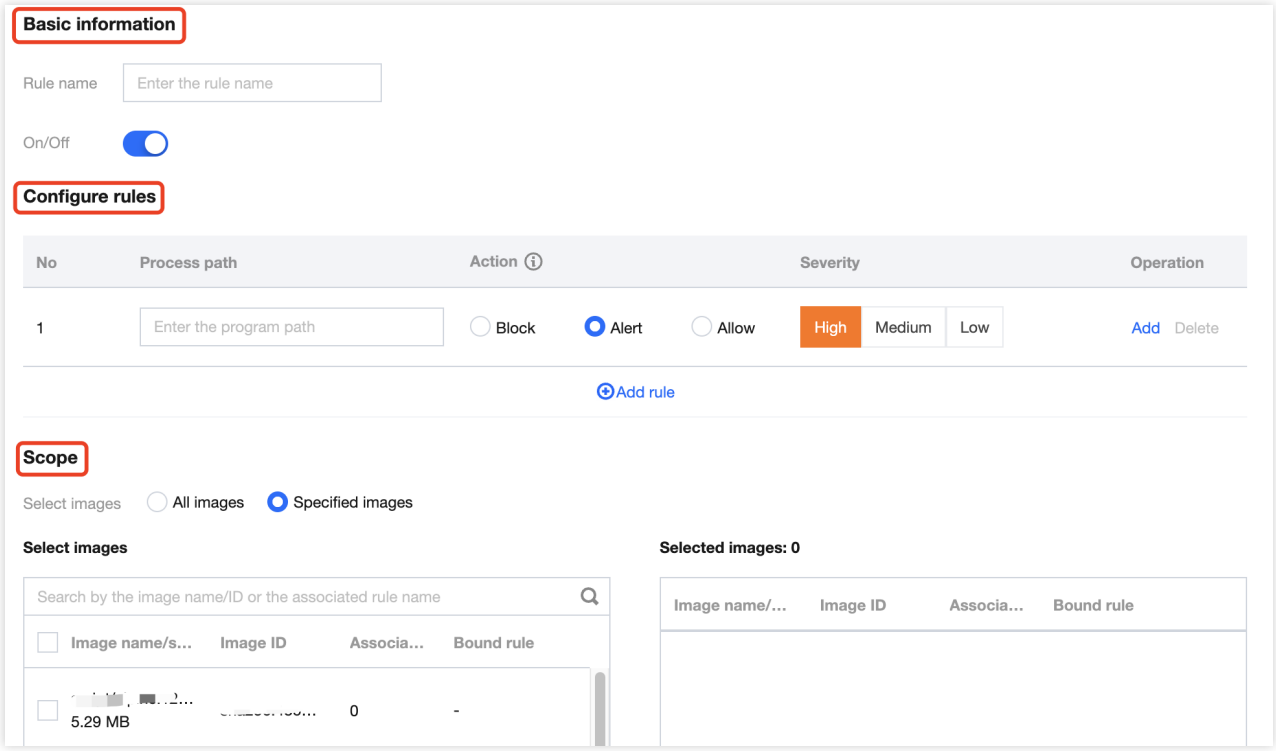
Editing a Rule

1. Log in to the TCSS console and click **Advanced Prevention** > **Abnormal Processes** > **Rule configuration** on the left sidebar.
2. On the **Rule configuration** page, click **Edit** on the right.



3. On the **Edit rule** page, modify the basic information, configure rules, and specify the scope.

©2013-2022 Tencent Cloud. All rights reserved.

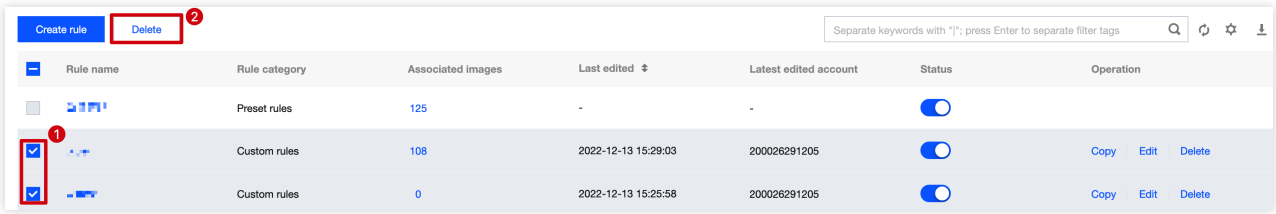


4. After selecting the target content, click **OK** or **Cancel**.

Deleting a Rule

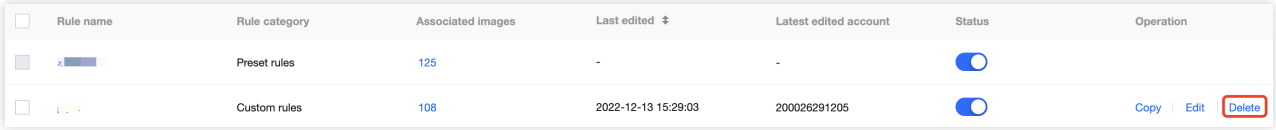
1. Log in to the TCSS console and click **Advanced Prevention** > **Abnormal Processes** > **Rule configuration** on the left sidebar.
2. On the **Rule configuration** page, delete a rule in either of the following methods:
Select the target rule, click

, and click **Delete** on the left in the **Operation** column.



©2013-2022 Tencent Cloud. All rights reserved.

Select the target rule and click **Delete** on the right.



3. In the pop-up window, click **Delete** or **Cancel**.

Note:

The rule cannot be recovered once deleted, and images associated with the rule will be automatically associated with the default system rule.

Exporting a Rule

1. Log in to the TCSS console and click **Advanced Prevention** > **Abnormal Processes** > **Rule configuration** on the left sidebar.
2. On the **Rule configuration** page, click

to select the target abnormal process rule and click

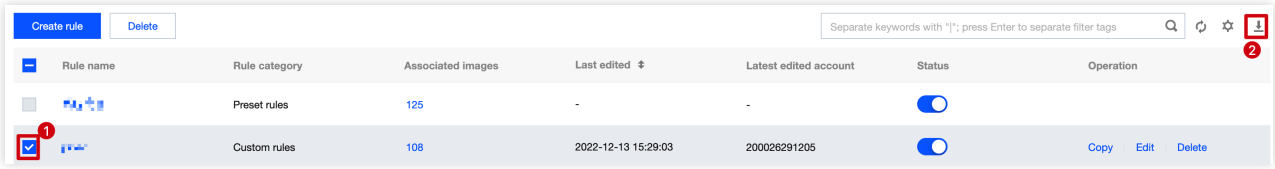
to export it.

Note:

Click

in the **Operation** column to select multiple ones.

©2013-2022 Tencent Cloud. All rights reserved.

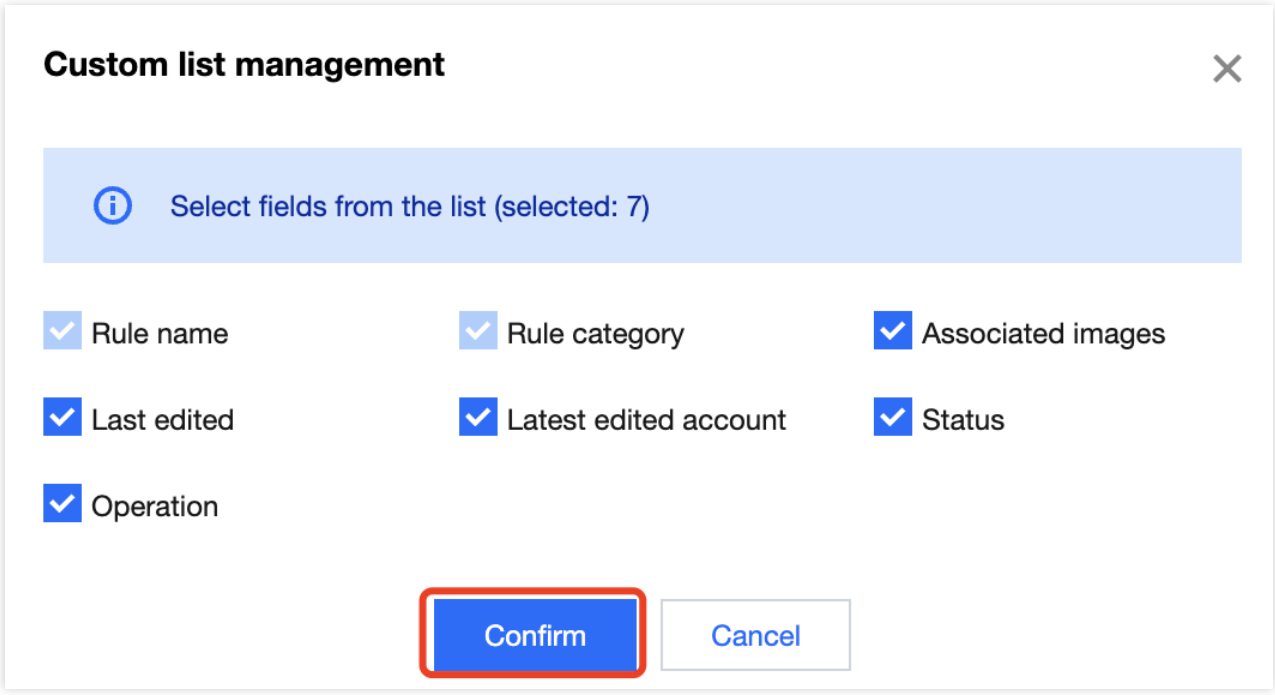


Custom List Management

1. Log in to the TCSS console and click **Advanced Prevention** > **Abnormal Processes** > **Rule configuration** on the left sidebar.
2. On the **Rule configuration** page, click

to pop up the **Custom List Management** window.

3. In the pop-up window, select the target type and click **OK**.

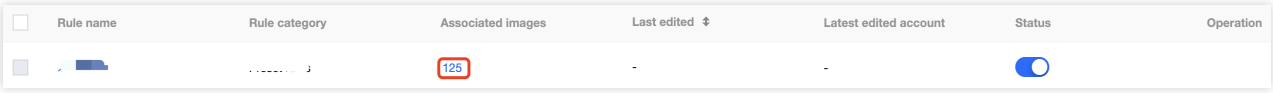


Key fields in the list

1. Rule category: Preset rule or custom rule.

©2013-2022 Tencent Cloud. All rights reserved.

2. Associated images: Number of images for which the rule takes effect. Click the number of affected images to pop up the drawer on the right, which displays the rule details.



3. Status: On/Off.
4. Operation: System rules can only be copied, and custom rules can be copied, edited, or deleted.

©2013-2022 Tencent Cloud. All rights reserved.

File Tampering
Event List

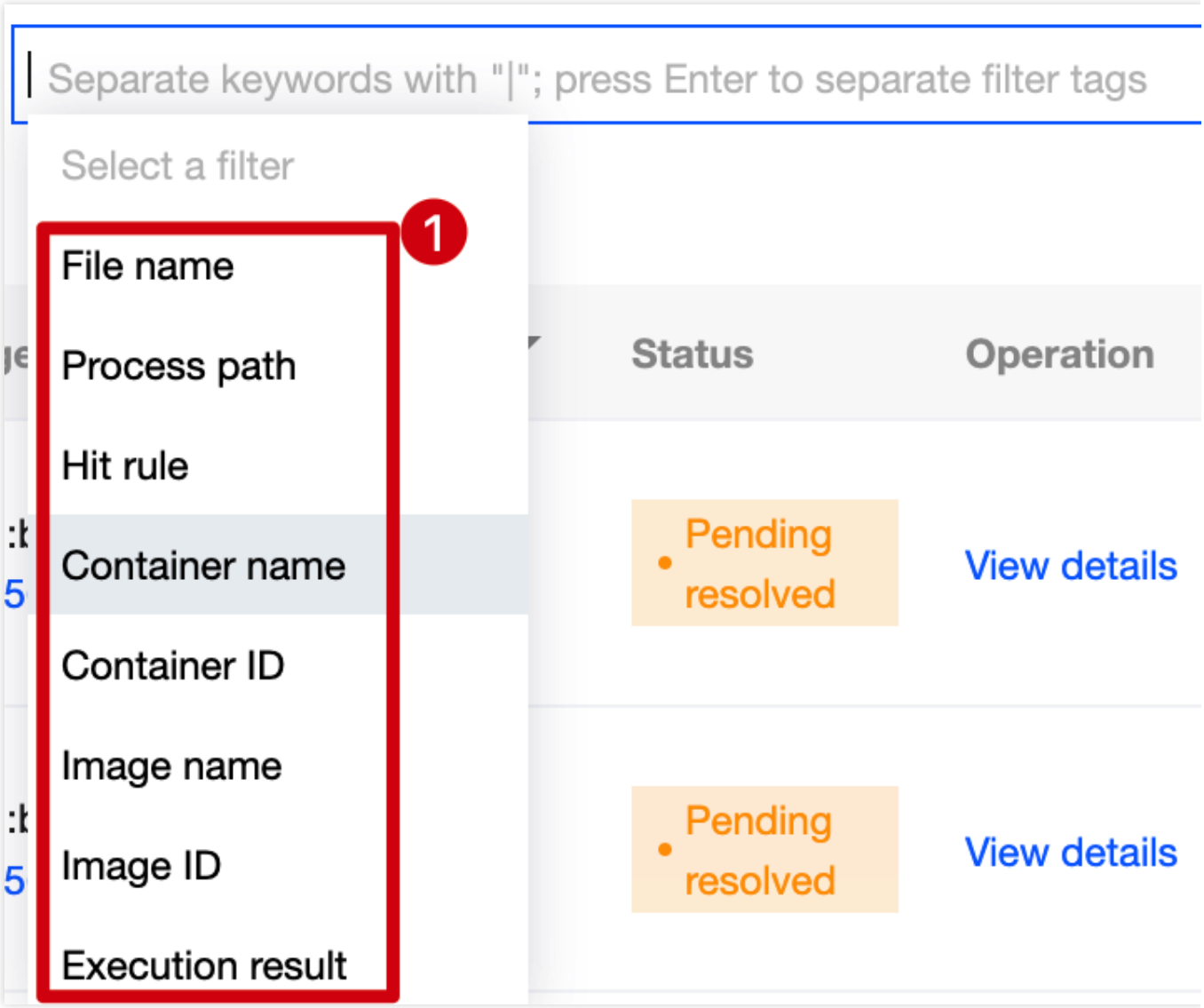
Last updated：2024-01-23 15:44:44

The file tampering feature provides the lists of monitored events and configured rules. The event list module displays the file tampering check results.

Filtering and Refreshing Events

1. Log in to the TCSS console and click **Advanced Prevention** > **File Tampering** > **Event list** on the left sidebar.
2. On the **Event list** page, click the search box and search for file tampering check results by keyword such as filename, process path, or hit rule.

©2013-2022 Tencent Cloud. All rights reserved.



3. On the **Event list** page, click

on the right of the **Operation** column to refresh the event list.

Exporting the Check Result

1. Log in to the TCSS console and click **Advanced Prevention** > **File Tampering** > **Event list** on the left sidebar.
2. On the **Event list** page, click

to select the target file tampering event and click

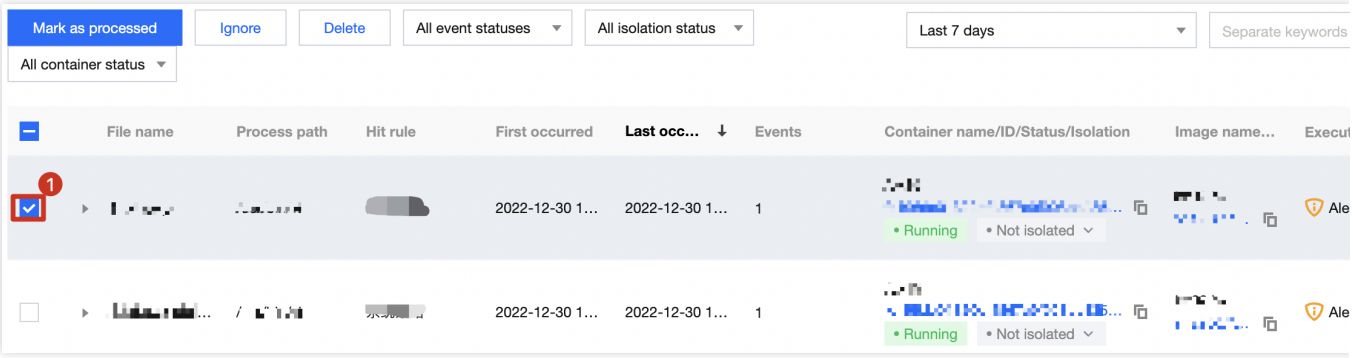
©2013-2022 Tencent Cloud. All rights reserved.

to export it.

Note:

Click

in the **Operation** column to select multiple ones.



Changing the Event Status

Log in to the TCSS console and click **Advanced Prevention** > **File Tampering** > **Event list** on the left sidebar.

Method 1

On the **Event list** page, you can mark a file tampering event as processed or ignore or delete it.

Mark as processed: Click

to select the target file tampering event and click **Mark as processed** > **OK**.

Note:

It's recommended to handle the event by following "Solution" in the event details and mark it as processed.

Ignore: Click

to select the target file tampering event and click **Ignore** > **OK**.

Note:

Only the selected events are ignored. Alerts will be triggered when the same events occur again.

Delete: Click

©2013-2022 Tencent Cloud. All rights reserved.

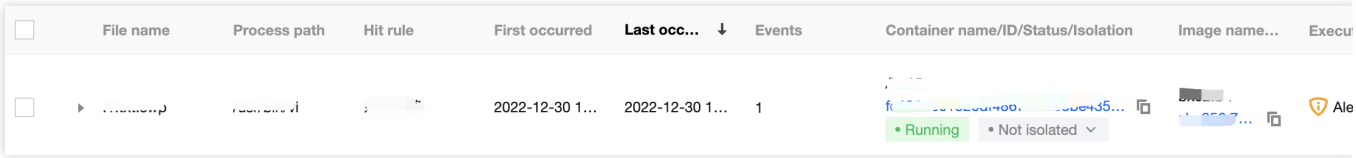
to select the target file tampering event and click **Delete** > **OK**.

Note:

The selected event record will no longer be displayed in the console and cannot be recovered once deleted. Proceed with caution.

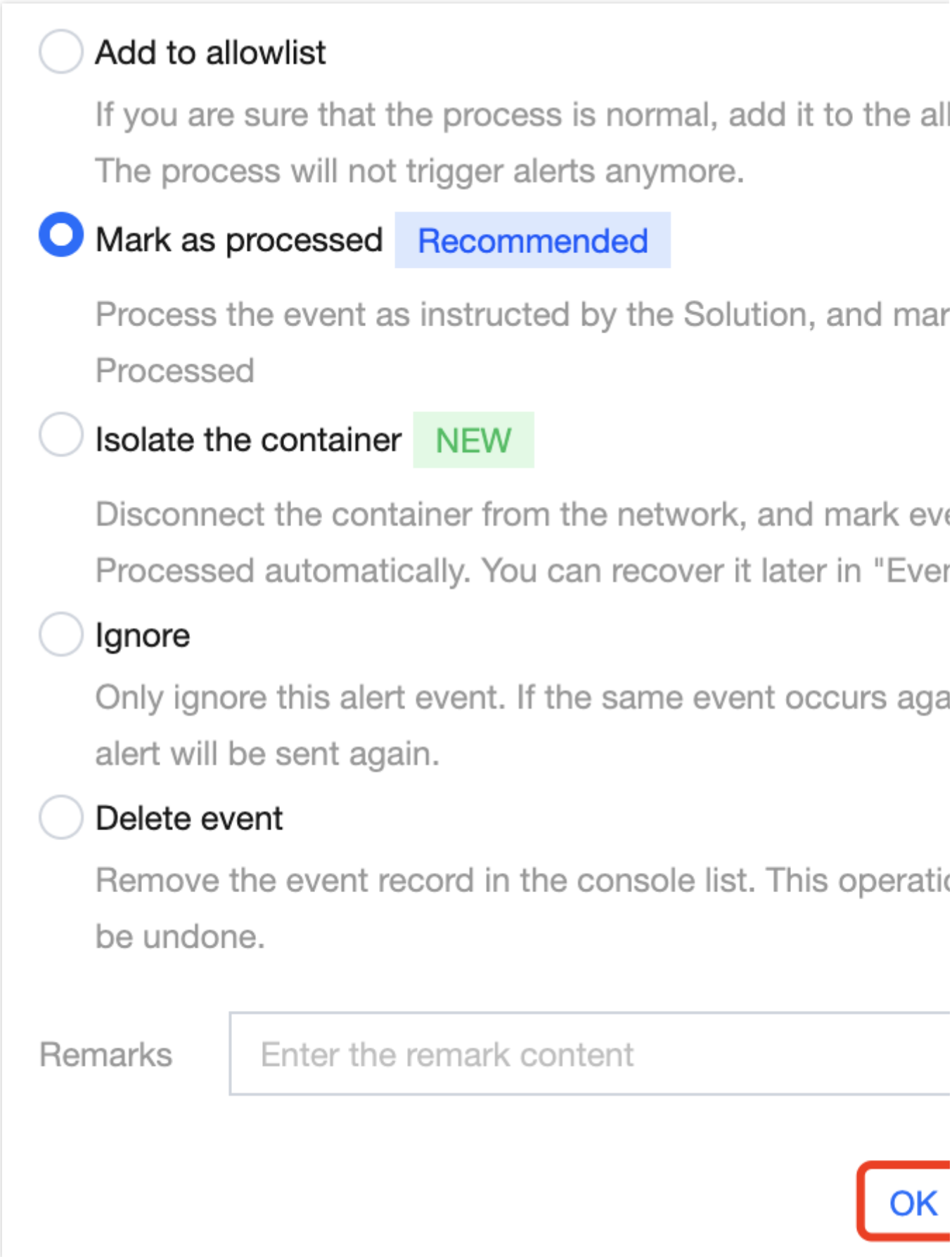
Method 2

1. On the **Event list** page, click **Process now** to add events in the **Pending resolved** status to the allowlist, mark them as processed, or ignore them.



2. Click **OK** or **Cancel**.

©2013-2022 Tencent Cloud. All rights reserved.



3. On the **Event list** page, click **Unignore** or **Delete** to unignore or delete events in the **Ignored** status.

©2013-2022 Tencent Cloud. All rights reserved.

Note:

As an event will be in the **Pending resolved** status once unignored, you need to click **OK** for confirmation.

The event record will no longer be displayed in the console and cannot be recovered once deleted. Proceed with caution.

4. On the **Event list** page, click **Delete** to delete events in the **Processed** status.

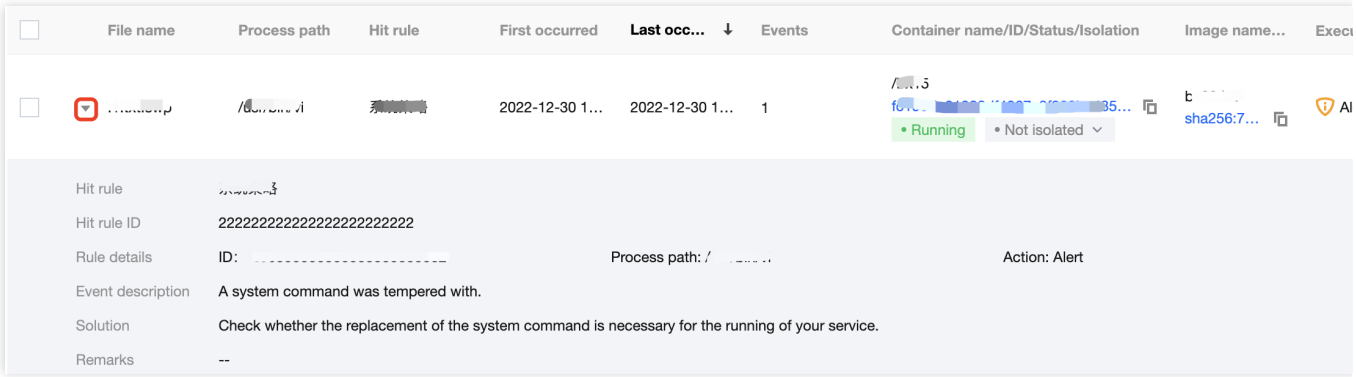
Note:

The event record will no longer be displayed in the console and cannot be recovered once deleted. Proceed with caution.

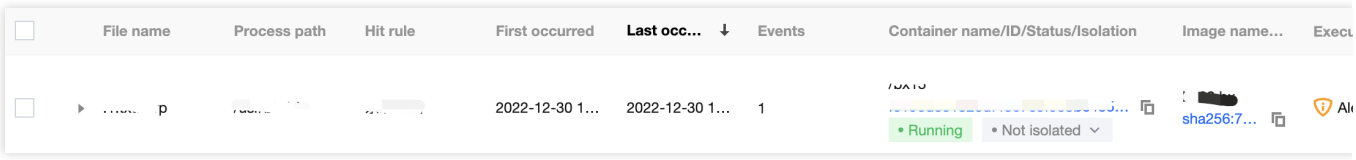
Viewing Event Details

1. Log in to the TCSS console and click **Advanced Prevention** > **File Tampering** > **Event list** on the left sidebar.
2. On the **Event list** page, click

on the left of the **Process path** to view the event description.



3. On the **Event list** page, click **View details**.



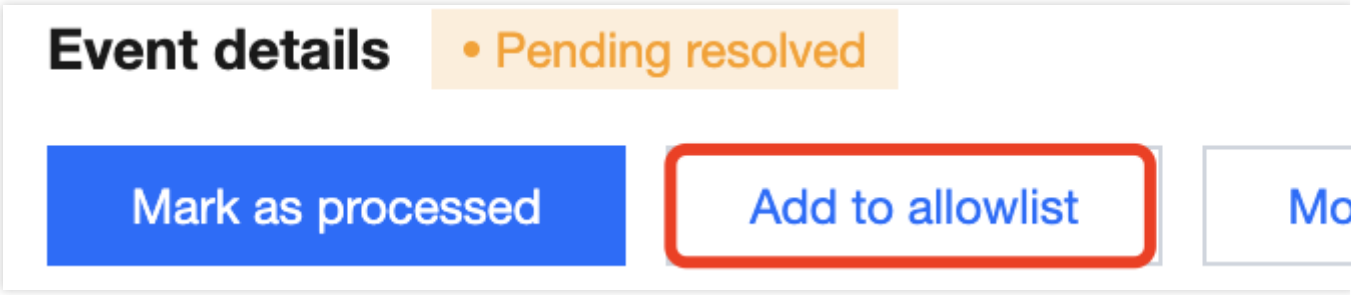
4. The **Event details** page displays the event details, process information, parent process information, and event description. You can mark the event as processed, ignore it, or add it to the allowlist.

Note:

For detailed directions on how to mark an event as processed or ignore or delete it, see Changing the Event Status.

5. On the **Event details** page, click **Add to allowlist** to enter the **Copy rule** page, where you need to configure the basic information and rules and specify the scope.

©2013-2022 Tencent Cloud. All rights reserved.

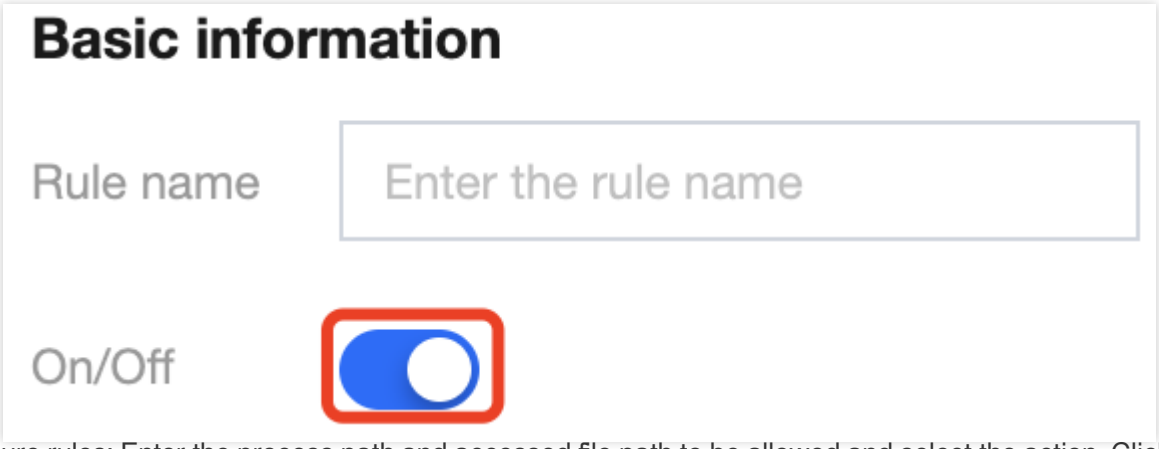


Basic information: Enter the rule name of the event. Toggle on or off

to enable or disable rule check.

Note:

This rule will no longer be executed once disabled.



Configure rules: Enter the process path and accessed file path to be allowed and select the action. Click **Add** or **Delete** to add or delete a rule.

Note:

You can configure up to 30 rules.

Actions to be executed include:

Block: Once a rule is hit, the process will be blocked and the event details will be recorded.

Alert: Trigger alerts about the event, allow running of the process and log the event details.

Allow: When a rule is hit, the process will be automatically allowed without being recorded.

Images: **All images** or **Specified images**. Click

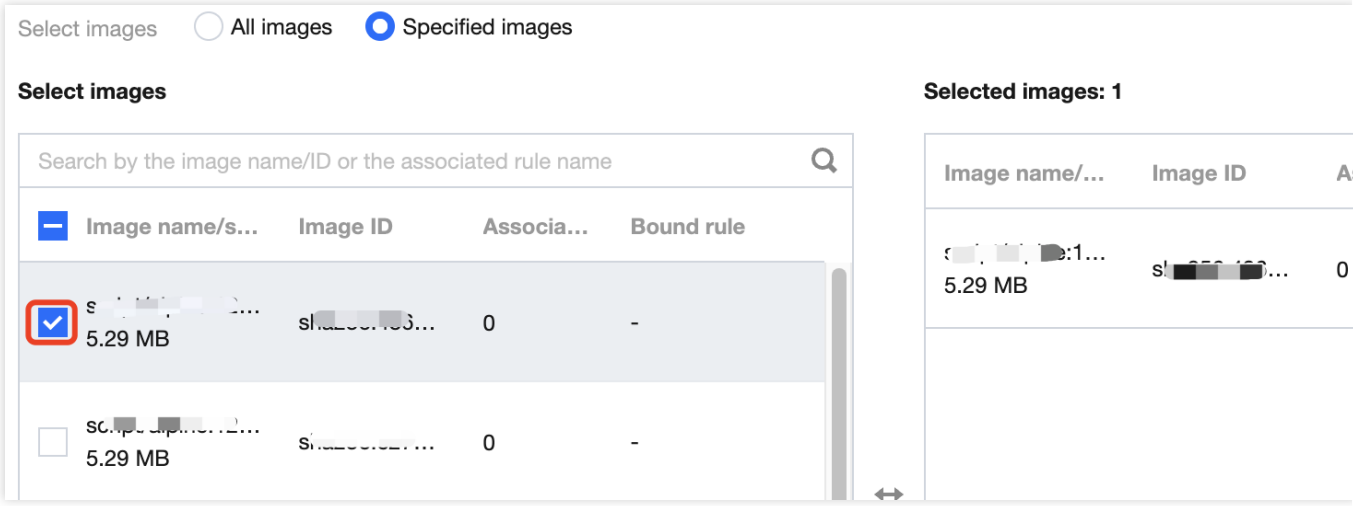
or

©2013-2022 Tencent Cloud. All rights reserved.

to select or delete the target specified image.

Note:

You can press Shift to select multiple ones.



6. After selecting the target content, click **Set** or **Cancel**.

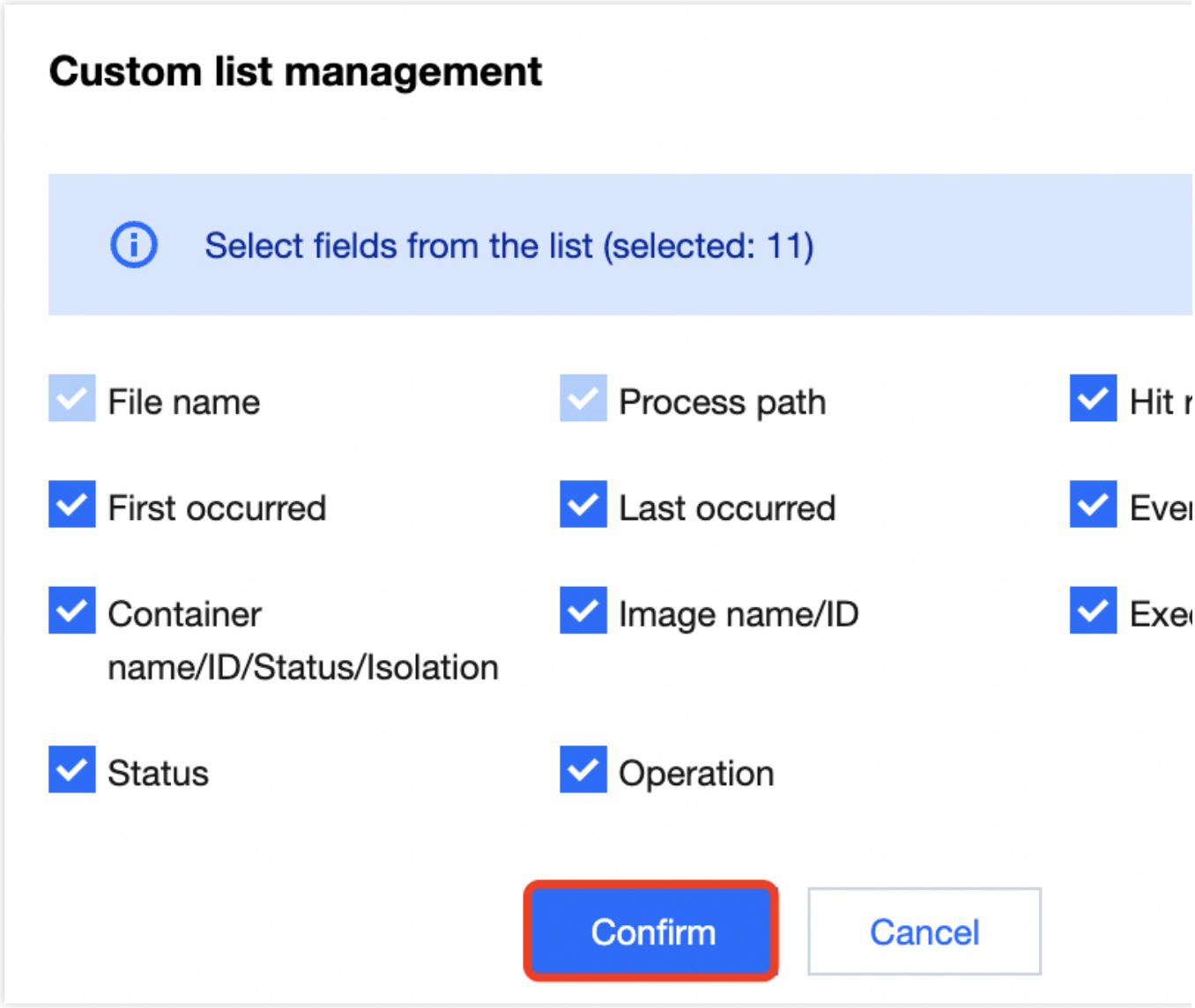
Custom List Management

1. Log in to the TCSS console and click **Advanced Prevention** > **File Tampering** > **Event list** on the left sidebar.
2. On the **Event list** page, click

to pop up the **Custom List Management** window.

3. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Key fields in the list

1. First occurred: The time when an alert is first triggered by the file tampering event. By default, the system aggregates the same alert events not processed.
2. Last occurred: The time when an alert is last triggered by the aggregated alert events. You can click the sort button on the right to sort the events in the list in chronological or reverse chronological order.
3. Events: Total number of alerts triggered by the file tampering event within the aggregation period.
4. Execution result: **Blocked successfully**, **Failed to block**, **Allowed**, or **Alert**. You can quickly filter events in the list by action execution result.
5. Status: **Processed**, **Ignored**, **Pending resolved**, or **Allowed**. You can quickly filter events in the list by status.

©2013-2022 Tencent Cloud. All rights reserved.

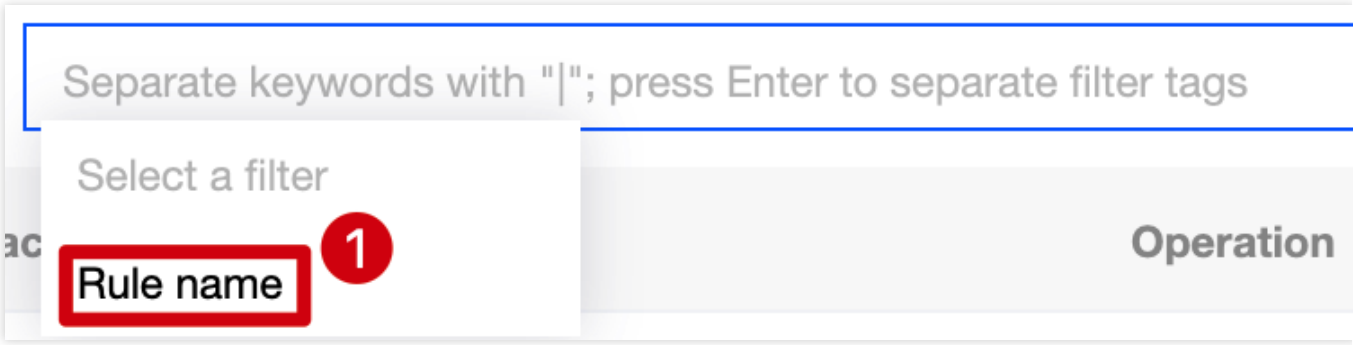
Rule Configuration

Last updated：2024-01-23 15:44:44

The file tampering feature provides the lists of monitored events and configured rules. The rule configuration module displays the list of configured rules.

Filtering and Refreshing Rules

1. Log in to the TCSS console and click **Advanced Prevention** > **File Tampering** > **Rule configuration** on the left sidebar.
2. On the **Rule configuration** page, click the search box and search for configured rules by rule name.



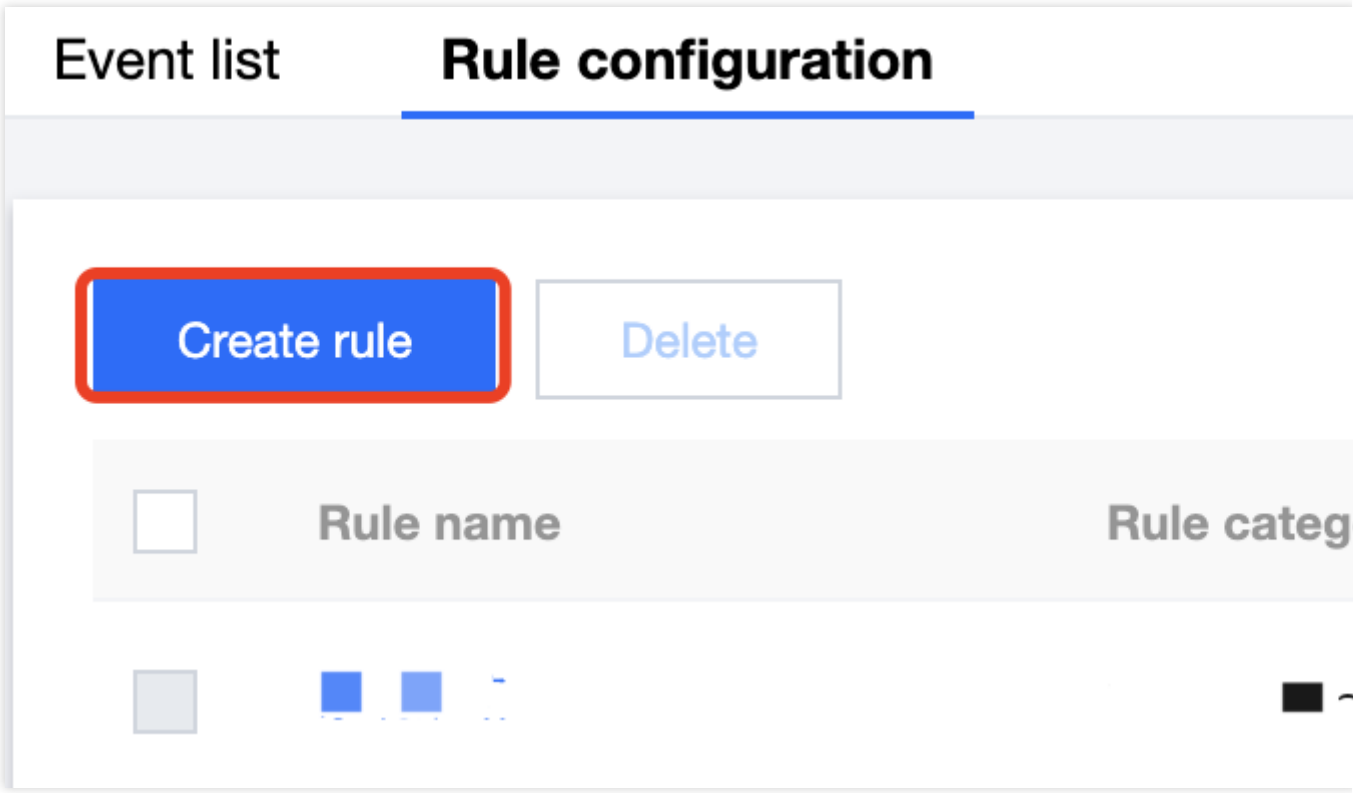
3. On the **Rule configuration** page, click

on the right of the **Operation** column to refresh the rule list.

Adding a Rule

1. Log in to the TCSS console and click **Advanced Prevention** > **File Tampering** > **Rule configuration** on the left sidebar.
2. On the **Rule configuration** page, click **Create rule**.

©2013-2022 Tencent Cloud. All rights reserved.



3. On the **Add rule** page, configure the basic information and rules and specify the scope.

Basic information: Enter the rule name of the event. Toggle on or off

to enable or disable rule check.

Note:

This rule will no longer be executed once disabled.

Configure rules: Enter the process path and accessed file path and select the action. Click **Add** or **Delete** to add or delete a rule.

Note:

You can configure up to 30 rules.

©2013-2022 Tencent Cloud. All rights reserved.

Actions to be executed include:

Block: Once a rule is hit, the process will be blocked and the event details will be recorded.

Alert: Trigger alerts about the event, allow running of the process and log the event details.

Allow: When a rule is hit, the process will be automatically allowed without being recorded.

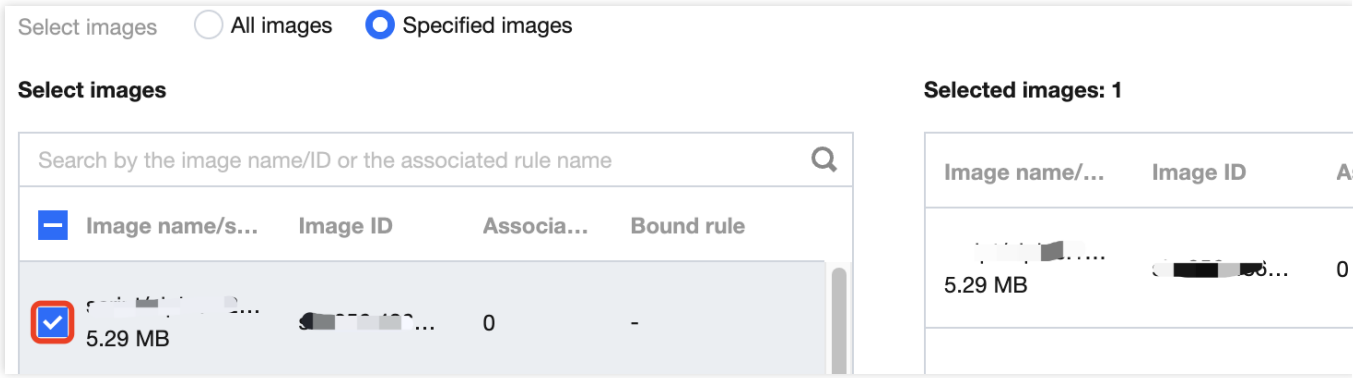
Images: **All images** or **Specified images**. Click

or

to select or delete the target specified image.

Note:

You can press Shift to select multiple ones.

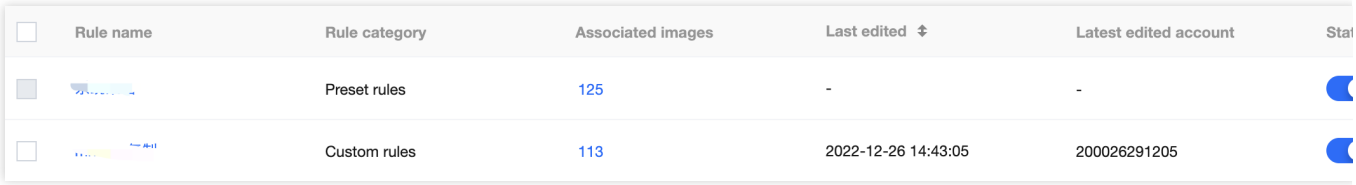


4. After selecting the target content, click **Set** or **Cancel**.

Copying a Rule

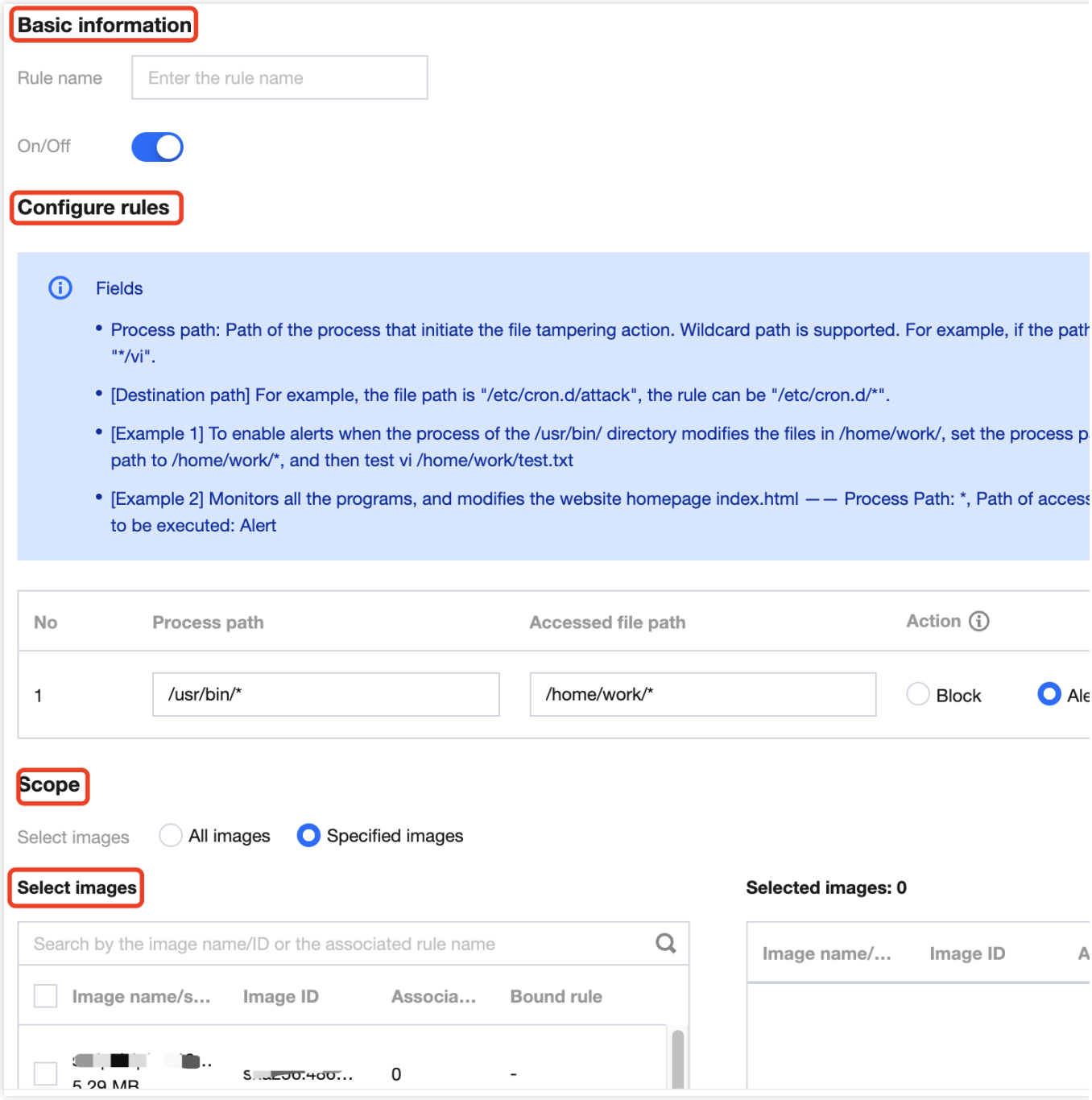
1. Log in to the TCSS console and click **Advanced Prevention** > **File Tampering** > **Rule configuration** on the left sidebar.

2. On the **Rule configuration** page, click **Copy** on the right.



3. On the **Copy rule** page, enter the rule name, toggle **On**/**Off**, configure rules, and specify the scope.

©2013-2022 Tencent Cloud. All rights reserved.

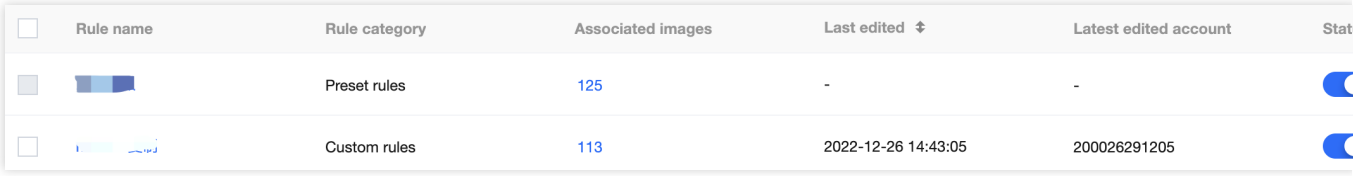


4. After selecting the target content, click **OK** or **Cancel**.

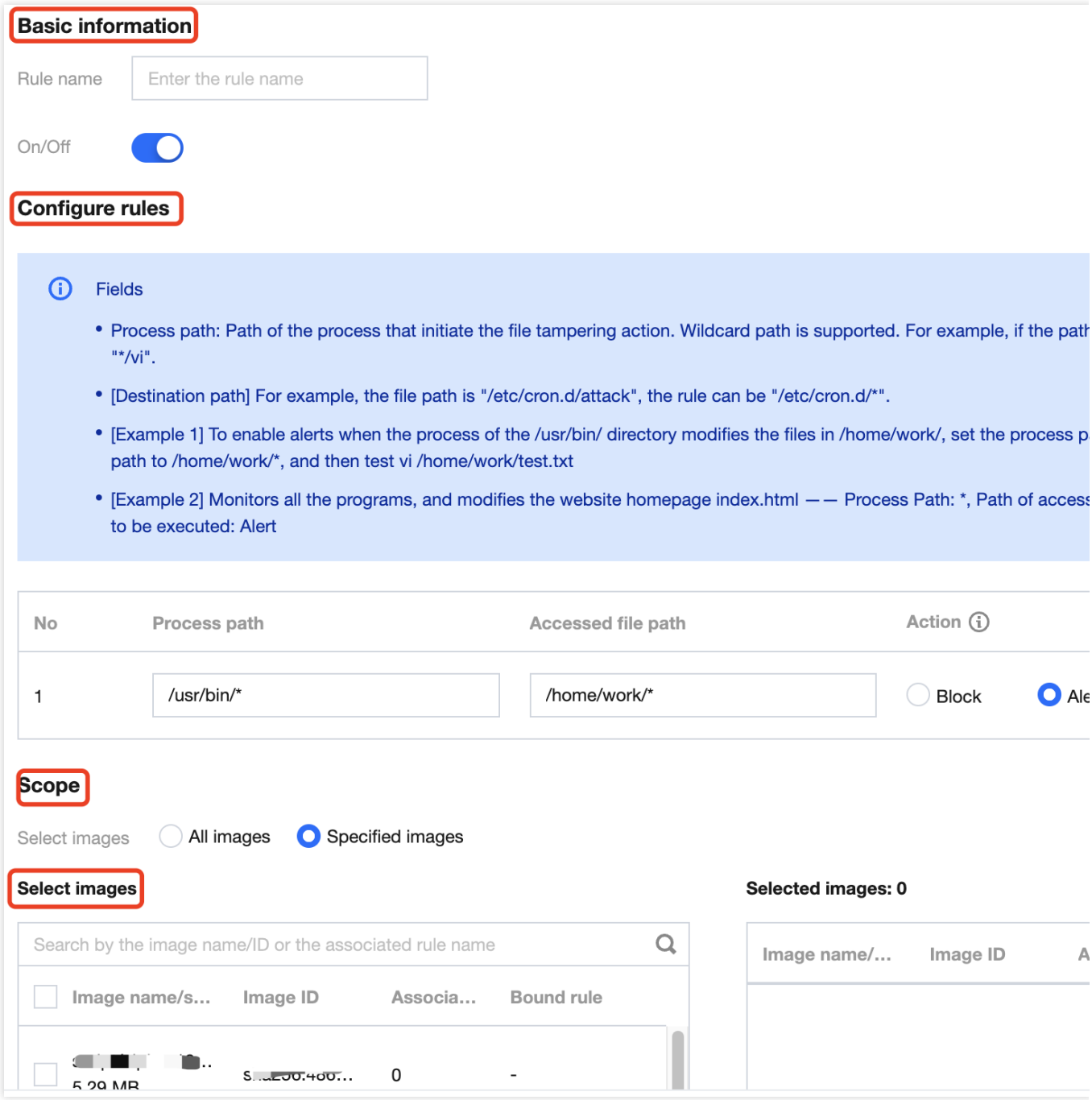
Editing a Rule

1. Log in to the TCSS console and click **Advanced Prevention** > **File Tampering** > **Rule configuration** on the left sidebar.
2. On the **Rule configuration** page, click **Edit** on the right.

©2013-2022 Tencent Cloud. All rights reserved.



3. On the **Edit rule** page, modify the basic information, configure rules, and specify the scope.



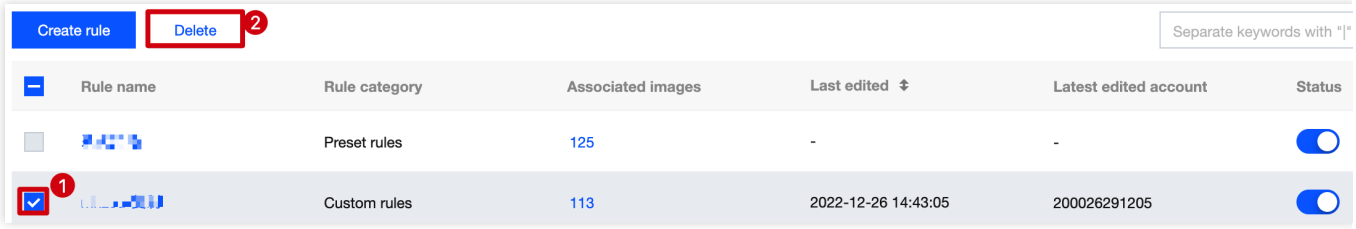
4. After selecting the target content, click **OK** or **Cancel**.

©2013-2022 Tencent Cloud. All rights reserved.

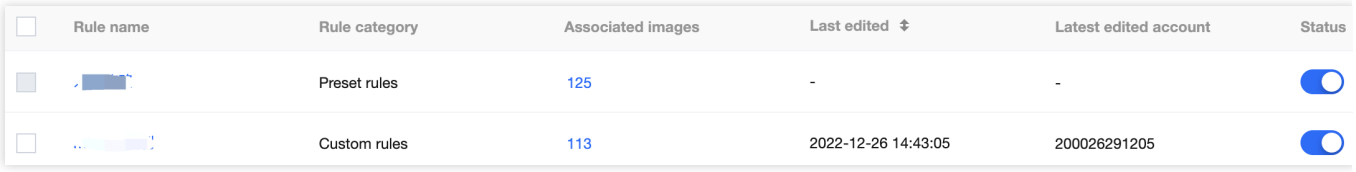
Deleting a Rule

1. Log in to the TCSS console and click **Advanced Prevention** > **File Tampering** > **Rule configuration** on the left sidebar.
2. On the **Rule configuration** page, delete a rule in either of the following methods:
Select the target rule, click

, and click **Delete** on the left in the **Operation** column.



Select the target rule and click **Delete**.



3. In the pop-up window, click **Delete** or **Cancel**.

Note:

The rule cannot be recovered once deleted, and images associated with the rule will be automatically associated with the default system rule.

Exporting a Rule

1. Log in to the TCSS console and click **Advanced Prevention** > **File Tampering** > **Rule configuration** on the left sidebar.
2. On the **Rule configuration** page, click

to select the target file tampering rule and click

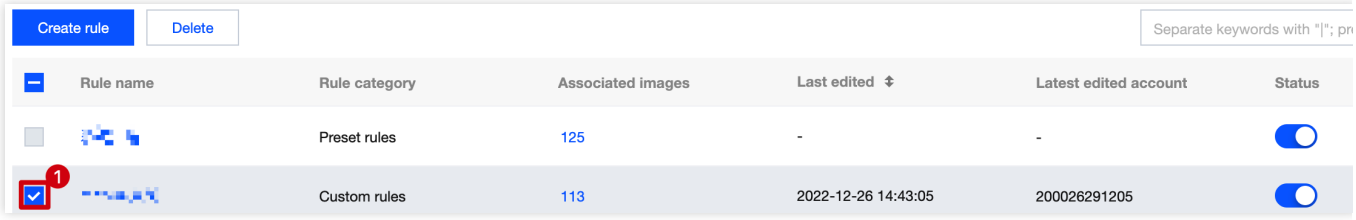
©2013-2022 Tencent Cloud. All rights reserved.

to export it.

Note:

Click

in the **Operation** column to select multiple ones.



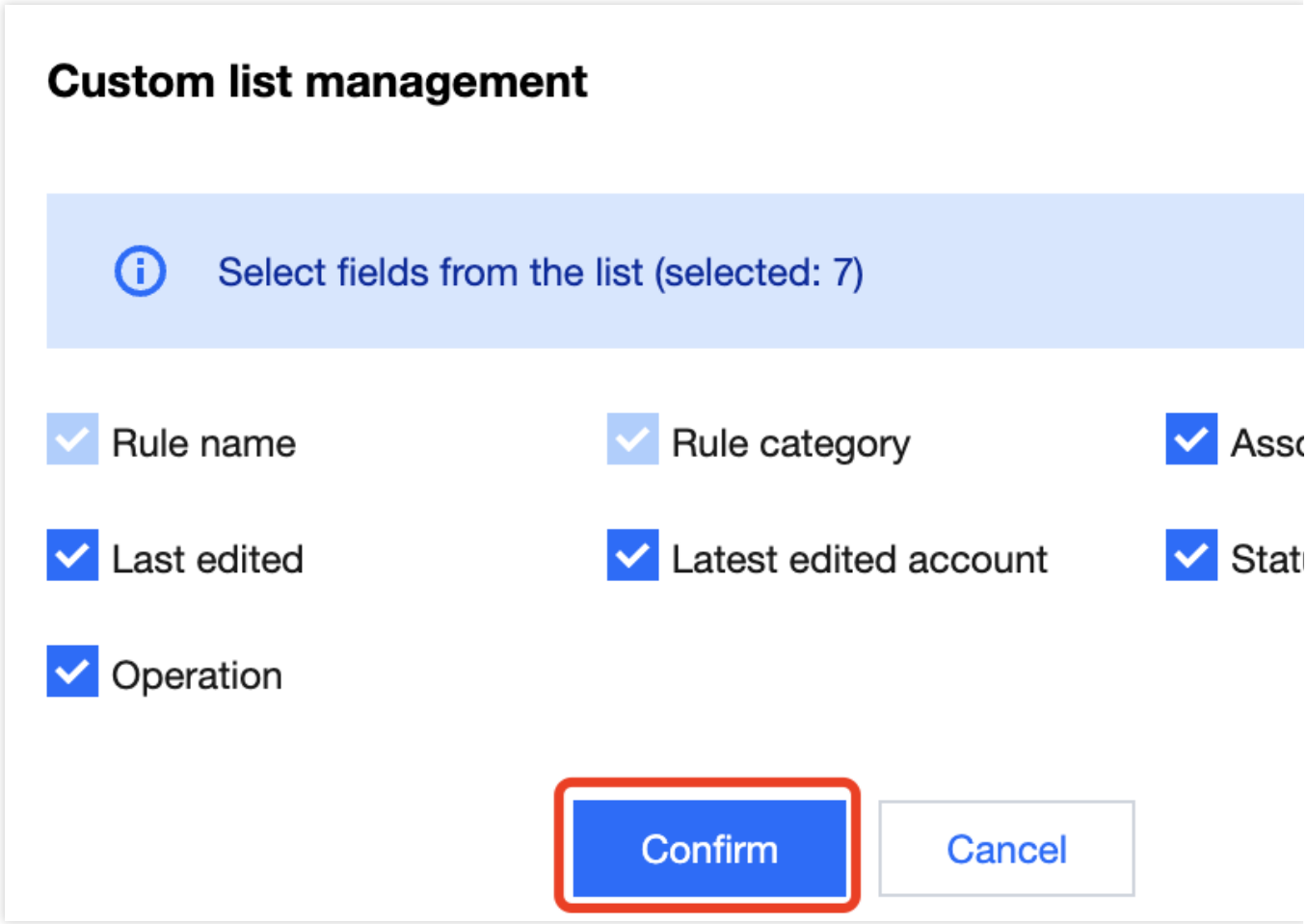
Custom List Management

1. Log in to the TCSS console and click **Advanced Prevention** > **File Tampering** > **Rule configuration** on the left sidebar.
2. On the **Rule configuration** page, click

to pop up the **Custom List Management** window.

3. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Key fields in the list

1. Rule category: Preset rule or custom rule.
2. Associated images: Number of images for which the rule takes effect. Click the number of affected images to pop up the drawer on the right, which displays the rule details.
3. Status: On/Off.
4. Operation: System rules can only be copied, and custom rules can be copied, edited, or deleted.

©2013-2022 Tencent Cloud. All rights reserved.

High-Risk Syscall Event List

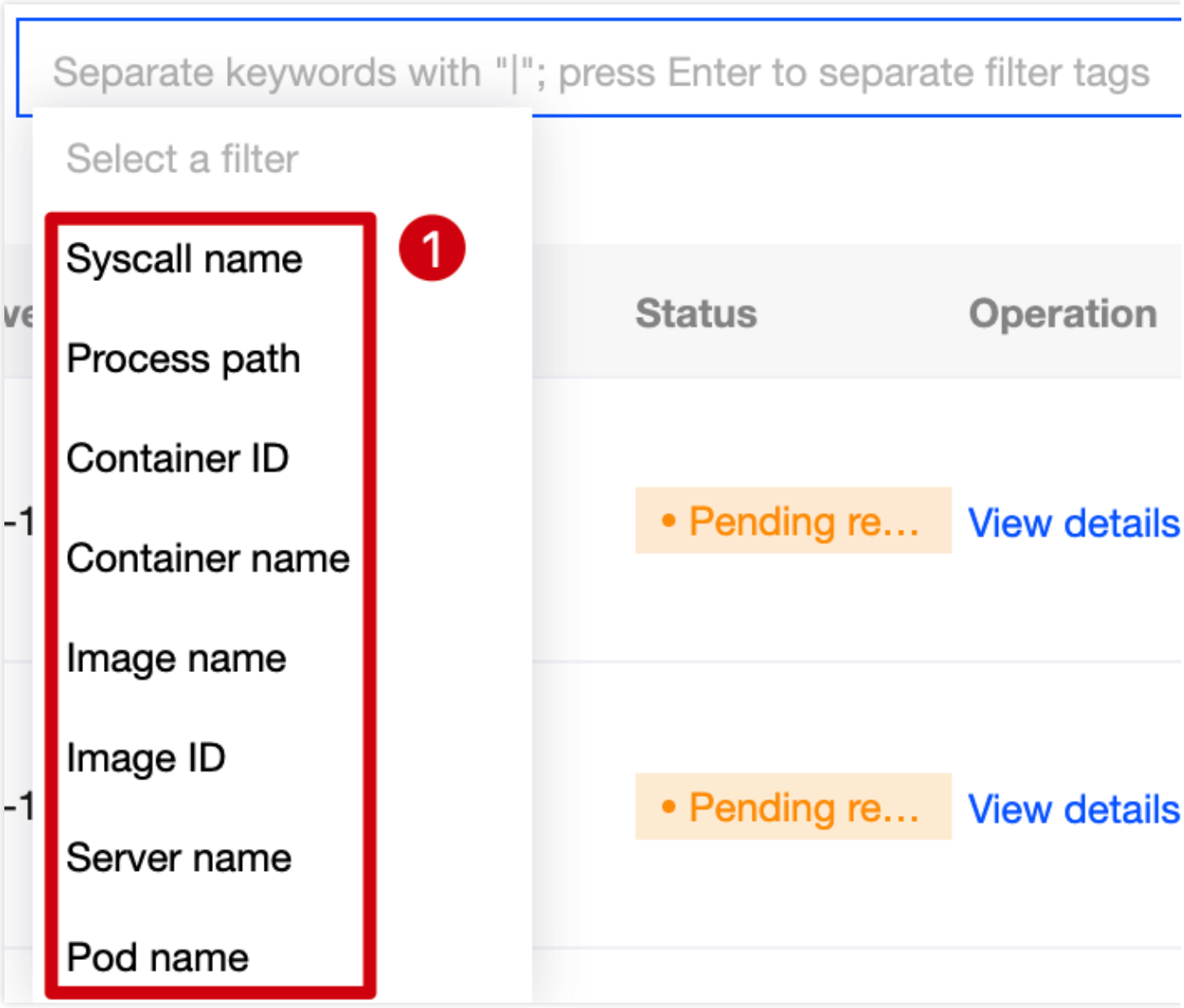
Last updated：2024-01-23 15:44:44

The high-risk syscall feature provides the lists of risky syscall events and allowlist policies. The event list module displays the high-risk syscall check results.

Filtering and Refreshing Events

1. Log in to the TCSS console and click **Advanced Prevention** > **High-risk Syscalls** > **Event list** on the left sidebar.
2. On the **Event list** page, click the search box and search for high-risk syscall events by keyword such as process path, syscall name, or container name.

©2013-2022 Tencent Cloud. All rights reserved.



3. On the **Event list** page, click

on the right of the **Operation** column to refresh the event list.

Exporting the Event List

1. Log in to the TCSS console and click **Advanced Prevention** > **High-risk Syscalls** > **Event list** on the left sidebar.
2. On the **Event list** page, click

©2013-2022 Tencent Cloud. All rights reserved.

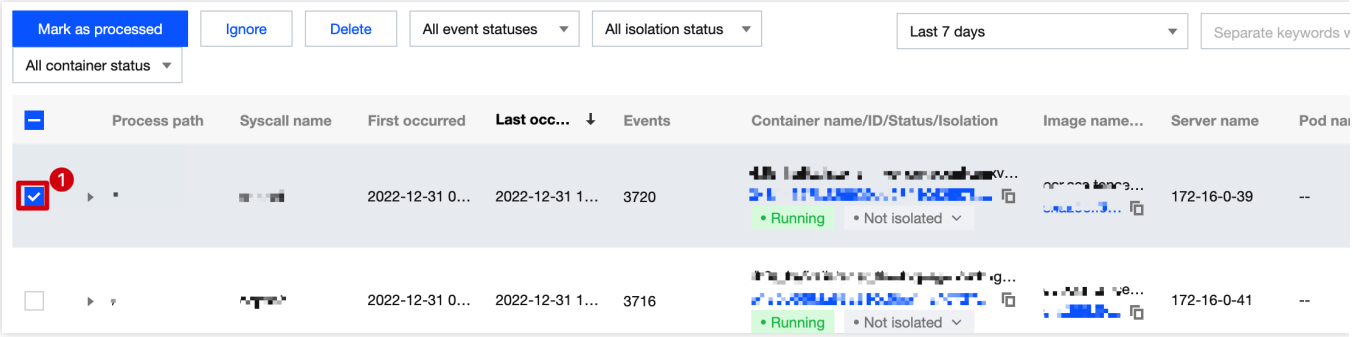
to select the target high-risk syscall event and click

to export it.

Note:

Click

in the **Operation** column to select multiple ones.



Changing the Event Status

Log in to the TCSS console and click **Advanced Prevention** > **High-risk Syscalls** > **Event list** on the left sidebar.

Method 1

On the **Event list** page, you can mark a high-risk syscall event as processed or ignore or delete it.

Mark as processed: Click

to select the target high-risk syscall event and click **Mark as processed** > **OK**.

Note:

It's recommended to handle the event by following "Solution" in the event details and mark it as processed.

Ignore: Click

to select the target high-risk syscall event and click **Ignore** > **OK**.

Note:

Only the selected events are ignored. Alerts will be triggered when the same events occur again.

©2013-2022 Tencent Cloud. All rights reserved.

Delete: Click

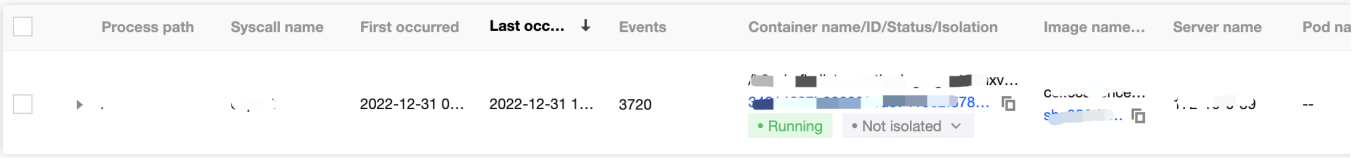
to select the target high-risk syscall event and click **Delete** > **OK**.

Note:

The selected event record will no longer be displayed in the console and cannot be recovered once deleted. Proceed with caution.

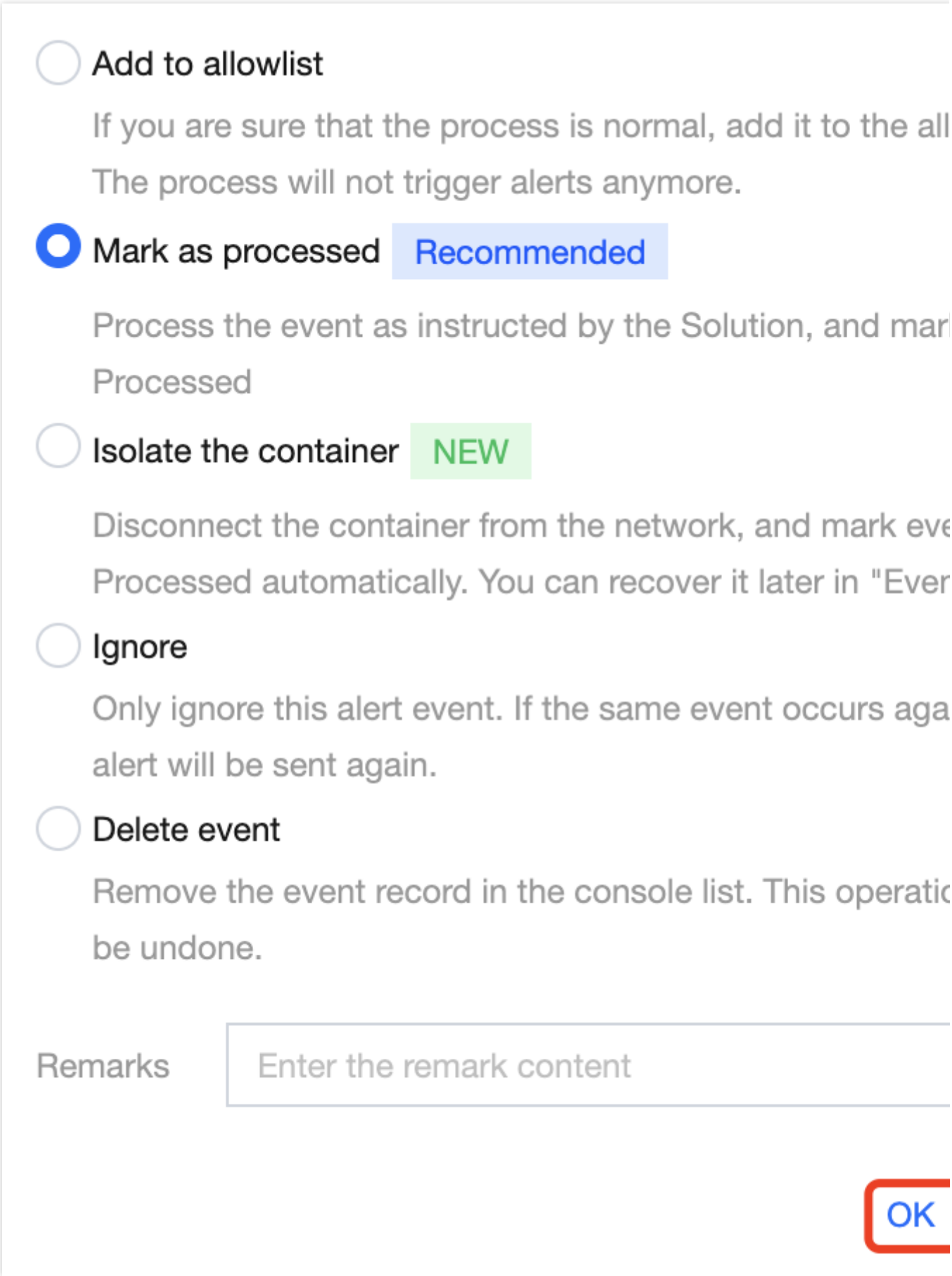
Method 2

1. On the **Event list** page, click **Process now** to add events in the **Pending resolved** status to the allowlist, mark them as processed, or ignore them.



2. Click **OK** or **Cancel**.

©2013-2022 Tencent Cloud. All rights reserved.



©2013-2022 Tencent Cloud. All rights reserved.

3. On the **Event list** page, click **Unignore** or **Delete** to unignore or delete events in the **Ignored** status.

Note:

As an event will be in the **Pending resolved** status once unignored, you need to click **OK** for confirmation.

The event record will no longer be displayed in the console and cannot be recovered once deleted. Proceed with caution.

4. On the **Event list** page, click **Delete** to delete events in the **Processed** status.

Note:

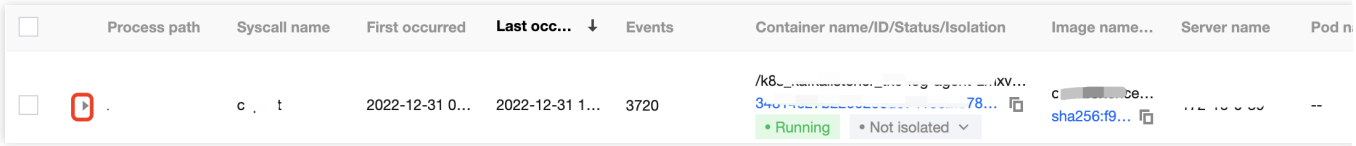
The event record will no longer be displayed in the console and cannot be recovered once deleted. Proceed with caution.

