Red Hat Advanced Cluster Security for Kubernetes 3.74

Release notes

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

Last Updated: 2024-02-14

Red Hat Advanced Cluster Security for Kubernetes 3.74 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 3.74

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
3.74.0	27 February 2023
3.74.1	20 March 2023
3.74.2	13 April 2023
3.74.3	2 May 2023
3.74.4	5 June 2023
3.74.5	13 July 2023
3.74.6	28 September 2023
3.74.7	24 October 2023
3.74.8	18 January 2024
3.74.9	12 February 2024

1.1. ABOUT THIS RELEASE

RHACS 3.74 includes the following new features, improvements, and updates:

- IBM Power, IBM zSystems, and IBM® LinuxONE support for secured clusters
- Clair scanner version 4 support
- Network graph 2.0 (Technology Preview)
- Updated global search in the RHACS portal
- Extra fields for improved syslog integration
- Troubleshooting guide enhanced when the Collector kernel module is missing
- Scale and performance improvements

1.2. NEW FEATURES

1.2.1. IBM Power, IBM zSystems, and IBM(R) LinuxONE support for secured clusters

RHACS version 3.74 extends support for RHACS secured clusters for:

- Red Hat OpenShift 4.12 to IBM Power (ppc64le)
- Red Hat OpenShift 4.10 and 4.12 to IBM zSystems (s390x) and IBM® LinuxONE (s390x)

With RHACS version 3.74, you can secure clusters running on Red Hat OpenShift on IBM Power, IBM zSystems, and IBM® LinuxONE by using the RHACS Operator.

NOTE

- You can now secure IBM Power, IBM zSystems, and IBM® LinuxONE clusters with RHACS. Central is not supported at this time.
- The Collector is delivered as a kernel module and eBPF probe for IBM Power, but is only delivered as a kernel module for IBM zSystems and IBM® LinuxONE. Red Hat plans to add support for eBPF probes for IBM zSystems and IBM® LinuxONE in a future release.
- RHACS supports scanning IBM Power, IBM zSystems, and IBM® LinuxONE images with the following limitations for multi-architecture images:
  - When you scan a multi-architecture image with a tag reference, RHACS reports the image scan results of the AMD64 layer.
  - When you scan a multi-architecture image with an SHA reference to a specific architecture layer, RHACS reports the image scan results of the specified architecture.

1.2.2. Clair scanner version 4 support

Clair is a set of microservices that perform vulnerability scanning of container images associated with multiple Linux operating systems. If you are using Clair version 4 (v4), you can now integrate Clair v4 with RHACS to get image vulnerability data. Integrating Clair v4 enables you to see image vulnerabilities from multiple sources in the RHACS portal and triage them from one place.

NOTE

- Red Hat has deprecated the previous CoreOS Clair integration in favor of Clair v4 integration.
- The next major version, RHACS 4.0, does not plan to support the JSON Web Token (JWT)-based authentication option for Clair v4 integration.

1.2.3. Network graph 2.0 (Technology Preview)

IMPORTANT

Network graph 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 .

