Technical Report

EqualLogic Virtual Storage Manager: Installation Considerations and Datastores Manager

Abstract

This technical report discusses the features of the VSM Datastores Manager and VASA Provider and focuses on a number of concepts that a user should consider prior to installation.

TR1067

v1.0

Authored By: David Glynn

January 2012

Preface

PS Series arrays optimize resources by automating performance and network load balancing. Additionally, PS Series arrays offer all-inclusive array management software, host software, and free firmware updates.

Audience

The information in this guide is intended for VMware vCenter administrators and PS Series SAN administrators.

Related Documentation

For detailed information about PS Series arrays, groups, volumes, array software, and host software, log in to the Documentation page at the customer support site.

Dell Online Services

You can learn about Dell products and services using this procedure:

1. Visit http://www.dell.com or the URL specified in any Dell product information.

2. Use the locale menu or click on the link that specifies your country or region.

Dell EqualLogic Storage Solutions

To learn more about Dell EqualLogic products and new releases being planned, visit the Dell EqualLogicTechCenter site: http://delltechcenter.com/page/EqualLogic. Here you can also find articles, demos, online discussions, technical documentation, and more details about the benefits of our product family.

For an updated Dell EqualLogic compatibility list please visit the following URL: https://support.equallogic.com/compatibility

Table of Contents

Revision Information

The following table describes the release history of this Technical Report.

Report	Date	Document Revision
1.0	January 2012	Initial Release

The following table shows the software and firmware used for the preparation of this Technical Report.

Vendor	Model	Software Revision
Dell	PS Series SAN	5.2 or higher, 6.x
VMware	vSphere vCenter	5.0 and 5.1
VMware	vSphere ESX/ESXi	4.1[1], 5.0 and 5.1
Dell	Virtual Storage Manager	3.5

Note: [1] vSphere ESX/ESXi 4.1 is supported when managed by vSphere vCenter 5.0 or above.

The following table lists the documents referred to in this Technical Report. All PS Series Technical Reports are available on the Customer Support site at: *support.dell.com*

Vendor	Document Title
Dell	TR1076: Virtual Machine Protection with Dell EqualLogic Virtual Storage Manager v3.5

Executive Summary

This technical report is aimed at VMware™ and Dell™ EqualLogic™ PS Series SAN administrators to guide them on the installation and usage of the Dell Virtual Storage Manager v3.5. This technical report will focus on understanding considerations around installation of VSM, and highlighting the functionality that is provided by the Datastores Manager component of the VSM plugin. Additional technical reports will cover the other feature of VSM.

Introduction

In today's Datacenters, customers are using VMware™ virtualization solutions and Dell™ EqualLogic™ PS Series SAN storage to consolidate servers and storage for better utilization, efficiency and ease of management. The encapsulation of a Virtual Machine (VM) into a set of files increases both the flexibility of data protection as well as the challenges of managing the protection of all these virtualized assets. VMware utilizes a snapshot technology within vCenter that can quiesce and help protect these VMs. Dell has combined the intelligence of native point-in-time PS Series SAN snapshots with these vCenter snapshots to provide a scalable and automated data protection package for the virtual environment.

The Dell Virtual Storage Manager v3.5 (VSM) is the next generation of VMware vCenter plug-ins that allows administrators to coordinate data protection and recovery within their virtual environment. The Dell VSM is a virtual appliance that is downloaded as part of the all-inclusive Dell EqualLogic software support and can be installed into an existing VMware vCenter environment. VSM contains many tools and capabilities that help VMware administrators gain better control and functionality over their EqualLogic environment including:

- Datastores Manager - a tool to provision, expand, delete and monitor EqualLogic Datastores across multiple EqualLogic groups.
- VSM Smart Copies and Replication - formerly known as Auto-Snapshot Manager/VMware, this tool allows the creation of hypervisor-consistent snapshots, clones and replicas for data protection and disaster recovery
- VDI Tool - a tool which coordinates SAN based thin cloning to provision space efficient virtual desktops within a VMware View environment
- Dell EqualLogic VASA Storage Provider - a set of tools that allow vCenter and the EqualLogic SAN to communicate for better storage awareness

Installation Considerations:

While the installation process for Virtual Storage Management v3.5 is straightforward, to insure a smooth installation, there are a few considerations that should be taken into account, and prerequisite that should be completed.

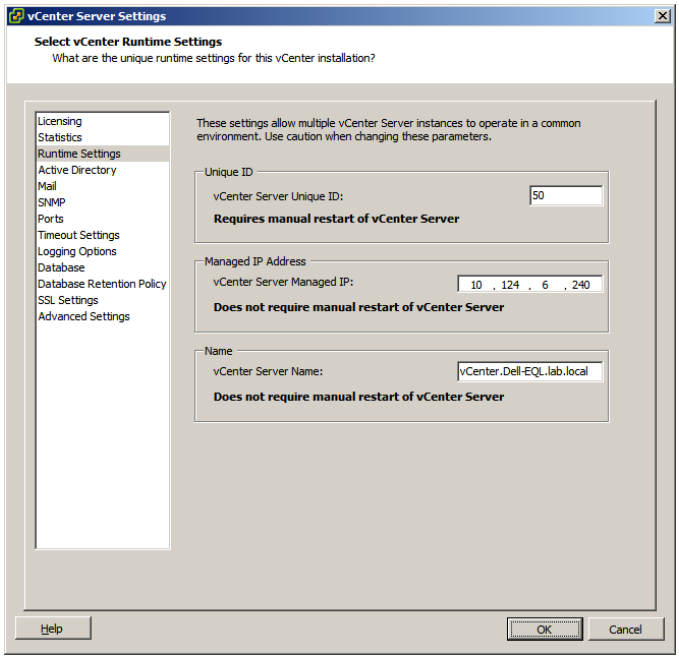
vCenter Server Managed IP requirement

The installation process for Virtual Storage Management v3.5 has been significantly streamlined over prior versions, with most of the configuration been done during the import of the VSM virtual appliance.

One of the settings that is populated automatically is the vCenter IP address. This is pulled from querying the vCenter into which the VSM virtual appliance is being installed, and is dependent upon the vCenter Server Managed IP address field being populated, as shown below.

To verify, or set the vCenter Server Managed IP:

1. From the vCenter client file menu, click on **Administration**, then **vCenter Server Settings**.
2. From vCenter Server Settings select **Runtime Settings**.
3. Verify or enter the vCenter Server's IP address in the **vCenter Server Managed IP** field.



4. Click **OK** to apply.

Protecting the VSM virtual appliance

Care should be exercised when selecting which datastore to host the virtual machine that is the Virtual Storage Management appliance. While VSM can be placed on a datastore that is being replicated or snapshotted by the array, it should *not* be placed on a datastore whose replication is being managed by VSM or that is being Smart Copied by VSM. This is because of the quiescing that is performed as part of these operations may disrupt the VSM while it is managing the replication or Smart Copy task.

As VSM is an integral part of a visualized environment data protection strategy, consideration needs to be given to protecting it. Use the vSphere High Availability feature to provide continued availability of VSM in the event of host failure. For more serious failures it may be necessary to re-install the VSM. The critical data that VSM contains exists in an internal database, of which a locally stored backup is automatically created daily. This database backup can be accessed via the VSM's CIFS share, \\<IP Address or Hostname>\ database\dbbackup.sql, and should be copied or backed up to another location. This database backup file, coupled with a newly installed instance of VSM, will quickly restore a corrupted or accidently deleted VSM to a working state as detailed below.

1. Install VSM following the instructions in **Installation** section of this technical report.
2. Browse to the VSM's CIFS share, \\<IP Address or Hostname>\ database\ and copy in the backup copy of the database. The backup filename must begin with dbbackup and have an extension of .sql.
3. Launch the VM console for the VSM virtual appliance and log into the VSM console.
4. From the menu select **Maintenance**, and then **Database Restore**.
5. The console will then display all of the database backups in the backup folder, select the appropriate backup and press enter. VSM will then begin the process of restoring the database backup.
   Note: Depending on the amount of data in the backup, it can take several minutes for the restore to complete.
6. Once the database restore operation is completed, the state of VSM will have been restored, include its knowledge and snapshots and replicas that it created on the EqualLogic array.

Connecting to the Storage Network

Virtual Storage Manager must communicate with vCenter and the EqualLogic PS Series array, and if using the VDI tool, also with the VMware View server. The default method for communicating with an EqualLogic PS Series array is the Group IP; however the Group IP exists on the iSCSI network, which is often kept isolated from the rest of the networking environment.

There are three options for enabling communications with the EqualLogic group:

1. Create an exception in the router isolating the iSCSI network to permit traffic from VSM to be passed.
2. In virtualized environment, there is frequently a need for guest OSes to directly access the storage. This is done to enable these guest OSes to use tools such as EqualLogic Auto Snapshot Manager for Windows and Linux to offer data protect to such applications as Exchange and SQL. In such cases the design of the virtualized environment's virtualized networking will include a VM network with access to the iSCSI network.
3. Enablement of the dedicated EqualLogic management network. This enables access to the EqualLogic's array management functions, but maintains the preferred isolation of the iSCSI network. For details on enabling the management network see the **About Dedicated Management Networks** section of the firmware's **Group Manager Administrator's Manual**.

Note: Option 1 does not require a second NIC in the VSM. Option 2 does require a second NIC in the VSM. Option 3 may require a second NIC in the VSM depending on upon the environments network configuration.

See the section titled **Adding a second NIC to the VSM** in the **Post-install Configuration** section.

Installation

The Dell EqualLogic Virtual Storage Manager v3.5 is delivered as a virtual appliance packaged in an OVA (Open Virtual Machine Format - Archive). The installation process is similar to that of other virtual appliances, with administrator entering typical information such as Name and Location; several additional properties are also requested that simplify and minimize the post-install configuration of VSM.

During the installation process a number of key pieces of information are required. The table below lists these:

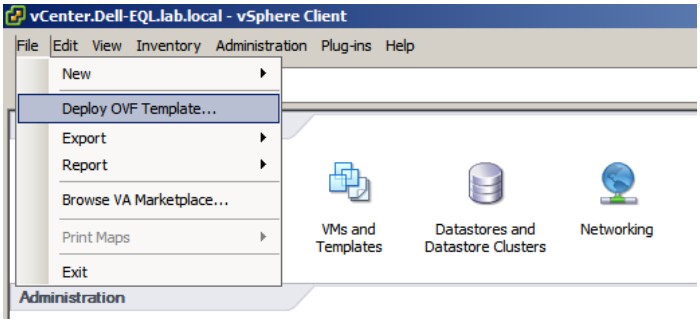
Option	**Description**	**Value**
Name	Name for the VSM virtual appliance as it is to appear in the vCenter inventory.	
Inventory location	Specifies the datacenter within vCenter that the VSM virtual appliance will reside, and optionally an inventory folder[1].	
Cluster or Host[1]	Specifies the cluster and depending upon the cluster's DRS setting, the specific host, that the VSM virtual appliance will be deployed.	
Resource Pool[1]	Specifies, if utilized, the cluster's resource pool that VSM virtual appliance should consume CPU and memory resource from.	
Datastore	Location where the virtual appliances files will reside. Optionally a VM Storage Profile[1] can be assigned at this point.	
Disk Format	A virtual machine's disk, or VMDK, can be of one of three types: Thick Provisioned Lazy Zero, Thick Provisioned Eager Zeroed, or Thin Provisioned. While a thick provisioned format is recommended, it is not required.	

Network Mapping	The VM network to connect the VSM's network interface to.	
Host Name	The network name by which the VSM virtual appliance is to be known by.	
Time Zone	The time zone of the environment in which the VSM virtual appliance is located.	
NTP Servers	Comma-separated list of NTP servers that can be synched with.	
vCenter username	The username of the account with which VSM will communicate with vCenter.	
vCenter password	Password for the above user account.	
Default gateway	The default gateway used for network access.	
DNS	Comma-separated list of DNS servers used to resolve hostnames.	
IP address	The IP address to be used by the VSM virtual appliance network interface.	
Netmask	The network mask to be used by the VSM virtual appliance network interface.	

