Red Hat Advanced Cluster Security for Kubernetes 3.71

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 3.71 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.
Table of Contents

CHAPTER 1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.71 ........................................ 5
  1.1. NEW FEATURES .............................................. 5
    1.1.1. New RHACS Dashboard ......................... 5
    1.1.1.1. Status bar hyperlinks ................... 5
    1.1.1.2. Dashboard filter ......................... 6
    1.1.1.3. Widget options ......................... 6
    1.1.1.4. Actionable widgets .................. 6
    1.1.1.5. Removed widgets ...................... 7
    1.1.2. New default policy for privilege escalation .................... 7
    1.1.3. New default policy for externally exposed service ................. 8
    1.1.4. Ability to assign multiple RHACS roles to users and groups .......... 8
    1.1.5. List of network policies in Deployment tab for violations ............. 8
    1.1.6. Alpine 3.16 support ...................... 8
  1.2. ENHANCEMENTS ........................................ 8
    1.2.1. Change to roxctl image scan behavior .............. 8
    1.2.2. Update to diagnostic bundles .................. 8
    1.2.3. Align OCP4–CIS scanning benchmarks control numbers .............. 8
  1.3. NOTABLE TECHNICAL CHANGES ......................... 9
    1.3.1. eBPF is now the default collection method ............... 9
    1.3.2. Shutdown of Stackrox image registry sites ............... 9
  1.4. DEPRECATED AND REMOVED FEATURES .................. 9
    1.4.1. Deprecated features ...................... 10
    1.4.2. Removed features ....................... 11
  1.5. BUG FIXES ........................................ 11
  1.6. UPGRADE INSTRUCTIONS FOR ROXCTL USERS .......... 12
  1.7. IMAGE VERSIONS ....................................... 12

CHAPTER 2. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.70 ........................................ 13
  2.1. NEW FEATURES ........................................ 13
    2.1.1. Verifying image signatures against Cosign public keys .......... 13
    2.1.2. Identifying missing Kubernetes network policies ................. 13
  2.2. ENHANCEMENTS ........................................ 13
    2.2.1. Identifying Spring critical vulnerabilities .................. 13
    2.2.2. Automatic Amazon ECR registry integration .................. 13
    2.2.3. Improved validation of pod security context .................. 14
    2.2.4. Increased number of allowed inclusion and exclusion scopes .......... 14
    2.2.5. Finding ACS admin user credentials easily in the OpenShift Container Platform console .......... 14
  2.3. NOTABLE TECHNICAL CHANGES ......................... 14
    2.3.1. Vulnerability scanning and reporting for RHCOS nodes .......... 14
  2.4. DEPRECATED AND REMOVED FEATURES .................. 14
    2.4.1. Deprecated features ...................... 15
    2.4.2. Removed features ....................... 16
  2.5. BUG FIXES ........................................ 16
    2.5.1. Resolved in version 3.70.1 ................... 16
    2.5.2. Resolved in version 3.70.0 ................... 16
  2.6. IMAGE VERSIONS ....................................... 16

CHAPTER 3. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.69 ........................................ 18
  3.1. NEW FEATURES ........................................ 18
    3.1.1. Released in version 3.69.1 ................... 18
      3.1.1.1. Scanning of the integrated OpenShift Container Registry .......... 18
3.1.1.2. Improved detection of Spring vulnerabilities
3.12. Released in version 3.69.0
3.12.1. New policies to manage operational deployment readiness
3.12.2. Inactive software component identification
3.12.3. Vulnerability scanning enhancements

3.2. IMPORTANT BUG FIXES
3.2.1. Resolved in version 3.69.2
3.2.2. Resolved in version 3.69.0

3.3. IMPORTANT SYSTEM CHANGES
3.3.1. Redesigned policy creation workflow
3.3.2. Enhancements to sorting and filtering image vulnerabilities
3.3.3. Enhanced compatibility with UEFI secure boot
3.3.4. Scanner memory limit increases

3.4. KNOWN ISSUES
3.5. DEPRECATION NOTICE
3.6. IMAGE VERSIONS

CHAPTER 4. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.68

4.1. NEW FEATURES
4.1.1. Vulnerability triage workflows
4.1.2. Report scheduling for vulnerabilities
4.1.3. Use AWS AssumeRoles
4.1.4. Enhancements for CI outputs
4.1.5. Automount Service Account Token policy criteria
4.2. IMPORTANT BUG FIXES
4.2.1. Resolved in version 3.68.2
4.2.2. Resolved in version 3.68.1
4.2.3. Resolved in version 3.68.0
4.3. SECURITY UPDATE
4.4. IMPORTANT SYSTEM CHANGES
4.4.1. Changes in version 3.68.1
4.4.2. Changes in version 3.68.0
4.5. IMAGE VERSIONS

CHAPTER 5. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.67

5.1. NEW FEATURES
5.1.1. Released in version 3.67.2
5.1.1.1. Log4Shell policy
5.1.2. Released in version 3.67.0
5.1.2.1. OpenShift Dedicated support
5.1.2.2. Use OpenShift Container Platform OAuth server as an identity provider
5.1.2.3. Enhancements for CI outputs
5.1.2.4. Runtime Class policy criteria
5.2. IMPORTANT BUG FIXES
5.2.1. Resolved in version 3.67.1
5.2.2. Resolved in version 3.67.2
5.3. IMPORTANT SYSTEM CHANGES
5.4. IMAGE VERSIONS

CHAPTER 6. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.66

6.1. NEW FEATURES
6.1.1. Scan deployment configurations in your CI pipeline
6.1.2. Active component identification
6.1.3. New configuration settings for Operator and Helm charts
6.2. IMPORTANT BUG FIXES
   6.2.1. Resolved in version 3.66.1
6.3. IMPORTANT SYSTEM CHANGES
6.4. IMAGE VERSIONS

CHAPTER 7. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.65

7.1. NEW FEATURES
   7.1.1. MITRE ATT&CK Containers Matrix
   7.1.2. Install on more platforms
   7.1.3. Admission control configuration
7.2. IMPORTANT BUG FIXES
   7.2.1. Resolved in version 3.65.1
7.3. IMPORTANT SYSTEM CHANGES
7.4. UPCOMING CHANGES
7.5. IMAGE VERSIONS

CHAPTER 8. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.64

8.1. NEW FEATURES
8.2. IMPORTANT BUG FIXES
   8.2.1. Resolved in version 3.64.1
   8.2.2. Resolved in version 3.64.2
8.3. IMPORTANT SYSTEM CHANGES
8.4. IMAGE VERSIONS

CHAPTER 9. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.63

9.1. RELEASE TAG VERSION CHANGE
9.2. NEW FEATURES
   Installing by using an Operator
   Scoped access control
   Improved alert functionality for OpenShift Container Platform
9.3. IMPORTANT SYSTEM CHANGES
9.4. IMAGE VERSIONS

CHAPTER 10. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.0.62

10.1. NEW FEATURES
   10.1.1. Compliance Operator integration
   10.1.2. Alpine image vulnerability feed updates
10.2. IMPORTANT BUG FIX
10.3. IMPORTANT SYSTEM CHANGES
10.4. RELEASE TAG VERSION CHANGE
10.5. IMAGE VERSIONS

CHAPTER 11. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.0.61

11.1. NEW FEATURES
11.2. IMPORTANT BUG FIXES
   11.2.1. Resolved in version 3.0.61.1
11.3. IMPORTANT SYSTEM CHANGES
11.4. IMAGE VERSIONS

CHAPTER 12. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.0.60

12.1. NEW FEATURES
12.2. IMPORTANT BUG FIXES
   12.2.1. Resolved in version 3.0.60.1
12.3. IMPORTANT SYSTEM CHANGES
12.4. IMAGE VERSIONS
CHAPTER 1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.71

Release date: 25 July 2022
Updated: 30 August 2022

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. It deploys in your infrastructure and integrates with your DevOps tooling and workflows to deliver better security and compliance and to enable DevOps and InfoSec teams to operationalize security.

RHACS 3.71 includes:

- A new top-level Dashboard to increase your efficiency
- Two new default policies to help improve your security posture
- Ability to set eBPF as the default collection method to boost performance
- Additional feature enhancements and bug fixes

1.1. NEW FEATURES

1.1.1. New RHACS Dashboard

RHACS introduces a new top-level Dashboard designed to provide quick access to the data you need. It provides additional navigation shortcuts and a panel of actionable widgets that are easy to filter and customize so that you can focus on what matters most to you. We would love to hear your feedback to help us shape future enhancements, including which widgets you would like on the Dashboard and how you would like to customize them.

The changes to the Dashboard in RHACS 3.71 are described in the following section. For more information, see Viewing the Dashboard.

