



Red Hat Advanced Cluster Security for Kubernetes 3.72

バックアップおよび復元

Red Hat Advanced Cluster Security for Kubernetes のバックアップおよび復元

Red Hat Advanced Cluster Security for Kubernetes 3.72 バックアップおよび復元

Red Hat Advanced Cluster Security for Kubernetes のバックアップおよび復元

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[®] 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.

概要

バックアップからシステムをバックアップし、復元する方法を説明します。

目次

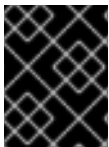
| | |
|--|---|
| 第1章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES のバックアップ | 3 |
| 1.1. ROXCTL CLI を使用したオンデマンドバックアップ | 3 |
| 第2章 バックアップからの復元 | 5 |
| 2.1. API トークンを使用した復元 | 5 |
| 2.2. 管理者パスワードを使用した復元 | 5 |
| 2.3. 復元操作の再開 | 6 |

第1章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES のバックアップ

Red Hat Advanced Cluster Security for Kubernetes のデータバックアップを実行できます。これらのバックアップは、インフラストラクチャーの災害やデータの破損が発生した場合のデータの復元に使用できます。

Amazon S3 または Google Cloud Storage と統合することで、自動バックアップまたはオンデマンドバックアップを設定できます。または、**roxctl** コマンドラインインターフェイス (CLI) を使用してオンデマンドバックアップを実行できます。

バックアップには、Red Hat Advanced Cluster Security for Kubernetes データベース全体が含まれます。これには、すべての設定、リソース、イベント、および証明書が含まれます。バックアップが安全に保存されていることを確認してください。



重要

3.0.53 以前の Red Hat Advanced Cluster Security for Kubernetes を使用している場合は、バックアップに証明書が含まれていません。

1.1. ROXCTL CLI を使用したオンデマンドバックアップ

roxctl CLI を使用して、**backup** コマンドを使用してバックアップを作成できます。このコマンドを実行するには、API トークンまたは管理者パスワードのいずれかが必要です。

1.1.1. API トークンを使用したオンデマンドバックアップ

API トークンを使用して、Red Hat Advanced Cluster Security for Kubernetes のデータベース全体をバックアップできます。

前提条件

- **Admin** ロールを持つ API トークンが必要です。
- **roxctl** CLI をインストールしている。

手順

1. **ROX_API_TOKEN** および **ROX_CENTRAL_ADDRESS** 環境変数を設定します。

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

```
$ export ROX_CENTRAL_ADDRESS=<address>:<port_number>
```

2. **backup** コマンドを実行します。

- Red Hat Advanced Cluster Security for Kubernetes 3.0.55 以降の場合:

```
$ roxctl -e "$ROX_CENTRAL_ADDRESS" central backup
```

- Red Hat Advanced Cluster Security for Kubernetes 3.0.54 以降の場合:

```
$ roxctl -e "$ROX_CENTRAL_ADDRESS" central db backup
```

デフォルトでは、**roxctl** CLI はコマンドを実行したディレクトリーにバックアップファイルを保存します。**--output** オプションを使用して、バックアップファイルの場所を指定できます。

関連情報

- [システムロール](#)

1.1.2. 管理者パスワードを使用したオンデマンドバックアップ

管理者パスワードを使用して、Red Hat Advanced Cluster Security for Kubernetes のデータベース全体をバックアップできます。

前提条件

- 管理者パスワードが必要である。
- **roxctl** CLI をインストールしている。

手順

1. **ROX_CENTRAL_ADDRESS** 環境変数を設定します。

```
$ export ROX_CENTRAL_ADDRESS=<address>:<port_number>
```

2. **backup** コマンドを実行します。

- Red Hat Advanced Cluster Security for Kubernetes 3.0.55 以降の場合:

```
$ roxctl -p <admin_password> -e "$ROX_CENTRAL_ADDRESS" central backup
```

