使用第三方工具保護數據

NetApp virtualization solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/netapp-solutions-virtualization/openshift/osv-vm-dp-using-velero-overview.html on August 18, 2025. Always check docs.netapp.com for the latest.

目錄

使用第三方工具保護數據 1
了解如何使用 OpenShift API for Data Protection (OADP) 對 Red Hat OpenShift Virtualization 中的虛擬機器進行資料保護 1
安裝 Red Hat OpenShift API for Data Protection (OADP) 操作員 2
先決條件 3
安裝 OADP Operator 的步驟 3
使用 Velero 為 Red Hat OpenShift Virtualization 中的虛擬機器建立隨選備份 12
建立虛擬機器備份的步驟 12
在 OpenShift 虛擬化中為虛擬機器建立排程備份 14
使用 Velero 從 Red Hat OpenShift Virtualization 中的備份還原虛擬機 15
先決條件 15
使用 Velero 在 Red Hat OpenShift Virtualization 中刪除備份 CR 或還原 CR 21
刪除備份 21
刪除恢復 21

使用第三方工具保護數據

了解如何使用 OpenShift API for Data Protection (OADP) 對 Red Hat OpenShift Virtualization 中的虛擬機器進行資料保護

帶有 Velero 的 OpenShift API for Data Protection (OADP) 為 OpenShift Virtualization 中的虛擬機器提供備份、復原和災難復原功能。使用Trident CSI 快照將持久磁碟區和 VM 元資料備份到NetApp ONTAP S3 或StorageGRID S3。 OADP 與 Velero API 和 CSI 儲存驅動程式集成，以管理容器化虛擬機器的資料保護操作。

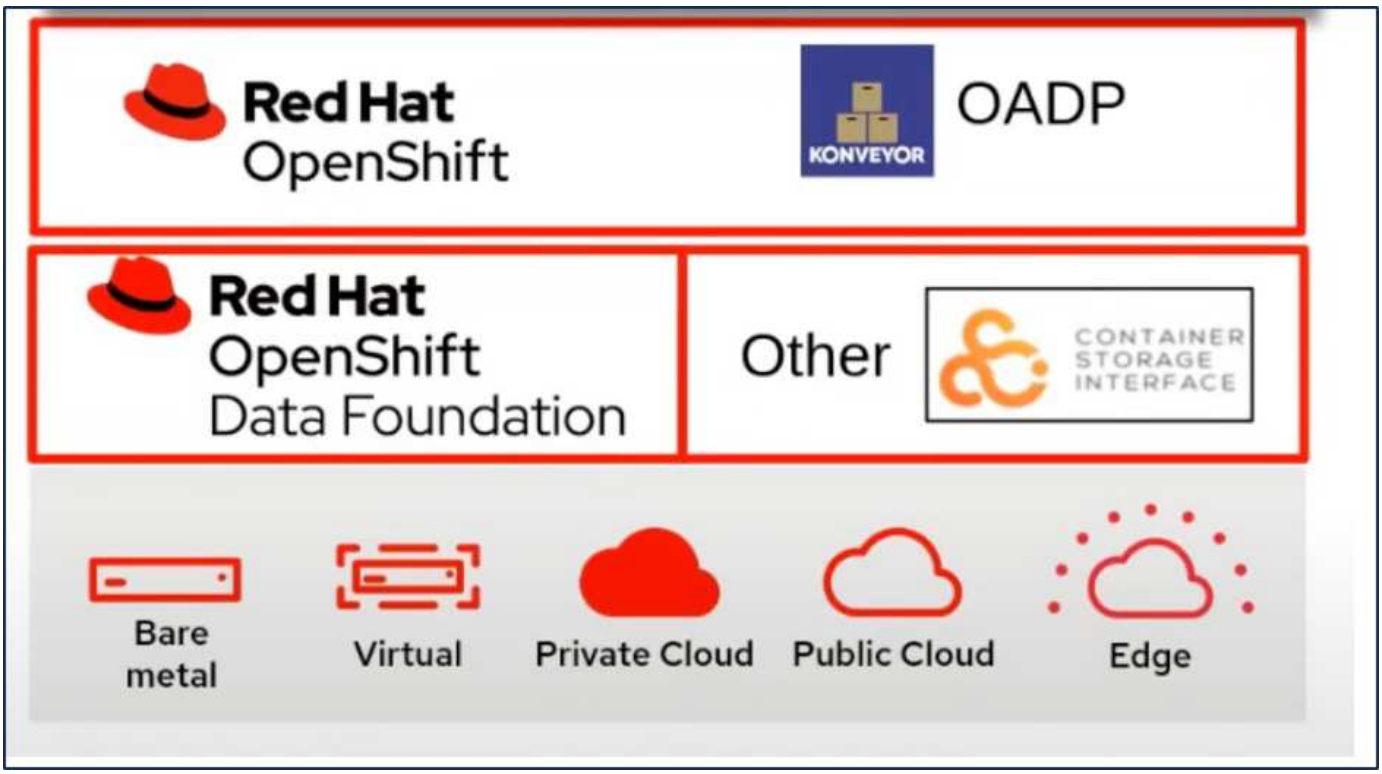
OpenShift 虛擬化環境中的虛擬機器是在 OpenShift 容器平台的工作節點中執行的容器化應用程式。保護虛擬機器元資料以及虛擬機器的持久性磁碟非常重要，以便在它們遺失或損壞時可以還原它們。

OpenShift 虛擬化虛擬機器的持久性磁碟可以透過使用整合到 OpenShift 叢集的ONTAP儲存進行支援"Trident犯罪現場調查"。在本節中我們使用"OpenShift 資料保護 API (OADP)"執行虛擬機器（包括其資料卷）的備份

- ONTAP物件存儲
- 儲存網格

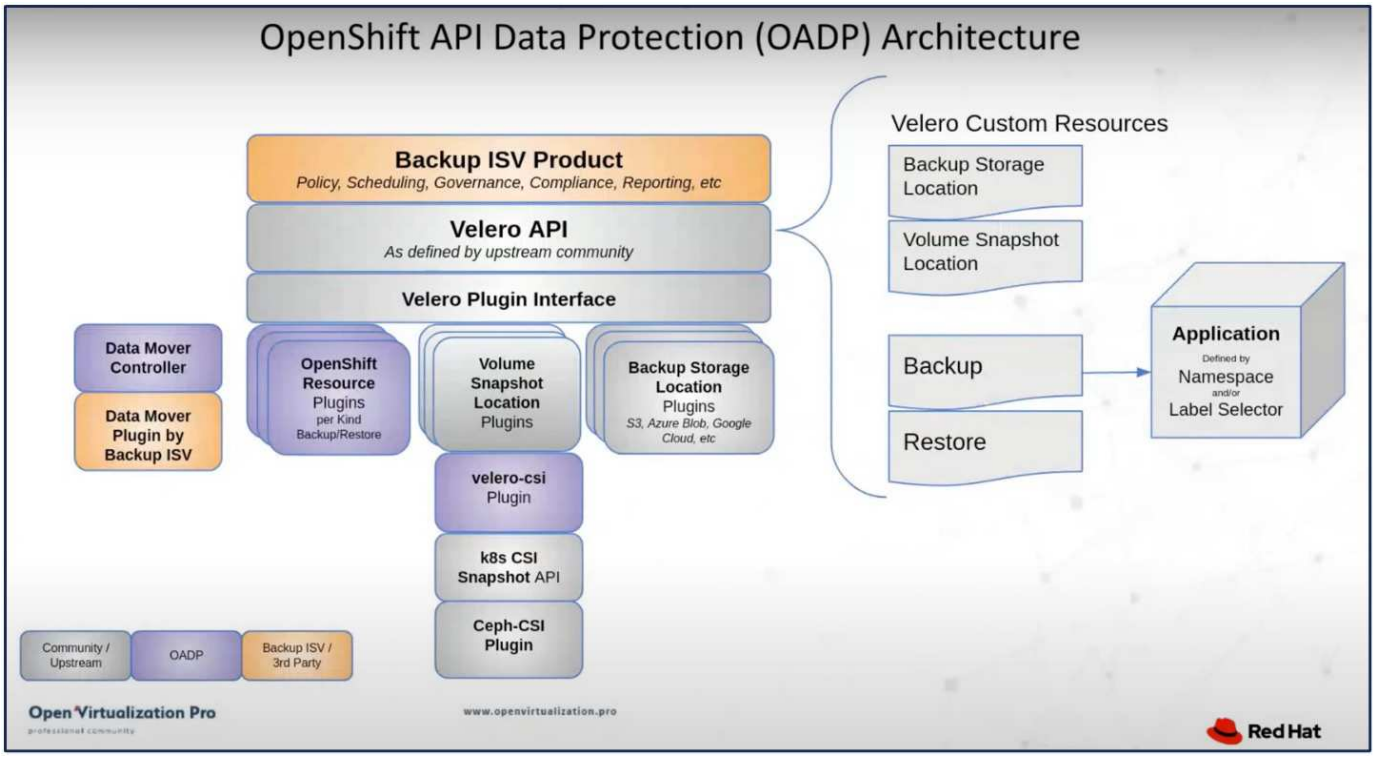
然後我們在需要時從備份中恢復。

OADP 支援 OpenShift 叢集上應用程式的備份、還原和災難復原。可以使用 OADP 保護的資料包括 Kubernetes 資源物件、持久磁碟區和內部映像。



