Dell EMC SC Series and VMware vSphere Virtual Volumes Best Practices

Abstract

Best practices for deploying and configuring VMware® vSphere® Virtual Volumes™ (vVols) with Dell EMC™ SC Series storage.

November 2019

Revisions

Date	Description
February 2016	Initial release
April 2016	Updated for Key Customer release
August 2016	Updated for DSM 2016 R2
September 2017	Updated requirements
November 2019	Updated link; vVols branding update

Acknowledgements

Author: Jason Boche

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

© 2016–2019 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Table of contents

1 Introduction to Virtual Volumes

Delivery of virtual machine and cloud storage through VMware® vSphere® Virtual Volumes™ (vVols) changes how storage is managed. Traditional shared storage management has matured over the years. Consolidating virtual machines onto a minimal number of datastores has been successful past through present and will continue to be a successful paradigm for years to come. However, with many array based integrations such as tiering, data deduplication, compression, RAID, snapshots, replication, and other data protection strategies occurring at the volume or datastore layer, the consolidated approach is not without identifiable challenges. Virtual Volumes address these challenges by allowing these integrations to be defined at the virtual machine or even application level. Management, deployment, and adherence becomes autonomous through vSphere integrated software defined storage policies. The end result is more granularity, greater scalability, and efficiency, Dell™ Storage Center OS (SCOS) 7.0 and Dell Storage Manager (DSM) 2016 R1 introduce compatibility and integration with Virtual Volumes.

2 Site preparation, requirements, and recommendations

When deploying Virtual Volumes, it is strongly encouraged to adhere to the following requirements and recommendations:

2.1 Requirements

- Dell SCOS 7.0 and supported SAN fabric such as Fibre Channel or iSCSI (VMware vSphere® software ISCSI only).
- Dell Storage Manager (DSM) 2016 R1 (R2 with external VASA Provider database for production environments), with incoming TCP 3034 allowed.
- VMware vSphere 6.0 infrastructure with Standard, Enterprise, or Enterprise Plus licensing.
- The Data Collector hosting the VASA Provider must have a static IP address or a dynamically assigned IP address which does not change. A corresponding Host (A) record should also be configured in DNS so that the VASA Provider may be registered using a FQDN.
- The Data Collector hosting the VASA Provider must be highly available and installed in a virtual machine with VMware vSphere High Availability (HA) protection enabled. VMware FT is an alternative option which can provide faster failover during an unplanned outage of the VASA Provider.
- The Data Collector hosting the VASA Provider should be deployed on a SAN volume which is configured with a high frequency of array-based snapshots to protect vVol metadata stored on the internal HSQL database.
- A Data Collector must not be deployed on a vVol which it is a VASA Provider for.
- An external database should be used in production environments to protect VASA Provider metadata. The external database must remain available and have redundant network paths to maintain VASA Provider operations availability.
- The external database for the Data Collector must not be deployed on a vVol which it is a VASA Provider for.
- A VASA Provider may be registered with one VMware vCenter™ Server only. Multiple vCenter Servers cannot be registered with the same VASA Provider.
- A vCenter Server may be registered with multiple VASA Providers. However, multiple VASA Providers cannot represent the same SC Series array to a single vCenter Server.
- The Data Collector hosting the VASA Provider may have up to a maximum of 50ms round trip network latency between it and the vCenter Server and a maximum of 10ms round trip network latency between it and vVol-enabled arrays.

2.2 Recommendations

- Install the Data Collector hosting the VASA Provider in an isolated management cluster
- Install the Data Collector hosting the VASA Provider in a VMware vSphere virtual machine with Fault Tolerance (FT) protection enabled
- Size the SC Series configuration appropriately to support the intended scale of the vVol environment. This may include flash storage to minimize the latency in creating and binding swap vVols associated with virtual machine power-on operations.

In addition, deployment and operational best practices should be followed for each piece of infrastructure as they are individually critical to the successful deployment and operation of Virtual Volumes. This includes but may not be limited to guidance found in the *Dell Storage Manager Administrator's Guide* as well as the *Dell EMC SC Series: VMware vSphere 5.x-6.x Best Practices*.

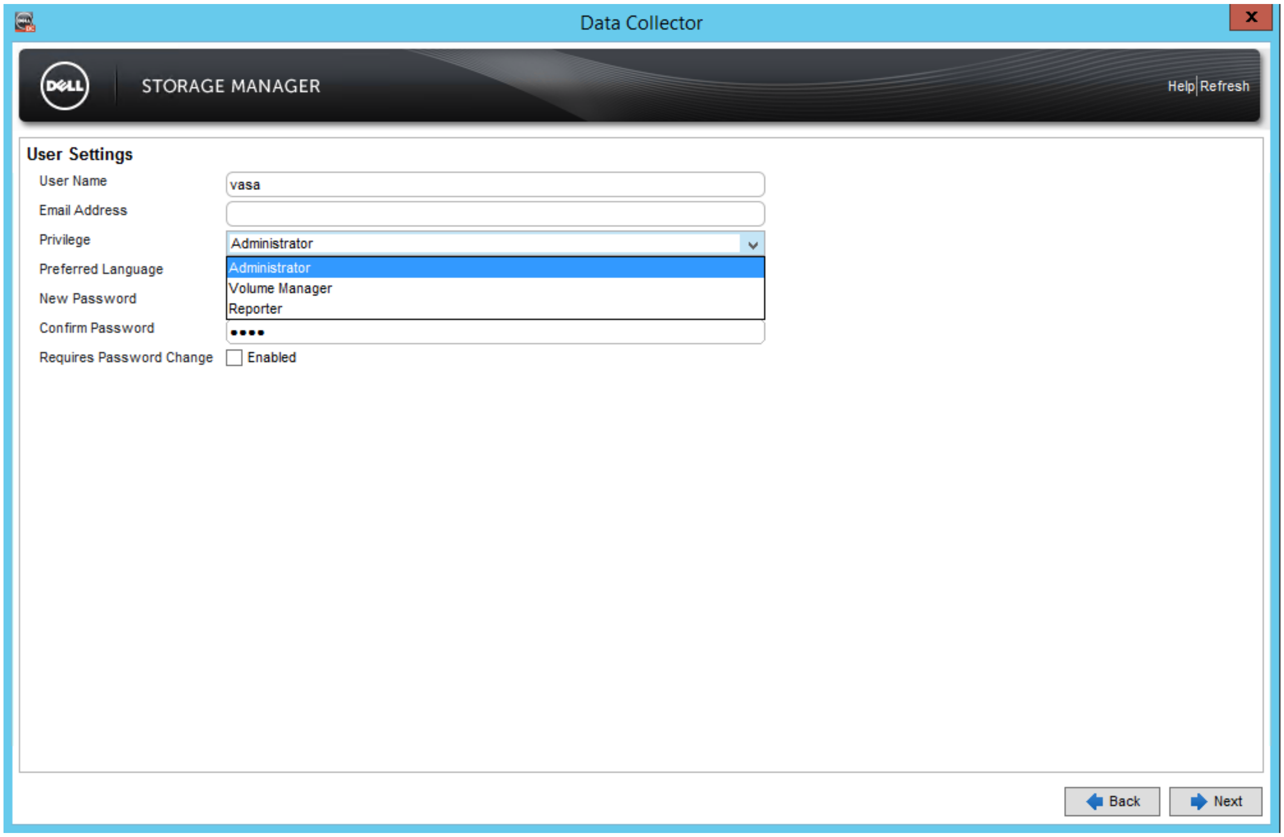
Note: Dell Storage Manager is an enterprise application. To maintain Virtual Volumes functionality and data availability, DSM, the VASA Provider, and its metadata must be made highly available by leveraging an external database. If the VASA Provider is impacted by a planned or unplanned outage (including network and database availability), vVol related operations will be impacted. This includes changing the installation of DSM (for example: uninstalling or reinstalling, or migrating the database that contains statistics and metadata). For any questions or concerns, or prior to making any changes impacting the VASA Provider in a production environment, contact Dell SupportAssist (see appendix A).

3 Deployment

The basic steps required to deploy Dell Storage Manager and Virtual Volumes are covered in the *Dell Storage Manager Administrator's Guide* and online help. Some of the steps will be highlighted here for the purposes of providing more depth or differentiation in methods available to complete a step. It is assumed at this point that a Dell EMC SC Series SAN, Dell Storage Manager, and VMware vSphere are online and available for Virtual Volumes deployment.

3.1 Dell Storage Manager and VASA Provider credentials

vSphere hosts do not have visibility or management capability of Virtual Volumes as traditional devices such as VMFS datastores or RDMs beyond the Storage Containers and Protocol Endpoints. The VASA Provider, bundled in Dell Storage Manager, provides out-of-band management of Virtual Volumes on SC Series from vCenter. Administrator or volume manager level credentials are required in DSM. A recommended best practice is to create a dedicated, documented, and secure service account for this function keeping in mind the implications if the account is subjected to a password rotation policy.



