Red Hat Advanced Cluster Security for Kubernetes 3.70

Support

Getting support for Red Hat Advanced Cluster Security for Kubernetes

Last Updated: 2022-12-06

Red Hat Advanced Cluster Security for Kubernetes 3.70 Support

Getting support for Red Hat Advanced Cluster Security for Kubernetes

Legal Notice

Abstract

This document provides information on getting support from Red Hat for Red Hat Advanced Cluster Security for Kubernetes and includes instructions on how to generate a diagnostic bundle.

Table of Contents

CHAPTER 1. GETTING SUPPORT FOR RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES

This topic provides information about the technical support for Red Hat Advanced Cluster Security for Kubernetes.

IMPORTANT

- The support-related information listed on this page is only applicable if you are a Red Hat customer.
- If you are not a Red Hat customer, and you purchased the StackRox Kubernetes Security Platform before the acquisition. Red Hat will honor the StackRox support policy for its duration. For details, see Getting support for StackRox Kubernetes Security Platform.

If you experience difficulty with a procedure described in this documentation, or with Red Hat Advanced Cluster Security for Kubernetes in general, visit the Red Hat Customer Portal . From the Customer Portal, you can:

- Search or browse through the Red Hat Knowledgebase of articles and solutions relating to Red Hat products.
- Submit a support case to Red Hat Support.
- Access other product documentation.

If you have a suggestion for improving this documentation or have found an error, please submit a Bugzilla report against the **Red Hat Advanced Cluster Security for Kubernetes**product for the **Documentation** component. Please provide specific details, such as the section name and Red Hat Advanced Cluster Security for Kubernetes version.

1.1. ABOUT THE RED HAT KNOWLEDGEBASE

The Red Hat Knowledgebase provides rich content aimed at helping you make the most of Red Hat products and technologies. The Red Hat Knowledgebase consists of articles, product documentation, and videos outlining best practices on installing, configuring, and using Red Hat products. In addition, you can search for solutions to known issues, each providing concise root cause descriptions and remedial steps.

1.2. SEARCHING THE RED HAT KNOWLEDGEBASE

In the event of an Red Hat Advanced Cluster Security for Kubernetes issue, you can perform an initial search to determine if a solution already exists within the Red Hat Knowledgebase.

Prerequisites

- You have a Red Hat Customer Portal account.

Procedure

1. Log in to the Red Hat Customer Portal .

2. In the main Red Hat Customer Portal search field, input keywords and strings relating to the problem, including:
    - Red Hat Advanced Cluster Security for Kubernetes components (such as **etcd**)
    - Related procedure (such as **installation**)
    - Warnings, error messages, and other outputs related to explicit failures
3. Click **Search**.
4. Select the **Red Hat Advanced Cluster Security for Kubernetes**product filter.
5. Select the **Knowledgebase** content type filter.

1.3. GENERATING A DIAGNOSTIC BUNDLE

You can generate a diagnostic bundle and send that data to enable the support team to provide insights into the status and health of Red Hat Advanced Cluster Security for Kubernetes components.

NOTE

The diagnostic bundle is unencrypted, and depending upon the number of clusters in your environment, the bundle size is between 100 KB and 1 MB.

1.3.1. Generating a diagnostic bundle by using the RHACS portal

You can generate a diagnostic bundle by using the system health dashboard on the RHACS portal.

Prerequisites

- To generate a diagnostic bundle, you need **read** permission for the **DebugLogs** resource.

Procedure

1. On the RHACS portal, select **Platform Configuration → System Health**.
2. On the **System Health** view header, click **Generate Diagnostic Bundle**.
3. For the **Filter by clusters** drop-down menu, select the clusters for which you want to generate the diagnostic data.
4. For **Filter by starting time**, specify the date and time (in UTC format) from which you want to include the diagnostic data.
5. Click **Download Diagnostic Bundle**.

1.3.2. Generating a diagnostic bundle by using the roxctl CLI

You can generate a diagnostic bundle by using the **roxctl** CLI.

Prerequisites

- To generate a diagnostic bundle, you need **read** permission for the **DebugLogs** resource.

Procedure

- Run the following command to generate a diagnostic bundle:

```
$ roxctl central debug download-diagnostics
```

1.4. SUBMITTING A SUPPORT CASE

Prerequisites

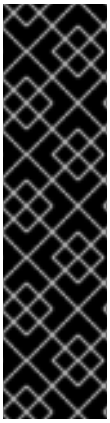
- You have access to the cluster.
- You have a Red Hat Customer Portal account.
- You have a Red Hat OpenShift Platform Plus subscription.

Procedure

1. Log in to the Red Hat Customer Portal and select **SUPPORT CASES → Open a case**.
2. Select the appropriate category for your issue (such as **Defect / Bug**), product (**Red Hat Advanced Cluster Security for Kubernetes**), and product version (**3.70**, if this is not already autofilled).
3. Review the list of suggested Red Hat Knowledgebase solutions for a potential match against the problem that is being reported. If the suggested articles do not address the issue, click **Continue**.
4. Enter a concise but descriptive problem summary and further details about the symptoms being experienced, as well as your expectations.
5. Review the updated list of suggested Red Hat Knowledgebase solutions for a potential match against the problem that is being reported. The list is refined as you provide more information during the case creation process. If the suggested articles do not address the issue, click **Continue**.
6. Ensure that the account information presented is as expected, and if not, amend accordingly.
7. Upload the generated diagnostic bundle and click **Continue**.
8. Input relevant case management details and click **Continue**.
9. Preview the case details and click **Submit**.