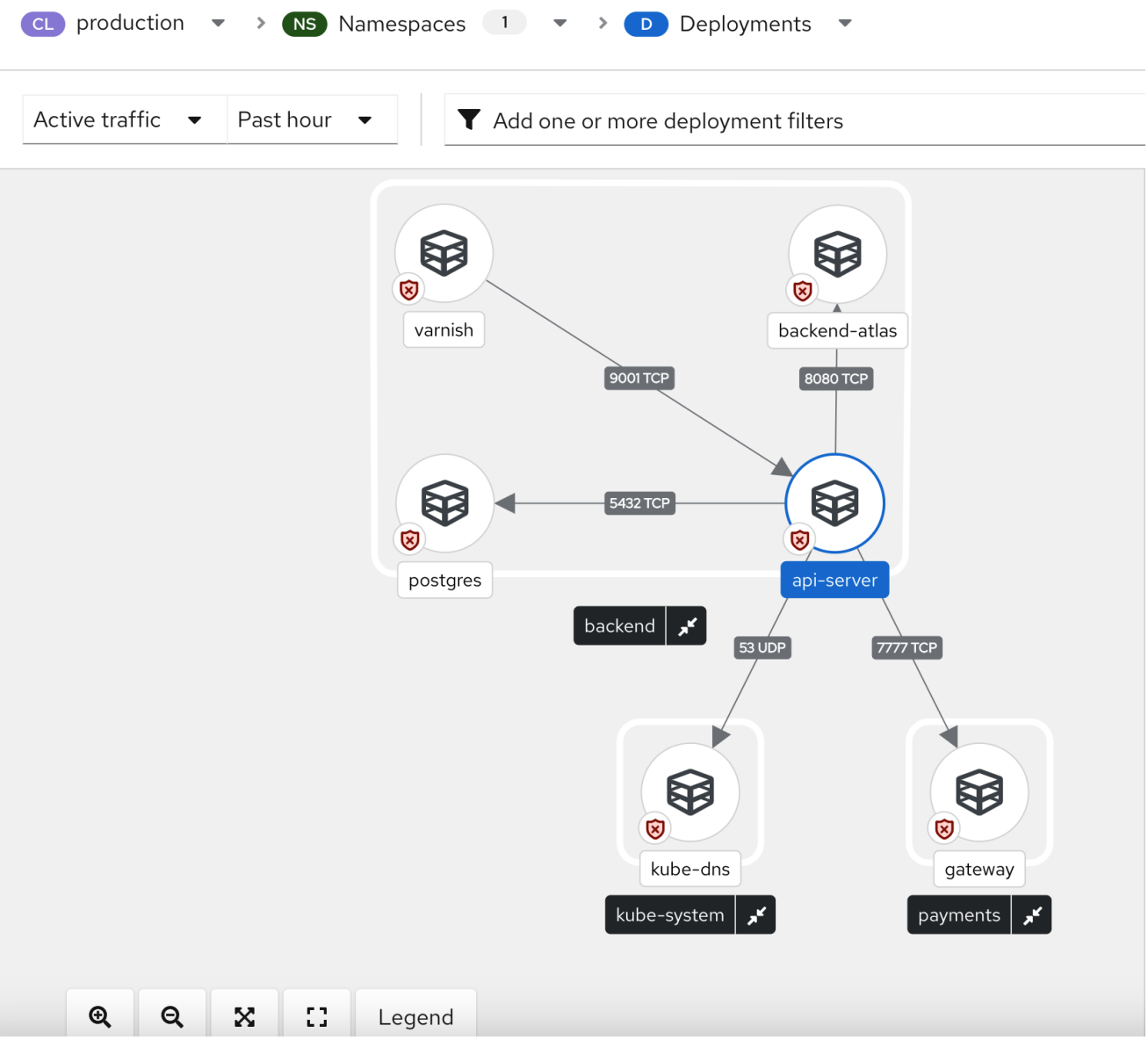
RHACS includes a network graph upgrade that provides intuitive navigation, enhanced functionality, and crisp graphs by using the Patternfly library. The new graph provides high-level and detailed information about deployments, network flows, and network policies in your environment. You can view traffic in the graph by selecting one of the following views:

- The **Active traffic** (default) view shows observed traffic, focused on the namespace or specific deployment that you click.
- The **Extraneous flows** view shows potential flows allowed by your network policies, helping you identify missing network policies needed to achieve tighter isolation.

