Red Hat Advanced Cluster Security for Kubernetes 4.3

Release notes

Highlights what is new and what has changed with Red Hat Advanced Cluster Security for Kubernetes releases
Red Hat Advanced Cluster Security for Kubernetes 4.3 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.
CHAPTER 1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 4.3

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

Table 1.1. Release dates

<table>
<thead>
<tr>
<th>RHACS version</th>
<th>Released on</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>15 November 2023</td>
</tr>
</tbody>
</table>

1.1. ABOUT THIS RELEASE

RHACS 4.3 adds new features, improvements, and updates.

1.2. NEW FEATURES

This release adds improvements related to the following components and concepts.

1.2.1. Increased support for hardware and software

RHACS support has been increased for the following hardware and software:

- Red Hat OpenShift on IBM Cloud: You can now protect Red Hat OpenShift on IBM Cloud by using RHACS. With this release, you can run secured clusters on Red Hat OpenShift on IBM Cloud.
- IBM Power and IBM Z: RHACS Central Services are now supported on IBM Power and IBM Z.
- Red Hat OpenShift Service on AWS: RHACS is supported on ROSA hosted control plane (HCP) enabled clusters.
- Red Hat OpenShift: This release is supported with OpenShift Container Platform 4.14.

For more information, see Supported platforms and installation methods.

1.2.2. Vulnerability reporting 2.0 is generally available

With this release, the Vulnerability Reporting option under the Vulnerability Management (2.0) menu is generally available. Several enhancements have been made to vulnerability reporting, including the ability to customize email templates that are used when reports are sent. For more information, see Vulnerability Reporting.

NOTE

Reports created in the Vulnerability Management 1.0 → Reporting page are automatically migrated. For more information, see Migration of vulnerability reports when upgrading to RHACS version 4.3 and later.
1.2.3. Watch and scan images in Vulnerability Management 2.0

The ability to mark an image as watched has been migrated from the Vulnerability Management (1.0) menu item to Vulnerability Management 2.0. Watched images are still scanned for vulnerabilities even when not in use by an active deployment.

For more information, see Scanning inactive images.

1.2.4. View administration events information

With this release, RHACS introduces an administration events dashboard that allows you to efficiently manage and troubleshoot events within your RHACS instance and significantly improves the reliability and security of your RHACS instance.

For more information, see Using the administration events page.

1.2.5. Scan images by using the roxctl CLI

You can now scan images stored in image registries, including cluster local registries such as the OpenShift Container Platform integrated image registry, by using the roxctl CLI.

For more information, see Image scanning by using the roxctl CLI.

1.2.6. Invite users to your RHACS instance

You can now invite users and define their roles to ensure accurate access control and improve the security of your RHACS instance.

For more information, see Inviting users to your RHACS instance.

1.3. NOTABLE TECHNICAL CHANGES

- When audit logging is enabled, audit log messages now include the source IP address of the audit log request. For more information, see Enabling audit logging.

- The default policy "Iptables Executed in Privileged Container" has been renamed to "Iptables or nftables Executed in Privileged Container" and now also detects the nft process that is used by nftables.

- Risk reprocessing has been changed from potentially being computed every 15 seconds to 10 minutes. This improves system performance by debouncing expensive risk calculations. To use the earlier value for risk reprocessing, set the environment variable ROX_RISK_REPROCESSING_INTERVAL to 15s.

1.4. NOTICE OF UPCOMING CHANGES TO RHACS VULNERABILITY MANAGEMENT

In the past several RHACS releases, we have optimized and enhanced RHACS features and functionality available in the Vulnerability Management (1.0) menu item and migrated them to the Vulnerability Management (2.0) menu item.

The existing page for Risk Acceptance in the Vulnerability Management (1.0) menu item will be migrated to the Vulnerability Management (2.0) menu item in an upcoming release. It will be renamed Vulnerability Exception Management.
We invite you to review the existing features in the Vulnerability Management (2.0) menu item and give us feedback by clicking the red Feedback button in the RHACS web portal.

