



サードパーティのツールを使用してデータを保護する

NetApp virtualization solutions

NetApp
August 18, 2025

目次

サードパーティのツールを使用してデータを保護する	1
OpenShift API for Data Protection (OADP) を使用した Red Hat OpenShift Virtualization の VM のデータ保護について学習します。	1
Red Hat OpenShift API for Data Protection (OADP) オペレーターをインストールする	3
前提条件	3
OADPオペレーターのインストール手順	4
Velero を使用して Red Hat OpenShift Virtualization の VM のオンデマンド バックアップを作成する	13
VMのバックアップを作成する手順	13
OpenShift Virtualization で VM のスケジュールされたバックアップを作成する	15
Velero を使用して Red Hat OpenShift Virtualization のバックアップから VM を復元する	16
前提条件	16
Velero を使用して Red Hat OpenShift Virtualization でバックアップ CR を削除または復元する	22
バックアップの削除	22
復元の削除	22

サードパーティのツールを使用してデータを保護する

OpenShift API for Data Protection (OADP) を使用した Red Hat OpenShift Virtualization の VM のデータ保護について学習します。

Velero を使用した OpenShift API for Data Protection (OADP) は、OpenShift Virtualization 内の VM のバックアップ、リストア、および災害復旧機能を提供します。Trident CSI スナップショットを使用して、永続ボリュームと VM メタデータを NetApp ONTAP S3 または StorageGRID S3 にバックアップします。OADP は Velero API および CSI ストレージ ドライバーと統合して、コンテナ化された VM のデータ保護操作を管理します。

OpenShift Virtualization 環境の仮想マシンは、OpenShift Container プラットフォームのワーカーノードで実行されるコンテナ化されたアプリケーションです。VM のメタデータと永続ディスクを保護して、それらが失われたり破損したりした場合に回復できるようにすることが重要です。

OpenShift Virtualization VM の永続ディスクは、OpenShift Cluster に統合された ONTAP ストレージによってバックアップできます。["TridentCSI"](#)。このセクションでは["データ保護のための OpenShift API \(OADP\)"](#)データボリュームを含む VM のバックアップを実行する

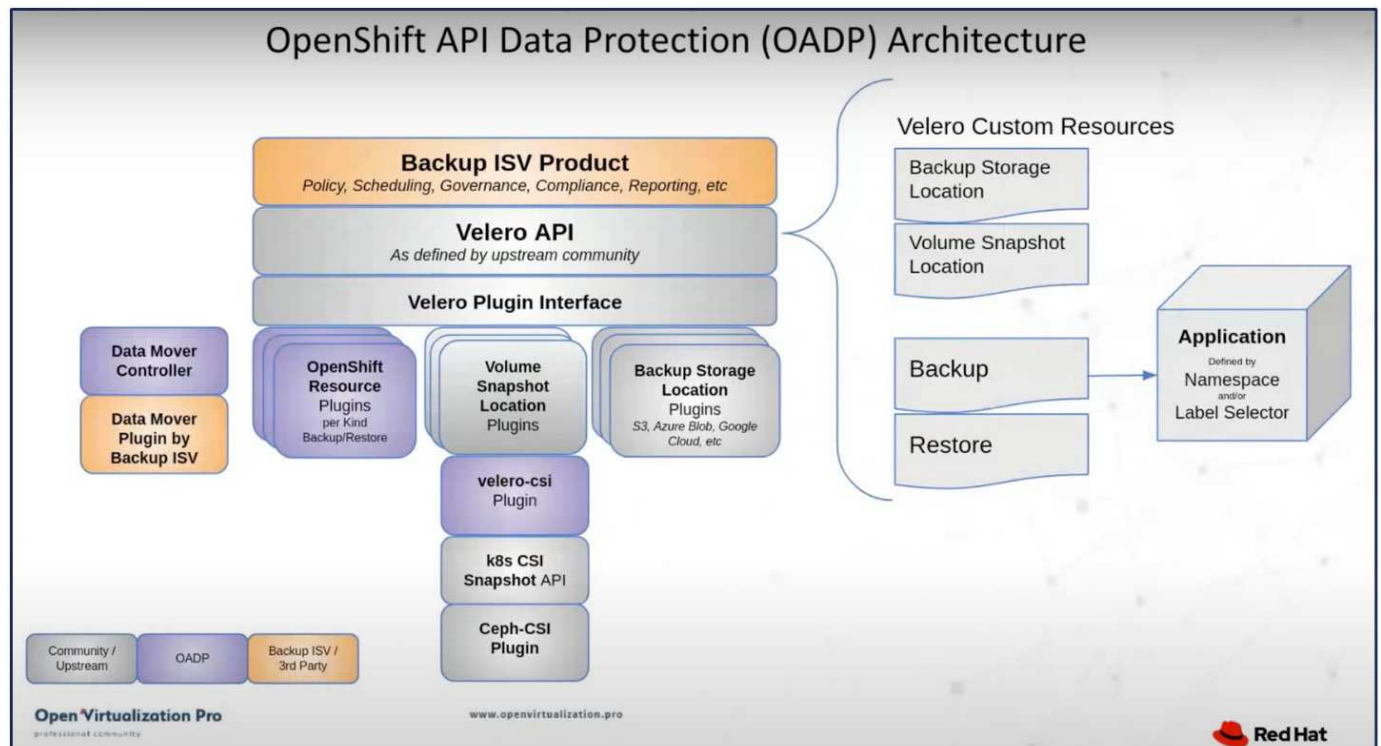
- ONTAP オブジェクトストレージ
- ストレージグリッド

必要に応じてバックアップから復元します。

OADP は、OpenShift クラスター上のアプリケーションのバックアップ、復元、および災害復旧を可能にします。OADP で保護できるデータには、Kubernetes リソース オブジェクト、永続ボリューム、内部イメージなどがあります。



Red Hat OpenShift は、データ保護のためにオープンソース コミュニティによって開発されたソリューションを活用しています。"ベレロ" Kubernetes クラスター リソースと永続ボリュームを安全にバックアップおよび復元し、災害復旧を実行し、移行するためのオープンソース ツールです。Velero を簡単に使用できるように、OpenShift は OADP オペレーターと、CSI ストレージ ドライバーと統合する Velero プラグインを開発しました。公開されている OADP API の中核は、Velero API に基づいています。OADP オペレータをインストールして構成した後、実行できるバックアップ/復元操作は、Velero API によって公開される操作に基づいて行われます。