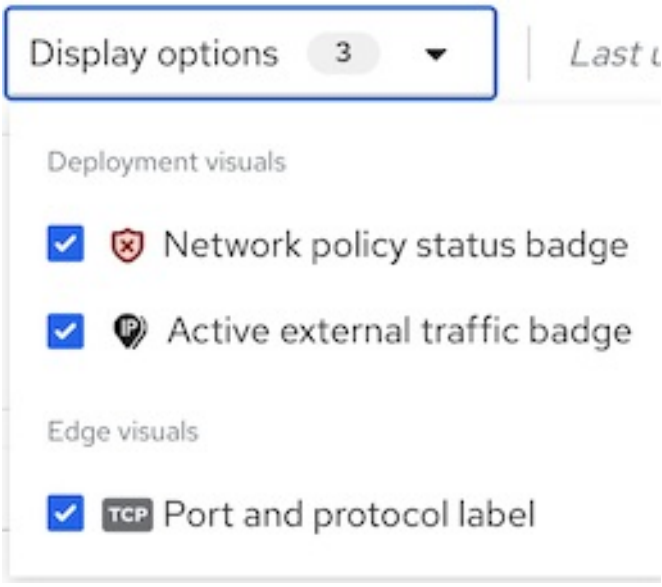
The new views use URLs that are displayed in your browser's address bar, allowing you to easily navigate, save views as bookmarks, and share links.

Filters and controls help you customize the information that is displayed. You can use the expanded top-level filter to focus on namespaces and deployments of interest. You can also collapse display items in the details tab to reduce clutter. The **Legend** button displays descriptions of the icons used in the graph.

The following image provides an example of the network graph. In this example, based on the options that the user has chosen, the graph depicts deployments and traffic flows between them. It also uses a red badge to indicate deployments that are missing policies and therefore allowing all network traffic.

