Red Hat Advanced Cluster Security for Kubernetes 3.73

Release notes

Highlights what is new and what has changed with Red Hat Advanced Cluster Security for Kubernetes releases

Last Updated: 2023-06-10

Red Hat Advanced Cluster Security for Kubernetes 3.73 Release notes

Highlights what is new and what has changed with Red Hat Advanced Cluster Security for Kubernetes releases

Abstract

The release notes for Red Hat Advanced Cluster Security for Kubernetes summarize all new features and enhancements, notable technical changes, deprecated and removed features, bug fixes, and any known bugs upon general availability.

Table of Contents

CHAPTER 1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.73

Red Hat Advanced Cluster Security for Kubernetes (RHACS) is an enterprise-ready, Kubernetes-native container security solution that protects your vital applications across build, deploy, and runtime stages of the application lifecycle. It deploys in your infrastructure and integrates with your DevOps tools and workflows to deliver better security and compliance and to enable DevOps and InfoSec teams to operationalize security.

Table 1.1. Release dates

RHACS version	Released on
3.73.0	6 December 2022
3.73.1	19 December 2022
3.73.2	6 February 2023
3.73.3	6 March 2023
3.73.4	11 April 2023
3.73.5	31 May 2023

1.1. ABOUT THIS RELEASE

RHACS 3.73 includes:

- Red Hat Advanced Cluster Security Cloud Service (Field Trial)
- Improved Vulnerability management dashboard for ACSCS users
- PostgreSQL database option (Technology Preview)
- Build-time Kubernetes network policy generator (Technology Preview)
- Feature enhancements and bug fixes

1.2. NEW FEATURES

1.2.1. Red Hat Advanced Cluster Security Cloud Service

Red Hat Advanced Cluster Security Cloud Service (ACSCS) is a Red Hat managed service that simplifies and accelerates RHACS deployments.

IMPORTANT

ACSCS is available as a Field Trial release. A Field Trial provides approved customers access to Red Hat Advanced Cluster Security Cloud Service for trial purposes. For more information, contact Red Hat Sales.

With ACSCS, Red Hat hosts and maintains your RHACS Central instance. Red Hat assures high availability of your instance with an industry-standard service level agreement (SLA). After launching an ACSCS instance, you can connect your secured clusters and image repositories, and configure integrations to secure your hybrid Kubernetes infrastructure across Red Hat OpenShift Container Platform, Amazon Elastic Kubernetes Service (EKS), Microsoft Azure Kubernetes Service (AKS), and Google Kubernetes Engine (GKE).

For more information and to try ACSCS, see Request early access to Red Hat Advanced Cluster Security Cloud Service.

The following new documentation topics are available for ACSCS installation:

- Getting started with RHACS Cloud Service
- Setting up RHACS Cloud Service on Red Hat OpenShift
- Setting up RHACS Cloud Service on other platforms

NOTE

The following documentation topics do not apply to ACSCS:

- Installing Central services for RHACS on Red Hat OpenShift
- Optional - Configuring Central configuration options for RHACS using the Operator
- Installing Central services for RHACS on other platforms
- Changing configuration options after deploying the central-services Helm charts
- Upgrading the Central cluster
- Enabling offline mode
- Exposing the RHACS portal over HTTP
- Configuring a proxy for external network access
- Configuring endpoints
- Monitoring with Prometheus
- Configuring OpenShift Container Platform OAuth server as an identity provider
- Backing up Red Hat Advanced Cluster Security for Kubernetes
- Restoring from a backup

1.2.1.1. Improved Vulnerability management dashboard for ACSCS users

ACSCS includes a few updates in the vulnerability management dashboard in the RHACS portal. On-premise RHACS installations will eventually include these updates in future versions. ACSCS includes the following changes:

- The vulnerability management dashboard now groups Common Vulnerabilities and Exposures (CVEs) into **Image CVEs**, **Node CVEs**, and **Platform CVEs** categories. You can access these categories when you click **CVEs** on the **Vulnerability Management** view header. Or, when viewing a list of entities, these categories are listed under **All entities**.
- In the **Node CVEs** and **Image CVEs** list views:
    - A new **Operating System** column shows the base operating system of the image that contains the CVE.
    - A new **Severity** column shows the severity of the package's vulnerability in the operating system context. One CVE may have different severity levels depending on the operating system.
- Some CVEs may occur in more than one category. When you select the Defer and Approve option for a CVE from a specific category, that CVE gets deferred only for the selected category. For example, if a CVE applies to both **Node CVEs** and **Image CVEs**, when you defer that CVE from the **Node CVEs** category, it still appears in the **Image CVEs** category.

