Proteja os dados usando ferramentas de terceiros

NetApp virtualization solutions

NetApp
August 18, 2025

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

Índice

Proteja os dados usando ferramentas de terceiros . . . 1
Aprenda sobre proteção de dados para VMs no Red Hat OpenShift Virtualization usando a API OpenShift para proteção de dados (OADP) . . . 1
Instalar o operador Red Hat OpenShift API for Data Protection (OADP) . . . 3
Pré-requisitos . . . 3
Etapas para instalar o operador OADP . . . 4
Crie backup sob demanda para VMs no Red Hat OpenShift Virtualization usando Velero . . . 13
Etapas para criar um backup de uma VM . . . 13
Criação de backups agendados para VMs no OpenShift Virtualization . . . 15
Restaurar uma VM a partir de um backup no Red Hat OpenShift Virtualization usando o Velero . . . 16
Pré-requisitos . . . 16
Excluir um CR de backup ou restaurar o CR no Red Hat OpenShift Virtualization usando o Velero . . . 22
Excluindo um backup . . . 22
Excluindo uma restauração . . . 22

Proteja os dados usando ferramentas de terceiros

Aprenda sobre proteção de dados para VMs no Red Hat OpenShift Virtualization usando a API OpenShift para proteção de dados (OADP)

A API OpenShift para proteção de dados (OADP) com Velero fornece recursos de backup, restauração e recuperação de desastres para VMs no OpenShift Virtualization. Use snapshots do Trident CSI para fazer backup de volumes persistentes e metadados de VM no NetApp ONTAP S3 ou StorageGRID S3. O OADP integra-se com APIs Velero e drivers de armazenamento CSI para gerenciar operações de proteção de dados para VMs em contêineres.

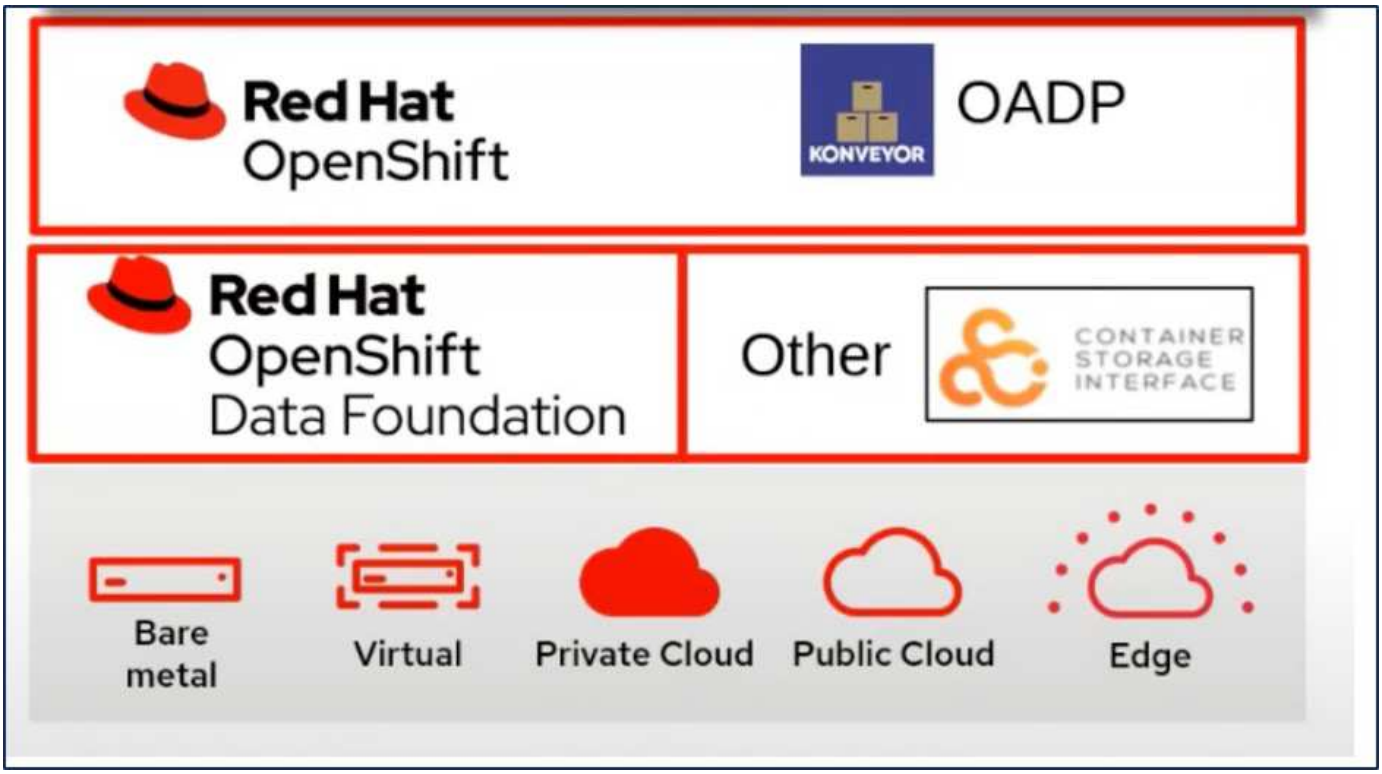
As máquinas virtuais no ambiente de virtualização OpenShift são aplicativos em contêineres executados nos nós de trabalho da sua plataforma OpenShift Container. É importante proteger os metadados da VM, bem como os discos persistentes das VMs, para que, quando eles forem perdidos ou corrompidos, você possa recuperá-los.

Os discos persistentes das VMs de virtualização OpenShift podem ser apoiados pelo armazenamento ONTAP integrado ao cluster OpenShift usando"Trident CSI" . Nesta seção usamos"API OpenShift para Proteção de Dados (OADP)" para executar backup de VMs, incluindo seus volumes de dados para

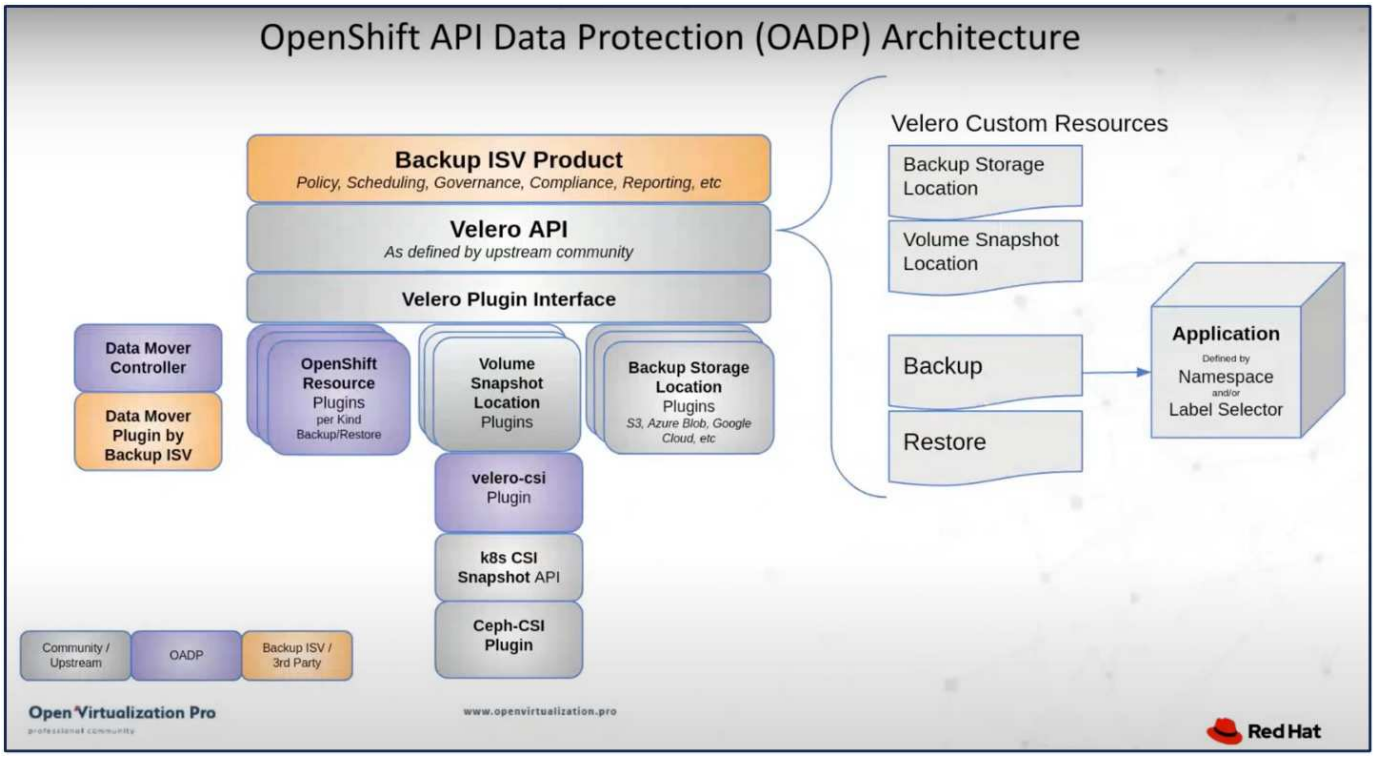
- Armazenamento de objetos ONTAP
- StorageGrid

Em seguida, restauramos a partir do backup quando necessário.