Red Hat OpenShift 利用開源社群開發的解決方案來保護資料。"維萊羅"是一個開源工具，用於安全地備份和復原、執行災難復原以及遷移 Kubernetes 叢集資源和持久磁碟區。為了輕鬆使用 Velero，OpenShift 開發了 OADP 操作符和 Velero 插件以與 CSI 儲存驅動程式整合。所公開的 OADP API 的核心是基於 Velero API。安裝

OADP 操作器並配置後，可以執行的備份/復原作業是基於 Velero API 公開的操作。



OADP 1.3 可從 OpenShift 叢集 4.12 及更高版本的操作員中心取得。它有一個內建的資料移動器，可以將 CSI 磁碟區快照移至遠端物件儲存。透過在備份期間將快照移至物件儲存位置，這提供了可移植性和耐用性。災難發生後，快照可用於復原。

以下是本節範例所使用的各個元件的版本

- OpenShift 叢集 4.14
- 透過 Operator 安裝的 OpenShift VirtualizationRed Hat 提供的 OpenShift Virtualization Operator
- Red Hat 提供的 OADP Operator 1.13
- 適用於 Linux 的 Velero CLI 1.13
- Trident24.02
- ONTAP 9.12

"Trident犯罪現場調查" "OpenShift 資料保護 API (OADP)" "維萊羅"

安裝 Red Hat OpenShift API for Data Protection (OADP) 操作員

安裝 OpenShift API for Data Protection (OADP) Operator 以啟用 OpenShift Virtualization 中虛擬機器的備份和復原功能。此過程包括從 OpenShift Operator Hub 部署 OADP Operator、配置 Velero 以使用NetApp ONTAP S3 或StorageGRID作為備份目標，以及設定必要的機密和備份位置。

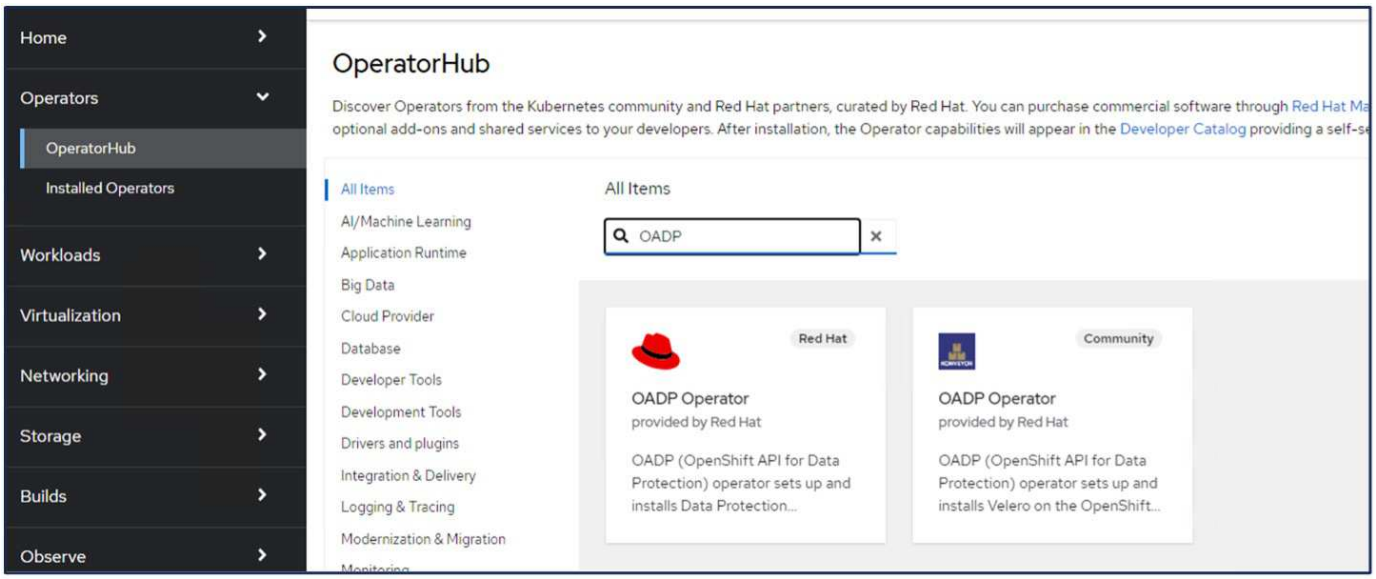
先決條件

- 安裝在裸機基礎架構上並帶有 RHCOS 工作節點的 Red Hat OpenShift 叢集（高於 4.12 版本）
- 使用Trident與叢集整合的NetApp ONTAP叢集
- 在ONTAP叢集上設定了 SVM 的Trident後端
- 在 OpenShift 叢集上設定 StorageClass，並使用Trident作為配置器
- 在叢集上建立的Trident Snapshot 類
- 叢集管理員存取 Red Hat OpenShift 叢集
- NetApp ONTAP叢集的管理員存取權限
- OpenShift 虛擬化操作員已安裝並配置
- 在 OpenShift 虛擬化的命名空間中部署的虛擬機
- 安裝了 tridentctl 和 oc 工具並新增至 $PATH 的管理員工作站

> ⓘ 如果您想在虛擬機器處於運作狀態時對其進行備份，則必須在該虛擬機器上安裝 QEMU 客戶代理程式。如果您使用現有範本安裝 VM，則會自動安裝 QEMU 代理程式。 QEMU 允許客戶代理在快照過程中使客戶作業系統中的動態資料靜止，並避免可能的資料損壞。如果您沒有安裝 QEMU，您可以在備份之前停止虛擬機器。

安裝 **OADP Operator** 的步驟

1. 進入叢集的 Operator Hub，選擇 Red Hat OADP 操作員。在安裝頁面中，使用所有預設選擇並按一下安裝。在下一頁上，再次使用所有預設設定並點擊“安裝”。OADP 操作員將安裝在命名空間 openshift-adp 中。



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	NS openshift-cnv	NS openshift-cnv	Succeeded Up to date
OADP Operator 1.3.0 provided by Red Hat	NS openshift-adp	NS openshift-adp	Succeeded Up to date
Package Server 0.0.1-snapshot provided by	NS openshift-operator-lifecycle-manager	NS openshift-operator-lifecycle-manager	Succeeded

使用 **Ontap S3** 詳細資訊進行 **Velero** 配置的先決條件

操作員安裝成功後，配置Velero的實例。Velero 可以配置為使用 S3 相容的物件儲存。使用所示步驟設定ONTAP S3"ONTAP文件的物件儲存管理部分" 。您將需要ONTAP S3 配置中的以下資訊才能與 Velero 整合。

- 可用於存取 S3 的邏輯介面 (LIF)
- 存取 S3 的使用者憑證，包括存取金鑰和秘密存取金鑰
- S3 中用於備份的儲存桶名稱，具有使用者存取權限
- 為了安全存取物件存儲，應在物件儲存伺服器上安裝 TLS 憑證。

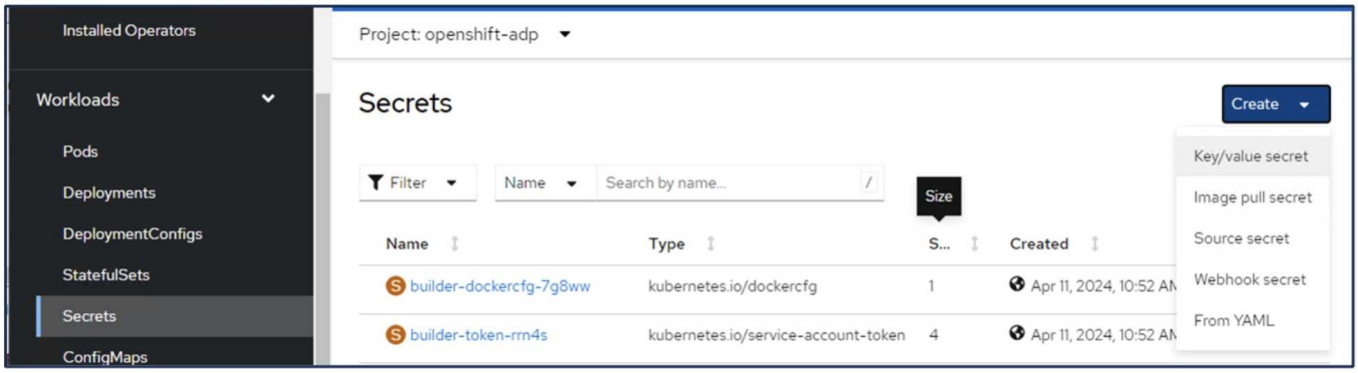
使用 **StorageGrid S3** 詳細資訊進行 **Velero** 配置的先決條件