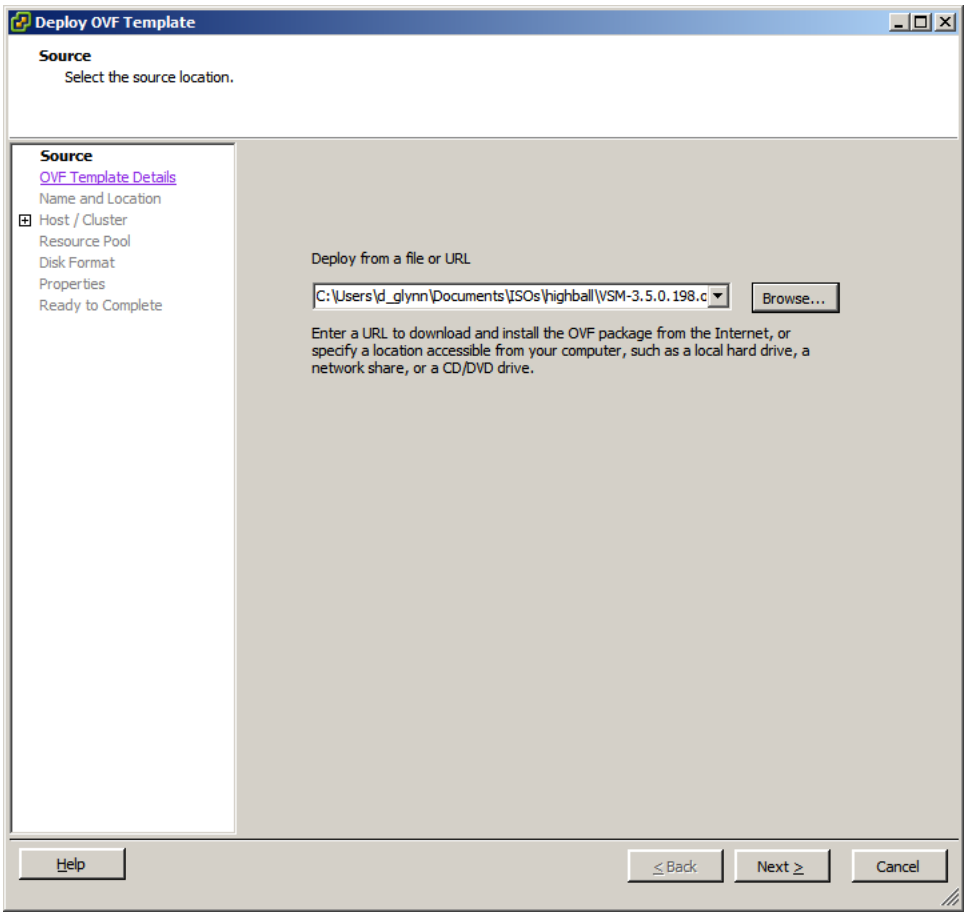
[1]Depending upon the configuration of the environment, these settings may not be required, or may not require user input.

Installation Process

1. From the vSphere Client file menu select **File**, and then **Deploy OVF Template**.

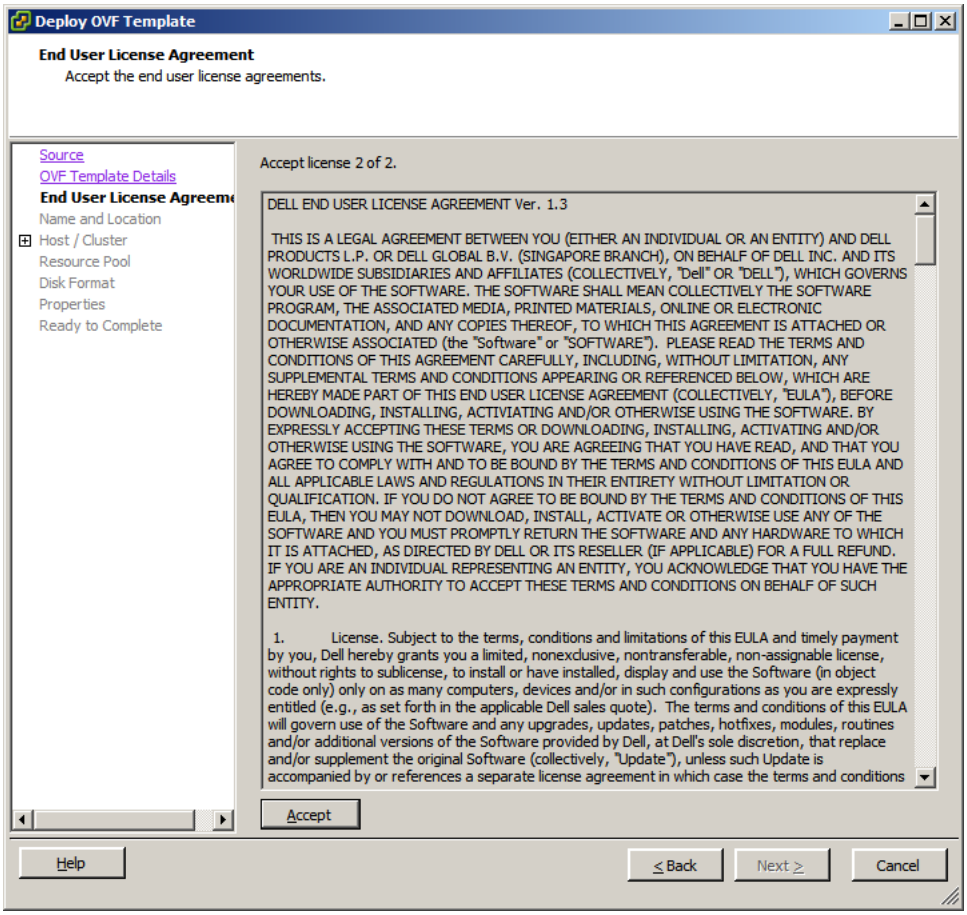


2. Click on the Browse button, and using the Windows Explorer window browse to the location when the OVA was downloaded or copied to. Select the VSM OVA file and click **Open**. With the VSM OVA selected, click **Next** to continue.

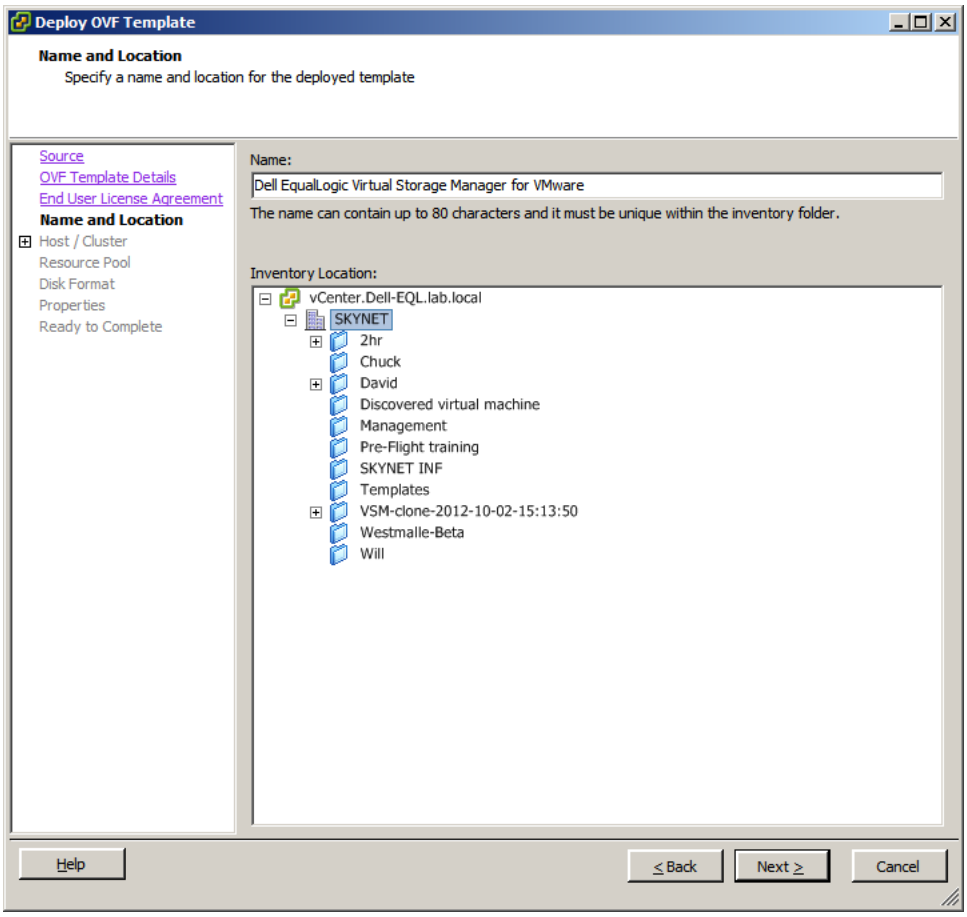


3. The OVF Template Details page displays additional information of the VSM virtual appliance. Click **Next** to continue.
4. The End User License Agreement, or EULA, is two pages long, with the first pages been utilized to remind administrators of the requirement to have the vCenter Server Managed IP field populated in vCenter Server Settings. Click **Accept** to continue.

   The second EULA page contains the End User License Agreement for the Dell EqualLogic Virtual Storage Manager. Click **Accept** to continue.

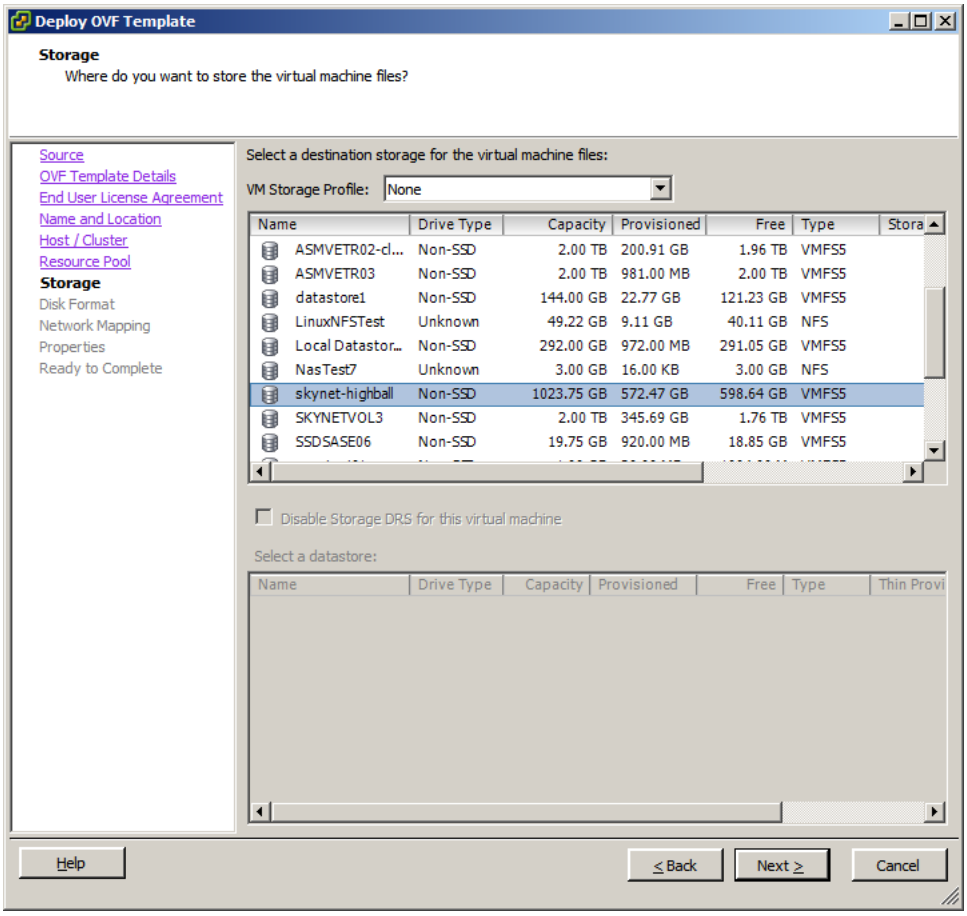


5. Specify a name for the VSM virtual appliance; this is the vCenter display name, and not the network hostname. Also specify the inventory location, which datacenter and which inventory folder, for the VSM virtual appliance.



6. Select the Cluster that the VSM virtual appliance will be located in. Depending upon the cluster's DRS setting it may be necessary to select an individual host.
7. Also depending upon the cluster's settings, there may be the opportunity to select a **Resource Pool** for the VSM virtual appliance. Select the resource pool and click **Next** to continue.

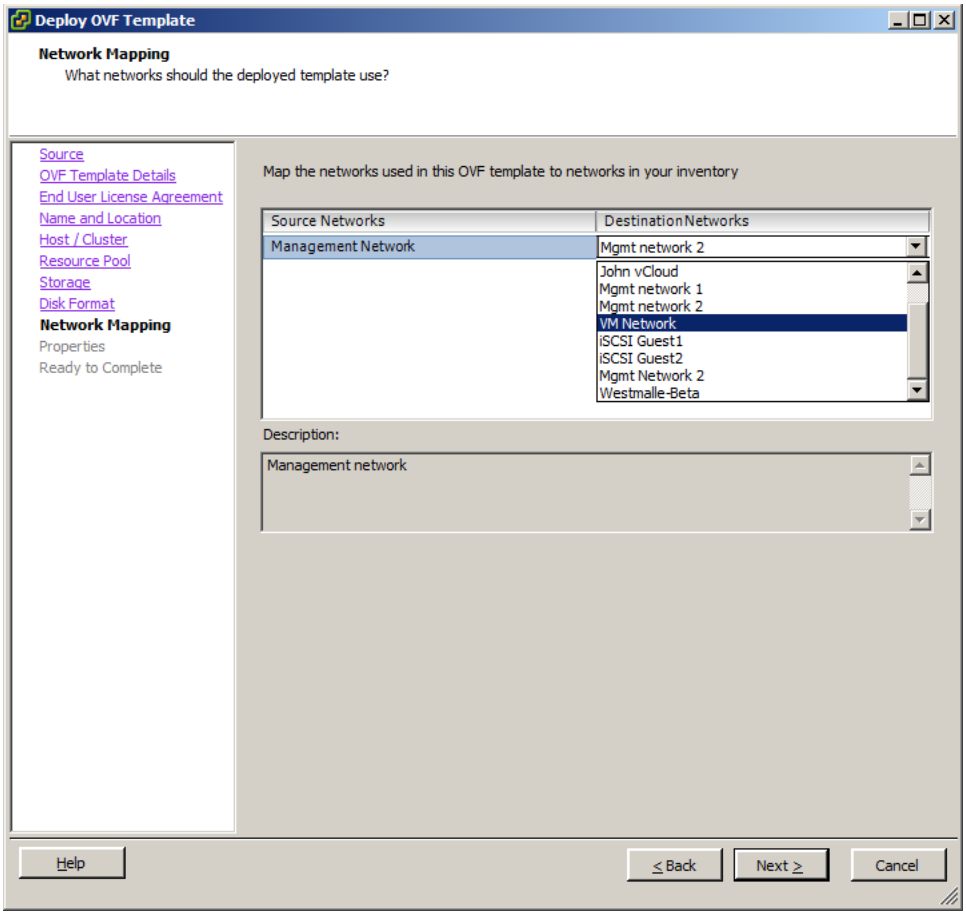
8. Select a suitable datastore where the VSM files will be located. Refer to **Datastore considerations and protecting the VSM virtual appliance** for considerations that should be taken into account when selecting a suitable datastore.



