NetBackup™ Kubernetes Installation and Configuration Guide

Release 10.3

Ports and requirements

Ports required for communication

Port number	From	To	Used for
(6)(8)443	Primary Server	Kubernetes cluster	HTTPS communications
443	Media Servers	Kubernetes cluster	HTTPS communications
1556 outbound	Kubernetes cluster	Primary Server	For certificate deployment and PBX communication with the Primary Server
1556 outbound	Kubernetes cluster	Media Servers	For certificate deployment
13724 bi-directional	Kubernetes cluster	Primary Server	VNETD for data movement
13724 bi-directional	Kubernetes cluster	Media Servers	VNETD for data movement

Deployment - Prerequisites for NetBackup Kubernetes Operators

- Check the SCL and HCL guide for supported configurations.
- Kubernetes operator requires 10Gi of storage, 100m CPU and 500Mi memory up to 150m max CPU and 600mi memory. All configuration is done during deployment.
- Kubernetes Operator requires administrative privileges to install.
- Customers either need access to a local repository to place the NBUKops and data mover packages for deployment. Or customers need internet access to the Veritas Customer Repository and use whatever tools customer generally use to copy mentioned packages into their local repository.
- A namespace must be configured to deploy the NBUKops image and data mover packages.
- Primary and Media servers must be created with FQDN, if they are created with short names. For more information, refer the section *Prerequisites for backup from snapshot and restore from backup operations* (Point 3 and 8) in the *NetBackup™ Web UI Kubernetes Administrator's Guide.*
- Namespaces with persistent storage must use CSI enabled storage with snapshot support, for more details refer to the HCL list. NBUKops supports only snapshot API version 'v1' for backup operations.
- Kubernetes supports DTE mode setting, Customer can configure DTE mode setting that is set on the datamover via backupserver specific configmap. Data-in-transit encryption of backup images is carried out based on the global DTE mode and the client DTE mode.

Upgrade

Upgrade

- All components (NBU Primary, Media, Kubernetes operators, and Data mover) must be same version.
- Existing policies continue to take backups but must be restored manually until the Kubernetes operator is updated.

Note: This is applicable to the NetBackup version 9.1 to 10.x upgrade.

Download the Veritas Kubernetes packages and load NetBackup Kubernetes Operator and Data mover into local registry

Download and extract Veritas Kubernetes packages

Get packages from VEMS

1. Go to the support.veritas.com, to log onto the **Veritas Entitlement Management System** (VEMS) and the, sign in and click **Licensing**.
2. Click **Entitlements** (within Veritas Entitlement Management System main menu).
3. Click **More Options** to expand filters.
4. Set the **Product Line** filter to NetBackup and click **Apply Filters**.
5. Look for entitlement's references, the version matches to the release note mentioned in the subject line.
6. To access your new software and license key(s) utilize the **Download Software** and **Generate License** buttons located in the Actions column.
7. You must download two packages:
   - ➢ NetBackup Kubernetes operator package (**netbackupkops-10.3.tar.gz**).
   - ➢ NetBackup Data mover image (**veritasnetbackup-datamover-10.3.tar**).

Download and extract Veritas Kubernetes packages

Package names and content

9. Extract the package to the home directory of a system that has access to the cluster where you can run **kubectl** commands. The netbackupkops-helm-chart is part of the KOps package and is in the home directory.

10. To list all cluster contexts, run the following command: kubectl config get-contexts

11. To switch to the cluster where you want to deploy the operator service, run the following command:

    kubectl config use-context <cluster-context-name>

Add the Kubernetes operator into your local registry

Follow these steps only if you have a private docker registry

1. Create a secret netbackupkops-docker-cred in the NetBackup namespace if container registry requires authentication. This secret is not needed if authentication is not configured.

   To log on to the private container registry, run the following command:

   docker login -u <username> <container-registry-url>

2. After logging in, the config.json file containing the authorization token is created or updated. To view the config.json file, run the following command:

   cat ~/.docker/config.json

   The output looks like below:

```
{
"auths": {
            "https://index.docker.io/v1/": {
           "auth": "c3R...zE2"
          } }
          }
```

Add the Kubernetes operator into your local registry

Follow these steps only if you have a private docker registry

3. To create a secret named netbackupkops-docker-cred in the NetBackup namespace, run the following command:

   ```
   kubectl create secret generic netbackupkops-docker-cred \ --from-file=.dockerconfigjson=.docker/config.json \ --type=kubernetes.io/dockerconfigjson -n <name of the namespace where the NetBackup operator will be deployed>
   ```

4. To check if the secret netbackupkops-docker-cred is created in the NetBackup namespace, run the following command:

   ```
   kubectl get secrets -n <name of the namespace where the NetBackup operator will be deployed>
   ```

Add the Kubernetes operator into your local registry

Push the Kubernetes Operator images to your registry

5. To load the image to the docker cache and push the image to the docker image repository, run the following commands:
   - ➢ docker load -i <name of the tar file>
   - ➢ docker tag <image name:tag of the loaded image> <repo-name/image-name:tag-name>
   - ➢ docker push <repo-name/image-name:tag-name>

6. Open the netbackupkops-helm-chart/values.yaml file in a text editor and then replace the value for image in the manager section, with your netbackupkops repo image name and tag repo-name/image-name:tag-name and then save the file

Add the Data mover to your local registry

To load the image to the docker cache and push the image to the docker image repository, run the following commands:

- docker load -i <name of the datamover image tar file>
- docker tag <datamover image name:tag of the loaded datamover image> <repo-name/image-name:tag-name>
- docker push <repo-name/image-name:tag-name>

APPENDIX

The following slides show steps that have been replaced with an automated process. If you want to run the manual configuration then, run the steps manually.

Installation and configuration

Installation and configuration

NetBackup Kubernetes operator deployment and configuration

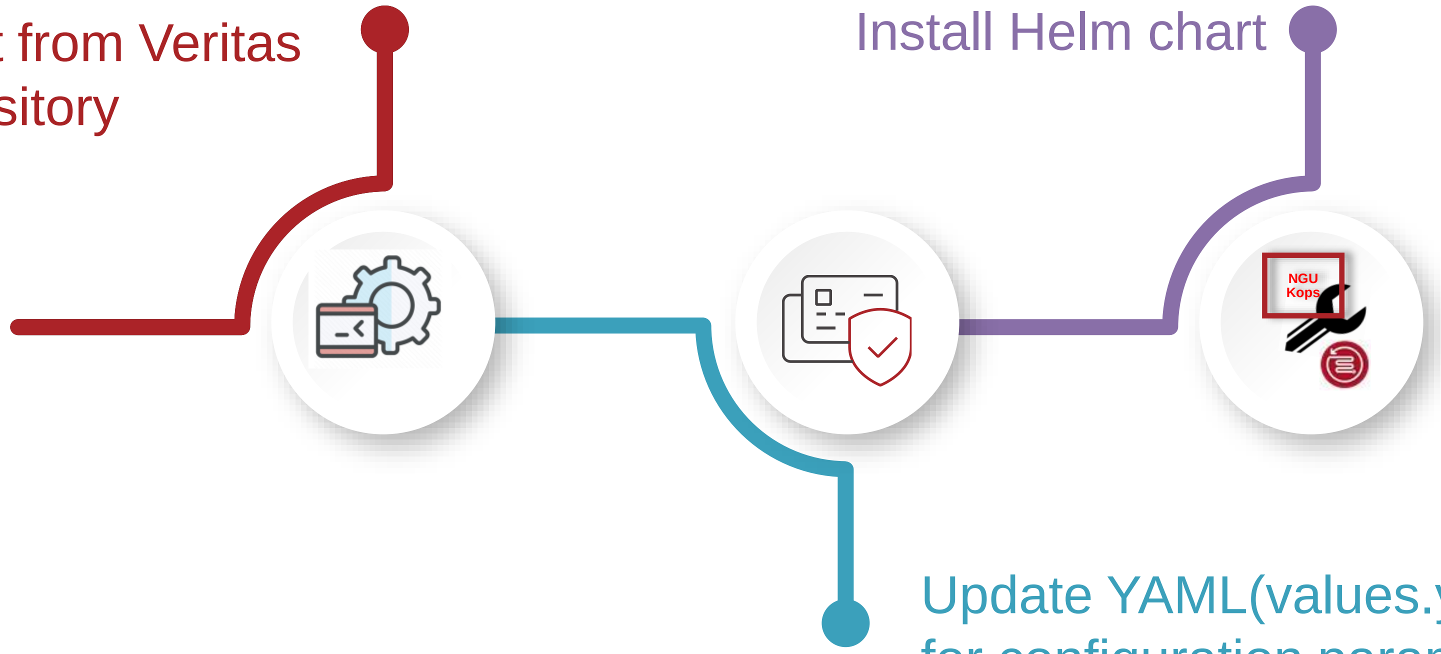
User can deploy and configure NBUKops in NetBackup web UI using the following methods:

1. **Provide required parameters in values.yaml file to use Automated configuration:**
   - ➢ Before you run the helm install, you need to provide required values in the **netbackupkops-helm-chart/values.yaml** file.
   - ➢ Follow the Helm install integrated manual configuration steps.
   - ➢ As part of configuration deployment, a pod gets created each time user runs helm install. This pod runs the script to configure Kubernetes workload protection.
   - ➢ This process includes following operations:
     - Prepares storage for backup and restore : Label volmesnapshotclass and storage classes for creating snapshots and PVCs.
     - Read service account token from nbukops namespace.
     - Create NetBackup credentials for Kubernetes in NetBackup.
     - Add Kubernetes Cluster to NetBackup.
     - Create NetBackup token and fetch sha256 fingerprint.
     - Create BackupServerCert for establishing secure communication for datamover pod.
     - Configure primary server specific configmap for datamover image.

2. **Use manual configuration steps.**

NetBackup Kubernetes Operator deployment and configuration using automated configuration

Deployment High-level steps using automated configuration



Download the Helm chart from Veritas repository

Update YAML(values.yaml) file for configuration parameters

Install Helm chart

Automated configuration

Update netbackupkops-helm-chart/values.yaml configuration file

1. Untar netbackupkops.tar.gz file (Command : *tar –xvf netbackupkops.tar.gz*) and provide inputs required for **netbackupkops-helm-chart/values.yaml**

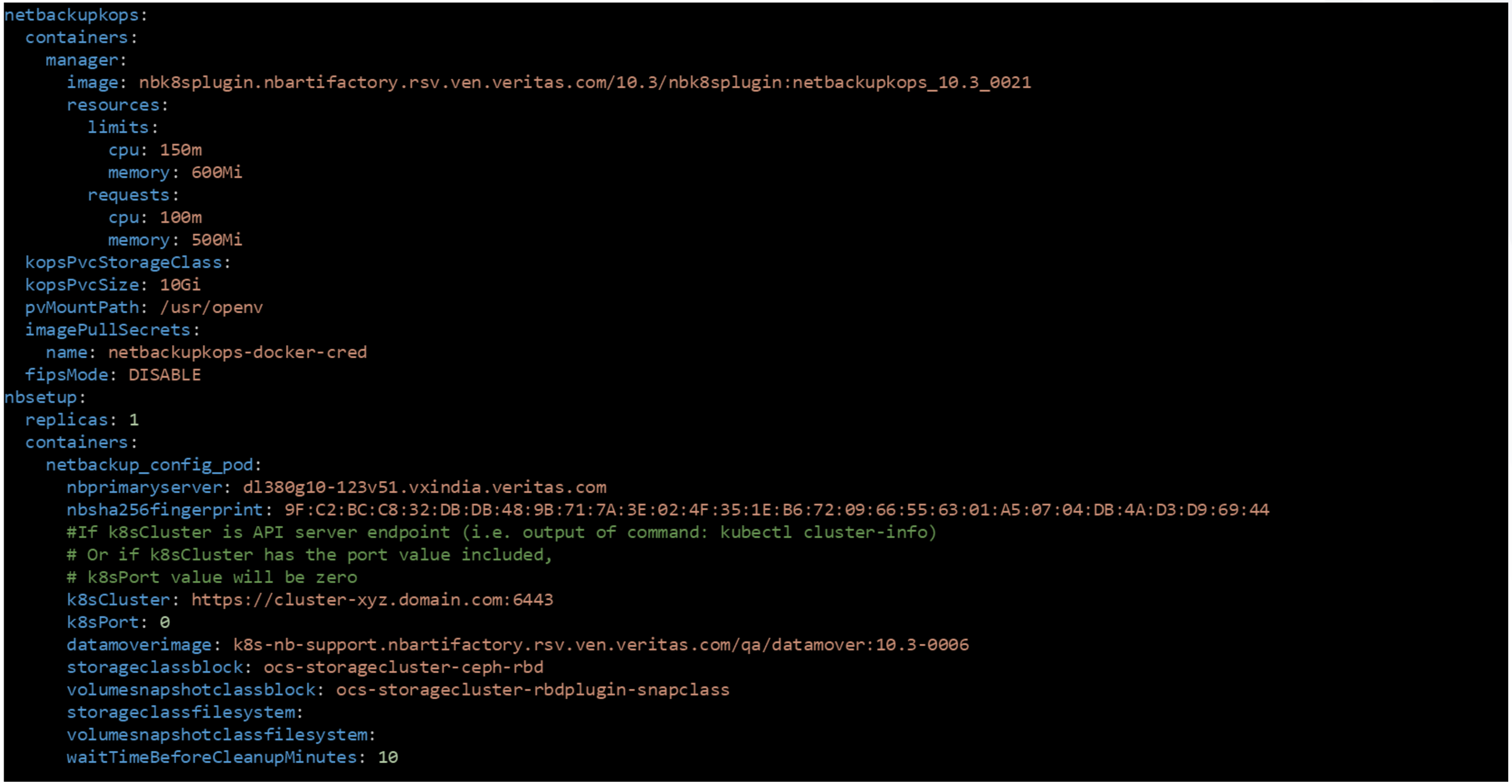
   netbackup_config_pod:

   - **nbprimaryserver :** <FQDN of NetBackup Primary Server>
   - **nbsha256fingerprint :** <Copy sha256 fingerprint from NetBackup Primary Server Web UI>
     (Go to NetBackup web UI → Security → Certificates → Click on Certificate Authority)
   - **k8sCluster :** <FQDN of Kubernetes cluster API server (Run command : kubectl cluster-info)>
   - **k8sPort :** <Port on which Kubernetes API server is listening>
   - **datamoverimage :** <Container registry URL for pulling datamover image>
   - **storageclassblock :** <Storage class used for provisioning block volumes (Run command : kubectl get storageclasses)>
   - **storageclassfilesystem :** <Storage class used for provisioning filesystem volumes (Run command : kubectl get storageclasses)>
   - **volumesnapshotclassblock :** <Volume snapshot class for creating block volume snapshots (Run command : kubectl get volumesnapshotclass)>
   - **volumesnapshotclassfilesystem :** <Volume snapshot class for creating filesystem volume snapshots (Run command : kubectl get volumesnapshotclass)>

Note: Automated configuration is currently supported **only for NBCA mode.** To learn more about the volume snapshot class and storage class names, refer to the **Label Storage for Backup and Restore** section in the NetBackup Kubernetes Administrator's guide.