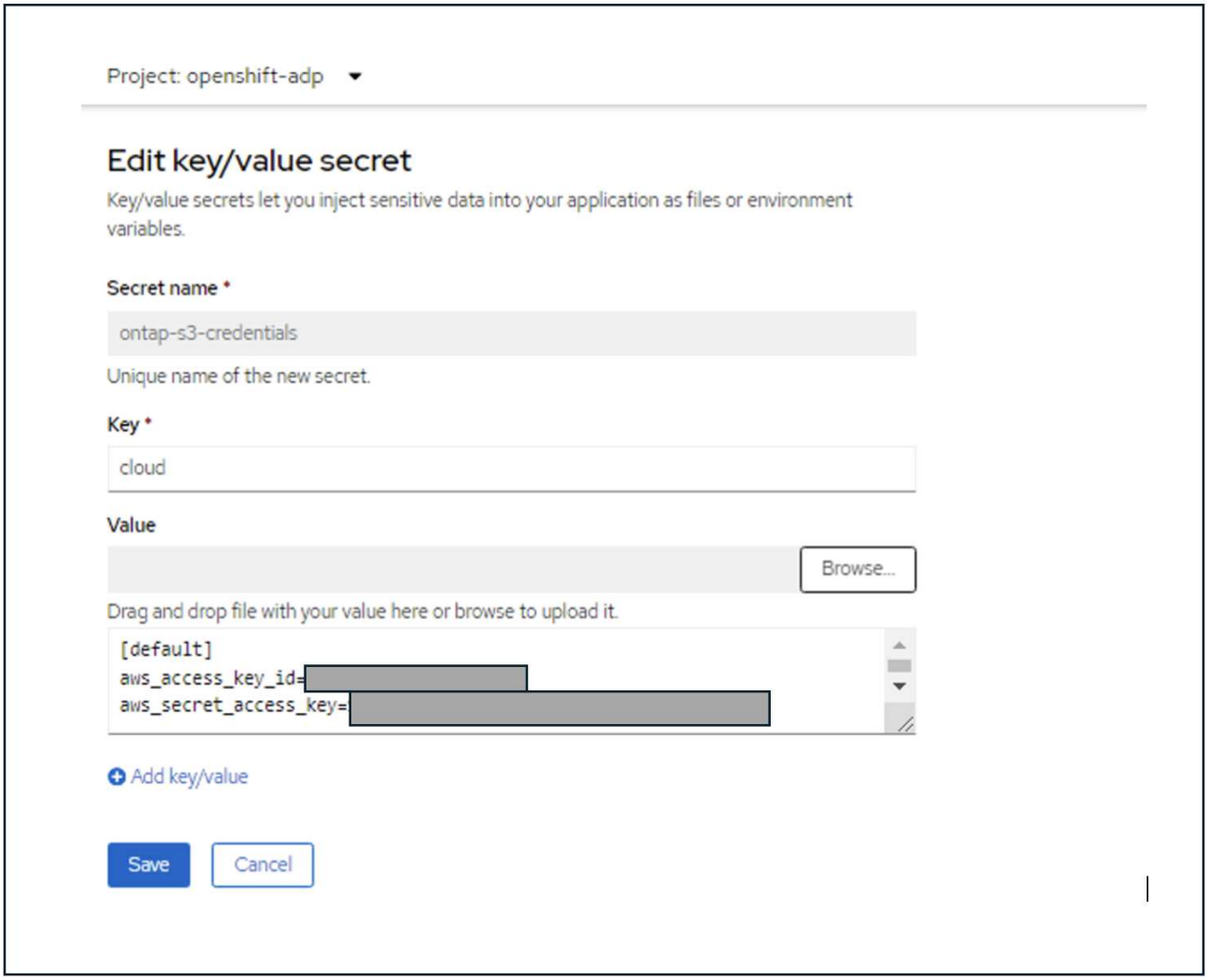
Velero 可以配置為使用 S3 相容的物件儲存。您可以使用以下所示的步驟來配置 StorageGrid S3"StorageGrid 文檔" 。您將需要 StorageGrid S3 配置中的以下資訊才能與 Velero 整合。

- 可用於存取 S3 的端點
- 存取 S3 的使用者憑證，包括存取金鑰和秘密存取金鑰
- S3 中用於備份的儲存桶名稱，具有使用者存取權限
- 為了安全存取物件存儲，應在物件儲存伺服器上安裝 TLS 憑證。

配置 **Velero** 的步驟

- 首先，為ONTAP S3 使用者憑證或 StorageGrid Tenant 使用者憑證建立一個金鑰。這將用於稍後配置 Velero。您可以從 CLI 或 Web 控制台建立機密。若要從 Web 控制台建立金鑰，請選擇“金鑰”，然後按一下“鍵/值金鑰”。提供憑證名稱、金鑰和值的值，如下所示。請務必使用您的 S3 使用者的存取金鑰 ID 和秘密存取金鑰。為秘密指定一個合適的名稱。在下面的範例中，建立了一個名為 ontap-s3-credentials 的具有ONTAP S3 使用者憑證的金鑰。

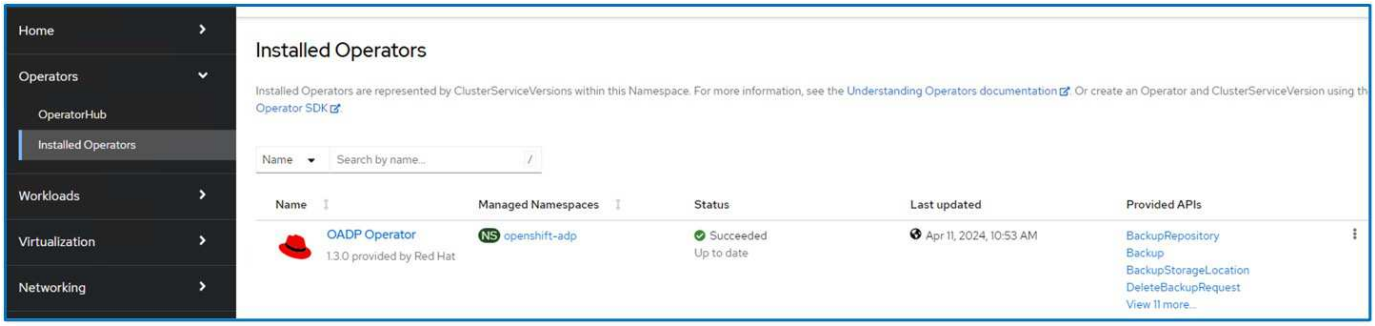




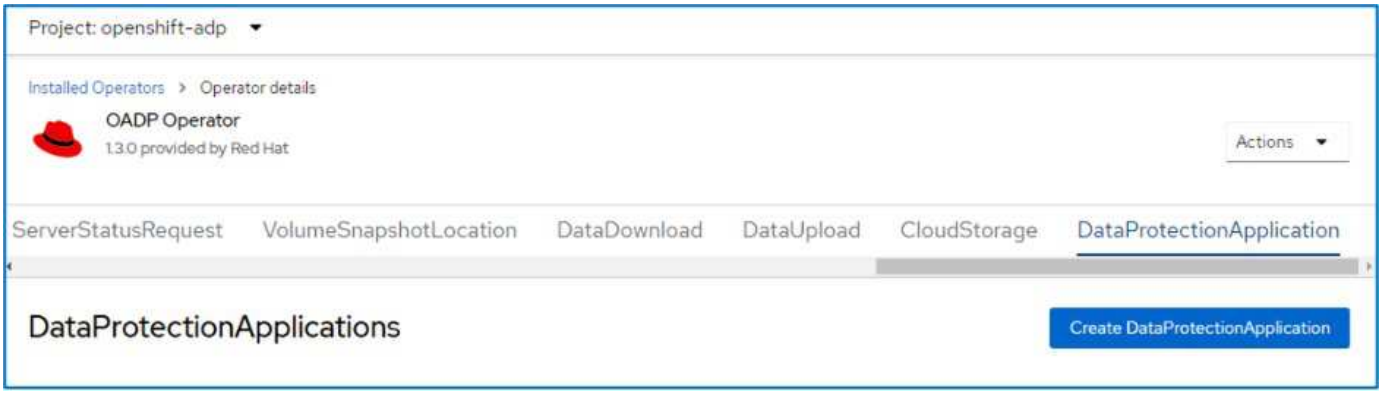
若要從 CLI 建立名為 sg-s3-credentials 的金鑰，您可以使用下列命令。

```
# 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>
```

