Red Hat Advanced Cluster Security for Kubernetes 4.1

Telemetry

Understanding telemetry
Understanding telemetry
Abstract

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

CHAPTER 1. ABOUT TELEMETRY  
1.1. INFORMATION COLLECTED BY TELEMETRY  

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAPTER 1. ABOUT TELEMETRY</td>
<td>3</td>
</tr>
<tr>
<td>1.1. INFORMATION COLLECTED BY TELEMETRY</td>
<td>3</td>
</tr>
<tr>
<td>CHAPTER 2. OPTING OUT OF TELEMETRY</td>
<td>4</td>
</tr>
<tr>
<td>2.1. CONSEQUENCES OF DISABLING TELEMETRY</td>
<td>4</td>
</tr>
<tr>
<td>2.2. DISABLING TELEMETRY</td>
<td>4</td>
</tr>
</tbody>
</table>
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

In Red Hat Advanced Cluster Security Cloud Service (RHACS Cloud Service), telemetry data collection is enabled by default.

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, navigate 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.