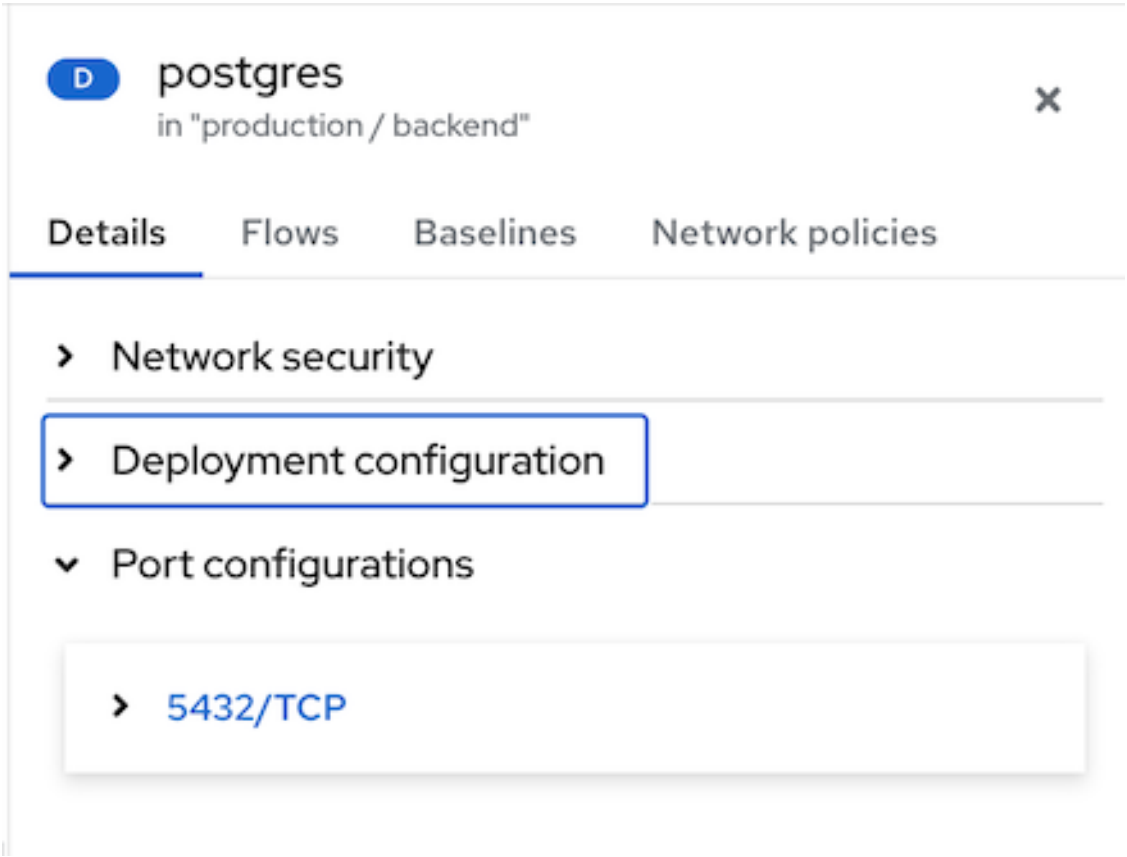


The **Display options** drop-down list lets you control the items and level of detail displayed on the graph, as shown in the following example.

