VMware vSphere Virtual Volumes (vVols) with Hitachi Virtual Storage Platform

Quick Start and Reference Guide

MK-AS-608-05
December 2024

Feedback

Hitachi Vantara welcomes your feedback. Please share your thoughts by sending an email message to SolutionLab@hitachivantara.com. To assist the routing of this message, use the paper number in the subject and the title of this white paper in the text.

Table of Contents

Part 1. Prepare Storage 3

Step 1. Create Storage Pools 4

Step 2. Create a Resource Group 7

Step 3. Create an Administrator User Account for vVols 9

Step 4. Create a Protocol Endpoint and Add it to ESXi Hosts 11

Part 2. VMware vSphere Administrator – Set up Hitachi Storage Provider for VMware vCenter 13

Step 5. Deploy Hitachi Storage (VASA) Provider OVA 13

Step 6. Configure Hitachi Storage Provider for VMware vCenter 15

Step 7. Register Hitachi Storage Provider for VMware vCenter 19

Step 8. Verify that the PE is Available and Visible 22

Step 9. Create a vVols Datastore 25

Step 10. Create a Test VM to Verify vVol Operation 28

Step 11. Examples of Advanced Storage Capabilities and Storage Policy Based Management 28

Step 12. Deploy VMs with VMware SPBM and View vVols 35

Conclusion 38

VMware vSphere Virtual Volumes (vVols) with Hitachi Virtual Storage Platform

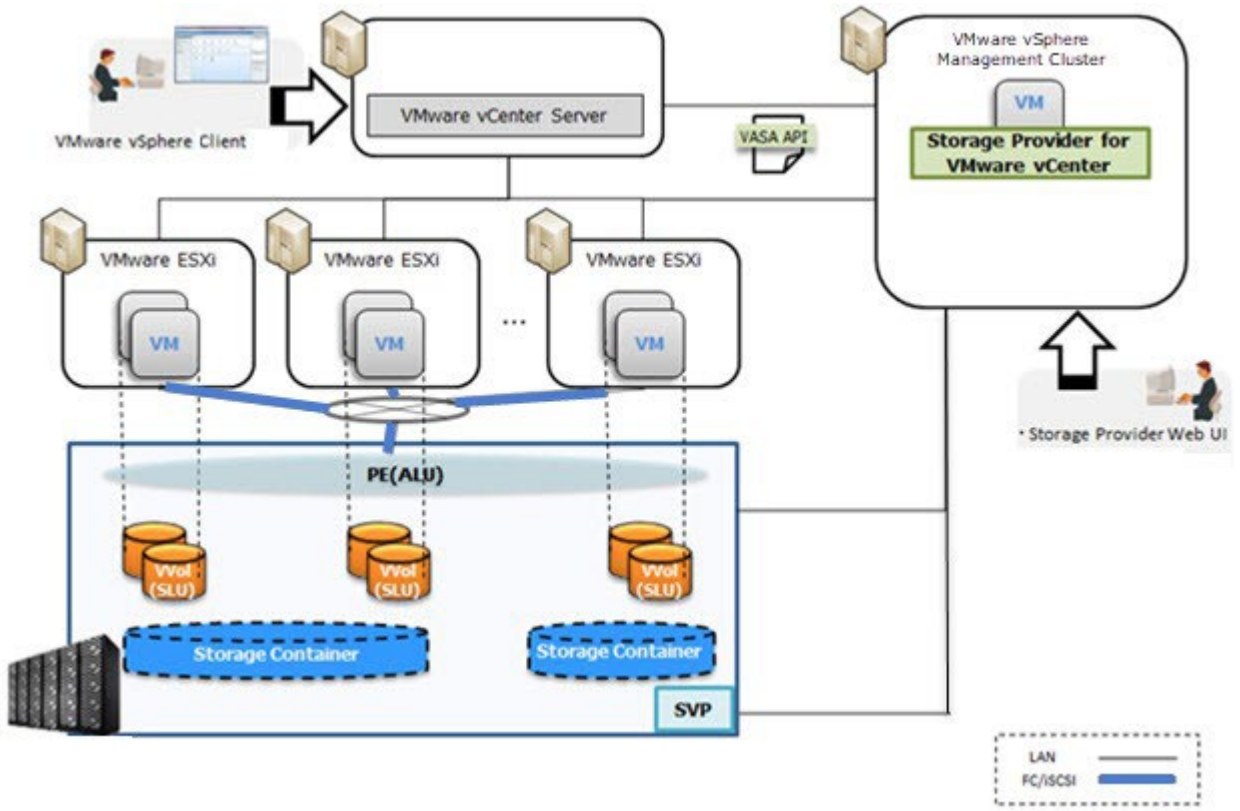
Quick Start and Reference Guide

This is a quick start guide for existing Hitachi Virtual Storage Platform (VSP) customers to set up their first VMware vSphere virtual volumes (vVols) environment**.**

This document describes the steps required to set up a vVols environment. The document assumes a greenfield environment with part 1 focusing on storage administrator actions, and part 2 for vSphere administrators. The vSphere administrator can skip to "Part 2. VMware vSphere Administrator – Set up Hitachi Storage Provider for VMware vCenter" on page 13.

Figure 1 shows the vVols architecture with Hitachi VSP series.

Figure 1



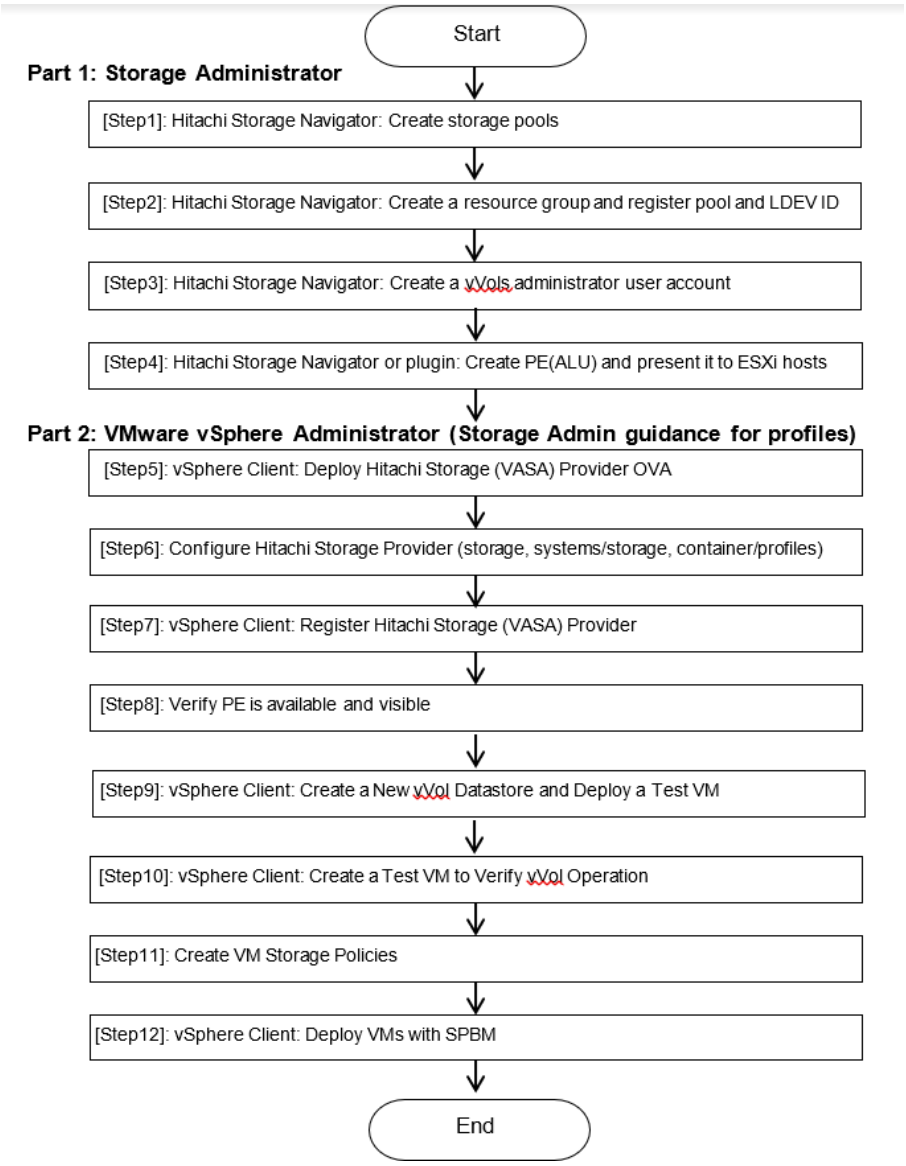
The Hitachi Storage Provider for VMware vCenter (VASA Provider) is deployed as an appliance virtual machine, similar to a vCenter or NSX appliance, into a management cluster. A single Hitachi VASA appliance can manage multiple arrays and connect with multiple vCenters to reduce management overhead.

The following are the prerequisites for a for a VMware vSphere vVols setup:

- Physical or VM-based SVP storage management node.
- Preferably a separate or a shared storage resource group. A meta resource group can also be used. (although a meta resource group can be used).

- One or more new or existing parity groups for HDP/HDT pools.
- One or more new or existing HDP/HDT pools.
- An HTI pool, for snapshots or clones, if using HDT pools.
- A dedicated storage user account with - admin privileges.
- IP address/FQDN for Hitachi Storage Provider for VMware vCenter.

This is an outline of the high-level procedure:



Part 1. Prepare Storage

To prepare storage for vVols, the storage administrators must run these procedures. Administrators can create a separate dedicated resource group for vVols or they can use the default resource group `meta_resource`. The next steps is to create and present a PE/ALU to ESXi hosts. Note that both vVols and VMFS datastores can share the same resource group.

If resource group is already created, you can skip to "Step 4. Create a Protocol Endpoint and Add it to ESXi Hosts" on page 11

The resource group for vVols contains the following:

- One or more dedicated dynamic pools (storage pools using HDP and/or HDT).
  - Dynamic provisioning pools cannot be shared with different resource groups.
  - LDEVs for vVols and LDEVs for VMFS datastores can co-exist in the same pool.
- An optional Hitachi Thin Image pool
  - If no Thin Image pool is added to the resource group, then the vVol snapshot images will be stored in the dynamic provisioning pool.
- LDEV IDs reserved for future vVols creation.

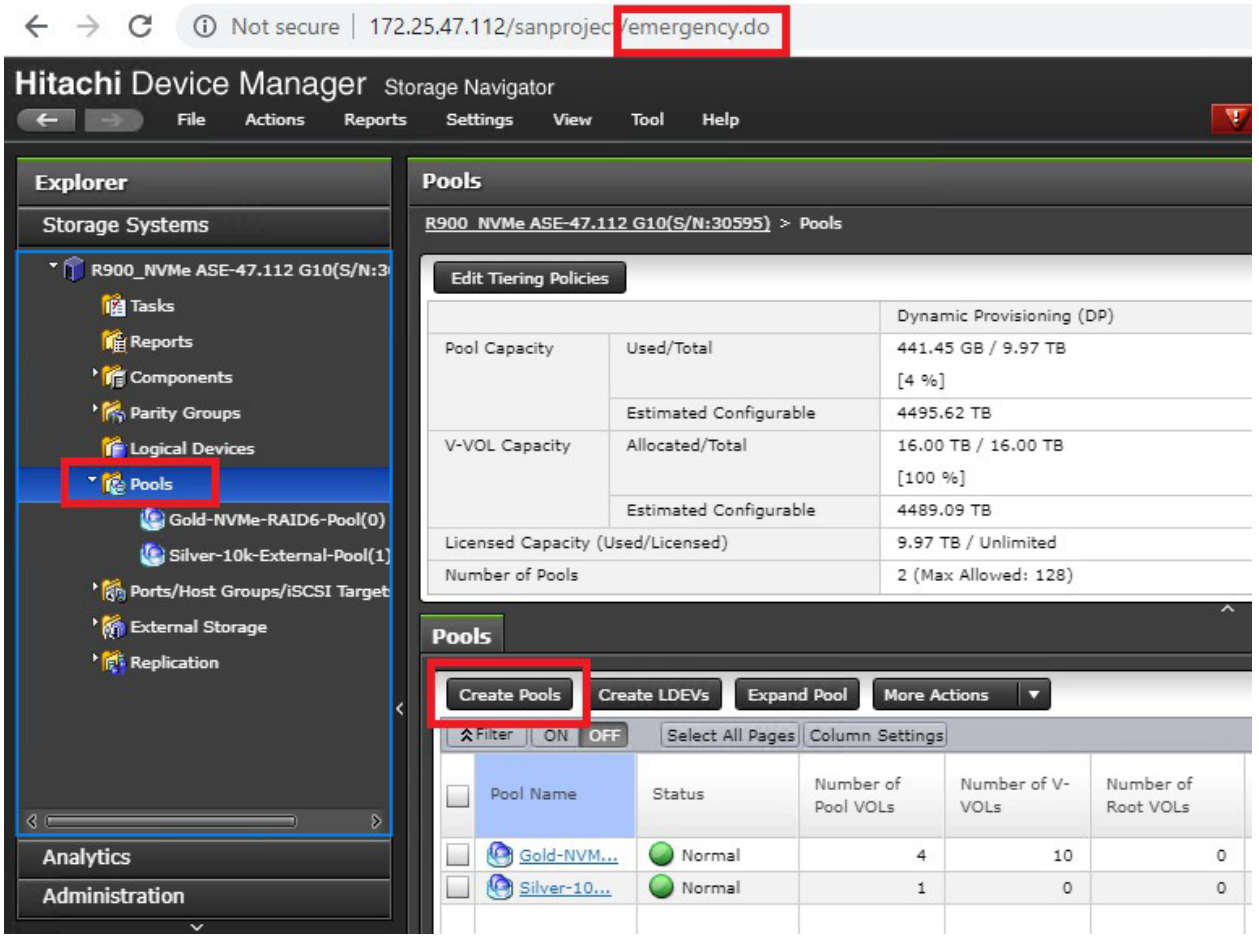
Step 1. Create Storage Pools

Log in to Hitachi Device Manager Storage Navigator. After entering the IP address of the Hitachi Virtual storage Platform (SVP) in the browser, you need to change the ending URL from `index.do` to `emergency.do` as shown in the following figure. You can create a dedicated storage pool for vVols or reuse an existing storage pool. To create a new pool, click **Create Pools**.

1. Log in to the Hitachi Device Manager Storage Navigator.

   After you enter the IP address of the SVP in the browser, change the ending URL from index.do to emergency.do, as shown in the following figure. You can create a dedicated storage pool for vVols or reuse an existing storage pool.

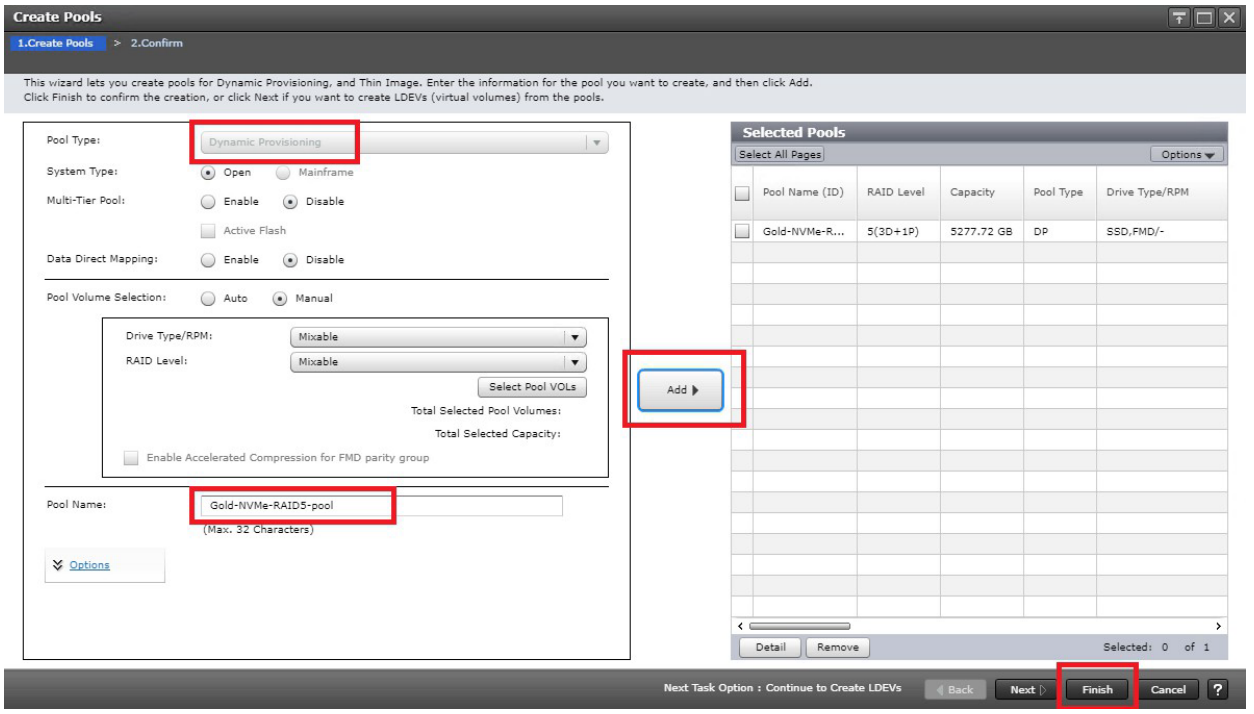
2. Click **Create Pools** to create a new pool.



3. Select **Dynamic Provisioning** for **Pool Type**.
4. Click **Select Pool VOLs** to select LDEVs to construct this storage pool.