O OADP permite backup, restauração e recuperação de desastres de aplicativos em um cluster OpenShift. Os dados que podem ser protegidos com OADP incluem objetos de recursos do Kubernetes, volumes persistentes e imagens internas.



O Red Hat OpenShift aproveitou as soluções desenvolvidas pelas comunidades OpenSource para proteção de dados. "Velero" é uma ferramenta de código aberto para fazer backup e restaurar com segurança, executar recuperação de desastres e migrar recursos de cluster e volumes persistentes do Kubernetes. Para usar o Velero facilmente, a OpenShift desenvolveu o operador OADP e o plugin Velero para integração com os drivers de armazenamento CSI. O núcleo das APIs OADP expostas são baseadas nas APIs Velero. Após instalar o operador OADP e configurá-lo, as operações de backup/restauração que podem ser executadas são baseadas nas operações expostas pela API do Velero.



O OADP 1.3 está disponível no hub do operador do cluster OpenShift 4.12 e posteriores. Ele tem um Data Mover integrado que pode mover instantâneos de volume CSI para um armazenamento de objetos remoto. Isso proporciona portabilidade e durabilidade ao mover instantâneos para um local de armazenamento de objetos durante o backup. Os instantâneos ficam então disponíveis para restauração após desastres.

A seguir estão as versões dos vários componentes usados nos exemplos desta seção

- Cluster OpenShift 4.14
- OpenShift Virtualization instalado via OperatorOpenShift Virtualization Operator fornecido pela Red Hat
- Operador OADP 1.13 fornecido pela Red Hat
- Velero CLI 1.13 para Linux
- Trident 24.02
- ONTAP 9.12

"Trident CSI" "API OpenShift para Proteção de Dados (OADP)" "Velero"

Instalar o operador Red Hat OpenShift API for Data Protection (OADP)

Instale o operador OpenShift API for Data Protection (OADP) para habilitar recursos de backup e restauração para VMs no OpenShift Virtualization. Este procedimento inclui a implantação do OADP Operator do OpenShift Operator Hub, a configuração do Velero para usar o NetApp ONTAP S3 ou o StorageGRID como destino de backup e a configuração dos segredos e locais de backup necessários.

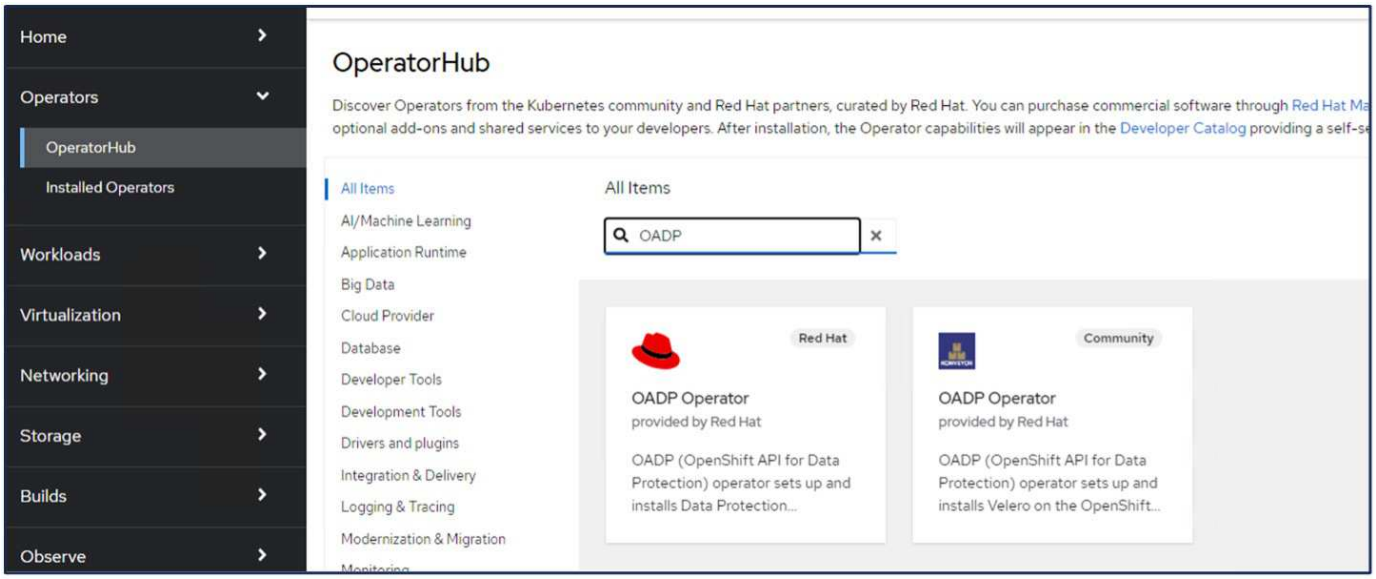
Pré-requisitos

- Um cluster Red Hat OpenShift (posterior à versão 4.12) instalado em infraestrutura bare-metal com nós de trabalho RHCOS
- Um cluster NetApp ONTAP integrado ao cluster usando Trident
- Um backend Trident configurado com um SVM no cluster ONTAP
- Um StorageClass configurado no cluster OpenShift com Trident como provisionador
- Classe Trident Snapshot criada no cluster
- Acesso de administrador de cluster ao cluster Red Hat OpenShift
- Acesso de administrador ao cluster NetApp ONTAP
- Operador de virtualização OpenShift instalado e configurado
- VMs implantadas em um namespace no OpenShift Virtualization
- Uma estação de trabalho de administração com as ferramentas tridentctl e oc instaladas e adicionadas ao $PATH

Se você quiser fazer um backup de uma VM quando ela estiver no estado Em execução, será necessário instalar o agente convidado QEMU nessa máquina virtual. Se você instalar a VM usando um modelo existente, o agente QEMU será instalado automaticamente. O QEMU permite que o agente convidado desative dados em execução no sistema operacional convidado durante o processo de snapshot e evite possível corrupção de dados. Se você não tiver o QEMU instalado, poderá parar a máquina virtual antes de fazer um backup.

Etapas para instalar o operador OADP

1. Acesse o Operator Hub do cluster e selecione o operador Red Hat OADP. Na página Instalar, use todas as seleções padrões e clique em instalar. Na próxima página, use novamente todos os padrões e clique em Instalar. O operador OADP será instalado no namespace openshift-adp.



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

Pré-requisitos para configuração do Velero com detalhes do Ontap S3

Após a instalação bem-sucedida do operador, configure a instância do Velero. O Velero pode ser configurado para usar o Object Storage compatível com S3. Configure o ONTAP S3 usando os procedimentos mostrados no"Seção de gerenciamento de armazenamento de objetos da documentação do ONTAP" . Você precisará das seguintes informações da sua configuração do ONTAP S3 para integrar com o Velero.

- Uma interface lógica (LIF) que pode ser usada para acessar o S3
- Credenciais do usuário para acessar o S3 que incluem a chave de acesso e a chave de acesso secreta
- Um nome de bucket no S3 para backups com permissões de acesso para o usuário
- Para acesso seguro ao armazenamento de objetos, o certificado TLS deve ser instalado no servidor de armazenamento de objetos.

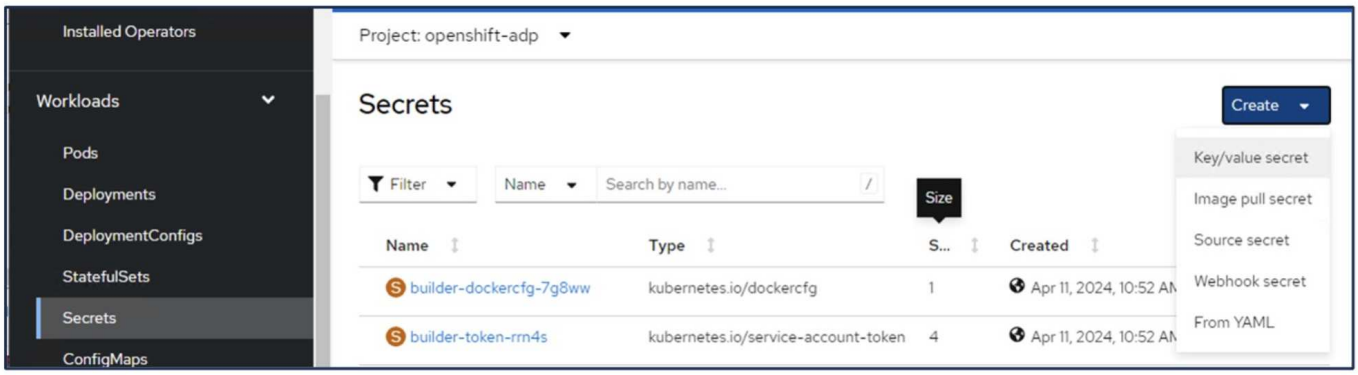
Pré-requisitos para configuração do Velero com detalhes do StorageGrid S3