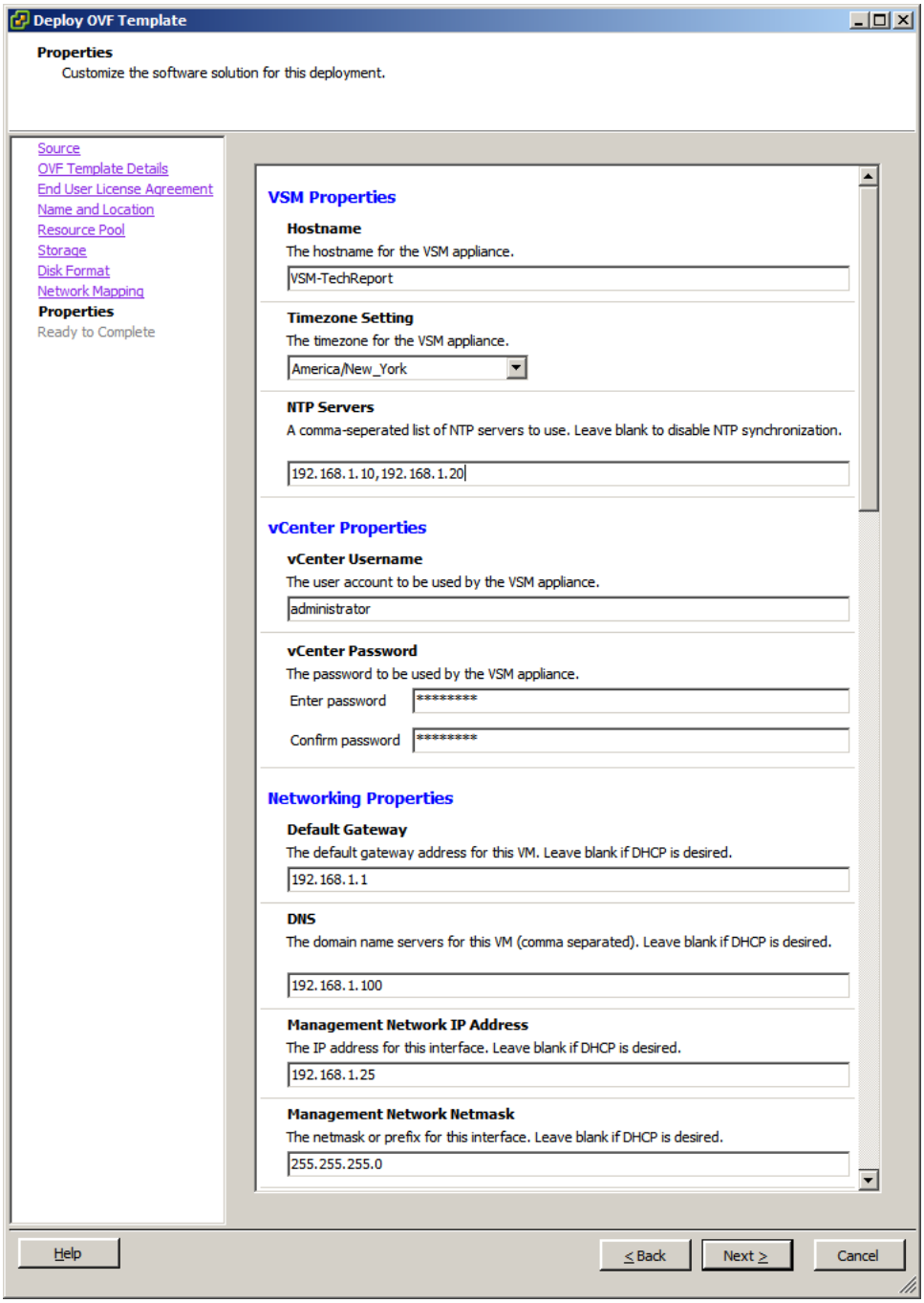
Depending upon the environment, business needs, and license availability, there may be an option to assign a **VM Storage Profile** to the virtual appliance. Click the drop down and select the appropriate Storage Profile. Click **Next** to continue.

9. Select the Disk Format. Best practice is to choose a disk format of type **Thick** be selected in all but test & development environments, however, all formats are supported in production environments. Click **Next** to continue.

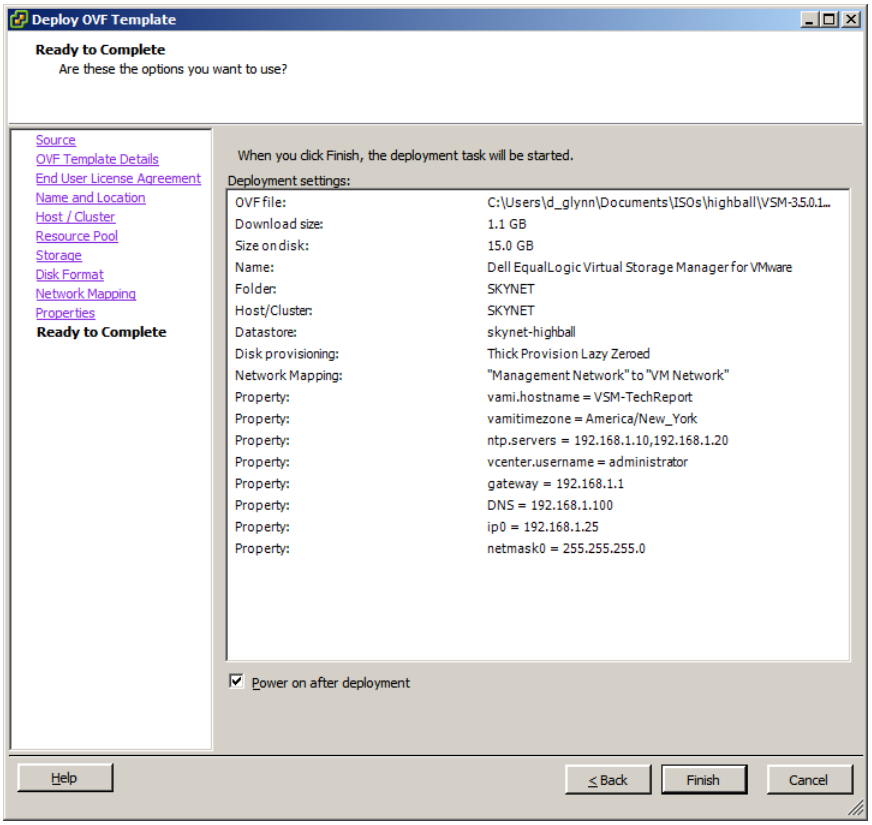
10. Select the appropriate **VM network** for the VSM virtual appliance to connect to. If the network in the environment is configured so that the EqualLogic array is isolated from this VM network, a second network interface can be added later. See the section **Adding a second NIC to the VSM** for more details. Click **Next** to continue.



11. On this page most of the settings that VSM will require are configured. Refer to the **Table XX** for an explanation of each of the individual fields. Complete the ones that are necessary for this environment and click **Next** to continue.

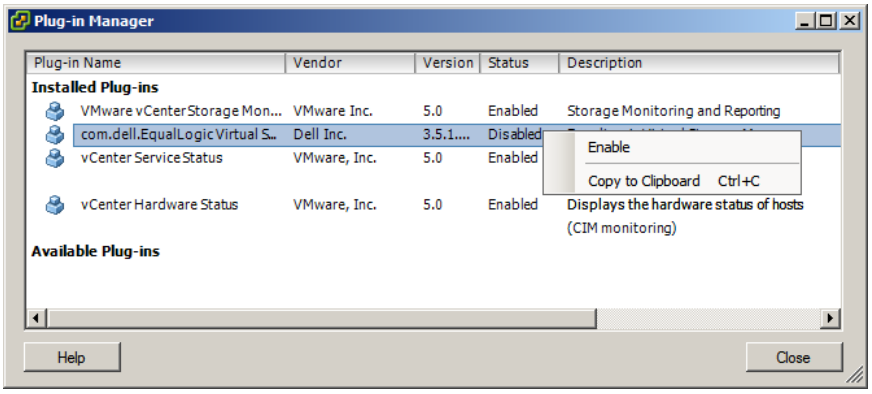


12. This final page will display a summary of the settings chosen though the OVF/OVA import process. Check the **Power on after deployment** checkbox to have the virtual appliance power up once the import process is complete. Click **Finish** to start the import process.



13. The import process will take several minutes to complete, depending upon the network connection speed. Once the import is complete the VSM virtual appliance will power on. The first boot of the VSM virtual appliance takes several minutes as it completes a number of first boot tasks, and registers with vCenter.

14. Once this has been completed the plugin can be enabled by selecting **Plug-ins** from the vSphere Client file menu, click **Manage Plug-ins**, and then right click on the EqualLogic Virtual Storage Manage entry and select **Enable** from the context menu.



Post-install Configuration

The above process of importing the VSM virtual appliance into vCenter requests the majority of the configuration information; however, the VASA Provider cannot be configured as part of the import process. It is also recommended that the VSM password be changed from the default. The steps for both of these tasks are covered below.

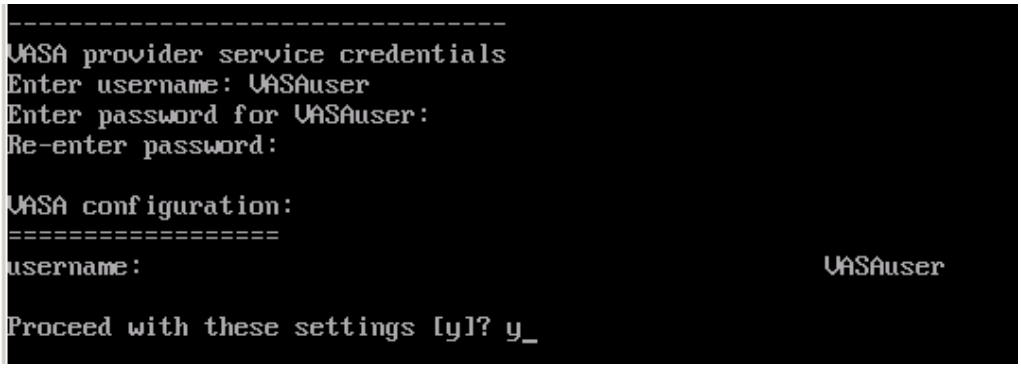
In some environment a second NIC may be required in order to communicate with the EqualLogic array, this is also detailed below.

Configuring the VASA Provider

1. From the vSphere client right click on the VSM and select **Open Console** from the context menu.
2. Log into the VSM console using the default credentials: username: **root** and password: **eql**.
3. From the **Setup** menu enter **1** to select **Configuration**.
4. From the **Configuration** menu enter **3** to select **Configure VASA**.
5. Provide a **username** for the credentials of the account to be created for the vCenter VASA Service and the EqualLogic VASA Provider to communicate with, than press **Enter**.

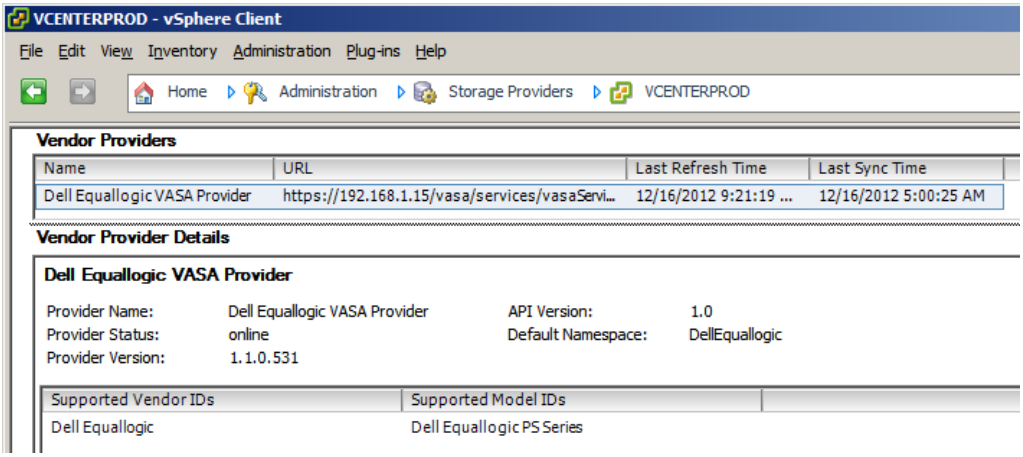
   Note: This is not the same account as used by VSM for communication with vCenter, but rather a unique set of credentials to be created for use by the vCenter VASA Service and EqualLogic VASA Provider to communicate.