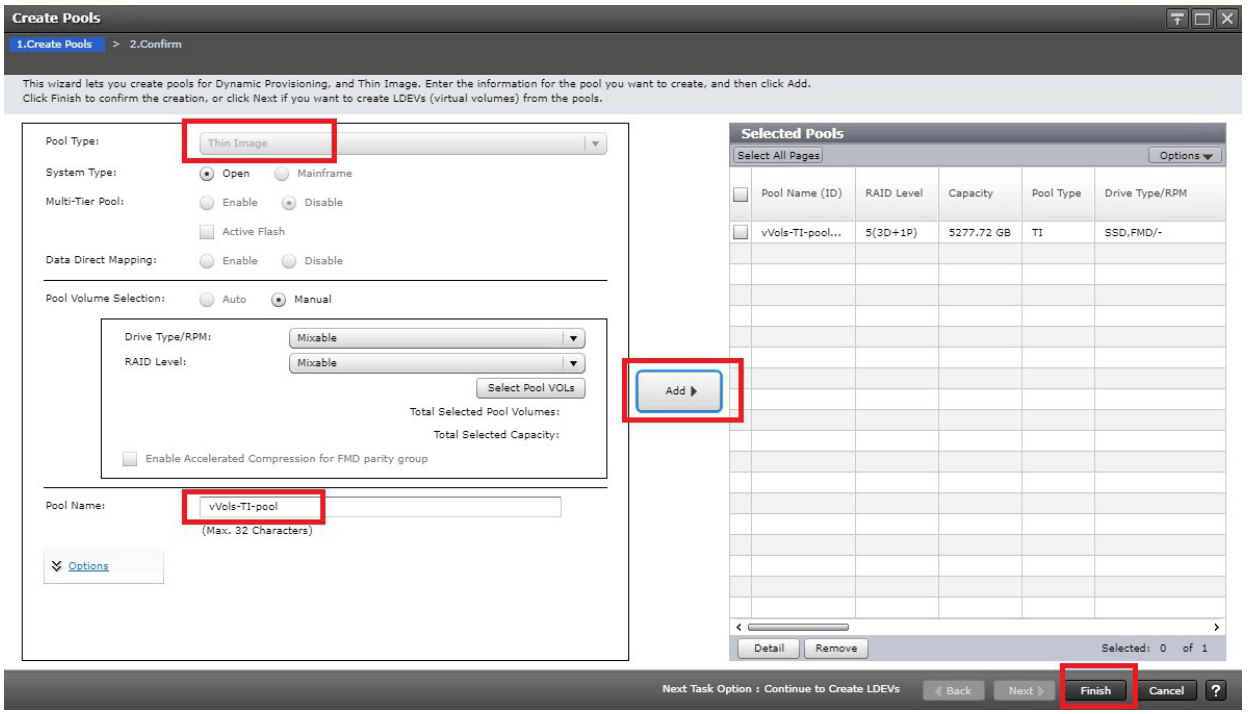
   In the following example a few basic LDEVs are already created from parity groups. Add these LDEV IDs to the resource group for vVols later.

5. Click **Finish** to create a pool.



Optionally you can create a Thin Image pool for VM-based snapshot images. This allows the snapshot images to be stored in a separate Thin Image pool rather than in the vVols storage pool that was already created.

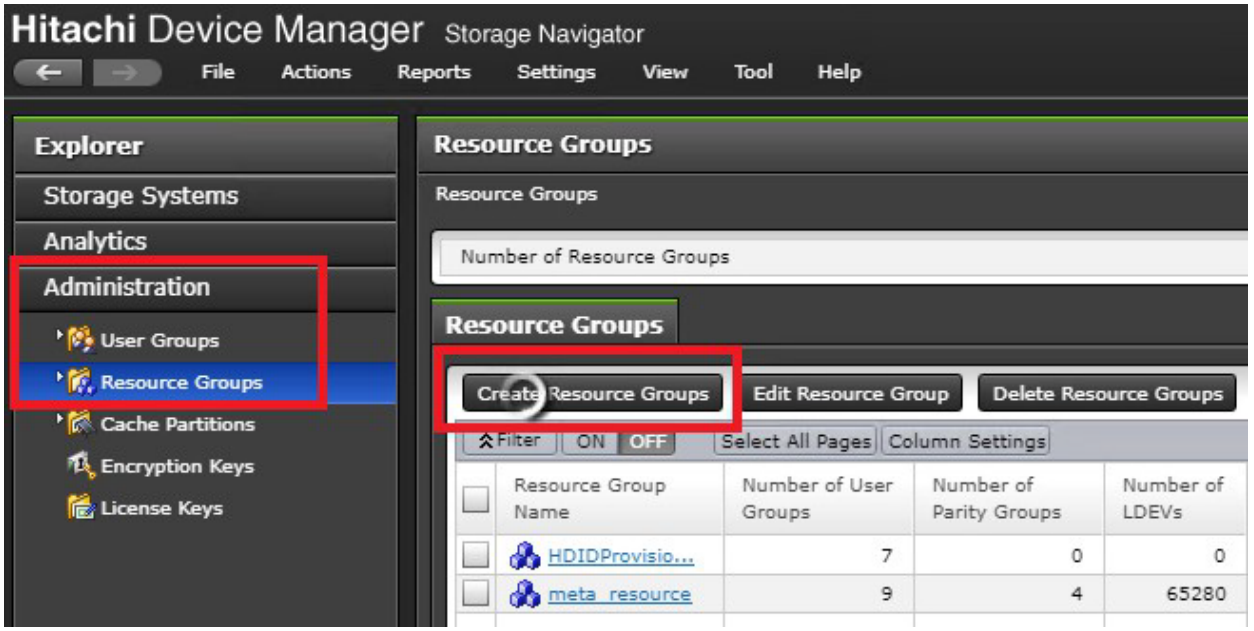
Use the default pool to share the same pool for data and snapshots. Use a dedicated pool to manage the snapshots and data separately.



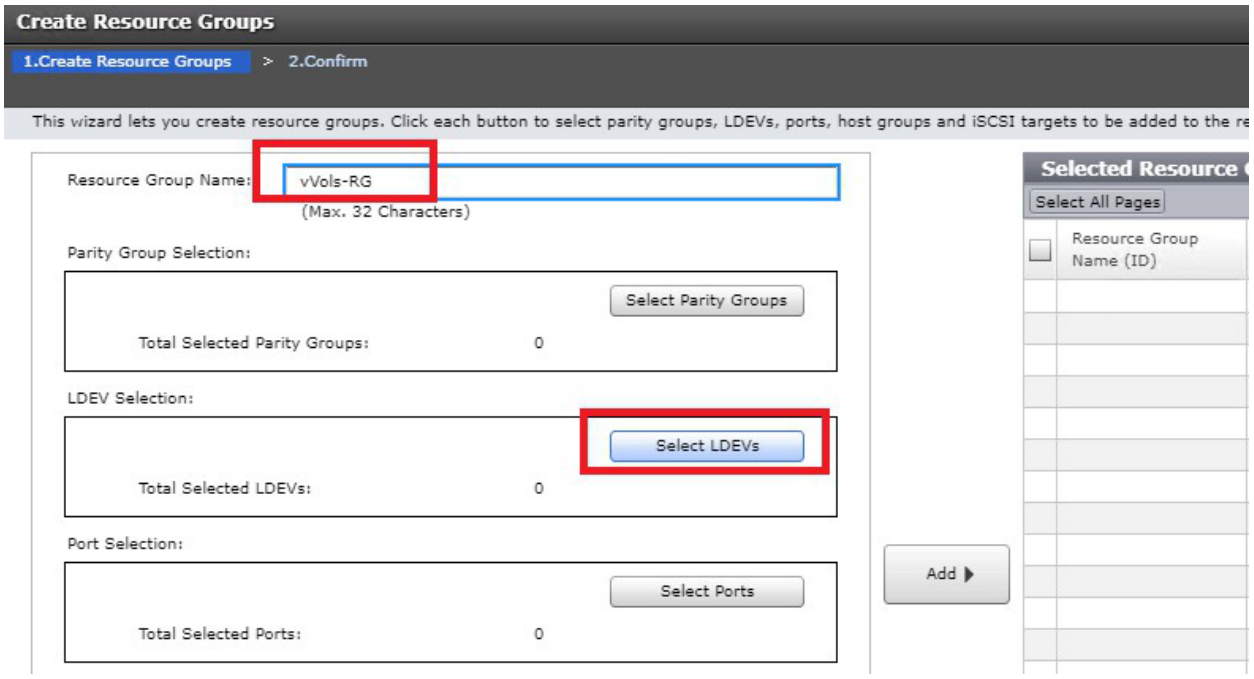
Step 2. Create a Resource Group

You can skip this step if are using the **meta_resource** group or an existing resource group.

1. To create a dedicated resource group for vVols, click **Create Resource Groups**.



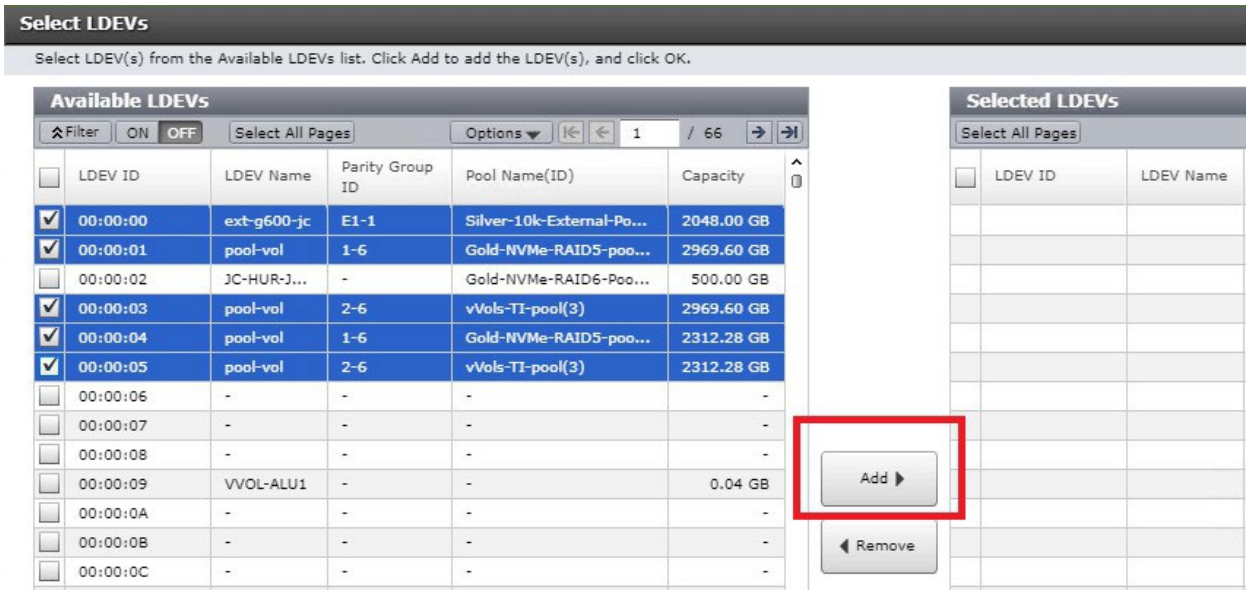
2. Click **Select LDEVs** to add LDEVs into this resource group.



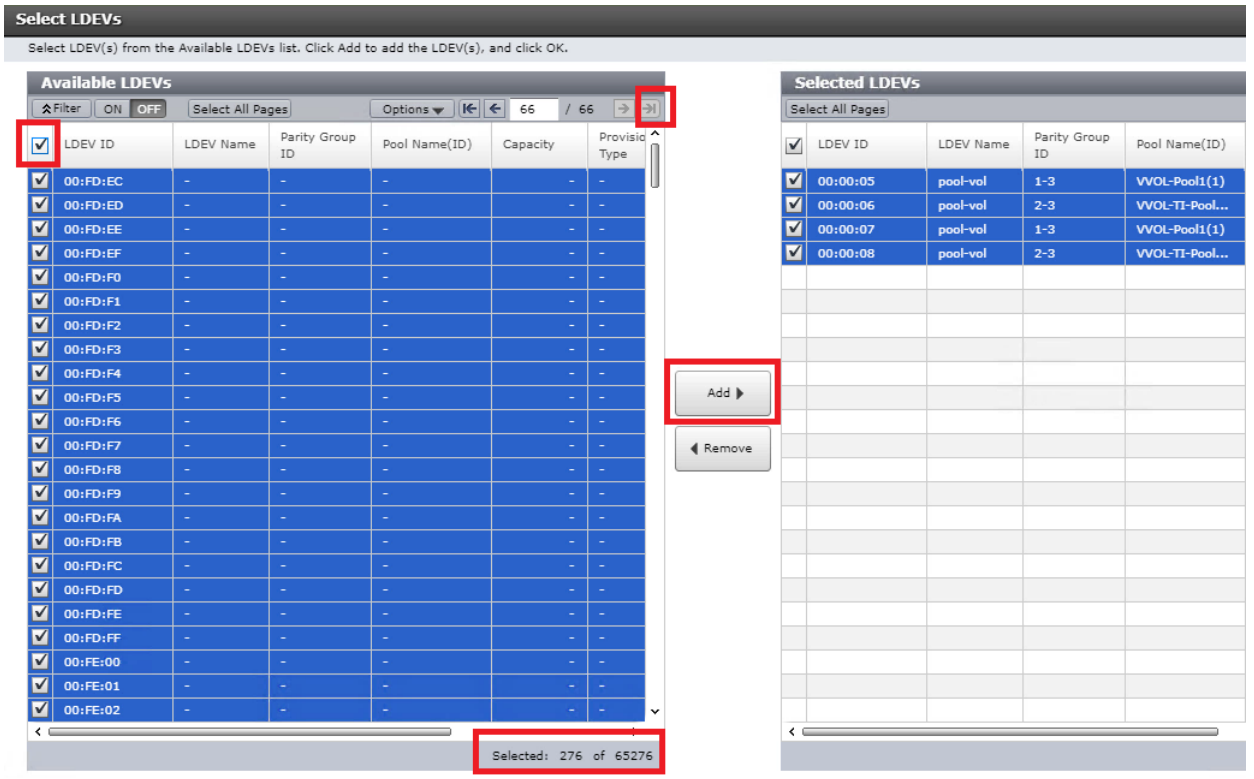
3. Add all the LDEVs that are associated to the storage pools.

   This ensures that Hitachi Storage Provider for VMware vCenter uses only these pools in this resource group.

For example, storage pools **Silver-10k-External-Pool**, **Gold-NVMe-RAID5-pool**, and **vVols-TI-pool** are added to this resource group, as shown in the following figure.



You must reserve a range of LDEV IDs for future vVols creation. In the following example, the entire last page of LDEVs are added to this resource group. Each VM takes at least three LDEVs. Add more LDEVs as your vVols environment grows.



Step 3. Create an Administrator User Account for vVols

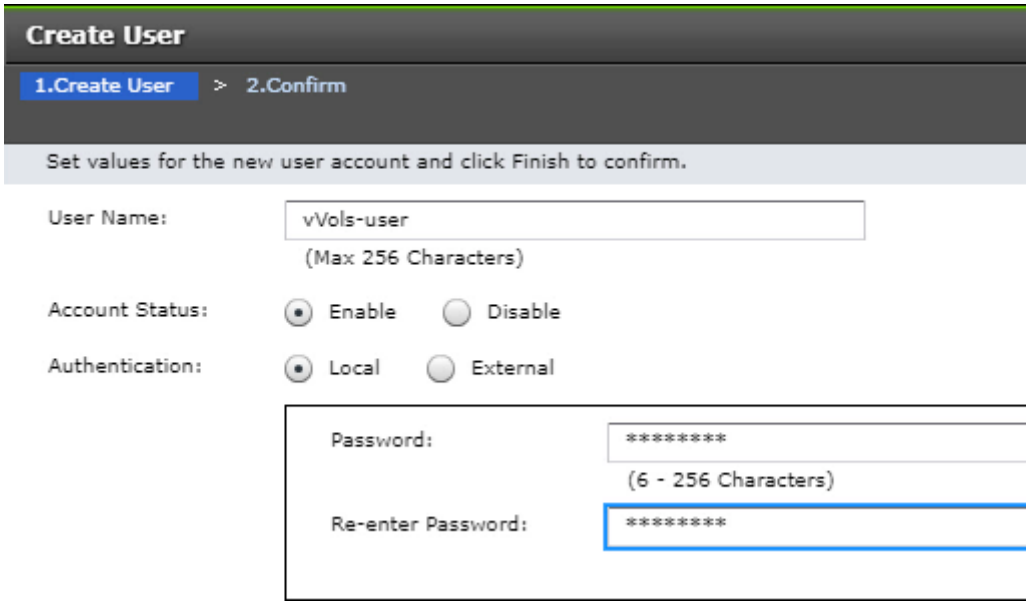
After the resource group is created, create a dedicated user for vVols operation.

1. Go to **Administrator User Group** and click **Create User**.

2. Create an account named vVols-user.

- Select the **Enable** option to enable the account status.
- Select the local authentication type.
- Enter the password and reconfirm the password.

3. Click **Confirm** to create the administrator user account.

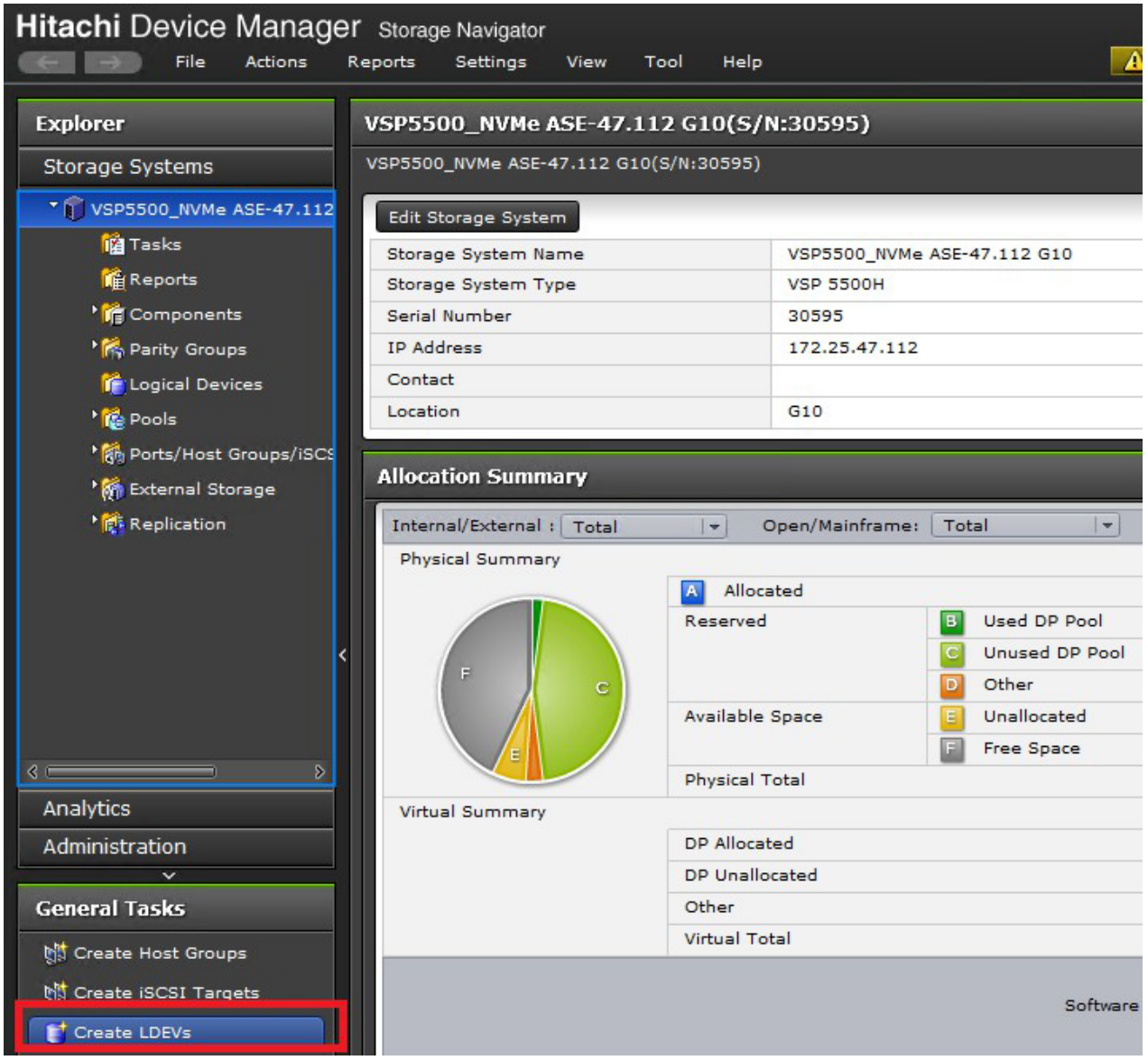


Note — If multiple VASA Providers are connecting to the storage, create a separate user account or each VASA Provider for tracking purposes. For example, vVols-user2.