OADP 1.3 は、OpenShift クラスター 4.12 以降のオペレーター ハブから入手できます。CSI ボリューム スナップショットをリモート オブジェクト ストアに移動できるデータ ムーバーが組み込まれています。これにより、バックアップ中にスナップショットをオブジェクト ストレージの場所に移動することで、移植性と耐久性が実現します。スナップショットは災害後の復元に利用できます。

以下は、このセクションの例で使用されているさまざまなコンポーネントのバージョンです

- OpenShift クラスター 4.14
- OpenShift Virtualization は Operator 経由でインストールされます。Red Hat が提供する OpenShift Virtualization Operator
- Red Hat が提供する OADP Operator 1.13
- Linux 用 Velero CLI 1.13
- Trident24.02
- ONTAP 9.12

"TridentCSI" "データ保護のための OpenShift API (OADP)" "ベレロ"

Red Hat OpenShift API for Data Protection (OADP) オペレーターをインストールする

OpenShift API for Data Protection (OADP) Operator をインストールして、OpenShift Virtualization 内の VM のバックアップおよび復元機能を有効にします。この手順には、OpenShift Operator Hub から OADP Operator をデプロイし、バックアップ ターゲットとしてNetApp ONTAP S3 またはStorageGRIDを使用するように Velero を構成し、必要なシークレットとバックアップの場所を設定することが含まれます。

前提条件

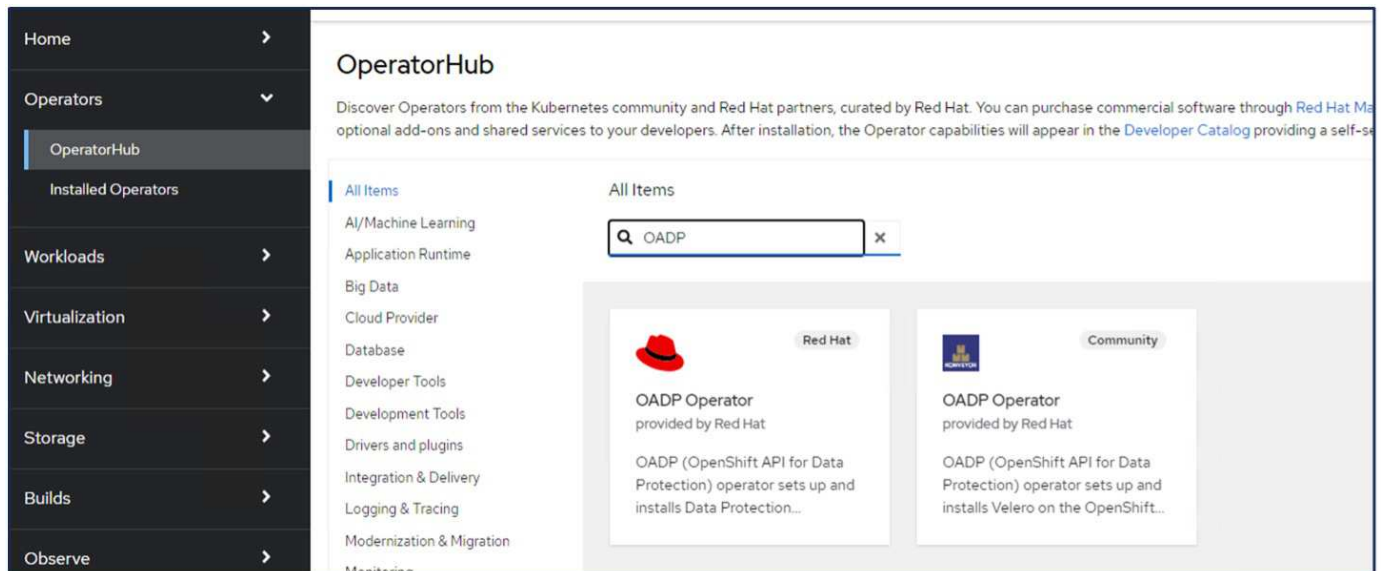
- RHCOS ワーカーノードを備えたベアメタル インフラストラクチャにインストールされた Red Hat OpenShift クラスター (バージョン 4.12 以降)
- Tridentを使用してクラスターに統合されたNetApp ONTAPクラスター
- ONTAPクラスター上のSVMで構成されたTridentバックエンド
- Tridentをプロビジョナーとして OpenShift クラスター上に構成された StorageClass
- クラスター上に作成されたTridentスナップショット クラス
- Red Hat OpenShift クラスターへのクラスター管理者アクセス
- NetApp ONTAPクラスターへの管理者アクセス
- OpenShift Virtualization オペレーターがインストールおよび設定されている
- OpenShift Virtualization 上の名前空間にデプロイされた VM
- tridentctl および oc ツールがインストールされ、\$PATH に追加された管理ワークステーション



VM が実行状態のときにバックアップを取得する場合は、その仮想マシンに QEMU ゲスト エージェントをインストールする必要があります。既存のテンプレートを使用して VM をインストールすると、QEMU エージェントが自動的にインストールされます。QEMU を使用すると、ゲスト エージェントはスナップショット プロセス中にゲスト OS 内の転送中のデータを静止させ、データ破損を回避できます。QEMU がインストールされていない場合は、バックアップを取る前に仮想マシンを停止できます。

OADPオペレーターのインストール手順

1. クラスターのオペレーター ハブに移動し、Red Hat OADP オペレーターを選択します。インストール ページで、すべてのデフォルトの選択を使用して、インストールをクリックします。次のページでは、再度すべてのデフォルトを使用し、「インストール」をクリックします。OADP オペレーターは、名前空間 openshift-adp にインストールされます。





OADP Operator

1.3.0 provided by Red Hat

Install

Channel

stable-1.3

Version

1.3.0

Capability level

- ☒ Basic Install
- ☒ Seamless Upgrades
- ☐ Full Lifecycle
- ☐ Deep Insights
- ☐ Auto Pilot

Source

Red Hat

Provider

Red Hat

Infrastructure features

Disconnected

OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.

Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.

OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.

- [Installing OADP for application backup and restore](#)
- [Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM](#)
- [Frequently Asked Questions](#)

Project: All Projects

Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the [Understanding Operators documentation](#) Operator and ClusterServiceVersion using the [Operator SDK](#).

Name Search by name...

