Red Hat Advanced Cluster Security for Kubernetes 4.2

Release notes

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

Last Updated: 2024-04-01

Red Hat Advanced Cluster Security for Kubernetes 4.2 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 4.2

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

RHACS version	Released on
4.2.0	18 September 2023
4.2.1	3 October 2023
4.2.2	23 October 2023
4.2.3	27 November 2023
4.2.4	22 January 2024
4.2.5	14 March 2024

1.1. ABOUT THIS RELEASE

RHACS 4.2 includes the following new features, improvements, and updates:

Platform

- Bring your own PostgreSQL database for RHACS Central (Technology Preview)
- The CORE BPF collection method is now GA
- RHACS Product usage report
- Performance improvements for the Compliance dashboard

Vulnerability management

- Vulnerability scanning support for Registry Mirrors in OpenShift Container Platform
- Configure delegated image scanning in the RHACS portal
- Define new system policies using CVE age or fixability
- On-demand and downloadable CVE report in Vulnerability Management 2.0
- Scanner supports additional operating systems

Network Security

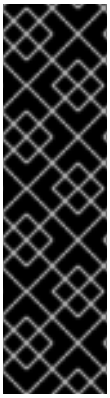
- Improvements to runtime network policy generation
- Build time Network Policy tools (Technology Preview)
- New Listening Endpoints menu in the RHACS portal
- Viewing network policy YAML files from a violation

1.2. NEW FEATURES

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

1.2.1. Bring your own PostgreSQL database for RHACS Central (Technology Preview)

When installing RHACS, instead of creating an exclusive RHACS PostgreSQL database instance, you can use your existing one.



IMPORTANT

Bring your own PostgreSQL database 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 .

For more information, see Installing Central with an external database using the Operator method .

1.2.2. The CORE BPF collection method is now generally available

The runtime collection method based on BPF CO-RE (Compile Once-Run Everywhere) introduced in RHACS 4.1 is now generally available on **x86_64** and **s390x** architectures. To enable it, set the value of your backed-up cluster's **collector.collectionMethod** parameter to **CORE_BPF**.

Additional resources

- Configuring the secured-cluster-services Helm chart with customizations

1.2.3. RHACS product usage report

RHACS now provides a product usage report to help estimate RHACS consumption for licensing. It lists the number of secured OpenShift Container Platform or Kubernetes nodes and the number of CPU units used for secured clusters. To download this report in CSV format, go to the **System Health** dashboard and click **Show product usage**. You can also get the product usage data using the API.

For more information, see Viewing product usage data.

1.2.4. Performance improvements for the Compliance dashboard

RHACS 4.2 includes significant performance improvements for the Compliance dashboard.

Based on testing with a 50-cluster and 4900-node-environment, these improvement includes:

- **2x** speed improvement in cold start.
- From **7x** to **500x** speed boost in **Request after caching**, with a minor improvement in requests involving large data transfers (**600** KiB).
- Memory utilization on Central has decreased from **10** GiB to just **500** MiB.
- CPU utilization has dropped from **4.5** vCPUs to **0.8** vCPUs.

1.2.5. Vulnerability scanning support for Registry Mirrors in OpenShift Container Platform

If you have a disconnected environment or use registry mirrors to satisfy your organizational controls on external content, RHACS can now scan images from your registry mirrors in OpenShift Container Platform environments.

This feature leverages the **delegated image scanning** functionality introduced in RHACS 4.1. The delegated image scanning functionality allows RHACS Secured cluster services to use Sensor to pull images for scanning from registry mirrors you have set up by using the **ImageContentSourcePolicy**, **ImageDigestMirrorSet**, or **ImageTagMirrorSet** custom resources.

For more details, see Accessing delegated image scanning.

1.2.6. Configure delegated image scanning in the RHACS portal

RHACS 4.1 introduced **Scanning support for images pulled from on-premise registries** to support RHACS Cloud Service environments, allowing you to delegate vulnerability scanning to the RHACS secured cluster services using APIs. With RHACS 4.2, the delegated image scanning feature is now available in RHACS, and you can configure it using the RHACS portal.