Step 4. Create a Protocol Endpoint and Add it to ESXi Hosts

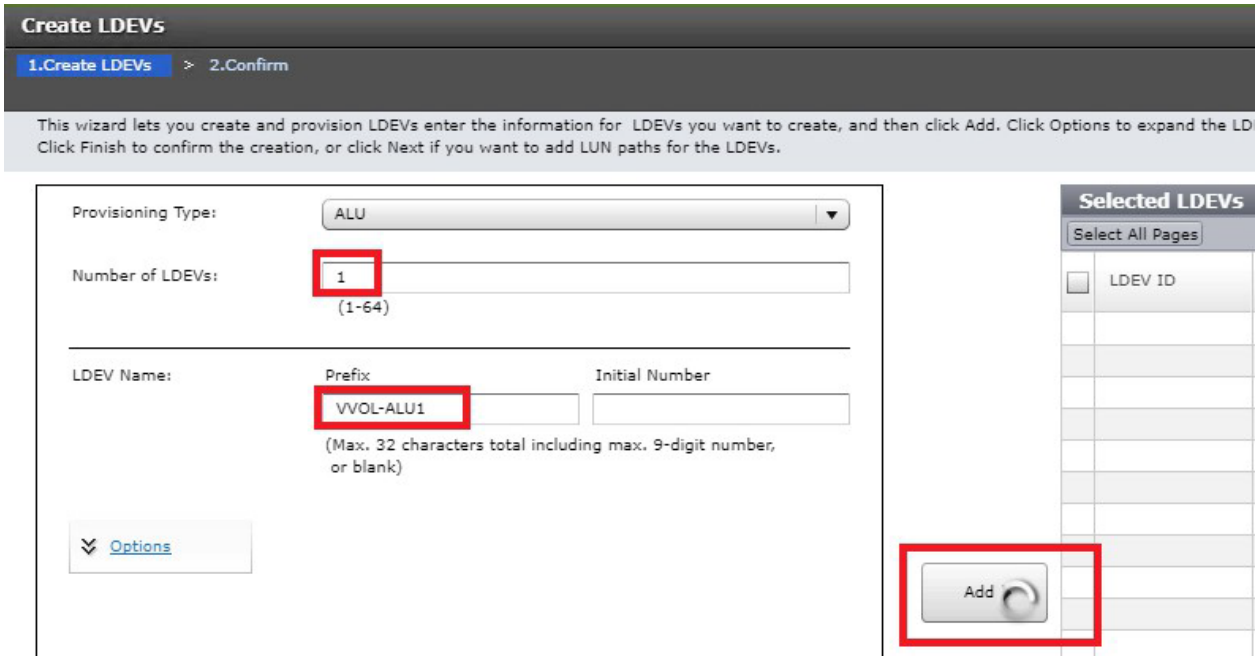
In VSP storage, a Protocol Endpoint (PE) is called an Administrative Logical Unit (ALU).

1. To create an ALU/PE, go to the **General Task** panel in the left-bottom of the Hitachi Device Manager Storage Navigator screen, and click **Create LDEVs**.



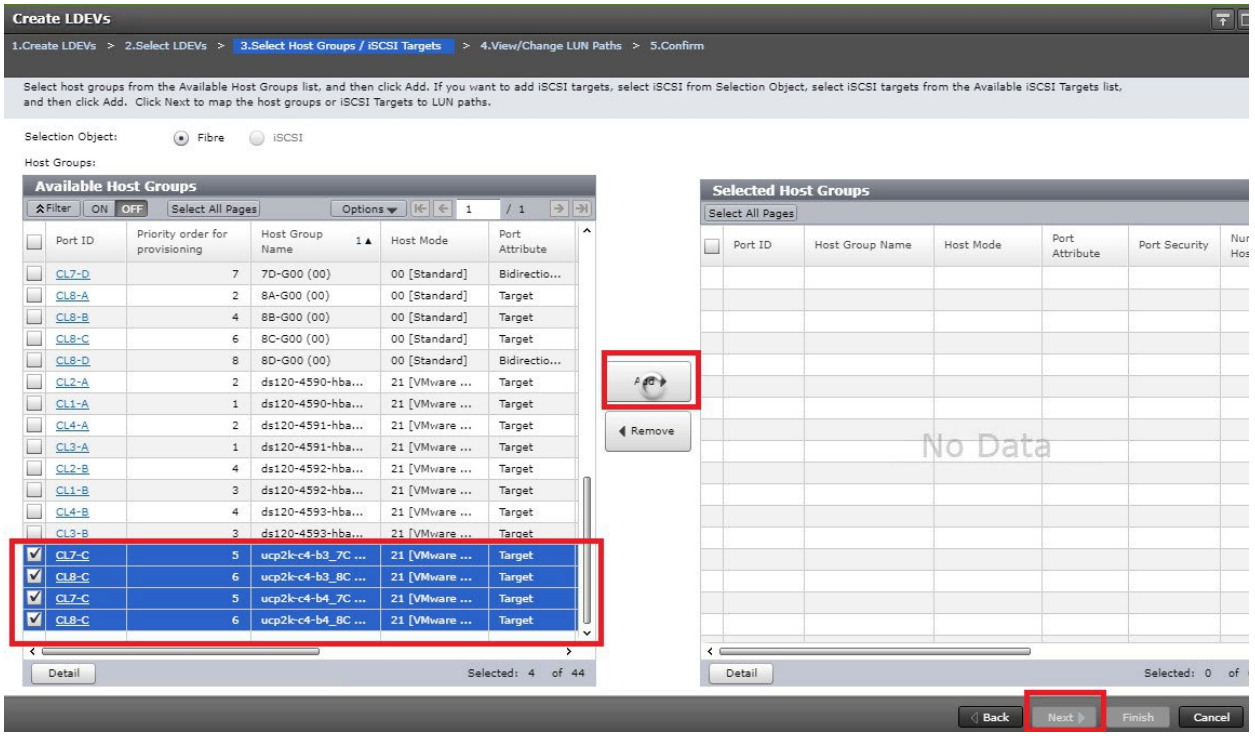
2. Select **ALU** in the **Provisioning Type** field.
3. Enter the value 1 in the Number of LDEVs field.

   You only need one ALU per storage system for approximately 16,000 vVols based on current vSphere limits.
4. Enter the LDEV name in the LDEV Name Prefix field. For example, VVOL-ALU1.
5. Click **Add** to add the ALU to the host group.



6. Continue to assign the ALU to host groups for ESXi hosts, just like a regular LUN. Ensure the host groups have Host Mode 21 [VMware Extension] with 63 and 114 as the host mode options.

Note — The host mode option 54 is optional, as the older VAAI plugin has been removed. Option 54 is no longer required, and is ignored.



Part 2. VMware vSphere Administrator – Set up Hitachi Storage Provider for VMware vCenter

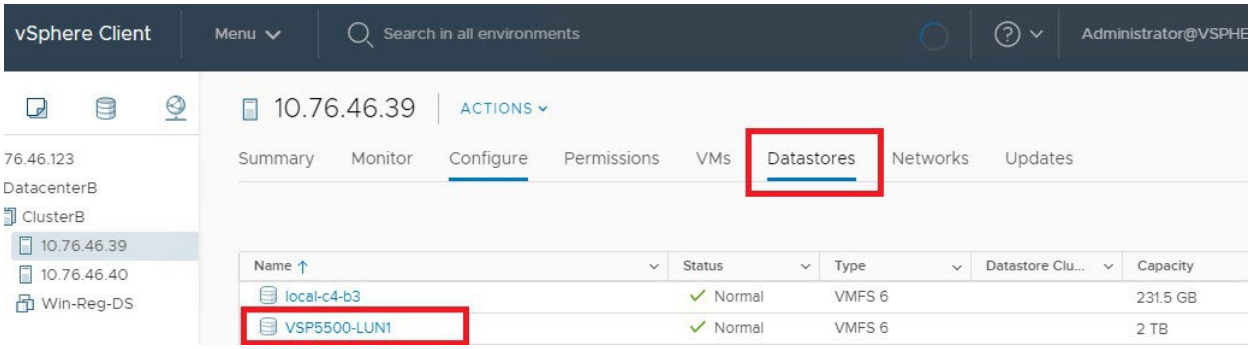
Step 5. Deploy Hitachi Storage (VASA) Provider OVA

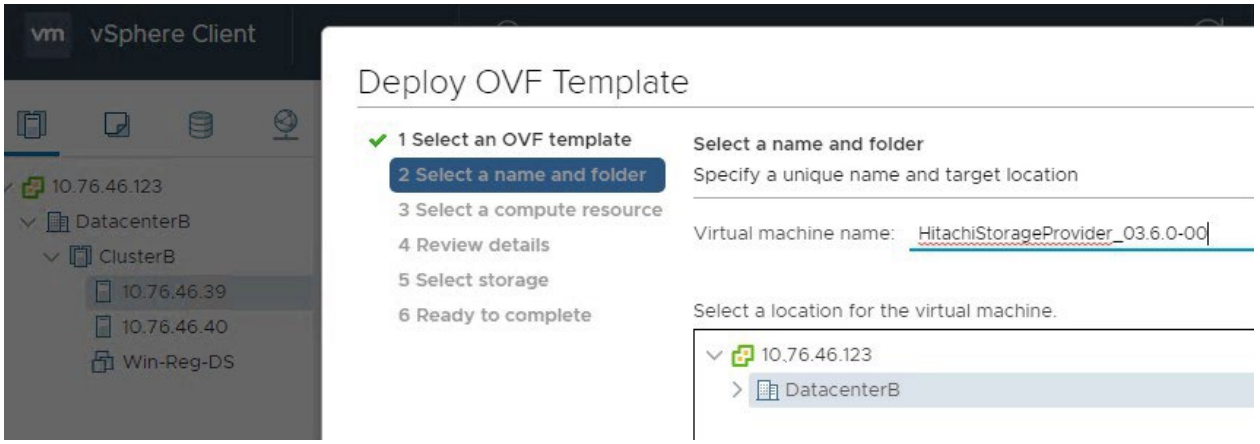
Hitachi Storage Provider for VMware vCenter is deployed from an OVF template. You can download the latest OVF file from Downloads Detail - Support | Hitachi Vantara.

This virtual machine is typically deployed into the vSphere management cluster where the vCenter Appliance (VCSA) is deployed. You can also deploy this virtual machine to any vSphere environment as long as it has a network access to the VSP storage. Ensure that the virtual machine is deployed into a High Availability-enabled vSphere Cluster, which is configured by default, to provide the first level of availability. (You can also deploy this virtual machine as a fault tolerant virtual machine to ensure high availability). Hitachi Storage Provider for VMware vCenter is typically deployed into a vCenter Management cluster.

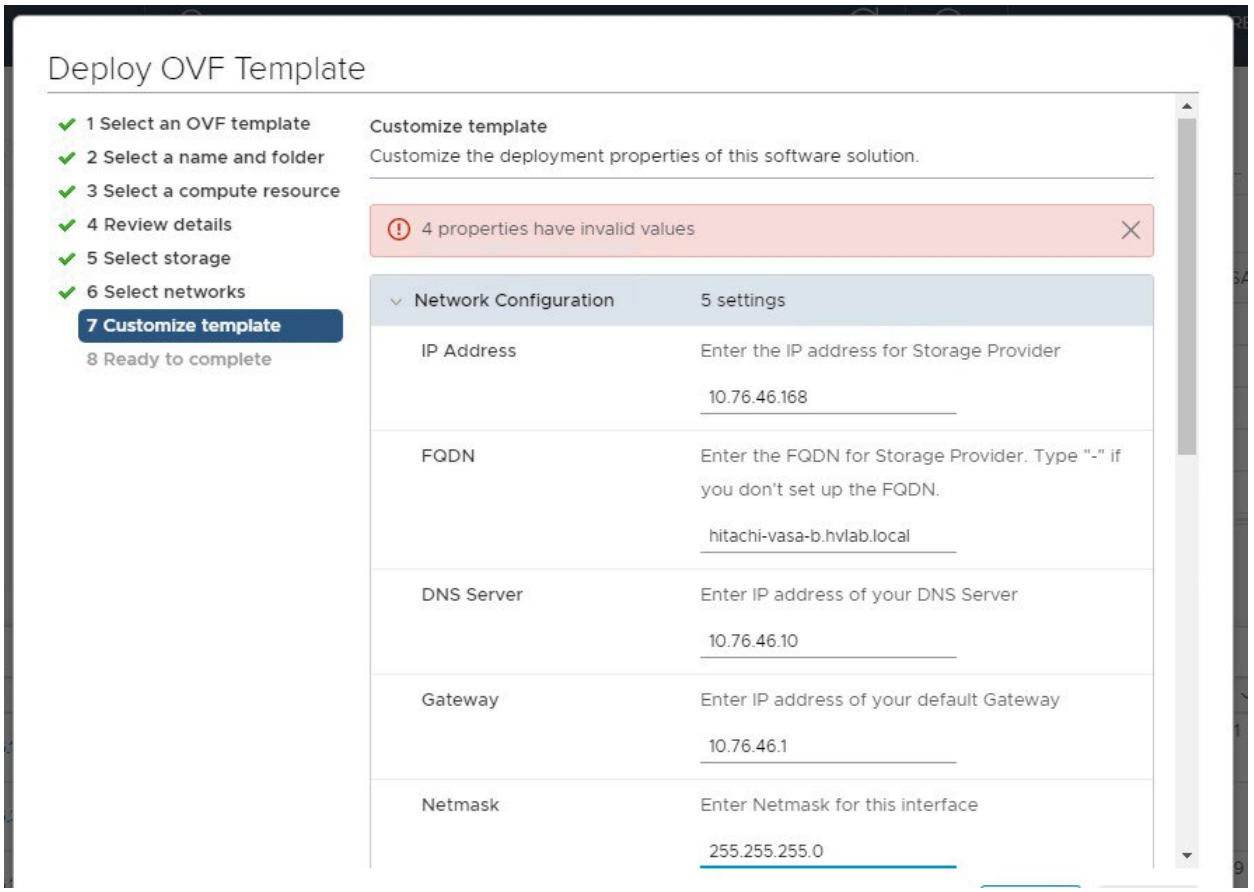
1. Ensure that you have a VMFS or vSAN datastore available to deploy the VASA Provider.

Note — You can create VMFS datastores using the Hitachi vCenter Storage Plugin or any other integrations that are available such as, PowerShell cmdlet or vRealize Orchestrator workflow.

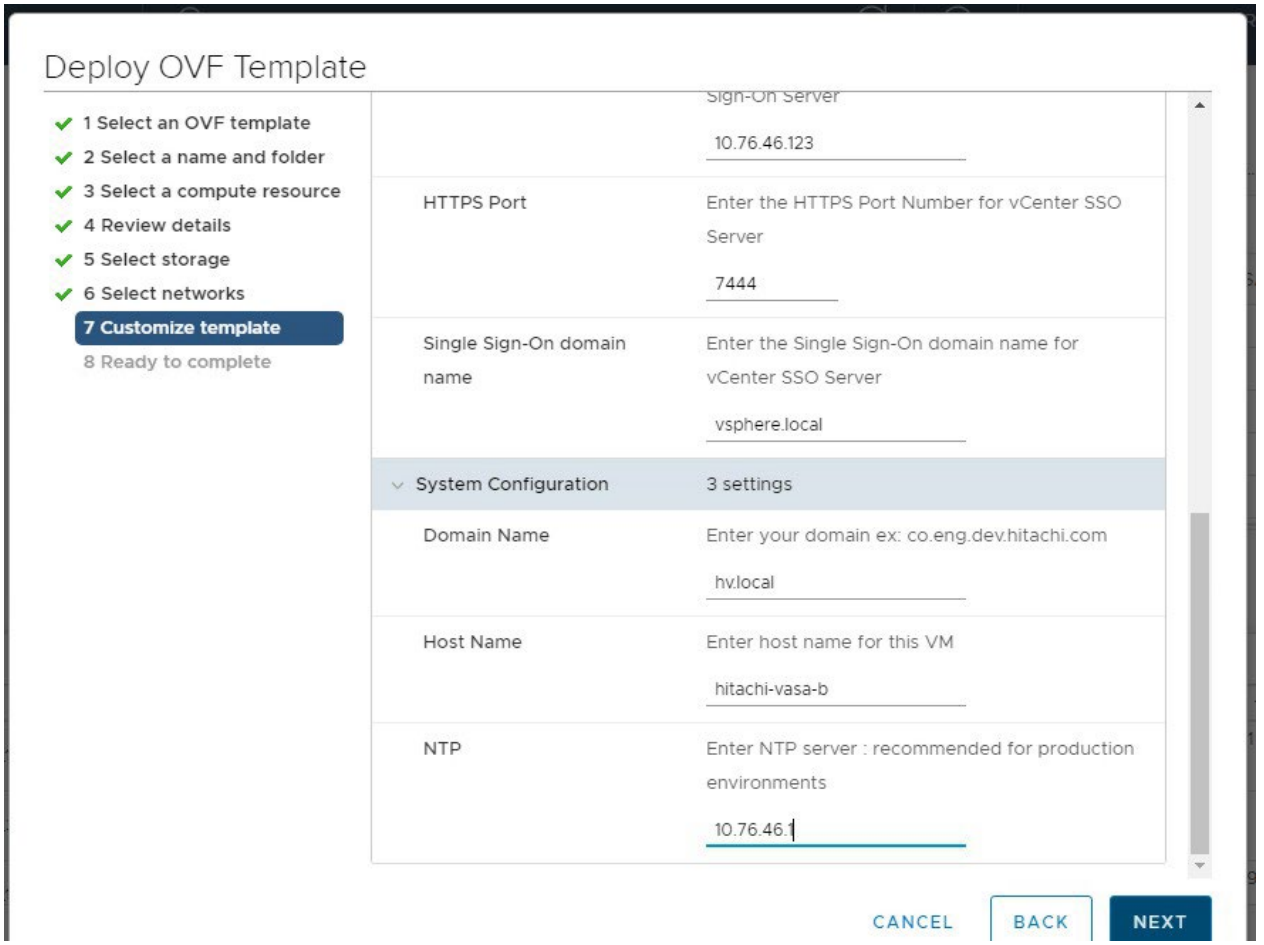




2. Assign an IP address/FQDN to the storage provider VM and complete all other required information.



Note — Generally, the SSO Server domain and the domain you log in to for the vSphere client are the same in the test environment. For example, vsphere.local. However, the template gives you an option to specify different domains.