Automated configuration netbackupkops-helm-chart/values.yaml file

A sample: values.yaml



```
netbackupkops:
  containers:
    manager:
      image: nbk8splugin.nbartifactory.rsv.ven.veritas.com/10.3/nbk8splugin:netbackupkops_10.3_0021
      resources:
        limits:
          cpu: 150m
          memory: 600Mi
        requests:
          cpu: 100m
          memory: 500Mi
  kopsPvcStorageClass:
  kopsPvcSize: 10Gi
  pvMountPath: /usr/openv
  imagePullSecrets:
    name: netbackupkops-docker-cred
  fipsMode: DISABLE
nbsetup:
  replicas: 1
  containers:
    netbackup_config_pod:
      nbprimaryserver: dl380g10-123v51.vxindia.veritas.com
      nbsha256fingerprint: 9F:C2:BC:C8:32:DB:DB:48:9B:71:7A:3E:02:4F:35:1E:B6:72:09:66:55:63:01:A5:07:04:DB:4A:D3:D9:69:44
      #If k8sCluster is API server endpoint (i.e. output of command: kubectl cluster-info)
      # Or if k8sCluster has the port value included,
      # k8sPort value will be zero
      k8sCluster: https://cluster-xyz.domain.com:6443
      k8sPort: 0
      datamoverimage: k8s-nb-support.nbartifactory.rsv.ven.veritas.com/qa/datamover:10.3-0006
      storageclassblock: ocs-storagecluster-ceph-rbd
      volumesnapshotclassblock: ocs-storagecluster-rbdplugin-snapclass
      storageclassfilesystem:
      volumesnapshotclassfilesystem:
      waitTimeBeforeCleanupMinutes: 10
```

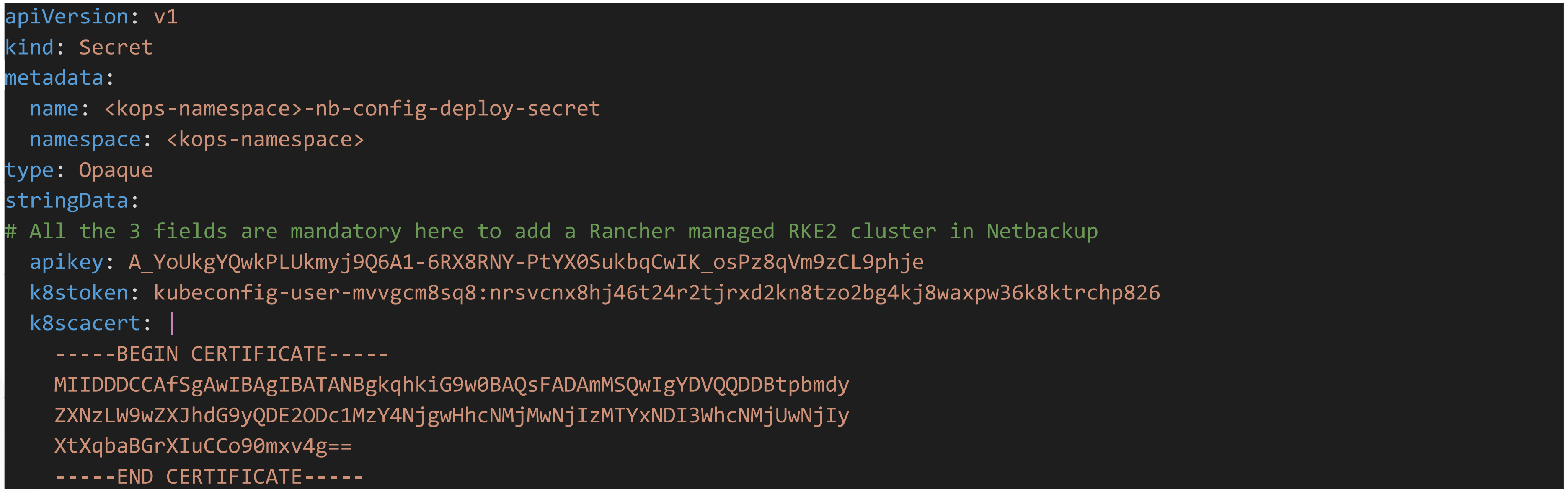
Automated configuration for Rancher managed RKE2 clusters

Create a secret for external cert and token configuration

3-a. If you are protecting a Rancher Managed RKE2 cluster, then follow the steps on this slide.

- Create a yaml file with the following format.
- Enter the first 2 values which you extracted earlier from your temporary files into this file
- Once the **k8stoken** and **k8scacert** values have been entered, move to the API Key creation phase to enter the value for **apikey**

Sample file : nb-config-deploy-secret.yaml



```yaml
apiVersion: v1
kind: Secret
metadata:
  name: <kops-namespace>-nb-config-deploy-secret
  namespace: <kops-namespace>
type: Opaque
stringData:
# All the 3 fields are mandatory here to add a Rancher managed RKE2 cluster in Netbackup
  apikey: A_YoUkgYQwkPLUkmyj9Q6A1-6RX8RNY-PtYX0SukbqCwIK_osPz8qVm9zCL9phje
  k8stoken: kubeconfig-user-mvvgcm8sq8:nrsvcnx8hj46t24r2tjrxd2kn8tzo2bg4kj8waxpw36k8ktrchp826
  k8scacert: |
    -----BEGIN CERTIFICATE-----
    MIIDDDCCAfSgAwIBAgIBATANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDDBtpbmdy
    ZXNzLW9wZXJhdG9yQDE2ODc1MzY4NjgwHhcNMjMwNjIzMTYxNDI3WhcNMjUwNjIy
    XtXqbaBGrXIuCCo90mxv4g==
    -----END CERTIFICATE-----
```

Automated configuration : Custom CA cert config (Optional)

Create a secret for external cert configuration

3-b. External CA certificate configuration for non-rancher k8s clusters

Note: This configuration step is necessary if you have custom CA certificates configured on your cluster's API server for external access. This step can be ignored if there is no custom CA setup

- If you have the custom CA certificates available, then simply enter them directly in the configuration yaml file mentioned in the next slide.
- If you don't have the certificates available, you can extract them using the command given below on your Netbackup primary host.
- You can also use the **openssl** command tool to perform the same step on any Linux host.

```
<NBU_Install_Path>/bin/goodies/vxsslcmd s_client -showcerts -connect <cluster-fqdn>:<port-no> 2>/dev/null </dev/null
|  sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
```

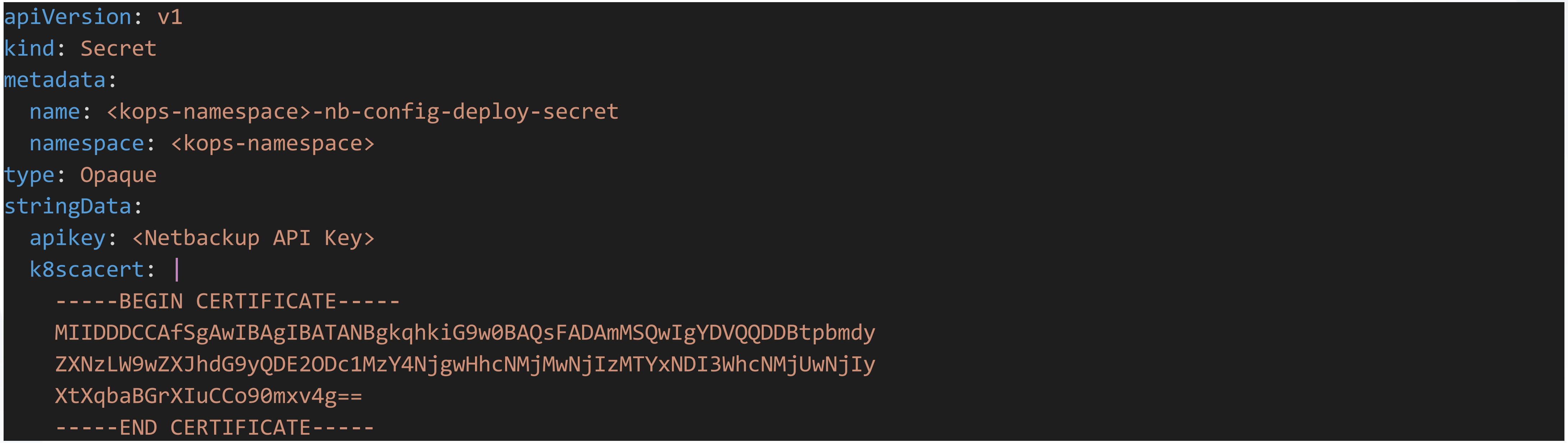
- Enter the certificate value which will be generated from the output of this command into the template file in the next step.

Automated configuration : Custom CA cert config (Optional)

Create a secret for external cert configuration

3-b. External CA certificate configuration for non-rancher k8s clusters using custom CA certs

- Prepare a yaml file based on the format shown below.
- **Note:-** Ensure the proper indentations are followed exactly like the template below.
- Enter the value which was extracted in the previous step into the **k8scacert** field & ensure the indentation is properly followed for the entire value.



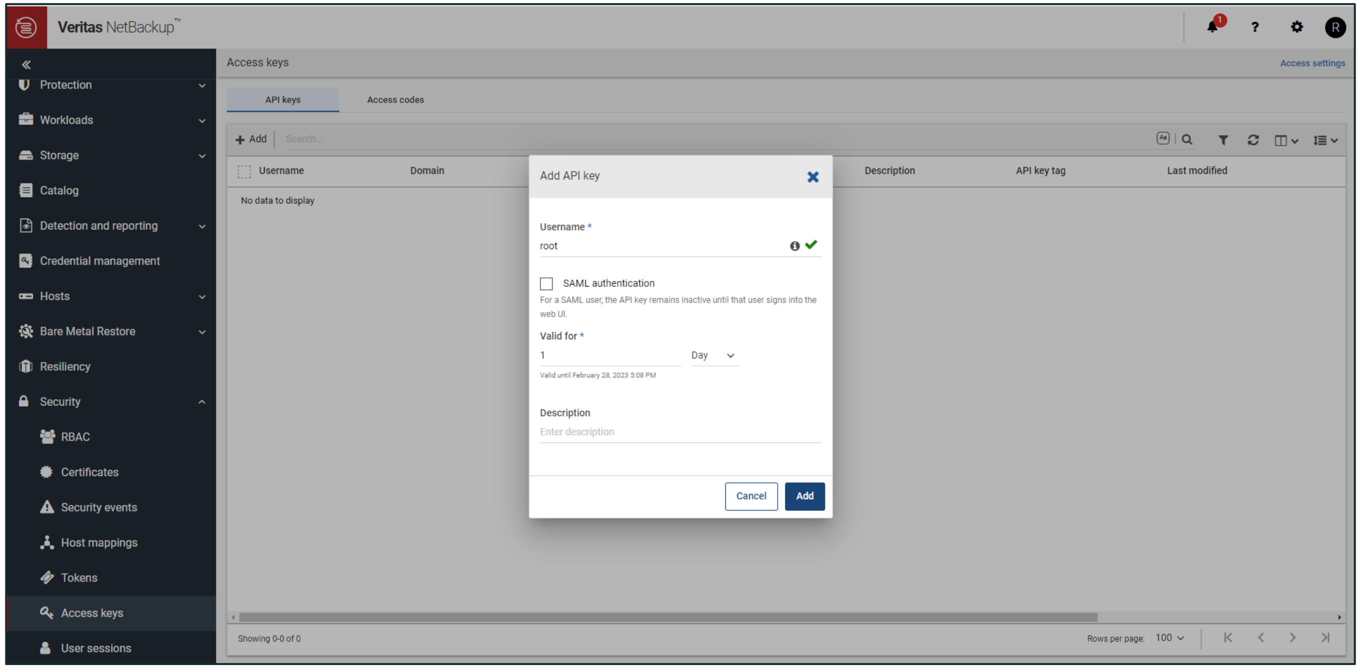
```
apiVersion: v1
kind: Secret
metadata:
  name: <kops-namespace>-nb-config-deploy-secret
  namespace: <kops-namespace>
type: Opaque
stringData:
  apikey: <Netbackup API Key>
  k8scacert: |
    -----BEGIN CERTIFICATE-----
    MIIDDDCCAfSgAwIBAgIBATANBgkqhkiG9w0BAQsFADAmMSQwIgYDVQQDDBtpbmdy
    ZXNzLW9wZXJhdG9yQDE2ODc1MzY4NjgwHhcNMjMwNjIzMTYxNDI3WhcNMjUwNjIy
    XtXqbaBGrXIuCCo90mxv4g==
    -----END CERTIFICATE-----
```

Automated configuration : API Key creation

Check Config deployment pod and create Netbackup API Key for nb-config-deploy-secret

4. If an API key already exists, same could be used in next step without creating a new api key. The details are hidden for already created apikey and must be collected from NetBackup admin.