6. Then enter a **password** for this account, press **Enter**, and then re-enter the password for verification.

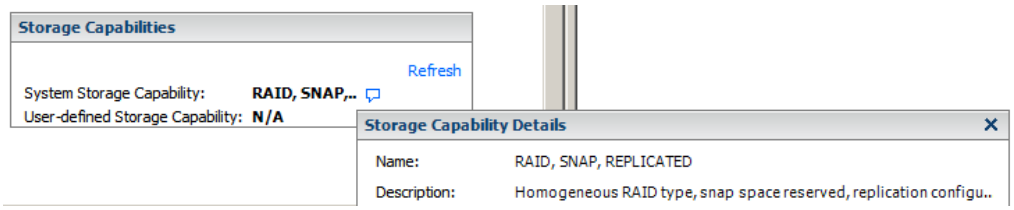


Enter **y** to proceed with these settings.

7. The VSM VASA provider will then communicate with the VASA service on the vCenter server, and the VASA service will register with the EqualLogic VASA Provider on the VSM. This process will take approximately 2 minutes. Once complete the EqualLogic VASA Provider will be listed under **Storage Providers.**



8. The vCenter Client will display a datastore's **Storage Capability** information.



Changing the root account password

It is strongly recommended to change the root password from the default. To do so follow the following steps:

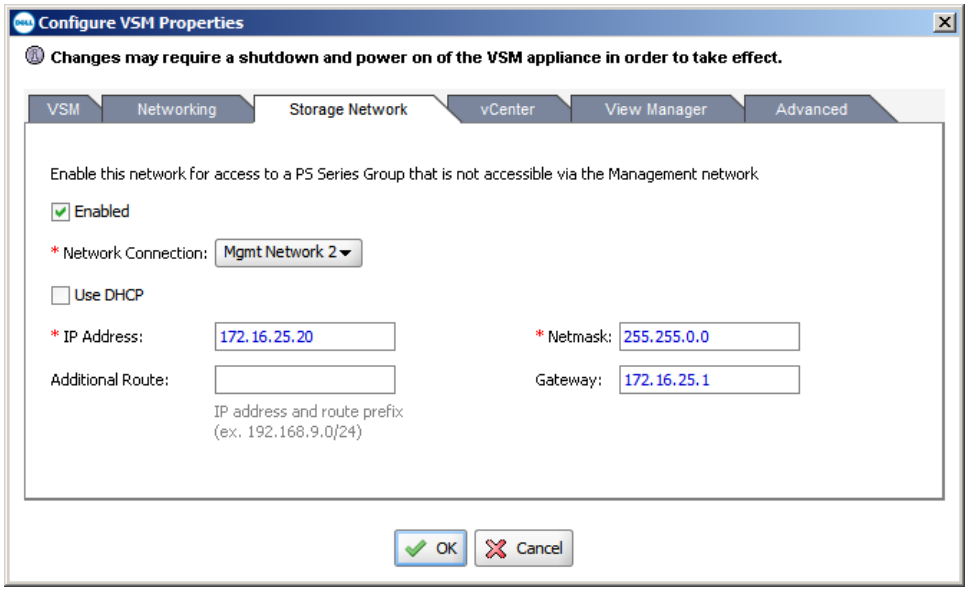
1. From the **Configuration** menu enter **4** to select **Change root password**.
2. At the prompt enter the new password, and then press **Enter.**
3. Re-enter the password to verify, and then press **Enter.**
4. The password will now be changed, press **Enter** to return to the main setup menu.

Adding a second NIC to the VSM

In the majority of environments a second NIC is not necessary; however, in some cases an additional NIC is necessary due to the subnet layout or security requirements. The steps for adding this second NIC using the vSphere client are covered below.

1. Complete the install process of the VSM as described in the **Install Guide** as normal.
2. From the vCenter client click **Home** and in the **Solutions and Applications** section click on **Dell EqualLogic Virtual Storage Manager**.
3. Click on the **VSM Properties** icon in the toolbar. Image?

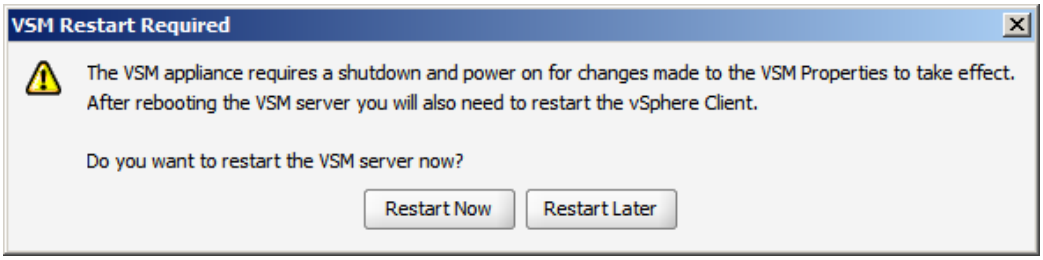
4. Click on the **Storage Network** tab, and populate the following fields:
    a. Check the **Enabled** checkbox.
    b. From the **Network Connection** dropdown menu, select the appropriate VM Network for communicating with the EqualLogic array.
    c. If using DHCP check the **Use DHCP** checkbox, otherwise, enter in the static **IP Address** and appropriate **Netmask**.



Note: Depending on how the network is configured, some environments may require the use of an **Additional Route** or a **Gateway** IP address.

Click **OK** to continue.

5. VSM will then start the process of reconfiguring the virtual appliance. Once this is complete a reboot is required before the new NIC can be used. Click **Restart Now** to continue.



6. Once the reboot is completed VSM will be able to communicate with the EqualLogic arrays on the newly added network.

Virtual Storage Manager Overview

This section will discuss the features that are provided by the Datastores Manager part of Virtual Storage Manager, as well as the EqualLogic VASA Provider. For information on protecting your virtual environment with Smart Copies or Replication see *TR1076 Virtual Machine Protection with Dell EqualLogic Virtual Storage Manager v3.5.*

Datastores Manager Overview

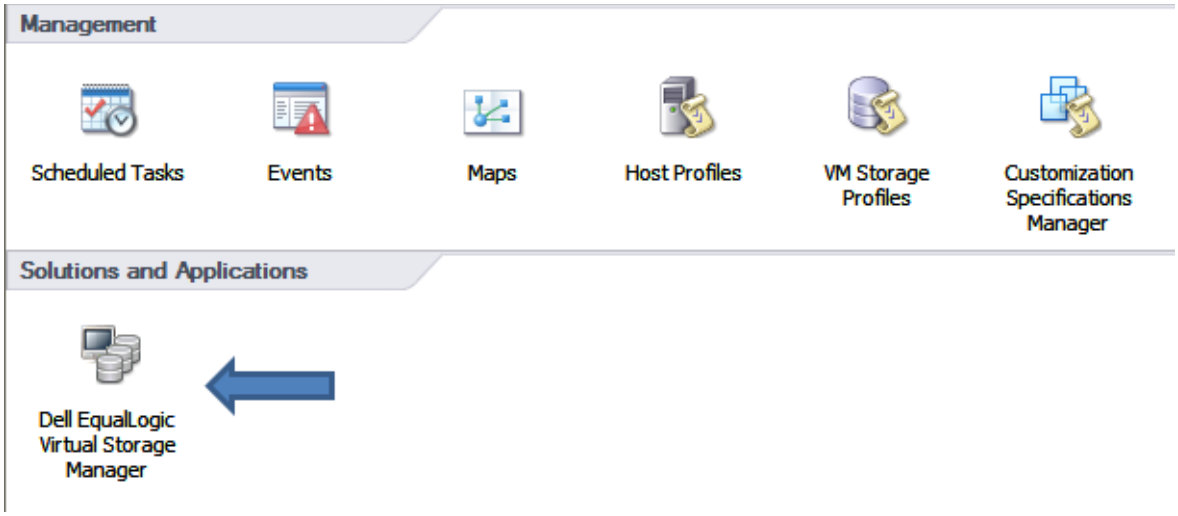
The Datastores Manager feature in VSM enables a central point from where vCenter administrators can get a single graphical and informational overview of the status of their EqualLogic-backed datastores. They can quickly ascertain the amount of free space available, the percentage of snapshot space being consumed, and the status of replications, along with several other metrics, as shown in the screenshot below. This enables vCenter administrators to verify that state of their EqualLogic-backed datastores, and quickly return to other duties.

From the VSM Datastores Manager interface the following tasks can also be performed to further ease the vCenter administrators' workload:

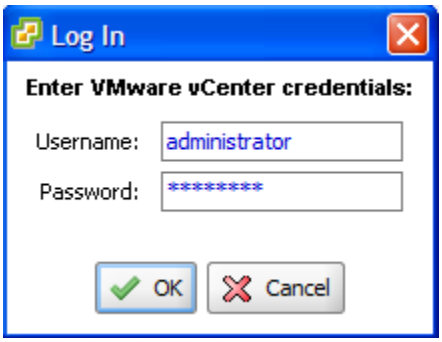
- Create a datastore or multiple datastores
- Increase the size of an on existing datastore
- Delete a no longer used datastore
- Create an ACL policy, either from an existing datastore, or from scratch
- Change the ACL policy assigned to a datastore volume
- Create a Smart Copy of a datastore
- Configure a datastore for replication
- Configure a schedule for the regular creation of Smart Copies or Replicas
- Enable Synchronous Replication for a datastore

Launching VSM

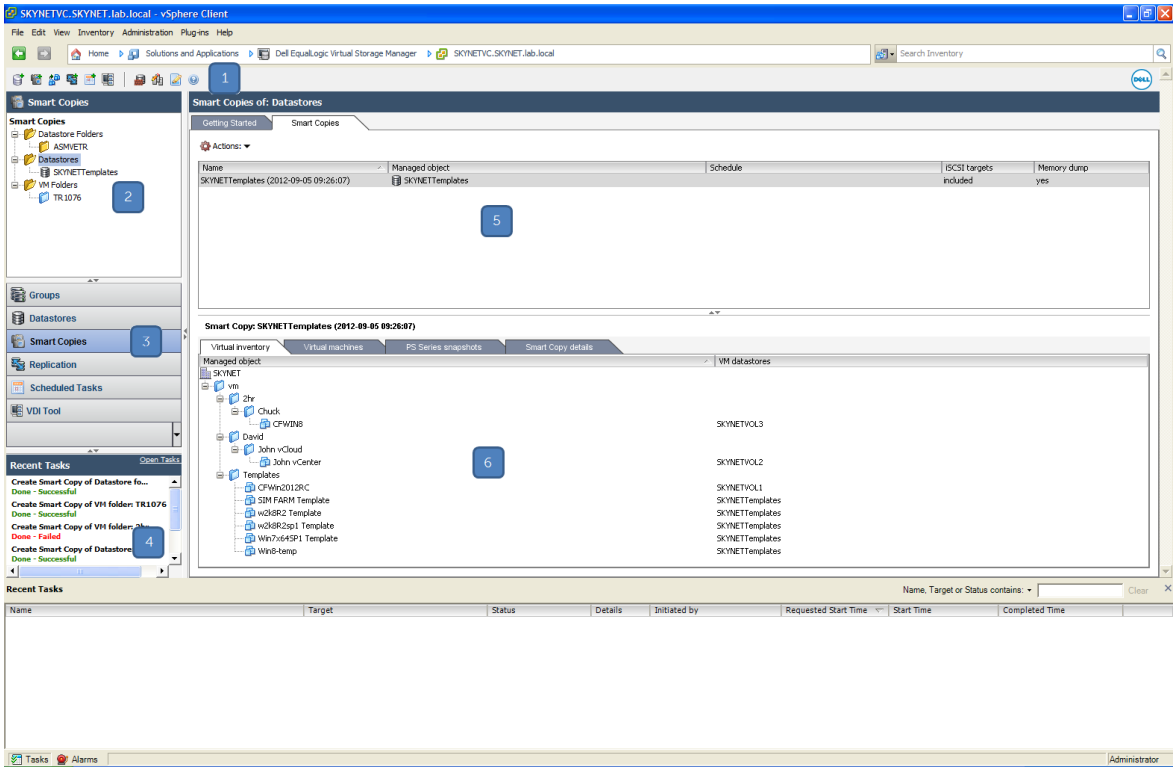
Once the VSM appliance is installed and running in the environment there will be a new icon under the Solutions and Applications area from the **Home** screen in the vCenter Client.



This will launch a login dialog box. Log into VSM with credentials that have vCenter administrative access privileges.