User Settings

User Name: vasa

Email Address:

Privilege: Administrator

- Administrator
- Volume Manager
- Reporter

Preferred Language

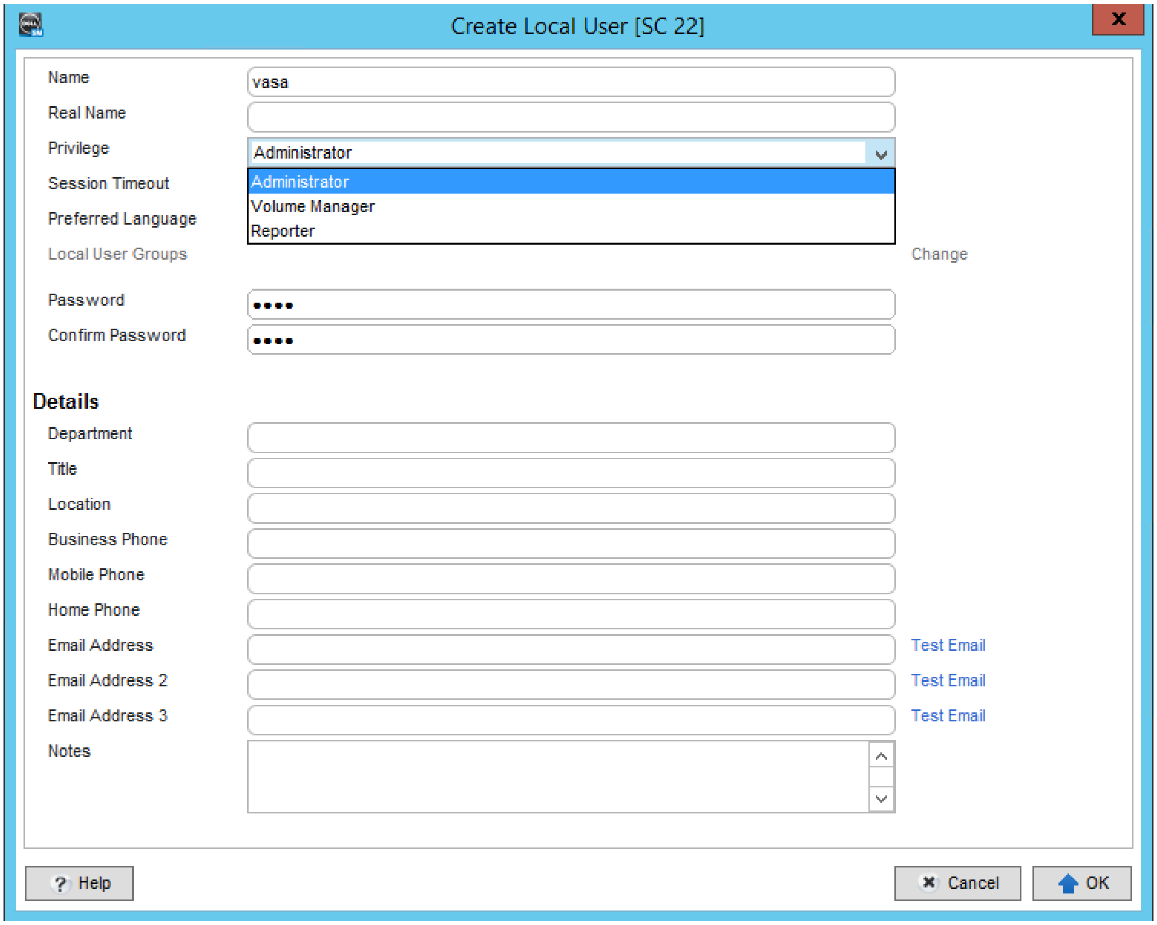
New Password

Confirm Password: ••••

Requires Password Change: □ Enabled

Figure 1 Create Dell Storage Manager credentials

Likewise, administrator or volume manager level credentials will need to be created on the SC Series array.



Name: vasa

Privilege: Administrator

Password: ••••

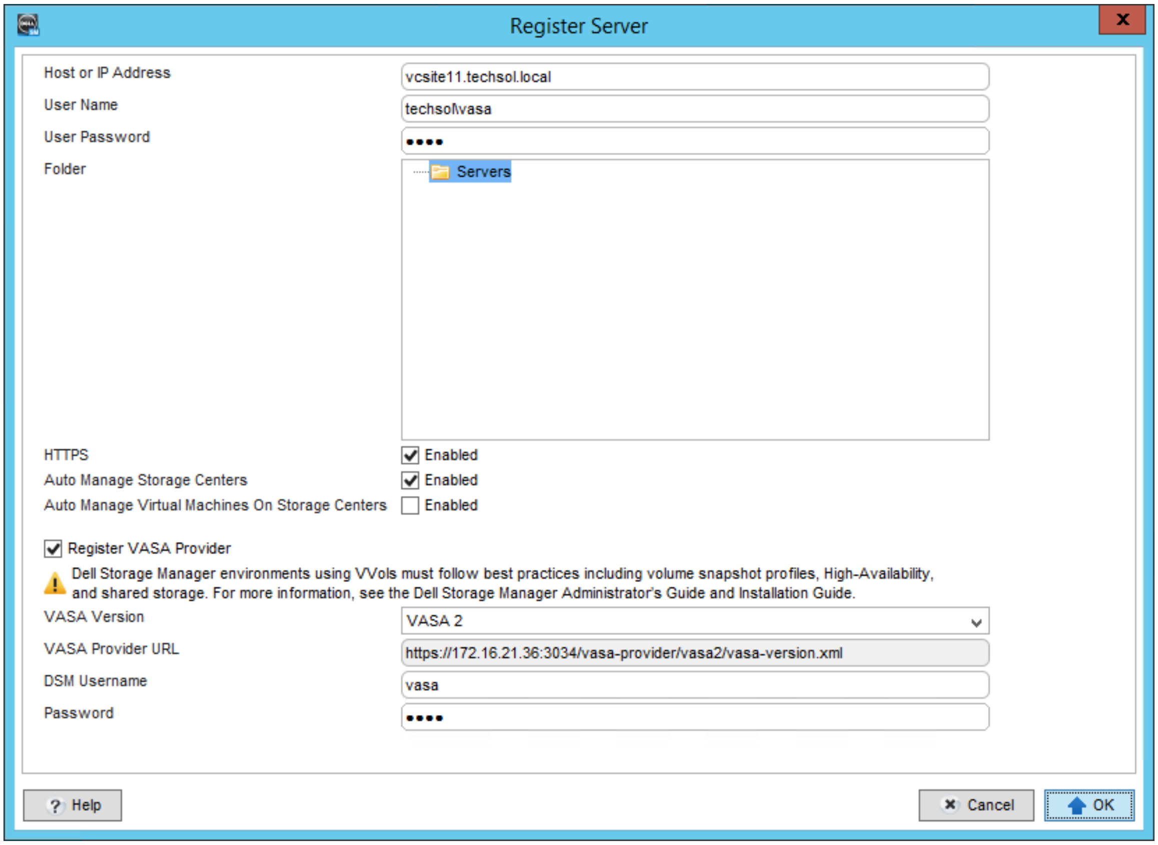
Confirm Password: ••••

Figure 2 Create SC Series user credentials

After the credentials are established on both DSM and SC Series array, launch the DSM Client, log in using the VASA Provider credentials, and use the **Add Storage Center** workflow to manage SC Series arrays where Virtual Volumes will be created. This is a good opportunity to validate the credentials as well as the health of the SC Series array and DSM. DSM currently supports managing up to 10 vVol-enabled SC Series arrays.

3.2 Register VMware vCenter Server in DSM

Register a vCenter Server in DSM by following the steps in the *Dell Storage Manager Administrator's Guide*. Optionally, the VASA Provider can also be registered at this time. The DSM username and password will be the VASA Provider credentials created in DSM earlier.



Host or IP Address: vcsite11.techsol.local

User Name: techsol\vasa

User Password: ••••

Folder: Servers

HTTPS ☑ Enabled

Auto Manage Storage Centers ☑ Enabled

Auto Manage Virtual Machines On Storage Centers ☐ Enabled

☑ Register VASA Provider

⚠ Dell Storage Manager environments using VVols must follow best practices including volume snapshot profiles, High-Availability, and shared storage. For more information, see the Dell Storage Manager Administrator's Guide and Installation Guide.