To create a new API Key :
Go to the NetBackup web UI → Security → Access keys and click Add. Add Username and select validity of 1 day to avoid misuse of API Key. You must delete the Secret after the configuration is done.



Add API key

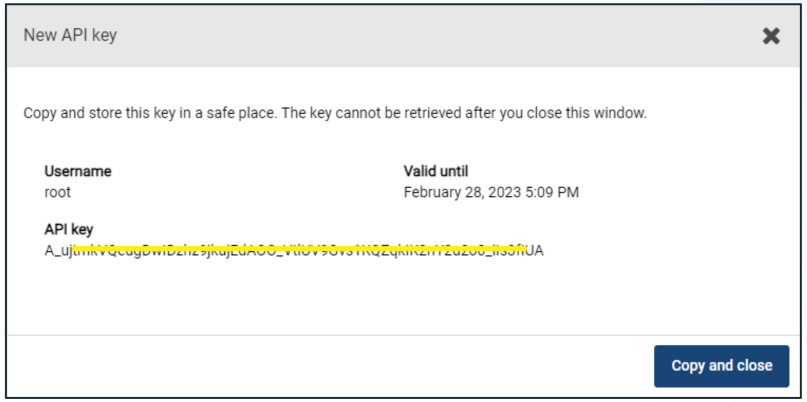
Username *
root

□ SAML authentication
For a SAML user, the API key remains inactive until that user signs into the web UI.

Valid for *
1 Day
Valid until February 28, 2023 5:08 PM

Description
Enter description

Cancel | Add



New API key

Copy and store this key in a safe place. The key cannot be retrieved after you close this window.

Username
root

Valid until
February 28, 2023 5:09 PM

API key
A_uj[redacted]UA

Copy and close

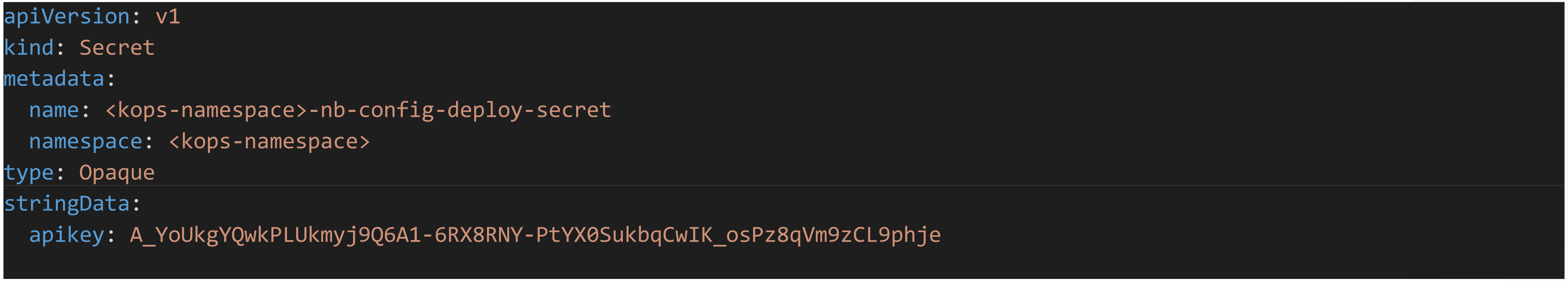
Automated configuration : API Key creation

Create secret for NetBackup configuration pod

Create a secret file as shown below containing NetBackup API key

Sample : **nb-config-deploy-secret.yaml**

Enter the API key value here which was extracted in the previous step.



```yaml
apiVersion: v1
kind: Secret
metadata:
  name: <kops-namespace>-nb-config-deploy-secret
  namespace: <kops-namespace>
type: Opaque
stringData:
  apikey: A_YoUkgYQwkPLUkmyj9Q6A1-6RX8RNY-PtYX0SukbqCwIK_osPz8qVm9zCL9phje
```

Once the file is ready with the values run :

*kubectl apply -f **nb-config-deploy-secret.yaml***

Automated configuration : Deploy the NetBackup Kubernetes Operator

Install operator via the Helm Chart

1. Ensure the **<kops-namespace>-nb-config-deploy-secret** has been created before running the helm install on the next step.

2. Run the following command to install the NetBackup Kubernetes Operator:

   helm install <user defined name of the deployment> ./netbackupkops-helm-chart -n <kops-namespace>

   An example:

   helm install veritas-netbackupkops ./netbackupkops-helm-chart -n netbackup

3. To check the status of the deployments, run the command:

   kubectl get pods -n <kops-namespace>

   An example:

   kubectl get pods -n netbackup

4. To verify that Kubernetes cluster is added to NetBackup, open NetBackup UI → Workloads → Kubernetes → Kubernetes Clusters. Kubernetes cluster should be listed on this page.
   If there is an issue, please check troubleshooting steps on next page.

Automated configuration

Troubleshooting the NetBackup configuration pod

Troubleshooting the configuration pod :

1. To check configuration pod logs using the following commands:
   ```
   kubectl get pods -n <kops-namespace>
   kubectl logs <netbackup-config-pod-name> -n <kops-namespace> > config-deploy.log
   ```
2. If you see any failures in the deployment due to incorrect input values, set the replica count to zero for deployment <kops-namespace>-netbackup-config-deploy to remove the deploy pod.
   ```
   kubectl scale deployment <kops-namespace>-netbackup-config-deploy -n <kops-namespace> --replicas=0
   ```
3. Correct the input values in deployment config.
   ```
   kubectl edit deployment <kops-namespace>-netbackup-config-deploy -n <kops-namespace>
   ```
4. Again, set the replica count to 1 to restart configuration. Use below command to set the replica count:
   ```
   kubectl scale deployment <kops-namespace>-netbackup-config-deploy -n <kops-namespace> --replicas=1
   ```

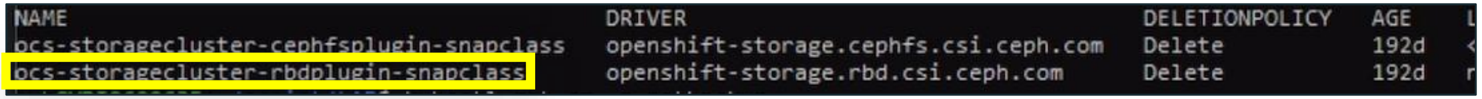
NetBackup Kubernetes Operator deployment and configuration using manual steps

Label storage for backup and restore

Prepare storage

Check for the valid volume snapshot class available in your environment

1. To see what volume snapshot classes are available in the environment, run the following command:
   - ***kubectl get volumesnapshotclass***
   - Following is the output example, you can see:



```
NAME                                          DRIVER                                  DELETIONPOLICY   AGE   L
ocs-storagecluster-cephfsplugin-snapclass    openshift-storage.cephfs.csi.ceph.com   Delete           192d  <
ocs-storagecluster-rbdplugin-snapclass       openshift-storage.rbd.csi.ceph.com      Delete           192d  r
```

   - The parameter you will use is the value in the name field from this command that is associated with the appropriate CSI driver.

2. User must label a valid volume snapshot classes on the block and file system volume snapshot classes to create a block and file system volume snapshots for NetBackup usage.

Prepare storage

Label a valid volume snapshot class for NetBackup usage

3. Add the following label on the block and file system volume snapshot classes to create block and file system volume snapshots:

   netbackup.veritas.com/default-csi-volume-snapshot-class=true

4. Run the following commands:

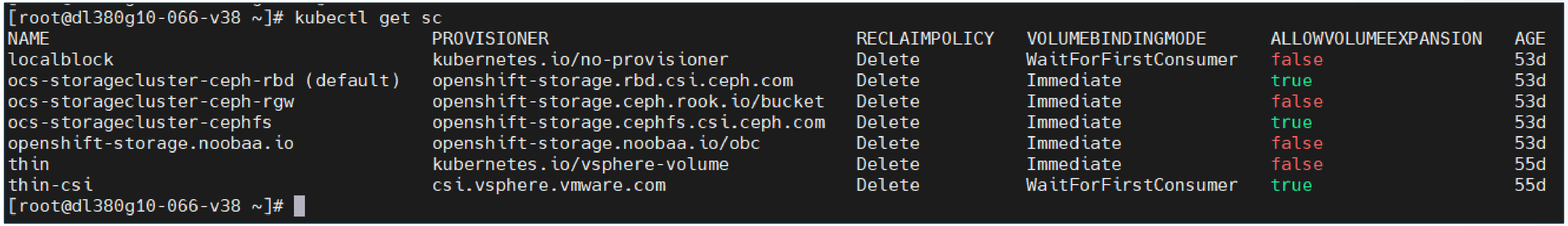
   ```
   kubectl label volumesnapshotclass <block-vol-snap-class-name> netbackup.veritas.com/default-csi-volume-snapshot-class=true
   kubectl label volumesnapshotclass <filesystem-vol-snap-class-name> netbackup.veritas.com/default-csi-volume-snapshot-class=true
   ```

5. If the NetBackup labeled VolumeSnapshotClass class is not found, then snapshot of a namespace consisting of persistent volume fails with an error message: Failed to create snapshot of the Kubernetes namespace.

Prepare storage

Check for the storage available in your environment

6. To see storage classes available in the environment, run the following command:
   - ***kubectl get sc***
   - Following is the output example, you can see:



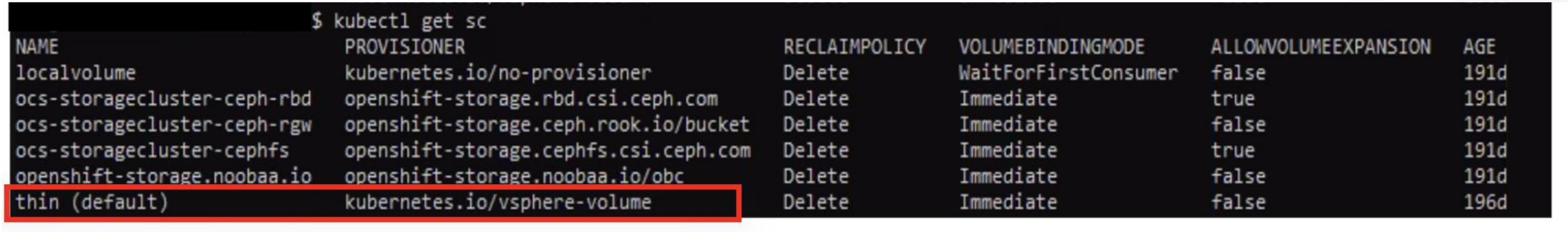
```
[root@dl380g10-066-v38 ~]# kubectl get sc
NAME                                    PROVISIONER                             RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
localblock                              kubernetes.io/no-provisioner            Delete          WaitForFirstConsumer   false                  53d
ocs-storagecluster-ceph-rbd (default)   openshift-storage.rbd.csi.ceph.com      Delete          Immediate              true                   53d
ocs-storagecluster-ceph-rgw             openshift-storage.ceph.rook.io/bucket   Delete          Immediate              false                  53d
ocs-storagecluster-cephfs               openshift-storage.cephfs.csi.ceph.com   Delete          Immediate              true                   53d
openshift-storage.noobaa.io             openshift-storage.noobaa.io/obc         Delete          Immediate              false                  53d
thin                                    kubernetes.io/vsphere-volume            Delete          Immediate              false                  55d
thin-csi                                csi.vsphere.vmware.com                  Delete          WaitForFirstConsumer   true                   55d
[root@dl380g10-066-v38 ~]#
```

7. Look for the storage that has CSI drivers listed under provisioner which consists of CSI in the name.
8. You must label each of the CSI supported storage classes with the labels in this section.