1.1.1.1. Status bar hyperlinks

The Status Bar provides at-a-glance numerical counters for key resources. The counters reflect what is visible with your current access scope, which is defined by the roles associated with your user profile. These counters are clickable, providing fast access to desired list view pages as follows:

<table>
<thead>
<tr>
<th>Counter</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clusters</td>
<td>Platform Configuration → Clusters</td>
</tr>
<tr>
<td>Nodes</td>
<td>Configuration Management → Application &amp; Infrastructure → Nodes</td>
</tr>
<tr>
<td>Violations</td>
<td>Violations main menu</td>
</tr>
<tr>
<td>Deployments</td>
<td>Configuration Management → Application &amp; Infrastructure → Deployments</td>
</tr>
</tbody>
</table>
### 1.1.2. Dashboard filter

The Dashboard now includes a top-level filter that applies simultaneously to all widgets. You can select one or more clusters, and one or more namespaces within selected clusters. When no clusters or namespaces are selected, the view automatically switches to All. Any change to the filter is immediately reflected by all widgets, limiting the data they present to the selected scope. The Dashboard filter does not affect the Status Bar.

### 1.1.3. Widget options

Some widgets are now customizable to help you focus on what matters the most to you. Widgets offer different controls that change how the data is sorted, allow you to filter the data, and help you to customize the widget’s output.

Widgets offer two ways to customize different aspects:

- An **Options** menu, when present, provides specific options applicable to that widget.
- A **dynamic axis legend**, when present, allows you to filter data by hiding one or more of the axis categories. For example, in the **Policy violations by category** widget, you can click on a severity to include or exclude respective violations from the data.

**NOTE**

Individual widget customization settings are short lived and are reset to the system default upon leaving the Dashboard.

### 1.1.4. Actionable widgets

The Dashboard provides the following actionable widgets:

- **Policy violations by severity.** This widget shows the distribution of violations across severity levels for the Dashboard-filtered scope. Clicking a **severity level** in the chart takes you to the Violations page, filtered for that severity and scope. It also lists the three most recent violations of a **Critical** level policy within the scope you defined in the Dashboard filter. Clicking a specific violation takes you directly to the Violations detail page for that violation.

- **Images at most risk**. This widget lists the top six vulnerable images within the Dashboard-filtered scope, sorted by their computed risk priority, along with the number of critical and important CVEs they contain. Click an image name to go directly to the **Image Findings** page under **Vulnerability Management**. Use the **Options** menu to focus on fixable CVEs, or further focus on active images.
NOTE

When clusters or namespaces have been selected in the Dashboard filter, the data displayed is already filtered to active images, or images that are being used by deployments within the filtered scope.

- **Deployments at most risk**: This widget provides the information that was previously available in the Top risky deployments widget, but displays additional information such as the resource location (cluster and namespace) and the risk priority score. Additionally, you can click on a deployment to view risk information about the deployment; for example, its policy violations and vulnerabilities.

- **Aging images**: Older images present a higher security risk as they can contain vulnerabilities that have already been addressed. If older images are active, they can expose deployments to exploits. This widget allows you to quickly assess your security posture and identify offending images. You can use the default ranges or customize the age intervals with your own values. You can view both inactive and active images or use the Dashboard filter to focus on a particular area for active images. You can then click on an age group in this widget to view only those images in the Vulnerability Management → Images page.

- **Policy violations by category**: This widget can help you gain insights about the challenges your organization is facing in complying with security policies, by analyzing which types of policies are violated more than others. The widget shows the five policy categories of highest interest. Explore the Options menu for different ways to slice the data. You can filter the data to focus exclusively on deploy or runtime violations. You can also change the sorting mode. By default, the data is sorted by the number of violations within the highest severity first. Therefore, all categories with critical policies will appear before categories without critical policies. The other sorting mode considers the total number of violations regardless of severity. As some categories contain no critical policies (for example, “Docker CIS”), the two sorting modes can provide significantly different views, offering additional insight. Click on a severity level at the bottom of the graph to include or exclude that level from the data, potentially resulting in a different top five selection, as well as a different ranking order. Data is filtered to the scope selected by the Dashboard filter.

- **Compliance by standard**: The Compliance widget is an improvement over a similar widget included in the past. It uses the Dashboard filter, allowing you to focus on areas that matter to you the most. The widget lists the top or bottom six compliance benchmarks, depending on sort order. Select Options to sort by the respective coverage percentage. Click on one of the benchmark labels or graphs to go directly to the Compliance Controls page, filtered by the Dashboard scope and the selected benchmark.

1.1.5. Removed widgets

- **Individual Policy Category widgets**: Previous product versions included a set of widgets showing the distribution of policy violations across severity levels, per policy category. The widgets were automatically generated for every policy category. To view similar data, use the Policy violations by category widget and click a category to get to the same Violations page.

- **Active violations by time**: Previous product versions included a line graph depicting the number of violations over a seven-day period. This graph has been removed with the understanding that more comprehensive historical metrics are desired. This topic is being considered as a product enhancement request.

1.1.2. New default policy for privilege escalation
This new default policy detects if a deployment is running with a container that has `allowPrivilegeEscalation` set to `true`. This policy is enabled by default. The privilege escalation setting is enabled in Kubernetes pods by default. A container process that can run with more privileges than its parent process can allow the container to run with unintended privileges, creating a security risk. This policy provides an alert so that you can verify whether privileged escalation is required. For example, it may be necessary if the required privileges cannot be provided with a subset of other controls.

1.1.3. New default policy for externally exposed service

This new policy detects if a deployment has any service that is externally exposed through any methods. The policy is disabled by default. Deployments with services exposed outside of the cluster are at a higher risk of attempted intrusions because they are reachable outside of the cluster. This policy provides an alert so that you can verify that service exposure outside of the cluster is required. If the service is only needed for intra-cluster communication, use service type `ClusterIP`.

1.1.4. Ability to assign multiple RHACS roles to users and groups

Role-based Access Control (RBAC) in RHACS has been enhanced to allow you to assign multiple roles to a single user or group. Previously, a key-value pair could only be assigned to a single role. Now, that key-value pair can be assigned to multiple RHACS roles. This change allows you to reuse existing roles and simplifies role management. For more information, see Managing RBAC in Red Hat Advanced Cluster Security for Kubernetes.

1.1.5. List of network policies in Deployment tab for violations

A new information section has been added to help resolve a "missing Kubernetes network policy" violation. When viewing a violation, select the Deployment tab and scroll to the new Network policy section. It lists all the Kubernetes network policies applicable to the namespace of the offending deployment. You can use this list to verify which network policies exist in the namespace to help you determine why a deployment was flagged as missing a network policy.

1.1.6. Alpine 3.16 support

Scanner now supports Alpine 3.16.

1.2. ENHANCEMENTS

1.2.1. Change to roxctl image scan behavior

The default value for the `--include-snoozed` option of the `roxctl image scan` command is set to `false`. If the `--include-snoozed` option is set to `false`, the scan does not include snoozed CVEs.

1.2.2. Update to diagnostic bundles

You can create diagnostic bundles to assist Red Hat in supporting you with RHACS. This diagnostic bundle has been enhanced to include notifiers, auth providers and auth provider groups, access control roles with attached permission set and access scope, and system configuration information. Users with the DebugLogs permission can read listed entities from a generated diagnostic bundle regardless of their respective permissions.

1.2.3. Align OCP4-CIS scanning benchmarks control numbers
The CIS control number has been added to compliance scan results to enable customers to reference the original control from the CIS benchmark standard (ROX-9986).

### 1.3. NOTABLE TECHNICAL CHANGES

#### 1.3.1. eBPF is now the default collection method

In RHACS 3.71, Red Hat has updated the default collection method for Collector to eBPF. Using eBPF for data collection takes advantage of modern kernel features and improves performance over kernel modules by 25%. Additionally, it reduces processed syscall events by 99%.

**NOTE**

You should switch to kernel module collection if you are using:

- OpenShift Container Platform version 3.11, which uses Red Hat Enterprise Linux (RHEL) 7. It does not support the features required for performance improvement.
- SELinux on RHEL 7, which may also prevent the loading of eBPF probes.

#### 1.3.2. Shutdown of Stackrox image registry sites

The image registries hosted at the stackrox.io and collector.stackrox.io addresses were shut down. Images for RHACS are available from registry.redhat.io.

### 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, refer to the table below. 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

