



Red Hat Advanced Cluster Security for Kubernetes 4.0

バックアップと復元

Red Hat Advanced Cluster Security for Kubernetes のバックアップと復元

Red Hat Advanced Cluster Security for Kubernetes 4.0 バックアップと復元

Red Hat Advanced Cluster Security for Kubernetes のバックアップと復元

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

システムをバックアップし、そのバックアップから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 CENTRAL データベースのバックアップ	3
1.2. CENTRAL デプロイメントのバックアップ	4
第2章 バックアップからの復元	6
2.1. ROXCTL CLI を使用した CENTRAL データベースの復元	6
2.2. ROXCTL CLI を使用した CENTRAL デプロイメントの復元	7
2.3. RHACS OPERATOR を使用した CENTRAL デプロイメントの復元	9
2.4. HELM を使用して中央デプロイメントを復元する	10
2.5. セントラルを別のクラスターまたは NAMESPACE に復元する	10

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し、インフラストラクチャの障害やデータの破損が発生した場合に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、Central データベースの自動バックアップを設定できます。**roxctl** CLI を使用して、Central データベースのオンデマンドバックアップを実行できます。RHACS Operator または Helm Chart のインストール方法を使用して、Central デプロイメントをバックアップすることもできます。

要件に応じて、2 種類のバックアップを作成できます。

1. Central データベースのバックアップ: RHACS 設定、リソース、イベント、および証明書が含まれます。データベース障害やデータ破損などの予期せぬ事態が発生した場合は、バックアップを使用して Central データベースを回復し、以前の機能状態に復元できます。これにより、重要なデータの可用性と整合性が確保され、大幅に中断したり重要な情報を失うことなく、通常の運用を継続できるようになります。
2. すべてのカスタムデプロイメント設定のバックアップ: Helm チャートまたは RHACS Operator を使用して RHACS をインストールした場合は、インストールに固有の設定、パラメーター、およびカスタマイズをバックアップできます。RHACS インストールが誤って削除されるか、別のクラスターまたは namespace に移行する必要がある場合は、デプロイメント設定のバックアップがあると、シームレスなリカバリープロセスが可能になります。さらに、バックアップからカスタム設定を復元することで、Central インストールに固有の要件と設定を効率的に元に戻し、システムの一貫性と正確なデプロイメントを確保できます。

バックアップファイルにはシークレットと証明書が含まれるため、バックアップファイルを安全に保存する必要があります。

1.1. ROXCTL CLI を使用した CENTRAL データベースのバックアップ

Central データベースのバックアップは、データの整合性とシステムの信頼性を確保するために重要です。必要な設定、リソース、イベント、証明書を含むデータベースを定期的にバックアップすることで、データベースの障害、破損、偶発的なデータ損失を防ぎます。

roxctl CLI を使用し、**backup** コマンドで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. **backup** コマンドを実行します。

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

- ❶ **--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。

デフォルトでは、**roxctl** CLI はコマンドを実行するディレクトリーにバックアップファイルを保存します。

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。

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

デフォルトでは、**roxctl** CLI が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。

1.2. CENTRAL デプロイメントのバックアップ

Central インスタンスのデプロイメントをバックアップできます。これは、同じ設定値を使用してセントラルを別の namespace またはクラスターに移行する場合に便利です。



注記

Red Hat は、**roxctl** CLI を使用したデプロイメント設定のバックアップをサポートしていません。**oc** または **kubectrl** CLI を使用して、Central インスタンスに関連するマニフェストをバックアップし、設定を復元できます。

1.2.1. RHACS Operator を使用したデプロイメントのバックアップ

RHACS Operator を使用して RHACS をインストールすると、OpenShift Container Platform は Central デプロイメントのすべてのカスタム設定を Central カスタムリソース内に保存します。Central カスタムリソース、**central-tls** シークレット、および管理者パスワードをバックアップできます。**Central-TLS** シークレットには、セキュリティーで保護されたクラスターでの認証と API トークンへの署名のための証明書が含まれています。

手順

1. 次のコマンドを実行して、Central カスタムリソースを YAML ファイルに保存します。

```
$ oc get central -n _<central-namespace>_ -o yaml > central-cr.yaml
```