For more information, see Accessing delegated image scanning.

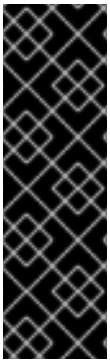
1.2.7. Define new system policies using CVE age or fixability

To support your organization's vulnerability management policies, you can now use the following new vulnerability management policy criteria:

- **CVE Is Fixable**: This criterion results in a violation only if the image in the deployment you are evaluating has a fixable CVE.
- **Days Since CVE Was First Discovered In Image** This criterion results in a violation only if it has been more than a specified number of days since RHACS discovered the CVE in a specific image.
- **Days Since CVE Was First Discovered In System** This criterion results in a violation only if it has been more than a specified number of days since RHACS discovered the CVE across all deployed images in all clusters that RHACS monitors.

1.2.8. On-demand and downloadable CVE report in Vulnerability Management 2.0 (Technology Preview)

RHACS 4.2 introduces workload vulnerability reporting in Vulnerability Management 2.0 (Technology Preview). You can now create on-demand reports and download them in CSV format. Like VM 1.0, you can continue generating scheduled or on-demand reports and sending them by an email notifier. The report includes rich detail for detected CVEs, including Deployment info, Image info, and detailed CVE data such as Fixable Status, Component Upgrade Version, Severity, CVSS score, and more.



IMPORTANT

Vulnerability Management 2.0 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 .

For more information, see Vulnerability reporting in Vulnerability Management 2.0 .

1.2.9. Scanner supports additional operating systems

RHACS 4.2 can now identify vulnerabilities in images with the following Linux distributions:

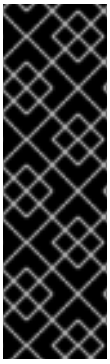
- **alpine:v3.18**
- **debian:12**
- **ubuntu:23.04**
- **ubuntu:23.10**

For more information, see Scanning Images.

1.2.10. Improvements to runtime network policy generation

With this release, you can now generate policies from within the **Network Graph** and narrow down policies that apply to specific deployments and namespaces in a cluster. You can also use the **Filter deployments** section criteria to narrow the generated policies' scope further. After generating network policies, you can compare the generated policies with the existing network policies and view them side-by-side to understand the differences in the YAML files for the policies. You can download the generated policies or share them with system notifiers, such as Slack, that you have previously set up using integrations in RHACS.

1.2.11. Build time Network Policy tools (Technology Preview)



IMPORTANT

Build time Network Policy tools 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 .

Based on user feedback, Red Hat has restructured the command-line syntax and expanded the toolset. The following three **netpol** tools operate on a given file directory, which includes all of the project's workload manifests, including network policy manifests if available.

These command line tools help teams to shift network security left. With the automated generation of Kubernetes network policies and the supplementary validation tools, Dev and DevOps teams can include network policy development into their Build pipeline, using the RHACS command-line interface, **roxctl**.

Command	Description
roxctl netpol generate	Generates Kubernetes network policies by analyzing your project's YAML manifests in a specified directory. In older versions, the command was **roxctl generate netpol**. For more information, seeUsing the build-time network policy generator.
roxctl netpol connectivity map	Lists the allowed connections between workloads based on the workload and Kubernetes network policy manifest in the specified directory. Results also include a graphical representation in **.dot** format. For more details, seeConnectivity mapping using the roxctl connectivity-map command.
roxctl netpol connectivity diff	Lists the differences in allowed connections between two project versions based on the workload and Kubernetes network policy manifest in each version directory. This feature shows the semantic differences which are not noticeable when performing a source code syntactic **diff**. For more details, seeIdentifying the differences in allowed connections between project versions.

Currently, you can use these tools without authenticating with RHACS. Red Hat plans to include more advanced features when you authenticate with RHACS in a future release.

1.2.12. New Listening Endpoints menu in the RHACS portal

RHACS provides information about processes listening on ports for all deployments in a secured cluster. Until now, this information was only accessible through the API. In RHACS 4.2, you can see detailed information about which processes are listening on what ports using the RHACS portal. It includes details about the process, port, pod, and container, and you can sort and filter the list using **Deployment**, **Namespace**, or **Cluster** criteria.