- 接下來，要設定 Velero，請從 Operators 下的選單項目中選擇 Installed Operators，按一下 OADP Operator，然後選擇 DataProtectionApplication 標籤。



按一下建立 DataProtectionApplication。在表單檢視中，為資料保護應用程式提供一個名稱或使用預設名稱。



現在轉到 YAML 視圖並取代規範訊息，如下面的 yaml 檔案範例所示。

使用**ONTAP S3** 作為備份位置配置 **Velero** 的範例 **yaml** 檔案

```
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
```

使用 **StorageGrid S3** 作為備份位置和快照位置來配置 **Velero** 的範例 **yaml** 檔案

```
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
```

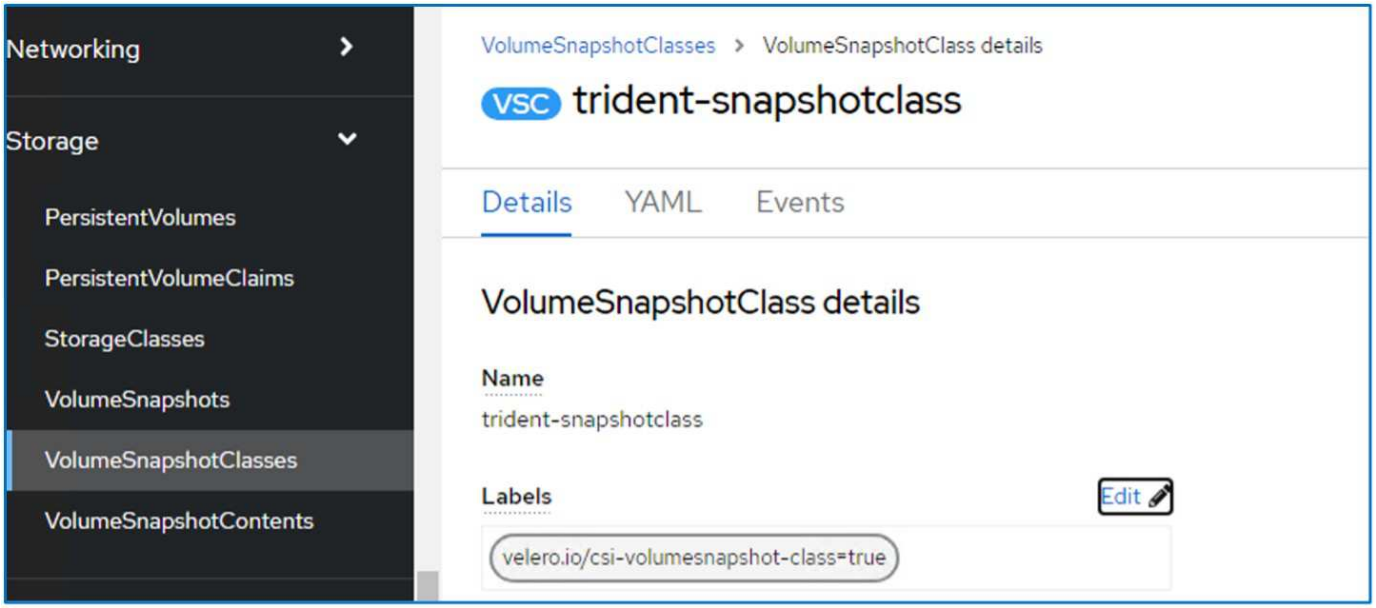
yaml 檔案中的 spec 部分應針對類似上述範例的下列參數進行適當配置

backupLocations ONTAP S3 或 StorageGrid S3（其憑證和其他資訊如 yaml 所示）配置為 velero 的預設 BackupLocation。

snapshotLocations 如果您使用容器儲存介面 (CSI) 快照，則無需指定快照位置，因為您將建立 VolumeSnapshotClass CR 來註冊 CSI 驅動程式。在我們的範例中，您使用Trident CSI，並且先前已使用Trident CSI 驅動程式建立了 VolumeSnapShotClass CR。

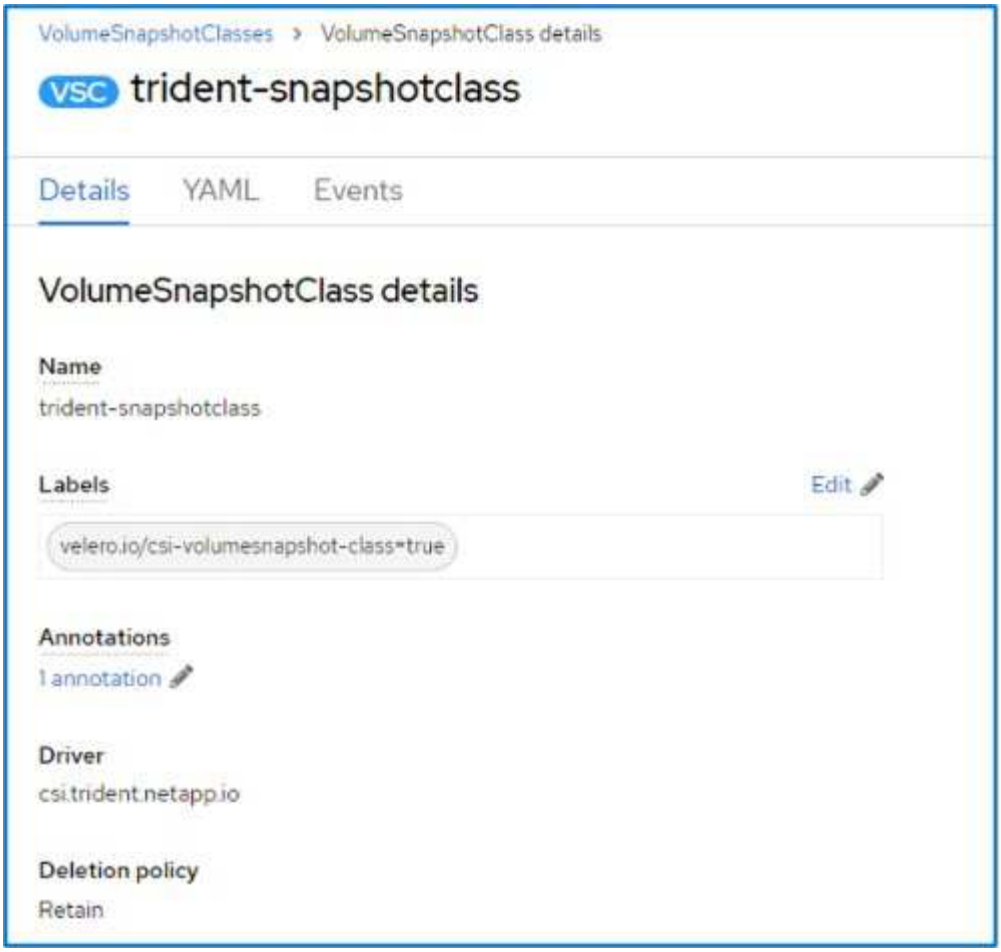
啟用 **CSI** 插件 將 csi 新增至 Velero 的預設插件中，以使用 CSI 快照備份持久性磁碟區。Velero CSI 外掛程式用於備份 CSI 支援的 PVC，它將選擇叢集中設定了 **velero.io/csi-volumesnapshot-class** 標籤的 VolumeSnapshotClass。為了這

- 您必須建立 trident VolumeSnapshotClass。
- 編輯 trident-snapshotclass 的標籤，並將其設定為 **velero.io/csi-volumesnapshot-class=true**，如下所示。