1.5. DEPRECATED AND REMOVED FEATURES

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

Deprecation 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, see the following table. 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

<table>
<thead>
<tr>
<th>Feature</th>
<th>RHACS 4.1</th>
<th>RHACS 4.2</th>
<th>RHACS 4.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIS Docker v1.2.0 Compliance Standard</td>
<td>NA</td>
<td>DEP</td>
<td>DEP</td>
</tr>
<tr>
<td>Custom Security Context Constraints (SCCs): stackrox-collector, stackrox-admission-control, and stackrox-sensor</td>
<td>DEP</td>
<td>DEP</td>
<td>REM</td>
</tr>
<tr>
<td>Expiration field in Exclusion proto</td>
<td>DEP</td>
<td>DEP</td>
<td>REM</td>
</tr>
<tr>
<td>roxctl connectivity-map</td>
<td>NA</td>
<td>DEP</td>
<td>DEP</td>
</tr>
<tr>
<td>roxctl generate netpol</td>
<td>NA</td>
<td>DEP</td>
<td>DEP</td>
</tr>
<tr>
<td>/v1/clustercves/suppress APIs</td>
<td>NA</td>
<td>NA</td>
<td>DEP</td>
</tr>
<tr>
<td>/v1/clustercves/unsuppress APIs</td>
<td>NA</td>
<td>NA</td>
<td>DEP</td>
</tr>
<tr>
<td>/v1/cve/requests APIs</td>
<td>NA</td>
<td>NA</td>
<td>DEP</td>
</tr>
<tr>
<td>/v1/nodecves/suppress APIs</td>
<td>NA</td>
<td>NA</td>
<td>DEP</td>
</tr>
</tbody>
</table>
### 1.5.1. Deprecated features

The following section provides additional information about deprecated features listed in the preceding table.

- The **Vulnerability Management (1.0)** menu item in the RHACS web portal has been deprecated and future removal is planned. It is replaced by **Vulnerability Management (2.0)**.

- The `/v1/cve/requests` APIs have been deprecated and will be replaced by `/v2/vulnerability-exceptions` APIs in the future. Vulnerability deferral management for host (`/node`) and platform (`/cluster`) vulnerabilities has been deprecated and will be removed in the future. After deferral management is removed, deferrals cannot be created for host and platform vulnerabilities and the existing exceptions enforced on host and platform vulnerabilities will be reverted. The affected APIs are `/v1/nodecves/suppress`, `/v1/nodecves/unsuppress`, `/v1/clustercves/suppress`, and `/v1/clustercves/unsuppress`.

### 1.5.2. Removed features

- The **Vulnerability Reporting** page in the **Vulnerability Management (1.0)** menu item has been removed. Vulnerability reporting is available under the **Vulnerability Management (2.0)** menu item.

- The `/v1/report` APIs have been removed. Use the `/v2/reports` APIs.

### 1.6. BUG FIXES
1.6.1. Resolved in version 4.3.0

Release date: 15 November 2023

- Fixed the diagnostic bundle generation returning an incomplete .zip file when the connection to a secured cluster is lost.
- Fixed an issue with the Sensor upgrade tool failing to upgrade from earlier versions on OpenShift Container Platform clusters.
- In some cases, Common Vulnerabilities and Exposures (CVEs) that were deferred and approved were not added to the list of snoozed CVEs. This behavior was caused by an issue with the /v1/suppress and /v1/unsuppress APIs and has been fixed.
- Fixed file search in the ca-setup.sh file that is used to configure additional Certificate Authorities (CAs). Previously, the script could not find any files in the directory, even with the correct .crt and .pem extensions.

1.7. KNOWN ISSUES

- RHACS version 4.2 introduced additional logic that considers the socket connection state to decide whether Collector reports a connection or not. The expected behavior is that the connection is not reported until it is successfully established. A known issue on the ppc64le architecture can cause a blocked or failing connection to be reported instead of being silenced. No workaround exists for this issue.
- RHACS Central components do not deploy correctly on a default ROSA cluster. The workaround is to scale the worker nodes to allow the RHACS components to be scheduled. See RHACS Central pods do not schedule on a default ROSA cluster for more information.

1.8. IMAGE VERSIONS

<table>
<thead>
<tr>
<th>Image</th>
<th>Description</th>
<th>Current version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main</td>
<td>Includes Central, Sensor, Admission controller, and Compliance. Also includes roxctl for use in continuous integration (CI) systems.</td>
<td>registry.redhat.io/advanced-cluster-security/rhacs-main-rhel8:4.3.0</td>
</tr>
<tr>
<td>Scanner</td>
<td>Scans images and nodes.</td>
<td>registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:4.3.0</td>
</tr>
<tr>
<td>Scanner DB</td>
<td>Stores image scan results and vulnerability definitions.</td>
<td>registry.redhat.io/advanced-cluster-security/rhacs-scanner-db-rhel8:4.3.0</td>
</tr>
<tr>
<td>Image</td>
<td>Description</td>
<td>Current version</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Collector   | Collects runtime activity in Kubernetes or OpenShift Container Platform clusters. | • registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:4.3.0  
• registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:4.3.0 |
| Central DB  | PostgreSQL instance that provides the database storage for Central.         | registry.redhat.io/advanced-cluster-security/rhacs-central-db-rhel8:4.3.0 |