For more information, see Auditing listening endpoints.

1.2.13. Viewing network policy YAML files from a violation

In the RHACS portal, the **Deployment** tab shows a new **Network policies** section when viewing violations for a specific policy. If the namespace to which the deployment belongs has network policies listed, you can click on a listed policy to view or download the entire YAML file for that network policy.

1.3. NOTABLE TECHNICAL CHANGES

- RHACS now includes **ALL** as a valid value for drop capabilities. The policy implementation has been changed so that if the policy criteria specifies that a deployment must drop a capability, for example, **A or B**, and a deployment manifest contains **DROP ALL**, it does not violate the policy.
- In RHACS 4.2, the **SecuredCluster** custom resource definition (CRD) includes a new parameter called **spec.admissionControl.replicas** to configure the number of replicas for the admission controller. The default value for this parameter is **3**.
- You do not need to set **ForceRollbackVersion** for rolling back from future RHACS 4.x releases to version 4.2 or later.
- Authentication is now mandatory for certain endpoints that were previously public. Specifically, **/v1/metadata**, **/v1/database/status**, and **/v1/mitreattackvectors** now require authentication. This change decreases the potential exposure to denial of service (DoS) attacks and blocks attackers from exploiting the information accessible through these endpoints.
- Non-autogenerated image integrations no longer use the **/v2/_catalog** registry repository list during matching. Additionally, to turn off repository list matching for autogenerated integrations, set the new environment variable **ROX_DISABLE_REGISTRY_REPO_LIST** to **true** on Central.
- The **Component Upgrade** column in vulnerability reports is renamed to **CVE Fixed In**.
- Previously, access to the **/api/docs/swagger** API required read permission for the **Integration** resource. Now, it only requires users to be authenticated to access it.
- Scanner now selects the image for scanning based on its architecture alignment with the Scanner's architecture, rather than consistently choosing **amd64** for multi-arch image scanning.
    - For example, if Scanner runs on **s390x** and an **s390x** version of the multi-arch image exists, it scans that **s390x** image.
    - If no image matches Scanner's architecture, then it attempts to scan the **amd64** version, as it did previously.
- Telemetry data collection is enabled by default, except for installations with the offline mode enabled. To disable telemetry, see Opting out of Telemetry.
- Integration with OpenShift Container Platform monitoring is configured and enabled by default for RHACS installations on OpenShift 4. To deactivate this integration, set the flag **monitoring.openshift.enabled** to **false**.
- Go executable in the following images available at **registry.redhat.io/advanced-cluster-security** are dynamically linked and compiled with the **CGO_ENABLED=1** option:
    - **rhacs-main-rhel8**
    - **rhacs-rhel8-operator**
    - **rhacs-scanner-rhel8**

- **rhacs-scanner-slim-rhel8**
- **rhacs-roxctl-rhel8**
  However, the **roxctl** binary which you download from the RHACS portal is still statically linked.

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, 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

Feature	RHACS 3.74	RHACS 4.0	RHACS 4.2
Examining images for Application-level dependencies for vulnerability reporting: **dotnet/shared/Microsoft.AspNetCore.App/** and **dotnet/shared/Microsoft.NETCore.App/**	DEP	DEP	DEP
Expiration field in **Exclusion** proto	DEP	DEP	DEP
Kernel module collection method	DEP	REM	NA
Network Graph version 1.0	DEP	REM	NA
roxctl scanner generate flag **offline-mode** (flag only)	DEP	DEP	REM
roxctl generate netpol	NA	NA	DEP
roxctl connectivity-map	NA	NA	DEP
/v1/report endpoint	DEP	DEP	DEP
/v1/serviceaccounts endpoint	DEP	DEP	DEP