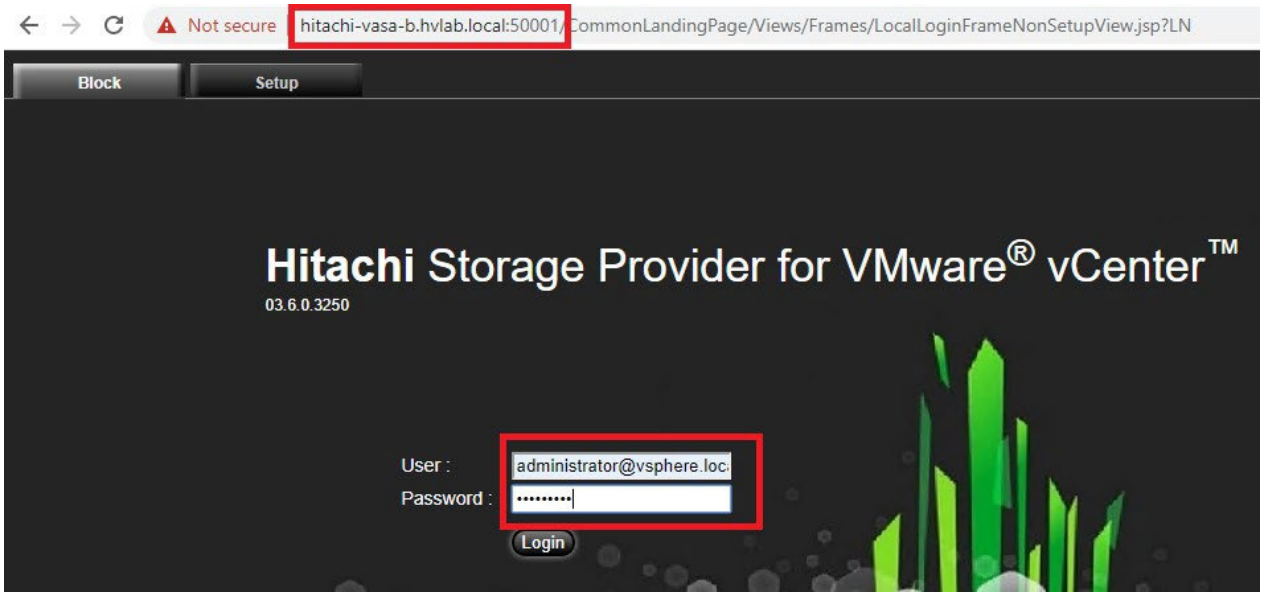
Step 6. Configure Hitachi Storage Provider for VMware vCenter

1. After the virtual machine is deployed and powered on, open a browser and enter the following URL to access the Hitachi Storage Provider for VMware vCenter web interface

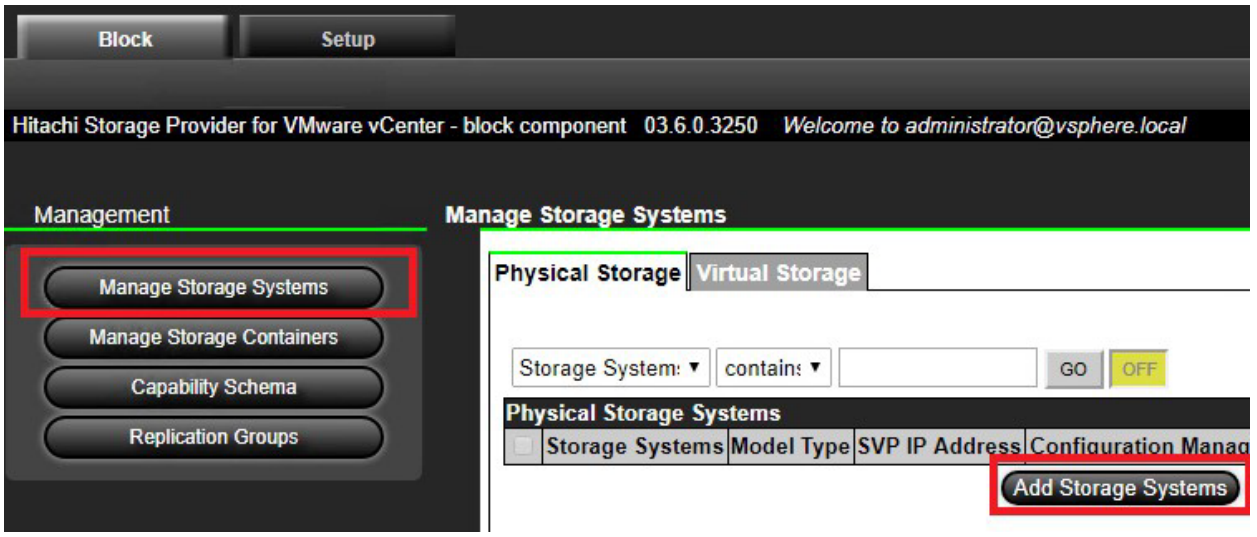
   https://VASA-Provider-IPAddress-or-FDQN:50001/

Note — Ensure that you add **https** at the beginning of the URL, and port 50001 at the end of the URL.

2. Log in with vCenter SSO credentials.



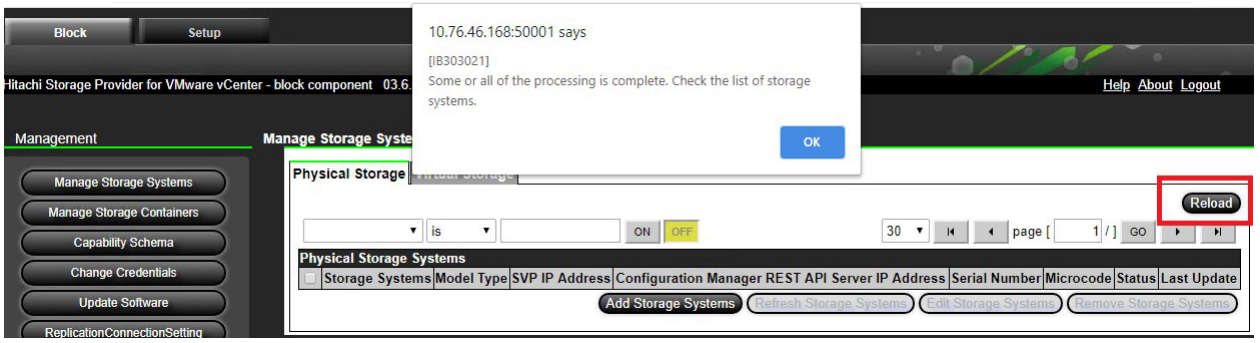
3. Select Manage Storage Systems under Management, and click **Add Storage Systems**.



4. Select a Storage System Type and enter the SVP IP address.
5. Enter the vVols user name and password that you created earlier.

6. Click **Reload** to update the progress until the storage system is added successfully.

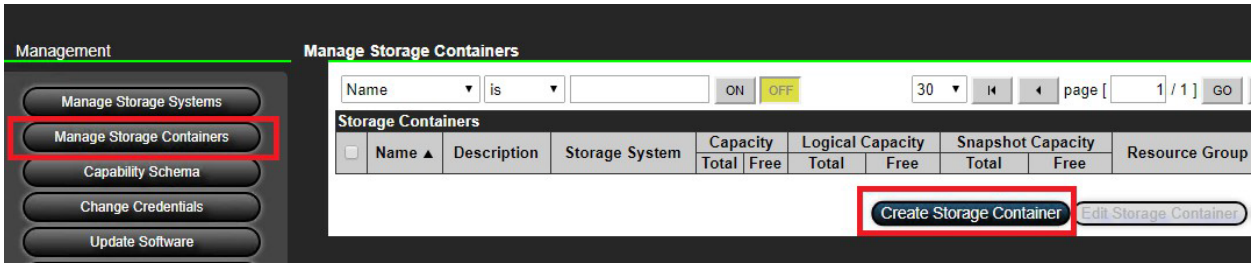
   You can add multiple storage systems into the same VASA Provider.



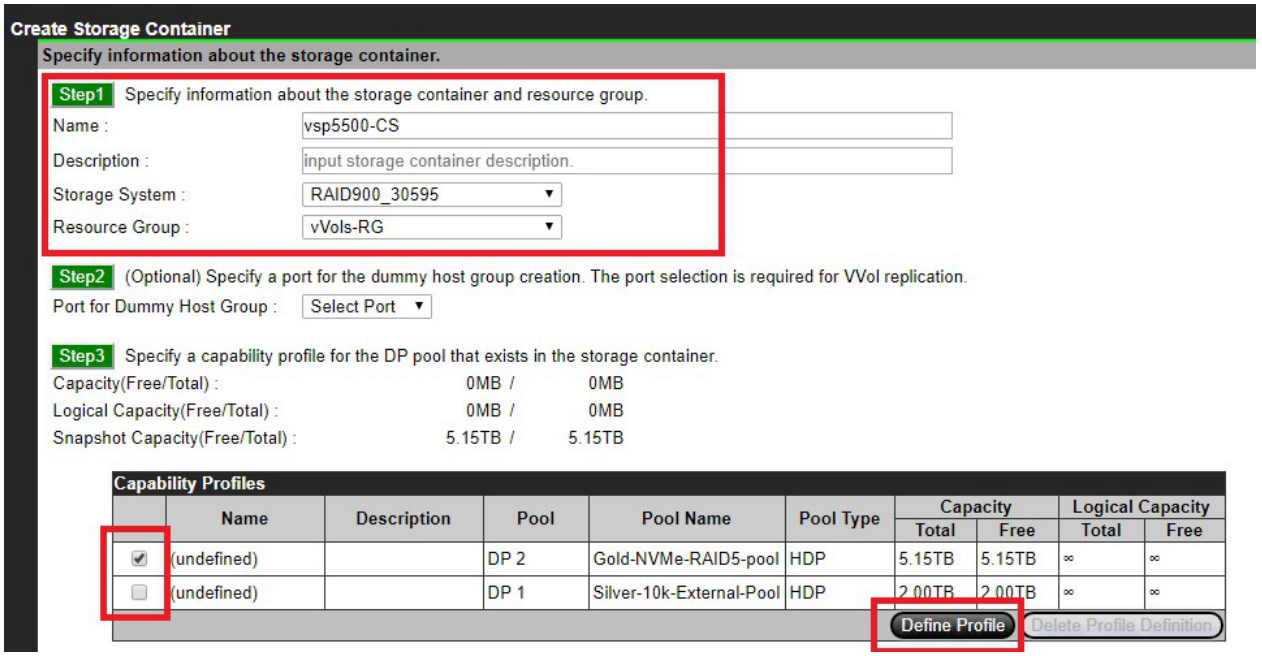
7. Create a storage container.

   There is a one-to-one relationship between a vVol storage container and a storage resource group.

8. Select **Manage Storage Containers** under Management, and click **Create Storage Container**.

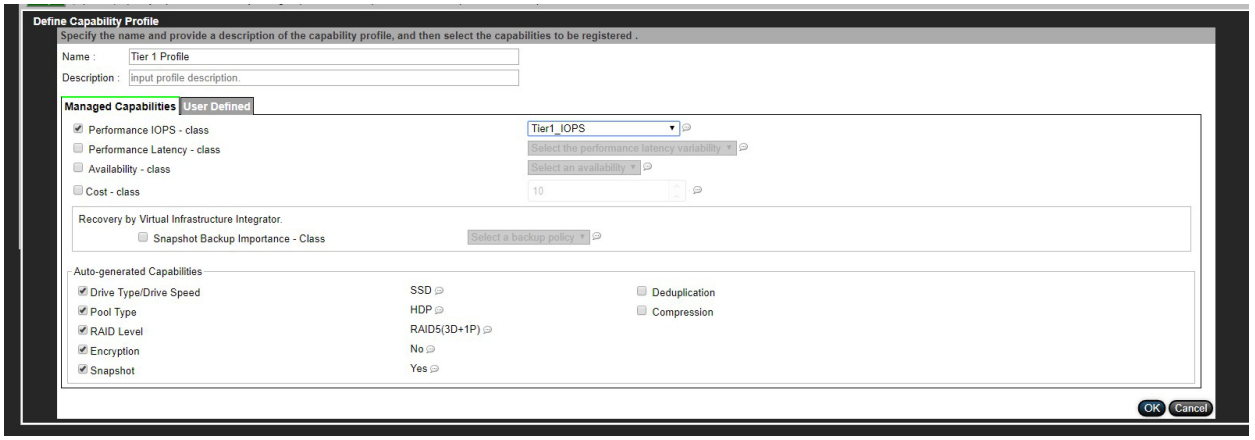


- Provide a name for this storage container.
- Select a storage system.
- Select a resource group. The available storage pool is listed in the **Capability Profiles** table.
- Select an undefined pool and click **Define Profile**.



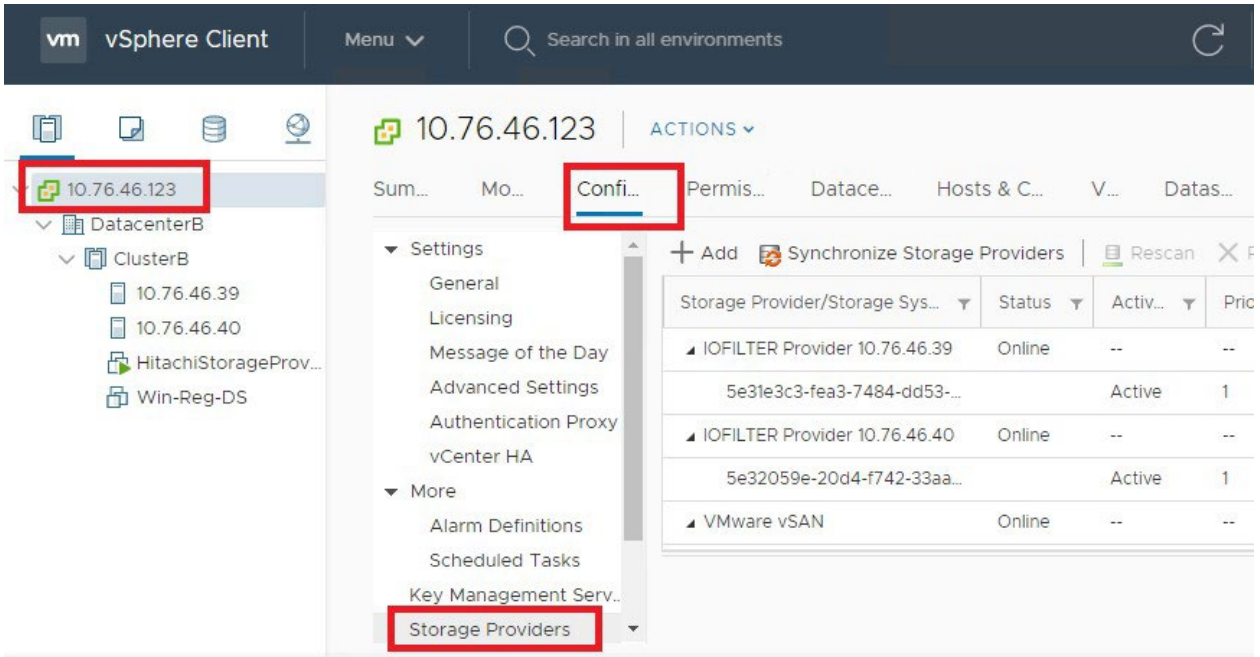
The system needs a profile for each pool. You can provide temporary values and complete the profile at a later point in time.

The following example shows an initial profile used to create a storage container. You can complete the storage profile for production use cases after testing the VM deployment.



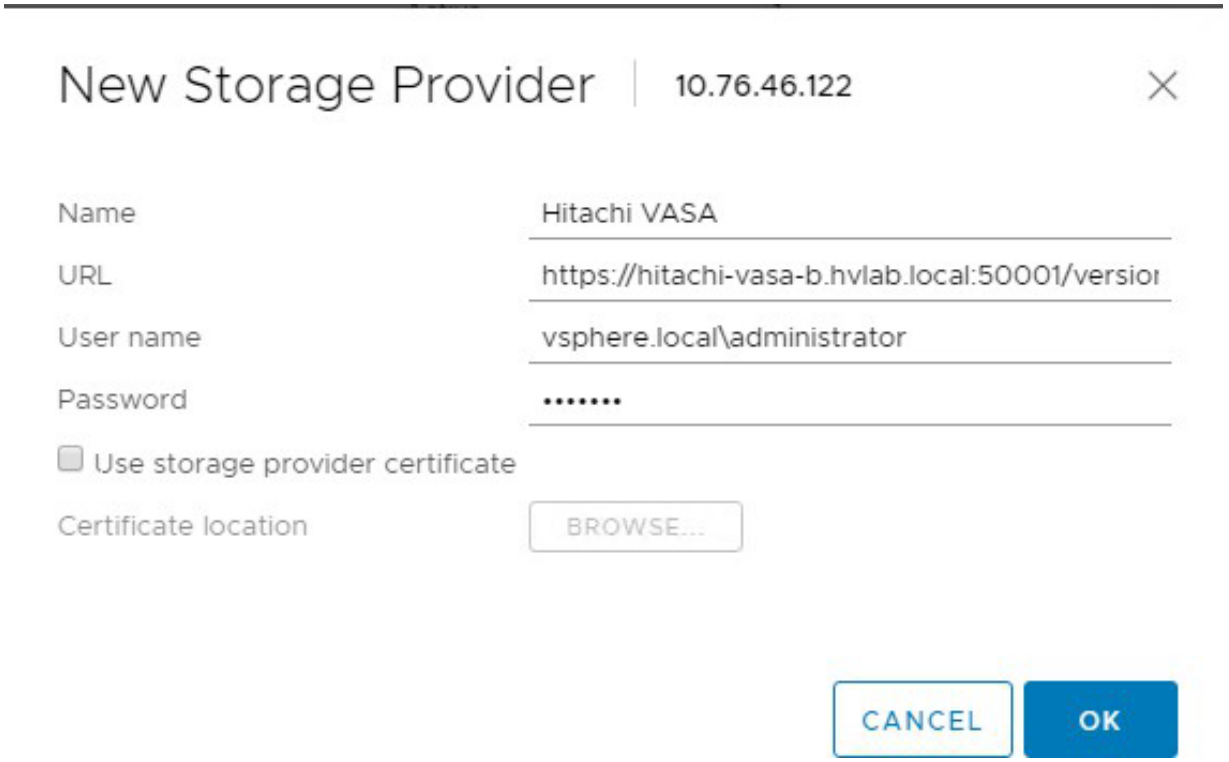
Step 7. Register Hitachi Storage Provider for VMware vCenter

1. Log in to the vSphere Client and select vCenter.
2. Under the Configuration tab, click **Storage Providers**, and then click **Add**.