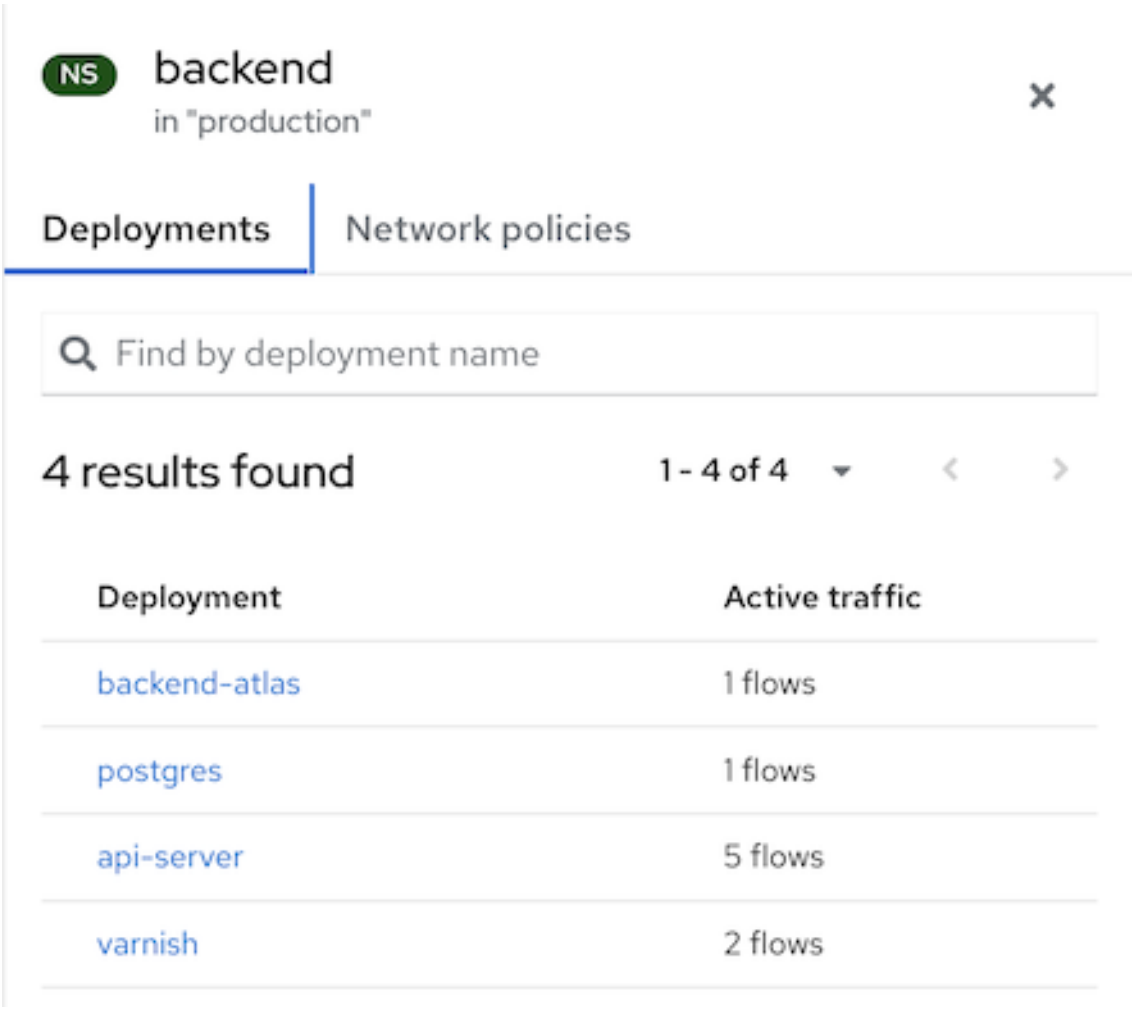


When you click an item in the graph, the rearranged side panel with collapsible sections presents

deployment and namespace information. The side panel switches between Deployment mode and Namespace mode based on item in the graph that you have selected. The D or NS label next to the item name in the header (in this example, "postgres,") indicates if it is a deployment or a namespace. The following example illustrates deployment mode.



In Namespace mode, the side panel includes a search bar and a list of deployments. You can click on a deployment to view its information. In Namespace mode, the side panel also includes a new **Network policies** tab. From this tab, you can view, copy to the clipboard, or export any network policy defined in that namespace, as shown in the following example.



1.2.3.1. Known limitations with network graph 2.0

The **Network graph 2.0 preview**menu item is available in the RHACS portal with the existing **Network graph (1.0)** menu item to make it easier for you to try it and provide us with feedback. The network graph 2.0 has the following known limitations:

- When you filter the graph, the result contains your filtered deployments and other derived deployments and namespaces they interact with. A way to visualize and control the additional (derived) deployments is needed.
- The simulate network policy feature is limited. Specifically, the graphic view does not reflect the simulation, whether it was generated from the **Simulate network policy**panel or as a result of uploading a YAML file.
- An option to toggle the view of orchestration components is missing.
- You cannot clear the new **Namespaces** or **Deployments** selection filter. You must deselect each entry to clear it.
- The **Active traffic/Extraneous flows** drop-down list stays up and responds to clicks. Clicking **Active traffic** at that point results in switching to **Extraneous flows** mode.

1.2.4. Updated global search in the RHACS portal

Global search has been redesigned and is now presented in a search page to help you quickly find information by using an extensive list of search criteria. Global search includes the following changes:

- Total search results are enumerated across more than 10 search categories, allowing you to zoom in on an area of interest.
- Individual search results are presented as line items, offering search category-sensitive direct links to view the result in the appropriate RHACS product page or to further view the results as a filter on the Violations or Risk pages.
- Search now uses URLs, allowing you to navigate by using the browser, open search results in new tabs, and share search links.

1.2.5. Extra fields for improved syslog integration

When integrating with a syslog receiver, RHACS automatically sends all violations and audit events to the configured syslog receiver. With RHACS 3.74, you can now specify custom key-value pairs to send to the external system. The new extra fields allow you to customize the data that you can filter in your syslog receiver.

For more information, see Integrating by using the syslog protocol .

1.2.6. Troubleshooting guide enhanced when the Collector kernel module is missing

The Collector troubleshooting guide has been updated with practical tips to help you navigate the most common startup errors and understand how to fix them. In addition, the RHACS portal health status dashboard has also been enhanced to redirect you to troubleshooting documents when the Collector status is unhealthy.

1.2.7. Scale and performance improvements

Continuing our ongoing investment in scale and performance, RHACS 3.74 includes these improvements to the Policy Violation widget in the Dashboard:

- Memory consumption in Central reduced by a factor of 10
- Typical widget load time in the RHACS portal is less than 2 seconds even with a very large number of violations; for example, more than 100,000

1.3. FEATURES AVAILABLE IF THE POSTGRESQL DATABASE OPTION IS INSTALLED

The features described in the following sections are available only if the PostgreSQL database option is installed.

