



# Red Hat Advanced Cluster Security for Kubernetes 3.71

## サポート

Red Hat Advanced Cluster Security for Kubernetes のサポートを受ける



## Red Hat Advanced Cluster Security for Kubernetes 3.71 サポート

---

Red Hat Advanced Cluster Security for Kubernetes のサポートを受ける

## 法律上の通知

Copyright © 2023 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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

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

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

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

Node.js<sup>®</sup> 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<sup>®</sup> 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.

## 概要

このドキュメントでは、Red Hat Advanced Cluster Security for Kubernetes の Red Hat からサポートを受ける方法、および診断バンドルの生成方法について説明します。

---

## 目次

第1章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES のサポート .....	3
1.1. RED HAT ナレッジベースについて	3
1.2. RED HAT ナレッジベースの検索	3
1.3. 診断バンドルの生成	4
1.4. サポートケースの送信	4



# 第1章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES のサポート

このトピックでは、Red Hat Advanced Cluster Security for Kubernetes のテクニカルサポートに関する情報を提供します。

このドキュメントで説明されている手順、または一般的な Kubernetes の Red Hat Advanced Cluster Security で問題が発生した場合は、[Red Hat Customer Portal](#) にアクセスしてください。カスタマーポータルでは、以下を行うことができます。

- Red Hat 製品に関するアークティクルおよびソリューションについての Red Hat ナレッジベースの検索またはブラウズ。
- Red Hat サポートに対するサポートケースの送信。
- その他の製品ドキュメントへのアクセス。

このドキュメントの改善に関するご提案または誤植を見つけられた場合は、コンポーネントが **Documentation**、製品が **Red Hat Advanced Cluster Security for Kubernetes** として、[Jira issue](#) を起票してください。フィードバックを効果的に管理できるように、セクション名や Red Hat Advanced Cluster Security for Kubernetes のバージョンなどの特定の詳細を必ず含めるようにしてください。

## 1.1. RED HAT ナレッジベースについて

[Red Hat ナレッジベース](#) は、お客様が Red Hat の製品やテクノロジーを最大限に活用できるようにするための豊富なコンテンツを提供します。Red Hat ナレッジベースは、Red Hat 製品のインストール、設定、および使用に関する記事、製品ドキュメント、および動画で設定されています。さらに、簡潔な根本的な原因についての説明や修正手順を説明した既知の問題のソリューションを検索できます。

## 1.2. RED HAT ナレッジベースの検索

Red Hat Advanced Cluster Security for Kubernetes の問題が発生した場合は、初期検索を実行して、Red Hat ナレッジベース内にソリューションがすでに存在するかどうかを判断できます。

### 前提条件

- Red Hat カスタマーポータルのアカウントがある。

### 手順

1. [Red Hat カスタマーポータル](#) にログインします。
2. 主な Red Hat カスタマーポータルの検索フィールドには、問題に関連する入力キーワードおよび文字列を入力します。これらには、以下が含まれます。
  - Kubernetes コンポーネント (**etcd** など) の Red Hat Advanced Cluster Security
  - 関連する手順 (**installation** など)
  - 明示的な失敗に関連する警告、エラーメッセージ、およびその他の出力
3. **Search** をクリックします。
4. **Red Hat Advanced Cluster Security for Kubernetes** 製品フィルターを選択します。

5. ナレッジベース のコンテンツタイプフィルターを選択します。

### 1.3. 診断バンドルの生成

診断バンドルを生成し、そのデータを送信して、サポートチームが Red Hat Advanced Cluster Security for Kubernetes コンポーネントのステータスと正常性に関する洞察を提供できるようにすることができます。



#### 注記

診断バンドルは暗号化されておらず、環境内のクラスターの数に応じて、バンドルサイズは 100 KB から 1MB の間です。

#### 1.3.1. RHACS ポータルを使用した診断バンドルの生成

RHACS ポータルのシステムヘルスダッシュボードを使用して、診断バンドルを生成できます。

##### 前提条件

- 診断バンドルを生成するには、**DebugLogs** リソースの **read** 権限が必要。

##### 手順

1. RHACS ポータルで、**Platform Configuration** → **System Health** を選択します。
2. **System Health** ビューヘッダーで、**Generate Diagnostic Bundle** をクリックします。
3. **Filter by clusters** ドロップダウンメニューで、診断データを生成するクラスターを選択します。
4. **Filter by starting time** で、診断データを含める日付および時刻 (UTC 形式) を指定します。
5. **Download Diagnostic Bundle** をクリックします。

#### 1.3.2. roxctl CLI を使用した診断バンドルの生成

**roxctl** CLI を使用して診断バンドルを生成できます。

##### 前提条件

- 診断バンドルを生成するには、**DebugLogs** リソースの **read** 権限が必要。

##### 手順

- 次のコマンドを実行して、診断バンドルを生成します。

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

### 1.4. サポートケースの送信

##### 前提条件



- クラスタにアクセスできる。
- Red Hat カスタマーポータルアカウントがある。
- [Red Hat OpenShift Platform Plus](#) サブスクリプションがある。

## 手順

1. [Red Hat カスタマーポータル](#) にログインし、**SUPPORT CASES** → **Open a case** を選択します。
2. 問題の該当するカテゴリー (**Defect / Bug** など)、製品 (**Red Hat Advanced Cluster Security for Kubernetes**)、および製品バージョン (すでに自動入力されていない場合は 3.71) を選択します。
3. 報告されている問題に対する一致に基づいて提案される Red Hat ナレッジベースソリューションの一覧を確認してください。提案されている記事が問題に対応していない場合は、**Continue** をクリックします。
4. 問題についての簡潔で説明的な概要と、確認されている現象および予想される動作についての詳細情報を入力します。
5. 報告されている問題に対する一致に基づいて提案される Red Hat ナレッジベースソリューションの更新された一覧を確認してください。ケース作成プロセスでより多くの情報を提供すると、この一覧の絞り込みが行われます。提案されている記事が問題に対応していない場合は、**Continue** をクリックします。
6. アカウント情報が予想通りに表示されていることを確認し、そうでない場合は適宜修正します。
7. 生成された診断バンドルをアップロードし、**Continue** をクリックします。
8. 関連するケース管理の詳細情報を入力し、**Continue** をクリックします。
9. ケースの詳細をプレビューし、**Submit** をクリックします。