2. 次のコマンドを実行して、**central-tls** を JSON ファイルに保存します。

```
$ oc get secret -n _<central-namespace>_ central-tls -o json | jq  
'del(.metadata.ownerReferences)' > central-tls.json
```

3. JSON ファイル内の管理者パスワードに対して次のコマンドを実行します。

```
$ oc get secret -n _<central-namespace>_ central-htpasswd -o json | jq  
'del(.metadata.ownerReferences)' > central-htpasswd.json
```

1.2.2. Helm を使用したデプロイメントのバックアップ

Helm チャートを使用して RHACS をインストールすると、Helm チャートに適用するカスタム値内に Central デプロイメントのすべてのカスタム設定が保存されます。

カスタム値をバックアップし、YAML ファイルに保存できます。

手順

- 次のコマンドを実行して、カスタム Helm チャートの値を YAML ファイルにバックアップします。

```
$ helm get values --all -n _<central-namespace>_ -o yaml >  
central-values-backup.yaml
```

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。

要件とバックアップしたデータに応じて、次のタイプのバックアップから復元できます。

1. **Restore Central database from the Central database backup** これを使用して、データベース障害またはデータ破損イベントから回復します。これにより、Central データベースを以前の機能状態に復元およびリカバリーできます。
2. **Restore Central from the Central deployment backup** Central を別のクラスターまたは名前空間に移行する場合は、これを使用します。このオプションは、Central インストールの設定を復元します。

2.1. ROXCTL CLI を使用した CENTRAL データベースの復元

roxctl CLI を使用し、**restore** コマンドで 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が必要です。

2.1.1. 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ある。
- 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>
```

2.1.2. 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ある。

- 管理者パスワードがある。
- **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>
```

2.1.3. 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った場合は、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時間に準じて行われます。
- **--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。**roxctl** CLI は、その時間が経過すると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、それを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、サーバー側における 24 時間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 時間以内を期限として Central が再起動する前に再起動する必要があります。そうしなければ、Red Hat Advanced Cluster Security for Kubernetes が復元操作をキャンセルします。

2.2. ROXCTL CLI を使用した CENTRAL デプロイメントの復元

作成したバックアップを使用して、Central デプロイメントを元の設定に復元できます。

まず **roxctl** CLI を使用して証明書を復元し、次に Central インストールスクリプトを実行して Central デプロイメントを復元する必要があります。

2.2.1. roxctl CLI を使用して証明書を復元する

roxctl CLI を使用して Kubernetes マニフェストを生成し、RHACS Central コンポーネントをクラスターにインストールします。これにより、セキュリティーで保護されたクラスターの認証証明書と API トークンが復元されたバージョンでも有効なままであることを確認できます。RHACS Central の別のインスタンスをバックアップした場合は、そのバックアップの証明書ファイルを使用できます。



注記

roxctl CLI では、Central デプロイメント全体を復元することはできません。代わりに、まず **roxctl** CLI を使用して、中央データバックアップ内の証明書を使用して新しいマニフェストを生成します。その後、これらのマニフェストを使用して Central をインストールします。

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。
- roxctl** CLI をインストールしている。

手順

- 対話型インストールコマンドを実行します。

```
$ roxctl central generate interactive
```

- 次のプロンプトに対して、Red Hat Advanced Cluster Security for Kubernetes バックアップファイルのパスを入力します。

```
Enter path to the backup bundle from which to restore keys and certificates (optional):
_<backup-file-path>_
```

- 後続のその他のプロンプトについては、**Enter** キーを押してデフォルト値を受け入れるか、必要に応じてカスタム値を入力します。

完了すると、対話型インストールコマンドは、**Central-bundle** という名前のフォルダーを作成します。このフォルダーには、Central をデプロイするために必要な YAML マニフェストとスクリプトが含まれています。

2.2.2. Central インストールスクリプトの実行

対話型インストーラーを実行したら、**setup.sh** スクリプトを実行して Central をインストールできます。

手順

- setup.sh** スクリプトを実行して、イメージレジストリーアクセスを設定します。

```
$ ./central-bundle/central/scripts/setup.sh
```