Name	Namespace	Managed Namespaces	Status
 OpenShift Virtualization 4.14.4 provided by Red Hat	 openshift-cnv	 openshift-cnv	 Succeeded Up to date
 OADP Operator 1.3.0 provided by Red Hat	 openshift-adp	 openshift-adp	 Succeeded Up to date
 Package Server 0.0.1-snapshot provided by	 openshift-operator-lifecycle-manager	 openshift-operator-lifecycle-manager	 Succeeded

Ontap S3 を使用した Velero 構成の前提条件の詳細

オペレーターのインストールが成功したら、Velero のインスタンスを構成します。Velero は、S3 互換のオブジェクト ストレージを使用するように構成できます。ONTAP S3を設定するには、["ONTAPドキュメントのオブジェクトストレージ管理セクション"](#)。Velero と統合するには、ONTAP S3 構成から次の情報が必要になります。

- S3にアクセスするために使用できる論理インターフェース（LIF）
- アクセスキーとシークレットアクセスキーを含む、S3 にアクセスするためのユーザー認証情報
- ユーザーのアクセス権限を持つバックアップ用のS3のバケット名
- オブジェクト ストレージへの安全なアクセスのために、オブジェクト ストレージ サーバーに TLS 証明書 をインストールする必要があります。

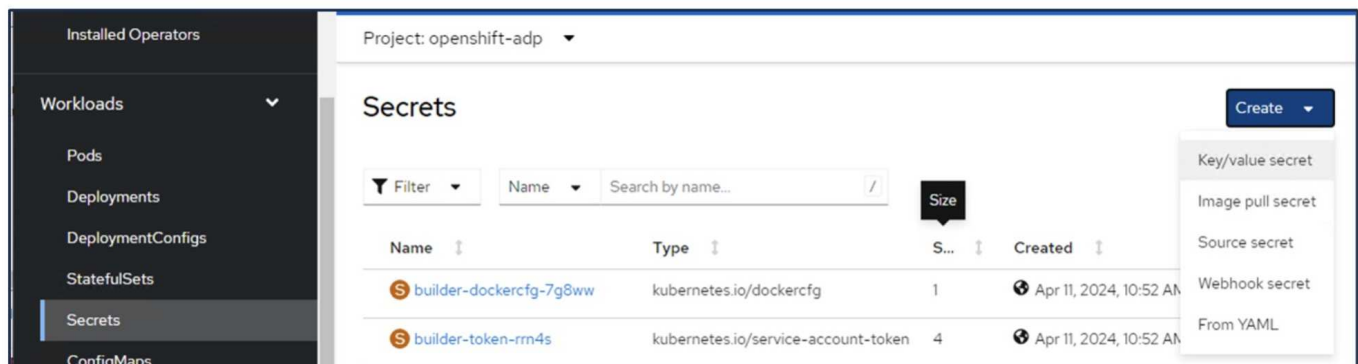
StorageGrid S3 を使用した Velero 構成の前提条件の詳細

Velero は、S3 互換のオブジェクト ストレージを使用するように構成できます。StorageGrid S3は、以下の手順で設定できます。["StorageGrid ドキュメント"](#)。Velero と統合するには、StorageGrid S3 構成から次の情報が必要になります。

- S3にアクセスするために使用できるエンドポイント
- アクセスキーとシークレットアクセスキーを含む、S3 にアクセスするためのユーザー認証情報
- ユーザーのアクセス権限を持つバックアップ用のS3のバケット名
- オブジェクト ストレージへの安全なアクセスのために、オブジェクト ストレージ サーバーに TLS 証明書 をインストールする必要があります。

Veleroの設定手順

- まず、ONTAP S3 ユーザー認証情報または StorageGrid テナント ユーザー認証情報のシークレットを作成します。これは後で Velero を構成するために使用されます。CLI または Web コンソールからシークレットを作成できます。Web コンソールからシークレットを作成するには、「シークレット」を選択し、「キー/値シークレット」をクリックします。示されているように、資格情報名、キー、および値の値を指定します。S3 ユーザーのアクセス キー ID とシークレット アクセスキーを必ず使用してください。秘密に適切な名前を付けます。以下のサンプルでは、ontap-s3-credentials という名前のONTAP S3 ユーザー認証情報を持つシークレットが作成されます。



Project: openshift-adp ▼

Edit key/value secret

Key/value secrets let you inject sensitive data into your application as files or environment variables.

Secret name *

ontap-s3-credentials

Unique name of the new secret.

Key *

cloud

Value

Browse...

Drag and drop file with your value here or browse to upload it.

```
[default]
aws_access_key_id=
aws_secret_access_key=
```

+ Add key/value

Save Cancel

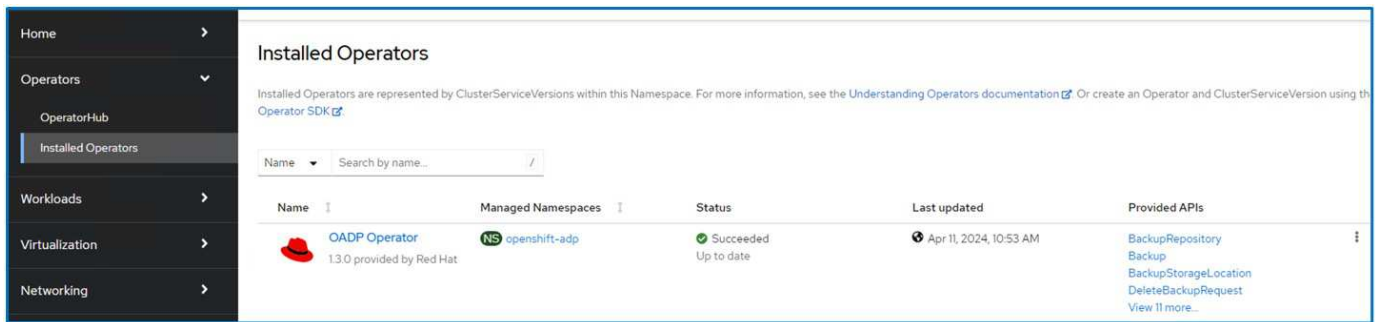
CLI から sg-s3-credentials という名前のシークレットを作成するには、次のコマンドを使用できます。