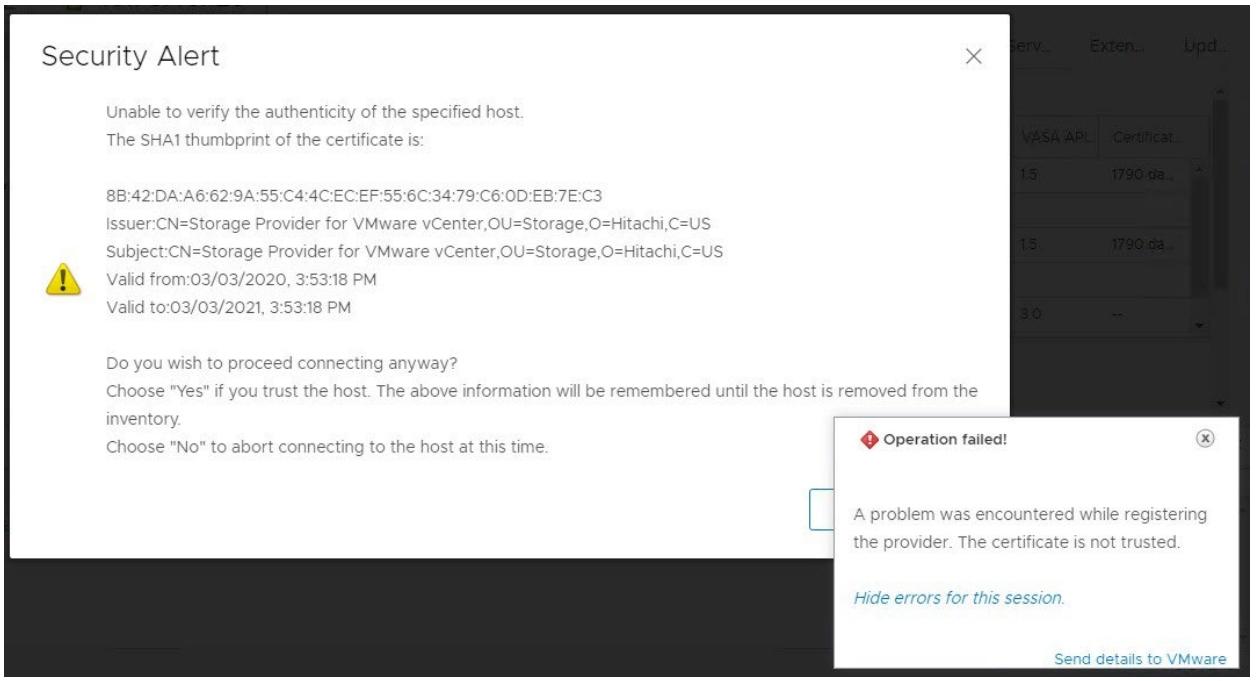


3. Provide the following information:

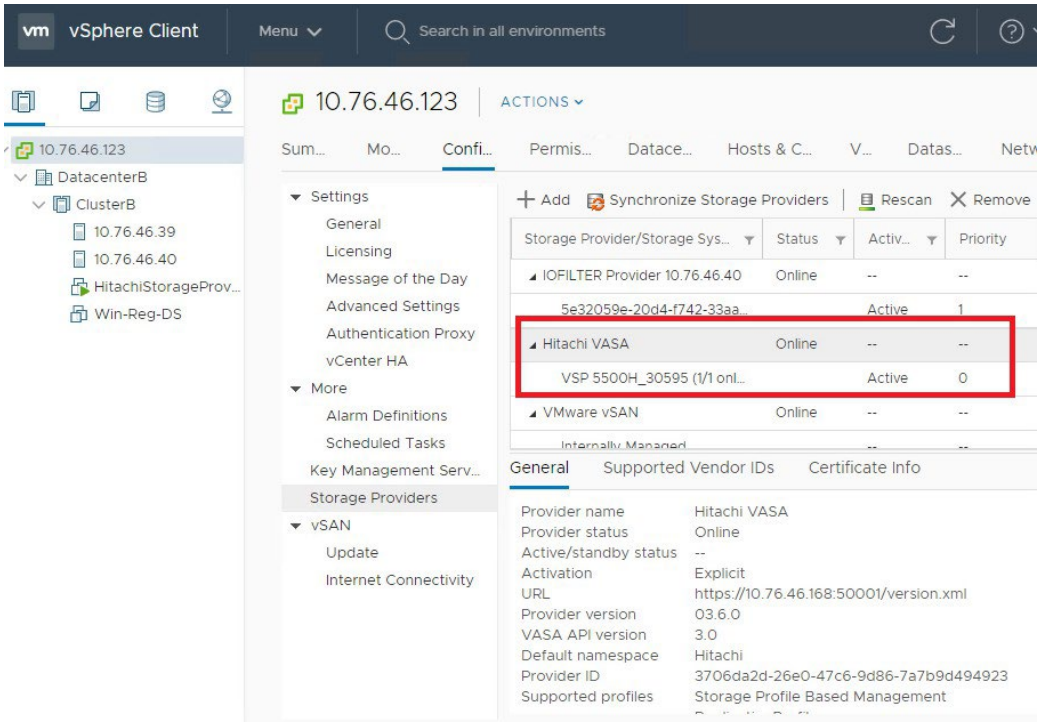
- In the URL field, enter `https://VASA-Provider-IP-or-FQDN:50001/version.xml`
  For example, https://vphost.xyz.com:50001/version.xml or https://10.76.46.120:50001/version.xml
- In the User name field, enter the vCenter user name in the format shown in the following figure.
- In the Password field, enter the vCenter password.



The following message might appear. Ignore this message and proceed.



The **Hitachi VASA** provider appears with an **Online** status.



Use a certificate from a local certificate authority (CA) if one is used in your production environment. For a test environment, you can skip the following and use the default self-signed certificate.

If the Hitachi VASA Provider certificate needs to be signed by a local certificate authority (CA), then follow this procedure:

Assuming the FQDN of Hitachi VASA Provider is vasaprod.xyz.org, run the following from VASA Provider

- Create a new keystore – "`keytool -genkey -alias vasaproviderservercertificate -keyalg RSA -keysize 2048 -keystore keystore.jks.SAN`" .
- Generate certificate signing request (CSR) – note the addition of the subject alternate name (SAN) option, which is required by VMware – "`keytool -certreq -alias vasaproviderservercertificate -file csrSAN.txt -keystore keystore.jks.SAN -ext SAN=dns:vasaprod.xyz.org`".
  - SAN is the FQDN of the Storage Provider VM.
- Use this CSR to request a certificate from local CA. Download the certificate from the CA to the VASA Provider (.p7b or similar certificate that CA generated)
- Import the certificate to the keystore – "`keytool -import -alias vasaproviderservercertificate -file vasaprod-SAN.p7b -keystore keystore.jks.SAN`"
- The keystore file keystore.jks.SAN is now copied to keystore.jks. Ensure that the owner of the keystore.jks file is either vptomcat or root.
- Reboot the VASA provider VM. The certificate with SAN is now being used by the Hitachi Storage Provider for VMware vCenter, and you can register it to the vCenter.

TIP: If you want to register the same Hitachi VASA provider to multiple vCenters, for example, a VMware Cloud Foundation (VCF) deployment, then ensure that the setting `multipleVcSupport` is set to `true` in the VasaProvider.properties config file. This is now default setting in releases greater than 3.5.9. This file is located in the `/usr/local/hitachivp-b/tomcat/webapps/VasaProvider/META-INF/` directory.

If the multipleVcSupport setting is not set prior to 3.5.9, then set it and run the createCertifications.sh script, which is located in the /usr/local/hitachivp-b/ directory. This script updates the registry and restarts the VASA Provider (VP). Other vCenters can now register to this VP.

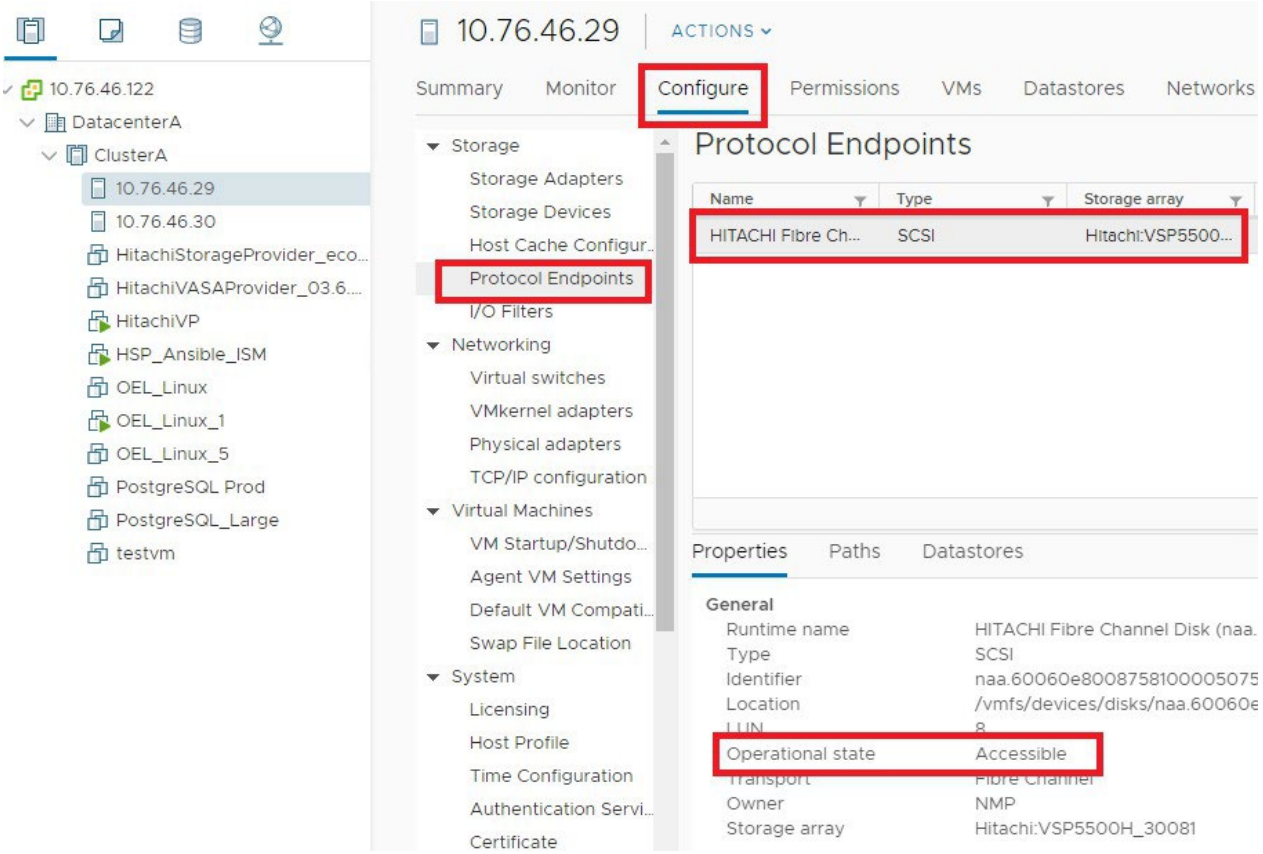
Step 8. Verify that the PE is Available and Visible

Verify that the protocol endpoint (PE) is visible in vSphere ESXi hosts either in the vCenter UI or from the `esxcli` command. This is the (ALU/PE) that the storage administrator presented to vSphere Cluster/ESXi hosts in "Step 4. Create a Protocol Endpoint and Add it to ESXi Hosts" on page 11.

Note: There are instances where the PE is not visible in the vCenter UI but the `esxcli storage core device list` command does indeed return VVOL=PE is TRUE. In this case, you can proceed to Step 9 (vVols datastore creation) which incidentally will also make the PE visible in vCenter UI.

1. Log in to the vSphere Client, select Hosts and Clusters, and then select an ESXi host.
2. Select Protocol Endpoints on the Configure tab.

   You will notice the protocol endpoint with the Operational state **Accessible**.



Optionally, on ESXi hosts, you can view the protocol endpoints (PEs) by running the following command from the esxcli command line.

```
esxcli storage core device list -p
```

This will display the devices that are recognized as PEs. Note the **Is VVOL PE=True** value.

```
[root@ucp2k-c2-b2:~] esxcli storage core device list -p
naa.60060e800875810000507581000000017
   Display Name: HITACHI Fibre Channel Disk (naa.60060e800875810000507581000000017)
   Has Settable Display Name: false
   Size: 46
   Device Type: Direct-Access
   Multipath Plugin: HPP
   Devfs Path: /vmfs/devices/disks/naa.60060e800875810000507581000000017
   Vendor: HITACHI
   Model: OPEN-0V-A
   Revision: 5001
   SCSI Level: 5
   Is Pseudo: false
   Status: degraded
   Is RDM Capable: false
   Is Local: false
   Is Removable: false
   Is SSD: false
   Is VVOL PE: true
   Is Offline: false
   Is Perennially Reserved: false
   Queue Full Sample Size: 0
   Queue Full Threshold: 0
   Thin Provisioning Status: yes
   Attached Filters:
   VAAI Status: supported
   Other UIDs: vml.020008000060060e800875810000507581000000174f50454e2d30
   Is Shared Clusterwide: true
   Is SAS: false
   Is USB: false
   Is Boot Device: false
   Device Max Queue Depth: 30
   No of outstanding IOs with competing worlds: 30
   Drive Type: unknown
   RAID Level: unknown
   Number of Physical Drives: unknown
   Protection Enabled: false
   PI Activated: false
   PI Type: 0
   PI Protection Mask: NO PROTECTION
   Supported Guard Types: NO GUARD SUPPORT
   DIX Enabled: false
   DIX Guard Type: NO GUARD SUPPORT
   Emulated DIX/DIF Enabled: false
```

The `esxcli storage vvol protocolendpoint list` command can show the PEs as well. However, there have been instances where creating the vVols datastore [step 9] has to be performed in order for vCenter UI to show the PE as visible.

For example:

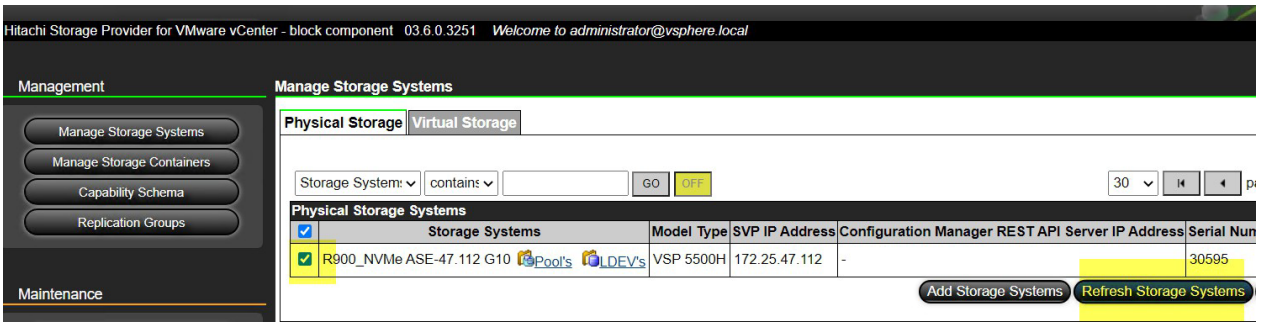
```
# esxcli storage vvol protocolendpoint list
```

```
[root@DC1-Node4:~] esxcli storage vvol protocolendpoint list
naa.60060E8140A3D140A3D1000000000001
    Host Id: naa.60060e8012a3d1005040a3d100000001
    Array Id: Hitachi:VSPG400G600_441937
    Type: SCSI
    Accessible: true
    Configured: true
    Lun Id: naa.60060e8012a3d1005040a3d100000001
    Remote Host:
    Remote Share:
    NFS4x Transport IPs:
    Server Scope:
    Server Major:
    Auth:
    User:
    Storage Containers: ad635618-ca2c-4600-ba12-464524e4d2b4
[root@DC1-Node4:~] esxcli storage vvol storagecontainer list
DC1_G600_vVol01
    StorageContainer Name: DC1_G600_vVol01
    UUID: vvol:ad635618ca2c4600-ba12464524e4d2b4
    Array: Hitachi:VSPG400G600_441937
    Size(MB): 31739610
    Free(MB): 14791434
    Accessible: true
    Default Policy:
[root@DC1-Node4:~] esxcli storage vvol vasaprovider list
Hitachi-0356
    VP Name: Hitachi-0356
    URL: https://dc1vasa0350.ucp.local:50001/version.xml
    Status: online
    Arrays:
            Array Id: Hitachi:VSPG400G600_441937
            Is Active: true
            Priority: 0
[root@DC1-Node4:~]
```

Note — If the protocol endpoint is not visible after running the `protocolendpoint list` command or is not visible in the vCenter UI under the **Hosts/ConfigureProtocol Endpoints** window, then you must perform a storage refresh in the Hitachi VASA Web user interface. This occurs if VASA is deployed first and then PEs are added. Perform a refresh of the storage system that is presenting the PE, which ensures that VASA PE information is current. Retry the `protocolendpoint list` command or view the protocol endpoint in the vCenter. If PE the is still not showing as visible but the esxcli storage core device list command shows "VVOL PE=True: value, move to Step 9 to create a vVols datastore. If vVols datastore creation fails, verify network connectivity to VASA port 50001 from vCenter and ESXi using a command such as ncat.