Viewing Event Details

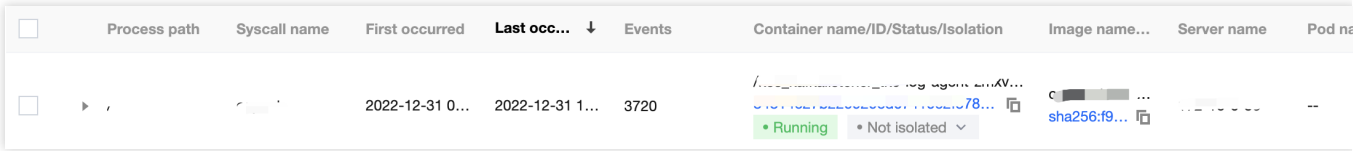
1. Log in to the TCSS console and click **Advanced Prevention** > **High-risk Syscalls** > **Event list** on the left sidebar.

2. On the **Event list** page, click

on the left of the **Process path** to view the event description.



3. On the **Event list** page, click **View details**.



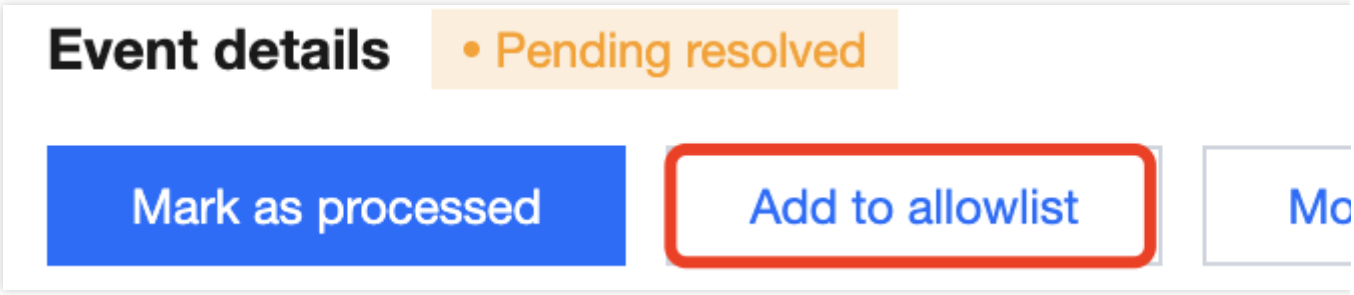
4. The **Event details** page displays the event details, process information, parent process information, and event description. You can mark the event as processed, ignore it, or add it to the allowlist.

Note:

For detailed directions on how to mark an event as processed or ignore or delete it, see Changing the Event Status.

5. On the **Event details** page, click **Add to allowlist** and confirm the conditions (process path and syscall name) and the scope.

©2013-2022 Tencent Cloud. All rights reserved.



Conditions: **Process path** and **Syscall name**, which cannot be changed.

Scope: **All images** or **Specified images**. Click

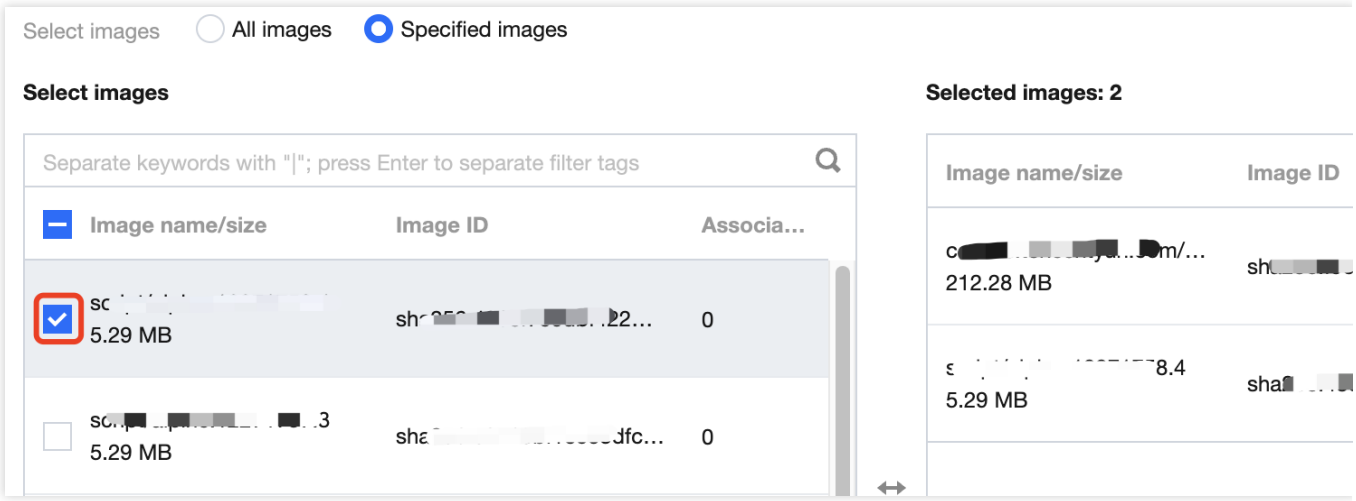
or

to select or delete the target specified image.

Note:

You can press Shift to select multiple ones.

©2013-2022 Tencent Cloud. All rights reserved.



6. After selecting the target content, click **Set** or **Cancel**.

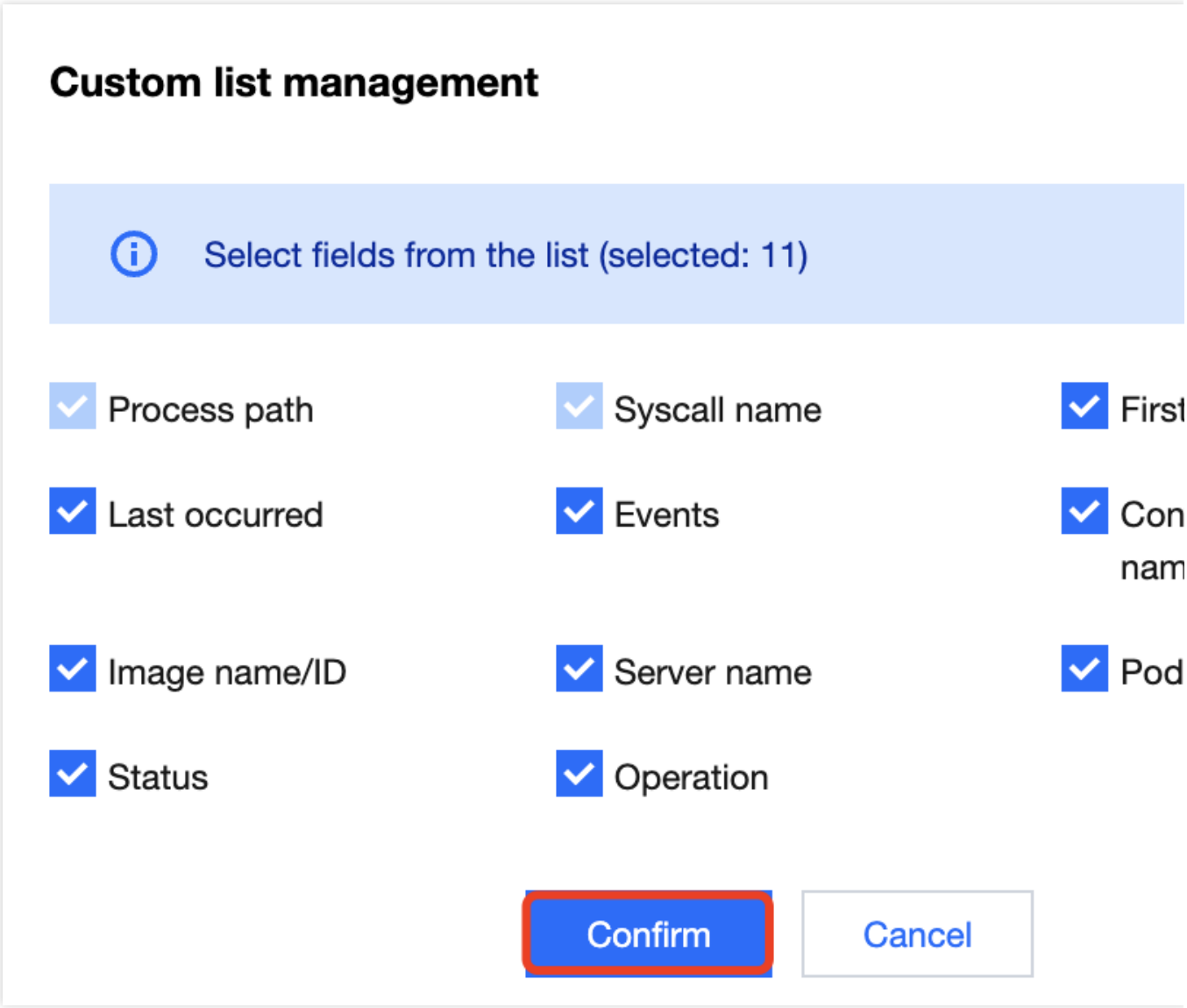
Custom List Management

1. Log in to the TCSS console and click **Advanced Prevention** > **High-risk Syscalls** > **Event list** on the left sidebar.
2. On the **Event list** page, click

to pop up the **Custom List Management** window.

3. In the pop-up window, select the target type and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Key fields in the list

1. First occurred: The time when an alert is first triggered by the syscall event. By default, the system aggregates the same alert events not processed.
2. Last occurred: The time when an alert is last triggered by the aggregated alert events. You can click the sort button on the right to sort the events in the list in chronological or reverse chronological order.
3. Events: Total number of alerts triggered by the syscall event within the aggregation period.
4. Execution result: **Blocked successfully**, **Failed to block**, **Allowed**, or **Alert**. You can quickly filter events in the list by action execution result.
5. Status: **Processed**, **Ignored**, **Pending resolved**, or **Allowed**. You can quickly filter events in the list by status.

©2013-2022 Tencent Cloud. All rights reserved.

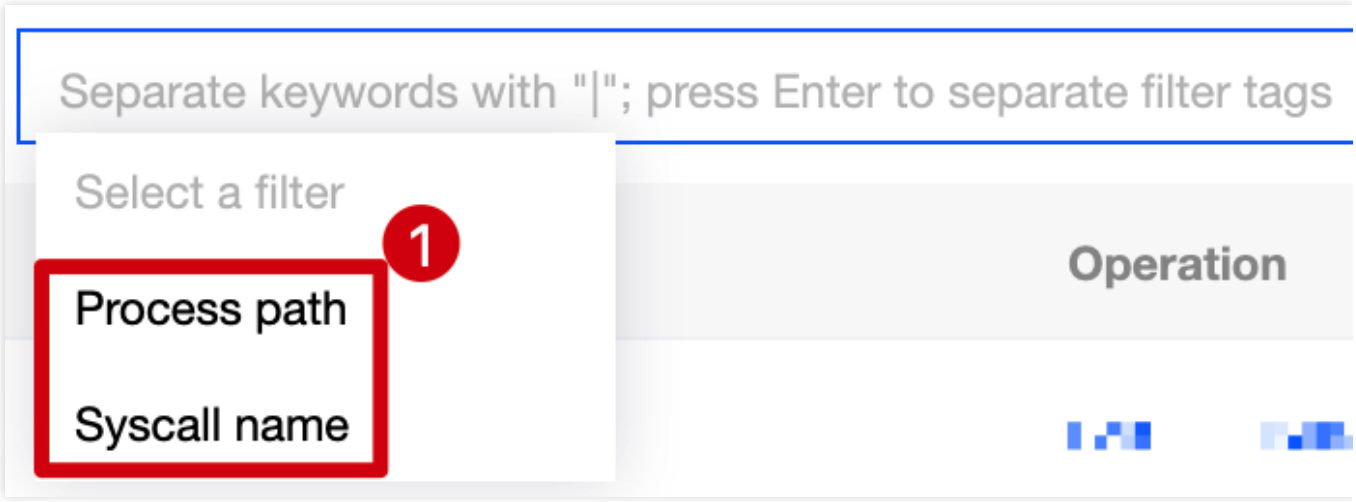
Allowlist Management

Last updated：2024-01-23 15:44:44

The allowlist policies module displays the option to configure the allowlist and the configured allowlist.

Filtering and Refreshing Allowed Images

1. Log in to the TCSS console and click **Advanced Prevention** > **High-risk Syscalls** > **Allowlist policies** on the left sidebar.
2. On the **Allowlist policies** tab, click the search box and search the configured allowlist by process path or syscall name.



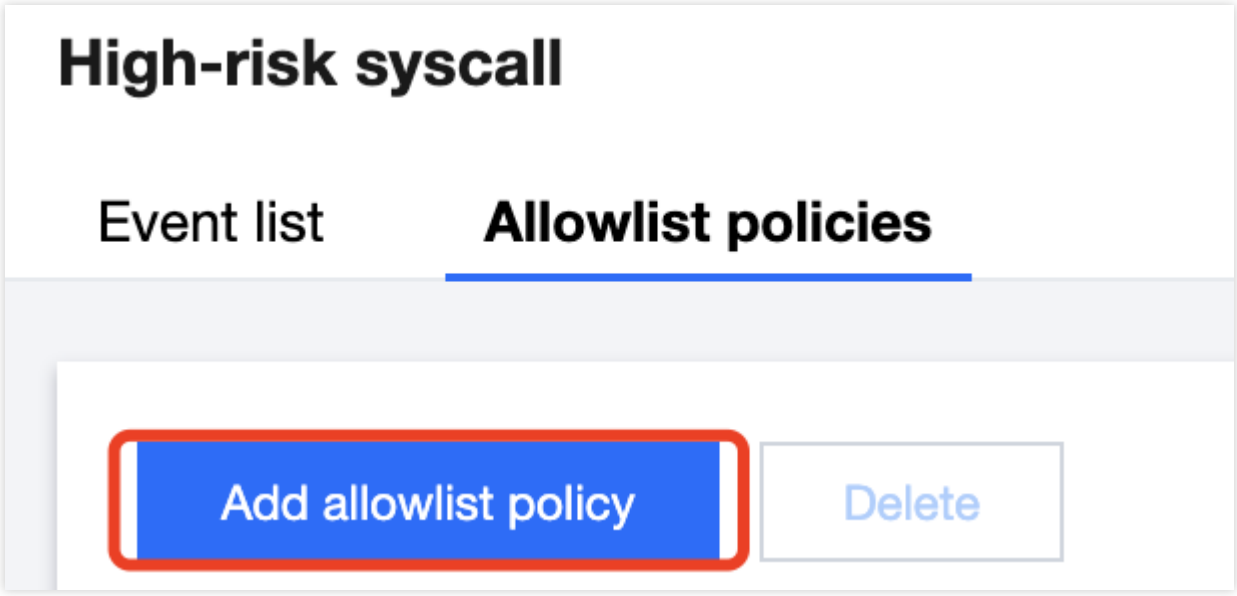
3. On the **Allowlist policies** tab, click

on the right of the **Operation** column to refresh the allowlist.

Adding an Allowlist Policy

1. Log in to the TCSS console and click **Advanced Prevention** > **High-risk Syscalls** > **Allowlist policies** on the left sidebar.
2. On the **Allowlist policies** tab, click **Add allowlist policy**.

©2013-2022 Tencent Cloud. All rights reserved.



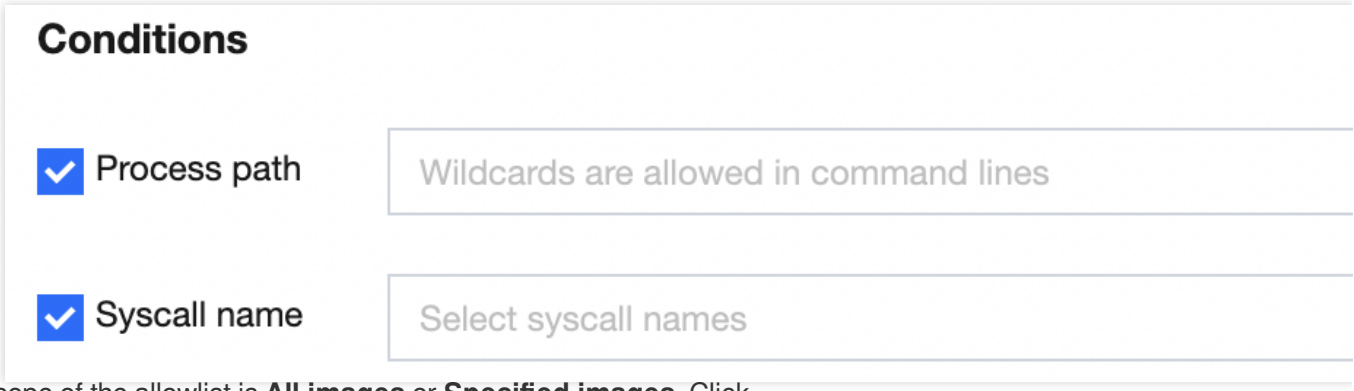
3. On the **Add allowlist policy** page, configure the target process path, syscall name, and scope.

Click

on the left of the **Process path** and **Syscall name**, enter the process path, and select the syscall name.

Note:

The process path is required.



The scope of the allowlist is **All images** or **Specified images**. Click

or

to select or delete the target specified image.

Note:

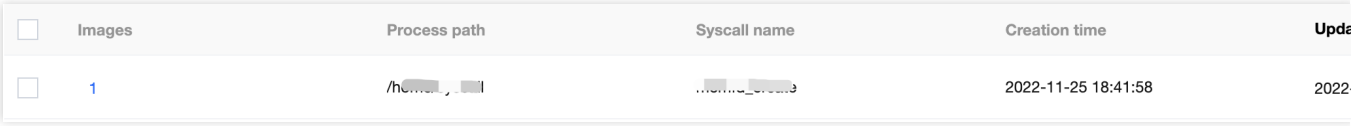
You can press Shift to select multiple ones.

©2013-2022 Tencent Cloud. All rights reserved.

4. After selecting the target content, click **OK** or **Cancel**.

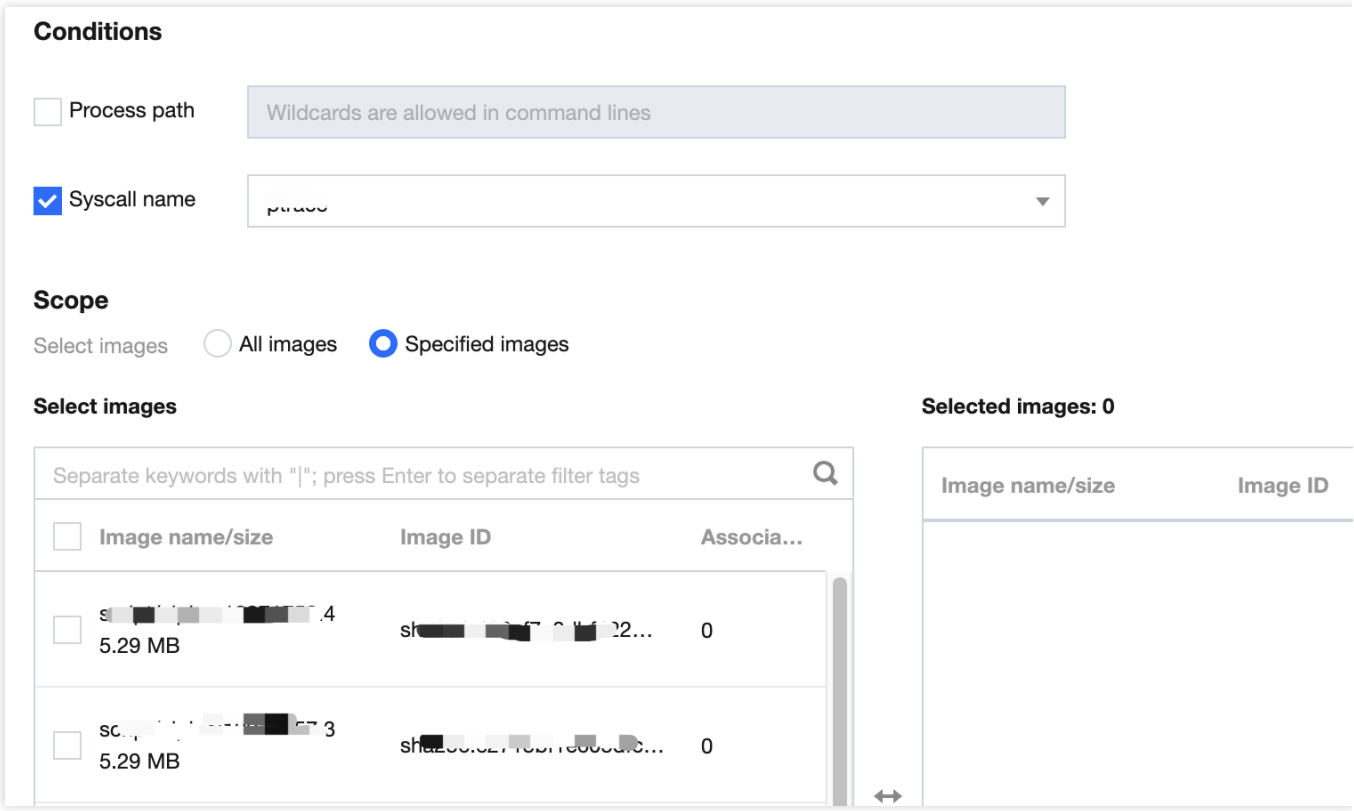
Editing the Allowlist

1. Log in to the TCSS console and click **Advanced Prevention** > **High-risk Syscalls** > **Allowlist policies** on the left sidebar.
2. On the **Allowlist policies** tab, click **Edit** on the right.



3. On the **Edit allowlist** page, modify the target process path, syscall name, and scope.

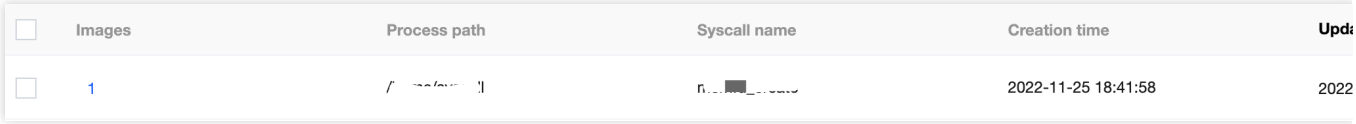
©2013-2022 Tencent Cloud. All rights reserved.



4. After selecting the target content, click **OK** or **Cancel**.

Deleting the Allowlist

1. Log in to the TCSS console and click **Advanced Prevention** > **High-risk Syscalls** > **Allowlist policies** on the left sidebar.
2. On the **Allowlist policies** tab, click **Delete** on the right.



3. In the pop-up window, click **Delete** or **Cancel**.

Note:

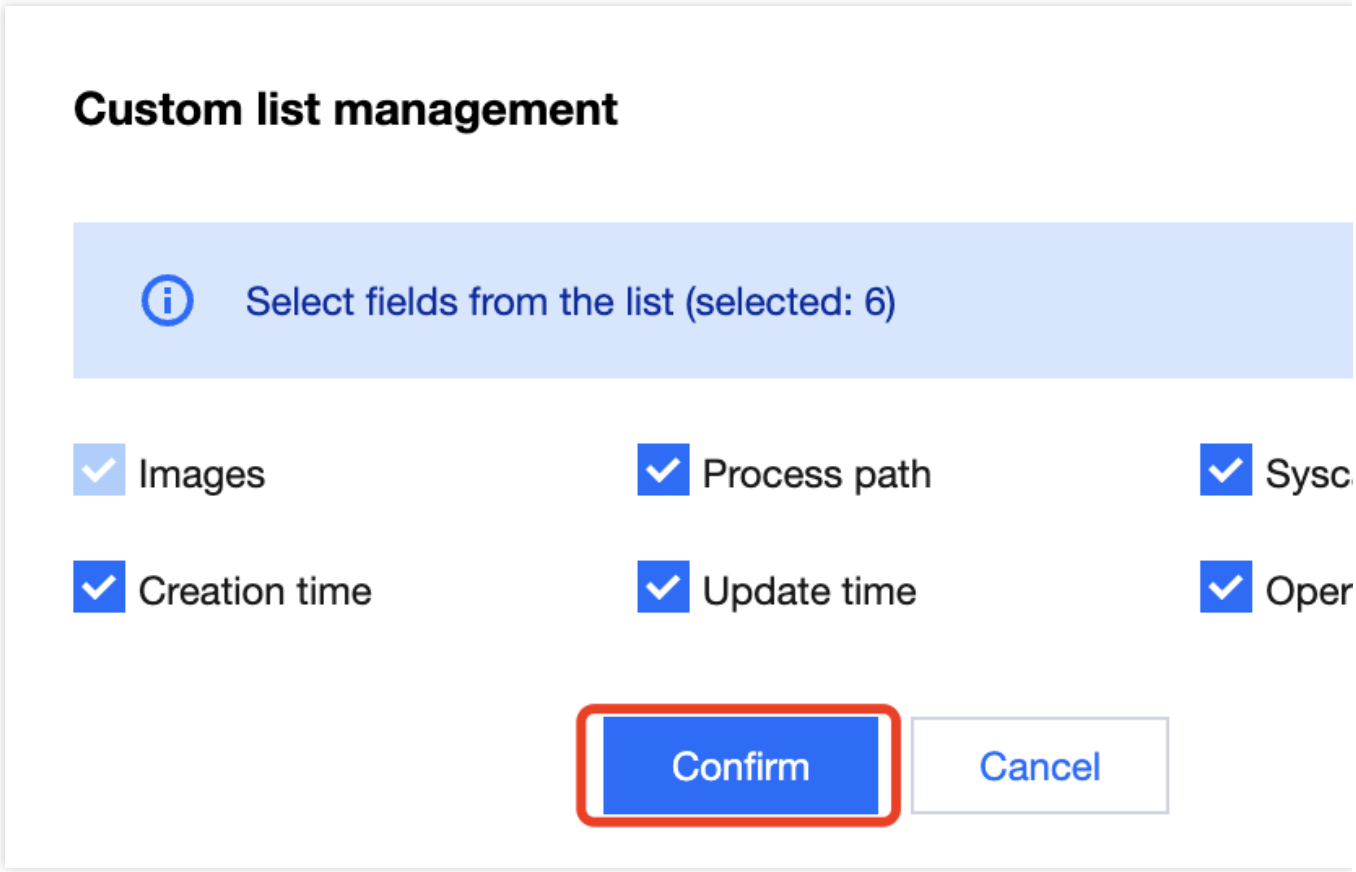
The allowlist cannot be recovered once deleted, and alerts will be generated when images associated with the allowlist trigger the preset policy.

Custom List Management

©2013-2022 Tencent Cloud. All rights reserved.

1. Log in to the TCSS console and click **Advanced Prevention** > **High-risk Syscalls** > **Allowlist policies** on the left sidebar.
2. On the **Allowlist policies** tab, click

to pop up the **Custom List Management** window.
3. In the pop-up window, select the target type and click **OK**.



Key fields in the list

1. Images: Images for which the allowlist takes effect.
2. Process path: Process path for which the allowlist takes effect.
3. Syscall name: Syscall name for which the allowlist takes effect.
4. Operation: Editing or deleting the allowlist.

©2013-2022 Tencent Cloud. All rights reserved.

Exceptional Requests of K8s APIs

Last updated：2024-08-13 17:10:53

Supports real-time monitoring of exceptional request behaviors of cluster APIs, and includes system policies and user-defined rules.
System Policy: Based on Tencent Cloud's security technology and multi-dimensional methods, it monitors exceptional request behaviors of cluster APIs through nine types of rules, including anonymous access, exceptional UA requests, anonymous permission change, credential acquisition, sensitive path mounts, command execution, exceptional scheduled task, static pod creation, and suspicious containers creation.
User-defined Rules: Supports custom exceptional request fields and specific effective ranges of K8s APIs, making it more flexible to meet actual business needs.

Event List

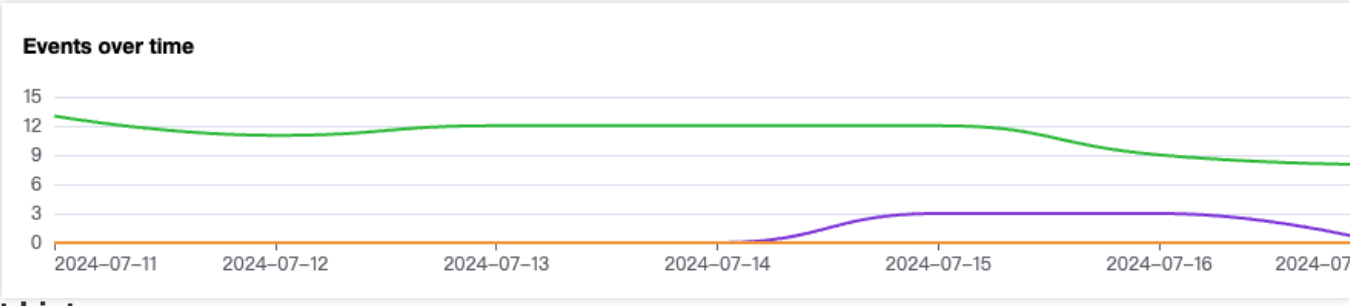
Log in to the TCSS console. In the left sidebar, click **Advanced Prevention** > **Abnormal K8s API requests**, and by default, you will enter the event list page.

Security Status and Events Trend

For the security status, the pending exceptional request events of K8s APIs and the number of security events counted by high, medium, low, and note risks will be collected according to the security events reported by the system.

For the events trend, the security events trend over the past seven days will be collected based on the hit system rules and custom rules according to the security events reported by the system.

©2013-2022 Tencent Cloud. All rights reserved.



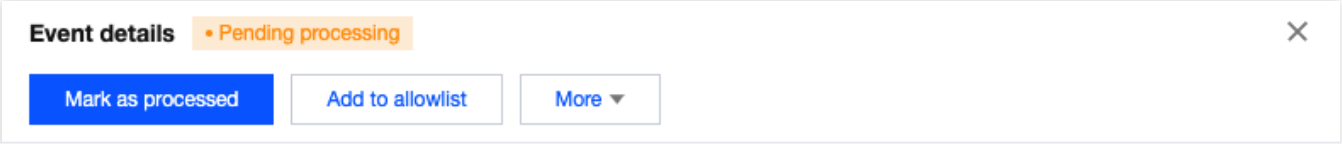
Event List

You can select the Last Occurred to view security events, or retrieve related events by cluster name or cluster ID. The fields in the event list include:

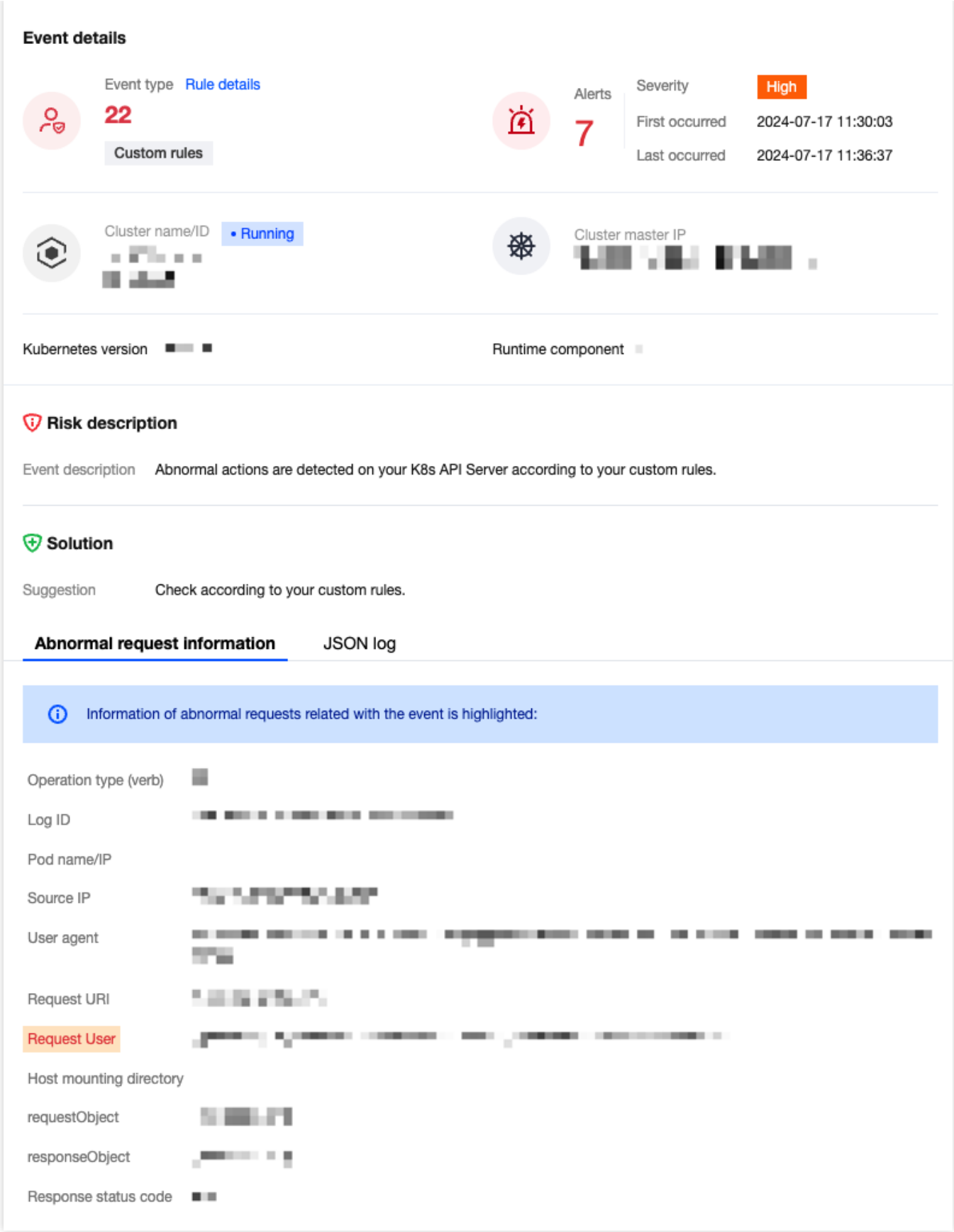
Field Name	Field Details
Hit Rules	Nine system rules and user-defined rules, including anonymous access, exceptional UA requests, anonymous permission change, credential acquisition, sensitive path mounts, command execution, exceptional scheduled task, static pod creation, and suspicious containers creation.
Rule Type	System rules, and user-defined rules
Threat Level	High, medium, low, and note
Cluster Name/ID/Running Status	Display the cluster name, cluster ID, and cluster running status impacted by the security events.
First Occurred	The time when this security event first occurred.
Last Occurred	The time when this security event most recently occurred.
Alarms	The system aggregates pending security events by cluster name, cluster ID, hit rules, and request logs. And the system displays them with an aggregation cycle of every day.
Status	Pending, processed, ignored, and allowlisted
Operation	Click **details** to view event details.

Viewing Details

In the event list, click **details** to view event details. Details include event details, cluster name/ID, cluster runtime components, risk description, recommended solution, exceptional request information, and JSON logs.



©2013-2022 Tencent Cloud. All rights reserved.

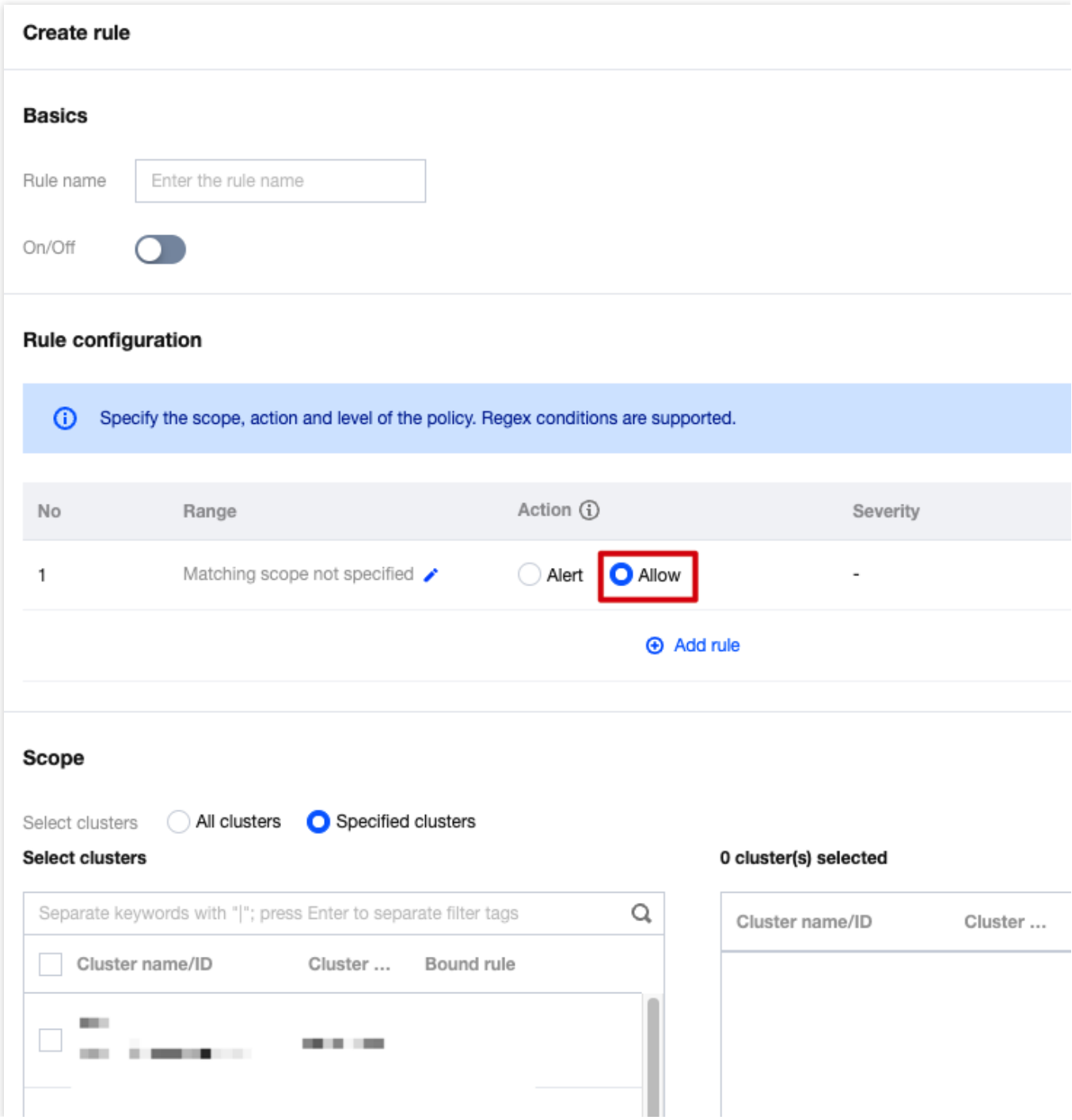


Processing the Event

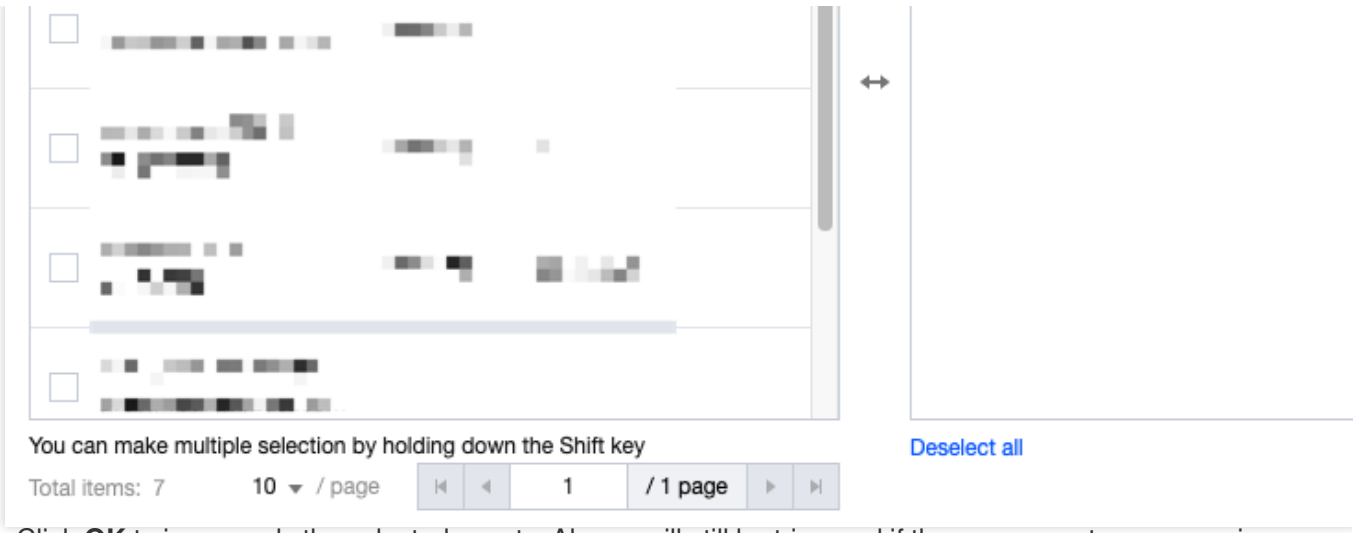
1. In the event list, click **Process**. You can select to mark the event as processed, add it to the allowlist, ignore it, or delete the records. Click **Confirm**.

©2013-2022 Tencent Cloud. All rights reserved.

2. In the secondary confirmation window, perform the following actions:
Mark as processed: It is recommended to process the event risk by following the solutions in the event details, and click **OK**. After processing, you can mark the event as processed.
Add to the allowlist: Configure relevant parameters, and click **OK**.
Note:
If you confirm that the K8s APIs request is a normal behavior, you can add it to the allowlist allow rules. Subsequent occurrences of this request will then be allowed to pass through without triggering alarms. Proceed with caution.
When users add to the allowlist, the system will automatically fill in the fields that trigger alarms and the cluster based on the source event. If needed, you can manually adjust the effective fields and effective cluster range of the allowlist.



©2013-2022 Tencent Cloud. All rights reserved.



Ignore: Click **OK** to ignore only the selected events. Alarms will still be triggered if the same events occur again.

Delete log: Click **OK**, the selected event record will be deleted. It will no longer be displayed in the console, and cannot be recovered. Proceed with caution.

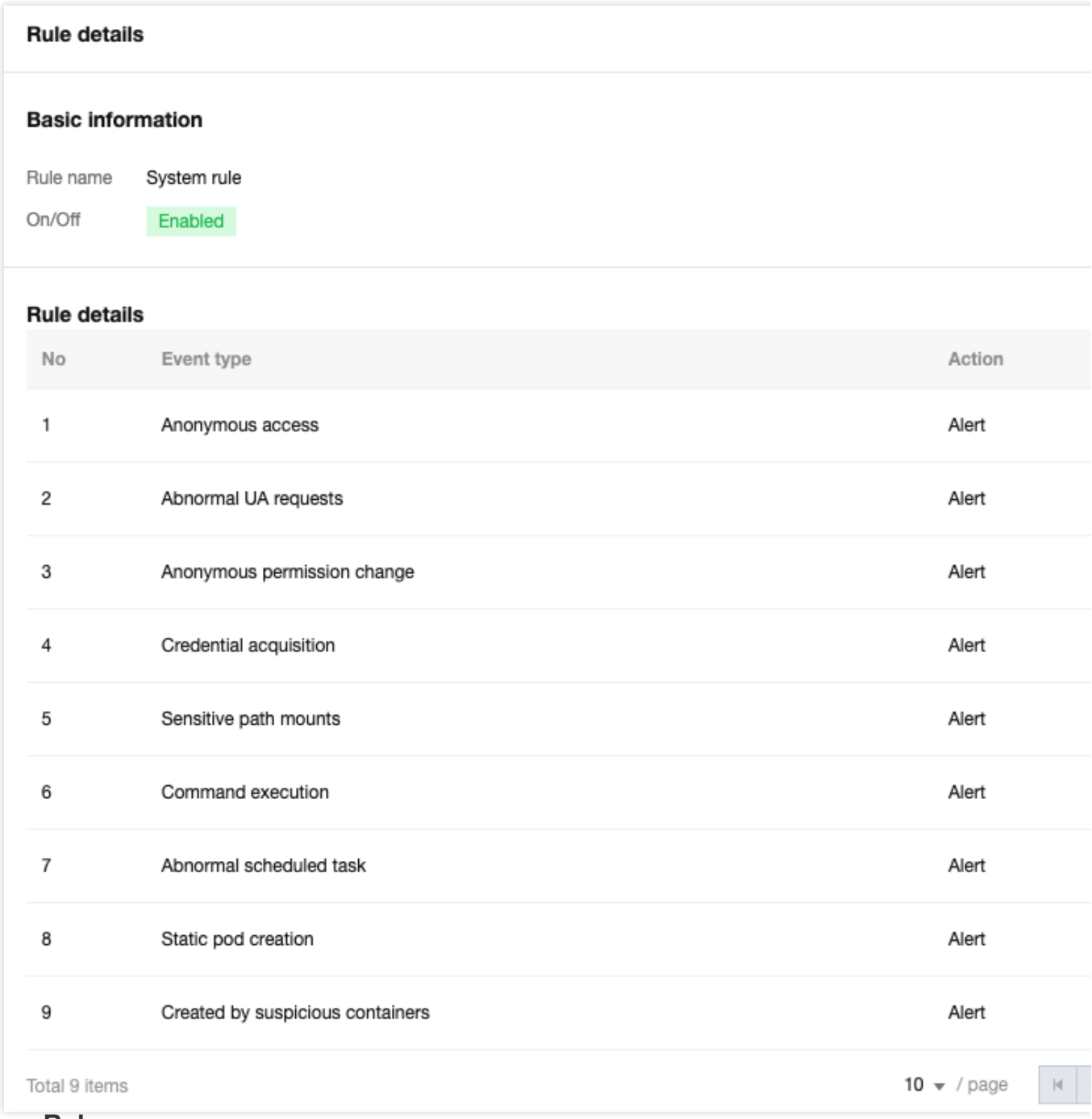
Rule Configuration

Log in to the TCSS console. In the left sidebar, click **Advanced Prevention** > **Abnormal K8s API Requests** > **Rule configuration** to enter the rule configuration page.

System Rules

On the rule configuration page, enable or disable system rules and custom rules. Click **Rule name** to view all types of system rules, as shown in the figure below. Users can also disable certain types of system rules through this page.

©2013-2022 Tencent Cloud. All rights reserved.

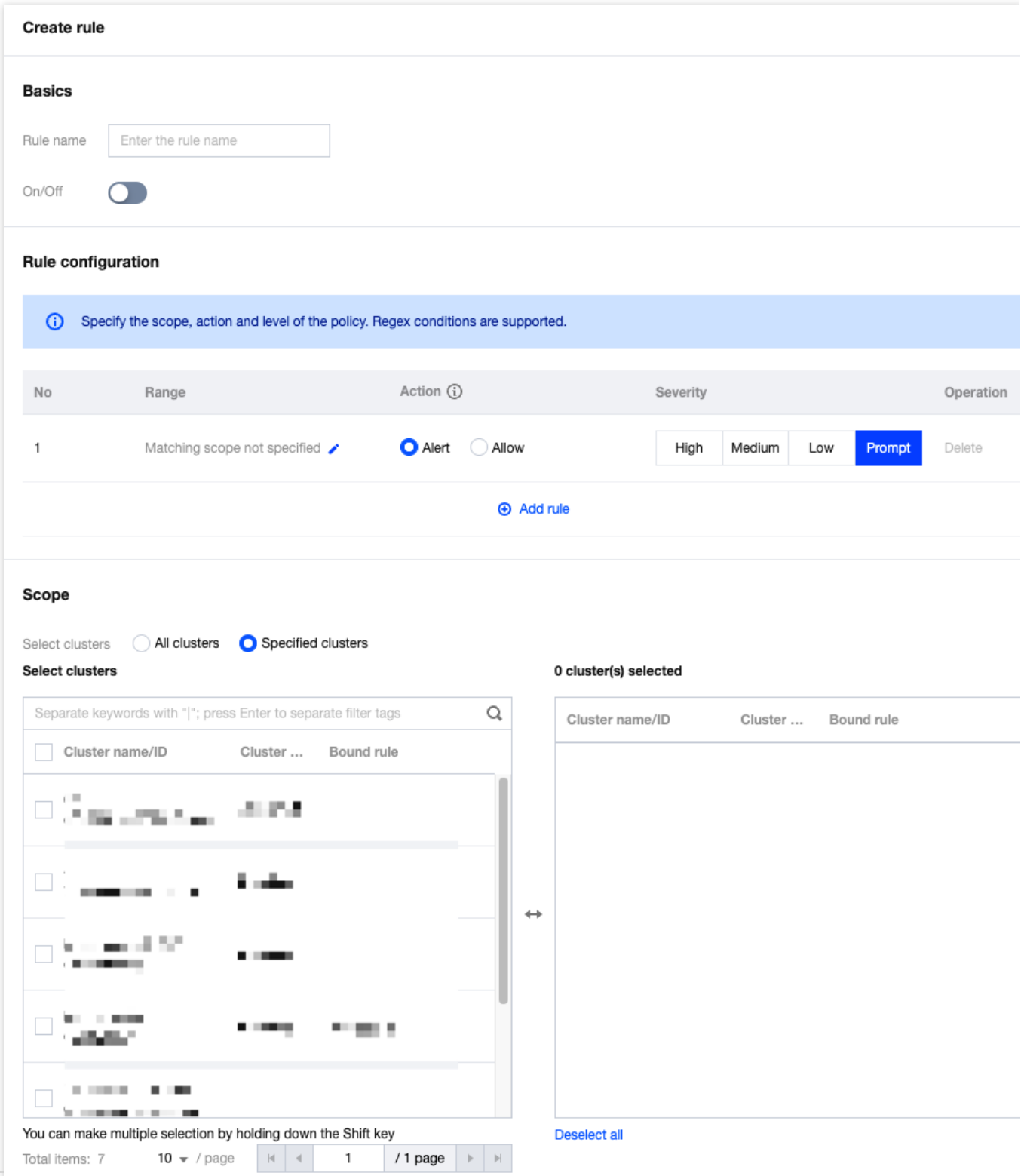


Custom Rules

In addition to the system rules provided by the TCSS products, users can also create custom rules.

On the rule configuration page, click **Create rule**, configure the relevant parameters, and click **Save**.

©2013-2022 Tencent Cloud. All rights reserved.



Field Name	Field Details
Basic Configuration	Includes the name of custom rules and the switch for enabling or disabling the rules.
Rule Configuration	Configure the fields for alarms and allowlisting in this section. When configuring alarm fields, you also need to concurrently configure the threat level for the rules. When there are multiple configuration items, click **Add rule** at the bottom.

©2013-2022 Tencent Cloud. All rights reserved.

	To configure the specific content of a rule, click **Edit** in the matching range column. Rule configuration supports regular expressions.
Effective Range	Users can select the custom effective cluster range for configuration rules. Note:**Only one custom rule can be bound to the same cluster.** If multiple detection rules need to be configured for one cluster, it is recommended to edit and add them within the same rule.

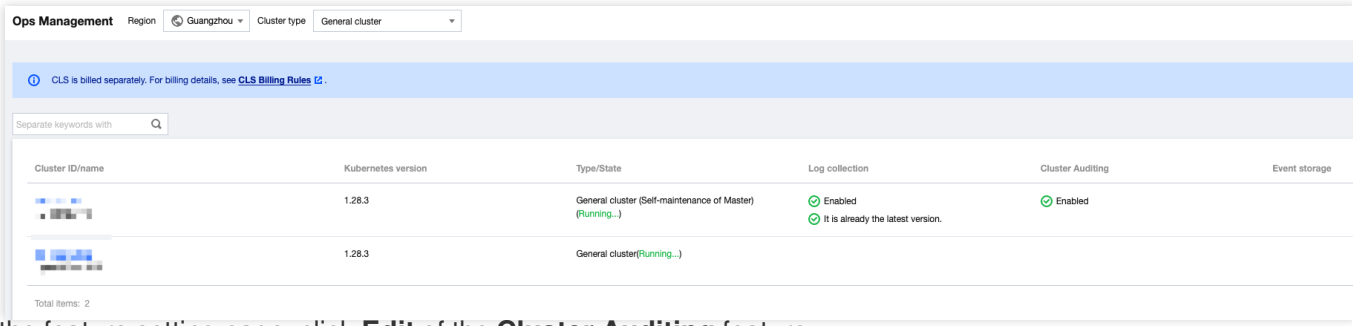
TKE K8s Cluster Enabling the Audit Process

When the audit feature of the cluster is not enabled, the audit logs of the K8s APIs cannot be collected for risk detection.

Note:

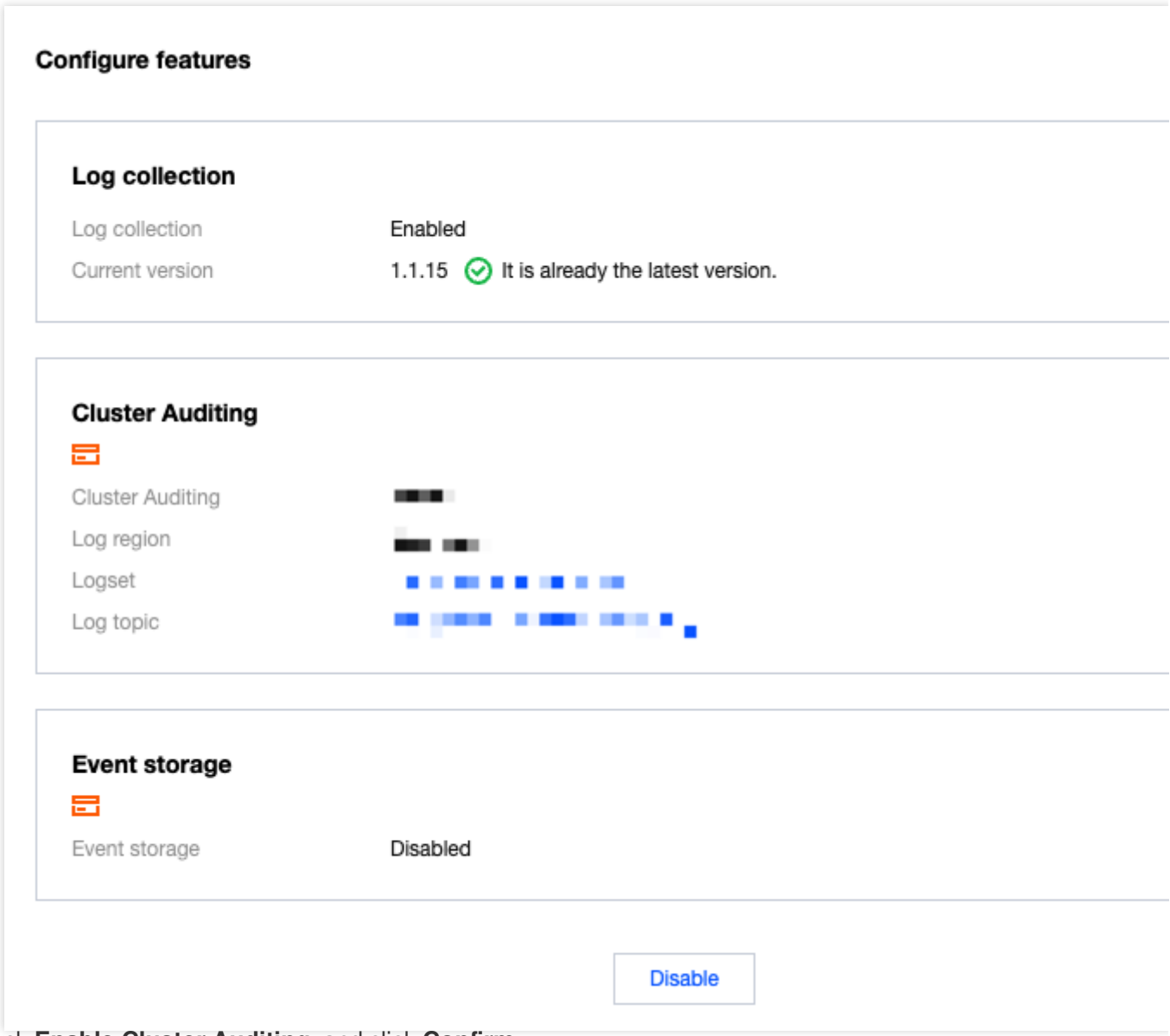
After the cluster audit is enabled, CLS will bill according to your actual usage. For billing standards, see the CLS billing overview.

1. On the TKE console's Operation and Maintenance Feature Management Page, select the cluster for which you need to enable auditing, and click **Set**.



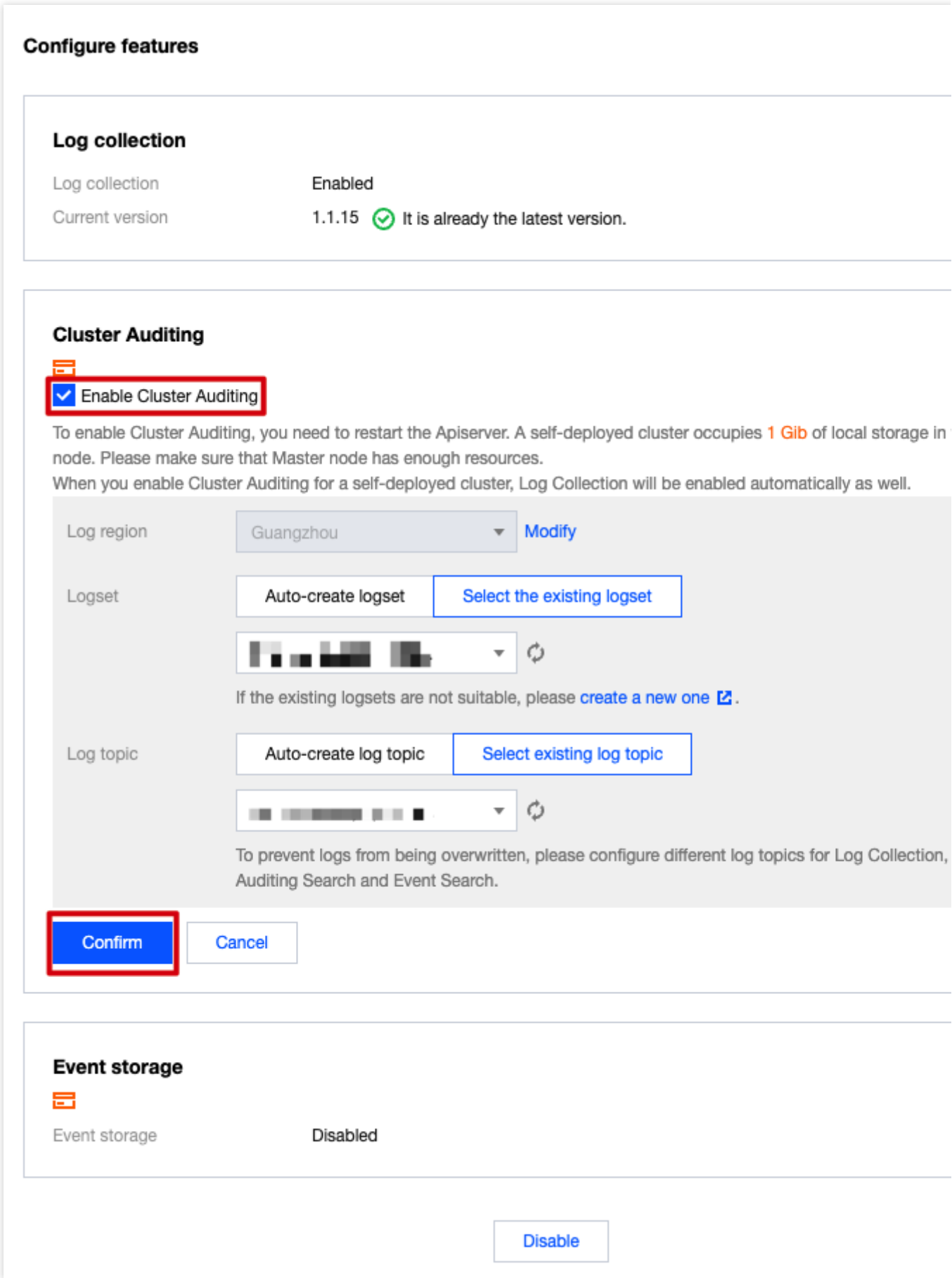
2. On the feature setting page, click **Edit** of the **Cluster Auditing** feature.

©2013-2022 Tencent Cloud. All rights reserved.



3. Check **Enable Cluster Auditing**, and click **Confirm**.

©2013-2022 Tencent Cloud. All rights reserved.



©2013-2022 Tencent Cloud. All rights reserved.

©2013-2022 Tencent Cloud. All rights reserved.

Policy Management
Container Network Policy
Policy Configuration

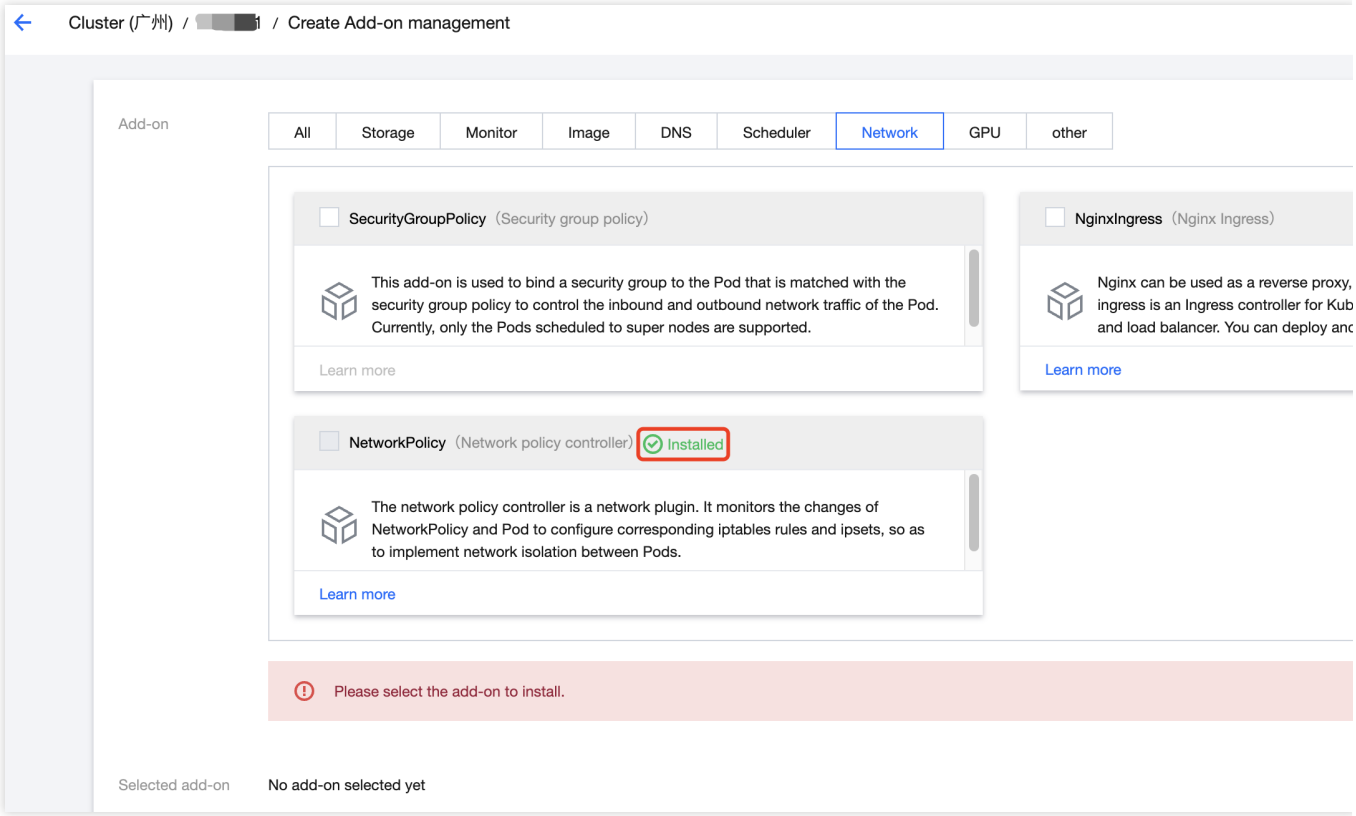
Last updated：2024-01-23 15:44:44

Container network policies provide network policy distribution and management capabilities for cluster containers based on native Kubernetes NetworkPolicies. It defines the protected targets in the cluster and sets their outbound and inbound rules to control network access between containers. This document describes how to configure and manage a container network policy and implement network isolation between containers.

Limits

Currently, container network policies are supported for the following clusters: TKE self-deployed clusters, TKE managed clusters, and self-built Kubernetes clusters.
Container network policies rely on the network component deployed in the cluster. Currently, the `Kube-router` network component is supported.
To use container network policies in a TKE cluster, make sure that the `NetworkPolicy` component is installed in the cluster. For more information on the component, see Network Policy.

©2013-2022 Tencent Cloud. All rights reserved.



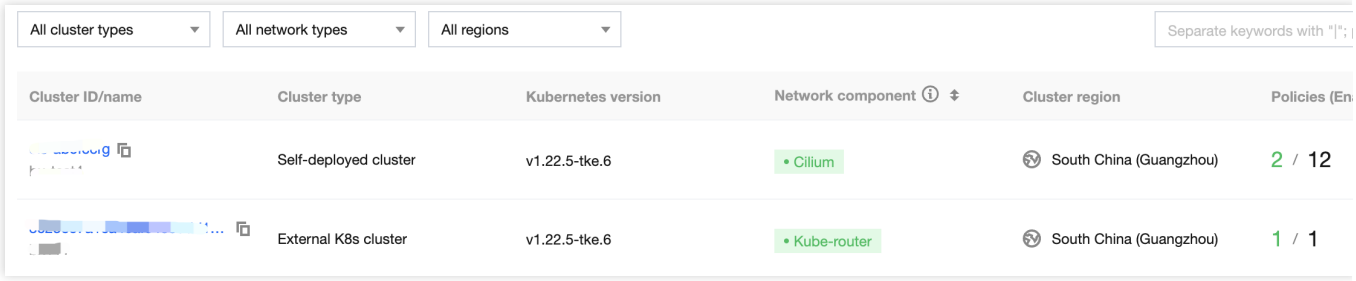
For directions on how to install the `Kube-router` network component in a self-built Kubernetes cluster, see User Guide - Kube-router.

As using container network policies **may compromise the cluster performance**, you should carefully assess the cluster size and performance loss first. For example, if the network policy is enabled during `Kube-router` component deployment, when the number of Pods increases from 2,000 to 8,000, the cluster performance will drop by 10% to 20%. For more information, see Using Network Policy for Network Access Control.

Managing Cluster Network Policies

1. Log in to the TCSS console and click **Policy Management** > **Container Network Policies** on the left sidebar.
2. On the **Container Network Policies** page, view the network component type, region, number of enabled policies, and total number of policies of the cluster.

©2013-2022 Tencent Cloud. All rights reserved.

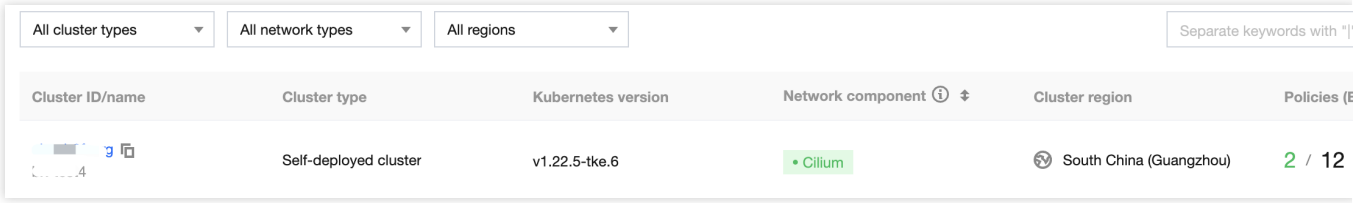


3. Select the target cluster and click **Policy Management** to enter the **Cluster policies** page, where you can add, edit, or delete policies or sync them from the cluster.

Note:

Currently, only the `Kube-router` network component is supported.

Container network policies rely on the network component deployed in the cluster. The cluster policy management feature is unavailable for network components not supported.



Creating a Cluster Network Policy

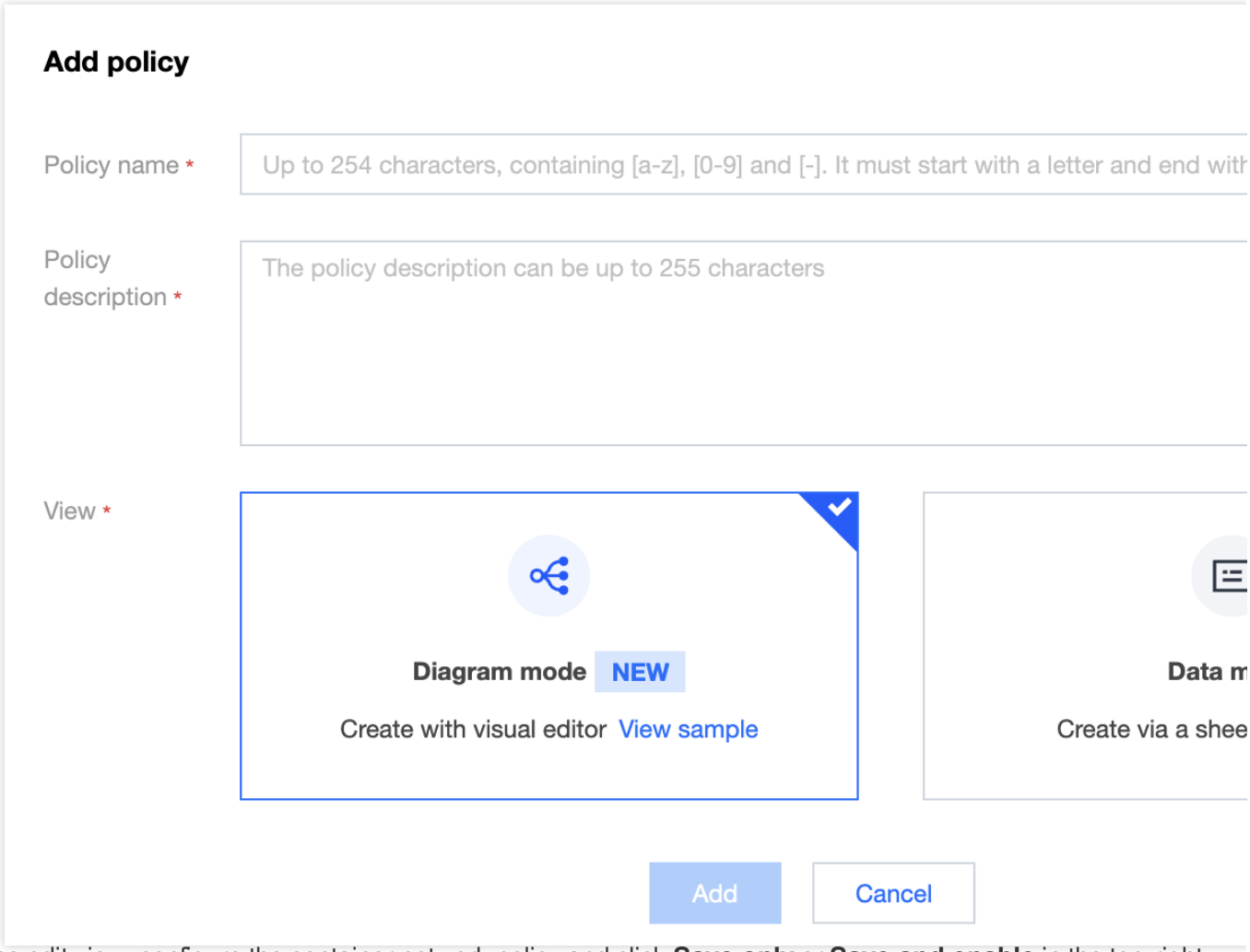
1. On the **Cluster policies** page, click **Create policy**.

2. In the **Create policy** pop-up window, enter the policy name and description and select the diagram mode or data mode to enter the container network policy editing page.

Note:

If the mode is switched in the edit view, the policy created in the original mode will not be saved, and a new empty policy will be created.

©2013-2022 Tencent Cloud. All rights reserved.



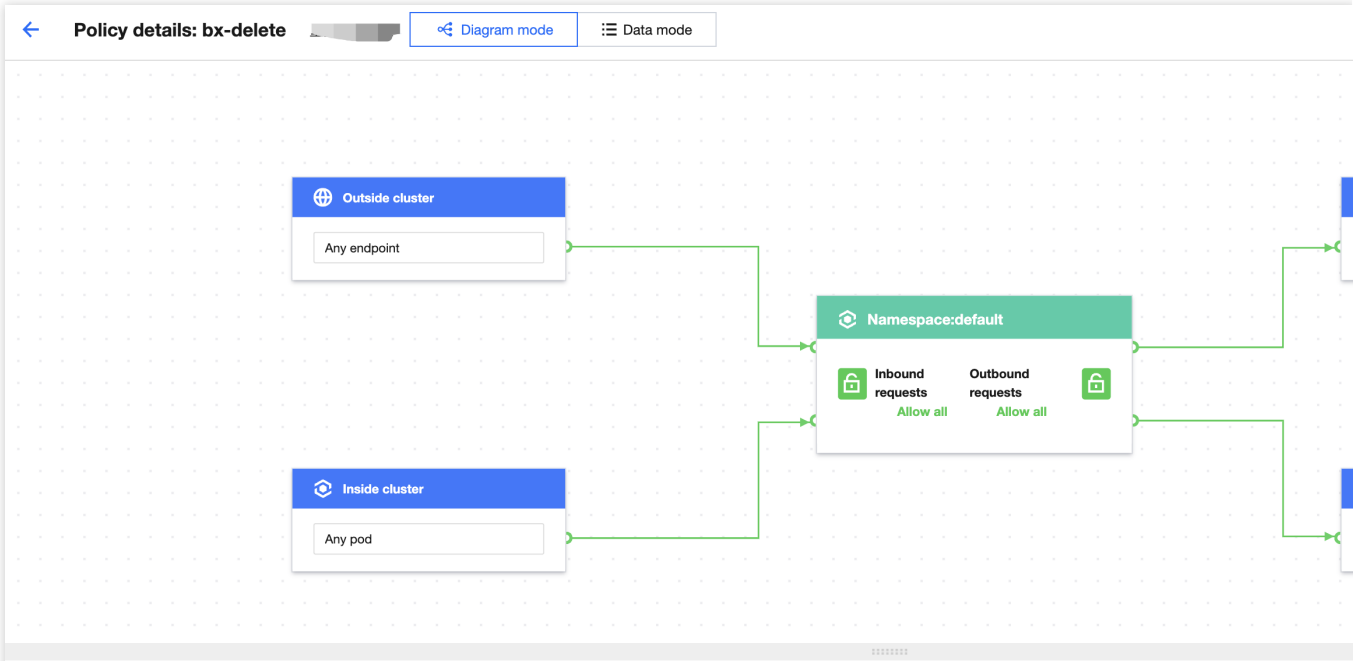
3. In the edit view, configure the container network policy and click **Save only** or **Save and enable** in the top-right corner.