#### Table 1.1. Deprecated and removed features tracker

<table>
<thead>
<tr>
<th>Feature</th>
<th>RHACS 3.69</th>
<th>RHACS 3.70</th>
<th>RHACS 3.71</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to add comments to alerts and processes</td>
<td>DEP</td>
<td>DEP</td>
<td>REM</td>
</tr>
<tr>
<td>Anchore, Tenable, and Docker Trusted registry integrations</td>
<td>DEP</td>
<td>DEP</td>
<td>REM</td>
</tr>
<tr>
<td>Feature</td>
<td>RHACS 3.69</td>
<td>RHACS 3.70</td>
<td>RHACS 3.71</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>External authorization plug-in for scoped access control</td>
<td>DEP</td>
<td>DEP</td>
<td>REM</td>
</tr>
<tr>
<td>FROM option in the Disallowed Dockerfile line policy field</td>
<td>GA</td>
<td>DEP</td>
<td>REM</td>
</tr>
<tr>
<td>PodSecurityPolicy (PSP) Kubernetes objects</td>
<td>GA</td>
<td>DEP</td>
<td>REM</td>
</tr>
<tr>
<td>RenamePolicyCategory and DeletePolicyCategory API endpoints</td>
<td>GA</td>
<td>DEP</td>
<td>DEP</td>
</tr>
<tr>
<td>--rhacs option for the roxctl helm output command</td>
<td>DEP</td>
<td>DEP</td>
<td>REM</td>
</tr>
<tr>
<td>/v1/nodes and /v1/images API endpoint response:</td>
<td>DEP</td>
<td>DEP</td>
<td>REM</td>
</tr>
<tr>
<td>firstNodeOccurrence response body parameter</td>
<td>GA</td>
<td>GA</td>
<td>DEP</td>
</tr>
<tr>
<td>Permissions: AuthPlugin, AuthProvider, Group, Licenses, Role, User, Indicator, NetworkBaseline, ProcessWhitelist, Risk, APIToken, BackupPlugins, ImageIntegration, Notifier, SignatureIntegration, ImageComponent</td>
<td>GA</td>
<td>GA</td>
<td>DEP</td>
</tr>
<tr>
<td>Retrieving groups by property</td>
<td>GA</td>
<td>GA</td>
<td>DEP</td>
</tr>
<tr>
<td>vulns fields of storage.Node object in response payload of v1/nodes</td>
<td>GA</td>
<td>GA</td>
<td>DEP</td>
</tr>
<tr>
<td>/v1/cves/suppress and /v1/cves/unsuppress</td>
<td>GA</td>
<td>GA</td>
<td>DEP</td>
</tr>
<tr>
<td>ids field in the /v1/cves/suppress and /v1/cves/unsuppress API payload</td>
<td>GA</td>
<td>GA</td>
<td>DEP</td>
</tr>
<tr>
<td>cves.ids field of the storage.VulnerabilityRequest object in the response of VulnerabilityRequestService endpoints</td>
<td>GA</td>
<td>GA</td>
<td>DEP</td>
</tr>
</tbody>
</table>

1.4.1. Deprecated features

- Permissions for permission sets will be grouped for simplification. The following list describes the new permissions and indicates the deprecated permissions that will be removed in a future release:
  - The Access permission will replace the following permissions: AuthPlugin, AuthProvider, Group, Licenses, Role, and User.
The DeploymentExtension permission will replace the following permissions: Indicator, NetworkBaseline, ProcessWhitelist, and Risk.

The Integration permission will deprecate the following permissions: APIToken, BackupPlugins, ImageIntegration, Notifier, and SignatureIntegration.

The Image permission will replace the permission ImageComponent.

Previously, groups were retrieved by the field props (props.authProviderId, props.key, props.value). This field will be replaced by the new props.id field. Use the props.id field to retrieve groups in the Application Programming Interface (API). Note the following:

Retrieval using the props fields will be removed in version a future release.

Until removal, retrieval using the props field will work if the result is unambiguous (no more than one group is found with the props field).

/v1/cves/suppress and /v1/cves/unsuppress have been deprecated and will be removed in a future release.

Use /v1/imagecves/suppress and /v1/imagecves/unsuppress to snooze and unsnooze image vulnerabilities.

Use /v1/nodecves/suppress and /v1/nodecves/unsuppress to snooze and unsnooze node and host vulnerabilities.

Use /v1/clustercves/suppress and /v1/clustercves/unsuppress to snooze and unsnooze platform (Kubernetes, Istio, and OpenShift Container Platform) vulnerabilities.

Updated 30 August 2022:

The ids field in the /v1/cves/suppress and /v1/cves/unsuppress API payload will be renamed to cves in the RHACS 3.73 release.

The cves.ids field of the storage.VulnerabilityRequest object in the response of VulnerabilityRequestService endpoints will be renamed to cves.cves in the RHACS 3.73 release.

1.4.2. Removed features

- Anchore, Tenable, and Docker Trusted Registry integrations: The RHACS scanner supersedes these integrations.

- External authorization plug-in for scoped access control: Use the existing in-product scoped access control.

- FROM option in the Disallowed Dockerfile line policy field: Any policies containing the Disallowed Dockerfile line policy field with the FROM option must be updated to remove those policy sections.

- PodSecurityPolicies (PSPs): PSPs can be disabled when generating deployment bundles and when configuring the Helm charts. The Helm charts also support auto-sensing availability of the PodSecurityPolicies API. You must disable PSPs when deploying to Kubernetes version 1.25 or later.

1.5. BUG FIXES
- The node affinity setting in Helm templates has been updated to discourage RHACS pods such as Central, Sensor, Scanner, and Scanner-db being scheduled on control plane nodes. (ROX-11533)

- Because the FROM option in the Disallowed Dockerfile line policy field has been deprecated, this update removed the option to create or edit policies that include this field. (ROX-10925)

1.6. UPGRADE INSTRUCTIONS FOR ROXCTL USERS

If you are upgrading to RHACS 3.71 using the roxctl CLI and YAML files, you need to perform some additional steps to upgrade Scanner. For upgrade steps, see Upgrading Scanner.

1.7. 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-rhel8:3.71</td>
</tr>
<tr>
<td>Scanner</td>
<td>Scans images and nodes.</td>
<td>registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:3.71</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-rhel8:3.71</td>
</tr>
</tbody>
</table>
CHAPTER 2. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.70

- 3.70.0 Release date: 2 June 2022
- 3.70.1 Release date: 22 June 2022

Red Hat Advanced Cluster Security for Kubernetes is an enterprise-ready, Kubernetes-native container security solution that protects your vital applications across build, deploy, and runtime. It deploys in your infrastructure and integrates with your DevOps tooling and workflows to deliver better security and compliance and to enable DevOps and InfoSec teams to operationalize security.

Red Hat Advanced Cluster Security for Kubernetes (RHACS) 3.70 includes feature enhancements, bug fixes, scale improvements, and other changes.

2.1. NEW FEATURES

2.1.1. Verifying image signatures against Cosign public keys

You can use RHACS to ensure the integrity of the container images in your clusters by verifying image signatures against preconfigured keys. You can also create policies to block unsigned images and images that do not have a verified signature and enforce the policy by using an admission controller to stop unauthorized deployment creation. Cosign key signature verification is supported. See Verifying image signatures for more information.

2.1.2. Identifying missing Kubernetes network policies

Kubernetes network policies are vital in helping to enable zero-trust networking within a cluster. They reduce the impact of network attacks by limiting the opportunity for lateral movement. By default, Kubernetes resources are not isolated. Applying network policies is a recommended best practice left to the user.

RHACS 3.70 ships with a new default policy that allows you to easily identify deployments that are not restricted by any ingress network policy and to trigger violation alerts accordingly.

- The default policy is named Deployments should have at least one ingress Network Policy. It is disabled by default.
- This default policy uses a new policy criterion called Alert on missing ingress Network Policy.
- To identify pod isolation gaps, you can clone this default policy or create a new one by using the policy criterion and enabling it on selected resources.

2.2. ENHANCEMENTS

2.2.1. Identifying Spring critical vulnerabilities

RHACS 3.70 adds a policy to detect the Spring Cloud Function RCE vulnerability (CVE-2022-22963) and the Spring Framework Spring4Shell RCE vulnerability (CVE-2022-22965). The policy has a severity level of Critical and is enabled by default.

2.2.2. Automatic Amazon ECR registry integration
Registry integrations for Amazon Elastic Container Registry (ECR) are now automatically generated for Amazon Web Services (AWS) clusters. This feature requires that the nodes' Instance Identity and Access Management (IAM) Role has been granted access to ECR. You can turn off this feature by disabling the EC2 instance metadata service in your nodes. See Amazon ECR integrations for more information.

### 2.2.3. Improved validation of pod security context

A new policy criterion has been added to validate the value of `allowPrivilegeEscalation` within the Kubernetes security context. You can use this policy criterion to provide alerts when a deployment is configured to allow a container process to gain more privileges than its parent process.

### 2.2.4. Increased number of allowed inclusion and exclusion scopes

Previously, RHACS limited the number of allowed inclusion and exclusion scopes within a scope to ten each. This restriction has been removed.

### 2.2.5. Finding ACS admin user credentials easily in the OpenShift Container Platform console

Customers using the recommended Operator method to deploy RHACS on OpenShift Container Platform can now view the credentials for the `admin` user in the OpenShift Container Platform console. When viewing the Central object, the Details tab provides a clickable link to the credentials under Admin Password Secret Reference. The displayed credentials are the default generated password or a previously configured and stored custom secret. See Verifying Central installation for more information.

