

Tencent Container Security Service

Release Notes

Product Documentation



Copyright Notice

©2013-2023 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



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.

Release Notes

Last updated : 2023-03-06 16:05:14

September 2022

Update	Description	Release Date	Documentation
Added the container network policy feature	The container network policy provides network policy distribution and management capabilities for cluster containers based on native Kubernetes NetworkPolicies. It defines the protection objects in the cluster and sets their outbound and inbound rules to control network access between containers.	2022-09-19	Container Network Policy

August 2022

Update	Description	Release Date	Documentation
Supported the escape allowlist	When container escape alarms are troubleshooted, certain alarms found to be triggered by the normal business don't need to be fixed and can be added to the allowlist.	2022-08-22	Escape Allowlist
Supported exploit prevention	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 alarming 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.	2022-08-11	Exploit Prevention

June 2022

Update	Description	Release Date	Documentation
Supported updating specified servers	Assets can be updated on specified servers for asset management and local images to avoid time-consuming full updates.	2022-06-22	Local Image
Supported vulnerability detection	Vulnerability detection provides vulnerability scan, troubleshooting, fix, and prevention throughout the entire process, helping you scan for more actual vulnerability risks and providing further countermeasures through exploit prevention and fix. It minimizes the possible impact of vulnerability risks on your business in a smarter and easier way.	2022-06-09	Vulnerability Scan
Supported automatic isolation of malicious samples	Container files found to be in the system blocklist are automatically isolated.	2022-06-07	Virus Scanning
Supported connecting self-built clusters to TCSS	Self-built clusters can be connected to TCSS for unified management as well as risk check and management.	2022-06-02	Self-Built Cluster

May 2022

Update	Description	Release Date	Documentation
Supported isolating compromised containers	The container network isolation feature can be used in runtime security, advanced defense, or asset management to prevent intrusions from becoming worse.	2022-05-26	Compromised Container Isolation

April 2022

Update	Description	Release Date	Documentation
Optimized the display of container escape	Security incidents are categorized into three types based on the sequence of container escapes performed by intruders: risky container, program privilege escalation, and container escape.	2022-04-20	Container Escape
Supported the display of cluster assets	Asset management supports displaying cluster asset details.	2022-04-18	Cluster Asset

March 2022

Update	Description	Release Date	Documentation
Supported baseline scans within a specified scope	The scope of check items can be set for a baseline scan, which takes effect for all baseline check items, including containers, images, and K8s.	2022-03-28	Baseline Management
Supported log analysis	Container bash logs, container startup audit logs, and Kubernetes API audit logs are provided, statement search and query are supported, and visual report, statistical analysis, and export features are available. All this helps you quickly query the business logs and trace the security incidents of containers.	2022-03-11	Log Analysis
Supported displaying the component information of local images	Image asset details display the information of components and their associated vulnerability risks.	2022-03-08	Local Image

February 2022

Update	Description	Release Date	Documentation
--------	-------------	--------------	---------------

Update	Description	Release Date	Documentation
Supported real-time update of the container status	When the container status changes, the latest status is reported in real time to help you get the latest asset information and handle security incidents.	2022-02-17	Container
Supported automatic licensing for images	After automatic licensing is enabled for images, newly added image assets within the specified scope will be automatically licensed during each asset data update, including agent asset reporting and manual sync.	2022-02-15	Local Image

January 2022

Update	Description	Release Date	Documentation
Supported filtering the latest version of repository images	The latest version of repository images can be quickly filtered.	2022-01-23	Repository Image

December 2021

Update	Description	Release Date	Documentation
Supported the hybrid cloud	The hybrid cloud management feature is launched to support connecting to non-Tencent Cloud instances for better unified management and container security monitoring.	2021-12-08	Hybrid Cloud Installation Guide

November 2021

Update	Description	Release Date	Documentation
--------	-------------	--------------	---------------

Update	Description	Release Date	Documentation
Supported cluster security	The cluster check feature provides the cluster checklist, cluster risk statistics, cluster check details, and check item management. It allows installing the check component for specified clusters, performing risk checks, and viewing risk details.	2021-11-10	Cluster Check

October 2021

Update	Description	Release Date	Documentation
Supported flexible billing	If the number of virtual cores in your purchased Pro Edition is fewer than the total number of cores on the container cluster node in the current business environment, and you don't purchase more cores, the flexible billing - postpaid mode will apply.	2021-10-21	Purchasing Pro Edition
Adapted container assets to containerd	The TCSS client is adapted to containerd to support reporting containerd container assets and intrusions.	2021-10-09	Container

September 2021

Update	Description	Release Date	Documentation
Supported the virus scanning feature for runtime security	The virus scanning feature checks for risky files called by running containers in real time. You can also manually trigger quick scan to check for malicious viruses, trojans, and web shells in the container.	2021-09-22	Virus Scanning

August 2021

Update	Description	Release Date	Documentation
Supported the Harbor repository for repository images	Repository images support TCR/CCR and the third-party Harbor repository.	2021-08-12	Repository Image

July 2021

Update	Description	Release Date	Documentation
Launched public cloud TCSS	TCSS provides rich security features such as container asset management, image security, and runtime intrusion detection. It safeguards containers throughout their entire lifecycle from image generation and storage to runtime and helps you set up a container security protection system.	2021-07-19	Overview