Note:

Save only: Save the current network policy but do not enable it.

Save and enable: Save the current network policy and enable it.

©2013-2022 Tencent Cloud. All rights reserved.




```yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: bx-delete
  namespace: default
spec:
  egress:
    - {}
  ingress:
    - {}
```

Policy Description

Basic information

Policy name: The policy name will be associated with the NetworkPolicy name. It must be unique, cannot be changed, and can contain up to 254 characters.
Policy description: It can contain up to 1,000 characters.

Policy type

A container network policy is either a **preset policy** or one **synched from the cluster**. The former is created and managed in the TCSS console, while the latter is automatically discovered and obtained by the system, including policies created and modified manually in the cluster.
A policy synced from the cluster will be included in the product policy library for unified management after confirmation. It can be enabled, disabled, or edited in the console.

Protected target

A protected target is a Pod associated through the Pod label in a namespace. Pod applications with the same label are a group of protected targets.

©2013-2022 Tencent Cloud. All rights reserved.

Note:

A label is a Kubernetes label, a key-value pair attached to a Kubernetes object (such as a Pod). For more information, see Labels and Selectors.

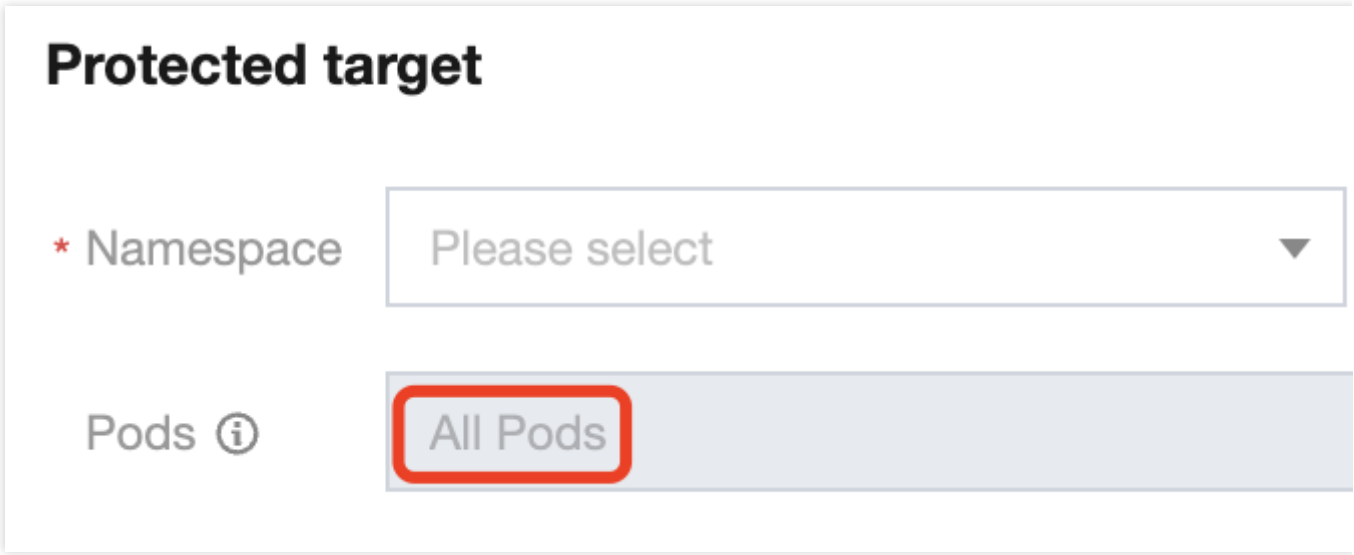
When a protected target is associated through multiple Pod labels, the logic between the labels is "AND", indicating that only Pod applications meeting all the label conditions will be associated with the protected target.

Namespace: Namespace of the protected target, which is `Default` by default.

Pods: When the Pod label is **All Pods**, all Pods in the namespace are protected targets. In this case, the network policy takes effect for the entire namespace.

Note:

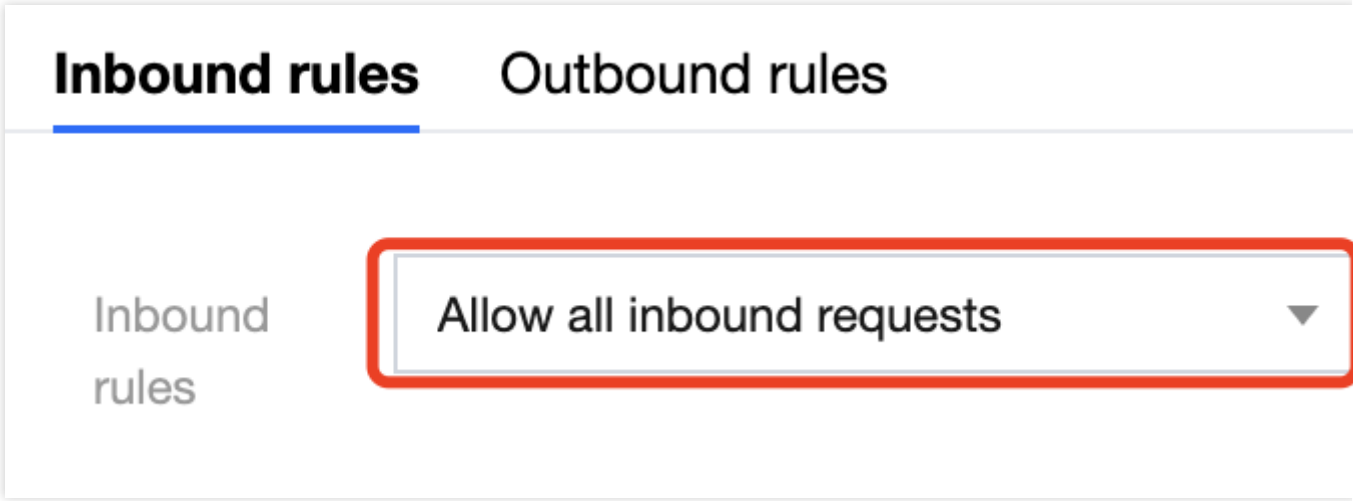
If multiple Pod labels are used to associate a protected target, when the key-value of a newly added label is the same as that of an existing one, only one key-value will take effect, and the label with the existing key-value will be overwritten. For example, if `app1=a` , `app1=b` , `app2=c` , and `app2=d` are used, only `app1=b` and `app2=d` will take effect.



Rule Description

By default, the container network policy is **Allow all inbound/outbound requests**. If you select **Reject all inbound requests**, the protected target will reject all connection requests. If you select **Reject all outbound requests**, the protected target will reject all initiated requests.

©2013-2022 Tencent Cloud. All rights reserved.

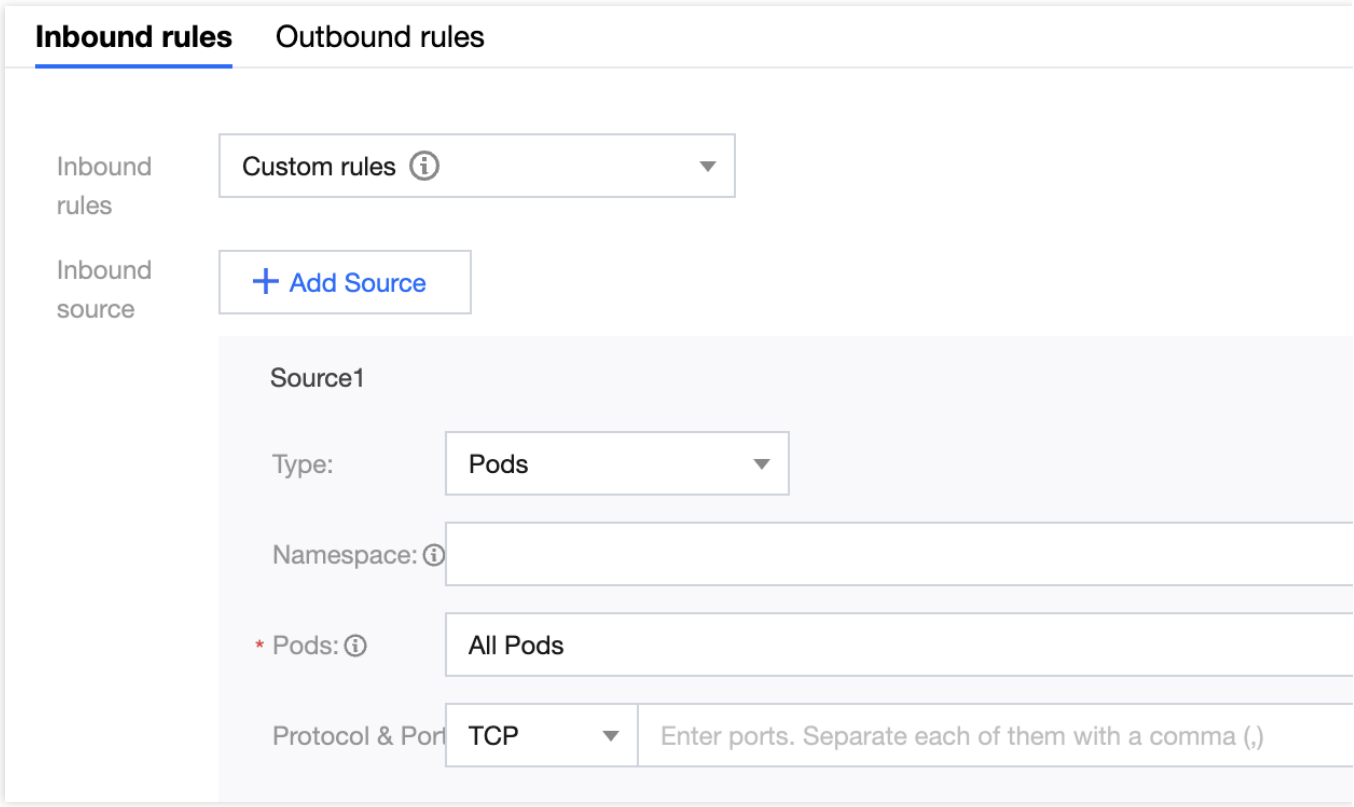


The rule takes effect about one minute after the container network policy is enabled. Usually, it takes only seconds to take effect.

After a custom inbound/outbound rule is configured and enabled in the policy, only requests meeting the rule will be allowed, and other requests will be rejected.

Custom rule description

When a custom rule is applied to the protected target, only requests from the specified sources or to the specified protocol port ranges will be allowed, while other requests will be rejected.



Type:

©2013-2022 Tencent Cloud. All rights reserved.

Pods: Specify the allowed Pod applications. The association is based on Pod labels, and a Pod is allowed when one of the label conditions is met. To specify the Pod label, you need to specify the namespace. If the namespace is left empty, the scope will be the current namespace (the namespace of the protected target).
Namespace: Specify the allowed namespace. The association is based on namespace labels, and a namespace is allowed when one of the label conditions is met.
IP: Specify the allowed IP range, which must be in the CIDR format and valid.
Protocol & Port: It can be used together with the above sources or target types. The protocol can be TCP or UDP, and the port is the Pod port number in the range of 1–65535. Separate ports by comma.
Note:
The configured protocol and port rules allow requests only through the specified port over the specified protocol. For example, "TCP 80" indicates to allow communication through port 80 over TCP, and communication over UDP is not affected.
You can add multiple allowed sources or targets to the custom rule, and the rule will be hit when any of them is matched.
Note:
If multiple labels are used to associate the Pod or namespace, when the key-value of a newly added label is the same as that of an existing one, only one key-value will take effect, and the label with the existing key-value will be overwritten. For example, if `app1=a` , `app1=b` , `app2=c` , and `app2=d` are used, only `app1=b` and `app2=d` will take effect.

Policy rule conflict

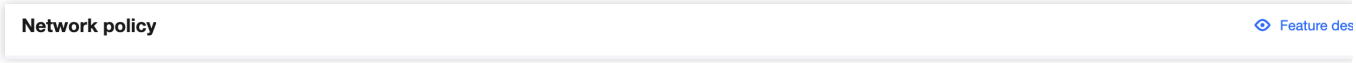
If the network policy rules for the same protected target conflict with each other, the Kubernetes NetworkPolicy conflict resolution principles will apply, for example:

Conflict Type	Sample Conflict	Sample Effect
Rule conflict for the same Pod	Rule A: The protected target is Pod 1 in namespace A, and the rule allows all inbound requests. Rule B: The protected target is Pod 1 in namespace A, and the rule rejects all inbound requests.	Pod 1 in namespace A allows all inbound requests.
Rule conflict for the Pod and namespace	Rule A: The protected target is namespace A (all Pods by default), and the rule allows all inbound requests. Rule B: The protected target is Pod 1 in namespace A, and the rule rejects all inbound requests.	Pod 1 in namespace A rejects all inbound requests, and other Pods in namespace A allow all inbound requests.
Rule conflict for the Pod and namespace	Rule A: The protected target is namespace A (all Pods by default), and the rule rejects all inbound requests. Rule B: The protected target is Pod 1 in namespace A, and the rule allows all inbound requests.	Pod 1 in namespace A allows all inbound requests, and other Pods in namespace A reject all inbound requests.

©2013-2022 Tencent Cloud. All rights reserved.

Policy Change Audit

On the **Network policy** page, click **Change history** in the top-right corner to view the change audit records of all policy rules. The audit operations include adding, enabling, disabling, editing, deleting, and confirming a policy.



References

For more information, see Use Cases.

©2013-2022 Tencent Cloud. All rights reserved.

Use Cases

Last updated：2024-01-23 15:44:44

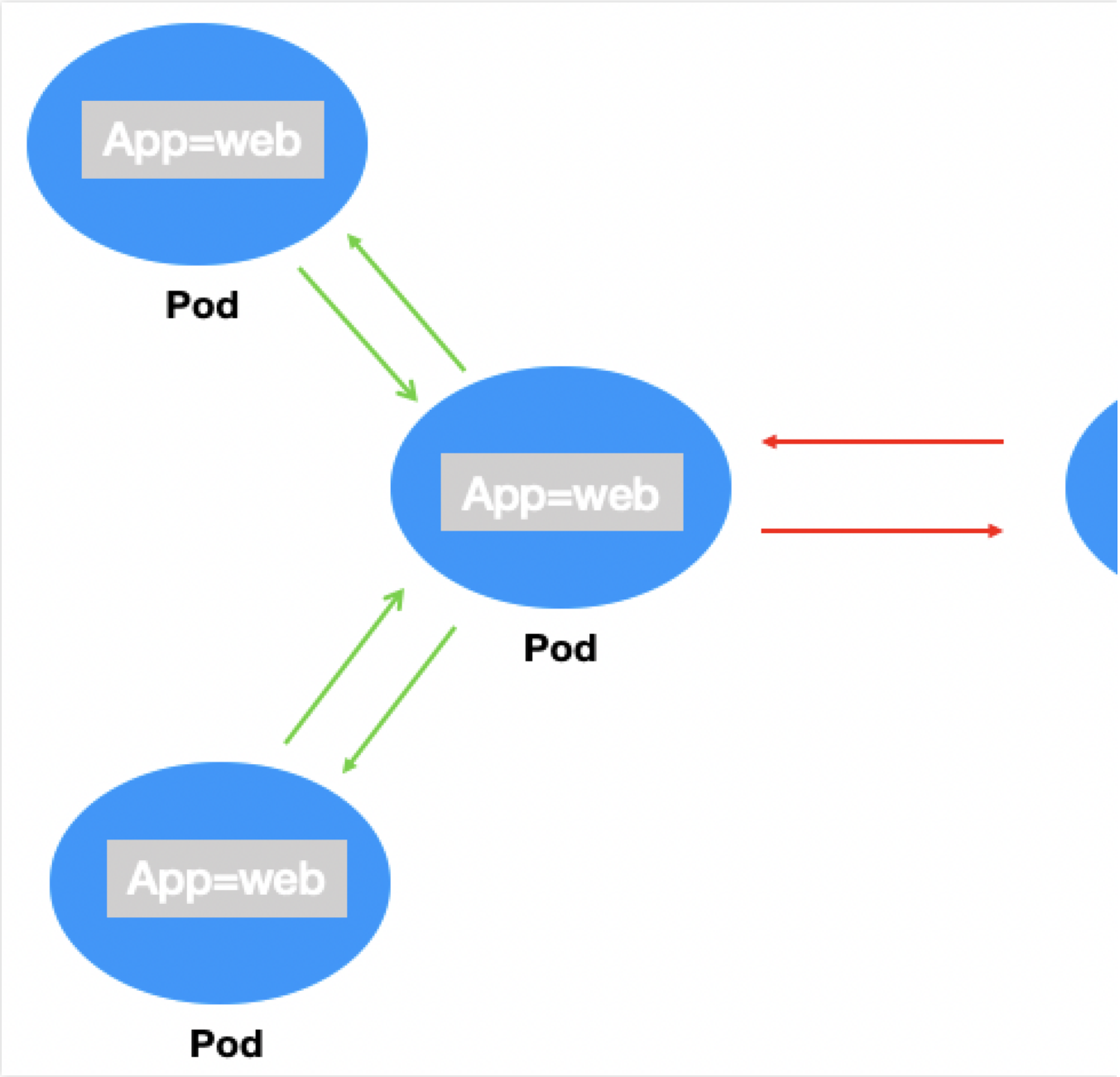
This document describes how to implement network isolation between containers in common scenarios based on container network policies.

Scenario 1. Set to allow requests only between specified Pods

Policy description

Set to allow requests only between Pod applications with the `app=web` label and reject requests from other Pods. This is commonly used to control the access between resources in a project.

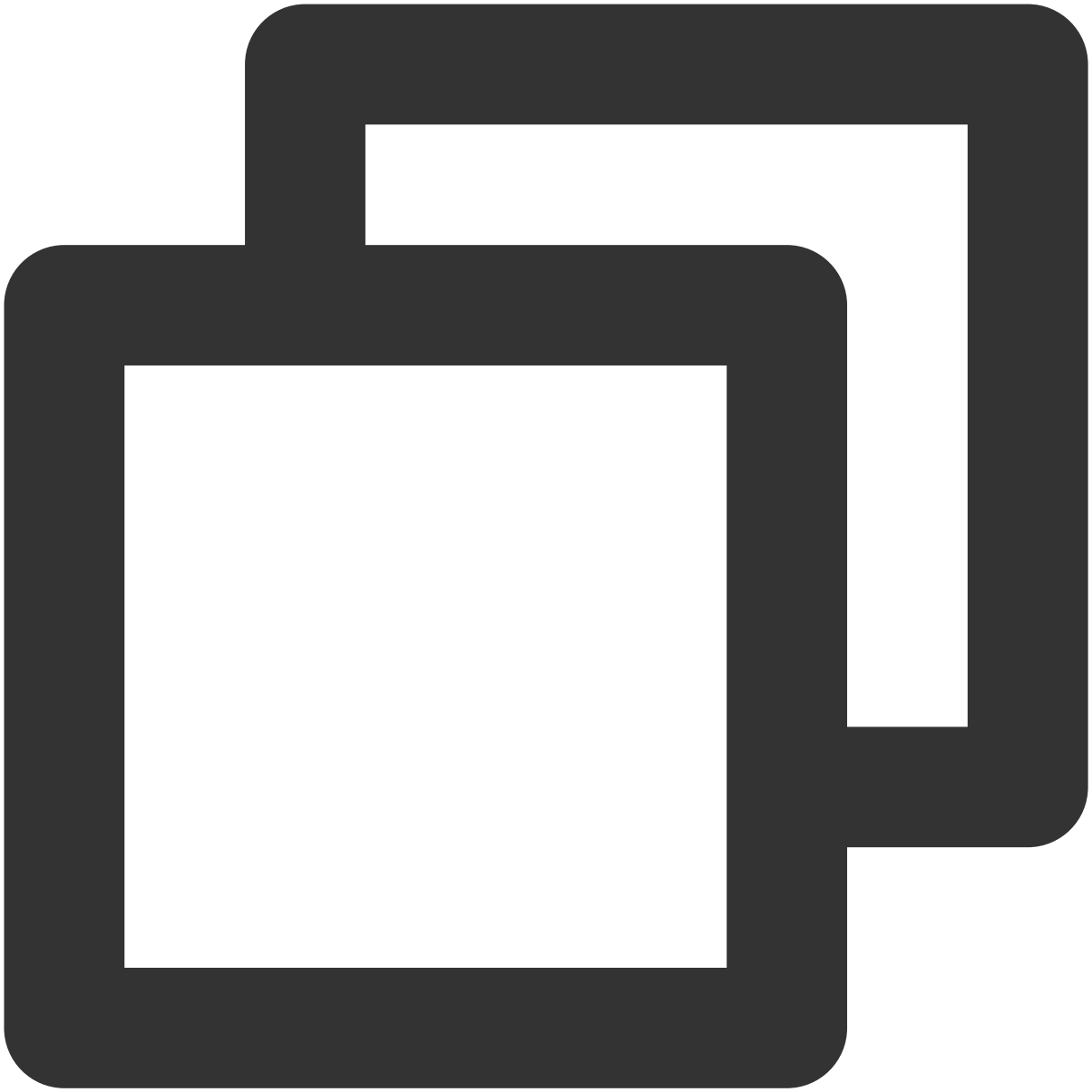
©2013-2022 Tencent Cloud. All rights reserved.



Verification steps

1. Create a Pod application with the `app=web` label and start the service.

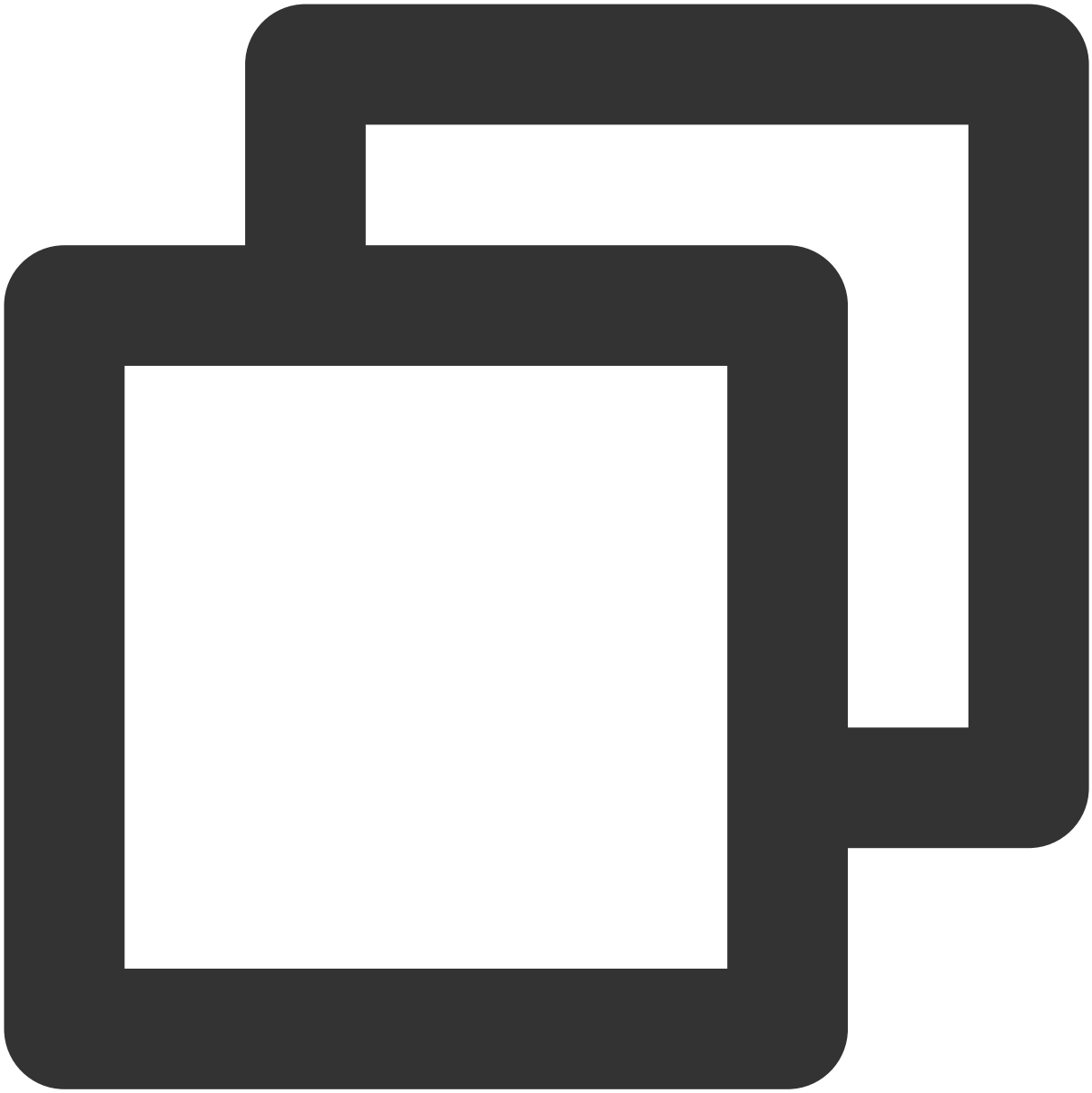
©2013-2022 Tencent Cloud. All rights reserved.



```
kubectl run --generator=run-pod/v1 apiserver --image=nginx --labels app=web --expos
```

Check whether the Pod is created successfully.

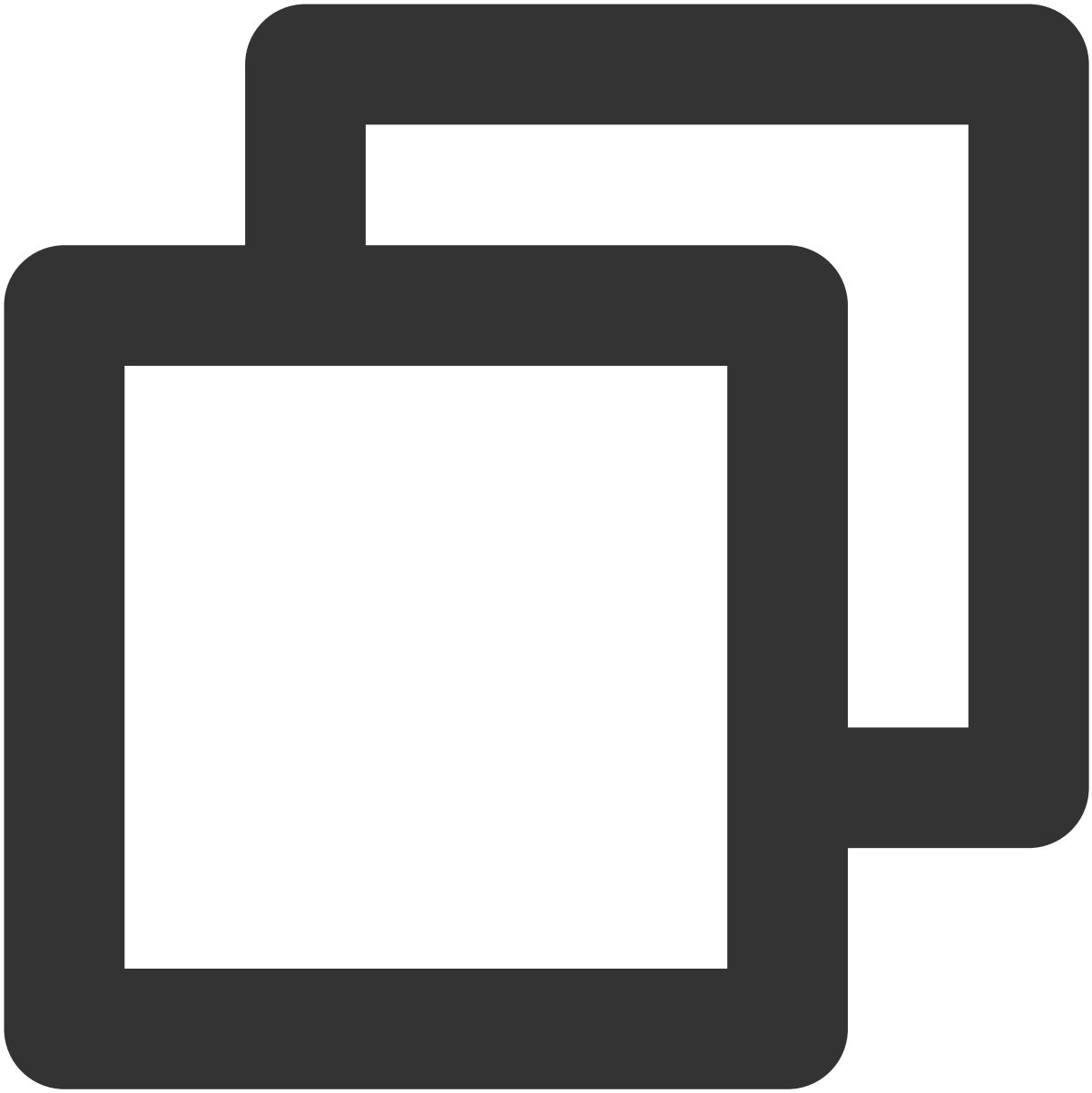
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl get pods web
NAME    READY    STATUS    RESTARTS    AGE
web     1/1      Running   0           4s
```

Check whether the svc is created successfully.

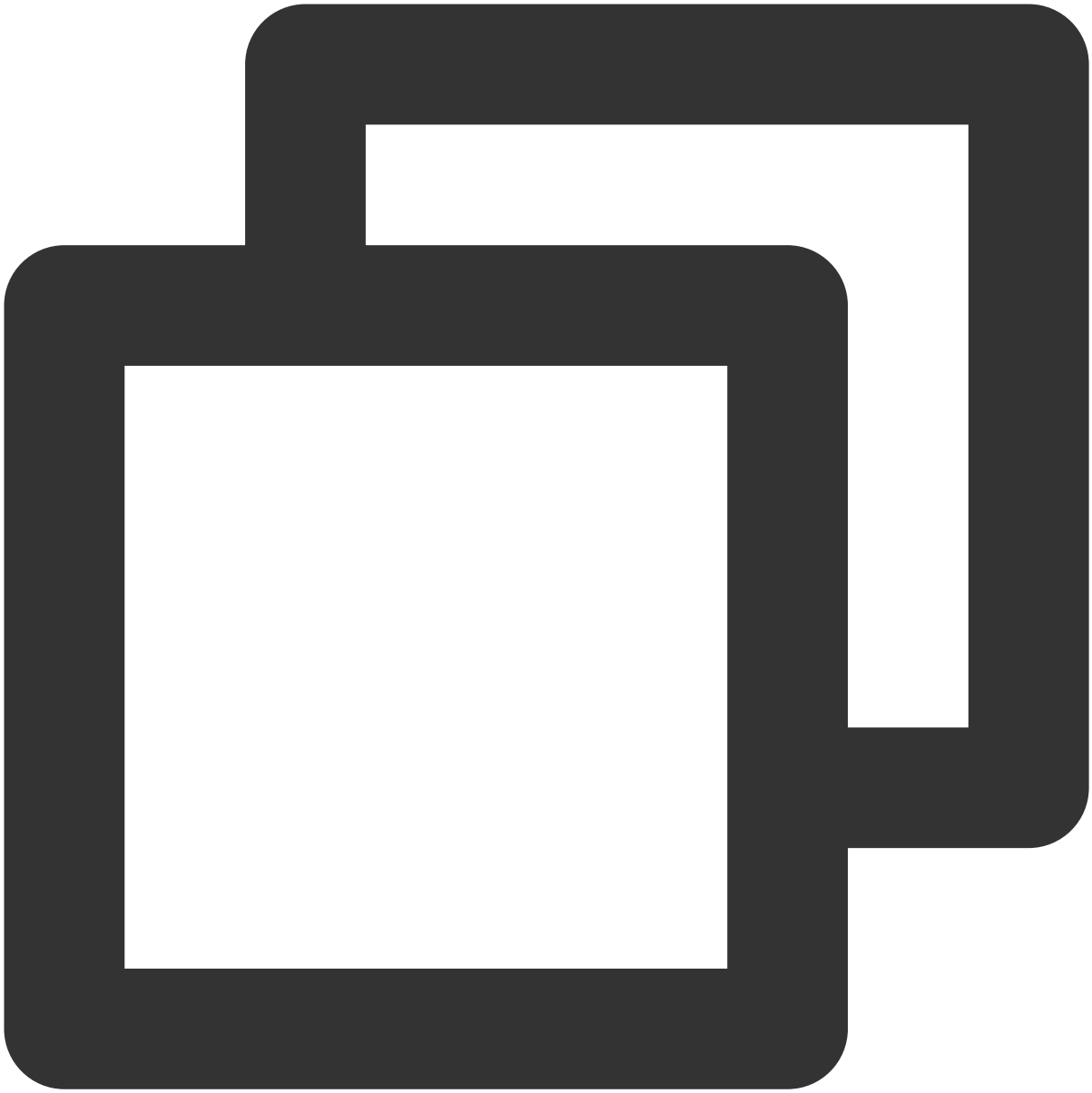
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl get svc web
NAME   TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)   AGE
web    ClusterIP   172.18.255.217   <none>        80/TCP    16s
```

2. Verify that the web service can be accessed from any source by default.

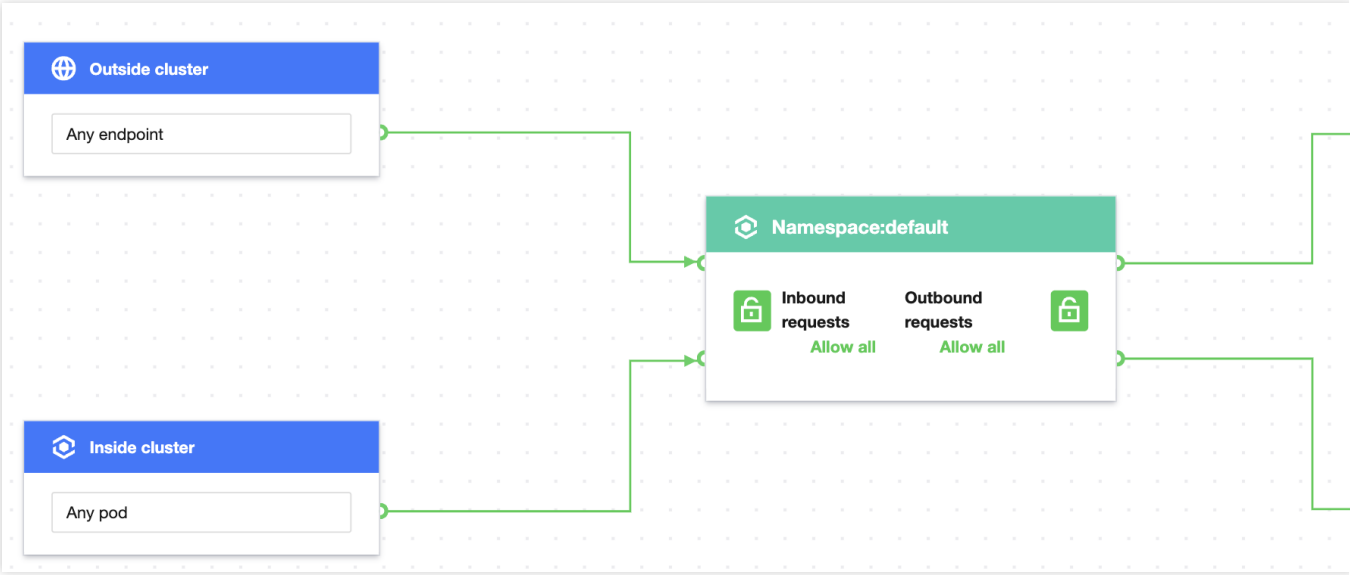
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl run --rm -it --image=alpine testweb
If you don't see a command prompt, try pressing enter.
/ # wget -qO- http://172.18.255.217
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

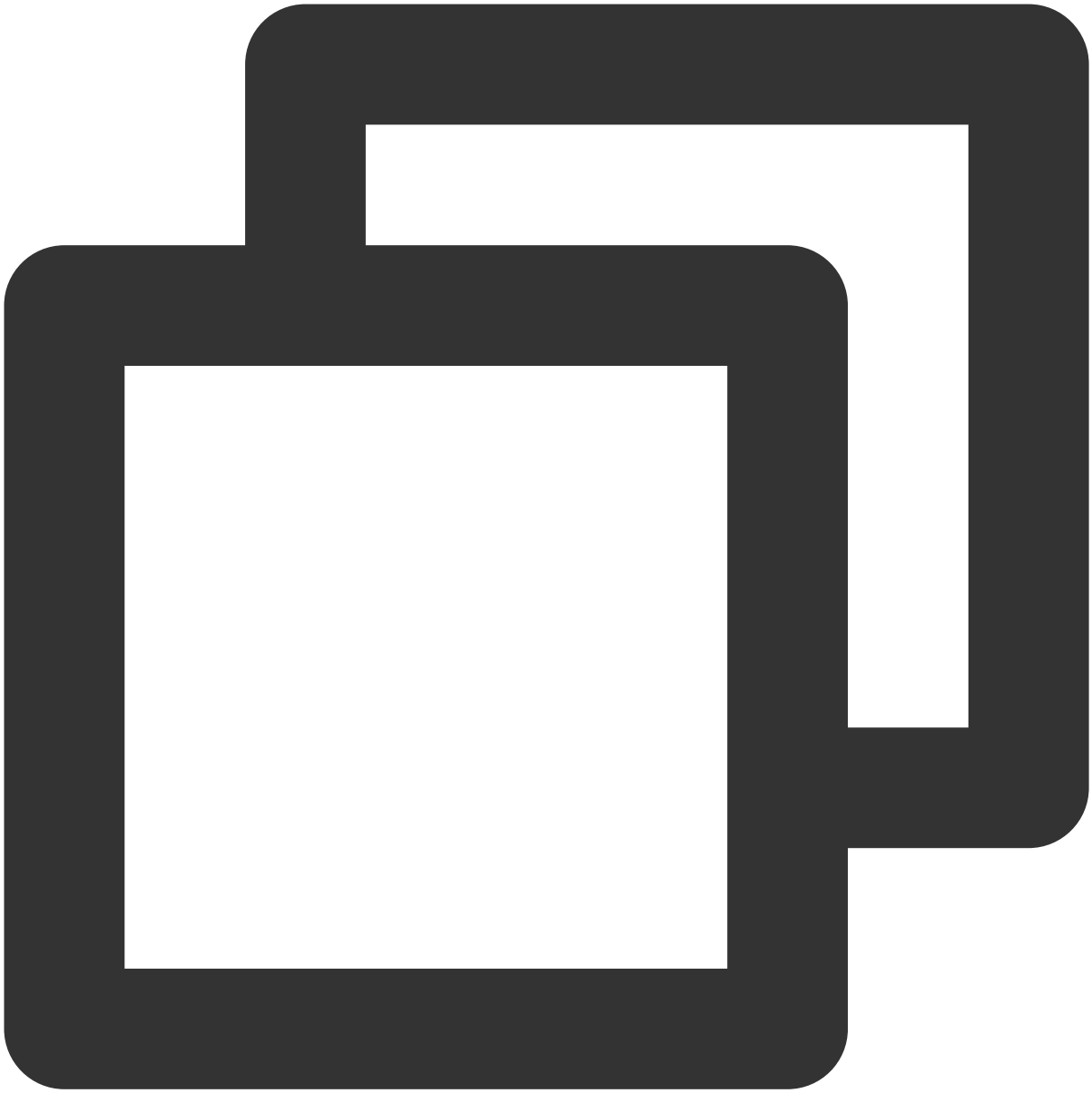
©2013-2022 Tencent Cloud. All rights reserved.

3. Create and enable the container network policy.
Set the label of the protected Pod as `app=web`, use custom inbound rules, configure the source type as the Pod, and specify the Pod with the `app=web` label as the allowed inbound source. The configuration is the same for outbound rules as shown below:



Note:
If no namespace is specified, the policy takes effect for the current namespace (default). In this case, requests from Pods in other namespaces will be rejected, even if their label is `app=web`.
4. Verify the effect of the network policy, i.e., only the Pod with the `app=web` label can access the web service.
The application with the `app=web` label in the current namespace can send requests to the web service.

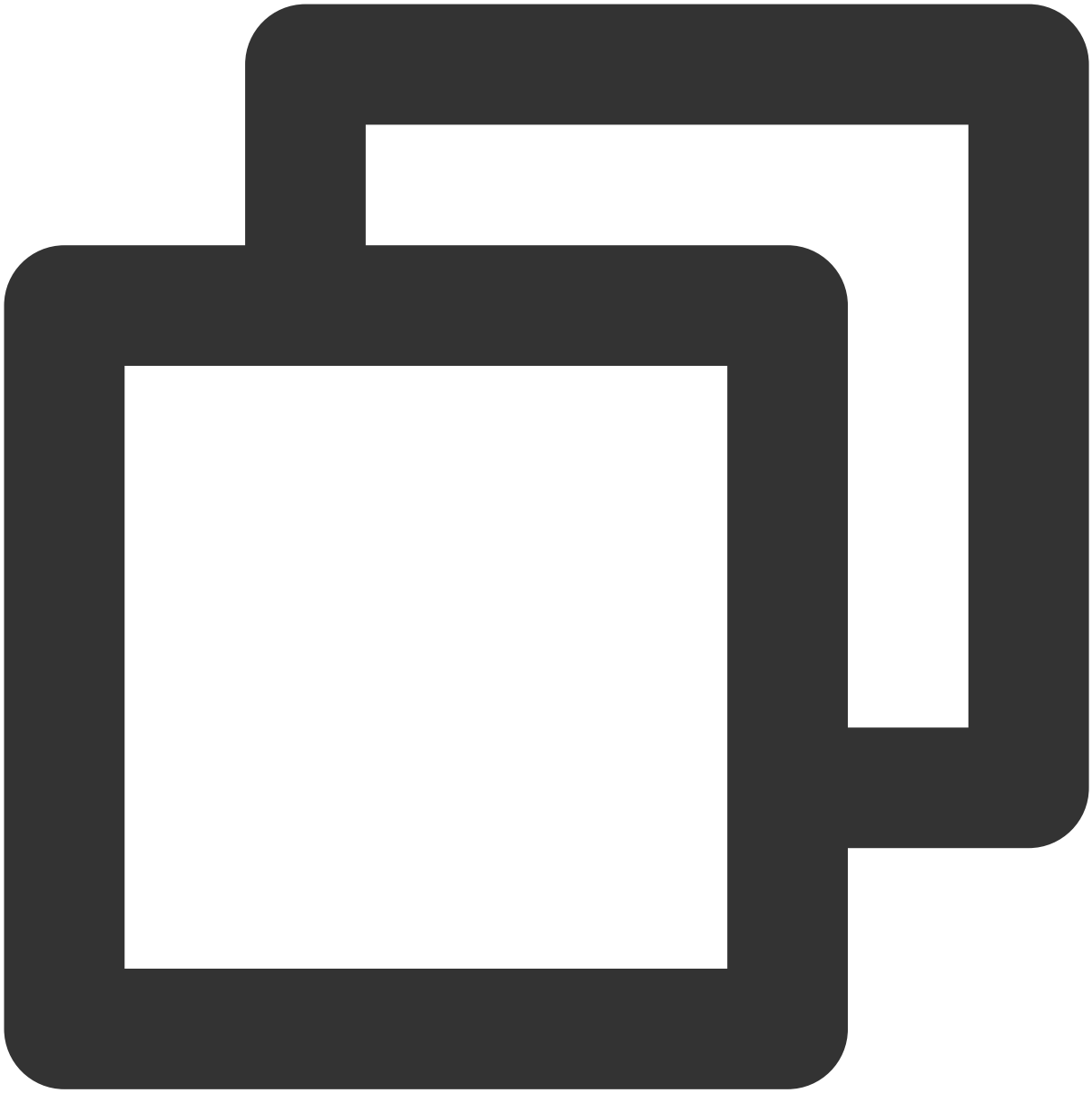
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl run --rm -it --image=alpine testweb --labels app=w
If you don't see a command prompt, try pressing enter.
/ # wget -qO- http://172.18.255.217
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

Applications without the `app=web` label in the current namespace cannot send requests to the web service.

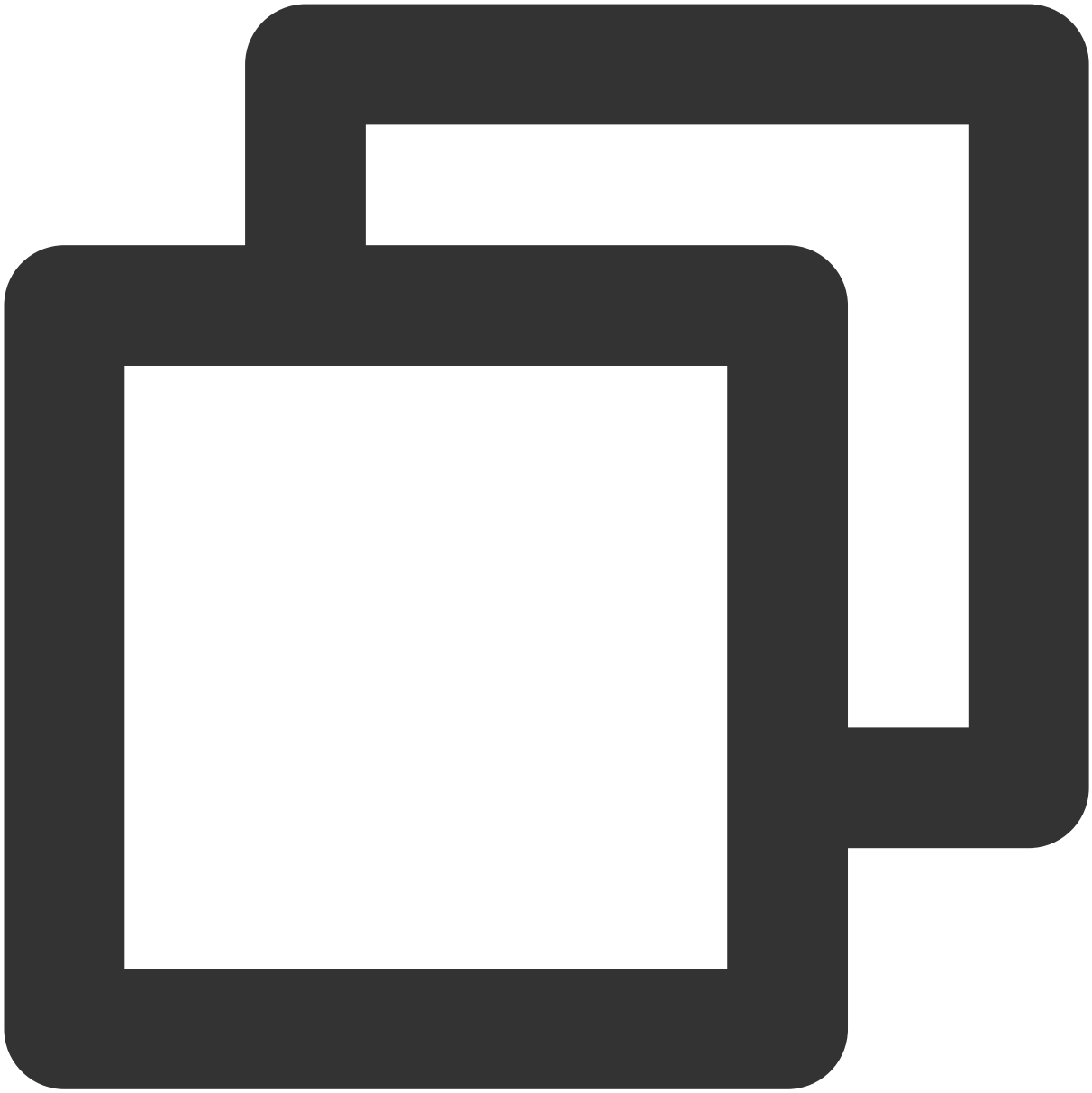
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl run --rm -it --image=alpine testweb --labels app2=
If you don't see a command prompt, try pressing enter.
/ # wget -qO- http://172.18.255.217
wget: can't connect to remote host (172.18.255.217): Connection refused
```

Applications with the `app=web` label in other namespaces can send requests to the web service.

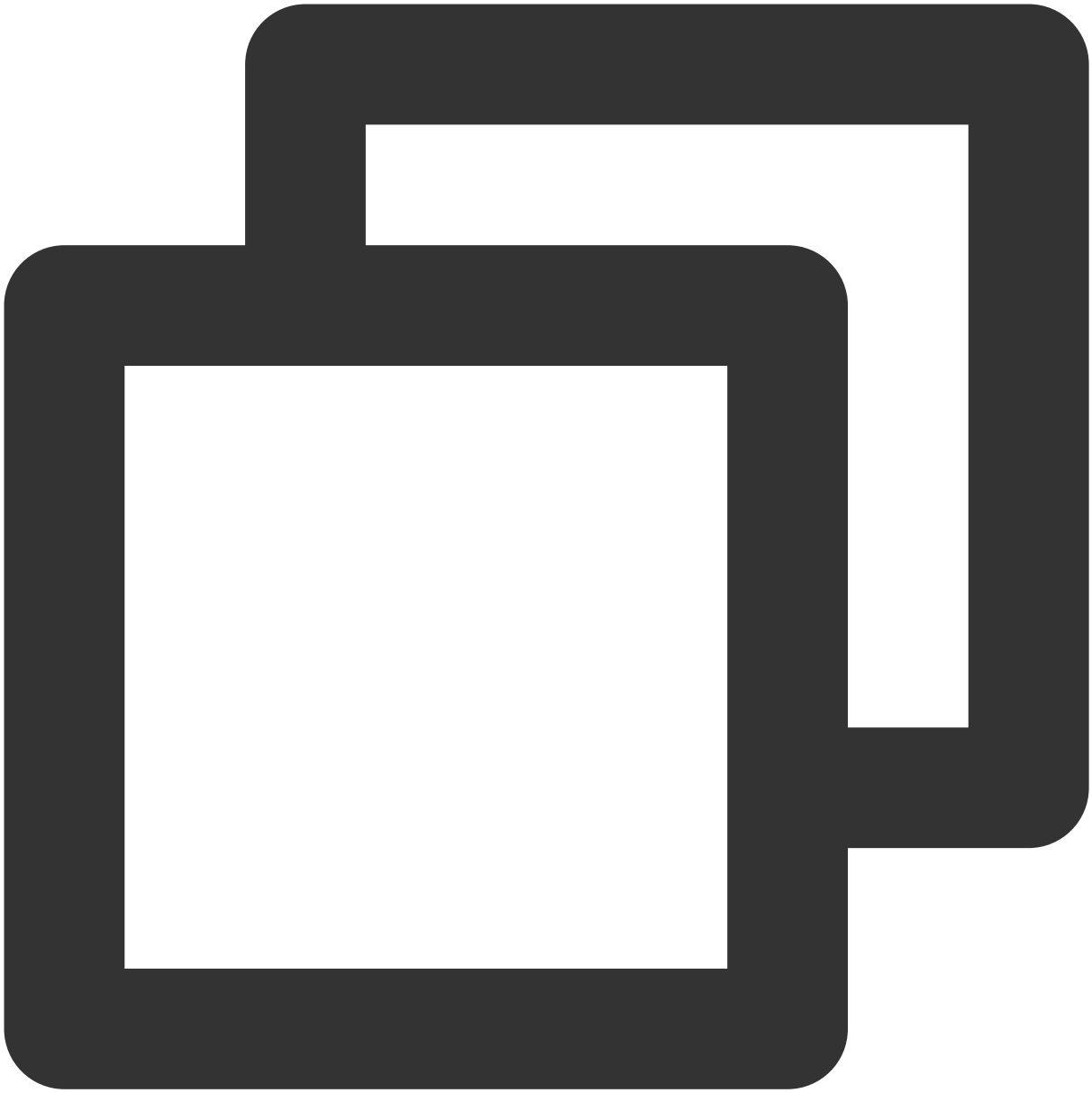
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl run --rm -it --image=alpine testweb --labels app=w
If you don't see a command prompt, try pressing enter.
/ # wget -qO- http://172.18.255.217
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

5. Clear the environment.

©2013-2022 Tencent Cloud. All rights reserved.



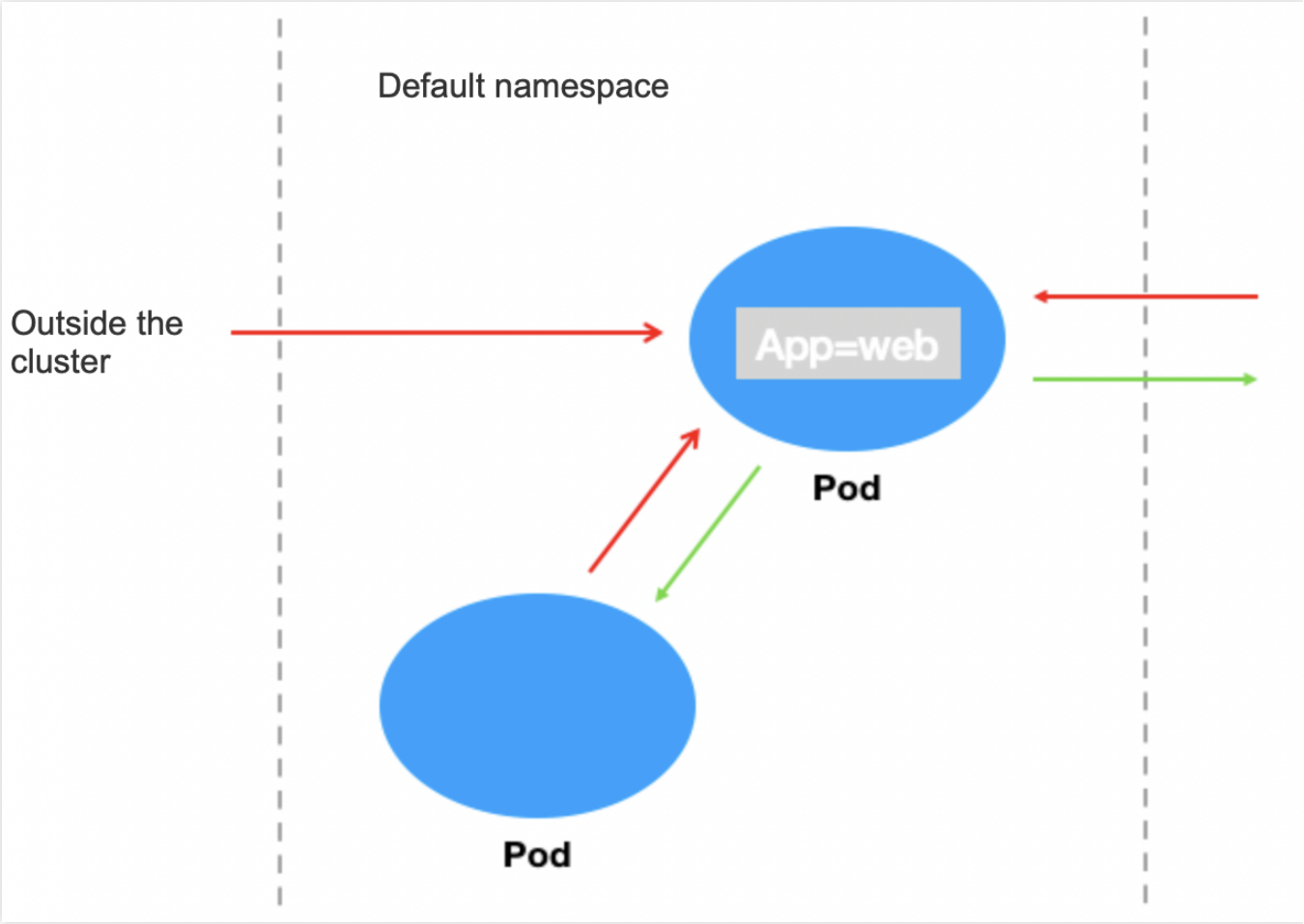
```
kubectl delete pod web
kubectl delete service web
Disable the network policy in the console// (This can also be done by running `kube
```

Scenario 2. Set to reject inbound requests to a Pod application

Policy description

©2013-2022 Tencent Cloud. All rights reserved.

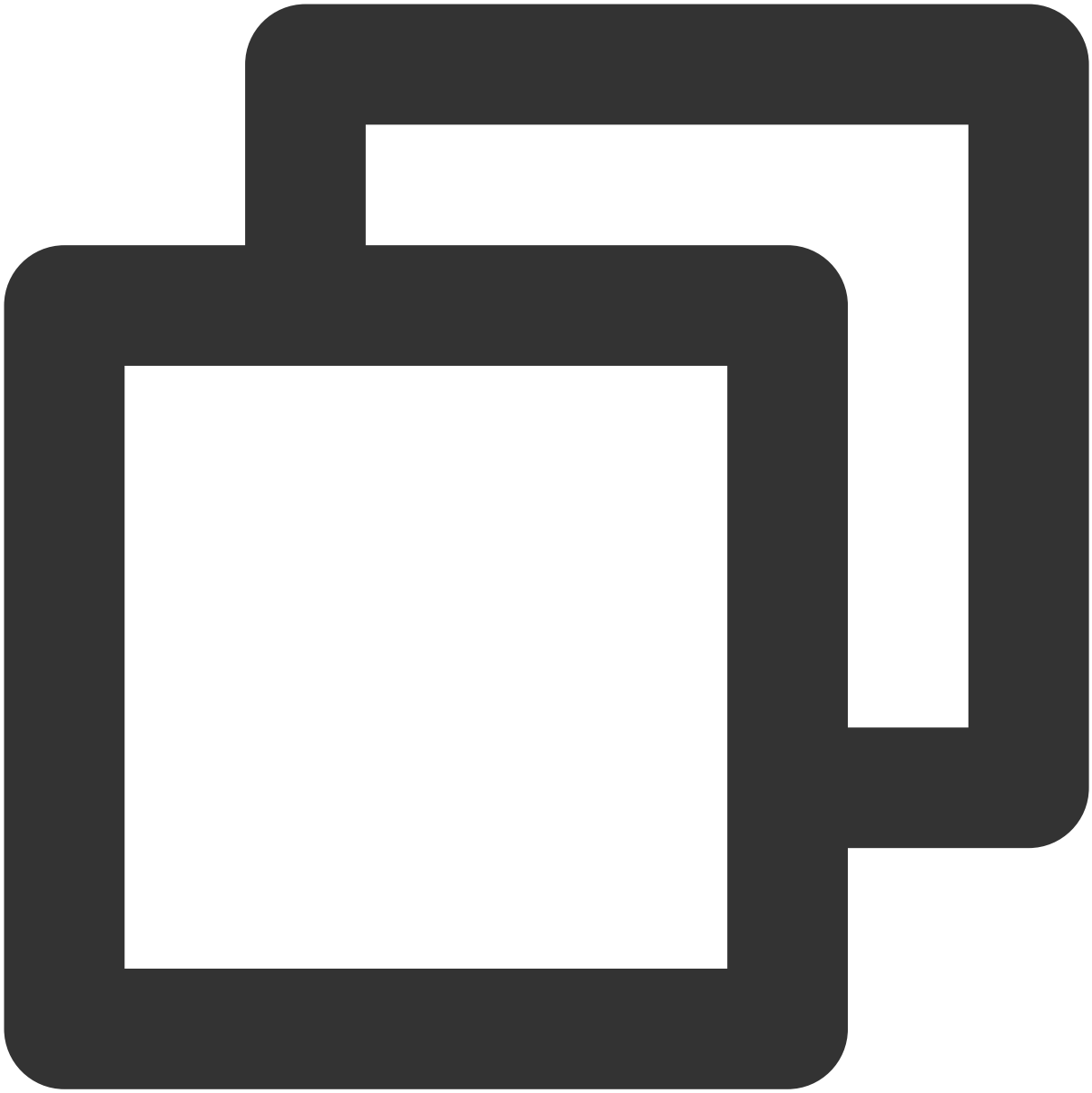
Set to reject inbound requests to the Pod with the `app=web` label. This doesn't affect outbound requests.



Verification steps

1. Create a Pod application with the `app=web` label and start the service.

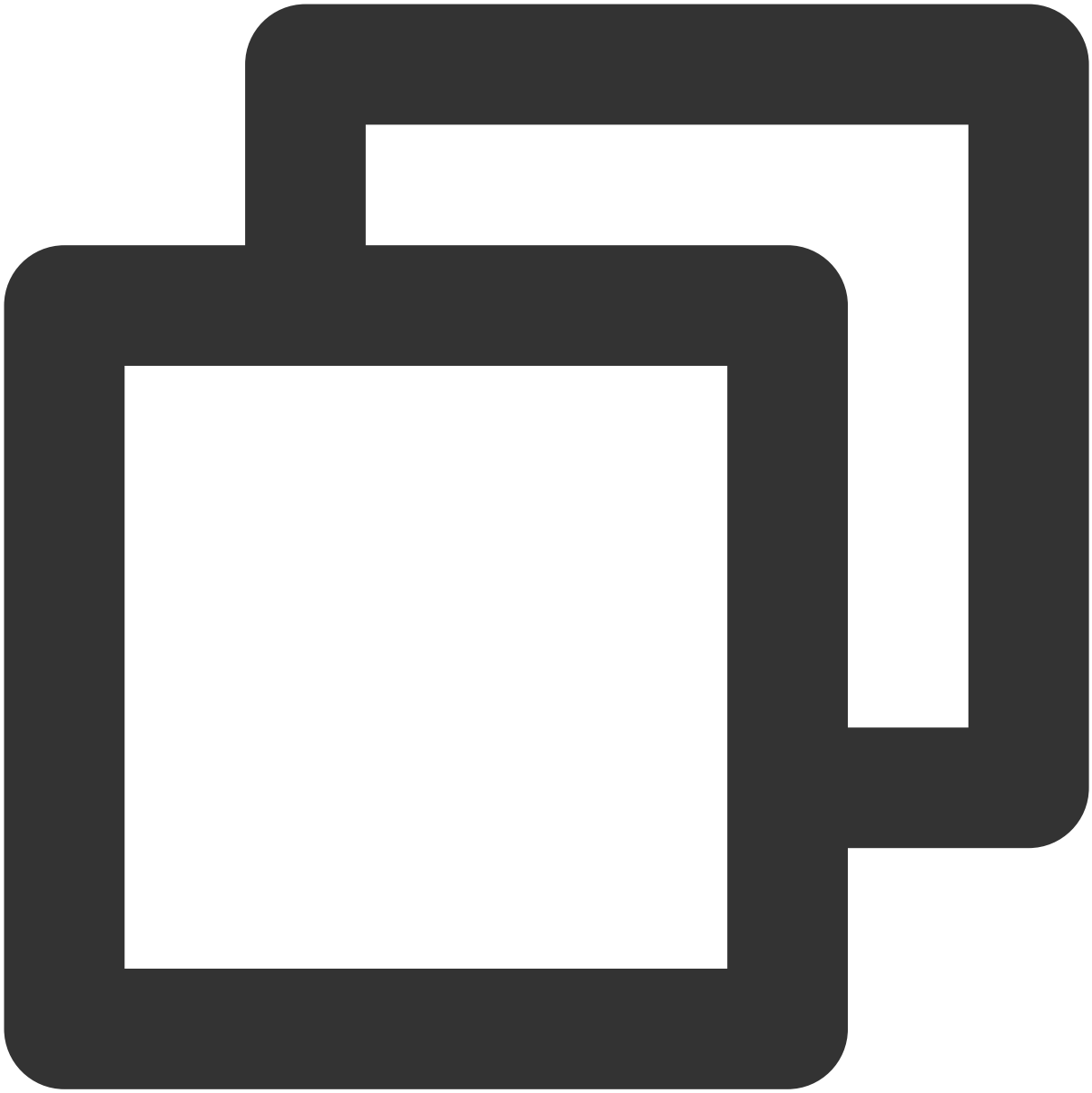
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl run web --image=nginx --labels app=web --expose --
service/web created
pod/web created
[root@VM-0-11-centos ~]# kubectl get pods web
NAME   READY   STATUS    RESTARTS   AGE
web    1/1     Running   0          4s
[root@VM-0-11-centos ~]# kubectl get svc web
NAME   TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)   AGE
web    ClusterIP   172.18.255.217   <none>        80/TCP    16s
```

2. Verify that the web service can be accessed from any sources by default.

©2013-2022 Tencent Cloud. All rights reserved.

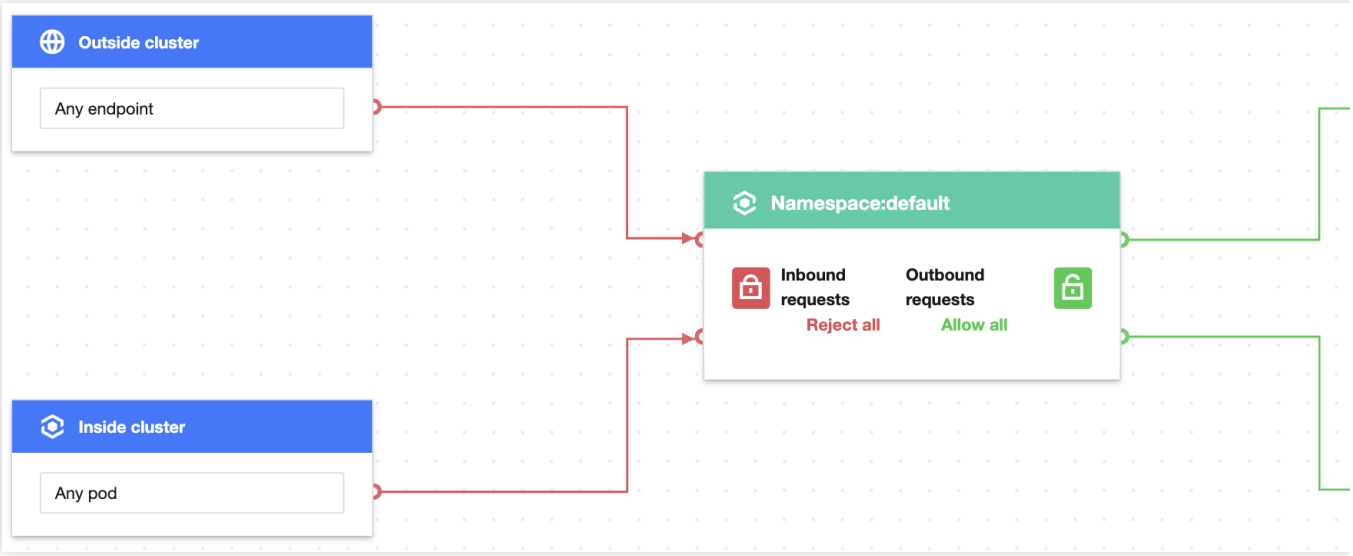


```
[root@VM-0-11-centos ~]# kubectl run --rm -it --image=alpine testweb
If you don't see a command prompt, try pressing enter.
/ # wget -qO- http://172.18.255.217
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

©2013-2022 Tencent Cloud. All rights reserved.

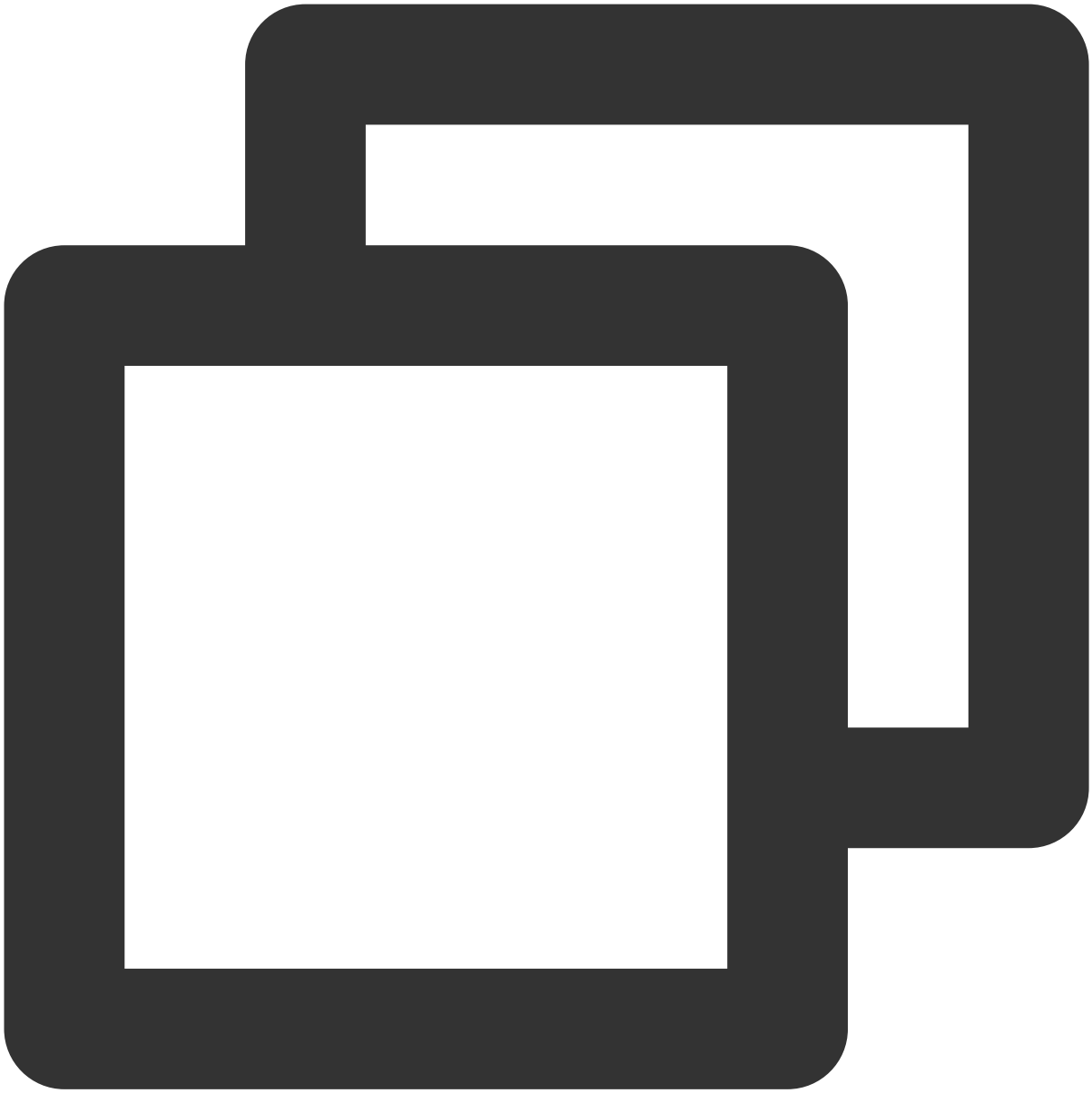
3. Create and enable the container network policy.

Set the label of the protected Pod as `app=web` and set to reject all inbound requests as shown below:



4. Verify the effect of the network policy, i.e., the application with the `app=web` label cannot be accessed from any external sources.

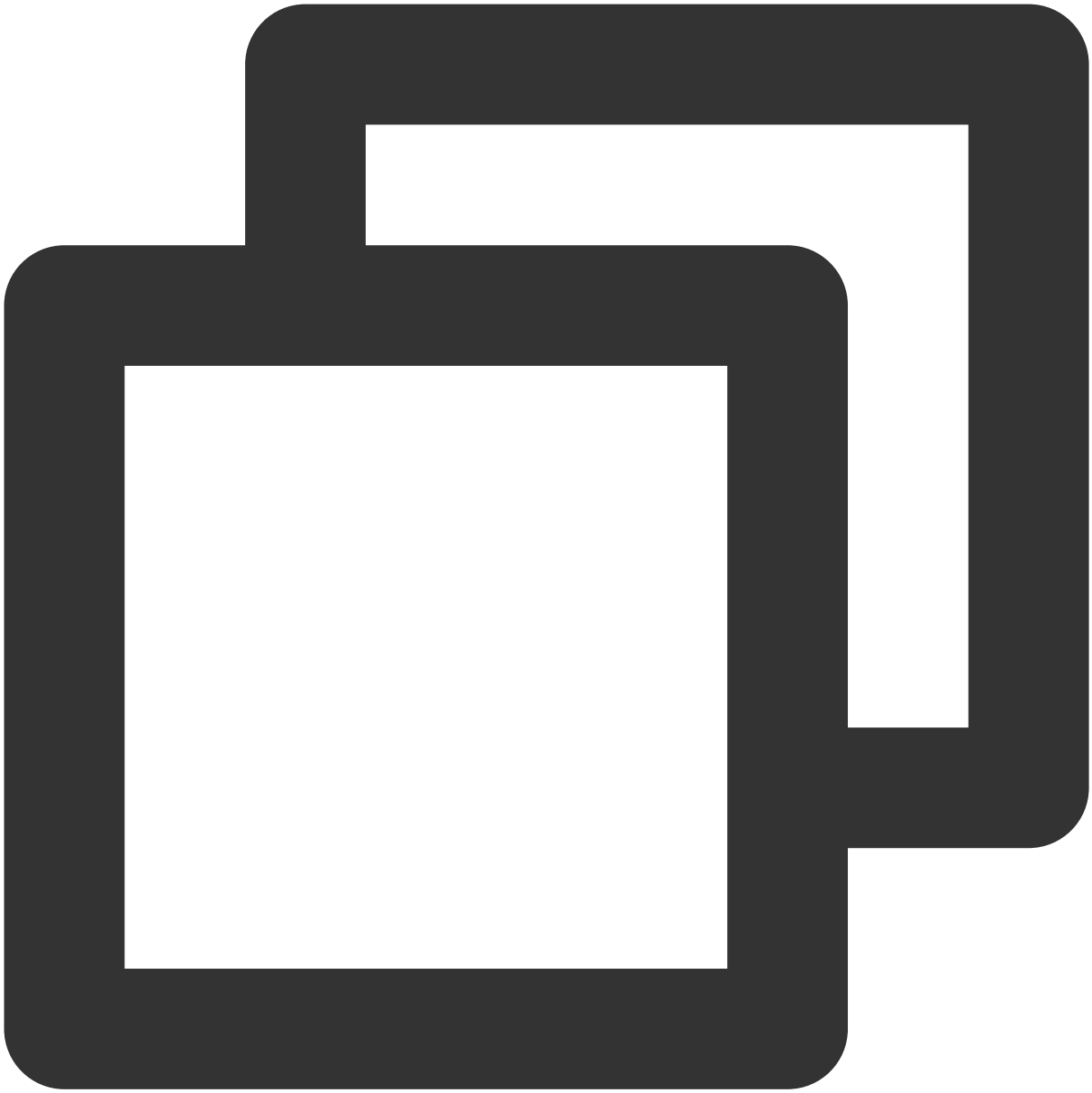
©2013-2022 Tencent Cloud. All rights reserved.