### 2.3. NOTABLE TECHNICAL CHANGES

#### 2.3.1. Vulnerability scanning and reporting for RHCOS nodes

Vulnerability scanning and reporting for Red Hat Enterprise Linux CoreOS (RHCOS) nodes has been disabled until scanning improvements are made for improved accuracy and to support full host-level scanning beyond just Kubernetes components. Currently, RHCOS uses National Vulnerability Database (NVD) vulnerability data for reporting vulnerabilities for Kubernetes components from RHCOS. In the enhanced version, vulnerability reporting will be based on Red Hat published security data. (ROX-10662)

### 2.4. 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, refer to the table below. 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
Table 2.1. Deprecated and removed features tracker

<table>
<thead>
<tr>
<th>Feature</th>
<th>RHACS 3.68</th>
<th>RHACS 3.69</th>
<th>RHACS 3.70</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to delete default policies</td>
<td>DEP</td>
<td>DEP</td>
<td>REM</td>
</tr>
<tr>
<td>Ability to add comments to alerts and processes</td>
<td>GA</td>
<td>DEP</td>
<td>DEP</td>
</tr>
<tr>
<td>Anchore, Tenable, and Docker Trusted registry integrations</td>
<td>GA</td>
<td>DEP</td>
<td>DEP</td>
</tr>
<tr>
<td>External authorization plug-in for scoped access control</td>
<td>GA</td>
<td>DEP</td>
<td>DEP</td>
</tr>
<tr>
<td>FROM option in the Disallowed Dockerfile line policy field</td>
<td>GA</td>
<td>GA</td>
<td>DEP</td>
</tr>
<tr>
<td>PodSecurityPolicy (PSP) Kubernetes objects</td>
<td>GA</td>
<td>GA</td>
<td>DEP</td>
</tr>
<tr>
<td>RenamePolicyCategory and DeletePolicyCategory API endpoints</td>
<td>GA</td>
<td>GA</td>
<td>DEP</td>
</tr>
<tr>
<td>--rhacs option for the roxctl helm output command</td>
<td>GA</td>
<td>DEP</td>
<td>DEP</td>
</tr>
<tr>
<td>Security policies without a policyVersion</td>
<td>DEP</td>
<td>DEP</td>
<td>REM</td>
</tr>
<tr>
<td>/v1/policies API endpoint response: field response body parameter</td>
<td>DEP</td>
<td>DEP</td>
<td>REM</td>
</tr>
<tr>
<td>/v1/policies API endpoint response: whitelists response body parameter</td>
<td>DEP</td>
<td>DEP</td>
<td>REM</td>
</tr>
<tr>
<td>/v1/nodes and /v1/images API endpoint response: firstNodeOccurrence response body parameter</td>
<td>GA</td>
<td>DEP</td>
<td>DEP</td>
</tr>
</tbody>
</table>

2.4.1. Deprecated features

- **Anchore, Tenable, and Docker Trusted Registry** integrations: The RHACS scanner supersedes these integrations.

- **External authorization plug-in for scoped access control** Use the existing in-product scoped access control.

- **FROM option in the Disallowed Dockerfile line policy field** Any policies containing the Disallowed Dockerfile line policy field with the **FROM** option must be updated to remove those policy sections.
2.4.2. Removed features

- RHACS 3.70 no longer supports security policies that do not have `policyVersion` 1.1, including (but not limited to) importing policies.

- Red Hat Advanced Cluster Security for Kubernetes will not allow deleting default policies. Rather than deleting policies, you can disable default policies that you do not need.

- The `/v1/policies` API endpoint response will not return the `field` response body parameter.

2.5. BUG FIXES

2.5.1. Resolved in version 3.70.1

Release date: 22 June 2022

- **CVE-2022-1902**: Previously, improper sanitization allowed authenticated users to retrieve Notifier secrets from the GraphQL API. This flaw has been fixed. (ROX-11490)

2.5.2. Resolved in version 3.70.0

Release date: 2 June 2022

- When configuring a JFrog Artifactory integration, the username and password fields are now optional to allow anonymous pulls. (ROX-10090)

- Validation to the web user interface for endpoint URLs in the generic webhook integration caused errors. This issue was fixed. (ROX-9902)

- The policy **OpenShift: Kubeadmin Secret Accessed** is no longer triggered if the request was from the default OpenShift `oauth-apiserver-sa` service account, because this is an expected access pattern for the OpenShift API server. (ROX-10018)

- The ability to enable or disable notifications for multiple policies selected in the **Policies** list has been reinstated. To change the notification status, select one or more policies and choose **Enable notification** or **Disable notification** from the **Bulk Actions** menu. (ROX-9985)

- Fixed a permission issue for vulnerability reports where users with read/write permission could still not create or edit reports. (ROX-9880)

- Fixed issue that caused connection problems to the OpenShift Container Platform console after connecting to RHACS or the inability to connect to RHACS if a connection to the OpenShift Container Platform console existed. Central will now respond with a 421 Misdirected Request status code to requests where the `ServerName` sent via TLS SNI does not match the `:authority` (Host) header. This feature can be turned off by setting the environment variable `ROX_ALLOW_MISDIRECTED_REQUESTS=true`. (ROX-9625)

- When editing a policy, the **Violations Preview** window was unavailable for disabled policies. This issue has been fixed. (ROX-9435)

- Added the ability to disable role-based access control (RBAC) related risk computation. Users can exclude RBAC from risk calculation by setting the environment variable `ROXINCLUDE_RBAC_IN_RISK=false` in the Central deployment spec. (ROX-10627)

2.6. 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 <code>roxctl</code> for use in continuous integration (CI) systems.</td>
<td><code>registry.redhat.io/advanced-cluster-security/rhacs-main-rhel8:3.70.1</code></td>
</tr>
<tr>
<td>Scanner</td>
<td>Scans images and nodes.</td>
<td><code>registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:3.70.1</code></td>
</tr>
<tr>
<td>Scanner DB</td>
<td>Stores image scan results and vulnerability definitions.</td>
<td><code>registry.redhat.io/advanced-cluster-security/rhacs-scanner-db-rhel8:3.70.1</code></td>
</tr>
<tr>
<td>Collector</td>
<td>Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.</td>
<td><code>registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:3.70</code>&lt;br&gt;<code>registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:3.70.1</code></td>
</tr>
</tbody>
</table>
CHAPTER 3. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.69

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

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

3.1. NEW FEATURES

3.1.1. Released in version 3.69.1

Release date: April 6, 2022

3.1.1.1. Scanning of the integrated OpenShift Container Registry

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

3.1.1.2. Improved detection of Spring vulnerabilities

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

3.1.2. Released in version 3.69.0

Release date: March 21, 2022

3.1.2.1. New policies to manage operational deployment readiness

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

3.1.2.2. Inactive software component identification

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

3.1.2.3. Vulnerability scanning enhancements

Scanner includes the following new capabilities:

- Support for Alpine 3.15
• Scanner now identifies busybox as a base operating system.

• Ubuntu vulnerability reference links now point to the updated address https://ubuntu.com/security/.

### 3.2. IMPORTANT BUG FIXES

### 3.2.1. Resolved in version 3.69.2

Release date: June 22, 2022

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

### 3.2.2. Resolved in version 3.69.0

Release date: March 21, 2022

• **ROX-9587**: Previously, emailed vulnerability reports were incompatible with some e-mail clients. This issue has been fixed.

• **ROX-9166**: Previously, snoozed CVEs that were unsnoozed were not reported in CI when scanning images. This issue has been fixed.

• **ROX-9400**: Previously, RHACS did not remove the related service accounts when you deleted a cluster. This issue has been fixed.

• **ROX-9483**: Previously, certain search conditions using a process name could sometimes cause Central to stop responding. This issue has been fixed.

### 3.3. IMPORTANT SYSTEM CHANGES

• Red Hat has changed the default `grpcPort` in Scanner’s configuration map to **8443**.

• Red Hat is deprecating the following API endpoints:
  
  
  - `/v1/helm/cluster/add`: Use the Helm charts directly.
  
  - Empty values for `role.access_scope_id` is deprecated in the `RoleService_CreateRole` and `RoleService_UpdateRole` methods for the `/v1/roles/` endpoint. It is now set to the unrestricted access scope ID `io.stackrox.authz.accessscope.unrestricted`.

### 3.3.1. Redesigned policy creation workflow

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

### 3.3.2. Enhancements to sorting and filtering image vulnerabilities

Red Hat Advanced Cluster Security for Kubernetes 3.69 includes new fields for vulnerabilities contained within an image that you use to sort and filter the vulnerabilities list.
3.3.3. Enhanced compatibility with UEFI secure boot

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

3.3.4. Scanner memory limit increases

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

3.4. KNOWN ISSUES

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

3.5. DEPRECATION NOTICE

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

- Red Hat Advanced Cluster Security for Kubernetes 3.71.0:
  - External authorization plug-in for scoped access control Use the existing in-product scoped access control.
  - Anchore, Tenable, and Docker Trusted Registry integrations. The RHACS scanner supersedes these integrations.
  - Alerts and Process Comments

- Red Hat Advanced Cluster Security for Kubernetes 3.70.0:
  - Red Hat Advanced Cluster Security for Kubernetes will not allow deleting default policies. So rather than deleting, you can disable default policies that you do not need.
  - The /v1/policies API endpoint response will not return the field response body parameter.

- In RHACS 3.70, Red Hat will remove the support for security policies that do not have a policyVersion. Therefore, if you have externally stored older policies (without policyVersion or version prior to 1.1), you must convert them to use policyVersion 1.1. To do this, import the old policies into RHACS and then export them again. You can check the policyVersion field for your stored policies to identify if they need conversion.

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

3.6. IMAGE VERSIONS

<table>
<thead>
<tr>
<th>Image</th>
<th>Description</th>
<th>Current version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>20</td>
</tr>
<tr>
<td>Image</td>
<td>Description</td>
<td>Current version</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Main</td>
<td>Includes Central, Sensor, Admission Controller, and Compliance. Also includes <strong>roxctl</strong> for use in continuous integration (CI) systems.</td>
<td>registry.redhat.io/advanced-cluster-security/rhacs-main-rhel8:3.69.2</td>
</tr>
<tr>
<td>Scanner</td>
<td>Scans images and nodes.</td>
<td>registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:3.69.2</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-rhel8:3.69.2</td>
</tr>
<tr>
<td>Collector</td>
<td>Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.</td>
<td>registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:3.69.2 registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:3.69.2</td>
</tr>
</tbody>
</table>
CHAPTER 4. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.68

Red Hat Advanced Cluster Security for Kubernetes (RHACS) 3.68 includes feature enhancements, bug fixes, scale improvements, and other changes.

