Red Hat Advanced Cluster Security for Kubernetes 3.69

Release notes

Enter a short description here.

Last Updated: 2022-10-21

Red Hat Advanced Cluster Security for Kubernetes 3.69 Release notes

Enter a short description here.

Legal Notice

Copyright © 2022 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

A short overview and summary of the book's subject and purpose, traditionally no more than one paragraph long.

Table of Contents

CHAPTER 1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.69 3
1.1. NEW FEATURES 3
1.1.1. Released in version 3.69.1 3
1.1.1.1. Scanning of the integrated OpenShift Container Registry 3
1.1.1.2. Improved detection of Spring vulnerabilities 3
1.1.2. Released in version 3.69.0 3
1.1.2.1. New policies to manage operational deployment readiness 3
1.1.2.2. Inactive software component identification 4
1.1.2.3. Vulnerability scanning enhancements 4
1.2. IMPORTANT BUG FIXES 4
1.2.1. Resolved in version 3.69.2 4
1.2.2. Resolved in version 3.69.0 4
1.3. IMPORTANT SYSTEM CHANGES 4
1.3.1. Redesigned policy creation workflow 5
1.3.2. Enhancements to sorting and filtering image vulnerabilities 5
1.3.3. Enhanced compatibility with UEFI secure boot 5
1.3.4. Scanner memory limit increases 5
1.4. KNOWN ISSUES 5
1.5. DEPRECATION NOTICE 5
1.6. IMAGE VERSIONS 6

CHAPTER 1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.69

Red Hat Advanced Cluster Security for Kubernetes (RHACS) 3.69 includes feature enhancements, bug fixes, scale improvements, and other changes.

- 3.69.0 Release date: March 21, 2022
- 3.69.1 Release date: April 6, 2022
- 3.69.2 Release date: June 22, 2022

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 .

1.1. NEW FEATURES

1.1.1. Released in version 3.69.1

Release date: April 6, 2022

1.1.1.1. Scanning of the integrated OpenShift Container Registry

Red Hat Advanced Cluster Security for Kubernetes 3.69.1 includes a lightweight version of Scanner delivered as part of the secured cluster services on OpenShift Container Platform to more effectively scan the OpenShift Container Registry. For OpenShift Container Platform users who do not use the Red Hat Advanced Cluster Security for Kubernetes Operator, Red Hat advises you to update your Helm charts to take advantage of these new capabilities.

1.1.1.2. Improved detection of Spring vulnerabilities

RHACS 3.69.1 includes enhancements in Scanner to identify vulnerabilities in packages that follow the Spring naming conventions. Scanner now detects Spring packages impacted by the newly discovered critical vulnerabilities CVE-2022-22963 and CVE-2022-22965 (Spring4Shell).

1.1.2. Released in version 3.69.0

Release date: March 21, 2022

1.1.2.1. New policies to manage operational deployment readiness

With Red Hat Advanced Cluster Security for Kubernetes 3.69, you can now set policies to define the operational readiness of a deployment. New policies include checks for liveness and readiness probes and predefined replica counts.

1.1.2.2. Inactive software component identification

You can now quickly identify if a software package inside a container image is inactive. You can use this information to consider removing the inactive software package as a hardening step or for vulnerability remediation.

1.1.2.3. Vulnerability scanning enhancements

Scanner includes the following new capabilities:

- Support for Alpine 3.15
- Scanner now identifies busybox as a base operating system.
- Ubuntu vulnerability reference links now point to the updated address https://ubuntu.com/security/.

1.2. IMPORTANT BUG FIXES

1.2.1. Resolved in version 3.69.2

Release date: June 22, 2022

ROX-11489: CVE-2022-1902: Previously, improper sanitization allowed authenticated users to retrieve Notifier secrets from the GraphQL API. This flaw has been fixed.

1.2.2. Resolved in version 3.69.0

Release date: March 21, 2022

- **ROX-9587**: Previously, emailed vulnerability reports were incompatible with some e-mail clients. This issue has been fixed.
- **ROX-9166**: Previously, snoozed CVEs that were unsnoozed were not reported in CI when scanning images. This issue has been fixed.
- **ROX-9400**: Previously, RHACS did not remove the related service accounts when you deleted a cluster. This issue has been fixed.
- **ROX-9483**: Previously, certain search conditions using a process name could sometimes cause Central to stop responding. This issue has been fixed.

1.3. IMPORTANT SYSTEM CHANGES

- Red Hat has changed the default **grpcPort** in Scanner's configuration map to **8443**.
- Red Hat is deprecating the following API endpoints:
  - **/v1/clusters-env/kernel-support-available**: Use **/v1/cluster-defaults** instead.
  - **/v1/helm/cluster/add**: Use the Helm charts directly.
  - Empty values for **role.access_scope_id** is deprecated in the **RoleService_CreateRole** and **RoleService_UpdateRole** methods for the **/v1/roles/** endpoint. It is now set to the unrestricted access scope ID **io.stackrox.authz.accessscope.unrestricted**.

1.3.1. Redesigned policy creation workflow

Red Hat Advanced Cluster Security for Kubernetes 3.69 includes more intuitive and easier-to-use policy creation and editing workflows.

1.3.2. Enhancements to sorting and filtering image vulnerabilities

Red Hat Advanced Cluster Security for Kubernetes 3.69 includes new fields for vulnerabilities contained within an image that you use to sort and filter the vulnerabilities list.

1.3.3. Enhanced compatibility with UEFI secure boot

Collector is incompatible with UEFI secure boot when collecting runtime data using kernel modules. In Red Hat Advanced Cluster Security for Kubernetes 3.69, when Collector detects that the host is using UEFI secure boot, it automatically fails over to use EBPF probes to prevent service disruption.

1.3.4. Scanner memory limit increases

Red Hat has increased the default Scanner memory limit from **3000** MiB to **4** GiB.

1.4. KNOWN ISSUES

- **ROX-9750**: The **FROM** instruction in the **DISALLOWED DOCKERFILE LINE** policy field is not recognized by RHACS. For example, creating a policy that disallows **FROM:unwanted.example.com** in the Dockerfile does not generate a policy violation.

1.5. DEPRECATION NOTICE

Red Hat is deprecating some of the features in Red Hat Advanced Cluster Security for Kubernetes 3.69. Red Hat will remove these deprecated features in the following release:

- Red Hat Advanced Cluster Security for Kubernetes 3.71.0:
  - **External authorization plug-in for scoped access control** Use the existing in-product scoped access control.
  - **Anchore**, **Tenable**, and **Docker Trusted Registry** integrations. The RHACS scanner supersedes these integrations.
  - **Alerts and Process Comments**.
- Red Hat Advanced Cluster Security for Kubernetes 3.70.0:
  - Red Hat Advanced Cluster Security for Kubernetes will not allow deleting default policies. So rather than deleting, you can disable default policies that you do not need.
  - The **/v1/policies** API endpoint response will not return the **field** response body parameter.
- In RHACS 3.70, Red Hat will remove the support for security policies that do not have a **policyVersion**. Therefore, if you have externally stored older policies (without **policyVersion** or version prior to 1.1), you must convert them to use **policyVersion** 1.1. To do this, import the old policies into RHACS and then export them again. You can check the **policyVersion** field for your stored policies to identify if they need conversion.

For any questions, please contact the Red Hat support team at support@redhat.com.

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-rhel8:3.69.2**
Scanner	Scans images and nodes.	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:3.69.2**
Scanner DB	Stores image scan results and vulnerability definitions.	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-db-rhel8:3.69.2**
Collector	Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.	**registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:3.69.2** **registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:3.69.2**