```
kubectl run --rm -i -t --image=alpine testweb -- sh
If you don't see a command prompt, try pressing enter.
/ # wget -qO- --timeout=2 http://web
wget: can't connect to remote host (172.18.255.217): Connection refused
```

5. Clear the environment.

©2013-2022 Tencent Cloud. All rights reserved.



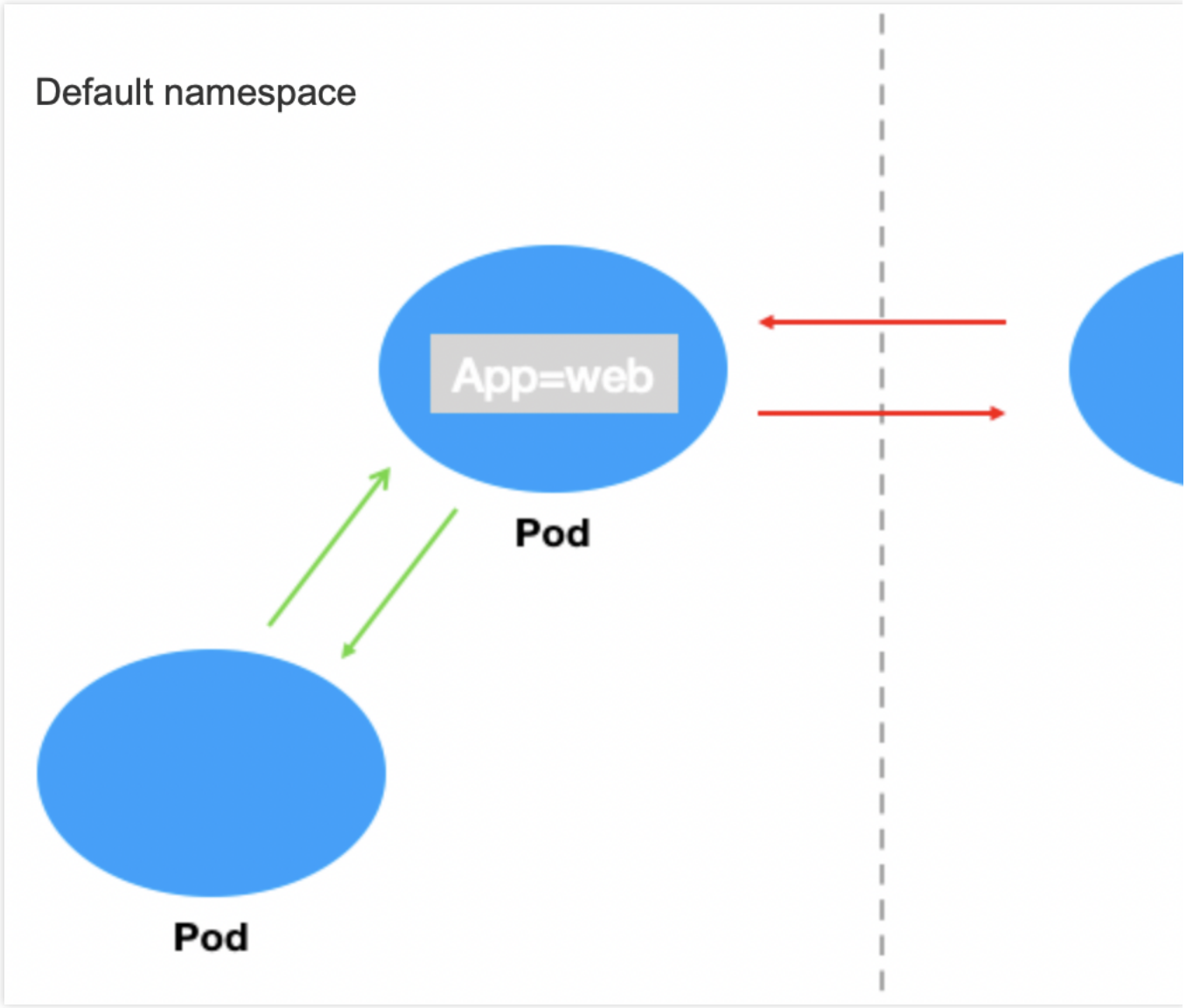
```
kubectl delete pod web
kubectl delete service web
Disable the network policy in the console// (This can also be done by running `kube
```

Scenario 3. Set to reject requests from other namespaces

Policy description

©2013-2022 Tencent Cloud. All rights reserved.

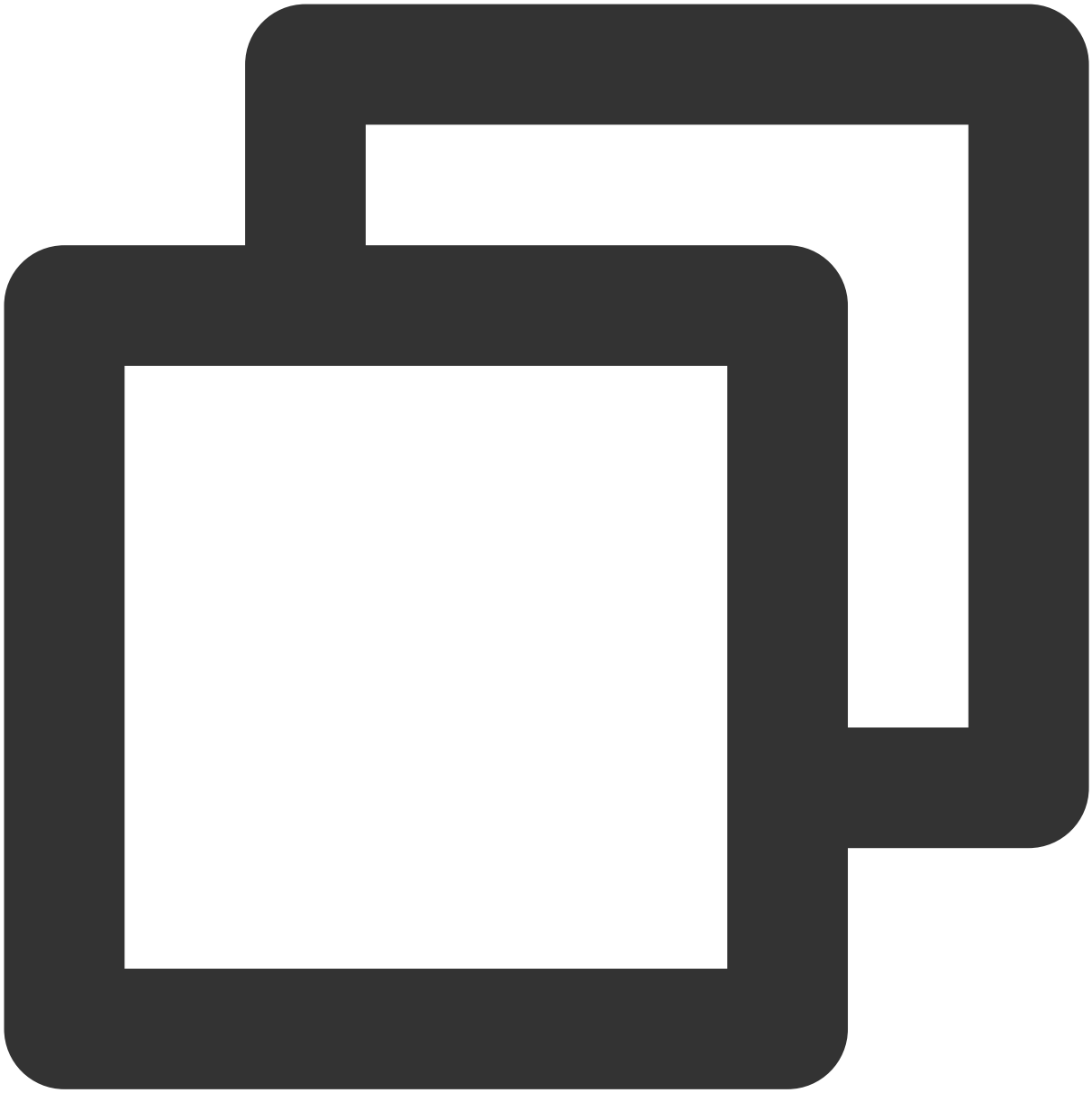
Set to reject requests from other namespaces to the applications with the `app=web` label and allow requests only from the current namespace as shown below:



Verification steps

1. Create a Pod application with the `app=web` label and start the service.

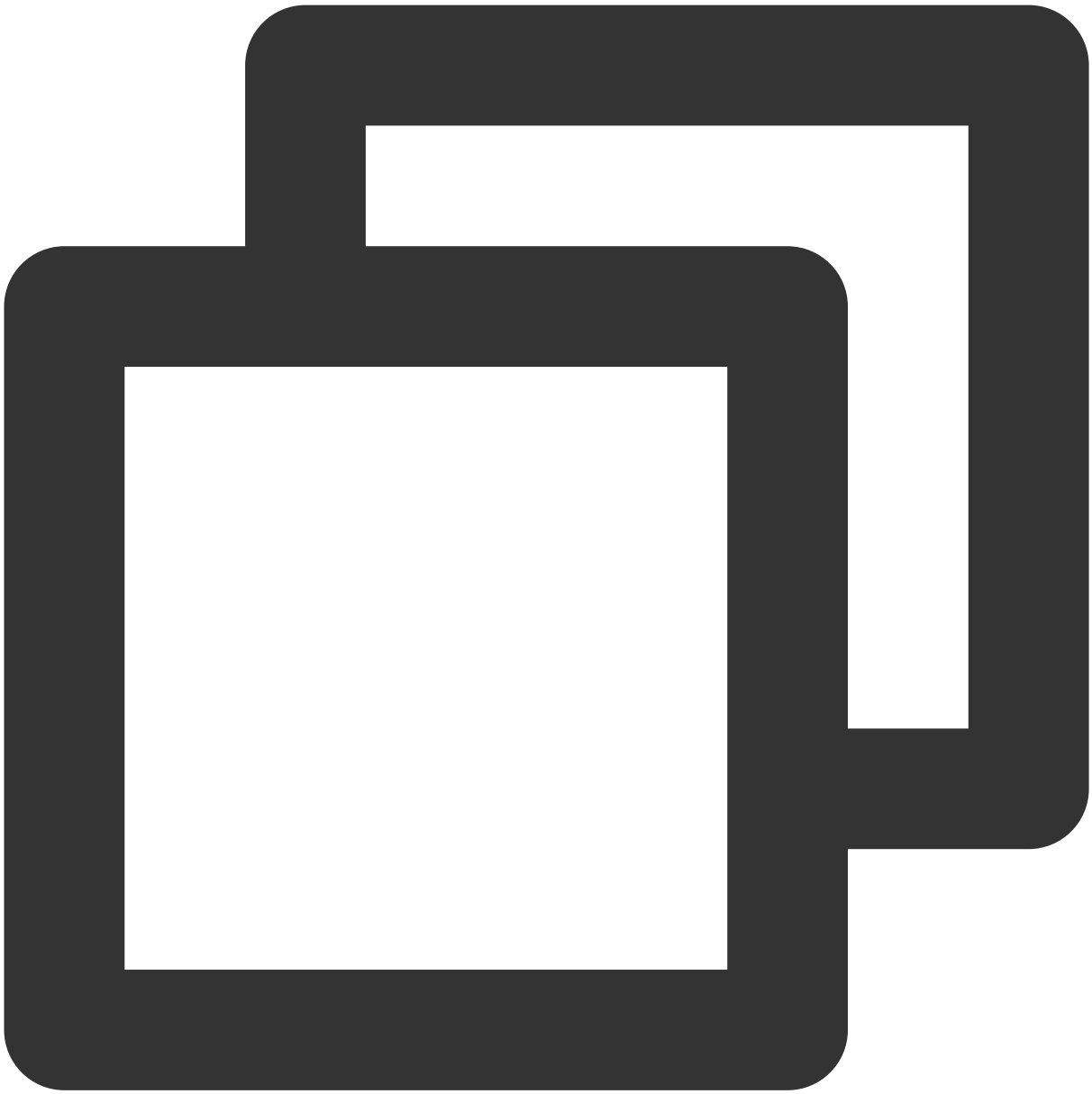
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl run web --image=nginx --labels app=web --expose --
service/web created
pod/web created
[root@VM-0-11-centos ~]# kubectl get pods web
NAME   READY   STATUS    RESTARTS   AGE
web    1/1     Running   0          5s
[root@VM-0-11-centos ~]# kubectl get svc web
NAME   TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)   AGE
web    ClusterIP   172.18.255.217   <none>        80/TCP    13s
```

©2013-2022 Tencent Cloud. All rights reserved.

2. Verify that requests can be sent from other namespaces to the application with the `app=web` label by default.

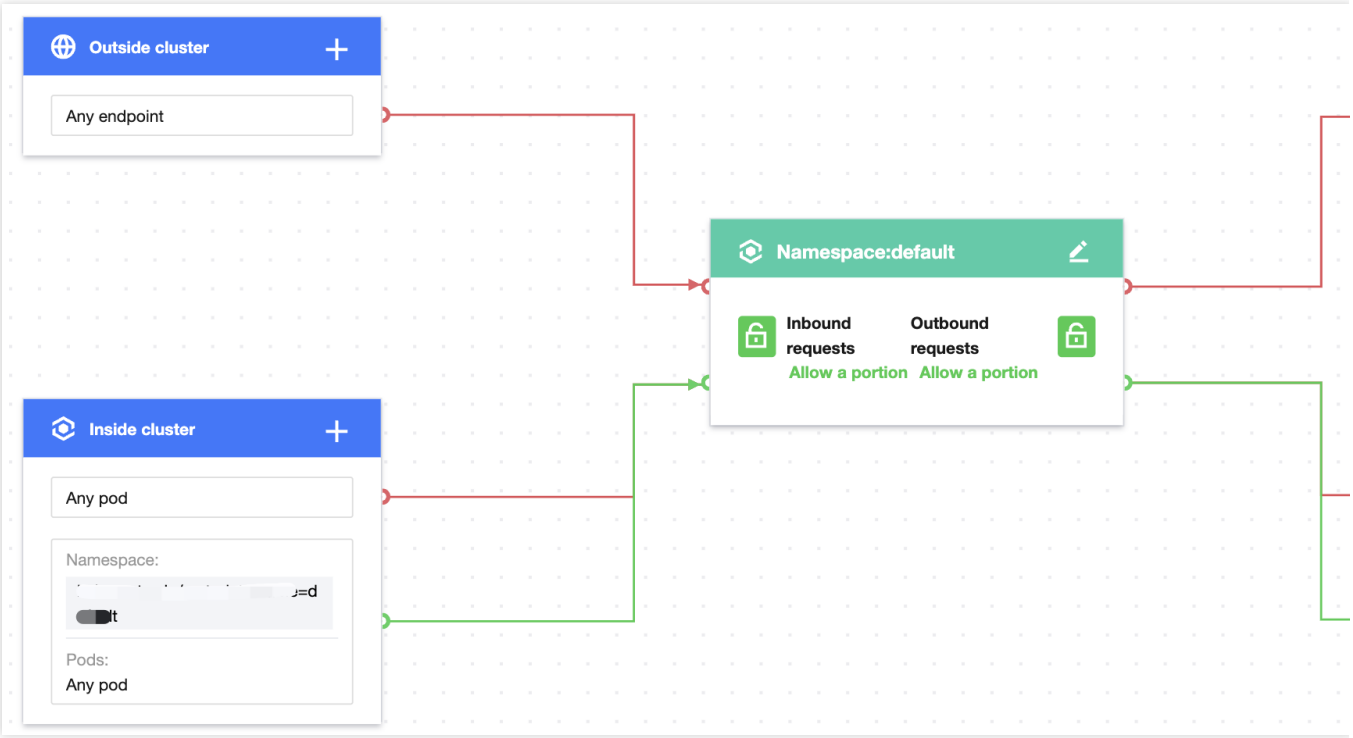


```
[root@VM-0-11-centos ~]# kubectl run --rm -it --image=alpine testweb --labels app=w
If you don't see a command prompt, try pressing enter.
/ # wget -qO- http://172.18.255.217
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

©2013-2022 Tencent Cloud. All rights reserved.

3. Create and enable the container network policy.

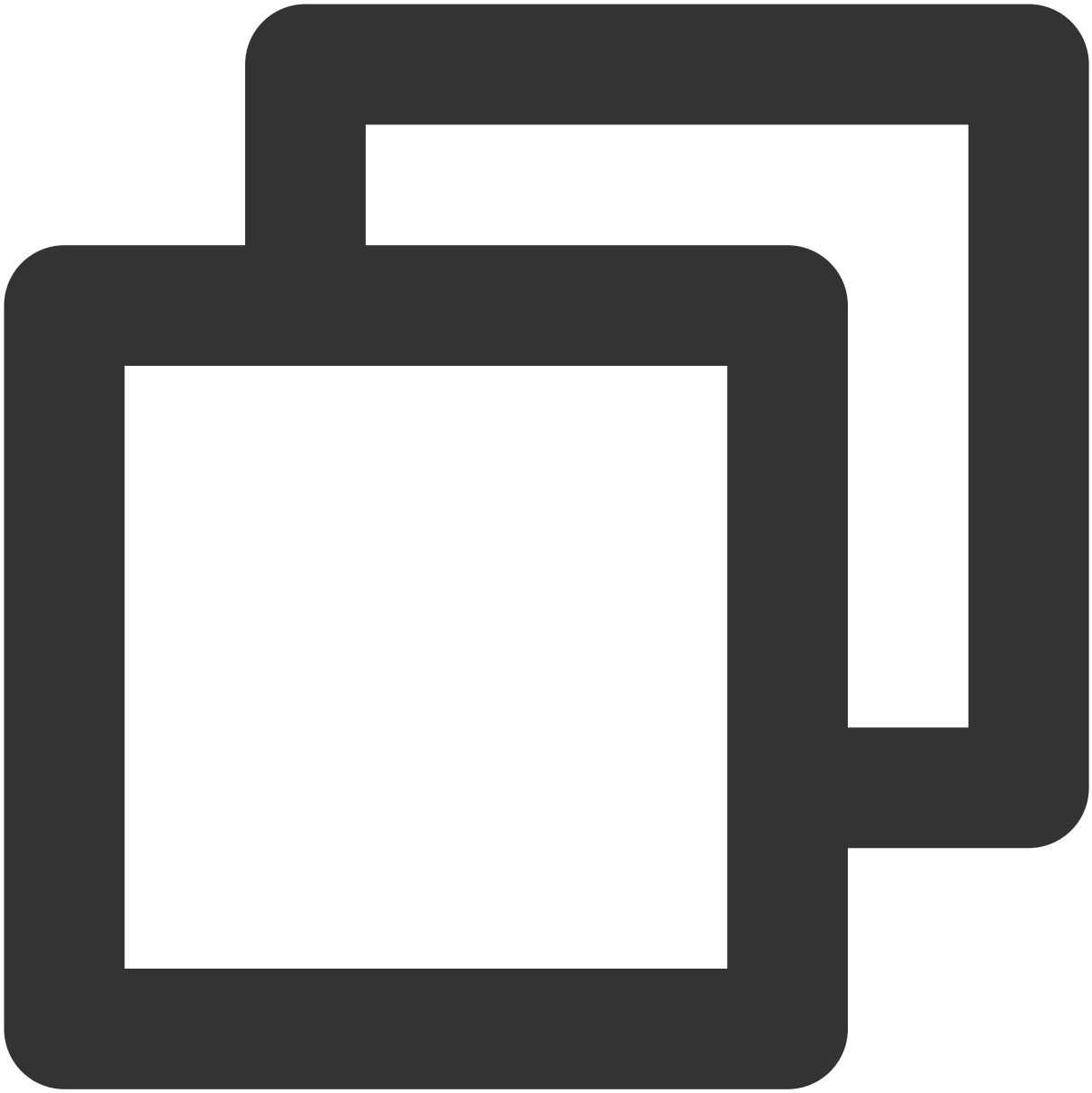
Set the label of the protected Pod as `app=web` , use custom inbound rules, configure the source type as the Pod, leave the namespace empty, and specify any Pod as the allowed inbound source. The configuration is the same for outbound rules as shown below:



4. Verify the effect of the network policy.

The Pod with the `app=web` label can be accessed from the current namespace.

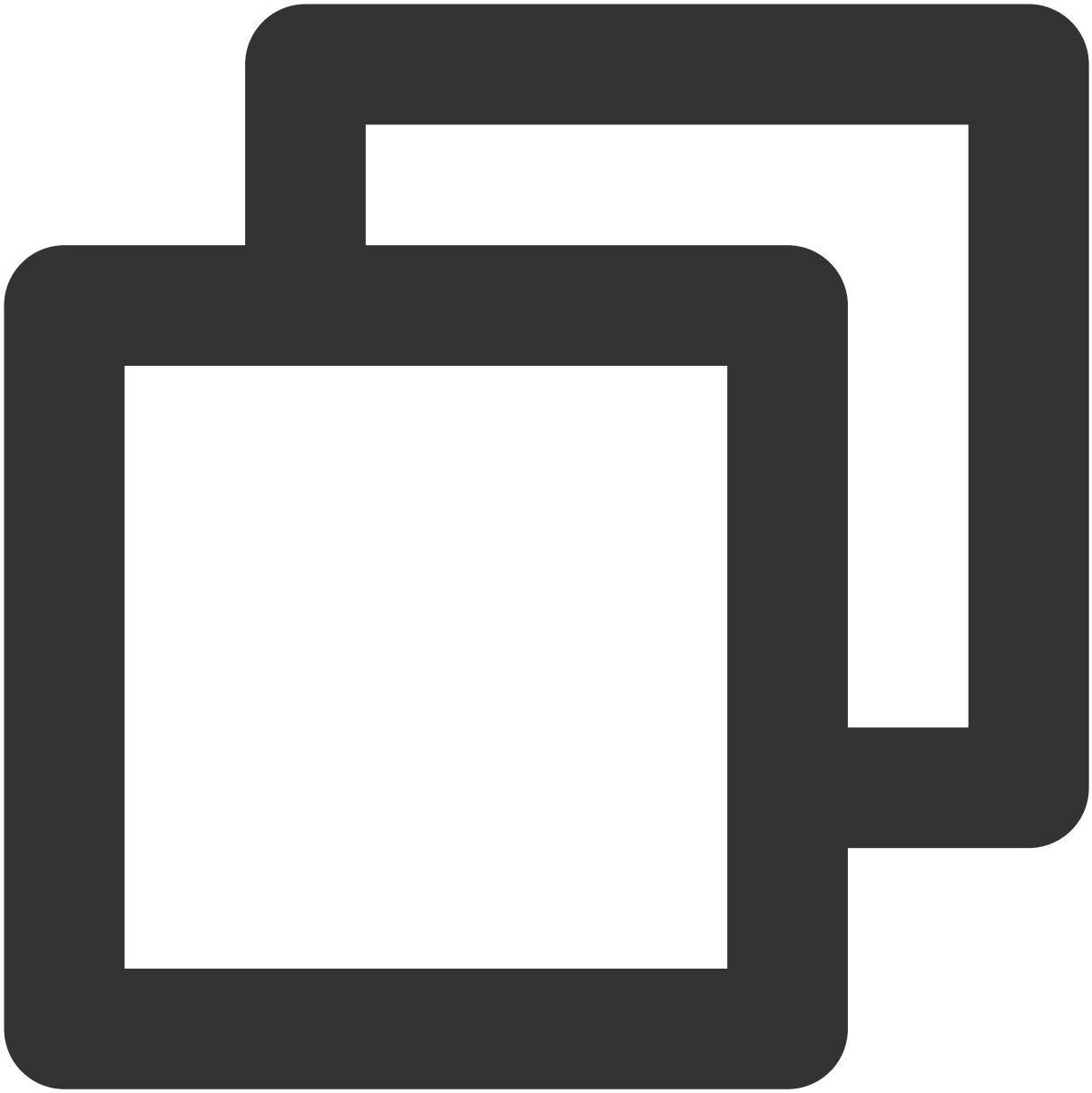
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl run testweb --namespace=default --rm -it --image=a
If you don't see a command prompt, try pressing enter.
/ # wget -qO- --timeout=2 http://web.default
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

The Pod with the `app=web` label cannot be accessed from other namespaces.

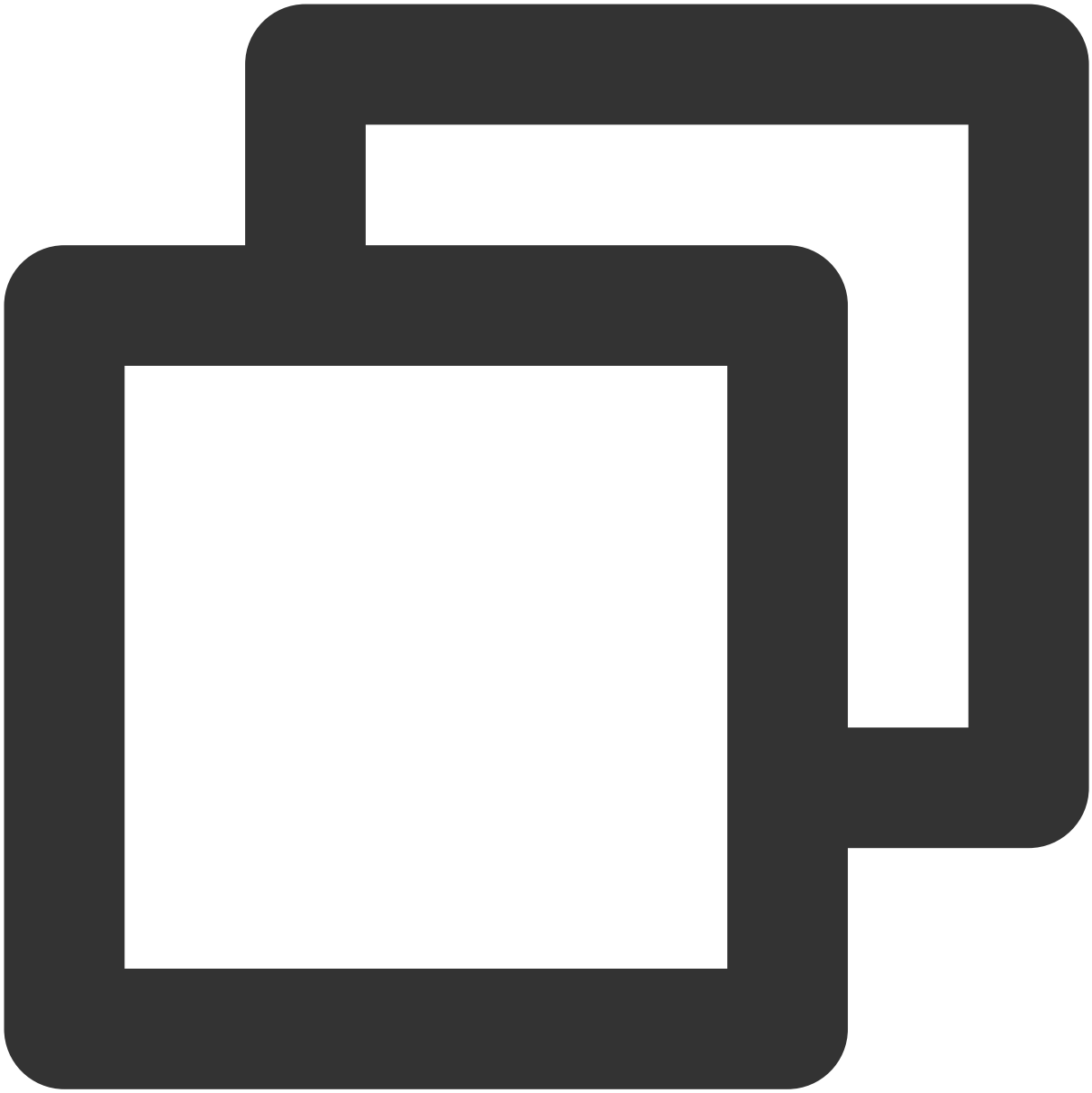
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl run --rm -it --image=alpine testweb --labels app=w
If you don't see a command prompt, try pressing enter.
/ # wget -qO- --timeout=2 http://web.default
wget: can't connect to remote host (172.18.255.217): Connection refused
```

5. Clear the environment.

©2013-2022 Tencent Cloud. All rights reserved.



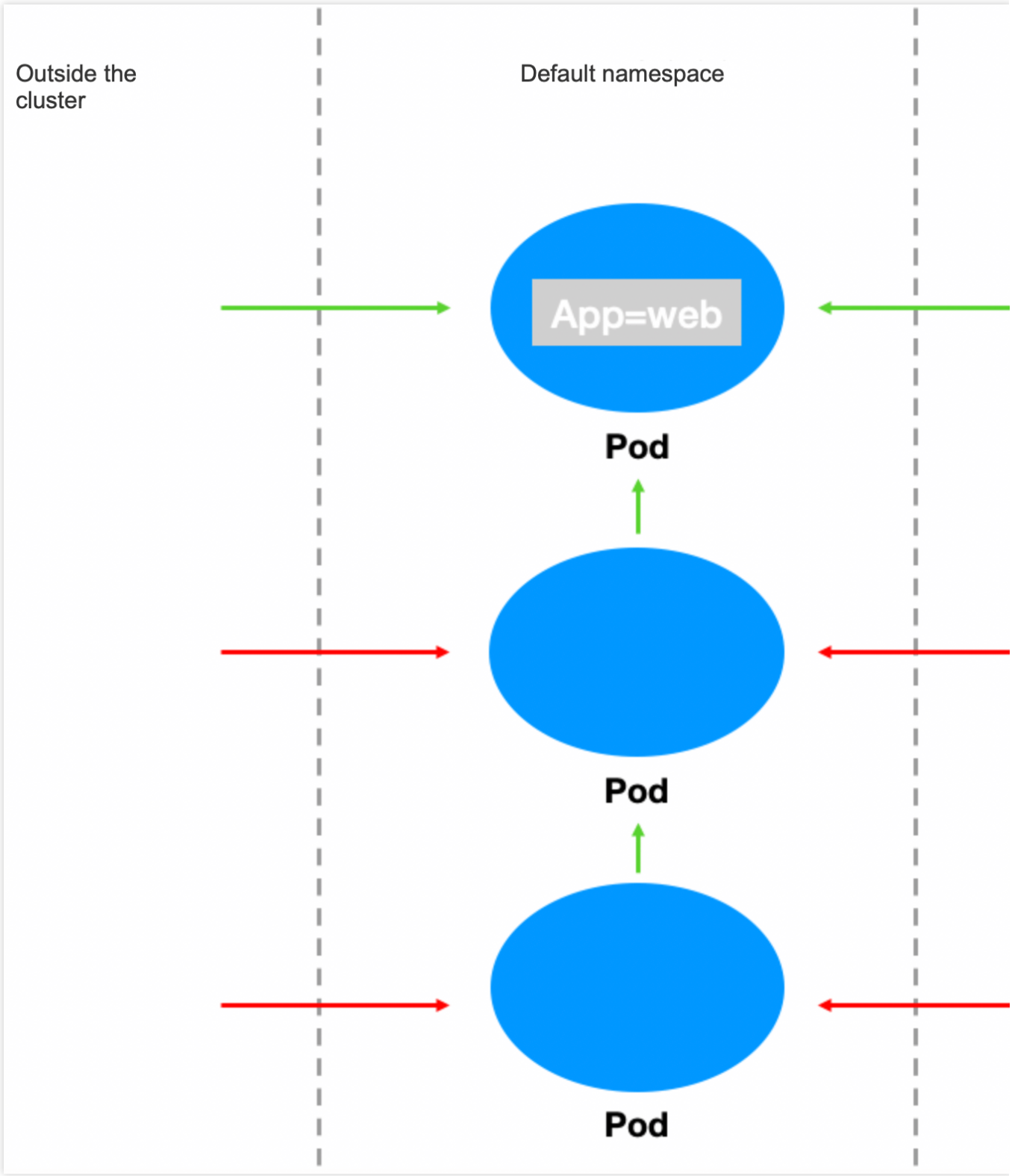
```
kubectl delete pod web
kubectl delete service web
Disable the network policy in the console// (This can also be done by running `kube
```

Scenario 4. Set to allow access only to specified Pods in the namespace

©2013-2022 Tencent Cloud. All rights reserved.

Policy description

Set to allow external requests only to the Pod with the `app=web` label in the namespace.

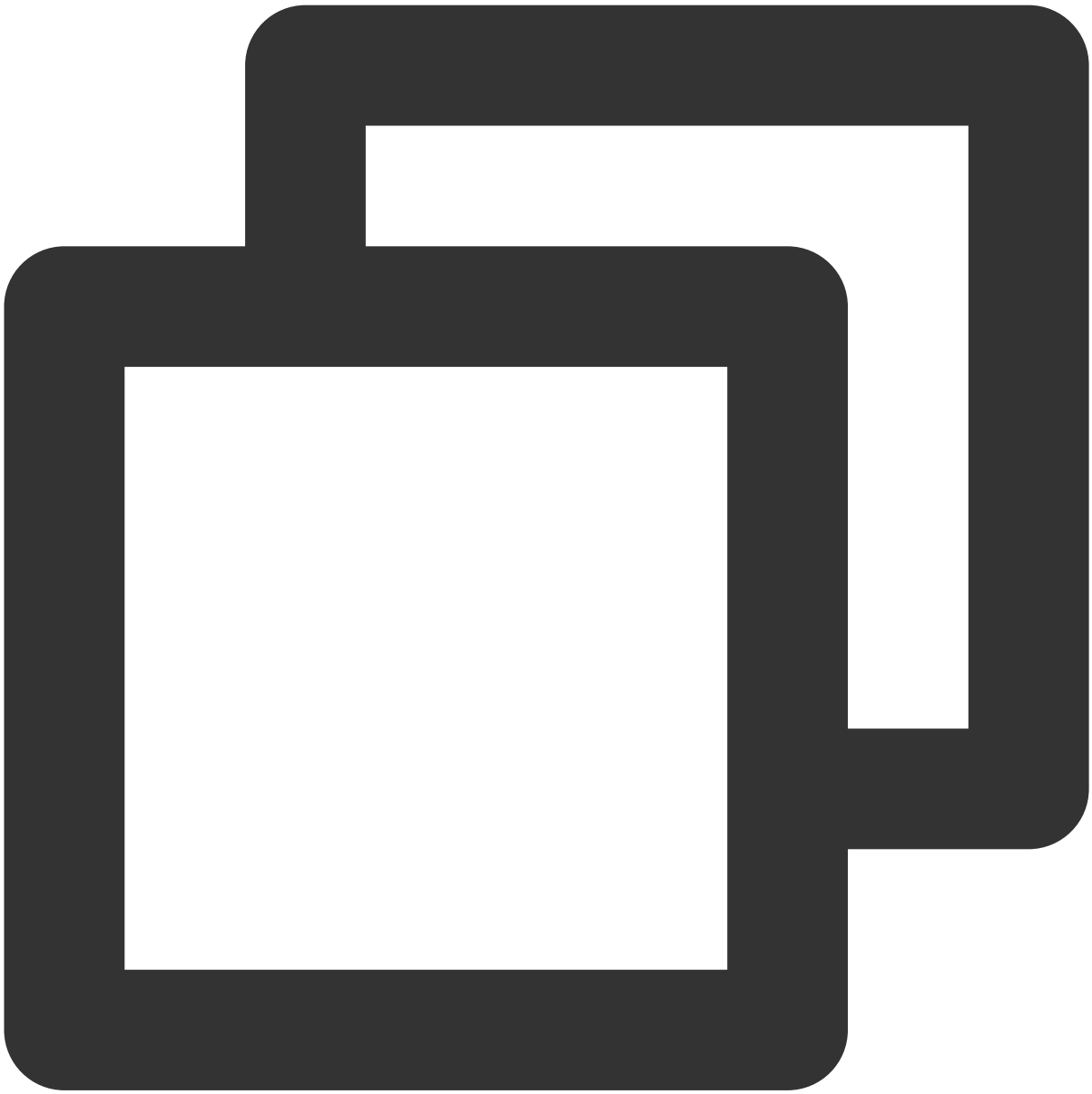


Verification steps

©2013-2022 Tencent Cloud. All rights reserved.

1. Create a Pod application with the `app=web` label and another with the `app=web1` label and start the services.

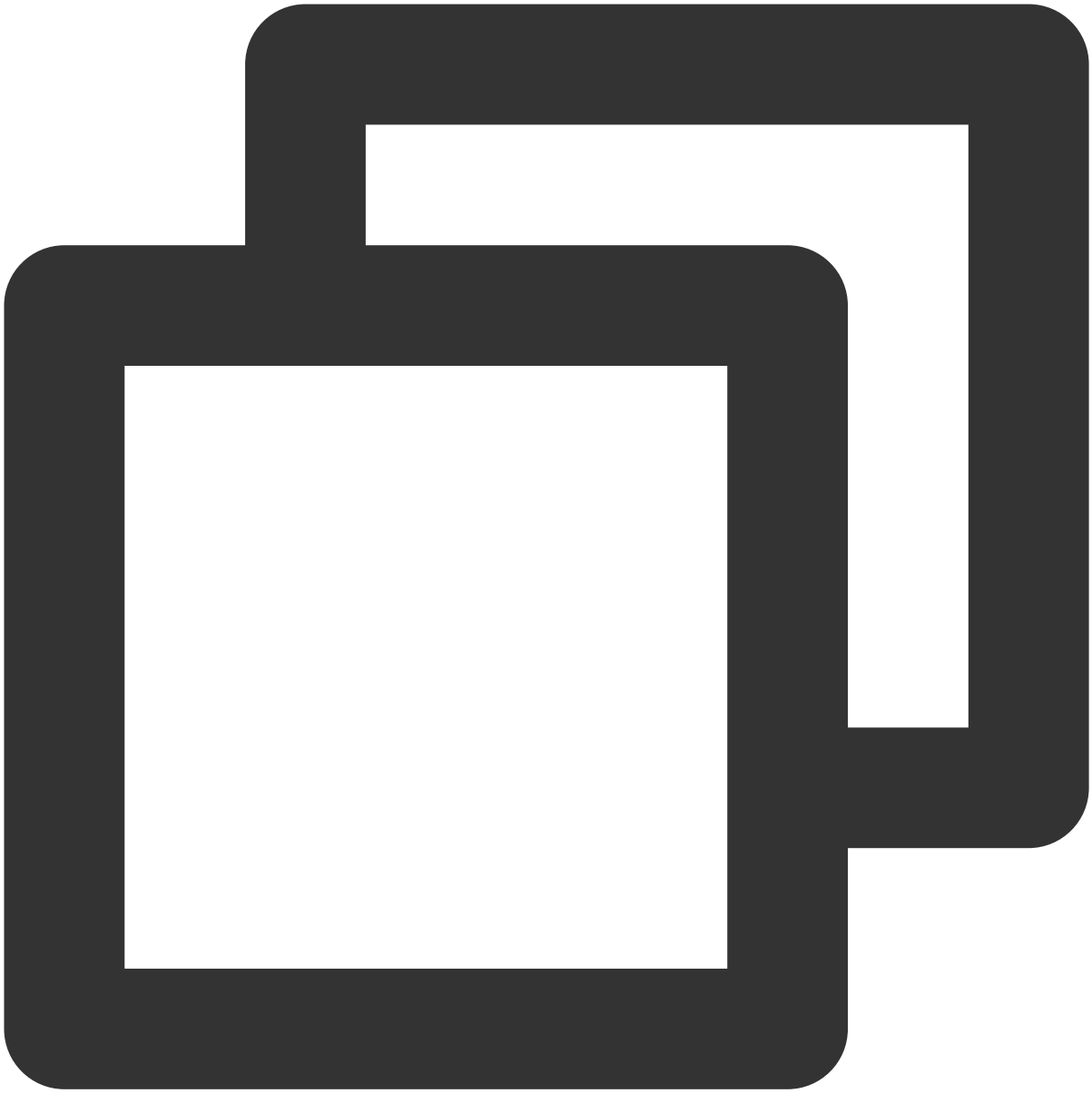
1.1 Create the application with the `app=web` label.



```
[root@VM-0-11-centos ~]# kubectl run web --image=nginx --namespace default --labels
service/web created
pod/web created
[root@VM-0-11-centos ~]# kubectl get svc web
NAME   TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)   AGE
web    ClusterIP   172.18.255.217   <none>        80/TCP    5s
```

1.2 Create the application with the `app=web1` label.

©2013-2022 Tencent Cloud. All rights reserved.

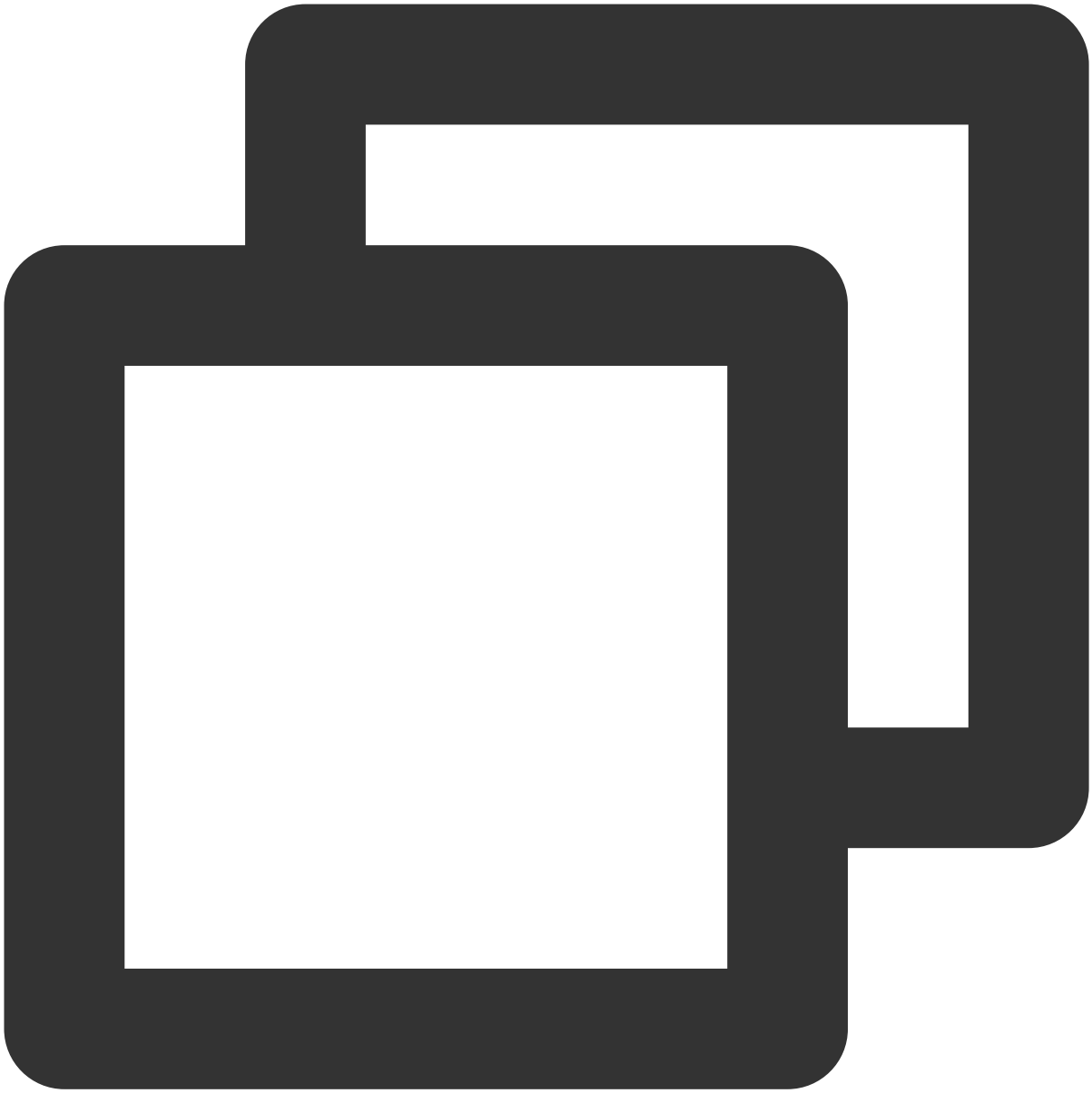


```
[root@VM-0-11-centos ~]# kubectl run  web1 --image=nginx --namespace default --labe
service/web1 created
pod/web1 created
[root@VM-0-11-centos ~]# kubectl get svc web1
NAME   TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)   AGE
web1   ClusterIP   172.18.255.39   <none>        80/TCP    7s
```

2. Verify that the Pods with the `app=web` and `app=web1` labels can be accessed by default.

2.1 The Pod with the `app=web` label can be accessed.

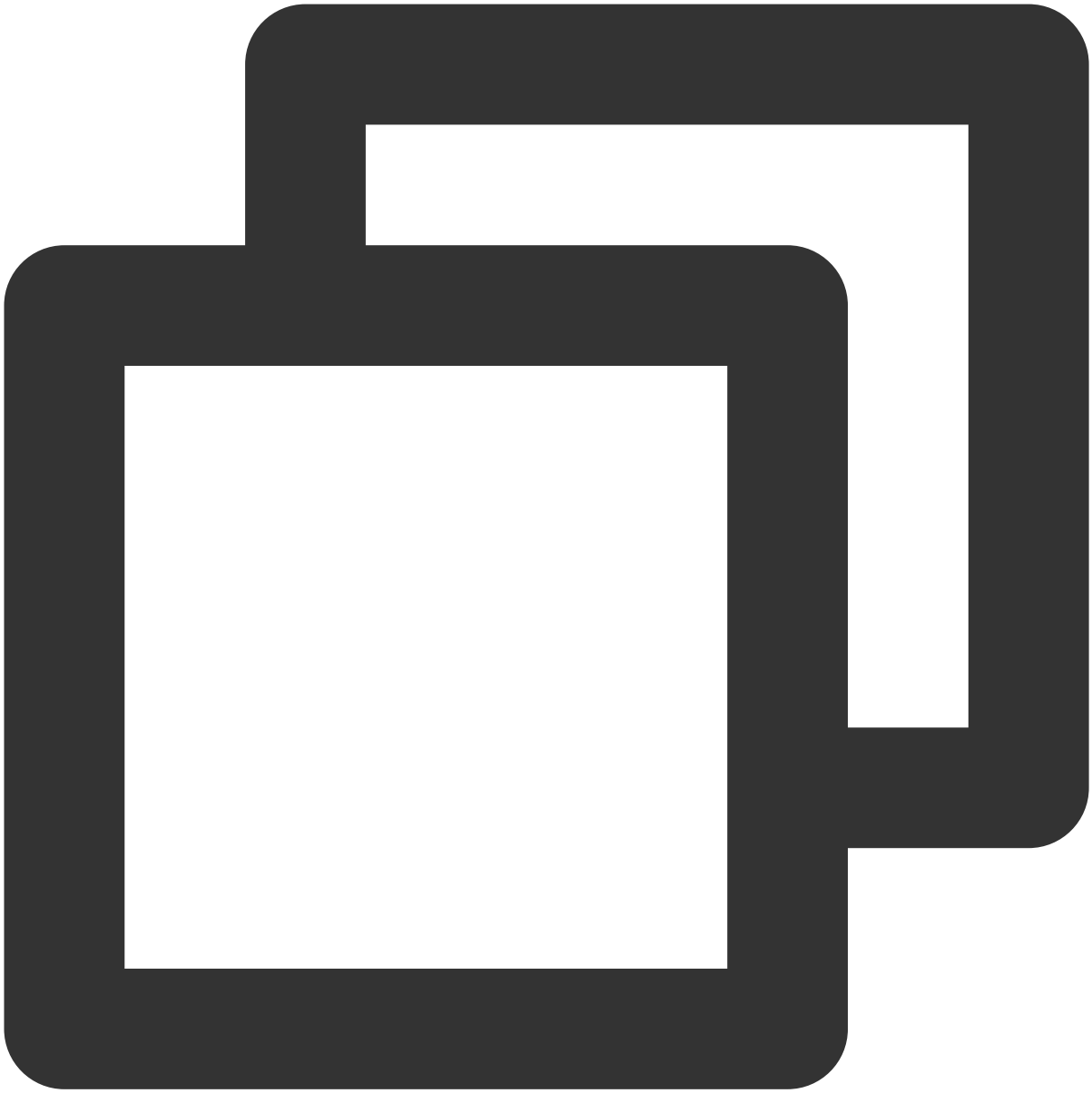
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl run --rm -it --image=alpine testweb -- sh
If you don't see a command prompt, try pressing enter.
/ # wget -qO- http://172.18.255.217
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

2.2 The Pod with the `app=web1` label can be accessed.

©2013-2022 Tencent Cloud. All rights reserved.

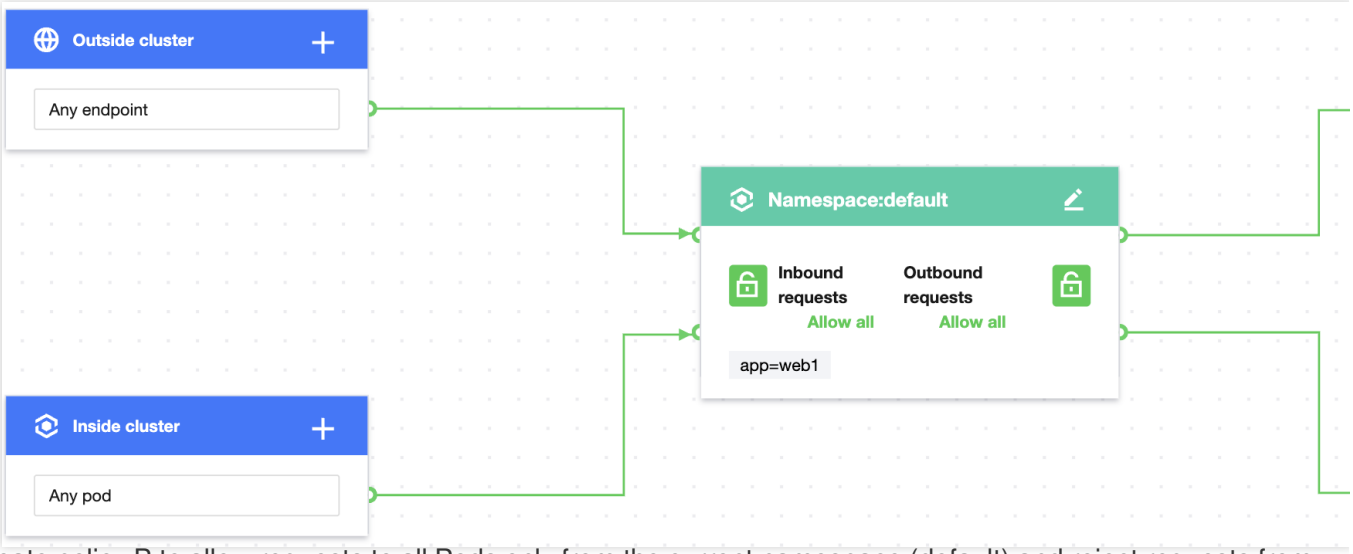


```
[root@VM-0-11-centos ~]# kubectl run --rm -it --image=alpine testweb -- sh
If you don't see a command prompt, try pressing enter.
/ # wget -qO- http://172.18.255.39
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

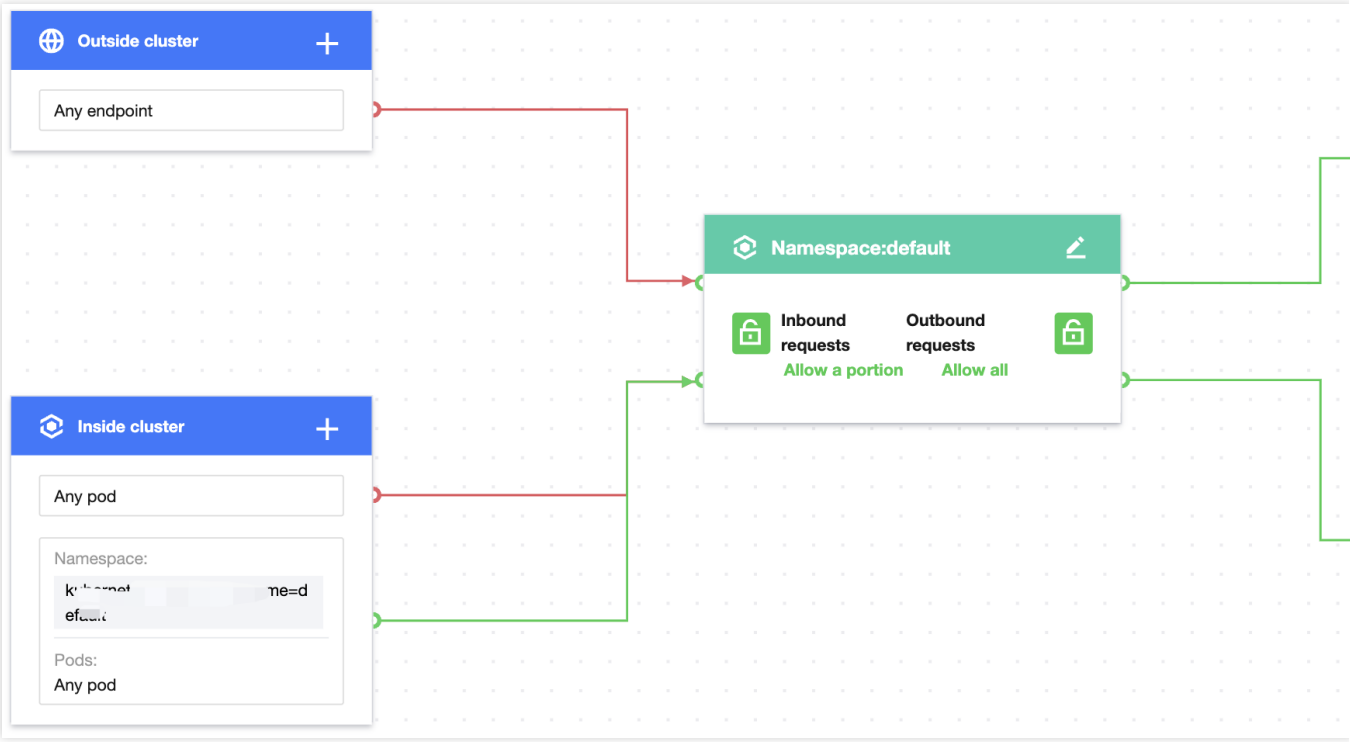
3. Create and enable the container network policy.

©2013-2022 Tencent Cloud. All rights reserved.

3.1 Create policy A to allow all inbound requests to the Pod with the `app=web` label, specifically, by specifying the current namespace (default) and the `app=web` label.

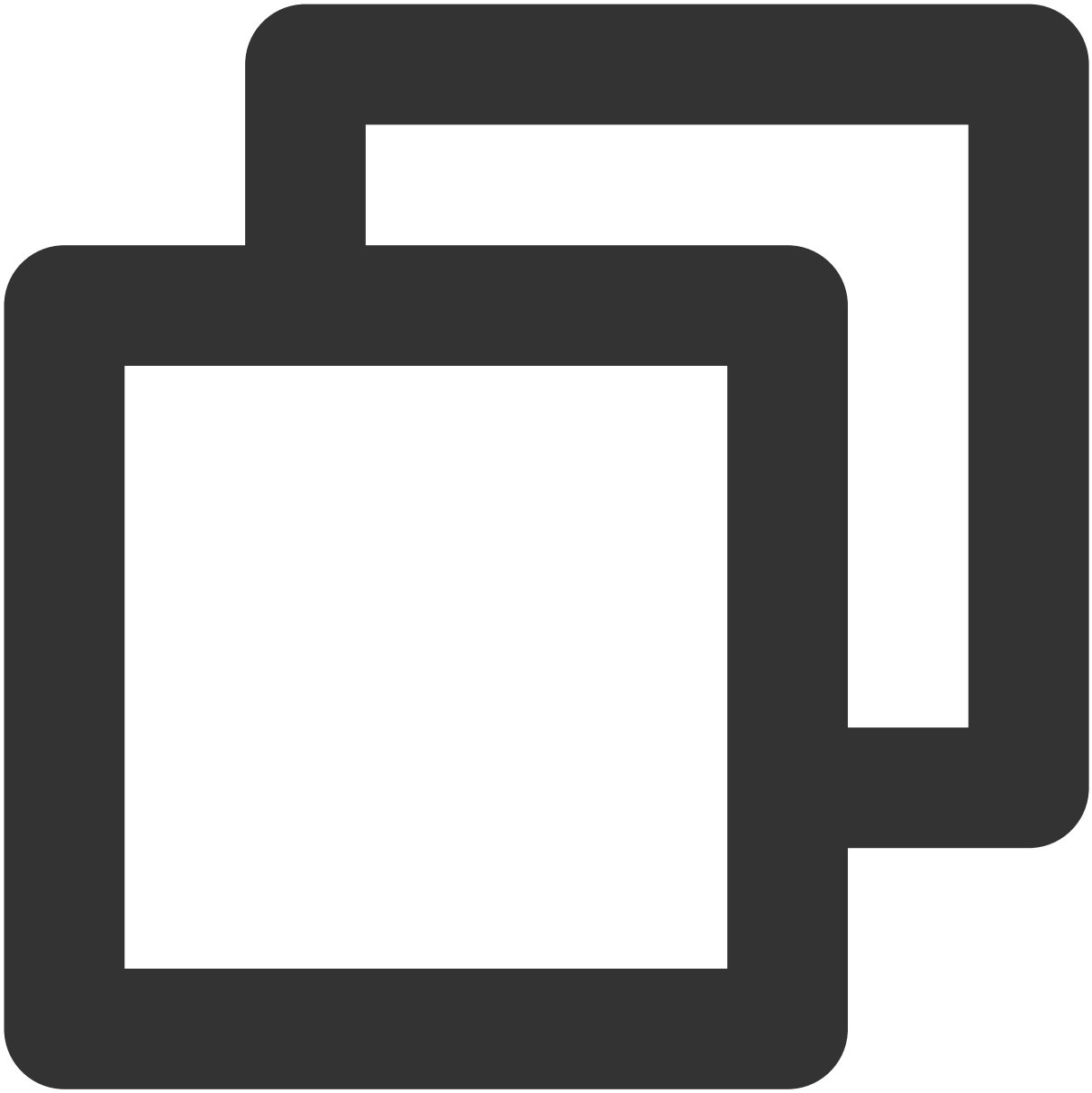


3.2 Create policy B to allow requests to all Pods only from the current namespace (default) and reject requests from other namespaces.



4. Verify the effect of the network policy. In the `default` namespace, only the Pod with the `app=web` label can be accessed from other namespaces, and other Pods (such as that with the `app=web1` label) cannot.
The Pod with the `app=web` label can be accessed from other namespaces.

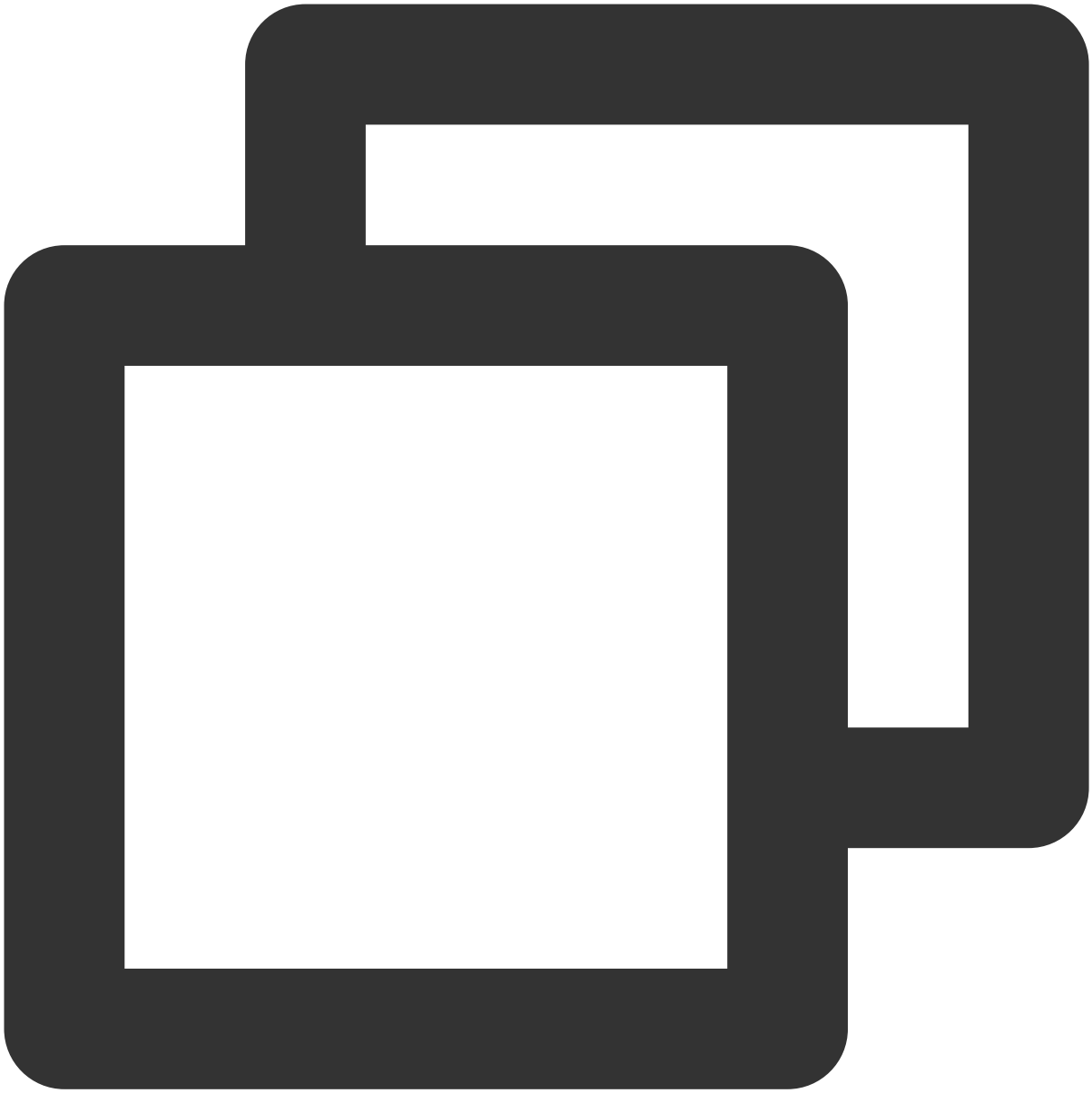
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl create namespace secondary
[root@VM-0-11-centos ~]# kubectl run  testweb --namespace=secondary --rm -i -t --im
/ # wget -qO- --timeout=2 http://web.default
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

The Pod with the `app=web1` label cannot be accessed from other namespaces.

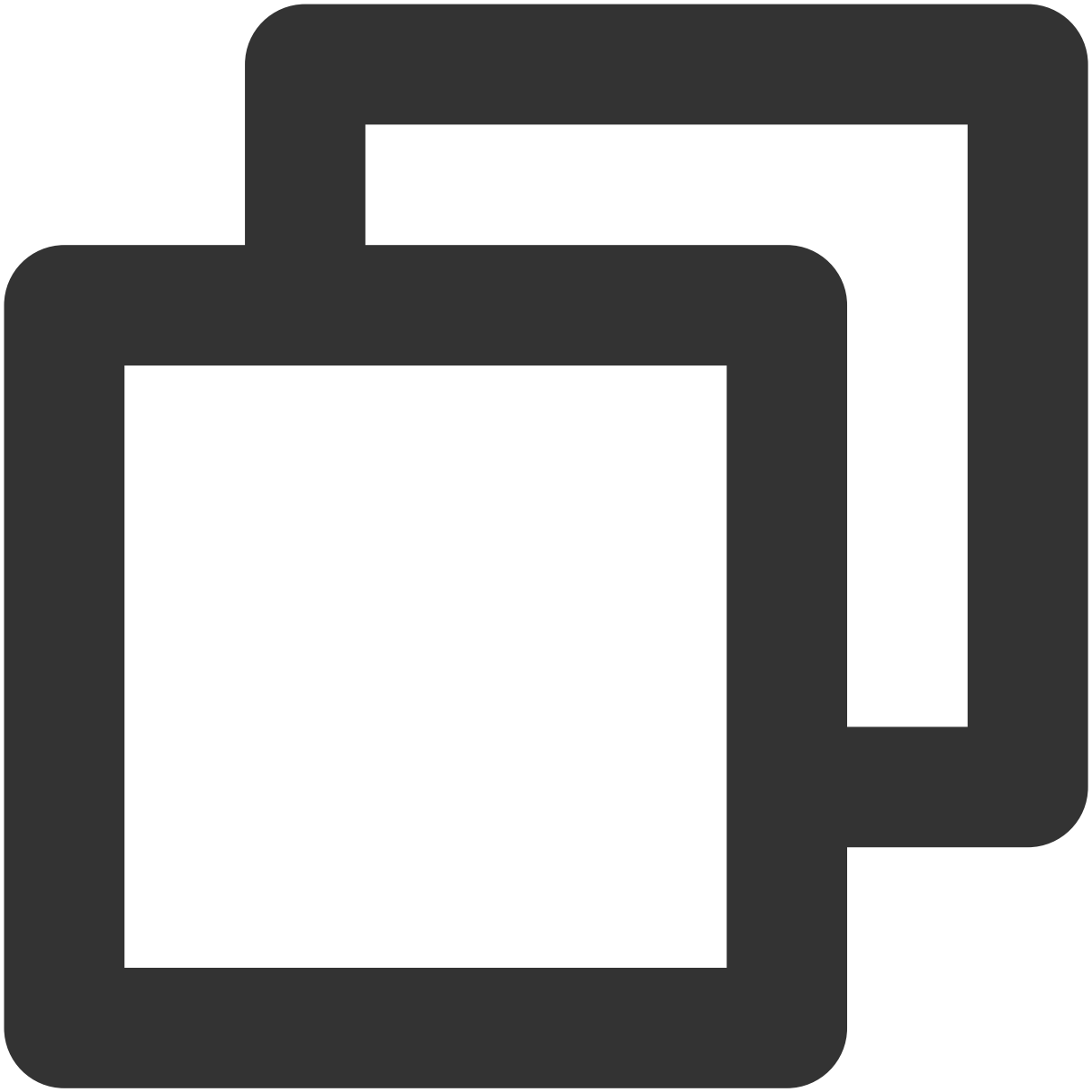
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl create namespace secondary
[root@VM-0-11-centos ~]# kubectl run  testweb --namespace=secondary --rm -i -t --im
/ # wget -qO- --timeout=2 http://web1.default
wget: can't connect to remote host (172.18.255.39): Connection refused
```

4. Clear the environment.

©2013-2022 Tencent Cloud. All rights reserved.



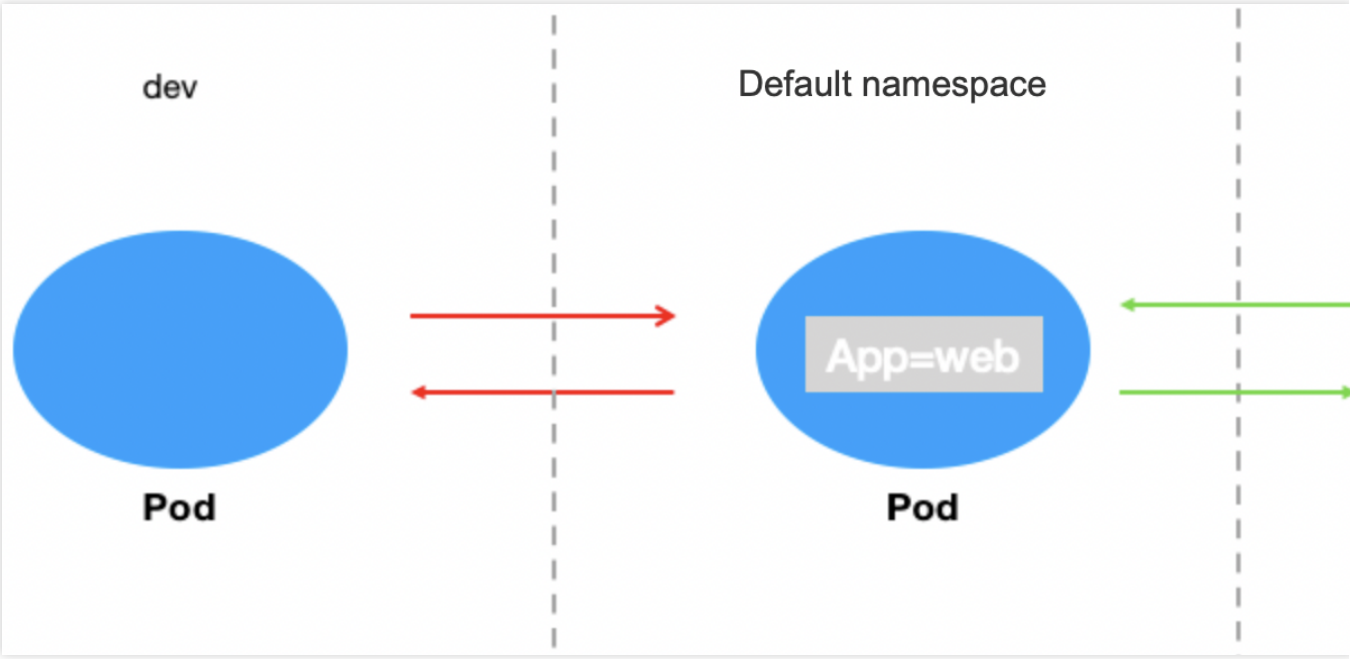
```
kubectl delete pod web -n default
kubectl delete service web -n default
kubectl delete namespace secondary
Disable the network policy in the console// (This can also be done by running `kube
```

Scenario 5. Set to allow access to a Pod only from the specified namespace

©2013-2022 Tencent Cloud. All rights reserved.

Policy description

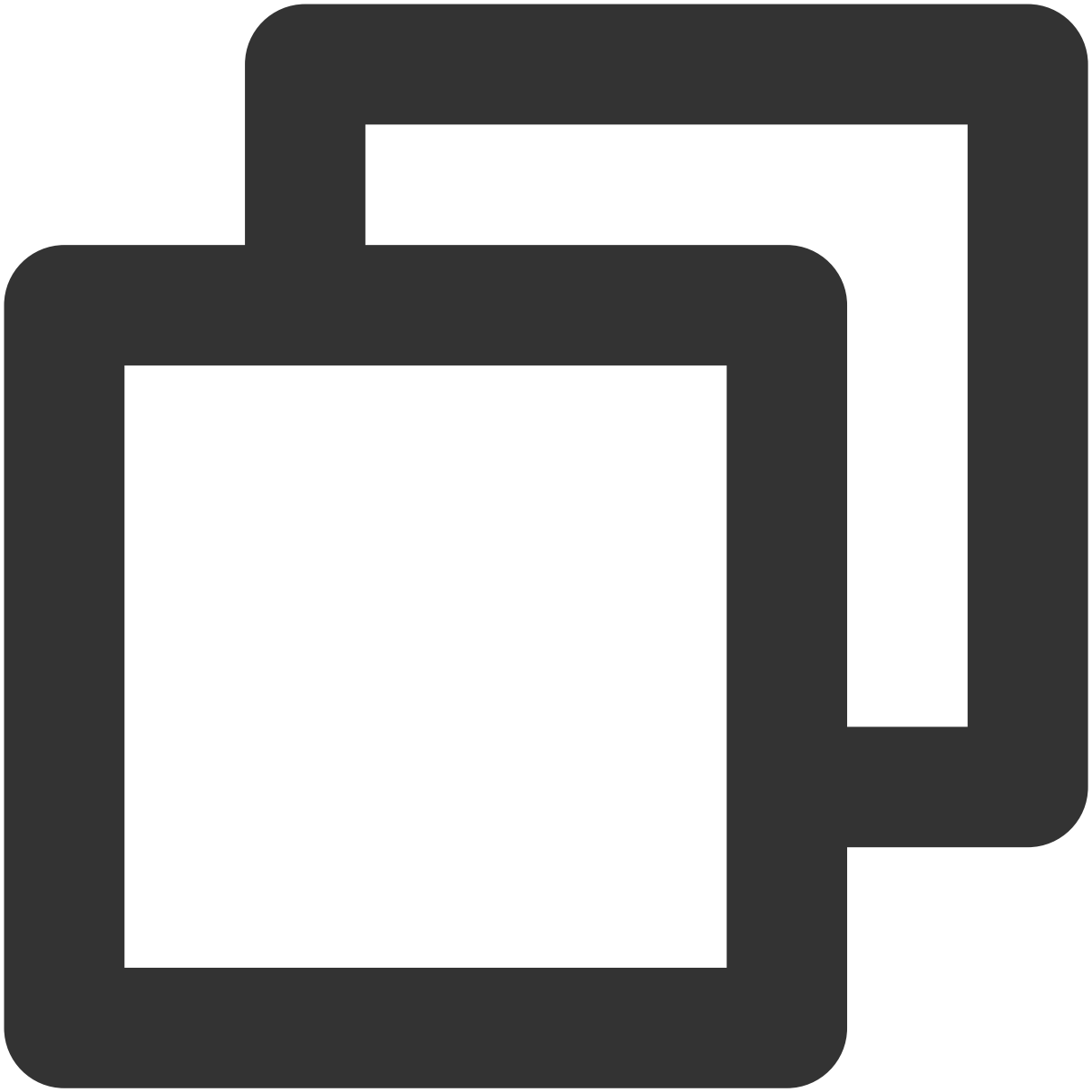
Set to allow access to the Pod with the `app=web` label only from the specified namespace.



Verification steps

1. Create a Pod application with the `app=web` label and start the service.

©2013-2022 Tencent Cloud. All rights reserved.

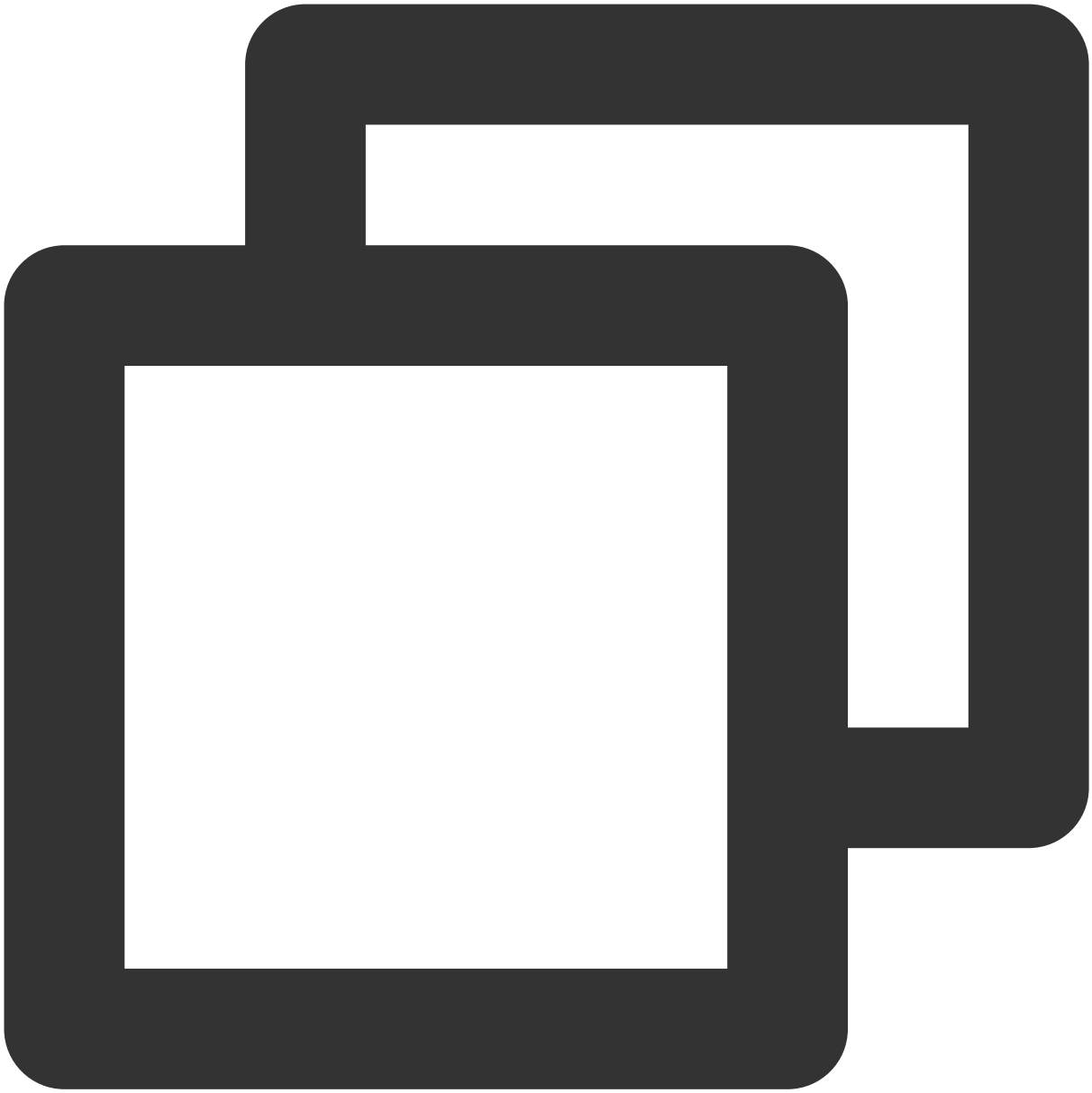


```
[root@VM-0-11-centos ~]# kubectl run web --image=nginx --namespace default --labels
service/web created
pod/web created

[root@VM-0-11-centos ~]# kubectl get svc web
NAME    TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)    AGE
web     ClusterIP   172.18.255.217   <none>        80/TCP     5s
```

2. Create the test namespaces `dev` and `production` and verify that the web application can be accessed from all namespaces by default.