Prepare storage

Validate the storage you use for deploying namespaces

9. The command ‘kubectl get sc’ you ran earlier takes note of the default storage listed:



```
[redacted] $ kubectl get sc
NAME                          PROVISIONER                              RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
localvolume                   kubernetes.io/no-provisioner             Delete          WaitForFirstConsumer   false                  191d
ocs-storagecluster-ceph-rbd   openshift-storage.rbd.csi.ceph.com       Delete          Immediate              true                   191d
ocs-storagecluster-ceph-rgw   openshift-storage.ceph.rook.io/bucket    Delete          Immediate              false                  191d
ocs-storagecluster-cephfs     openshift-storage.cephfs.csi.ceph.com    Delete          Immediate              true                   191d
openshift-storage.noobaa.io   openshift-storage.noobaa.io/obc          Delete          Immediate              false                  191d
thin (default)                kubernetes.io/vsphere-volume             Delete          Immediate              false                  196d
```

10. If the default storage for the cluster is not associated with the CSI storage you labeled. Then, any namespaces created with default storage will not be able to protect.

11. Customers either must change the default storage to CSI storage which needs to protect, or explicitly point to the CSI storage when the namespaces are created.

Prepare storage

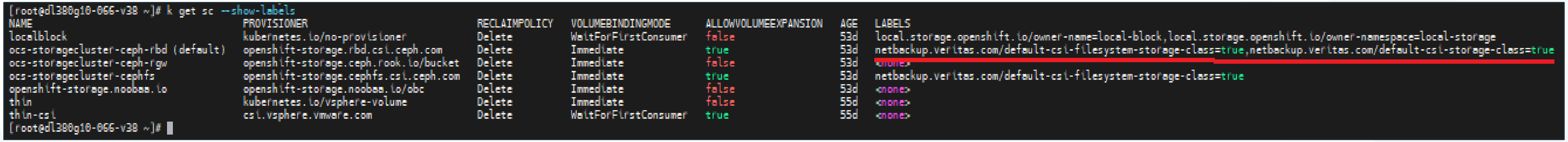
Label a valid storage class for NetBackup usage

12. Add the following labels on CSI supported storage class:
    - ***netbackup.veritas.com/default-csi-storage-class=true*** is used to label where storage class provisions volumes based on raw block.
    - **netbackup.veritas.com/default-csi-filesystem-storage-class=true** is used to label where storage class provisions volumes based on file system.
13. Run the following commands:
    - ***kubectl label sc <storage class> netbackup.veritas.com/default-csi-storage-class=true***
    - ***Kubectl label sc <storage class> netbackup.veritas.com/default-csi-filesystem-storage-class=true***
    - ***<Storage class> will be from the name section of the 'kubectl get sc' command for each CSI compliant storage you will need to protect.***
14. If NetBackup labeled storage class is not found, then backup from snapshot job for metadata image and restore jobs fails with an error message No eligible storage classes found.

Prepare storage

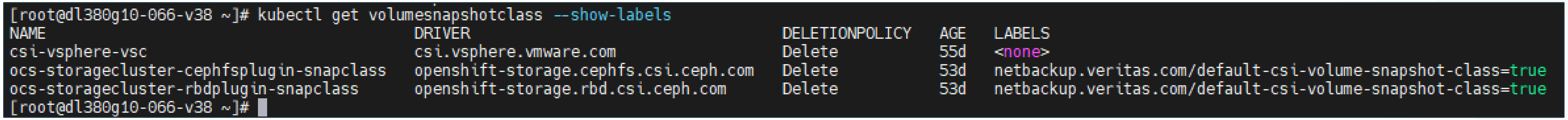
Validate that labels were applied

1. To verify the result, run the following commands:
   - *kubectl get sc --show-labels*



```
[root@dl380g10-066-v38 ~]# k get sc --show-labels
NAME                                    PROVISIONER                             RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE   LABELS
localblock                              kubernetes.io/no-provisioner            Delete          WaitForFirstConsumer   false                  53d   local.storage.openshift.io/owner-name=local-block,local.storage.openshift.io/owner-namespace=local-storage
ocs-storagecluster-ceph-rbd (default)   openshift-storage.rbd.csi.ceph.com      Delete          Immediate              true                   53d   netbackup.veritas.com/default-csi-filesystem-storage-class=true,netbackup.veritas.com/default-csi-storage-class=true
ocs-storagecluster-ceph-rgw             openshift-storage.ceph.rook.io/bucket   Delete          Immediate              false                  53d   <none>
ocs-storagecluster-cephfs               openshift-storage.cephfs.csi.ceph.com   Delete          Immediate              true                   53d   netbackup.veritas.com/default-csi-filesystem-storage-class=true
openshift-storage.noobaa.io             openshift-storage.noobaa.io/obc         Delete          Immediate              false                  53d   <none>
thin                                    kubernetes.io/vsphere-volume            Delete          Immediate              false                  55d   <none>
thin-csi                                csi.vsphere.vmware.com                  Delete          WaitForFirstConsumer   true                   55d   <none>
[root@dl380g10-066-v38 ~]#
```

   - *kubectl get volumesnapshotclass --show-labels*



```
[root@dl380g10-066-v38 ~]# kubectl get volumesnapshotclass --show-labels
NAME                                     DRIVER                                  DELETIONPOLICY   AGE   LABELS
csi-vsphere-vsc                          csi.vsphere.vmware.com                  Delete           55d   <none>
ocs-storagecluster-cephfsplugin-snapclass   openshift-storage.cephfs.csi.ceph.com   Delete           53d   netbackup.veritas.com/default-csi-volume-snapshot-class=true
ocs-storagecluster-rbdplugin-snapclass   openshift-storage.rbd.csi.ceph.com      Delete           53d   netbackup.veritas.com/default-csi-volume-snapshot-class=true
[root@dl380g10-066-v38 ~]#
```

Prerequisites for NetBackup backup from snapshot and restore from backup operations

Prerequisites for NetBackup BFS and RFS operations

- Ensure that the user label a valid storage class (Block and Filesystem) for NetBackup usage. (Refer :Prepare Storage section)

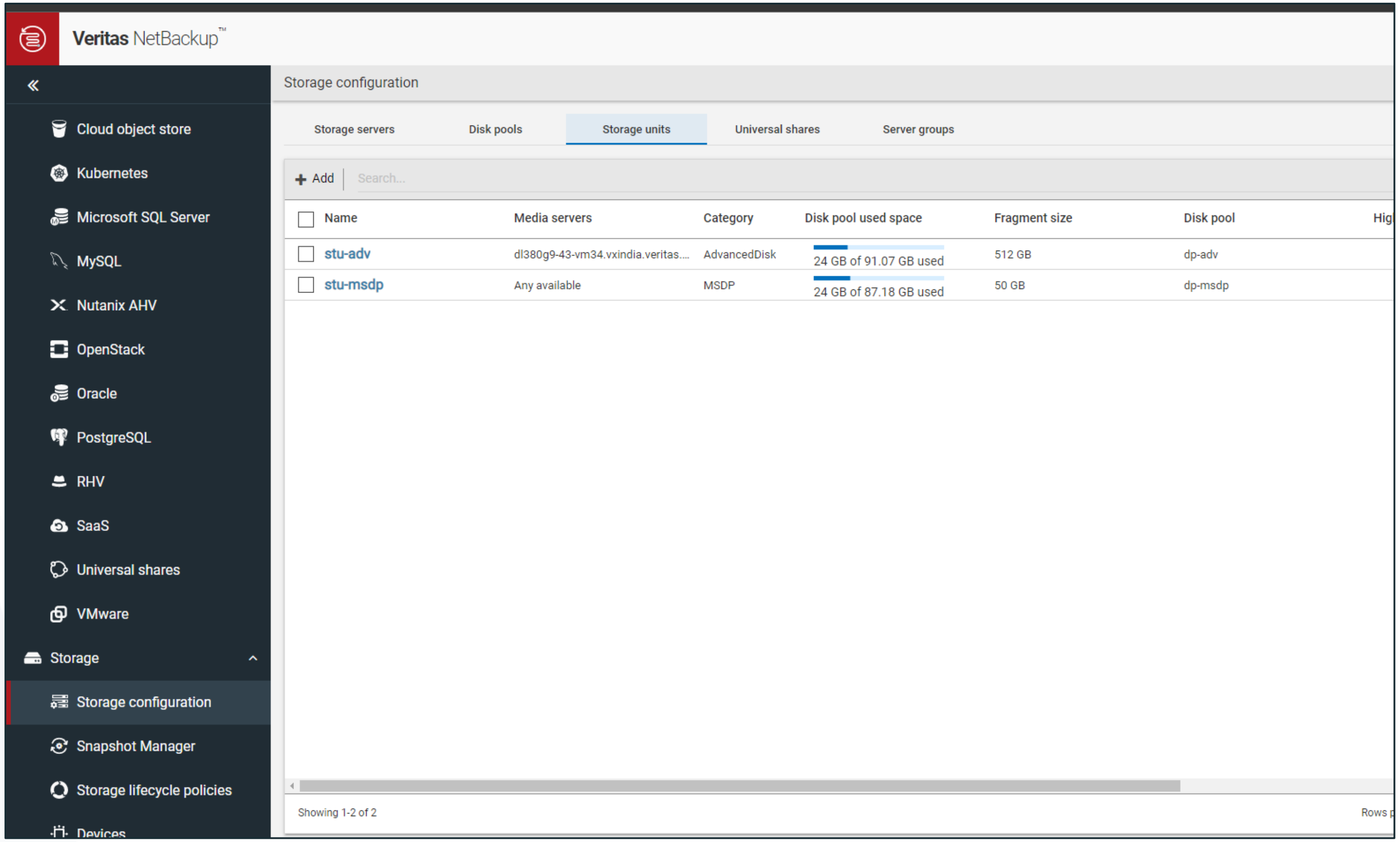
- Ensure that the user label a valid snapshotvolumeclass for NetBackup usage. (Refer: Prepare PV for Backup section)

- Each primary server which runs the backup from snapshot and restore from backup copy operations, needs to create a separate ConfigMap with the primary server's name. (Refer: Deploy the NetBackup Kubernetes Operator - Create configmap.yaml file for each Primary Server protecting the cluster)

- Ensure that the user deployed certificates on the Kubernetes operator. (Refer: Deploy certificates on the Kubernetes Operator section)

Configure Duplication

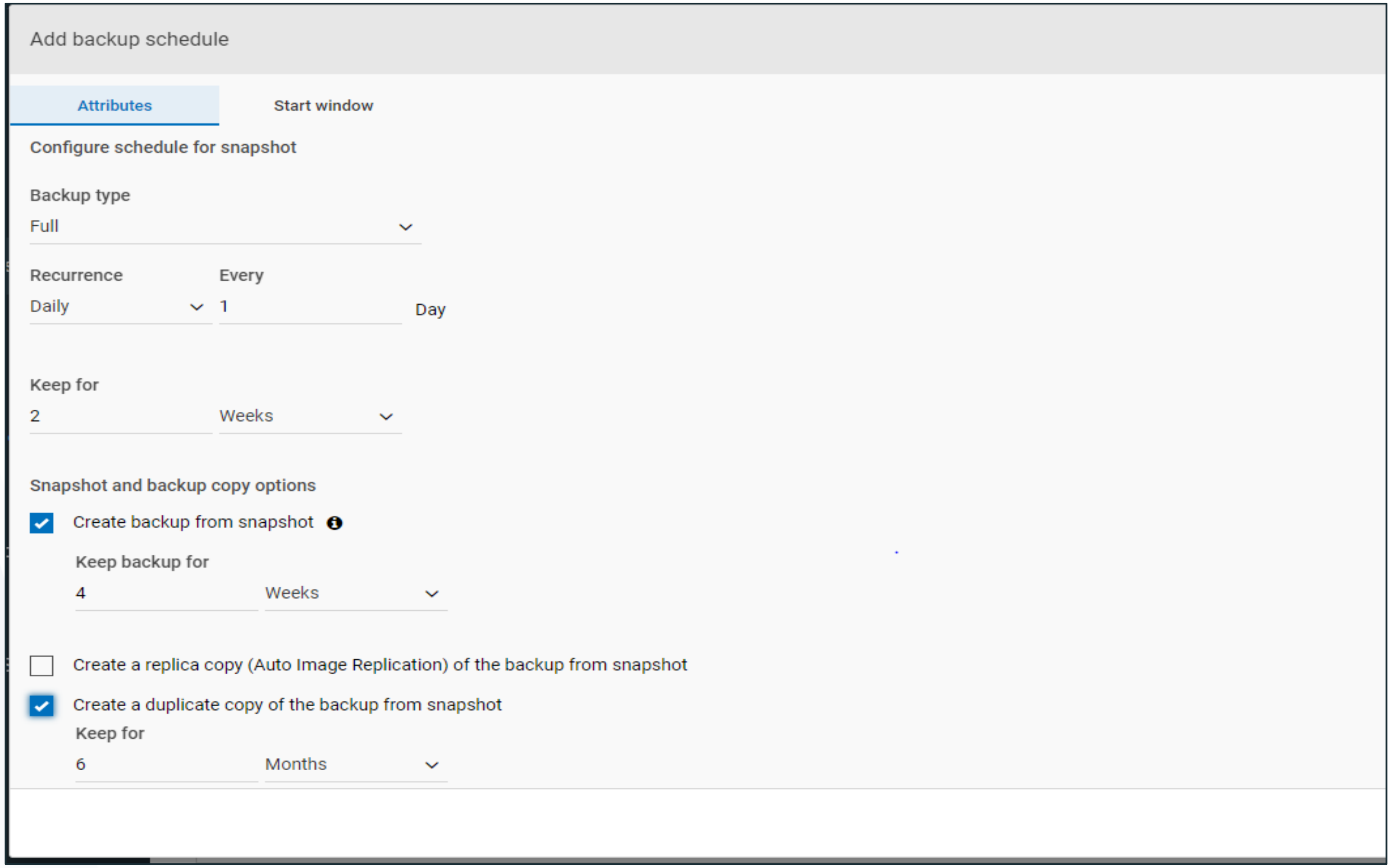
Configure Duplication



□ Name	Media servers	Category	Disk pool used space	Fragment size	Disk pool	Hig
□ stu-adv	dl380g9-43-vm34.vxindia.veritas....	AdvancedDisk	24 GB of 91.07 GB used	512 GB	dp-adv	
□ stu-msdp	Any available	MSDP	24 GB of 87.18 GB used	50 GB	dp-msdp	