Once logged into the VSM the main landing page is presented. From this screen all of the tools and features within VSM can be accessed.



1 List of commonly used toolbar shortcut icons.
2 Main object pane for the particular VSM tool currently in use.
3 Tool buttons to launch any of the management tools inside VSM. These can be minimized to small icon buttons.
4 The VSM Recent Tasks pane.
5 This information pane area will show more information about the individual object selected in the object pane, 2, including a Getting Started tab with common functions and a more detailed tab showing context aware information for the selected object.
6 More detailed information based on the selection highlighted inside the information pane, 5.

Connecting to EqualLogic storage

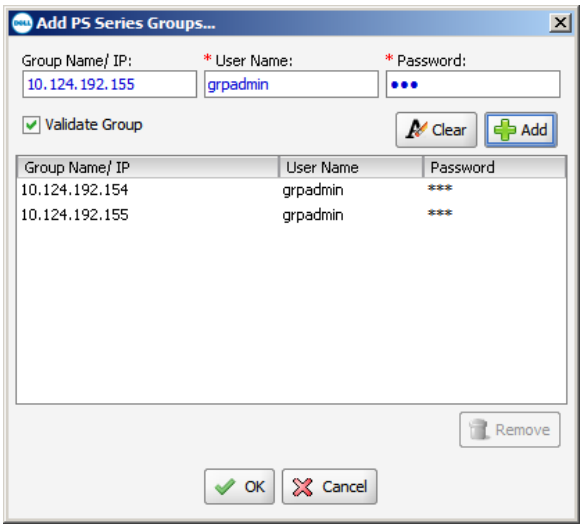
Once the installation and configuration of VSM is completed, it needs to be connected to the EqualLogic storage supporting the virtualized environment.

VSM v3.5 supports managing multiple EqualLogic groups. This capability enables additional capabilities such as:

- End to end management of SAN based replication
- Storage Recovery Replica
- Low cost disaster recovery

The steps for connecting to an EqualLogic group or multiple groups are covered below.

1. From the main object pane select **Groups.**
2. From the Groups **Getting Started** tab click on **Add PS Series Groups.**
3. In the Add PS Series Group wizard enter in the EqualLogic group's Group Name or IP, and a username and password with group administrator privileges. Click **Add** to continue.



4. Repeat step 3 for each Group that is to be managed from this VSM, then click **OK** to continue.
5. VSM will connect and log into each of the groups, and begin to populate VSM with information about the groups.

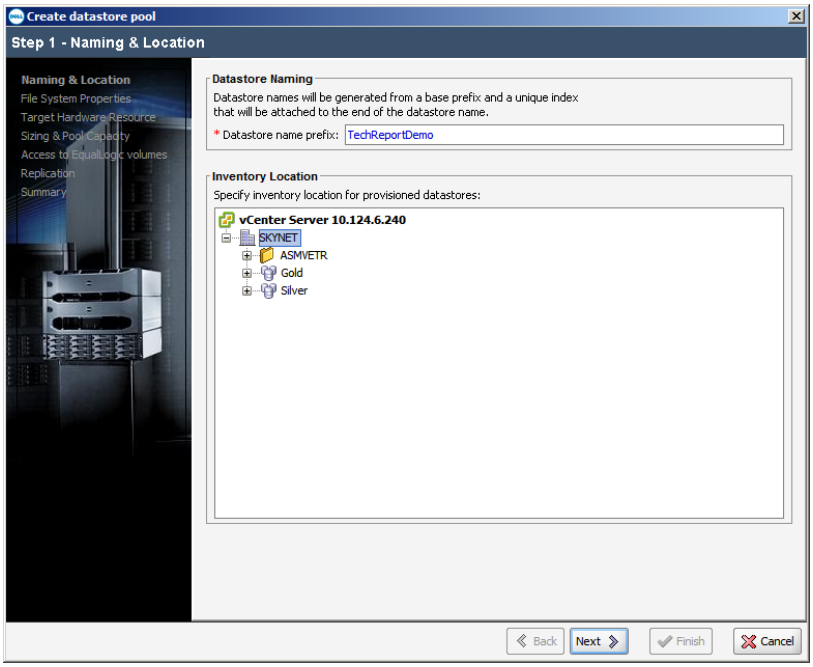
VSM can now be used to manage these EqualLogic groups, enabling the creation of datastores, and the protection of virtual machines through SmartCopy Snapshots and SmartCopy Replication.

Create a datastore or multiple datastores

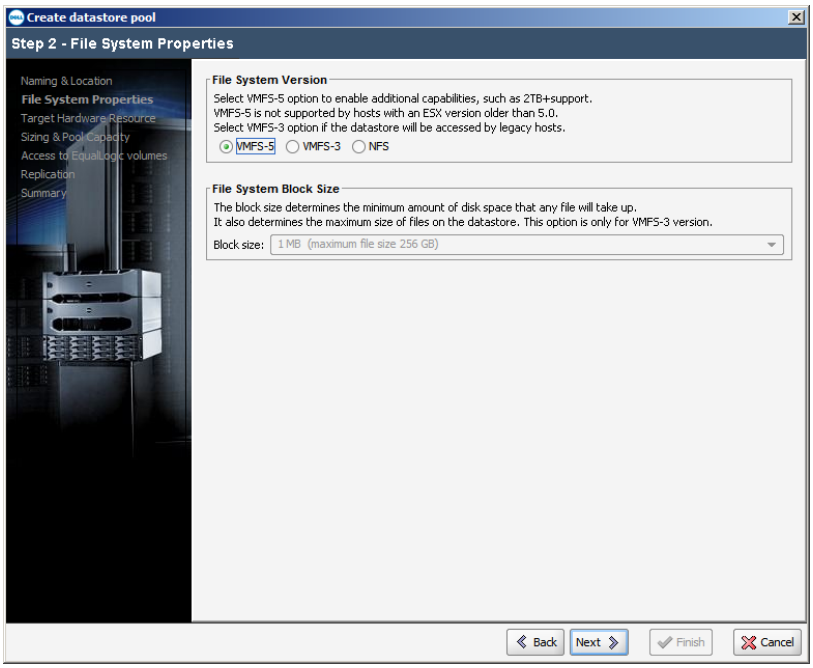
Creating a new datastore and its associated volume can be initiated either from the **Host and Clusters** view by right clicking on a particular cluster or host in the datacenter, or by clicking on the **Create Datastores** icon in VSM. Right clicking on a particular cluster or host skips the **Target Hardware Resource** step in the wizard.

1. From the EqualLogic VSM screen, click on the **Create Datastore** icon.
2. In step 1 of the wizard, enter the datastore prefix to be used, and select the inventory location in which to place the datastores. It is only necessary to select the datacenter, but there is the option to add the datastore to an existing datastore folder or datastore cluster if desired.

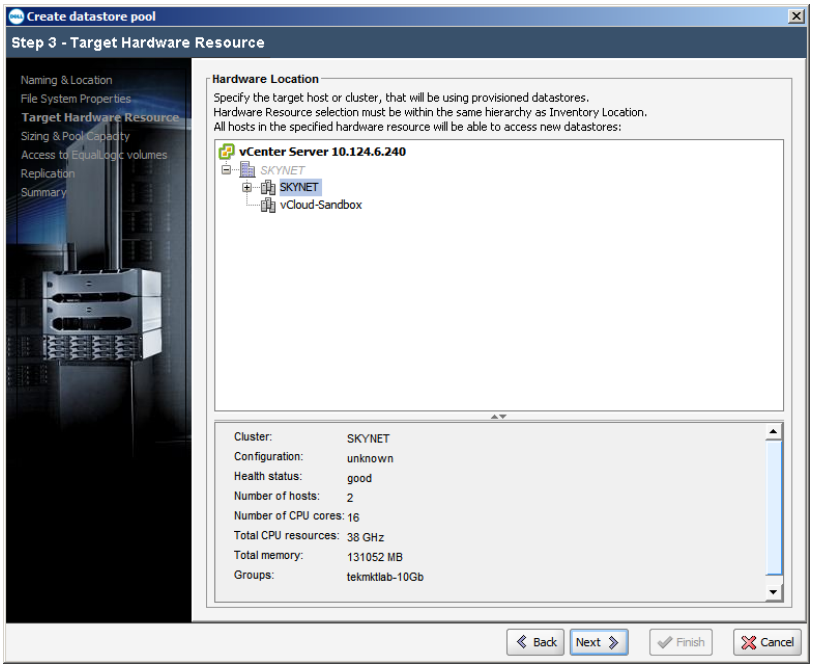
   Note: When creating multiple datastores the datastore prefix will be suffixed with a two digit number starting at 01. If a volume of that name already exists, the next higher number will be used.



3. In step 2, select the File System to be used; VMFS-3, VMFS-5 or NFS. If VMFS-3 is select, the option to select the File System Block Size will be presented.



4. In step 3, select the cluster or individual host the datastore is to be associated with.

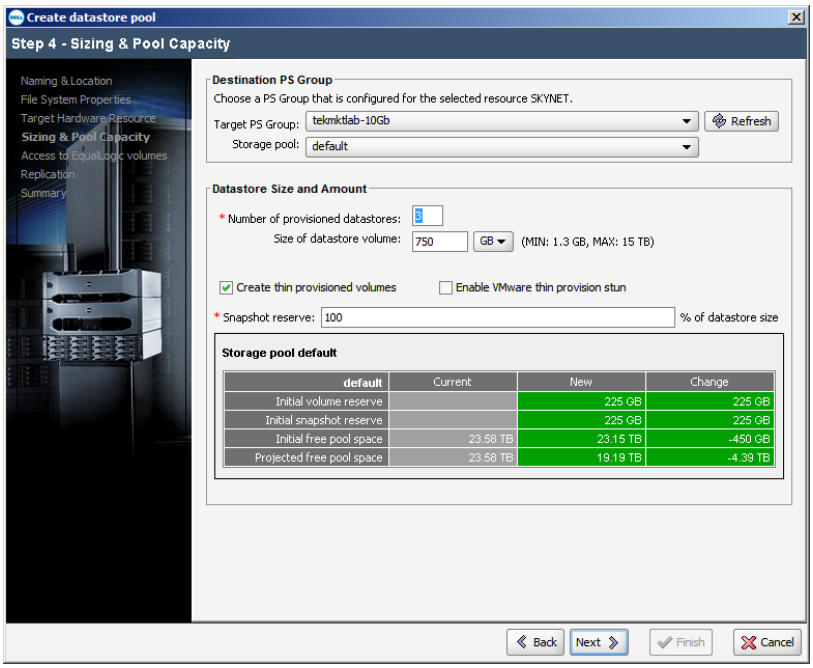


5. In step 4, select from the dropdowns into which EqualLogic PS Series group and pool the volume(s) should be created.
   Enter the number of datastores to be created as well as their size. With vSphere 5.0 datastores greater that 2TB can be created, without the use of extents. **Note:** The maximum EqualLogic volume size is 15TB.

   Select if the datastores are to be thin provisioned, and if so, whether the VMware VAAI primitive Thin Provision Stun is to be enabled. For more information on VMware Thin Provision Stun see EqualLogic technical report *TR1066: Advanced Storage Features in VMware vSphere*.

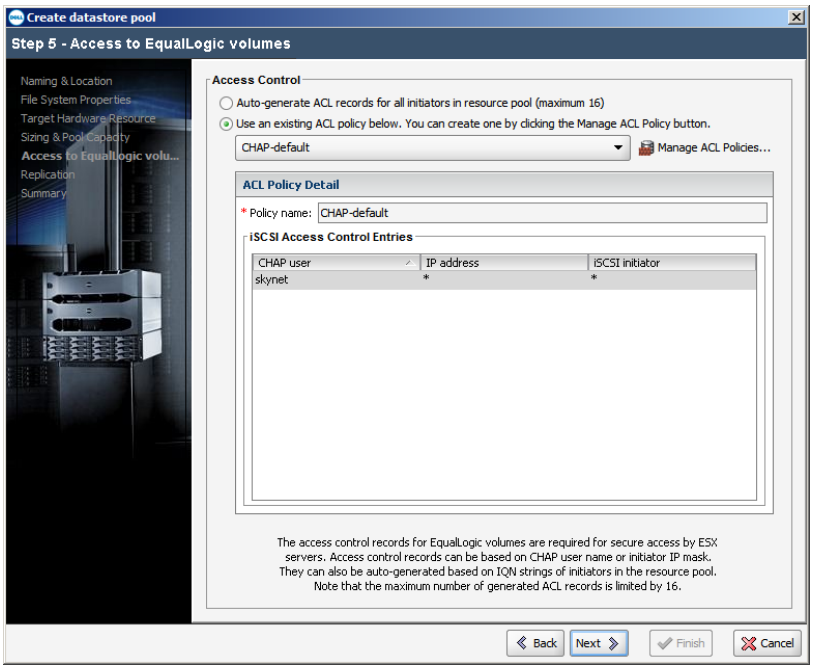
   Finally, select the size of the snap reserve space. This is additional space that is reserved from the free pool space for the storage of volume snapshots. By default it is set at a conservative 100%, but can easily be re-sized at a later point in time if a different amount of reserve space is required to store the desired number of snapshots.

   The table at the bottom of this wizard step will reflect the changes in space consumption the new datastores will require in the selected pool.