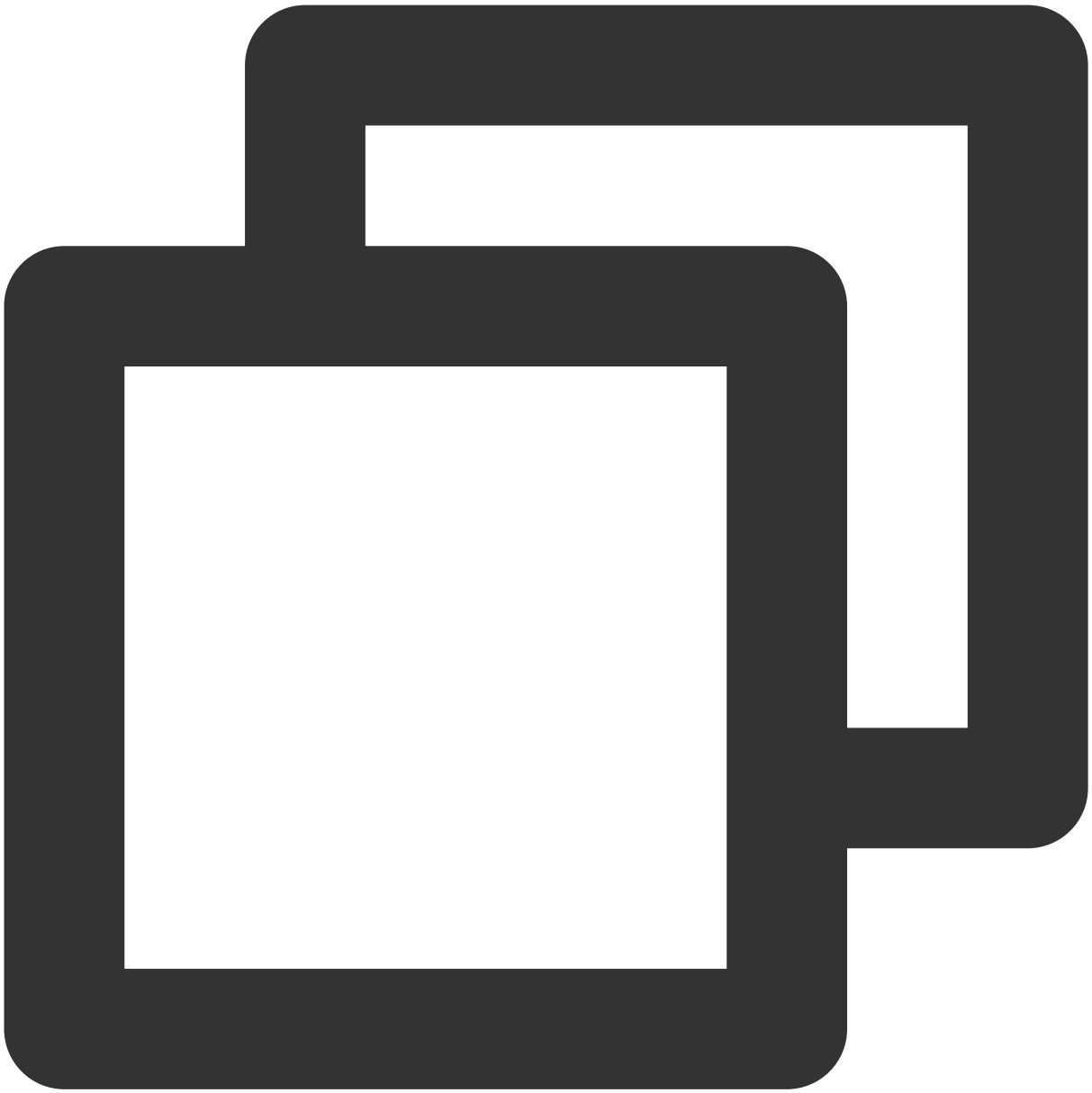
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl create namespace dev
namespace/dev created
[root@VM-0-11-centos ~]# kubectl label namespace/dev env=dev
namespace/dev labeled
[root@VM-0-11-centos ~]# kubectl create namespace production
namespace/production created
[root@VM-0-11-centos ~]# kubectl label namespace/production env=production
namespace/production labeled
[root@VM-0-11-centos ~]#
```

©2013-2022 Tencent Cloud. All rights reserved.

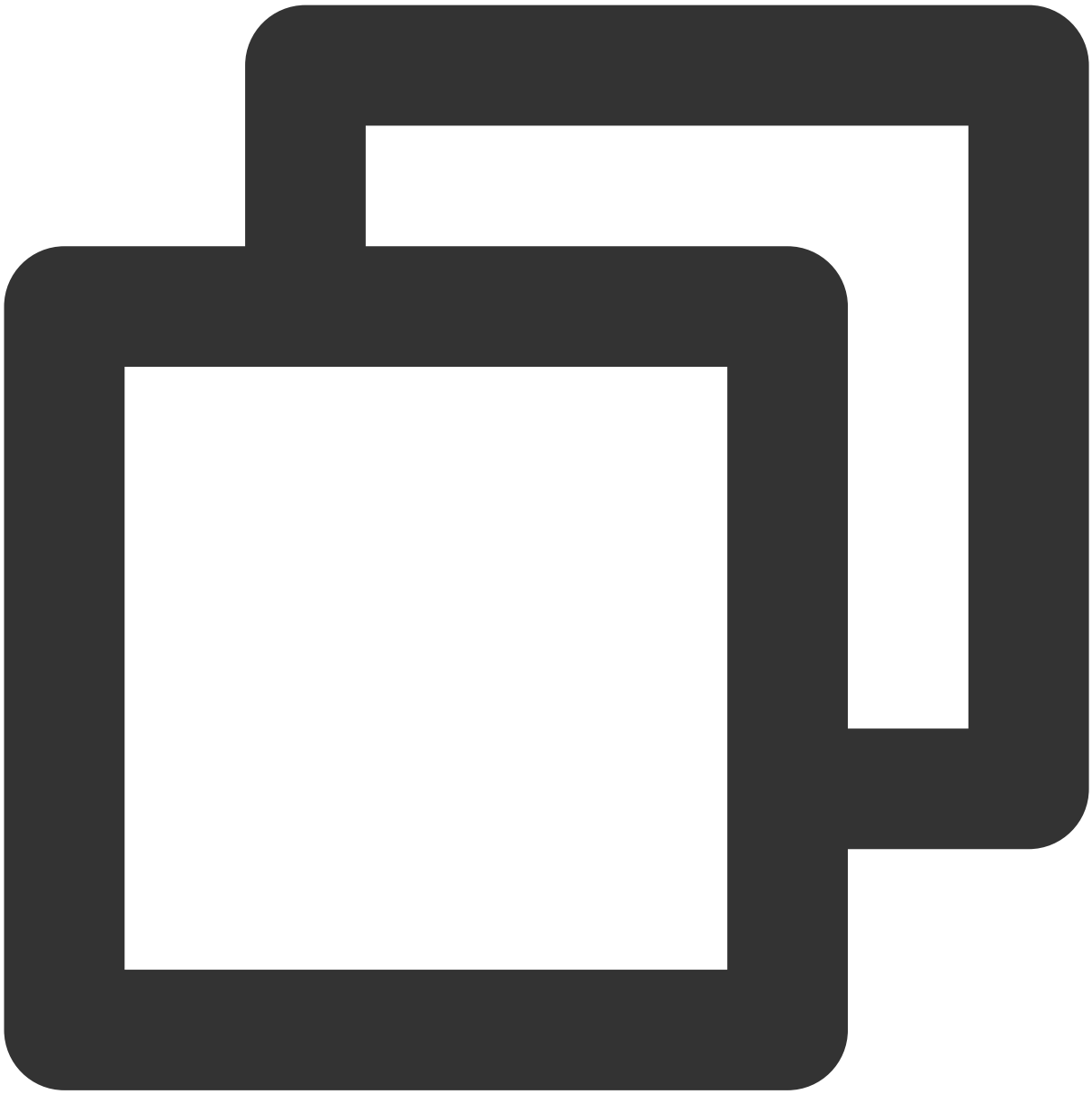
By default, the web application can be accessed from the `dev` namespace.



```
kubectl run  testweb --namespace=dev --rm -i -t --image=alpine -- sh
If you don't see a command prompt, try pressing enter.
/ # wget -qO- --timeout=2 http://web.default
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

©2013-2022 Tencent Cloud. All rights reserved.

By default, the web application can be accessed from the `production` namespace.

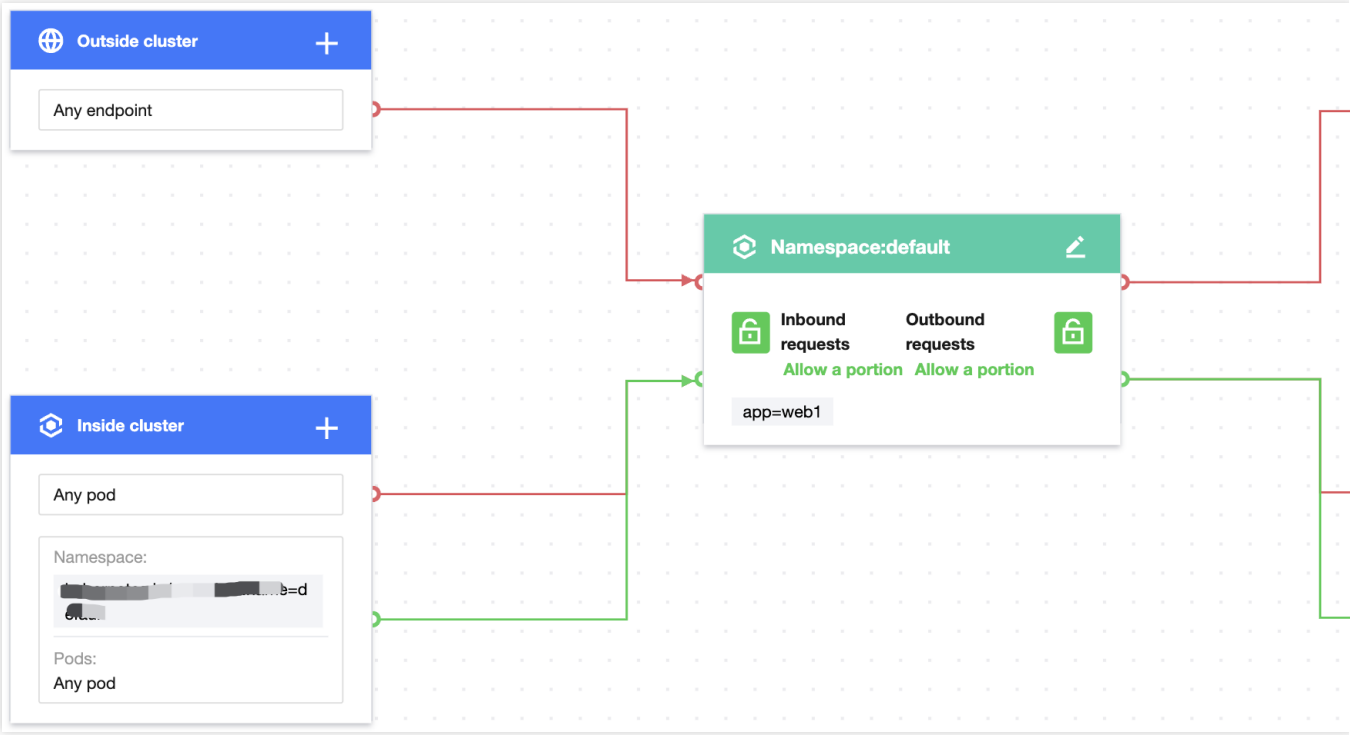


```
kubectl run  testweb --namespace=production --rm -i -t --image=alpine -- sh
If you don't see a command prompt, try pressing enter.
/ # wget -qO- --timeout=2 http://web.default
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

©2013-2022 Tencent Cloud. All rights reserved.

3. Create and enable the container network policy.

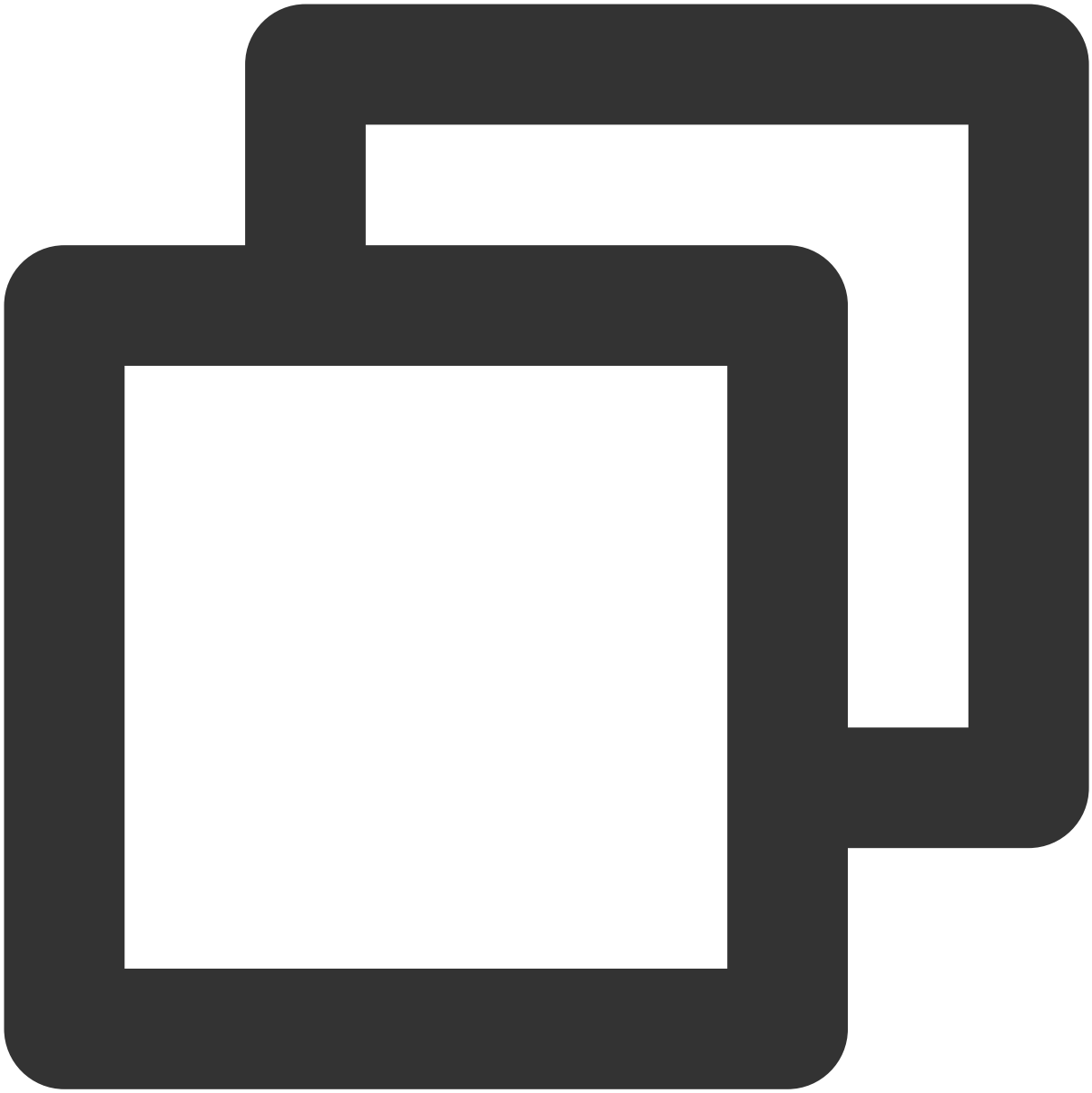
Set the label of the protected Pod as `app=web` , configure the source type as the namespace, and set to allow requests only from the namespace with the `env=production` label. The configuration is the same for outbound rules as shown below:



4. Verify the effect of the network policy.

The web service cannot be accessed from the `dev` namespace.

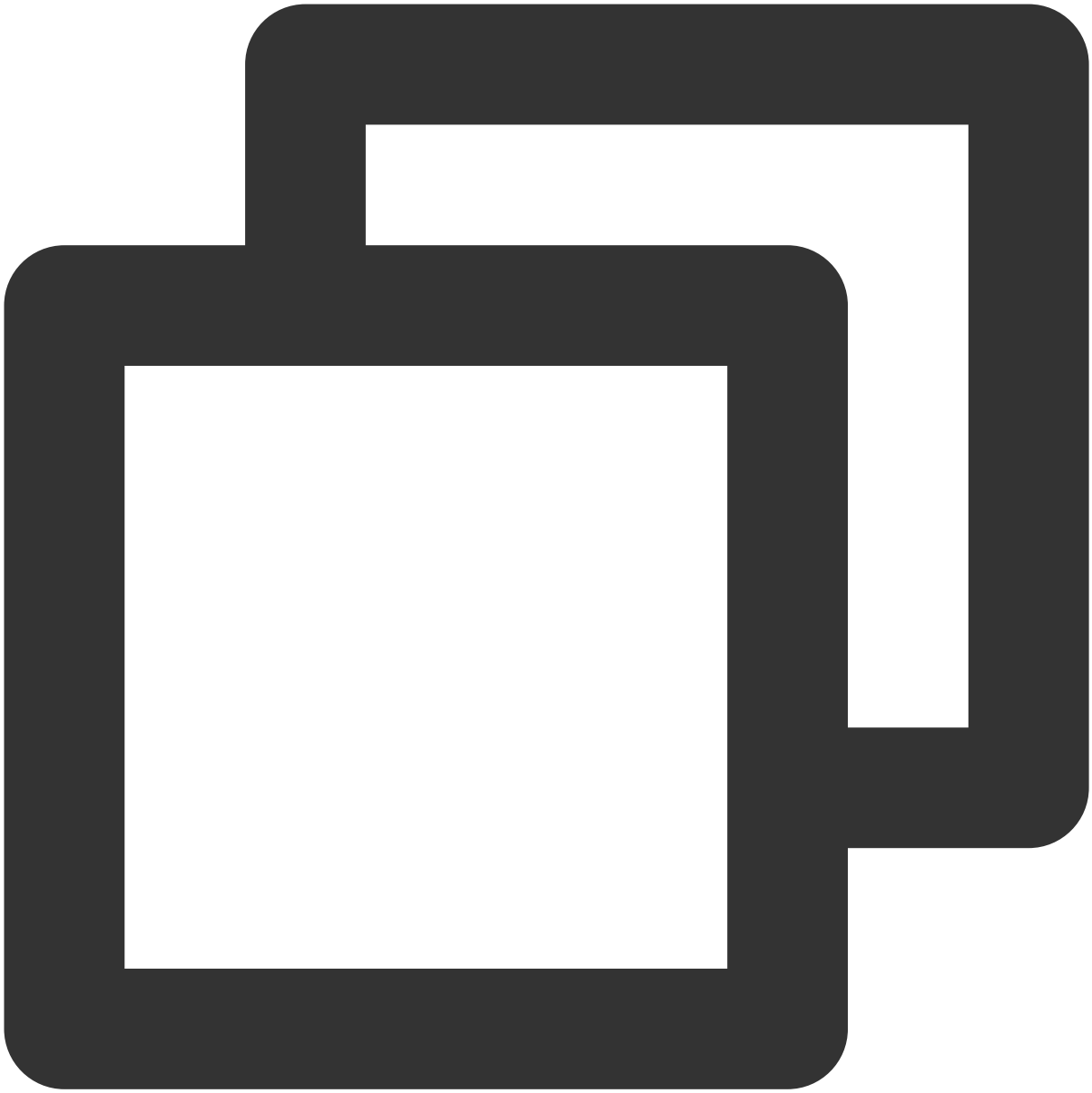
©2013-2022 Tencent Cloud. All rights reserved.



```
kubectl run  testweb --namespace=dev --rm -i -t --image=alpine -- sh
If you don't see a command prompt, try pressing enter.
/ # wget -qO- --timeout=2 http://web.default
wget: can't connect to remote host (172.18.255.217): Connection refused
```

The web service can be accessed from the `production` namespace.

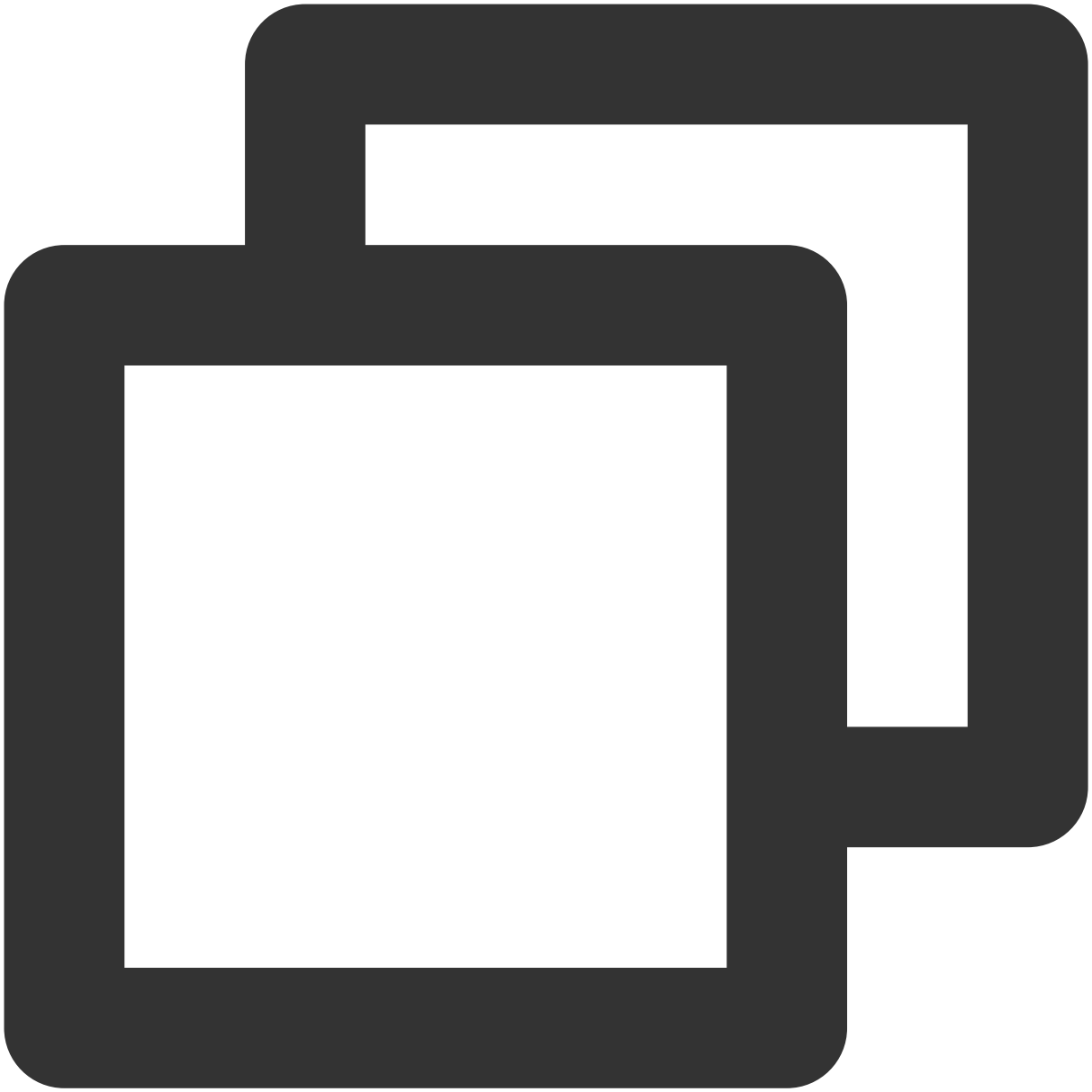
©2013-2022 Tencent Cloud. All rights reserved.



```
kubectl run  testweb --namespace=production --rm -i -t --image=alpine -- sh
If you don't see a command prompt, try pressing enter.
/ # wget -qO- --timeout=2 http://web.default
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

5. Clear the environment.

©2013-2022 Tencent Cloud. All rights reserved.



```
kubectl delete pod web
kubectl delete service web
kubectl delete namespace {prod,dev}
Disable the network policy in the console// (This can also be done by running `kube
```

Scenario 6. Set to allow requests to a Pod only from the cluster

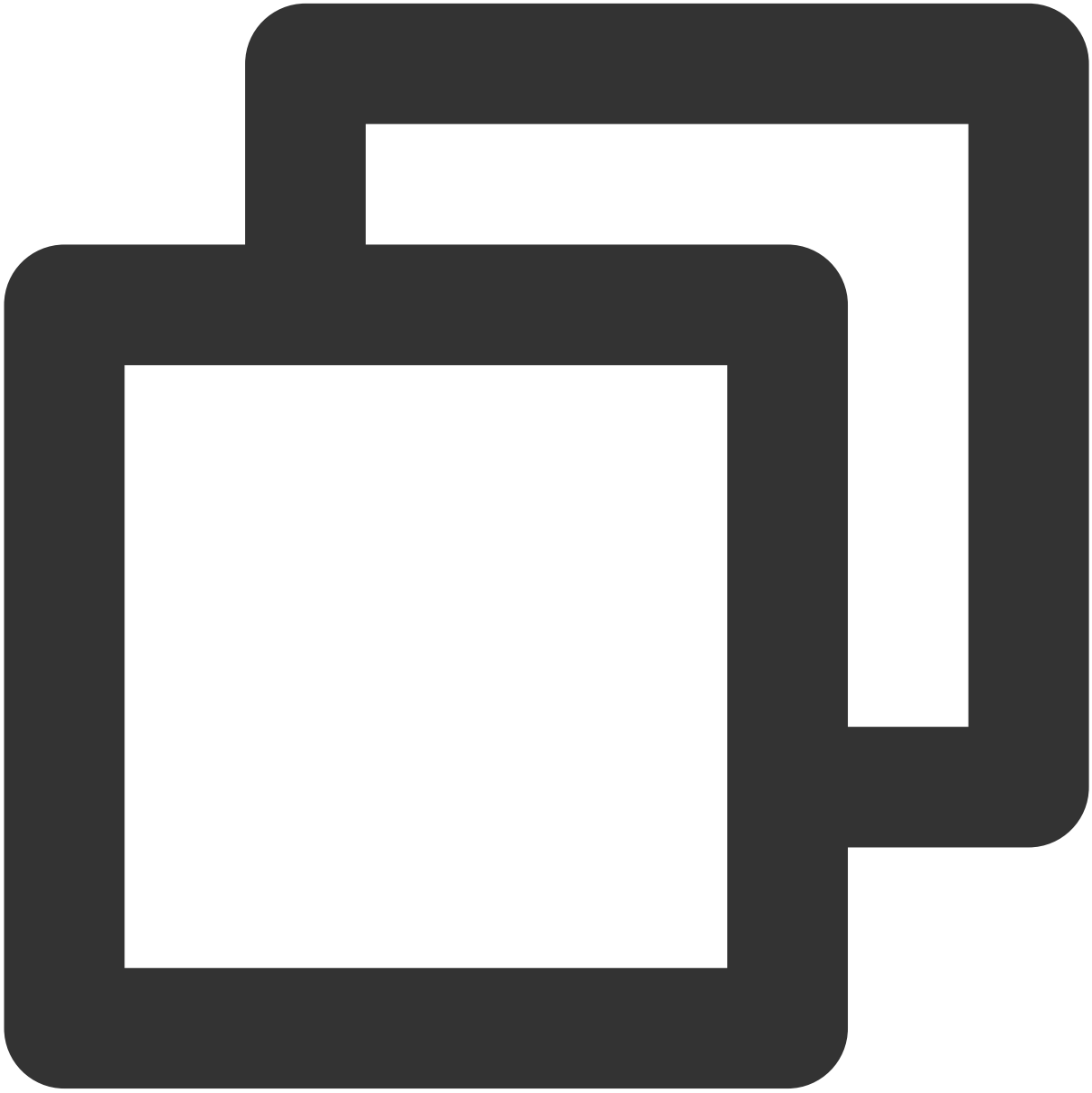
Policy description

©2013-2022 Tencent Cloud. All rights reserved.

Set to allow requests to the application with the `app=web` label only from the cluster and reject those from outside the cluster.

Verification steps

1. Create a Pod application with the `app=web` label and another with the `app=web1` label and start the services. `web1` simulates a service in the cluster.



```
[root@VM-0-11-centos ~]# kubectl run web --image=nginx  --labels=app=web --expose -
service/web created
pod/web created
```

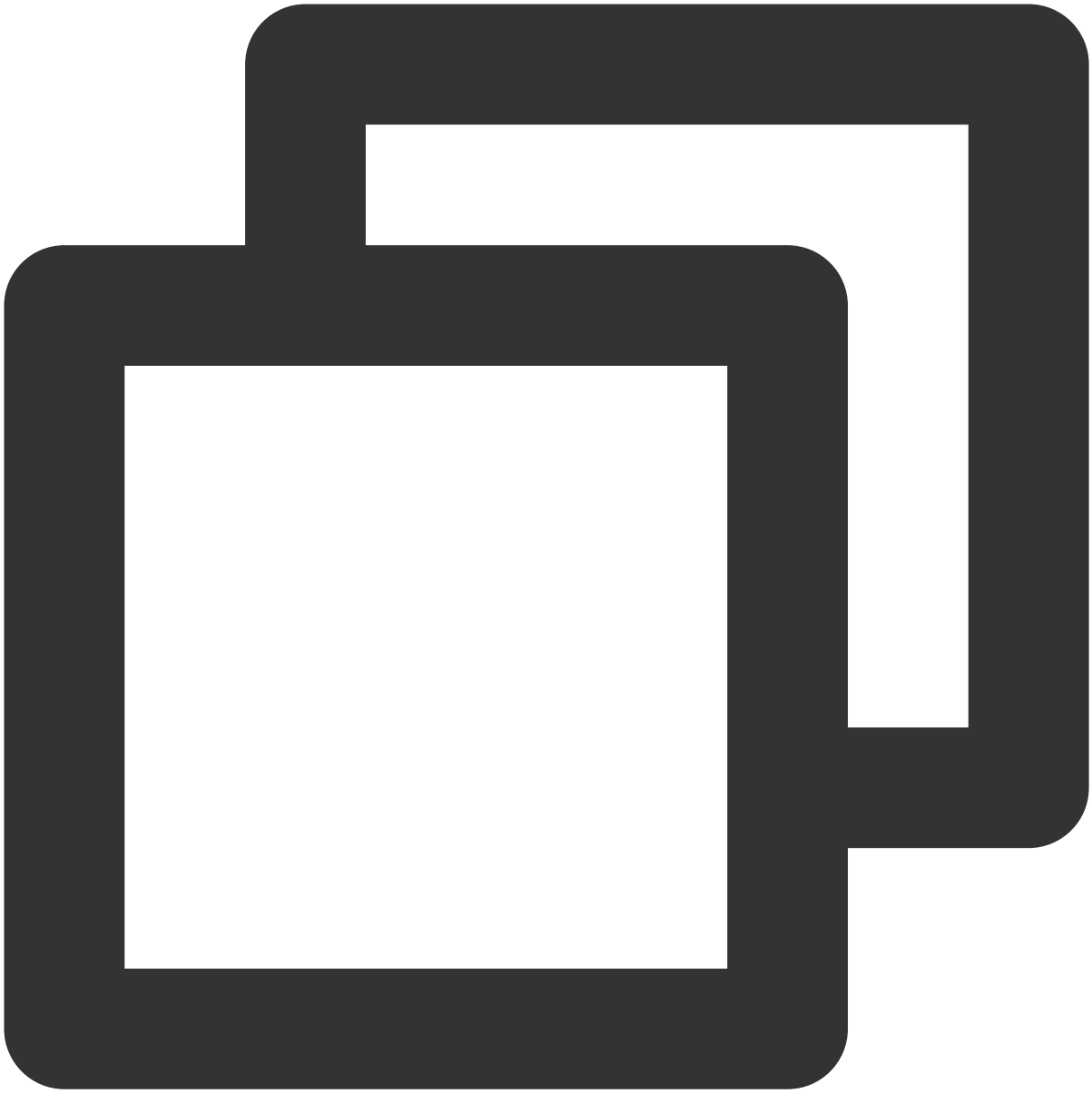
©2013-2022 Tencent Cloud. All rights reserved.

```
[root@VM-0-11-centos ~]# kubectl run web1 --image=nginx  --labels=app=web1 --expose
service/web created
pod/web created
[root@VM-0-11-centos ~]# kubectl get svc web
NAME   TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)   AGE
web    ClusterIP   172.18.255.217   <none>        80/TCP    5s
[root@VM-0-11-centos ~]# kubectl get svc web1
NAME   TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)   AGE
web1   ClusterIP   172.18.255.39   <none>        80/TCP    7s
```

2. Verify that the web service can access the service in the cluster and external IPs by default.

The web application can access the `web1` service in the cluster.

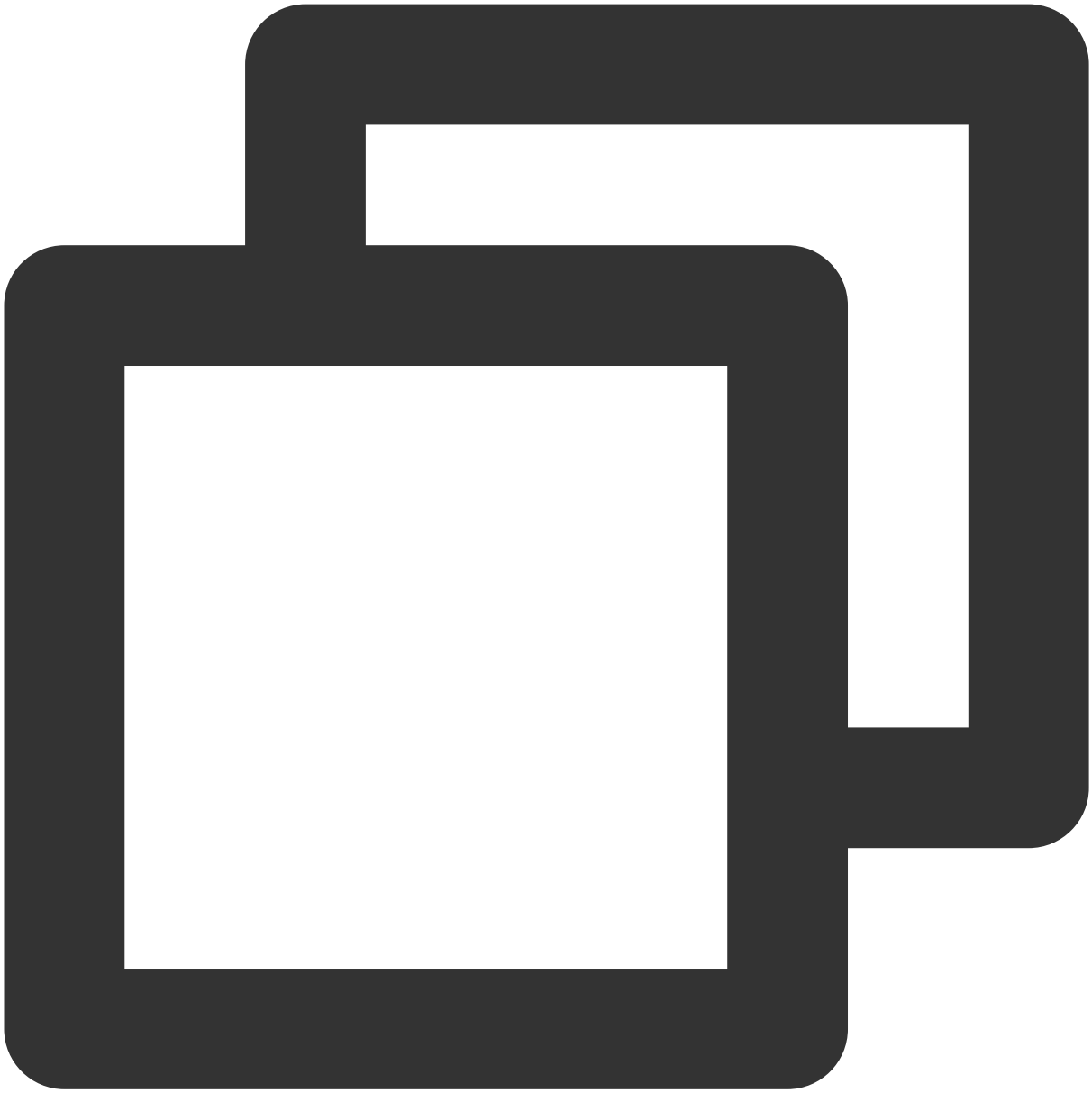
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl exec -it web -- sh
# curl 172.18.255.39:80
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

The web application can access external IPs.

©2013-2022 Tencent Cloud. All rights reserved.

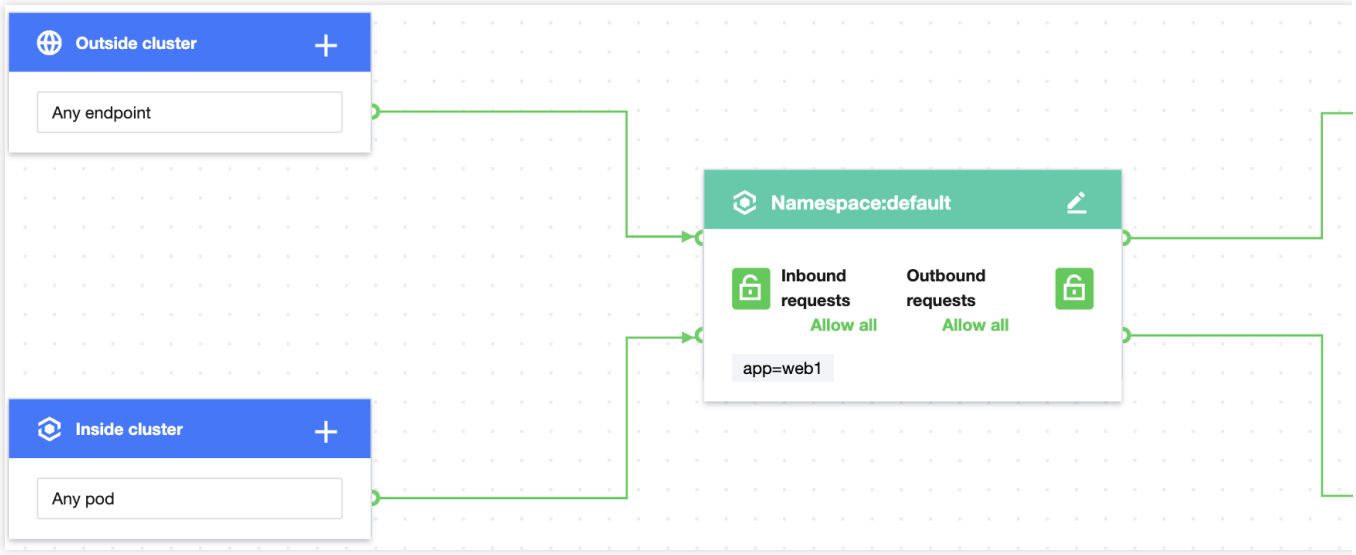


```
[root@VM-0-11-centos ~]# kubectl exec -it web -- sh
# curl 220.181.38.148:80
<html>
<meta http-equiv="refresh" content="0;url=http://www.baidu.com/">
</html>
```

3. Create and enable the network policy.

Set the label of the protected Pod as `app=web` and allow requests from any namespace in the cluster. The configuration is the same for outbound rules as shown below:

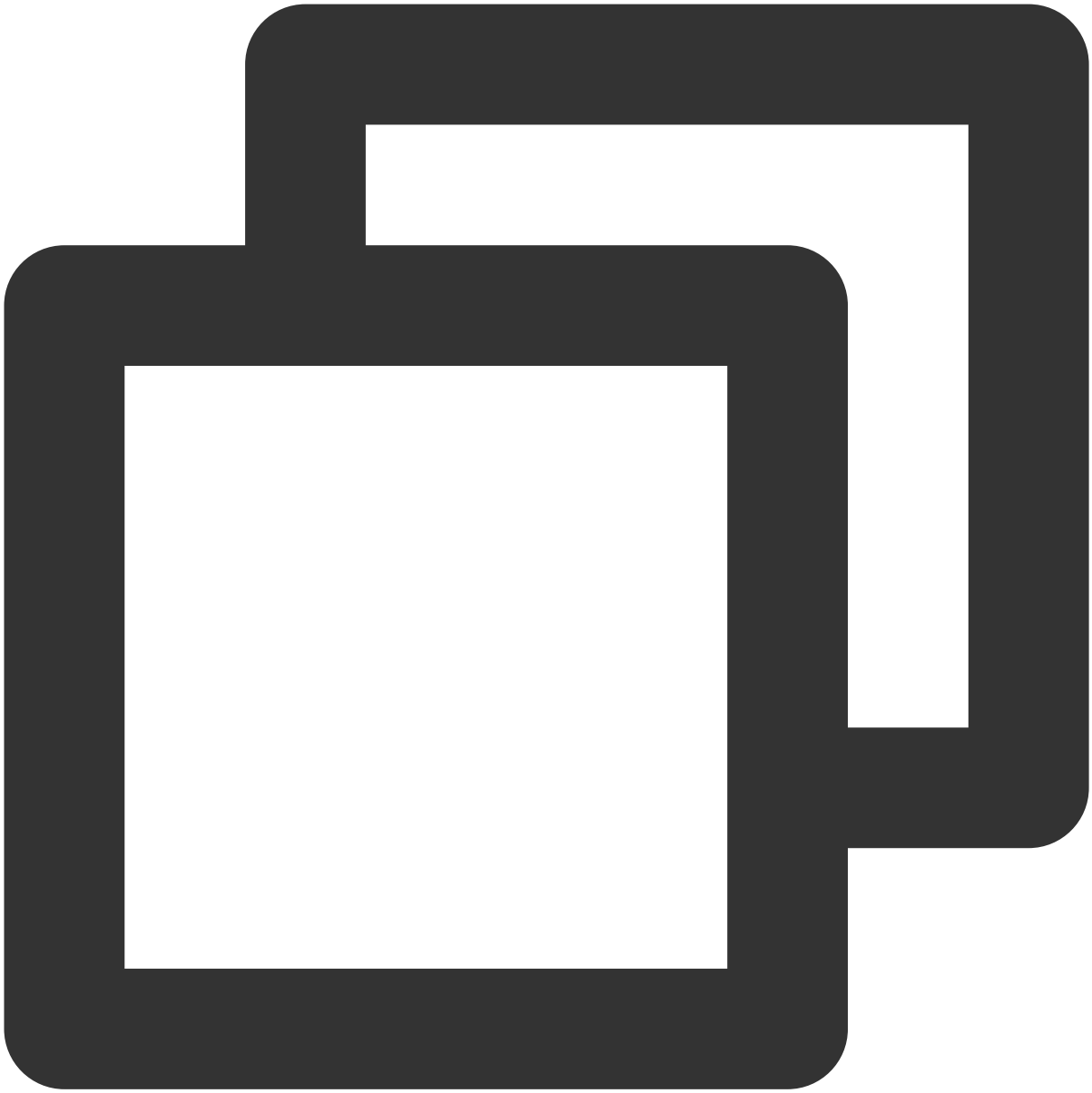
©2013-2022 Tencent Cloud. All rights reserved.



4. Verify the effect of the network policy.

The web application can access the `web1` service in the cluster.

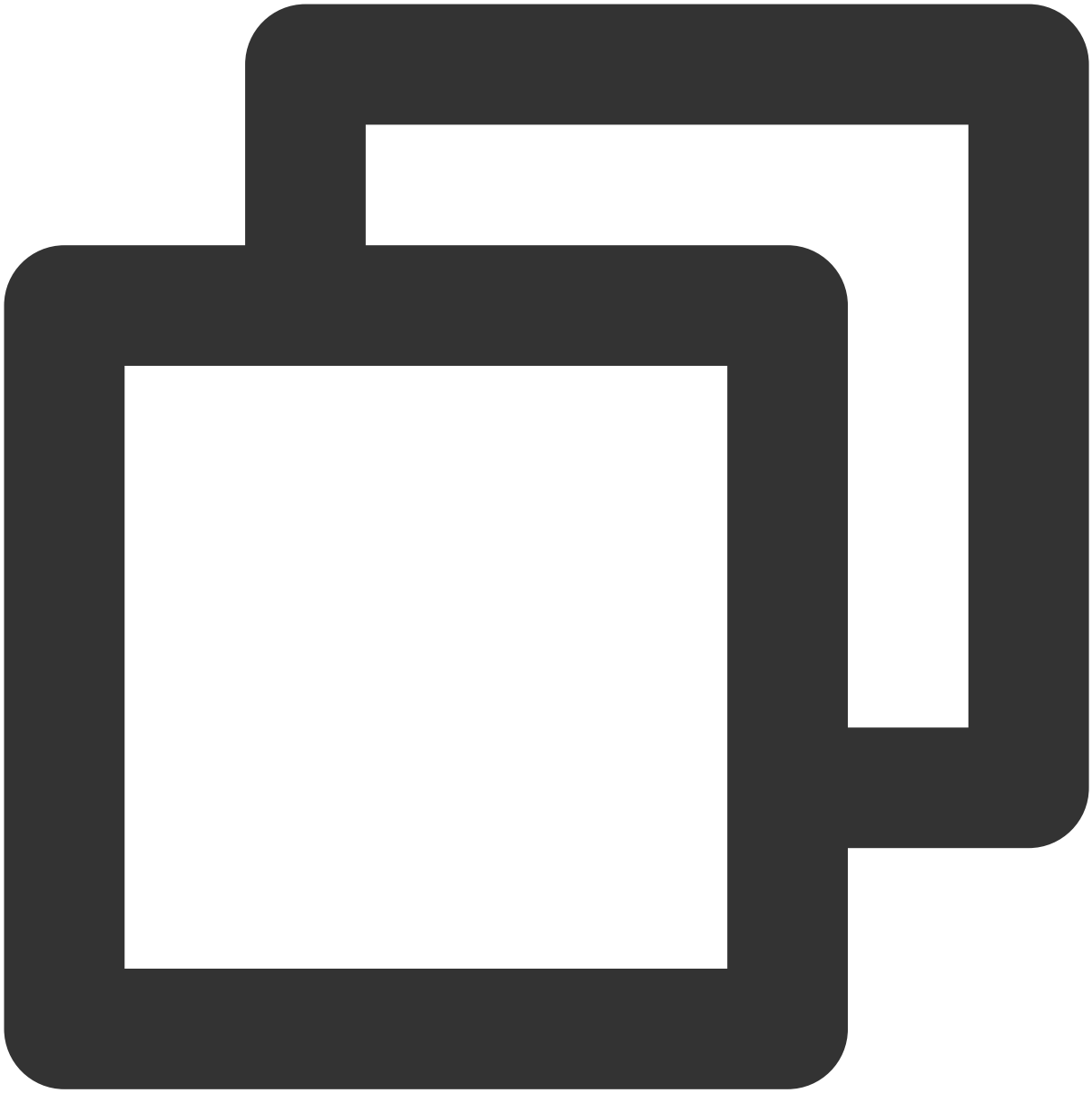
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl exec -it web -- sh
# curl 172.18.255.39:80
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

The web application cannot access external IPs.

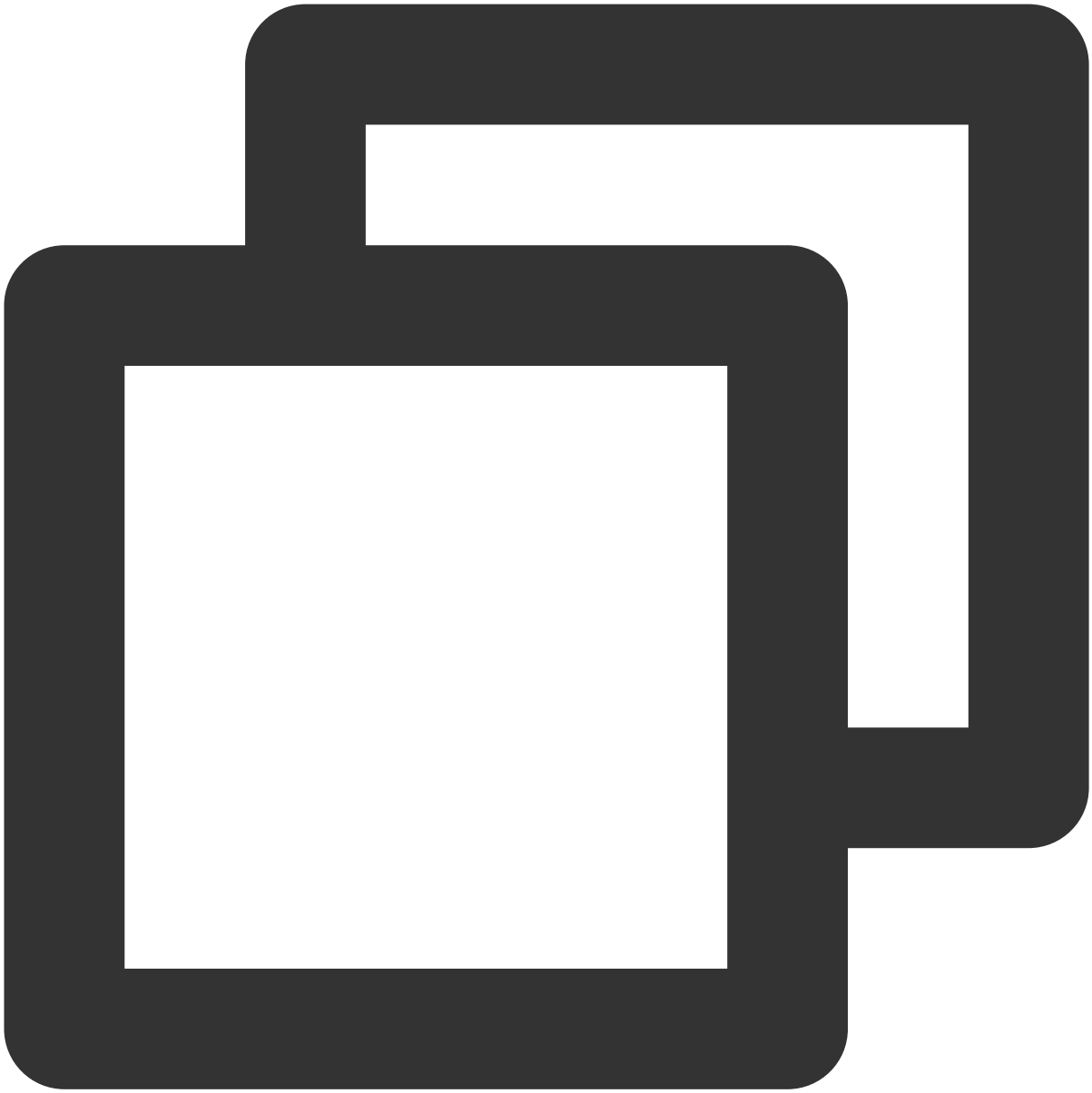
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl exec -it web -- sh
# curl 220.181.38.148:80
curl: (: not foundo connect to 220.181.38.148 port 80: Connection refused
```

5. Clear the environment.

©2013-2022 Tencent Cloud. All rights reserved.



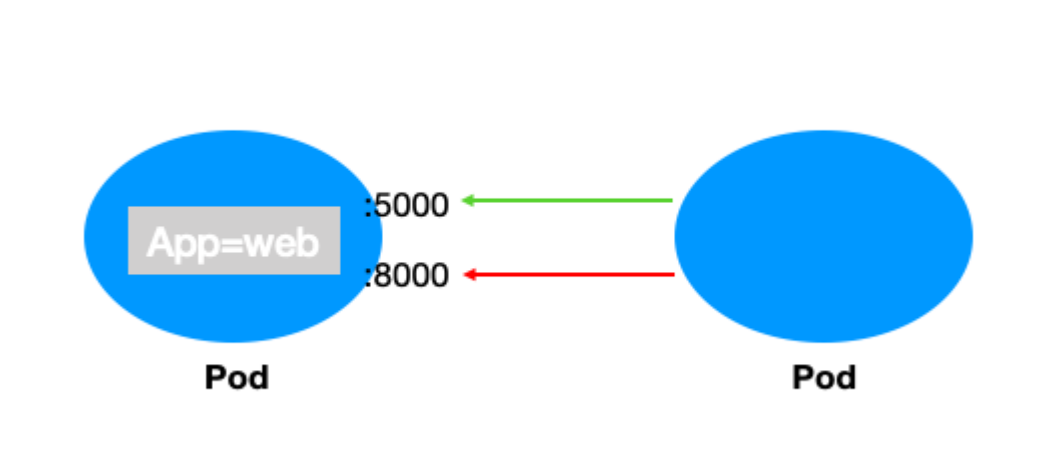
```
kubectl delete pod web
kubectl delete service web
kubectl delete pod web1
kubectl delete service web1
Disable the network policy in the console// (This can also be done by running `kube
```

©2013-2022 Tencent Cloud. All rights reserved.

Scenario 7. Set to allow access to a Pod only through the specified port

Policy description

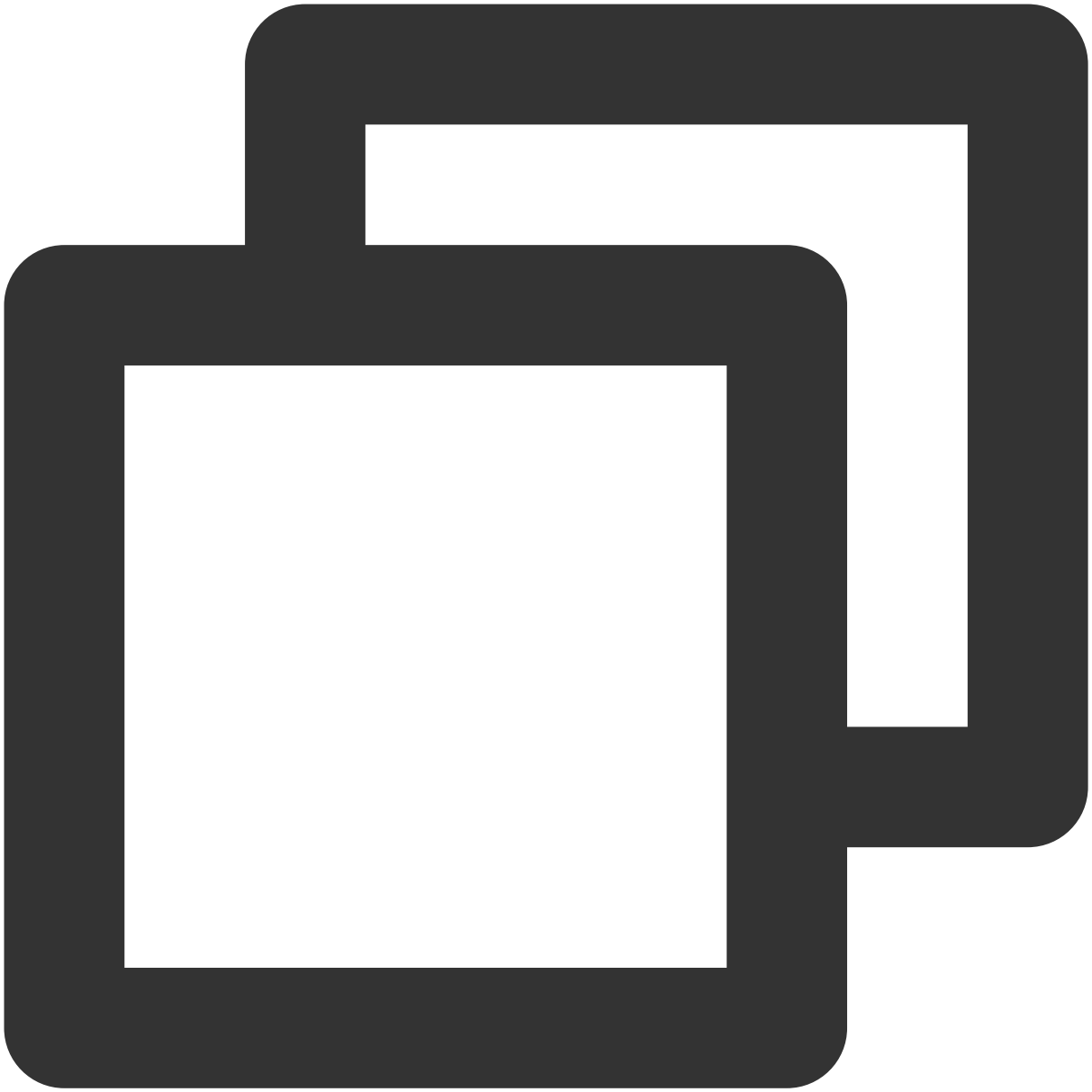
Set to allow access to the application with the `app=web` label only from TCP port 5000 and reject requests from other ports (this doesn't affect UDP access).



Verification steps

1. Create a Pod application with the `app=web` label and open ports 5000 and 8000.

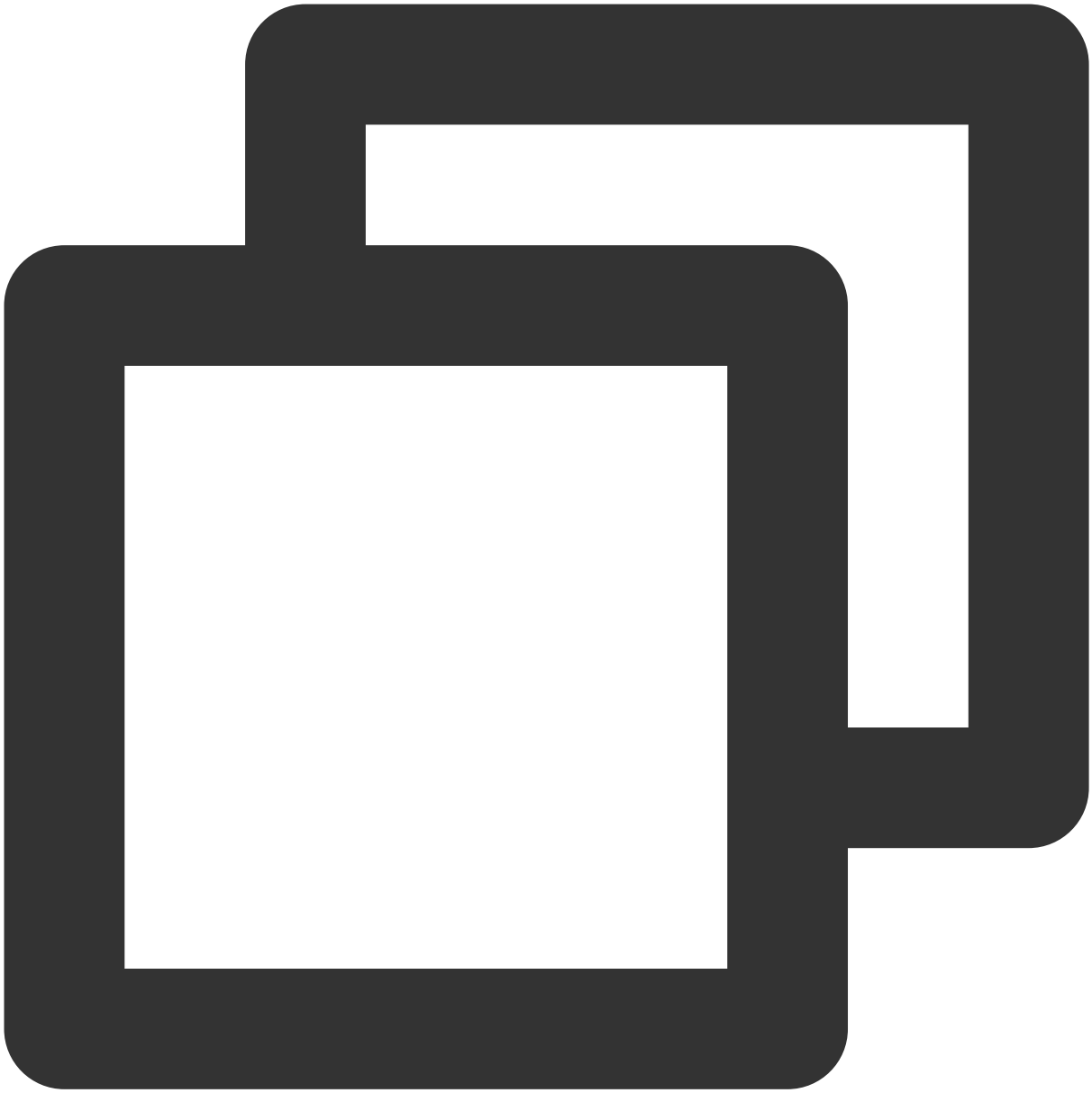
©2013-2022 Tencent Cloud. All rights reserved.



```
kubectl run web --image=ahmet/app-on-two-ports --labels app=web
pod/web created
[root@VM-0-11-centos ~]# kubectl get pod web -o wide
NAME   READY   STATUS    RESTARTS   AGE    IP            NODE          NOMINATED NO
web    1/1     Running   0          117s   172.18.0.42   172.16.0.11   <none>
```

2. Verify that ports 5000 and 8000 of the web application can be accessed by default.

©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl run  testweb --namespace=dev --rm -i -t --image=al
If you don't see a command prompt, try pressing enter.
/ # wget -qO- http://172.18.0.42:5000/metrics
http.requests=2
go.goroutines=5
go.cpus=4
/ # wget -qO- http://172.18.0.42:8000
Hello from HTTP server.
```

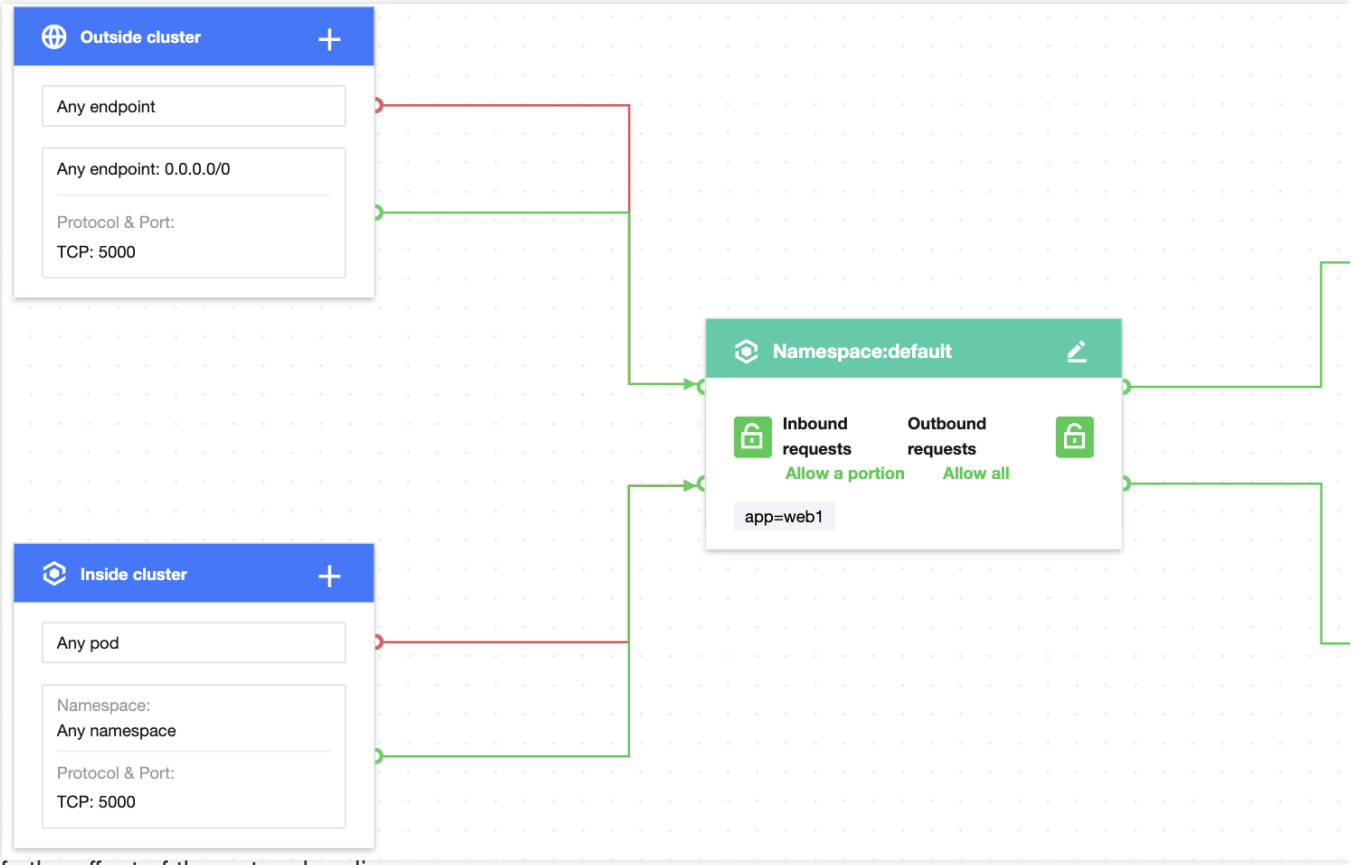
©2013-2022 Tencent Cloud. All rights reserved.

3. Create and enable the network policy.

Set the label of the protected Pod as `app=web` , allow requests only from TCP port 5000 in any namespace in the cluster, and allow requests only from TCP port 5000 at any endpoint outside the cluster as shown below:

Note:

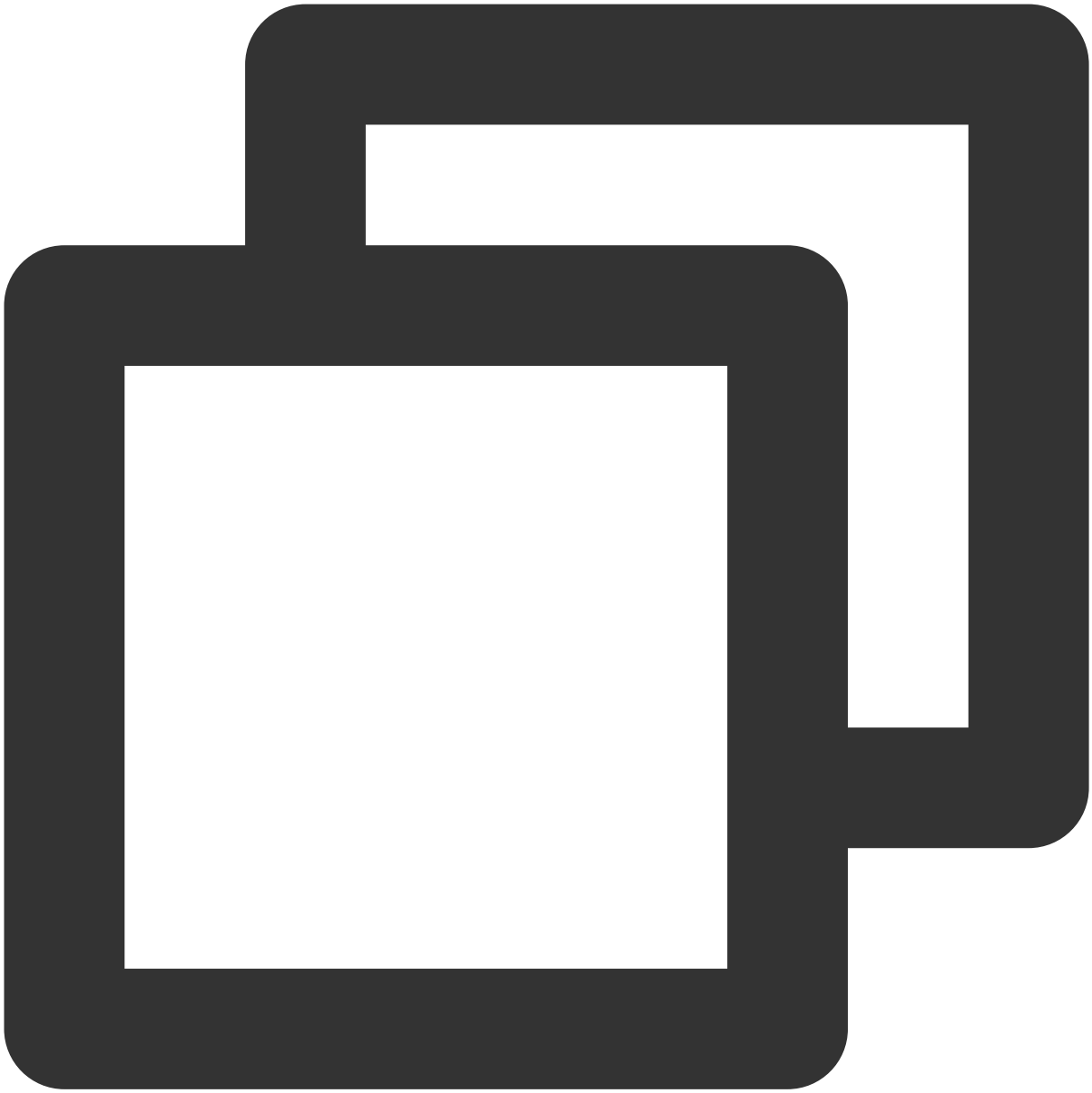
To set access only through the specified UDP port, you need to add UDP port rules.



4. Verify the effect of the network policy.

Port 5000 of the web application can be accessed, but port 8000 of the web application cannot.

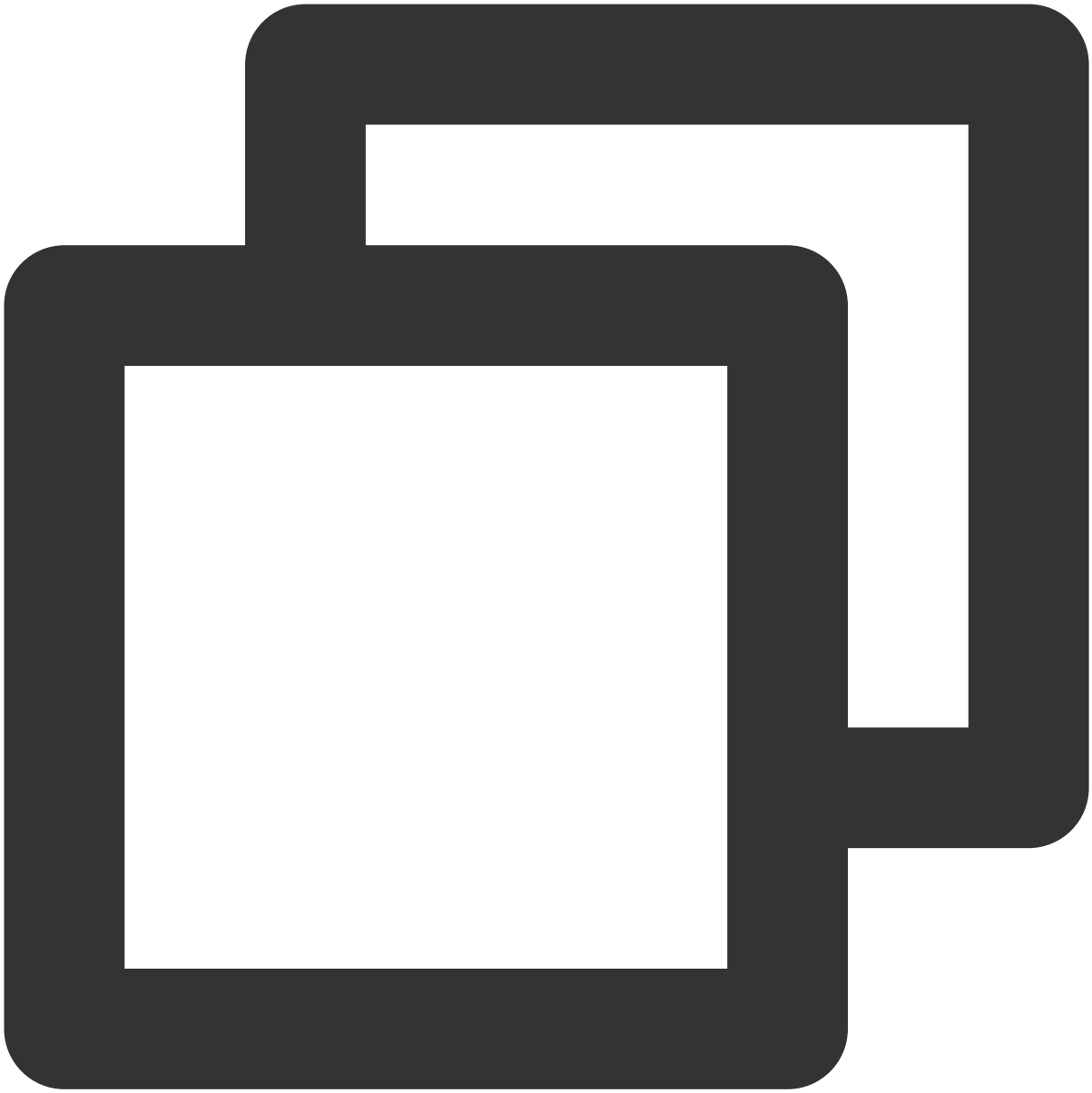
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl run  testweb --namespace=dev --rm -i -t --image=al
If you don't see a command prompt, try pressing enter.
/ # wget -qO- http://172.18.0.42:5000/metrics
http.requests=2
go.goroutines=5
go.cpus=4
/ # wget -qO- http://172.18.0.42:8000
wget: can't connect to remote host (172.18.0.42): Connection refused
```

5. Clear the environment.

©2013-2022 Tencent Cloud. All rights reserved.