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt
```

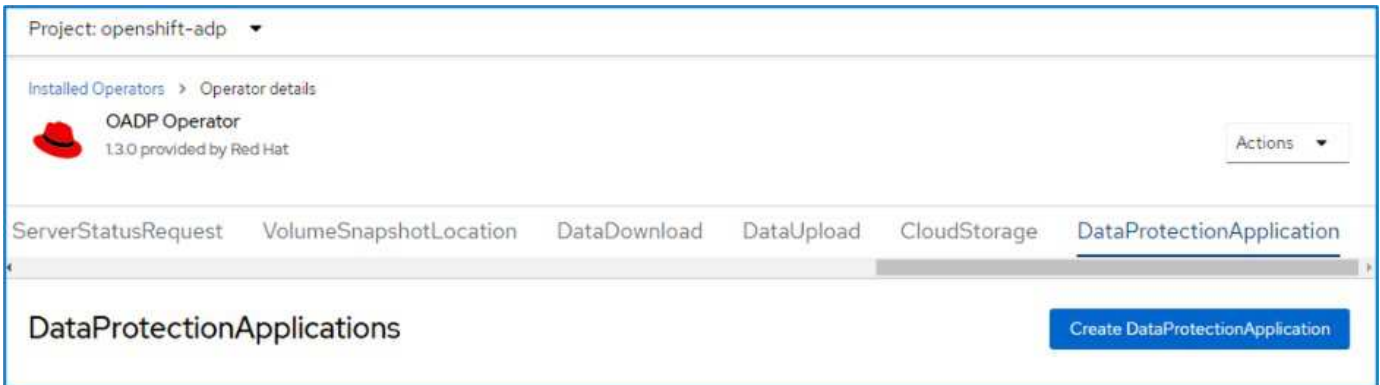
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3 user in the following format:

```
[default]
aws_access_key_id=< Access Key ID of S3 user>
aws_secret_access_key=<Secret Access key of S3 user>
```

- 次に、Velero を構成するには、[Operators] の下のメニュー項目から [Installed Operators] を選択し、[OADP Operator] をクリックして、[DataProtectionApplication] タブを選択します。



「DataProtectionApplication の作成」をクリックします。フォーム ビューで、DataProtection アプリケーションの名前を入力するか、既定の名前を使用します。



次に、YAML ビューに移動し、以下の yaml ファイルの例に示すように仕様情報を置き換えます。

- ONTAP S3 をバックアップ場所として Velero を構成するためのサンプル yaml ファイル**

