Red Hat Advanced Cluster Security for Kubernetes 4.1

Support

Getting support for Red Hat Advanced Cluster Security for Kubernetes

Last Updated: 2024-04-01

Red Hat Advanced Cluster Security for Kubernetes 4.1 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.

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 the documentation or have identified an error, create a Jira issue against the **Red Hat Advanced Cluster Security for Kubernetes**product for the **Documentation** component. Ensure that you include specific details such as the section name and the version of Red Hat Advanced Cluster Security for Kubernetes for us to manage your feedback effectively.

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.

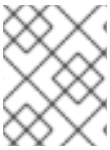
Procedure

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 with the Red Hat Advanced Cluster Security for Kubernetes (RHACS) administrator password or API token and central address by using the **roxctl** CLI.

Prerequisites

- To generate a diagnostic bundle, you need **read** permission for the **Administration** resource. This is required for versions of the **DebugLogs** resource older than version 3.73.0.
- You must have configured the RHACS administrator password or API token and central address.

Procedure

- To generate a diagnostic bundle by using the RHACS administrator password, perform the following steps:
    1. Run the following command to configure the **ROX_PASSWORD** and **ROX_CENTRAL_ADDRESS** environment variables:

```
$ export ROX_PASSWORD=<rox_password> && export
ROX_CENTRAL_ADDRESS=<address>:<port_number> 1
```

1 For **<rox_password>**, specify the RHACS administrator password.

2. Run the following command to generate a diagnostic bundle by using the RHACS administrator password:

```
$ roxctl -e "$ROX_CENTRAL_ADDRESS" -p "$ROX_PASSWORD" central debug
download-diagnostics
```

- To generate a diagnostic bundle by using the API token, perform the following steps:
  1. Run the following command to configure the **ROX_API_TOKEN** environment variable:

```
$ export ROX_API_TOKEN=<api_token>
```

  2. Run the following command to generate a diagnostic bundle by using the API token:

```
$ roxctl -e "$ROX_CENTRAL_ADDRESS" 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 (**4.1**, 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**.