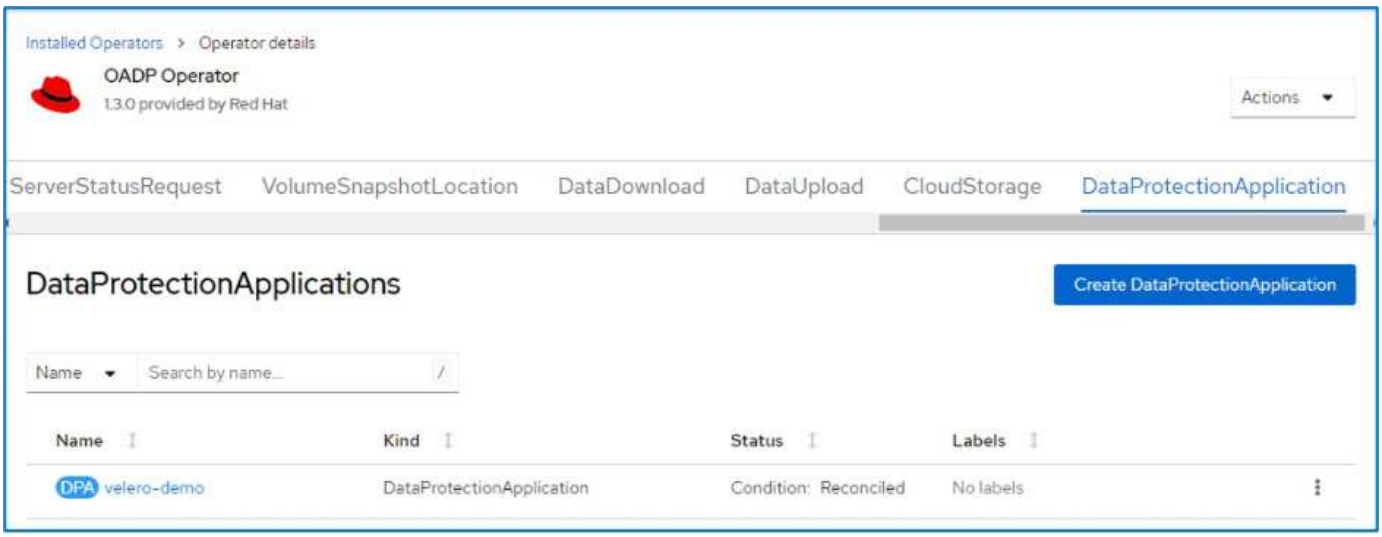


確保即使 VolumeSnapshot 物件被刪除，快照也能保留。這可以透過將 **deletionPolicy** 設為 Retain 來實現。如果不是，刪除命名空間將完全遺失其中備份的所有 PVC。

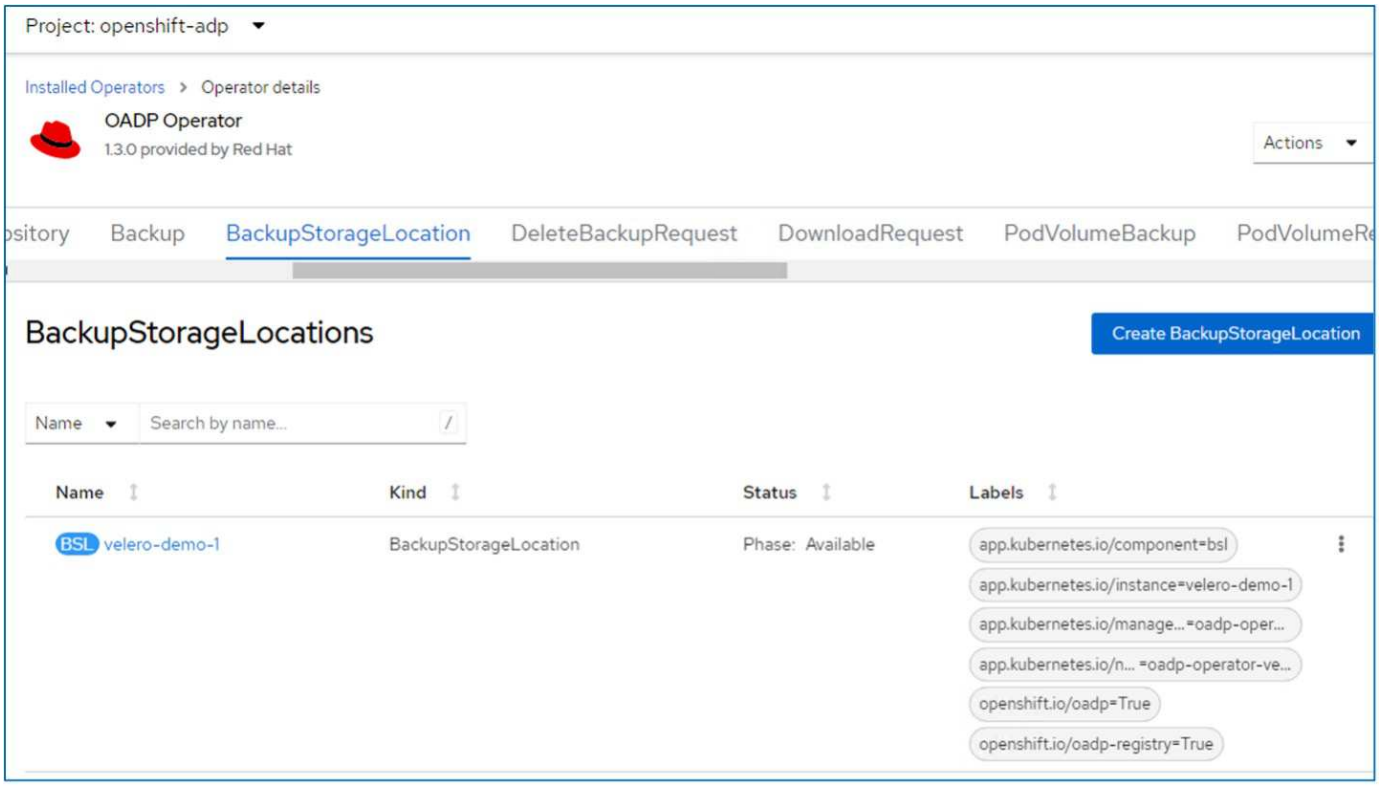
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



確保 DataProtectionApplication 已建立並且處於「狀態：Reconciled」。



OADP 操作員將建立對應的 BackupStorageLocation。這將在建立備份時使用。



使用 Velero 為 Red Hat OpenShift Virtualization 中的虛擬機器建立隨選備份

使用 Velero 和NetApp ONTAP S3 或StorageGRID在 OpenShift Virtualization 中備份虛擬機器。此過程包括為按需備份建立備份自訂資源 (CR) 和為計劃備份建立計劃 CR。每個備份都會擷取虛擬機器元資料和持久性卷，並將它們儲存在指定的物件儲存位置以用於復原或合規目的。

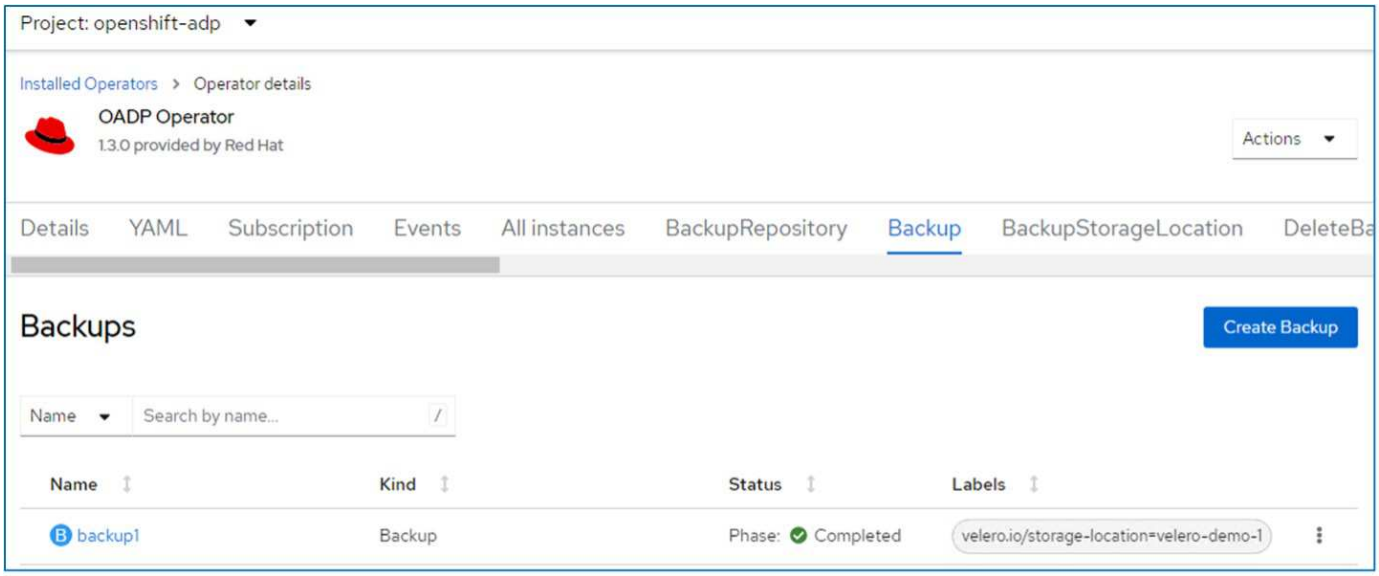
建立虛擬機器備份的步驟

若要建立整個 VM（VM 元資料和 VM 磁碟）的隨選備份，請按一下「備份」標籤。這將建立一個備份自訂資源 (CR)。提供了一個範例 yaml 來建立備份 CR。使用此 yaml，將備份指定命名空間中的 VM 及其磁碟。可以設定其他參數，如下所示"文件"。