2. 必要なリソースを作成します。

```
$ oc create -R -f central-bundle/central
```

3. デプロイメントの進行状況を確認します。

```
$ oc get pod -n stackrox -w
```

4. Central の実行後、RHACS ポータルの IP アドレスを見つけて、ブラウザで開きます。プロンプトに応答するときを選択した公開方法に応じて、次のいずれかの方法を使用して IP アドレスを取得します。

公開方法	コマンド	アドレス	例
ルート	oc -n stackrox get route central	出力の HOST/PORT 列の下アドレス	https://central-stackrox.example.route
ノードポート	oc get node -owide && oc -n stackrox get svc central-loadbalancer	サービス用に表示されたポート上の任意のノードの IP またはホスト名	https://198.51.100.0:31489
ロードバランサー	oc -n stackrox get svc central-loadbalancer	EXTERNAL-IP、またはポート 443 でサービスに表示されるホスト名	https://192.0.2.0
なし	central-bundle/central/scripts/port-forward.sh 8443	https://localhost:8443	https://localhost:8443

注記

対話型インストール中に自動生成されたパスワードを選択した場合は、次のコマンドを実行して、Central にログインするためのパスワードを確認できます。

```
$ cat central-bundle/password
```

2.3. RHACS OPERATOR を使用した CENTRAL デプロイメントの復元

RHACS Operator を使用して、Central デプロイメントを元の設定に復元できます。正常に復元するには、Central カスタムリソース (**central-tls**) と管理者パスワードのバックアップが必要です。

前提条件

- **Central-TLS** バックアップファイルがある。
- Central カスタムリソースバックアップファイルがある。
- 管理者パスワードのバックアップファイルがある。

手順

1. **Central-TLS** バックアップファイルを使用してリソースを作成します。

```
$ oc apply -f central-tls.json
```

2. **Central-htpasswd** バックアップファイルを使用してシークレットを作成します。

```
$ oc apply -f central-htpasswd.json
```

3. **Central-cr.yaml** ファイルを使用して、Central デプロイメントを作成します。

```
$ oc apply -f central-cr.yaml
```

2.4. HELM を使用して中央デプロイメントを復元する

Helm を使用すると、Central デプロイメントを元の設定に復元できます。正常に復元するには、Central カスタムリソース、**central-tls** シークレット、および管理者パスワードのバックアップが必要です。

前提条件

- Helm 値のバックアップファイルがある。
- Red Hat Advanced Cluster Security for Kubernetes バックアップファイルがある。
- **roxctl** CLI をインストールしている。

手順

1. RHACS データベースのバックアップファイルから **value-private.yaml** を生成します。

```
$ roxctl central generate k8s pvc --backup-bundle _<path-to-backup-file>_ --output-format "helm-values"
```

2. **helm install** コマンドを実行し、バックアップファイルを指定します。

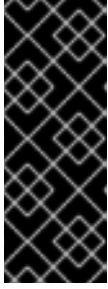
```
$ helm install -n stackrox --create-namespace stackrox-central-services rhacs/central-services -f central-values-backup.yaml -f central-bundle/values-private.yaml
```

2.5. セントラルを別のクラスターまたは NAMESPACE に復元する

RHACS Central データベースとデプロイメントのバックアップを使用して、Central を別のクラスターまたは namespace に復元できます。

次のリストは、インストール手順の概要を示しています。

1. インストール方法に応じて、最初に次のトピックの手順に従って Central デプロイメントを復元する必要があります。



重要

- 古い Central インスタンスによって発行された保護されたクラスターと API トークンが有効なままになるように、バックアップされた Central 証明書を必ず使用してください。
- 別の namespace にデプロイする場合は、バックアップされたリソースまたはコマンドの namespace を変更する必要があります。

- [roxctl CLI を使用した Central デプロイメントの復元](#)
 - [RHACS Operator を使用した Central デプロイメントの復元](#)
 - [Helm を使用して中央デプロイメントを復元する](#)
2. [roxctl CLI を使用したセントラルデータベースの復元](#) の指示に従って、セントラルデータベースを復元します。
 3. 古い RHACS Central インスタンスを指す外部 DNS エントリーがある場合は、作成した新しい RHACS Central インスタンスを指すように再設定する必要があります。