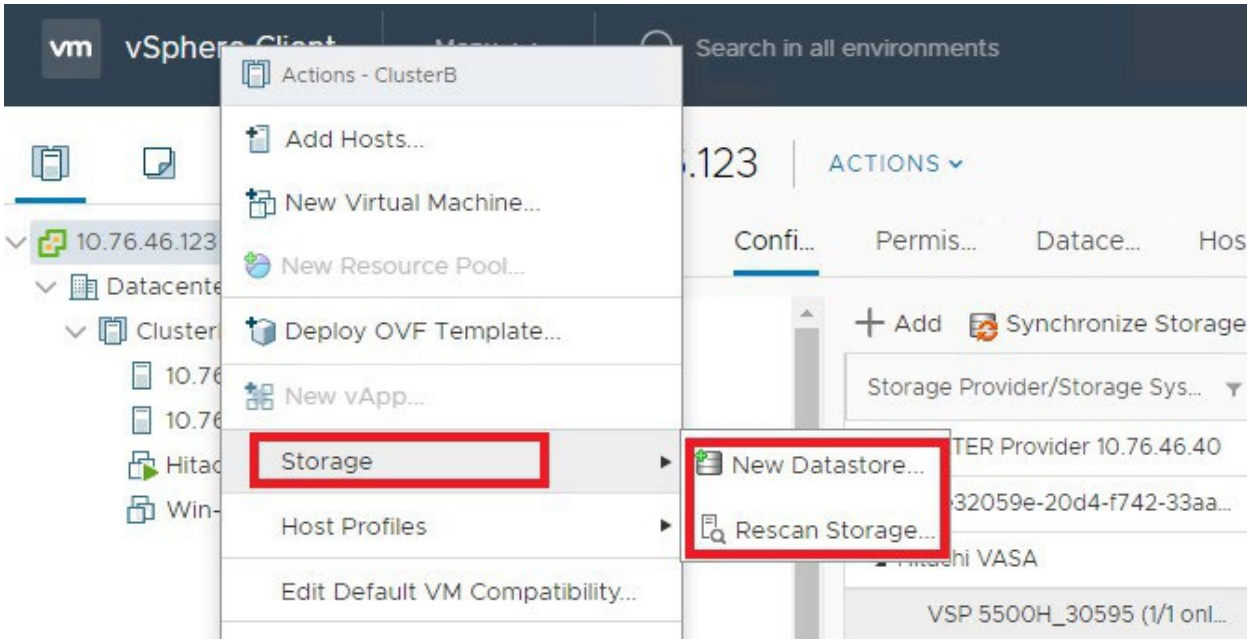
For example:

```
nc -zv VASA-FQDN 50001
```

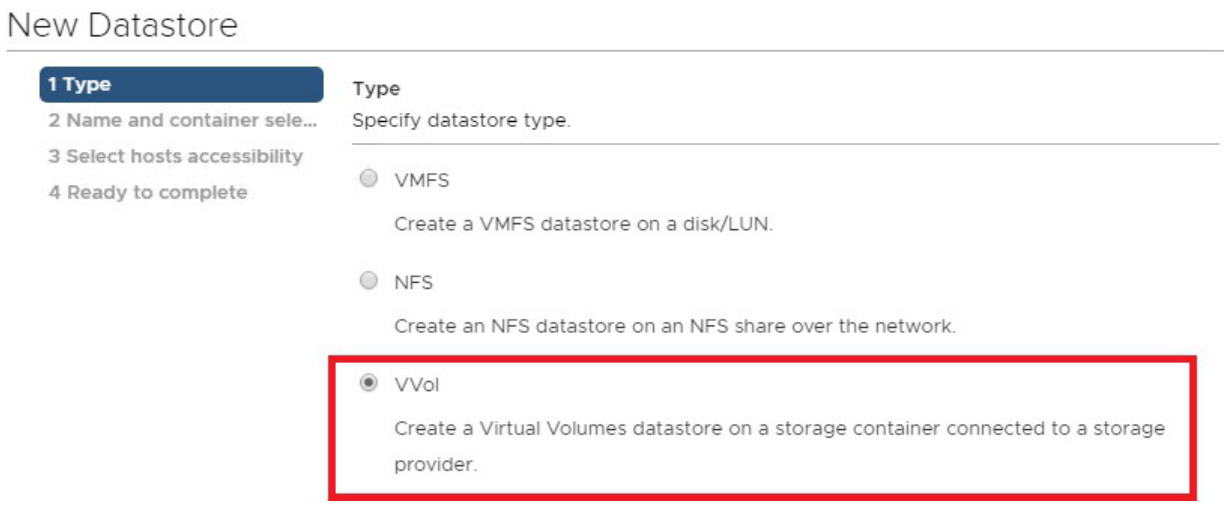


Step 9. Create a vVols Datastore

1. 1. Right-click **Cluster**, select Storage, and then select Rescan Storage.
2. 2. Click **New Datastore** after the rescan is complete.



3. In the New Datastore window, select **VVol** and then click **Next**.



You should see the storage container that was previously created by Hitachi Storage Provider for VMware vCenter.

4. Select the storage container and provide a name.
5. Continue the process to complete the VVol Datastore creation.

New Datastore

- ✔ 1 Type
- 2 Name and container sele...
- 3 Select hosts accessibility
- 4 Ready to complete

Name and container selection

Specify datastore name and backing storage container.

Datastore name: VVOL-DS-vsp5500

Backing Storage Container

Name	Identifier	Maxim...	Existing Datastore
vsp5500-SC	vvol:77201e5cacd... b9d31a3dc8dc4ba7	60 TB	--

1 items

For SCSI-backed VVol datastores, PE LUNs need to be configured manually. Configure SCSI PE LUNs before creating a datastore. If the datastore is created without configuring PE LUNs, the ESXi host marks corresponding VVol datastore as inaccessible.

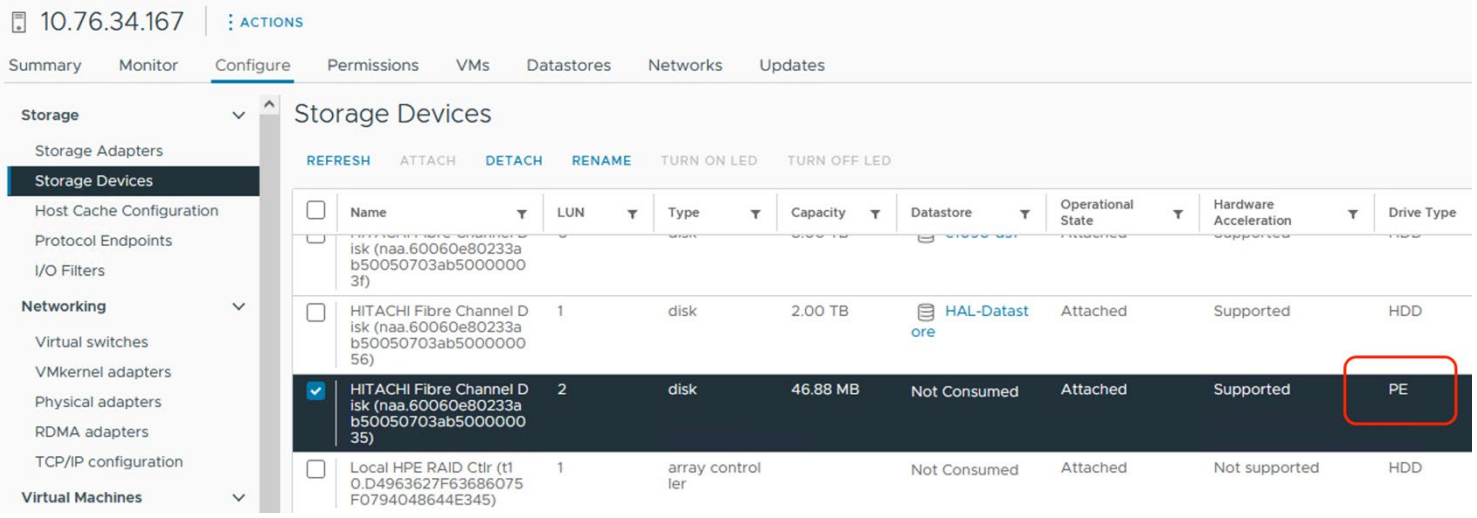
Backing Storage Container Details

Storage array(s)	VSP 5500H_30595
Storage provider(s)	Hitachi VASA

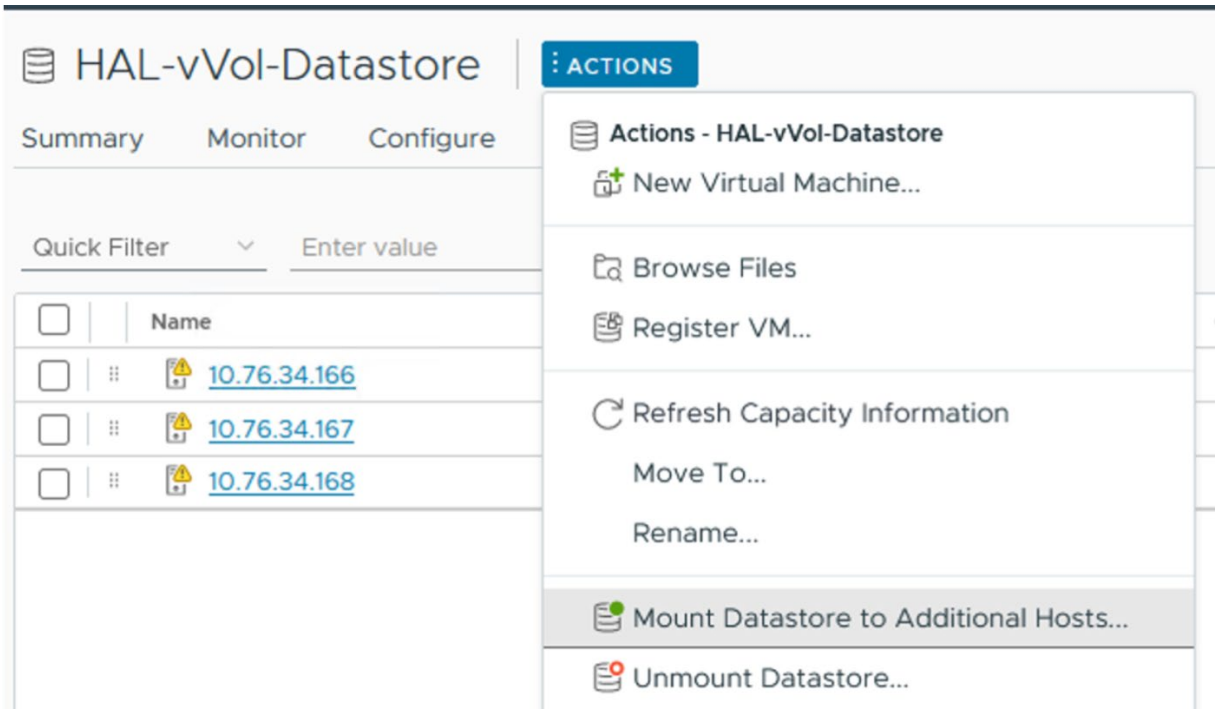
If there are any issues at this stage, you can run the following commands to list ESXi status.

```
[root@DC1-Node4:~] esxcli storage vvol protocolendpoint list
naa.60060E8140A3D140A3D1000000000001
   Host Id: naa.60060e8012a3d1005040a3d100000001
   Array Id: Hitachi:VSPG400G600_441937
   Type: SCSI
   Accessible: true
   Configured: true
   Lun Id: naa.60060e8012a3d1005040a3d100000001
   Remote Host:
   Remote Share:
   NFS4x Transport IPs:
   Server Scope:
   Server Major:
   Auth:
   User:
   Storage Containers: ad635618-ca2c-4600-ba12-464524e4d2b4
[root@DC1-Node4:~] esxcli storage vvol storagecontainer list
DC1_G600_vVol01
   StorageContainer Name: DC1_G600_vVol01
   UUID: vvol:ad635618ca2c4600-ba12464524e4d2b4
   Array: Hitachi:VSPG400G600_441937
   Size(MB): 31739610
   Free(MB): 14791434
   Accessible: true
   Default Policy:
[root@DC1-Node4:~] esxcli storage vvol vasaprovider list
Hitachi-0356
   VP Name: Hitachi-0356
   URL: https://dc1vasa0350.ucp.local:50001/version.xml
   Status: online
   Arrays:
         Array Id: Hitachi:VSPG400G600_441937
         Is Active: true
         Priority: 0
[root@DC1-Node4:~]
```

If the new VVol Datastore is created successfully in one ESXi host, but the PE or VVol Datastore is not showing up in other hosts, you will need to manually mount it to all other hosts in the cluster. Make sure that ALU/PE devices are listed in the **Storage Devices** as shown.



1. Go to the newly created VVol Datastore and click **ACTIONS**
2. Click **Mount Datastore to Additional Hosts** and continue to add other hosts in the cluster.



Step 10. Create a Test VM to Verify vVol Operation

After the vVols datastore is created, create a test virtual machine (VM) for initial validation.

A quick way to verify the vVol operation is to clone a VM from VMFS datastore to a vVols datastore.

1. Right click on an existing VM, select Clone and then select Clone to Virtual Machine.
2. In the **Select Storage** section, select **VVol No Requirements Policy**

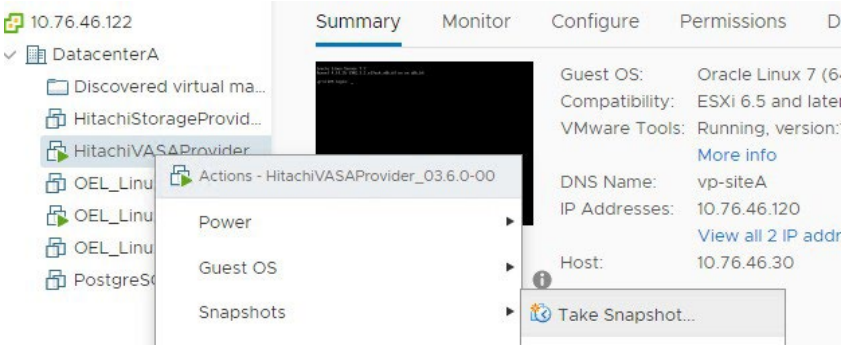
   A vVol datastore should appear at top of the list as compatible storage.

3. Select the vVol datastore and select clone.

4. Power on the test VM that you just cloned, and ensure that it powers on successfully.

   This confirms that you have successfully deployed a basic vVols environment.

5. Take a snapshot of your configured Hitachi VASA Provider. If you want to reset the configuration after some basic tests, you can use this snapshot to revert.



Step 11. Examples of Advanced Storage Capabilities and Storage Policy Based Management

When the vVol environment is operational, the following advanced capabilities are available:

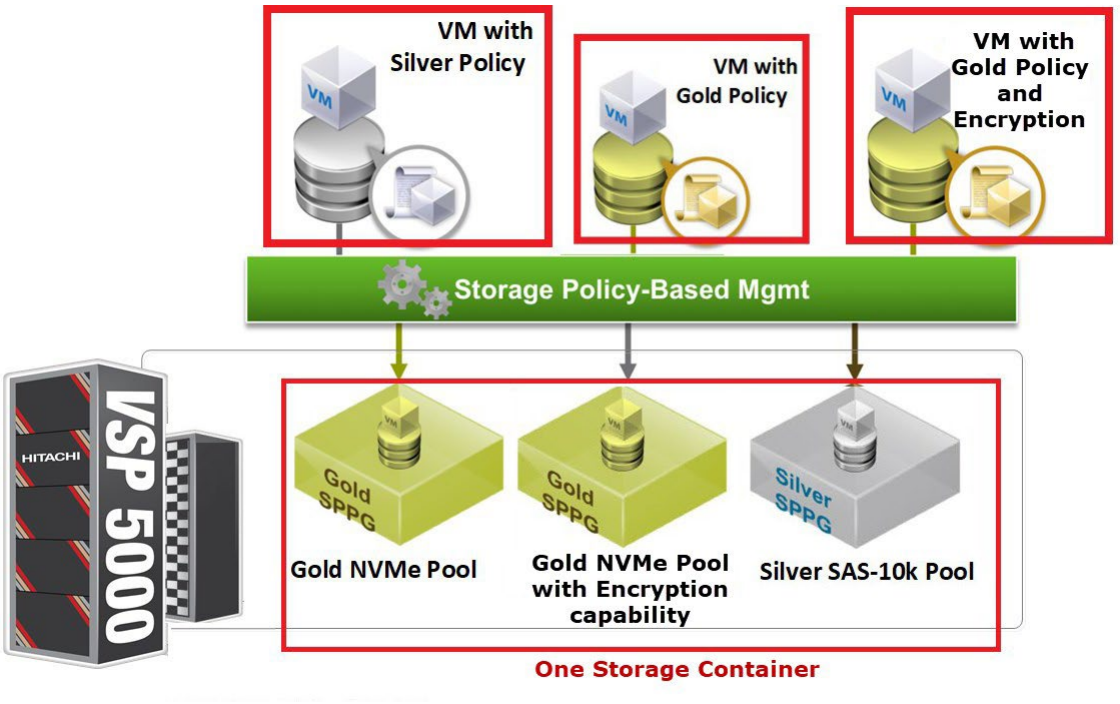
- Stage 1: In the Hitachi Storage Provider, apply storage capabilities on one or more pools that make up the storage container.
- Stage 2: In the vSphere client, set up VM storage policies that specifies a combination of these capabilities.

The following figure shows an example of how vVols Storage container and Storage Policy-Based Management (SPBM) policies can be configured with the Hitachi Implementation. There are more advanced configurations possible for production use cases. This example shows that the virtual machines (VMs) with a certain policy applied will land in a certain area of a storage container that matches that capability. vSphere administrators need not pick a datastore with a specific capability. The storage container, vVol datastore supports all capabilities.

In the following example, the virtualization capabilities of the VSP Storage use external pool resources from other VSPs or third party arrays.

- Two Gold NVMe Dynamic Provisioning (DP) pools were created in VSP 5500. One of the pools has encryption capabilities.
- Silver SAS 10k DP pool was created in VSP 5500 from external volumes from virtualized VSP or third party arrays.
- VASA Provider advertises the following to vSphere SPBM:
  - Gold Resources with Tier-1 performance capability with choice of encryption (Yes/No).
  - Silver Resources with Tier-2 performance capability.

Use the vSphere SPBM to enable vSphere administrators and VM owners the ability to choose Tier 1 Gold, Tier 1 Gold with Encryption, or Tier 2 Silver policies for VM and container services.

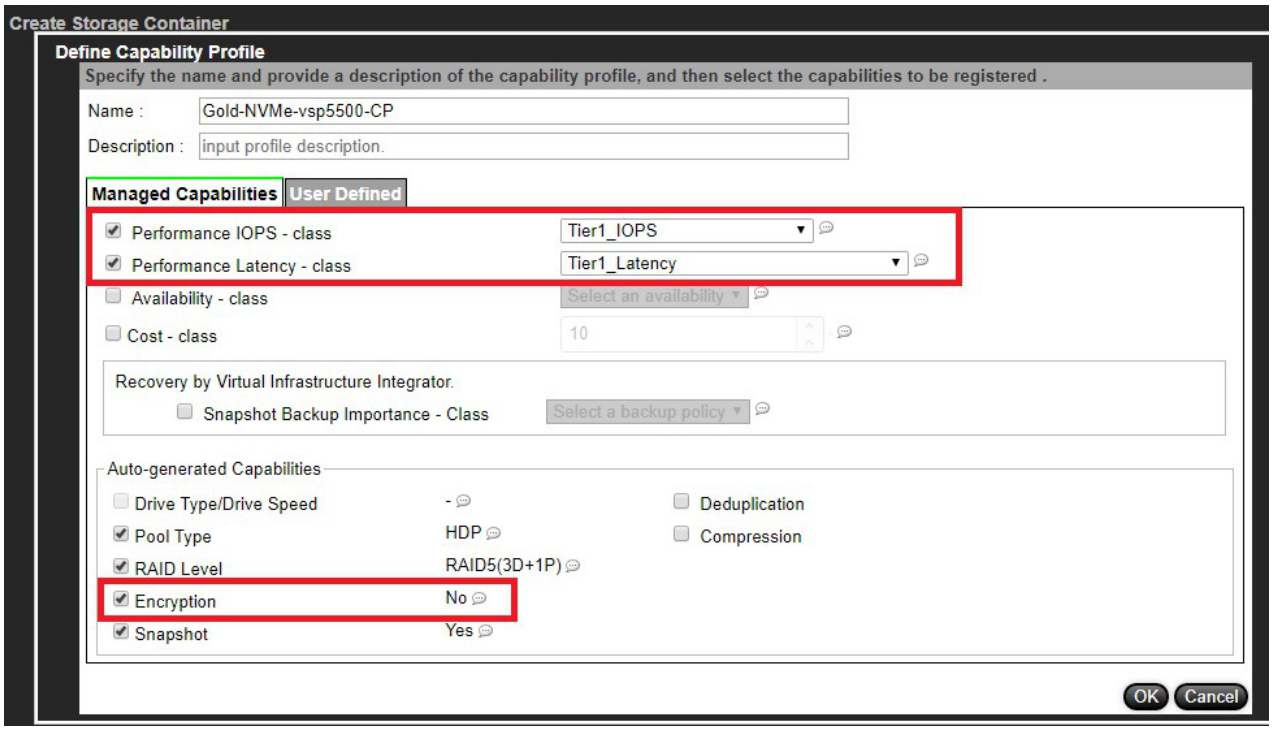


Stage 1 is to enable additional capabilities on the storage pools that are configured as part of the storage container.