CSI 將建立支援磁碟的持久性磁碟區的快照。建立虛擬機器的備份及其磁碟的快照，並將其儲存在 yaml 中指定的備份位置。備份將按照 ttl 的規定在系統中保留 30 天。

```
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
```

備份完成後，其階段將顯示為已完成。



您可以使用 S3 瀏覽器應用程式檢查物件儲存中的備份。備份路徑顯示在配置的儲存桶中，前綴名稱為（velero/demobackup）。您可以看到備份的內容包括虛擬機器的磁碟區快照、日誌和其他元資料。

> 在 StorageGrid 中，您也可以使用租用戶管理器提供的 S3 控制台來檢視備份物件。

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

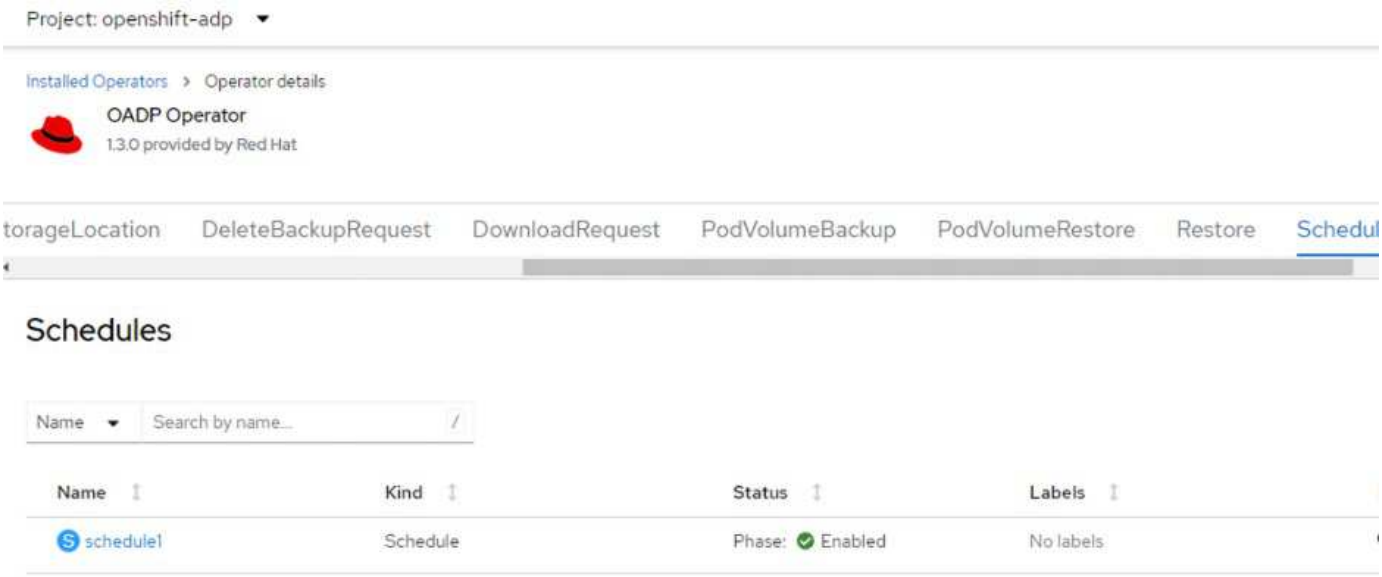
在 OpenShift 虛擬化中為虛擬機器建立排程備份

若要按排程建立備份，您需要建立計劃 CR。該計劃只是一個 Cron 表達式，可讓您指定要建立備份的時間。用於建立 Schedule CR 的範例 yaml。

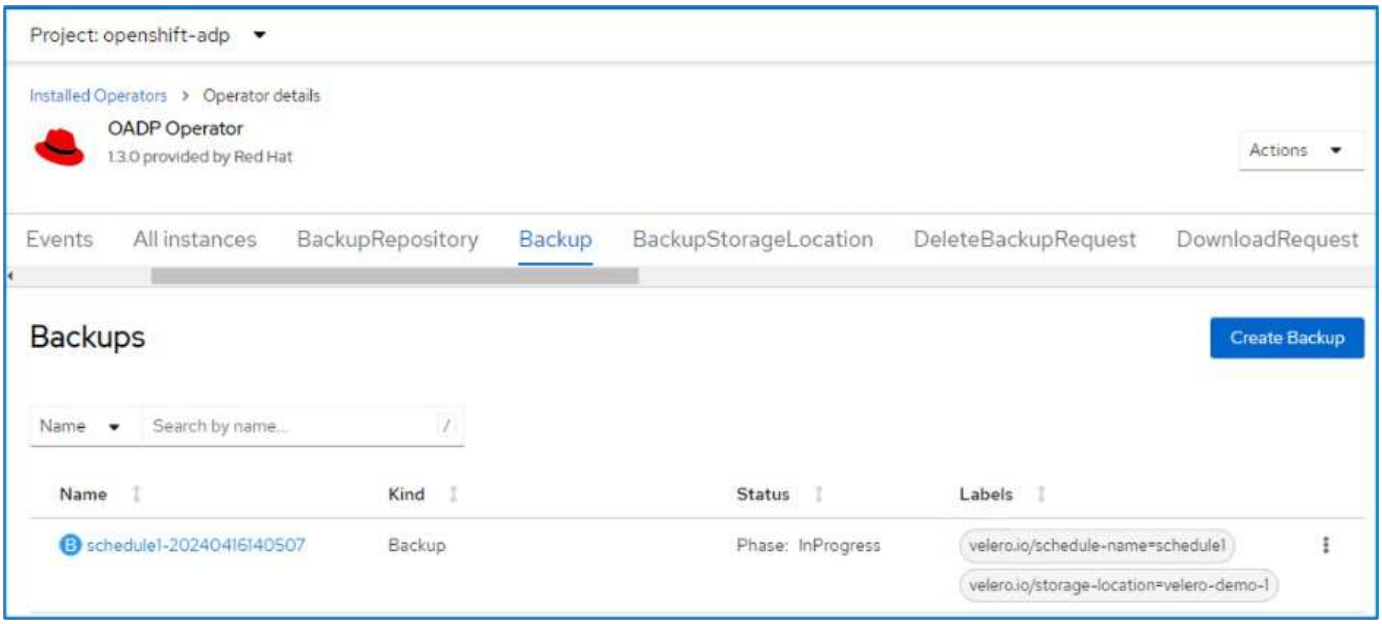
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s
```

Cron表達式 0 7 * * * 表示每天7:00建立備份。也指定了要包含在備份中的命名空間和備份的儲存位置。因此，不是使用備份 CR，而是使用計劃 CR 在指定的時間和頻率建立備份。

一旦創建了計劃，它將被啟用。



備份將根據此計劃創建，並可從「備份」標籤中查看。



使用 Velero 從 Red Hat OpenShift Virtualization 中的備份還原虛擬機

使用 Velero 和 OpenShift API for Data Protection (OADP) 在 OpenShift Virtualization 中還原虛擬機器。此流程包括建立復原自訂資源 (CR) 以從備份中還原虛擬機器及其持久性磁碟區，並可選擇還原至原始命名空間、不同的命名空間或使用備用儲存類別。

先決條件

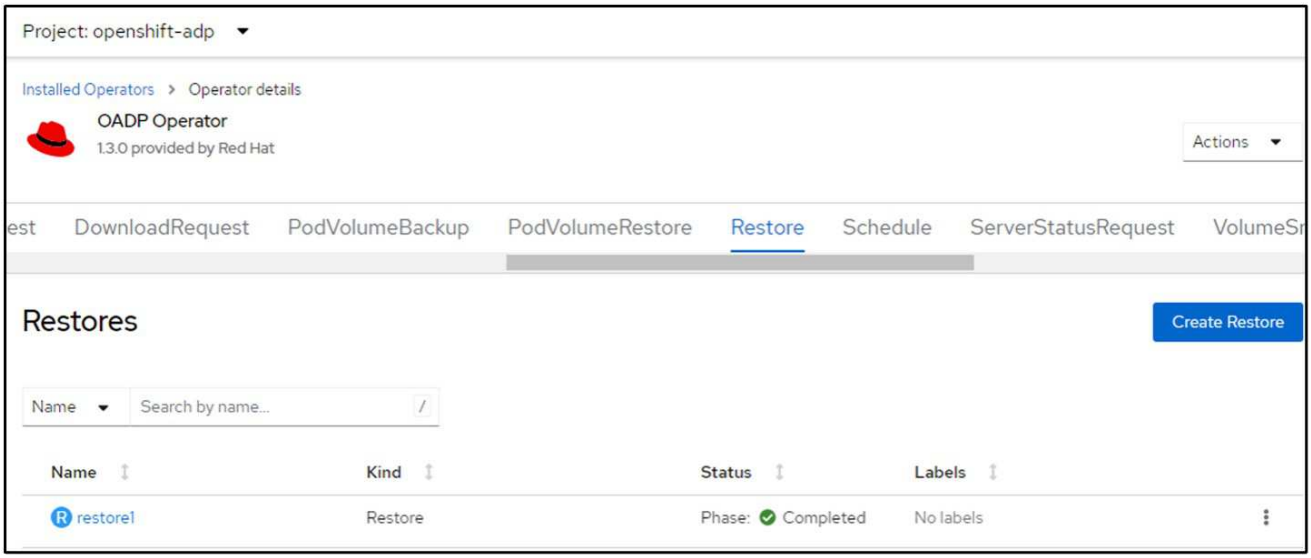
為了從備份中恢復，我們假設虛擬機器所在的命名空間被意外刪除了。

還原到同一命名空間

要從我們剛剛建立的備份中恢復，我們需要建立一個恢復自訂資源 (CR)。我們需要為其提供一個名稱，提供我們想要從中還原的備份的名稱，並將 restorePVs 設為 true。可以設定其他參數，如下所示"文件"。點選建立按鈕。

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

當階段顯示完成時，您可以看到虛擬機器已恢復到拍攝快照時的狀態。 （如果備份是在虛擬機器運行時建立的，則從備份還原虛擬機器將啟動還原的虛擬機器並使其處於運作狀態）。 VM 恢復到相同的命名空間。



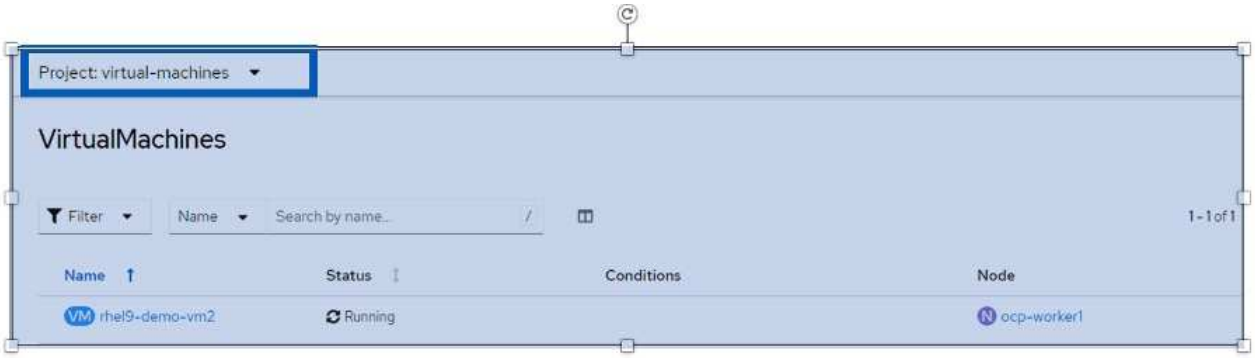
還原到不同的命名空間

若要將 VM 還原到不同的命名空間，您可以在 Restore CR 的 yaml 定義中提供 namespaceMapping。

以下範例 yaml 檔案建立一個復原 CR，以在將備份帶到虛擬機器命名空間時還原虛擬機器及其磁碟在虛擬機器-demo 命名空間中。