1.2.2. PostgreSQL database option (Technology Preview)

IMPORTANT

PostgreSQL support is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope .

RHACS will use PostgreSQL as its backend database in the future, replacing the in-memory RocksDB database used today. This transition will be a part of a future release upgrade, with a fully-automated migration from the current architecture to PostgreSQL-based architecture.

With PostgreSQL, customers benefit from improved performance, standard database procedures for scaling the database, backup and restore, and recovery from a disaster using PostgreSQL database backups. In addition, you can use your existing PostgreSQL infrastructure to provision a PostgreSQL database for RHACS.

With RHACS version 3.73, the PostgreSQL option is available as a Technology Preview feature. If you are interested in participating in the Tech Preview program, Red Hat will work with you to manually migrate to PostgreSQL so that you can explore these benefits in a test environment before we release this feature. Contact your Red Hat account representative to participate.

NOTE

When Red Hat releases this feature, PostgreSQL will become a requirement for RHACS, and you will not be able to upgrade RHACS without using PostgreSQL.

1.2.3. Build-time Kubernetes network policy generator (Technology Preview)

IMPORTANT

Build-time Kubernetes network policy generator is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope .

RHACS 3.73 introduces a new build-time capability in the **roxctl** command-line interface (CLI), to generate Kubernetes network policies based on Application YAML manifests. You can use it to develop network policies as part of the CI/CD pipeline before deploying applications on your cluster.

Red Hat developed this feature in partnership with the developers of the NP-Guard project. The build-time network policy generator analyzes Kubernetes manifests in a local folder, including service manifests, configuration maps and workload manifests such as Pod, Deployment, ReplicaSet, Job, DaemonSet, and StatefulSet. It discovers the required connectivity and creates the Kubernetes network policies to achieve pod isolation. These policies allow no more and no less than the needed ingress and egress traffic. For the build-time network policy generation feature, **roxctl** CLI does not need to communicate with RHACS Central. Therefore you can use it in any development environment.

For more details, see Using build-time network policy generator .

1.3. NOTABLE TECHNICAL CHANGES

- RHACS uses GraphQL internally to show data in the RHACS portal. However, Red Hat does not support querying RHACS using GraphQL. Instead, use the REST API queries to access data. The RHACS 3.73 release introduces some breaking changes in the existing GraphQL queries. If you are using GraphQL, see https://access.redhat.com/articles/6986289 and contact Red Hat Consulting.

- Sensor no longer uses **anyuid** Security Context Constraint (SCC). Instead, the default SCC for Sensor is now **restricted[-v2]** or **stackrox-sensor**, depending on the settings. In addition, the **runAsUser** and **fsGroup** for the Admission control and Sensor deployments are no longer hard-coded to **4000** on OpenShift clusters to allow using the **restricted** and **restricted-v2** SCCs. (ROX-9342)

- The service account **central**, which the Central deployment uses, now includes **get** and **list** access to the following resources in the namespace where you deploy Central:

  - pods
  - events
  - Namespaces

- The CSV export API **/api/vm/export/csv** now requires the **CVE Type** filter as part of the input query parameter. Requests that do not have the filter returns an error. Supported values for **CVE Type** are **IMAGE_CVE**, **K8S_CVE**, **ISTIO_CVE**, **NODE_CVE**, and **OPENSHIFT_CVE**.

1.4. DEPRECATED AND REMOVED FEATURES

Some features available in previous releases have been deprecated or removed.

Deprecated functionality is still included in RHACS and continues to be supported; however, it will be removed in a future release of this product and is not recommended for new deployments. For the most recent list of major functionality deprecated and removed, refer to the table below. Additional information about some removed or deprecated functionality is available after the table.