- 3.68.0 Release date: February 2, 2022
- 3.68.1 Release date: February 14, 2022
- 3.68.2 Release date: June 20, 2022

4.1. NEW FEATURES

4.1.1. Vulnerability triage workflows

Red Hat Advanced Cluster Security for Kubernetes 3.68 includes the ability to triage vulnerabilities in a variety of ways to support your vulnerability management process. See Managing vulnerabilities for more information.

4.1.2. Report scheduling for vulnerabilities

Red Hat Advanced Cluster Security for Kubernetes 3.68 includes the ability to schedule reports for vulnerabilities which helps you to send scheduled communications to key stakeholders to assist in the vulnerability management process. See Reporting vulnerabilities to teams for more information.

4.1.3. Use AWS AssumeRoles

AWS AssumeRoles allows you to define roles with specific permissions and then granting users access to those roles. With Red Hat Advanced Cluster Security for Kubernetes 3.68 you can use AssumeRoles when you integrate with Amazon ECR. For more details, see Using AssumeRole with Amazon ECR.

4.1.4. Enhancements for CI outputs

Red Hat has improved the usability of Red Hat Advanced Cluster Security for Kubernetes CI integrations. CI outputs now show additional detailed information about the vulnerabilities and the security policies responsible for broken builds. For more details, see Configuring output format.

4.1.5. Automount Service Account Token policy criteria

Kubernetes automatically provisions a service account during pod creation and mounts the account’s secret token within the pod at runtime. Many containerized applications do not require direct access to the service account. If a threat actor compromises an application, they might obtain the account token to further compromise the server. Therefore, when an application does not need to access the service account directly, administrators must ensure that the pod specifications disable the default behaviour. You can now use the Automount Service Account Token policy criteria to find the pods that have the service account mounted.

4.2. IMPORTANT BUG FIXES

4.2.1. Resolved in version 3.68.2
Release date: June 20, 2022

- **ROX-10845**: CVE-2022-1902: GraphQL exposes Notifiers secrets.

### 4.2.2. Resolved in version 3.68.1

Release date: February 14, 2022

- **ROX-9243**: In RHACS 3.68.0, Central would sometimes stop responding if the vulnerability data was not available. This issue has been fixed. Central now reports an error for such cases.

### 4.2.3. Resolved in version 3.68.0

- **ROX-8709**: Previously, searching for CVEs with a specific severity did not return any results. This issue has been fixed.
- **ROX-8983**: Previously, when configuring the Manage Watches feature, if you added more than 12 images to the watch list, the image list did not display properly. This issue has been fixed.
- **ROX-8276**: Previously, when the RHACS Operator accessed the central-htpasswd secret, it created a false positive policy violation for the OpenShift: Advanced Cluster Security Central Admin Secret Accessed default policy. This issue has been fixed.

### 4.3. SECURITY UPDATE

In earlier versions of Red Hat Advanced Cluster Security for Kubernetes, the write permission for the APIToken resource allowed users to create API tokens for any role, including the admin role. This issue has been fixed.

### 4.4. IMPORTANT SYSTEM CHANGES

#### 4.4.1. Changes in version 3.68.1

Release date: February 14, 2022

RHACS 3.68.1 includes stability improvements for the automatic registry integrations to handle failure and reduce the load on registries more effectively. RHACS 3.68.1 also includes a new ROX_DISABLE_AUTOGENERATED_REGISTRIES environment variable. You can set its value to true to ignore all new registry integrations from Sensors.

#### 4.4.2. Changes in version 3.68.0

Release date: February 2, 2022

- RHACS 3.68 includes updates for the Log4Shell vulnerability detection policy. With this update this policy also detects CVE-2021-45046, and it includes the updated remediation based on the latest guidance by the Apache Logging security team.

- Before this release, snoozing CVEs required write permission for the Images resource. Beginning with RHACS 3.68:
  - To snooze CVEs, you must have write permission for the VulnerabilityManagementRequests resource.
To approve requests, you must have write permission for the `VulnerabilityManagementApprovals` resource.

When you upgrade to RHACS 3.68, roles that include write access on the `Images` resource will have write permissions for both `VulnerabilityManagementRequests` and `VulnerabilityManagementApprovals` resource. Red Hat recommends updating the roles to only include the least amount of resources required for each role.

If you installed Red Hat Advanced Cluster Security for Kubernetes using Helm, this update disabled the cluster configuration options in the RHACS portal. You can continue to use Helm configuration files.

RHACS 3.68 sends notifications for every runtime policy violation rather than sending notifications only the first encountered violation. This is the default behavior. To change it, you must set the `NOTIFY_EVERY_RUNTIME_EVENT` to `false`.

**IMPORTANT**

Red Hat will remove this environment variable in future releases. Contact the support team for any related inquiries.

Red Hat has moved the following images to new repositories:

<table>
<thead>
<tr>
<th>Image</th>
<th>Old repository</th>
<th>New repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>main</td>
<td>registry.redhat.io/rh-acs/main</td>
<td>registry.redhat.io/advanced-cluster-security/rhacs-main-rhel8</td>
</tr>
<tr>
<td>collector</td>
<td>registry.redhat.io/rh-acs/collector, with the -latest tag.</td>
<td>registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8</td>
</tr>
<tr>
<td>collector-slim</td>
<td>registry.redhat.io/rh-acs/collector-slim, with the -slim tag.</td>
<td>registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8</td>
</tr>
<tr>
<td>scanner</td>
<td>registry.redhat.io/rh-acs/scanner</td>
<td>registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8</td>
</tr>
<tr>
<td>scanner-db</td>
<td>registry.redhat.io/rh-acs/scanner-db</td>
<td>registry.redhat.io/advanced-cluster-security/rhacs-scanner-db-rhel8</td>
</tr>
</tbody>
</table>

Tags of the `scanner`, `scanner-db`, and `collector` images, including the `collector-slim` variant, are now identical to the `main` image tag. In addition, all these tags now match the version of Red Hat Advanced Cluster Security for Kubernetes. For example, a scanner image for RHACS 3.68.0 is now identified as `registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:3.68.0` and `stackrox.io/scanner:3.68.0`. Make sure you follow the same versioning scheme when you upgrade manually.

Red Hat has changed the image names for `collector-slim`. `-slim` is no longer part of the image name.
tag. Collector Slim image for the release 3.68.0 is identified as `registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:3.68.0` and `collector.stackrox.io/collector-slim:3.68.0`.

- Scanner DB image at `registry.redhat.io/advanced-cluster-security/rhacs-scanner-db-rhel8` is now based on `rhel8/postgresql-12`.

- The `roxctl` CLI includes a new `--image-defaults` option for the `roxctl helm output` and `roxctl central generate` commands. It allows selecting the default registry from which container images are taken for deploying central and scanner.

- Red Hat has deprecated the `--rhacs` option for the `roxctl helm output` command. Use `--rhacs-image-defaults` option instead.

- By default, the `roxctl helm output` command now uses the images from `registry.redhat.io` rather than `stackrox.io`.

### 4.5. IMAGE VERSIONS

**IMPORTANT**

Beginning with RHACS 3.68, Red Hat has updated the image versioning convention for the **Scanner**, **Scanner DB**, and **Collector** images. As a result, the version numbers for these images now match the version numbers for the **Main** image. In addition, due to the change in image repository names in `registry.redhat.io`, if you mirror RHACS image repositories, you must verify your mirroring is set up to mirror images from the new locations.

<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 <code>roxctl</code> for use in continuous integration (CI) systems.</td>
<td><code>registry.redhat.io/advanced-cluster-security/rhacs-main-rhel8:3.68.2</code></td>
</tr>
<tr>
<td>Scanner</td>
<td>Scans images and nodes.</td>
<td><code>registry.redhat.io/advanced-cluster-security/rhacs-scanner-rhel8:3.68.2</code></td>
</tr>
<tr>
<td>Scanner DB</td>
<td>Stores image scan results and vulnerability definitions.</td>
<td><code>registry.redhat.io/advanced-cluster-security/rhacs-scanner-db-rhel8:3.68.2</code></td>
</tr>
<tr>
<td>Collector</td>
<td>Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.</td>
<td><code>registry.redhat.io/advanced-cluster-security/rhacs-collector-rhel8:3.68.2</code> <code>registry.redhat.io/advanced-cluster-security/rhacs-collector-slim-rhel8:3.68.2</code></td>
</tr>
</tbody>
</table>
CHAPTER 5. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.67

Red Hat Advanced Cluster Security for Kubernetes (RHACS) 3.67 includes feature enhancements, bug fixes, scale improvements, and other changes.