IMPORTANT

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 .

1.3.1. RHACS collections

RHACS introduces a new concept called “collections” that provides the ability to define a collection of deployments by using matching patterns, and name this collection for repeatable use. A collection in RHACS is a user-defined, named reference. It defines a logical grouping by using selection rules, offering you a power of expression as follows:

- Rules can match by using the name or the label of a deployment, namespace, or cluster.
- You can specify rules by using exact matches or regular expressions.
- Collections are resolved at run time. The rules can refer to objects that do not exist at the time of definition.
- Collections can be constructed by using other collections to describe complex hierarchies.

Collections provide you with a language to describe how your dynamic infrastructure is organized, eliminating the need for cloning and repetitive editing of RHACS properties such as inclusion and exclusion scopes.

You can use collections to identify any group of deployments in your system, such as:

- An infrastructure area that is owned by a specific development team
- An application which requires different policy exceptions when running in a development or in a production cluster
- A distributed application that spans multiple namespaces, defined through a common deployment label
- The entire production or test environment using nested collections, cluster names, or labels

NOTE

In this Technology Preview release, collections are included only in the Vulnerability Reporting workflow, and existing report scopes are automatically migrated to collections. You must verify that the migration resulted in the correct configuration for your existing reports. See the “Migration of report scopes to collections” section for more information about the migration process.

In upcoming releases, it is anticipated that collections will be made available in other workflows in the product, starting with simplified policy management. Over time, it is planned that collections will be available in the dashboards, the network graph, and everywhere a RHACS search or filter is used, allowing you to easily focus on an area of interest.

1.3.2. Policy categories

Policy categories help you manage violations that are related to a similar cause by grouping and filtering violations according to policy category. Before RHACS version 3.74, you could create policy categories inline within a policy. In version 3.74, policy categories receive higher visibility and greater importance in RHACS systems using the PostgreSQL database option.

The RHACS portal introduces a new **Policy Categories** tab in **Policy Management**. This tab provides the ability to view, create, rename, or delete categories. Before deleting a category, RHACS determines if a category is used by any policy. System-defined policy categories are protected and you cannot modify or delete them.

The same actions for policy categories that are available in the RHACS portal are also available through the API by using the **PolicyCategoryService** service. For more information, see the API documentation by navigating to **Help → API reference** in the RHACS portal.

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 (updated 20 March 2023)

Feature	RHACS 3.72	RHACS 3.73	RHACS 3.74
BuildDate attribute	GA	GA	DEP
Clair scanner version 2	GA	GA	DEP
ClusterCVE permission	DEP	DEP	REM
ids field in the /v1/cves/suppress` and **/v1/cves/unsuppress** API payload	DEP	• DEP in RHACS 3.73 • REM in Advanced Cluster Security Cloud Service (ACSCS) (Field Trial)	DEP

Feature	RHACS 3.72	RHACS 3.73	RHACS 3.74
Kernel module collection method	GA	GA	DEP
Policy permission	GA	GA	DEP
Role permission	GA	GA	DEP
VulnerabilityReports permission	GA	GA	DEP
ScopeManager default role	GA	GA	DEP
/v1/cves/suppress and **/v1/cves/unsuppress**	DEP	• DEP in RHACS 3.73 • REM in ACSCS (Field Trial)	DEP
vulns fields of **storage.Node** object in response payload of **v1/nodes**	DEP	DEP	DEP

1.4.1. Deprecated features

The following sections describe the new permissions and indicate the deprecated permissions that will be removed in a future release.

1.4.1.1. Removed attribute

The product **BuildDate** attribute is deprecated and is planned to be removed in the next major version, RHACS 4.0. The **/debug/versions.json** endpoint and **roxctl version --json** command will no longer return this attribute.

1.4.1.1.1. Actions you must take

No action is required.