```
kubectl delete pod web
kubectl delete service web
Disable the network policy in the console// (This can also be done by running `kube
```

Scenario 8. Set to allow access to a Pod only from the specified IP

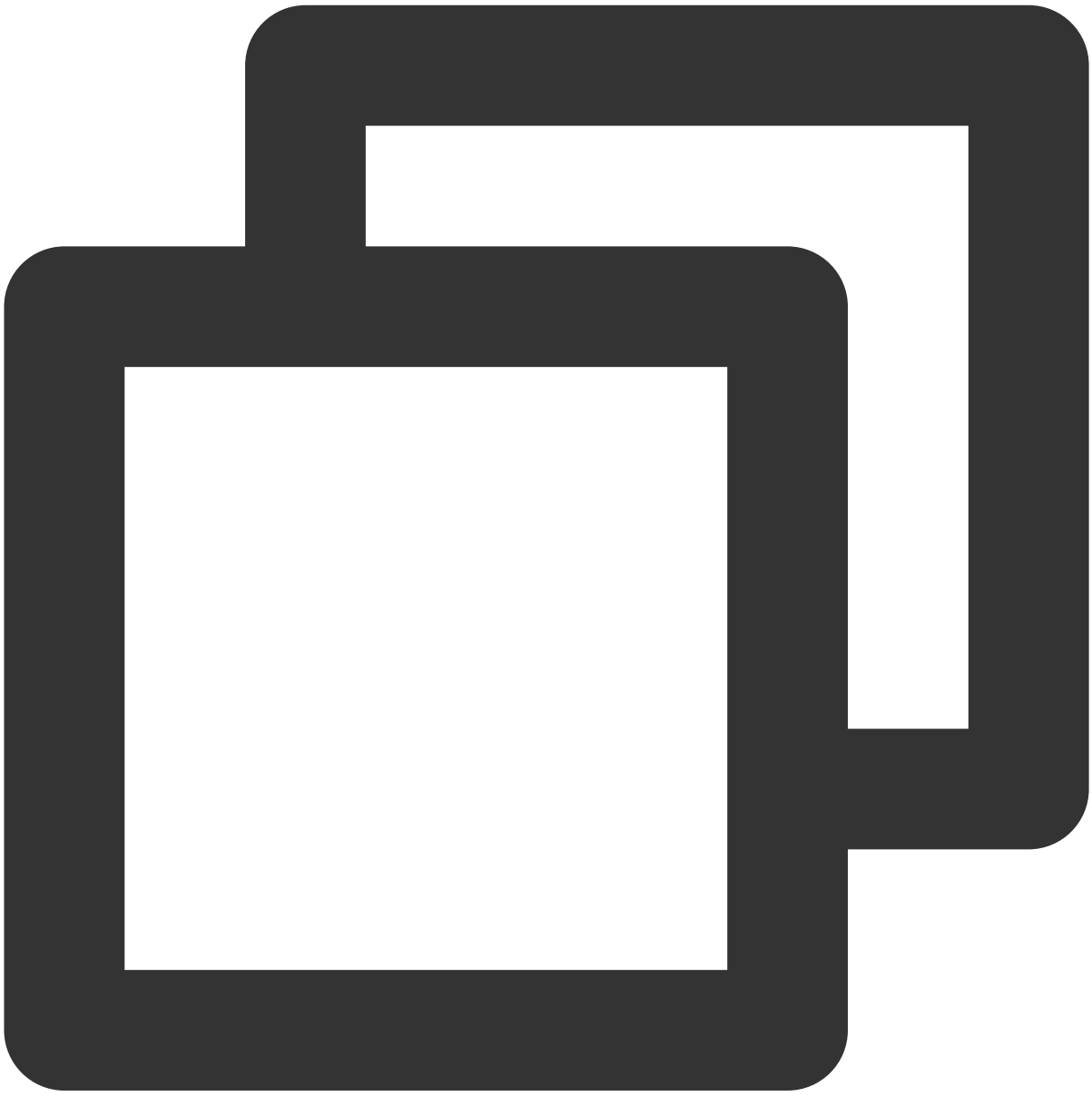
Policy description

©2013-2022 Tencent Cloud. All rights reserved.

Set to allow access to the Pod with the `app=web` label only from the specified IP.

Verification steps

1. Create a Pod application with the `app=web` label and start the service.

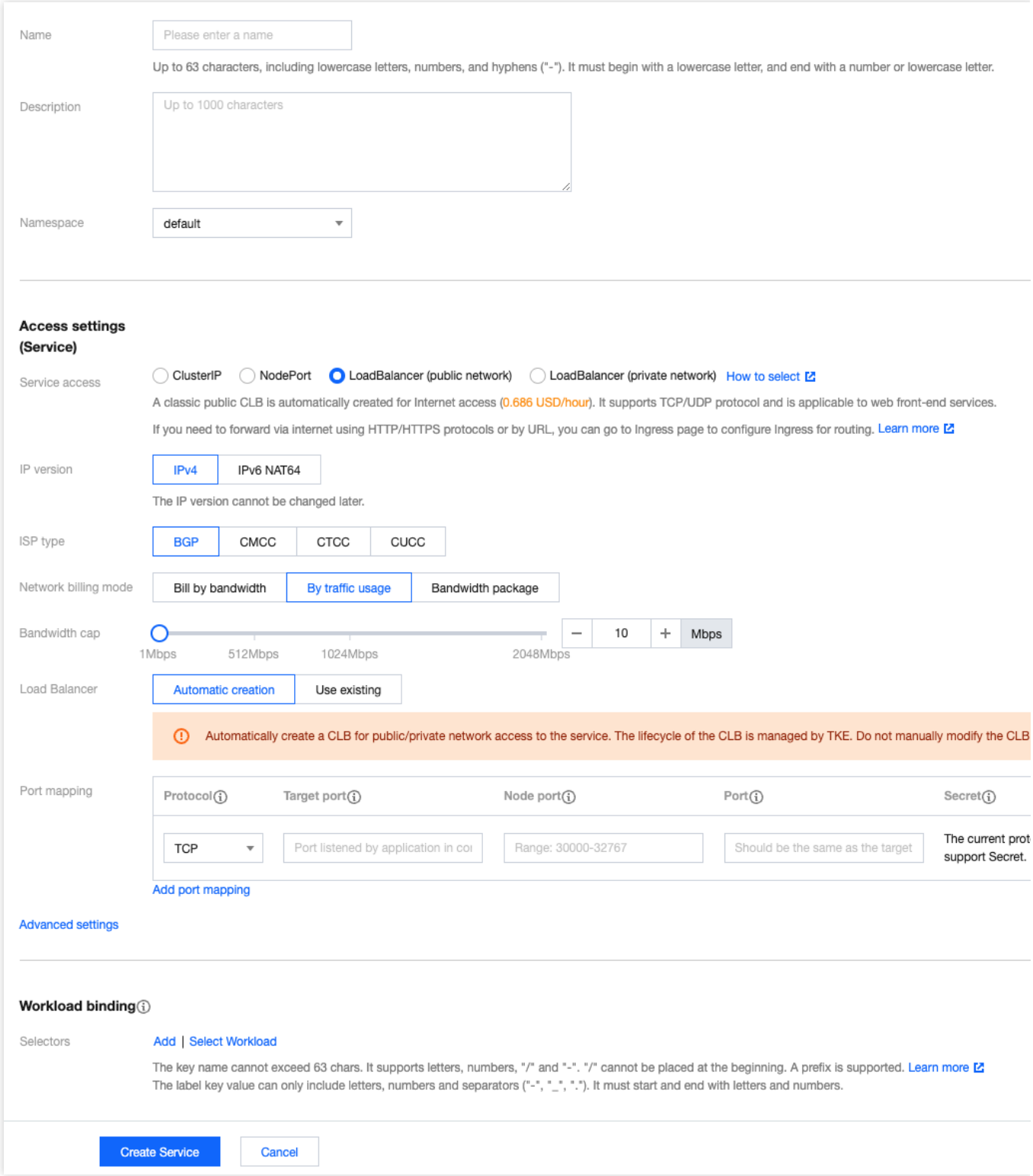


```
[root@VM-0-11-centos ~]# kubectl run web --namespace default --image=nginx --labels
pod/web created
[root@VM-0-11-centos ~]# kubectl get svc web
NAME    TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)    AGE
web     ClusterIP   172.18.255.217   <none>        80/TCP     6s
```

©2013-2022 Tencent Cloud. All rights reserved.

2. Bind the public network IP to the web service.

2.1 On the **Cluster** page, create the public network LB service and bind the web service. For more information, see Basic Features.



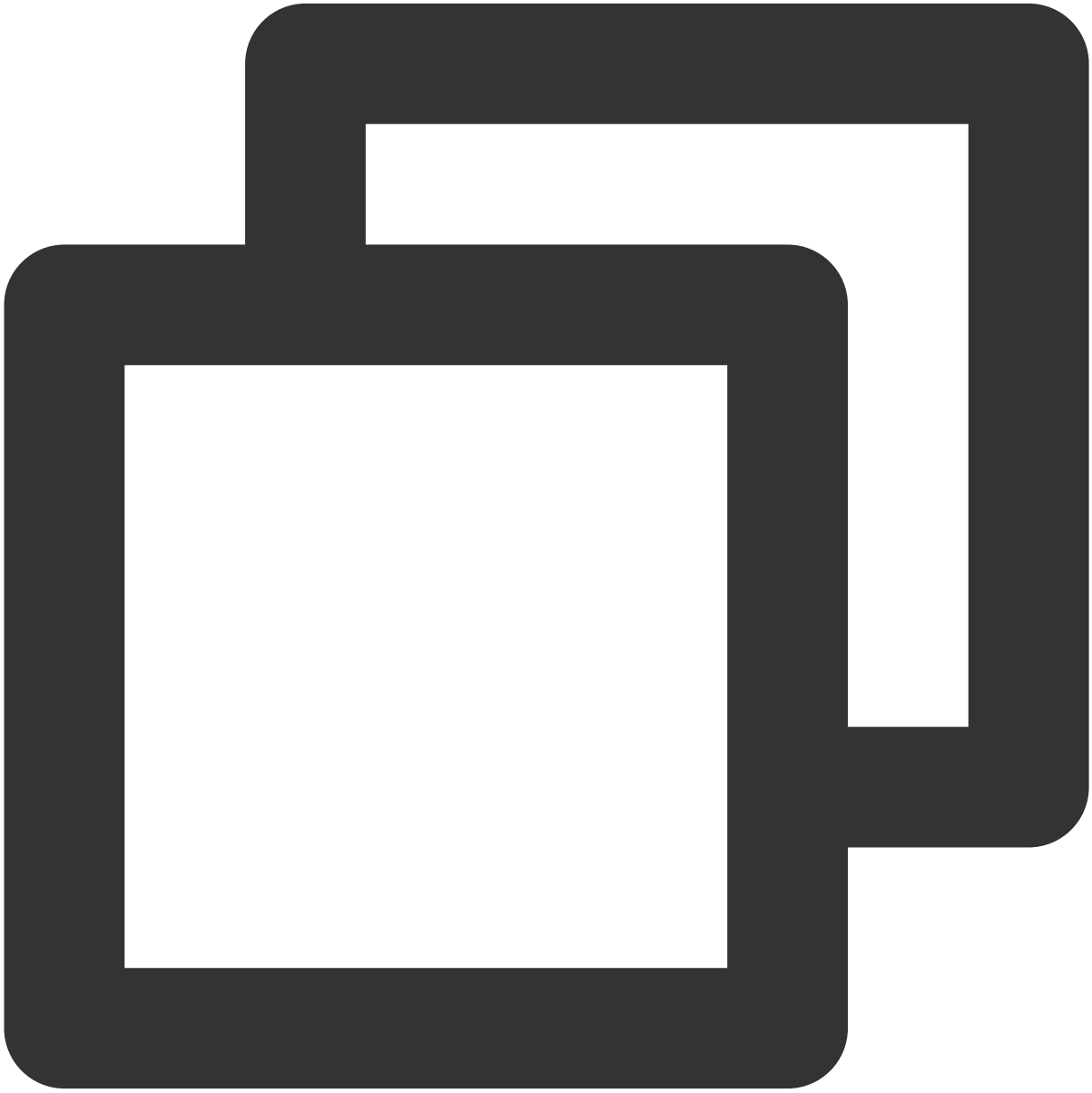
2.2 The public network LB is created successfully, and the access address is `106.xx.xx.61`.

©2013-2022 Tencent Cloud. All rights reserved.

Name	Labels	Type	Selector	IP address	Time created
[redacted]	component:apiserver provider:kubernetes	ClusterIP	-	-(IPV4) [redacted]1(Service IP)	2022-11-28 1

3. Verify that the web application can be accessed from any IP by default.

Any Pod can access the web application.

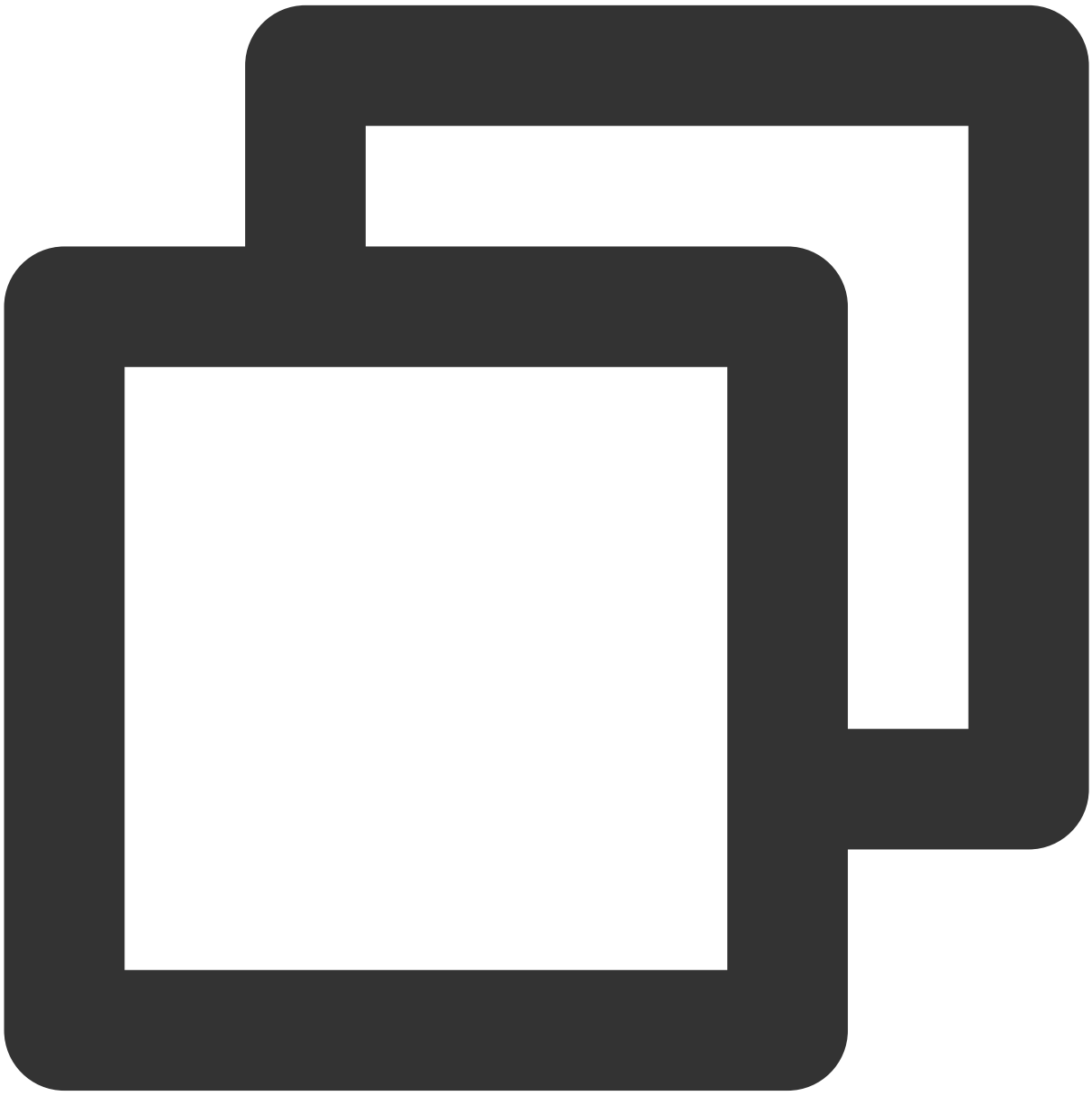


```
[root@VM-0-11-centos ~]# kubectl run --rm -it --image=alpine testweb -- sh
If you don't see a command prompt, try pressing enter.
/ # wget -qO- http://web.default
```

©2013-2022 Tencent Cloud. All rights reserved.

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

The web application can be accessed from any IP.



```
 ~/workspace/networkpolicy_test   curl cip.cc
IP: 113.xx.xx.70
Address: Shenzhen, Guangdong Province, China
ISP: China Telecom
```

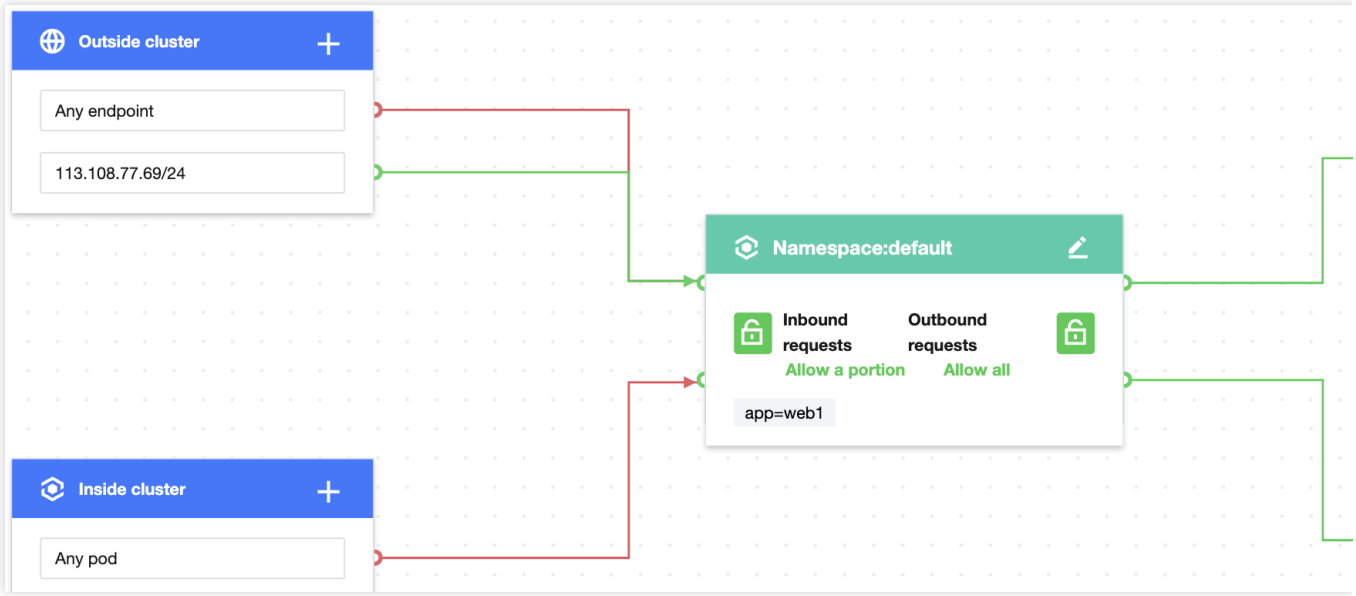
©2013-2022 Tencent Cloud. All rights reserved.

```
Data 2: Shenzhen, Guangdong Province | Tencent Cloud
Data 3: Shenzhen, Guangdong Province, China | China Telecom
URL: http://www.cip.cc/113.xx.xx.70
 ~/workspace/networkpolicy_test   curl 106.xx.xx.61
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...

[root@VM-0-11-centos ~]# curl cip.cc
IP: 175.xx.xx.176
Address: China China
Data 2: Guangzhou, Guangdong Province | Tencent Cloud
Data 3: Xiamen, Fujian Province, China | Tencent
URL: http://www.cip.cc/175.xx.xx.176
[root@VM-0-11-centos ~]# curl --connect-timeout 5 106.xx.xx.61
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

4. Create and enable the network policy.

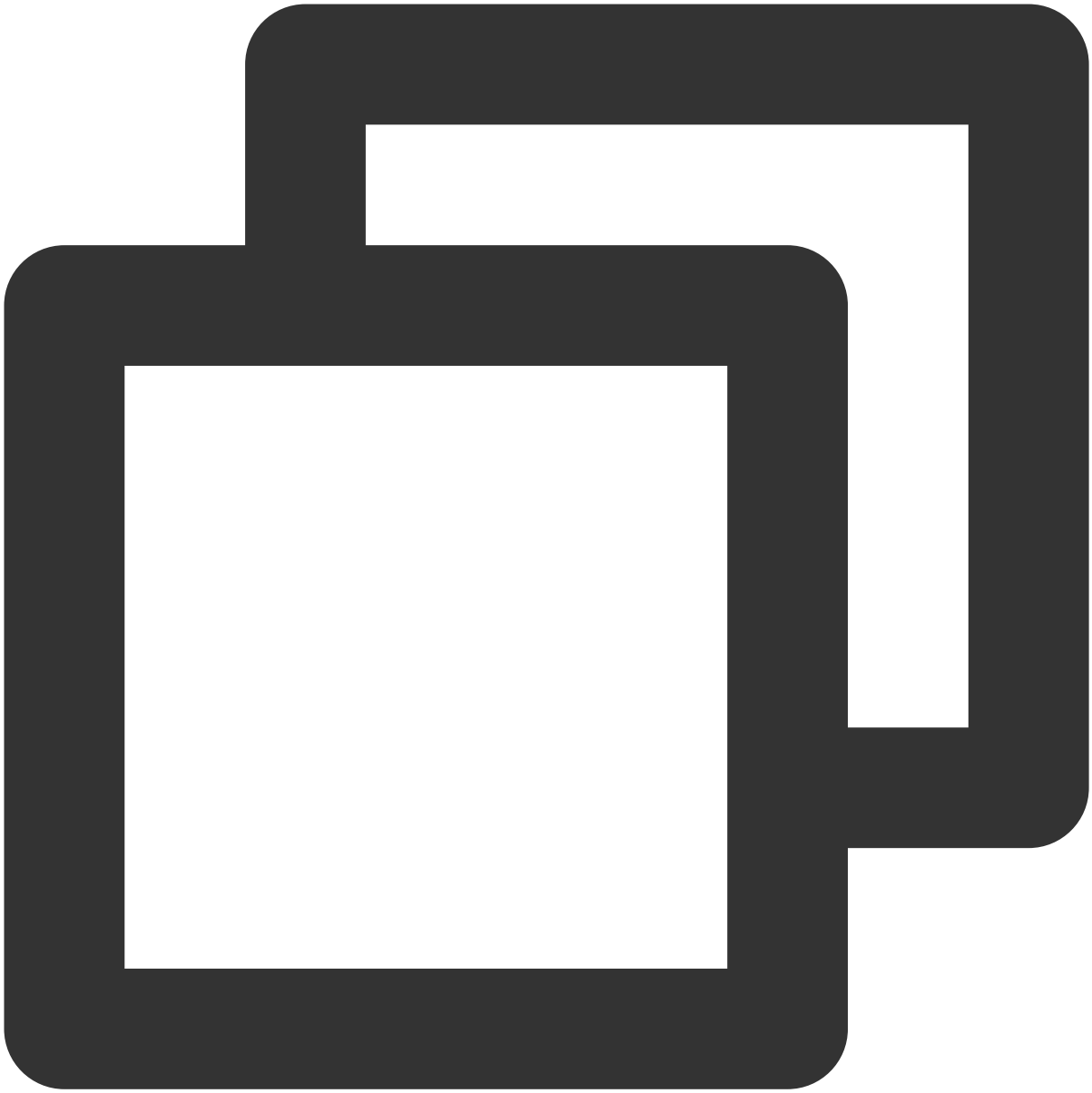
Set the label of the protected Pod as `app=web` and allow requests only from the specified IP outside the cluster as shown below:



5. Verify the effect of the network policy.

The web application can be accessed only from the specified IP.

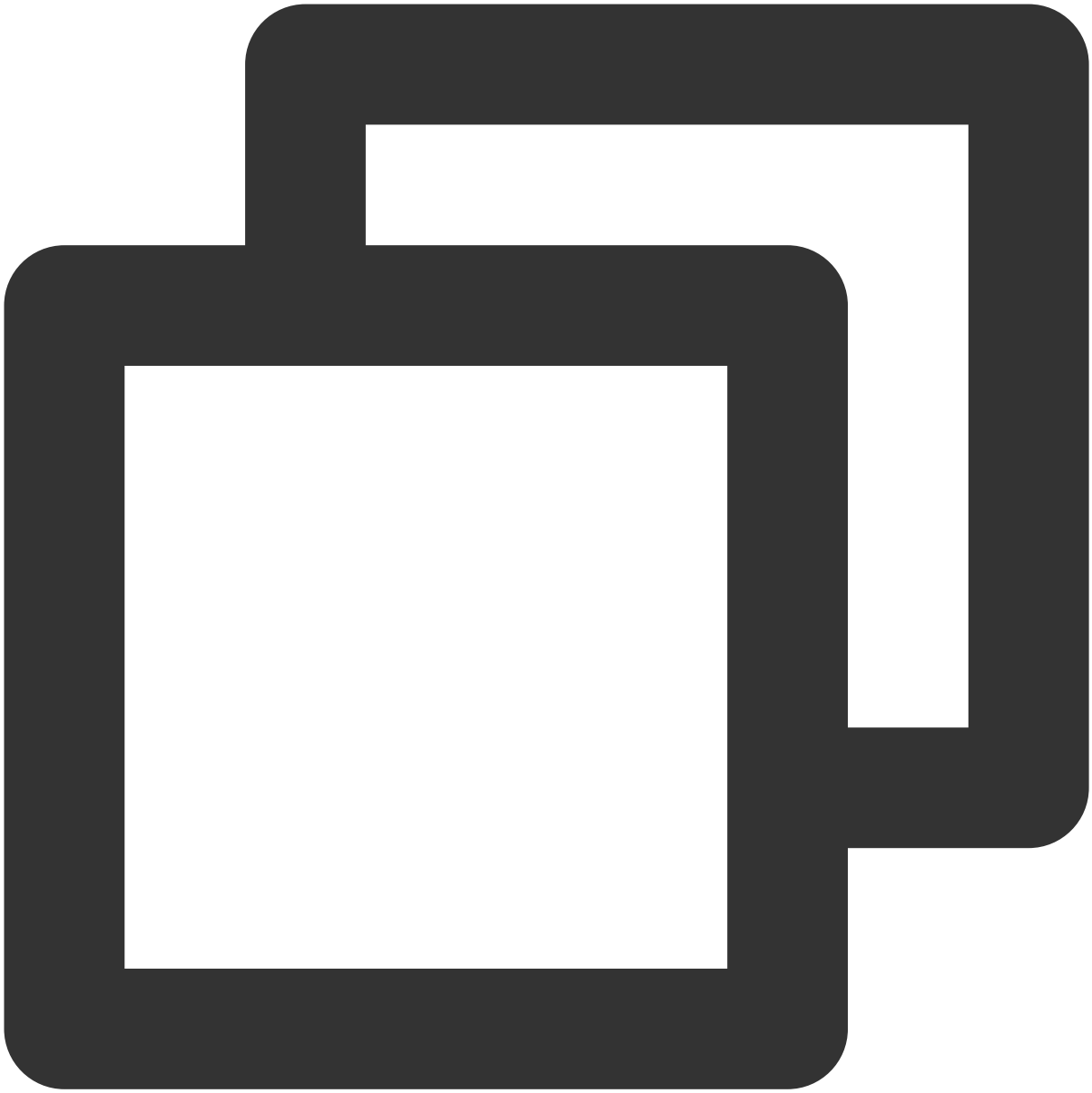
©2013-2022 Tencent Cloud. All rights reserved.



```
   ~/workspace/networkpolicy_test   curl 106.xx.xx.61
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

The web application cannot be accessed from other IPs.

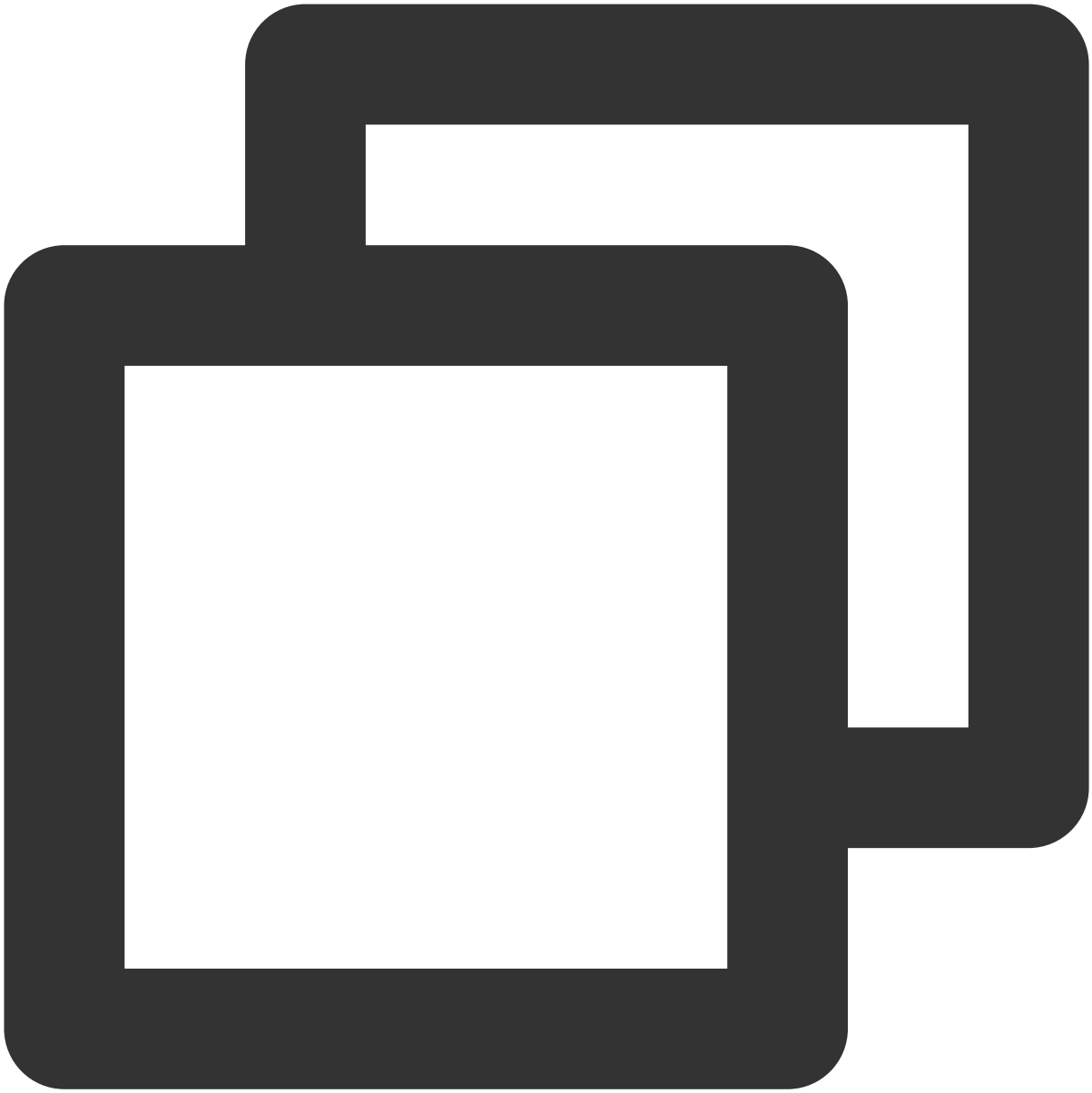
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# curl cip.cc
IP: 175.xx.xx.176
Address: China China
Data 2: Guangzhou, Guangdong Province | Tencent Cloud
Data 3: Xiamen, Fujian Province, China | Tencent
URL: http://www.cip.cc/175.xx.xx.176
[root@VM-0-11-centos ~]# curl --connect-timeout 5 106.xx.xx.61
curl: (28) Connection timed out after 5001 milliseconds
```

6. Clear the environment.

©2013-2022 Tencent Cloud. All rights reserved.



```
kubectl delete pod web
kubectl delete service web
Disable the network policy in the console// (This can also be done by running `kube
```

Scenario 9. Set to allow a Pod to access only the specified port and IP

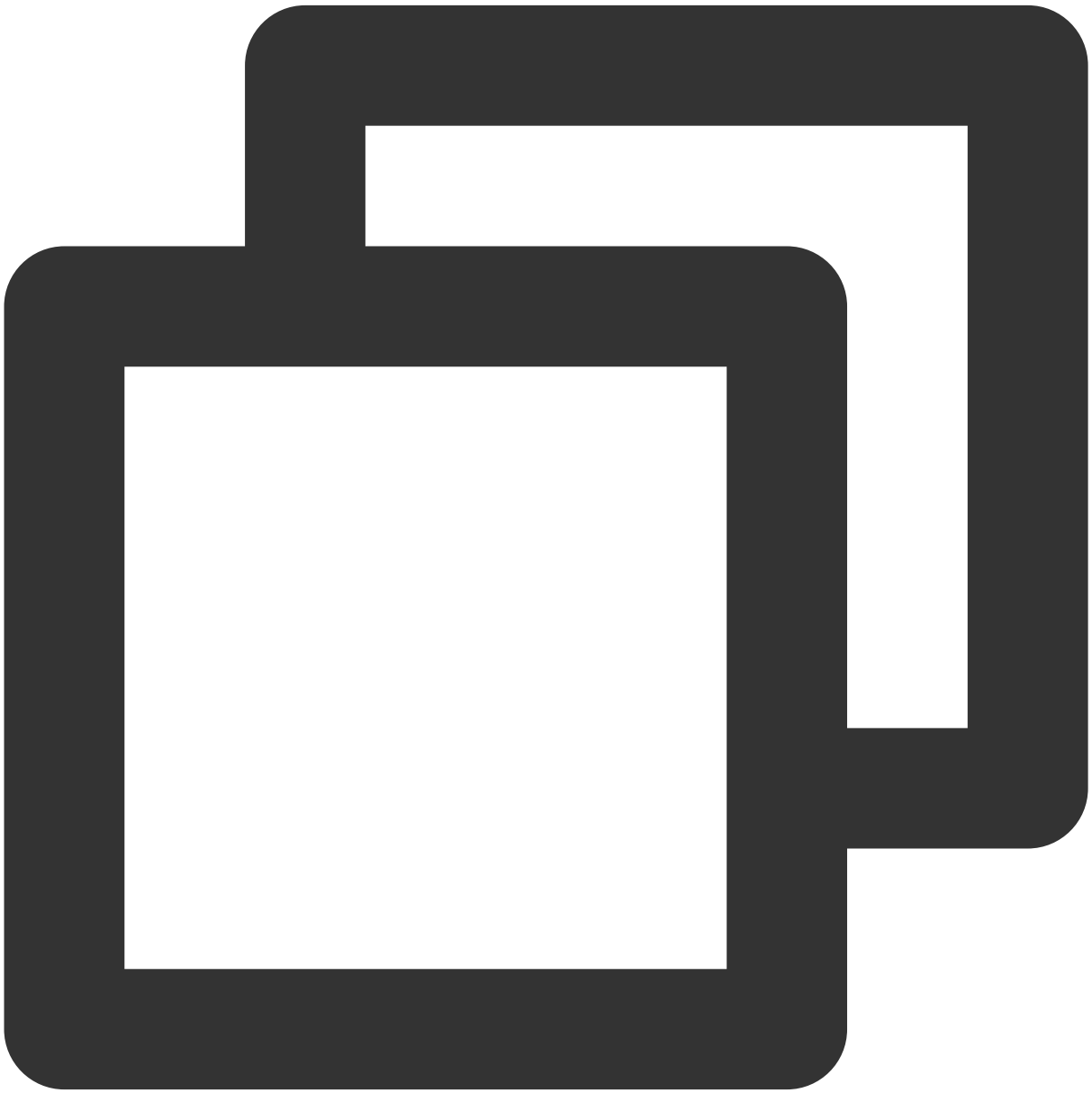
©2013-2022 Tencent Cloud. All rights reserved.

Policy description

Set to allow the Pod with the `app=web` label to access only port 80 of the Pod with the `app=db` label and the specified IP.

Verification steps

1. Create a Pod application with the `app=web` label and another with the `app=db` label and start the services.



```
[root@VM-0-11-centos ~]# kubectl run web --image=nginx  --labels=app=web --expose -
service/web created
pod/web created
```

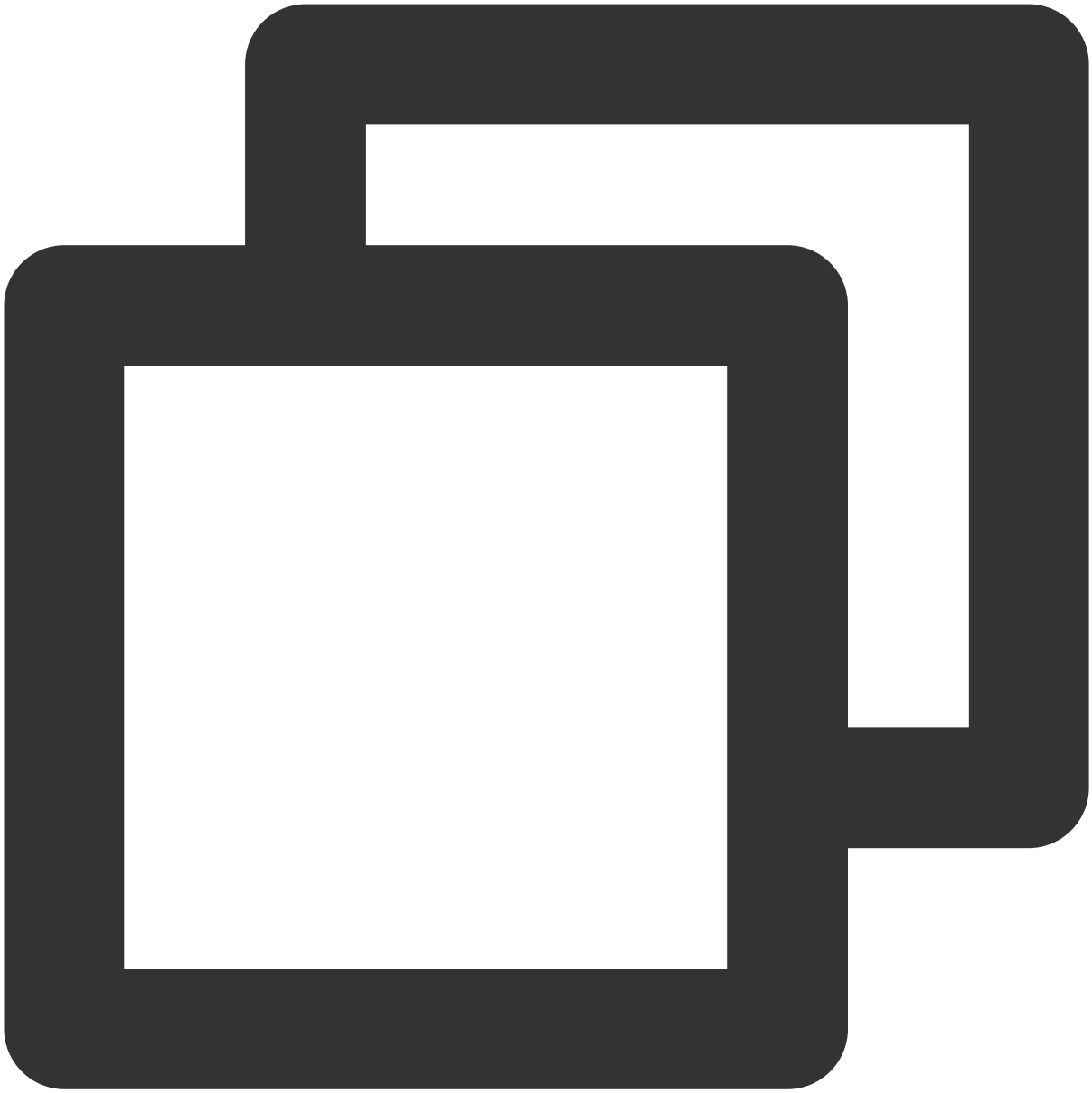
©2013-2022 Tencent Cloud. All rights reserved.

```
[root@VM-0-11-centos ~]# kubectl get svc web
NAME   TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)   AGE
web    ClusterIP   172.18.255.217   <none>        80/TCP    5s

[root@VM-0-11-centos ~]# kubectl run db --image=nginx --port 80 --expose --labels a
service/db created
pod/db created
[root@VM-0-11-centos ~]# kubectl get svc db
NAME   TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)   AGE
db     ClusterIP   172.18.254.45   <none>        80/TCP    6s
```

2. Verify that the web service can access any Pod application and any IP by default.

©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl exec -it web -- sh
# curl 172.18.254.45
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
# curl 220.181.38.148:80
<html>
<meta http-equiv="refresh" content="0;url=http://www.baidu.com/">
</html>
```

©2013-2022 Tencent Cloud. All rights reserved.

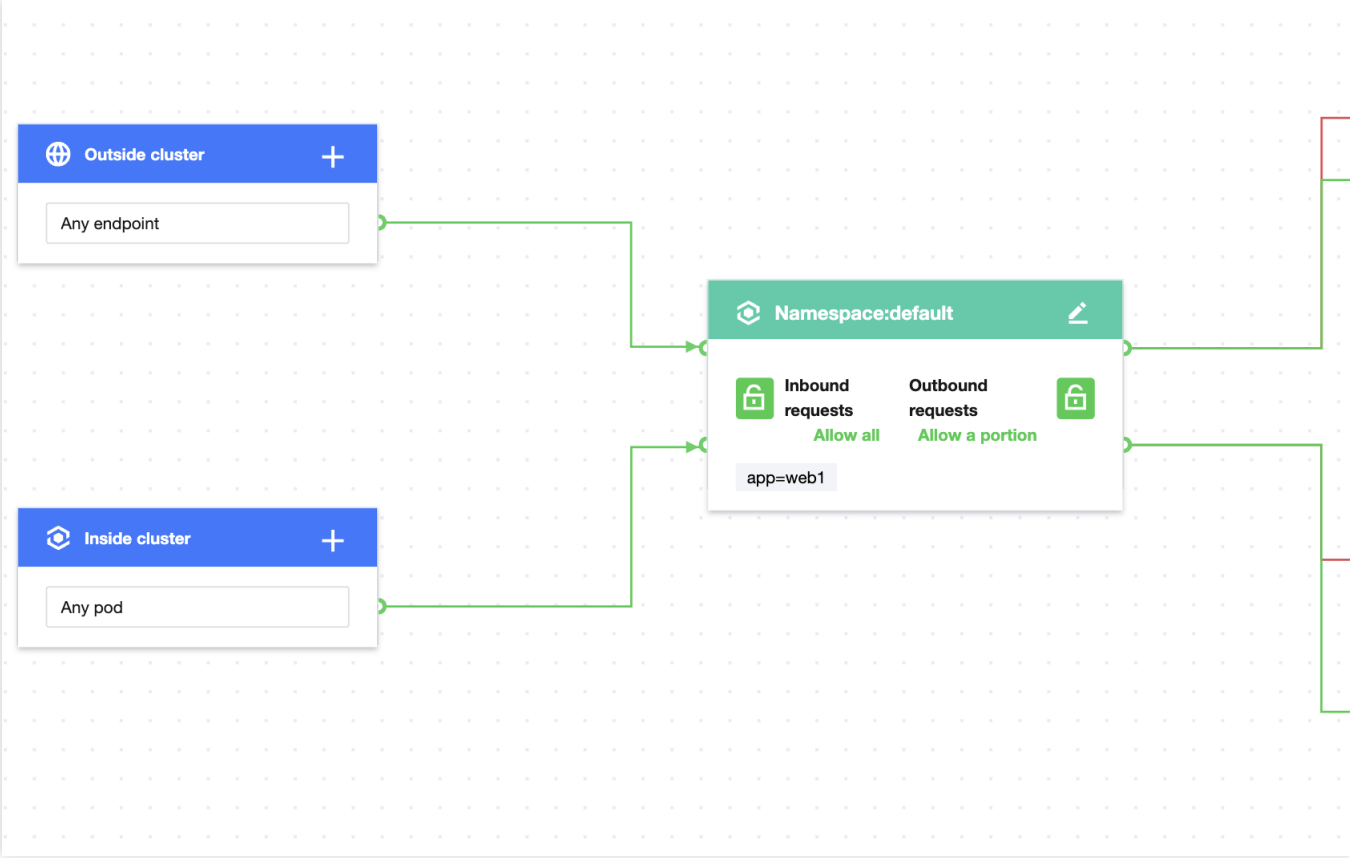
```
# curl 103.41.167.234:80
<!DOCTYPE html>
<html lang="zh">
...
```

3. Create and enable the network policy.

Set the label of the protected Pod as `app=web` , allow outbound requests only from the specified IP outside the cluster, and allow TCP requests only through port 80 of the Pod with the `app=db` label in any namespace as shown below:

Note:

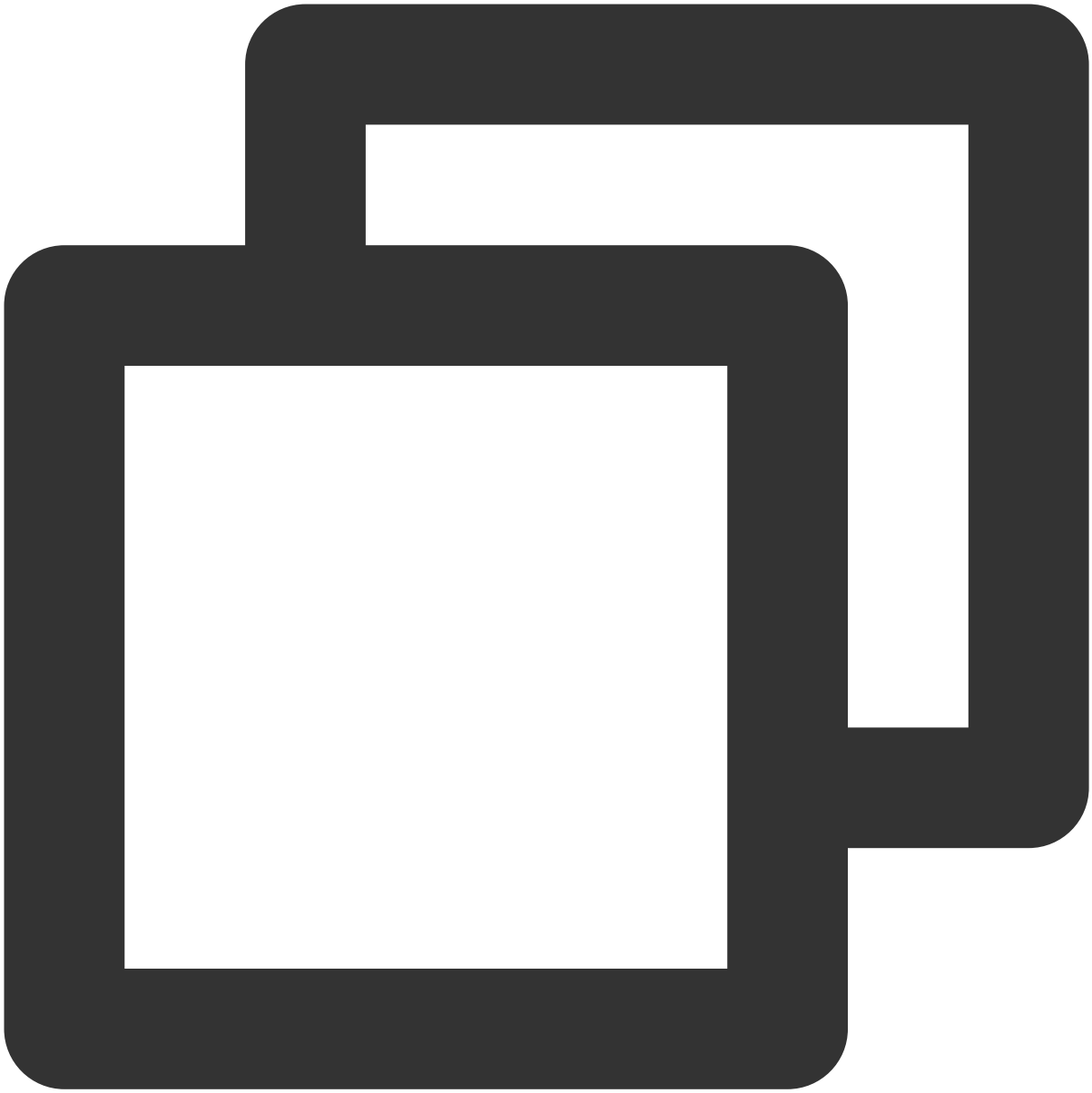
This policy doesn't take effect for UDP, as it is not configured.



4. Verify the effect of the network policy.

The web service can access port 80 of the service with the `app=db` label.

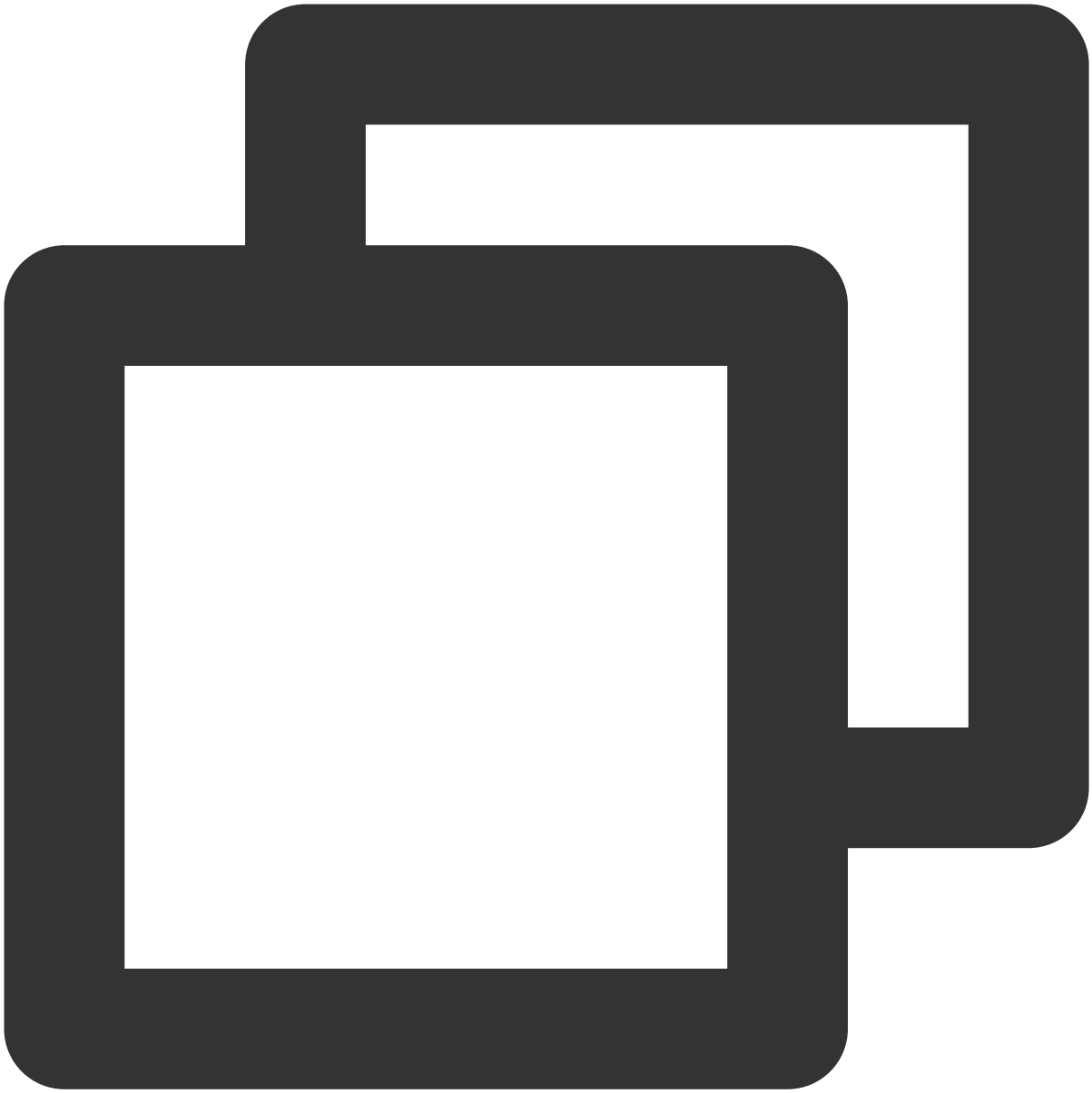
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl exec -it web -- sh
# curl 172.18.254.45:80
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
...
```

The web service cannot access other ports of the service with the `app=db` label.

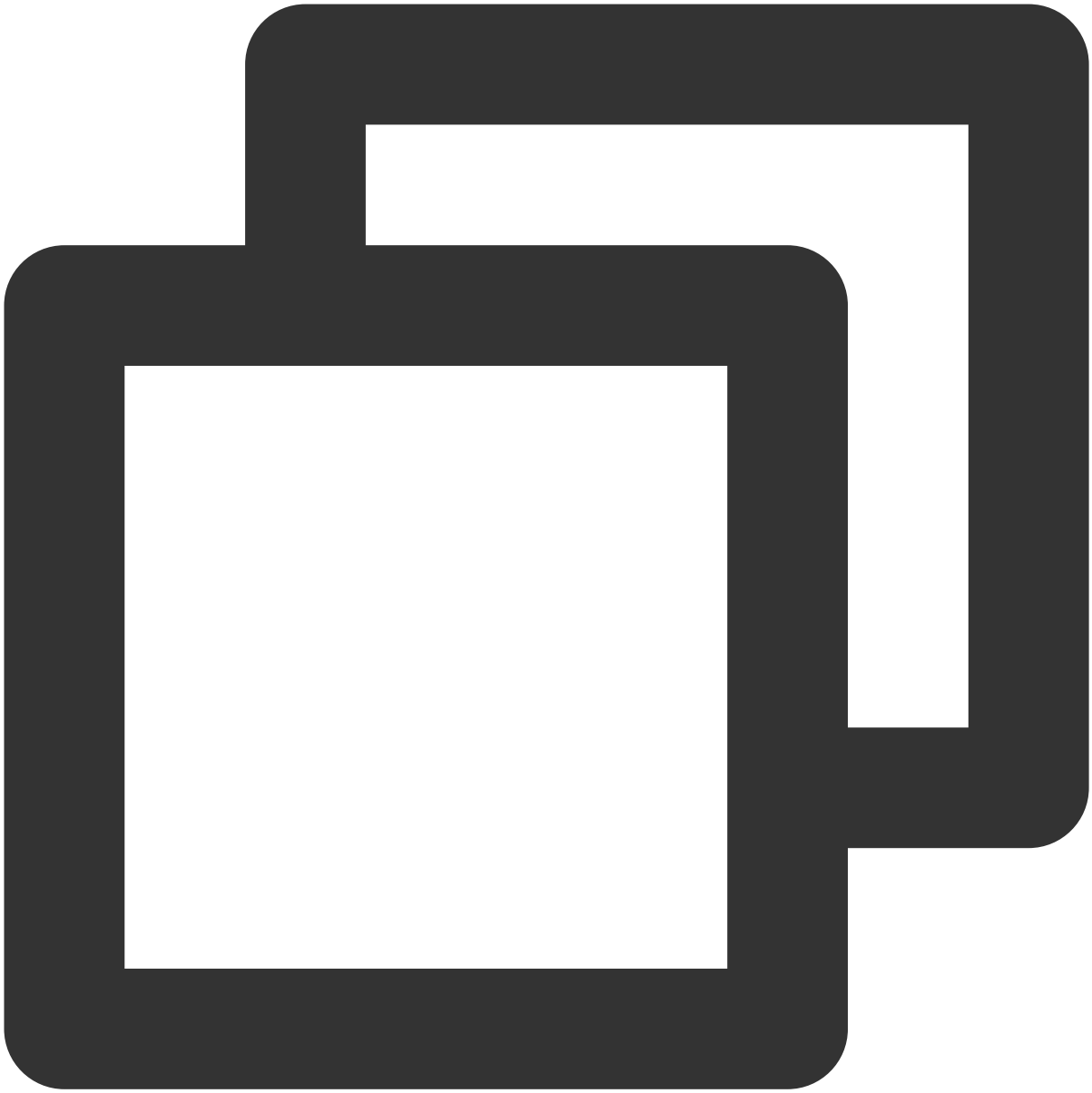
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl exec -it web -- sh
# curl 172.18.254.45:81
curl: (7) Failed to connect to 172.18.254.45 port 81: Connection refused
```

The web service cannot access other Pod services.

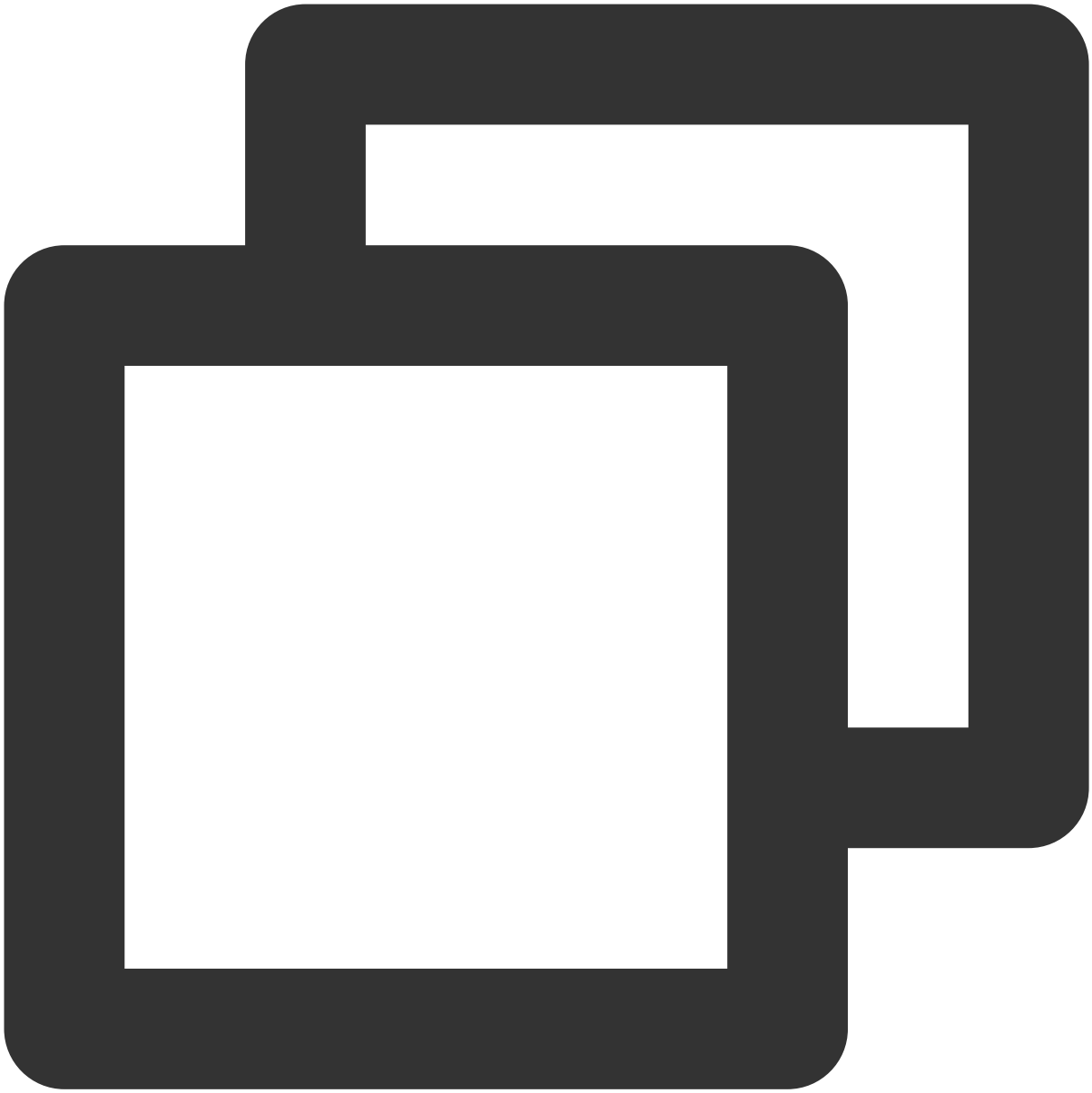
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl get svc web1
NAME   TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)   AGE
web1   ClusterIP   172.18.255.39   <none>        80/TCP    55m
[root@VM-0-11-centos ~]# kubectl exec -it web -- sh
# curl 172.18.255.39:80
curl: (7) Failed to connect to 172.18.255.39 port 80: Connection refused
```

The web service can access the specified IP.

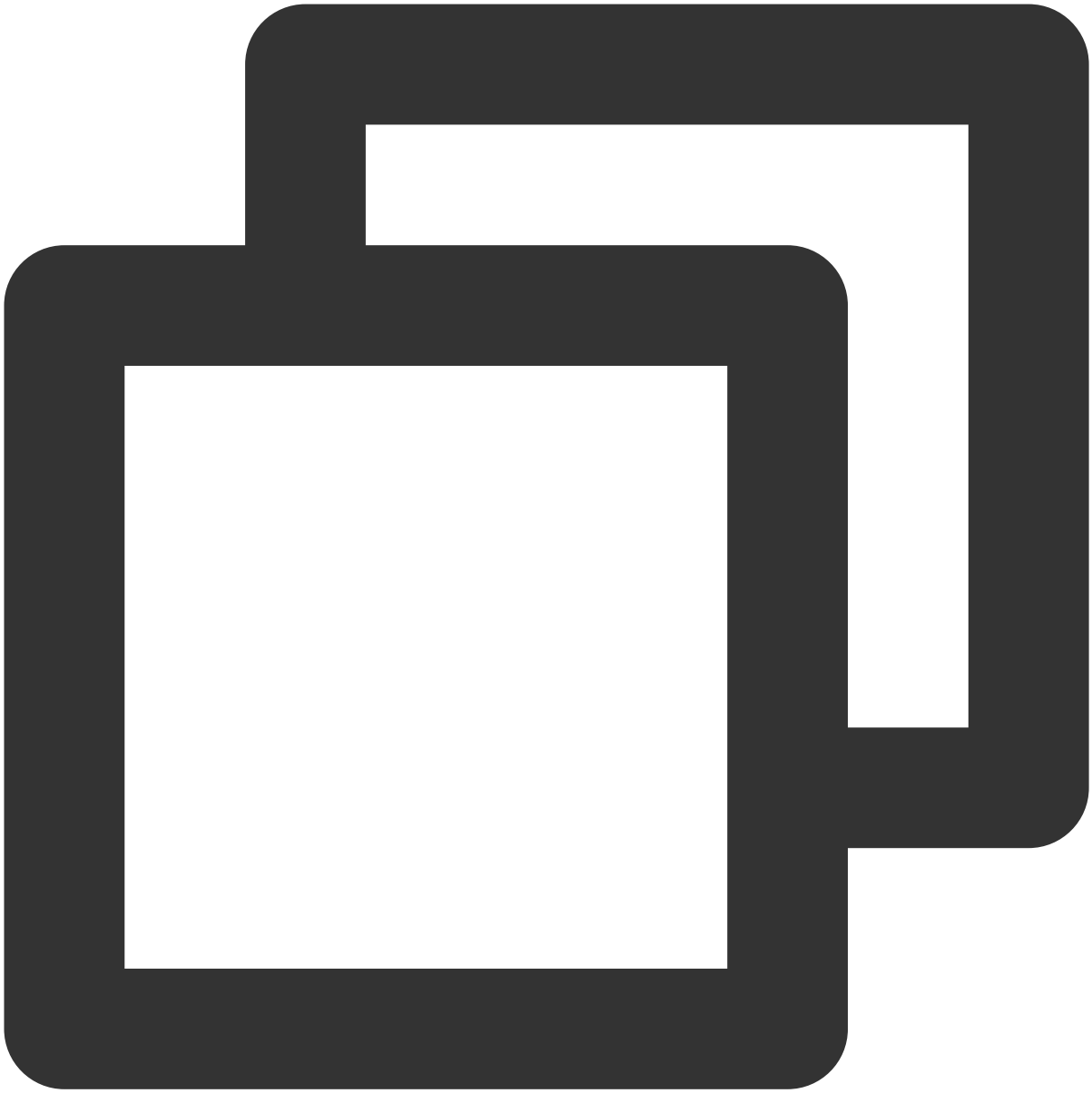
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl exec -it web -- sh
# curl 220.181.38.148:80
<html>
<meta http-equiv="refresh" content="0;url=http://www.baidu.com/">
</html>
```

The web service cannot access other IPs.

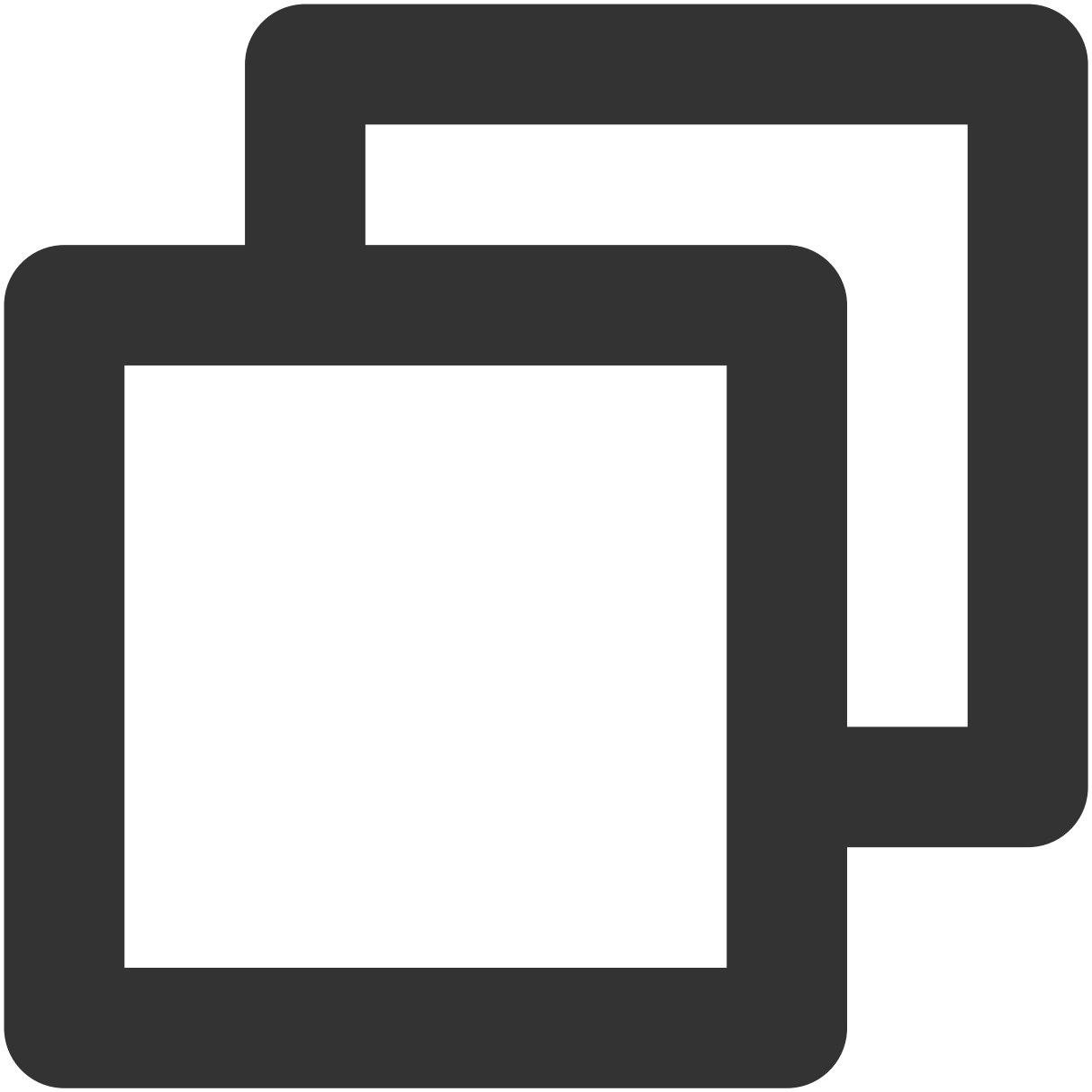
©2013-2022 Tencent Cloud. All rights reserved.