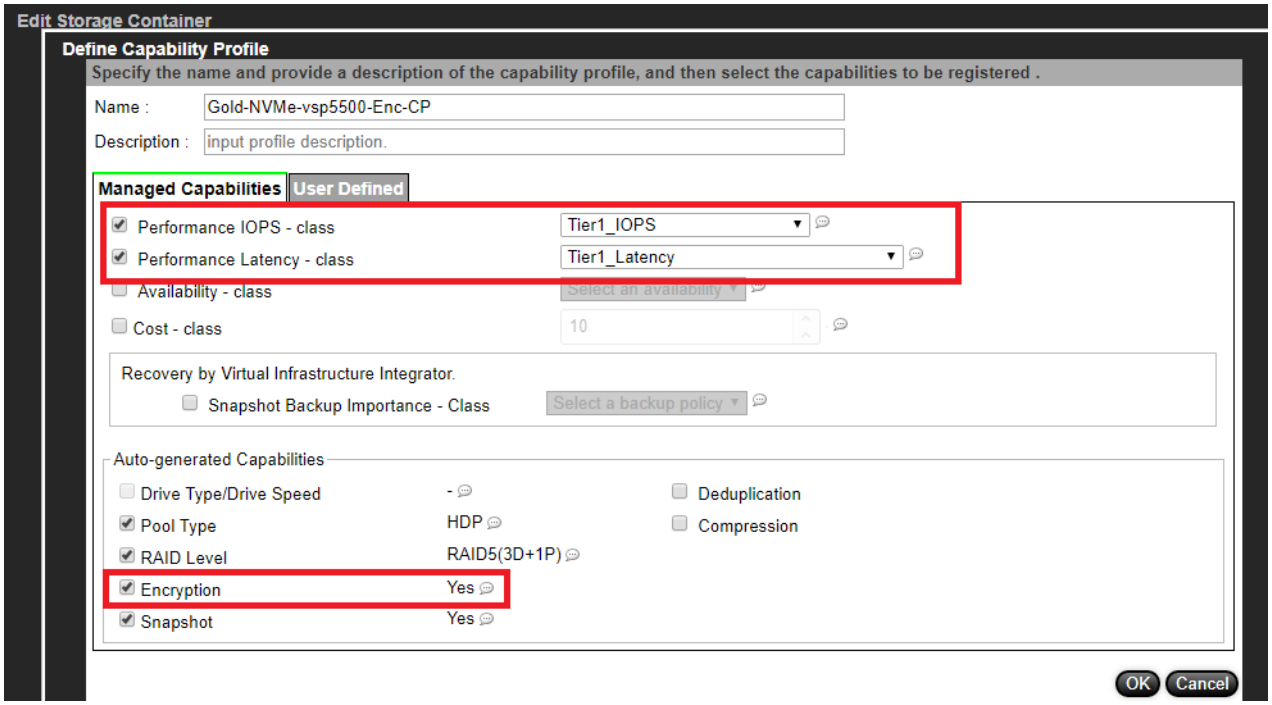
1. On Hitachi Storage Provider for VMware vCenter, go to **Manage Storage Containers**.
2. Select a storage container and click **Edit Storage Container**.
3. Select a pool in **Capability Profiles** and click **Define Profile**.

   The system automatically detects certain capabilities, (for example encryption, and allows other managed capabilities to be assigned various values based on the pool or system configuration.

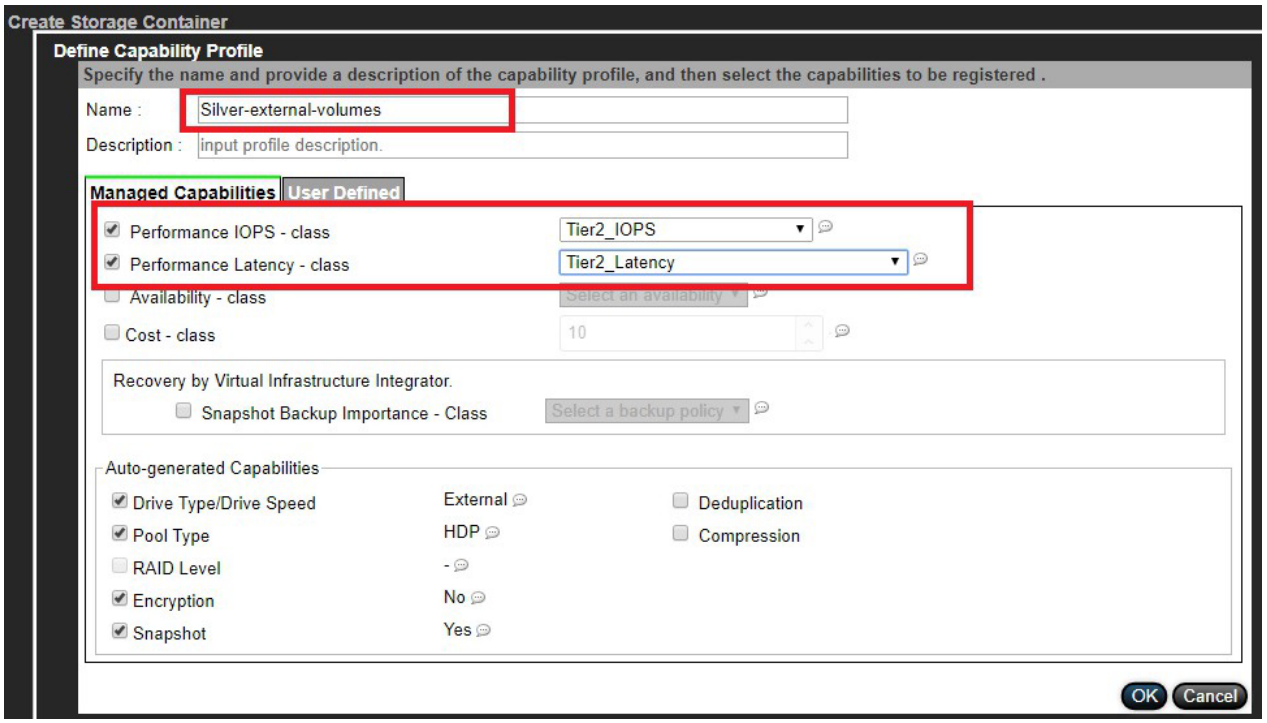
   In the following examples, the encryption is set to yes for the Gold-NVMe-vsp5500-CP pool and the encryption is set to no for the Gold-NVMe-vsp5500-Enc-CP pool. vSphere administrators now have a choice for encryption capability when building their VM policy. A storage administrator can provide other capabilities such as latency, IOPS, availability, and cost metrics.



As shown in the following figure, **Tier 1_IOPS** and **Tier 1_Latency** are set for the capability profile for both the Gold pools. However, they have different encryption policies.

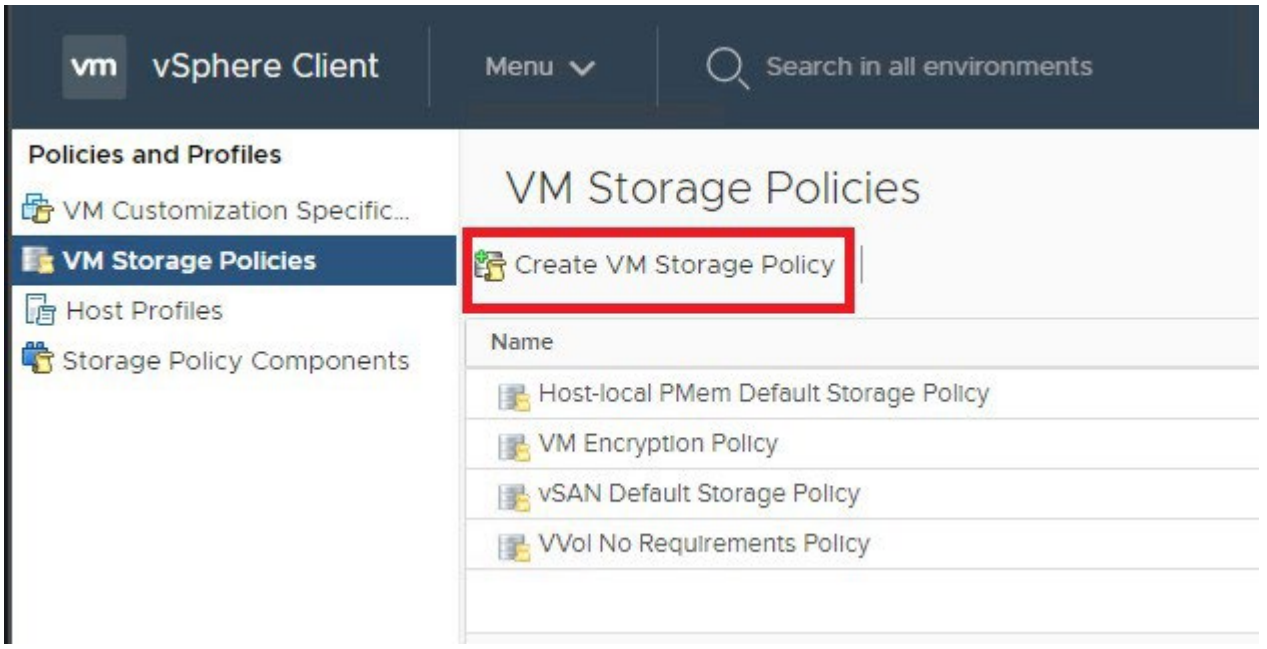


4. Create another capability profile for Silver-SAS-10k-External-pool with Tier 2 performance settings.

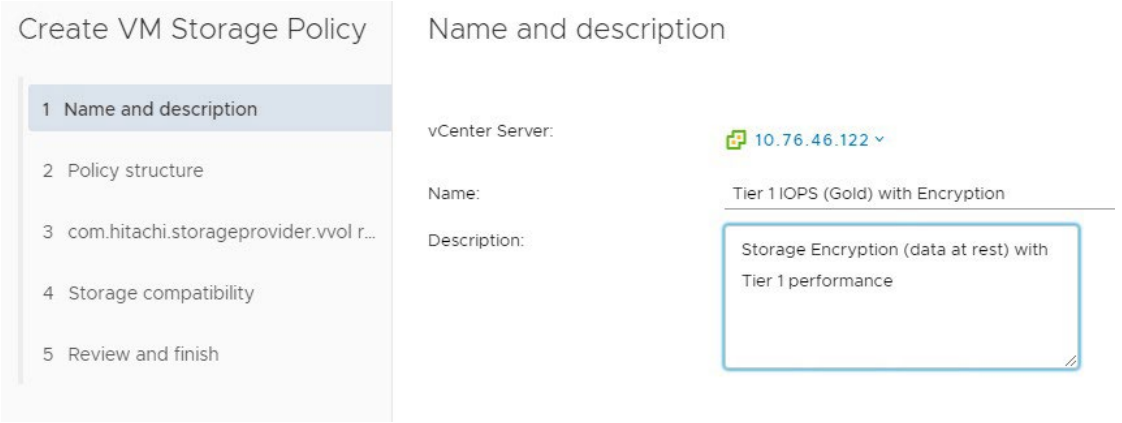


5. Configure the VM storage policies that are chosen during VM creation.
6. Log in to the vSphere Client.
7. On the home page, select VM Storage Policies under Policies and Profiles.

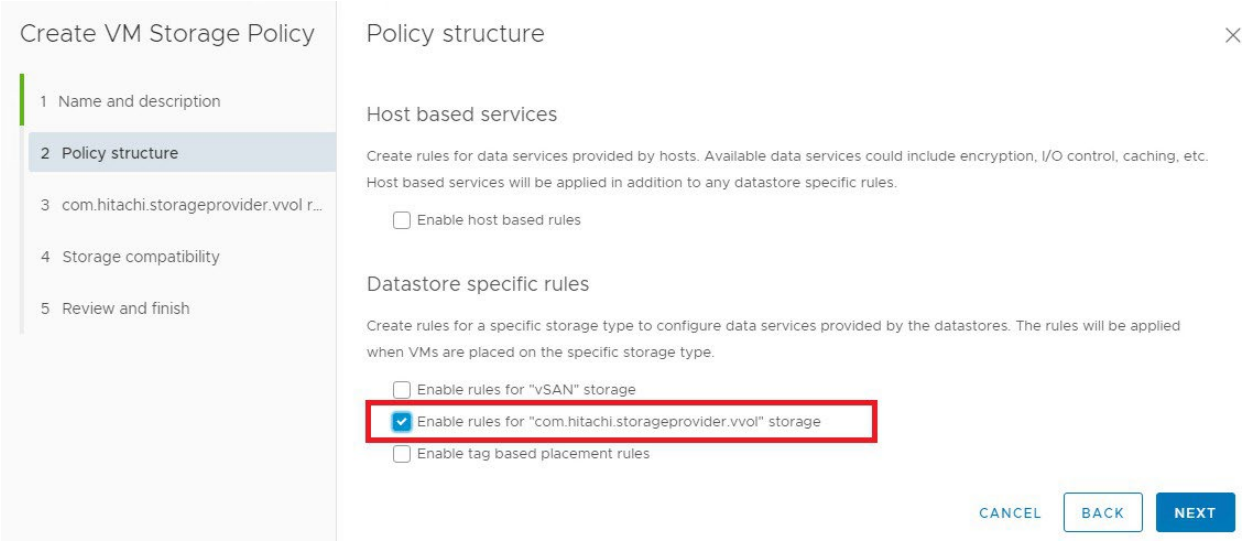
8. Click **Create VM Storage Policy**.



9. Create two Gold Policies. Specify encryption for one policy.
10. For each policy, provide a name and click **Next**.

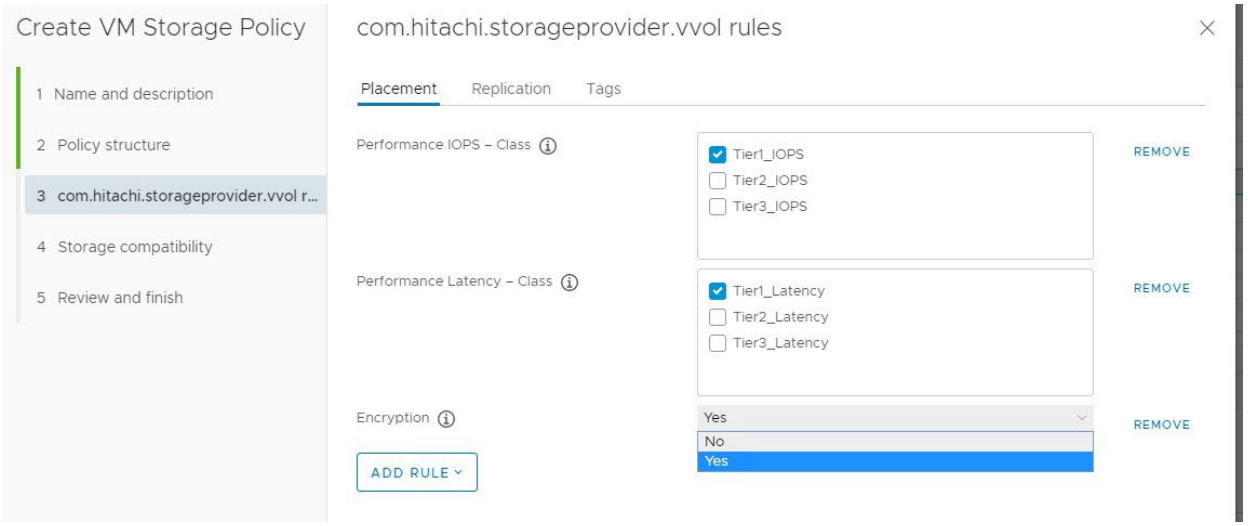


11. On **Datastore specific rule**, select **Enable rule for "com.hitachi.storageprovider.vvol" storage** and click **Next**.



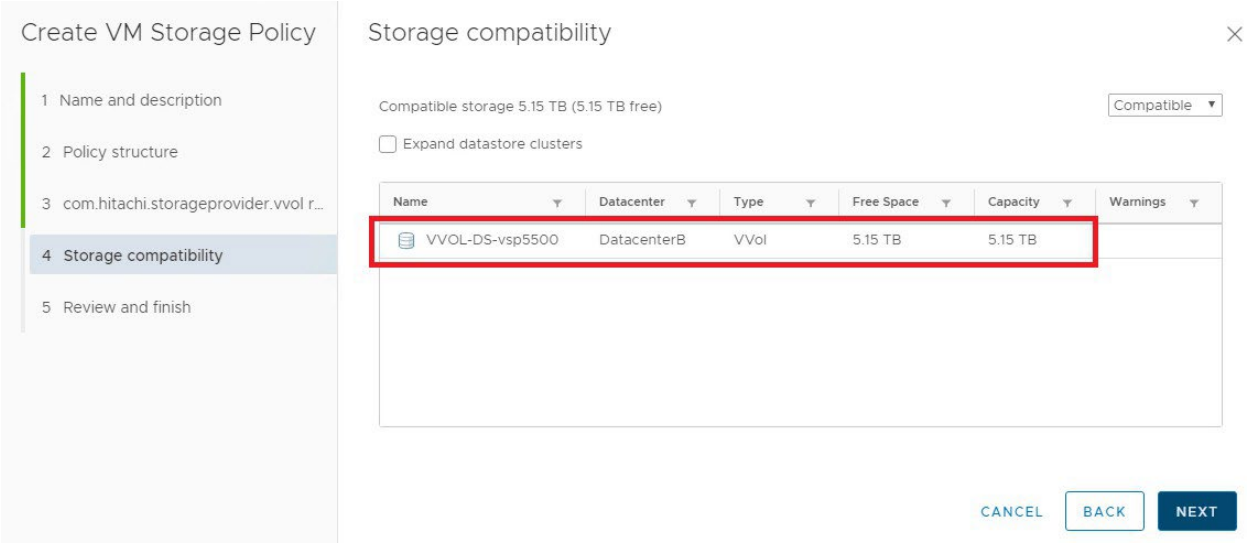
12. Select rule placement capabilities.