1.4.1.2. Future permissions changes

To continue to simplify access control management, RHACS will group some permissions in permission sets. As a result, the following changes are planned for an upcoming release:

- The permission **WorkflowAdministration** will deprecate the permissions **Policy** and **VulnerabilityReports**.
- The permission **Access** will deprecate the permissions **Role**.

- The default role **Scope Manager** will be removed.
- The permission **WorkflowAdministration** are planned to replace **Policy** and **VulnerabilityReports** in permission sets in the RHACS version 4.1 release. During the migration of the permission sets, the **WorfklowAdministration** permission will have the lowest access permission granted for either **Policy** or **VulnerabilityReports**. For example, a permission set with WRITE Policy and READ **VulnerabilityReports** access will have READ **WorkflowAdministration** access after the migration that is planned to occur with the RHACS version 4.1 release. These changes in access can lead to unwanted side effects and missing access rights if you do not update your permission sets before the release.

1.4.1.2.1. New WorkflowAdministration role

The permission **WorkflowAdministration** will deprecate the permissions **Policy** and **VulnerabilityReports**.

1.4.1.2.2. Actions you must take

Preemptively replace the **Policy** and **VulnerabilityReports** resources within your permission sets in favor of **WorkflowAdministration**.

1.4.1.2.3. Change to Access role

The permission **Access** is planned to replace **Role** in permission sets in the RHACS version 4.1 release. During the migration of the permission sets, the **Access** permission will have the lowest access permission granted for either **Access** or **Role**. For example, a permission set with READ Access and WRITE Role will have READ access after the migration. These changes in access can lead to unwanted side effects and missing access rights if you do not update your permission sets before the release.

1.4.1.2.4. Actions you must take

Preemptively replace the **Role** resource within your permission sets with **Access**.

1.4.1.2.5. Change to ScopeManager role

The default **ScopeManager** role is planned for removal in the RHACS version 4.1 release. During the migration, authentication provider rules referencing that role will be updated to use the **None** role.

1.4.1.2.6. Actions you must take

If authentication provider rules reference the **ScopeManager** role for other purposes than Vulnerability Report management, you should manually create a similar role and replace references to **ScopeManager** with the new role in the authentication provider rules.

1.5. REMOVE KERNEL MODULE AS COLLECTION METHOD

Added 20 March 2023

Currently, secured clusters can specify three options of collection methods for runtime events: eBPF (selected by default), kernel module, or no collection. Kernel module as a collection method is deprecated in the RHACS version 3.74 release and is planned for removal in the RHACS version 4.1 release.

1.5.1. Actions you must take

Verify the collection method of your secured clusters. This value is set in the **collector.collectionMethod** parameter and is one of the following methods:

- **EBPF**
- **KERNEL_MODULE**
- **NO_COLLECTION**

If any of your secured clusters uses **KERNEL_MODULE** as a collection method, change it to **EBPF**.

1.5.2. In-product docs removal

With this release, Red Hat removed the in-product docs accessible from the help menu. If you are using the in-product docs, you can instead download the Product Documentation for Red Hat Advanced Cluster Security for Kubernetes in PDF format. (ROX-12839)

1.6. NOTICE OF UPCOMING SUPPORT CHANGES

RHACS version 3.74 is the last release that supports OpenShift Container Platform versions 4.6, 4.7, 4.8, and 4.9. The next major version, RHACS 4.0, will not support these OpenShift Container Platform versions or earlier releases. See the Red Hat Advanced Cluster Security for Kubernetes Support Policy for more information.