Feature	RHACS 3.74	RHACS 4.0	RHACS 4.2
Vulnerability Management 1.0: Image CVEs, Image Components, Images, Deployments, and Namespaces.	GA	DEP	DEP
Custom Security Context Constraints (SCCs): **stackrox-collector**,**stackrox-admission-control**, and **stackrox-sensor**	GA	DEP	DEP
Vulnerability Management Approver permission	GA	DEP	DEP
Vulnerability Management Requester permission	GA	DEP	DEP
Vulnerability Report Creator permission	GA	GA	DEP
Vulnerability Reports and **Policy** permission	DEP	REM	NA
Role resource	DEP	REM	NA
Scope Manager system role and permission set	DEP	REM	NA
ROX_FORCE_LOCAL_IMAGE_SCANNING environment variable	DEP	REM	NA
CIS Docker v1.2.0 Compliance Standard	NA	NA	DEP

1.4.1. Deprecated features

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

- Red Hat has deprecated the following commands for build-time network policy generation (Technology Preview) feature:
  - **roxctl generate netpol**, use the **roxctl netpol generate** command instead.
  - **roxctl connectivity-map**, use the **roxctl netpol connectivity map** command instead.
- Red Hat is scheduled to remove the CIS Docker v1.2.0 standard from RHACS Compliance checks starting in RHACS 4.4.
- Starting with version 4.0, RHACS does not evaluate the risk associated with service account permissions for deployments.

1.4.2. Removed features

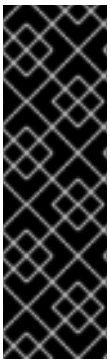
The following section provides additional information about the removed features listed in the preceding table.

1.4.2.1. Dark mode

Dark mode in RHACS Cloud Service had rendering issues with buttons and images, leading to an inconsistent experience. Therefore, the dark mode and its toggle button are now removed from the navigation. (ROX-16515)

1.4.2.2. PDF export

Red Hat removed the PDF export feature from the Vulnerability Management dashboard. Instead, you can use the updated vulnerability reporting feature in Vulnerability Management 2.0 (Technology Preview). (ROX-16394)



IMPORTANT

Vulnerability Management 2.0 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 .

1.4.2.3. Report configuration without an associated collection

In version 4.0, RHACS released the collections feature that replaced access scopes used in report configurations. RHACS automatically created equivalent collections for access scopes used in existing report configurations and migrated report configurations to use newly-created collections. If the migration failed, the report configurations became non-functional, and RHACS logged the error messages in Central logs and in the RHACS web portal.

RHACS 4.2 deletes the report configurations that could not be migrated. To avoid losing any existing report configurations, create valid collections for reports that failed the migration and attach the collection to the report configuration before you upgrade to RHACS 4.2.

For more information on collections, see Creating and using deployment collections .

1.4.2.4. Offline-mode flag

Red Hat has removed the **--offline-mode** flag for the **roxctl scanner generate** command.

1.4.2.5. Use Container IAM role option in ECR integration for RHACS Cloud Service

Red Hat has removed the **Use Container IAM role** option from RHACS Cloud Service from the ECR integration configuration page.

1.5. NOTICE FOR UPCOMING CHANGES

- Previously, the Syslog notifier sent an incorrect message header; RHACS flipped the severity and name fields. When configuring the notifier, you can now select the following options:
  - **CEF**: The corrected message header. Default option when you are configuring using the RHACS portal.
  - **CEF (legacy field order)**: This is the previous incorrect message header. Default option if

you use API and do not specify a value for the message header. Red Hat plans to remove the wrong message header option **CEF (legacy field order)** in version 4.4. Additionally, all legacy field order notifiers will be migrated to **CEF**.