```

spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'True' ->This allows use of IP in s3URL
          s3Url: 'https://10.xx.xx.xx' ->LIF to access S3. Ensure TLS
certificate for S3 is configured
          credential:
            key: cloud
            name: ontap-s3-credentials ->previously created secret
          default: true
          objectStorage:
            bucket: velero ->Your bucket name previously created in S3 for
backups
            prefix: demobackup ->The folder that will be created in the
bucket
            provider: aws
          configuration:
            nodeAgent:
              enable: true
              uploaderType: kopia
              #default Data Mover uses Kopia to move snapshots to Object Storage
            velero:
              defaultPlugins:
                - csi ->Add this plugin
                - openshift
                - aws
                - kubevirt ->Add this plugin

```

StorageGrid S3 をバックアップロケーションおよびスナップショットロケーションとして **Velero** を構成するためのサンプル **yaml** ファイル

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
          key: cloud
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

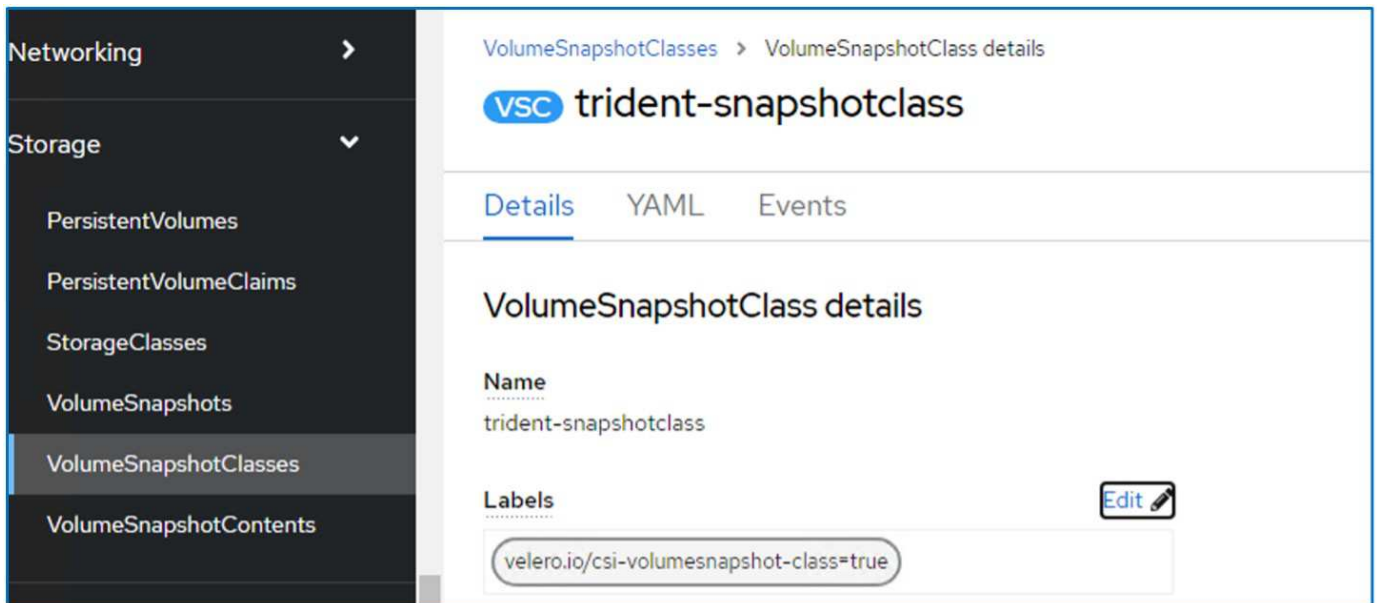
yaml ファイルの spec セクションは、上記の例と同様に、次のパラメータに対して適切に構成する必要があります。

backupLocations ONTAP S3 または StorageGrid S3 (yaml に示されている認証情報とその他の情報を含む) が、velero のデフォルトの BackupLocation として設定されています。

snapshotLocations Container Storage Interface (CSI) スナップショットを使用する場合は、CSI ドライバーを登録するために VolumeSnapshotClass CR を作成するため、スナップショットの場所を指定する必要はありません。この例では、Trident CSI を使用し、以前に Trident CSI ドライバーを使用して VolumeSnapShotClass CR を作成しました。

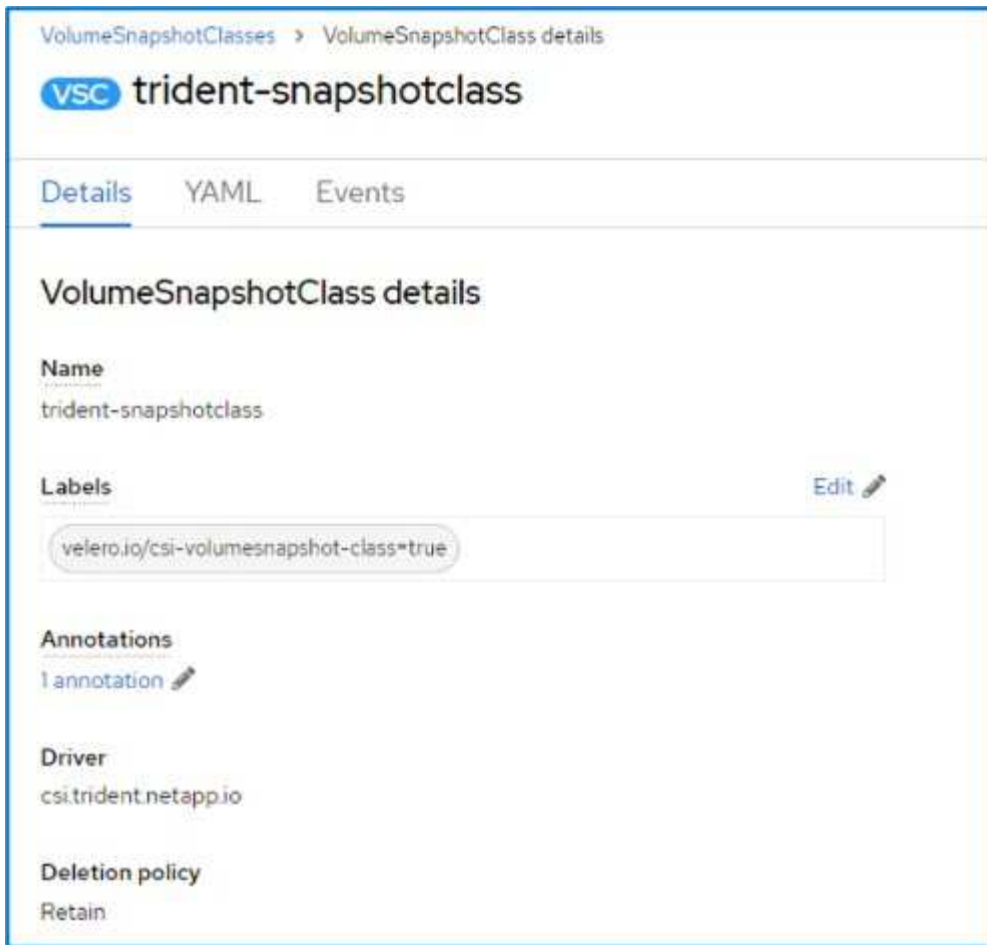
CSI プラグインを有効にする CSI スナップショットを使用して永続ボリュームをバックアップするには、Velero の defaultPlugins に csi を追加します。Velero CSI プラグインは、CSI でバックアップされた PVC をバックアップするために、**velero.io/csi-volumesnapshot-class** ラベルが設定されたクラスター内の VolumeSnapshotClass を選択します。このために

- trident VolumeSnapshotClass を作成する必要があります。
- trident-snapshotclass のラベルを編集し、以下に示すように **velero.io/csi-volumesnapshot-class=true** に設定します。

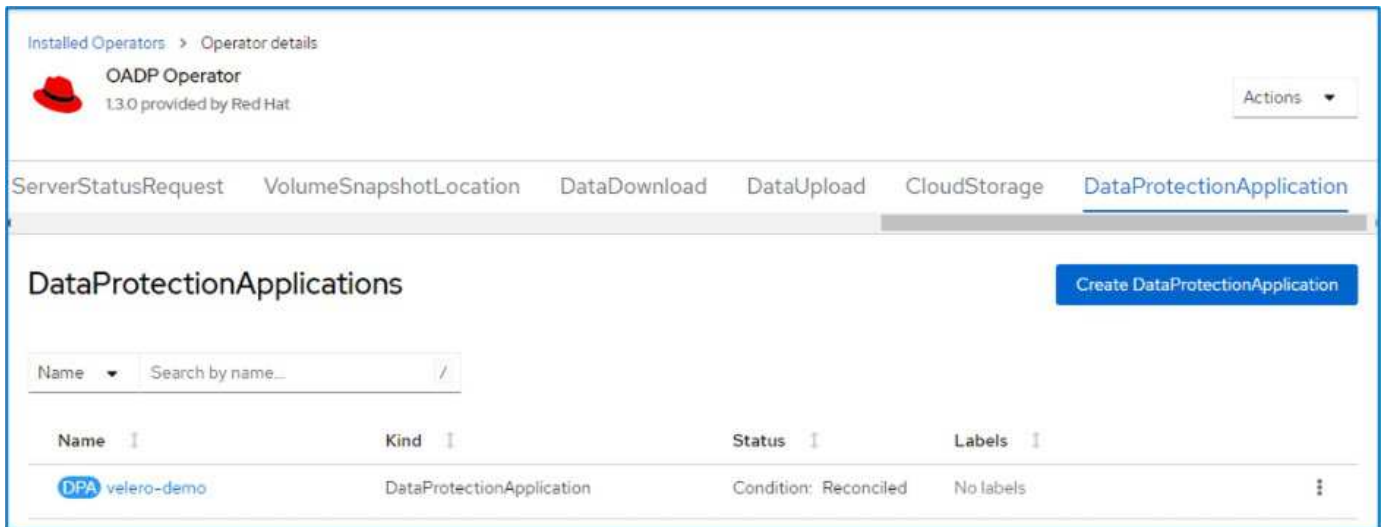


VolumeSnapshot オブジェクトが削除された場合でもスナップショットが保持されることを確認します。これは、**deletionPolicy** を Retain に設定することで実行できます。そうでない場合、名前空間を削除すると、そこにバックアップされたすべての PVC が完全に失われます。

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



DataProtectionApplication が作成され、状態が Reconciled であることを確認します。



OADP オペレータは対応する BackupStorageLocation を作成します。これはバックアップの作成時に使用されます。

Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat

Actions ▾

Repository Backup BackupStorageLocation DeleteBackupRequest DownloadRequest PodVolumeBackup PodVolumeRecovery

BackupStorageLocations

Create BackupStorageLocation

Name ▾ Search by name... /

Name ▴ ▾	Kind ▴ ▾	Status ▴ ▾	Labels ▴ ▾
 velero-demo-1	BackupStorageLocation	Phase: Available	app.kubernetes.io/component=bsl app.kubernetes.io/instance=velero-demo-1 app.kubernetes.io/managed-by=oadp-operator app.kubernetes.io/name=oadp-operator-velero openshift.io/oadp=True openshift.io/oadp-registry=True

Velero を使用して Red Hat OpenShift Virtualization の VM の オンデマンド バックアップを作成する

Velero と NetApp ONTAP S3 または StorageGRID を使用して OpenShift Virtualization で VM をバックアップします。この手順には、オンデマンド バックアップ用のバックアップ カスタム リソース (CR) と、スケジュールされたバックアップ用のスケジュール CR の作成が含まれます。各バックアップは VM メタデータと永続ボリュームをキャプチャし、リカバリまたはコンプライアンスの目的で指定されたオブジェクト ストレージの場所に保存します。

VM のバックアップを作成する手順

VM 全体 (VM メタデータと VM ディスク) のオンデマンド バックアップを作成するには、[バックアップ] タブをクリックします。これにより、バックアップ カスタム リソース (CR) が作成されます。バックアップ CR を作成するためのサンプル yamI が提供されています。この yamI を使用すると、指定された名前空間内の VM とそのディスクがバックアップされます。追加のパラメータは、["ドキュメント"](#)。

ディスクをバックアップする永続ボリュームのスナップショットは、CSI によって作成されます。VM のバックアップとそのディスクのスナップショットが作成され、yamI で指定されたバックアップの場所に保存されます。バックアップは、TTL で指定されたとおり 30 日間システム内に残ります。

