Red Hat Advanced Cluster Security for Kubernetes 4.1

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 4.1 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 4.1

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
4.1	29 June 2023
4.1.1	11 July 2023
4.1.2	26 July 2023
4.1.3	21 August 2023
4.1.4	17 October 2023
4.1.5	8 November 2023
4.1.6	22 January 2024

1.1. ABOUT THIS RELEASE

IMPORTANT

If you are using OpenShift Container Platform and the RHACS Operator, and your upgrades are failing, see RHACS Operator upgrade to 4.1.0 stuck in Pending state due to removal of "KernelModule" collection method for important information and steps you must take to resolve those issues.

RHACS 4.1 includes the following new features, improvements, and updates:

- Manual renewal of Central and Sensor certificates
- Vulnerability Management 2.0 (Technology Preview)
- RHACS Cloud Service scanning support for images pulled from on-premise registries
- eBPF collection method on IBM Z and IBM® LinuxONE
- Ability to configure the display of default compliance standards in the Compliance Dashboard
- Declarative configurations for authentication and authorization
- SSO configuration using the roxctl CLI

- New collection method based on BPF CO-RE (Technology Preview)
- Network graph updates
- Policy Management simplification
- New permission sets
- Improvements for Sensor resync (General Availability)

1.2. NEW FEATURES

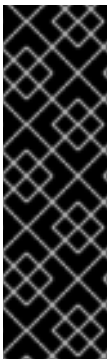
1.2.1. Manual renewal of Central and Sensor certificates

You now have the ability to renew certificates for RHACS components when security breaches occur or when you want to renew certificates on your preferred schedule. With RHACS 4.1, you can renew certificates for Central, Scanner, and **scanner-db** directly from the RHACS portal. This ensures continuous and secure communication between Central and all the Sensor components.

Previously, you would receive an information banner notifying you when the Central certificate expired. Additionally, you were provided with new certificates for Central along with instructions for renewing Scanner and **scanner-db** certificates. Only users with administrative access to RHACS can initiate the renewal and replacement of these certificates.

1.2.2. Vulnerability Management 2.0 (Technology Preview)

In RHACS 4.1, you can experience significant improvements in Vulnerability Management with the introduction of Workload CVEs (Technology Preview). This feature is the first function in Vulnerability Management 2.0 and provides you with improved workflows that are purposeful and effortless to navigate.



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 .

These improved workflows provide actionable data to help you address vulnerabilities. It is anticipated that Vulnerability Management 1.0 functionality will transition to Vulnerability Management 2.0 in upcoming releases.

This release provides a new navigation menu item, **Vulnerability Management 2.0**, which provides a view of vulnerabilities in applications running on clusters in your system. It is anticipated that in upcoming releases, this menu item will also provide a view of vulnerabilities present in the platform and nodes.

The **Workload CVEs** page provides a view of vulnerabilities in images and deployments, as well as options to filter and sort the data displayed. You can select specific vulnerabilities to view additional details, such as the Dockerfile layer in which the vulnerability exists and whether or not it can be fixed.

In this technology preview, you can explore the read-only **Workload CVEs** page. However, upcoming releases are expected to include additional functionality. For more information, see Vulnerability Management process.

1.2.3. RHACS Cloud Service scanning support for images pulled from on-premise registries

RHACS 4.1 introduces a new feature to support RHACS Cloud Service environments where the container registries are not accessible from the RHACS Cloud Service Central Services. This feature brings architectural changes to the RHACS scanning functionality that allow you to delegate vulnerability scanning to the RHACS secured cluster services. You can configure the settings required to delegate scanning through the RHACS APIs. It is anticipated that in an upcoming release, you will also be able to do this configuration by using the RHACS portal.

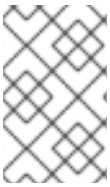
1.2.4. eBPF collection method on IBM Z and IBM(R) LinuxONE

With this release, RHACS has extended support for the eBPF collection method to IBM Z and IBM® LinuxONE. Now you can use this method to capture and analyze process and network activity in your OpenShift cluster on IBM Z and IBM® LinuxONE.

1.2.5. Ability to configure the display of default compliance standards in the Compliance Dashboard

You can now simplify and focus the Compliance Dashboard results by selecting only the built-in default standards you want to see in your results. You can now configure the dashboard to display specific default compliance standards, such as CIS Docker v1.2.0 and HIPAA 164, and remove standards that you do not want to display. You can configure the display by using the **Manage standards** button in the Compliance Dashboard.