1.7. BUG FIXES

1.7.1. Resolved in version 3.74.0

Release date: 27 February 2023

- The RHACS Operator previously incorrectly removed owner references from the **stackrox-db** persistent volume claim (PVC). This can cause an error such as **Failed reconciling PVC "stackrox-db". Please remove the storageClassName and size properties from your spec [...]**. The bug is fixed. However, if you receive this message, you need to perform the steps described in the Knowledgebase article. (ROX-14335)
- The **v1/alerts/summary/counts** endpoint, which is used by the **Policy violations by severity** and **Policy violations by category** widgets on the Dashboard, was fixed to prevent Central from crashing in highly-scaled environments. (ROX-13829)
- RHACS previously was not able to correctly identify the signature of images that contained the same content but were stored in different registries, causing problems with alerts and enforcement. This issue has been fixed and RHACS now correctly identifies signatures of images from different registries. (ROX-12400)

1.7.2. Resolved in version 3.74.1

Release date: 20 March 2023

- Previously, Sensor that was installed on secured clusters could not connect to Central when using a proxy, even if the proxy was specified in the proxy configuration file or in environment variables. This issue is fixed and Sensor on secured clusters now connects to Central when using a proxy. (ROX-15279)

1.7.3. Resolved in version 3.74.2

Release date: 13 April 2023

- This release of RHACS includes a fix for RHSA-2023:1405 OpenSSL security update for Red Hat Enterprise Linux (RHEL) 8.
- This release fixes a crash that occurs during migration to the PostgreSQL database (Technology Preview) when there are clusters that have not checked in recently.

1.7.4. Resolved in version 3.74.3

Release date: 2 May 2023

- This release of RHACS includes a fix for CVE-2023-28617 for RHEL.
- This release includes a fix for an issue with migration to the PostgreSQL database (Technology Preview).

1.7.5. Resolved in version 3.74.4

Release date: 5 June 2023

- RHACS 3.74.4 is built with updated Golang to fix the following CVEs:
  - CVE-2023-24540
  - CVE-2023-24539
  - CVE-2023-29400

1.7.6. Resolved in version 3.74.5

Release date: 13 July 2023

- Fixed an issue with Sensor upgrade errors caused by Pod Security Policies (PSPs) that are not supported in Kubernetes version 1.25 and later.
- Fixed an issue with upgrades failing because RHACS applied PSPs, even when not enabled.
- Provides a Python3 security update. (RHSA-2023:3591)

1.7.7. Resolved in version 3.74.6

Release date: 28 September 2023

This release of RHACS fixes the following security vulnerabilities:

- CVE-2023-2828: BIND vulnerability that allows the configured **max-cache-size** limit to be exceeded significantly
- CVE-2023-3899: Vulnerability in subscription-manager that allows local privilege escalation due to inadequate authorization

1.7.8. Resolved in version 3.74.7

Release date: 24 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

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.

1.7.9. Resolved in version 3.74.8

Release date: 18 January 2024

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

- All containers have been rebuilt and now include container CVE fixes for CVE-2023-44487: Flaw in handling multiplexed streams in the HTTP/2 protocol and CVE-2023-40217: Python 3 ssl.SSLSocket vulnerability.
- The HTTP/2 functionality in the RHACS Operator webhook has been disabled to mitigate CVE-2023-44487.
- Fixed PostgreSQL vulnerabilities in multiple images.

1.7.10. Resolved in version 3.74.9

Release date: 12 February 2024

This release of RHACS fixes a compatibility issue during startup between recent versions of Central and Sensors in 3.74.

1.7.11. Known issues

- Currently, RHACS does not support alerts for security policy violations for containers running with default **seccomp profiles-Unconfined**. The alert violations for Unconfined **seccomp** profiles are generated only if the **seccomp** profile is explicitly set to "Unconfined" in the container specification. There is no workaround. (ROX-13490)
- In the RHACS portal, the **Platform Configuration → Clusters** page does not display information in the **Cloud Provider** field for Azure Red Hat OpenShift and Red Hat OpenShift Service on AWS (ROSA) clusters. There is no workaround. (ROX-14399)

1.8. IMAGE VERSIONS

Image	Description	Current version

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-rhel8:3.74.9**
Scanner	Scans images and nodes.	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:3.74.9**
Scanner DB	Stores image scan results and vulnerability definitions.	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-db-rhel8:3.74.9**
Collector	Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.	• **registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:3.74.9** • **registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:3.74.9**