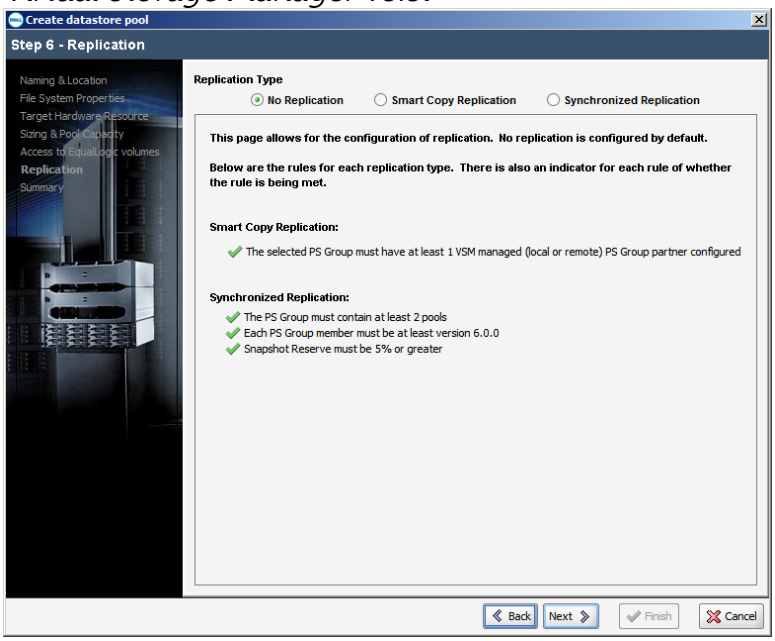


6. In step 5 the Access Control List (ACL) for the datastore volume is set. The ACL is what is used to control which initiators can access the datastore volume. There are two options here for assigning the ACL: the first option is to have VSM auto-generate the ACL using the iSCSI IQN for all the initiators selected in Step 3 of the wizard. However, as an EqualLogic ACL list is limited to 16 entries, this may not be sufficient in some environments. The second option is to use the ACL Policy Manager. ACL access policies can be defined and saved in the ACL Policy Manager for future use, thereby reducing the opportunity for error when assigning the ACL.

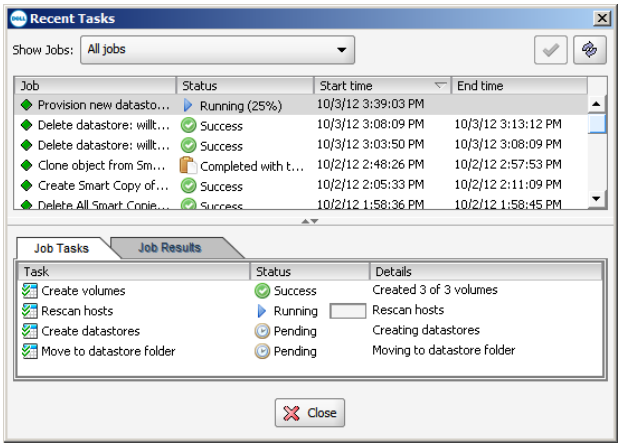
   For more information on the ACL Policy Manager see the section **Creating an ACL policy**.



7. Step 6 provides the opportunity to configure replication based data protection for the datastore. This topic is covered in detail in EqualLogic technical report TR1076 *Virtual Machine Protection with Dell EqualLogic Virtual Storage Manager v3.5*.



8. Step 7 is the final step in the Create Datastore wizard, and it displays a summary of the options chosen. Click **Finish** to initiate the task for VSM to create the datastores and the volumes backing the datastores.
9. The status of the create datastore task can be observed in the VSM **Recent Tasks** pane in the lower left corner of the vSphere client. For more details on the task status clock on the **Open Tasks** button.



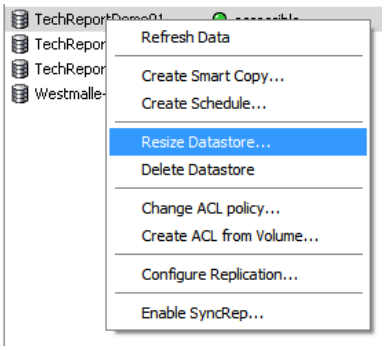
10. Once the task is completed the datastores will be displayed in the VSM Datastore pane, and available for use within the vSphere environment.

Increase the size of a datastore

Virtual environments are in continuous flux, reflecting the ever-changing demands of the businesses they support. What is expected from storage often shifts from day to day, and the EqualLogic PS Series array architecture is designed to continuously balance the workload among several arrays. For more information on the EqualLogic load balancers see *TR1070: EqualLogic PS Series Architecture: Load Balancers*.

Performance is not the only storage requirement that shifts over time; often the capacity requirements of a datastore can change over time as well. VSM enables the task of increasing the size of a datastore to be completed in a minimal number of steps.

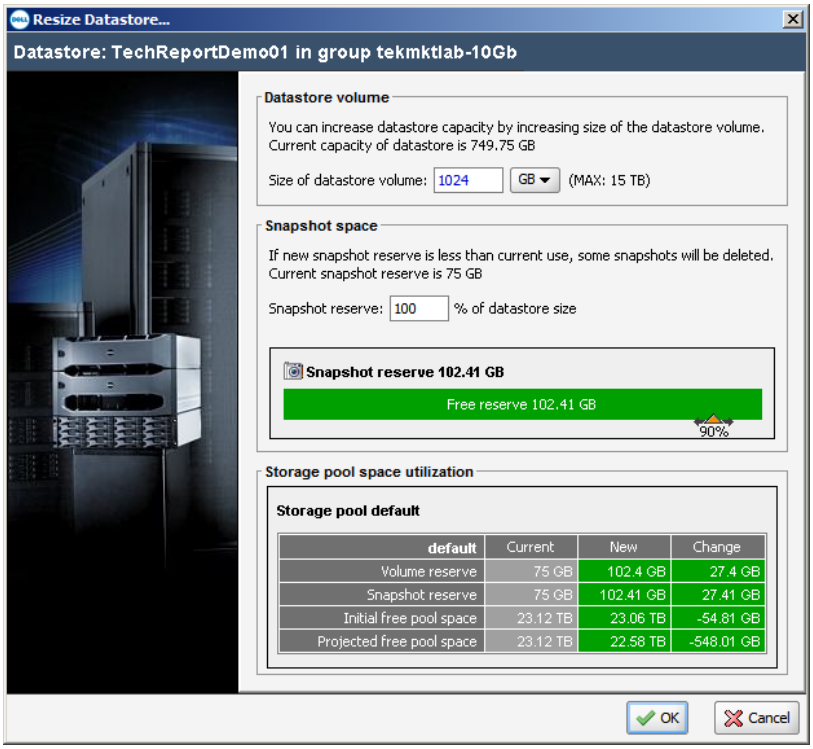
1. From the VSM datastore screen, right click on the datastore to be resized and select **Resize Datastore** form the context menu.



2. Change the size of the datastore volume to the desired new size. Optionally, the datastore's volume snapshot reserve percentage can also be altered at this stage.

   Click **Ok**, to start the resize task.

   Note: It is only possible to increase the size of a datastore.



3. At this stage a warning message dialog box will be displayed. It is recommended that prior to performing a resize operation that a Smart Copy of the datastore be created. This enable returning to the original datastore size in the future if the wrong datastore was selected, or should anything negative occur during the operation.

   To create the Smart Copy click **Yes** once the Smart Copy has been completed, run the Resize Datastore wizard again. To continue with the Resize Datastore operation click **No**.

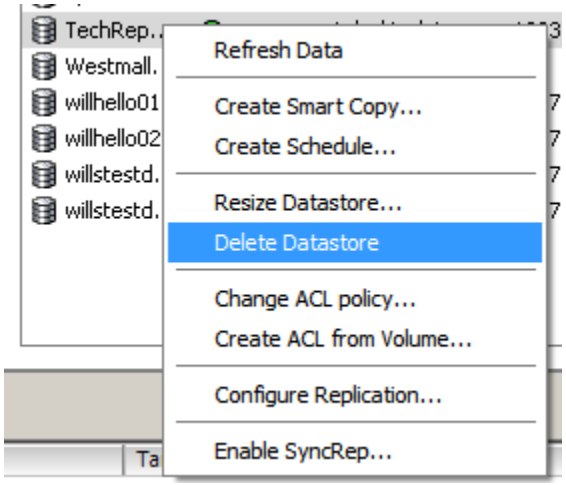
4. VSM will then complete the task of increasing the size of the volume on the array, and increasing the VMFS partition on the volume, resulting in additional capacity being available on that datastore.

Deleting a datastore

Occasionally, datastores need to be deleted from the virtual infrastructure. Typically this involves a number of steps in vCenter, followed by some steps on the array. VSM reduces this to just a few clicks from within vCenter.

1. From the VSM datastore screen, right click on the datastore to be deleted and select **Delete Datastore** from the context menu.

   If there are any virtual machines registered on that volume, the option to delete the datastore will be grayed out, and unavailable.



2. A verification dialogue is displayed next, with the reminder that the deletion of the datastores volume will also cause the deletion of any Smart Copies or Smart Replicas that were based on this datastore.

   Check the **Destroy xxGB of data?** check box and click **Yes** to start the task.

3. VSM will perform all the necessary tasks within vCenter to unmount the datastore from all hosts which access it, log the iSCSI initiators out, and then delete the datastore volume from the EqualLogic array.

Creating an ACL policy

Access to iSCSI volumes is restricted through the use of an Access Control List or ACL for short. An ACL record entry consists of a CHAP user, an IP address, or an iSCSI initiator's IQN string. Depending on the ACL type chosen, the configuration of the environment and the number of hosts accessing the volume, more than one ACL record maybe required.

Creating an ACL Policy in VSM ensures a reduction in ACL configuration when new datastore volumes are created, as all that is required to set the ACL on a new datastore volume, or change it on an existing datastore volume, is to select the appropriate ACL from a drop down list.

Explanation of different ACL types:

CHAP user name: CHAP authentication, which uses a CHAP account on the array or on a RADIUS server, can provide an administrator flexible yet secure means of restricting access to a volume. One CHAP ACL record entry can be used to permit all the hosts in a vSphere cluster access to a volume, by configuring each host with the same CHAP account. When additional hosts are added to the cluster, it is only necessary to configure CHAP on the initiator; no changes need to be made on the array or volume to grant access.

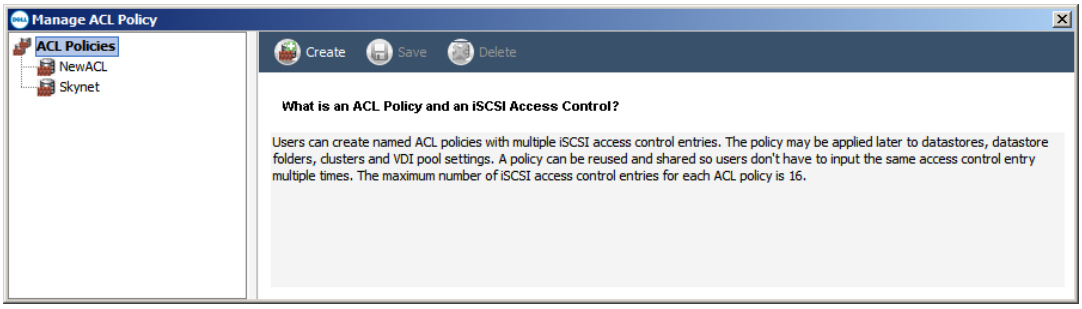
IP address: When using IP address ACL records it is necessary to create an entry for each VMkernel Port that is bound to the software iSCSI initiator or for each iSCSI HBA in the hosts that require access to that volume. While it is possible to configure an IP address with wild cards, eg 192.168.10.*, this practice is strongly discouraged as it is not secure, as any initiator routed to that subnet can access the volume, including non-ESXi initiators.

iSCSI initiator name: When using the iSCSI initiator name (IQN), it is necessary to create an entry for each initiator in each of the hosts that requires access to that volume. For hosts where dependent or independent HBAs are used, multiple ACL records will be required as each HBA in the host will have its own unique IQN.

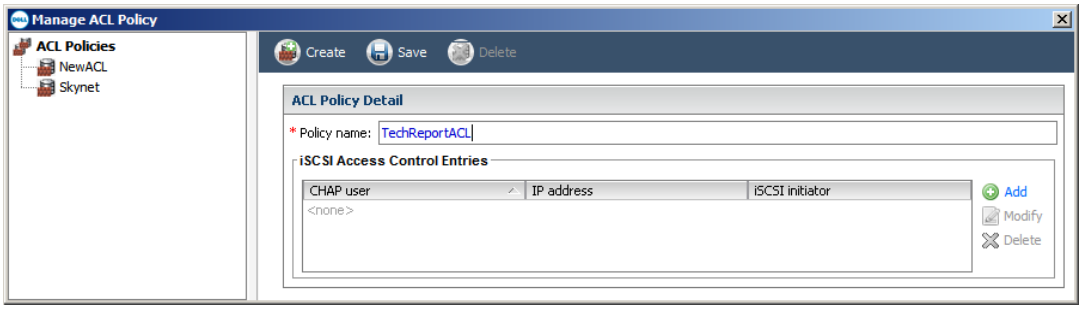
Note: Only 16 ACL records can be create on any individual volume. Future growth of the vSphere cluster should be considered when selecting an ACL Policy.