In the table, features are marked with the following statuses:

- GA: General Availability
- TP: Technology Preview
- DEP: Deprecated
- REM: Removed
- NA: Not applicable

Table 1.2. Deprecated and removed features tracker

Feature	RHACS 3.71	RHACS 3.72	RHACS 3.73
RenamePolicyCategory and DeletePolicyCategory Application Programming Interface (API) endpoints	DEP	DEP	REM
Support for violation tags and process tags	DEP	REM	NA
Permissions: **AuthPlugin**, **AuthProvider**, **Group**, **Licenses**, **Role**, **User**, **Indicator**, **NetworkBaseline**, **ProcessWhitelist**, **Risk**, **APIToken**, **BackupPlugins**, **ImageIntegration**, **Notifier**, **SignatureIntegration**, **ImageComponent**	DEP	DEP	REM
Retrieving groups by property	DEP	DEP	REM
vulns fields of **storage.Node** object in response payload of **v1/nodes**	DEP	DEP	REM
/v1/cves/suppress and **/v1/cves/unsuppress**	DEP	DEP	• DEP in RHACS 3.73 • REM in ACSCS

Feature	RHACS 3.71	RHACS 3.72	RHACS 3.73
ids field in the **/v1/cves/suppress** and **/v1/cves/unsuppress** API payload	DEP	DEP	● DEP in RHACS 3.73 ● REM in ACSCS
cves.ids field of the **storage.VulnerabilityRequest** object in the response of **VulnerabilityRequestService** endpoints	DEP	DEP	REM
Scanning support for Ubuntu 21.10	GA	REM	NA
Permission **ClusterCVE**	GA	DEP	DEP
Label and **Annotation** search options	GA	DEP	DEP
Environment variable **ROX_WHITELIST_GENERATION_DURATION**	NA	NA	REM

1.4.1. Removed features

This section provides additional information about some of the removed features listed in the previous table.

- The **ROX_WHITELIST_GENERATION_DURATION** environment variable is removed in the RHACS 3.73 release. You can use **ROX_BASELINE_GENERATION_DURATION** instead.
- Red Hat has removed **whitelist_statuses** from the response of the **/v1/deploymentswithprocessinfo** endpoint.
- The **ids** field in the **/v1/cves/suppress** and **/v1/cves/unsuppress** API payload is renamed to **cves** in the RHACS 3.73 release.
- The **cves.ids** field of the **storage.VulnerabilityRequest** object in the response of **VulnerabilityRequestService** endpoints is renamed to **cves.cves** in the RHACS 3.73 release.
- For the **/v1/groups** endpoint, you can no longer use the **Get**, **Update**, **Mutate**, and **Remove** functions without specifying a value for **props.id** field when using the **props** field. (ROX-11592)
- Red Hat has removed the **ComplianceRunSchedule** resource, which RHACS did not use.
- Red Hat has simplified the RHACS access permissions. The following list describes the new permissions and indicates the removed permissions in the RHACS 3.73.0 release:

  - The **Access** permission replaces the **AuthPlugin**, **AuthProvider**, **Group**, **Licenses**, **Role**, and **User** permissions.
  - The **DeploymentExtension** permission replaces the **Indicator**, **NetworkBaseline**, **ProcessWhitelist**, and **Risk** permissions.
  - The **Integration** permission deprecates the **APIToken**, **BackupPlugins**, **ImageIntegration**, **Notifier**, and **SignatureIntegration** permissions.
  - The **Image** permission replaces the **ImageComponent** permission.

- Central reaches out to Scanner on the **scanner.<namespace>.svc** endpoint instead of **scanner.<namespace>** to respect OpenShift Container Platform’s **NO_PROXY** configuration. If you are using **NO_PROXY** and you experience connectivity issues for image scanning, add ***.svc** or **scanner.<namespace>.svc** to your **NO_PROXY** configuration. (ROX-13034)

- **Label** and **Annotation** search options are removed in the RHACS 3.73 release. They are replaced by the search options listed in the following table:

