Red Hat Advanced Cluster Security for Kubernetes 4.0

Support

Red Hat Advanced Cluster Security for Kubernetes のサポート

Last Updated: 2024-04-02

Red Hat Advanced Cluster Security for Kubernetes 4.0 Support

Red Hat Advanced Cluster Security for Kubernetes のサポート

法律上の通知

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を説明します。

目次

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 製品に関するアーティクルおよびソリューションを対象とした 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提案がある場合、または誤植が見つかった場合は、Jira issue を起票してください。コンポーネントは **Documentation**、製品は **Red Hat Advanced Cluster Security for Kubernetes** を選択してください。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詳細を必ず記入してください。

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、既知の問題に対する解決策を検索でき、それぞれに根本原因の簡潔な説明と修復手順が記載されています。

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。

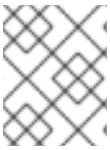
手順

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、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。たとえば、以下を入力します。
   - 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 SecurityforKubernetes**製品フィルターを選択します。

5. コンテンツタイプフィルターで **ナレッジベース** を選択します。

1.3. 診断バンドルの生成

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、診断バンドルを生成して、そのデータを送信してください。



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 1 MB 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、Red Hat Advanced Cluster Security for Kubernetes (RHACS) 管理者パスワードまたは API トークンと中央アドレスで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ために、**Administration** リソースの **read** パーミッションを用意する。これは、バージョン 3.73.0 よりも古い **DebugLogs** リソースのバージョンで必要です。
- RHACS 管理者パスワード、API トークン、および中央アドレスを設定している。

手順

- RHACS 管理者パスワードを使用して診断バンドルを生成するには、以下の手順を実行します。
  1. 以下のコマンドを実行して **ROX_PASSWORD** および **ROX_CENTRAL_ADDRESS** 環境変数を設定します。

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

1 **<rox_password>** には、RHACS 管理者パスワードを指定します。

2. 次のコマンドを実行して、RHACS 管理者パスワードを使用して診断バンドルを生成します。

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

- API トークンを使用して診断バンドルを生成するには、以下の手順を実行します。

1. 以下のコマンドを実行して **ROX_API_TOKEN** 環境変数を設定します。

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

2. 以下のコマンドを実行して API トークンを使用して診断バンドルを生成します。

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

1.4. サポートケースの送信

前提条件

- クラスターにアクセスできる。
- Red Hat カスタマーポータルのアカウントがある。
- 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. 問題の適切なカテゴリー (**Defect/Bug** など)、製品 (**Red Hat Advanced Cluster Security for Kubernetes**)、製品バージョン (自動入力されない場合は **4.0**) を選択します。
3. Red Hat ナレッジベースで推奨されるソリューション一覧を確認してください。この一覧に上げられているソリューションは、報告しようとしている問題に適用される可能性があります。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。
4. 問題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の詳細情報を入力します。
5. 報告している問題に対する一致に基づいて推奨される Red Hat ナレッジベースソリューションの一覧が更新されること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。