Creating a new ACL policy

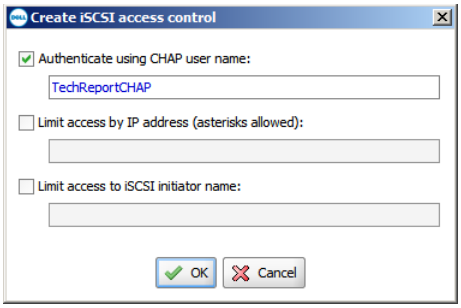
1. Click on the **Manage ACL Policy** button in the VSM toolbar.
2. Click on the **Create** button.



3. Provide a suitable name for the new ACL Policy, and then click **Add**.

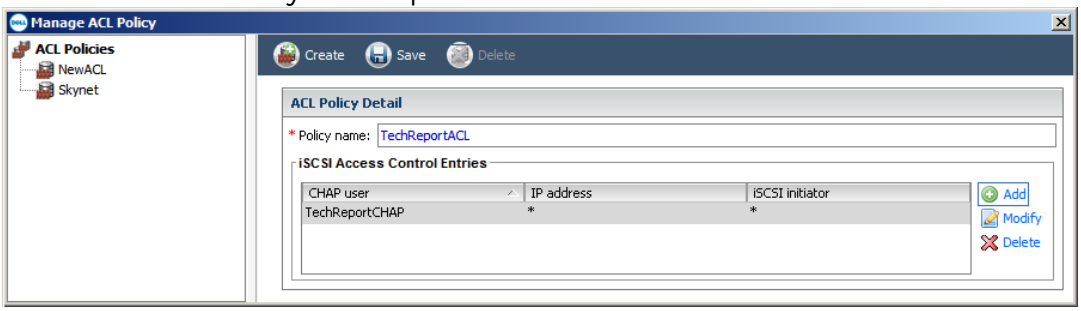


4. Enter the appropriate ACL record, and click **OK**.



5. If the ACL Policy requires multiple ACL records, click Add again and repeat steps 3 and 4, until the policy has all the ACL records required. Remember, if using IP address ACLs to include the IP address of each VMkernel Ports on each host, or if using IQN ACLs to include the IQN of each HBA. On hosts with dependent or independent HBAs the IQN of each HBA used must be included in the ACL.

6. Once the ACL Policy is complete click **Save**.

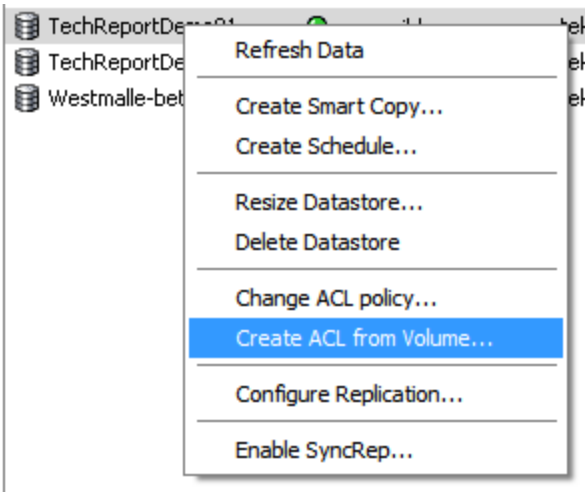


7. To exit the ACL Policy Manager click on the **X** in the top right corner of the dialog.

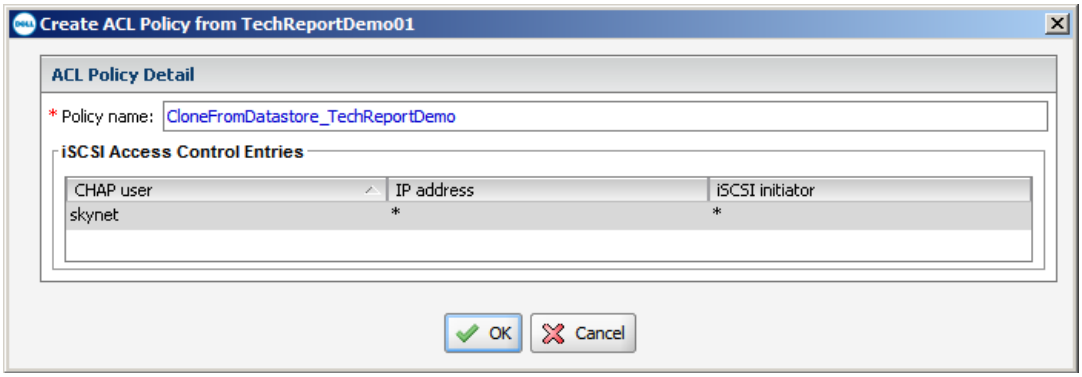
Creating an ACL policy from an existing datastore volume

In an existing environment there is likely to be existing datastore volumes that have a suitable ACL that an ACL Policy can be copied.

1. From the VSM datastore screen, right click on the datastore with the suitable ACL, and select **Create ACL from Volume**.



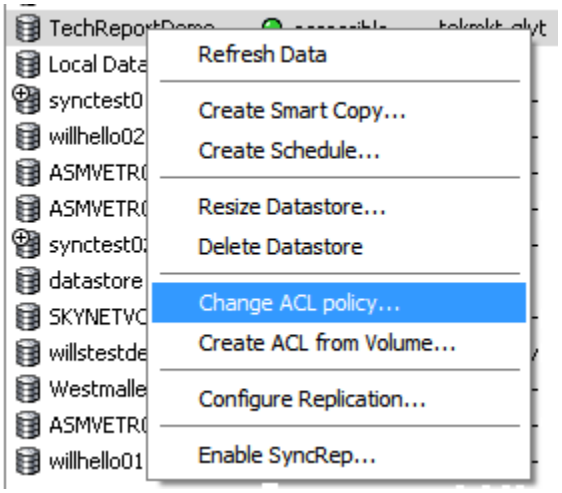
2. Provide a suitable name for the ACL Policy, and then click **Ok**.



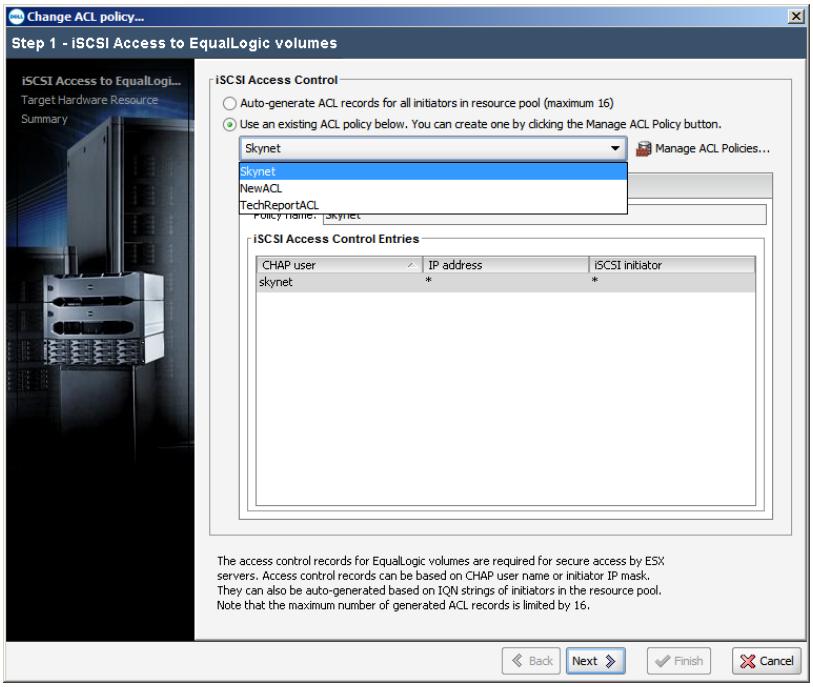
Existing ACL Policies can be edited and deleted from the **Manage ACL Policy** page. However, editing or deleting an ACL Policy does not alter the ACLs on datastore volumes that used that ACL Policy. Only newly created datastore volumes will receive the changed ACL Policy.

Changing the ACL on an existing datastore

1. From the VSM datastore screen, right click on the datastore with the suitable ACL, and select **Change ACL Policy**.



2. Select the desired new ACL Policy from the drop down menu. The details of the ACL Policy are displayed. Click **Next** to continue.



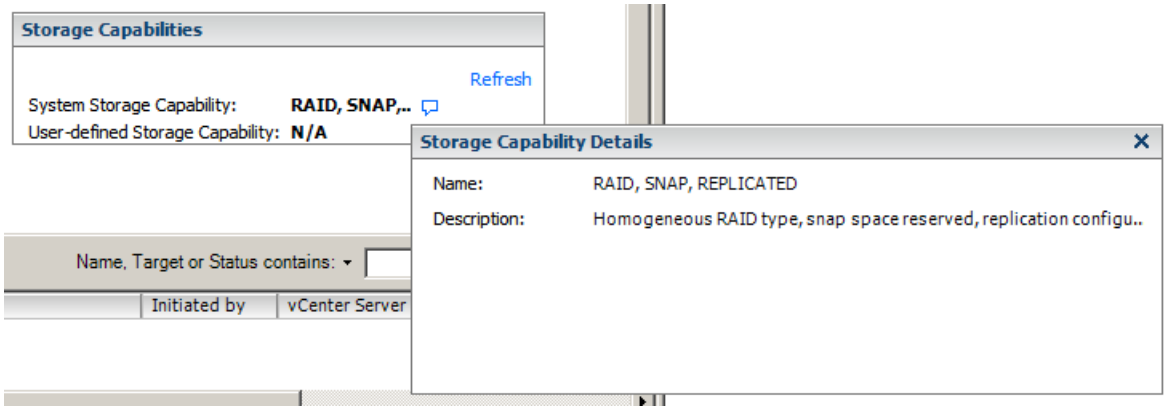
3. On the Summary page, review the setting changes, and click **Finish**.

Note: Care should be taken when changing the ACL on an existing datastore volume. An error in the new ACL would lead to hosts no longer having login rights to the volume. Such an error would not be imminently apparent as existing sessions would not be impacted; only newly created sessions or sessions that are moved as part of a load balancing operation would be impacted.

VASA Provider

Included with the EqualLogic VSM virtual appliance is the EqualLogic VASA Provider. VASA (VMware APIs for Storage Awareness) is a set of APIs that enable vCenter to communicate with the virtual environment's underlying storage. This non-SCSI communication with the EqualLogic array enables vSphere to learn the capabilities of each datastore volume presented to the virtual environment. These datastore volume capabilities are displayed in a number of locations in the vSphere Client interface, providing virtual administrators with valuable information about their storage infrastructure.

VSM displays these datastore volume capabilities in the Datastore section of the plug-in, in the System Storage Capability column, as shown below.



While the capabilities of VASA described thus far do not require a particular vSphere license, there are two vSphere features that leverage this information from VASA that do require Enterprise Plus licensing. These features are **Profile-Driven Storage** and the **Storage Distributed Resource Scheduler**.

Profile-Driven Storage uses this VASA-provided information to ensure that virtual machines reside on datastores that meet that virtual machine's needs. An administrator can create various Storage Profiles that reflect particular data protection needs. When a virtual machine is created, the administrator can select the Storage Profile that meets the requirements of the virtual machine, and place the virtual machine on a datastore that provides these capabilities. If the virtual machine is later migrated to a datastore that does not meet the Storage Profile, or should the capabilities of the datastore change so as to no longer meet the Storage Profile, the virtual machine will fail its storage profile compliance check. This compliance status can be seen on the individual virtual machine's summary page, and on the VM Storage Profile for all virtual machines assigned a Storage Profile. Profile-Driven Storage through the use of the EqualLogic VASA Provider enables administrators to place virtual machines on

the right datastore, and quickly ensure that virtual machines continue to reside on a datastore that meet their needs.

Storage Distributed Resource Scheduler, ("Storage DRS") applies VMware's CPU and memory resource management concept and applies them to datastores. Similar to VMware's traditional DRS capability, Storage DRS groups datastores with like performance characteristics into a Datastore Cluster. When a virtual machine is deployed, it is not deployed to a particular datastore, but rather to a datastore cluster. Storage DRS determines on which datastore to place the virtual machine, based on space utilization and I/O load. Like DRS, Storage DRS continuously monitors the cluster's space utilization, and the I/O load (using Storage I/O Control). Should space utilization or I/O response time thresholds be exceeded, or, if there is a significant difference in space utilization among the datastores within the datastore cluster, Storage DRS will seek to relocate a virtual machine using Storage vMotion.

However, while Storage DRS is aware of which datastores are involved (and therefore which volumes) it is not aware of where in the EqualLogic storage these volumes exist. Therefore prior to initiating a Storage vMotion action on a virtual machine, Storage DRS will consult with the EqualLogic VASA Provider. It queries to find out whether the migration of the virtual machine and its workload would benefit the overall I/O workload distribution of the EqualLogic array. If the migration will not result in an improvement in the distribution of the I/O workload (for example if the volumes involved reside on the same PS Series group members) the EqualLogic VASA Provider will inform Storage DRS not to perform the migration. Conversely, if the EqualLogic VASA Provider agrees that the migration will result in an improvement in the distribution of I/O (for example if the volumes involved reside on different PS Series group members) the Provider will approve of the migration request. In this case, Storage DRS leverages Storage vMotion to move the virtual machine and its I/O workload to the selected datastore.

In another parallel to VMware's classic DRS feature, Storage DRS has the concept of maintenance mode. When a datastore in a datastore cluster is placed in maintenance mode, the virtual machines and VMDKs residing on the datastore are moved to other datastores within the datastore cluster via Storage vMotion. Storage DRS will ensure that the I/O workload and space utilization remains balanced across the remaining datastores not in maintenance mode.

Storage DRS also has a placement constraint rule that is enforced during migrations. The first option, enabled by default, is the "Intra-VM VMDK affinity rule" which keeps all of a specific virtual machine's VMDKs together on the same datastore. The inverse of that rule, the "VMDK anti-affinity rule", keeps a

specific virtual machine's VMDKs on separate datastores within the datastore cluster. Finally, there is the "VM anti-affinity rule" which prevents certain virtual machines from sharing the same datastore.

Summary

In this technical report a number of installation consideration were discussed, enabling vSphere administrators to make informed decision when deploying EqualLogic Virtual Storage Manager to benefit from the additional ease of management and advanced virtual machine data protection in their virtualized environment.

The benefits to vSphere administrators of VSM are multiple. VSM enables administrators to perform storage related tasks with ease, to be aware of the capabilities of individual datastores, and provide tiered levels of data protection to their virtualized environment.

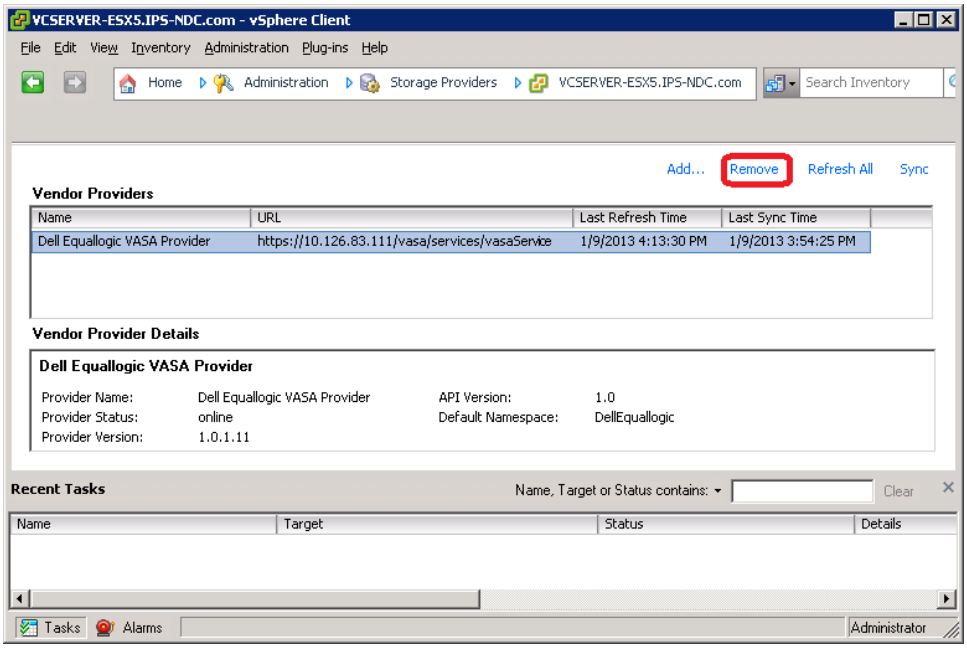
Appendix

Appendix A: Upgrading HIT/VE 3.1 to VSM 3.5

For customers with an existing install of EqualLogic Host Integration Toolkit for VMware (HIT/VE) the precursor to Virtual Storage Manager 3.5, these upgrade steps cover the process of upgrading from HIT/VE to VSM while maintaining the history and schedules of snapshots and replication.

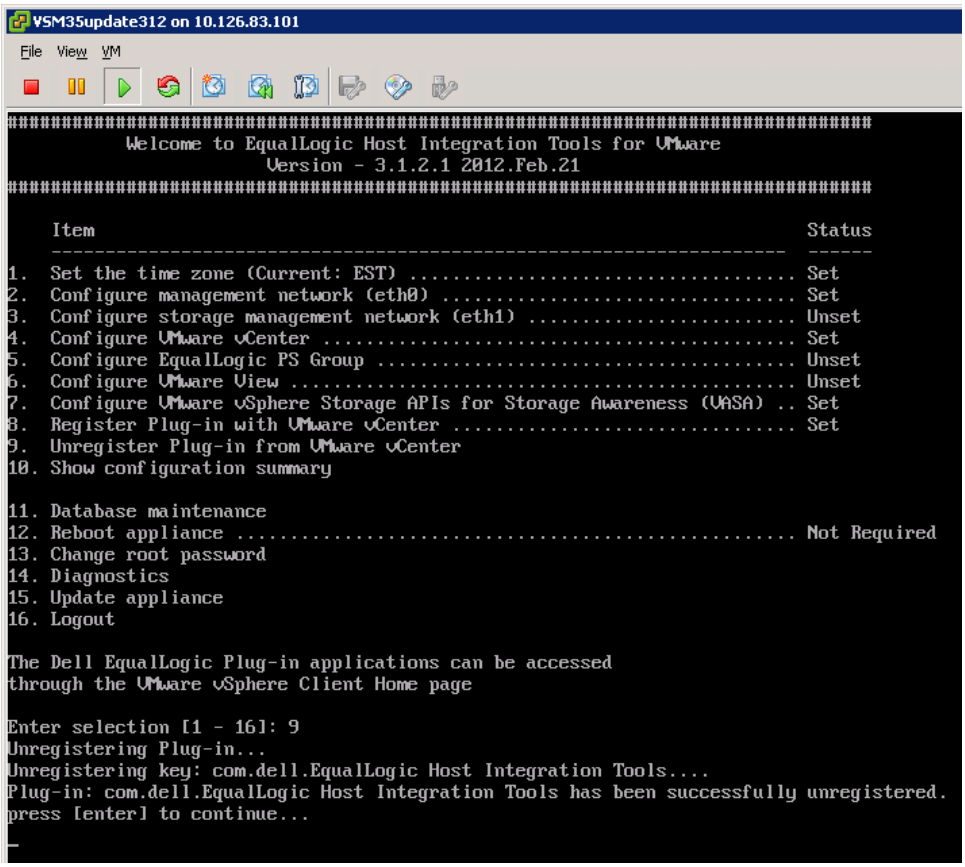
Prior to starting the upgrade process, verify that no scheduled tasks are planned to run. If there are scheduled tasks planned to run, either reschedule the upgrade or temporarily disable the scheduled tasks and re-enable it once the upgrade is completed.

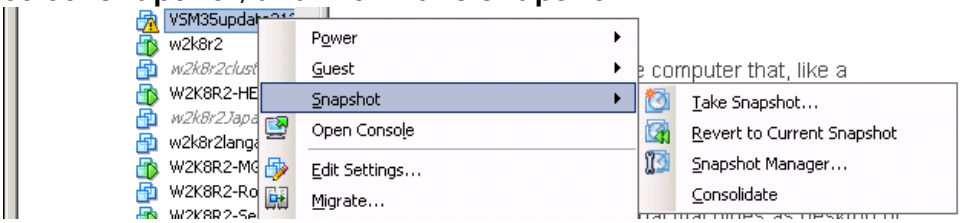
1. First the VASA Provider and plug-in must be unregistered from vCenter:
   a. To unregister the VASA Provider; from the **vSphere Client** goto **Storage Providers** which can be found in the **Administration** section on the **Home** screen.
   b. From Storage Providers highlight the Dell EqualLogic VASA Provider and click on **Remove**.



   c. To unregister the plug-in; go to the virtual machine console of the HIT/VE virtual appliance, and log in.

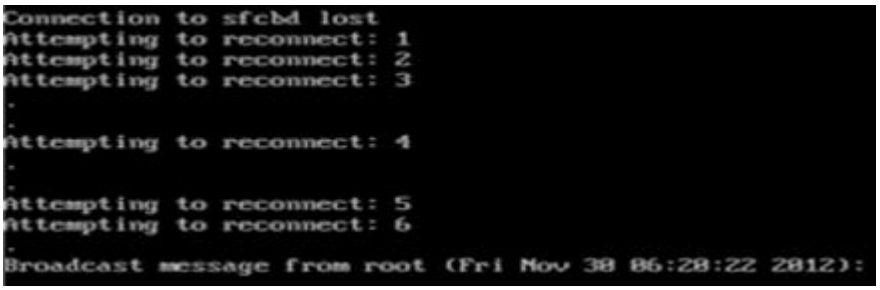
d. Select option 9, **Unregister Plug-in from VMware vCenter**, from the menu, and click **Enter** to continue.



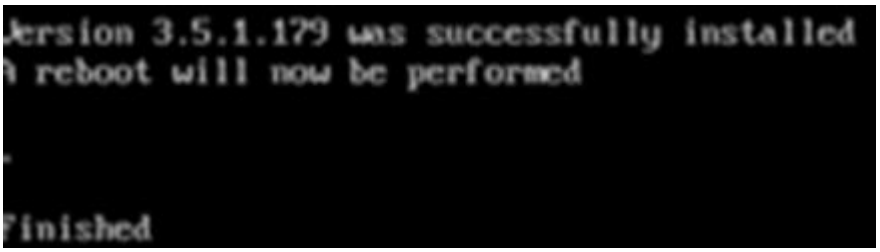
2. While it is not a required part of the upgrade process, it is recommended that a VMware snapshot be created of the virtual appliance.
   a. Right click on the HIT/VE virtual appliance, from the context menu select **Snapshot**, and then **Take Snapshot**.
   b. 

   Provide a logical name and optionally a description for the snapshot and click **OK.**
   c. Wait until the snapshot task has completed, it will only take a few minutes.

3. Mount the VSM 3.5 upgrade ISO in the virtual appliance's CD-ROM drive, ensuring to check the **Connect** checkbox.
    a. Return to the HIT/VE virtual appliance console, and from the main menu select option **15: Update appliance**.
    b. From the Update appliance menu select option **2: Check for updates**. This will analyze the mounted ISO and verify that it contains a valid upgrade. Press **Enter** to return to the Update appliance menu
    c. From the Update appliance menu select option **3: Install update**. Verify that you wish to upgrade the virtual appliance and press **Enter** to continue.
    d. The upgrade process will now begin. It is normal to see the message "*Connection to sfcdb lost*" and multiple "*Attempting to reconnect: XX*" messages, do not interrupt the upgrade process.

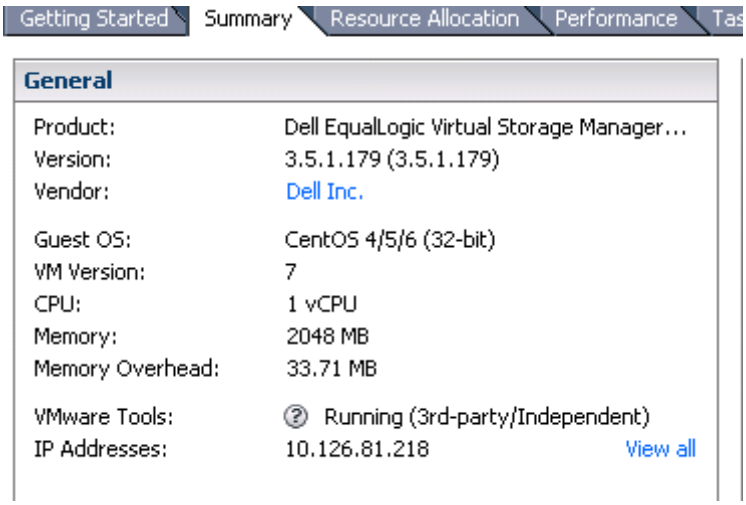


    e. Once the upgrade process is completed, a reboot will be automatically preformed.



    f. Once the reboot is completed VSM will automatically register with vCenter it is installed within, as long as the **vCenter Server Managed IP** is set. It will be necessary to re-configure VASA as shown in the **Configuring the VASA Provider** section of this technical report.

4. With the upgrade completed, the summary tab of the VSM virtual appliance the following information:



5. Once the upgrade has been verified as successful, re-enable any scheduled tasks that we're disabled, and remove the VMware snapshot of the VM that was created.

Technical Support and Customer Service

Dell support service is available to answer your questions about PS Series SAN arrays.

Contacting Dell

1. If you have an Express Service Code, have it ready.
   The code helps the Dell automated support telephone system direct your call more efficiently.

2. If you are a customer in the United States or Canada in need of technical support,
   call 1-800-945-3355. If not, go to Step 3.

3. Visit support.dell.com/equallogic.

4. Log in, or click "Create Account" to request a new support account.

5. At the top right, click "Contact Us," and call the phone number or select the link for the type
   of support you need.