Table 1.3. Search options

Resource	Deprecated search option	New search option
Node	**Label**	**Node Label**
Node	**Annotation**	**Node Annotation**
Namespace	**Label**	**Namespace Label**
Deployment	**Label**	**Deployment Label**
ServiceAccount	**Label**	**Service Account Label**
ServiceAccount	**Annotation**	**Service Account Annotation**
K8sRole	**Label**	**Role Binding Label**
K8sRoleAnnotation	**Annotation**	**Role Binding Annotation**

1.4.2. Deprecated features

The following list describes the new permissions and indicates the deprecated permissions that will be removed in a future release:

- New permission **Administration** will deprecate the permissions **AllComments**, **Config**, **DebugLogs**, **NetworkGraphConfig**, **ProbeUpload**, **ScannerBundle**, **ScannerDefinitions**, **SensorUpgradeConfig**, and **ServiceIdentity**.
- The permission **Compliance** will deprecate the permission **ComplianceRuns**.

1.4.3. Notice of upcoming in-product docs removal

Beginning in the RHACS 3.74 release, Red Hat will remove the in-product docs accessible from the help menu. If you are using the in-product docs, you can instead download the required documentation in PDF format from Red Hat Customer Portal . (link:ROX-12839)

1.5. KNOWN ISSUES

ACSCS: PKI authentication for user certificates is not supported in this release.

1.6. BUG FIXES

1.6.1. Resolved in version 3.73.0

- Previously, if you were using StackRox Kubernetes Security Platform - Splunk Technology Add-on, results for the **ocp4-cis-node** compliance standard was missing from Splunk. The Splunk integration now includes the **ocp4-cis-node** compliance standard results. (ROX-11937)
- Previously, Central failed on the **v1 CronJob** deployment YAML check. This issue is fixed. (ROX-13500)
- Previously, when you rebooted the OpenShift Container Platform cluster **scanner-db** pod would get stuck in the **init** state. This issue is fixed. (ROX-12556)

1.6.2. Resolved in version 3.73.1

- Previously, after upgrading to RHACS 3.73.0, the Central pod entered a **CrashLoopBackOff** state because of a failing readiness probe. The patch release 3.73.1 fixes this issue.
- The patch release 3.73.1 fixes an issue where the Compliance dashboard in the RHACS portal failed to load compliance results.

1.6.3. Resolved in version 3.73.2

- The patch release 3.73.2 fixes an issue where Central crashed during the migration from rocksDB to PostgreSQL. (ROX-14469)
- Because of an issue in RHACS Operator versions 3.73.0 and 3.73.1, when you tried to update, the Operator incorrectly removed the **metadata.ownerReferences** field on the central PersistentVolumeClaim (PVC), and you could not update Central and Scanner. The patch release 3.73.2 fixes this issue. (ROX-14335)

1.6.4. Resolved in version 3.73.3

Release date: 6 March 2023

- This release of RHACS fixes CVE-2022-47629 in the Docker base image.
- Before this update, RHACS did not show runtime data when the secured cluster was running OpenShift Container Platform 4.12. For more information, refer to the Red Hat Knowledgebase article RHACS is not showing runtime data . This issue is now fixed.
- Previously, due to an issue with the alert reconciliation workflow, Central could crash when reconciling stored and new runtime policy violations. RHACS now logs an error when an unexpected runtime process alert occurs. (ROX-15198)

1.6.5. Resolved in version 3.73.4

Release date: 11 April 2023

- This release of RHACS includes a fix for RHSA-2023:1405 OpenSSL security update for Red Hat Enterprise Linux (RHEL) 8.

1.6.6. Resolved in version 3.73.5

Release date: 31 May 2023

- This release of RHACS includes a fix for CVE-2023-24540 by building RHACS with updated Golang.

1.7. IMAGE VERSIONS

Image	Description	Current version
Main	Includes Central, Sensor, Admission controller, and Compliance. Also includes **roxctl** for use in continuous integration (CI) systems.	**registry.redhat.io/advanced-cluster-security/rhacs-main-rhel8:3.73**
Scanner	Scans images and nodes.	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:3.73**
Scanner DB	Stores image scan results and vulnerability definitions.	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-db-rhel8:3.73**
Collector	Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.	● **registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:3.73** ● **registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:3.73**