- In a future version, Red Hat plans to enable authentication for the following API endpoints:
  - **/v1/featureflags**
  - **/v1/resources**
- If you are using these API endpoints, you must prepare to use them with authentication.
- Starting from RHACS 4.3, Red Hat will not support rolling back to RHACS 3.x or RHACS 4.0.
- Red Hat has delayed the removal of the **/v1/report** API endpoint in RHACS 4.2; it will now be removed in RHACS 4.3.
- Red Hat will remove the following widgets from the Compliance dashboard in RHACS 4.4:
  - CIS Docker v1.2.0 Compliance
  - PCI DSS 3.2.1 Compliance
  - CIS Kubernetes v1.5 Compliance
  - NIST SP 800-53 Compliance
  - NIST SP 800-190 Compliance
  - HIPAA 164 Compliance

1.6. BUG FIXES

1.6.1. Resolved in version 4.2.0

Release date: 18 September 2023

- Previously, if a non-blocking socket failed to open a connection, Collector would still report that as a connection. This issue has been fixed. (ROX-17486)
- In RHACS 4.2, Collector correctly handles asynchronous connection establishment.(ROX-17486)
- Previously, Operator installations broke if the OpenShift cluster-wide proxy was enabled and Central or SecuredCluster CR configured an egress proxy environment variable. This issue is fixed. (ROX-18477)
- Previously, when using eBPF on IBM Z, RHACS reported incorrect process UNIX group IDs (GID). This issue is now fixed. (ROX-17459)
- In previous RHACS versions, there was a mismatch in the number of CVEs reported by JSON output and table output. This issue is now fixed. (ROX-15277)
- Previously, integrating RHACS with Jira failed when you used an OAuth token or JWT while configuring the integration. This issue is fixed. (ROX-17992)

1.6.2. Resolved in version 4.2.1

Release date: 3 October 2023

- A sensor panic could occur in version 4.2.0 if a cluster contained deployments with an invalid image reference, for example, **image: " "**, and delegated scanning was enabled for all registries. This issue has been fixed.
- The minimum permissions required to display 6 of the sidebar links in the RHACS web portal were too strict in the 4.2.0 release, and are reduced in this release.

1.6.3. Resolved in version 4.2.2

Release date: 23 October 2023

This release of RHACS fixes the following security vulnerabilities:

- CVE-2023-44487 and CVE-2023-39325: Flaw in handling multiplexed streams in the HTTP/2 protocol
- Various CVEs in containers, including CVE-2023-4527, CVE-2023-4806, CVE-2023-4813, and CVE-2023-4911: glibc security issues

It contains the following bug fixes and changes:

- Previously, OpenShift Container Platform customers using the downloaded manifest bundle with automatic upgrades enabled found that Sensor did not automatically upgrade, and failed with a **PRE_FLIGHT_CHECKS_FAILED** error. This issue has been fixed. (ROX-19955)
- A new default policy has been added, "Rapid Reset: Denial of Service Vulnerability in HTTP/2 Protocol". This policy alerts on deployments with images containing components that are susceptible to a Denial of Service (DoS) vulnerability for HTTP/2 servers, as described in CVE-2023-44487 and CVE-2023-39325. This policy applies to the build or deploy life cycle stage.

1.6.4. Resolved in version 4.2.3

Release date: 27 November 2023

This release of RHACS includes updates to Red Hat Enterprise Linux (RHEL) base images and includes the following fixes:

- CVE-2023-44487: Flaw in handling multiplexed streams in the HTTP/2 protocol.
- The HTTP/2 functionality in the RHACS Operator webhook has been disabled to mitigate CVE-2023-44487.
- In some cases, CVEs that were deferred and approved were not added to the list of snoozed CVEs. An issue with the **/v1/suppress** and **/v1/unsuppress** APIs caused this behavior, and has been fixed.

1.6.5. Resolved in version 4.2.4

Release date: 22 January 2024

- Fixed PostgreSQL vulnerabilities in **scanner-db** containers.

1.6.6. Resolved in version 4.2.5

Release date: 14 March 2024

This release provides the following bug fix:

- Fixed an issue where an upgrade to version 4.2 from an earlier version caused the Central component to enter a crash loop.

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-rhel8:4.2.5**
Scanner	Scans images and nodes.	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:4.2.5**
Scanner DB	Stores image scan results and vulnerability definitions.	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-db-rhel8:4.2.5**
Collector	Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.	• **registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:4.2.5** • **registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:4.2.5**
Central DB	Postgres instance that provides the database storage for Central.	**registry.redhat.io/advanced-cluster-security/rhacs-central-db-rhel8:4.2.5**