5.1. NEW FEATURES

5.1.1. Released in version 3.67.2

Release date: December 16, 2021

5.1.1.1. Log4Shell policy

Red Hat Advanced Cluster Security for Kubernetes 3.67.2 includes a new policy named Log4Shell: CVE-2021-44228 - log4j Remote Code Execution vulnerability. This policy creates alerts for deployments that have images containing the Log4Shell vulnerability (CVE-2021-44228).

5.1.2. Released in version 3.67.0

Release date: December 1, 2021

5.1.2.1. OpenShift Dedicated support

Red Hat Advanced Cluster Security for Kubernetes 3.67 is thoroughly tested and supported on OpenShift Dedicated on Amazon Web Services and Google Cloud Platform.

5.1.2.2. Use OpenShift Container Platform OAuth server as an identity provider

If you are using Red Hat Advanced Cluster Security for Kubernetes with OpenShift Container Platform, you can now configure the built-in OpenShift Container Platform OAuth server as an identity provider for Red Hat Advanced Cluster Security for Kubernetes. For more details, see Configuring OpenShift Container Platform Oauth server as an identity provider in Red Hat Advanced Cluster Security for Kubernetes.

5.1.2.3. Enhancements for CI outputs

Red Hat has improved the usability of Red Hat Advanced Cluster Security for Kubernetes CI integrations. CI outputs now show additional detailed information about the vulnerabilities and the security policies responsible for broken builds.

5.1.2.4. Runtime Class policy criteria

Users can now use RHACS to define the container runtime configuration. This configuration can be used to run a pod’s containers using the Runtime Class policy criteria.

5.2. IMPORTANT BUG FIXES

- ROX-7815: Previously, when using RHACS with the Compliance Operator integration, RHACS did not respect or populate Compliance Operator TailoredProfiles. This issue has been fixed.
• **ROX-7254**: Previously, the Alpine Linux package manager (APK) in Image policy looked for the presence of `apk` package in the image rather than the `apk-tools` package. This issue has been fixed.

5.2.1. Resolved in version 3.67.1

Release date: December 6, 2021

• **ROX-8698**: In RHACS 3.67.0, the TLS verification would fail when you integrated RHACS with OpenShift Container Platform OAuth server for OpenShift Container Platform 4.8 and later. This issue has been fixed.

5.2.2. Resolved in version 3.67.2

Release date: December 16, 2021

• **ROX-8773**: Before this update, when integrating with Microsoft Teams, the RHACS user interface field validation did not pass certain Microsoft Teams webhook addresses. This issue has been fixed.

• **ROX-8736**: In RHACS 3.67.0, the `roxctl image check` command would retry on policy failures that broke builds. This issue has been fixed.

• **ROX-8702**: In RHACS 3.67.0, when using OpenShift OAuth, the user name is incorrectly listed as the User email, if an email address is unavailable. This issue has been fixed.

5.3. IMPORTANT SYSTEM CHANGES

• Scanner now identifies vulnerabilities in Ubuntu 21.10 images.

• The Port exposure method policy criteria now include `route` as an exposure method.

• The OpenShift: Kubeadmin Secret Accessed security policy now allows the OpenShift Compliance Operator to check for the existence of the Kubeadmin secret without creating a violation.

• The OpenShift Compliance Operator integration now supports using TailoredProfiles.

• The Red Hat Advanced Cluster Security for Kubernetes Jenkins plugin now provides additional security information.

• When you enable the environment variable `ROX_NETWORK_ACCESS_LOG` for Central, the logs contain the Request URI and X-Forwarded-For header values.

**NOTE**

Red Hat recommends that you only use the `ROX_NETWORK_ACCESS_LOG` environment variable for debugging network connectivity issues.

• The default `uid:gid` pair for the Scanner image is now `65534:65534`. Red Hat Advanced Cluster Security for Kubernetes adds a new default Scope Manager role that includes minimum permissions to create and modify access scopes. For more information, see the System roles topic.
- If `microdnf` is part of an image or shows up in process execution, Red Hat Advanced Cluster Security for Kubernetes reports it as a security violation for the Red Hat Package Manager in Image or the Red Hat Package Manager Execution security policies.

- In addition to manually uploading vulnerability definitions in offline mode, you can now upload definitions in online mode. Red Hat Advanced Cluster Security for Kubernetes always uses the most recent vulnerability definitions.

NOTE

Red Hat Advanced Cluster Security for Kubernetes ignores Kubernetes and Istio vulnerability definitions when you manually upload the vulnerability definitions in online mode.

- You can now format the output of the following `roxctl` CLI commands in table, csv, or JSON format:
  - `image scan`
  - `image check`
  - `deployment check`

- You can now use a regular expression for the deployment name while specifying policy exclusions.

5.4. 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 <code>roxctl</code> for use in continuous integration (CI) systems.</td>
<td>registry.redhat.io/rh-acs/main:3.67.2</td>
</tr>
<tr>
<td>Scanner</td>
<td>Scans images and nodes.</td>
<td>registry.redhat.io/rh-acs/scanner:2.21.3</td>
</tr>
<tr>
<td>Scanner DB</td>
<td>Stores image scan results and vulnerability definitions.</td>
<td>registry.redhat.io/rh-acs/scanner-db:2.21.3</td>
</tr>
<tr>
<td>Collector</td>
<td>Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.</td>
<td>registry.redhat.io/rh-acs/collector:3.5.0-latest</td>
</tr>
</tbody>
</table>
CHAPTER 6. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.66

Red Hat Advanced Cluster Security for Kubernetes (RHACS) 3.66 includes feature enhancements, bug fixes, scale improvements, and other changes.

Release date: October 19, 2021

6.1. NEW FEATURES

6.1.1. Scan deployment configurations in your CI pipeline

You can now identify misconfigurations in your OpenShift Container Platform deployment configuration files by running the `roxctl deployment check` command in your CI pipeline.

6.1.2. Active component identification

Red Hat Advanced Cluster Security for Kubernetes now identifies if a component is in use by a process at runtime and then asserts that component as an active component.

6.1.3. New configuration settings for Operator and Helm charts


- You can now disable the automatic administrator password generation for Central by specifying the `adminPasswordGenerationDisabled` as `true` in the RHACS Operator configuration.

6.2. IMPORTANT BUG FIXES

- **ROX-7912**: Previously, Red Hat Advanced Cluster Security for Kubernetes reported the CVE-2019-9893 as both fixable and not fixable. This has been fixed.

- **ROX-7414** and **ROX-5180**: Previously, sometimes Central and Sensor consumed all available memory, and their pods stopped with `OOMKilled` status. The high memory consumption was because of resource-intensive evaluation of roles, bindings, and service accounts. This issue has been fixed.

- **ROX-7978**: Previously, Central crashed sometimes if you sent build-time notifications by using the Syslog protocol. This has been fixed.

- **ROX-8055**: Previously, the downloading of runtime probes failed in IPV6 only environments. This has been fixed.

- **ROX-8093**: Previously, the Red Hat Advanced Cluster Security for Kubernetes portal would sometimes show an error message under the MITRE ATT&CK section. This has been fixed.

6.2.1. Resolved in version 3.66.1

Release date: October 20, 2021
• **ROX-8281**: Because of an issue in the cluster init bundle generation script, the downloaded cluster init bundles were base64 encoded rather than plain text. This issue has been fixed.

### 6.3. IMPORTANT SYSTEM CHANGES

- In Red Hat Advanced Cluster Security for Kubernetes 3.66, Red Hat has deprecated the following default security policies:
  - DockerHub NGINX 1.10
  - Shellshock: Multiple CVEs
  - Heartbleed: CVE-2014-0160
- Red Hat has deprecated the Alpine-based images of Red Hat Advanced Cluster Security for Kubernetes. All images are now based on Red Hat Universal Base Image (UBI).
- The admission controller settings for the RHACS Operator now listen to both *update* and *create* events by default.
- You can no longer delete the default security policies on fresh installations of Red Hat Advanced Cluster Security for Kubernetes 3.65 or newer. However, if you upgrade from an older version to 3.65 or newer, you can still delete the default security policies.
- In Red Hat Advanced Cluster Security for Kubernetes 3.66:
  - the **Analyst** permission set and role does not contain the **DebugLogs** permission.
  - the **Mount Docker Socket** policy is renamed to **Mount Container Runtime Socket**. This policy also detects if a deployment mounts the CRI-O socket for both Kubernetes and OpenShift Container Platform.
  - the **Docker CIS 4.4: Ensure images are scanned and rebuilt to include security patches** policy is disabled by default.
- The **roxctl** CLI now supports command-line completion for **bash**, **zsh**, **fish** and PowerShell.

### 6.4. 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 <strong>roxctl</strong> for use in continuous integration (CI) systems.</td>
<td>registry.redhat.io/rh-acs/main:3.66.1</td>
</tr>
<tr>
<td>Scanner</td>
<td>Scans images and nodes.</td>
<td>registry.redhat.io/rh-acs/scanner:2.20.0</td>
</tr>
<tr>
<td>Scanner DB</td>
<td>Stores image scan results and vulnerability definitions.</td>
<td>registry.redhat.io/rh-acs/scanner-db:2.20.0</td>
</tr>
<tr>
<td>Image</td>
<td>Description</td>
<td>Current version</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Collector</td>
<td>Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.</td>
<td>registry.redhat.io/rh-ac/s/collector:3.4.1-latest</td>
</tr>
</tbody>
</table>
CHAPTER 7. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.65

Red Hat Advanced Cluster Security for Kubernetes (RHACS) 3.65 includes feature enhancements, bug fixes, scale improvements, and other changes.