```

apiVersion: velero.io/v1
kind: Backup
metadata:
  name: backup1
  namespace: openshift-adp
spec:
  includedNamespaces:
  - virtual-machines-demo
  snapshotVolumes: true
  storageLocation: velero-demo-1 -->this is the backupStorageLocation
  previously created
                                when Velero is configured.

  ttl: 720h0m0s

```

バックアップが完了すると、そのフェーズは完了として表示されます。

The screenshot shows the Velero web console interface. At the top, it says 'Project: openshift-adp'. Below that, there's a section for 'Installed Operators' with 'OADP Operator 13.0 provided by Red Hat'. The main navigation bar includes 'Details', 'YAML', 'Subscription', 'Events', 'All instances', 'BackupRepository', 'Backup' (which is selected), 'BackupStorageLocation', and 'DeleteBa'. The 'Backups' section is active, showing a table with one backup entry: 'backup1' of kind 'Backup'. The status is 'Phase: Completed' with a green checkmark. The label 'velero.io/storage-location=velero-demo-1' is also visible. A 'Create Backup' button is in the top right of the backups section.

S3 ブラウザ アプリケーションを使用して、オブジェクトストレージ内のバックアップを検査できます。バックアップのパスは、プレフィックス名 (velero/demobackup) が付いた設定されたバケットに表示されます。バックアップの内容には、仮想マシンのボリューム スナップショット、ログ、その他のメタデータが含まれていることがわかります。



StorageGrid では、テナント マネージャーから利用できる S3 コンソールを使用してバックアップ オブジェクトを表示することもできます。

Path: / demobackup/ backups/ backup1/				
Name	Size	Type	Last Modified	Storage Class
backup1.tar.gz	230.36 KB	GZ File	4/15/2024 10:26:29 PM	STANDARD
velero-backup.json	3.35 KB	JSON File	4/15/2024 10:26:29 PM	STANDARD
backup1-resource-list.json.gz	1.12 KB	GZ File	4/15/2024 10:26:29 PM	STANDARD
backup1-itemoperations.json.gz	600 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-volumesnapshots.json.gz	29 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-podvolumebackups.json.gz	29 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-results.gz	49 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshotclasses.json.gz	426 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshotcontents.json.gz	1.43 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshots.json.gz	1.34 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-logs.gz	13.49 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD

OpenShift Virtualization で VM のスケジュールされたバックアップを作成する

スケジュールに従ってバックアップを作成するには、スケジュール CR を作成する必要があります。スケジュールは、バックアップを作成する時間を指定できる単純な Cron 式です。スケジュール CR を作成するためのサンプル yaml。

```

apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s

```

Cron 式 0 7 * * * は、毎日 7:00 にバックアップが作成されることを意味します。バックアップに含める名前空間とバックアップの保存場所も指定します。したがって、バックアップ CR の代わりに、スケジュール CR を使用して、指定された時間と頻度でバックアップを作成します。

スケジュールが作成されると、有効になります。

Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat

storageLocation DeleteBackupRequest DownloadRequest PodVolumeBackup PodVolumeRestore Restore Schedule

Schedules

Name ▾ Search by name... /

Name	Kind	Status	Labels
 schedule1	Schedule	Phase:  Enabled	No labels

バックアップはこのスケジュールに従って作成され、[バックアップ] タブから表示できます。

Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat

Events All instances BackupRepository Backup BackupStorageLocation DeleteBackupRequest DownloadRequest

Backups

Create Backup

Name ▾ Search by name... /

Name	Kind	Status	Labels
 schedule1-20240416140507	Backup	Phase: InProgress	velero.io/schedule-name=schedule1 velero.io/storage-location=velero-demo-1

Velero を使用して Red Hat OpenShift Virtualization のバックアップから VM を復元する

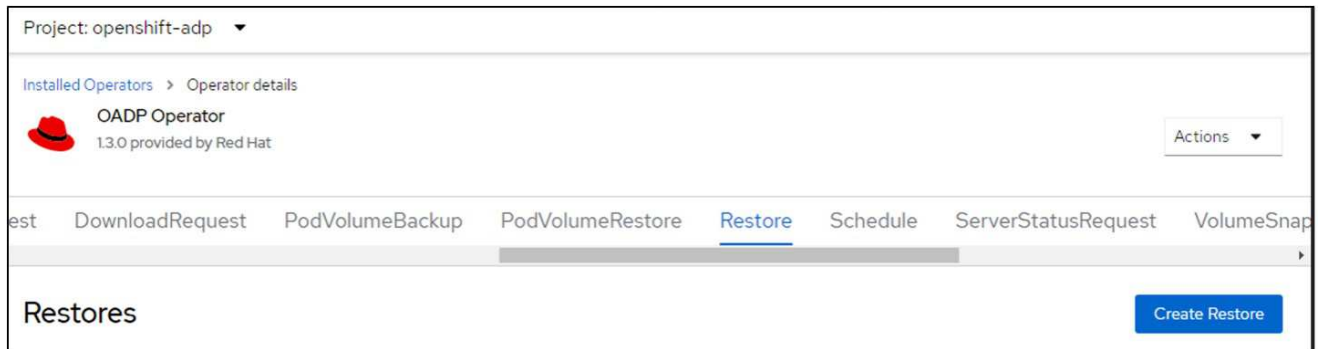
Velero と OpenShift API for Data Protection (OADP) を使用して、OpenShift Virtualization で VM を復元します。この手順には、元の名前空間、別の名前空間、または代替ストレージ クラスに復元するオプションを使用して、バックアップから VM とその永続ボリュームを回復するための復元カスタム リソース (CR) の作成が含まれます。

前提条件

バックアップから復元するには、仮想マシンが存在していた名前空間が誤って削除されたと仮定します。

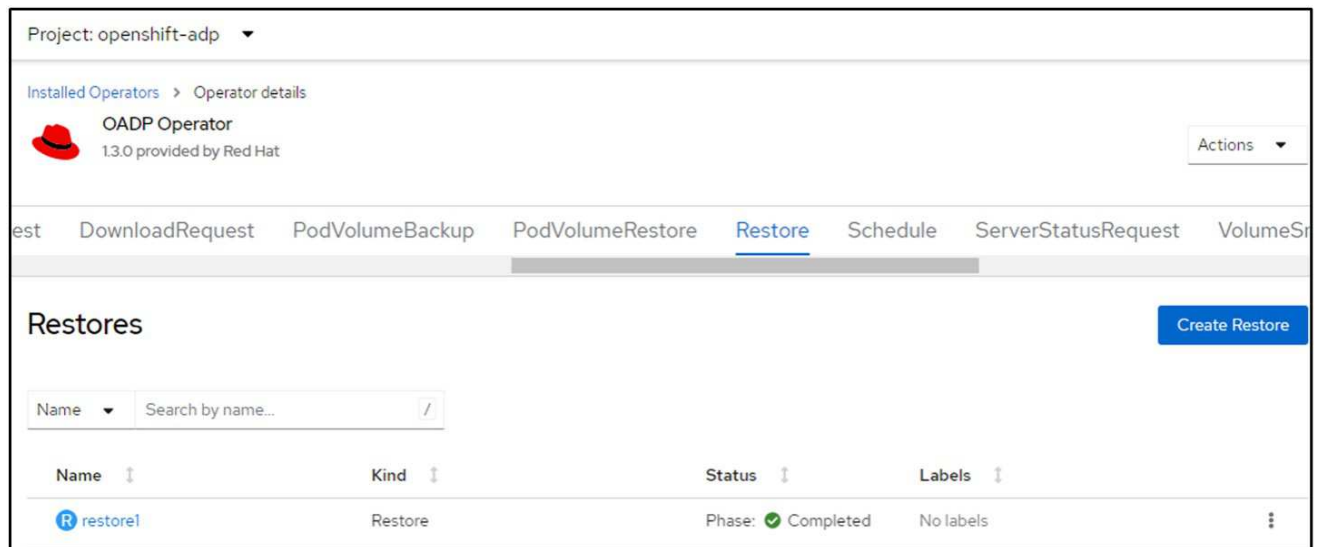
同じ名前空間に復元する

作成したバックアップから復元するには、復元カスタム リソース (CR) を作成する必要があります。名前を付け、復元元のバックアップの名前を指定して、restorePVs を true に設定する必要があります。追加のパラメータは、"**ドキュメント**"。「作成」ボタンをクリックします。