```
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
```

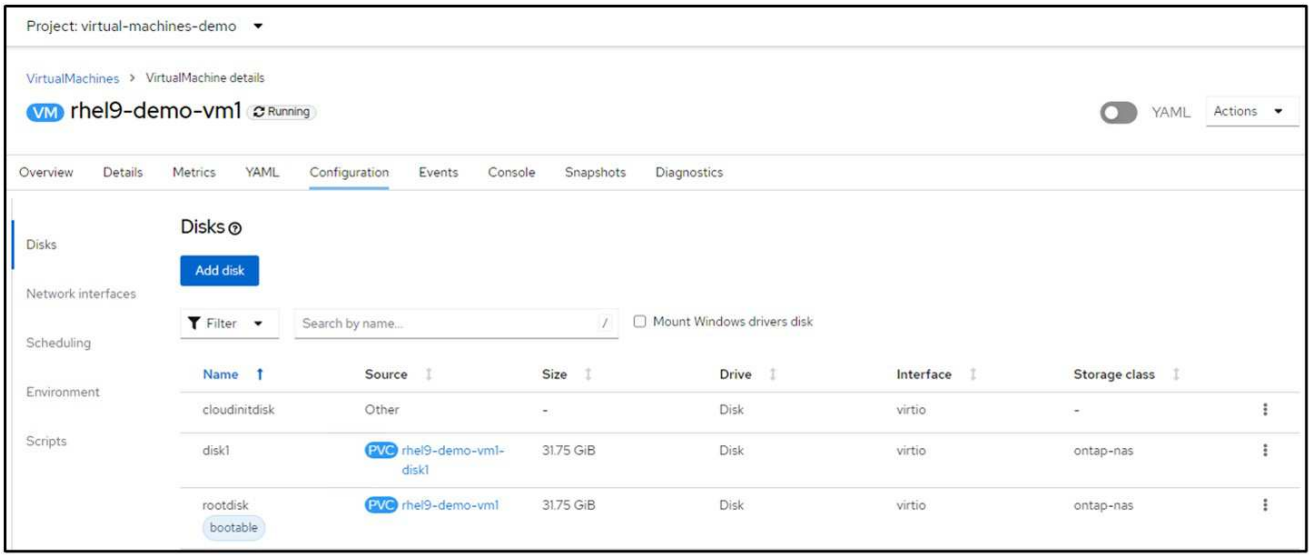
當階段顯示完成時，您可以看到虛擬機器已恢復到拍攝快照時的狀態。 （如果備份是在虛擬機器運行時建立的，則從備份還原虛擬機器將啟動還原的虛擬機器並使其處於運作狀態）。 VM 已還原至 yaml 中指定的不同命名空間。

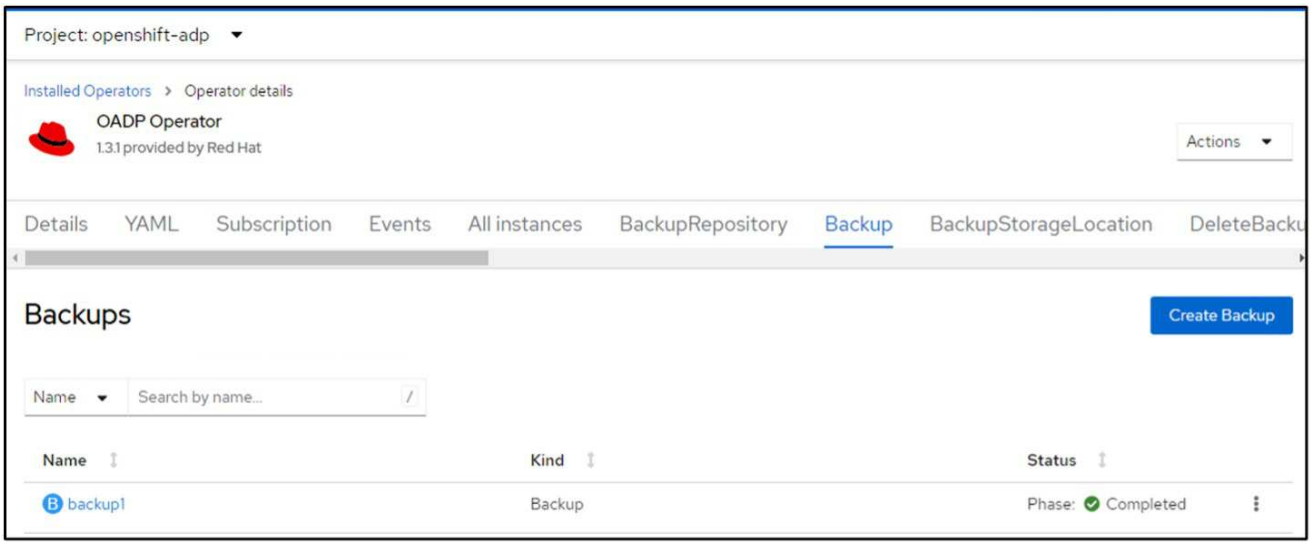


還原到不同的儲存類別

Velero 提供了透過指定 json 補丁來修改復原期間資源的通用功能。在恢復資源之前，json 補丁會套用到資源上。json 補丁在 configmap 中指定，並在 restore 命令中引用該 configmap。此功能使您能夠使用不同的儲存類別進行復原。

在下面的範例中，虛擬機器在建立期間使用 ontap-nas 作為其磁碟的儲存類別。建立了名為backup1的虛擬機器備份。





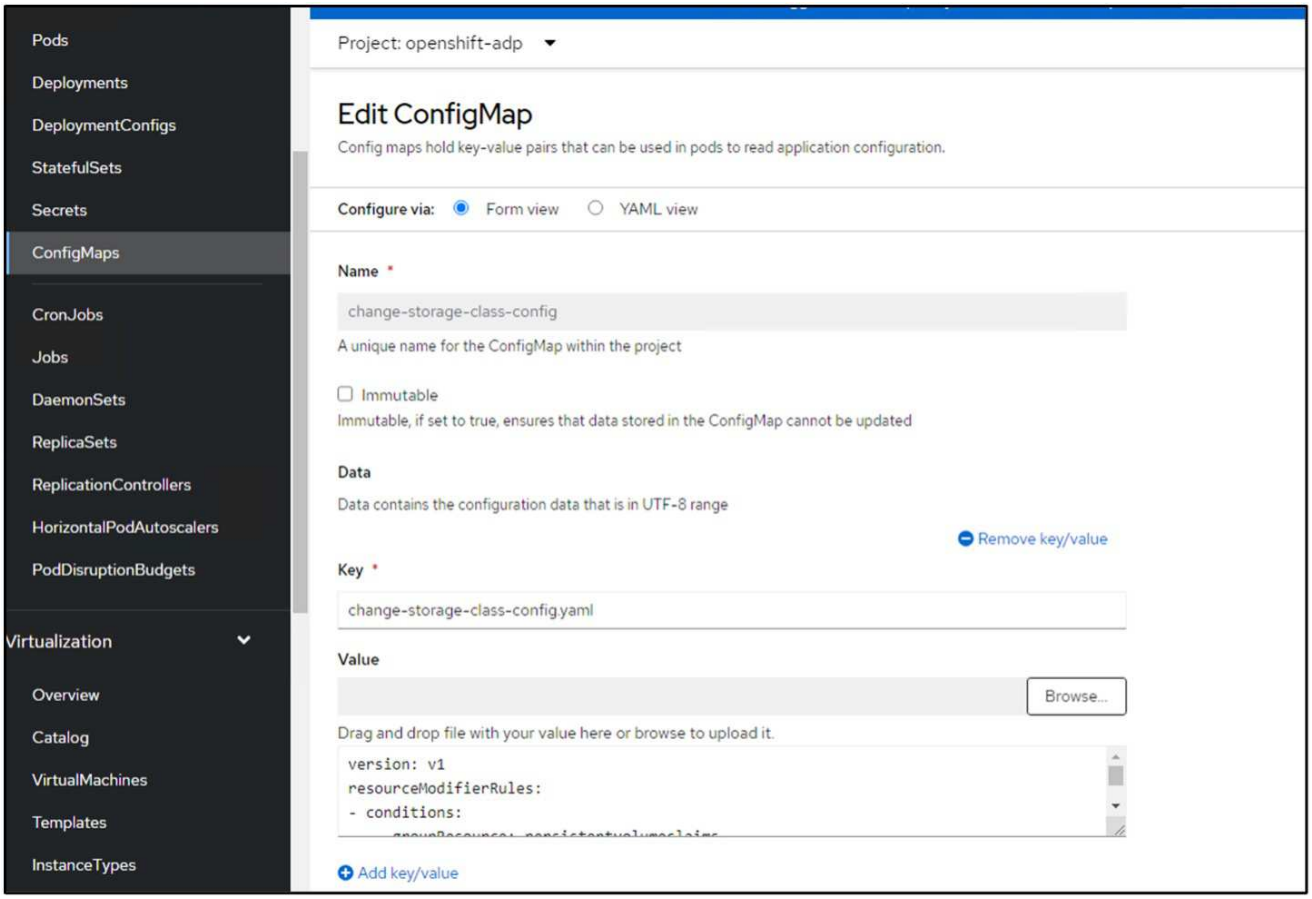
透過刪除虛擬機器來模擬虛擬機器的遺失。

要使用不同的儲存類別（例如 ontap-nas-eco 儲存類別）還原虛擬機，您需要執行以下兩個步驟：

步驟 **1**

在 openshift-adp 命名空間中建立一個設定映射（控制台），如下所示： 填寫螢幕截圖中顯示的詳細資訊： 選擇命名空間：openshift-adp 名稱：change-storage-class-config（可以是任意名稱） 鍵：change-storage-class-config.yaml： 值：

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



產生的配置映射物件應如下所示（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>
```

