# Dell MD Storage Array vCenter Plug-in

# User's Guide

# Notes and Cautions

**NOTE:** A NOTE indicates important information that helps you make better use of your computer

**CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.**

**June 2011**          **Rev. A02**

# Contents

**1**

# Dell MD Storage Array vCenter Plug-in Overview

The Dell MD Storage Array vCenter Management Plug-in Installation and User Guide is a VMware vCenter Server 4.x Plug-in that provides integrated management of Dell MD Storage Array series from a vSphere Client. The vCenter Plug-in allows administrators to have a single management interface (vSphere Client) to manage all of their day-to-day storage needs along with their VMware infrastructure. This alleviates the need for vCenter administrators to learn another management tool and focus instead on the entire virtual infrastructure.

The vCenter Plug-in enables the vCenter administrator to configure ESX and ESXi hosts to Dell MD Storage Arrays, create, map, delete virtual disks from the Dell MD Storage Arrays to the ESX host, and view the vCenter datastores to Dell MD Storage Array virtual disks. The vCenter Plug-in also allows the creation of hardware snapshots, virtual disk copies, and remote replication, when these premium features are enabled on the storage array. The vCenter Plug-in uses an application server to facilitate the interface between the vSphere Client and the Dell MD Storage Array based on the authenticated logged-in user and the privileges assigned to that user's role.

✎ **NOTE:** The vCenter Plug-in requires that a vCenter Server be installed within the environment. The vCenter Plug-in does not function in a vSphere client and ESX host-only configuration.

**Figure 1.  Communication Details**
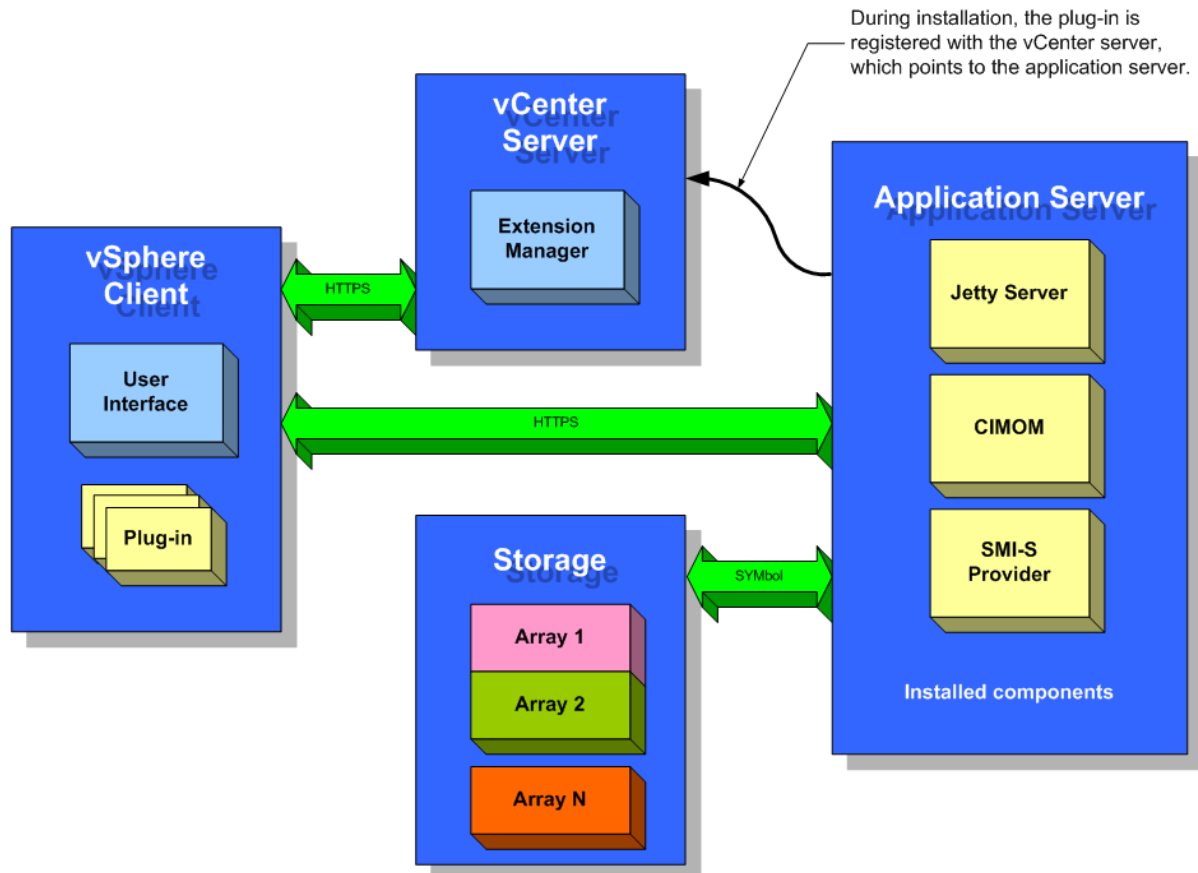
# Installation Prerequisites

To install and use the vCenter Plug-in, the following prerequisites must be met.

- The VMware vCenter 4.x server is installed
- One of the following servers is available to be the application server:
    - Windows 2003 server
    - Windows, 2003 R2 server
    - 32-bit Windows 2008 server
    - 64-bit Windows 2008 server
    - 32-bit Windows 2008 R2 server
    - 64-bit Windows 2008 R2 server
- Dell MD Storage Array with VMware certified firmware
- The vCenter Plug-in requires the following firmware versions:
    - 7.35
    - 7.60
    - 7.70
    - 7.75
    - 7.77

# Recommended Configurations

The vCenter Plug-in uses the SMI-S protocol to communicate with the storage arrays that are managed within the vSphere infrastructure. Many procedure calls are made to obtain and send changes to the storage arrays, which require large amounts of data to be passed between the storage arrays, the application server, and the vSphere client. The number of managed storage arrays, the number of virtual disks, and the number of physical disks on each storage array determine the overall performance of the vCenter Plug-in. Therefore, limit the number of managed system components to the following:

- No more than 10 Dell MD series storage arrays
- No more than 256 objects, such as virtual disks, virtual disk copies, and snapshots, on each array
- No more than 16 remote replications

# Downloading the vCenter Plug-in

Obtain the correct version of the Dell Storage vCenter Plug-in for your environment (x86 or x64) from the Download and Drivers area at support.dell.com. See the Support Matrix at support.dell.com/manuals for the most current versions. The file should be copied to the application server.

# Installing the vCenter Application Server

Install the vCenter application server on a different Windows 2003 server or Windows 2008 server than the VMware vCenter Server is installed on.

> **NOTE:** When adequate resources are available on the vCenter Server system, you can install the application server on the same host as the vCenter Server, but it is not recommended.

After you have downloaded the vCenter Plug-in software, copy the file to the system that will be the application server. Run the vCenter Plug-in installer to launch the installation wizard. The installation wizard installs a Jetty application server and the SMI-S provider. After the installation is complete, the installation wizard registers the vCenter Plug-in with the vCenter Server.

During the installation process, you must provide information about the system components, such as the storage array names, the IP addresses, and the DNS names, used during the installation. *Table 1* shows the information required for each component.

**Table 1. Configuration Worksheet Example**

| vCenter Server Names | VCENTER-4 | DNS Names<br>IP Addresses | vCenter-4.domain.com<br>192.168.51.217 |
|---|---|---|---|
| vCenter Administrator Name: | administrator | Password: | password |
| Application Server Name: | App-Server | DNS Name: IP Address: | app-server.domain.com<br>192.168.51.225 |
| Dell MD Storage Array 1 Name: | MD3600-01 | IP Addresses: Password: | 192.168.51.89<br>192.168.51.90 |
| Dell MD Storage Array 2 Name: | MD3600-02 | IIP Addresses: Password: | 192.168.51.91<br>192.168.51.92 |
| Dell MD Storage Array 3 Name: | | IP Addresses: Password: | |
| Storage Administrator User ID: | User1 | | |
| Storage Administrator User ID: | | | |

*NOTE:* When you are upgrading from an earlier version of the vCenter Plug-in, and the storage arrays already have passwords, re-enter the previous passwords in the updated version of the vCenter Plug-in for each storage array. You cannot modify the storage arrays until the passwords have been re-entered.

# Installing the vCenter Plug-in

1  Read the introduction screen and then click **Next**.

2  Read through the license agreement and if you accept the terms, select the appropriate radio button and click **Next**.

3  Select the local installation directory for the vCenter Plug-in manager or click **Next** for the default.

4  Review the installation details and click **Install** if the details are correct.

5  Change the port number of the Jetty server or accept the default of 8084 and 8081 and click **Next**.

*NOTE:* If the vCenter Plug-In will be installed on the same system as an active vCenter Server, and VMware Update Manager is installed, the port number 8084 for the plug-in must be changed from the default to an unused port number.

6  Change the IP address of the application server when desired. The IP address defaults to the IP address of the system the installer is running on. Click **Next**.

7  The next screen prompts you for the IP address of the vCenter server on which to install the vCenter Plug-in. Enter the IP address of the vCenter server and click **Next**.

8  Enter the Administrator's email address for alerts and click **Next**.

9  Enter the vCenter Administrator's User ID and click **Next**.

10  Enter the vCenter Administrator's password and click **Next**.

11  The installation is now complete. Click **Done** to close the installation wizard.

12  To verify that the application server was installed successfully, run the services.msc command, and verify that the cimserver service was installed and that both the cimserver service and the Jetty6-Service service have started.

*NOTE:* After the application server reboots, the name of the CIMOM service changes to Pegasus CIM Object Manager.

*NOTE:* In the event one of these services crash or is stopped, the CIMOM service must be started before the Jetty service or no updates/modifications will occur.

# 2

# Configuring the Application Server and the vCenter Plug-In

After the application server and the vCenter Plug-in were installed, verify that the vCenter Plug-in was successfully registered with the vCenter server.

- Open the vSphere Client to the vCenter Server.

- On the menu bar, select **Plug-ins->Manage Plug-ins.**

- The Dell MD Storage Array vCenter Management Plug-in is listed as Enabled.

- However if the vCenter Plug-in is listed as disabled with an error message stating that it cannot communicate with the application server, verify that the port number defined for the Jetty server is enabled to pass through any firewalls that might be in use. The default Jetty TCP port number is 8084 and 8081.

After the application server and vCenter server have been configured, the **Dell MD Storage Array vCenter Management vCenter Plug-in icon** appears in the Solution and Application section of the vSphere Client page.

**Figure 2  vSphere Client Home Page**
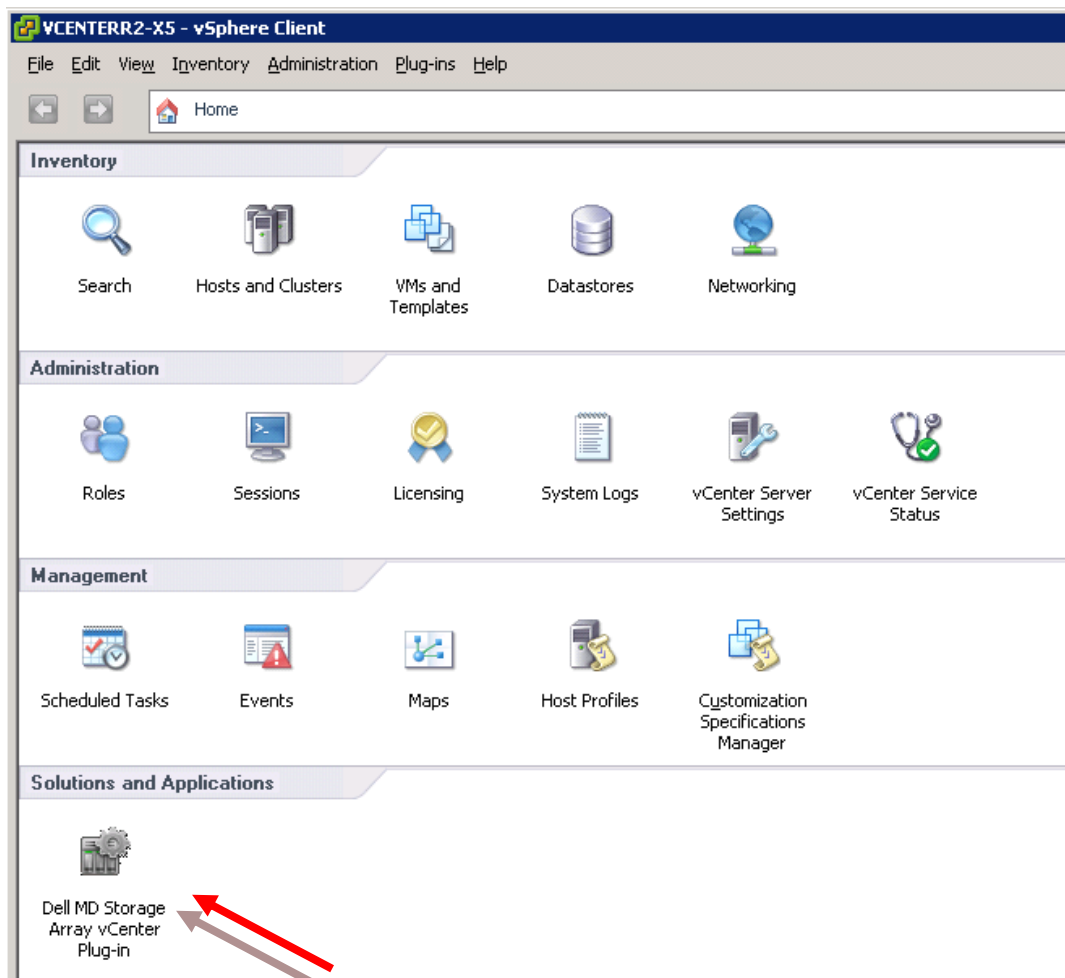
# Configuring Storage Administrator Roles

By default, all defined vCenter user IDs have no rights to Dell MD Storage Arrays. When a user requires either read permissions or read/write permissions to access the vCenter Plug-in, the user's role must be modified to permit access to the vCenter Plug-in.

### Creating and a Role

**1**  In the Administration area on the vSphere Client Home page, as shown in *Figure 2*, click on the **Roles** icon.  The list of roles and usages appears.

**Figure 3.  vCenter Plug-In Roles List**
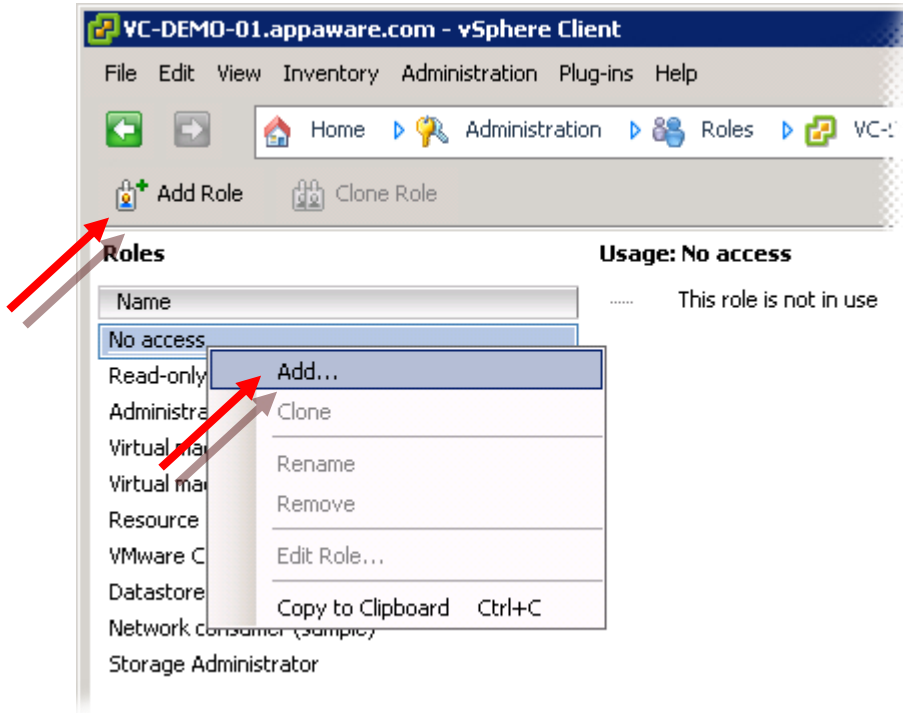


**2**  Click on **Add Role** icon or right-click.

A pop-up menu appears, as shown in *Figure 3*.

**3**  Select **Add**.

The Add New Role window opens.

**Figure 4.  Add New Role Window**
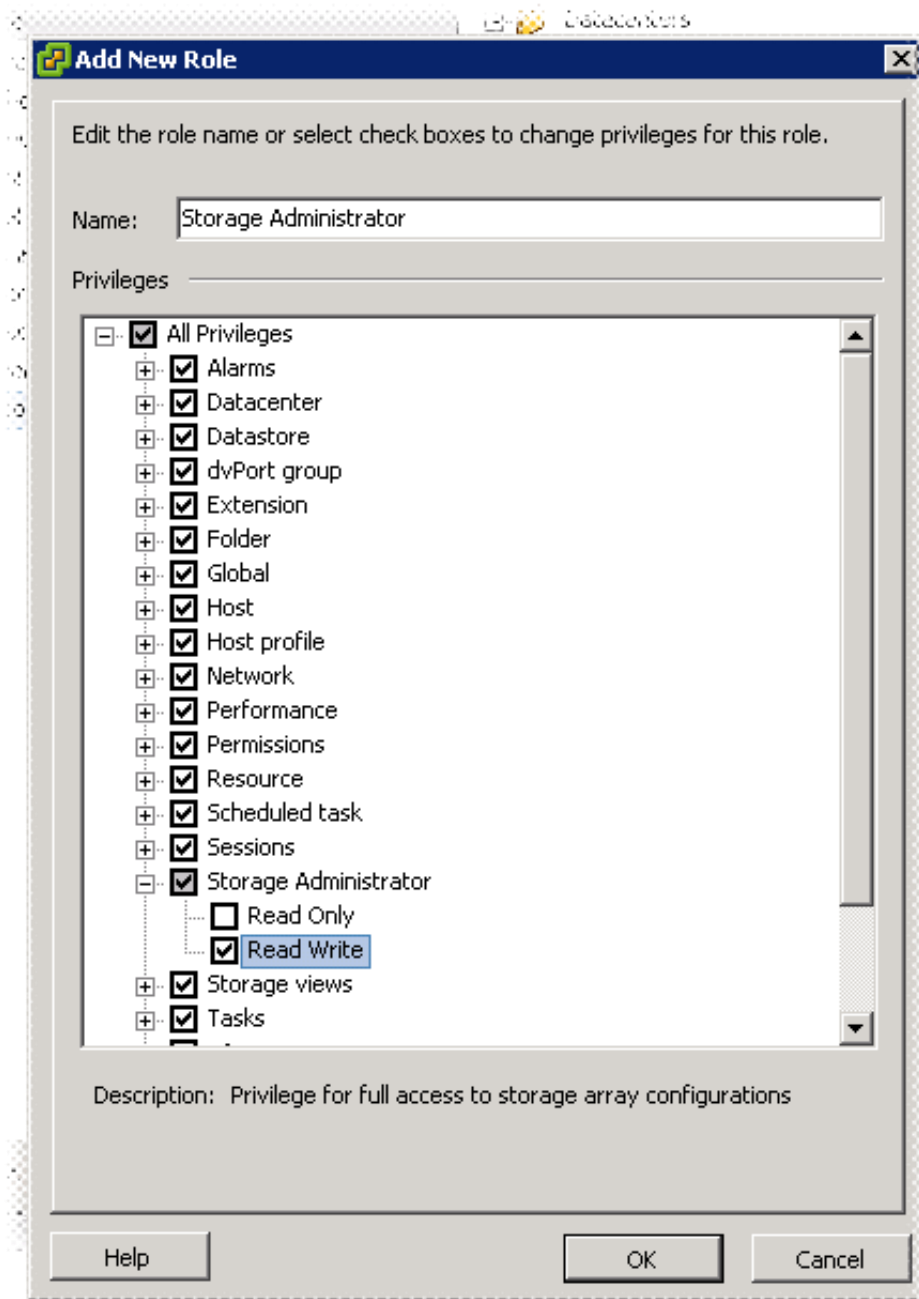


4    In the Name text box, type the name of the new role.

5    On the Privileges list, select the access permissions to assign to this role.

*NOTE: The administrator role is not editable and, therefore, if the administrator user will be used to manage storage, a new role must be created that has all of the privileges added to it. The administrator user must then be added to this role as the following procedure details.*

6    To allow Read Only or Read Write access permissions to the storage arrays, select the appropriate permission from the Storage Administrator group. See *Figure 4*.

7    Click **OK**.

*NOTE: Existing roles may also be modified to include the Storage Administrator privileges, except for the Administrator role, which cannot be modified.*

## Adding a User ID to a Role

1. From the Home screen, select Hosts and Clusters and then select the vCenter server element and select the Permissions tab. See *Figure 5*.
2. Right-click and select Add Permission to define the users who are members of the Role.

**Figure 5. Assign Storage Administrator Role**
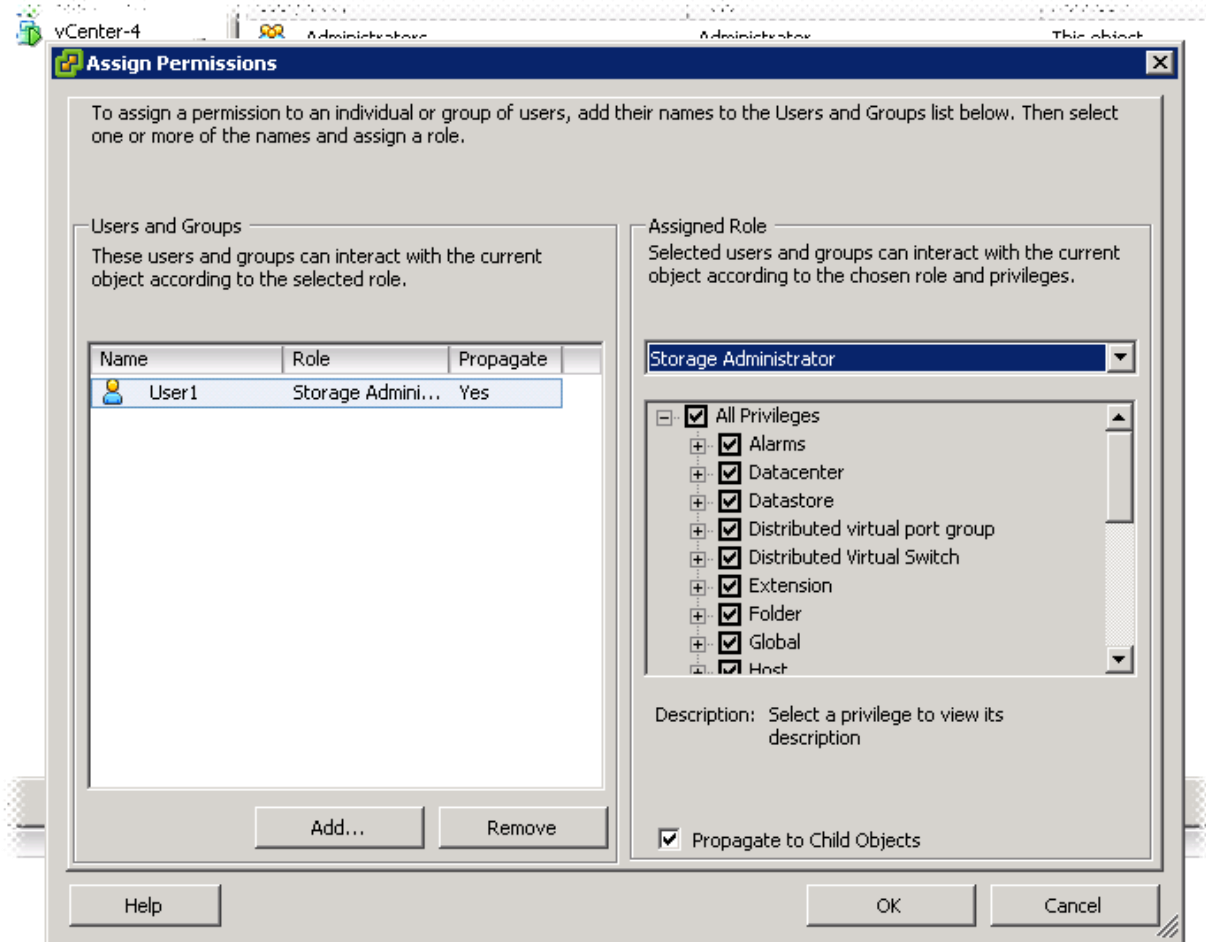


3. From the wizard, click Add and select the User ID (s) that require access to the storage arrays.
4. Then select the modified Role from the drop down box and click **OK** to apply changes.
5. Click **OK** to apply permissions to the role.

## No Access

If users are not members of a role that has either the Read Only or Read Write Storage Administrator permission, they cannot view any statistics from the vCenter Plug-in. If they attempt to access a vCenter Plug-in feature they receive the User is not authorized to use this plug-in message as shown in Figure 6.

**Figure 6. No Access Message**



## SAS Support on ESX/ESXi hosts

For the vCenter Plug-in to configure ESX and ESXi hosts to the Dell MD Storage Arrays, with SAS connections, an updated version of the LSI SAS SMI-S provider must be installed on the ESX and ESXi hosts. This section describes how to upgrade the SAS SMI-S provider.

> **NOTE:** SAS Support is only available for ESX/ESXi 4.1 and later hosts. Previous versions of ESX and ESXi are not supported.

> **NOTE:** This upgrade is only required to allow for the Host to Storage Configuration option to configure SAS connected storage arrays. If this functionality is not required (the storage arrays are already configured or not using SAS connected storage arrays), the in-box provider does not need to be upgraded.

To use the SAS provider, it must first be deployed on the ESX/ESXi servers to be configured. This requires that SFTP or SCP be enabled on the ESX/ESXi hosts. Root access is also required to install the package, and to install the package by remote login, either a new user must be created with host login rights or the root user must be enabled for remote logins.

### Enabling Root Login from a Console Login on ESX Hosts

1  Log in as *root*.

2  Open the **/etc/ssh/sshd_config** file.

3  On the line that contains **PermitRootLogin**, change **no** to **yes**.

4  Save and close the file.

5  At the shell prompt, run the **# service sshd restart** command to reload the service.

### Enabling Root Login from a Console Login on ESXi Hosts

1  Press F2 to switch to the diagnostic console.

2  Select **Troubleshooting Options**.

3  Select **Enable Remote Tech Support**.

4  Select **Restart Management Agents**.

5  Press Esc to close the **Configuration** menu.

### Creating a New User Login

**1** Connect the vCenter client directly to the ESX/ESXi host to be configured.

**2** Select the **User & Groups** tab from **Home->Inventory->Inventory** window.

**3** Right-click and select **Add**.

**4** Supply the relevant information for the new user and make sure to select '**Grant shell access to this user**' option.

**5** Click **OK** to save changes.

**6** After logging in as this new user, use the **>su -** command to assume super user role.

# Installing the SAS Provider Upgrade

**1** Either SFTP the **vmware-esx-provider-lsi-provider.vib** file to the target ESX host or SCP the file to the target ESXi host.

**2** Log in to the ESX/ESXi 4.1 host as *root*.

✍ **NOTE:** If *root* is not enabled, log in as a shell-enabled user, and **su** to super user.

**3** From the shell prompt, **vmware -v** to verify the version is 4.1.

✍ **NOTE:** If *root* is not enabled, log in as a shell-enabled user, and **su** to super user.

**4** Enter **rpm -q lsi-provider** for ESX or **esxupdate --vib-view query | grep lsi-provider** for ESXi hosts. The version listed should be: **lsi-provider-410.04.V0.24-140815**.

**5** Enter **esxupdate -b file:$PWD/vmware-esx-provider-lsi-provider.vib --nodeps --nosigcheck --maintenancemode update**, this assumes the .vib file is located in the same directory that **esxupdate** is being executed from, if not, change **$PWD** to the directory where the .vib file is located.

**6** You should see Unpacking cross_lsi-provider, Installing lsi-provider, and Cleaning up lsi-provider

**7** After the update finishes, enter **esxupdate --vib-view query | grep lsi-provider**.

You should see the following information:

- **cross_lsi-provider_410.04.V0.24-260xxx pending,installed**
- **cross_lsi-provider_410.04.V0.24-140815 retired**

**8** Reboot the host after stopping any running VMs.

**9** Upon reboot, verify that the update was applied with **rpm -q lsi-provider** for ESX or **esxupdate --vib-view query | grep lsi-provider** for ESXi hosts.

**10** Done

# vCenter Plug-in Security

## Accepting and Installing the Trusted SSL Certificate

The vCenter Plug-in uses Secure Sockets Layer (SSL) to communicate securely between the vSphere client and application server. During the vCenter Server installation process, a SSL certificate was generated for the vCenter Server system. If this certificate has not been added to the system's Trusted Root Certification Authorities store, you will see a Security Alert dialog box appear, as shown in Figure 7.

**Figure 7. SSL Security Alert Message**
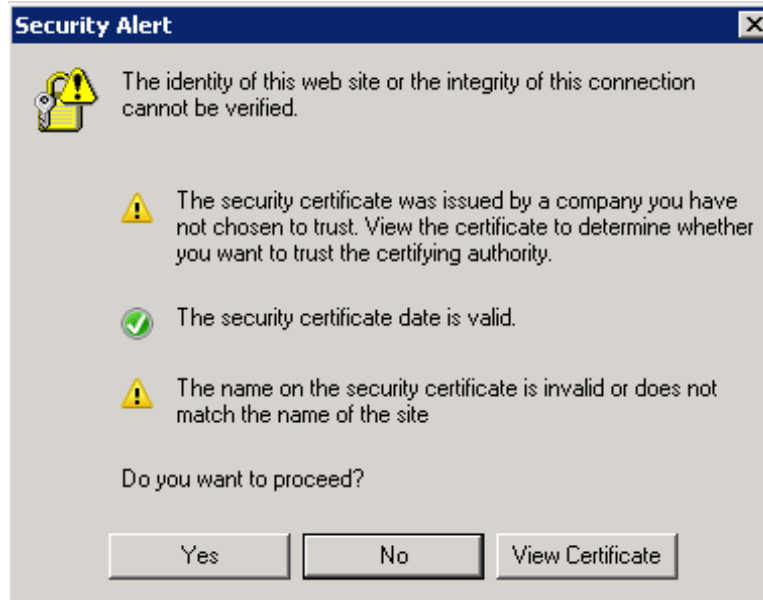


To avoid this message, you can import the install generated certificate into the systems Trusted Root Certification Authorities store as listed below:

**1**   Click **View Certificate**
**2**   Click **Install Certificate** see Figure 8.

**Figure 8.  Install Certificate Dialog Box**
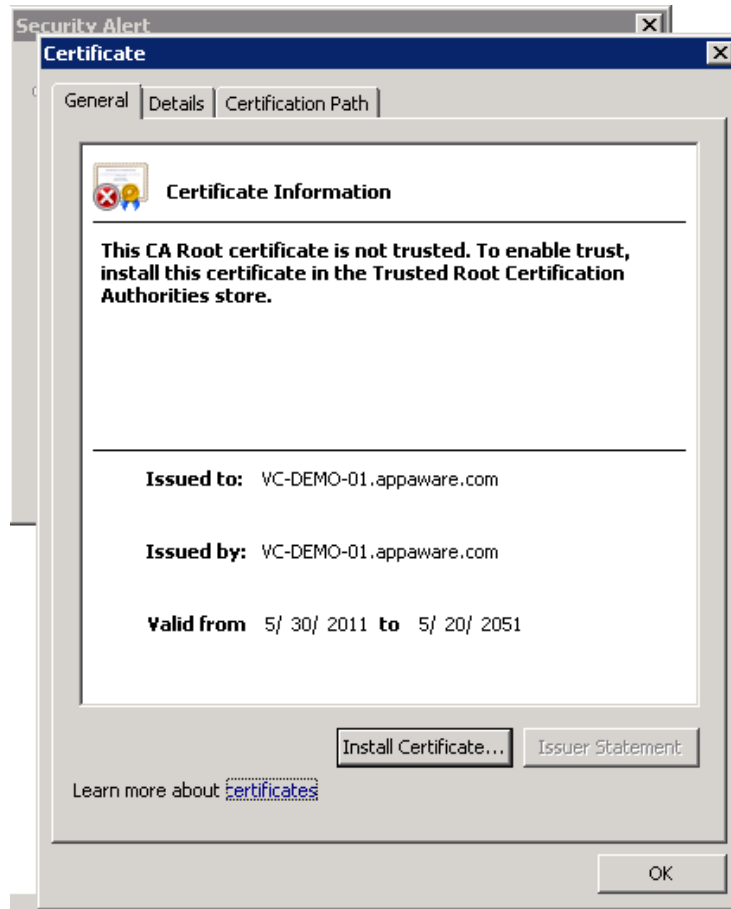


**3** Click **Next** from the Certificate Import Wizard message box. See Figure 9.

**Figure 9.  Certificate Import Wizard**
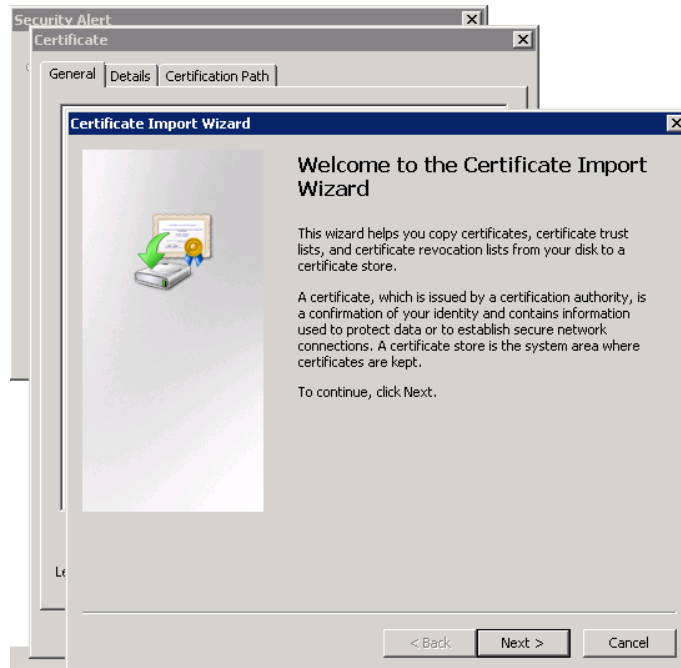
**4**     Select the **Place all certificates in the following store** radio button

**5**     Click **Browse**

**6**     Highlight the **Trusted Root Certification Authorities** folder. See Figure 10.

**Figure 10. Select Certificate Store Dialog Box**
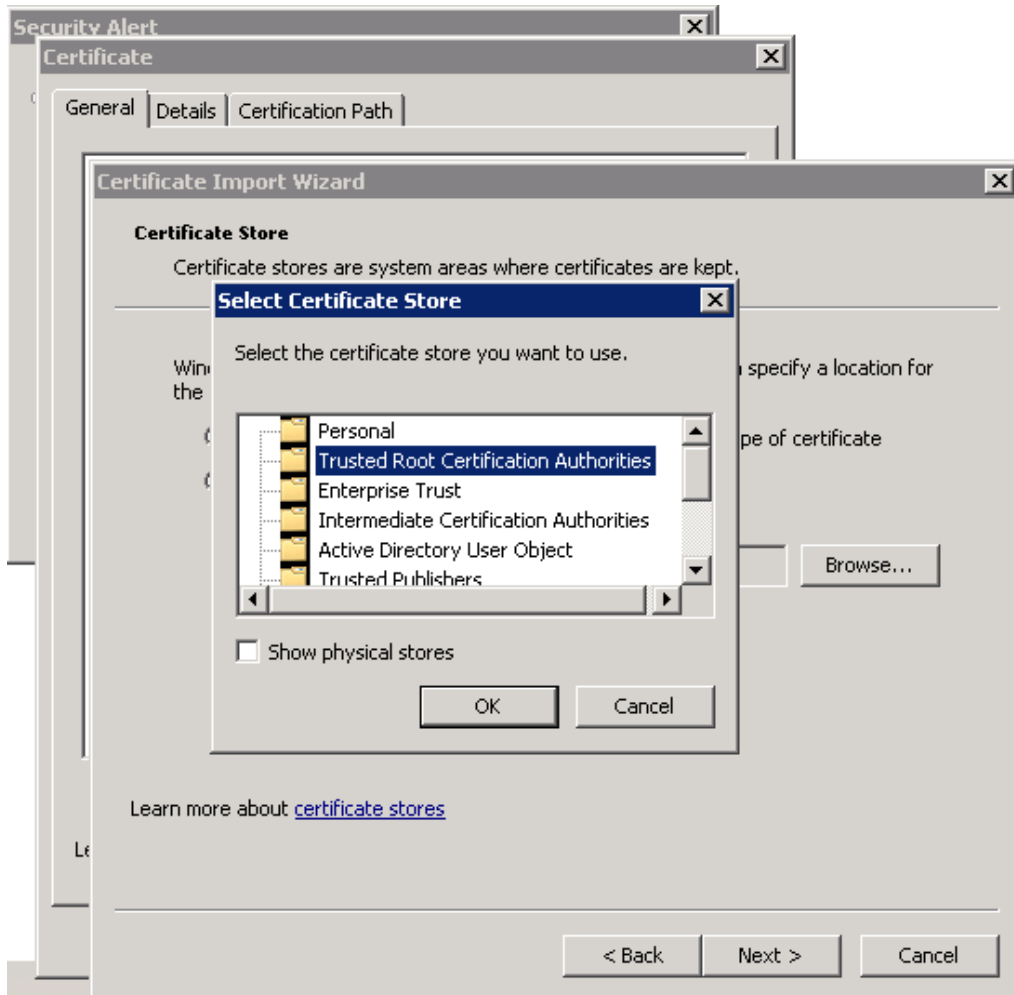
**7** Click **OK**

**8** Click **Next**

**9** Click **Finish**

**10** A Security Warning message box will be displayed.  Verify the information and click **Yes** to add the certificate to the trust store. See Figure 11.

**Figure 11.  Security Warning Message Box**



**NOTE:** The subject name of the system, in the certificate must match the system name of the vCenter Server during the vSphere Client login screen or you will continue to receive a warning message stating the certificate does not match the site name.

## Enhanced IE Security

When Microsoft's Enhanced IE Security is installed on the vSphere client system, the enhanced security configuration blocks content from the web site. The warning message shown in Figure 12 appears.

- Click Add to establish a trust relationship with the application server.

**Figure 12. IE Enhanced Security Message**

# 3

# Dell MD Storage vCenter Plug-in Features

## vCenter Plug-in Features

The following vCenter Plug-in features enable the integrated management of Dell MD Storage Arrays:

- Array Manager view
- Copy services management
- A configuration wizard for ESX/ESXi host storage
- Virtual disk management of storage arrays
- Datastores to virtual disk details
- Event log viewer for storage array events
- Automatic and manual storage array configuration backup

## Configuring Storage Arrays

To use the vCenter Plug-in to create or modify virtual disks on the storage array, click on the **Dell MD Storage Array vCenter Management Plug-in** icon on the vSphere Client Home page under Solutions and Applications. See *Figure 13*.

**Figure 13.  Dell MD Storage Array vCenter Management Plug-In Icon**
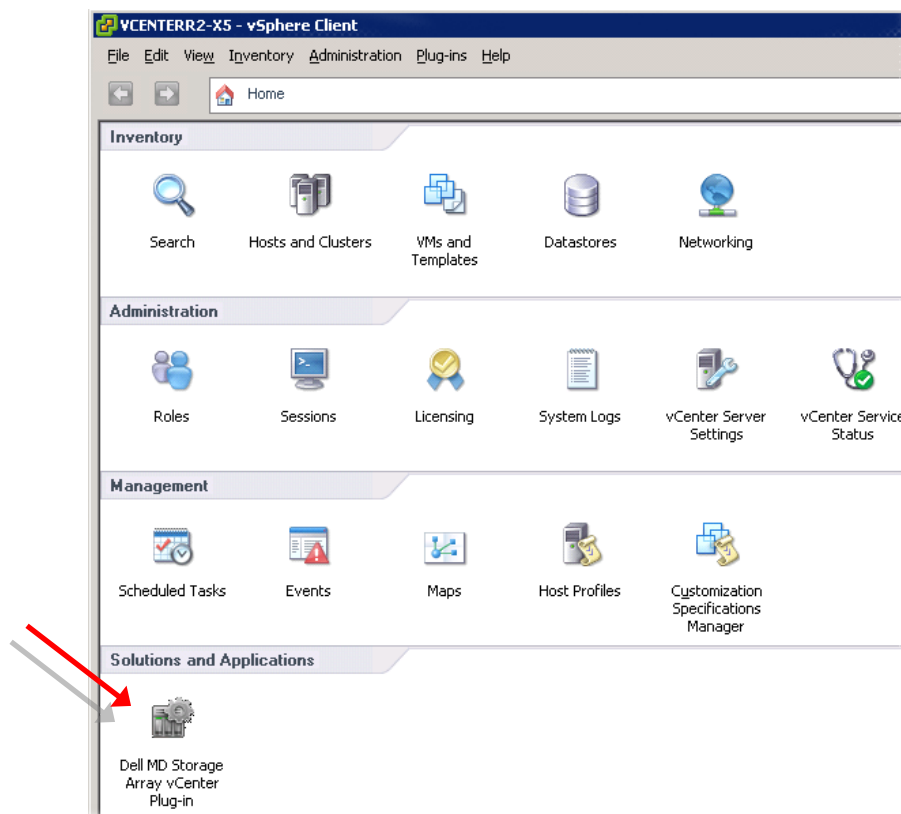
Clicking the icon will open the Storage Array Manager view where you can manage Dell storage arrays. The Storage Array Manager view displays a list of known storage arrays and lets additional storage arrays be added or removed. See Figure 14.

**Figure 14.  vCenter Plug-in Array Manager View**
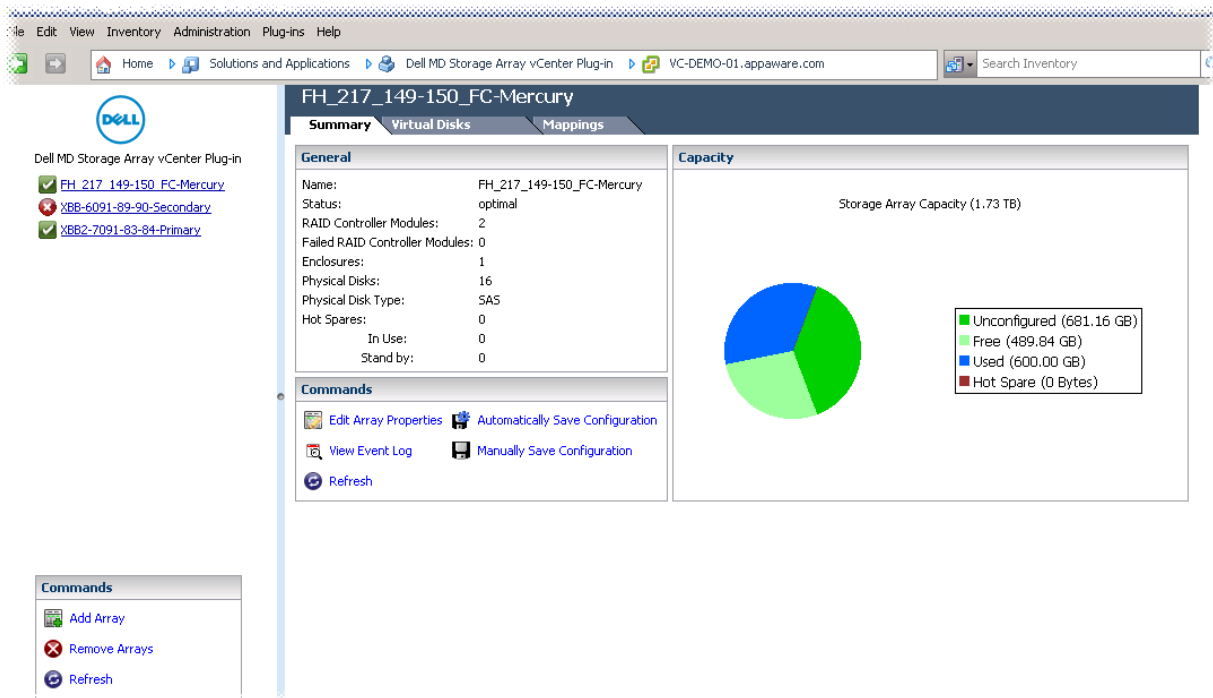


# Adding a Storage Array

**1**  In the Commands area of the vCenter Plug-in Array Manager view, click **Add Array**.

**2**  A dialog box appears with the DNS Name or IP Address text boxes and the Password text box. See Figure 15.

**Figure 15.  Add Array Dialog Box**
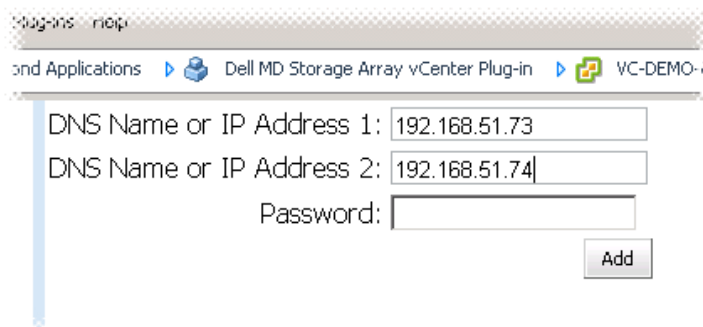


**3**  In the DNS name or IP address 1 text box, type the IP address or name of the storage array's controller A.

**4**  In the DNS name or IP address 2 text box, type the IP address or name of the storage array's controller B.

**5**  In the Password text box, type the password for the storage array that you are adding to the vCenter Plug-in.

**6**  Click **Add**.

# Removing a Storage array

**1** In the vSphere Client Storage array Manager View, click Remove Arrays.

The Remove Arrays Properties dialog box appears.

**2** Select the storage array to be removed, and click OK.

# Editing System Properties

## Changing a Storage Array Password

**1** Open the Storage Array Manager View. See Figure 14.

**2** In the left pane, click the name of the storage array.

The storage array properties are displayed in the right pane.

**3** In the right pane, click **Edit Array Properties** link.

The Edit Array Properties dialog box appears.

**4** In the Password text box, type the new array password, and click **OK**.

## Resolving a Password Mismatch

When the vCenter Plug-in password and the storage array password do not match, you can run passive, read-only commands, such as Read and View, on the storage array; however, active, read/write commands to the array, such as create and delete, will fail. The vCenter Plug-in displays the properties of the storage array whether the passwords match or do not match. To resolve a password mismatch, perform the previous procedure, Changing a Storage Array Password.

# Storage Array Configuration Backup

Version 2.2 of the vCenter Plug-in supports storage array configuration backups to script files that may be applied to a storage array from the Dell Modular Disk Storage Manager (MDSM). These script files will facilitate the restoration of the storage array configuration, such as storage array name, disk group configurations, virtual disk names, virtual disk capacities, etc. **IT WILL NOT BACKUP DATA RESIDING ON THE STORAGE ARRAY!** A traditional backup strategy must still be employed to provide recovery of user data residing on the virtual disks.

⚠ **CAUTION: Only the storage array configuration information is saved during the save configuration operation, NOT data stored on the virtual disks.**

✐ **NOTE:** Only the base storage array configuration information is saved. Objects such as snapshots, virtual disk copies, and remote replications are not saved to the script file.

The vCenter Plug-in Automatic Save Configuration will perform a save configuration of the storage array after a configuration event has occurred on the storage array, either from the vCenter Plug-in or from MDSM. A storage array modification event will start a 4 minute timer, on the application server, at the time of the event on the storage array. If within that 4 minute time window, no other configuration events have occurred on the storage array, a save configuration will occur. If another modification event occurs within the 4 minute time window, the timer will be reset to 4 minutes. When no modification events are detected on the storage array within the 4 minute window, a save configuration will be performed. Automatic Save Configuration will maintain the last 15 save configuration script files.

## Enable Automatic Save Configuration Backups

These backups can be set to automatic or manually initiated. To enable automatic backups of the storage array base configuration, perform the procedure below:

**1** Open the Storage Array Manager View. See Figure 14.

**2** In the left pane, click the name of the storage array.

The storage array properties are displayed in the right pane.

**3** In the right pane, click **Automatically Save Configuration** link.

The Automatically Save Configuration dialog box appears. See Figure 16.

**4** Check the Enable automatic save configuration box.

**5**    Click **OK** to enable automatic configuration backups.

**Figure 16.  Automatic Save Configuration Message Box**
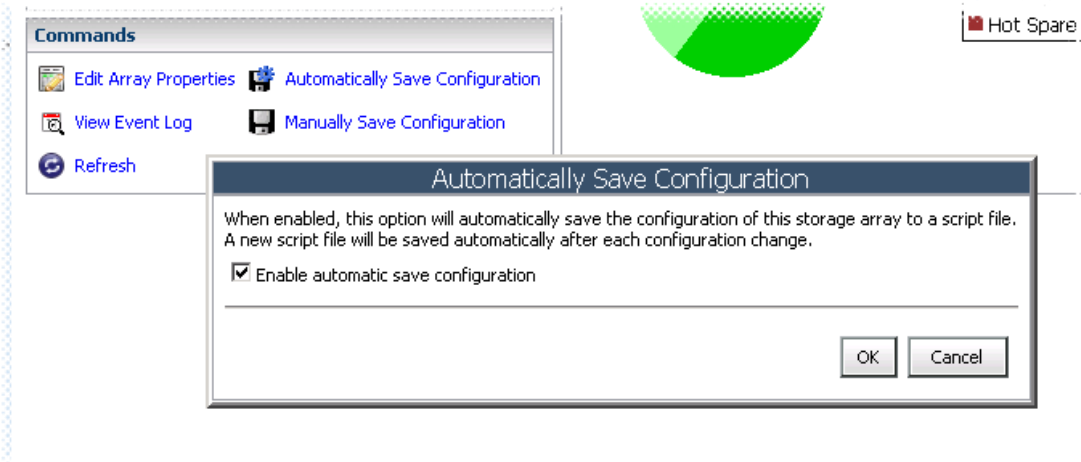


📝    **NOTE:** The automatic backup script files are located under `C:\Program Files (x86)\Dell\MD Storage Array vCenter Plug-In\jetty\savecfg` directory.

## Initiate A Manual Save Configuration

To perform a manual save configuration, perform the procedure below:

**1**    Open the Storage Array Manager View. See Figure 14.

**2**    In the left pane, click the name of the storage array.

The storage array properties are displayed in the right pane.

**3**    In the right pane, click **Manually Save Configuration** link.

The Manually Save Configuration dialog box appears.  See Figure 17.

**Figure 17.  Manually Save Configuration Message Box**
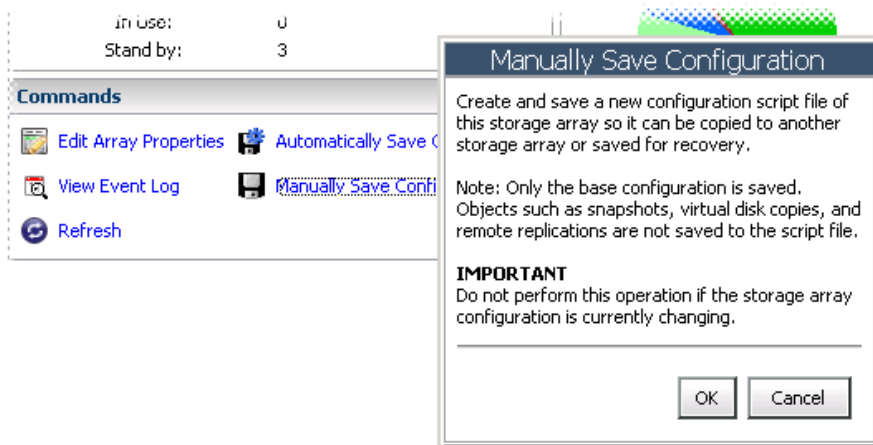
**4** Click **OK**

Internet Explorer will launch a File Download dialog box. See Figure 18.

**Figure 18.  Internet Explorer File Download Dialog Box**
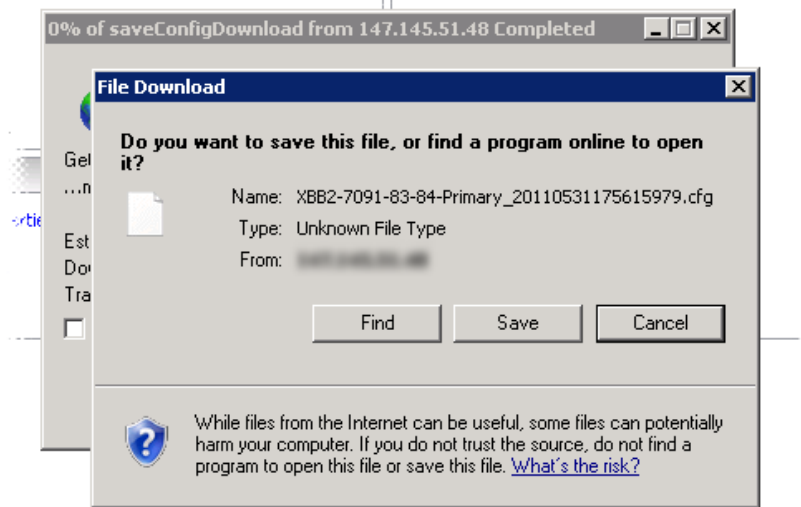


**5** Click **Save**

A Save As dialog box will be displayed.  See Figure 19.

**Figure 19.  Save As Dialog Box**



**6** Select the location and file name to save the backup configuration script as.

**7** Click **Save**

# 4

# ESX Host SAN Configuration
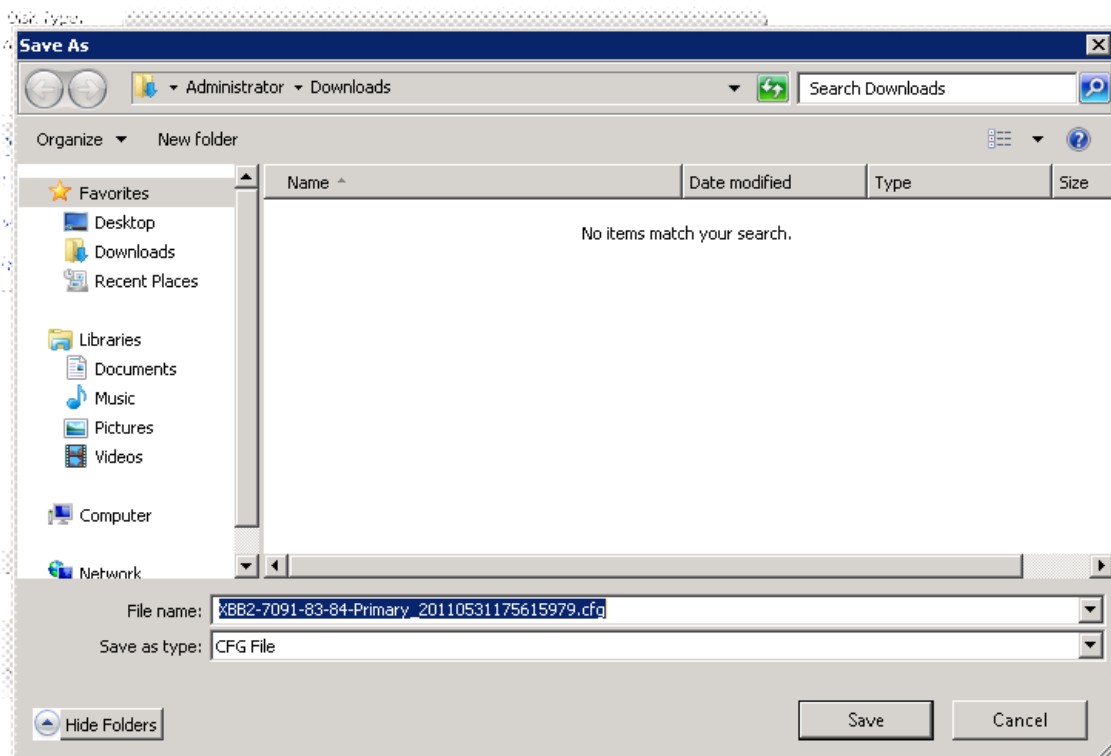
This vCenter Plug-in allows for an ESX host to be automatically configured to use a Dell MD Storage Array by detecting the installed Host Bus Adapters (HBAs) within the ESX host and configuring new hosts on the storage array with the Worldwide Names (WWNs) of the HBAs from the ESX host. The default ESX multipathing mode for Dell MD Storage Arrays is Most Recently Used (MRU). To ensure optimum performance for the ESX host with more than two HBAs, the ESX host should be configured to use the storage array in pairs of HBAs. This method allows for the maximum I/O throughput from the ESX host to the storage array. Using this method requires proper SAN configuration and balancing of LUNs between hosts/host groups. *Figure 20* shows a properly configured two HBA port ESX host SAN configuration utilizing two fabric switches and a dual controller storage array.

**Figure 20.  Dual Port HBA Configuration**
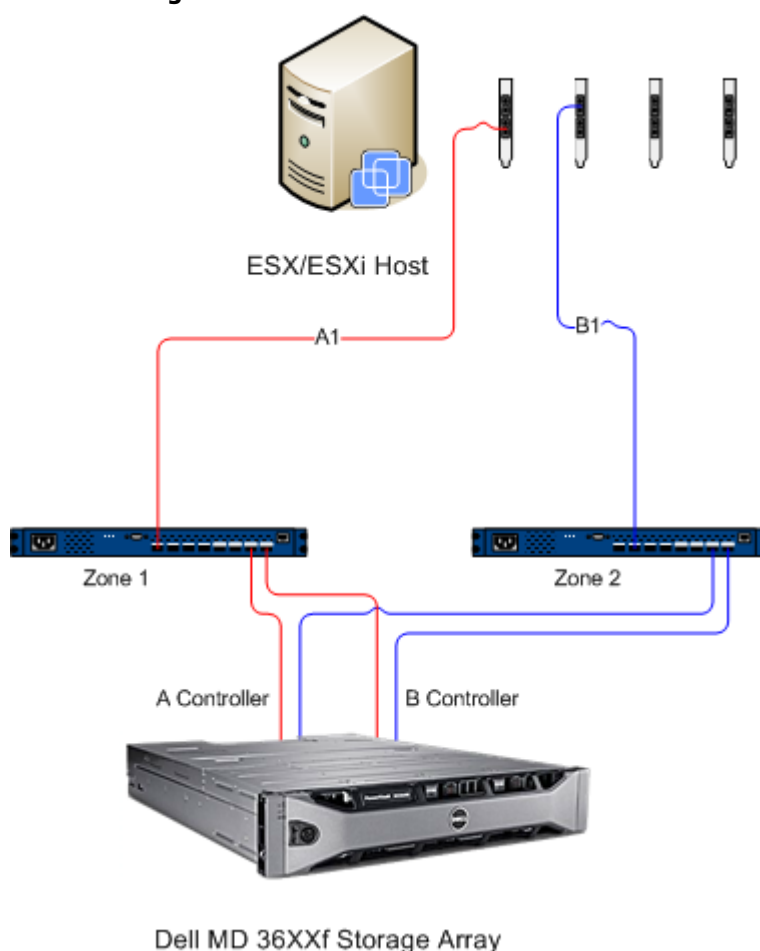
This example shows a fully redundant fabric configuration. If an FC switch or HBA fails, *Figure 21* the alternate switch still connects to both storage controllers in the storage array. If a storage controller also fails *Figure 22*, the ESX host can still access the remaining controller, and all virtual disks fail over to that controller. A complete loss of access to storage occurs if any other element fails.
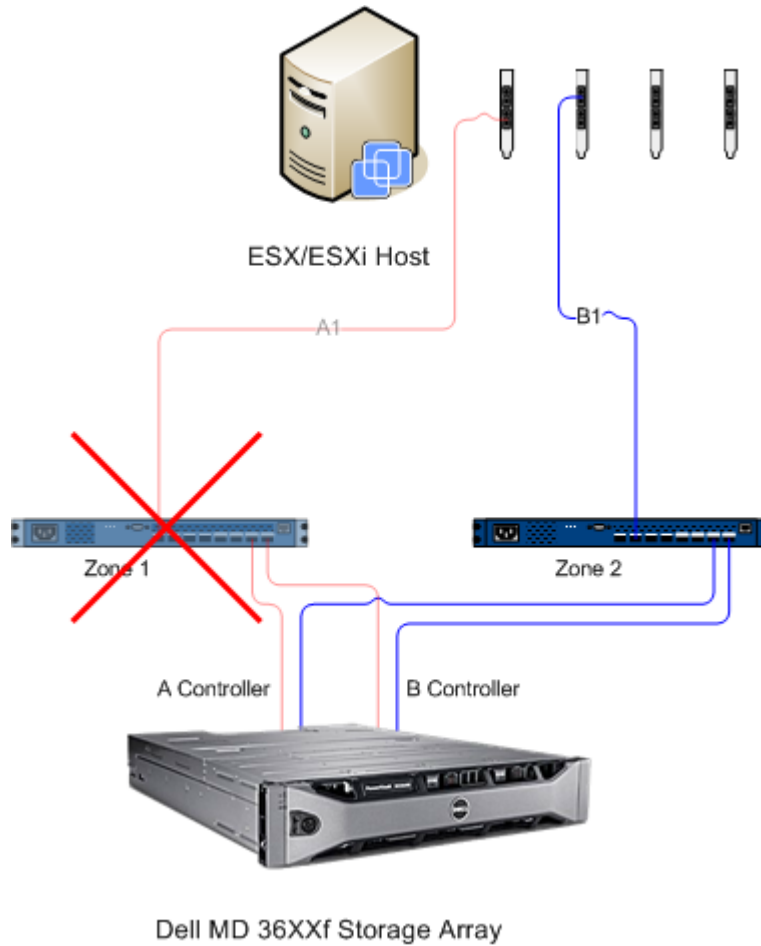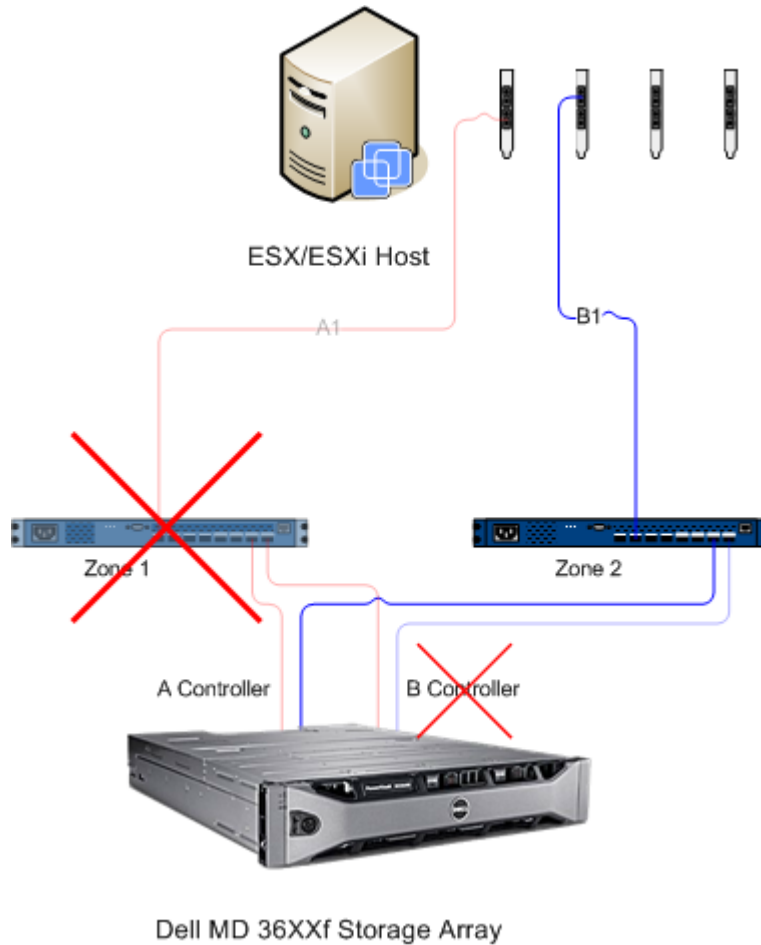
**Figure 21.  Single Failure**



Dell MD 36XXf Storage Array

**Figure 22.  Double Failure**



Dell MD 36XXf Storage Array

This method works well to maintain the in-case of a hardware failure; however, MRU only maintains one active path for each HBA group. Therefore, if you have an ESX host with four HBAs, only one HBA is active at a time. To achieve higher I/O throughput from the ESX host to the storage array, it is recommended that you group the HBAs in pairs and create virtual hosts for each pair of HBAs. This allows for a fully redundant configuration but also allows for two of the HBAs to be active at the same time versus a single HBA. See *Figure 23*. From the storage array, the second pair of HBAs is defined as a separate host and virtual disks can then be mapped directly to the new host or host group. This same methodology can be used to group additional HBAs in the same manner. This does require additional management to balance the LUNs between the hosts/host groups to fully use the fibre channel bandwidth between all HBA groups. When this method is used in the array, the Automatic ESX host configuration utility cannot determine which HBAs are configured to each zone in the and the user must verify that a single HBA is connected to both fabric zones for each HBA pair group.

**Figure 23.  Quad HBA Port Configuration**



Dell MD 36XXf Storage Array
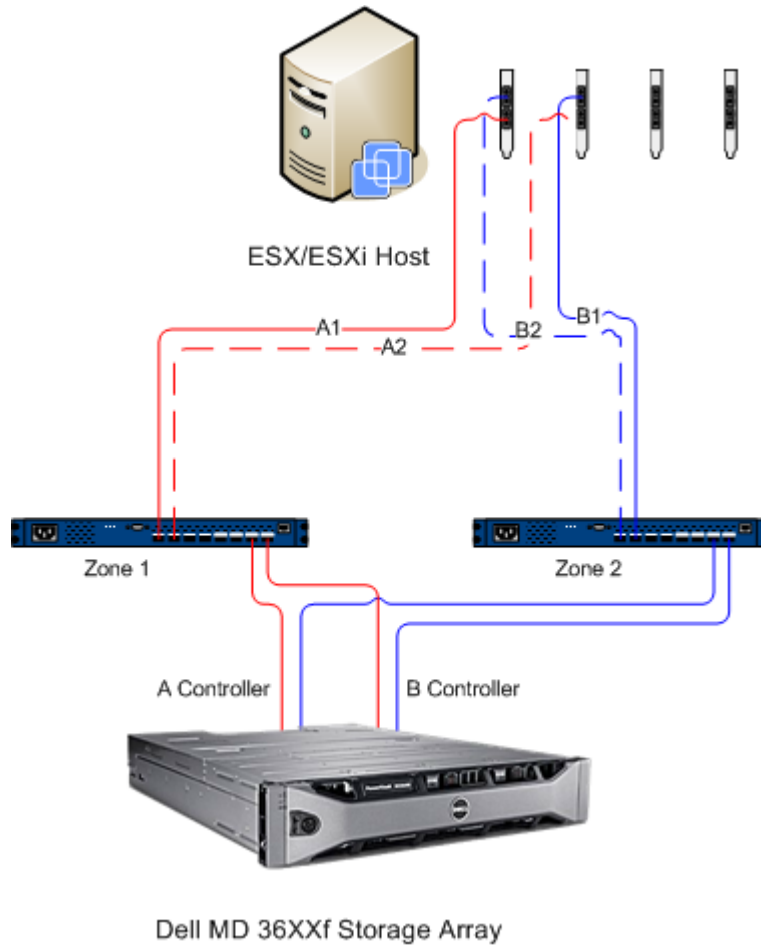
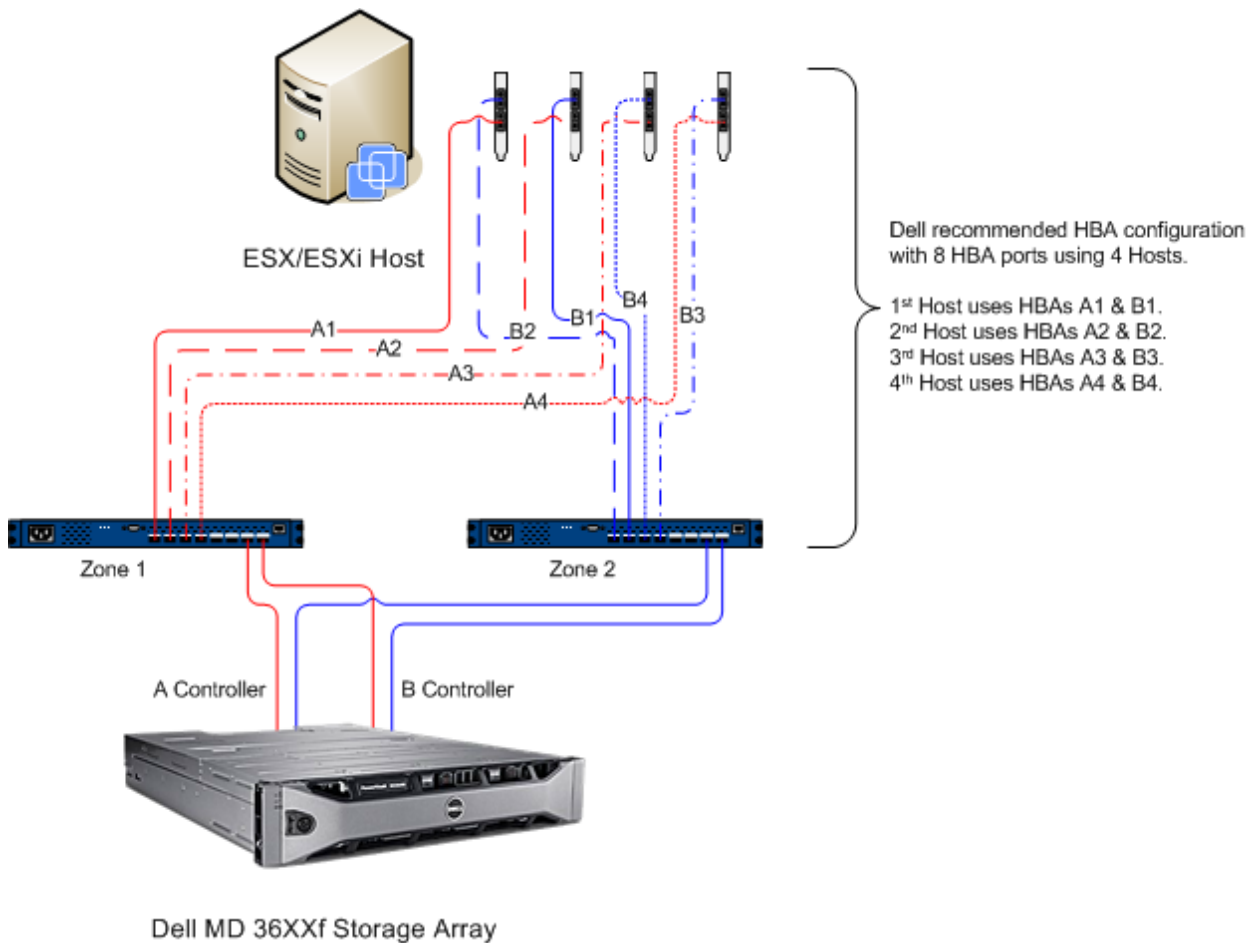📝 **NOTE:** The intent of this configuration is to pair the HBAs so that no group of HBA ports would be contained on a single HBA card (if dual port cards are being used).

*Figure 24* shows how an 8 port HBA configuration can be configured.

**Figure 24.  8 HBA Port Configuration**



## Networking Configuration for Software iSCSI Storage

To configure the network for software iSCSI storage, create an iSCSI VMkernel port and map it to a physical network interface card (NIC) that handles iSCSI traffic. Depending on the number of physical NICs that you use for iSCSI traffic, the networking setup can be different.

### Connecting to a Dell MD3600i Storage Array with VMware ESX 4.1.0, 260247

The Dell MD3600i storage array is not currently listed in the VMware SATP driver and therefore requires the user to manually add the product ID to the SATP in-order to properly configure failover for the MD3600i storage array. This is accomplished with the following commands before mapping any virtual disks from the storage array to the ESX host.

From the ESX console, issue the following commands:

```
#esxcli nmp satp addrule –v DELL –M MD36xxi –s VMW_SATP_LSI
#esxcli nmp satp listrules |grep DELL
```

Ensure that Dell MD36xxi is listed in the output.

### Additional Information

For more information about network configuration for software iSCSI storage, refer to *iSCSI SAN Configuration Guide: Configuring iSCSI Initiators and Storage: Setting Up Software iSCSI Initiators: Networking Configuration for Software iSCSI Storage* in the VMware® vSphere Online Library.

# 5

# ESX Host Configuration Wizard

To use the Automatic Host Configuration utility, navigate to Hosts and Clusters within the vSphere client and select the ESX host to be configured; Right select the ESX host, and select the Configure ESX Host to Storage Array option from the pull-down menu. See *Figure 25*.

**Figure 25.  ESX Host Configuration Wizard Menu**
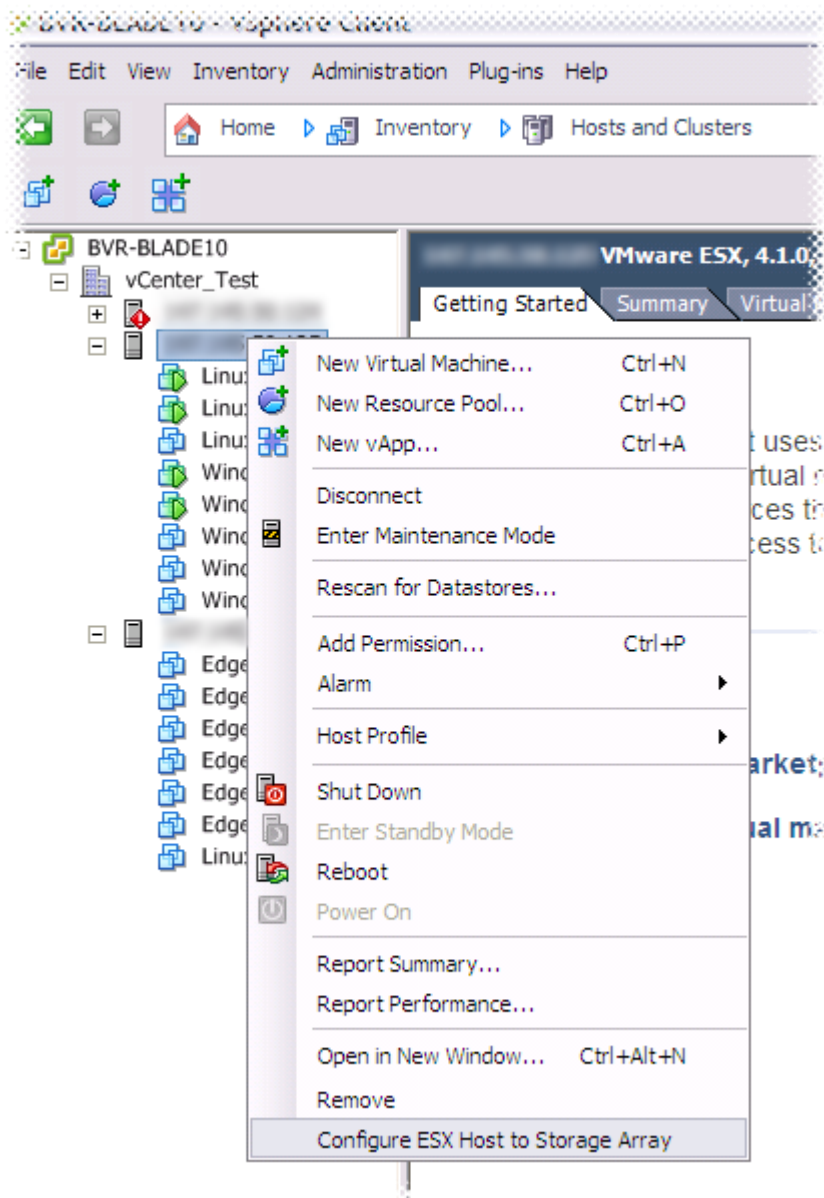
This launches the Configure ESX Host to Storage Array wizard. See Figure 26. From this wizard, you can see how the current ESX host is configured to the storage array (if it is already configured). You can also add a host or host group, rename a host or host group, remove a host or host group and automatically configure the ESX host to another storage array.

**Figure 26. FC Configure ESX Host to Storage Array Wizard**
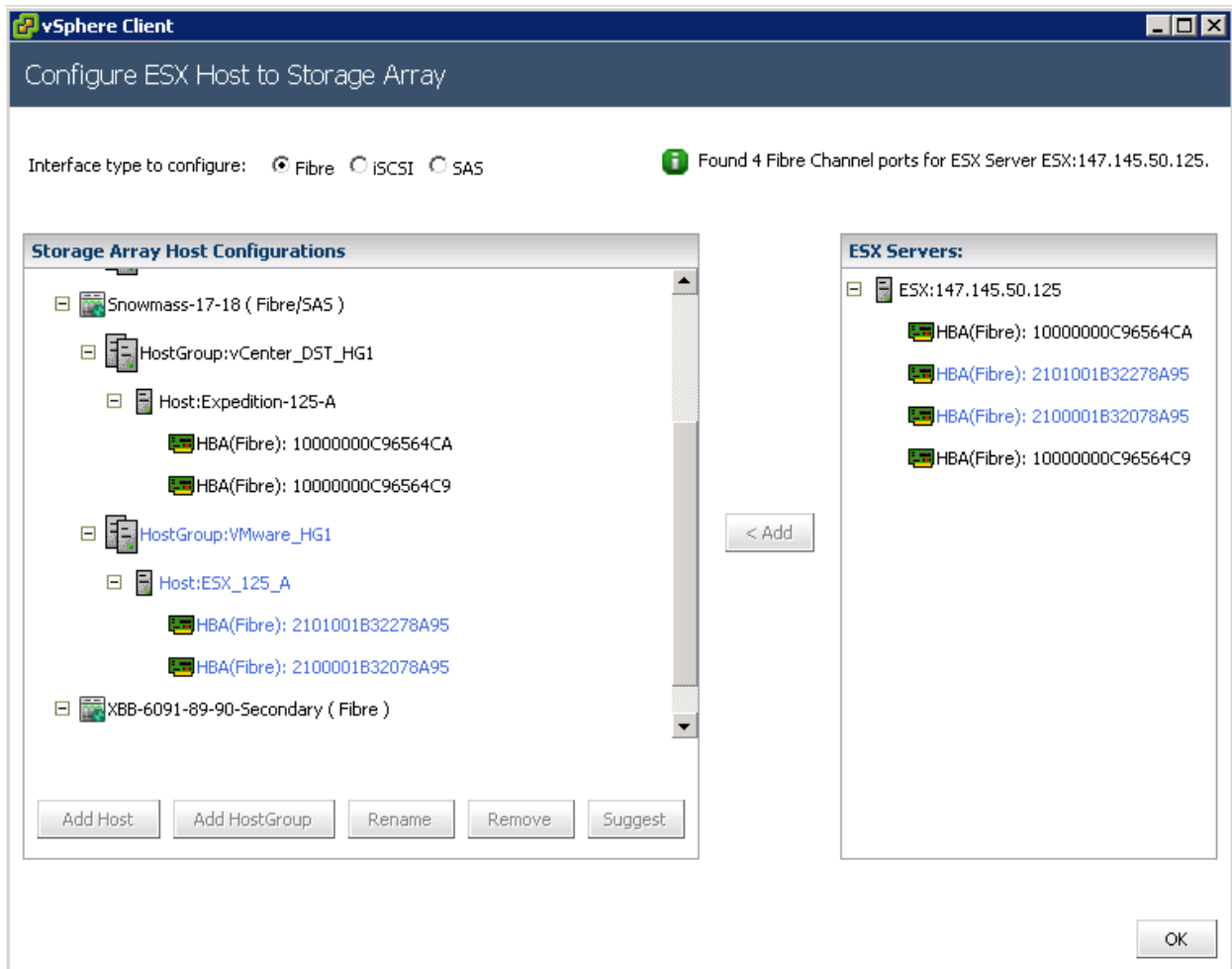


To automatically configure the ESX host to the Dell MD Storage Arrays, select the storage array to be configured, and click Suggest. This groups any unassigned HBA ports into pairs and define a new host and host group for the groups of HBAs Figure 26. When the suggested configuration is correct, click **OK** to apply the changes to the storage array or modify the configuration based on the fibre channel zoning rules from the previous ESX Host SAN Configuration section. Suggested changes will be shown in blue, the Rename and Remove options only apply to the uncommitted changes. You cannot rename or remote existing configured hosts or host groups. Existing host and host group configuration changes must be performed from MDSM.

The wizard displays progress while the requested configuration changes are being made. You must manually close the progress window once the changes are complete. See Figure 29.

**NOTE:** To use multiple host groups as described, the storage array must have the Storage Partitioning premium feature enabled.

**Figure 27.  iSCSI Configure ESX Host to Storage Array View**
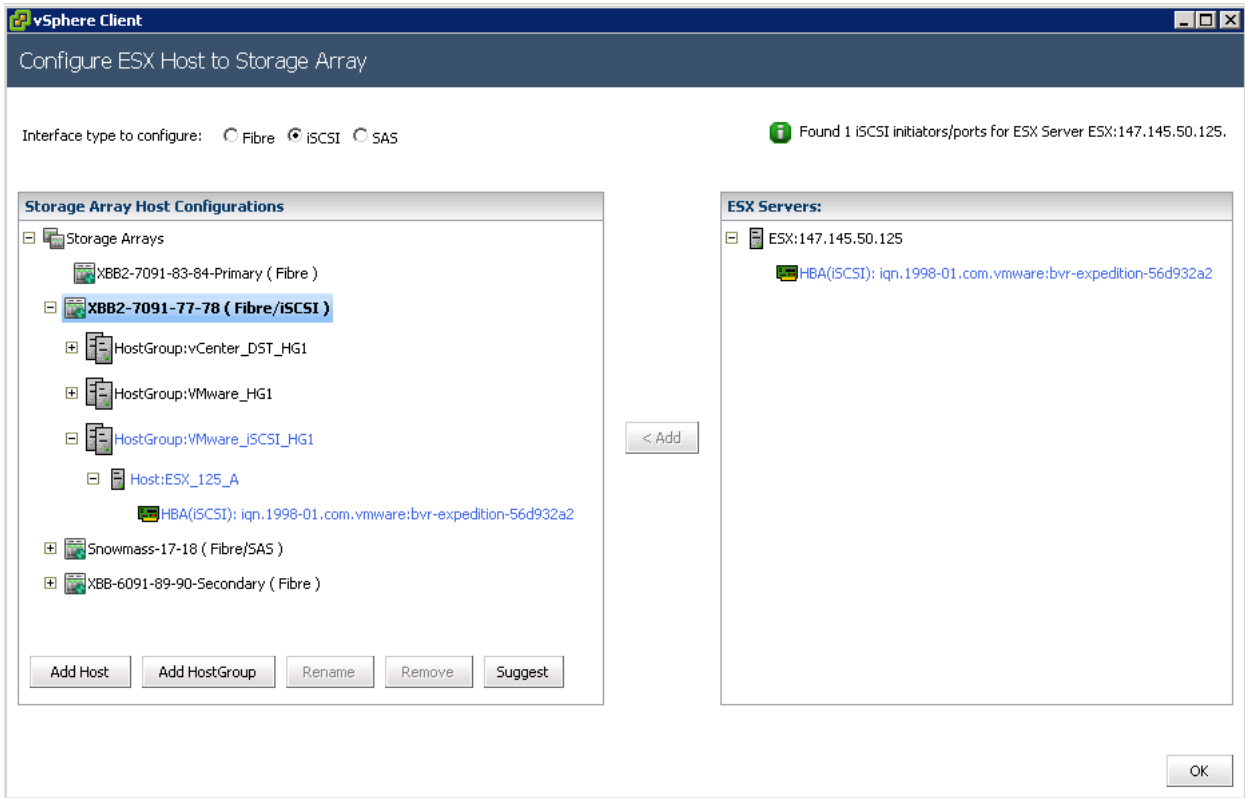


**Figure 28.  SAS Configure ESX Host to Storage Array View**
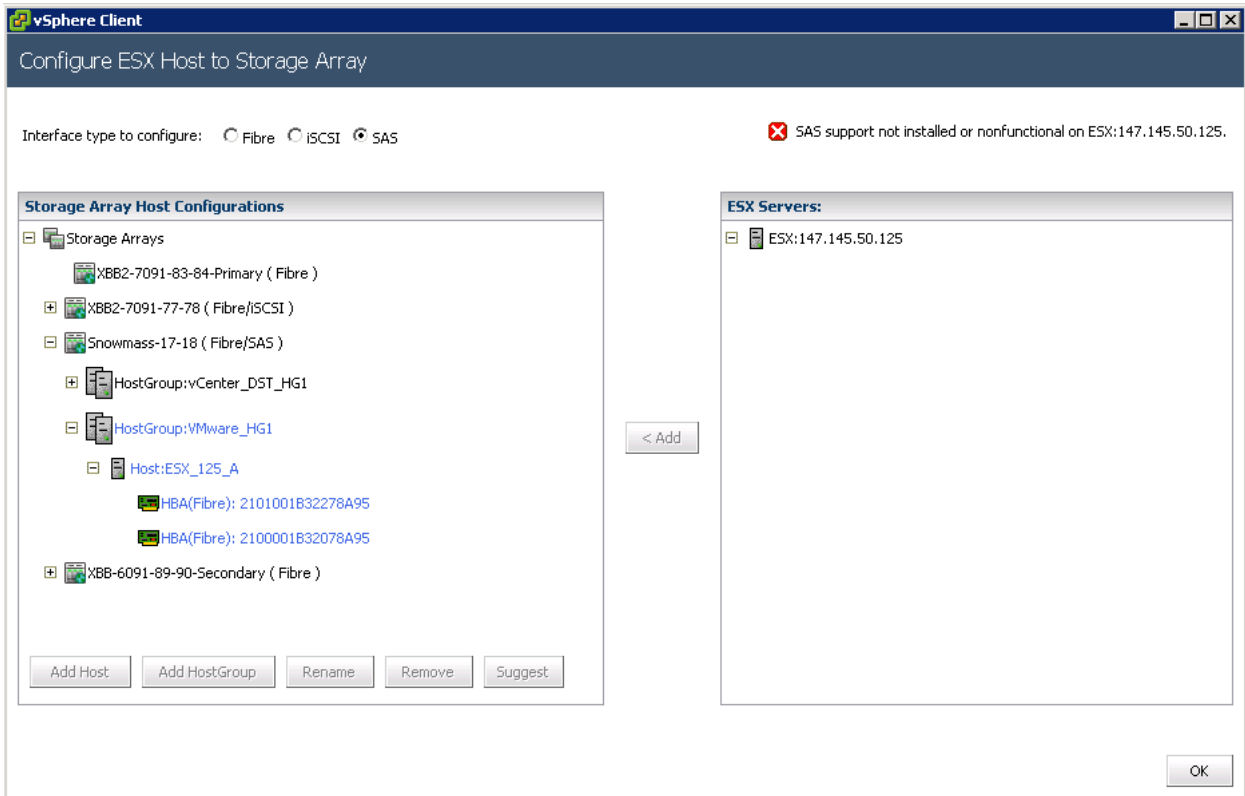
**NOTE:** To detect the SAS HBA addresses, the LSI SAS SMI-S provider must be upgraded to the version included with the install and as described in section *Installing the SAS Provider Upgrade*. When the provider is not upgraded, the list of address does not appear and the icon above the servers will be red. See Figure 28.

**Figure 29.  Commit Changes**



The ESX host has now been configured to the storage array. The next step is to create new virtual disks on the storage array to be used by the ESX host. New virtual disks are created using the vCenter Plug-in.

# Storage Array Summary

**Clicking on a storage array from the array manager view displays a summary of the selected storage array. See Figure 30. This includes information on the status of the storage array, the number of controllers, the number of failed controllers, the number of drive trays, number of physical drives, physical drive types, hot spares, and capacity usage. The storage array event log is also accessible from this tab by clicking on the View Event Log link. See section Figure 43. Datastores View**
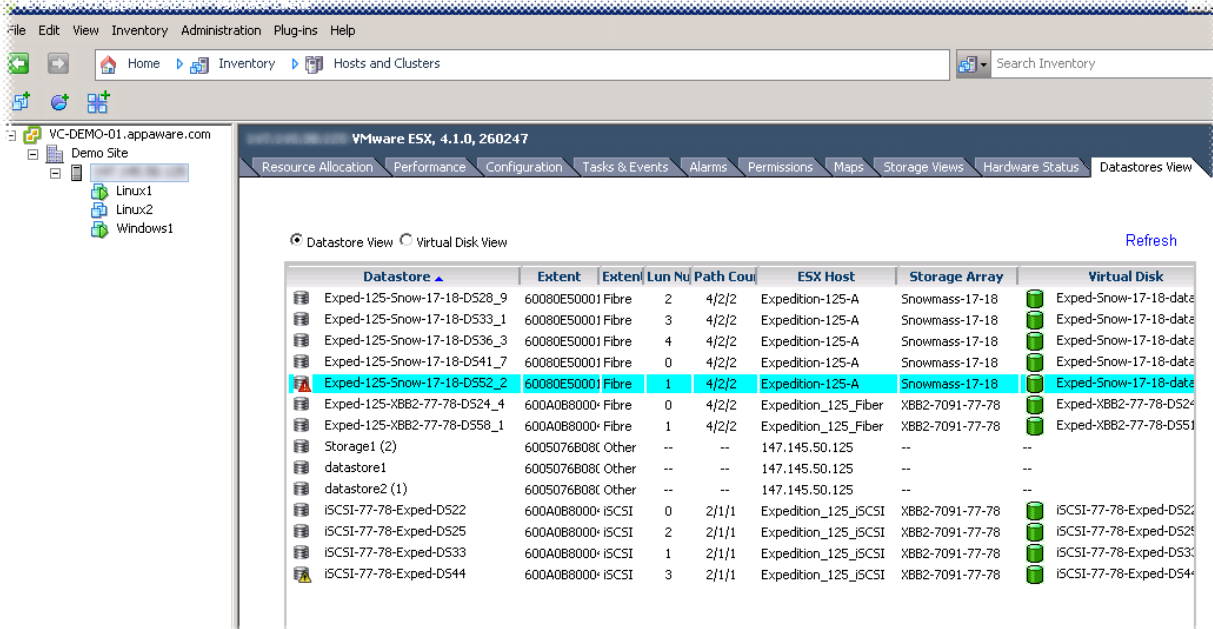


Storage Array Event Log for additional event log details.

**Figure 30  Storage Array Summary**
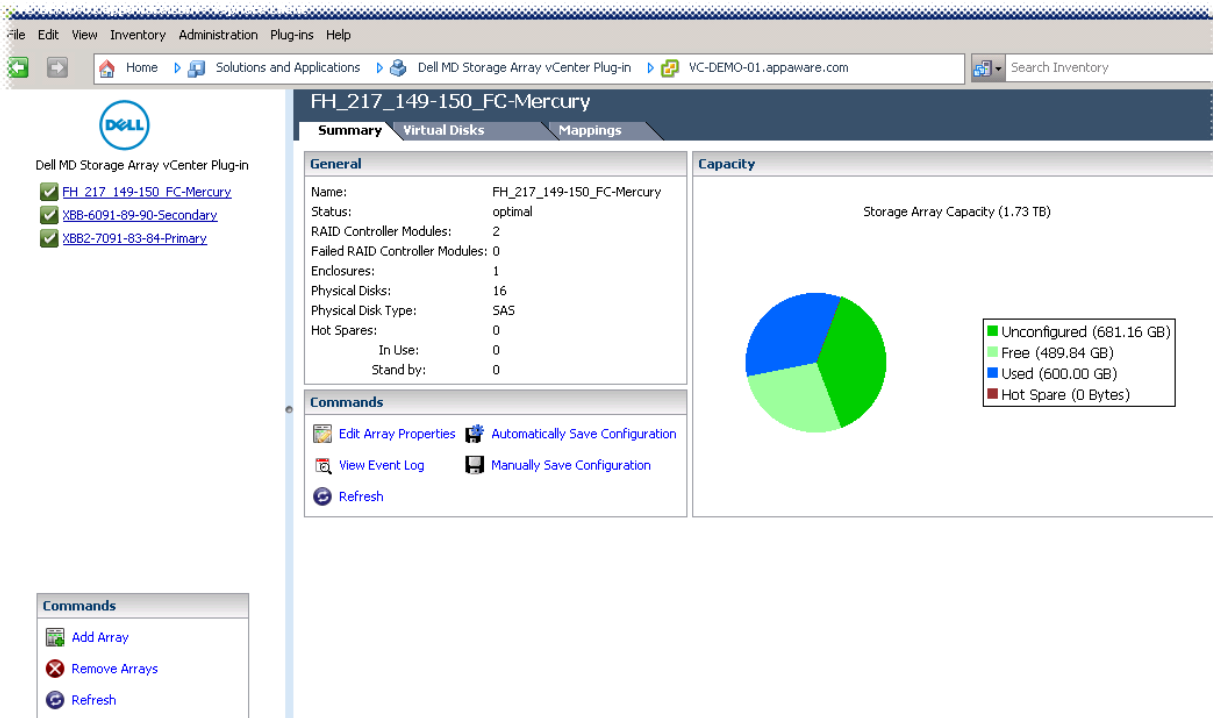
# Create Disk Group

Selecting the Virtual Disks tab shows a logical view that displays how storage capacity is allocated. This view also allows you to create new disk groups and virtual disks. Additionally, existing virtual disks and disk groups can be modified or deleted here. To create a new disk group, click Create Disk Group.

**Figure 31. Storage Array Virtual Disks**
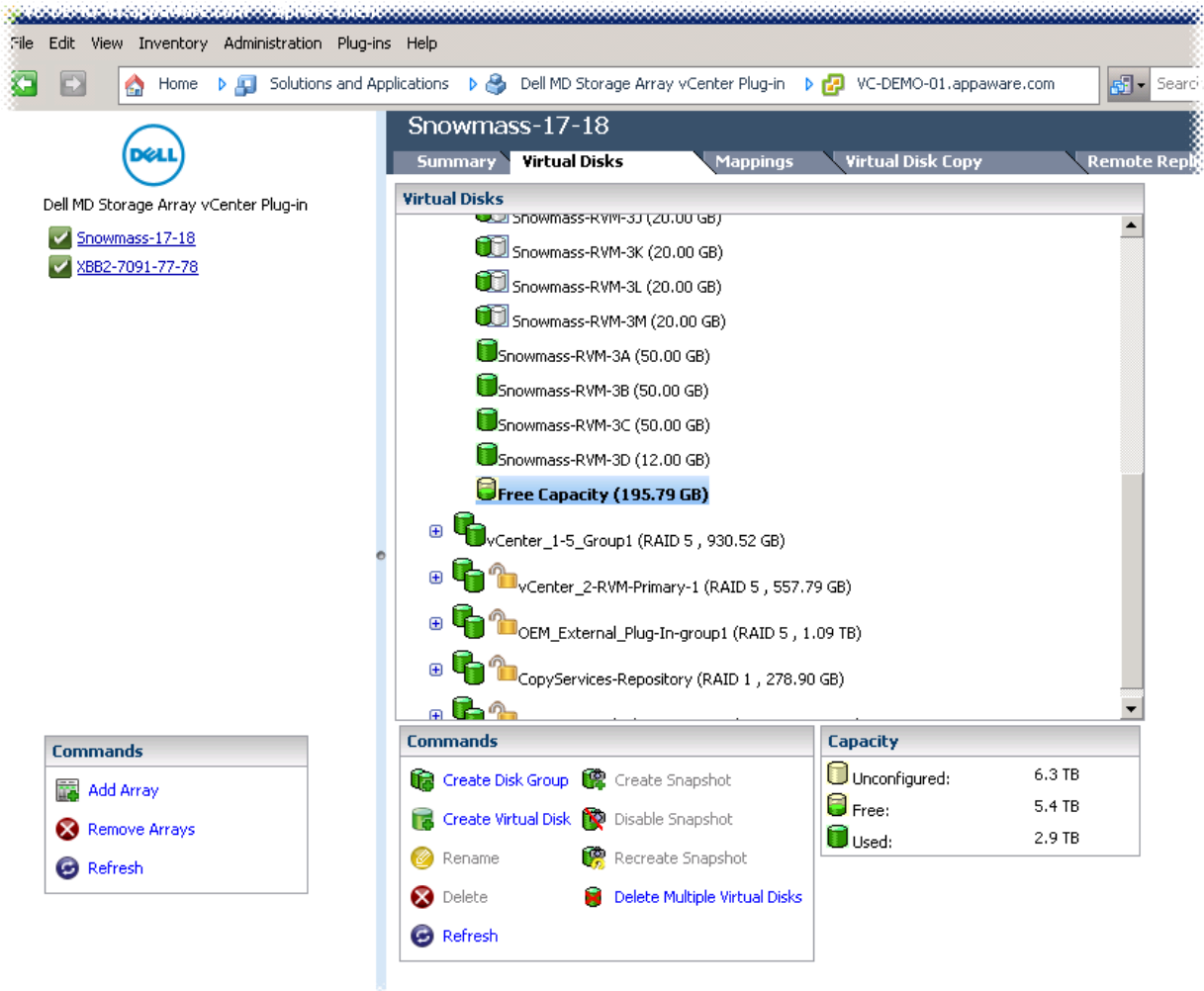


The Create Disk Group link launches a wizard to walk you through creating a new disk group (Figure 26). During this process, you must choose from the available free drives, the drives that make up the new disk group, and select the RAID level to be used.

**Figure 32.  Create Disk Group Dialog Box**
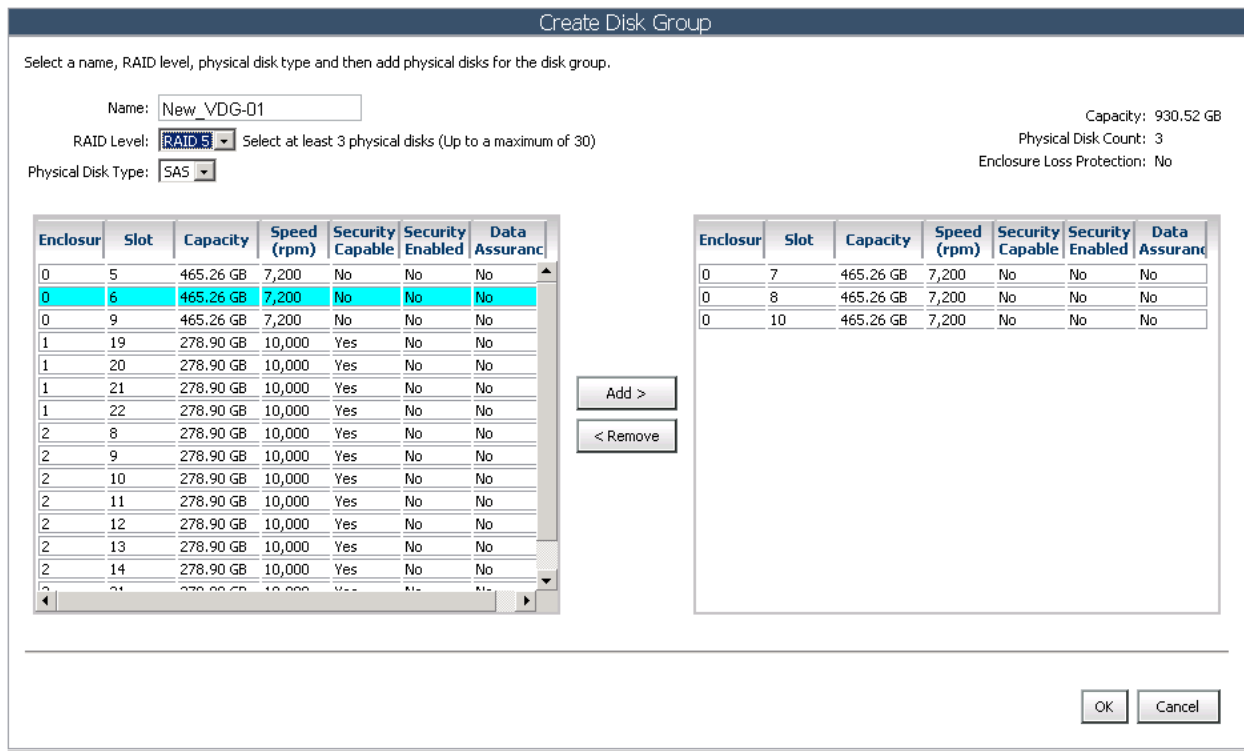


## Formatting Virtual Disks

Before you format virtual disks with VMFS datastores, you must plan how to set up storage for the ESX/ESXi systems, including deciding on the number of virtual disks to use and the size of the virtual disks.

> **NOTE:** For more information about making virtual disk decisions, including predictive schemes, adaptive schemes, and disk shares, refer to the *iSCSI SAN Configuration Guide: Using ESX/ESXi with an iSCSI Storage Area Network: Making LUN Decisions* in the VMware® vSphere Online Library.

- When you are deciding how to format the virtual disks, keep in mind the following considerations:
    - Make sure that each virtual disk has the correct RAID level and storage characteristics for applications in the virtual machines that use that virtual disk. Make sure that each virtual disk contains only one VMFS datastore.
    - When multiple virtual machines access the same VMFS datastore, use disk shares to prioritize virtual machines.
- Fewer, larger virtual disks are appropriate for the following reasons:
    - More flexibility to create virtual machines without asking the storage administrator for more space.
    - More flexibility for resizing virtual disks, doing snapshots, and so on.
    - Fewer VMFS datastores to manage.
- More, smaller virtual disks are appropriate for the following reasons:
    - Less wasted storage space.
    - Different applications might need different RAID characteristics.
    - More flexibility, as the multipathing policy and disk shares are set per virtual disk.
    - Use of Microsoft Cluster Service requires that each cluster disk resource is in its own virtual disk.
    - Better performance because there is less contention for a single virtual disk.

# Decision-Making Schemes

When the storage characterization for a virtual machine is not available, you can use either the predictive scheme or the adaptive scheme to decide on the virtual disk size and number of virtual disks to use.

## Using the Predictive Scheme to Make virtual disk Decisions

**1** Create several virtual disks with different storage characteristics.

**2** Build a VMFS Datastore on each virtual disk. Label each Datastore according to its characteristics.

**3** Allocate virtual disks to contain the data for virtual machine applications in the VMFS datastores built on virtual disks with the appropriate RAID level for the applications' requirements.

**4** Use disk shares to distinguish high-priority virtual machines from low-priority virtual machines.

**NOTE:** Disk shares are relevant only within a given host. The shares assigned to virtual machines on one host have no effect on virtual machines on other hosts.

**5** Run the applications to determine whether virtual machine performance is acceptable.

## Using the Adaptive Scheme to Make Virtual Disk Decisions

**1** Create a large virtual disk, such as RAID 1+0 or RAID 5, with write caching enabled.

**2** Build a VMFS datastore on that virtual disk.

**3** Place four or five virtual disks on the VMFS datastore.

**4** Run the applications to determine whether disk performance is acceptable.

- If performance is acceptable, you can place additional virtual disks on the VMFS datastore.

- If performance is not acceptable, create a new, larger virtual disk, and repeat the process. You can use a different RAID level. Use migration so that you do not lose virtual machines when you re-create the virtual disk.
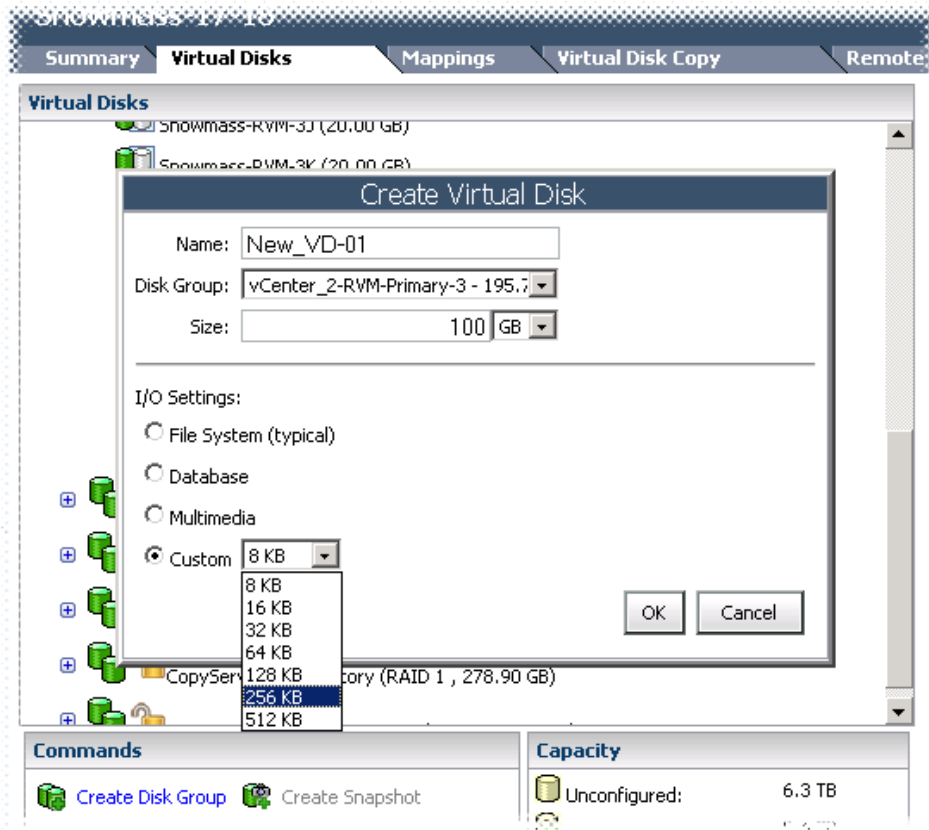
# Creating a Virtual Disk

After a new disk group was created, you can create new virtual disks from the free capacity in the disk group. To create a new virtual disk, perform these steps:

1 Click **Create Virtual Disk** link.

The Create Virtual Disk wizard appears. See Figure 33

**Figure 33. Create Virtual Disk Dialog Box**



2 In the Name text box, type the virtual disk name.

3 From the Disk Group drop-down list, select the disk group to use for the new virtual disk.

4 In the Size text box, type the size of the new virtual disk, and select the rate from the drop-down list.

5 In the I/O settings area, select the I/O characteristics of the virtual disk.

6 Click **OK** to create the virtual disk.

# Snapshots Premium Feature

When the Snapshots premium feature is enabled on the storage array, these additional options are available in the Commands area:

- Create Snapshot – Create a new snapshot of a base virtual disk.
- Disable Snapshot – Disable the snapshot of a base virtual disk.
- Recreate Snapshot – Re-create a disabled snapshot.
- Delete – Delete a snapshot of a virtual disk.

### Creating a Snapshot of a Base Virtual Disk

1 Highlight the base virtual disk, and click Create Snapshot in the Command area.

The Snapshot wizard appears.

**Figure 34.  Create Snapshot Dialog Box**
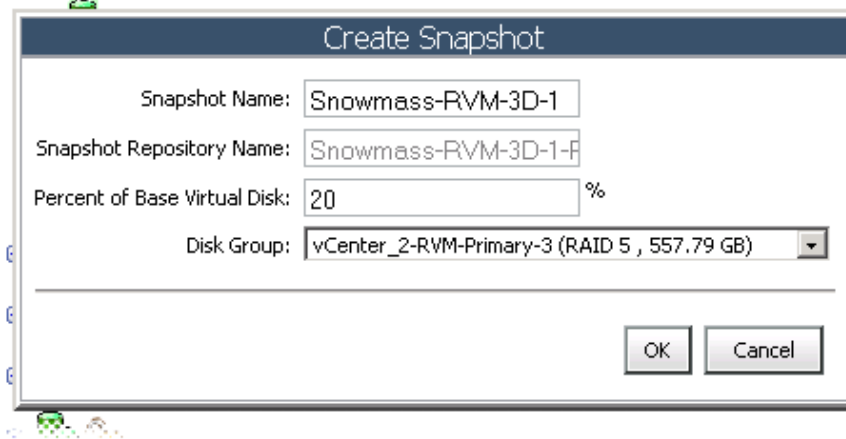


2    Change one or more of the snapshot attributes:

- Snapshot Name – the name of the new snapshot virtual disk.
- Snapshot Repository Name – the name of the new repository virtual disk.
- Percent of Base Virtual Disk – the percentage of the base virtual disk to use for the repository.
- Disk Group – the name of the disk group in which to place the repository virtual disk.

📝 **NOTE:** After the size of the snapshot exceeds the percentage of the base virtual disk, the snapshot fails. The snapshot is no longer available for use until it is re-established by re-creating it. See Re-creating a Snapshot.

## Disabling a Snapshot

To temporarily deactivate a snapshot so that it can be used again later, highlight the snapshot virtual disk in the Virtual Disks tree, and click Disable Snapshot in the Command area. The snapshot process stops, but the relationship remains between the snapshot and the base virtual disk and the repository virtual disks.

## Re-creating a Snapshot

To re-establish a deactivated snapshot, click Recreate Snapshot in the Commands area. A new copy of the base virtual disk that can be used as the snapshot is created.

📝 **NOTE:** Re-creating a snapshot disables the original snapshot before the new snapshot is created.

## Deleting a Snapshot

Select the snapshot virtual disk in the Virtual Disks tree, and click Delete in the Commands area.

# Creating a Virtual Disk Copy

When the Virtual Disk Copy premium feature is enabled on a storage array managed by the vCenter Plug-in, the Virtual Disk Copy tab appears next to the Mappings tab. This tab allows the management of virtual disk copies on the selected storage array. See Figure 35.
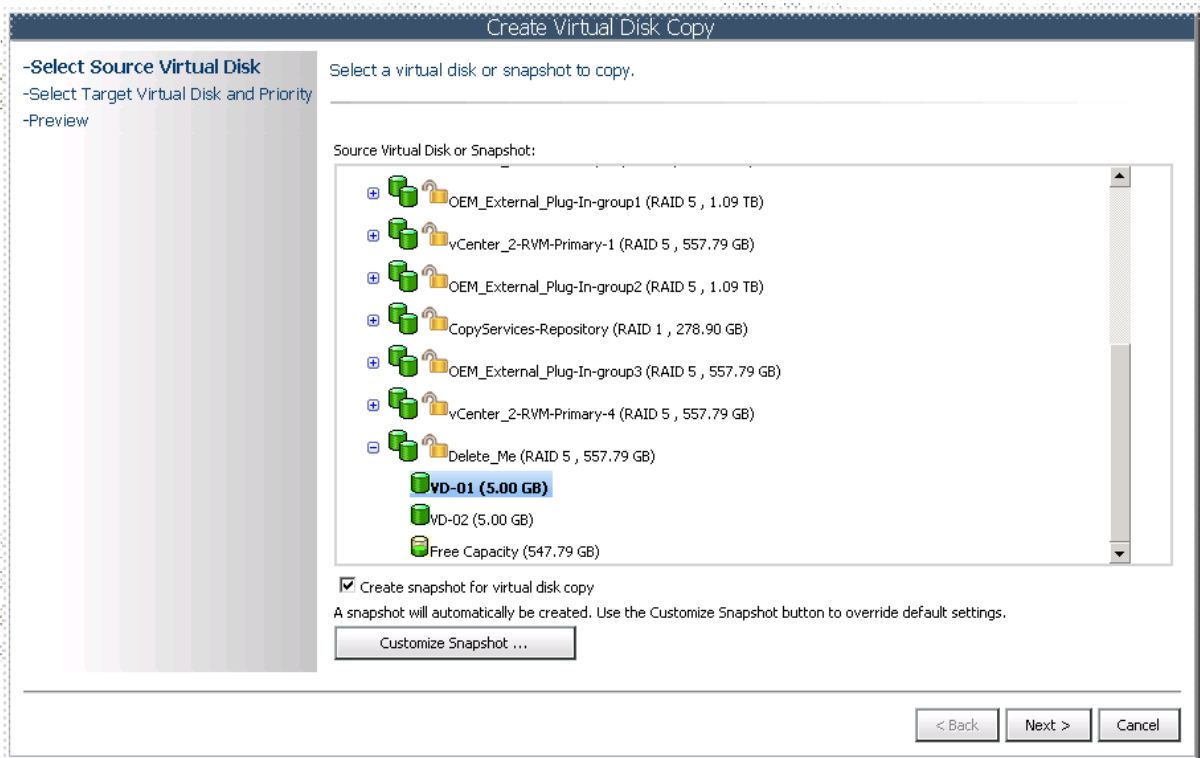
**Figure 35.  Virtual Disk Copy Management**
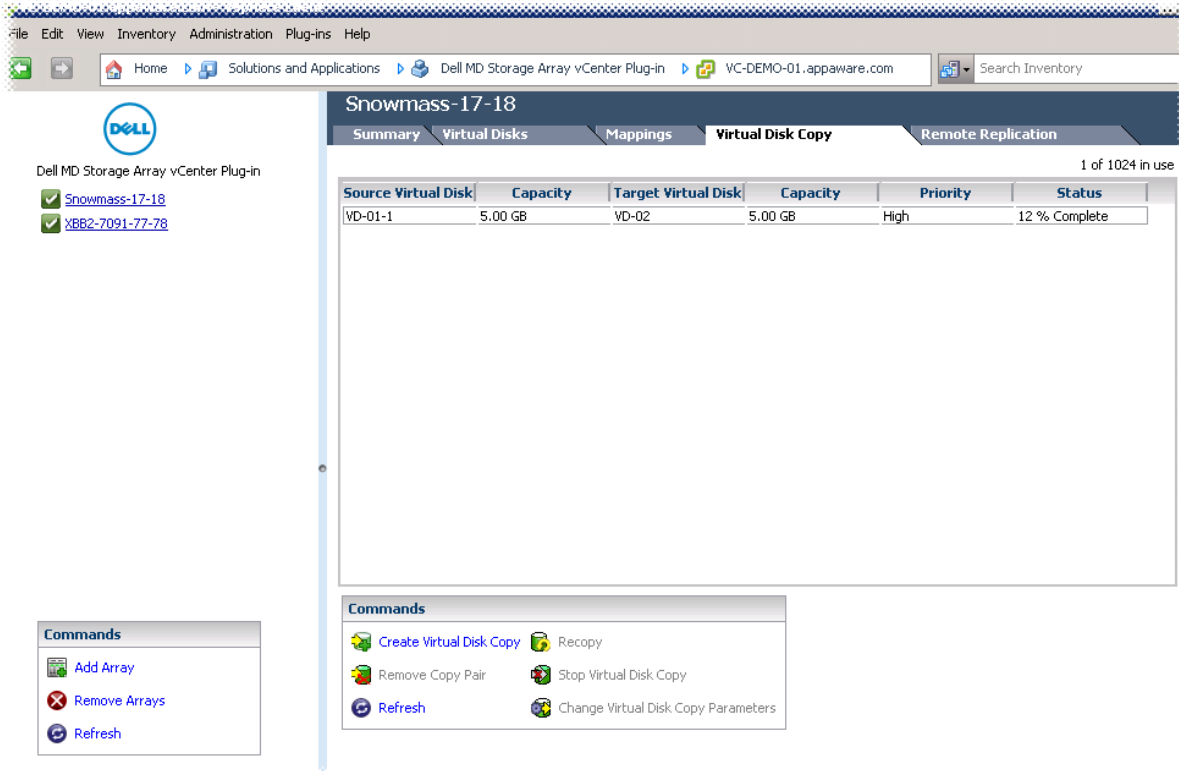


From this tab, all virtual disk copy operations are displayed along with the current status of all virtual disk copies. From the Commands area, the following options are available: Create Virtual Disk Copy, Recopy, Stop, Change Virtual Disk Copy Parameters, Remove Copy, and Refresh. To create a new virtual disk copy, click Create Virtual Disk Copy in the Commands area, which launches the Virtual Disk Copy wizard. From this wizard, select the source virtual disk to use for the virtual disk copy.

> **NOTE:** While the virtual disk copy is being established, the source virtual disk is read-only to the host to which the virtual disk copy is presented. When the Snapshot premium feature is enabled, the vCenter Plug-in uses the feature to create a snapshot of the source virtual disk before the virtual disk copy is initiated and the virtual disk copy operation uses the snapshot virtual disk to establish the virtual disk copy with. This allows for continued read-write operations to the source virtual disk from the host during the establish period.

**Figure 36.  Create Virtual Disk Copy Dialog Box**



**1**    Click Next to select the target virtual disk for the virtual disk copy and select the copy priority to use.

**Figure 37.  Virtual Disk Copy Target Dialog Box**
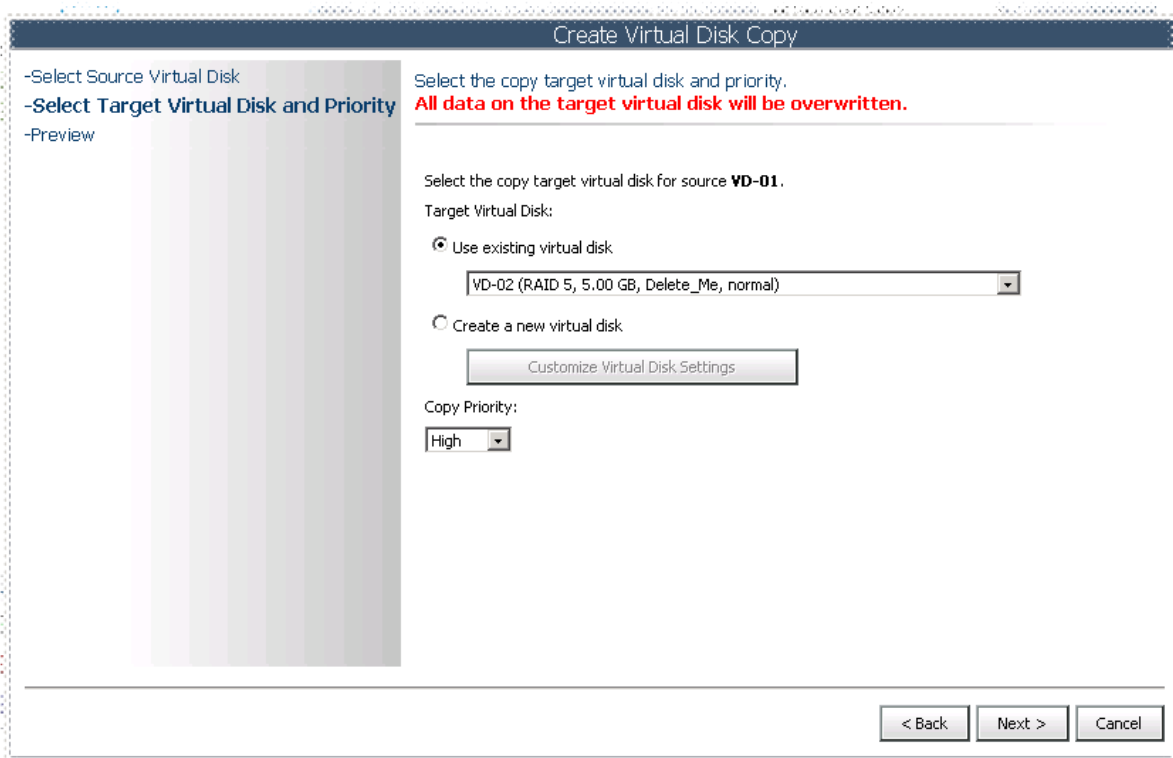
After the virtual disk copy is established, it can be managed from the Virtual Disk Copy tab. To stop a copy operation that is occurring, select the copy set to modify and click Stop in the Commands area. To recopy an existing in the , click the copy set, and click the Recopy link. To delete a copy set, select the copy set to modify, and click the Remove Copy link. This removes the virtual disk copy relationship between the two virtual disks, but does not modify or delete the target virtual disk that still contains a copy of the original data from the source virtual disk.

# Remote Replication

When the Remote Replication premium feature is enabled on the storage array, the Remote Replication tab appears within the vCenter Plug-in. From this tab, existing remote replication pairs are displayed along with the Commands area which allows for creation of new replication pairs, suspending an existing replication pair, resuming a replication pair, removing a replication pair, testing replication communications, or change replication parameters.
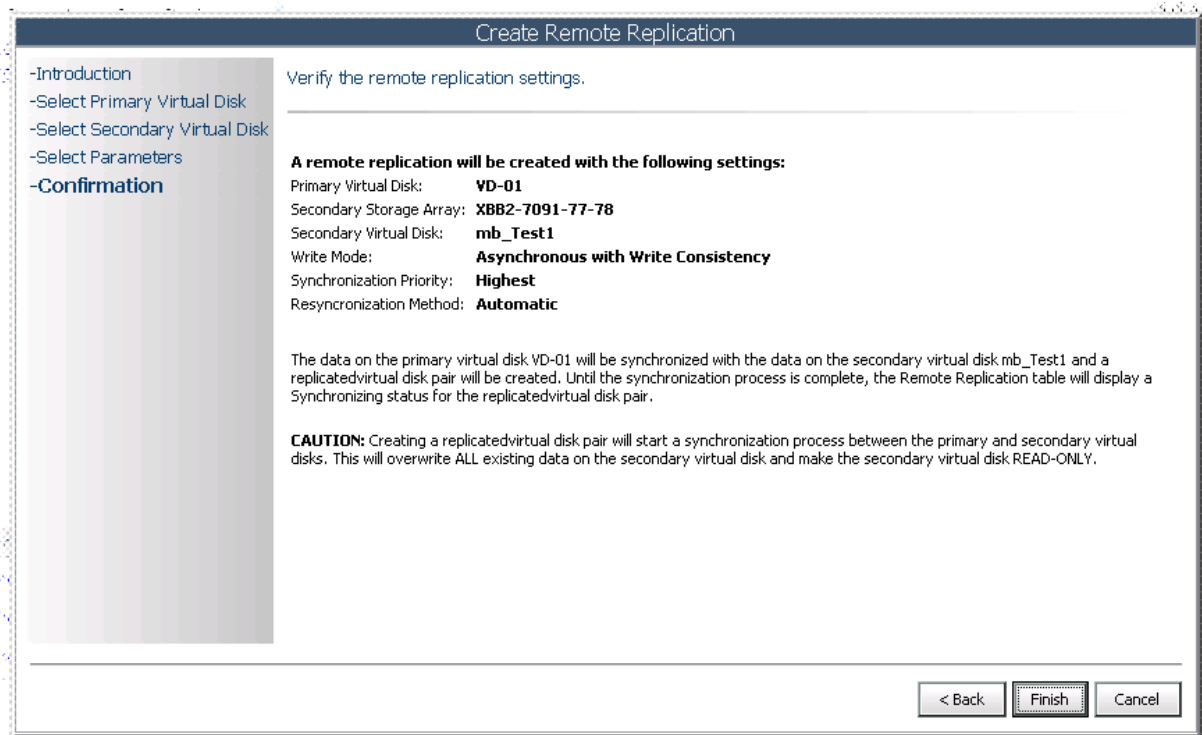
**Figure 38.  Remote Replication View**
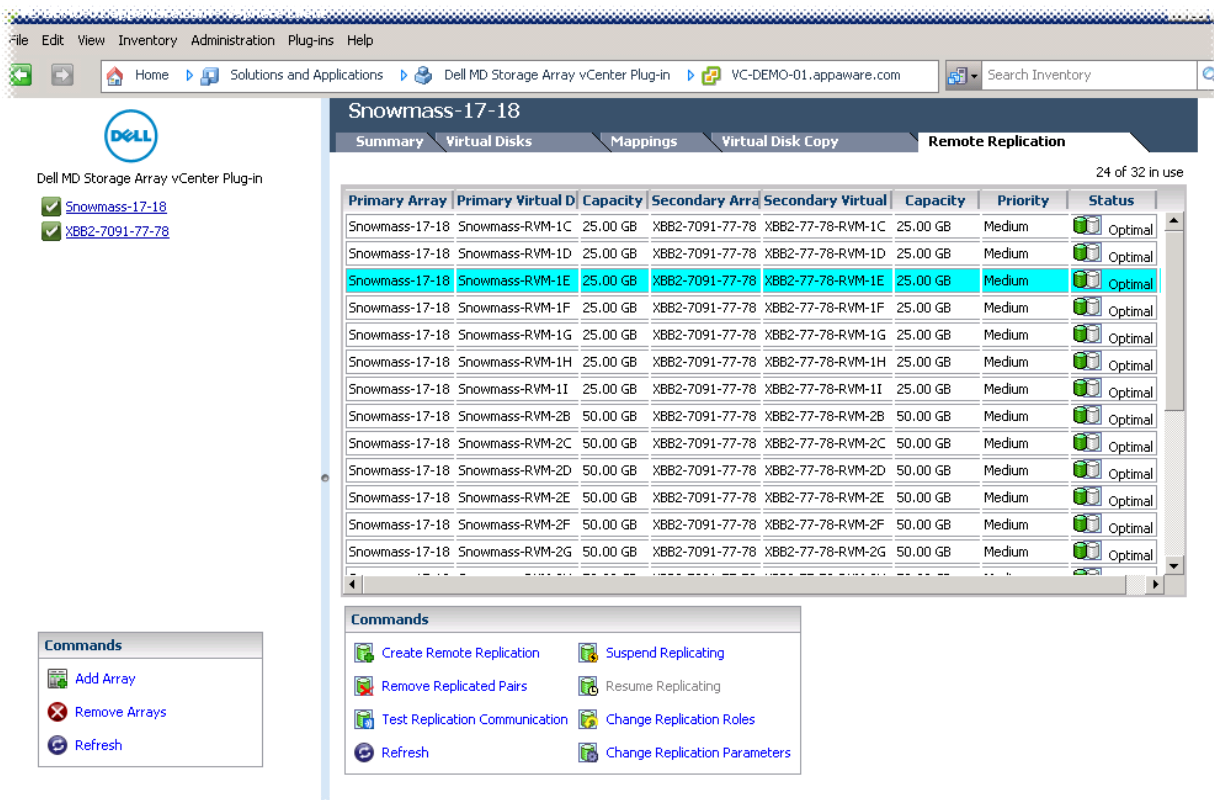


## Create Remote Replication Procedure

The following procedure details the steps required to create a remote replication using the vCenter Plug-in.

> **NOTE:** To create a remote replication, both storage arrays (local and remote) must be added to the array manager view.  See Figure 14**.**

1   From the Remote Replication tab, click the **Create Remote Replication** link.

2   Click **Next** after reading the introduction wizard page.

3   From the Virtual Disk tree view, select the source virtual disk for the mirror relationship and click **Next**.

4   Select the remote storage array for the mirror.

5   From the drop-down list, select the secondary virtual disk to be the target of the source remote replication.

6   Choose the write mode for the remote mirror and click **Next**.

7   Review the summary information on the Confirmation page and click **Finish** to establish the mirror relationship.  See Figure 39.

**Figure 39.  Remote Replication Confirmation Dialog Box**



Create Remote Replication

-Introduction
-Select Primary Virtual Disk
-Select Secondary Virtual Disk
-Select Parameters
**-Confirmation**

Verify the remote replication settings.

**A remote replication will be created with the following settings:**
Primary Virtual Disk:      **VD-01**
Secondary Storage Array:   **XBB2-7091-77-78**
Secondary Virtual Disk:    **mb_Test1**
Write Mode:                **Asynchronous with Write Consistency**
Synchronization Priority:  **Highest**
Resyncronization Method:   **Automatic**

The data on the primary virtual disk VD-01 will be synchronized with the data on the secondary virtual disk mb_Test1 and a replicatedvirtual disk pair will be created. Until the synchronization process is complete, the Remote Replication table will display a Synchronizing status for the replicatedvirtual disk pair.

**CAUTION:** Creating a replicatedvirtual disk pair will start a synchronization process between the primary and secondary virtual disks. This will overwrite ALL existing data on the secondary virtual disk and make the secondary virtual disk READ-ONLY.

[ < Back ]  [ Finish ]  [ Cancel ]

## Mapping a Virtual Disk

After creating new virtual disks, use the Mappings tab to present the virtual disks to the ESX host for use. See . From this view, you can manage hosts, host groups, and virtual disk mappings. To present a new virtual disk to an ESX host, click the Add Mapping link to start the Add Mapping wizard.

**Figure 40.  Virtual Disk Mapping View**
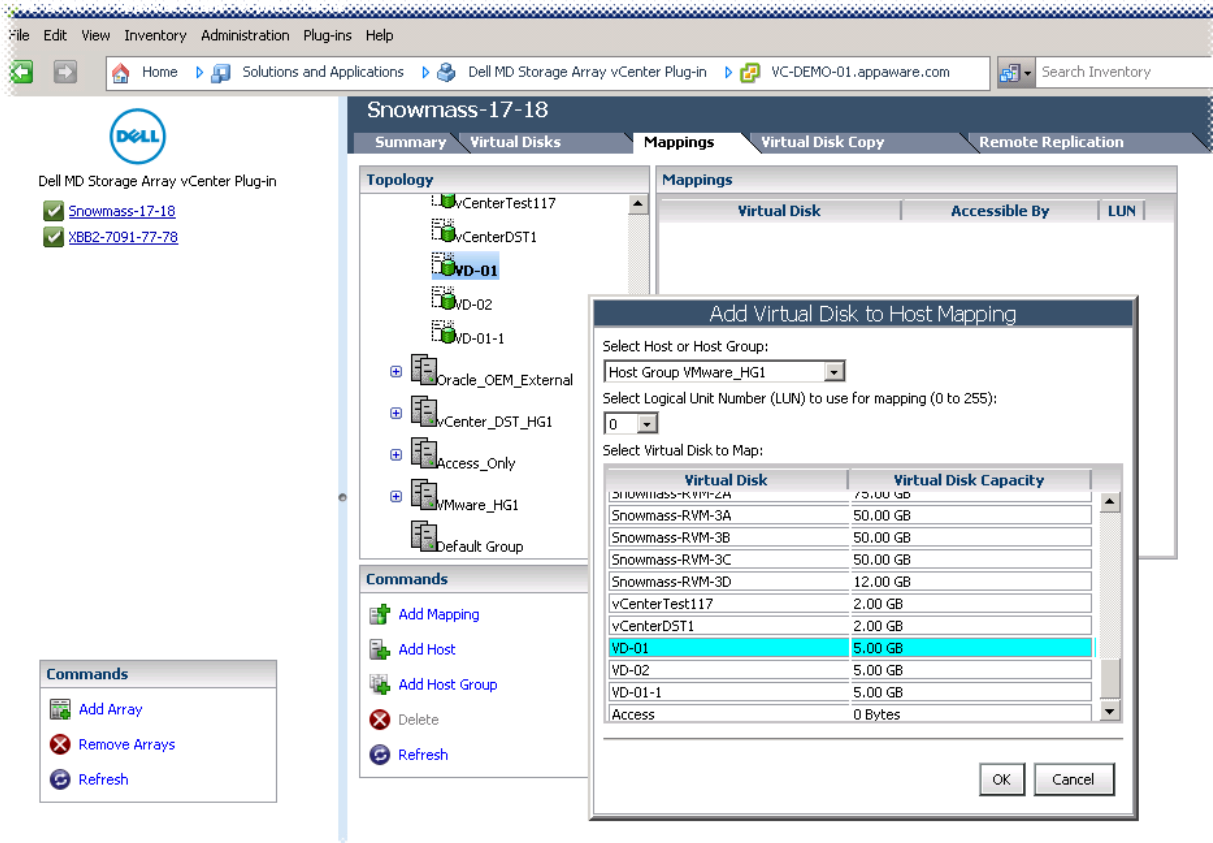


1   Select the host group or host to which to map the new virtual disk.

2   Select the virtual disk number to use and virtual disk to be mapped.

3   Click **OK**

📝  **NOTE:** When your storage array uses multiple groups of HBAs per ESX host, the new virtual disks should be balanced across all hosts/host groups. Do not add all the virtual disks to a single host/host group; no I/O balancing can occur in this case.

After the virtual disks have been mapped to the ESX host, the storage adapters on the ESX host must be rescanned to detect the new storage virtual disks. This action is accomplished from Hosts and Clusters view >> Configuration tab >> Storage Adapters for the ESX host being configured. See Figure 41.

📝  **NOTE:** You may need to run the Rescan, from vCenter, twice to detect all of the new storage virtual disks that have been mapped to the ESX host.

**Figure 41.  Storage Adapters Rescan**
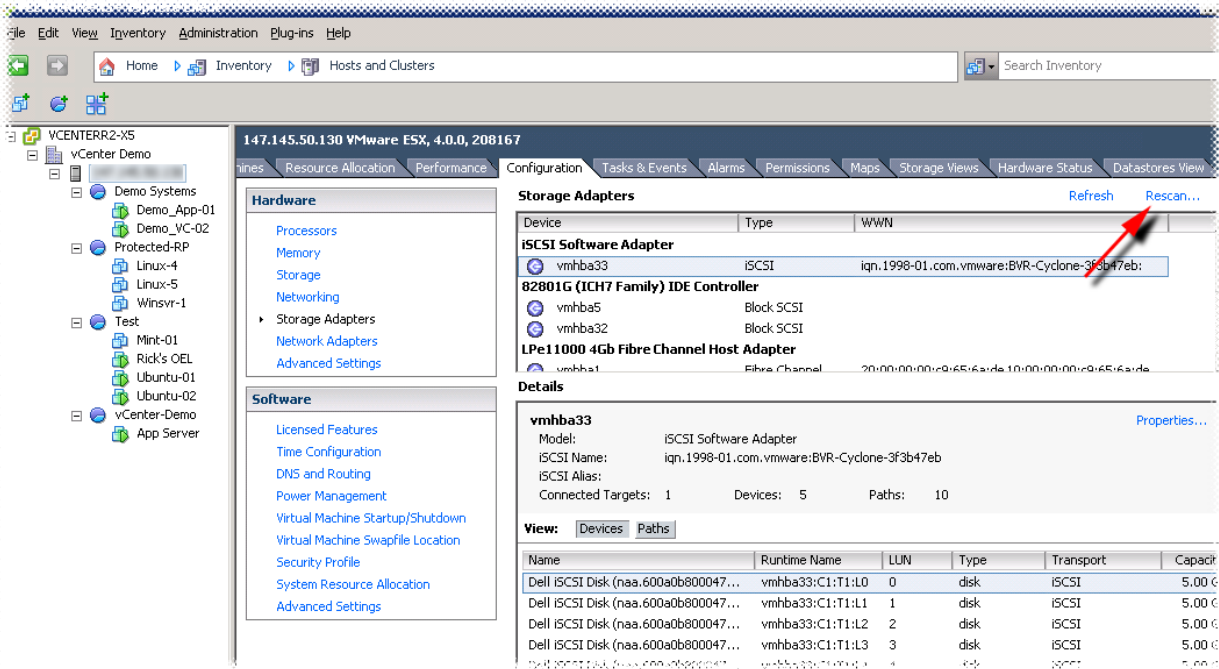


From this view, the user can also verify that the correct number of paths have been configured. By right-clicking on one of the devices listed under the storage adapter and selecting Manage Paths, a window opens and shows the number of paths for the target device. There should be 4 paths to each device with two Active and two Standby as shown in Figure 42.

**Figure 42.  Physical Disk Path Configuration**
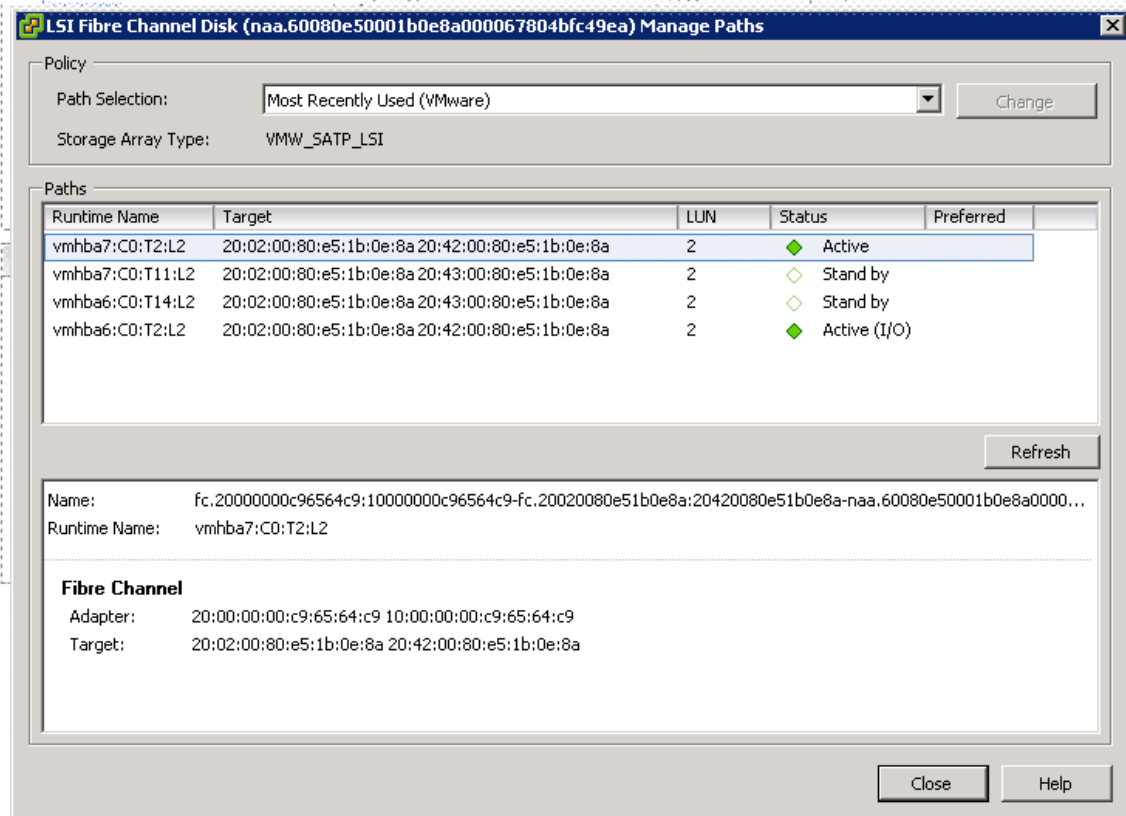
# Datastores View

After datastores are created on storage array virtual disks, the Datastores View tab can be used to understand the mapping of datastores to storage array virtual disks. The intent of this view is to provide you with a quick status and view of the datastores and their underlying storage virtual disks.

Use this view to identify the storage array where the datastore resides and the associated storage array virtual disk. You can view the health status of the virtual disk, the associated host/host group, RAID level, capacity and datastore free space. This view also displays the details of the datastore, such as the extent, LUN number, and health status.

The Datastores View, Figure 43 is context sensitive, so selecting a VM in the tree only displays storage elements for the selected VM.

**Figure 43. Datastores View**
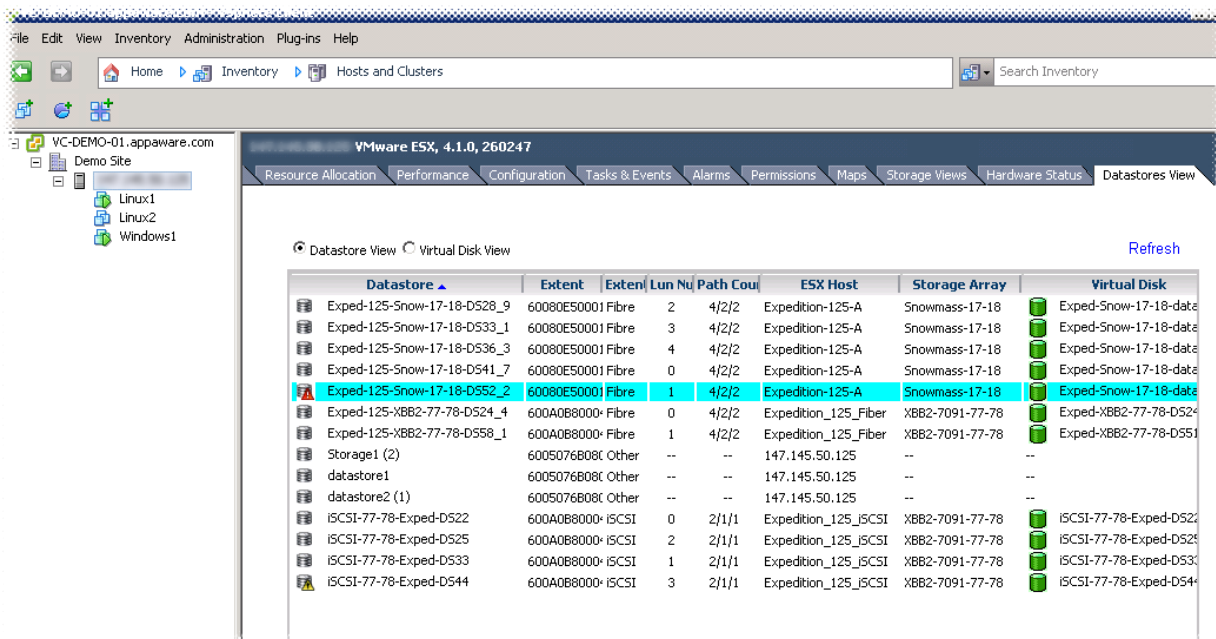


# Storage Array Event Log

The vCenter Plug-in allows you to view the Event Log for a storage array, as shown in Figure 53. To access the event log, click View Event Log in the storage array Summary window. You can set filters in the Event Log to show either critical events or all events. You can view the details for a selected event. By default, the Event Log retrieves the most recent 100 events, but from the Retrieve the most recent events drop-down list, you can specify the number of events for the Event Log to retrieve.

**NOTE:** The event log might contain some duplicate entries.

- After changing the number of events to retrieve, click Update.
- After changing the Event Log settings, click Save as, and click Close.

**Figure 44.  Event Log Viewer**
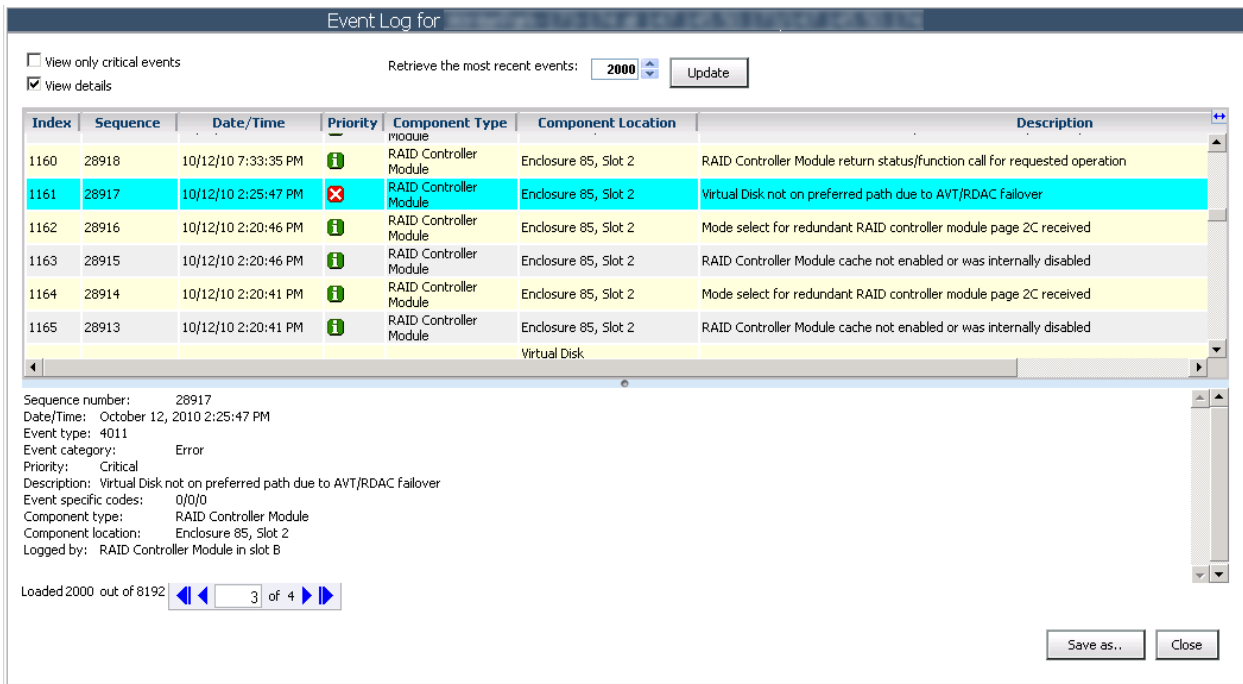


## Manually Unregistering the vCenter Plug-in

If the vCenter Plug-in needs to be removed, the following procedure can be used when it is not possible to uninstall the vCenter Plug-in from the application server.

**1**   Start a web browser and navigate to the IP address of the vCenter server with /mob appended to the IP address (example: http://192.168.51.21/mob).

**2**   Click the **content** link to navigate to the available ServiceContent.

**3**   Click the **ExtensionManager** link to display a list of registered extensions

**4**   Click the **UnregisterExtension** link and enter the extension name to be unregistered from the list of available extensions (example: Dell MD Storage Array vCenter Management Plug-in)

**5**   Click the **Invoke Method** link to unregister the extension.

**6**   The vSphere client must be restarted to reflect the changes.

**Figure 45. Manual Unregister Extension**
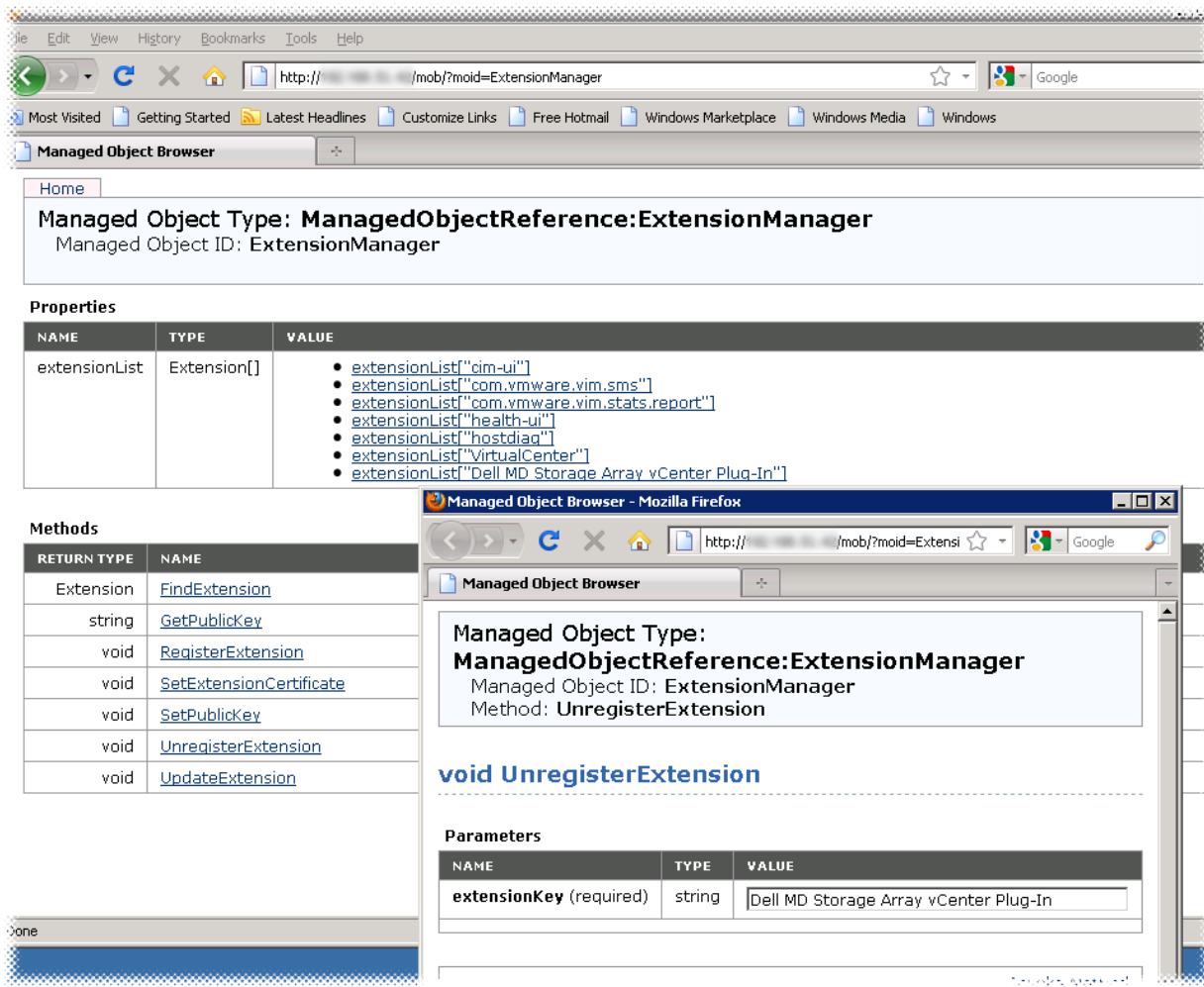


## Uninstall the vCenter Plug-in

The vCenter Plug-in can be uninstalled using the supplied uninstaller located on the application server at

```
C:\Program Files\Dell MD Storage Array vCenter Management Plug-
in\Uninstall Dell MD Storage Array vCenter Plug-In\Uninstall Dell MD
Storage Array vCenter Management Plug-in.exe
```

or from the application server run Add/Remove Programs (Programs and Features on Windows 2008) and select the vCenter Plug-in package to uninstall the vCenter Plug-in and SMI-S provider packages.

# Troubleshooting vCenter Plug-in Issues

This section describes how to open and read vCenter Plug-in log file, provides answers to some frequently asked questions, and describes and, describes how to resolve some common problems you might encounter with the vCenter Plug-in.

## Application Server Logs

All procedures that are performed from the vCenter Plug-In are logged in to the following log file on the application server:

C:\Program Files\Dell MD Storage Array vCenter Management

Plug-in\jetty\logs\

vCenter2-logx.y.csv

The file is archived every 24 hours and stored for 10 days, after which the file is overwritten. The file is in CSV format. You can open the file and view it in Notepad, CVSed, or a similar viewer.
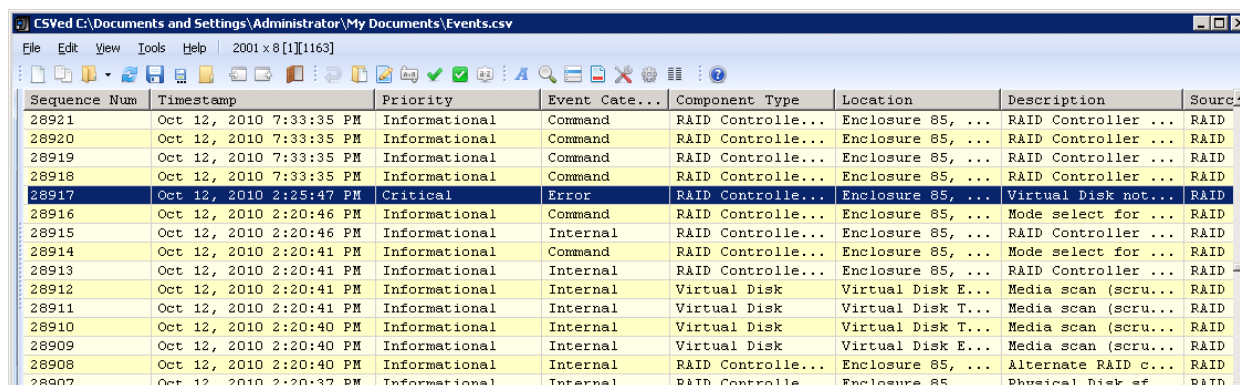
> **NOTE:** If the file is locked, you can create a copy of the file with a different name, open the copied file, and it view it.

**Figure 46.  vCenter Plug-in Log view**



Additional log files that are useful for technical support to resolve issues are also maintained in this directory, but these files are generally not in a user-friendly format.

- **`vCenter2debug-x.log.y`** -- Debug log used by technical support
- **`jetty-service.log`** -- Jetty service log, used by technical support
- **`<date/time stamp>.request.log`** -- Log of IP addresses for all Jetty service requests from clients

## The Installation Log Not Show that the Pegasus Service Started

Verify that the cimserver service was started from services.msc window.

> **NOTE:** In the event one of these services crash or is stopped, the CIMOM service must be started before the Jetty service or no updates/modifications will occur.

## I Cannot Communicate with the Application Server

1    Check the firewall settings to verify that the Jetty TCP port is enabled. If the Jetty TCP port is not enabled, enable it.

**2**   Verify that the cimserver/Pegasus server service is started on the application server. If the cimserver/Pegasus server service is stopped, start it.

**3**   Verify that the Jetty6-Service is started on the application server. If the Jetty6-Service is stopped, start it.

> 📝 **NOTE:** If the vCenter Plug-In will be installed on the same system as an active vCenter Server, and VMware Update Manager is installed, the port number 8084 for the plug-in must be changed from the default to an unused port number.

# I Cannot Create or Delete Objects

Verify that the user ID has the required storage administrator privileges assigned for the user's role. For more information about storage administrator roles, go to "Configuring Storage Administrator Roles" on page 10

# How Can I Maximize Client Performance

The Dell MD Storage Array vCenter Management Plug-in is a client-side, intensive application, so a fast CPU client, with sufficient memory to avoid page swapping, provides the best environment for running the vSphere client.

# How Do I Suppress Slow Script Warning Messages

Depending on the size of the storage array being managed, some of the views might generate a slow script warning message and delay the processing of the view. These warning messages can be suppressed by applying the following registry change on the storage array the vSphere client is being run from as detailed in `http://support.microsoft.com/kb/175500` Knowledge Base article from Microsoft.

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Styles
- DWORD MaxScriptStatements set to 0xFFFFFFFF

# I Cannot Make Changes to a Storage Array?

You can make changes to the storage array only when the password in the vCenter Plug-in matches the password set on the storage array.

- When the passwords do not match, such as when the storage array password is changed, but the password in the vCenter Plug-in is not changed, you can run passive commands from the vCenter Plug-in to the storage array, but active commands to the array will fail.
- The vCenter Plug-in displays the properties of the storage array whether the passwords match or do not match.

After you change the password on the storage array, change the password in the Plug-in so that the vCenter Plug-in password matches the storage array password. Resolving a Password Mismatch describes how to resolve a password mismatch.

# The vCenter Plug-in Does Not Show the New Storage Array Name after a Clear Configuration Operation in MDSM

You can perform a Clear Configuration operation in Modular Disk Storage Manager (MDSM) in two ways:

- The Clear Configuration operation on a disk group only deletes the virtual disk configuration. The storage array name does not change, so the vCenter Plug-in still sees the same storage array name.
- The Clear Configuration operation on a storage array clears the entire configuration and changes the storage array name to the default name. After a Clear Configuration operation, the vCenter Plug-in considers the storage array to be a first-time installation. For the vCenter Plug-in to recognize the storage array, perform the following actions:

  a   Remove the storage array from the vCenter Plug-in.

  b   In MDSM, rename the storage array.

  c   Re-add the storage array to the vCenter Plug-in.

# The vCenter Plug-in Displays Incorrect Error Messages

Incorrect error codes might appear because of the limited return codes from the SMI-S Provider. When you troubleshoot incorrect error codes, make sure you include all detailed information about the errors.

**Please send your feedback to support@dell.com.**

# 7

# Getting Help

## Contacting Dell

For customers in the United States, call 800-WWW-DELL (800-999-3355).

> **NOTE**: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1 Visit **support.dell.com**.

2 Click your country/region at the bottom of the page. For a full listing of country/region click **All**.

3 Click **All Support** from **Support** menu.

4 Select the appropriate service or support link based on your need.

5 Choose the method of contacting Dell that is convenient for you.