```
[root@VM-0-11-centos ~]# kubectl exec -it web -- sh
# curl 103.xx.xx.234
curl: (7) Failed to connect to 103.xx.xx.234 port 80: Connection refused
```

4. Clear the environment.

©2013-2022 Tencent Cloud. All rights reserved.



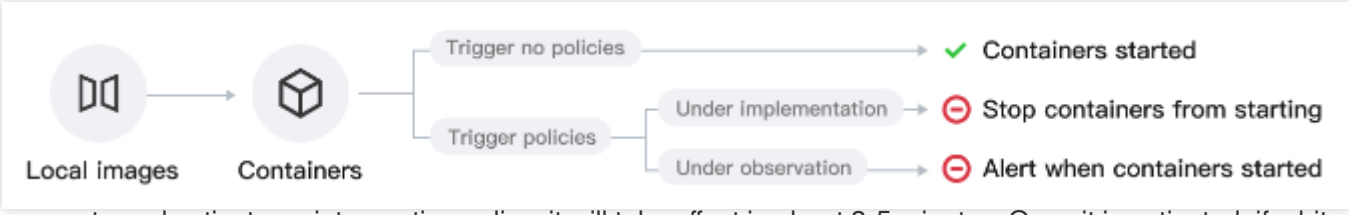
```
kubectl delete pod web
kubectl delete service web
kubectl delete pod db
kubectl delete service db1
Disable the network policy in the console// (This can also be done by running `kube
```

©2013-2022 Tencent Cloud. All rights reserved.

Image Interception Policies

Last updated：2024-08-13 17:12:06

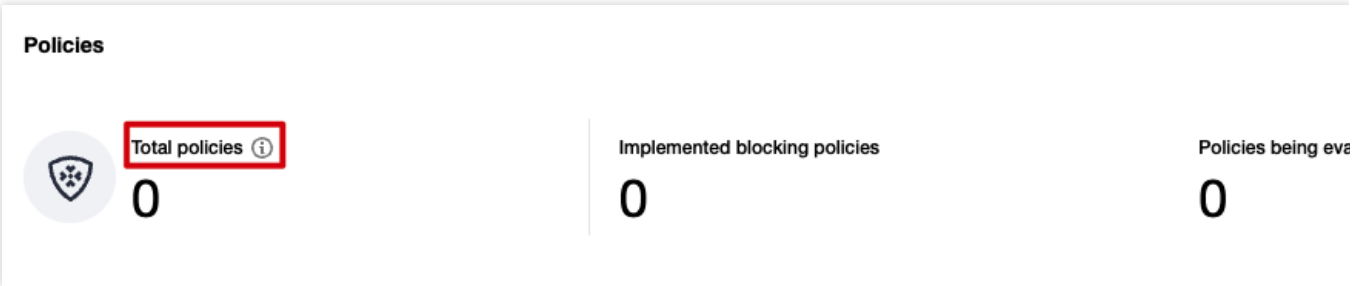
Users can configure alarms and interception policies on the image interception policies page. The image interception policy allows you to intercept the startup of containers with images that have critical security issues in clusters of multiple clouds (precondition: node host has installed TCSS Agent), preventing malicious images from running container services.



After you create and activate an interception policy, it will take effect in about 3-5 minutes. Once it is activated, if a hit risk image attempts to start a container, the system will alarm or intercept the container startup and report the interception records, based on the configured policy's alarm and interception requirements.
Currently supported intercepted image types: Images with critical and high-risk vulnerabilities, Trojan viruses, and sensitive information risks, as well as images started in privileged mode.
Privileged image interception supports only one rule configured. To modify the range of intercepted images, you can edit the configured rule.

Viewing Policy Overview

After users have configured the alarm and interception policies, the system will count the total number of enabled policies, as well as the number of included effective interception policies and observation period policies.



Viewing Event Overview

Once the user configures the image startup interception policy and sets it to take immediate effect, attempts to start containers using targeted risky images will be intercepted in real-time, with the image startup actions reported and

©2013-2022 Tencent Cloud. All rights reserved.

recorded. If the policy includes an observation period, during which only alarms are issued without interception, attempts to start containers using targeted risky images will trigger real-time reporting of the image startup actions. In both scenarios, event logs will be generated.

In the event overview, daily statistics will be provided for both image startup interception events and events where only alarms were triggered. Trend charts for both types of events over the past 7 days and the current total number of events will be displayed. Click **View event details** to navigate to **Image Risk Management** >**Image Interception Events** page to view details of the image interception events.

Creating a Policy

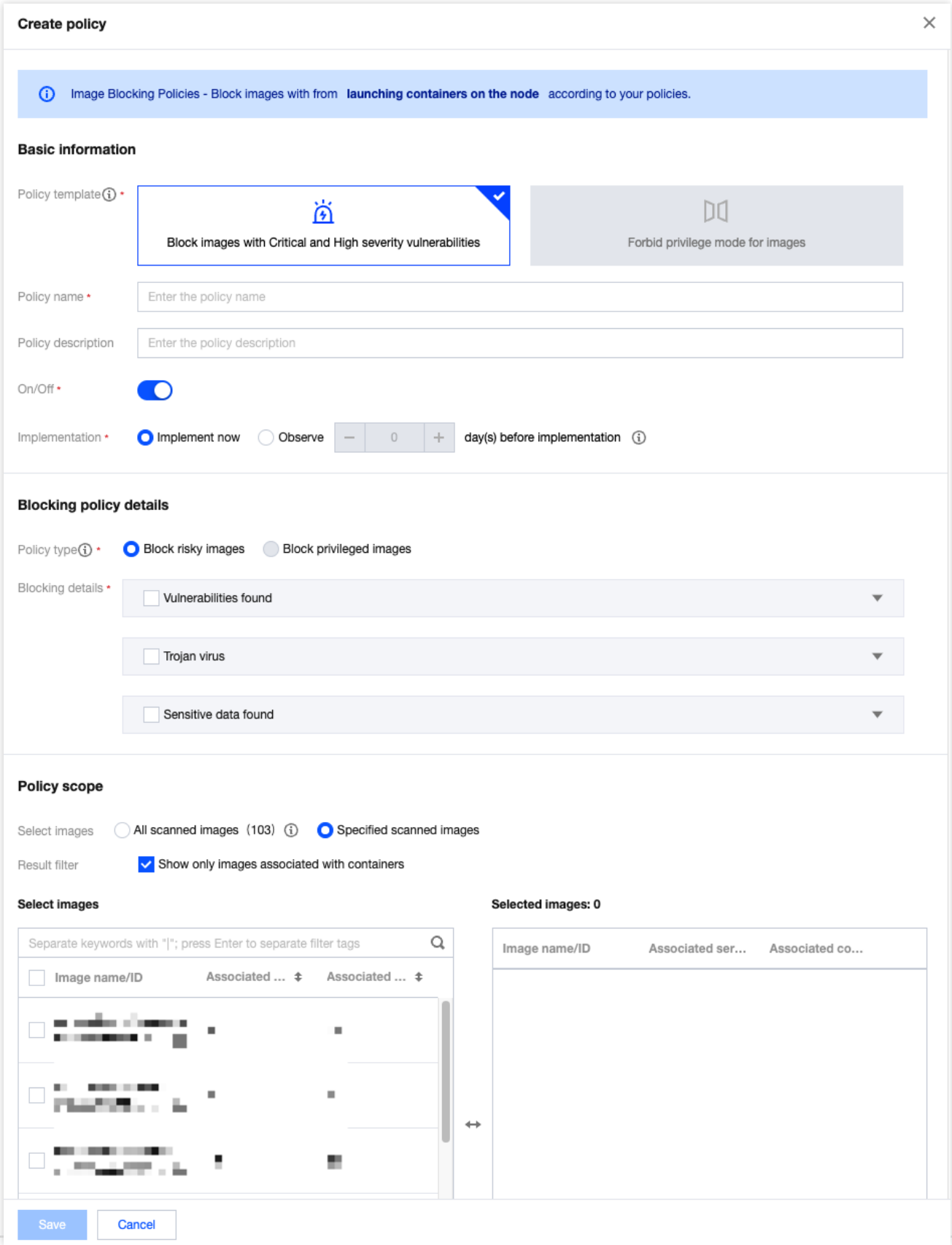
1. Log in to the TCSS console. In the left sidebar, choose **Policy Management** > **Image Interception Policy**.
2. On the image interception policy page, click **Create Policy**, configure the relevant parameters, and click **OK**.

Note

According to the set policy, the startup of containers on the node will be intercepted. Image interception may affect the business. Proceed with caution.

Create New Risk Image Interception Policy

©2013-2022 Tencent Cloud. All rights reserved.



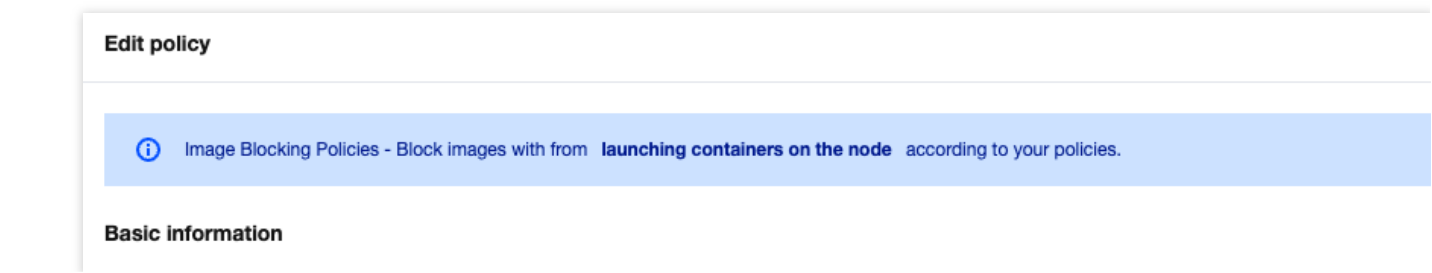
Parameter Category	Parameter Name	Parameter Details
Basic	Policy Template	Required, select Intercept Images with Critical and High-Risk

©2013-2022 Tencent Cloud. All rights reserved.

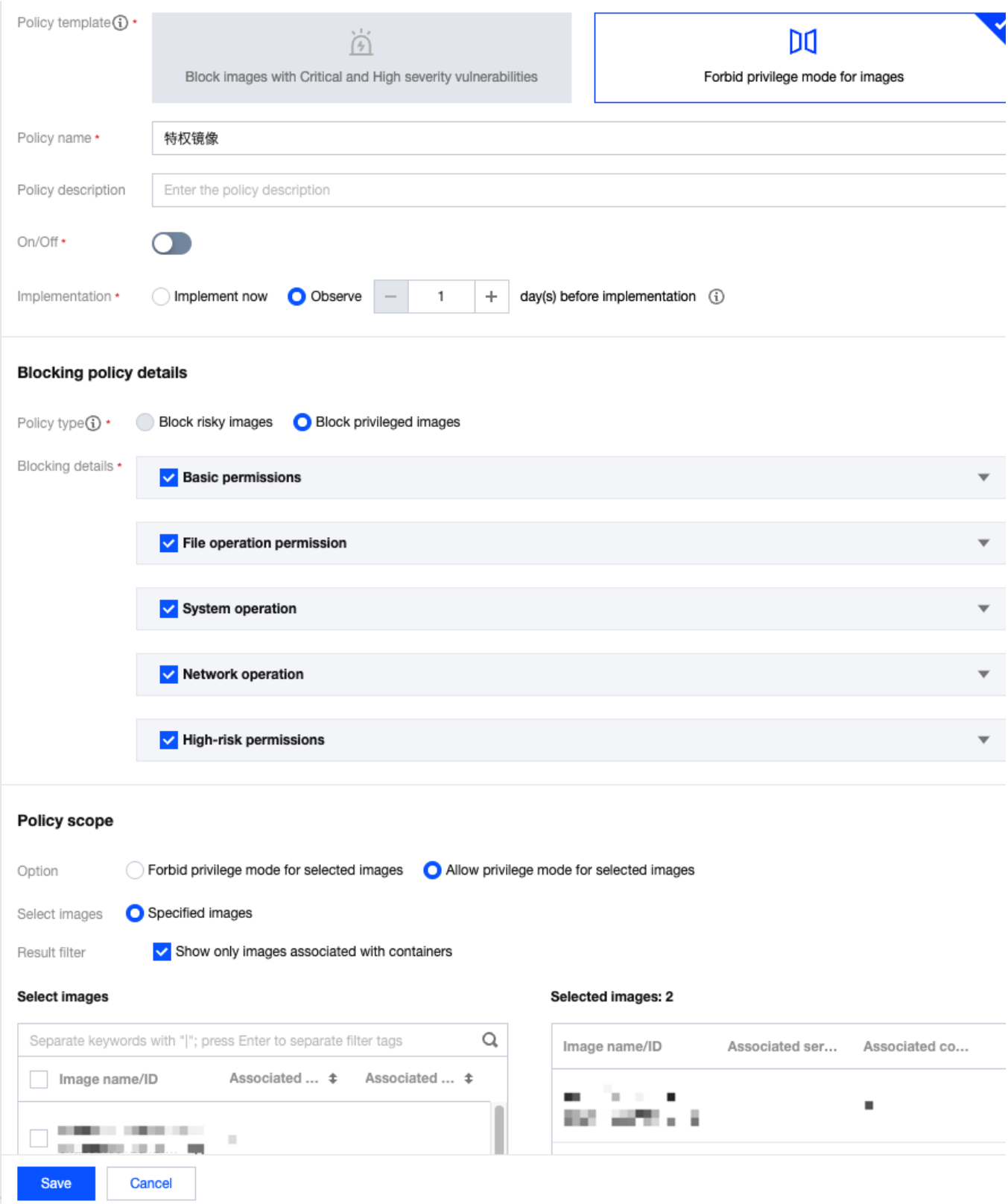
Information		Vulnerabilities.
	Policy Name	Required, up to 128 characters.
	Policy Description	Optional, up to 256 characters.
	Enable/Disable	Enable: Start intercepting images or the countdown for the observation period. Disable: Policy is not effective.
	Implementation	Implement now: After the policy is issued, the intercepting action is executed immediately when the target image is hit. Observe n day(s) before implementation: During the observation period, only alarms are triggered without interception. The intercepting action is executed immediately after the observation period ends.
Intercepting Policy Details	Policy Type	Select Intercept Images with Critical and High-Risk Vulnerabilities for the policy template and intercept risky images for the policy type. If you need to change the policy type, adjust the policy template.
	Intercepting details	For the three categories, vulnerabilities found, Trojan virus, and sensitive data found, at least one of them must be configured. Vulnerabilities Found can be configured based on the CVE number, component name and version number, or vulnerability classification. Trojan Virus can be configured based on the file MD5 or Trojan virus type. Sensitive Data Found can be configured based on the threat level and type of sensitive data.
Effective Range	Images Selection	When you configure risk image interception, the effective range of the policy must be for scanned images. The system cannot determine the presence of vulnerabilities, Trojan viruses, or sensitive data risks in unscanned images.

Create an Interception Policy for Privileged Images

When you create an interception policy for privileged images , **if a privileged image interception policy has already been created, a new one cannot be created**. You need to edit or create policies for those already existed. If not created, you can click **Create Policy** to configure directly.



©2013-2022 Tencent Cloud. All rights reserved.



Parameter Category	Parameter Name	Parameter Details
Basic Information	Policy Template	Required, select Intercept container images started in privileged mode.
	Policy Name	Required, up to 128 characters.

©2013-2022 Tencent Cloud. All rights reserved.

	Policy Description	Optional, up to 256 characters.
	Enable/Disable	Enable: Start intercepting images or begin the countdown for the observation period. Disable: The policy is not effective.
	Implementation	Implement now: After the policy is issued, the intercepting action is executed immediately when the target image is hit. Observe n day(s) before implementation: During the observation period, only alarms are triggered without interception. The intercepting action is executed immediately after the observation period ends.
Intercepting Policy Details	Policy Type	Select Intercept container images started in privileged mode for the policy template and Privileged Image Interception for the policy type. If you need to change the policy type, adjust the policy template.
	Intercepting Details	Users can check privileged startup parameters, defaulting to all. The system categorizes privileged parameters into five categories: base permissions, file operation permission, system operation, network operation, and high-risk permissions. Users can adjust categories or specific classifications within a category.
Effective Range	Effective Method	When users configure the privileged image interception policy, the option for effective method includes "selected images are not allowed to run in privileged mode" or "only selected images are allowed to run in privileged mode (privileged startup of other images will be blocked)".
	Images Selection	Users can select all images or custom images.

Managing a Policy

View: On the image interception policy page, click **image interception policy name** to view the details of the interception policy.

Enable or Disable: Adjust the policy's effectiveness by toggling the button in the startup status column.

When it is enabled, start intercepting images or the countdown for the observation period.

When it is disabled, the policy is not effective.

Edit: Click **Edit** to adjust the policy's name, description, startup status, policy effectiveness status, interception policy details, and policy effective range. The policy template cannot be adjusted.

©2013-2022 Tencent Cloud. All rights reserved.

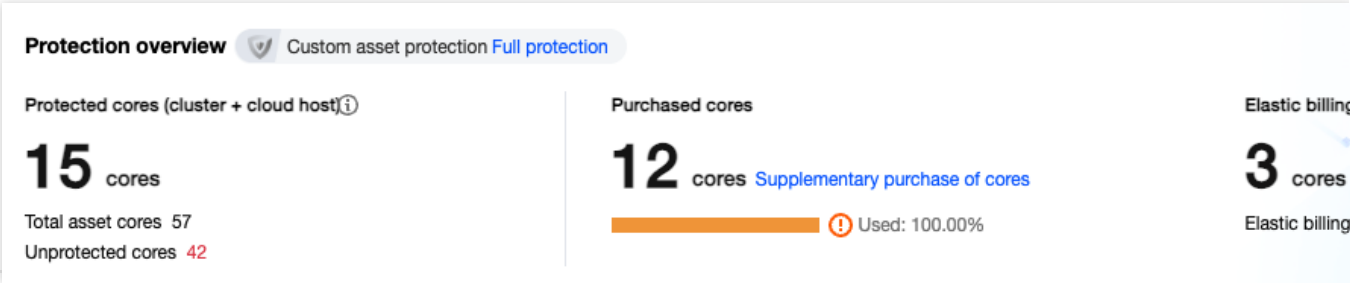
Protection Switch

Last updated：2024-08-13 17:13:56

After enabling TCSS, you can adjust TCSS activation for clusters and CVMs with statically launched containers on the Protection Switch page.

Protection Overview

Displays details of TCSS activation, including both full protection and custom asset protection. You can switch based on your protection needs:
Full protection: All clusters and CVMs with statically launched containers in your current business environment will have TCSS enabled. If new clusters or CVMs with statically launched containers are added to your business in the future, TCSS will automatically be enabled for your new assets. During activation, your unused cores will be consumed by default. If there are insufficient remaining cores, additional fees will be charged through post-paid elastic billing.
Custom asset protection: Select specific clusters or CVMs with statically launched containers to enable TCSS, rather than full activation.



Field Name	Description
Protected Cores	The number of cluster and CVM node resource cores with the protection switch enabled and under effective protection. Some assets may not count as effectively protected due to reasons such as the agent being offline for an extended period or Docker not being installed. These cores will not be included in the protected cores.
Total Asset Cores	The total number of cores for all clusters and CVMs running containers under this account.
Unprotected Cores	The number of cores for clusters and CVMs running containers without TCSS enabled.
Purchased Cores	The number of cores purchased for billing. When more assets need TCSS enabled and the purchased cores are insufficient, you can click **Supplementary purchase of core** count to make an additional purchase.

©2013-2022 Tencent Cloud. All rights reserved.

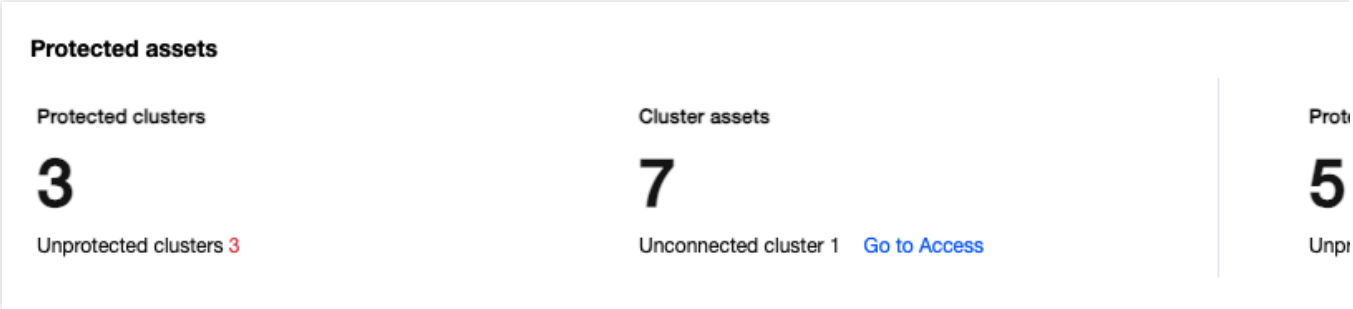
Flexible Billing Cores	Flexible billing will be calculated based on the daily average of unprotected cores (calculated hourly). This section only displays the total flexible billing cores for the day up to the current time. You can click **Edit** to adjust the flexible billing cores, with a default value of 5,000.

Protected Assets

Display the number of clusters with TCSS enabled, clusters without TCSS enabled, full cluster assets (including clusters not connected to the console), and the number of CVMs with statically launched containers with TCSS enabled, as well as the number of CVMs with statically launched containers without TCSS enabled.

Note:

CVMs with Statically Launched Containers: CVMs running containers that are not associated with any cluster resources.



Protection List

You can view the details of enabling TCSS for clusters and CVMs with statically launched containers in the list, or adjust the enable/disable services for clusters and CVMs. It is recommended to update the assets before you enable the service by clicking **Synchronize Assets** at the top right of the page to obtain the latest asset details.

Cluster Protection

① Click **All enable protections** to batch enable TCSS for all clusters.

② You can also check multiple clusters and click **Disable protections** to batch disable them.

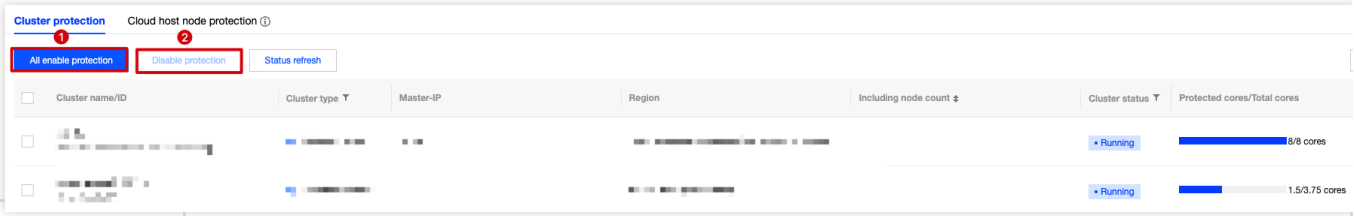
Note:

If the number of clusters enabled exceeds the purchased cores, it is recommended to purchase additional cores. If not purchased in time, the excess cores will be charged through elastic billing.

If the exceeded cores exceed both the purchased cores and the elastic billing core limit, the cluster protection switch cannot be enabled. It is recommended to purchase additional cores or increase elastic billing cores before you proceed.

©2013-2022 Tencent Cloud. All rights reserved.

③ To enable or disable a single cluster, you can adjust it in the protection switch column by clicking **Protection switch**.



Field Name	Description
Cluster Name/ID	Name/ID of the cluster integrated with TCSS. For clusters not connected, complete the connection on the cluster inspection page before enabling the service.
Cluster Type	Includes Tencent Cloud managed cluster, Tencent Cloud independent cluster, Tencent Cloud Serverless cluster, self-built cluster (Tencent Cloud), and self-built cluster (Non-Tencent Cloud).
Master-IP	Cluster control node, used to identify the cluster. You can use this information for cluster retrieval.
Region	The belonging region.
Including Node Count	Number of nodes included in the cluster.
Cluster Status	Cluster running status, including running, creating, and exceptional.
Protected Cores/Total Cores	The number of protected cores in clusters with TCSS enabled, and the total number of cores in the cluster. When the purchased cores or elastic cores are sufficient, the cluster is fully protected. If the purchased or elastic cores are insufficient, this column will show partial protection or no protection, indicating that you need to purchase more cores or increase the elastic billing cores.
Protection Switch	You can enable or disable TCSS for individual clusters.
Operation	Click **View cluster** to navigate to the cluster inspection page to view the configuration risk and vulnerability risk of the cluster.

CVM Node Protection

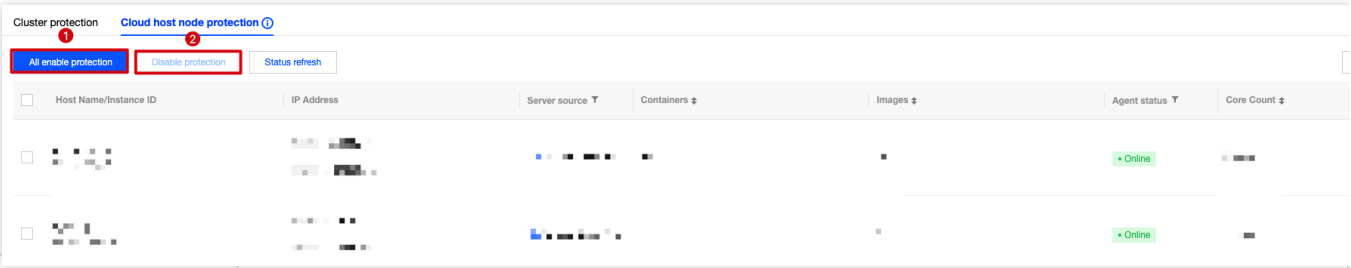
① Click **All enable protections** to batch enable TCSS for all CVMs with statically launched containers.

② You can also check multiple nodes and click **Disable protections** to batch disable them.

Note:

©2013-2022 Tencent Cloud. All rights reserved.

If the number of CVMs enabled exceeds the purchased cores, it is recommended to purchase additional cores. If not purchased in time, the excess cores will be charged through elastic billing.
If the exceeded cores exceed both the purchased cores and the elastic billing core limit, the CVM protection switch cannot be enabled. It is recommended to purchase additional cores or increase elastic billing cores before you proceed.
③ To enable or disable a single CVM, you can adjust it in the protection switch column by clicking **Protection switch**.



Field Name	Description
Host Name/Instance ID	Name/Instance ID of the CVM with statically launched containers.
IP Address	Private and public IP address of the CVM with statically launched containers.
Project	Project information configured at the time of purchasing the CVM for easy filtering.
Server Source	Including Tencent CVMs and Non-Tencent CVMs.
Containers	Number of containers running on the CVM with statically launched containers.
Images	Number of local images on the CVM with statically launched containers.
Agent Status	Includes online, offline, and not installed.
Core Count	Cores of the CVM with statically launched containers.
Protected Cores	When the purchased cores or elastic cores are sufficient, the CVM is under full protection, and the number of protected cores are the same as the CVM cores. When the purchased cores and elastic billing cores are insufficient and TCSS is enabled on the CVM, the protected cores will be fewer than the CVM cores. It is recommended to purchase additional cores or increase elastic billing cores before you proceed. Alternatively, it may be due to the Agent being offline for an extended period on your host node, causing an exceptional condition. The current host node protection cores will be displayed as 0 and will not be billed.
Protection Switch	You can enable or disable TCSS on a single CVM.
Operation	Click **Manage assets** to go to the host node list.

©2013-2022 Tencent Cloud. All rights reserved.

©2013-2022 Tencent Cloud. All rights reserved.

Alarm Settings

Last updated：2024-01-23 15:44:44

This document describes how to configure alert policies for image security events and runtime security events.

Prerequisites

Make sure you have subscribed to TCSS in "Message Center - Subscription Management", which can be set by clicking here.

Event types

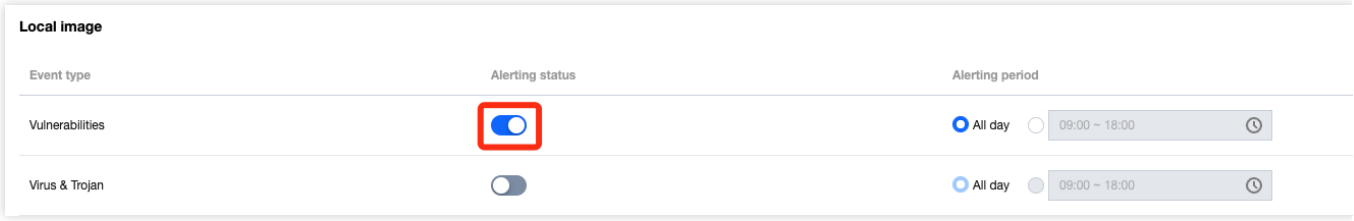
The following table lists the event types, default alerting period, and alert triggers in alert policies:

Event Type	Default Alerting Period	Default Alert Triggers
Vulnerability	All day	Critical
Virus and trojan	All day	Critical, High, Medium, Low
Sensitive data	All day	Critical, High, Medium, Low
Container escape	All day	-
Abnormal process	All day	Failed to block, Alert
File tampering	All day	Failed to block, Alert
Reverse shell	All day	-
Virus scanning	All day	-

Directions

1. Log in to the TCSS console and click **Alert Policies** on the left sidebar.
2. On the **Alert Policies** page, toggle on the **Alerting status** switch.

©2013-2022 Tencent Cloud. All rights reserved.

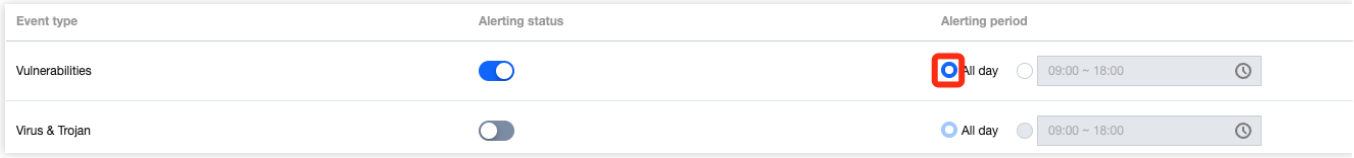


3. After enabling the alert policy mode, click

to select the alerting period (**All day** or custom).

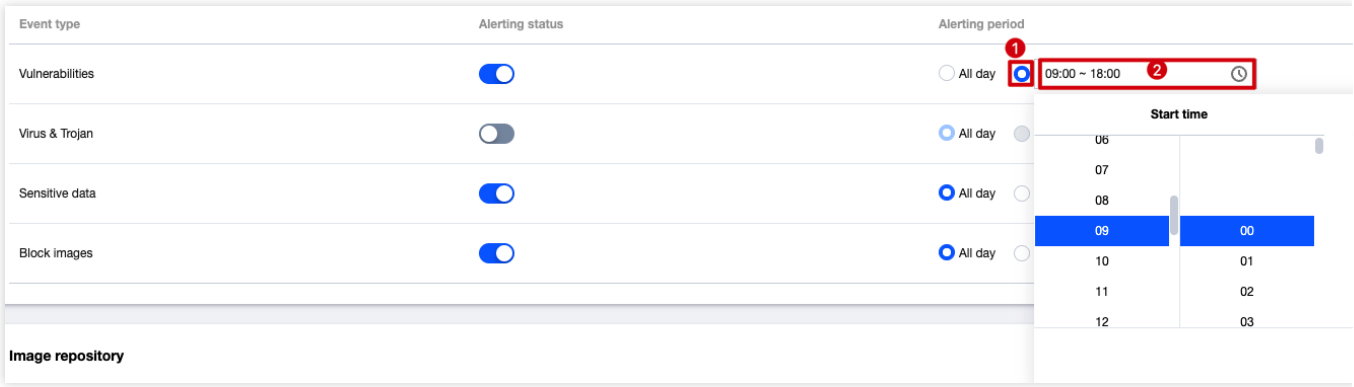
Select

on the left of **All day** to send alert notifications all day.



Select

on the left of the custom time box, select the start time and end time, and click **OK** to send alert notifications during the period.



©2013-2022 Tencent Cloud. All rights reserved.

Log Analysis Overview

Last updated：2024-01-23 15:44:44

This document describes how to use the log analysis feature, view the container bash logs, container startup audit logs, and Kubernetes API audit logs, and configure and ship logs.

Background

Log analysis provides container bash logs, container startup audit logs, and Kubernetes API audit logs, supports statement search and query, and offers visual report, statistical analysis, and export features. It helps you quickly query the business logs, trace the container security events, and improve the operations efficiency.
Container bash logs: Provide bash log audit to help you trace abnormal processes.
Container startup audit logs: Provide container startup log audit to help you log container startups.
Kubernetes API audit logs: Help you log Kubernetes API calls.
We recommend you enable the log audit feature for core assets and purchase storage as needed for log data collection and retention.
TCSS Pro Edition provides the log collection feature. We recommend you purchase the Pro Edition and then log storage. If you have purchased log storage but the capacity becomes insufficient, the log analysis service will clear historical log data. We recommend you expand the storage capacity promptly.

Prerequisites

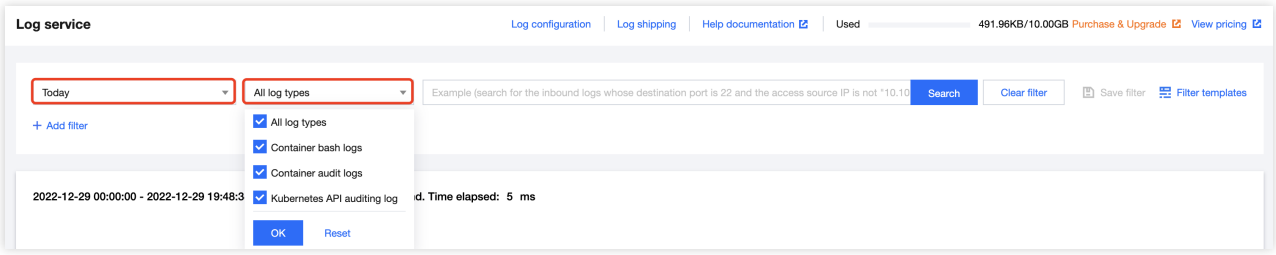
Log analysis and storage is a value-added service of TCSS. You need to purchase it separately on the TCSS purchase page.

©2013-2022 Tencent Cloud. All rights reserved.

Querying Log

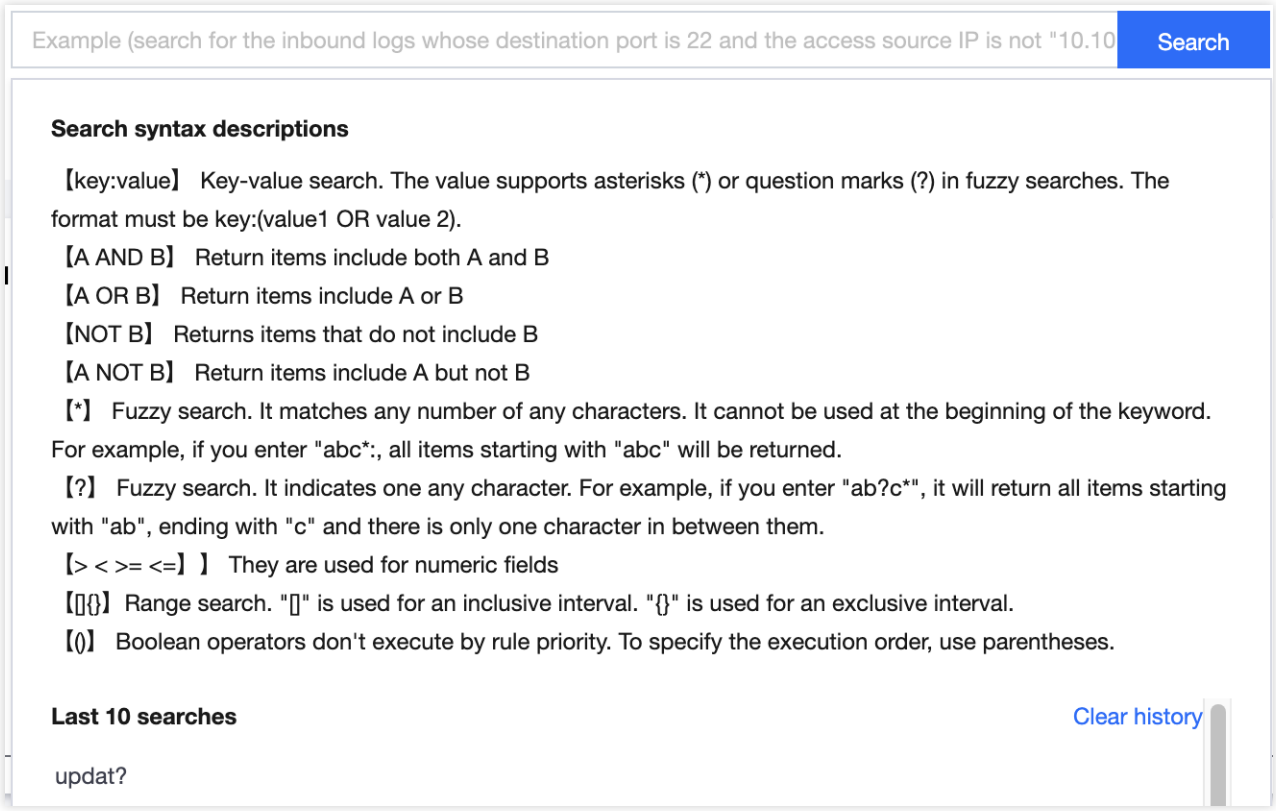
Last updated：2024-01-23 15:44:44

1. Log in to the TCSS console and click **Security Operations** > **Log Analysis** on the left sidebar.
2. On the **Log Analysis** page, filter log analysis results and perform appropriate operations.
Filter logs by time or type: At the top of the **Log Analysis** page, filter log analysis results by time (last 15 minutes, last hour, last 12 hours, last 24 hours, today, last 7 days, last 14 days, last 30 days, last 90 days, or a custom period) or by log type and click **OK**.

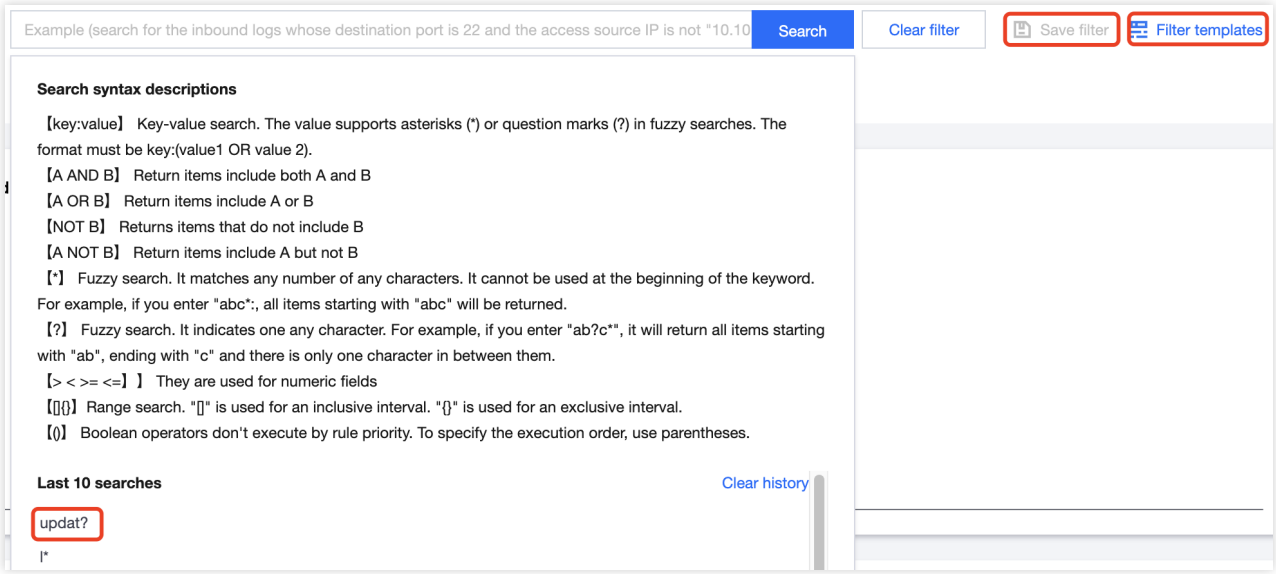


Filter logs by record field: At the top of the **Log Analysis** page, filter logs by field, which can be entered manually or automatically.
Manually enter the field: Enter the target field in the format of field name and field value and click **Search**. The search syntax description is as shown below.

©2013-2022 Tencent Cloud. All rights reserved.



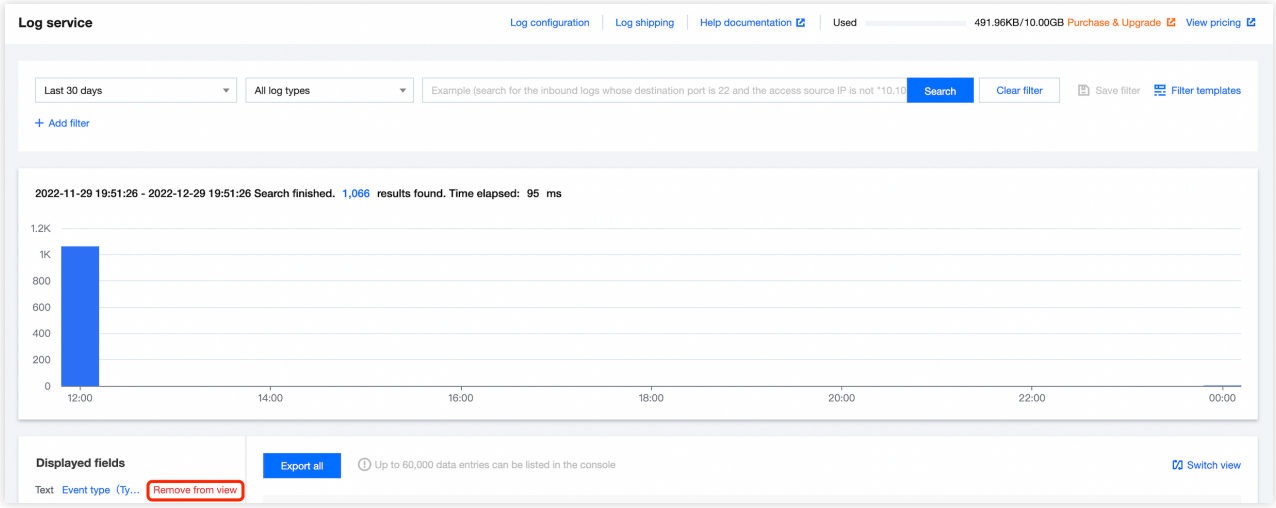
Automatically enter the field: Click **Filter templates** and select the target template name, or click the historical record in the input box as shown above. To reuse a query template, click **Save filter** when manually entering a query statement to save the current configuration (log type and keyword).



Quickly view the log trend chart:

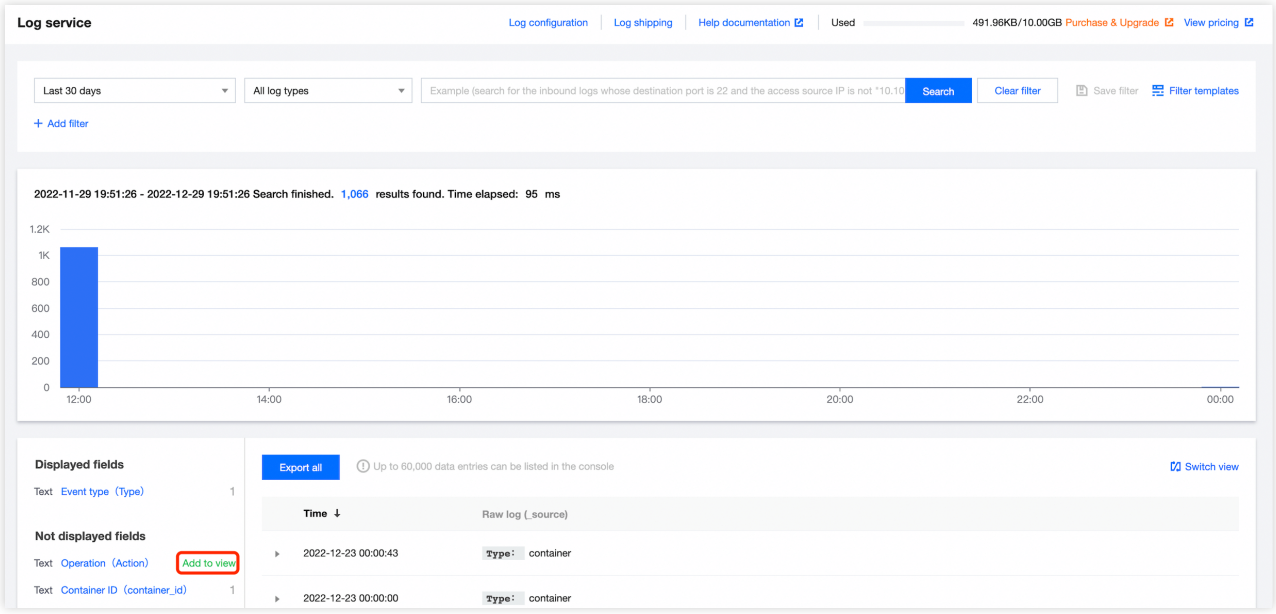
©2013-2022 Tencent Cloud. All rights reserved.

Method 1: To view logs within a specified period, scroll the mouse wheel to quickly view the blue bar chart above the log trend chart, which displays the statistical period and number of logs.
Method 2: Click the blue bar chart above the log trend chart to view more details.
3. On the **Log Analysis** page, fields are displayed in the log list based on the **Displayed fields**. If **Displayed fields** is **Raw log (_source)**, all log fields are listed. Up to 60,000 data entries can be listed in the console.
Customize fields to be displayed or hidden:
Add to view: Move the cursor to a hidden field and click **Add to view** on the right to add it to the displayed fields. Only selected displayed fields are listed, and hidden fields are not.

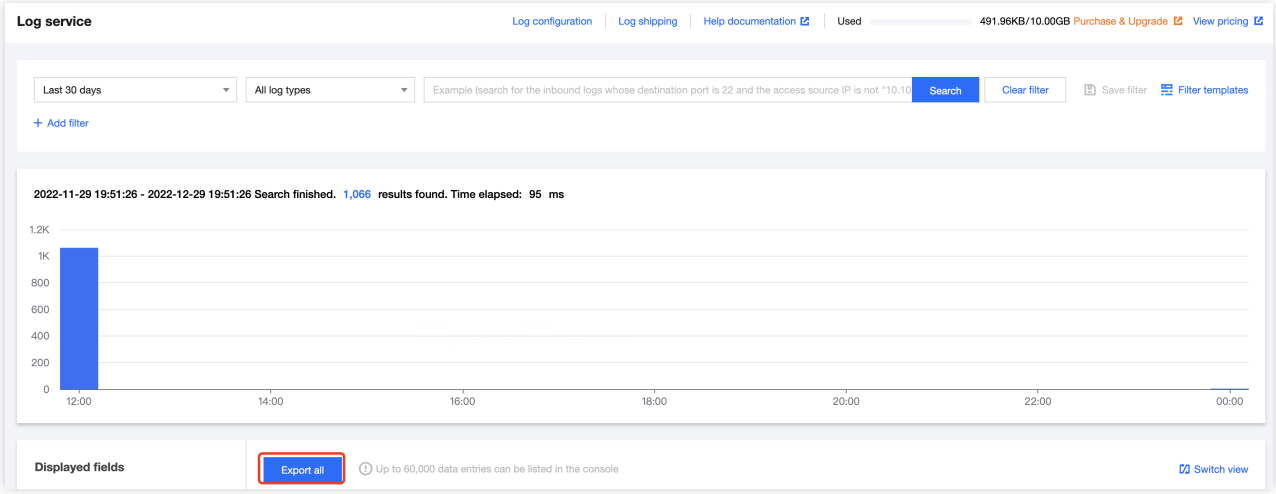


Hide: Move the cursor to a displayed field and click **Remove** on the right to remove it from the displayed fields. The list on the right will no longer display this field.

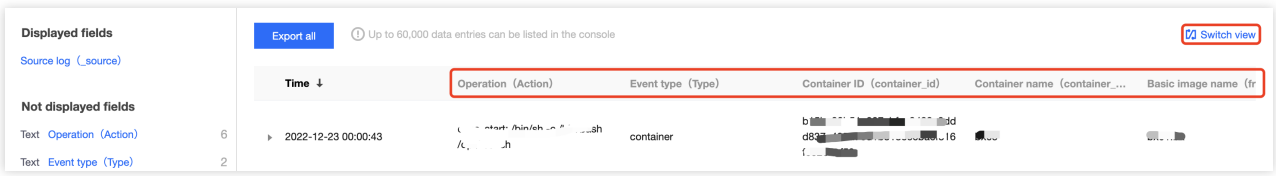
©2013-2022 Tencent Cloud. All rights reserved.



Export: Click **Export all** in the top-left corner of the field details, and log analysis will export 60,000 logs meeting the search condition as a file and download it through the browser to a local directory.



Switch the display mode: Click **Switch view** in the top-right corner of the field details to display the displayed fields in a table column.



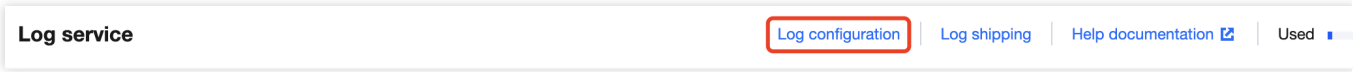
©2013-2022 Tencent Cloud. All rights reserved.

Configuring Log

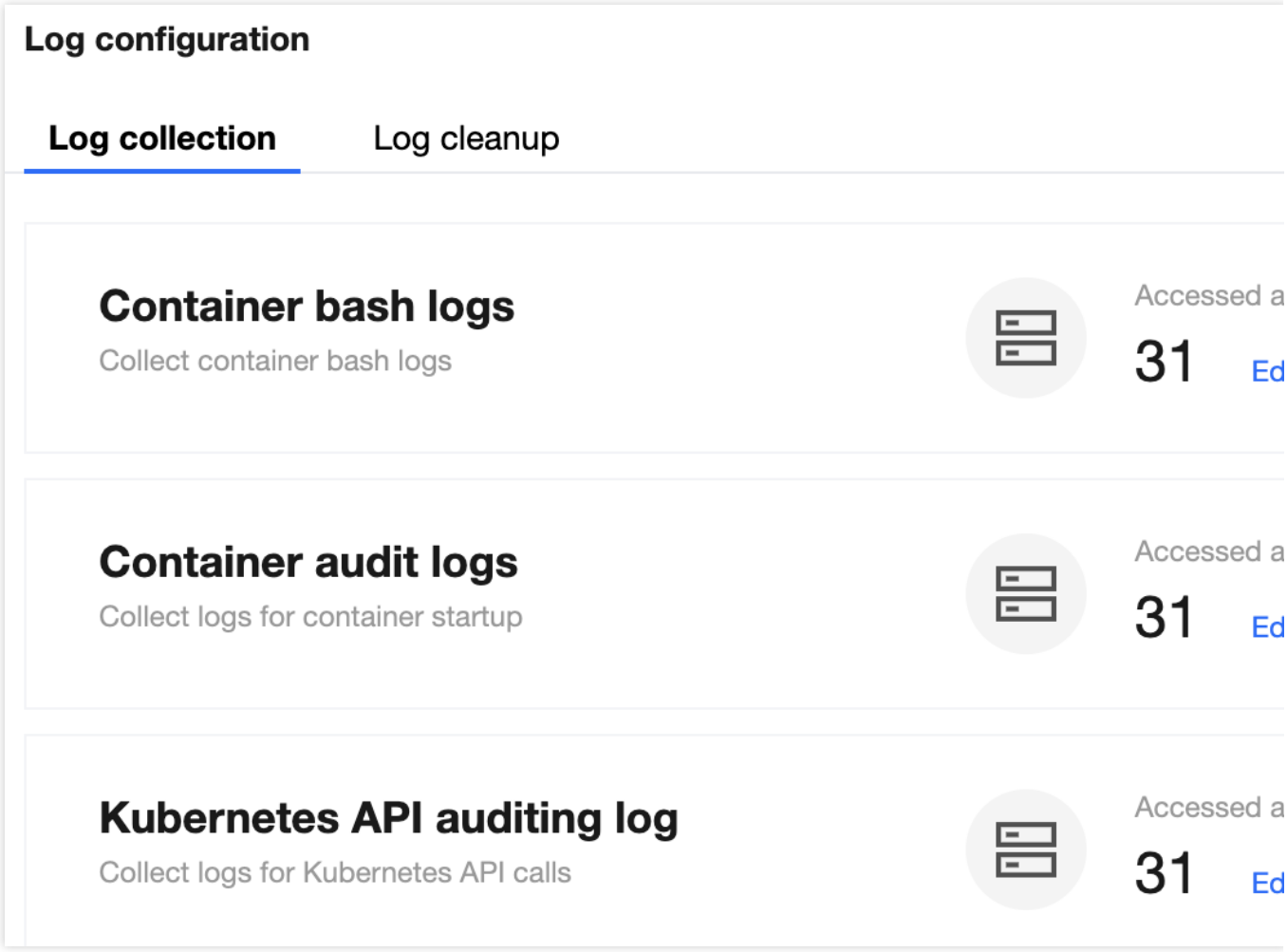
Last updated：2024-01-23 15:44:44

Log collection

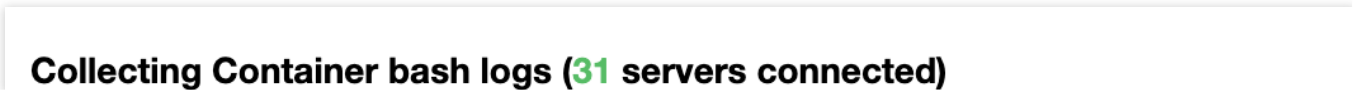
1. On the **Log Analysis** page, click **Log configuration** > **Log collection** at the top.



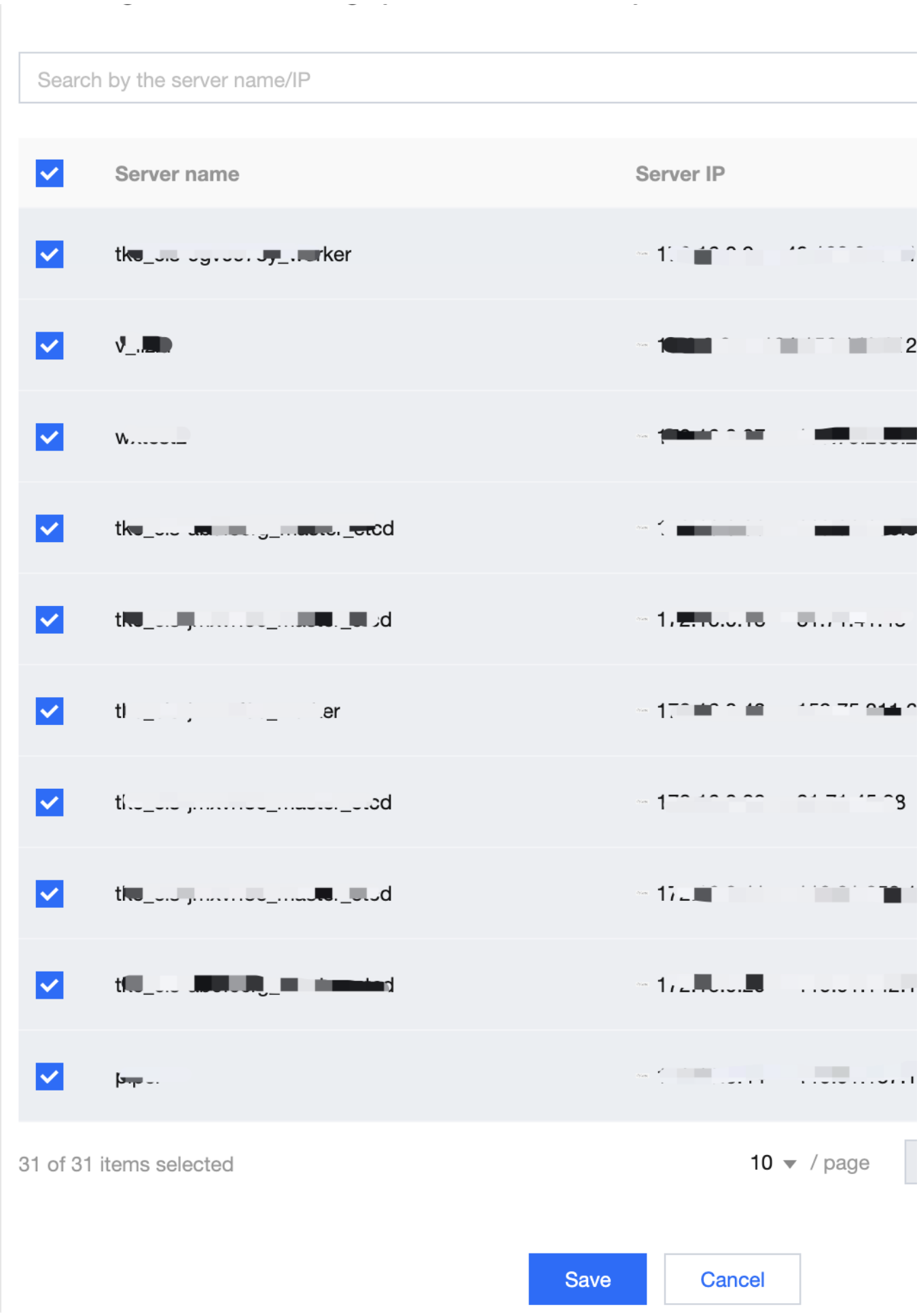
2. On the **Log collection** tab, toggle on or off the **Enabled** switch to enable or disable the collection of container bash logs, container startup audit logs, and Kubernetes API audit logs.



3. On the **Log collection** tab, click **Edit** in the **Accessed assets** column to configure the node scope for log collection. Select the servers for log collection and click **Submit**.



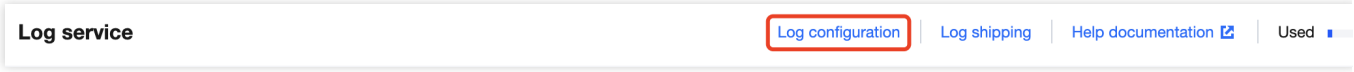
©2013-2022 Tencent Cloud. All rights reserved.



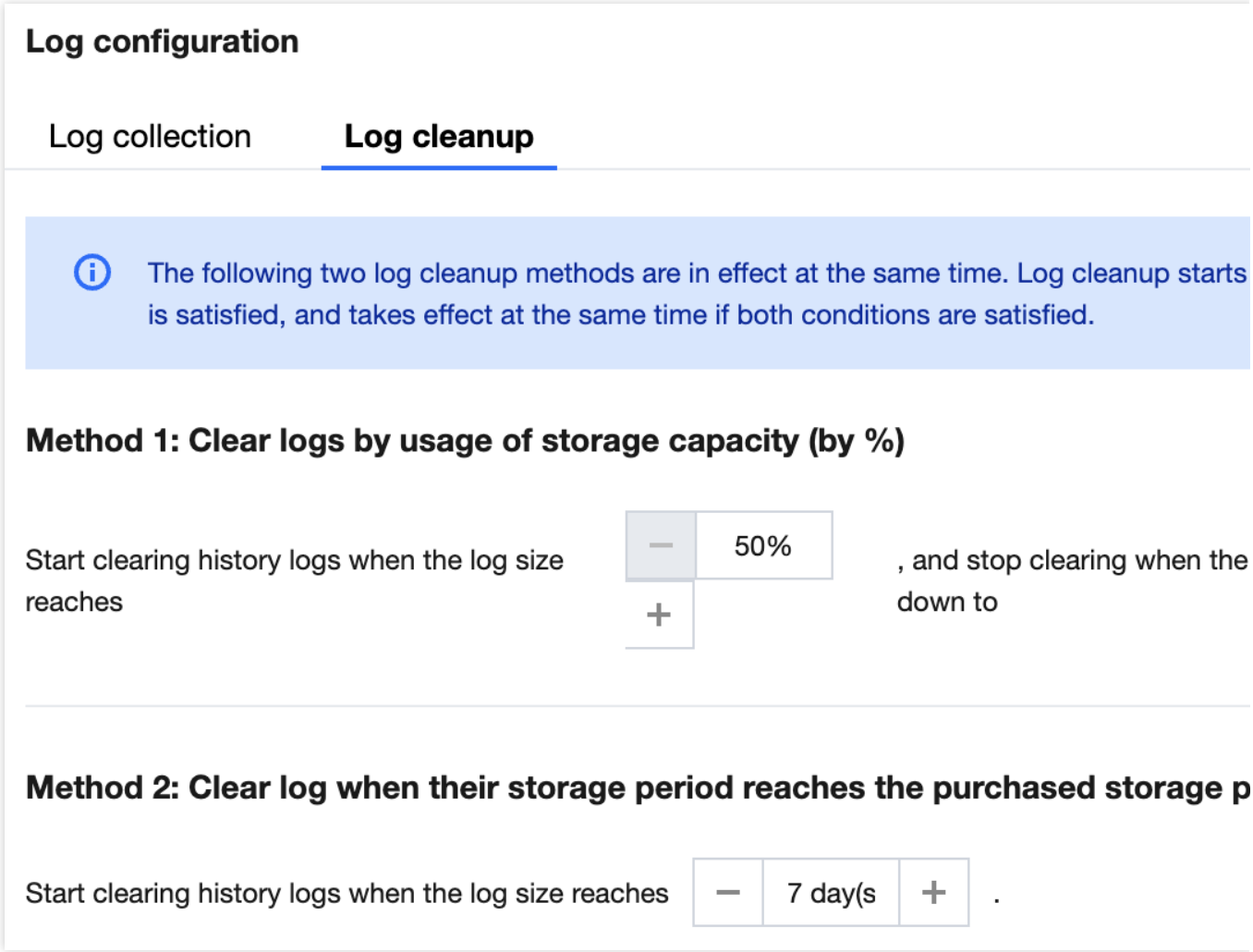
©2013-2022 Tencent Cloud. All rights reserved.

Log cleanup

1. On the **Log Analysis** page, select **Log configuration** > **Log cleanup** at the top.



2. On the **Log cleanup** tab, clear logs by percentage or storage period.
Clear logs by percentage: When the log storage volume reaches the configured percentage, historical logs are cleared until the configured percentage.
Clear logs by storage period: When the log storage period reaches the configured value, historical logs are cleared, and only those within the configured storage period are retained.
Note:
The two cleanup methods take effect at the same time, which means log cleanup starts when either of the two conditions is met.



©2013-2022 Tencent Cloud. All rights reserved.

Log Shipping

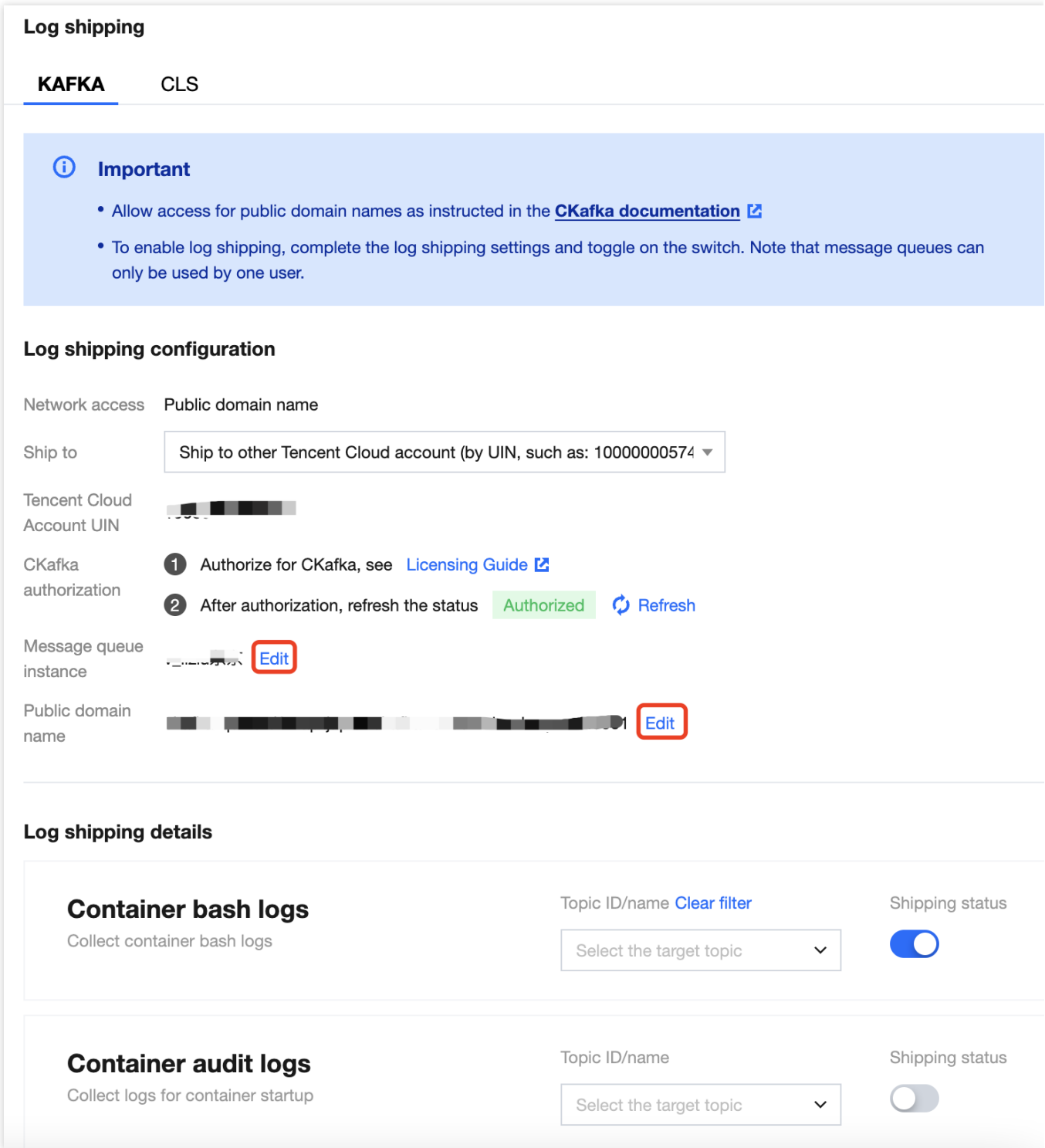
Last updated：2024-01-23 15:44:44

You can ship logs to CKafka or CLS.

Shipping to CKafka

1. On the **Log Analysis** page, click **Log shipping** > **KAFKA** at the top.
2. On the **KAFKA** tab, click **Configure now**.

©2013-2022 Tencent Cloud. All rights reserved.



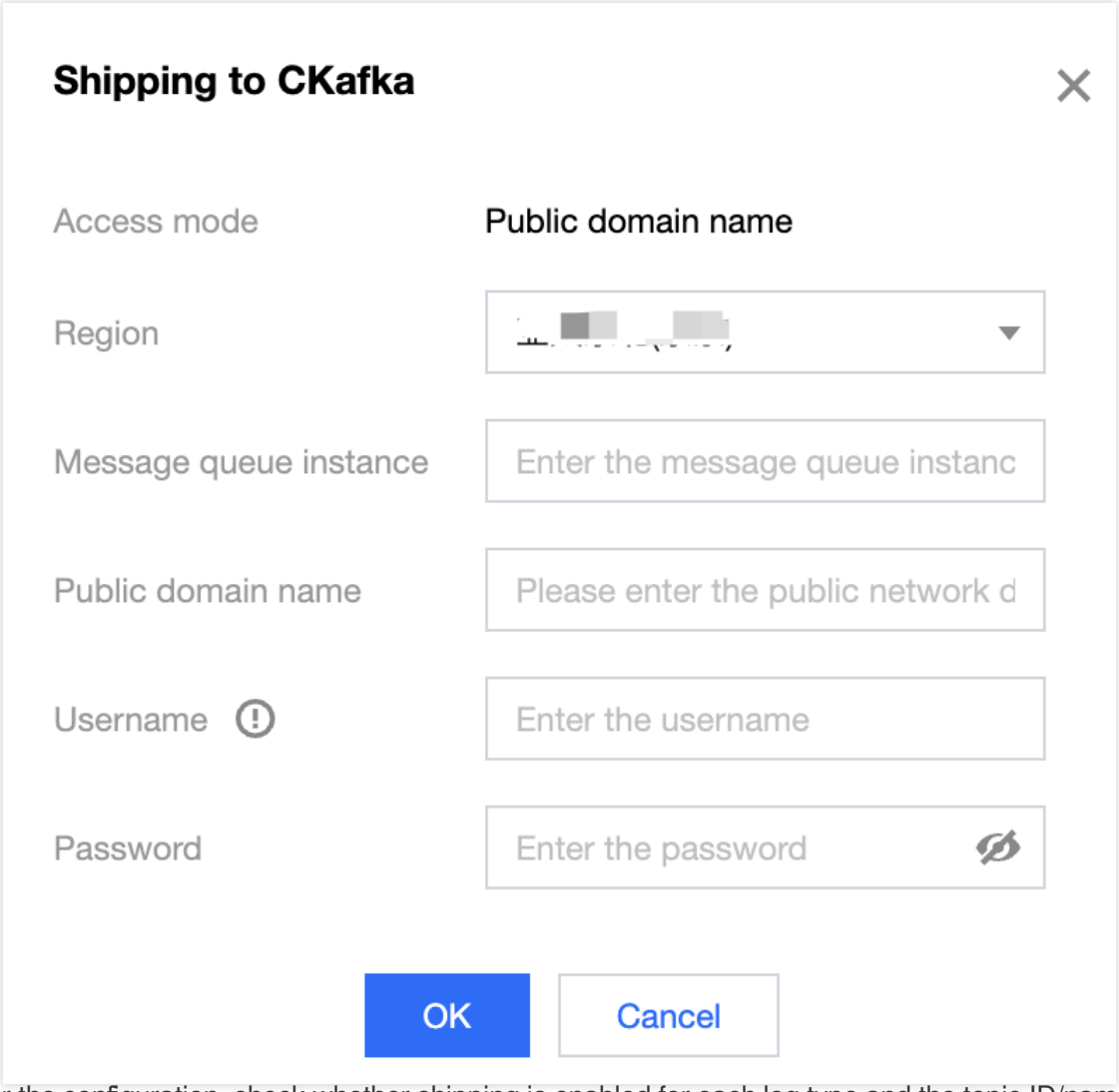
3. On the **Shipping to CKafka** page, grant the access, configure the message queue instance, public domain name, username, and password, and click **OK**.

Note:

Network access is set to **Public domain name** by default.

You can select **Ship to the current Tencent Cloud account** or **Ship to another Tencent Cloud account** for **Ship to**.

©2013-2022 Tencent Cloud. All rights reserved.



4. After the configuration, check whether shipping is enabled for each log type and the topic ID/name.

Cross-Account Log Shipping Through the Public Domain Name

Step 1. Select the shipping method

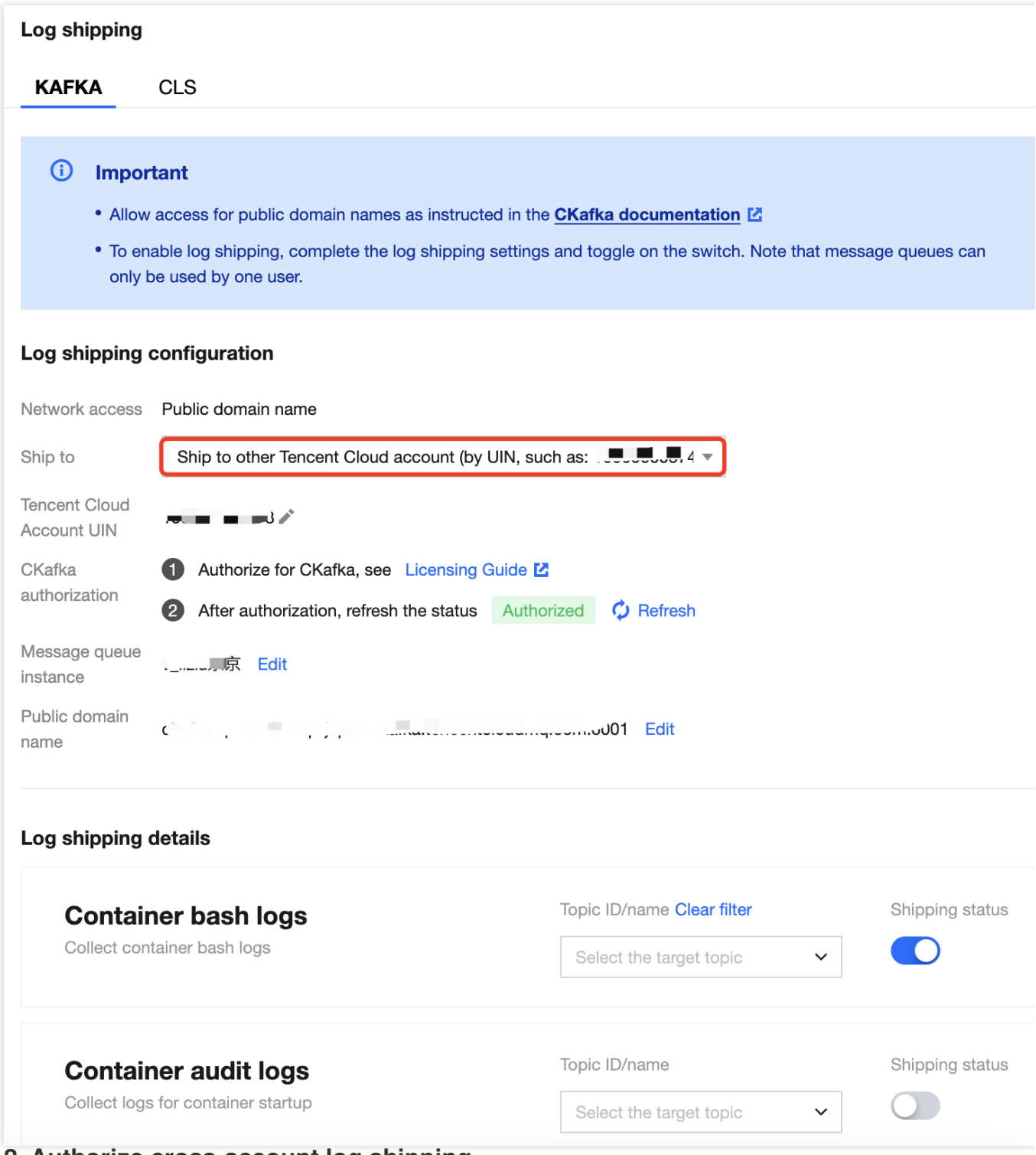
1. On the **Log Analysis** page, click **Log shipping** > **KAFKA/CLS** at the top.
2. On the **KAFKA** tab, select **Ship to another Tencent Cloud account** and enter the UIN of the recipient account.

Note:

When configuring the message instance for the recipient account in the CKafka console, you need to select **Public domain name and create three topics that can receive TCSS audit logs.

Back up the ID and public domain name of the message instance, as well as the ID and name of the topics for receiving the three types of logs. Remember the username and password. After cross-account authorization, you need to enter the above information for the shipping account.

©2013-2022 Tencent Cloud. All rights reserved.



Step 2. Authorize cross-account log shipping

To ship TCSS logs across accounts, you need to perform authorization for the recipient account and allow the shipping account to verify the CKafka instance of the recipient account and pull the topic ID and name.

If a TCSS role already exists

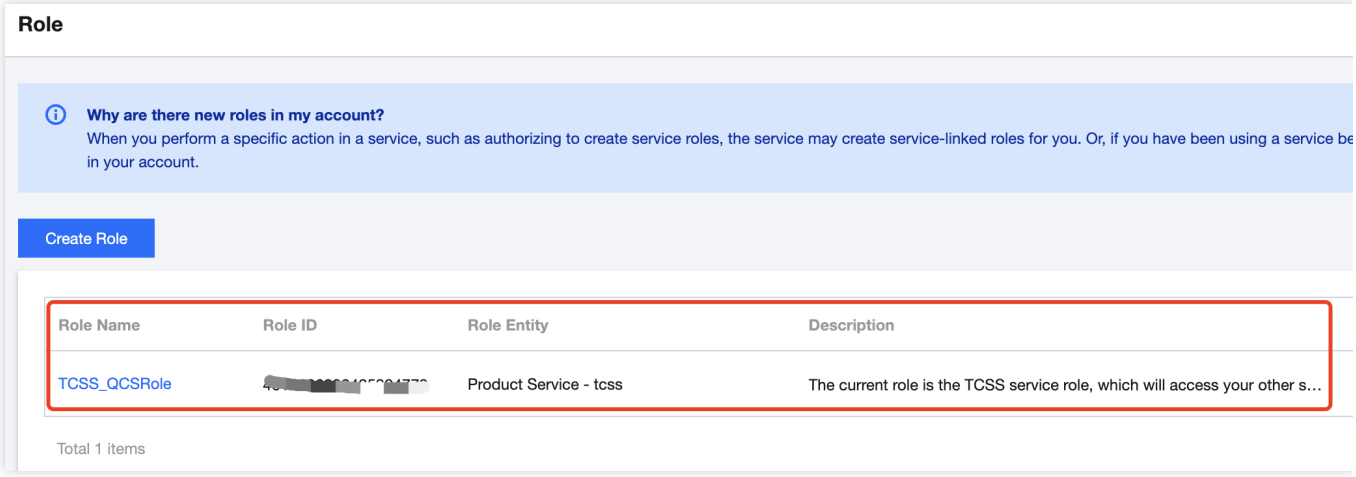
1. Log in to CAM console and click **Role** on the left sidebar.

©2013-2022 Tencent Cloud. All rights reserved.

2. On the **Role** page, enter **TCSS** in the search box. If the following content is found: role name: `TCSS_QCSRole` ; role entity: `Product Service - tcss` , a TCSS role has been bound to the account, and you only need to add the CAM and CKafka policy permissions in **Associate Policy**.

Note:

The UIN of the recipient account should be the same as that entered in step 1.



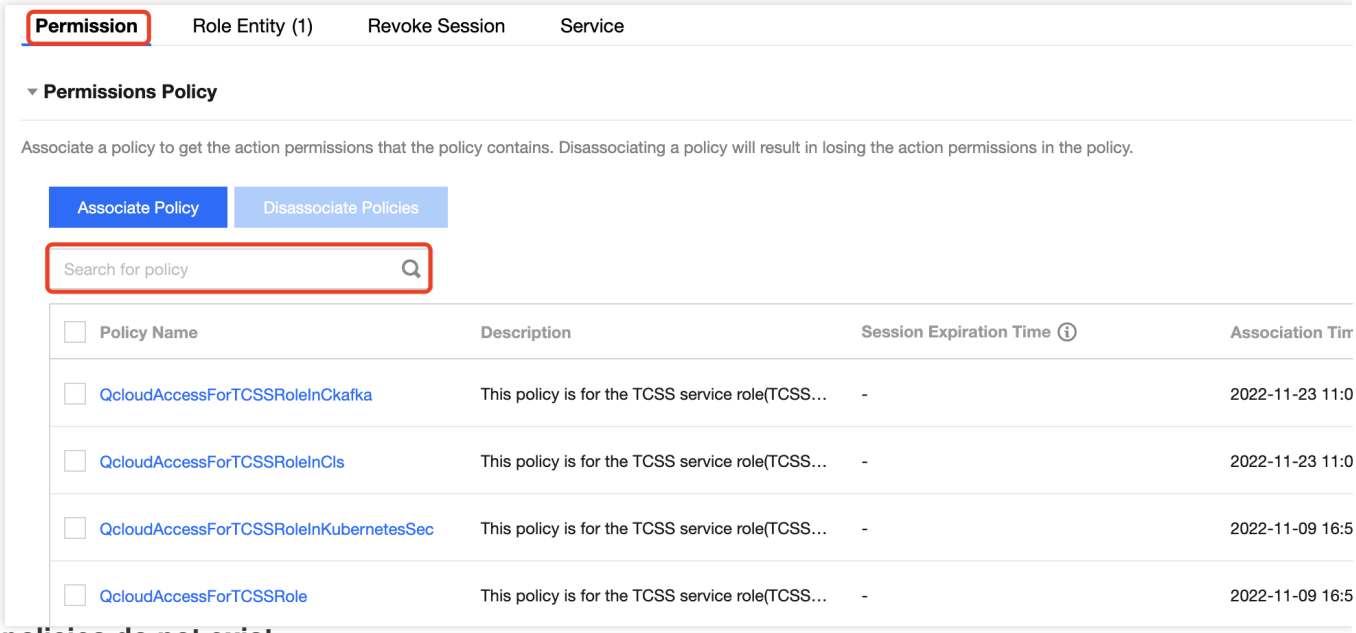
3. Click **TCSS_QCSRole** to enter the **Permission** tab.

4. On the **Permission** tab, search for `QcloudCamSubaccountsAuthorizeRoleFullAccess` and `QcloudAccessForTCSSRoleInCkafka` policies.

If the policies already exist:

Go back to the TCSS console, log in to the shipping account, and check whether the authorization is successful as prompted on the page, and if so, configure the public domain name, message queue, and topic information for log shipping to CKafka.

©2013-2022 Tencent Cloud. All rights reserved.

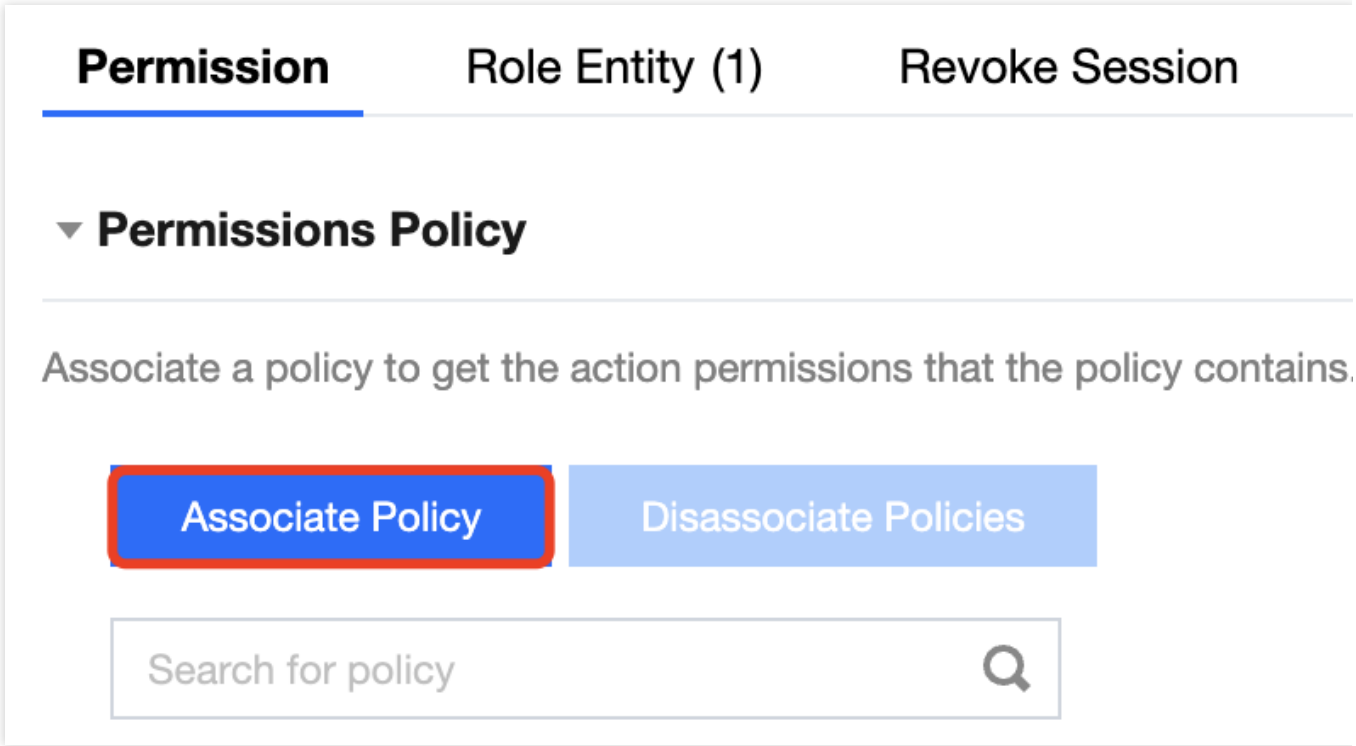


If the policies do not exist:

2.1 Click **Associate Policy** and confirm the information to pop up the **Associate Policy** window.

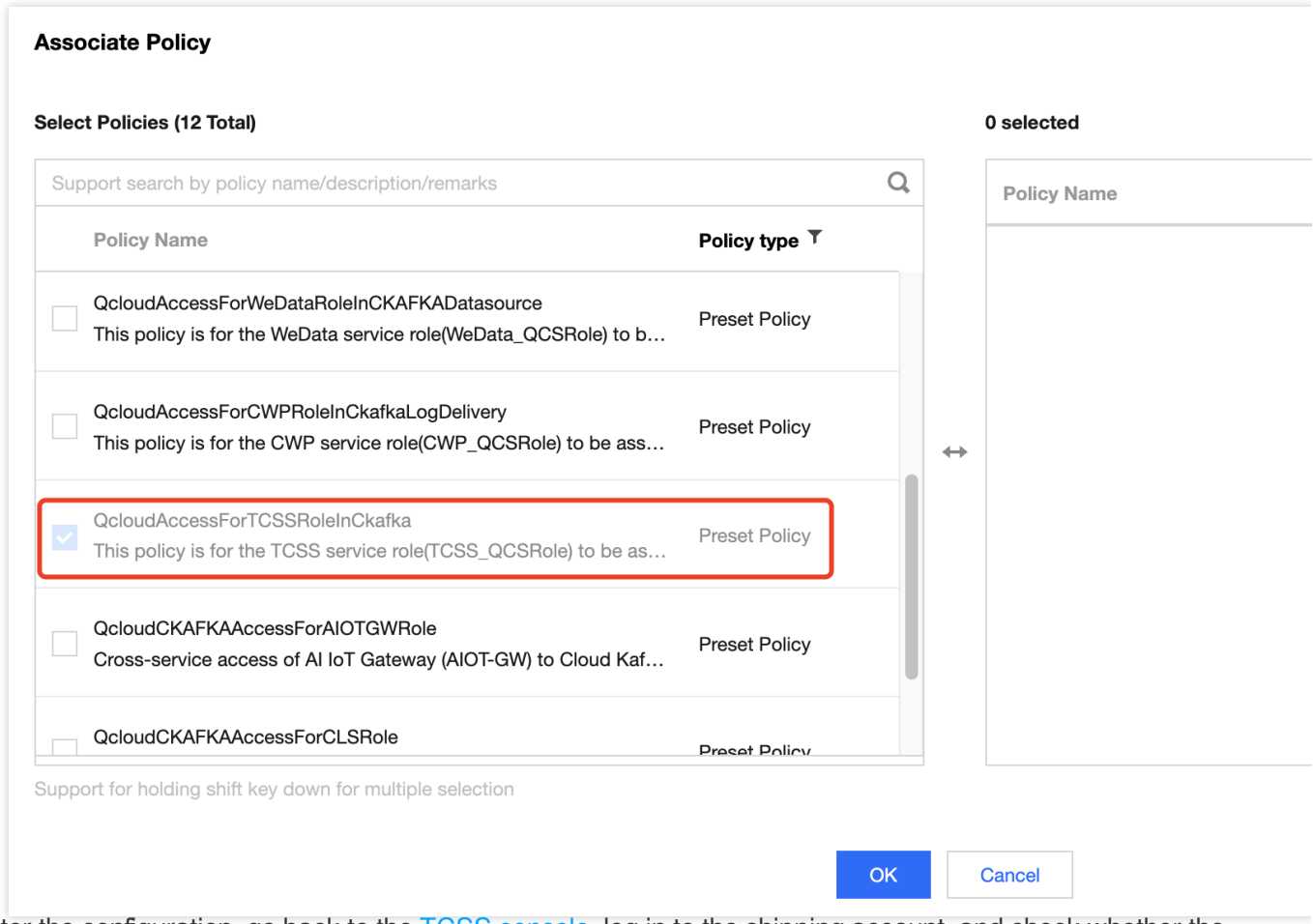
Note:

The role is authorized by you and changes to the role content (such as the associated policy and role entity) may lead to the consequence that the service you authorize the role to cannot use the role normally.



2.2 In the Associate Policy pop-up window, search for QcloudCamSubaccountsAuthorizeRoleFullAccess and QcloudAccessForTCSSRoleInCkafka policies, select the policies, and click OK. Then, you can view the policies in the details of the TCSS_QCSRole role.

©2013-2022 Tencent Cloud. All rights reserved.

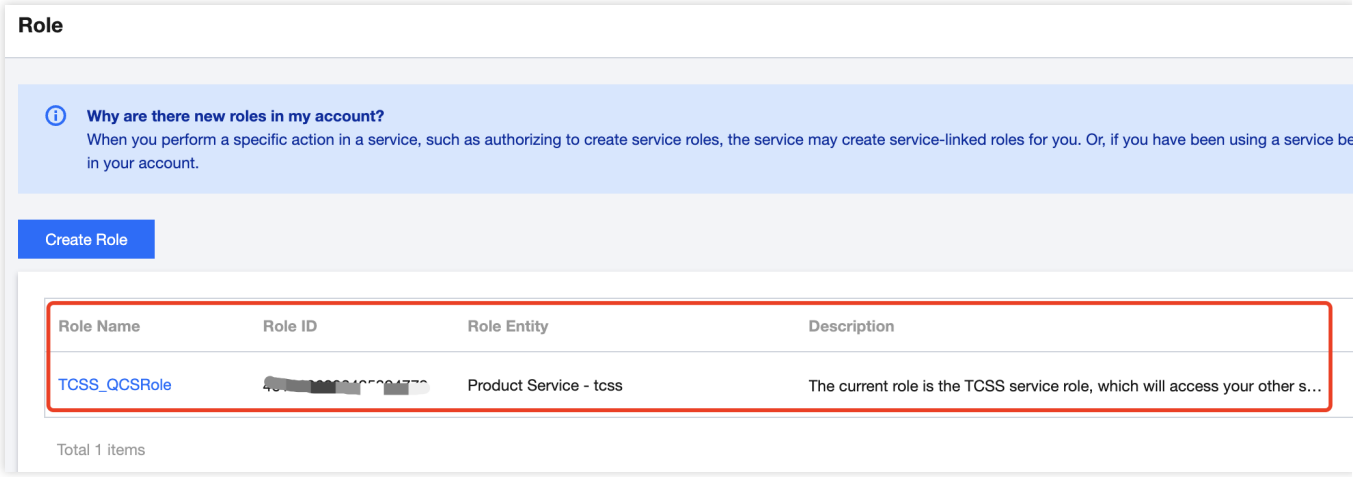


2.3 After the configuration, go back to the TCSS console, log in to the shipping account, and check whether the authorization is successful as prompted on the page, and if so, configure the public domain name, message queue, and topic information for log shipping to CKafka.

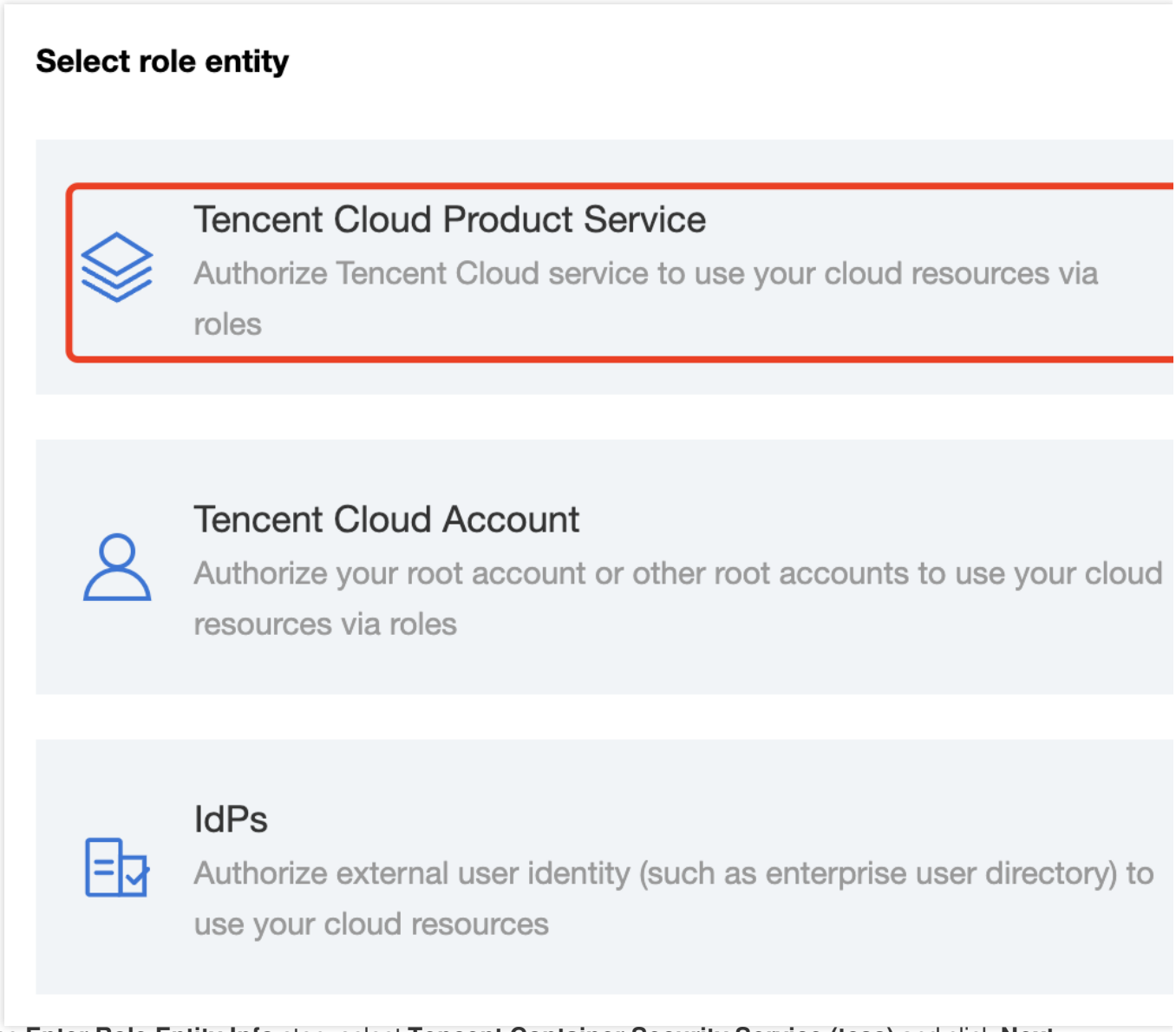
If no TCSS roles exist

1. On the **Role** page, enter **TCSS** in the search box. If the following content cannot be found: role name: `TCSS_QCSRole` ; role entity: `Product Service - tcss` , no TCSS roles have been bound to the account, and you need to create a role in the list.

©2013-2022 Tencent Cloud. All rights reserved.



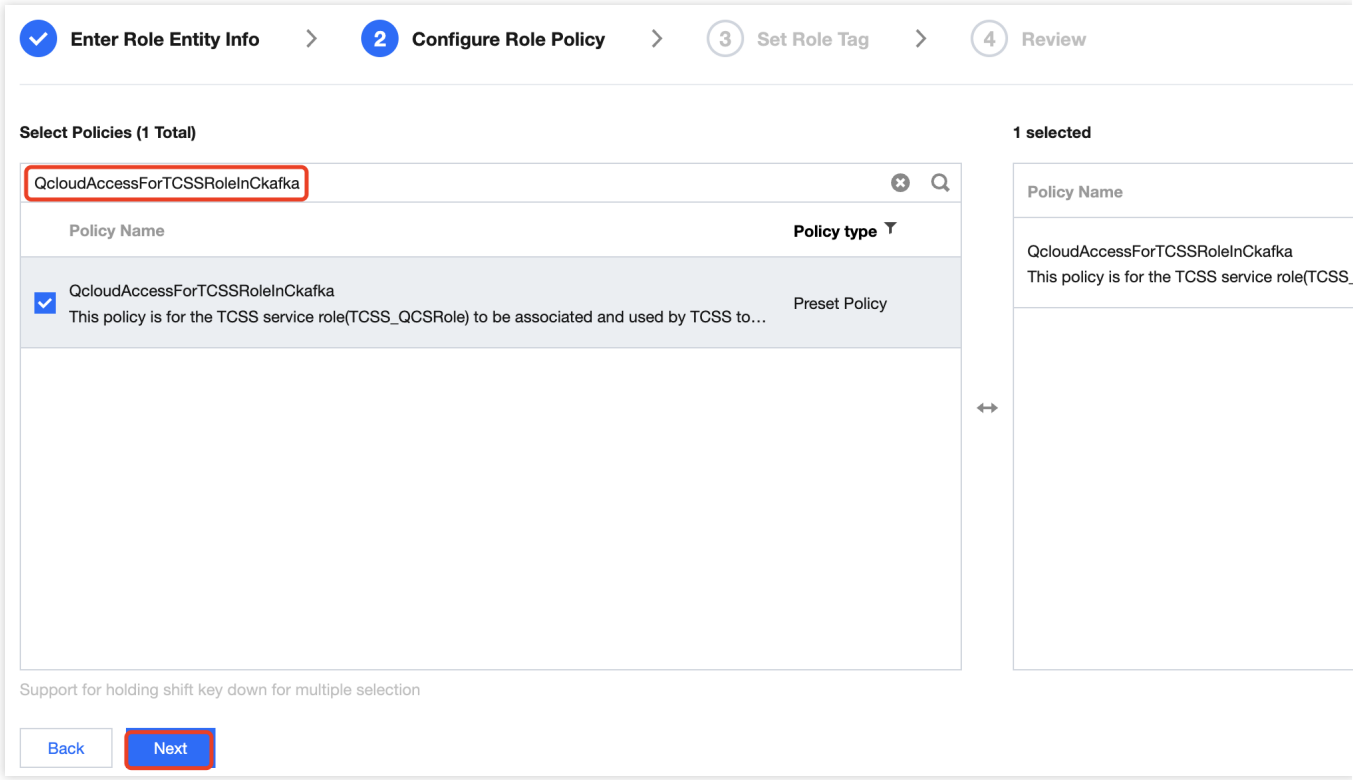
2. On the **Role** page, click **Create Role** and select **Tencent Cloud Product Service**.



3. In the **Enter Role Entity Info** step, select **Tencent Container Security Service (tcss)** and click **Next**.

©2013-2022 Tencent Cloud. All rights reserved.

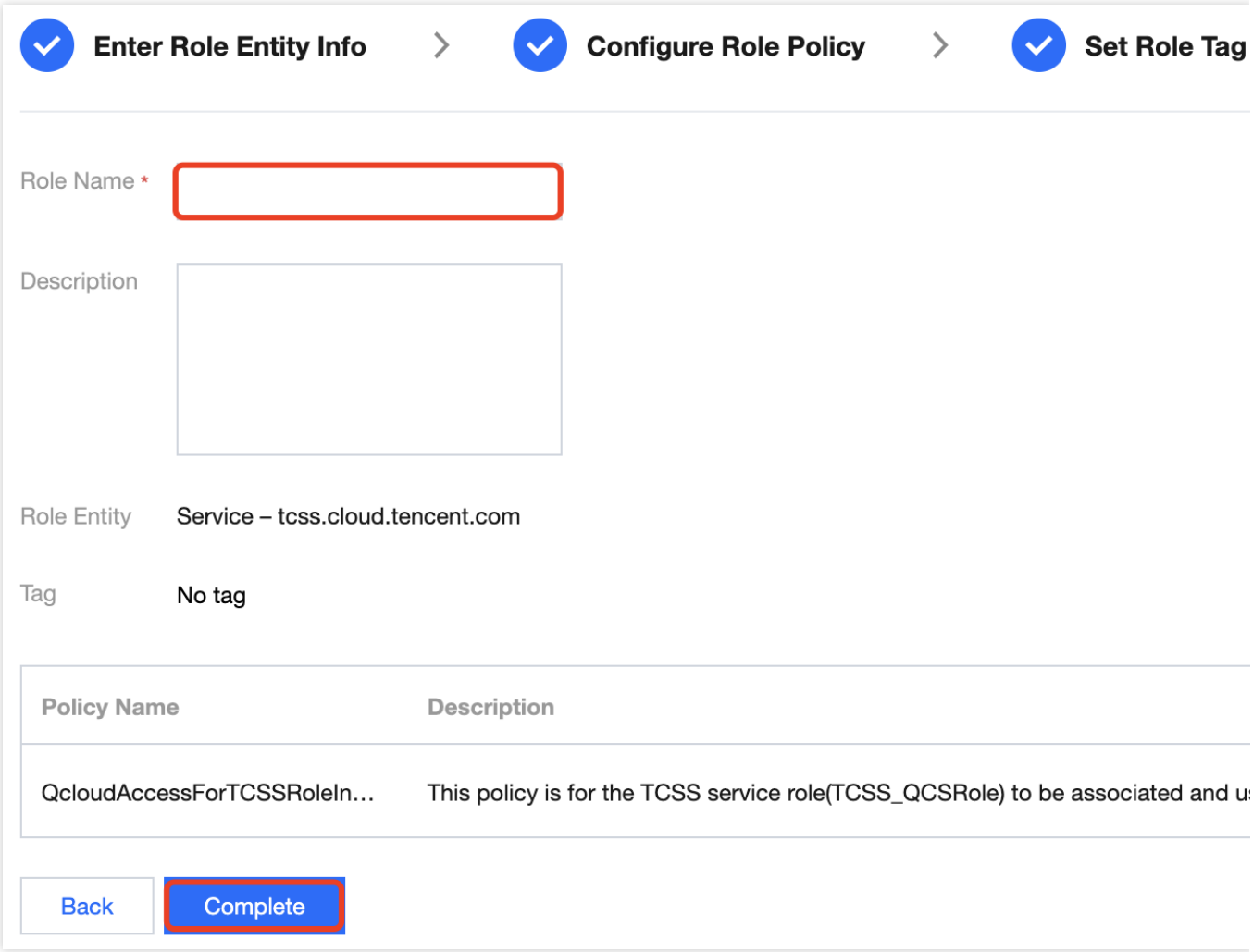
4. In the **Configure Role Policy** step, search for and select `QcloudCamSubaccountsAuthorizeRoleFullAccess` and `QcloudAccessForTCSSRoleInCkafka` and click **Next**.



5. In the **Set Role Tag** step, customize the role tag or leave it empty and click **Next**.

6. In the **Review** step, configure **Role Name** as **TCSS_QCSRole** (as TCSS pulls the configured permission based on the role name) and customize **Description** or leave it empty. After the configuration, click **Complete**. Then, you can view the role and associated policy on the **Role** page after authentication.

©2013-2022 Tencent Cloud. All rights reserved.



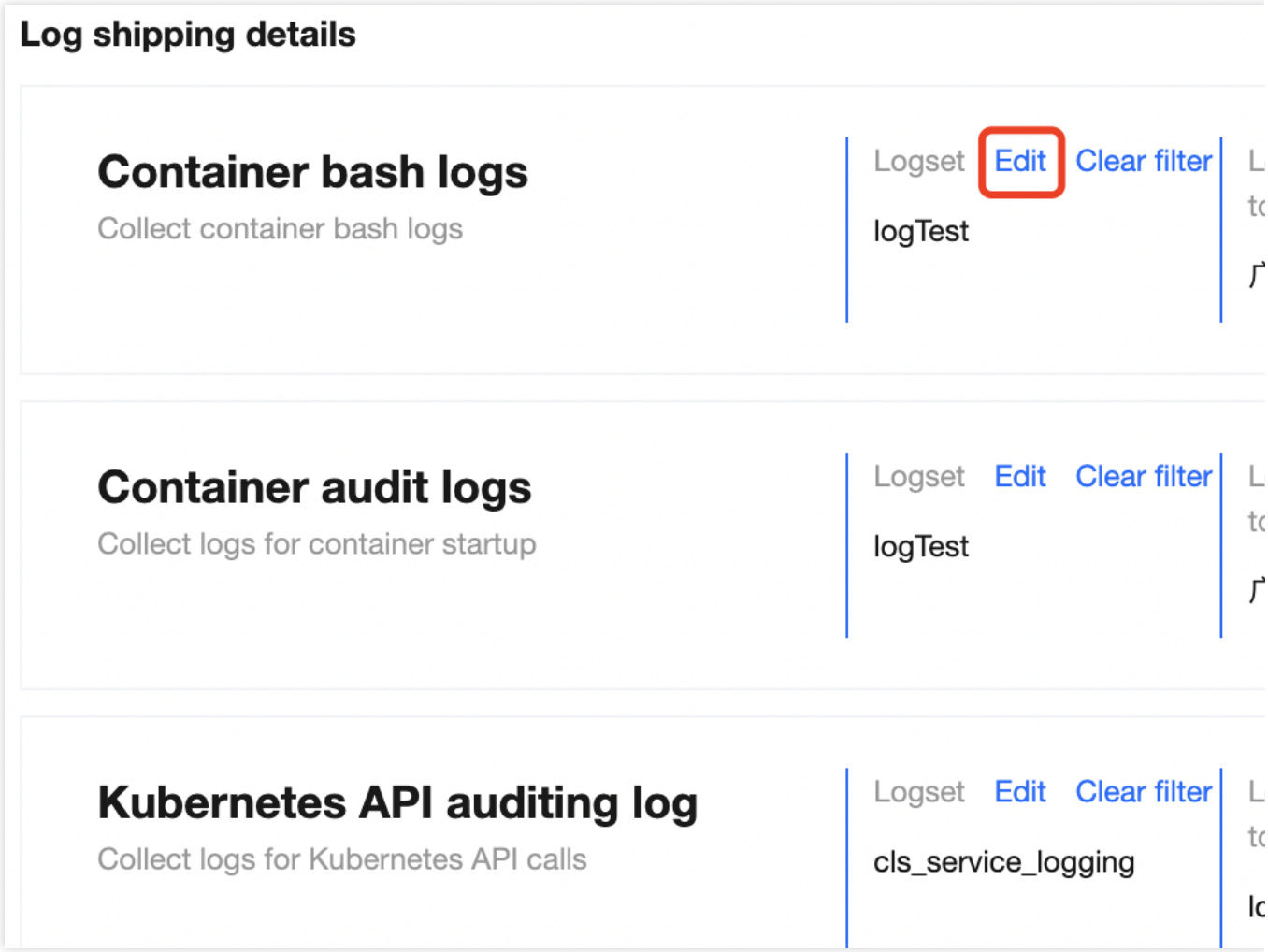
7. After the configuration, go back to the TCSS console, log in to the shipping account, and check whether the authorization is successful as prompted on the page, and if so, configure the public domain name, message queue, and topic information for log shipping to CKafka.

Shipping to CLS

Shipping to CLS requires authorization for access. After the authorization, check whether shipping is enabled for each log type and the logset and log topic information.

1. On the **Log Analysis** page, click **Log shipping** > **CLS** at the top.
2. On the **CLS** tab, select the target log type and click **Configure now**.

©2013-2022 Tencent Cloud. All rights reserved.

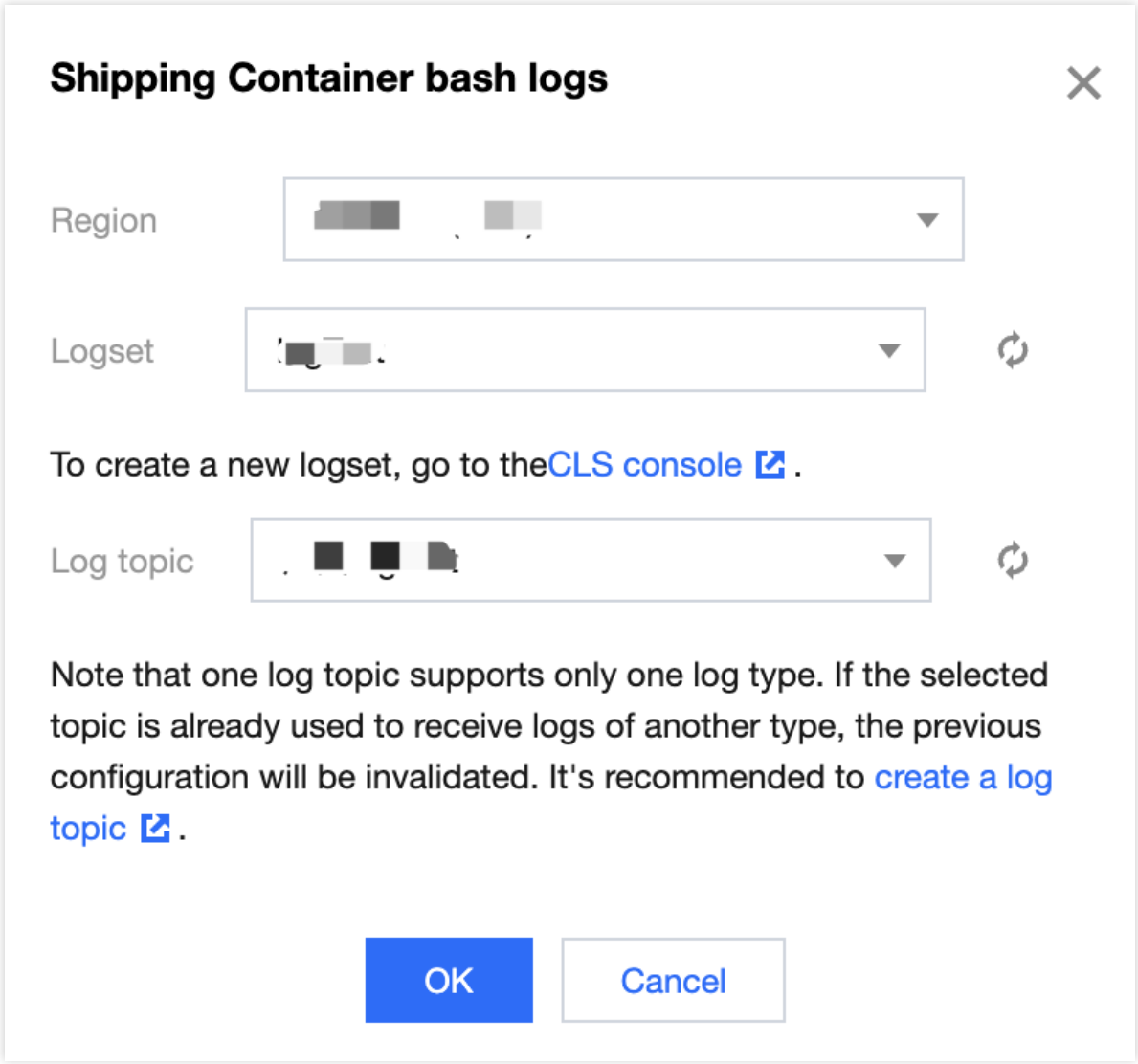


3. On the shipping settings page, configure parameters and click **OK**.

Note:

After CLS access is authorized and shipping to CLS is enabled under your account, pay-as-you-go storage space will be automatically created in CLS, along with pay-as-you-go bills. For billing details, see Billing Overview.

©2013-2022 Tencent Cloud. All rights reserved.



©2013-2022 Tencent Cloud. All rights reserved.

Hybrid Cloud Installation Guide
Overview

Last updated：2024-01-23 15:44:44

Background

With the popularity of cloud migration, more and more medium and large enterprises adopt the hybrid cloud mode, as it is as cost-effective, agile, flexible, and easy to use as the public cloud and as controllable, secure, and highly available as the private cloud. The hybrid cloud management feature is launched to support connecting to non-Tencent Cloud instances for better unified management and container security monitoring.

Feature overview

ECM and Lighthouse instances can be automatically connected to TSCC.
Non-Tencent Cloud instances can be manually connected to TSCC, such as those in the private cloud, Alibaba Cloud, Huawei Cloud, QingCloud, AWS, and UCloud.

System compatibility

Linux:
RHEL: 6 and 7 (64-bit)
Ubuntu: 9.10–18.04 (64-bit)
Debian: 6, 7, 8, and 9 (64-bit)
CentOS: 6 (64-bit) and later

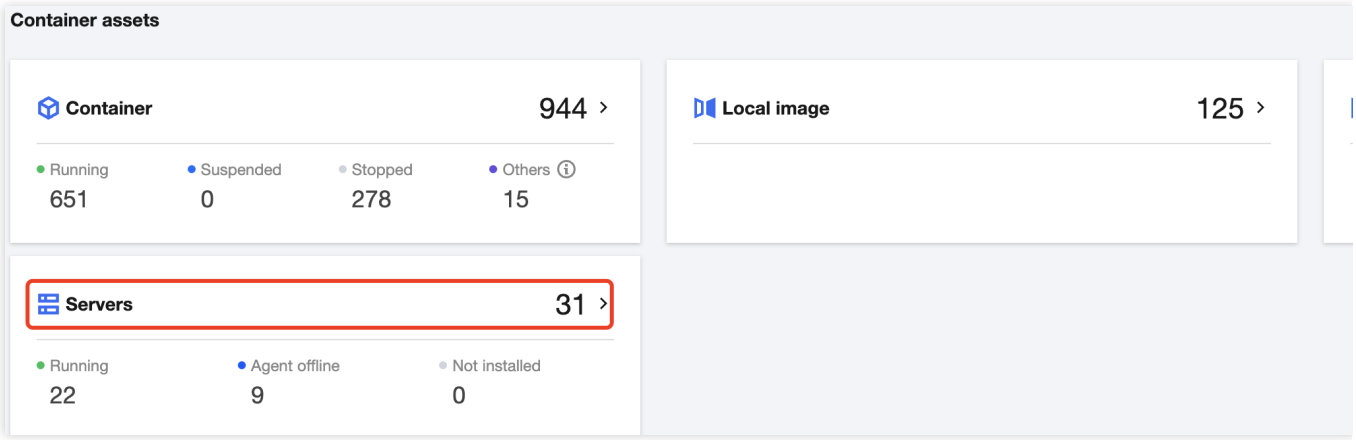
©2013-2022 Tencent Cloud. All rights reserved.

Configuring Non-Tencent Cloud Server

Last updated：2024-01-23 15:44:44

Step 1. Install the TCSS agent

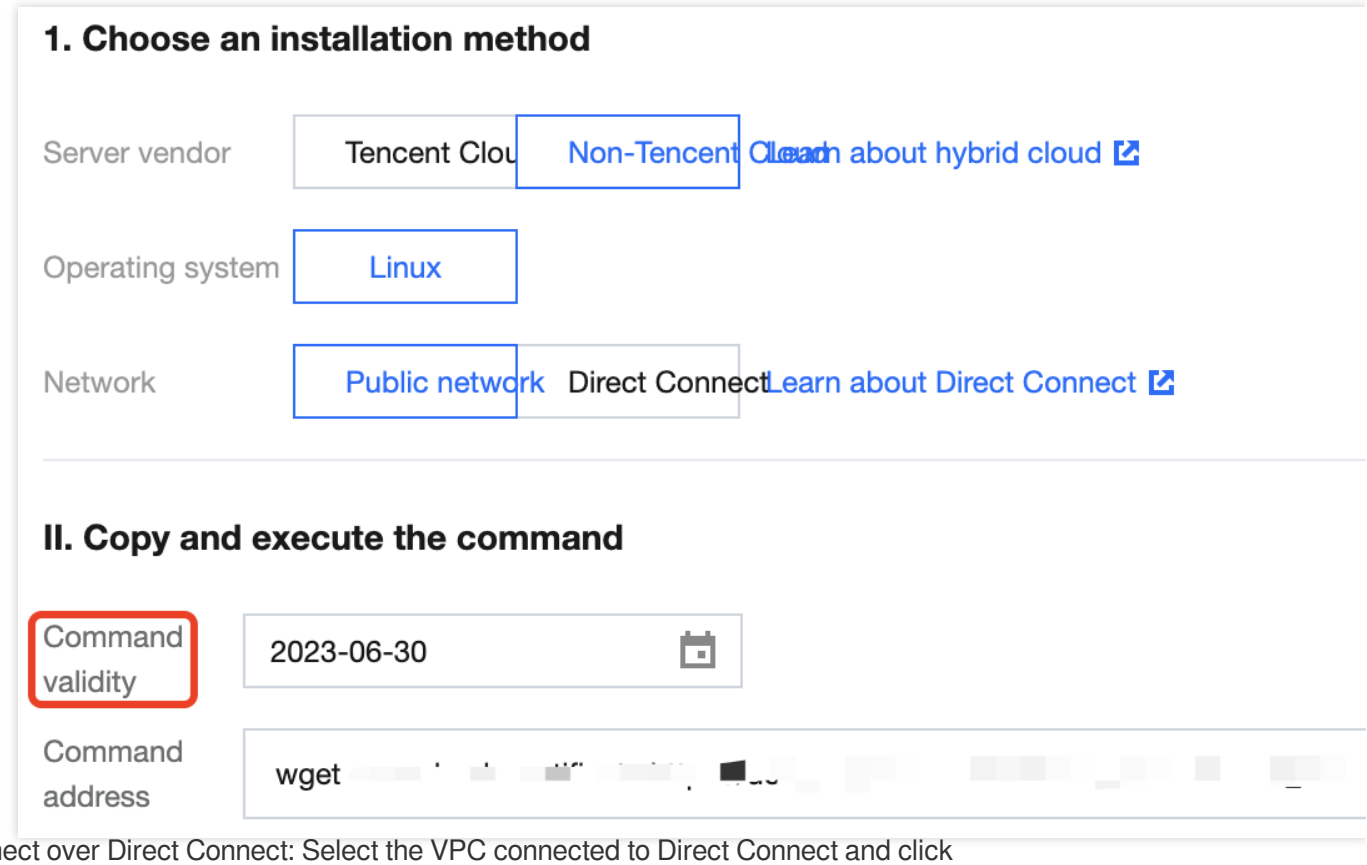
1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Servers** > **Install a TCSS agent** to pop up the **Installation guide** window on the right.



3. In the pop-up window, select the **Server vendor**, **Server type**, and **Network**. To connect over Direct Connect, select **Direct Connect**; otherwise, select **Public network**.
Connect over the public network: Click

to copy and run the corresponding command to install the TCSS agent. Pay attention to the command validity.

©2013-2022 Tencent Cloud. All rights reserved.



Connect over Direct Connect: Select the VPC connected to Direct Connect and click

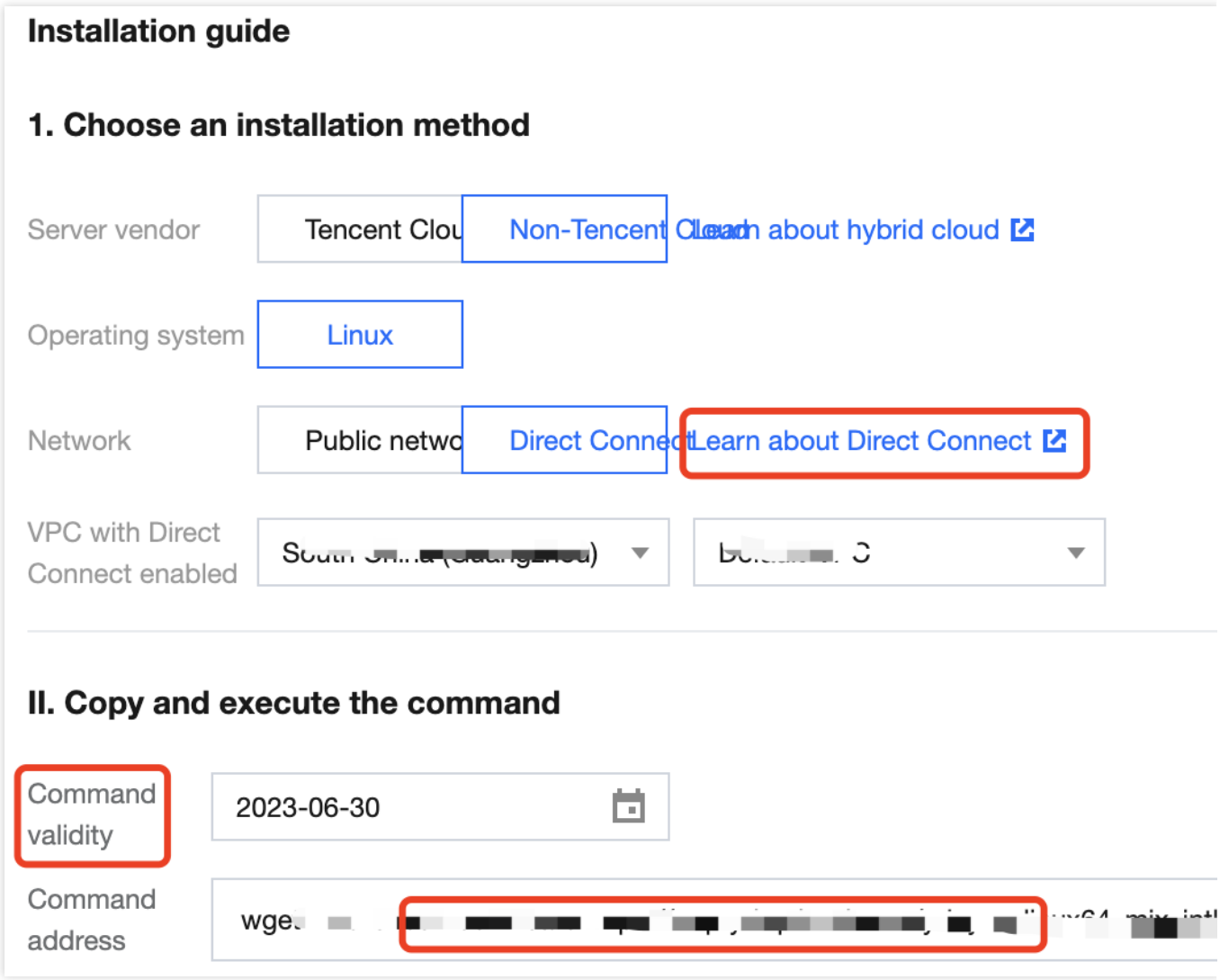
to copy and run the corresponding command to install the TCSS agent. **Pay attention to the command validity**.

Note:

For more information on Direct Connect, click **Learn about Direct Connect** to go to the Direct Connect console.

To allow the target IP in the firewall, grant the permission as instructed below.

©2013-2022 Tencent Cloud. All rights reserved.



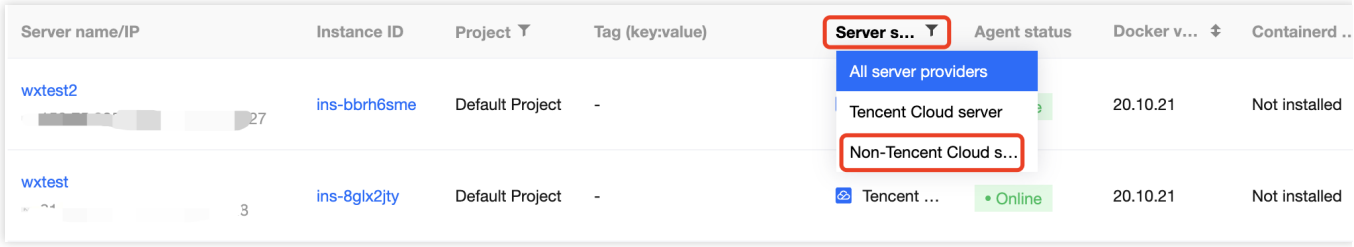
Step 2. Check whether the installation is successful

1. Check whether the installation command runs successfully according to the installation guide. Open the task manager and check whether the YDLive process is running, and if so, the installation is successful.
Run the `ps -ef | grep YD` command to check whether the YDService and YDLive processes are running.
If not, the root user can run the `/usr/local/qcloud/YunJing/YDEyes/YDService` command to manually start the program.