VASA Version: VASA 2

VASA Provider URL: https://172.16.21.36:3034/vasa-provider/vasa2/vasa-version.xml

DSM Username: vasa

Password: ••••

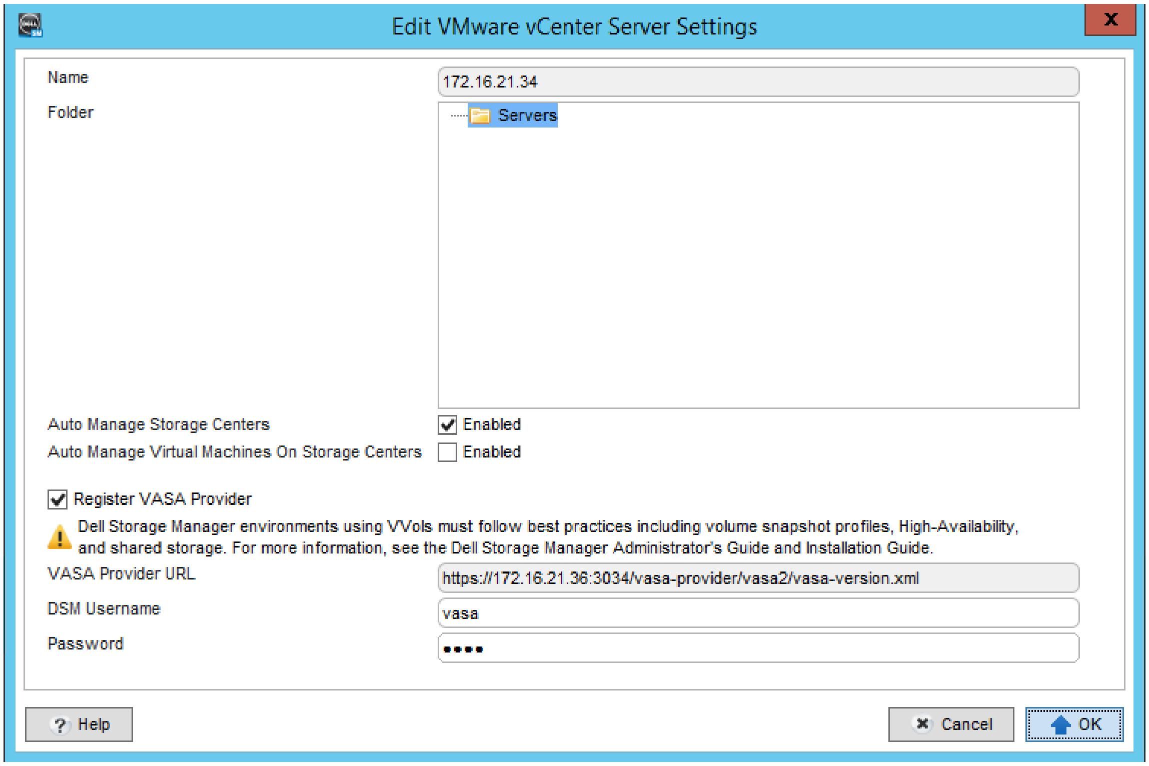
Figure 3 Register a VMware vCenter Server in DSM with or without registering the VASA Provider

Registering a vCenter server in the DSM servers view will automatically import clusters and servers on the Storage view along with the respective HBA details (WWIDs or IQNs) as well as configure the operating system type of VMware ESXi 6.0. This automatic import saves time and provides administrative consistency, especially for vSphere clusters with a larger number of hosts. DSM currently supports up to 50 clusters and 100 hosts per vCenter.

Note: The VASA 2.0 Provider URL format is: https://<DSM FQDN or IP Address>:3034/vasa-provider/vasa2/vasa-version.xml

3.3 Register the VASA Provider

If not completed during the vCenter Server registration, register the VASA 2.0 Provider in DSM by following the steps in the *Dell Storage Manager Administrator's Guide*. Although the VASA Provider may be registered in the VMware vSphere® Web Client, the preferred method is through DSM as outlined in the previous section.



Edit VMware vCenter Server Settings

Name: 172.16.21.34

Folder: Servers

Auto Manage Storage Centers: ☑ Enabled

Auto Manage Virtual Machines On Storage Centers: □ Enabled

☑ Register VASA Provider

Dell Storage Manager environments using VVols must follow best practices including volume snapshot profiles, High-Availability, and shared storage. For more information, see the Dell Storage Manager Administrator's Guide and Installation Guide.

VASA Provider URL: https://172.16.21.36:3034/vasa-provider/vasa2/vasa-version.xml

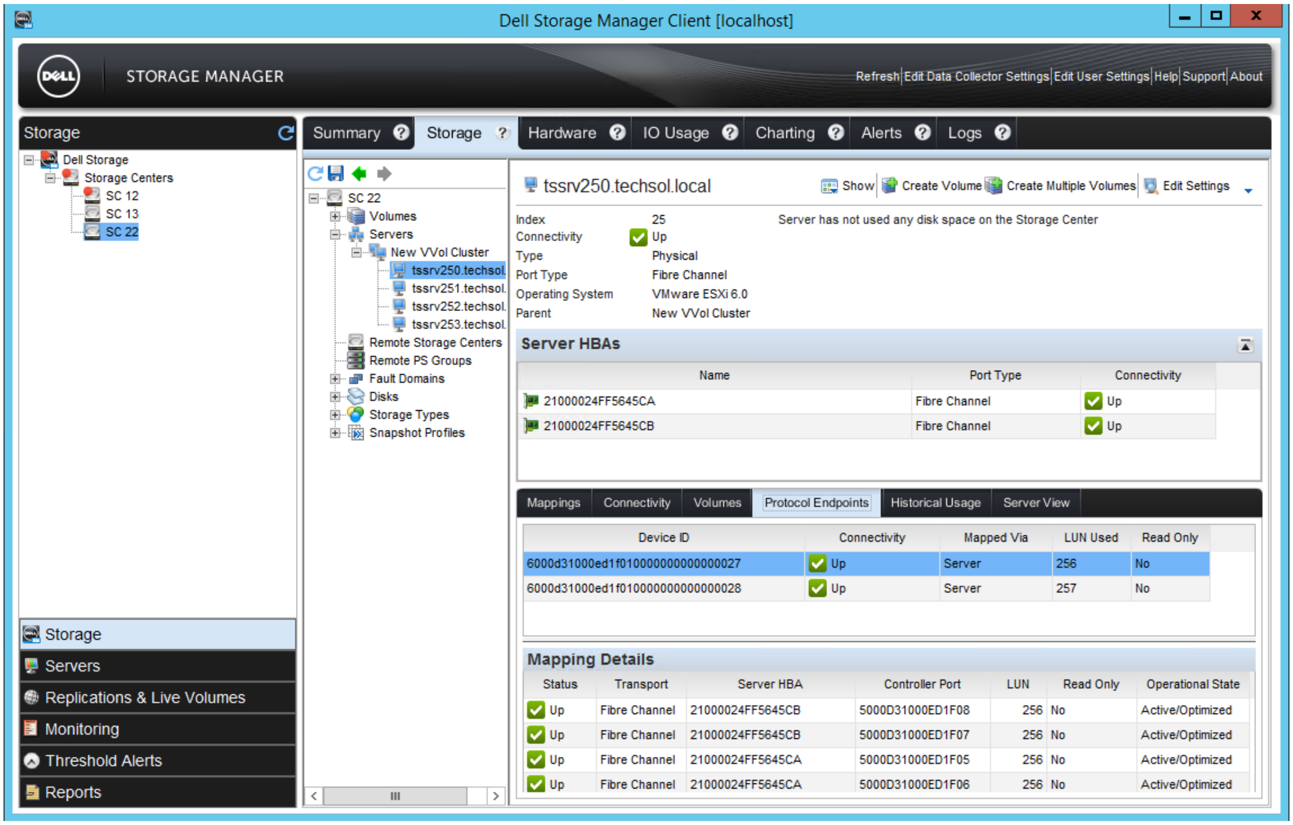
DSM Username: vasa

Password: ••••

Figure 4 Registering the VASA Provider in DSM

3.4 Protocol endpoints

When servers with a VMware ESXi 6.0 operating system are presented to SC Series arrays, protocol endpoints are created and presented to each of the vSphere hosts with LUN ID 256 (or next sequentially available up to 1,023). One protocol endpoint per controller is created per host. SC Series arrays support up to 50 protocol endpoints per controller. Each vSphere host supports up to 256 protocol endpoints for environments with multiple arrays hosting Virtual Volumes. The protocol endpoints are detected by the vSphere hosts as 512 Byte devices but they are not identified by vSphere as protocol endpoints until the VASA Provider is registered and a Storage Container is created. Protocol endpoints should not be used as traditional VMFS datastores.