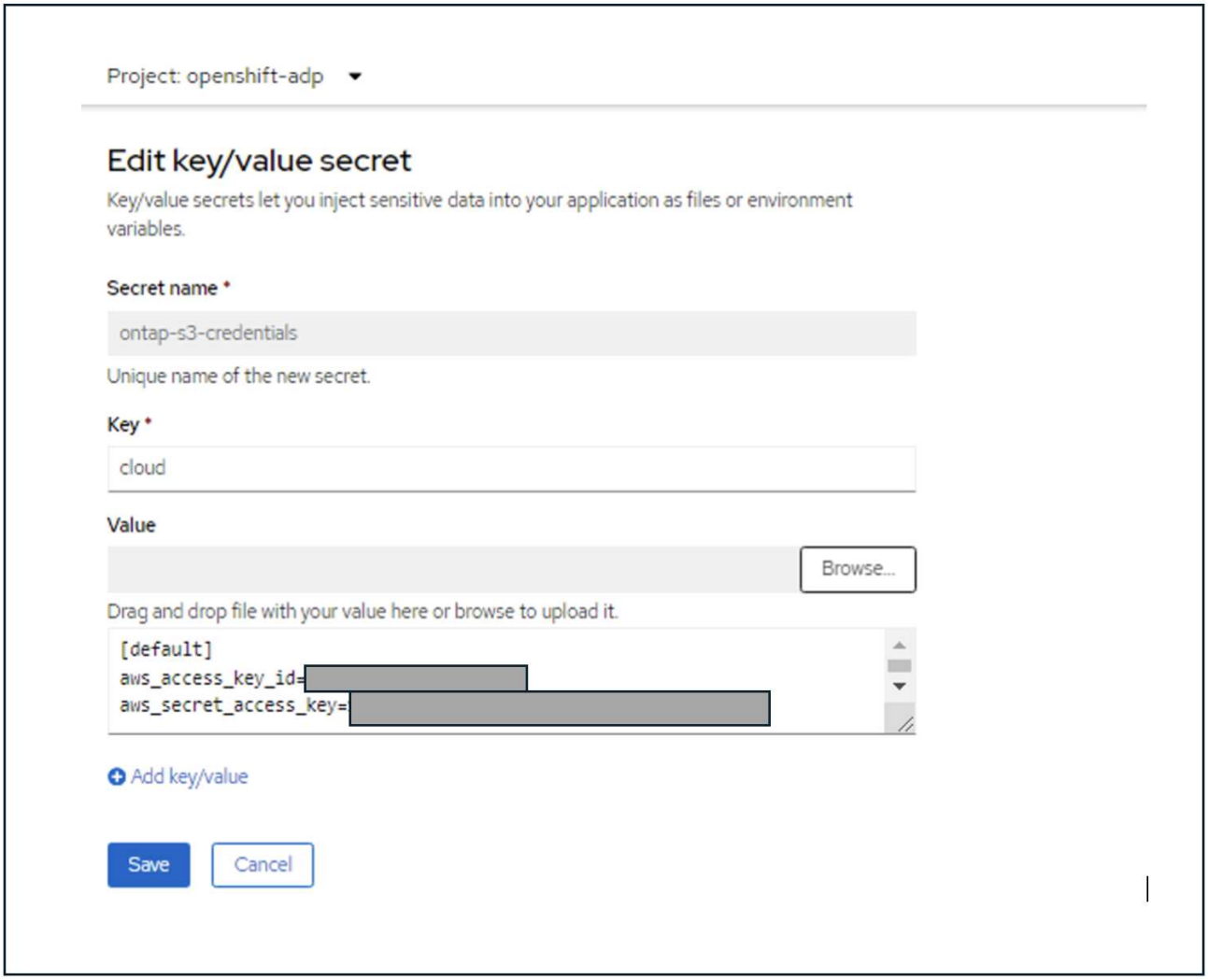
O Velero pode ser configurado para usar o Object Storage compatível com S3. Você pode configurar o StorageGrid S3 usando os procedimentos mostrados no"Documentação do StorageGrid" . Você precisará das seguintes informações da configuração do StorageGrid S3 para integrar com o Velero.

- O ponto de extremidade que pode ser usado para acessar o S3
- Credenciais do usuário para acessar o S3 que incluem a chave de acesso e a chave de acesso secreta
- Um nome de bucket no S3 para backups com permissões de acesso para o usuário
- Para acesso seguro ao armazenamento de objetos, o certificado TLS deve ser instalado no servidor de armazenamento de objetos.

Etapas para configurar o Velero

- Primeiro, crie um segredo para uma credencial de usuário do ONTAP S3 ou credenciais de usuário do StorageGrid Tenant. Isso será usado para configurar o Velero mais tarde. Você pode criar um segredo a partir da CLI ou do console da web. Para criar um segredo no console da web, selecione Segredos e clique em Segredo de chave/valor. Forneça os valores para o nome da credencial, a chave e o valor, conforme mostrado. Certifique-se de usar o ID da chave de acesso e a chave de acesso secreta do seu usuário do S3. Dê um nome apropriado ao segredo. No exemplo abaixo, um segredo com credenciais de usuário do ONTAP S3 chamado ontap-s3-credentials é criado.

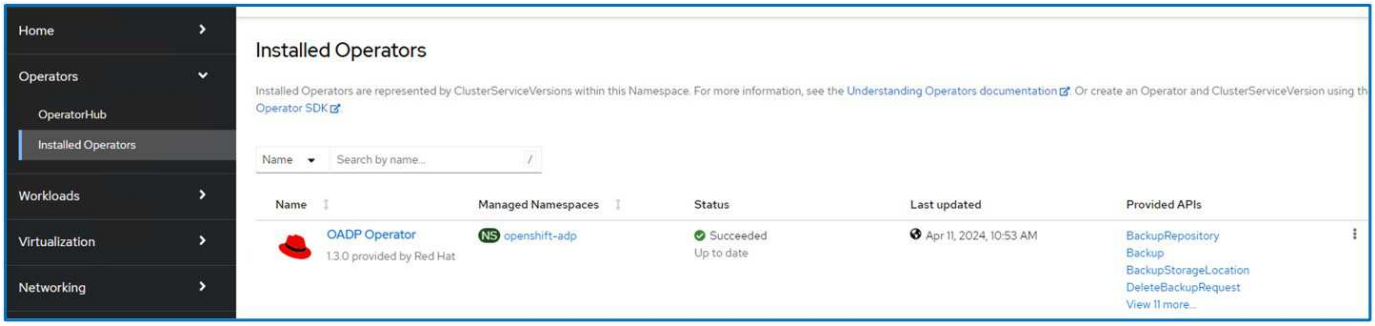




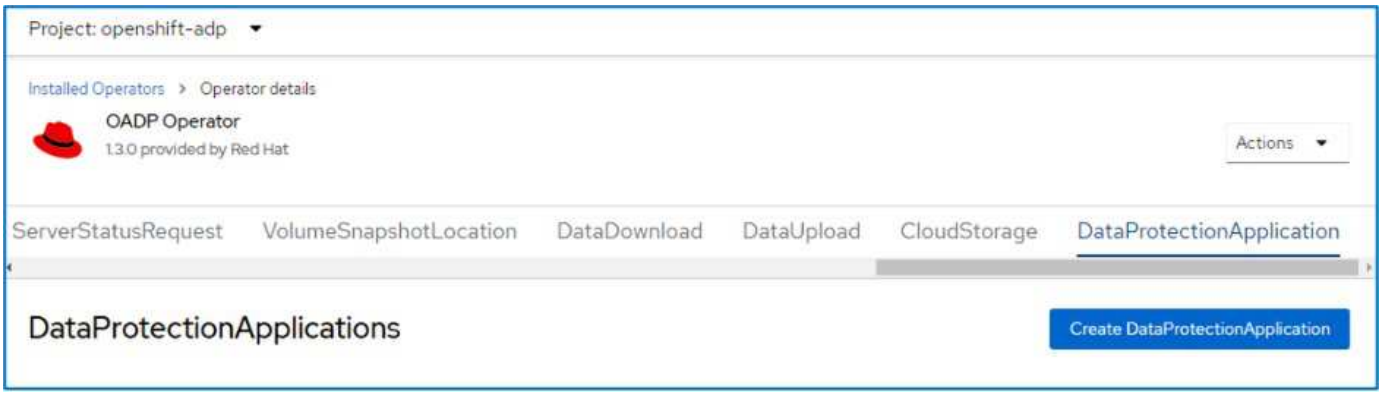
Para criar um segredo chamado sg-s3-credentials na CLI, você pode usar o seguinte comando.

```
# 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>
```

- Em seguida, para configurar o Velero, selecione Operadores instalados no item de menu em Operadores, clique no operador OADP e selecione a guia DataProtectionApplication.



Clique em Criar DataProtectionApplication. Na visualização de formulário, forneça um nome para o aplicativo DataProtection ou use o nome padrão.



