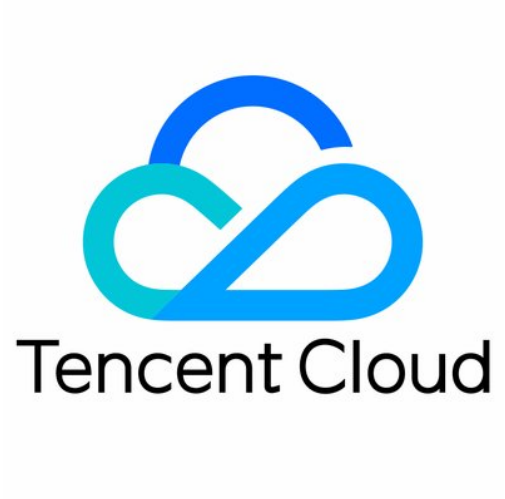
Tencent Container Security Service

FAQs

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.

FAQs

Last updated：2024-01-23 15:35:06

How do I protect the container security?

TCSS can quickly scan images and image repositories for various problems, including vulnerabilities, trojans, viruses, and sensitive information, to help you protect image security. It provides security features such as container escape, process allowlist/blocklist, and file access control to protect the container runtime security. It also offers security operations logs to assist you in visualizing container security.

How do I monitor the container health?

You can use the security operations feature of TCSS to visualize the container security information, and then leverage features such as security policy to improve the security operations quality and efficiency.

Does TCSS conflict with other security products?

No. Traditional server security products take effect only for the operating system layer and cannot identify security problems in containers. Traditional firewalls are mainly designed for the north-south traffic business model and cannot manage massive and complicated container environments at a fine granularity.

How often is the vulnerability library of TCSS updated?

TCSS gets vulnerability information from official sources in real time and updates the vulnerability library at a fixed time every day.

Can I use TCSS across regions?

No.

Can I deploy TCSS offline or across platforms?

Yes. For more information, see Hybrid Cloud Installation Guide.

What is the relationship between an image and a container?

An image is a read-only file that contains the environment and code necessary for a program to run. It is the basis for container running. Containers depend on images when they are started or created. Different containers can be created from different images or from the same image based on different parameters.
A container is a running instance created from an image. Each container can be enabled, started, stopped, or deleted. Containers are isolated from each other to secure application operations.

©2013-2022 Tencent Cloud. All rights reserved.