For more information, see Running a compliance scan.



NOTE

Standards controlled by the compliance operator cannot be disabled or hidden in RHACS. You must configure the compliance operator custom resource definitions (CRDs) to remove them from display.

1.2.6. Declarative configurations for authentication and authorization

Customers following the cloud-native paradigm, prefer to use declarative configurations for versioning and auditability. Declarative configurations allow you to use configuration management tools to configure and update resources in your environment, rather than configuring resources directly in the system each time you want to make changes.

After using declarative configuration to specify parameters for resources, you can quickly update configurations that are stored in repositories and apply them to the system using a GitOps workflow.

You can create declarative configurations for authentication and authorization resources such as authentication providers, roles, permission sets, and access scopes. Configurations are stored in YAML files and mounted during Central installation. For more information, see Declarative configuration for authentication and authorization resources.

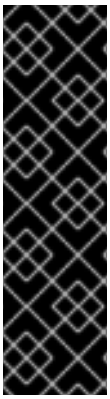
1.2.7. SSO configuration using the roxctl CLI

In RHACS 4.1, you can enhance Central's security and login capabilities with the new feature of using an authentication provider to authorize the **roxctl** CLI. This feature enables you to use the **roxctl** CLI and integrate with authentication systems such as OpenID Connect (OIDC) for a seamless single sign-on (SSO) experience without requiring additional tokens or passwords. Previously, the **roxctl** CLI only supported token and password-based workflows.

For more information, see Using an authentication provider to authenticate with roxctl .

1.2.8. New collection method based on BPF CO-RE (Technology Preview)

With this release, you can test a new runtime collection method that no longer requires a precompiled driver (either downloaded or provided through support package upload) for the host operating system (OS).



IMPORTANT

The **CORE_BPF** collection method 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 .

This feature is available for testing on **x86_64** and **s390x** architectures and is based on the new Linux BPF features, including CO-RE (Compile Once-Run Everywhere). To enable it, set the value of the **collector.collectionMethod** parameter of your backed-up cluster to **CORE_BPF**.

The new method offers several advantages:

- The clusters built on a host OS that is not currently part of the Collector support package can now be secured.
- Improved uptime and fewer issues related to kernel drivers not being available.
- Offline customers can update the kernel of the host OS without uploading a new support package to Central.

Using CORE_BPF can have a higher performance overhead than other collection methods under certain conditions.

1.2.9. Network graph updates

The Network graph (previously, version 2.0 preview) is now in general availability (GA). The earlier **Network graph (1.0)** page has been removed. Improvements and bug fixes have been made to the network graph page, including the following changes:

- Ability to view filtered and related namespaces.
- Improvements to existing badges, icons, and labels.
- Fixed bug for anomalous traffic details.

- Additional verbal clarification for generation of network policies added for the network policy simulation feature in the RHACS portal.

The option to apply recommended network policies directly from the network graph has been discontinued, as this is not a recommended best practice. For network graph documentation, see Managing network policies.

1.2.10. Policy Management simplification

RHACS 4.1 introduces improvements to policy creation and editing in the RHACS portal to provide a more intuitive experience and reduce the potential for errors. Some criteria field names have been revised to be more descriptive. When you drag a criteria field into place, a clear sentence in natural language now indicates the condition that triggers that criteria.

Additionally, the RHACS portal now only displays the criteria that are relevant to the selected policy and hides all unnecessary options. In addition, the documentation has been adapted to the layout of the RHACS portal to ensure consistency and make it easier for you to find the help and guidance you need.

Finally, the **Policy List** in the **Policy Management** section includes a new **Origin** column that allows you to easily distinguish between system default policies and user-created policies.

1.2.11. New permission sets

The following new roles and permission sets have been added:

- Network Graph Viewer: With the RHACS 4.1 release, you now have the ability to restrict network graph views to specific namespaces to which the user has access, rather than allowing the user to view network graphs for the entire cluster. The Network Graph Viewer role provides read-only access to the network graph pages.
- Vulnerability Management Admin: This permission set provides administrative access to analyze vulnerabilities, generate reports, and manage the risk acceptance process.
- Vulnerability Management Consumer: This permission set provides read-only access to analyze vulnerabilities and initiate the risk acceptance process.