CHAPTER 2. GETTING SUPPORT FOR THE STACKROX KUBERNETES SECURITY PLATFORM

This topic provides information about the technical support for the StackRox Kubernetes Security Platform and details about other supported software and infrastructure.

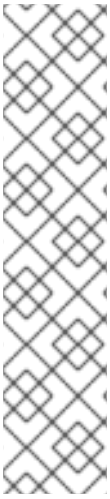


IMPORTANT

- The support-related information listed on this page is only applicable if you are not a Red Hat customer and you purchased the StackRox Kubernetes Security Platform before the acquisition. Red Hat will honor the StackRox support policy for its duration.
- If you are a Red Hat customer, see the following resources:
  - Getting support for Red Hat Advanced Cluster Security for Kubernetes
  - Red Hat Advanced Cluster Security for Kubernetes Support Policy

2.1. STACKROX KUBERNETES SECURITY PLATFORM SUPPORT

StackRox supports the StackRox Kubernetes Security Platform versions for up to six months after its release, which corresponds to the previous nine released versions. StackRox will make reasonable efforts and assist you in supporting some older versions. However, the support team may request you to upgrade to a newer released version of the StackRox Kubernetes Security Platform for full support.



NOTE

For the StackRox Kubernetes Security Platform, StackRox supports:

- The latest released version (referred to as *N*).
- Nine earlier versions.

The support window of the StackRox Kubernetes Security Platform versions is known as N-9 where: N (latest release) - 9 (earlier versions).

Along with our N-9 support window, StackRox might support version N-10 to N-13, depending on a case-by-case basis. StackRox will not support any earlier versions than N-13.

2.2. SUPPORT ON VARIOUS PLATFORMS

The StackRox support team supports a platform version based on the upstream (or vendor) product's support lifecycle for that version. When support for a platform version reaches its end of life (EOL) or is not actively maintained, StackRox no longer supports it.

WARNING

StackRox does not support:

- Installing the StackRox Kubernetes Security Platform on Minikube and other similar single-node clusters.
- Amazon Elastic File System (EFS). Use Amazon Elastic Block Store (EBS) with the default GP2 volume type instead.
- Older CPUs that do not have the Streaming SIMD Extensions (SSE) 4.2 instruction set, for example Intel processors older than Sandy Bridge and AMD processors older than Bulldozer. Both of these processors were released in 2011.

2.2.1. Operating systems

Operating system	Version
Ubuntu	16.04 LTS, 18.04 LTS, and 20.04 LTS with standard or cloud-provider-specific kernel versions
Debian	9, 10
Red Hat Enterprise Linux	7.3 till 7.9, 8.0 and newer
CentOS	7, 8
Fedora CoreOS	Stable stream 32.20200824.3.0 and newer
Flatcar Container Linux	2023.4.0 and newer
Google COS	77 and newer
Amazon Linux	2
Garden Linux	27.0 and newer

2.2.2. Container runtimes

Container runtimes	Version
Docker	17.03 and newer
CRI-O and runC	-

NOTE

CRI-O and runC support is available starting from Red Hat Advanced Cluster Security for Kubernetes version 2.5.31.0.

2.2.3. Container orchestrators and platforms

Container orchestrators and platforms	Version
Kubernetes[1]	1.15 and newer
OpenShift Container Platform	3.10, 3.11, 4.1, and newer
DC/OS Kubernetes[2]	2.0.0 and newer

NOTE

1. StackRox supports new versions of Kubernetes within three months of its open-source general-availability release. You might need to upgrade the Red Hat Advanced Cluster Security for Kubernetes to get support for the latest Kubernetes versions. See the Kubernetes support section for more details.
2. DC/OS support is available starting from Red Hat Advanced Cluster Security for Kubernetes 2.5.31.0.

2.2.3.1. Kubernetes support

The following table lists the minimum version of the StackRox Kubernetes Security Platform that StackRox support based on the Kubernetes version.

Kubernetes version	StackRox minimum support version
1.15, 1.16, 1.17	3.0.42.0
1.18	3.0.47.1
1.19	3.0.52.0

2.2.4. Managed Kubernetes services

StackRox support recent Kubernetes and OpenShift Container Platform versions, and test on managed Kubernetes service from all major cloud providers, including:

- Amazon Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)
- Google Kubernetes Engine (GKE)

NOTE

To install Collector on GKE clusters that have secure boot enabled, you must use eBPF probes because the third-party unsigned kernel module, unsigned by Google's CA, cannot be loaded when secure boot is enabled. Collector identifies Secure Boot status at the start and switches to eBPF probes if required.

Along with other types of clusters, StackRox also supports clusters created by using the kops - Kubernetes Operations tool with the default configurations on Amazon Web Services (AWS).