```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore1
  namespace: openshift-adp
spec:
  backupName: backup1
  restorePVs: true
```

フェーズが完了したことが表示されると、仮想マシンがスナップショットが作成された時点の状態に復元されたことがわかります。(VM の実行中にバックアップが作成された場合、バックアップから VM を復元すると、復元された VM が起動し、実行状態になります)。VM は同じ名前空間に復元されます。



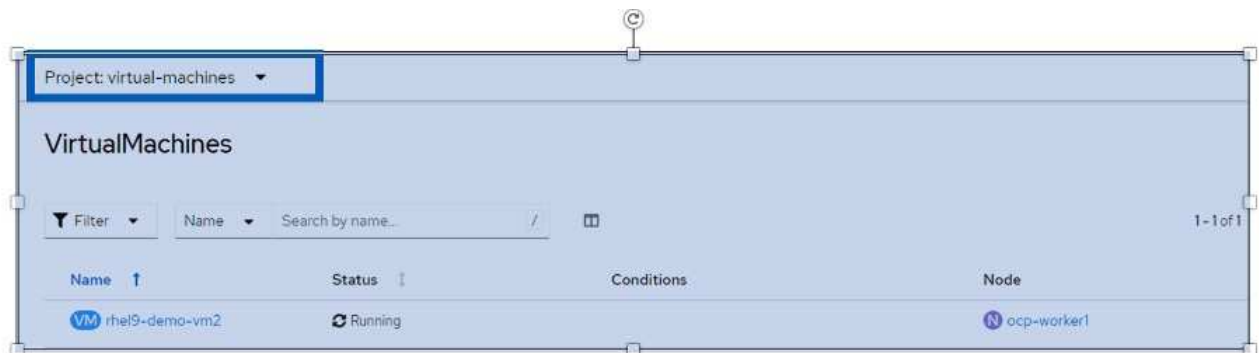
別の名前空間に復元する

VM を別の名前空間に復元するには、Restore CR の yaml 定義で namespaceMapping を指定できます。

次のサンプル yaml ファイルは、バックアップが virtual-machines 名前空間に取得されたときに、virtual-machines-demo 名前空間内の VM とそのディスクを復元するための Restore CR を作成します。

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup
  restorePVs: true
  includedNamespaces:
  - virtual-machines-demo
  namespaceMapping:
    virtual-machines-demo: virtual-machines
```

フェーズが完了したことが表示されると、仮想マシンがスナップショットが作成された時点の状態に復元されていることがわかります。(VM の実行中にバックアップが作成された場合、バックアップから VM を復元すると、復元された VM が起動し、実行状態になります)。VM は、yaml で指定された別の名前空間に復元されます。



別のストレージクラスに復元する

Velero は、json パッチを指定して復元中にリソースを変更する一般的な機能を提供します。リソースが復元される前に、json パッチが適用されます。json パッチは configmap で指定され、configmap は復元コマンドで参照されます。この機能を使用すると、異なるストレージ クラスを使用して復元できます。

以下の例では、仮想マシンは作成時に、ディスクのストレージ クラスとして ontap-nas を使用します。「backup1」という名前の仮想マシンのバックアップが作成されます。

The screenshot shows the 'VirtualMachine details' page for 'rhel9-demo-vm1' in the 'virtual-machines-demo' project. The 'Configuration' tab is selected, and the 'Disks' section is expanded. A table lists the disks:

Name	Source	Size	Drive	Interface	Storage class
cloudinitdisk	Other	-	Disk	virtio	-
disk1	PVC rhel9-demo-vm1-disk1	31.75 GiB	Disk	virtio	ontap-nas
rootdisk	PVC rhel9-demo-vm1	31.75 GiB	Disk	virtio	ontap-nas

The screenshot shows the 'Backup' tab in the 'Operator details' page for 'OADP Operator' in the 'openshift-adp' project. A table lists the backups:

Name	Kind	Status
backup1	Backup	Phase: Completed

VM を削除して VM の損失をシミュレートします。

別のストレージ クラス (ontap-nas-eco ストレージ クラスなど) を使用して VM を復元するには、次の 2 つの手順を実行する必要があります。

ステップ1

次のように、openshift-adp 名前空間に構成マップ (コンソール) を作成します。スクリーンショットに示すように詳細を入力します。名前空間を選択: openshift-adp 名前: change-storage-class-config (任意の名前にすることができます) キー: change-storage-class-config.yaml 値:

```

version: v1
resourceModifierRules:
- conditions:
    groupResource: persistentvolumeclaims
    resourceNameRegex: "^rhel*"
    namespaces:
    - virtual-machines-demo
patches:
- operation: replace
  path: "/spec/storageClassName"
  value: "ontap-nas-eco"

```

Project: openshift-adp

Edit ConfigMap

Config maps hold key-value pairs that can be used in pods to read application configuration.

Configure via: ☒ Form view ☐ YAML view

Name *

change-storage-class-config

A unique name for the ConfigMap within the project

☐ Immutable

Immutable, if set to true, ensures that data stored in the ConfigMap cannot be updated

Data

Data contains the configuration data that is in UTF-8 range

[Remove key/value](#)

Key *

change-storage-class-config.yaml

Value

[Browse...](#)

Drag and drop file with your value here or browse to upload it.

```

version: v1
resourceModifierRules:
- conditions:
    groupResource: persistentvolumeclaims
    resourceNameRegex: "^rhel*"
    namespaces:
    - virtual-machines-demo

```

[Add key/value](#)

結果の構成マップ オブジェクトは次のようになります (CLI)。

```
# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:          change-storage-class-config
Namespace:     openshift-adp
Labels:        velero.io/change-storage-class=RestoreItemAction
                velero.io/plugin-config=
Annotations:   <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
    groupResource: persistentvolumeclaims
    resourceNameRegex: "^rhel*"
    namespaces:
    - virtual-machines-demo
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"

BinaryData
====

Events:   <none>
```

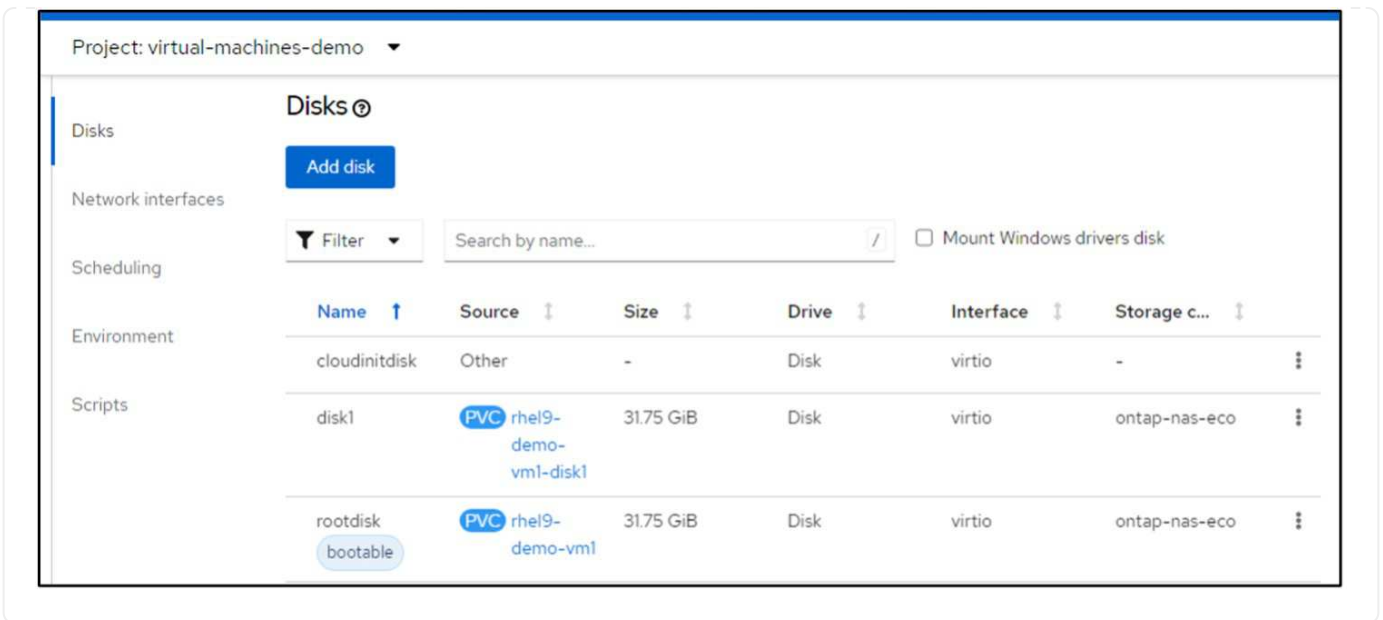
この構成マップは、復元の作成時にリソース修飾子ルールを適用します。rhel で始まるすべての永続ボリューム要求のストレージ クラス名を ontap-nas-eco に置き換えるパッチが適用されます。

ステップ2

VM を復元するには、Velero CLI から次のコマンドを使用します。

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

VM は、ストレージ クラス ontap-nas-eco を使用して作成されたディスクと同じ名前空間に復元されます。



Velero を使用して Red Hat OpenShift Virtualization でバックアップ CR を削除または復元する

Velero を使用して OpenShift Virtualization 内の VM のバックアップおよび復元リソースを削除します。OpenShift CLI を使用してオブジェクト ストレージ データを保持したままバックアップを削除するか、Velero CLI を使用してバックアップ カスタム リソース (CR) と関連するストレージ データの両方を削除します。

バックアップの削除

OC CLI ツールを使用して、オブジェクト ストレージ データを削除せずにバックアップ CR を削除できます。

```
oc delete backup <backup_CR_name> -n <velero_namespace>
```

バックアップ CR を削除し、関連するオブジェクト ストレージ データを削除する場合は、Velero CLI ツールを使用して実行できます。

指示に従ってCLIをダウンロードしてください。"[Velero ドキュメント](#)"。

Velero CLIを使用して次の削除コマンドを実行します。

```
velero backup delete <backup_CR_name> -n <velero_namespace>
```

復元の削除

Velero CLIを使用してRestore CRを削除できます。

```
velero restore delete restore --namespace openshift-adp
```

復元CRを削除するには、OCコマンドとUIを使用できます。

```
oc delete backup <backup_CR_name> -n <velero_namespace>
```

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。