```
[root@VM_90_131_centos conf]# ps -ef|grep YD
root     16216 21992  0 14:33 pts/3    00:00:00 grep --color=auto YD
root     32707     1  0 11:23 ?        00:00:09 /usr/local/qcloud/YunJing/YDEyes/YDService
root     32724     1  0 11:23 ?        00:00:01 /usr/local/qcloud/YunJing/YDLive/YDLive
[root@VM_90_131_centos conf]# ps -ef|grep YD
```

2. After the successful installation, go to the **Servers** page and select **Server source** > **Non-Tencent Cloud server**.

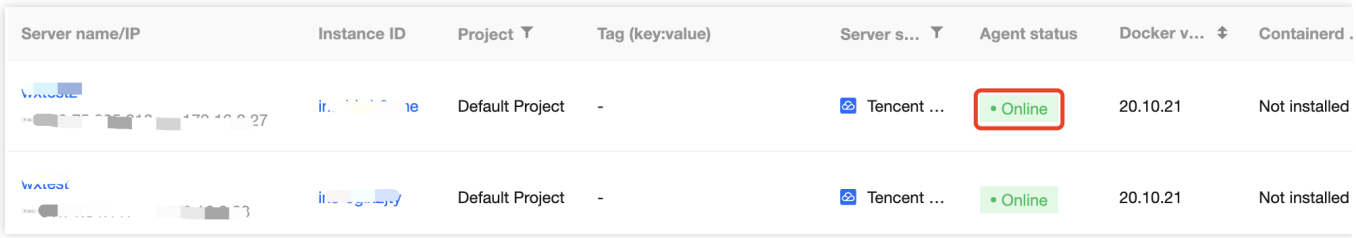
©2013-2022 Tencent Cloud. All rights reserved.



3. If the **Agent status** is **Online**, the installed service is online.

Note:

If it is not online, contact us for assistance.



©2013-2022 Tencent Cloud. All rights reserved.

Connecting Dedicated VPC

Last updated：2024-01-23 15:44:44

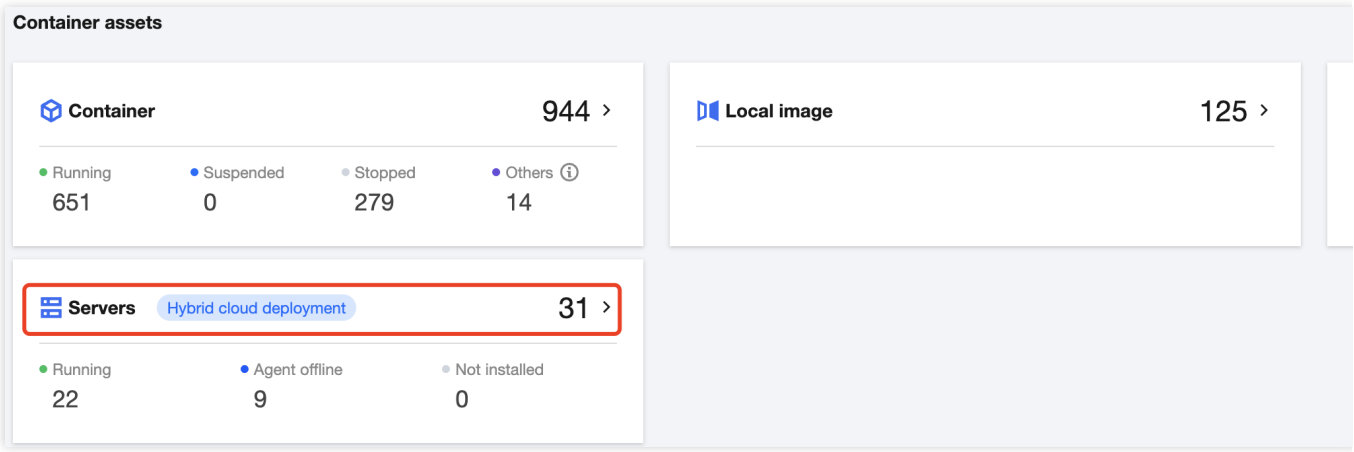
Background

Currently, connection to a VPC over DC is only supported in Southeast Asia (Singapore) region. The public cloud can communicate with the customer's data center network over a VPC, and the agent can be directly installed.
If connection to a VPC over DC is not supported in a region, you need to use CCN to connect the Direct Connect gateway (VPN) and the VPC. You need to purchase the Direct Connect gateway and set up the connection to the VPC over DC.

Directions

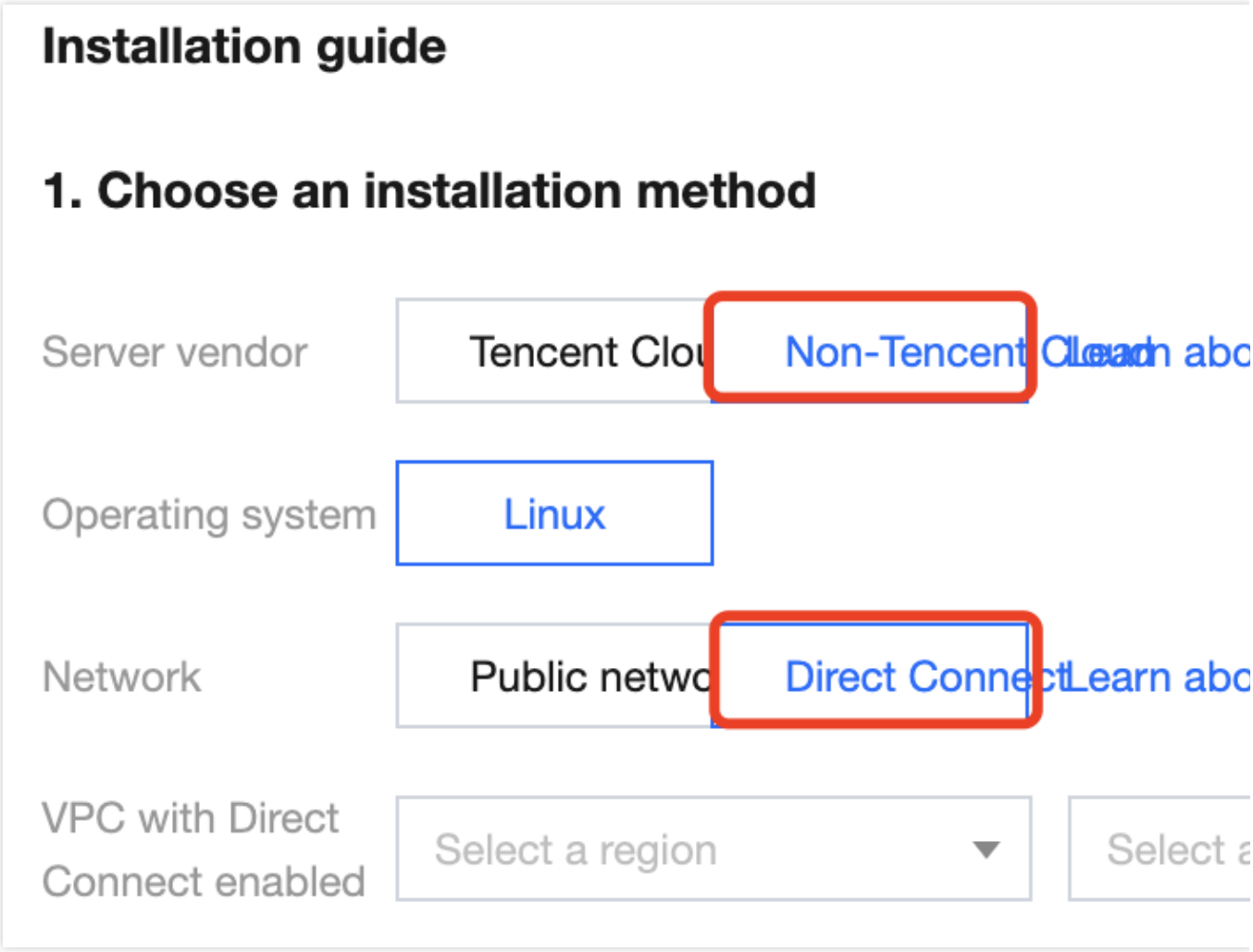
Step 1. Check whether CCN is required for connection

1. Log in to the TCSS console and click **Asset Management** on the left sidebar.
2. On the **Asset Management** page, click **Servers** > **Install a TCSS agent** to pop up the **Installation guide** window on the right.



3. In the pop-up window, select **Non-Tencent Cloud** for **Server vendor** and **Direct Connect** for **Network**.

©2013-2022 Tencent Cloud. All rights reserved.



4. If you are in Southeast Asia (Singapore) region:

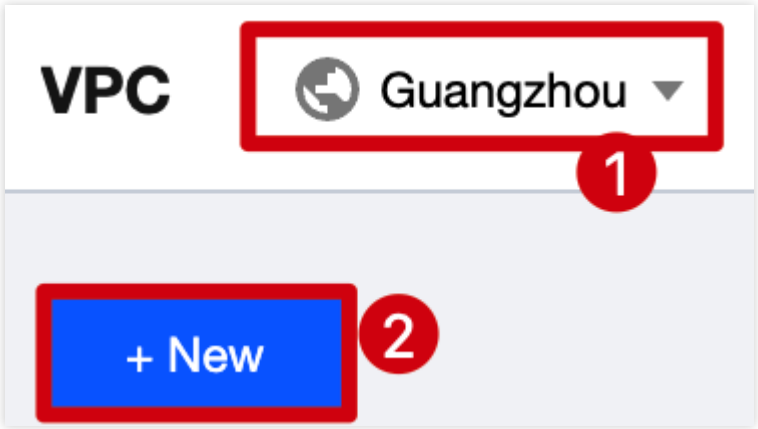
If you have a VPC connected to the non-Tencent Cloud data center network, select the VPC connected to Direct Connect and run the installation command.

If you find no VPC for connection to your non-Tencent Cloud data center network, see step 2.

Step 2. Confirm the VPC for connection to Direct Connect

1. If you have no VPC in Southeast Asia (Singapore) region, log in to the VPC console and click **VPC**.
2. On the **VPC** page, click the drop-down list to select the target region and click **+ New**.

©2013-2022 Tencent Cloud. All rights reserved.



3. In the **Create VPC** pop-up window, enter the required parameters and click **OK**.

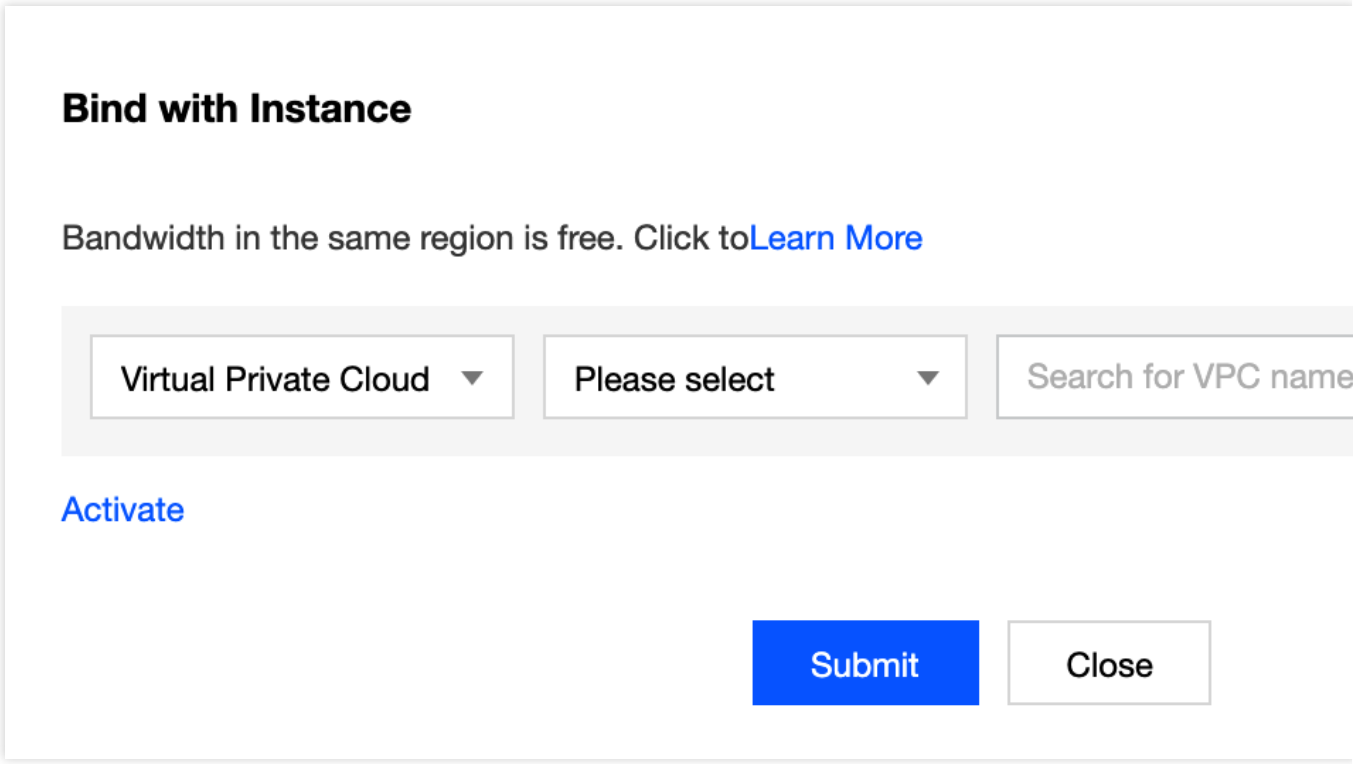
Step 3. Use CCN to connect the VPC to the non-Tencent Cloud data center network connected to Direct Connect

1. If you have the CCN instance connected to the non-Tencent Cloud data center network, add the VPC instance selected in step 2 to the CCN instance.

1.1 Log in to the VPC console and select **CCN** on the left sidebar.

1.2 On the **CCN** page, click **Manage instances** > **Associated to** on the right.

1.3 On the **Associated to** page, click **Add instance**, add the VPC instance selected in step 2 to the CCN instance, and click **OK**.



2. If you haven't configured a CCN instance, create one.

©2013-2022 Tencent Cloud. All rights reserved.

2.1 Log in to the VPC console and select **CCN** on the left sidebar.

2.2 On the **CCN** page, click **+ New**.

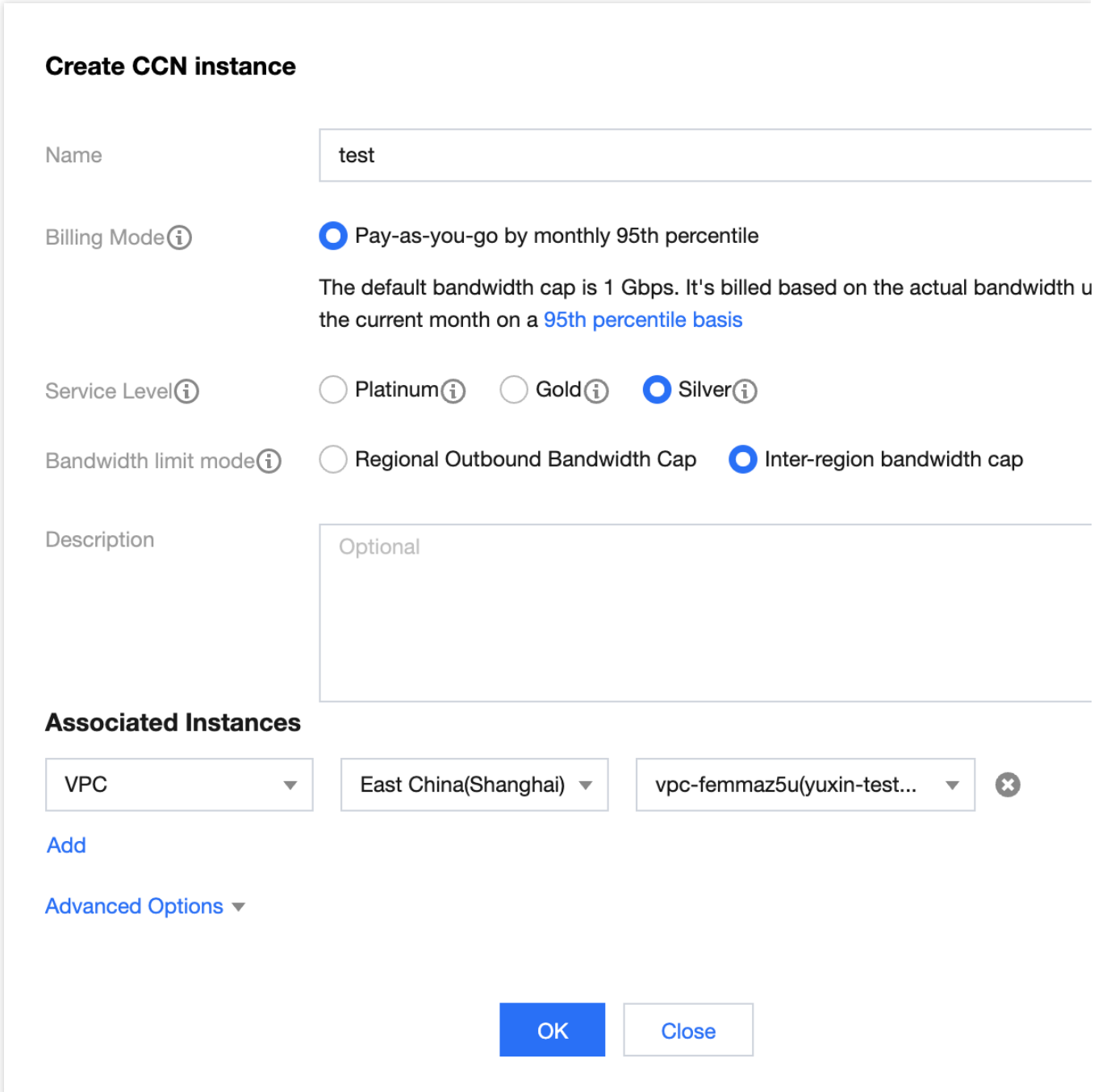
2.3 In the **Create CCN instance** pop-up window, enter the required parameters and click **OK**.

Note:

Direct connect gateway: Select the Direct Connect gateway connected to your non-Tencent Cloud data center network.

VPC: Select the VPC instance selected in step 2.

If an IP range conflict occurs, go back to step 2 and select another VPC instance or create one.



3. Go back to the TCSS console and get the installation command as instructed in step 1. You need to open ports 5574, 8080, 80, and 9080 of the IP described in step 1 for your non-Tencent Cloud data center network.

©2013-2022 Tencent Cloud. All rights reserved.

FAQs

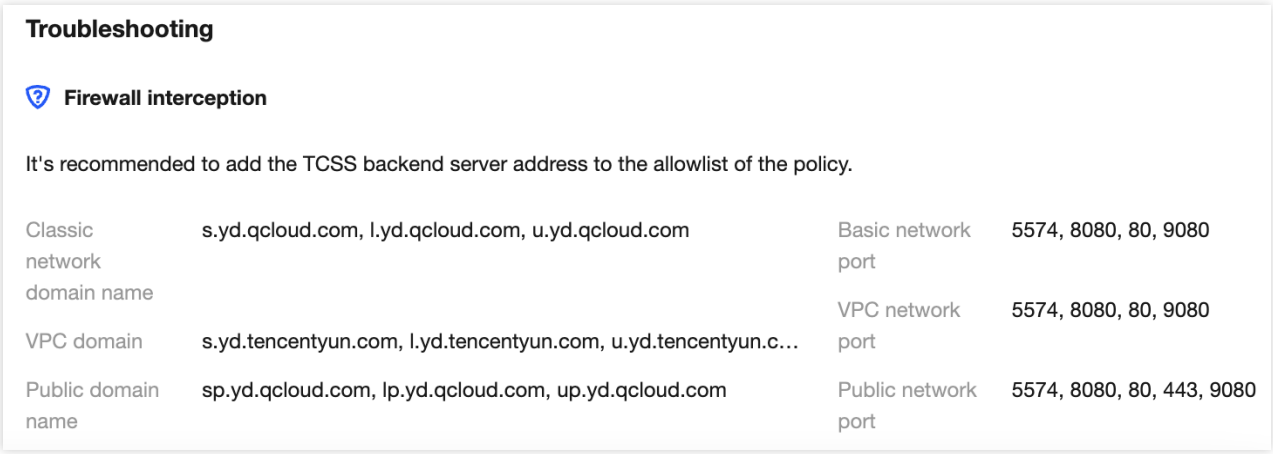
Last updated：2024-01-23 15:44:44

What are the destination address and ports for the cloud connection over Direct Connect?

Allow the destination address and ports in the firewall as shown below.

Note:

The address and ports will not change.



Can the TCSS agent be installed for IDCs outside the Chinese mainland?

Yes. The TCSS agent can be installed as long as the network is connected and the system meets the requirements.

When will the non-Tencent Cloud instance be displayed in the console after the agent is installed?

Within seconds.

Do I need to purchase the console if I use a non-Tencent Cloud instance?

No. The management and billing take place in the public cloud console.

What are the destination IP and ports for IDC access to the cloud network?

The destination IP is included in the installation command, and the ports are 5574, 80, 8080, and 9080.

Can I use TCSS if the private network instance cannot access the public network or there is no Direct Connect?

No.

Does the hybrid cloud agent conflict with Zabbix processes?

©2013-2022 Tencent Cloud. All rights reserved.

There is no special processing for Zabbix or injection. Check for other agent installation drivers on the instance.

©2013-2022 Tencent Cloud. All rights reserved.

Compromised Container Isolation

Last updated：2024-01-23 15:44:44

In case of container attacks in the business environment, such as container escape, viruses, trojans, infectious worms, horizontal detection or attacks by compromised containers, or malicious container pull by attackers due to cluster/node vulnerabilities or improper configuration, you need to quickly isolate the container network.

Note:

As isolating the container network may affect normal business operations, we recommend you first confirm that the container is risky and isolation is necessary to avoid intrusions.

Isolating the Container Network

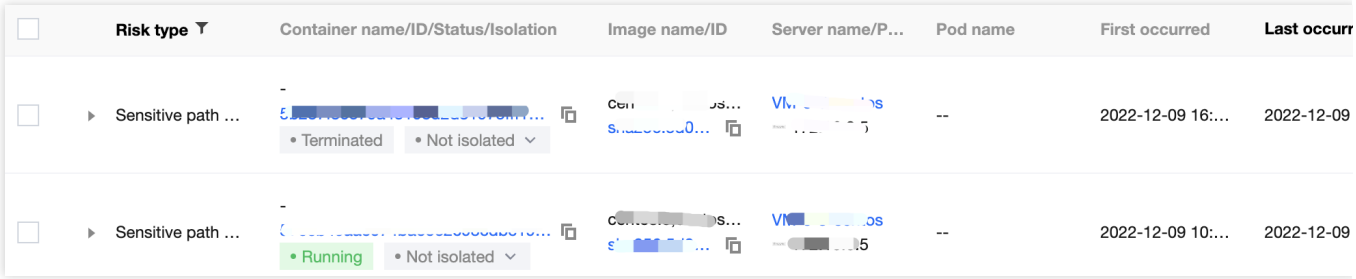
You can use the container network isolation feature on the Runtime Security, Advanced Prevention, or Asset Management page. The effect may differ by module as shown below:

Module Name	Feature Details
Container escape	If the container is isolated successfully in case of a security event, the system will disconnect the container from the network and mark the security event as processed.
Reverse shell	
Abnormal process	
File tampering	
High-risk syscall	
Virus scanning	Isolating the container alone cannot eliminate virus or trojan risks. Therefore, after the container is isolated successfully in case of a security event, the system will disconnect the container from the network but will not mark the security event as processed. To change the event status, you need to have the viruses or trojans in the container automatically isolated or isolate them manually.

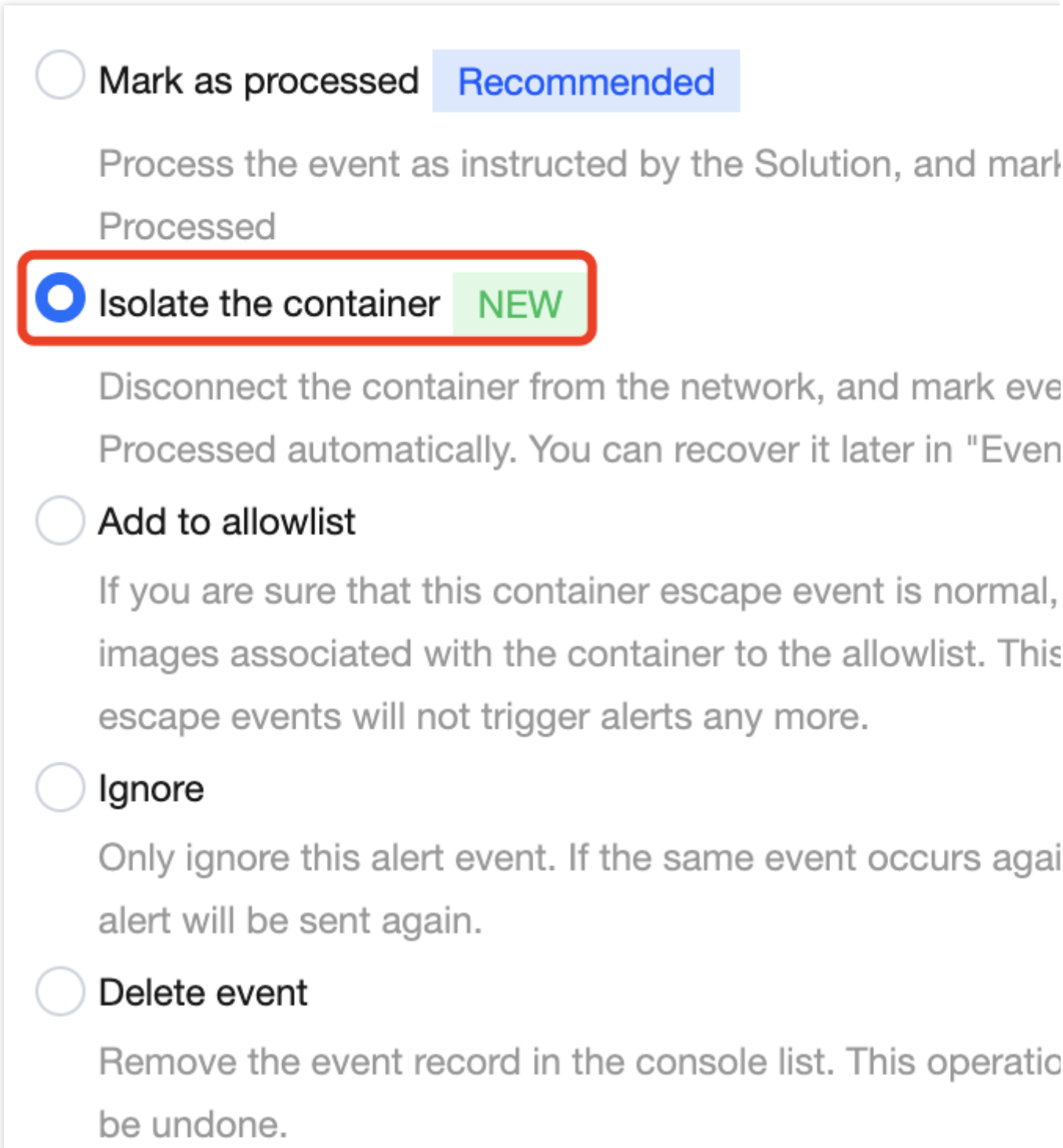
Runtime security or advanced prevention

1. Log in to the TCSS console and click **Runtime Security** > **Container Escape** on the left sidebar.
2. On the **Container Escape** page, select the target container and click **Process** in the **Operation** column.

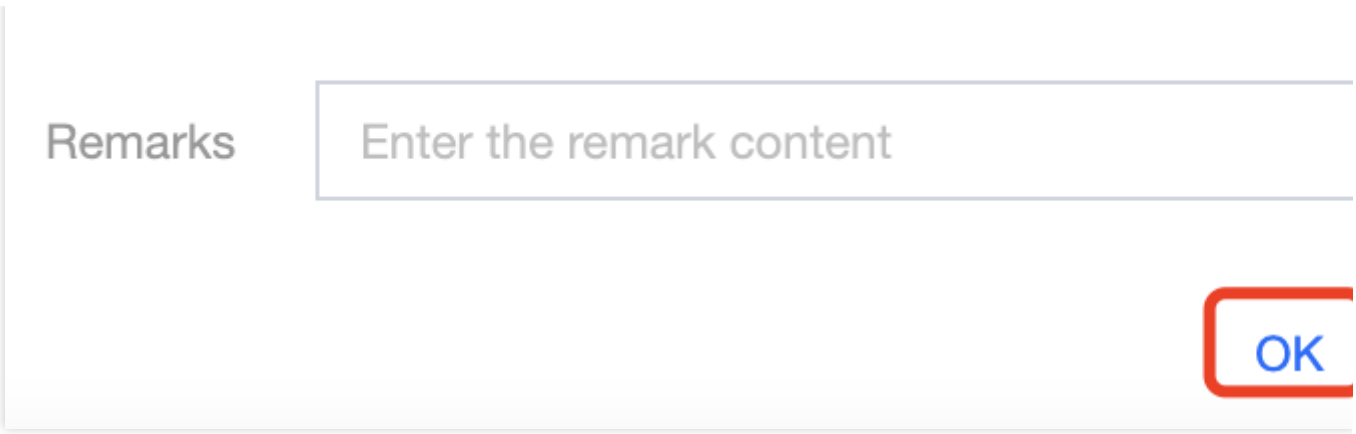
©2013-2022 Tencent Cloud. All rights reserved.



3. Select **Isolate the container**, enter the remarks, and click **OK**.

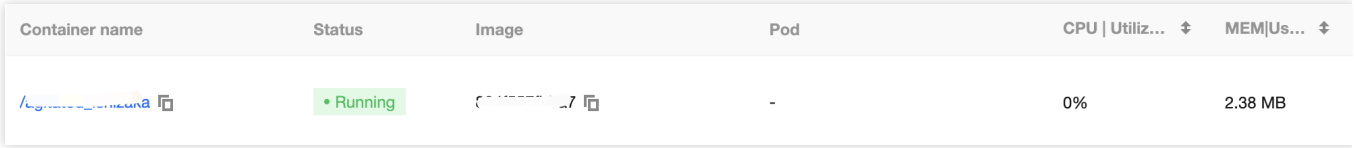


©2013-2022 Tencent Cloud. All rights reserved.



Asset management

1. On the **Asset Management** page, click **Container**.
2. On the **Container** page, select the target container and click **Isolate the container**.



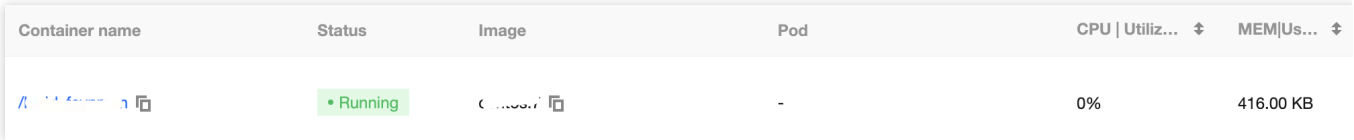
3. In the pop-up window, click **OK**.

Note:

If the container is isolated, it will be disconnected from the network.

Canceling Isolation of the Container Network

To recover the container network after processing the risks in the container, click **More** > **Cancel isolation** in the security event list on the **Runtime Security** or **Advanced Prevention** page, or click **Asset Management** > **Container**, select the target container, and click **Cancel isolation**.



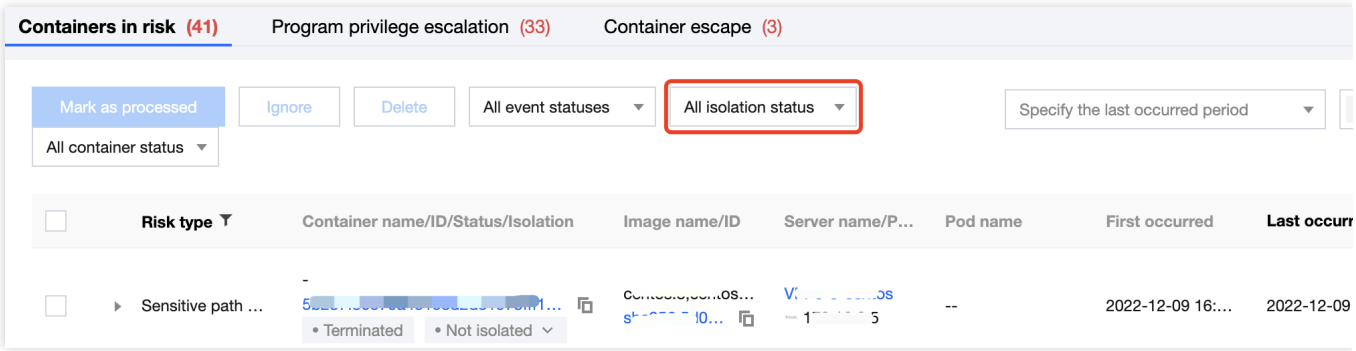
Viewing the Container Isolation Status

The container isolation status is refreshed as one of the container asset attributes on the **Runtime Security**, **Advanced Prevention**, or **Asset Management** page. For example, if you successfully isolate the container network

©2013-2022 Tencent Cloud. All rights reserved.

in the security event list on the **Runtime Security** > **Container Escape** page, you can see that the container is in the **Isolated** status in the list on the **Asset Management** > **Container** page. Similarly, if you isolate the container network in the list on the **Asset Management** > **Container** page, the status will be refreshed in the list on the **Runtime Security** or **Advanced Prevention** page.

You can click the container isolation status drop-down list above the list to filter container events.



©2013-2022 Tencent Cloud. All rights reserved.