Agora vá para a visualização YAML e substitua as informações de especificação conforme mostrado nos exemplos de arquivo yaml abaixo.

Arquivo yaml de exemplo para configurar o Velero com o ONTAP S3 como backupLocation

```
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
```

Arquivo yaml de exemplo para configurar o Velero com StorageGrid S3 como backupLocation e snapshotLocation

```
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
```

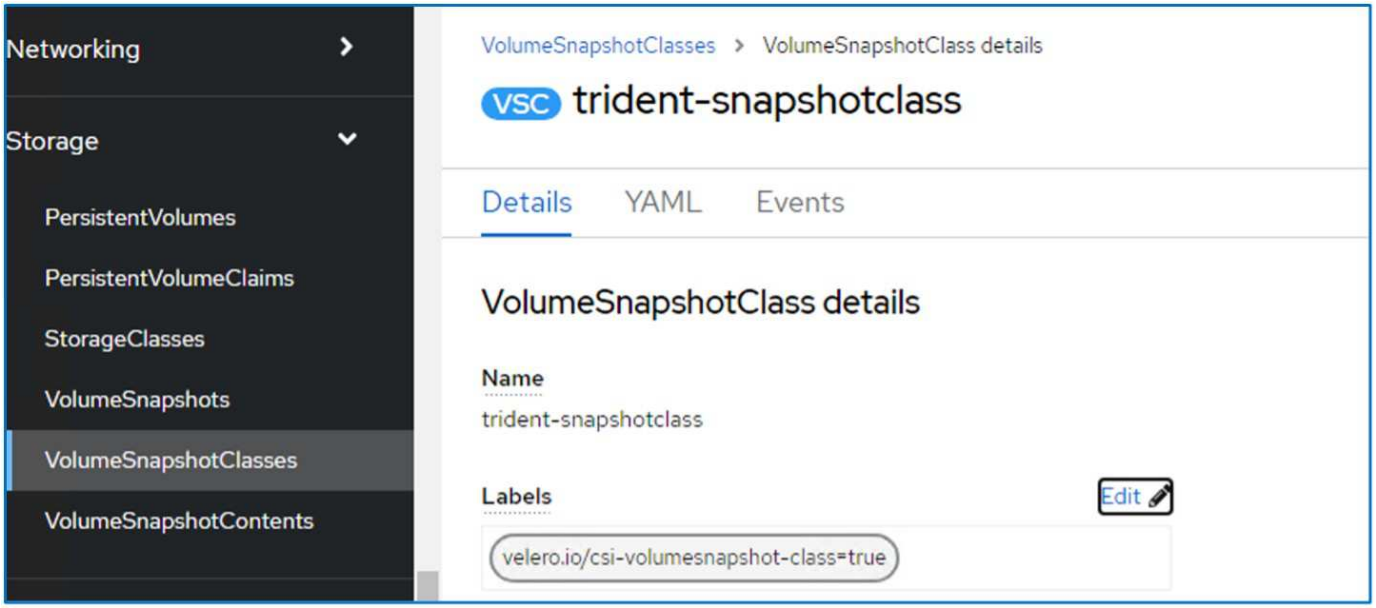
A seção de especificações no arquivo yaml deve ser configurada apropriadamente para os seguintes parâmetros, semelhante ao exemplo acima

backupLocations ONTAP S3 ou StorageGrid S3 (com suas credenciais e outras informações conforme mostrado no yaml) é configurado como o BackupLocation padrão para o velero.

snapshotLocations Se você usar snapshots da Container Storage Interface (CSI), não precisará especificar um local de snapshot porque você criará um VolumeSnapshotClass CR para registrar o driver CSI. Em nosso exemplo, você usa o Trident CSI e criou anteriormente o VolumeSnapShotClass CR usando o driver Trident CSI.

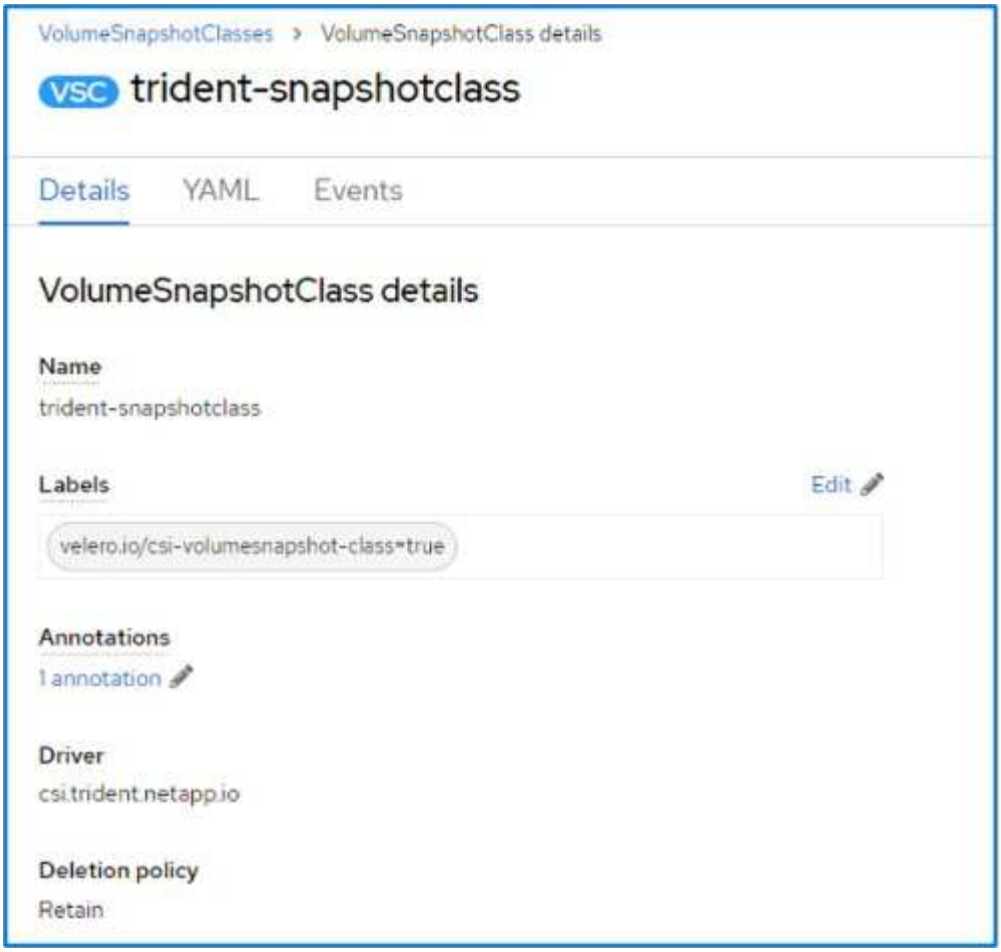
Habilitar plugin CSI Adicione csi aos defaultPlugins para que o Velero faça backup de volumes persistentes com snapshots CSI. Os plug-ins Velero CSI, para fazer backup de PVCs com suporte a CSI, escolherão o VolumeSnapshotClass no cluster que tem o rótulo **velero.io/csi-volumesnapshot-class** definido. Por esta

- Você deve ter o trident VolumeSnapshotClass criado.
- Edite o rótulo da classe trident-snapshot e defina-o como **velero.io/csi-volumesnapshot-class=true** conforme mostrado abaixo.

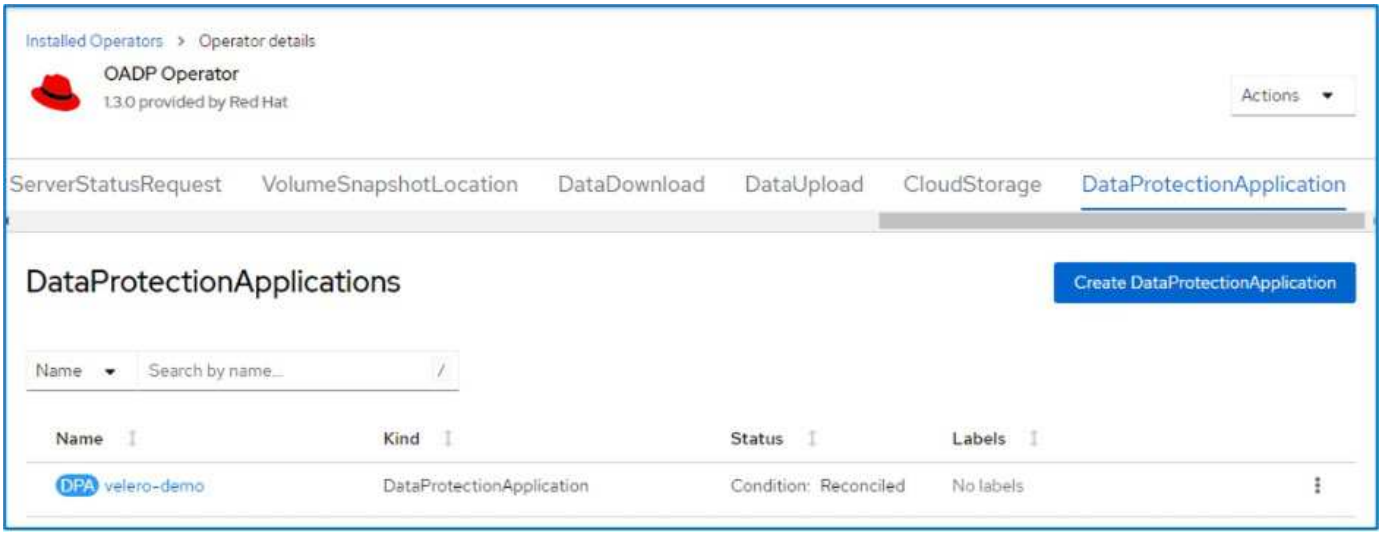


Garanta que os snapshots possam persistir mesmo se os objetos VolumeSnapshot forem excluídos. Isso pode ser feito definindo **deletionPolicy** como Retain. Caso contrário, a exclusão de um namespace perderá completamente todos os PVCs já armazenados em backup nele.