For more information, see System permission sets.

1.2.12. Improvements for Sensor resync (General Availability)

In RHACS 4.1, improvements have been made to reduce the use of the central processing unit (CPU), which is required to resync Sensor with Central. This feature, previously introduced as a technology preview in RHACS 4.0, focuses on reducing the usage of CPU, which is required to resync Sensor with Central.

The changes in the use of CPU becomes apparent over time. Since this new feature reduces the need to constantly process Kubernetes events, you should notice a significant improvement in your use of CPU after a few hours.

1.3. NOTABLE TECHNICAL CHANGES

- The workflow for adding policy criteria during policy creation has been improved. You can now only choose policy criteria that is available for the lifecycle stage of the policy. For more information, see Creating custom policies.

- The syslog integration now includes namespace label information for alert messages.
- The Central persistent volume claim (PVC) **stackrox-db** is deprecated and is no longer needed after this upgrade.
- The output of the **roxctl central whoami** command now includes the username, which provides additional information in the results.
- The Helm setting **collector.nodeInventoryResources** has been renamed **collector.nodeScanningResources** for clarity and consistency.
- A new Helm setting, **admissionController.replica**, is introduced to configure the number of replicas for the Admission Controller.
- The **k8s-istio.zip** file in the **scanner-vuln-updates.zip** package (downloaded from https://install.stackrox.io/scanner/scanner-vuln-updates.zip to update Scanner vulnerabilities in offline mode) is no longer required. The **k8s-istio.zip** file is still included to support older versions of the product, but it is ignored during the update process.
- You can now configure the time interval used to determine the frequency of scanning Orchestrator-level components (Kubernetes, OpenShift, Istio) with the **ROX_ORCHESTRATOR_VULN_SCAN_INTERVAL** environment variable.
- You can now synchronize image integrations with secured clusters that have local scanning enabled.

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 4.1
Examining images for Application-level dependencies for vulnerability reporting: **dotnet/shared/Microsoft.AspNetCore.App/** and **dotnet/shared/Microsoft.NETCore.App/**	GA	DEP	DEP

Feature	RHACS 3.74	RHACS 4.0	RHACS 4.1
Expiration field in **Exclusion** proto	GA	DEP	DEP
Kernel module collection method	DEP	DEP	REM
Network Graph version 1.0	GA	DEP	REM
roxctl scanner generate flag **offline-mode** (flag only)	GA	DEP	DEP
/v1/report endpoint	GA	DEP	DEP
/v1/serviceaccounts endpoint	GA	DEP	DEP
Vulnerability Management 1.0: Image CVEs, Image Components, Images, Deployments, and Namespaces.	GA	GA	DEP
Custom Security Context Constraints (SCCs): **stackrox-collector**,**stackrox-admission-control**, and **stackrox-sensor**	GA	GA	DEP
Vulnerability Management Approver permission	GA	GA	DEP
Vulnerability Management Requester permission	GA	GA	DEP
Vulnerability Report Creator permission	GA	GA	DEP
Vulnerability Reports and **Policy** permission	DEP	DEP	REM
Role resource	DEP	DEP	REM
Scope Manager system role and permission set	DEP	DEP	REM
ROX_FORCE_LOCAL_IMAGE_SCANNING environment variable	DEP	DEP	REM

1.4.1. Deprecated features

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

- Avoid using the following sections in Vulnerability Management 1.0: Image CVEs, Image Components, Images, Deployments, and Namespaces. They are deprecated and it is anticipated that these sections will be removed in a future release. Instead, use Vulnerability Management

2.0 to manage workload vulnerabilities.

- Ensure that you do not use custom security context constraints (SCCs) such as **stackrox-collector**,**stackrox-admission-control**, and **stackrox-sensor** for workloads other than RHACS. These SCCs are deprecated and it is anticipated that they will be removed in a future release.

- The default **Vulnerability Management Approver** permission set is deprecated. Use the **Vulnerability Management Admin** permission instead. Existing roles that use **Vulnerability Management Approver** will be updated to use **Vulnerability Management Admin** when the permission set is removed in the future.

- The default **Vulnerability Management Requester** permission set is deprecated. Use the **Vulnerability Management Consumer** permission instead. Existing roles that use **Vulnerability Management Requester** will be updated to use **Vulnerability Management Consumer** when the permission set is removed in the future.

