Red Hat Advanced Cluster Security for Kubernetes 3.70

Release notes

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

Last Updated: 2022-12-06

Red Hat Advanced Cluster Security for Kubernetes 3.70 Release notes

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

Legal Notice

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.

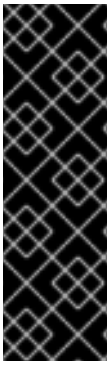
Table of Contents

CHAPTER 1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.70

Table 1.1. Release dates

RHACS version	Released on
3.70.0	2 June 2022
3.70.1	22 June 2022
3.70.2	5 October 2022

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



IMPORTANT

Because of an unexpected schema change in an upstream vulnerability feed on 20 October 2022, Red Hat published a corrupted CVE data file to https://definitions.stackrox.io, and many Central instances downloaded the corrupted file. As a result, when Central processes the corrupted feed data, it fails and enters a **CrashLoopBackOff** state. Although Red Hat has already taken steps to fix the corrupted CVE data file, already affected Central instances do not automatically get out of the **CrashLoopBackOff** state. To get Central back to working condition, follow the instructions at Central in CrashLoopBackOff - 2022-10-20 Incident .

Red Hat Advanced Cluster Security for Kubernetes (RHACS) 3.70 includes feature enhancements, bug fixes, scale improvements, and other changes.

1.1. NEW FEATURES

1.1.1. Verifying image signatures against Cosign public keys

You can use RHACS to ensure the integrity of the container images in your clusters by verifying image signatures against preconfigured keys. You can also create policies to block unsigned images and images that do not have a verified signature and enforce the policy by using an admission controller to stop unauthorized deployment creation. Cosign key signature verification is supported. See Verifying image signatures for more information.

1.1.2. Identifying missing Kubernetes network policies

Kubernetes network policies are vital in helping to enable zero-trust networking within a cluster. They reduce the impact of network attacks by limiting the opportunity for lateral movement. By default, Kubernetes resources are not isolated. Applying network policies is a recommended best practice left to the user.

RHACS 3.70 ships with a new default policy that allows you to easily identify deployments that are not restricted by any ingress network policy and to trigger violation alerts accordingly.

- The default policy is named **Deployments should have at least one ingress Network Policy** It is disabled by default.
- This default policy uses a new policy criterion called **Alert on missing ingress Network Policy**.
- To identify pod isolation gaps, you can clone this default policy or create a new one by using the policy criterion and enabling it on selected resources.

1.2. ENHANCEMENTS

1.2.1. Identifying Spring critical vulnerabilities

RHACS 3.70 adds a policy to detect the Spring Cloud Function RCE vulnerability (CVE-2022-22963) and the Spring Framework Spring4Shell RCE vulnerability (CVE-2022-22965). The policy has a severity level of Critical and is enabled by default.

1.2.2. Automatic Amazon ECR registry integration

Registry integrations for Amazon Elastic Container Registry (ECR) are now automatically generated for Amazon Web Services (AWS) clusters. This feature requires that the nodes' Instance Identity and Access Management (IAM) Role has been granted access to ECR. You can turn off this feature by disabling the EC2 instance metadata service in your nodes. See Amazon ECR integrations for more information.

1.2.3. Improved validation of pod security context

A new policy criterion has been added to validate the value of **allowPrivilegeEscalation** within the Kubernetes security context. You can use this policy criterion to provide alerts when a deployment is configured to allow a container process to gain more privileges than its parent process.

1.2.4. Increased number of allowed inclusion and exclusion scopes

Previously, RHACS limited the number of allowed inclusion and exclusion scopes within a scope to ten each. This restriction has been removed.

1.2.5. Finding ACS admin user credentials easily in the OpenShift Container Platform console

Customers using the recommended Operator method to deploy RHACS on OpenShift Container Platform can now view the credentials for the **admin** user in the OpenShift Container Platform console. When viewing the Central object, the **Details** tab provides a clickable link to the credentials under **Admin Password Secret Reference**. The displayed credentials are the default generated password or a previously configured and stored custom secret. See Verifying Central installation for more information.