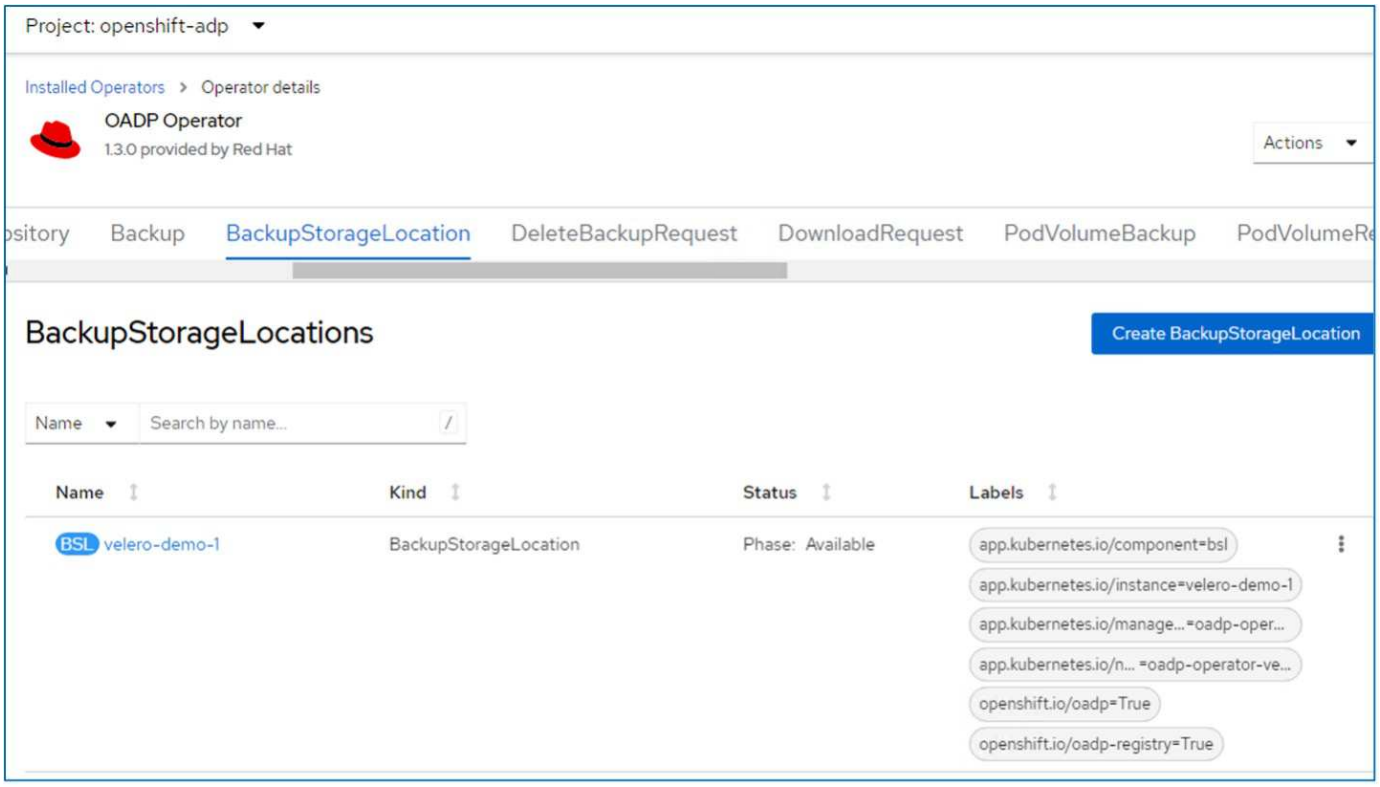
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



Certifique-se de que o DataProtectionApplication foi criado e está na condição:Reconciliado.



O operador OADP criará um BackupStorageLocation correspondente. Ele será usado ao criar um backup.



Crie backup sob demanda para VMs no Red Hat OpenShift Virtualization usando Velero

Faça backup de VMs no OpenShift Virtualization usando Velero e NetApp ONTAP S3 ou StorageGRID. Este procedimento inclui a criação de Recursos Personalizados de Backup (CRs) para backups sob demanda e CRs Agendados para backups agendados. Cada backup captura metadados de VM e volumes persistentes, armazenando-os no local de armazenamento de objetos especificado para fins de recuperação ou conformidade.

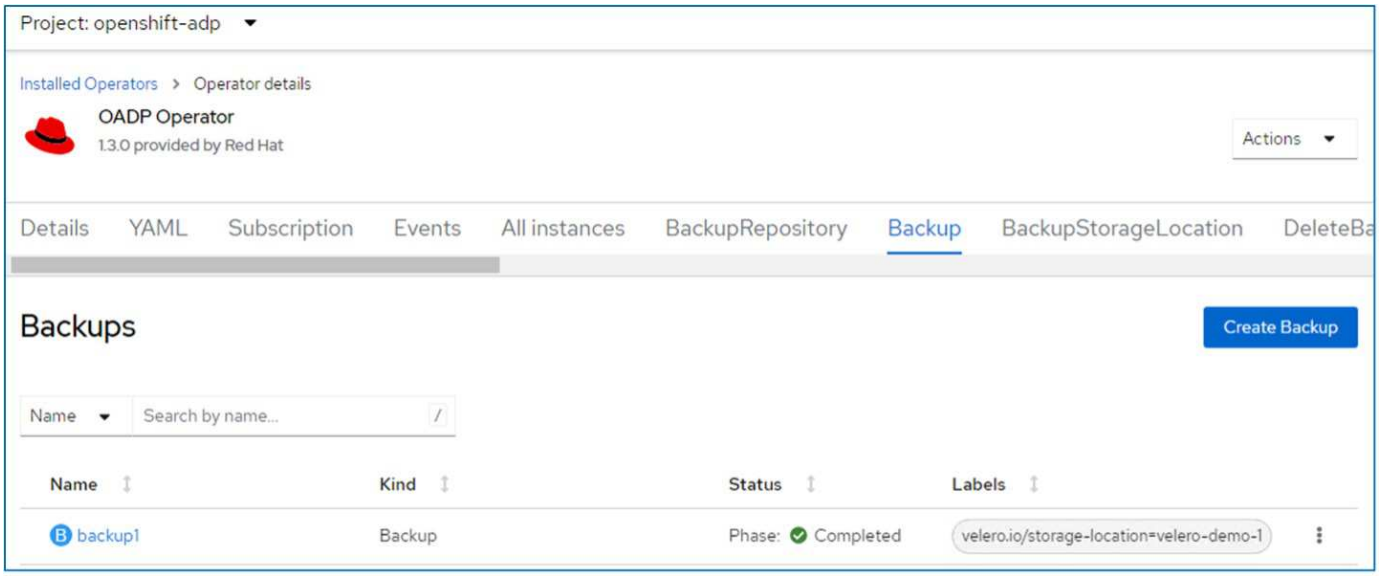
Etapas para criar um backup de uma VM

Para criar um backup sob demanda de toda a VM (metadados da VM e discos da VM), clique na guia **Backup**. Isso cria um Recurso Personalizado de Backup (CR). Um exemplo de yaml é fornecido para criar o Backup CR. Usando este yaml, a VM e seus discos no namespace especificado serão copiados. Parâmetros adicionais podem ser definidos conforme mostrado na"documentação" .

Um instantâneo dos volumes persistentes que dão suporte aos discos será criado pelo CSI. Um backup da VM junto com o instantâneo de seus discos são criados e armazenados no local de backup especificado no yaml. O backup permanecerá no sistema por 30 dias, conforme especificado no ttl.

```
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
```

Quando o backup for concluído, sua Fase será exibida como concluída.



Você pode inspecionar o backup no armazenamento de objetos com a ajuda de um aplicativo de navegador S3. O caminho do backup é exibido no bucket configurado com o prefixo nome (velero/demobackup). Você pode ver que o conteúdo do backup inclui instantâneos de volume, logs e outros metadados da máquina virtual.

> No StorageGrid, você também pode usar o console S3 disponível no Tenant Manager para visualizar os objetos de backup.