tssrv250.techsol.local

Index	25
Connectivity	✓ Up
Type	Physical
Port Type	Fibre Channel
Operating System	VMware ESXi 6.0
Parent	New VVol Cluster

Server has not used any disk space on the Storage Center

Server HBAs

Name	Port Type	Connectivity
21000024FF5645CA	Fibre Channel	✓ Up
21000024FF5645CB	Fibre Channel	✓ Up

Device ID	Connectivity	Mapped Via	LUN Used	Read Only
6000d31000ed1f010000000000000027	✓ Up	Server	256	No
6000d31000ed1f010000000000000028	✓ Up	Server	257	No

Mapping Details

Status	Transport	Server HBA	Controller Port	LUN	Read Only	Operational State
✓ Up	Fibre Channel	21000024FF5645CB	5000D31000ED1F08	256	No	Active/Optimized
✓ Up	Fibre Channel	21000024FF5645CB	5000D31000ED1F07	256	No	Active/Optimized
✓ Up	Fibre Channel	21000024FF5645CA	5000D31000ED1F05	256	No	Active/Optimized
✓ Up	Fibre Channel	21000024FF5645CA	5000D31000ED1F06	256	No	Active/Optimized

Figure 5 Protocol Endpoints assigned by DSM

Note: Protocol Endpoints and their associated LUN IDs are automatically managed by DSM. Protocol endpoints may not be manually created or destroyed and their LUN IDs may not be modified.

4 Configuration and management

The foundational tasks involved with implementing Virtual Volumes in an environment may be performed only once or very seldom. This includes the registration of vCenter servers in DSM, creation of protocol endpoints, registration of the VASA Provider, and the creation of storage containers. This section will identify configuration and management options post deployment.

4.1 Creating and mapping an SC Series array

Before virtual machines can be deployed with Virtual Volumes and powered on, a datastore of type vVol (also commonly referred to as a vVol datastore) must be created from a storage container. Storage containers are seen by vSphere hosts as datastores. This enables many existing vSphere processes and workflows to remain seamless with the introduction of Virtual Volumes. One vVol datastore typically replaces several VMFS datastores. SCOS 7.0 storage containers are created per array, per page pool and may not cross array or page pool boundaries. Create a storage container in DSM by following the steps in the *Dell Storage Manager Administrator's Guide*. When storage containers are being created for a number of hosts in a vSphere cluster, this action should be performed on the cluster object in DSM rather than on the individual hosts. While DSM allows the creation of storage containers both in the Storage view and the Servers view, it is preferable to create storage containers from the Servers view. This is because the workflow also includes the mapping of the Storage Container to all of the vSphere hosts in the cluster as well as mounting the Storage Container on all of the vSphere hosts in the cluster for consistency. SC Series arrays currently support up to 50 storage containers. VMware supports up to 256 storage containers per host each having a size up to 2^{64} bytes.

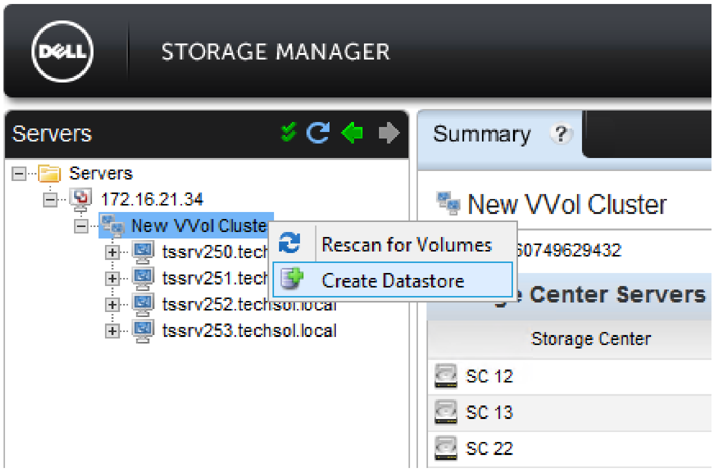
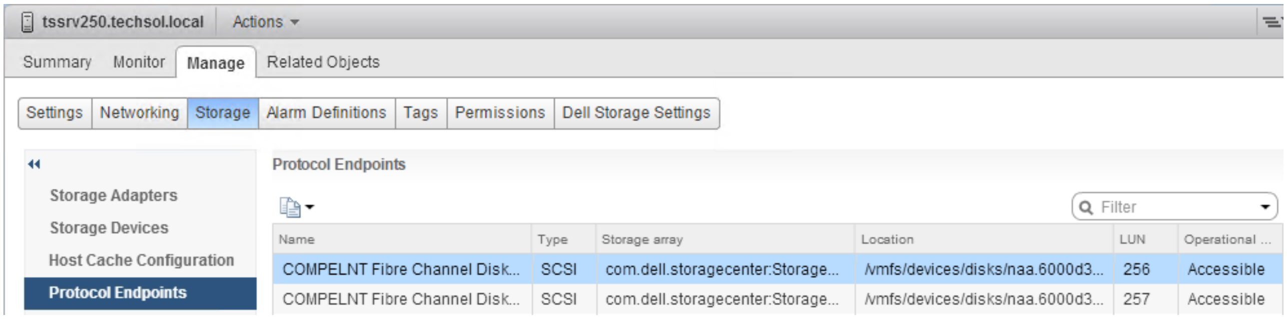


Figure 6 Best practice: Create storage containers in the Servers view

After the VASA Provider is registered and a storage container is created, vSphere hosts will recognize the protocol endpoints created and presented by DSM as protocol endpoints rather than just 512 Byte devices.

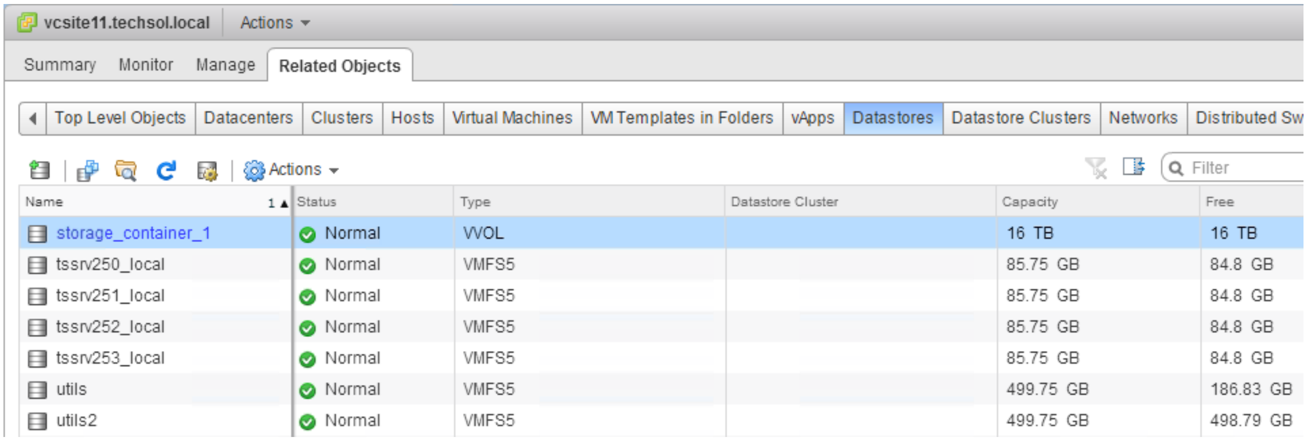


Protocol Endpoints

Name	Type	Storage array	Location	LUN	Operational ...
COMPELNT Fibre Channel Disk...	SCSI	com.dell.storagecenter:Storage...	/vmfs/devices/disks/naa.6000d3...	256	Accessible
COMPELNT Fibre Channel Disk...	SCSI	com.dell.storagecenter:Storage...	/vmfs/devices/disks/naa.6000d3...	257	Accessible

Figure 7 Protocol endpoints are visible in the vSphere Web Client after the storage container is created and presented to the hosts

The storage container becomes the pool of storage where various Virtual Volumes are created. Most notably these will be Config vVols, and Data vVols. A Swap vVol is created when the corresponding virtual machine is powered on.