Release date: September 6, 2021

7.1. NEW FEATURES

7.1.1. MITRE ATT&CK Containers Matrix

You can now use the MITRE ATT&CK Containers Matrix to categorize policies in the Red Hat Advanced Cluster Security for Kubernetes. When you create custom security policies, you can now add MITRE ATT&CK Matrix adversary tactics and techniques related information.

7.1.2. Install on more platforms

You can now install Red Hat Advanced Cluster Security for Kubernetes on:

- Red Hat OpenShift Service on AWS (ROSA)
- Azure Red Hat OpenShift

7.1.3. Admission control configuration

You can now configure the dynamic admission control settings in the Red Hat Advanced Cluster Security for Kubernetes Operator. It now includes the following new admission control settings:

- admissionControl.bypass: Use this parameter to bypass the admission controller.
- admissionControl.contactImageScanners: Specify true to enable inline scanning of images that are not already scanned during a deployment’s admission review.
- admissionControl.timeoutSeconds: Use this parameter to specify the maximum number of seconds Red Hat Advanced Cluster Security for Kubernetes should wait for an admission review before marking it as fail open.

See admission controller settings to view all available configuration options.

7.2. IMPORTANT BUG FIXES

- ROX-6988: Previously, Red Hat Advanced Cluster Security for Kubernetes did not delete the CVEs and did not update the advisory when some Red Hat packages that transitioned from unfixable to a fixable state.

- ROX-7170: Previously, Red Hat Advanced Cluster Security for Kubernetes only collected the error logs in the diagnostic bundle if you have installed Red Hat Advanced Cluster Security for Kubernetes services in the stackrox namespace.

- ROX-7861: Previously, Red Hat Advanced Cluster Security for Kubernetes compliance control NIST 800-190 Control 4.1.4 did not correctly detect policies used for secrets protection.
7.2.1. Resolved in version 3.65.1

Release date: September 22, 2021

- **ROX-8008**: Previously, you could not use URN-based IdP Issuers while configuring SAML identity providers. This has been fixed.

- **ROX-8033**: Due to how Red Hat Advanced Cluster Security for Kubernetes previously addressed its internal service endpoints, OpenShift clusters with enabled proxy failed to download the correct kernel probes.

- **ROX-8034**: Previously, if you were using backported 5.11 kernels for Ubuntu 20.04, the Collector sometimes failed on upgrade due to a change in the Ubuntu kernel build.

7.3. IMPORTANT SYSTEM CHANGES

- Red Hat Advanced Cluster Security for Kubernetes 3.65 includes the updated `host-pid` policy, which adds an exception for the `openshift-sdn` namespace because the `sdn` deployment in the `openshift-sdn` namespace shares the host process namespace, and it resulted in an inaccurate violation.

- The alert notification titles for PagerDuty, Slack, Microsoft Teams, JIRA, and email notifiers now include the cluster and the policy names in addition to the deployment or image name if it exists.

- The alert notification for PagerDuty now includes the full alert in the JSON format as a custom detail.

- All default policy criteria for security policies are now read-only. However, you can still edit the policy criteria fields for the custom policies or policies you create by cloning a system policy.

7.4. UPCOMING CHANGES

- In Red Hat Advanced Cluster Security for Kubernetes 3.66, Red Hat will deprecate the following default security policies:
  - DockerHub NGINX 1.10
  - Shellshock: Multiple CVEs
  - Heartbleed: CVE-2014-0160

- In Red Hat Advanced Cluster Security for Kubernetes 3.66, Red Hat will disable the following default security policy:
  - **DOCKER CIS 4.4: Ensure images are scanned and rebuilt to include security patches**

You can create custom policies to monitor for these violations.

7.5. IMAGE VERSIONS

<table>
<thead>
<tr>
<th>Image</th>
<th>Description</th>
<th>Current version</th>
</tr>
</thead>
</table>

33
<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 <code>roxctl</code> for use in continuous integration (CI) systems.</td>
<td>registry.redhat.io/rh-accs/main:3.65.1</td>
</tr>
<tr>
<td>Scanner</td>
<td>Scans images and nodes.</td>
<td>registry.redhat.io/rh-accs/scanner:2.19.1</td>
</tr>
<tr>
<td>Scanner DB</td>
<td>Stores image scan results and vulnerability definitions.</td>
<td>registry.redhat.io/rh-accs/scanner-db:2.19.1</td>
</tr>
<tr>
<td>Collector</td>
<td>Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.</td>
<td>registry.redhat.io/rh-accs/collector:3.3.1-latest</td>
</tr>
</tbody>
</table>
Red Hat Advanced Cluster Security for Kubernetes (RHACS) 3.64 includes feature enhancements, bug fixes, scale improvements, and other changes.

Release date: August 11, 2021

8.1. NEW FEATURES

- **ROX-7230**: You can now use deployment and namespace annotations to define where Red Hat Advanced Cluster Security for Kubernetes sends violation notifications when configuring your notifiers. Notifications can be sent to Slack, Microsoft Teams, Email, and others.

- **ROX-7534**: With the Red Hat Advanced Cluster Security for Kubernetes Operator, you can now configure the enforcement behavior of the admission controller as part of the custom resource setting.


8.2. IMPORTANT BUG FIXES

- **ROX-6326**: Previously, users with a large number of namespaces would receive sporadic 504 gateway errors when sending requests to the `/v1/namespaces/` endpoint. Red Hat Advanced Cluster Security for Kubernetes includes the updated endpoint, which supports pagination to fix this issue.

8.2.1. Resolved in version 3.64.1

Release date: August 26, 2021

- **ROX-7850**: Due to a bug in the previous RHACS Operator image, configuring the proxy support in the Operator Lifecycle Manager would incorrectly send internal traffic through the proxy. The bug caused internal communication failure, and the RHACS services would fail to start. The updated image uses the fully qualified domain names for RHACS services to fix this issue.

- **ROX-7872**: The updated Operator image sets the memory limit to 1 GiB and memory requests to 200 MiB to address out-of-memory issues when using the RHACS Operator at scale.

8.2.2. Resolved in version 3.64.2

Release date: September 22, 2021

- **ROX-8008**: Previously, you could not use URN-based IdP Issuers while configuring SAML identity providers. This has been fixed.

- **ROX-8033**: Due to how Red Hat Advanced Cluster Security for Kubernetes previously addressed its internal service endpoints, OpenShift clusters with enabled proxy failed to download the correct kernel probes.

- **ROX-8034**: Previously, if you were using backported 5.11 kernels for Ubuntu 20.04, the Collector sometimes failed on upgrade due to a change in the Ubuntu kernel build.
8.3. IMPORTANT SYSTEM CHANGES

- **ROX-6258**: Red Hat Advanced Cluster Security for Kubernetes now prefixes the optional security context constraint name with `stackrox` to avoid global naming conflicts.

- **ROX-7318**: Previously, violations for `port forwards` and `exec` events did not contain information about the user who performed the action that generated the events. The violations now include the user context.

- **ROX-7449**: Cluster init bundles contain the secrets required for internal Red Hat Advanced Cluster Security for Kubernetes services to communicate with each other. You can rotate secrets by deleting these, but doing so can cause outages. Red Hat Advanced Cluster Security for Kubernetes now includes an updated deletion workflow that gives a warning about the possible impact of deletion on the environment.

- **ROX-7684**: The OpenShift Compliance Operator uses RPM only for querying, and it does not install any packages. Red Hat Advanced Cluster Security for Kubernetes includes a policy exception for this pod by default to reduce the violations count.

8.4. 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 <code>roxctl</code> for use in continuous integration (CI) systems.</td>
<td>registry.redhat.io/rh-accs/main:3.64.2</td>
</tr>
<tr>
<td>Scanner</td>
<td>Scans images and nodes.</td>
<td>registry.redhat.io/rh-accs/scanner:2.18.4</td>
</tr>
<tr>
<td>Scanner DB</td>
<td>Stores image scan results and vulnerability definitions.</td>
<td>registry.redhat.io/rh-accs/scanner-db:2.18.4</td>
</tr>
<tr>
<td>Collector</td>
<td>Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.</td>
<td>registry.redhat.io/rh-accs/collector:3.3.1-latest</td>
</tr>
</tbody>
</table>
CHAPTER 9. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.63

Red Hat Advanced Cluster Security for Kubernetes 3.63 includes feature enhancements, bug fixes, scale improvements, and other changes.

Release date: July 26, 2021

9.1. RELEASE TAG VERSION CHANGE

This release and the subsequent releases of Red Hat Advanced Cluster Security for Kubernetes will use the updated version number convention as major-release.minor-release.patch-release.

9.2. NEW FEATURES

Installing by using an Operator

Scoped access control
The way that Red Hat Advanced Cluster Security for Kubernetes handles access control has been updated. You can now define scopes for Kubernetes resources, such as namespaces and clusters, and assign those scopes to roles. See Managing RBAC in Red Hat Advanced Cluster Security for Kubernetes 3.63 and newer for more information.