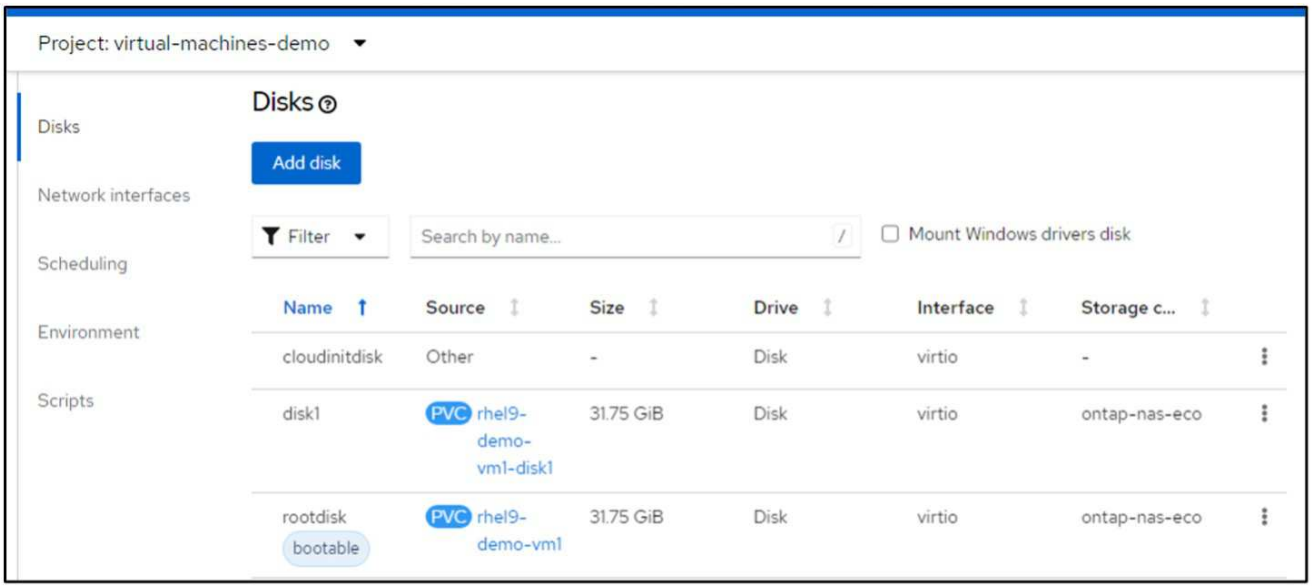
此配置圖將在建立復原時套用資源修改規則。將應用程式補丁將以 rhel 開頭的所有持久化卷聲明的儲存類別名稱替換為 ontap-nas-eco。

步驟 **2**

若要復原虛擬機，請使用 Velero CLI 中的下列命令：

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

虛擬機器與使用儲存類別 ontap-nas-eco 建立的磁碟在相同命名空間中復原。



使用 Velero 在 Red Hat OpenShift Virtualization 中刪除備份 CR 或還原 CR

使用 Velero 刪除 OpenShift Virtualization 中虛擬機器的備份和復原資源。使用 OpenShift CLI 刪除備份同時保留物件儲存數據，或使用 Velero CLI 刪除備份自訂資源 (CR) 和相關儲存數據。

刪除備份

您可以使用 OC CLI 工具刪除備份 CR，而不刪除物件儲存資料。

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

如果您想要刪除備份 CR 並刪除相關的物件儲存數據，您可以使用 Velero CLI 工具來執行此操作。

按照說明下載 CLI"Velero 文檔" 。

使用 Velero CLI 執行以下刪除命令

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

刪除恢復

您可以使用 Velero CLI 刪除 Restore CR

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

您可以使用 oc 指令以及 UI 來刪除復原 CR

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

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。