- The default **Vulnerability Report Creator** permission set is deprecated. Use the **Vulnerability Management Admin** permission instead. Existing roles that use **Vulnerability Report Creator** will be updated to use **Vulnerability Management Admin** when the permission set is removed in the future.

1.4.2. Removed features

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

1.4.2.1. Role resource

The **Role** resource has been removed in this release. To address this change, replace the deprecated resource with the appropriate replacement and remove the deprecated resource from the code base.

1.4.2.2. Scope Manager system role and permission set

As announced in the Release notes for RHACS 3.74.0, the **Scope Manager** system role and permission set are removed in this release. If you have existing installations that reference the **Scope Manager** system role and the permission set, adjustments are observed in the referenced objects.

These adjustments include a description of the removal and the objects are no longer marked as system resources. It is important to note that the Scope Manager system role and permission set will be completely removed from the system.

To address this change, you must update the configurations accordingly to ensure continued functionality.

1.4.2.3. ROX_FORCE_LOCAL_IMAGE_SCANNING environment variable

The **ROX_FORCE_LOCAL_IMAGE_SCANNING** environment variable has been removed in this release. To address this change, replace references to this variable with the one that uses the delegated registry configuration.

1.4.2.4. Kernel module collection method (updated 11 July 2023)

The kernel module collection method has been removed in this release following its deprecation in RHACS 4.0.

If you are using OpenShift Container Platform and the RHACS Operator, and your upgrades are failing, see RHACS Operator upgrade to 4.1.0 stuck in Pending state due to removal of "KernelModule" collection method for important information and steps you must take to resolve those issues.

1.4.2.5. Network graph 1.0

Network graph 1.0 has been removed after the depreciation notice in RHACS 4.0. Network graph 2.0 performs the same functionality and is in GA.

1.5. NOTICE OF UPCOMING CHANGE FOR REPORTS

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.

We expect in the next RHACS release to delete those 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. For more information on collections, see Creating and using deployment collections .

1.6. BUG FIXES

1.6.1. Resolved in version 4.1

Release date: 29 Jun 2023

- Previously, if you encountered a scenario where the Pod Security Policies (PSPs) were not enabled, the upgrader might trigger an error because it assumed they should be valid based on the files present in the bundle. This has been fixed. (ROX-17771)
- Previously, when automatically detecting whether PSPs were allowed, there was a problem that Collector PSPs were always applied first, regardless of whether the PSPs were enabled or not. This has been fixed. (ROX-17734)
- Previously, the RHACS Cloud Service console portal crashed and displayed a Sentry error when attempting to access such instances. This situation could occur because either the instance was deleted or an incorrect URL was entered. This has been fixed. Now, such instances are handled gracefully and a 404 page is displayed instead. (ROX-17475)
- Previously, the **roxctl -e $ROX_CENTRAL_ADDRESS image scan** command failed to scan a multi-arch image due to unsupported OCI indexes. The error message indicated problems retrieving metadata and manifest digests, resulting in an HTTP 404 response. With this update, you need to upgrade to the latest version that correctly processes multi-arch images and provides accurate reports or appropriate error messages. (ROX-17197)
- Previously, when you upgraded the RHACS Operator to 4.0, the Central pod experienced frequent restarts and panics with a stack trace. Despite a restart of the deployments, the issue persisted. This has been fixed. (ROX-17189)
- Previously, Collector bounced frequently during upgrade tests, causing throttling and preventing kernel components from downloading. This has been fixed. (ROX-17134)
- Previously, an upgrade to RHACS 4.0 resulted in increased memory usage in the Collector

container. The issue resulted from Collector using a **hostPath** volume to access the CRI socket, which is not available in the **cri-o** engine used by Openshift. With this update, you can either restore the CRI connection by inserting the required socket paths, patch falco to remove inactive containers, or disable the collection of user information. (ROX-17096)

- Fixed an issue where the **Network Policies** tab would display a strange entry and the view would frequently refresh when interacting with the list or cursor. (ROX-17028)

- Fixed an issue where you could not scroll through the Access Control roles to view all the potential roles. (ROX-16992)