Improved alert functionality for OpenShift Container Platform
You can now set alerts for detections against the OpenShift Container Platform API server for secrets and config maps.

9.3. IMPORTANT SYSTEM CHANGES

- Red Hat Advanced Cluster Security for Kubernetes includes new default policies to monitor access to the kubeadmin secret, the Central Admin secret, and impersonated access to secrets.

- Red Hat Advanced Cluster Security for Kubernetes 3.63 replaced a default policy, which provides alerts on images that have vulnerabilities with a CVSS score of 7 or higher, with a new default policy that searches for critical severity issues. This new policy is enabled by default. This change only impacts new installations of Red Hat Advanced Cluster Security for Kubernetes.

9.4. 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 CI (continuous integration) systems.</td>
<td>registry.redhat.io/rh-acs/main:3.63.0</td>
</tr>
<tr>
<td>Image</td>
<td>Description</td>
<td>Current version</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>Scanner</td>
<td>Scans images and nodes.</td>
<td>registry.redhat.io/rh-acsc/scanner:2.17.4</td>
</tr>
<tr>
<td>Scanner DB</td>
<td>Stores image scan results and vulnerability definitions.</td>
<td>registry.redhat.io/rh-acsc/scanner-db:2.17.4</td>
</tr>
<tr>
<td>Collector</td>
<td>Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.</td>
<td>registry.redhat.io/rh-acsc/collector:3.1.30-latest</td>
</tr>
</tbody>
</table>
CHAPTER 10. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.0.62

Red Hat Advanced Cluster Security for Kubernetes 3.0.62 includes feature enhancements, bug fixes, scale improvements, and other changes.

Release date: June 30, 2021

10.1. NEW FEATURES

10.1.1. Compliance Operator integration

Red Hat Advanced Cluster Security for Kubernetes now supports OpenShift Container Platform configuration compliance standards through an integration with the OpenShift Container Platform Compliance Operator. In addition, it allows you to measure and report on configuration security best practices for OpenShift Container Platform.

10.1.2. Alpine image vulnerability feed updates


10.2. IMPORTANT BUG FIX

- ROX-7420: Previously, alert notifications would not trigger when the admission controller blocked a deployment from being created because of a policy violation.

10.3. IMPORTANT SYSTEM CHANGES

- Red Hat Advanced Cluster Security for Kubernetes crypto miner policy now supports the miner 'xmrig' by default. It addresses some currently active crypto-mining campaigns.
- Red Hat Advanced Cluster Security for Kubernetes no longer marks the Alpine image version 3.2-3.7 as stale because these versions are still receiving updates.
- Improved logging for errors if no registry integration exists in Red Hat Advanced Cluster Security for Kubernetes.
- Improved network graph lookup performance and collector performance.

10.4. RELEASE TAG VERSION CHANGE

The next release and the subsequent releases of Red Hat Advanced Cluster Security for Kubernetes will use the updated version number convention as major-release.minor-release.patch-release.

Therefore the version for the next release of Red Hat Advanced Cluster Security for Kubernetes will be 3.63.

10.5. IMAGE VERSIONS
<table>
<thead>
<tr>
<th>Image</th>
<th>Description</th>
<th>Current version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main</td>
<td>It includes Central, Sensor, Admission Controller, and Compliance. It also includes <strong>roxc</strong> for use in CI (continuous integration) systems.</td>
<td><code>registry.redhat.io/rh-acr/main:3.0.62.0</code></td>
</tr>
<tr>
<td>Scanner</td>
<td>Scans images and nodes.</td>
<td><code>registry.redhat.io/rh-acr/scanner:2.16.0</code></td>
</tr>
<tr>
<td>Scanner DB</td>
<td>Stores image scan results and vulnerability definitions.</td>
<td><code>registry.redhat.io/rh-acr/scanner-db:2.16.0</code></td>
</tr>
<tr>
<td>Collector</td>
<td>Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.</td>
<td><code>registry.redhat.io/rh-acr/collector:3.1.27-latest</code></td>
</tr>
</tbody>
</table>
CHAPTER 11. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.0.61

Red Hat Advanced Cluster Security for Kubernetes 3.0.61 includes feature enhancements, bug fixes, scale improvements, and other changes.

Release date: June 10, 2021

11.1. NEW FEATURES

- **ROX-6639**: Red Hat Advanced Cluster Security for Kubernetes includes a new policy criteria for vulnerabilities severity score in an image’s contents. It provides a more accurate reflection of risk than a CVSS score.

11.2. IMPORTANT BUG FIXES

- **ROX-6991 and ROX-7058**: Previously, CSV exports of security risks were inconsistent with the RHACS user interface.
- **ROX-7004**: Previously, CVE-2016-4074 was reported as a false positive when images contained the component `jq 1.6-r0` or `jq 1.6-r1`.
- **ROX-7270**: Previously, under certain conditions, searched images would not correctly index and display.
- **ROX-7276**: Previously, improper handling of very short-lived tokens caused the GitLab OIDC authentication provider to prematurely log users out.

11.2.1. Resolved in version 3.0.61.1

Release date: June 21, 2021

- **ROX-7387**: Previously, in deployments using non-standard namespaces, admission controller failed to enforce or monitor deploy time policies.

11.3. IMPORTANT SYSTEM CHANGES

- **ROX-6639**: Red Hat Advanced Cluster Security for Kubernetes includes a new default policy to flag fixable high or important severity vulnerabilities in images.
- **ROX-7133**: Red Hat Advanced Cluster Security for Kubernetes now calculates the image risk using a score assigned to the severity rating of a vulnerability rather than the CVSS score. Doing this provides a more accurate reflection of an image’s risk.

11.4. IMAGE VERSIONS

<table>
<thead>
<tr>
<th>Image</th>
<th>Description</th>
<th>Current version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Image</td>
<td>Description</td>
<td>Current version</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>Main</td>
<td>It includes Central, Sensor, Admission Controller, and Compliance. It also includes <code>roxctl</code> for use in CI (continuous integration) systems.</td>
<td>registry.redhat.io/rh-acs/main:3.0.61.1</td>
</tr>
<tr>
<td>Scanner</td>
<td>Scans images and nodes.</td>
<td>registry.redhat.io/rh-acs/scanner:2.15.2</td>
</tr>
<tr>
<td>Scanner DB</td>
<td>Stores image scan results and vulnerability definitions.</td>
<td>registry.redhat.io/rh-acs/scanner-db:2.15.2</td>
</tr>
<tr>
<td>Collector</td>
<td>Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.</td>
<td>registry.redhat.io/rh-acs/collector:3.1.25-latest</td>
</tr>
</tbody>
</table>
CHAPTER 12. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 3.0.60

Red Hat Advanced Cluster Security for Kubernetes 3.0.60 includes feature enhancements, bug fixes, scale improvements, and other changes.

Release date: May 19, 2021

12.1. NEW FEATURES

- **ROX-7189**: Red Hat Advanced Cluster Security for Kubernetes has achieved the Red Hat Certified Vulnerability Scanner designation. It now includes updated Red Hat severity classifications and improved base image scanning on RHEL images.


12.2. IMPORTANT BUG FIXES

- **ROX-6979**: Previously, the automatically generated image registry integration for registry.redhat.io resulted in integration errors.

- **ROX-7004**: Previously, environments with more than 50 clusters did not show the entire cluster list.

- **ROX-7155**: Previously, under certain conditions inactive images would continue to be reported after their deletion schedule.

12.2.1. Resolved in version 3.0.60.1

Release date: May 26, 2021

- **ROX-7253**: Previously, in version 3.0.60.0, scanner would fail to update vulnerability definitions and incorrectly report as healthy.

12.3. IMPORTANT SYSTEM CHANGES

- **ROX-7059**: Red Hat Advanced Cluster Security for Kubernetes includes an updated user interface to show resource summary counts after removing them in 3.0.58.0.

- **ROX-6632**: Scanner now reports vulnerabilities in alignment with the RHEL scanning certification in preparation for formal certification.

- **ROX-7069**: Network policy simulator no longer generates policies for hidden orchestrator components.

12.4. IMAGE VERSIONS

<table>
<thead>
<tr>
<th>Image</th>
<th>Description</th>
<th>Current version</th>
</tr>
</thead>
</table>


<table>
<thead>
<tr>
<th>Image</th>
<th>Description</th>
<th>Current version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main</td>
<td>It includes Central, Sensor, Admission Controller, and Compliance. It also includes <strong>roxctl</strong> for use in CI (continuous integration) systems.</td>
<td>registry.redhat.io/rh-acs/main:3.0.60.1</td>
</tr>
<tr>
<td>Scanner</td>
<td>Scans images and nodes.</td>
<td>registry.redhat.io/rh-acs/scanner:2.14.1</td>
</tr>
<tr>
<td>Scanner DB</td>
<td>Stores image scan results and vulnerability definitions.</td>
<td>registry.redhat.io/rh-acs/scanner-db:2.14.1</td>
</tr>
<tr>
<td>Collector</td>
<td>Collects runtime activity in Kubernetes or OpenShift Container Platform clusters.</td>
<td>registry.redhat.io/rh-acs/collector:3.1.22-latest</td>
</tr>
</tbody>
</table>