1.3. NOTABLE TECHNICAL CHANGES

1.3.1. Vulnerability scanning and reporting for RHCOS nodes

Vulnerability scanning and reporting for Red Hat Enterprise Linux CoreOS (RHCOS) nodes has been disabled until scanning improvements are made for improved accuracy and to support full host-level scanning beyond just Kubernetes components. Currently, RHCOS uses National Vulnerability Database

(NVD) vulnerability data for reporting vulnerabilities for Kubernetes components from RHCOS. In the enhanced version, vulnerability reporting will be based on Red Hat published security data. (**ROX-10662**)

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

Table 1.2. Deprecated and removed features tracker

Feature	RHACS 3.68	RHACS 3.69	RHACS 3.70
Ability to delete default policies	DEP	DEP	REM
Ability to add comments to alerts and processes	GA	DEP	DEP
Anchore, Tenable, and Docker Trusted registry integrations	GA	DEP	DEP
External authorization plug-in for scoped access control	GA	DEP	DEP
FROM option in the Disallowed Dockerfile line policy field	GA	GA	DEP
PodSecurityPolicy (PSP) Kubernetes objects	GA	GA	DEP
RenamePolicyCategory and **DeletePolicyCategory** API endpoints	GA	GA	DEP
--rhacs option for the **roxctl** helm output command	GA	DEP	DEP
Security policies without a **policyVersion**	DEP	DEP	REM
/v1/policies API endpoint response: **field** response body parameter	DEP	DEP	REM

Feature	RHACS 3.68	RHACS 3.69	RHACS 3.70
/v1/policies API endpoint response: **whitelists** response body parameter	DEP	DEP	REM
/v1/nodes and **/v1/images** API endpoint response: **firstNodeOccurrence** response body parameter	GA	DEP	DEP

1.4.1. Deprecated features

- **Anchore**, **Tenable**, and **Docker Trusted Registry** integrations: The RHACS scanner supersedes these integrations.
- **External authorization plug-in for scoped access control** Use the existing in-product scoped access control.
- **FROM option in the Disallowed Dockerfile line policy field** Any policies containing the Disallowed Dockerfile line policy field with the **FROM** option must be updated to remove those policy sections.

1.4.2. Removed features

- RHACS 3.70 no longer supports security policies that do not have **policyVersion** 1.1, including (but not limited to) importing policies.
- Red Hat Advanced Cluster Security for Kubernetes will not allow deleting default policies. Rather than deleting policies, you can disable default policies that you do not need.
- The **/v1/policies** API endpoint response will not return the **field** response body parameter.

1.5. BUG FIXES

1.5.1. Resolved in version 3.70.2

Release date: 5 October 2022

This release contains security updates to address the following common vulnerabilities and exposures (CVEs) in the base images:

- CVE-2022-2526: **systemd-resolved**: **use-after-free** when dealing with **DnsStream** in **resolved-dns-stream.c**
- CVE-2022-29154: **rsync**: remote arbitrary files write inside the directories of connecting peers

1.5.2. Resolved in version 3.70.1

Release date: 22 June 2022

- CVE-2022-1902: Previously, improper sanitization allowed authenticated users to retrieve Notifier secrets from the GraphQL API. This flaw has been fixed. (**ROX-11490**)

1.5.3. Resolved in version 3.70.0

Release date: 2 June 2022

- When configuring a JFrog Artifactory integration, the username and password fields are now optional to allow anonymous pulls. (**ROX-10090**)
- Validation to the web user interface for endpoint URLs in the generic webhook integration caused errors. This issue was fixed. (**ROX-9902**)
- The policy **OpenShift: Kubeadmin Secret Accessed**is no longer triggered if the request was from the default OpenShift **oauth-apiserver-sa** service account, because this is an expected access pattern for the OpenShift API server. (**ROX-10018**)
- The ability to enable or disable notifications for multiple policies selected in the **Policies** list has been reinstated. To change the notification status, select one or more policies and choose **Enable notification** or **Disable notification** from the **Bulk Actions** menu. (**ROX-9985**)
- Fixed a permission issue for vulnerability reports where users with read/write permission could still not create or edit reports. (**ROX-9880**)
- Fixed issue that caused connection problems to the OpenShift Container Platform console after connecting to RHACS or the inability to connect to RHACS if a connection to the OpenShift Container Platform console existed. Central will now respond with a **421 Misdirected Request** status code to requests where the **ServerName** sent via TLS SNI does not match the **:authority** (Host) header. This feature can be turned off by setting the environment variable **ROX_ALLOW_MISDIRECTED_REQUESTS=true**. (ROX-9625)
- When editing a policy, the **Violations Preview** window was unavailable for disabled policies. This issue has been fixed. (**ROX-9435**)
- Added the ability to disable role-based access control (RBAC) related risk computation. Users can exclude RBAC from risk calculation by setting the environment variable **ROX_INCLUDE_RBAC_IN_RISK=false** in the Central deployment spec. (**ROX-10627**)

1.6. 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-rhel8:3.70.2**
Scanner	Scans images and nodes.	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:3.70.2**
Scanner DB	Stores image scan results and vulnerability definitions.	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-db-rhel8:3.70.2**

Image	Description	Current version
Collector	Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.	• **registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:3.70.2** • **registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:3.70.2**