Name	Status	Type	Datastore Cluster	Capacity	Free
storage_container_1	Normal	VVOL		16 TB	16 TB
tssrv250_local	Normal	VMFS5		85.75 GB	84.8 GB
tssrv251_local	Normal	VMFS5		85.75 GB	84.8 GB
tssrv252_local	Normal	VMFS5		85.75 GB	84.8 GB
tssrv253_local	Normal	VMFS5		85.75 GB	84.8 GB
utils	Normal	VMFS5		499.75 GB	186.83 GB
utils2	Normal	VMFS5		499.75 GB	498.79 GB

Figure 8 A storage container mounted and seen as a vVol datastore in the vSphere Web Client

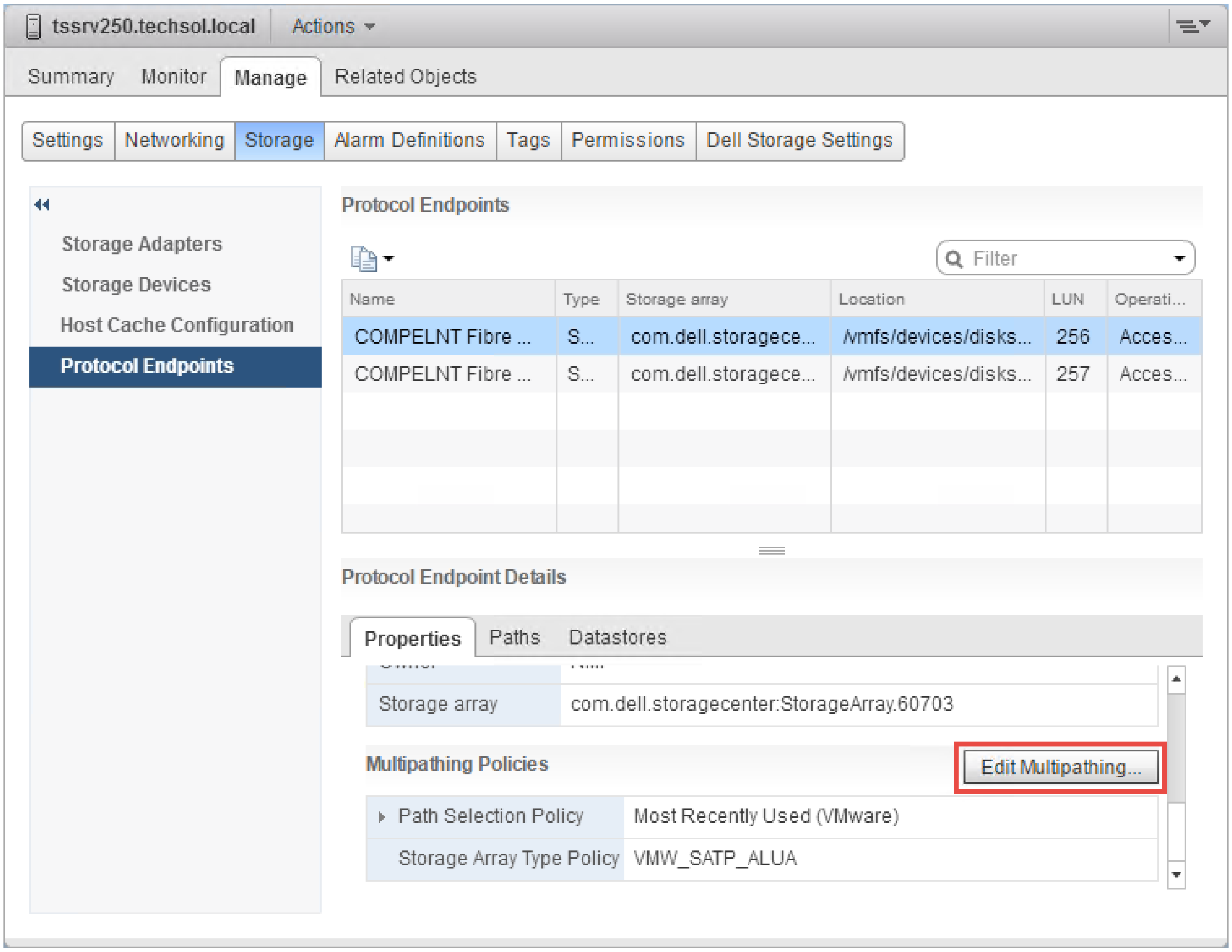
Note: Storage Containers or vVol datastores may be used as heartbeat datastores for vSphere clusters configured with High Availability (HA) enabled.

4.2 Changing the Protocol Endpoint Path Selection Policy

With Virtual Volumes enabled, I/O generated by virtual machines is multiplexed through protocol endpoints. Protocol endpoints are claimed by the VMW_SATP_ALUA Storage Array Type Plugin (SATP) which uses a default Path Selection Policy (PSP) of Most Recently Used (MRU). Dell recommends using the Round Robin or Fixed PSP for SC Series devices. This can be performed with the vSphere Web Client, esxcli, or VMware vSphere® PowerCLI™.

4.2.1 vSphere Web Client

To change the PSP to Round Robin or Fixed using the vSphere Web Client, navigate to the Protocol Endpoints view.



Protocol Endpoints

Name	Type	Storage array	Location	LUN	Operati...
COMPELNT Fibre ...	S...	com.dell.storagece...	/vmfs/devices/disks...	256	Acces...
COMPELNT Fibre ...	S...	com.dell.storagece...	/vmfs/devices/disks...	257	Acces...

Storage array	com.dell.storagecenter:StorageArray.60703

Multipathing Policies

Path Selection Policy	Most Recently Used (VMware)
Storage Array Type Policy	VMW_SATP_ALUA

Figure 9 Modifying the Protocol Endpoint PSP with the vSphere Web Client

4.2.2 esxcli

The following esxcli command reveals a protocol endpoint is using the VMW_PSP_MRU Path Selection Policy:

```
[root@tssrv251:~] esxcli storage nmp device list -d
naa.6000d31000ed1f010000000000000025
naa.6000d31000ed1f010000000000000025
   Device Display Name: COMPELNT Fibre Channel Disk
(naa.6000d31000ed1f010000000000000025)
   Storage Array Type: VMW_SATP_ALUA
   Storage Array Type Device Config: {implicit_support=on;explicit_support=off;
explicit_allow=on;alua_followover=on; action_OnRetryErrors=off;
{TPG_id=61448,TPG_state=AO}{TPG_id=61447,TPG_state=AO}{TPG_id=61445,TPG_state=AO
}{TPG_id=61446,TPG_state=AO}}
   Path Selection Policy: VMW_PSP_MRU
   Path Selection Policy Device Config: Current Path=vmhba1:C0:T0:L256
   Path Selection Policy Device Custom Config:
   Working Paths: vmhba1:C0:T0:L256
   Is USB: false
```

Esxcli can be used to modify the Protocol Endpoint PSP:

```
[root@tssrv251:~] esxcli storage nmp device set -d
naa.6000d31000ed1f010000000000000025 -P VMW_PSP_RR
```

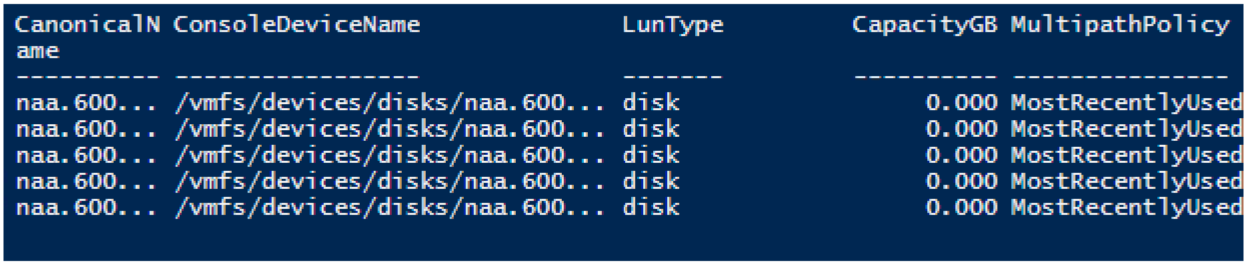
The Protocol Endpoint is now using the Round Robin Path Selection Policy:

```
[root@tssrv251:~] esxcli storage nmp device list -d
naa.6000d31000ed1f010000000000000025
naa.6000d31000ed1f010000000000000025
   Device Display Name: COMPELNT Fibre Channel Disk
(naa.6000d31000ed1f010000000000000025)
   Storage Array Type: VMW_SATP_ALUA
   Storage Array Type Device Config: {implicit_support=on;explicit_support=off;
explicit_allow=on;alua_followover=on; action_OnRetryErrors=off;
{TPG_id=61448,TPG_state=AO}{TPG_id=61447,TPG_state=AO}{TPG_id=61445,TPG_state=AO
}{TPG_id=61446,TPG_state=AO}}
   Path Selection Policy: VMW_PSP_RR
   Path Selection Policy Device Config:
{policy=rr,iops=1000,bytes=10485760,useANO=0; lastPathIndex=1:
NumIOsPending=0,numBytesPending=0}
   Path Selection Policy Device Custom Config:
   Working Paths: vmhba2:C0:T1:L256, vmhba2:C0:T0:L256, vmhba1:C0:T0:L256,
vmhba1:C0:T1:L256
   Is USB: false
```