- Red Hat Advanced Cluster Security for Kubernetes 3.0.54 以降の場合:

```
$ roxctl -p <admin_password> -e "$ROX_CENTRAL_ADDRESS" central db backup
```

デフォルトでは、**roxctl** CLI はコマンドを実行したディレクトリーにバックアップファイルを保存します。**--output** オプションを使用して、バックアップファイルの場所を指定できます。

第2章 バックアップからの復元

roxctl コマンドラインインターフェイス (CLI) を使用して、既存のバックアップから Red Hat Advanced Cluster Security for Kubernetes を復元できます。

roxctl CLI を使用して、**restore** コマンドを使用して Red Hat Advanced Cluster Security for Kubernetes を復元できます。このコマンドを実行するには、API トークンまたは管理者パスワードのいずれかが必要です。

2.1. API トークンを使用した復元

API トークンを使用して、Red Hat Advanced Cluster Security for Kubernetes のデータベース全体を復元できます。

前提条件

- Red Hat Advanced Cluster Security for Kubernetes バックアップファイルが必要です。
- 管理者ロールを持つ API トークンがある。
- **roxctl** CLI をインストールしている。

手順

1. **ROX_API_TOKEN** および **ROX_CENTRAL_ADDRESS** 環境変数を設定します。

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

```
$ export ROX_CENTRAL_ADDRESS=<address>:<port_number>
```

2. **restore** コマンドを実行します。

```
$ roxctl -e "$ROX_CENTRAL_ADDRESS" central db restore <backup_file>
```

2.2. 管理者パスワードを使用した復元

管理者パスワードを使用して、Red Hat Advanced Cluster Security for Kubernetes のデータベース全体を復元できます。

前提条件

- Red Hat Advanced Cluster Security for Kubernetes バックアップファイルが必要です。
- 管理者パスワードが必要である。
- **roxctl** CLI をインストールしている。

手順

1. **ROX_CENTRAL_ADDRESS** 環境変数を設定します。

```
$ export ROX_CENTRAL_ADDRESS=<address>:<port_number>
```

2. **restore** コマンドを実行します。

```
$ roxctl -p <admin_password> -e "$ROX_CENTRAL_ADDRESS" central db restore
<backup_file>
```

2.3. 復元操作の再開

復元操作中に接続が中断された場合、またはオフラインにする必要がある場合は、復元操作を再開できます。

- 再開操作を実行しているマシンにアクセスできない場合は、**roxctl central db restore status** コマンドを使用して、進行中の復元操作の状況を確認してください。
- 接続が中断された場合、**roxctl** CLI は、接続が使用可能になると自動的にタスクの復元を試みます。自動接続の再試行は、**timeout** オプションで指定された期間によって異なります。
- timeout** オプションを使用して、時間を秒、分、または時間で指定します。その後、**roxctl** CLI は復元操作の再開を停止します。指定しない場合、デフォルトのタイムアウトは 10 分 (10m) です。
- 復元操作がスタックしている場合、またはそれをキャンセルしたい場合は、**roxctl central db restore cancel** コマンドを使用して、進行中の復元操作をキャンセルします。
- 復元操作がスタックしている場合、キャンセルした場合、またはタイムアウトした場合は、元のコマンドを再実行することで以前の復元を再開できます。

注記

- 中断中、Red Hat Advanced Cluster Security for Kubernetes は、進行中の復元操作を 24 時間キャッシュします。元の復元コマンドを再実行すると、この操作を再開できます。
- timeout** オプションは、クライアント側の接続の再試行のみを管理し、24 時間のサーバー側の復元キャッシュには影響しません。
- Central Pod を再起動しても、復元操作を再開することはできません。
- 復元操作が中断された場合は、24 時間以内に、Central が再起動する前に再起動する必要があります。そうしないと、Red Hat Advanced Cluster Security for Kubernetes が復元操作をキャンセルします。