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

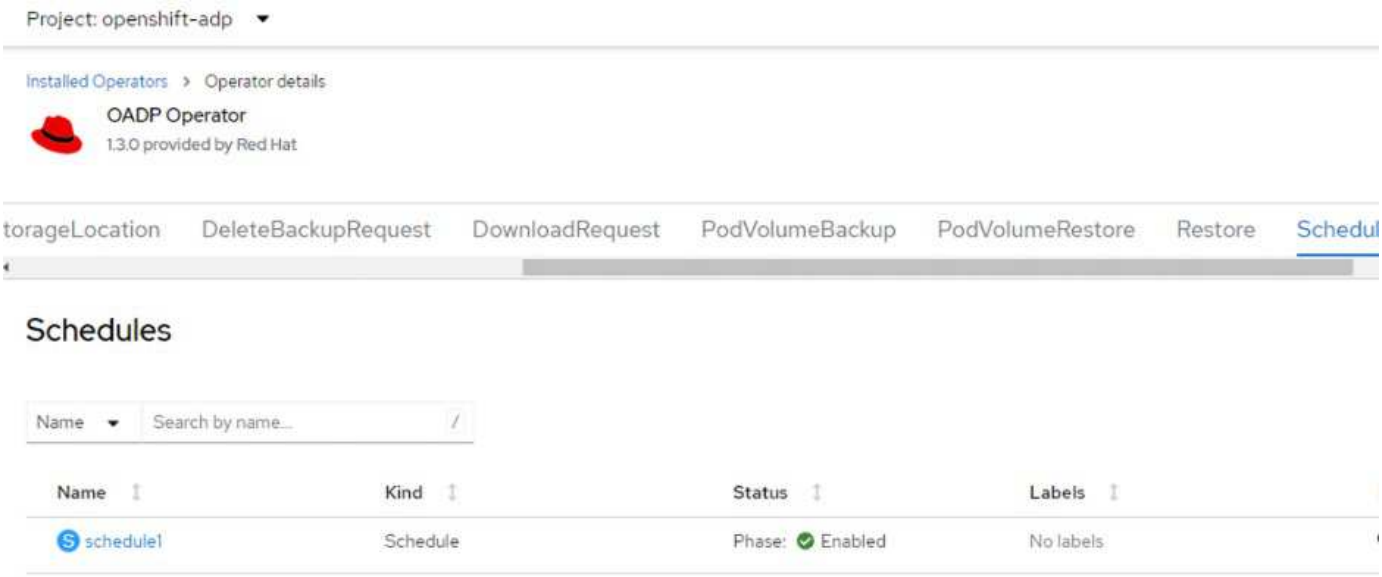
Criação de backups agendados para VMs no OpenShift Virtualization

Para criar backups agendados, você precisa criar uma CR agendada. O agendamento é simplesmente uma expressão Cron que permite que você especifique o horário em que deseja criar o backup. Um exemplo de yaml para criar um Schedule CR.

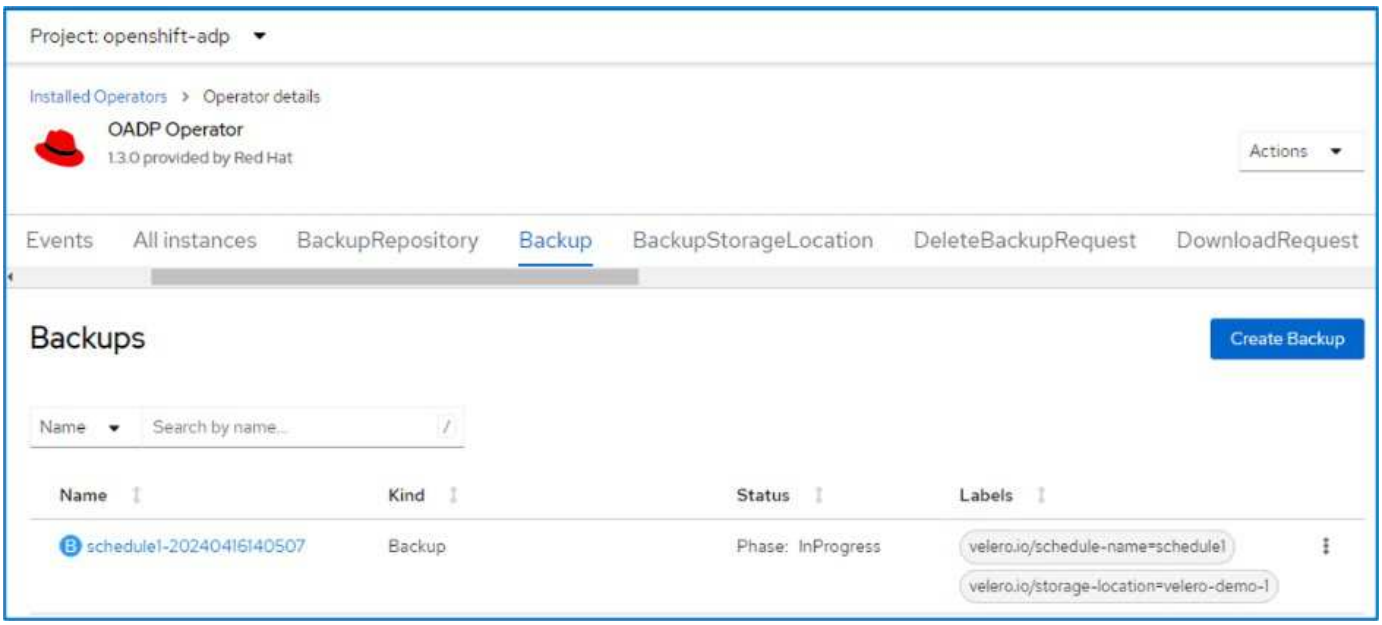
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s
```

A expressão Cron 0 7 * * * significa que um backup será criado às 7:00 todos os dias. Os namespaces a serem incluídos no backup e o local de armazenamento do backup também são especificados. Então, em vez de um CR de backup, o CR agendado é usado para criar um backup no horário e na frequência especificados.

Depois que o agendamento for criado, ele será habilitado.



Os backups serão criados de acordo com esta programação e podem ser visualizados na aba Backup.



Restaurar uma VM a partir de um backup no Red Hat OpenShift Virtualization usando o Velero

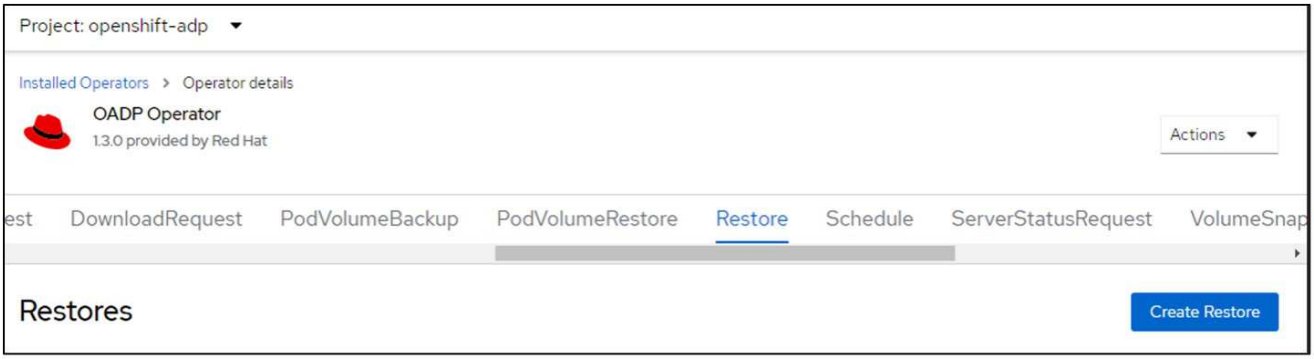
Restaure VMs no OpenShift Virtualization usando o Velero e a API OpenShift para proteção de dados (OADP). Este procedimento inclui a criação de um Recurso Personalizado de Restauração (CR) para recuperar VMs e seus volumes persistentes de backups, com opções para restaurar para o namespace original, um namespace diferente ou usar uma classe de armazenamento alternativa.

Pré-requisitos

Para restaurar a partir de um backup, vamos supor que o namespace onde a máquina virtual existia foi excluído acidentalmente.

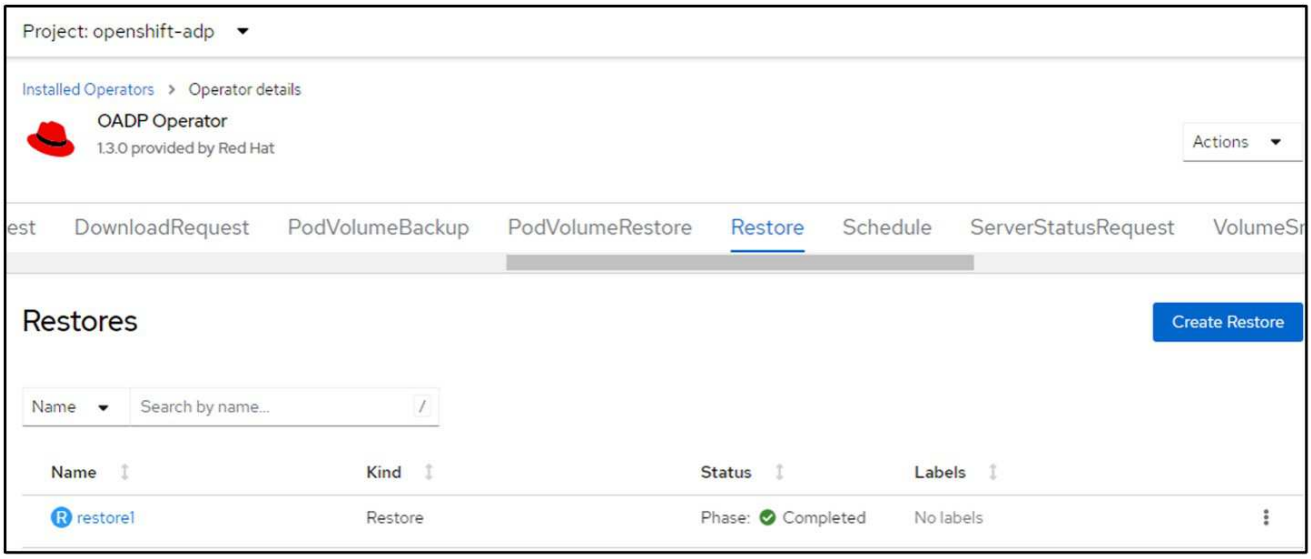
Restaurar para o mesmo namespace

Para restaurar o backup que acabamos de criar, precisamos criar um Recurso Personalizado de Restauração (CR). Precisamos fornecer um nome, fornecer o nome do backup que queremos restaurar e definir restorePVs como verdadeiro. Parâmetros adicionais podem ser definidos conforme mostrado na"documentação" . Clique no botão Criar.




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

Quando a fase for exibida como concluída, você poderá ver que as máquinas virtuais foram restauradas ao estado em que o instantâneo foi tirado. (Se o backup foi criado quando a VM estava em execução, restaurar a VM a partir do backup iniciará a VM restaurada e a colocará em um estado de execução). A VM é restaurada para o mesmo namespace.



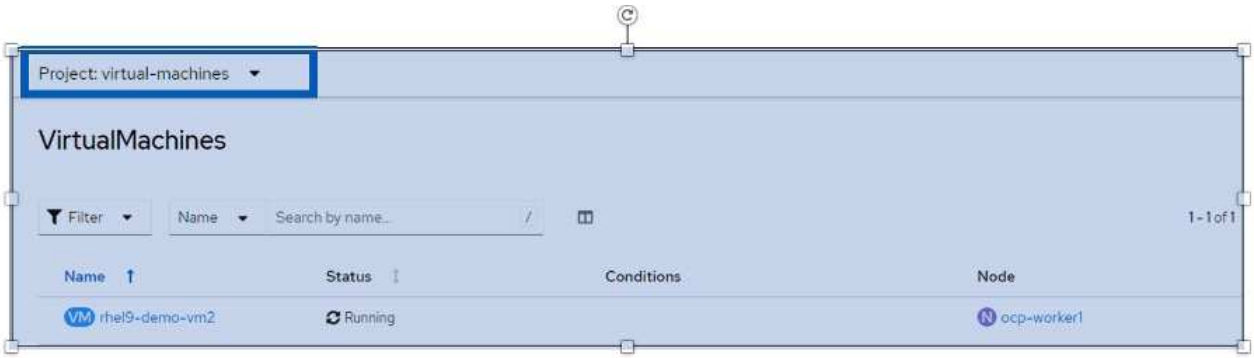
Restaurar para um namespace diferente

Para restaurar a VM para um namespace diferente, você pode fornecer um namespaceMapping na definição yaml do CR de restauração.

O arquivo yaml de exemplo a seguir cria um CR de restauração para restaurar uma VM e seus discos no namespace virtual-machines-demo quando o backup foi feito para o namespace virtual-machines.

```
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
```

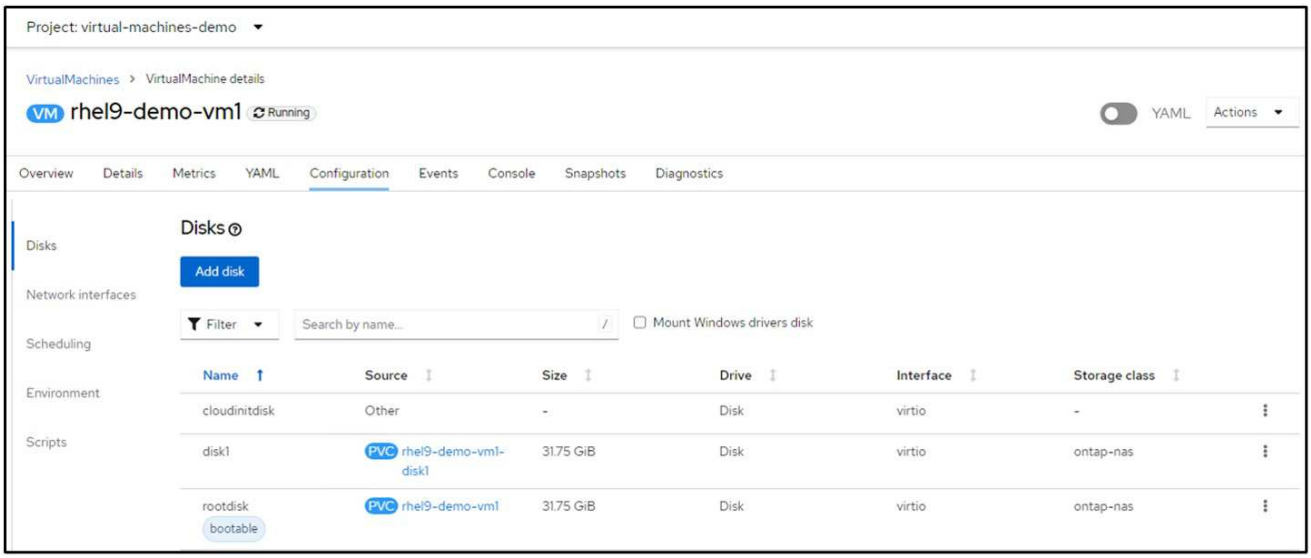
Quando a fase for exibida como concluída, você poderá ver que as máquinas virtuais foram restauradas ao estado em que o instantâneo foi tirado. (Se o backup foi criado quando a VM estava em execução, restaurar a VM a partir do backup iniciará a VM restaurada e a colocará em um estado de execução). A VM é restaurada para um namespace diferente, conforme especificado no yaml.

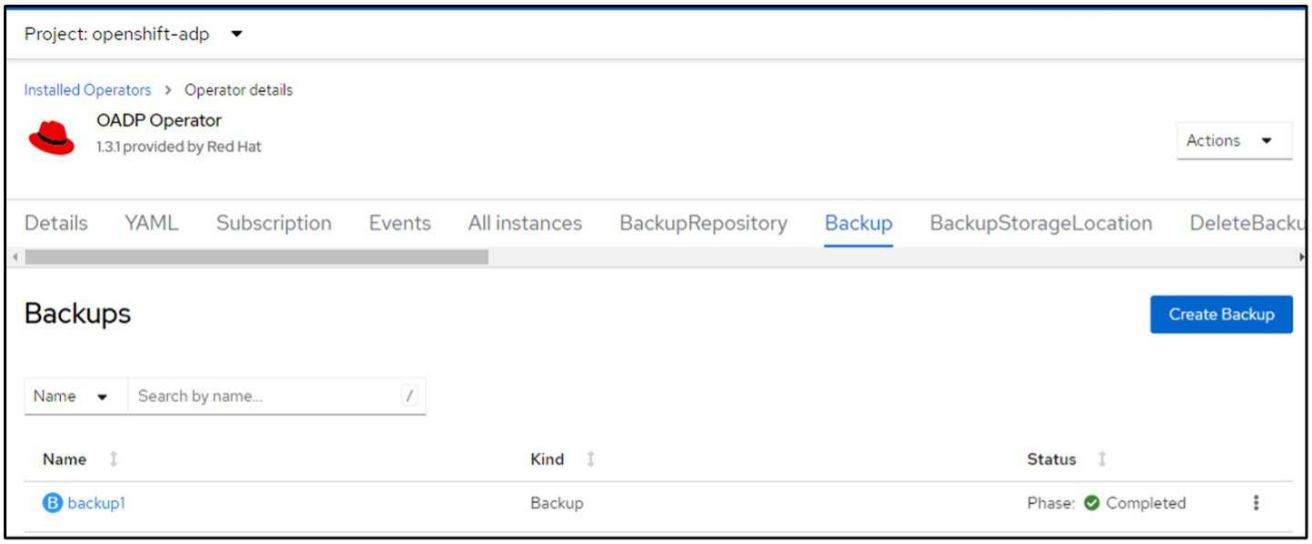


Restaurar para uma classe de armazenamento diferente

O Velero fornece uma capacidade genérica de modificar os recursos durante a restauração especificando patches json. Os patches json são aplicados aos recursos antes de serem restaurados. Os patches json são especificados em um configmap e o configmap é referenciado no comando restore. Este recurso permite que você restaure usando diferentes classes de armazenamento.

No exemplo abaixo, a máquina virtual, durante a criação, usa ontap-nas como classe de armazenamento para seus discos. Um backup da máquina virtual chamada backup1 é criado.





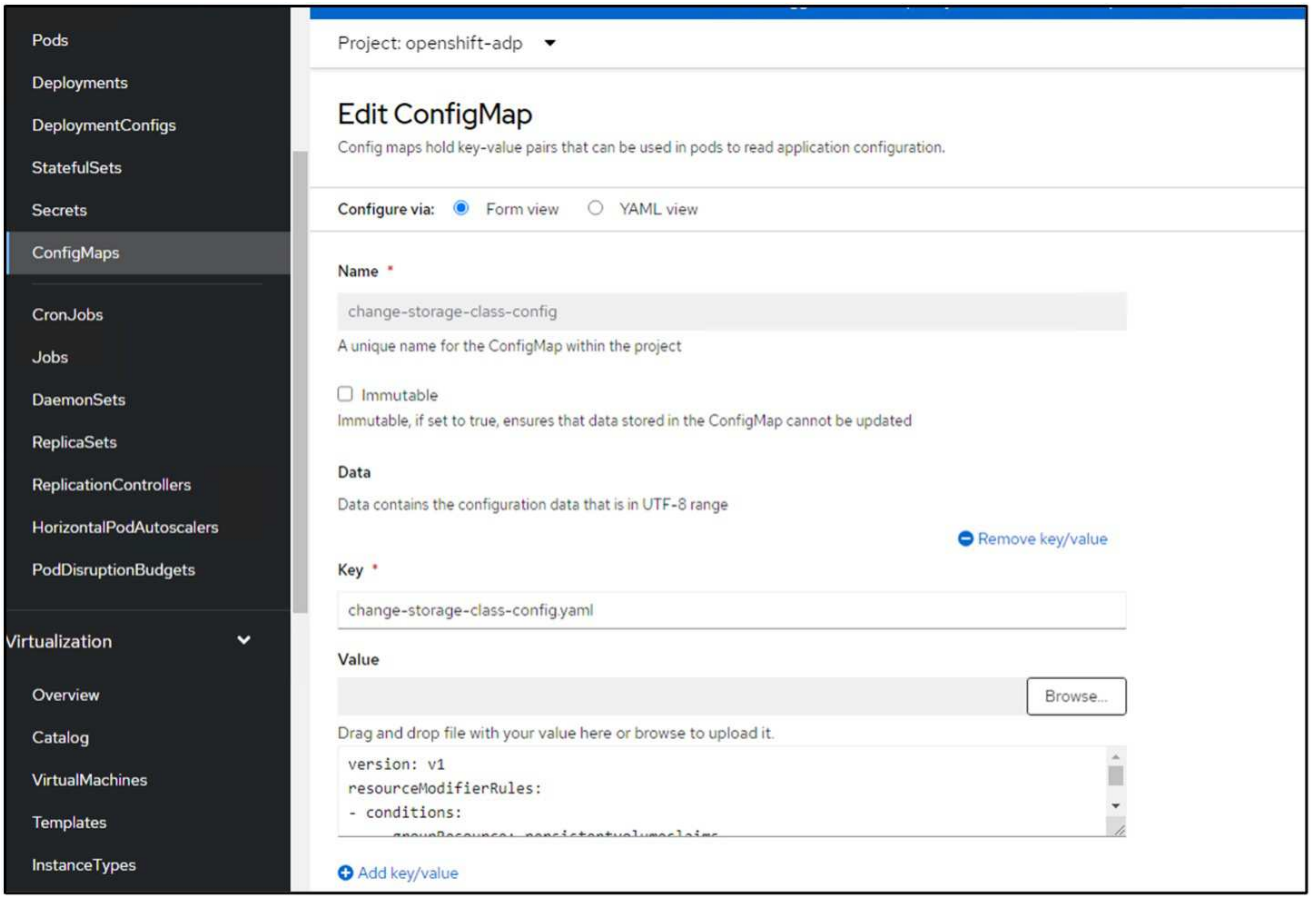
Simule uma perda da VM excluindo-a.

Para restaurar a VM usando uma classe de armazenamento diferente, por exemplo, classe de armazenamento ontap-nas-eco, você precisa seguir estas duas etapas:

Etapa 1

Crie um mapa de configuração (console) no namespace openshift-adp da seguinte maneira: Preencha os detalhes conforme mostrado na captura de tela: Selecione o namespace: openshift-adp Nome: change-storage-class-config (pode ser qualquer nome) Chave: change-storage-class-config.yaml: Valor:

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



O objeto do mapa de configuração resultante deve ter esta aparência (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>
```

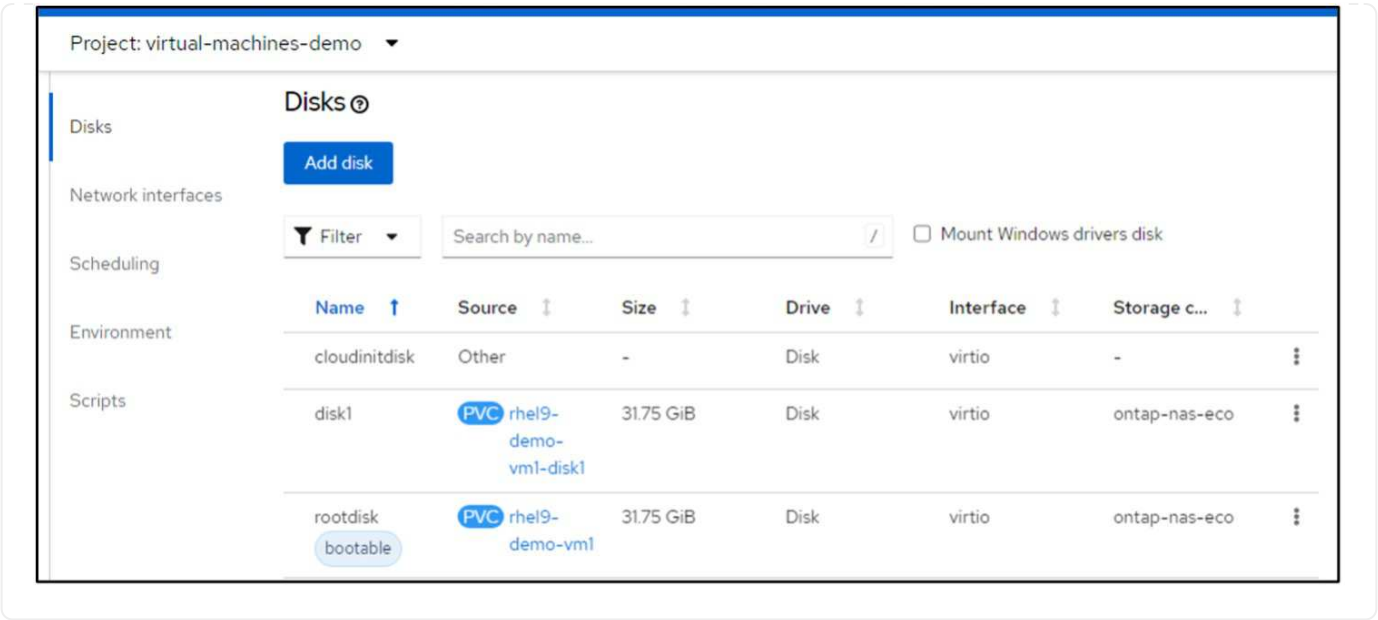
Este mapa de configuração aplicará a regra do modificador de recursos quando a restauração for criada. Um patch será aplicado para substituir o nome da classe de armazenamento para ontap-nas-eco para todas as declarações de volume persistentes que começam com rhel.

Etapa 2

Para restaurar a VM, use o seguinte comando do Velero CLI:

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

A VM é restaurada no mesmo namespace com os discos criados usando a classe de armazenamento ontap-nas-eco.



Excluir um CR de backup ou restaurar o CR no Red Hat OpenShift Virtualization usando o Velero

Exclua recursos de backup e restauração para VMs no OpenShift Virtualization usando o Velero. Use a CLI do OpenShift para excluir backups enquanto retém os dados de armazenamento de objetos, ou a CLI do Velero para excluir o recurso personalizado de backup (CR) e os dados de armazenamento associados.

Excluindo um backup

Você pode excluir um CR de backup sem excluir os dados do Object Storage usando a ferramenta OC CLI.

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

Se você quiser excluir o Backup CR e excluir os dados de armazenamento de objetos associados, poderá fazer isso usando a ferramenta Velero CLI.

Baixe o CLI conforme as instruções no"Documentação do Velero" .

Execute o seguinte comando delete usando o Velero CLI

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

Excluindo uma restauração

Você pode excluir o CR de restauração usando o Velero CLI

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

Você pode usar o comando oc e também a IU para excluir o CR de restauração

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

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.