    In the following example, IOPS – Class and Latency – Class with **Tier 1** values are added for the Gold policy and the encryption is set to yes. Therefore, the policy is named Tier 1 IOPS (Gold) with Encryption. The other gold policy does not need to specify the encryption.

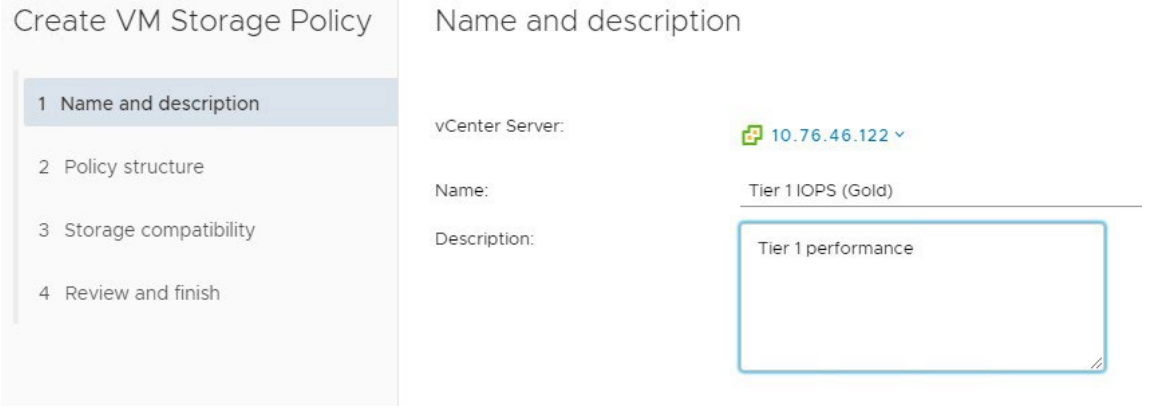


The compatible vVol Datastore shows up in the list.

13. Click **Next** and continue to complete the **Create VM Storage Policy** wizard.



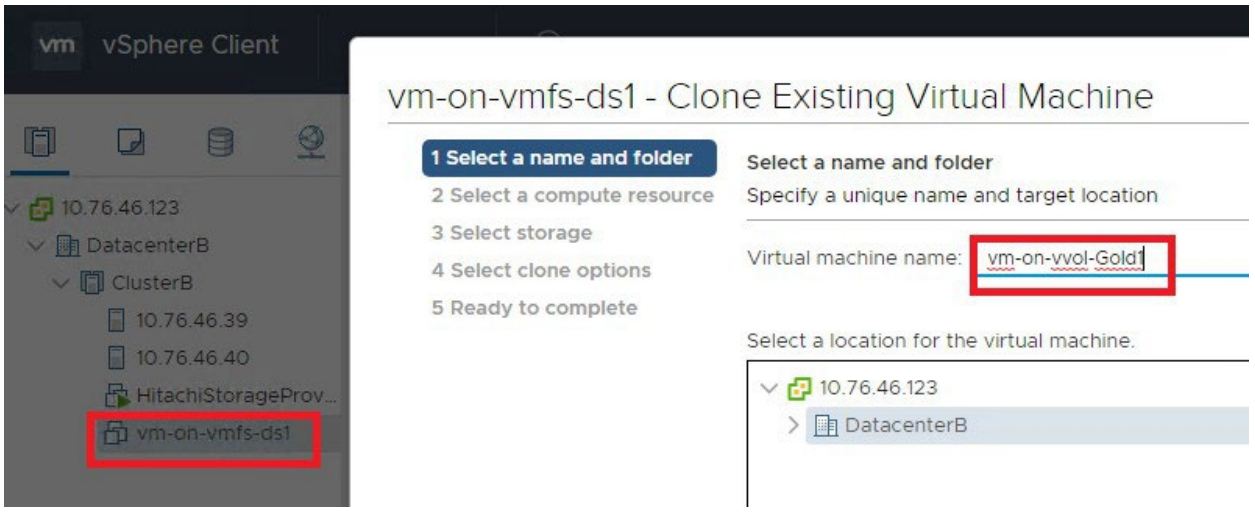
14. Repeat these steps to create the second gold policy without **Encryption** being specified as a capability.

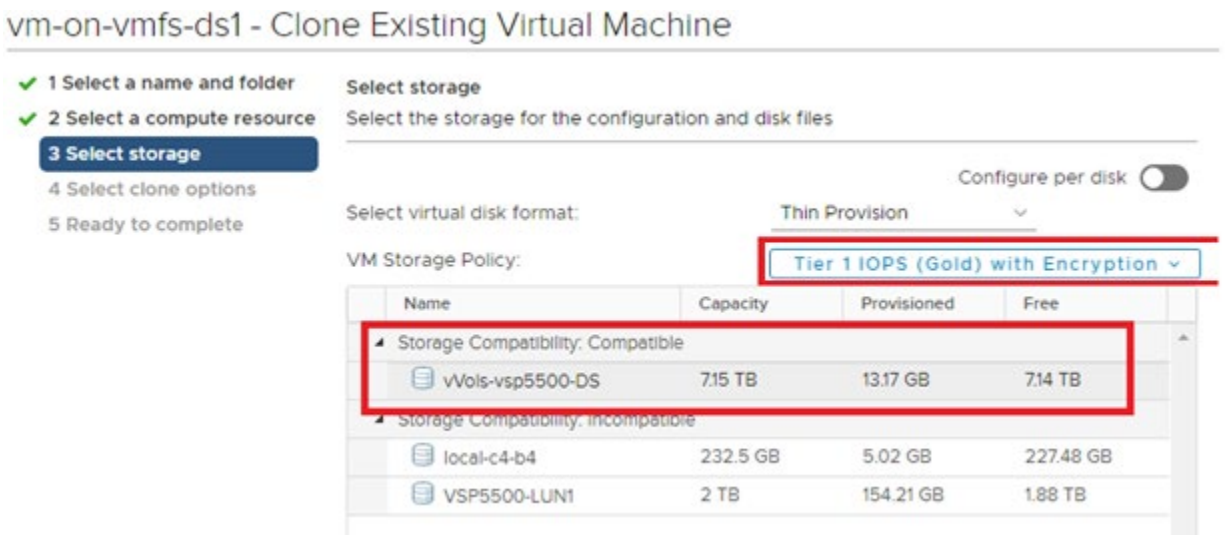


15. Repeat these steps to create a third VM storage policy: **Tier 2 IOPS (Silver)** with **Tier 2** performance capabilities.

Step 12. Deploy VMs with VMware SPBM and View vVols

1. Click Create New VM to create a new virtual machine (VM) or right-click on an existing VM and click **Clone to Virtual Machine** to clone an existing virtual machine.





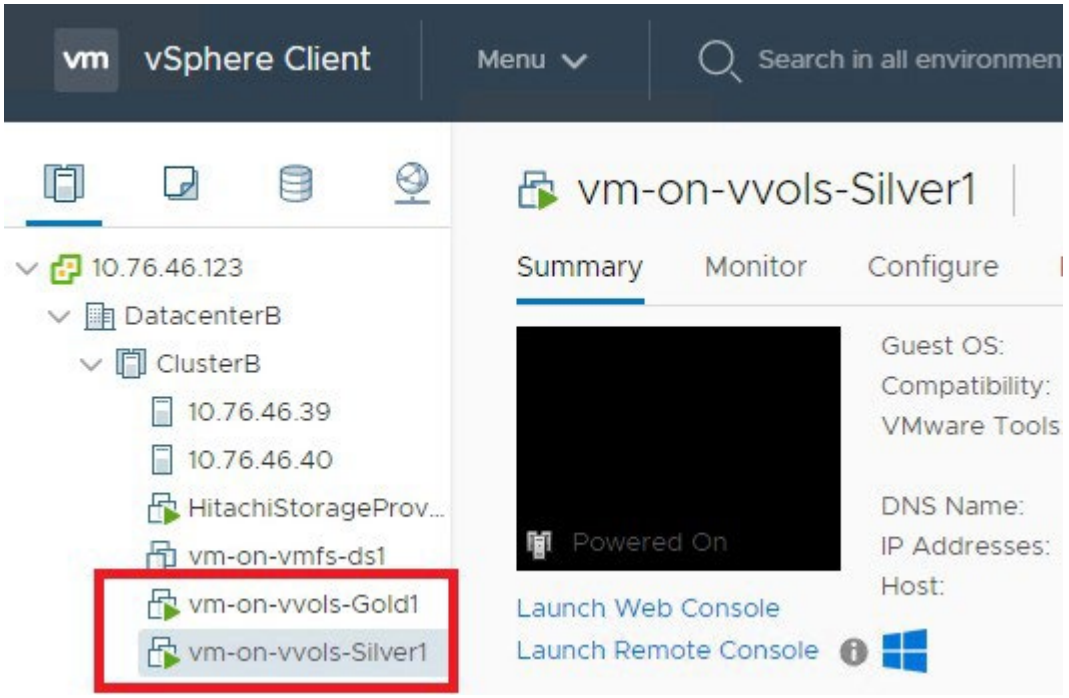
2. On the **Select storage** page, select the **VM Storage Policy: Tier 1 IOPS with or without Encryption.**

   For this example, a policy with Encryption is selected. The vVol datastore is shown as compatible.

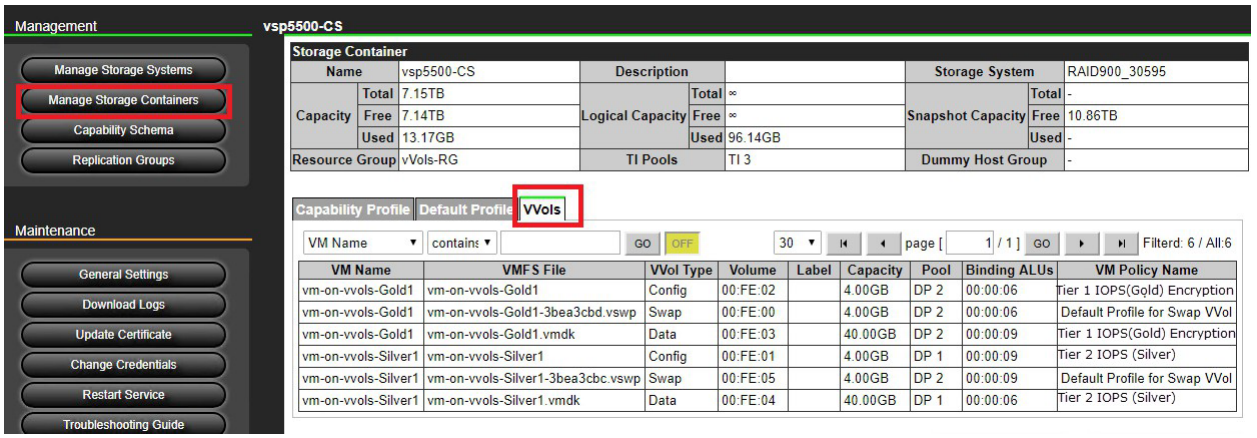
3. Click **Next**.

4. Repeat the clone VM steps (step numbers to be specified) to create a second vVol VM with **VM Storage Policy: Tier 2 IOPS (Silver).**

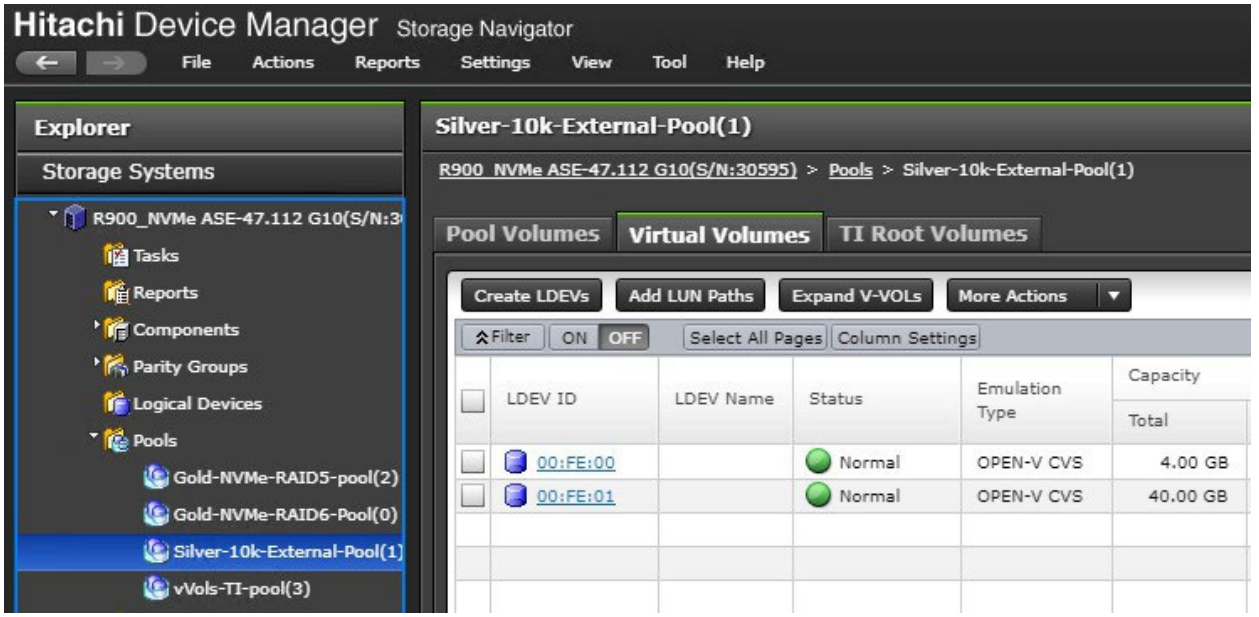
   A second VM with Silver policy is added.



5. After all the vVol VMs are created, verify the vVols in the Hitachi Storage Provider web interface.
6. Select **Manage Storage Container** under Management.
7. Select the storage container, and then select the VVols tab.

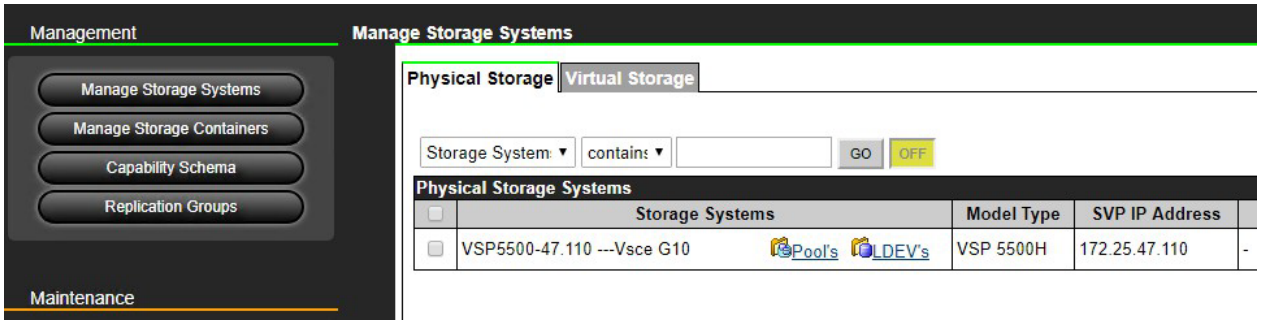


This lists the vVols created and their associated mapping to storage objects and policies. Storage administrators with an assigned read-only vCenter credentials can view this information. They can also access this information from tools such as, the Storage Navigator.

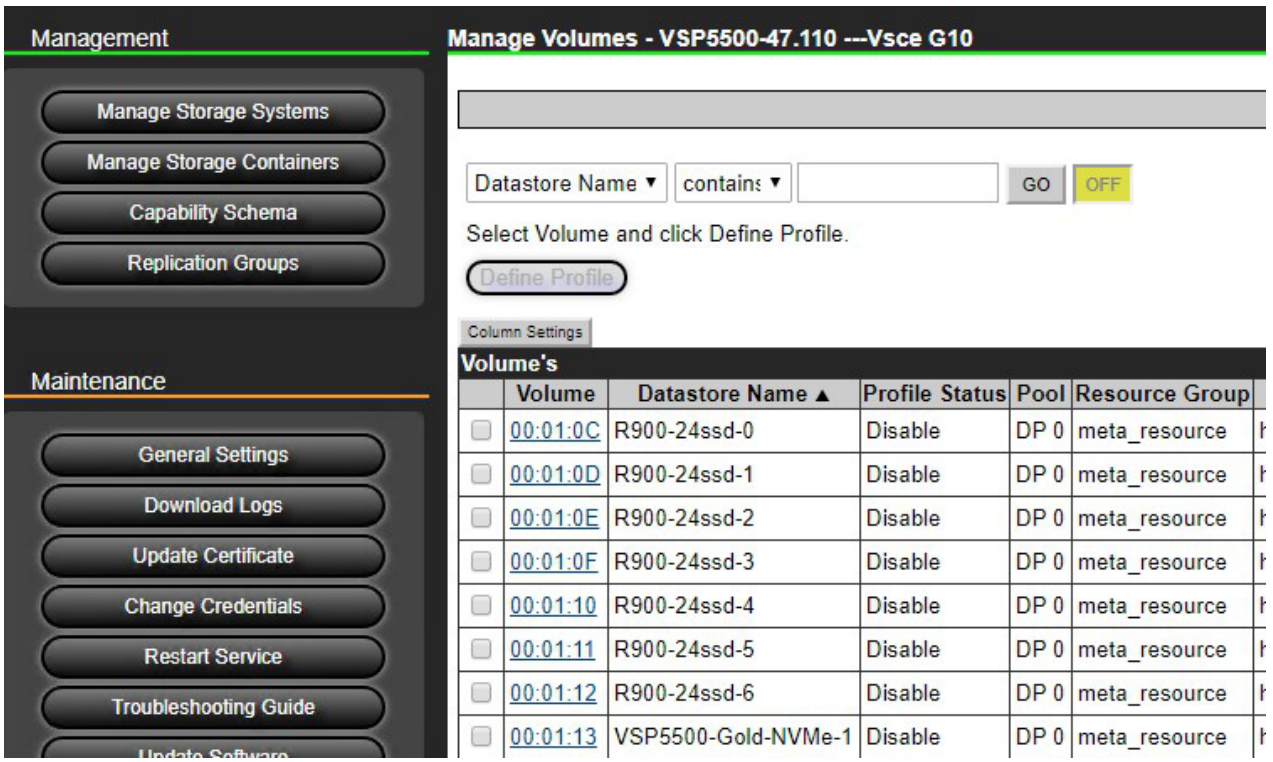


You can view VMFS volumes and storage pools within the Hitachi VASA Provider web interface.

1. **Select Manage Storage Systems** under Management, and click **LDEVs** to view the VMFS volumes and storage pools.



Datastores and their mapping to storage objects are listed.



Conclusion

For additional information, consult the Hitachi VASA provider deployment guide and release notes, available here. This location also includes the OVA/OVF files for download.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact