NetApp® SANtricity® Plug-in for VMware vCenter Version 3.0

User Guide

June 2016 | 215-09821_B0
doccomments@netapp.com

NetApp®

Table of Contents

OVERVIEW OF THE NETAPP SANTRICITY PLUG-IN FOR VMWARE VCENTER

The NetApp SANtricity Plug-in for VMware® vCenter® is a VMware vCenter Server plug-in that provides integrated management of NetApp E-Series and EF-Series storage arrays from within a VMware Web Client session. The Web Client is a single management interface that you can use to manage the VMware infrastructure and all of your day-to-day storage needs. You do not need to learn another management tool, so you can focus instead on the entire virtual infrastructure.

Note: The NetApp plug-in is not a direct replacement for the NetApp SANtricity Storage Manager software, which is still required for performing certain storage administration tasks.

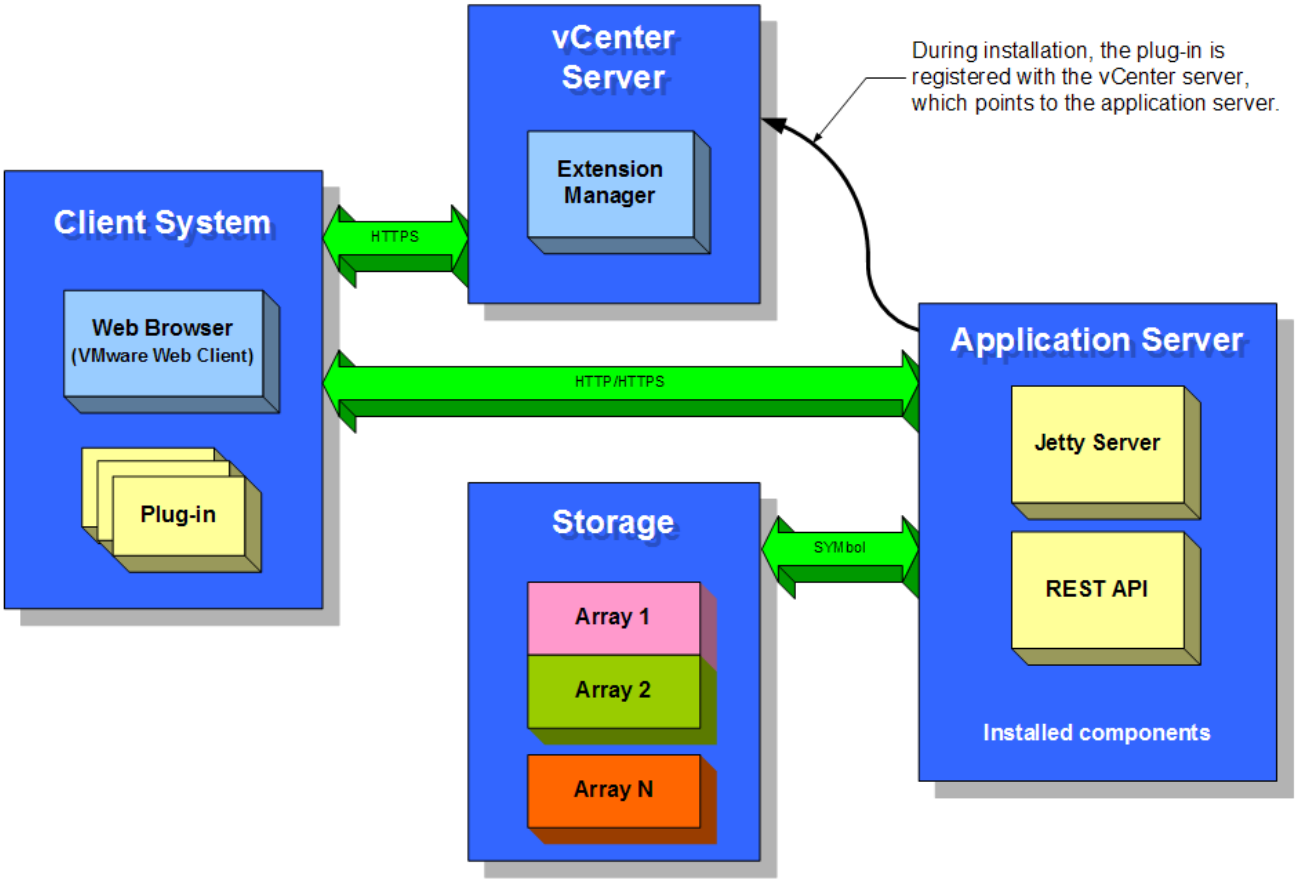
The NetApp plug-in enables you to perform the following tasks:

- Configure ESXi hosts to NetApp E-Series and EF-Series storage arrays.
- Create and delete volumes.
- Map volumes from the NetApp E-Series and EF-Series storage arrays to the ESXi host.
- View the vCenter Datastores to NetApp storage array volumes.

You can create hardware snapshots, volume copies, synchronous, and asynchronous mirroring when these premium features are enabled on the storage array. The NetApp plug-in uses an application server to facilitate the interface between the Web Client and the NetApp E-Series and EF-Series storage based on the authenticated logged-in user and the privileges assigned to that user's role.

The NetApp plug-in requires that a VMware vCenter Server is installed within the environment. The NetApp plug-in does not function in a configuration with only a Web Client and an ESXi host configuration.

Figure 1) Communication Details.



NetApp Plug-in Features

The following NetApp plug-in features enable the integrated management of NetApp E-Series and EF-Series storage arrays:

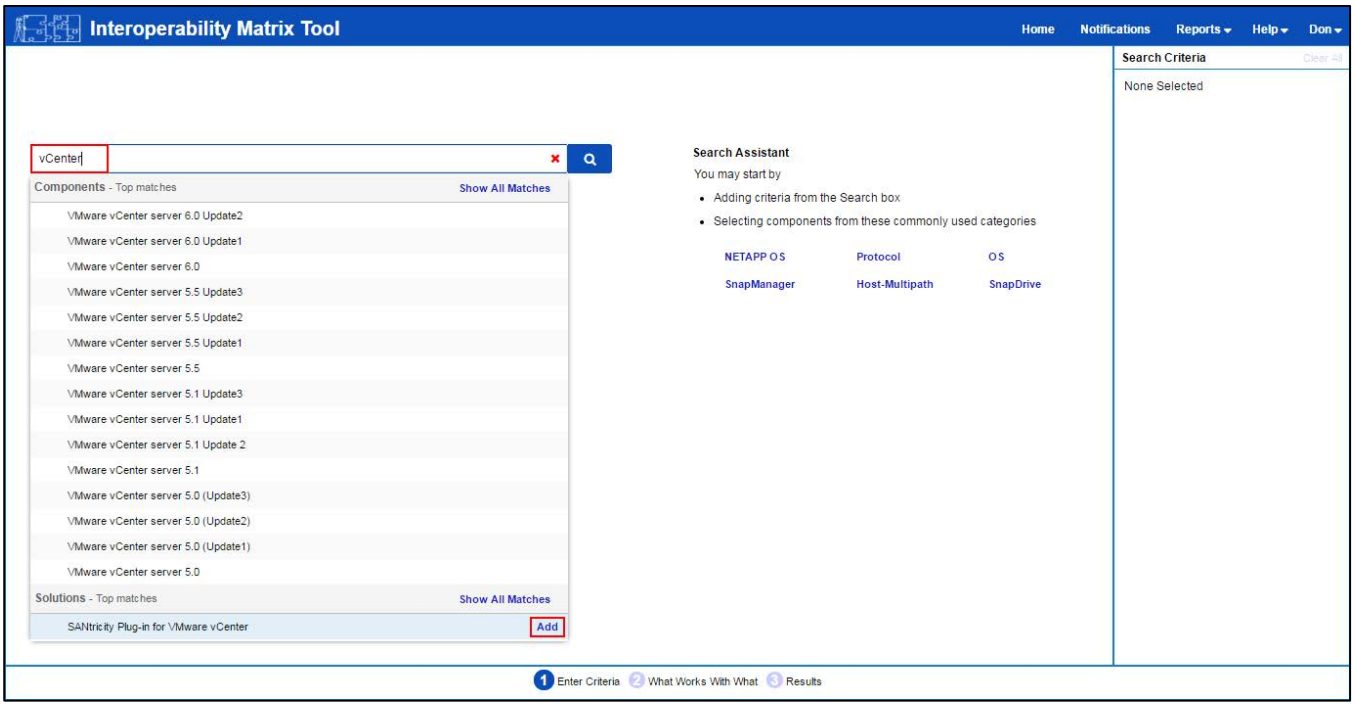
- Storage array information
- Storage array organization
- Automatic and manual storage array configuration backup
- Storage provisioning and volume mapping
- Copy services management
- Remote Volume Mirroring
- Asynchronous Remove Volume Mirroring
- Datastores to volume details
- ESXi host configuration

Installation Prerequisites

For a complete and up-to-date listing of all compatible host, server, and firmware for the SANtricity plug-in, refer to the NetApp Interoperability Matrix Tool.

To locate the latest compatibility information from the Interoperability Matrix Tool, enter **vCenter** under the search field and click **Add** next to the SANtricity Plug-in for VMware vCenter option.

Table 1) Interoperability Matrix Tool



Supported Browsers

The NetApp plug-in has been tested on and supports the following browsers:

- Chrome version 40+
- Firefox 35+
- Internet Explorer 9, 10, 11

Scalability

The NetApp SANtricity Plug-in for VMware vCenter version 3.0 will support the configuration of many storage arrays limited by the conditions of your environment. Performance of the plug-in will be determined by the client system. Support of large numbers of arrays (2000+) will require 3+ GB of RAM. See Configuring Application Server Memory section for configuration details.

Application Server Memory Requirements

Table 2) Memory Requirements.

No. of Arrays	Windows Memory Requirements	Linux Memory Requirements
1-250	1024 MB RAM	1024 MB RAM
251-500	1536 MB RAM	1536 MB RAM
501-1000	2048 MB RAM	2048 MB RAM
1001-2000	3096 MB RAM	3096 MB RAM

INSTALLING THE NETAPP SANTRICITY PLUG-IN FOR VMWARE VCENTER

Downloading the NetApp SANtricity Plug-in for VMware vCenter

Obtain the latest version of the NetApp plug-in from the NetApp web site. See the support matrix at the NetApp web site for the most current versions. The file should be copied to the host that will be used as the application server.

- Windows installer binary: vCenterInstaller-03.00.3000.*xxxx*.exe
- Linux installer binary: vCenterInstaller-03.00.7000.*xxxx*.bin

Note: After downloading the Linux binary, add the execute attribute to the binary file to enable execution of the installer (**`chmod +x vCenterInstaller-03.00.7000.xxxx.bin`**).

Installing the NetApp Application Server

Install the NetApp application server on a different Windows server than the VMware vCenter Server is installed on.

Note: When adequate resources are available on the VMware vCenter Server system, you can install the application server on the same host that the VMware vCenter Server is installed on, but this is not recommended.

After you have downloaded the NetApp plug-in software, copy the file to the system that is the application server. Run the NetApp plug-in installer to launch the installation wizard. The installation wizard will install an application server and associated jar files. After the installation is complete, the installation wizard registers the NetApp plug-in with the VMware vCenter Server.

Upgrading from Previous Versions

If upgrading from a previous version of the NetApp plug-in and you wish to use the same host for the application server, copy the new installation file to the existing application server and run the installer executable. This will automatically upgrade the previous NetApp plug-in version to this release.

Note: This version of the NetApp plug-in **ONLY** supports the VMware Web Client and will not function with the VMware vSphere Client. If you still use the vSphere Client, you must use the previous version of the NetApp plug-in, release 2.7, to manage NetApp E-Series and EF-Series storage arrays from within the vSphere Client.

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 3** shows the information required for each component. See Configuration Worksheet for a printable worksheet.

Table 3) Configuration Worksheet Example.

	Example Information	Required Information	Example Information
vCenter Server Name:	*VC-01*	DNS name: IP Address:	*vc-01.domain.com* *192.168.51.217*
vCenter Administrator Name:	*administrator*	Password:	*password*
Application Server Name:	*APP-01*	DNS name: IP Address:	*app-01.domain.com* *192.168.51.225*
Storage Array 1 Name:	*E5400*	IP Addresses: Password:	*192.168.51.89/90* *none*
Storage Array 2 Name:	*E2600*	IP Addresses: Password:	*192.168.51.91/92* *none*
Storage Array 3 Name:		IP Addresses: Password:	
Storage Administrator User ID:	*User1*	The user's level of storage administrator rights (See figure for examples)	Read-Only
Storage Administrator User ID:	*User2*	The user's level of storage administrator rights (See figure for examples)	Read-Write

Installing the NetApp Plug-in

Launch the NetApp SANtricity Plug-in for VMware vCenter installer binary file on the target host system that will be used as the application server.

1. Read the introduction screen, and click **Next**.
2. Read the license agreement. If you accept the terms, select the appropriate radio button, and click **Next**.
3. **Select** the local installation directory for the NetApp 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 application server or accept the default number of either 8084 or 8081, and click **Next**.

Note: If the NetApp plug-in is installed on the same system as an active vCenter Server, and VMware Update Manager is also installed, the default port number 8084 for the plug-in must be changed 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 NetApp 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**.

Note: If the Plug-in will be installed into a vSphere 5.5 or 6.0 environment with SSO, the default user ID may need to be changed to match the vSphere 5.5 or 6.0 domain configuration (Example: administrator@ vsphere.local).

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

11. The installation is now complete. Click **Done** to close the installation wizard.
12. (Windows) To verify that the application server was installed successfully, run the **`services.msc`** command, and verify that the **NetApp Application Server (vCP)** service was installed and the service started.
13. (Linux) To verify that the application server has been started, run **`service Application-Server-vCP status`**.

```
root@ictm-linux-01:/# service Application-Server-vCP status
Application-Server-vCP process is running
 *
root@ictm-linux-01:/#
```

CONFIGURING THE NETAPP APPLICATION SERVER AND PLUG-IN

After the application server and the NetApp plug-in are installed, verify that the NetApp 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 NetApp SANtricity Plug-in for VMware vCenter is listed as Enabled.
- However if the NetApp 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 application server is enabled to pass through any firewalls that might be in use. The default application server Transmission Control Protocol (TCP) port numbers are 8084 and 8081.

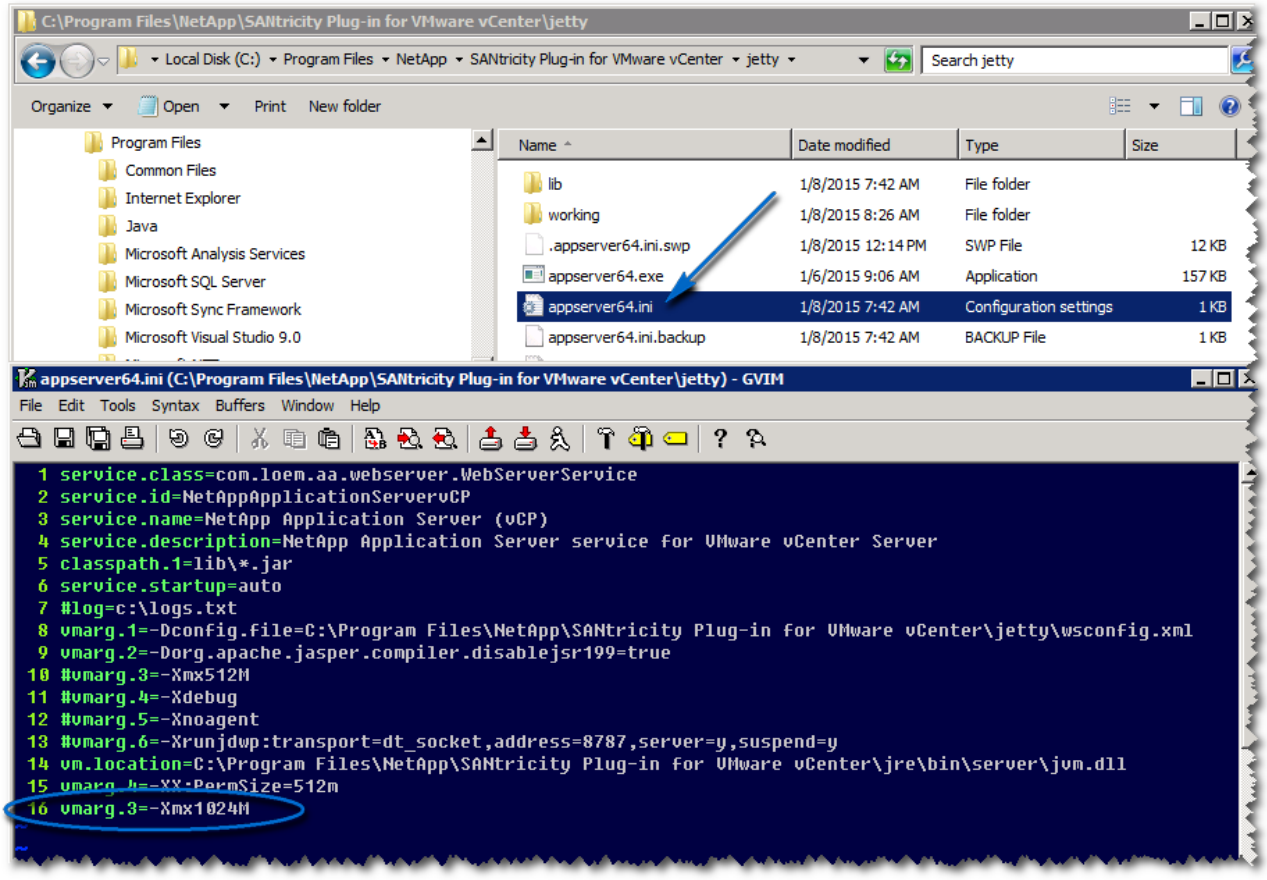
After the application server and VMware vCenter Server have been configured, the **NetApp SANtricity Plug-in for VMware vCenter** icon appears in the Solution and Application section of the vSphere Client Home page.

Configuring Application Server Memory

If more than 250 storage arrays will be managed from the **NetApp SANtricity Plug-in for VMware vCenter**, then the application server configuration file will need to be modified. The application server by default is configured for 1024 MB of RAM usage. To adjust the settings to support more than 250 arrays, modify the **`appserver64.ini`** file located on the application server in the **`C:\Program Files\NetApp\SANtricity Plug-in for VMware vCenter\jetty directory`**.

1. Open the **`appserver64.ini`** file in a text editor.

Figure 2) Application Server Memory Settings.



2. Locate the **`vmarg.3=-Xmx1024M`** line.
3. Change **`1024`** to the number associated with the number of storage arrays to be managed from Table 2 above.
4. Save the configuration file.
5. Restart the **`NetApp Application Server (vCP)`** service.

Note: If the application server is reinstalled, this setting will be reverted to the original setting of 1024 MB and must be edited again to adjust the application server memory for your environment.

Configuring Storage Administrator Roles

By default, all defined VMware vCenter user IDs have no rights to NetApp E-Series storage arrays. When a user requires either read permissions or read-write permissions to access the NetApp plug-in, the user's role must be modified to permit access to the NetApp plug-in.

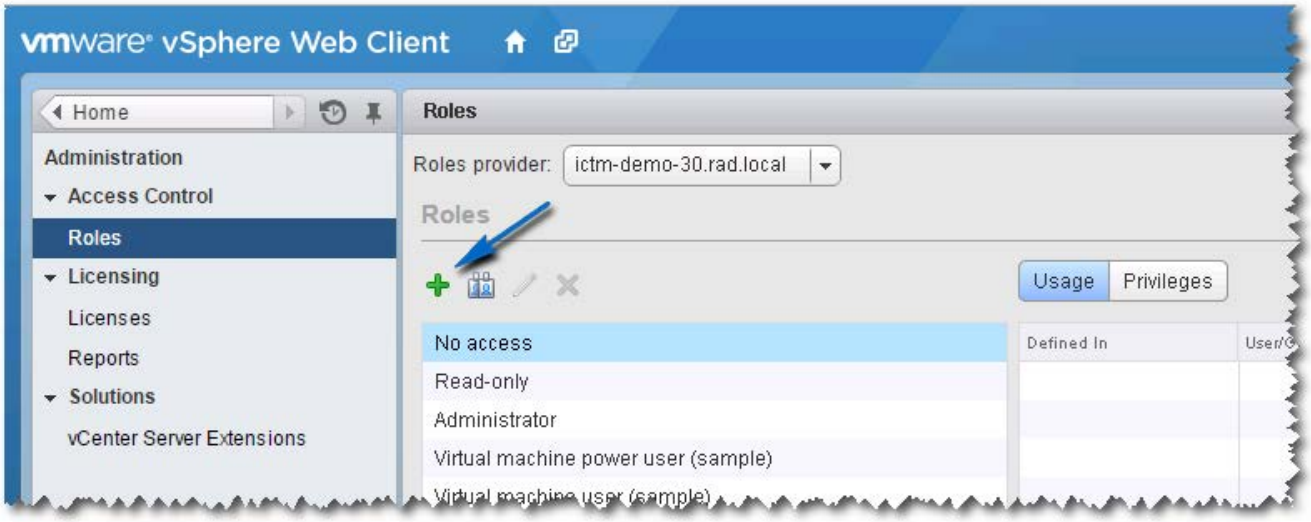
Note: If attempting to access the client and you encounter a Not Authorized message, you must restart the vSphere Client after defining the new Storage Administrator role before access is granted.

Creating a Role

1. In the Administration area on the vSphere Client Home page. Click the **Roles** icon. The list of roles and usages appears.

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

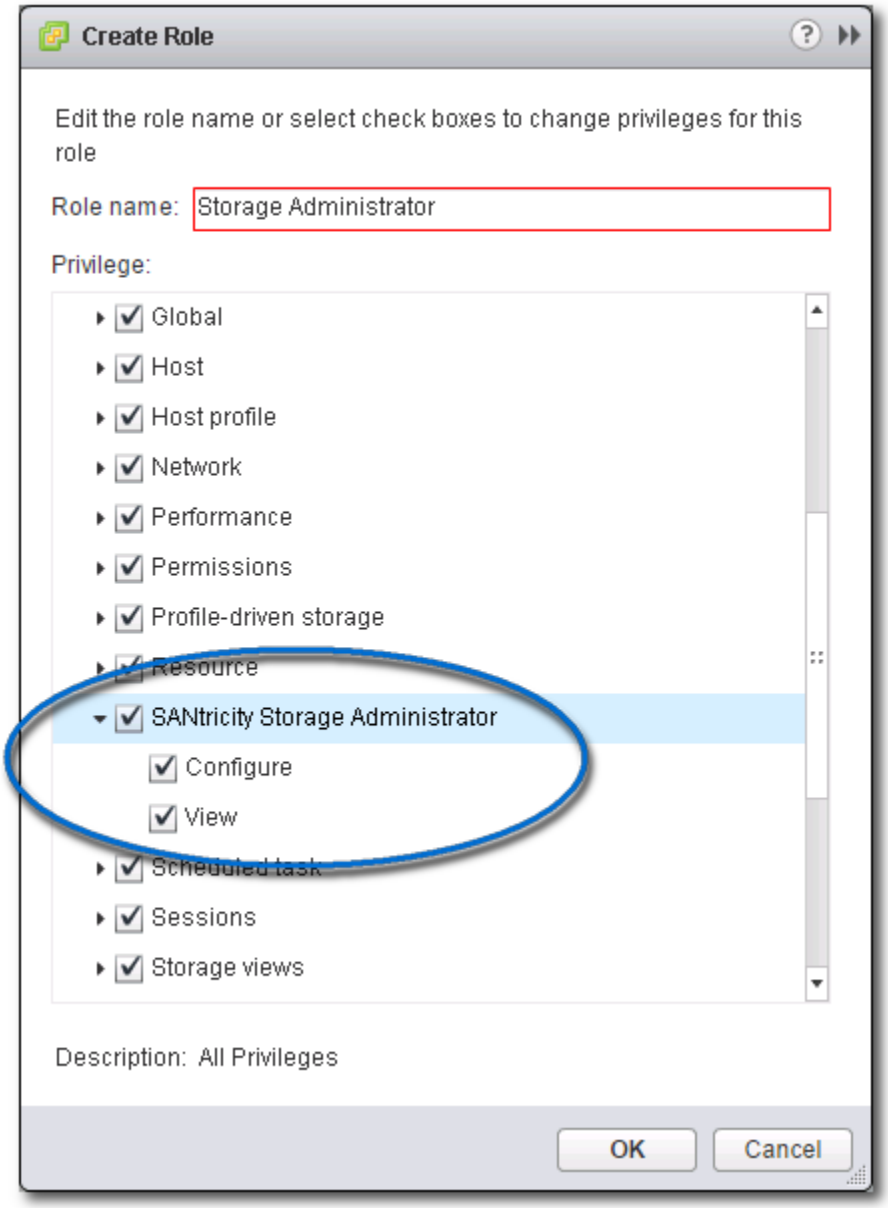
Figure 3) vCenter Server Roles List.



2. Click the green plus icon to add a new role.

The **Create Role** window opens.

Figure 4) Create Role Window.



3. In the **Role Name** text box, type the name of the new role.
4. In the **Privileges** list, select the access permissions to assign to this role.

Note: The administrator role is not editable; therefore, if the administrator user is 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.

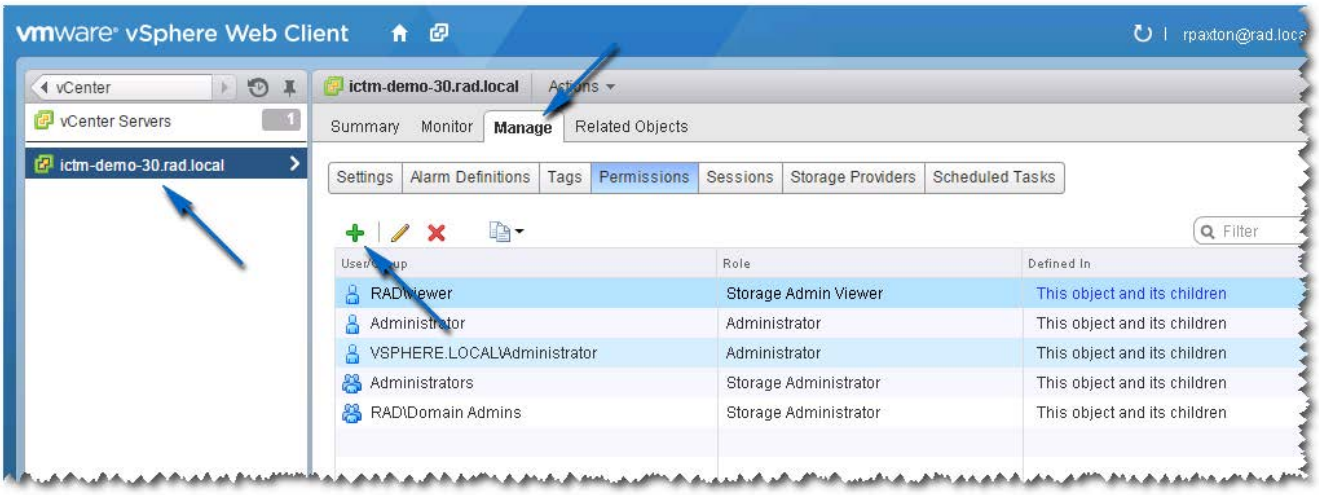
5. To allow **Read-Only** (View) or **Read-Write** (Configure) access permissions to the storage arrays, select the appropriate permission from the Storage Administrator group.
6. Click **OK**.

Note: Existing roles can 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. Click the **VMware Home** icon, select **vCenter Inventory List** and then click on **vCenter Servers** under Resources Lists.
2. Select the **vCenter server** element to manage, and select the **Manage** tab.

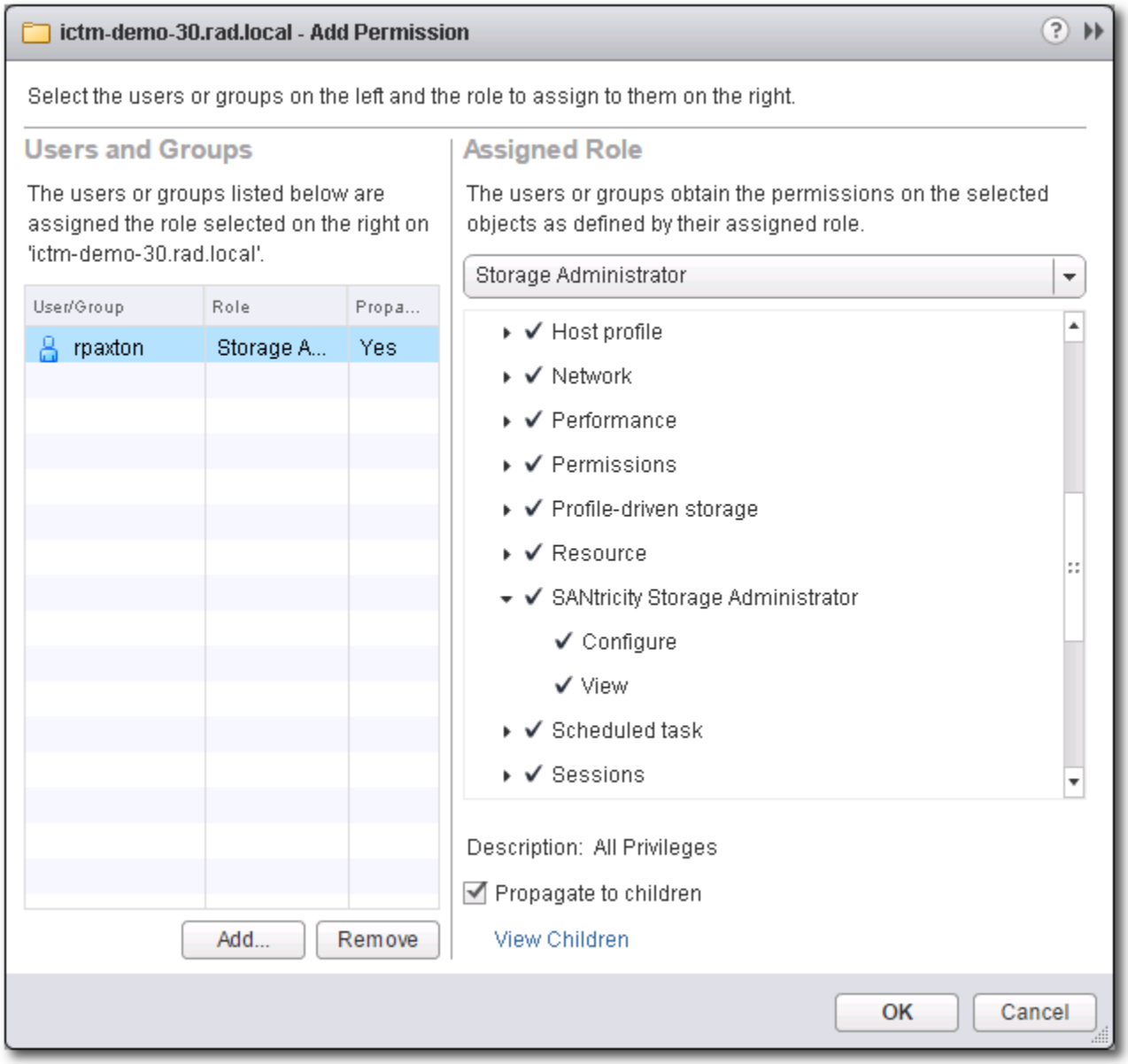
Figure 5) Add Permission.



3. Click the **green plus** icon, to define the users who are members of the Role.

The **Add Permission** wizard is then displayed.

Figure 6) Add Permission Wizard.



4. In the wizard, click **Add**, and select the User ID(s) that requires access to the storage arrays.
5. Select the assigned role from the drop-down box, and click **OK** to apply changes.
6. Click **OK** to apply permissions to the role.

No Access

If users are not members of a role that has either the View or Configure SANtricity Storage Administrator permission, they cannot view any statistics from the NetApp plug-in. If they attempt to access a NetApp plug-in feature, they receive the User is not authorized to use this plug-in message.

NetApp SANtricity Plug-in Security

The NetApp SANtricity Plug-in utilizes TLS 1.2 for secure https communication between the Web Client and NetApp application server. This necessitates the need for SSL certificate management to establish communication between the client and the application server. Depending on the client browser used to communicate with the Web Client, will dictate what procedures are needed to establish communication with the application server. If your environment utilizes trusted CA signed SSL certificates, once the application server certificate is signed and re-imported, the following procedures are not be needed.

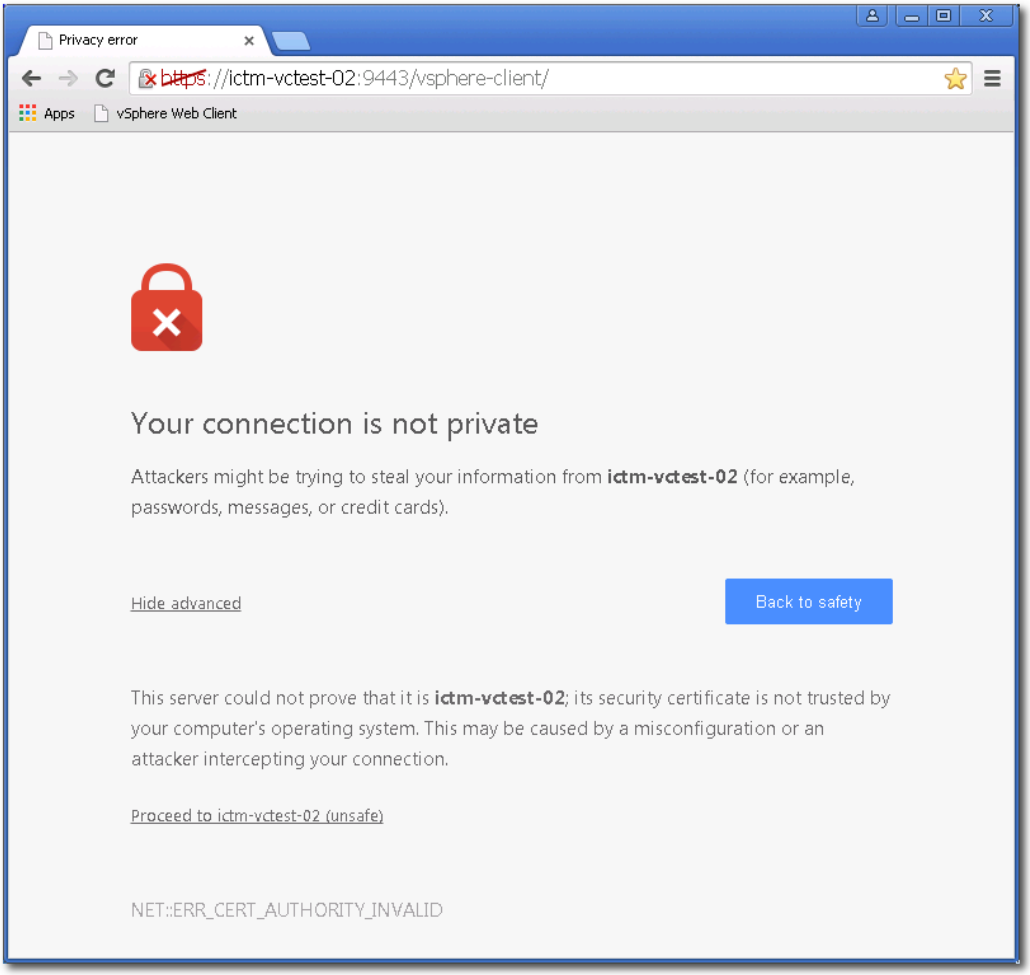
Mozilla Firefox

For Mozilla Firefox, currently you can accept the self-signed SSL certificate via the Getting Started pages and permanently store the certificate in Firefox's truststore. This will then be remembered for future connections between the Web Client and the application server.

Google Chrome

For Google Chrome, enter the URL for the vCenter Server to connect to and then select the Advanced option, and click the Proceed to VMware vCenter Server link, proceed to log into the vCenter Server as normal. Click on the SANtricity Plug-in icon from the home page and then select the *How to configure browser security* link from the Getting Started tab. Follow the procedures documented on the SSL Certificate Setup page to establish communication to the application server. Once communication has been established, the NetApp SANtricity plug-in should function as normal.

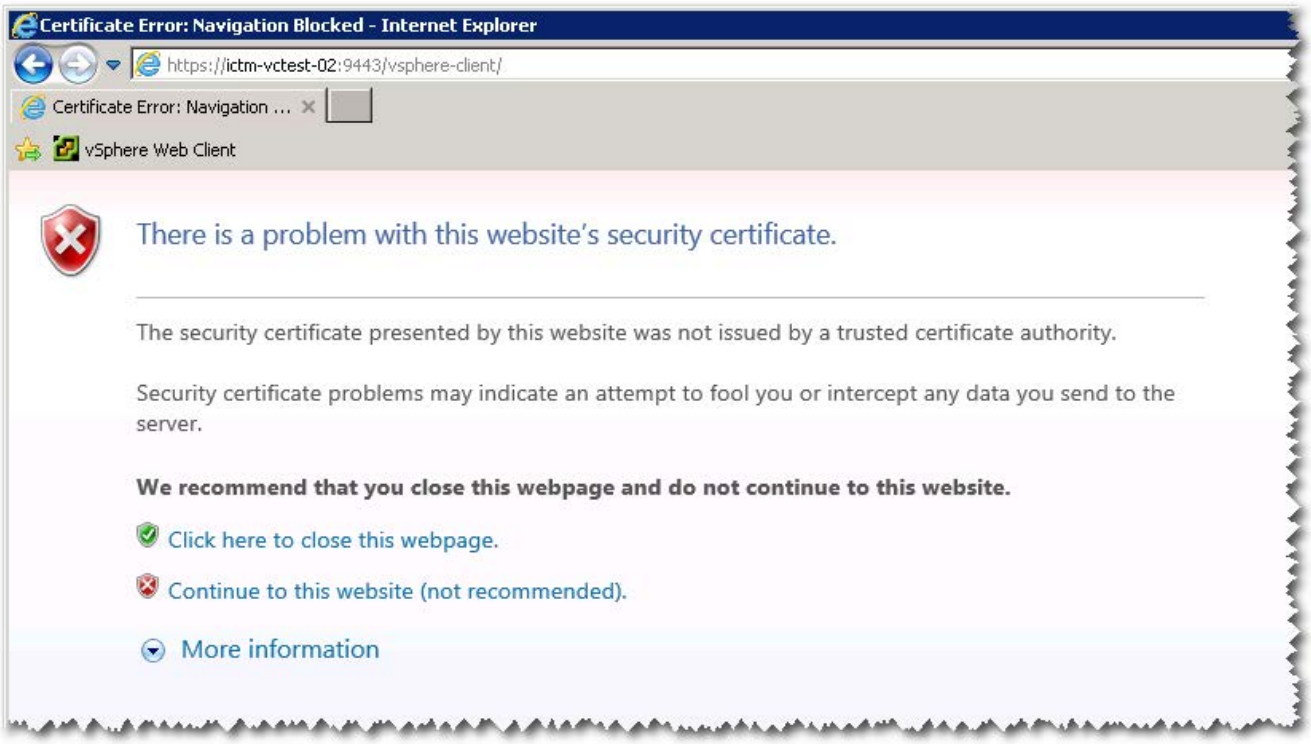
Figure 7) Chrome security page.



Microsoft Internet Explorer

For Internet Explorer, enter the URL for the vCenter Server to connect to and then click the "*Continue to this website (not recommended)*" link to proceed to site. You may also have to install the vCenter Server SSL certificate to establish connection. Once connected to the vCenter Server, click the SANtricity Plug-in icon from the home screen and then click on the *How to configure browser security* link and follow the procedures on the SSL Certificate Setup page.

Figure 8) Internet Explorer certificate error page.



Note: Once communication has been established with the application server, it may take a couple of minutes for the Summary tab information to display.

NetApp Application Server Certificate Management

To resolve the self-signed certificate errors with latest browsers, you will need to have the application server certificate signed by a trusted Certification Authority (CA). During the installation of the NetApp plug-in, an SSL certificate was generated for the application server along with a certificate signing request (CSR) that is specific to that application server. The CSR must be signed by a trusted CA and then reimported into the Java keystore to implement a fully trusted certificate chain. The following steps detail how to import the application server certificate after it has been signed by a trusted CA:

Note: The CSR is typically located on the application server host directory **`C:\Program Files\NetApp\SANtricity Plug-in for VMware vCenter\jetty\working`**. The file will be named ***`<host_name>`*`.csr`**. After the CSR has been signed by a trusted CA, copy the signed certificate and the CA certificate to the same directory.

Import Signed Application Server Certificate

On the application server host system, open a command line window / terminal.

1. Change directory to **`C:\Program Files\NetApp\SANtricity Plug-in for VMware vCenter\jetty\working`** directory.

Assumed both the signed certificate and the CA certificate have been copied to the working directory.

2. Import the CA certificate into the Java keystore (if not already in trustedcacerts keystore) by executing the following on the command line: **`..\..\jre\bin\keytool -import -trustcacerts -alias root -file <ca_cert> -keystore keystore -storepass changeit`**
3. Import the signed application server certificate into the Java keystore with the following on the command line: **`..\..\jre\bin\keytool -import -trustcacerts -alias jetty -file <signed_cert> -keystore keystore -storepass changeit`**
4. Restart the **`NetApp Application Server (vCP)`** service and allow a minute or two for the service to initialize.
5. Verify the certificate is working by accessing the following URL (Assumed default port number for https connection.): **`https://`**`<application_server_address>`**`:8084/vcenter2/About.html`**

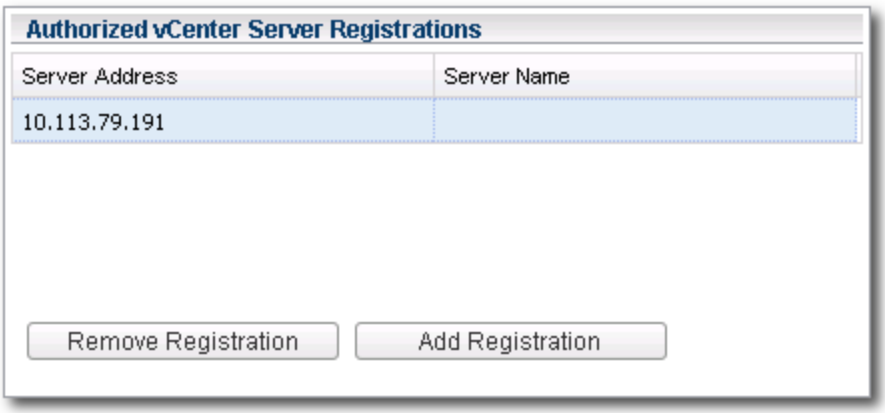
Note: Mozilla Firefox users will also need to ensure the CA certificate has been imported into the browser's authorities' truststore (Options -> Advanced -> Certificates -> View Certificates -> Authorities).

Register vCenter Server to Application Server

If the jetty SSL certificate has been recreated, the vCenter Server must be re-registered with the application server to detect the new certificate ID. To re-register the vCenter Server, navigate to the SANtricity Plug-in Getting Started page and click on the **Manage vCenter Server Access** link and login to the **Manage vCenter Server Access** page.

The **Authorized vCenter Server Registrations** dialog is displayed.

Figure 9) Authorized vCenter Server Registrations dialog box.



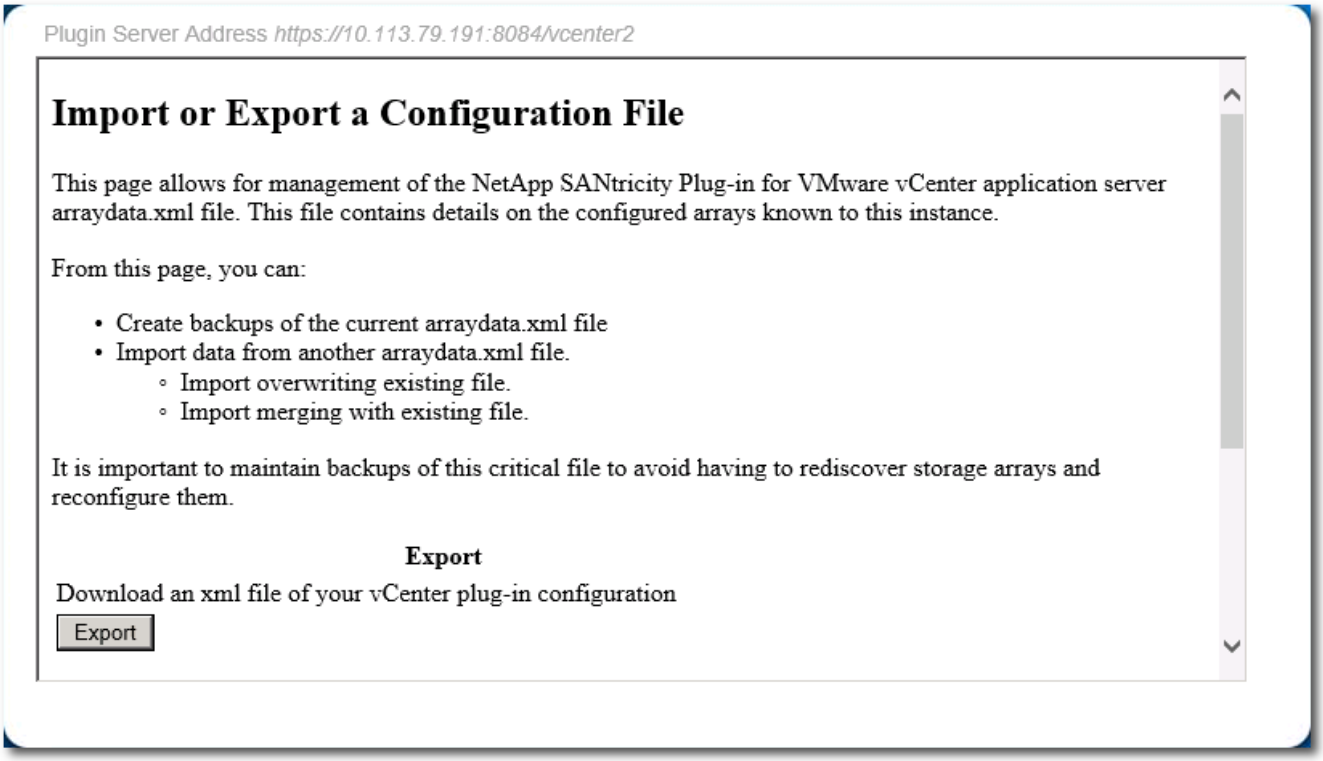
1. **Select** the vCenter Server IP address of the vCenter Server to re-configure.
2. Click the **Remove Registration** button to remove the old registration.
3. Click the **Add Registration** button and enter the vCenter Server Address, DNS Name, User ID, and Password.
4. Click the **Add** button.

Import - Export Configuration File

The NetApp plug-in supports the ability to import or export the storage array manager configuration file that maintains the list of configured storage arrays and metadata information. This feature is useful for backing up array configurations or deployment of new application server using an existing configuration file. To access this functionality, navigate to the SANtricity Plug-In Getting Started page and click on the **Manage Arraydata.xml Data** link. Follow the procedures documented on the **Manage Arraydata.xml File** page to login to the application server.

Once logged into the application server, the **Import or Export a Configuration File** page is displayed.

Figure 10) Import or Export a Configuration File Page.



Export

To export the current configuration file, click the **Export** button and select the location to save the file to.

Import

To import a previously saved configuration file, perform the following steps:

1. Click the **Browse** button.
2. Navigate to the configuration file to import and click **Open**.
3. Select the import radio button option to use (**Merge** or **Overwrite**).
4. Click the **Import** button.

Application Server User Management

The application server user management is controlled via the **users.properties** file located in **C:\Program Files\NetApp\SANtricity Plug-in for VMware vCenter\jetty\working\config** directory.

The format of the **users.properties** file is ID name, MD5 password hash, user ID.

```
#
#Thu Apr 11 18:02:33 PDT 2013
admin=MD5\:21232f297a57a5a743894a0e4a801fc3,admin
ro=MD5\:3605c251087b88216c9bca890e07ad9c,storage.ro
#rw=MD5\:038c0dc8a958ffea17af047244fb6960,storage.rw
vcenter=MD5\:736849783cb137f97c4e535c246afd4b,storage.rw
```

The passwords may be stored in clear text, but is not recommended. A MD5 password hash may be generated from the following site: http://md5hashgenerator.com/index.php. Enter the password to be hashed within the String textbox, and then click Generate MD5 Hash. Copy the hashed results to the **users.properties** file in place of the existing user password hash.

Alternatively, you may use **md5sum** on a UNIX system to generate the MD5 has using the following (substitute your password for *YOUR_PASSWORD_HERE*):

```
$ echo -n "YOUR_PASSWORD_HERE" | md5sum | awk '{print $1}'
635893277b6b217e327565d3427ee5e8
```

Copy and replace the MD5 hash, in the **users.properties** file for the specific user, with the output of the above command.

Note: You must specify the '-n' option to avoid passing carriage return from echo to md5sum utility.

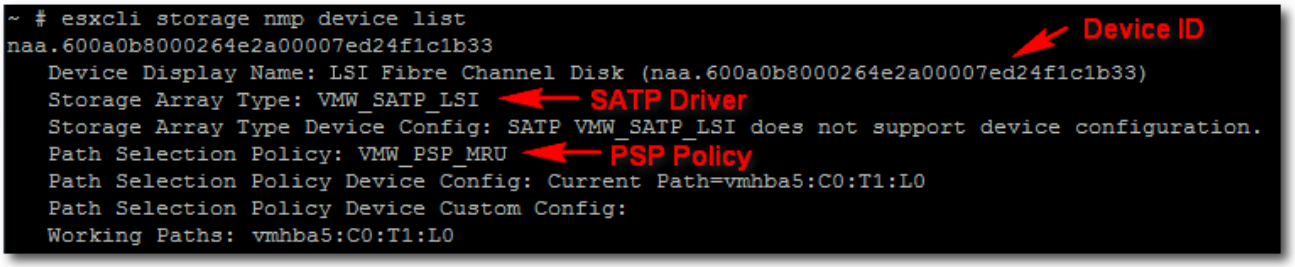
CONFIGURING VMWARE ESXI HOSTS

Configuring ALUA SUPPORT

Firmware versions 7.84 and later allows for support of an Asymmetric Logical Unit Access (ALUA) configuration when the Target Port Group Support (TPGS) flag is set to on (default for 7.84). This allows for active-active I/O throughput between all paths to the current owning controller and LUN transfer to the alternate controller in failure scenarios. Depending on your environment you may be able to achieve higher performance by switching the default multipath policy from MRU to Round Robin (RR). This is accomplished by the following steps:

- Identify current SATP claim rule in use for your storage.
- Identify default PSP rule for SATP in use.

Figure 11) esxcli storage nmp device list.



- (Optionally) Change default PSP rule to VMware RR.

Adding ALUA SATP Claim Rule

To create a new claim rule enter the following:

```
#esxcli storage nmp satp rule add -s VMW_SATP_ALUA -V LSI -M INF-01-00 -c tpgs_on -P
VMW_PSP_RR -e "LSI ALUA Claim Rule"
```

This will create a new claim rule for the VMW_SATP_ALUA satp rule to claim any LUNs matching the following:

```
Vendor ID = LSI
 Model ID = INF-01-00
TPGS Flag = on
```

and assign the default path selection policy to round robin (VMW_PSP_RR).

Note: There are different methods to manage SATP claim rules, and your environment may require different parameters to enable ALUA support. Please consult the VMware Knowledge Base for additional information.

Figure 12) ALUA Configured Storage.

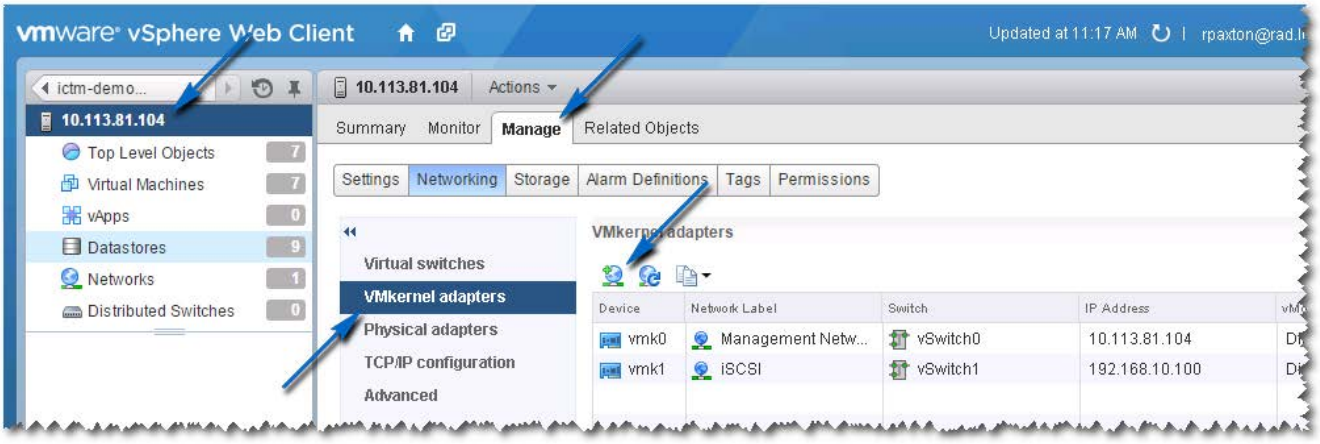
Configuring iSCSI Storage

To configure the network for software iSCSI storage, create an iSCSI VM kernel 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.

To configure iSCSI adapters with this wizard, iSCSI HBAs must already be defined within vSphere. This is accomplished by configuring an iSCSI network and adding iSCSI software initiator under storage adapters.

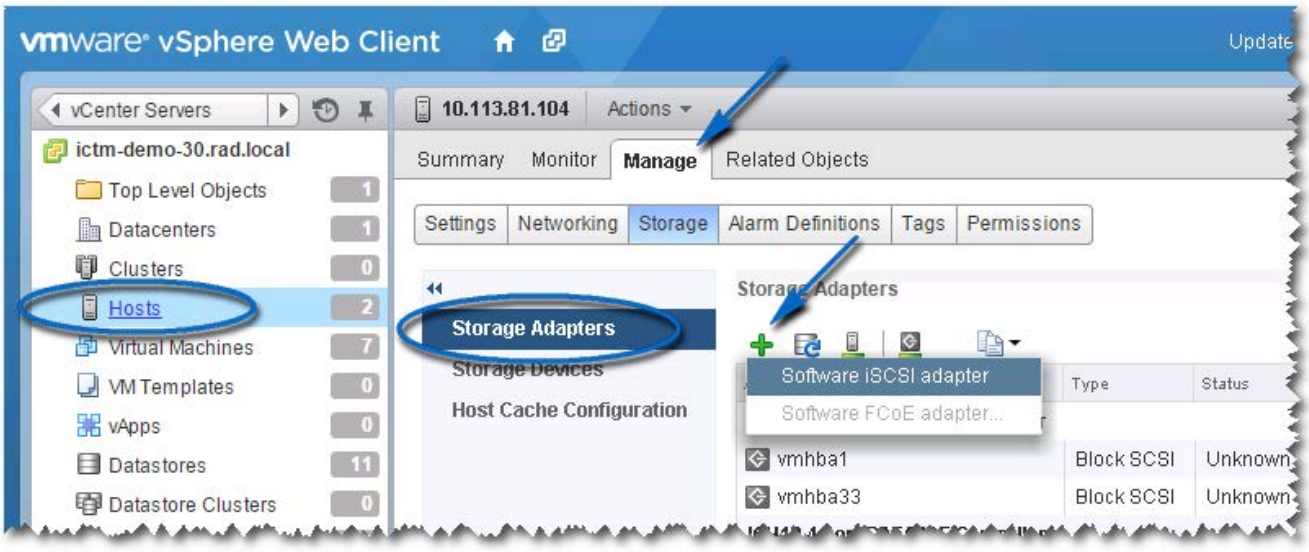
To configure iSCSI storage, I recommend thoroughly reading the VMware Best Practices for Running VMware vSphere on iSCSI. I would also recommend searching for videos on implementing iSCSI with vSphere.

Figure 13) Networking Configuration View.



- Add a VMkernel network for iSCSI communication
- Select NIC(s) to use for iSCSI and configure
- From the Storage Adapters view, click Add and select Add Software iSCSI Adapter

Figure 14) Add Software iSCSI Adapter.



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.

Configuring SAS Support on ESXi Hosts

For the NetApp plug-in to configure ESXi hosts to the NetApp E-Series storage arrays, with SAS connections, an updated version of the LSI SAS SMI-S provider must be installed on the ESXi hosts.

Upgrading the SAS SMI-S Provider

Note: SAS support is available only for ESXi version 5.1 and later hosts. Previous versions of ESX and ESXi are not supported.

Note: This upgrade is required only to allow the Host to Storage Configuration option to configure SAS connected storage arrays. When the storage arrays are already configured, or the storage arrays are not SAS-connected, the in-box provider does not need to be upgraded.

To use the SAS provider, it must first be deployed on the ESXi servers to be configured. This requires that either Secure File Transfer Protocol (SFTP) or Secure Copy (SCP) is enabled on the ESXi host. To install the SAS SMI-S Provider upgrade package, you must have *root* access. To install the package by remote login, either create a new user with host login privileges, or enable remote logins for the *root* user.

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 ESXi host to be configured.
2. Select the User & Groups tab in the 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.
5. Click OK to save changes.
6. After logging in as this new user, use the su command to assume the super user role.

Installing the SAS Provider Upgrade of ESXi

1. Use scp (or a utility like FileZilla) to copy the **`vmware-esx-provider-lsiprovider.vib`** file to the target ESXi host.
2. Log into the ESXi server as *root*.

Note: If root is not enabled, enable it temporarily for this install.

3. Run **`esxcli software vib install -v /tmp/vmware-esx-provider-lsiprovider.vib`** all on same line (This assumes the **`.vib`** file is located in the **`/tmp`** directory.

The following message appears:

```
~ # esxcli software vib install -v /tmp/vmware-esx-provider-lsiprovider.vib
Installation Result
```

```
   Message: The update completed successfully, but the system needs to be rebooted for the
changes to be effective.
   Reboot Required: true
   VIBs Installed: LSI_bootbank_lsiprovider_500.04.V0.54-0004
   VIBs Removed:
   VIBs Skipped:Reboot the host after stopping any running VMs.
```

4. After the host reboots, run **`esxcli software vib list |grep LSI`** to verify the update has been applied.

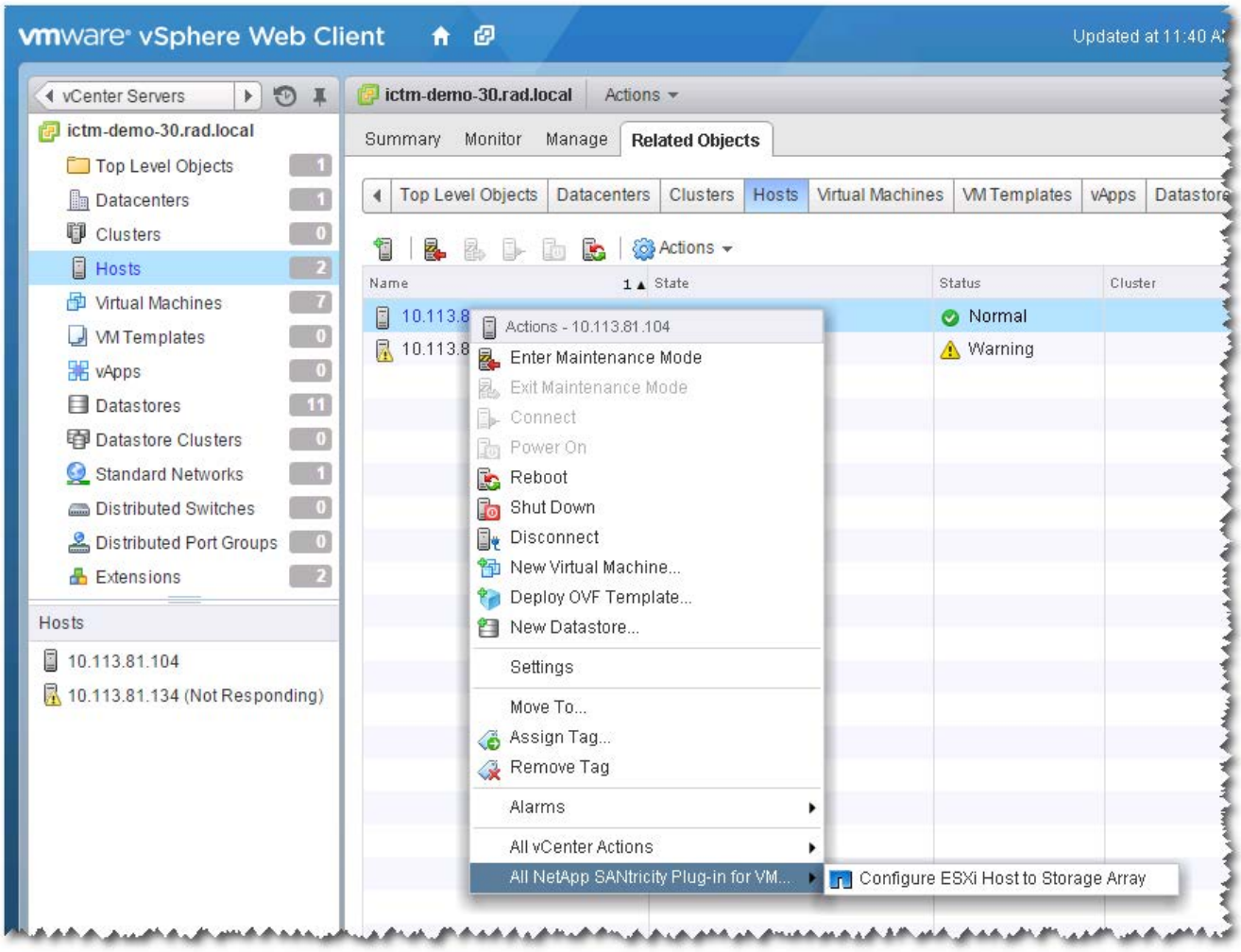
```
~ # esxcli software vib list |grep LSI
lsiprovider            500.04.V0.54-0004          LSI     VMwareAccepted    2015-02-05
```

Configuring ESXi Hosts to Storage Arrays

Note: Before configuring ESXi hosts to storage arrays, you must already have added or discovered storage arrays within your environment (see Add Array and Discovery Arrays sections).

To use the Automatic Host Configuration utility, navigate to **Hosts** within the Web Client, and select the ESXi host to be configured; Right-click the ESXi host, and select **Configure ESXi Host to Storage Array** from the pull-down menu under **All NetApp SANtricity Plug-in for VMware vCenter Actions**.

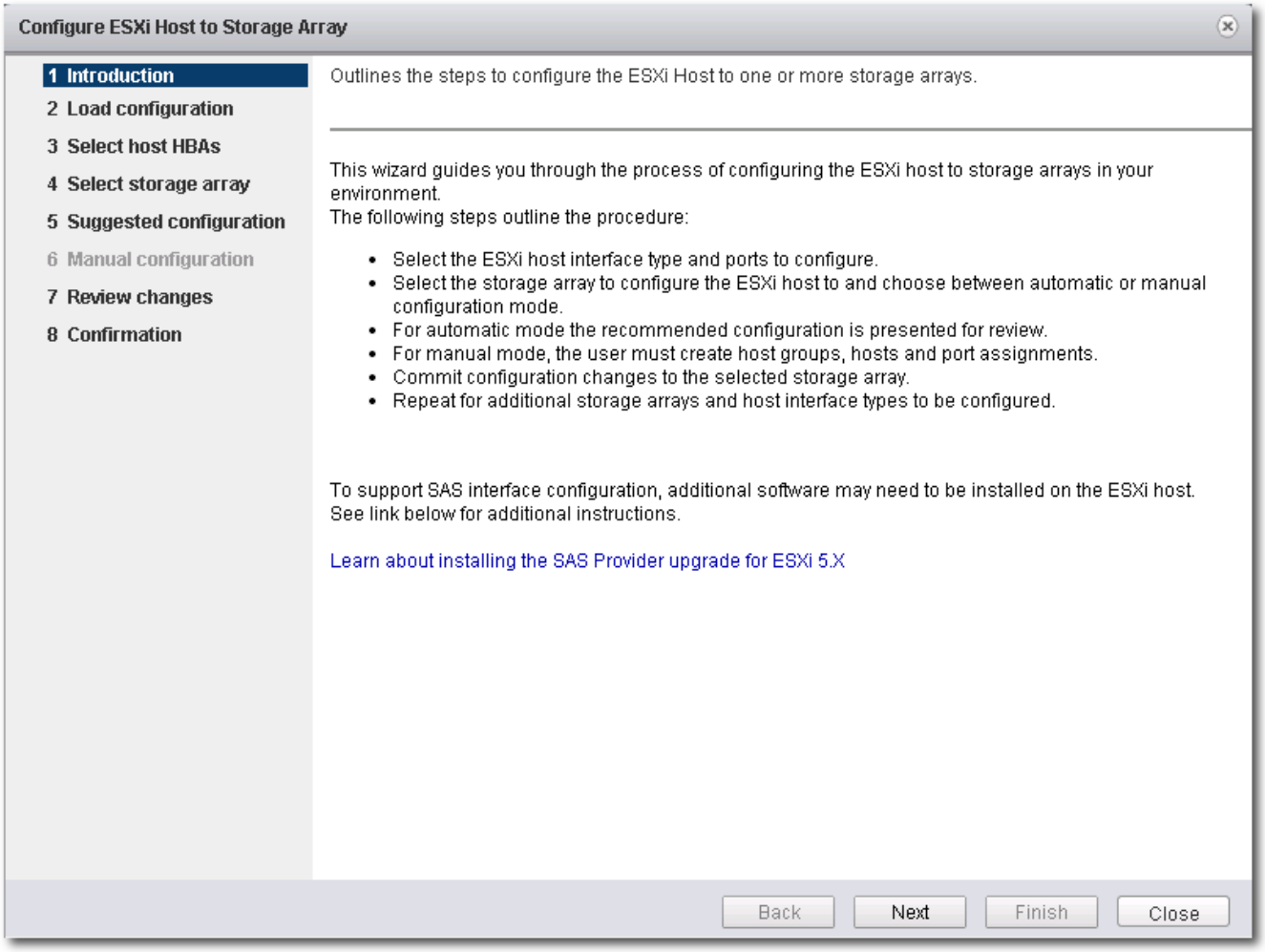
Figure 15) Configure ESXi Host to Storage Array Configuration Wizard Menu.



This launches the **Configure ESXi Host to Storage Array** wizard. From this wizard, you can see how the current ESXi 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 ESXi host to another storage array.

Configure ESXi Host to Storage Array Wizard

Figure 16) Configure ESXi Host to Storage Array Wizard.



The wizard will walk through the process of configuring the HBAs on the selected ESXi host to the storage arrays configured within the Array Manager. The wizard also provides additional information needed to detect and configure SAS HBAs within the ESXi hosts.

1. Click **Next** after reading through the Introduction page.

The Inspect Configuration page is then initiated which verifies user privileges, gathers information on the selected ESXi host, and gathers information on the configured storage arrays. This process may take a few minutes depending on the number of HBAs, and storage arrays configured within the system.

2. Click **Next** after all three discovery process complete and three green check marks are displayed.

The Select Host HBAs page allows for selection of the HBAs to be configured from the ESXi host. Select the radio button next to the interface type to be configured. It is recommended to select all of the HBA ports that will be configured for the target storage array.

3. Click **Next** after selecting the HBA ports to be configured.

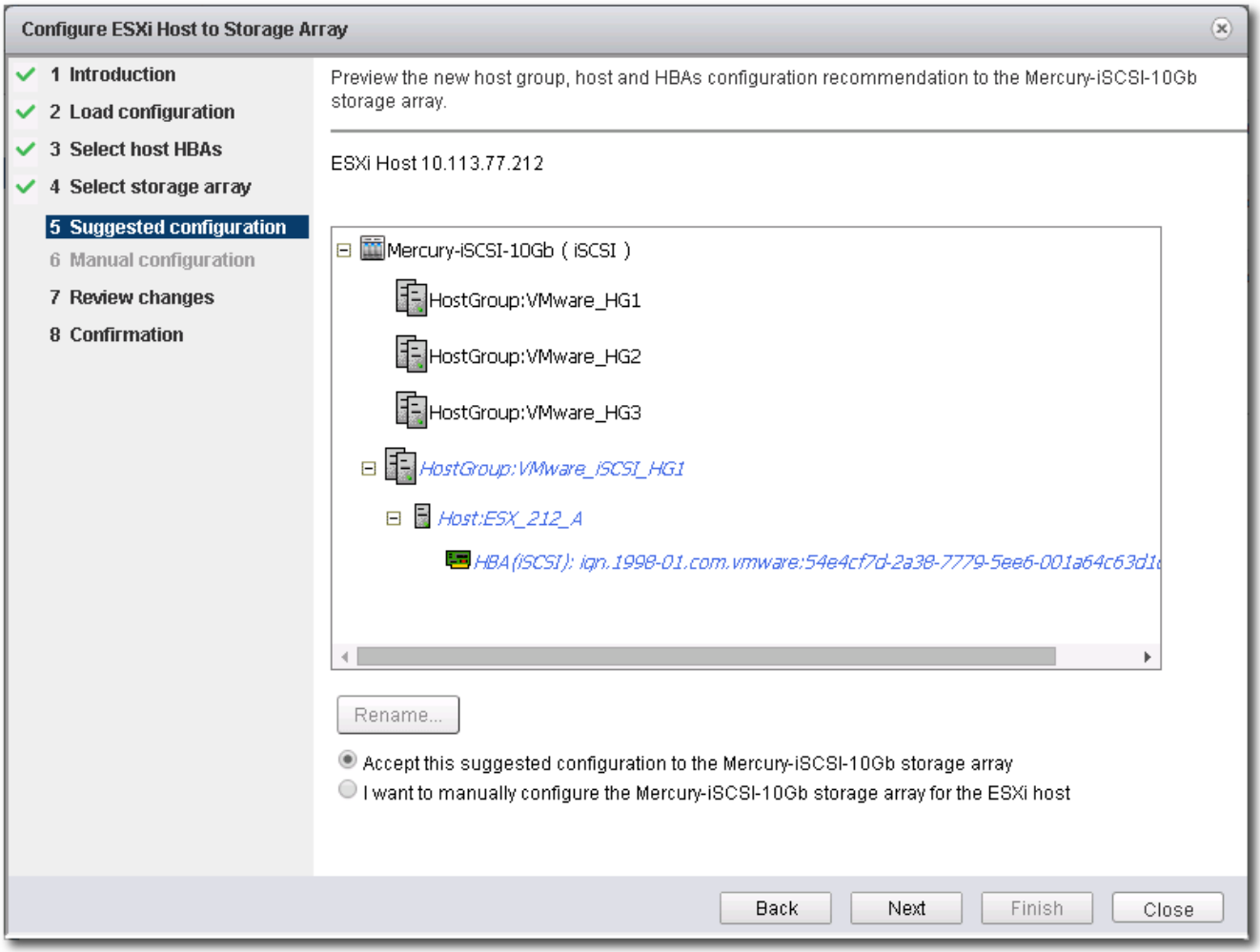
The Select Storage Array page is then displayed.

4. **Select** the storage array that will be used by the ESXi host being configured. Click **Next** after selection.

The Suggested Configuration page is then displayed showing the recommended HBA port configuration, host configuration, and host group configuration. The suggested changes are displayed in blue italics (see Figure 17).

5. To accept the suggest configuration, click **Next** or to manually configure the ESXi host, select the **Use manual configuration** radio button and click **Next**.

Figure 17) Suggested ESXi Host Configuration.

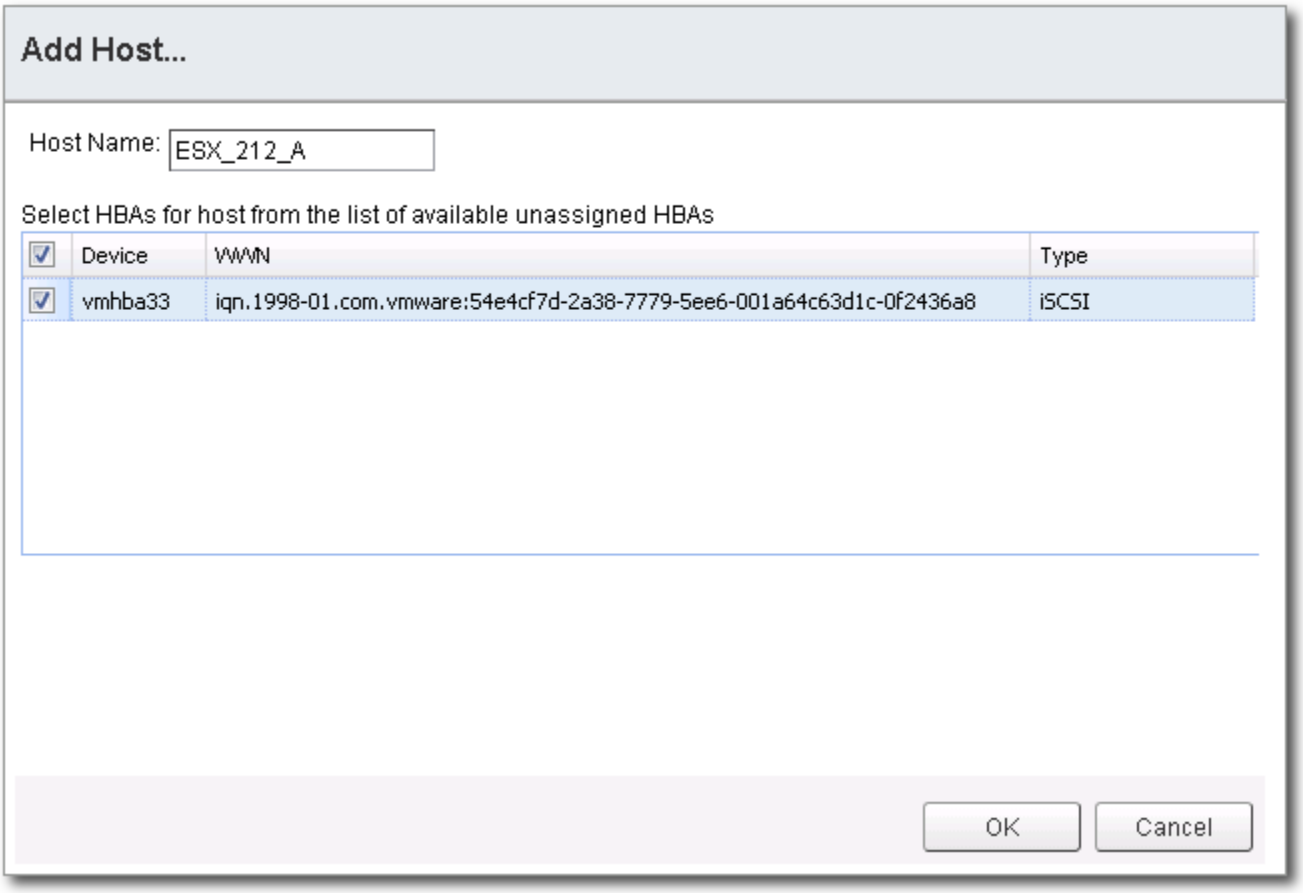


If the **manual configuration** radio button was selected, the Manual Configuration page will be displayed. If the ESXi host will be participating in a cluster configuration with other ESXi hosts, and no existing host group exists for the cluster configuration, select the storage array name and click the **Add Host Group** button. Enter the name for the new host group and click **OK**. If the host group for the cluster already exists, select the host group name to add this host to. Click **Add Host** button and enter the name for this ESXi host and select the check boxes next to the HBAs to be used for the host definition (see Figure 18).

6. Select **Next** after completing manual configuration.

Note: Additional host configurations should be placed in a different host group from the previously defined host.

Figure 18) Manual Add Host Dialog.



Note: The Configure ESXi Host to Storage Array wizard does not detect how the switch fabric is zoned and suggested configurations are based on how the HBA ports are detected. The suggested configuration may require the FC fabric to be rezoned based on the environment's cabling.

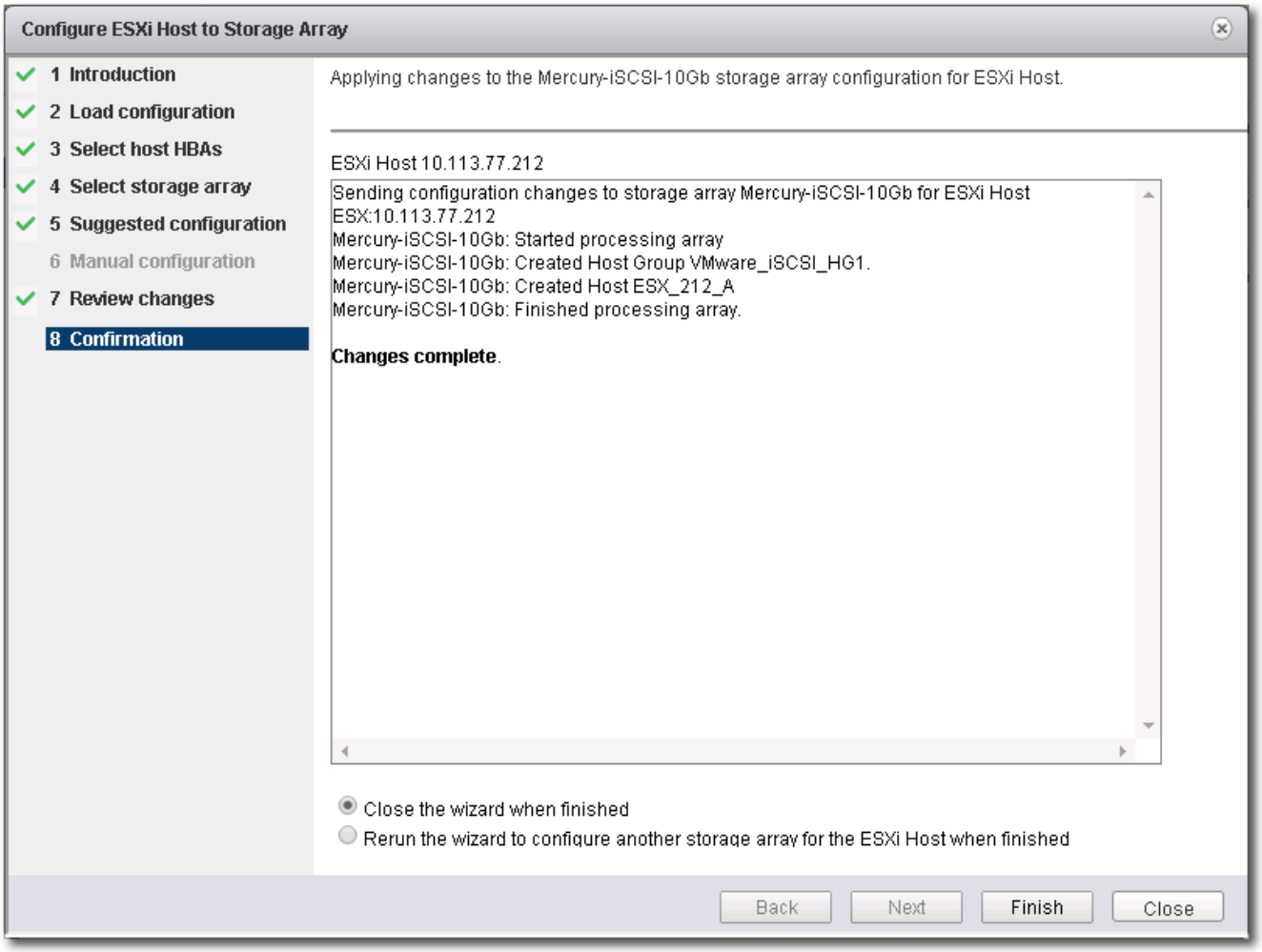
You cannot rename or remove existing configured hosts or host groups. Existing host and host group configuration changes must be performed from the storage management software. Click **Next** after all host groups and hosts have been defined.

7. The Review Changes page is then displayed showing what changes will be applied to the storage array. If you are satisfied with the changes, click the **Next** button.
8. A real-time summary page is then displayed showing the status of the changes being applied to the selected storage array. Once the changes have been applied, you may select **Rerun** radio button to repeat the configuration process on another storage array or select **Close** button to close the configuration wizard. You must manually close the progress window after the changes are complete.

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

Note: By default, the wizard will only display hosts that are prefixed with 'ESX_' and host groups prefixed with 'VMware_'. Other hosts or host groups configured on the storage array will not be displayed in the wizard unless the **Show all host groups** check box is selected.

Figure 19) Apply Changes Message Box.