4.2.3 PowerCLI

PowerCLI can also be used to manage the Path Selection Policy for protocol endpoints. Of the three methods covered here, PowerCLI is going to be the fastest and most consistent across an environment. The following PowerCLI reveals a protocol endpoint is using the VMW_PSP_MRU Path Selection Policy:

```
Get-Cluster -Name "New VVol Cluster" | Get-VMHost | Get-ScsiLun | where
{$_.Vendor -eq “COMPELNT” CapacityMB -lt 1 –and $_.Multipathpolicy -eq
“MostRecentlyUsed”}
```

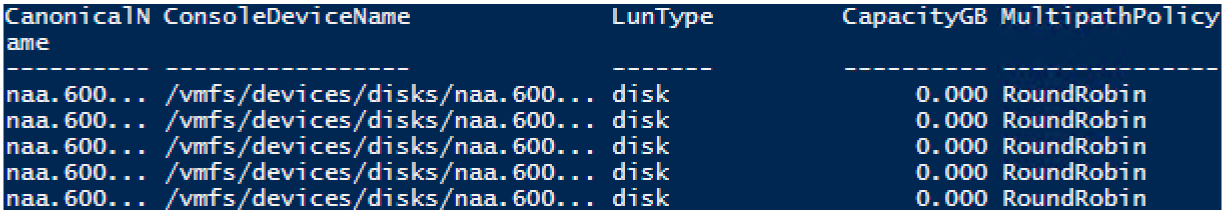


```
CanonicalN ConsoleDeviceName                LunType         CapacityGB MultipathPolicy
ame
---------- -----------------                -------         ---------- ---------------
naa.600... /vmfs/devices/disks/naa.600... disk                   0.000 MostRecentlyUsed
naa.600... /vmfs/devices/disks/naa.600... disk                   0.000 MostRecentlyUsed
naa.600... /vmfs/devices/disks/naa.600... disk                   0.000 MostRecentlyUsed
naa.600... /vmfs/devices/disks/naa.600... disk                   0.000 MostRecentlyUsed
naa.600... /vmfs/devices/disks/naa.600... disk                   0.000 MostRecentlyUsed
```

Figure 10 PowerCLI reflects a list of protocol endpoints using the Most Recently Used PSP

We can use similar PowerCLI to modify the PSP to Round Robin:

```
Get-Cluster -Name "New VVol Cluster" | Get-VMHost | Get-ScsiLun | where
{$_.Vendor -eq “COMPELNT” –and CapacityMB -lt 1 –and $_.Multipathpolicy -eq
“MostRecentlyUsed”} | Set-ScsiLun -Multipathpolicy RoundRobin
```



```
CanonicalN ConsoleDeviceName                LunType         CapacityGB MultipathPolicy
ame
---------- -----------------                -------         ---------- ---------------
naa.600... /vmfs/devices/disks/naa.600... disk                   0.000 RoundRobin
naa.600... /vmfs/devices/disks/naa.600... disk                   0.000 RoundRobin
naa.600... /vmfs/devices/disks/naa.600... disk                   0.000 RoundRobin
naa.600... /vmfs/devices/disks/naa.600... disk                   0.000 RoundRobin
naa.600... /vmfs/devices/disks/naa.600... disk                   0.000 RoundRobin
```

Figure 11 PowerCLI now reflects a list of protocol endpoints using the Round Robin PSP

4.3 Changing the default Path Selection Policy

Rather than change the PSP after devices are created and presented to the hosts in the vSphere cluster, it can be configured automatically as newly presented devices are discovered by the hosts. This would provide device PSP consistency within the cluster. Following are examples of a few methods which can be used to accomplish this.

4.3.1 esxcli

The following esxcli changes the default PSP for the VMW_SATP_ALUA SATP to Round Robin on a single host. This command would need to be executed on each host:

```
[root@tssrv251:~] esxcli storage nmp satp set -P VMW_PSP_RR -s VMW_SATP_ALUA
Default PSP for VMW_SATP_ALUA is now VMW_PSP_RR
```

4.3.2 PowerCLI

The following PowerCLI changes the default PSP for the VMW_SATP_ALUA SATP to Round Robin on all hosts in a cluster:

```
$Cluster = Get-Cluster -Name "New VVol Cluster"
ForEach ( $VMHost in ( Get-VMHost -Location $Cluster | Sort-Object Name ) )
{
    Write-Host "Working on host `"$($VMHost.Name)`"" -ForegroundColor Green
    $EsxCli = Get-EsxCli -VMHost $VMHost
    $EsxCli.storage.nmp.satp.list() | Where-Object { $_.Name -eq "VMW_SATP_ALUA"
}
    $EsxCli.storage.nmp.satp.set( $null, "VMW_PSP_RR", "VMW_SATP_ALUA" )
    $EsxCli.storage.nmp.satp.list() | Where-Object { $_.Name -eq "VMW_SATP_ALUA"
}
}
```

Note: The default Storage Array Type Plugin (SATP) used with SCOS 7.0 is VMW_SATP_ALUA and the default PSP for that plugin is MRU. Configure each protocol endpoint for either Round Robin or Fixed with a Preferred path. For more information about vSphere MPIO and SC Series arrays, refer to *Dell EMC SC Series: VMware vSphere 5.x-6.x Best Practices*.

4.4 Miscellaneous esxcli

Esxcli commands may be executed on a vSphere host to reveal Virtual Volume components exposed to vSphere. Following are a few examples relating to VASA Providers, protocol endpoints, and storage containers.

```
[root@tssrv251:~] esxcli storage vvol vasaprovider list
Dell Storage VASA 2.0 Provider
   VP Name: Dell Storage VASA 2.0 Provider
   URL: https://172.16.21.36:3034/vasa-provider/vasa2/vasa-version.xml
   Status: online
   Arrays:
         Array Id: com.dell.storagecenter:StorageArray.60703
         Is Active: true
         Priority: 0

[root@tssrv251:~] esxcli storage vvol protocolendpoint list
naa.6000d31000ed1f010000000000000025
   Host Id: naa.6000d31000ed1f010000000000000025
   Array Id: com.dell.storagecenter:StorageArray.60703
   Type: SCSI
   Accessible: true
   Configured: true
   Lun Id: naa.6000d31000ed1f010000000000000025
   Remote Host:
   Remote Share:
   Storage Containers: 6000d310-00ed-1f02-0000-00000000000a
```

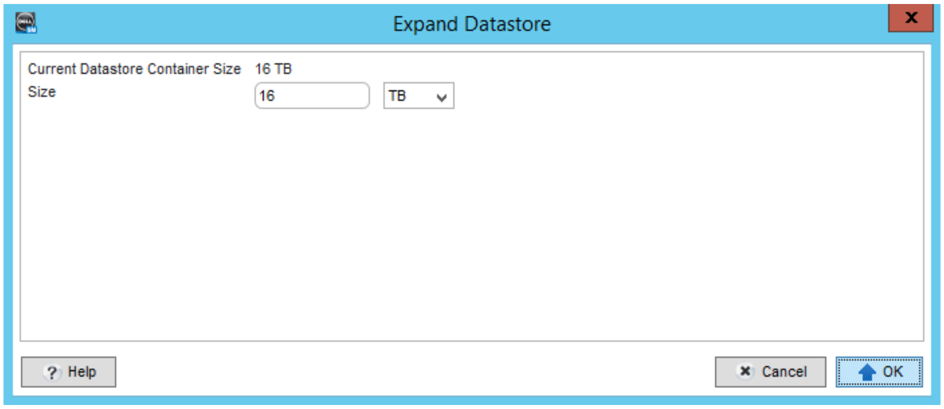
```
naa.6000d31000ed1f010000000000000026
   Host Id: naa.6000d31000ed1f010000000000000026
   Array Id: com.dell.storagecenter:StorageArray.60703
   Type: SCSI
   Accessible: true
   Configured: true
   Lun Id: naa.6000d31000ed1f010000000000000026
   Remote Host:
   Remote Share:
   Storage Containers: 6000d310-00ed-1f02-0000-00000000000a

[root@tssrv251:~] esxcli storage vvol storagecontainer list
storage_container_1
   StorageContainer Name: storage_container_1
   UUID: vvol:6000d31000ed1f02-000000000000000a
   Array: com.dell.storagecenter:StorageArray.60703
   Size(MB): 16777216
   Free(MB): 16723542
   Accessible: true
   Default Policy:
```

One thing to keep in mind when it comes to managing Virtual Volumes is that ESXi host visibility to storage ends at the storage container layer. A native command such as `esxcli storage core device list` would not reveal individual Virtual Volumes.

