Red Hat Advanced Cluster Security for Kubernetes 4.4

Telemetry

Understanding telemetry

Last Updated: 2024-04-22

Red Hat Advanced Cluster Security for Kubernetes 4.4 Telemetry

Understanding telemetry

Legal Notice

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

Guidance on understanding telemetry and the steps for opting out of telemetry data collection.

Table of Contents

CHAPTER 1. ABOUT TELEMETRY 3
1.1. INFORMATION COLLECTED BY TELEMETRY 3

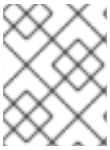
CHAPTER 2. OPTING OUT OF TELEMETRY 4
2.1. CONSEQUENCES OF DISABLING TELEMETRY 4
2.2. DISABLING TELEMETRY 4

CHAPTER 1. ABOUT TELEMETRY

Red Hat Advanced Cluster Security for Kubernetes (RHACS) collects anonymized aggregated information about product usage and product configuration. It helps Red Hat understand how everyone uses the product and identify areas to prioritize for improvements. In addition, Red Hat uses this information to improve the user experience.

1.1. INFORMATION COLLECTED BY TELEMETRY

Telemetry does not collect identifying information such as user names, passwords, or the names or addresses of user resources.



NOTE

Telemetry data collection is enabled by default, except for the installations with the offline mode enabled.

Telemetry collects the following information:

- API, **roxctl** CLI, and user interface (UI) features and settings to know how you use Red Hat Advanced Cluster Security for Kubernetes (RHACS), which helps prioritize efforts.
- The time you spend on UI screens to help us improve user experience.
- The integrations are used to know if there are integrations that you have never used.
- The number of connected secured clusters and their configurations.
- Errors you encounter to identify the most common problems.

CHAPTER 2. OPTING OUT OF TELEMETRY

The decision to opt out of telemetry should be based on your specific needs and requirements, as well as any applicable regulations or policies that you need to comply with.

2.1. CONSEQUENCES OF DISABLING TELEMETRY

In Red Hat Advanced Cluster Security for Kubernetes (RHACS) version 4.0, you can opt out of Telemetry. However, telemetry is embedded as a core component, so opting out is strongly discouraged. Opting out of telemetry limits the ability of Red Hat to understand how everyone uses the product and which areas to prioritize for improvements.

2.2. DISABLING TELEMETRY

If you have configured Telemetry by setting the key in your environment, you can disable Telemetry data collection from the Red Hat Advanced Cluster Security for Kubernetes (RHACS) user interface (UI).

Procedure

1. In the RHACS portal, go to **Platform Configuration > System Configuration**
2. In the **System Configuration** header, click **Edit**.
3. Scroll down and ensure that **Online Telemetry Data Collection** is set to **Disabled.**