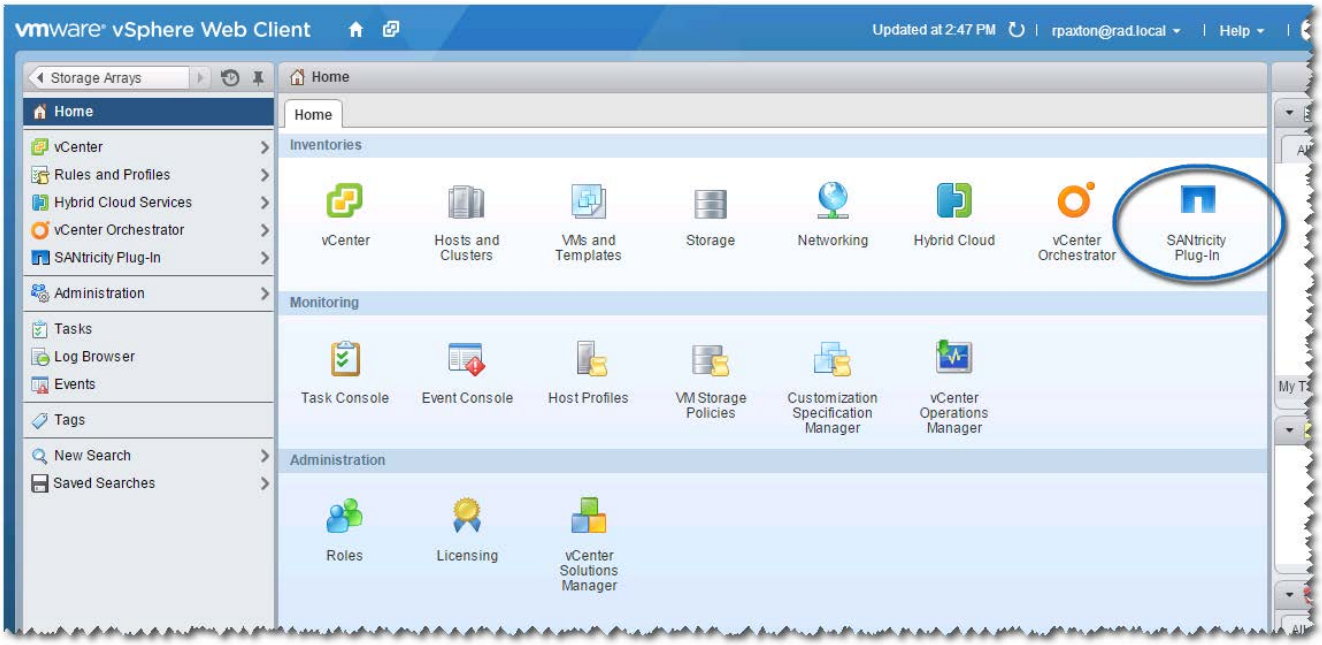


SANTRICITY PLUG-IN MANAGER

SANtricity Plug-in Features

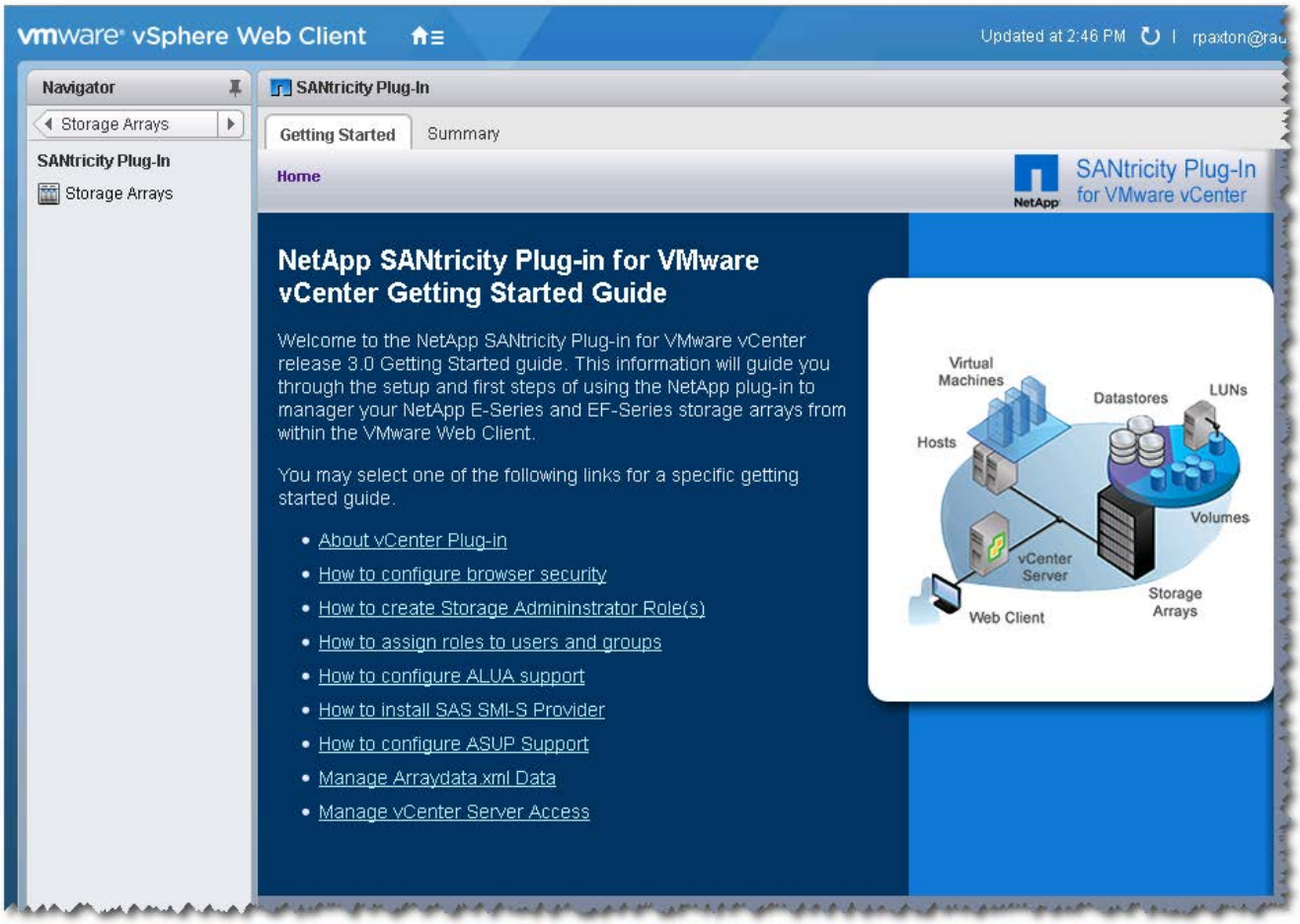
To use the SANtricity plug-in to manage NetApp E-Series and EF-Series storage arrays, click the **SANtricity Plug-in** icon on the Web Client home page in the Inventories section.

Figure 20) NetApp SANtricity Plug-in for VMware vCenter Icon.



This will display the Storage Arrays container, in the leftmost window and the **Getting Started** page in the main window. The **Storage Arrays** container provides direct access to management of the configured storage arrays within the plug-in. The **Getting Started** pages provide help tips to setup and configure the SANtricity plug-in. The **Summary** tab displays summary information for all storage arrays known to the plug-in.

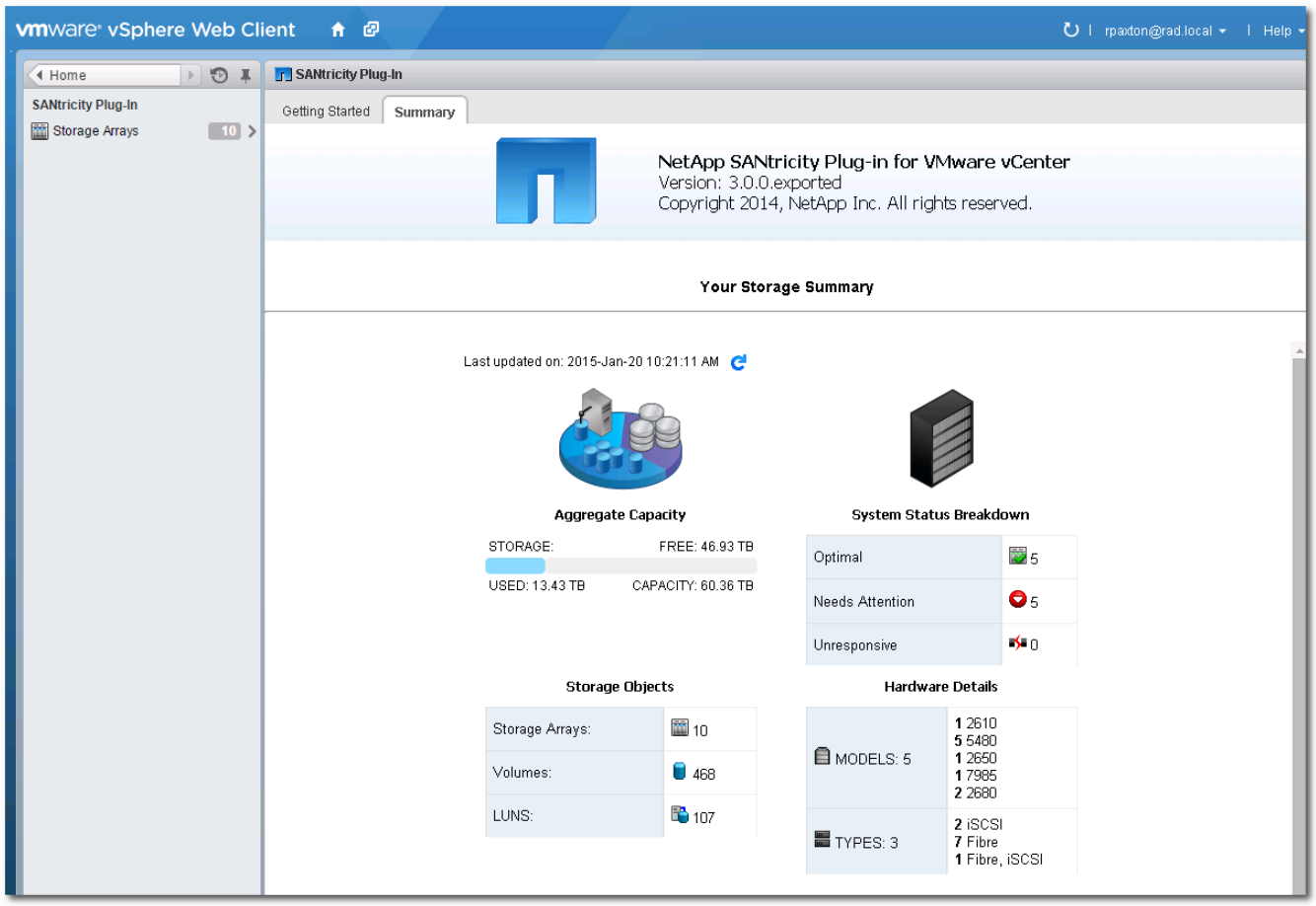
Figure 21) Getting Started page.



The SANtricity Plug-In **Summary** tab provides summary information for all of the storage arrays configured within the plug-in including:

- Plug-in version and copyright
- Aggregate storage capacity
- Storage array status breakdown
- Storage array objects
- Storage array hardware details

Figure 22) Storage Array Summary.

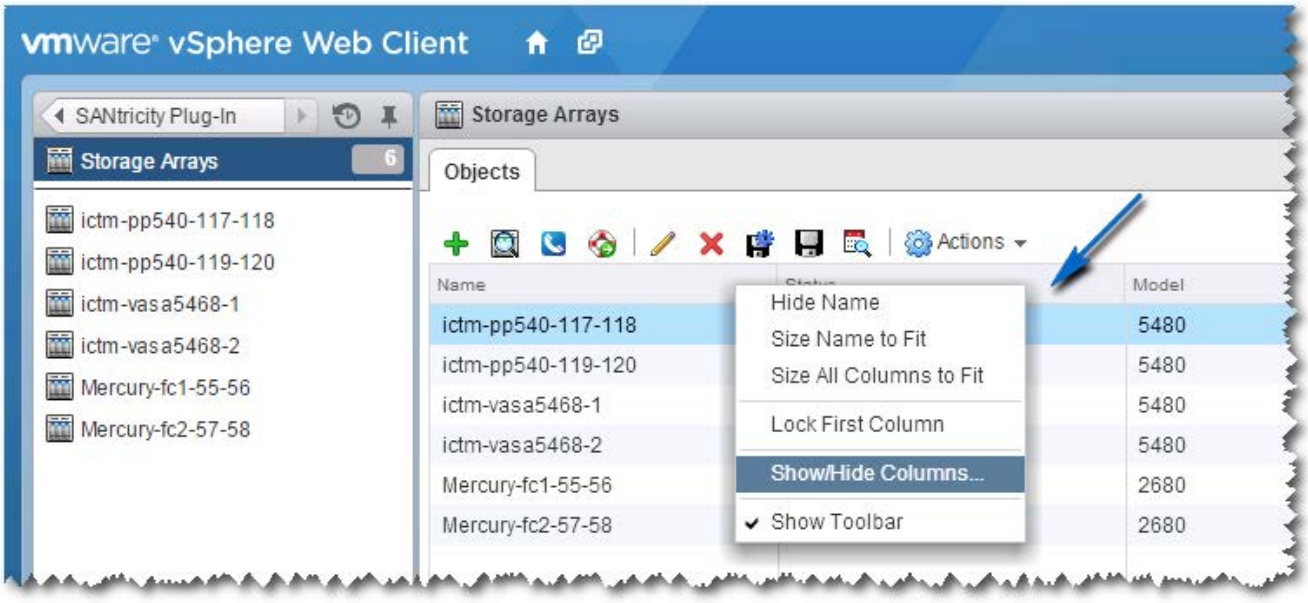


STORAGE ARRAYS OBJECTS VIEW

Storage Arrays Objects View

The Storage Arrays Objects view displays all of the known storage arrays in a list view that can be customized by selecting one of the drop-down arrows from the column headers and selecting which columns to display. The columns can also be sorted.

Figure 23) All Storage Arrays Table View.



The Storage Arrays container view shows a list of known storage arrays and lets additional storage arrays be added or removed. The following options are available from the storage array manager view:

- Add Storage Array....
- Discover Storage Arrays….
- AutoSupport….
- Collect Support Bundle….
- Edit Storage Array….
- Remove Storage Array….
- Configure Auto Save….
- Manual Save Config….
- View Event Log….

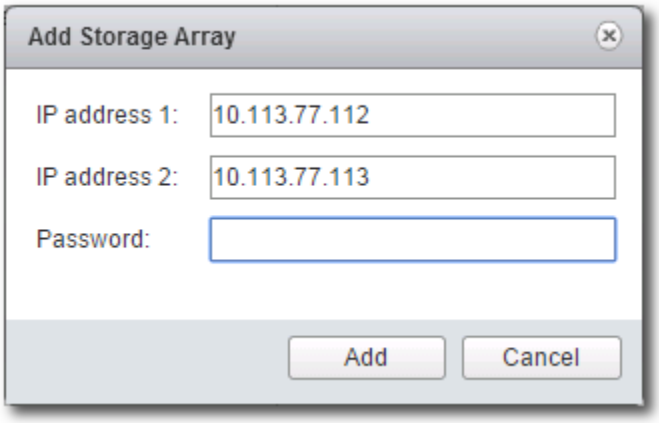
Add Storage Array

Add Array provides the ability to add a single storage array to the array manager view and supply the storage array password if necessary. The Add Array also provides the ability to assign asset tags to the new storage array. If multiple arrays need to be added, please see the **Discover Storage Arrays** command.

1. In the Commands area of the NetApp plug-in Array Manager view, click **Add Storage Array**.

The Add Storage Array window opens.

Figure 24) Add Storage Array Window.



2. In the **Controller A** text box, type the IP address or DNS name of the storage array's controller A.
3. In the **Controller B** text box, type the IP address or DNS name of the storage array's controller B.
4. In the **Password** text box, type the password for the storage array that you are adding to the NetApp plug-in.
5. Click **Add**.