4.5 Storage container expansion

Aside from leveraging vSphere SPBM, there is very little to managing storage containers or protocol endpoints on a day-to-day basis. One exception might be expanding the storage container for growth. Storage containers can be grown by right clicking on the storage container from the Servers view in DSM and choosing **Expand Datastore**. Much like VMFS datastore expansion, storage containers can expanded on the fly.



Current Datastore Container Size 16 TB
Size 16 TB

Figure 12 A storage container can be expanded through the Servers view of DSM

4.6 Update Information in Dell Storage Manager

The Servers view in Dell Storage Manager is periodically updated with inventory changes which occur in vSphere with respect to clusters, hosts, datastores, storage containers, and virtual machines. Recent changes can be learned immediately in DSM by selecting the vCenter Server with a right mouse click and choosing the **Update Information** feature.

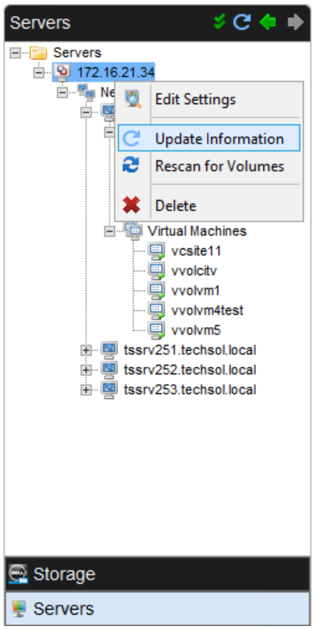


Figure 13 Force an update of vSphere inventory in DSM

4.7 Storage container deletion

If a storage container must be deleted, the most efficient and preferred method to perform this is through DSM from the Servers view. Before a storage container can be deleted, all supported child Virtual Volumes must first be removed or migrated using the vSphere Web Client.

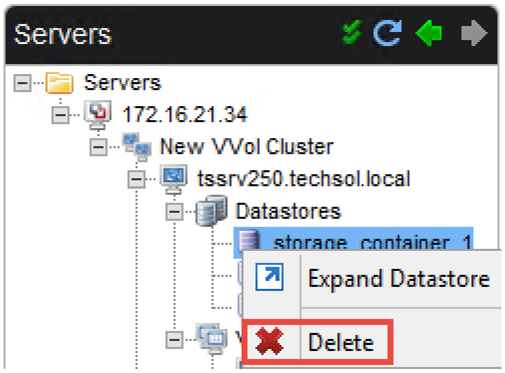
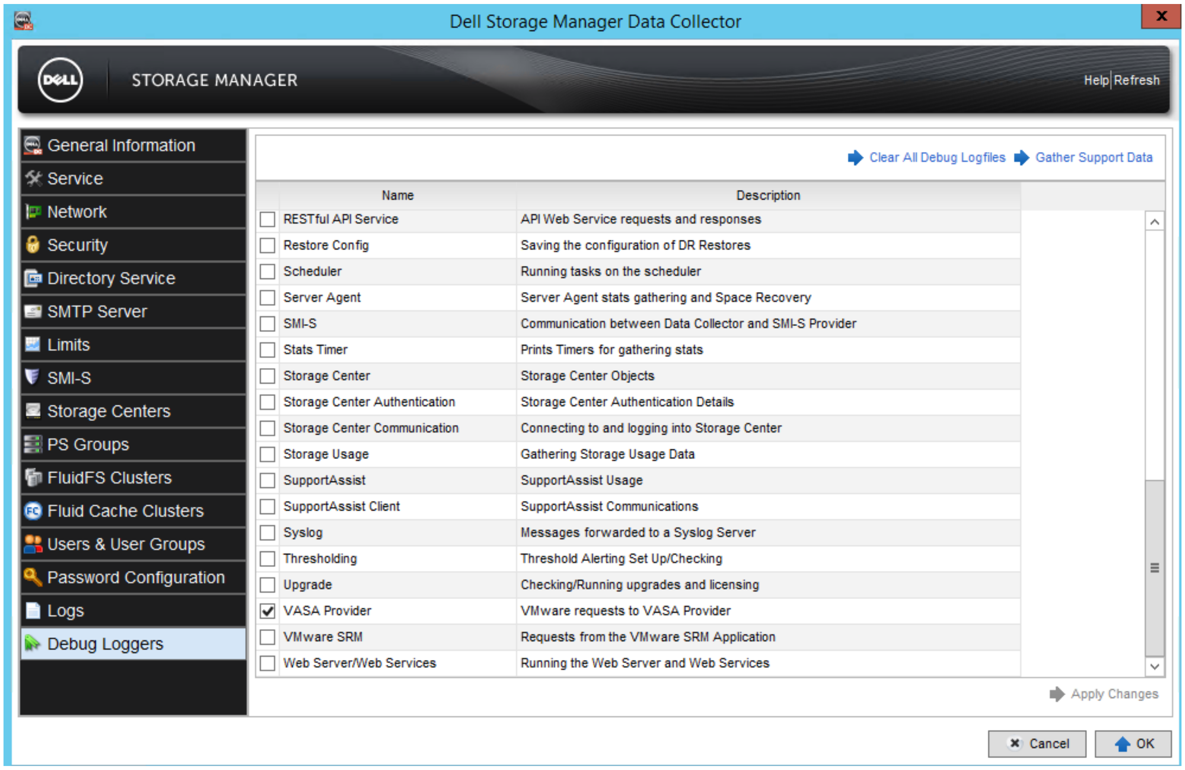


Figure 14 Deleting a storage container from the Servers view in DSM

4.8 Debugging and logging

VASA Provider debug logging is enabled by default in Dell Storage Manager. Dell recommends leaving this enabled.



	Name	Description
☐	RESTful API Service	API Web Service requests and responses
☐	Restore Config	Saving the configuration of DR Restores
☐	Scheduler	Running tasks on the scheduler
☐	Server Agent	Server Agent stats gathering and Space Recovery
☐	SMI-S	Communication between Data Collector and SMI-S Provider
☐	Stats Timer	Prints Timers for gathering stats
☐	Storage Center	Storage Center Objects
☐	Storage Center Authentication	Storage Center Authentication Details
☐	Storage Center Communication	Connecting to and logging into Storage Center
☐	Storage Usage	Gathering Storage Usage Data
☐	SupportAssist	SupportAssist Usage
☐	SupportAssist Client	SupportAssist Communications
☐	Syslog	Messages forwarded to a Syslog Server
☐	Thresholding	Threshold Alerting Set Up/Checking
☐	Upgrade	Checking/Running upgrades and licensing
☑	VASA Provider	VMware requests to VASA Provider
☐	VMware SRM	Requests from the VMware SRM Application
☐	Web Server/Web Services	Running the Web Server and Web Services

Figure 15 Debug Loggers in Dell Storage Manager Data Collector

A variety of log files exist to troubleshoot Virtual Volumes and the VASA Provider. The purpose and locations of these log files are listed below.

4.8.1 Dell Storage Manager

- Jboss server logs: C:\Program Files (x86)\Compellent Technologies\Compellent Enterprise Manager\msaservice\wildfly-8.2.1.Final\standalone\log\server.log
- DSM Support Data Zip file (includes logs from major DSM modules): C:\Program Files (x86)\Compellent Technologies\Compellent Enterprise Manager\msaservice\tmp.emzip

4.8.2 vCenter Server

- vCenter Server and VASA Provider registration interaction: vmware-sps/sps.log
- vCenter Server log: vpxd/vpxd.log
- vSphere Web Client log: vsphere-client/logs/vsphere_client_virgo.log

4.8.3 ESXi

- ESXi and VASA Provider interaction: /var/log/vvold.log
- Core VMkernel logs for ESXi containing SCSI interaction with Storage Center: /var/log/vmkernel.log
- Config vVol related requests forwarded to vvold.log: /var/log/osfsd.log
- ESXi host management service logs: /var/log/hostd.log

5 Storage Policy-Based Management (SPBM)

VM Storage Policies combine with Virtual Volumes to provide a software defined approach to storage management on a granular per-VM basis. Virtual machines, applications, and services are tied to a VM Storage Policy during initial deployment or storage migration. In turn, Virtual Volumes are provisioned with storage capabilities provided by the storage container which support the VM Storage Policy. Compliance checks are performed throughout the lifecycle of the virtual machine to ensure service level agreements (SLAs) are being met for the applications and services it provides.

5.1 Capabilities

The VASA 2.0 Provider can report any combination of the following storage container capabilities.

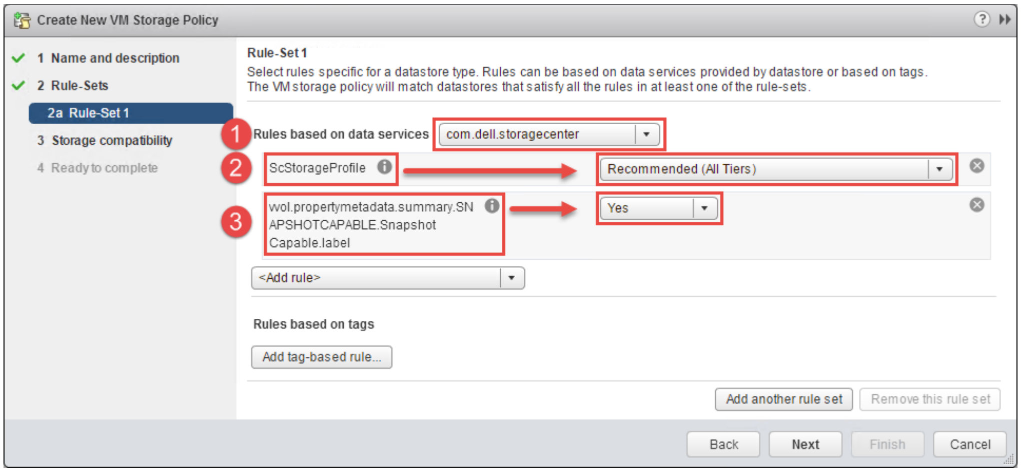
Table 1 VASA 2.0 Provider reported capabilities

Name	Value
Compression	True or False
Deduplication	True or False
Encryption	True or False
SnapshotCapable	True or False
ScStorageProfile	List of available SC Series storage profiles

5.2 Creating a VM storage policy

In the following example, a new VM storage policy is created with two storage capability requirements:

1. Choose the **com.dell.storagecenter** VASA 2.0 Provider.
2. Select the **Recommend (All Tiers)** storage profile, meaning that data is initially ingested into an upper performance tier and migrated to a lower tier when it becomes inactive.
3. Select **Yes** to make sure the Virtual Volume(s) are snapshot capable.



Rule-Set 1

Select rules specific for a datastore type. Rules can be based on data services provided by datastore or based on tags. The VM storage policy will match datastores that satisfy all the rules in at least one of the rule-sets.

Rules based on data services: com.dell.storagecenter

ScStorageProfile: Recommended (All Tiers)

wol.propertymetadata.summary.SNAPSHOTCAPABLE.SnapshotCapable.label: Yes

Rules based on tags

Figure 16 Creating a new VM storage policy

During initial deployment or storage migration of a virtual machine, this policy can be used for guidance and maintaining of compliance.

6 Virtual Volume operations

Virtual Volumes differ from traditional SC Series volumes in that certain operations available with traditional volumes are not available with vVols. Dell Storage Manager will not permit the following operations on a vVol:

- Edit or Delete
- Copy/Mirror/Migrate
- Map to Server

In the context of Virtual Volumes, creation, snapshot, reverting to snapshot, and deleting Virtual Volumes are generally transparent storage operations invoked by the vSphere Web Client.

Note: Block VAAI primitives are supported with Virtual Volumes. For more information changes with Virtual Volumes and the Thin Provision UNMAP primitive, please see VMware KB 2112333.

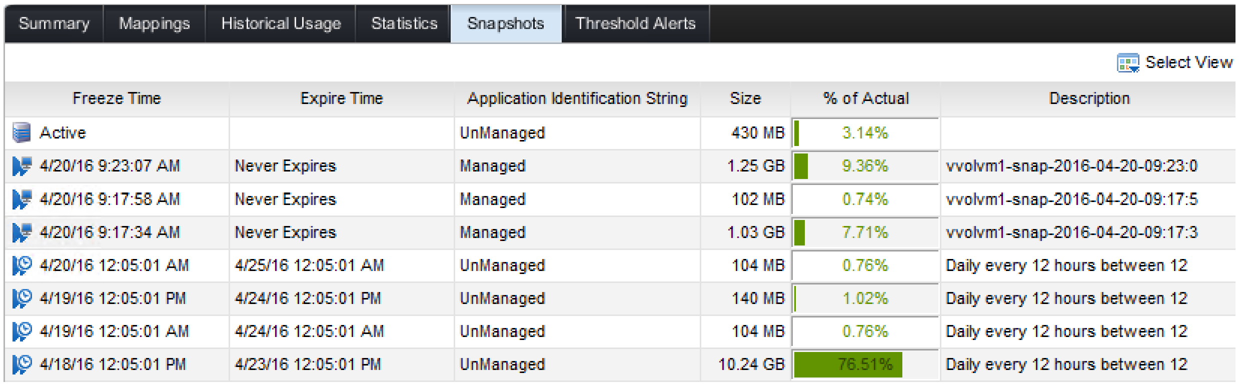
6.1 Creation

The creation of various Virtual Volumes occurs as a result of actions performed through vSphere. One example would be the creation of a new virtual machine, deploy from template, or cloning process. In these examples, Config and Data vVols will automatically be created to support the new virtual machine. Another example would be power-on operations of a virtual machine at which time a Swap vVol is created. A third example would be the addition of a virtual disk to an existing virtual machine hardware inventory which would create an additional Data vVol. Data-vVols are created in a Thin Provision virtual disk format on SC Series arrays.

Note: The Thick Provision virtual disk format of Data-vVols on SC Series arrays is not supported. When presented with the option during virtual machine operations, choose Thin Provision or the operation will fail. Be aware of operations where the default or native value selected is Thick Provision. The Thin Provision virtual disk format must be forced.

6.2 Snapshots

Snapshots created through vSphere with the vSphere Web Client or PowerCLI result in SC Series array-based snapshots of the type "Managed". SC Series arrays support up to 16,000 snapshots depending on the controller model. These snapshots will be maintained with no expiration on the array until they are deleted through vSphere. Unmanaged snapshots of a Virtual Volume occur outside of vSphere. Examples would be the creation of a snapshot using Snapshot Profile, Dell Storage Manager, or Dell PowerShell SDK.



Freeze Time	Expire Time	Application Identification String	Size	% of Actual	Description
Active		UnManaged	430 MB	3.14%	
4/20/16 9:23:07 AM	Never Expires	Managed	1.25 GB	9.36%	vvolvm1-snap-2016-04-20-09:23:0
4/20/16 9:17:58 AM	Never Expires	Managed	102 MB	0.74%	vvolvm1-snap-2016-04-20-09:17:5
4/20/16 9:17:34 AM	Never Expires	Managed	1.03 GB	7.71%	vvolvm1-snap-2016-04-20-09:17:3
4/20/16 12:05:01 AM	4/25/16 12:05:01 AM	UnManaged	104 MB	0.76%	Daily every 12 hours between 12
4/19/16 12:05:01 PM	4/24/16 12:05:01 PM	UnManaged	140 MB	1.02%	Daily every 12 hours between 12
4/19/16 12:05:01 AM	4/24/16 12:05:01 AM	UnManaged	104 MB	0.76%	Daily every 12 hours between 12
4/18/16 12:05:01 PM	4/23/16 12:05:01 PM	UnManaged	10.24 GB	76.51%	Daily every 12 hours between 12

Figure 17 Managed versus Unmanaged snapshots of a Data vVol

Note: Snapshots of virtual machines with Virtual Volumes is not supported if the virtual machines use VMFS or RDMs for storage.

6.3 Renaming

Renaming a virtual machine will not automatically result in the renaming of its associated Virtual Volumes. If it is desired that vVol names match the changed virtual machine name, migrate the virtual machine to a different datastore. vSphere will automatically change the associated names during the migration process. Optionally, migrate the virtual machine back to its original storage container to ensure storage policy adherence.

6.4 Deletion

Much like the creation of Virtual Volumes, the deletion of Virtual Volumes occurs through virtual machine operations. Powering off a virtual machine results in the unbinding and deletion of the Swap vVol. Deleting a virtual machine from inventory instructs the SC Series array through the VASA Provider to delete respective Config and Data vVols including any Data vVol snapshots which may exist.

Note: vVols cannot be deleted through Dell Storage Manager. Removal of a storage container through Dell Storage Manager cannot occur until all child vVols have been removed from the storage container through vSphere.

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell EMC storage platforms.

A.1 Related resources

Referenced or recommended Dell EMC publications:

- Dell Storage Manager Administrator's Guide
- Dell EMC SC Series: VMware vSphere 5.x–6.x Best Practices https://downloads.dell.com/manuals/common/sc-series-vmware-vsphere-best-practices_en-us.pdf

Referenced or recommended VMware publications:

- vSphere Storage Guide: http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-601-storage-guide.pdf
- vSphere Configuration Maximums: https://www.vmware.com/pdf/vsphere6/r60/vsphere-60-configuration-maximums.pdf