1. Create Storage Unit to keep duplicate image copies.

Configure Duplication



Add backup schedule

Configure schedule for snapshot

Backup type: Full

Recurrence: Daily

Every: 1 Day

Keep for: 2 Weeks

Snapshot and backup copy options

☑ Create backup from snapshot

Keep backup for: 4 Weeks

□ Create a replica copy (Auto Image Replication) of the backup from snapshot

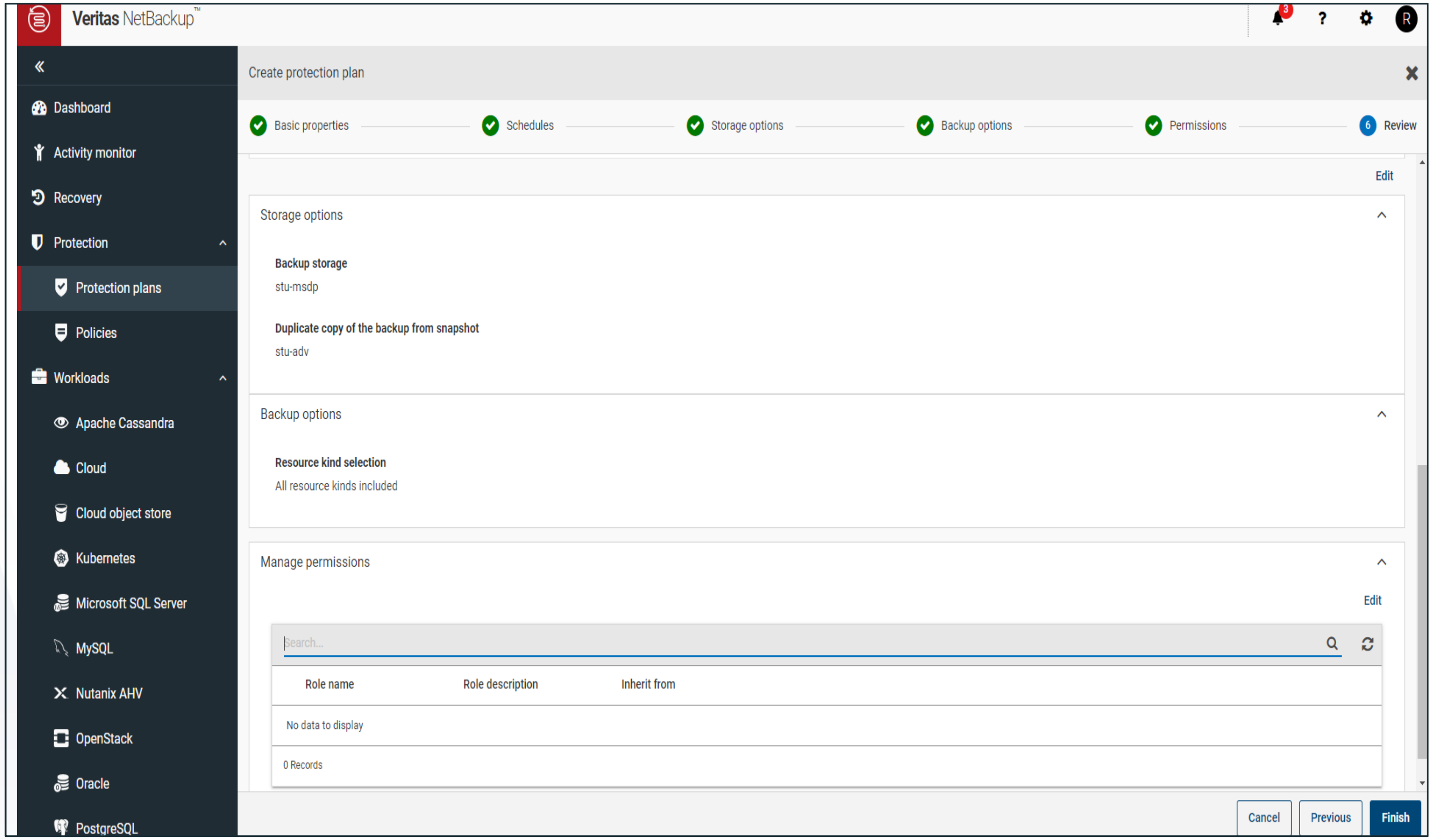
☑ Create a duplicate copy of the backup from snapshot

Keep for: 6 Months

2. Create Protection plan with duplication.

3. Enter retention period of each copies.

Configure Duplication



Create protection plan

Storage options

Backup storage
stu-msdp

Duplicate copy of the backup from snapshot
stu-adv

Backup options

Resource kind selection
All resource kinds included

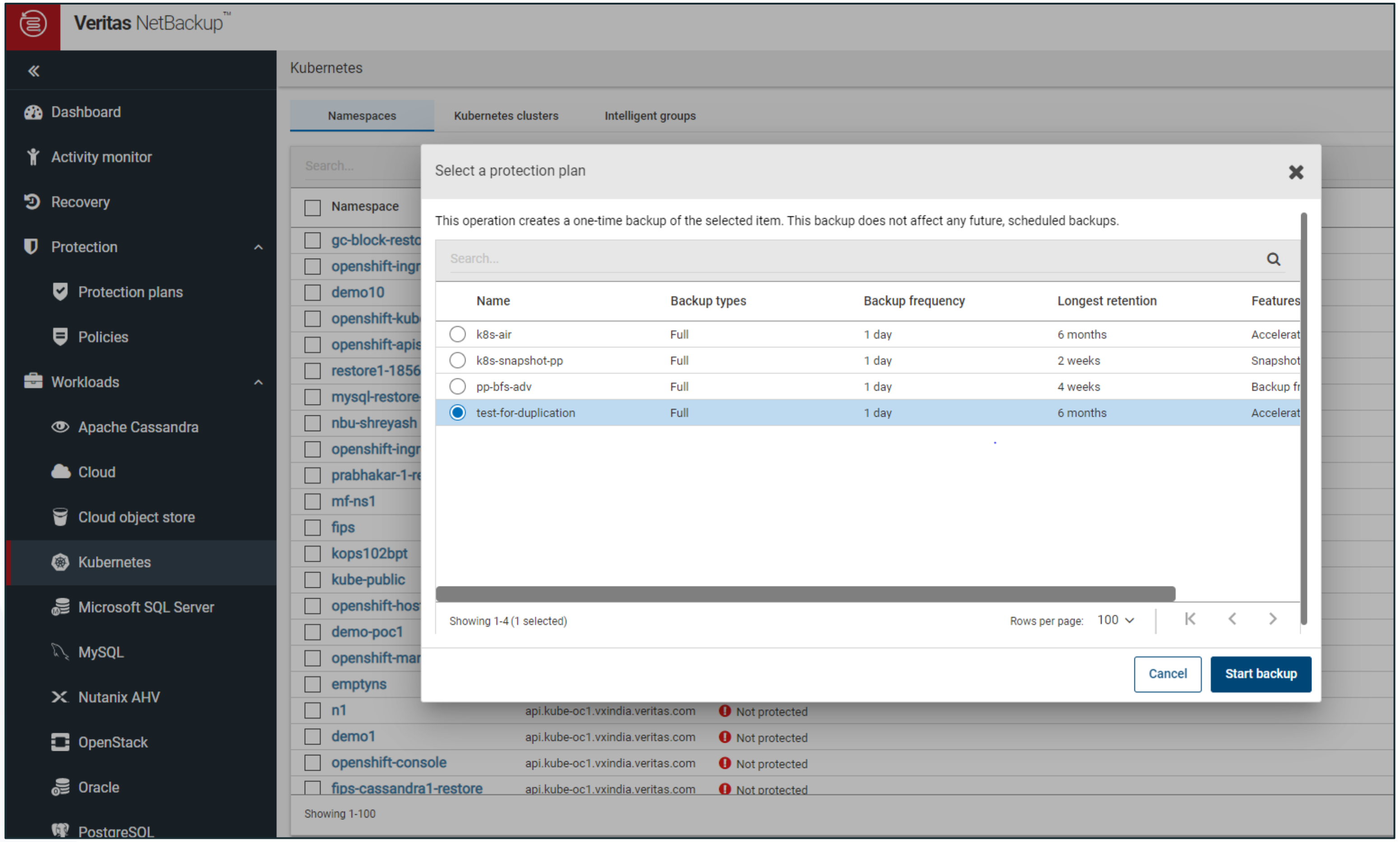
Manage permissions

Role name	Role description	Inherit from
No data to display		

0 Records

1. Enter storage for each copies during protection plan creation step.
2. Click Finish.

Configure Duplication



Select a protection plan ✖

This operation creates a one-time backup of the selected item. This backup does not affect any future, scheduled backups.

Search...

	Name	Backup types	Backup frequency	Longest retention	Features
○	k8s-air	Full	1 day	6 months	Accelerat
○	k8s-snapshot-pp	Full	1 day	2 weeks	Snapshot
○	pp-bfs-adv	Full	1 day	4 weeks	Backup fr
●	test-for-duplication	Full	1 day	6 months	Accelerat

Showing 1-4 (1 selected)

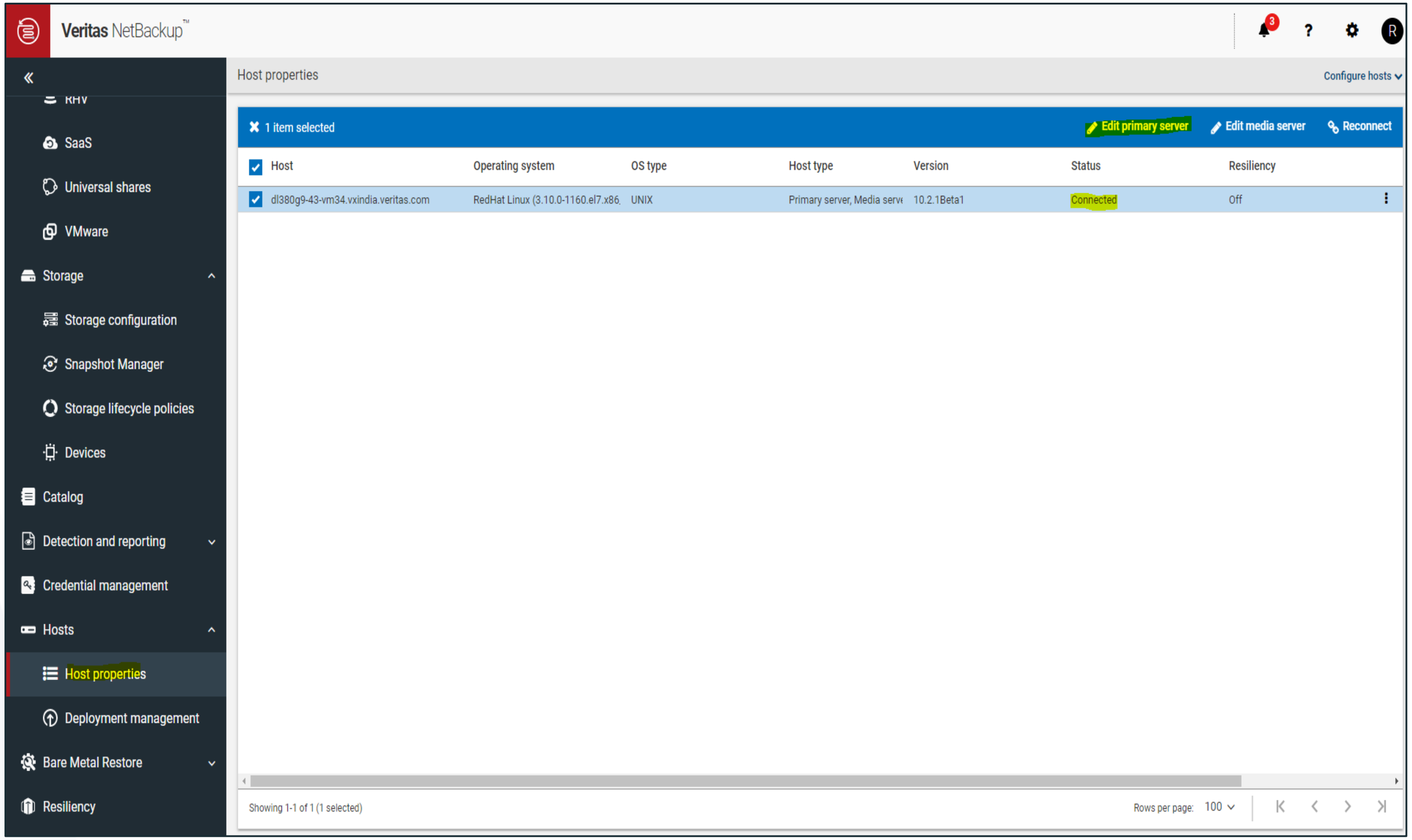
Rows per page: 100

Cancel | Start backup

3. Start backup of Kubernetes asset using the protection plan.
4. Duplication jobs gets triggered only after backup completed.
5. Duplication happen using the backup from snapshot copy

Configure Client-side Deduplication

Configure Client-side Deduplication



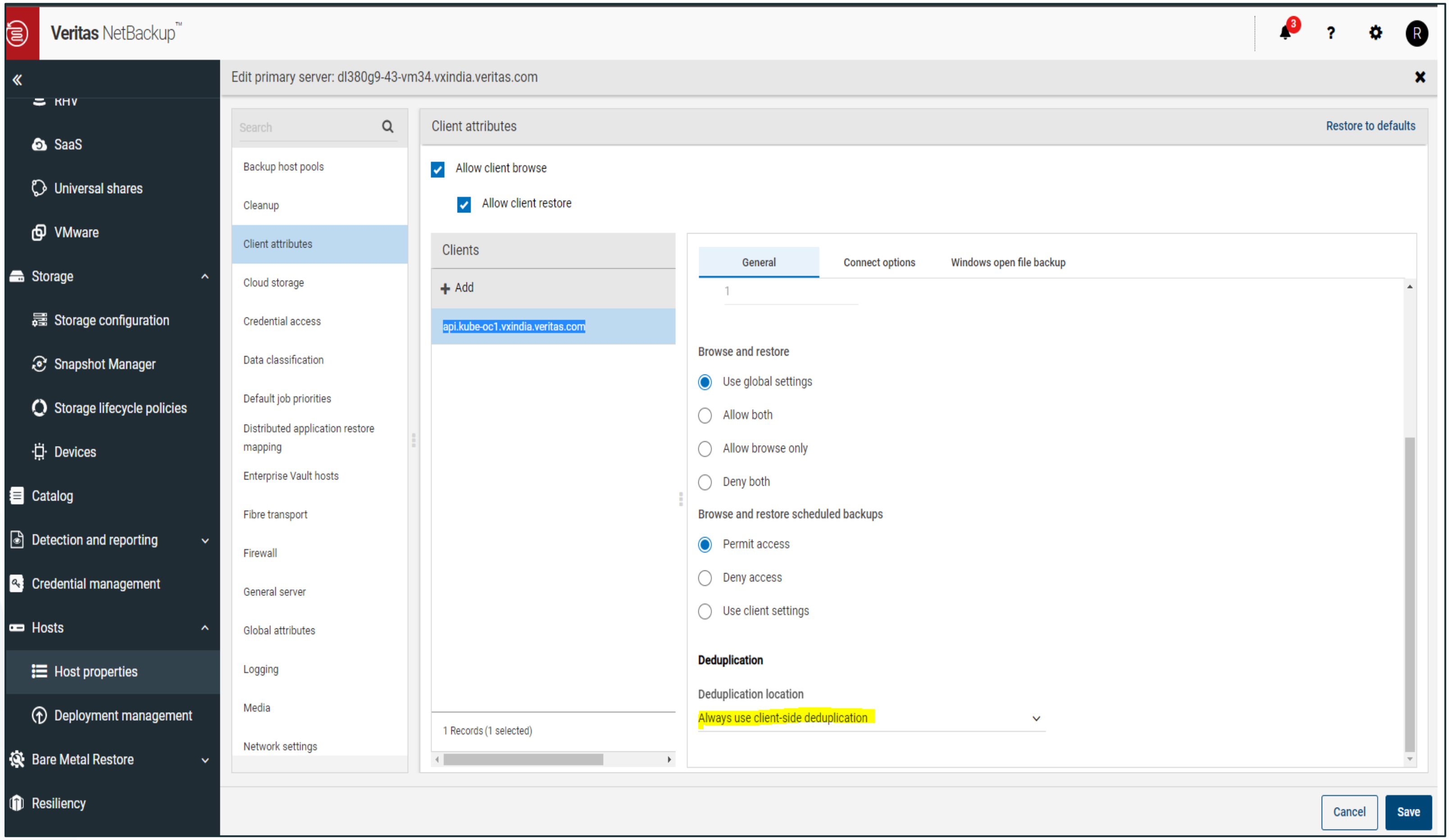
☑ Host	Operating system	OS type	Host type	Version	Status	Resiliency
☑ dl380g9-43-vm34.vxindia.veritas.com	RedHat Linux (3.10.0-1160.el7.x86_	UNIX	Primary server, Media serve	10.2.1Beta1	Connected	Off

Showing 1-1 of 1 (1 selected)

Rows per page: 100

Click **Host Properties** to connect to the primary server.

Configure Client-side Deduplication



Edit primary server: dl380g9-43-vm34.vxindia.veritas.com

Client attributes

☑ Allow client browse

☑ Allow client restore

Clients

api.kube-oc1.vxindia.veritas.com

1 Records (1 selected)

1

Browse and restore

● Use global settings

○ Allow both

○ Allow browse only

○ Deny both

Browse and restore scheduled backups

● Permit access

○ Deny access

○ Use client settings

Deduplication

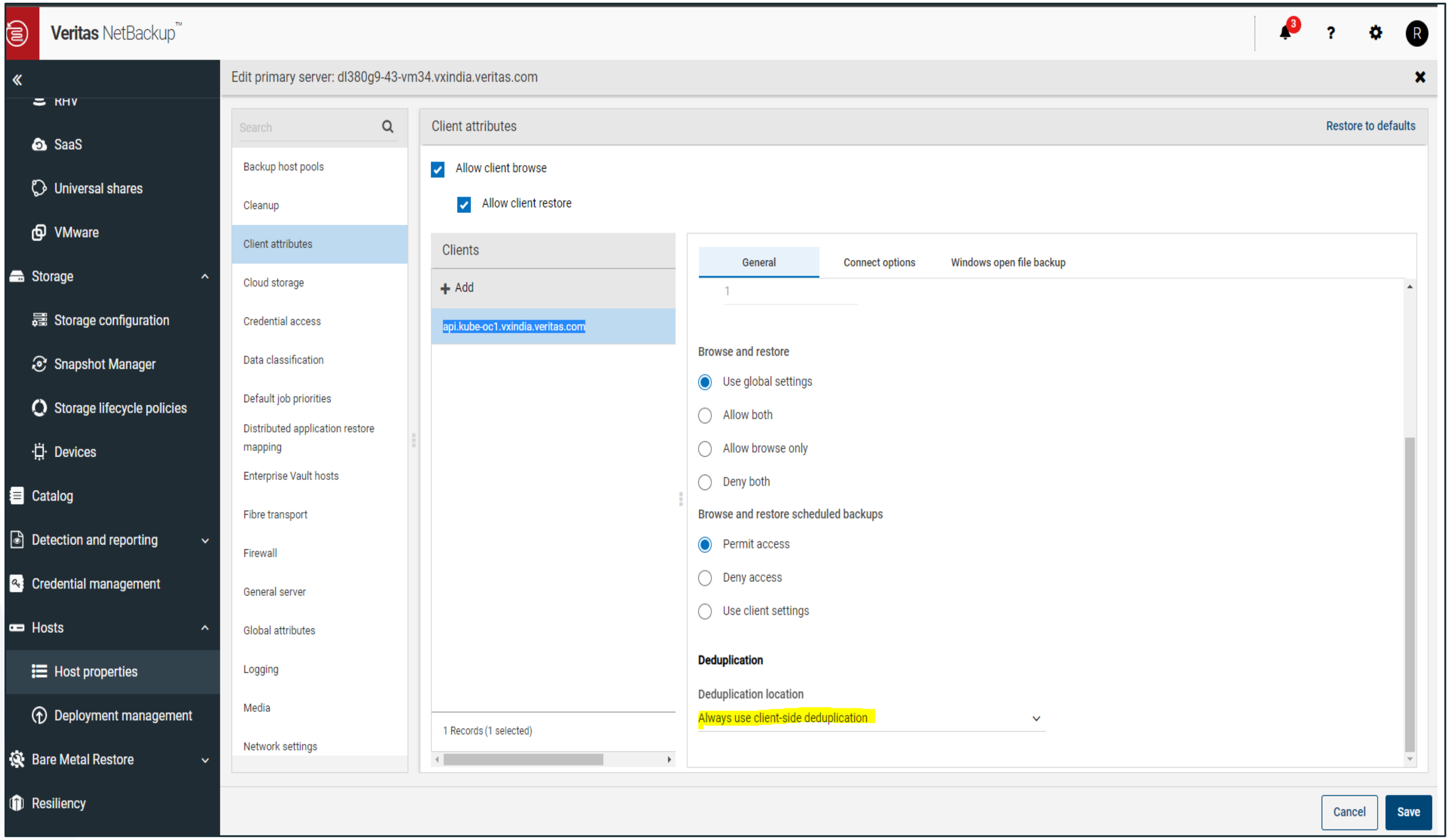
Deduplication location

Always use client-side deduplication

- Edit Primary server **Client attributes**, add Kubernetes cluster name under **Clients** tab.
- You can retrieve the Kubernetes cluster name running the following command on the cluster.

  kubectl cluster-info
- Cluster name can also be found on the NetBackup web UI.
- Workloads > **Kubernetes** > **Kubernetes clusters** > **Name** column.

Configure Client-side Deduplication



Edit primary server: dl380g9-43-vm34.vxindia.veritas.com

Client attributes

☑ Allow client browse

☑ Allow client restore

Clients

api.kube-oc1.vxindia.veritas.com

1 Records (1 selected)

Browse and restore

● Use global settings
○ Allow both
○ Allow browse only
○ Deny both

Browse and restore scheduled backups

● Permit access
○ Deny access
○ Use client settings

Deduplication

Deduplication location

Always use client-side deduplication

- ➢ Select **Always use client side deduplication** from deduplication location dropdown list.
- ➢ Click **Save**.

Note: Storage unit configured in Protection Plan for Backup from snapshot should be of MSDP type.

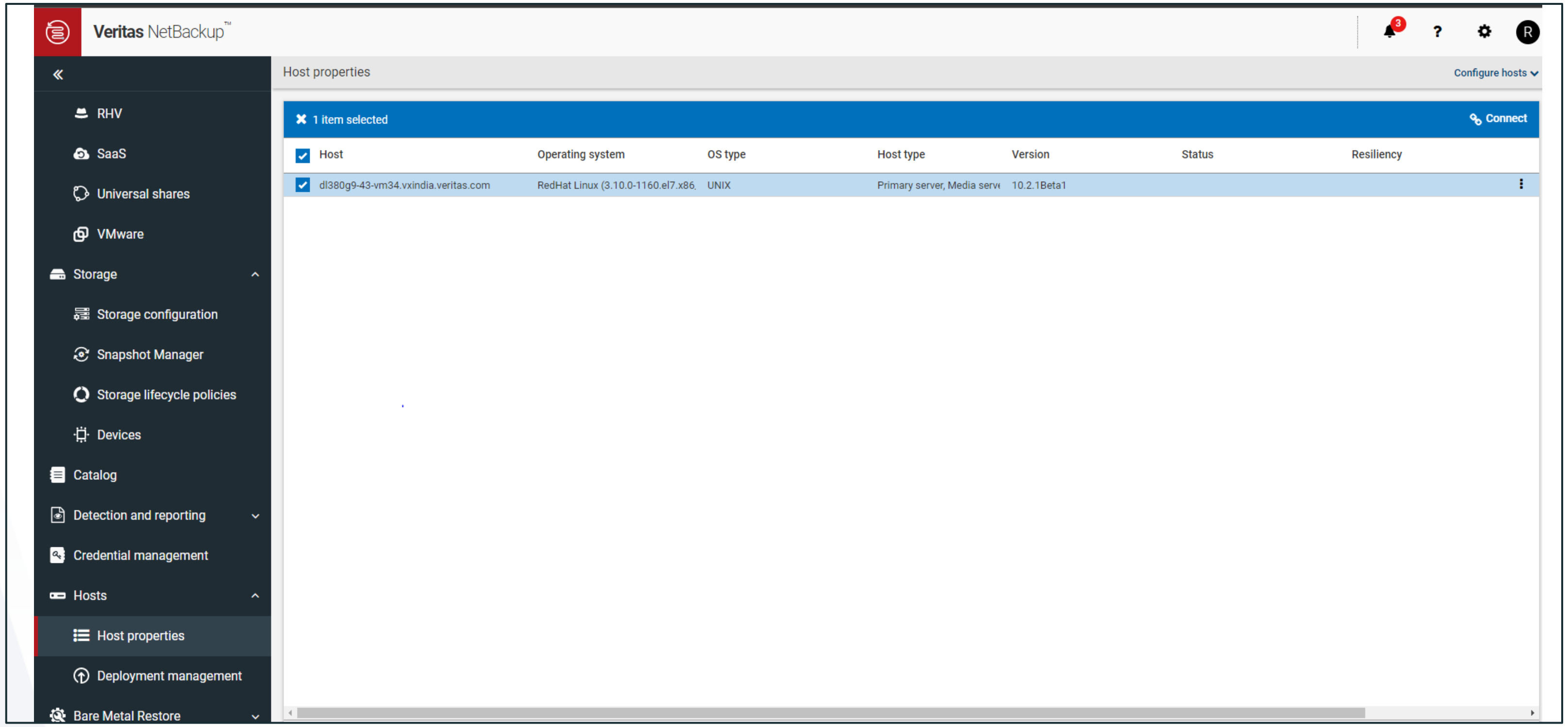
Configure Auto Image Replication(AIR)

Configure Auto Image Replication

Pre-requisite for AIR:

- ❑ Source and target NetBackup primary servers must have MSDP storage configured as storage unit.
- ❑ Source and target primary servers must be reachable to each other.

Configure Auto Image Replication



Host properties

✖ 1 item selected

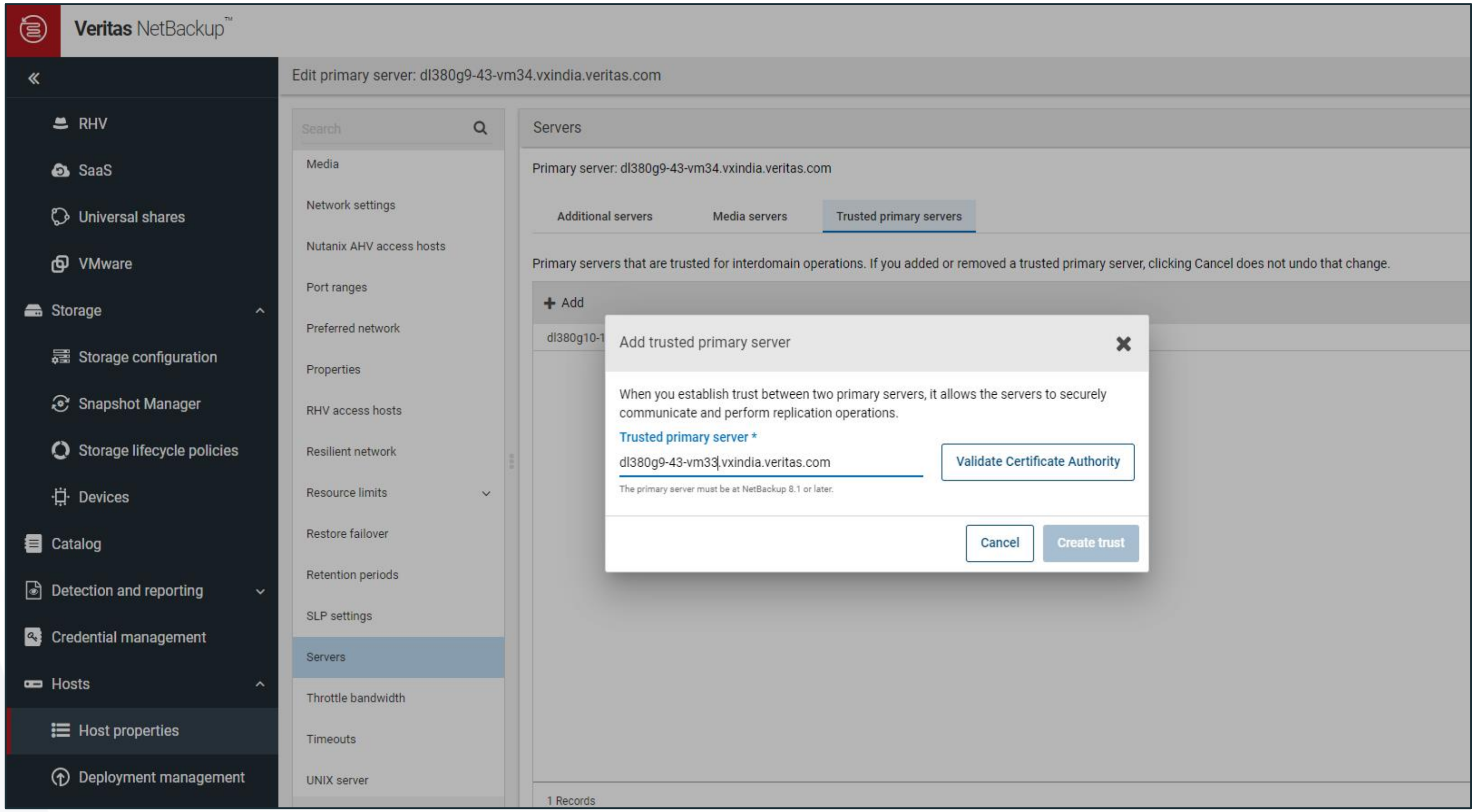
☑	Host	Operating system	OS type	Host type	Version	Status	Resiliency
☑	dl380g9-43-vm34.vxindia.veritas.com	RedHat Linux (3.10.0-1160.el7.x86_	UNIX	Primary server, Media serve	10.2.1Beta1		

Configuration on the source primary server.

Step 1

- Add target primary server entry under trusted servers.
- In the NetBackup web UI navigate to the Host properties
  - Select primary server in host entries, and connect.

Configure Auto Image Replication



Edit primary server: dl380g9-43-vm34.vxindia.veritas.com

Primary server: dl380g9-43-vm34.vxindia.veritas.com

Primary servers that are trusted for interdomain operations. If you added or removed a trusted primary server, clicking Cancel does not undo that change.

Add trusted primary server

When you establish trust between two primary servers, it allows the servers to securely communicate and perform replication operations.

Trusted primary server *: dl380g9-43-vm33.vxindia.veritas.com

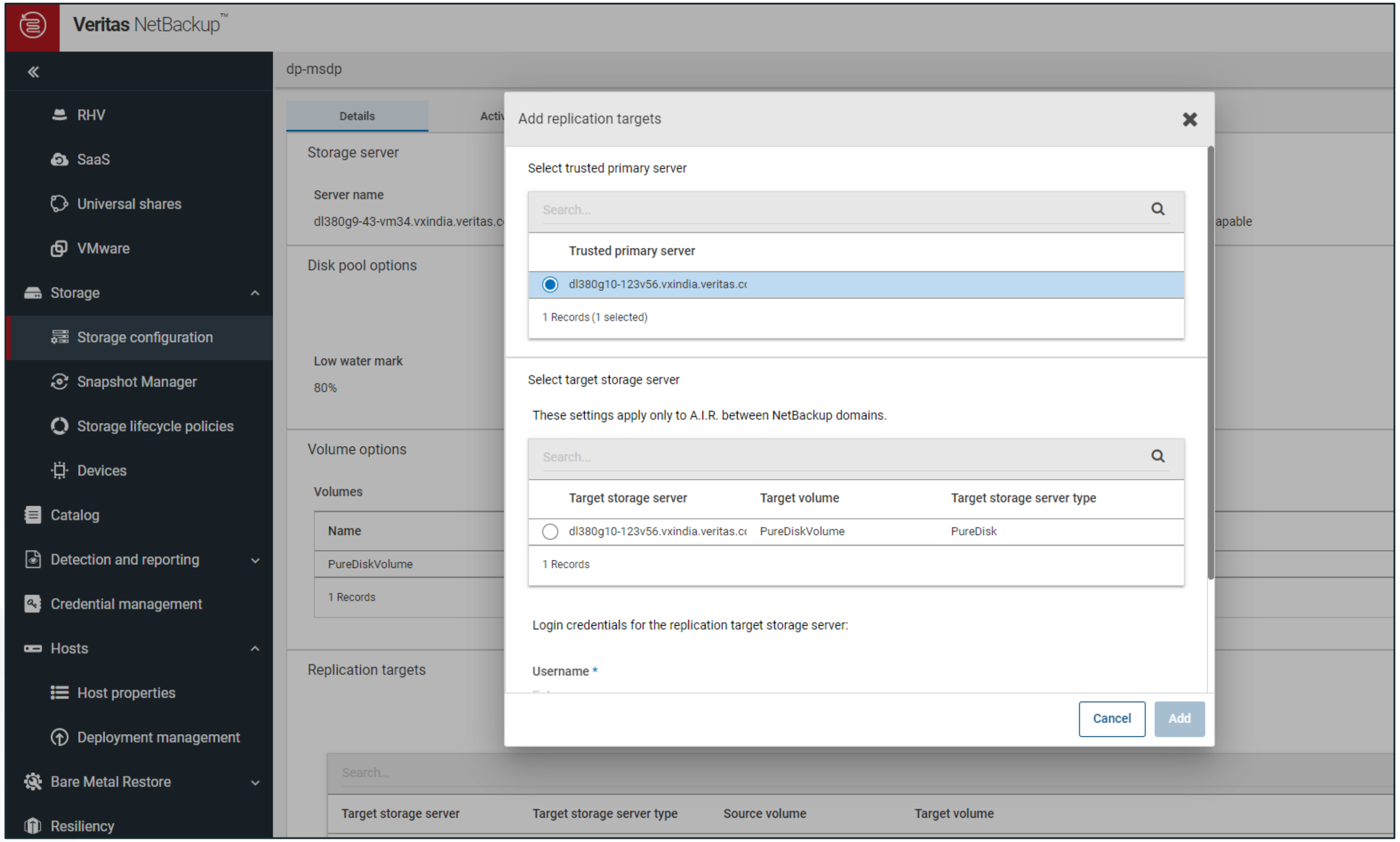
The primary server must be at NetBackup 8.1 or later.

Configuration on source primary server.

Step 2

- Navigate to **Servers** in **Edit Primary server** page
- Under **Trusted primary server** tab **Add** entry of target primary server.
- Click **Validate Certificate Authority**
- Enter **Target primary server credentials** and click **Create Trust.**

Configure Auto Image Replication



Storage server

Server name
dl380g9-43-vm34.vxindia.veritas.c

Disk pool options

Low water mark
80%

Volume options

Volumes

Name
PureDiskVolume

1 Records

Replication targets

Search...

Target storage server	Target storage server type	Source volume	Target volume

Add replication targets

Select trusted primary server

Search...

	Trusted primary server
●	dl380g10-123v56.vxindia.veritas.c

1 Records (1 selected)

Select target storage server

These settings apply only to A.I.R. between NetBackup domains.

Search...

	Target storage server	Target volume	Target storage server type
○	dl380g10-123v56.vxindia.veritas.c	PureDiskVolume	PureDisk

1 Records

Login credentials for the replication target storage server:

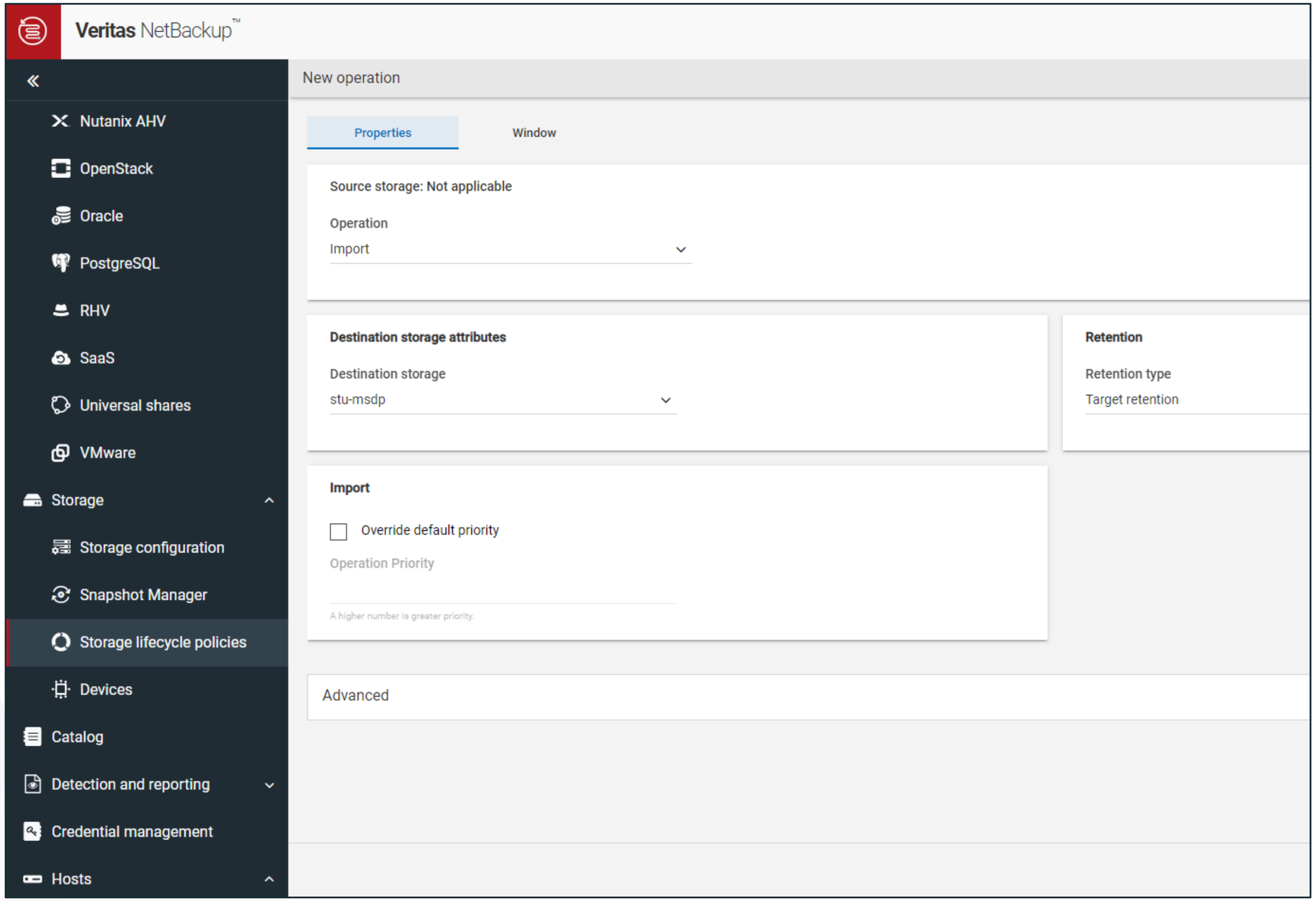
Username *

Configuration on source primary server.

Step 3

- ➢ Navigate to **Storage** > **Storage Configuration** in the NetBackup web UI
- ➢ Select **Disk-pools** tab.
- ➢ Select disk-pool having MSDP category
- ➢ Add entry for Replication targets.
  - ➢ Select trusted primary server
  - ➢ Enter the primary server credentials.
  - ➢ Click **Add**.

Configure Auto Image Replication



New operation

Properties | Window

Source storage: Not applicable

Operation: Import

Destination storage attributes

Destination storage: stu-msdp

Retention

Retention type: Target retention

Import

□ Override default priority

Operation Priority

A higher number is greater priority.

Advanced

Configuration on Target primary server.

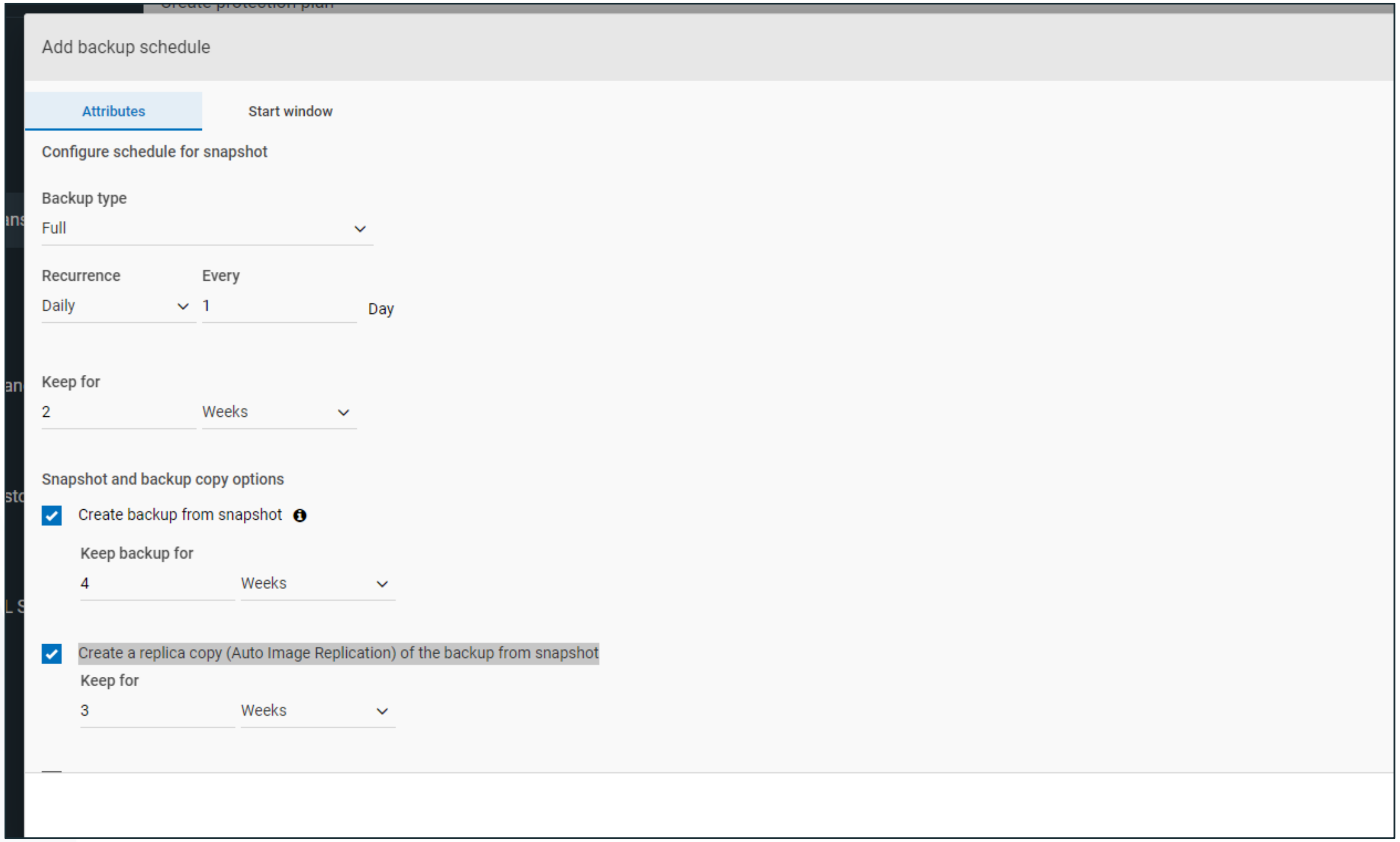
Step 1

Follow the Configuration of source primary server Step 1 and 2 to add trusted primary servers.

Step 2

- ➢ Create Storage lifecycle policies
- ➢ Navigate to Storage > Storage lifecycle policies in Target machine NetBackup web UI.
- ➢ Create SLP with operation import.
- ➢ Select Destination storage of MSDP type.
- ➢ Select Retention type.
- ➢ Click Create.
- ➢ Same SLP name is visible during configuration of source primary server step 5

Configure Auto Image Replication



Add backup schedule

Configure schedule for snapshot

Backup type: Full

Recurrence: Daily

Every: 1 Day

Keep for: 2 Weeks

Snapshot and backup copy options

☑ Create backup from snapshot

Keep backup for: 4 Weeks

☑ Create a replica copy (Auto Image Replication) of the backup from snapshot

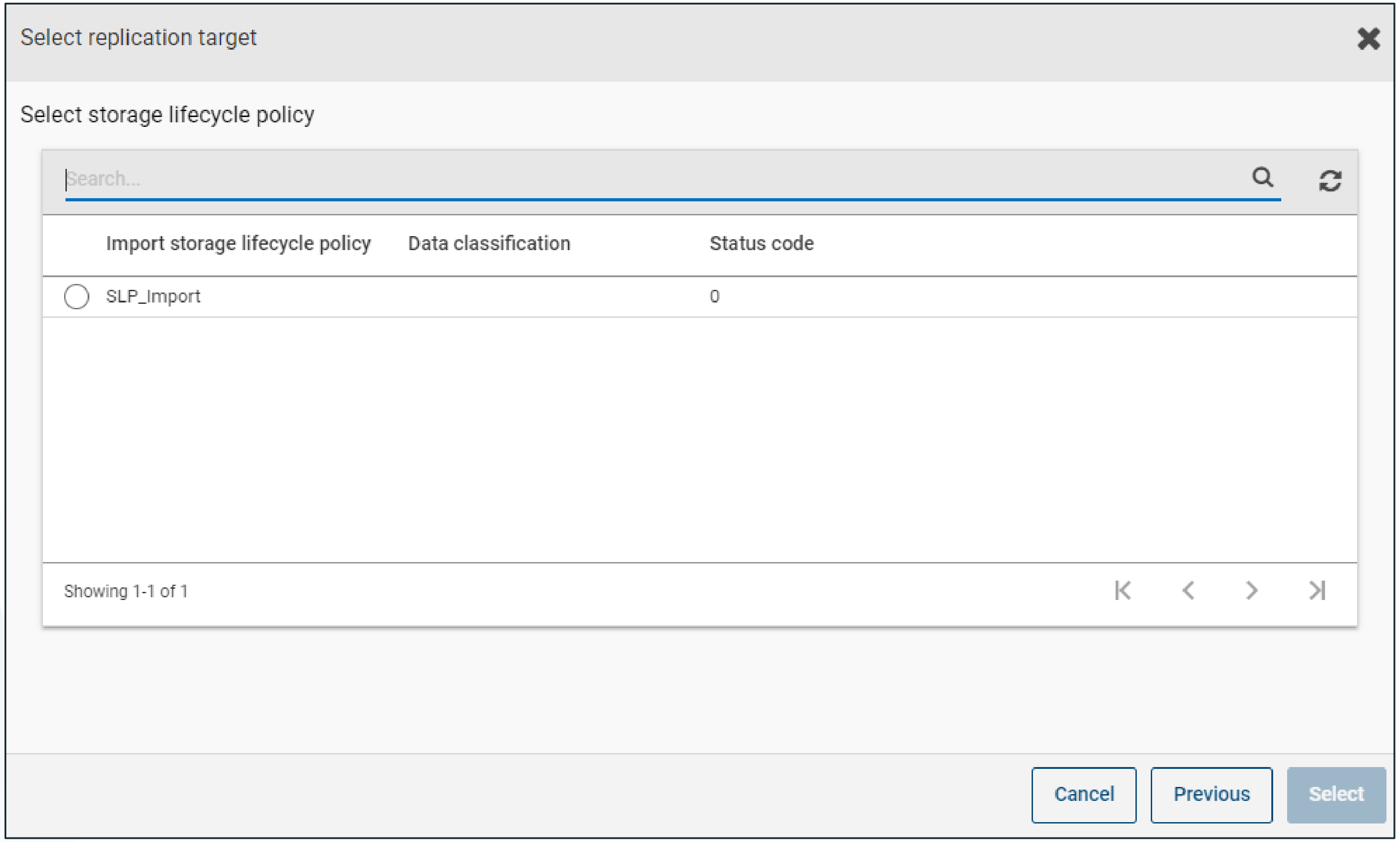
Keep for: 3 Weeks

Configuration on source primary server.

Step 4

- ➢ Create protection plan for Kubernetes workload, with **Create a replica copy (Auto Image Replication) of the backup from snapshot** option selected.
- ➢ Add Schedules of protection plan.

Configure Auto Image Replication



Select replication target

Select storage lifecycle policy

Search...

	Import storage lifecycle policy	Data classification	Status code
○	SLP_Import		0

Showing 1-1 of 1

Configuration on source primary server.

Step 5

- In **Create protection plan storage** options, select storage unit for backup from snapshot as local MSDP storage unit.
- For Replica copy of the backup from snapshot
  - Select target primary server.
  - Click **Next**.
  - Select storage lifecycle policy, this is created in “Configuration of target primary server step 2”
- Click **Next.**
- Select **Resource for Protection,** and click **Next.**
- Select the roles you want to have access to this protection plan.
- Click **Finish.**

FIPS Enablement

Configure FIPS enablement

Starting with NetBackup 10.2.1 (Sequoia) release, NetBackup K8s workload has started providing FIPS Support for Redhat based NetBackup deployments. All the K8s-WL component involving in NetBackup, NetBackup Kubernetes operator and NetBackup DataMover should be running in FIPS mode. In-order to achieve the FIPS support, there are certain requirements that needs to be met across all these components.

Configure FIPS enablement

System Requirement -

- NetBackup Primary and NetBackup Media
  - ❑ Both Primary and Media should be deployed on NetBackup 10.2.1 with underlying RHEL-8 system which is enabled with FIPS.
  - ❑ RHEL OS version should be greater than REHL8.
    - ○ You can check version of Redhat machine.
      - ▪ cat /etc/Redhat-release
    - ○ You can check if underlying system has FIPS is enabled using below command
      - ▪ fips-mode-setup --check
      - ▪ For more information, you can check man page entry for command fips-mode-setup

- Kubernetes Cluster
  - ❑ Kubernetes cluster should be deployed with FIPS enabled mode.
  - ❑ The process to deploy K8s cluster in FIPS mode in vendor dependent.
  - ❑ For example, deploying Openshift with FIPS Enabled.

Configure FIPS enablement

Configuration -

- NetBackup Primary and NetBackup Media
  - ❑ Enabling NetBackup process to run in FIPS mode –
    - ○ Update <Netbackup-Installation-Path>/netbackup/bp.conf with below key
    - ○ NB_FIPS_MODE = ENABLE

- NetBackup Kubernetes Operator
  - ❑ User can follow any one of the below steps to enable FIPS mode.
    - ○ Update the value of parameter **fipsMode to ENABLE** in values.yaml file from the Helm Chart.

      OR
    - ○ Update the value of parameter **NB_FIPS_MODE to ENABLE** in backup-operator.

Note – Customer need to make sure all the system on which K8s-WL is running are FIPS compliant.

Advanced troubleshooting

Troubleshooting

Troubleshooting of some known issues

- If Kubernetes add cluster operation fails in NetBackup with an error message Failed to validate cluster <cluster-name>. An unknown error occurred. Then, there may be the following reasons for failure:
  - ❑ User might have created credentials with incomplete ca.crt value in NetBackup.
  - ❑ The ca.crt value was properly copied but the cluster's service account and API endpoint have a different Certifying Authority (CA). User can check CA by extracting CA certificate from the cluster API endpoint.
  - ❑ Verify if <kops-namespace>-nb-config-deploy-secret has proper values for k8scacert,k8stoken with the right indentation.
- Solution: Refer to the techNote x509 certificate signed by unknown authority error during discovery and backupservercert configuration of NetBackup Kubernetes setup
- In customer environment, where access to external repositories is limited, to pull 'kube-rbac-proxy' image while deploying NetBackup Kops. NBUKops pod will fail to pull 'kube-rbac-proxy' image from external repositories.