- Previously, creating roles with declarative configurations failed due to invalid arguments when referencing default access scopes and permission sets. The transformer assigned the name to a UUID, but the UUID for the default access scopes and permission sets was different.
  The acceptance criteria should ensure that a declarative configuration for a role could successfully reference the default permission sets and permission scopes during creation. This has been fixed. To avoid issues when creating roles, ensure that your configuration contains the correct UUID for the default access scope and permission set. (ROX -16983)

- Fixed an issue with sensor certificate rotation in secured clusters deployed with RHACS Operator. The issue was also fixed for Helm-based and manifest-based installations where image references were provided with **sha256** digests instead of image tags. (ROX-16212)

- Fixed an issue with inconsistent API responses in the network policy graph. The fix ensures that the network graph now provides consistent and accurate network policy information. (ROX-14668)

- Previously, there was a crash loop when reinstalling Central with Postgres enabled. This issue occurred due to a mismatch between the life cycle of the **central-db-password** secret and the **central-db** PVC. The operator intentionally did not delete the PVCs when deleting Central to avoid data loss, but deleted the secret that contained the password.
  When Central was reinstalled, the password of the new secret didn't match the one stored in the PVC, resulting in an authentication failure. With this update, you can keep the secret if the PVC is kept, and delete the PVC or restore the secret before reinstalling. (ROX-13947)

1.6.2. Resolved in version 4.1.1

Release date: 11 July 2023

- Previously, upgrading from RHACS 4.0.2 to RHACS 4.1 using the RHACS Operator would fail because of the deprecated KernelModule collector support in RHACS 4.1. The updated image fixes this issue.

1.6.3. Resolved in version 4.1.2

Release date: 26 July 2023

- RHACS 4.1.2 includes a fix for an issue where an operator-based RHACS installation failed to upgrade from versions earlier than RHACS 3.71. The failure occurred because the older versions did not implement PSP auto-sensing on the Kubernetes cluster 1.25 or later.

- Previously, if you were using RHACS with Istio, the Scanner pods would crash if Istio reported the version as **latest** instead of the actual version number, such as **1.17**. The updated image fixes this issue.

- Fixed an issue where upgrading from RHACS 3.74.3 to RHACS 4.1.1 failed with an "insert... violates foreign key restraint" error.

1.6.4. Resolved in version 4.1.3

Release date: 21 August 2023

- Fixed an issue where RHACS reported an incorrect component version for Tomcat used in an application.
- Removed a check that prevented a rollback to an earlier version of RHACS after migration.
- 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.

1.6.5. Resolved in version 4.1.4

Release date: 17 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.

1.6.6. Resolved in version 4.1.5

Release date: 8 November 2023

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.

1.6.7. Resolved in version 4.1.6

Release date: 22 January 2024

This release of RHACS fixes PostgreSQL vulnerabilities in the **central**, **central-db**, and **scanner-db** containers.

1.6.8. Known issues (updated 11 July 2023)

- For secured clusters on IBM Z and IBM® LinuxONE that are running OpenShift Container Platform 4.10, Collector fails to start when the default configuration is used. As a workaround, enable the CORE_BPF collection method (Technology Preview). (ROX-18058)

- For secured clusters on IBM Z and IBM® LinuxONE, there is a known issue with the Process Group Identifier (GID) in the **ProcessesService** API where the reported GID can be incorrect and display a value of **-1**. This affects process details provided through the **/v1/processes/deployment/{deploymentId}** API endpoint and other APIs that provide process signal information.
  This can lead to inaccuracies or inconsistencies in the reported GID. This issue does not impact the RHACS portal or policy criteria. Also, when using ePBF on IBM Z and IBM® LinuxONE, the GID process might be invalid (**-1**) for processes that terminate shortly after execution. There is currently no workaround for this issue. (ROX-17459)

- Currently, the Syslog common event format (CEF) sends the name and severity fields in an incorrect order. There is currently no workaround for this issue.

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-rhel8:4.1.5**
Scanner	Scans images and nodes.	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:4.1.5**
Scanner DB	Stores image scan results and vulnerability definitions.	**registry.redhat.io/advanced-cluster-security/rhacs-scanner-db-rhel8:4.1.5**
Collector	Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.	• **registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:4.1.5** • **registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:4.1.5**
Central DB	Postgres instance that provides the database storage for Central.	**registry.redhat.io/advanced-cluster-security/rhacs-central-db-rhel8:4.1.5**