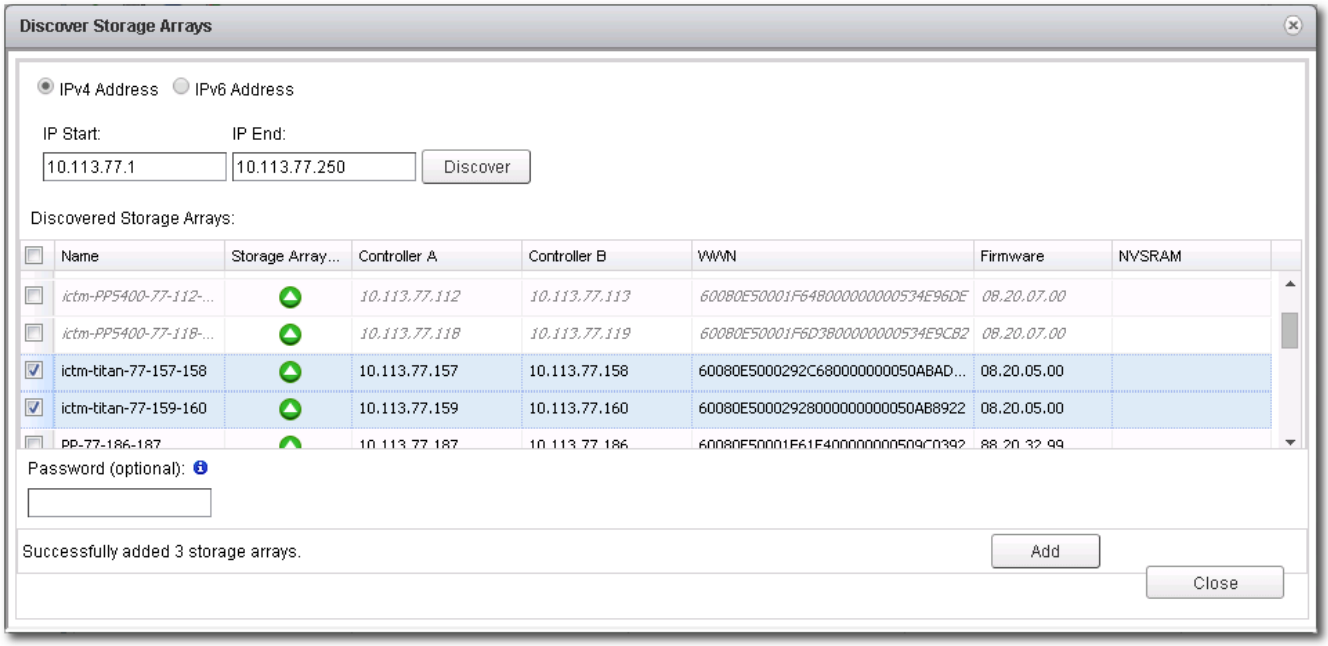
Discover Storage Arrays

The NetApp plug-in supports the ability to auto discover storage arrays within a subnet to add to the Storage Arrays container. To perform an auto discovery:

1. In the Commands area, click **Discover Storage Arrays** icon.

The **Discover Storage Arrays** window opens, Figure 25 with **IP Start** and **IP End** along with the global array **Password** settings box.

Figure 25) Discover Storage Arrays Window.



2. Enter the starting TCP/IP address of the IP range to discover storage arrays on.
3. Enter the ending TCP/IP address of the IP range to discover storage arrays on.
4. Click **Discover** button to start the scan.

Note: This may take several minutes depending on the scope of discovery.

5. (Optional) If the same array password is used for all the arrays to be added, you can specify it now in the **Password** textbox.
6. Click **Add** to add all selected storage arrays to the NetApp plug-in Array Manager.
7. Click **Close** button to close the Discover Storage Arrays window when finished adding arrays.

AutoSupport

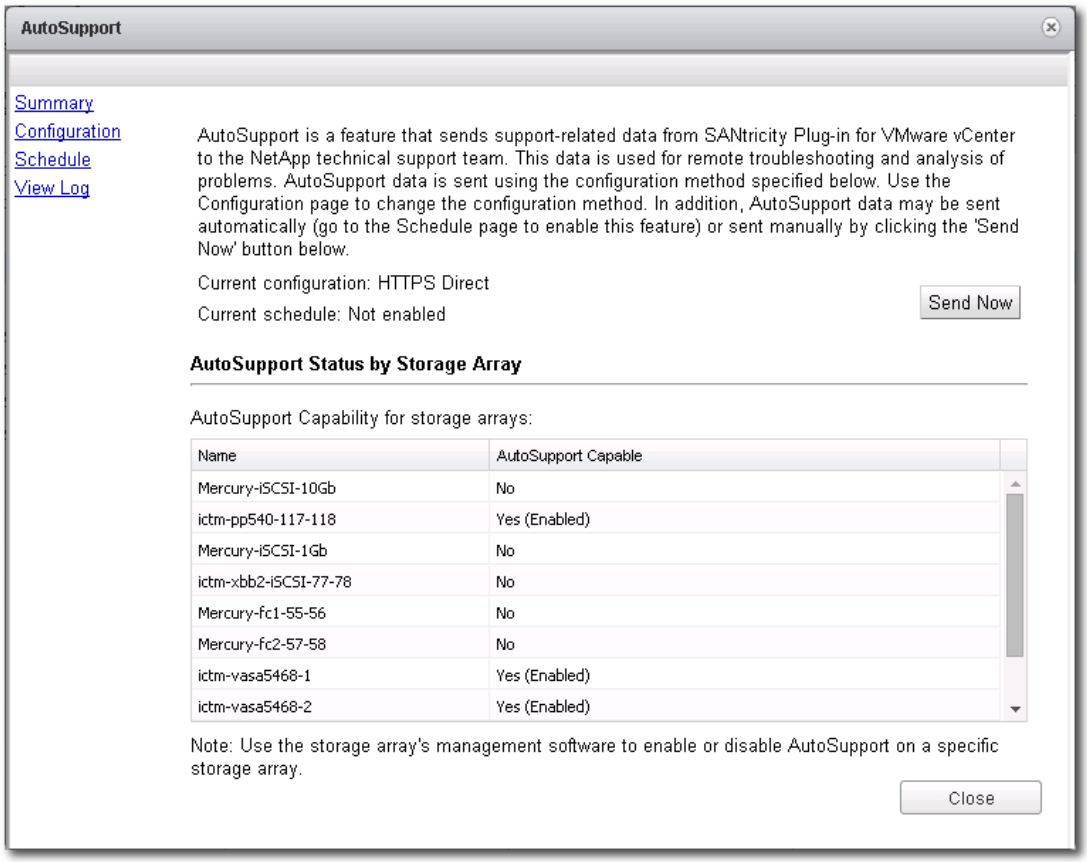
One of the new features of this release is the ability to configure AutoSupport. This feature allows the NetApp SANtricity Plug-in for VMware vCenter to send information to NetApp technical support team to remotely diagnosis issues within the system. The information also provides NetApp with details on how the plug-in is being used to assist in future development. To enable AutoSupport (ASUP), perform the following:

1. From the Objects tab under Storage Arrays click the **AutoSupport** icon.

The **AutoSupport** wizard is then displayed.

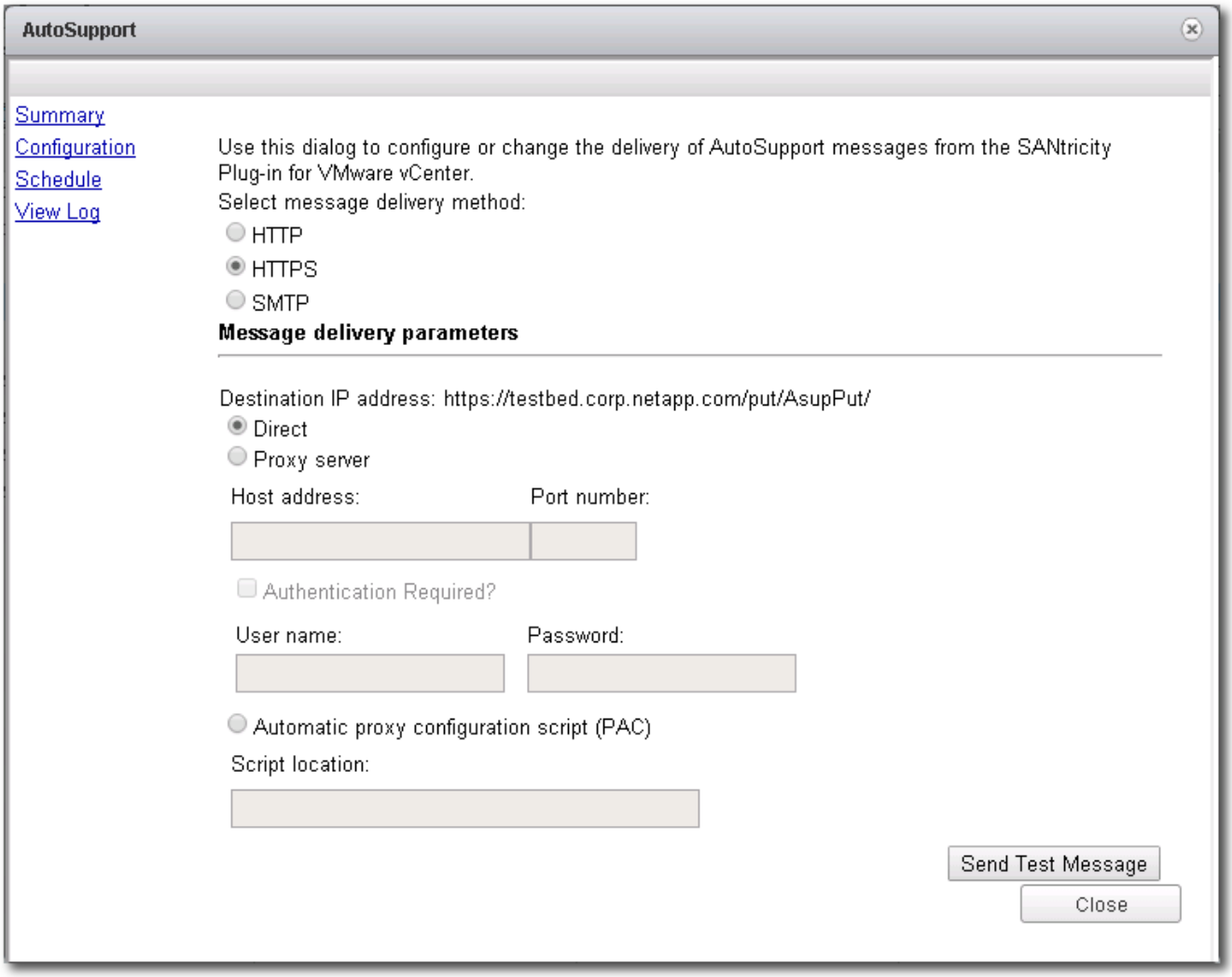
2. From the Summary page, you have the option to immediately send a support bundle via the currently configured configuration. You are also shown a display of your current storage arrays and their AutoSupport status (you cannot modify their status from within the plug-in; you must configure them from NetApp SANtricity Storage Manager).

Figure 26) AutoSupport Wizard, Summary Page.



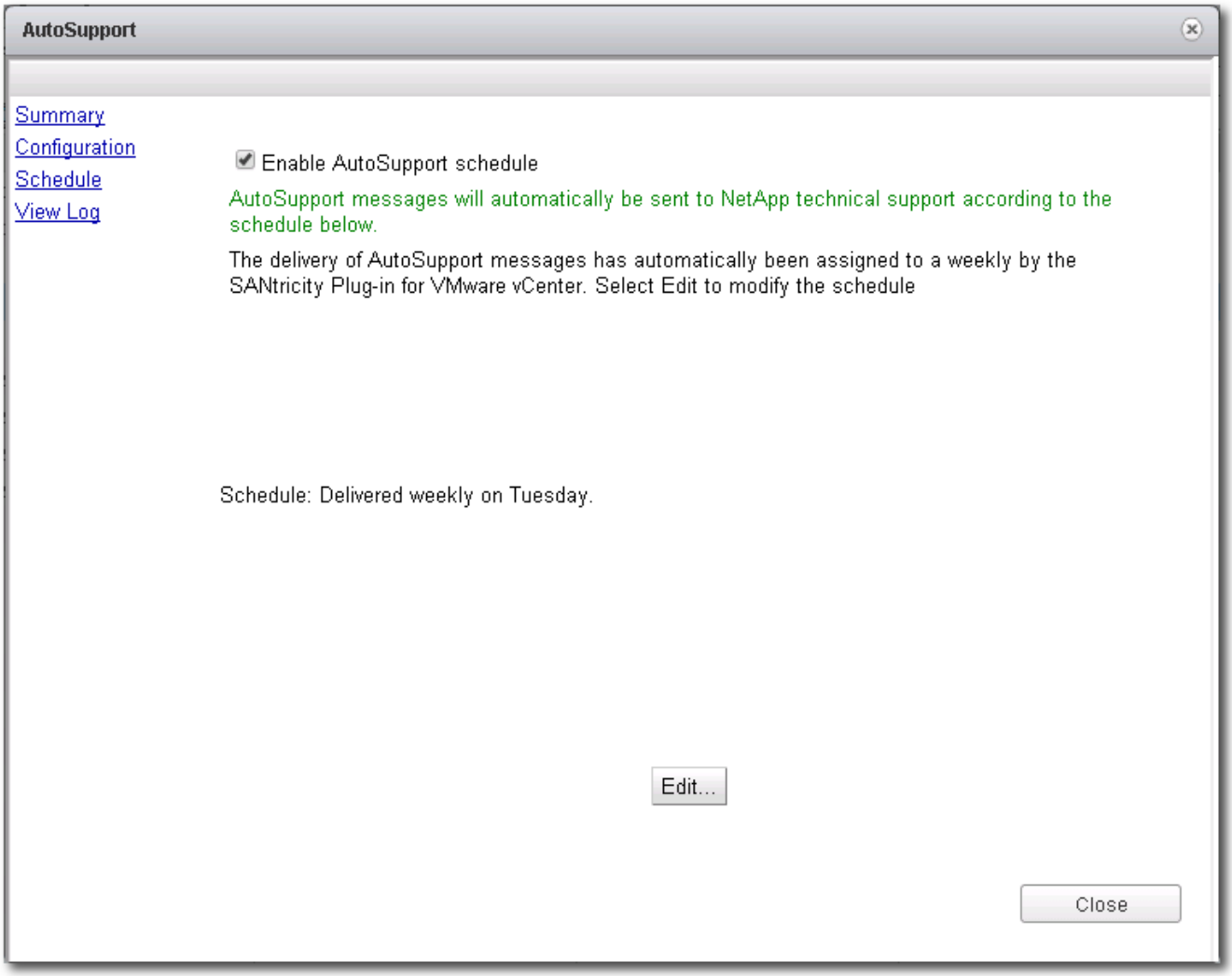
3. From the Configuration page, you have the option to configure how the AutoSupport information is sent to NetApp.

Figure 27) AutoSupport Configuration Wizard.



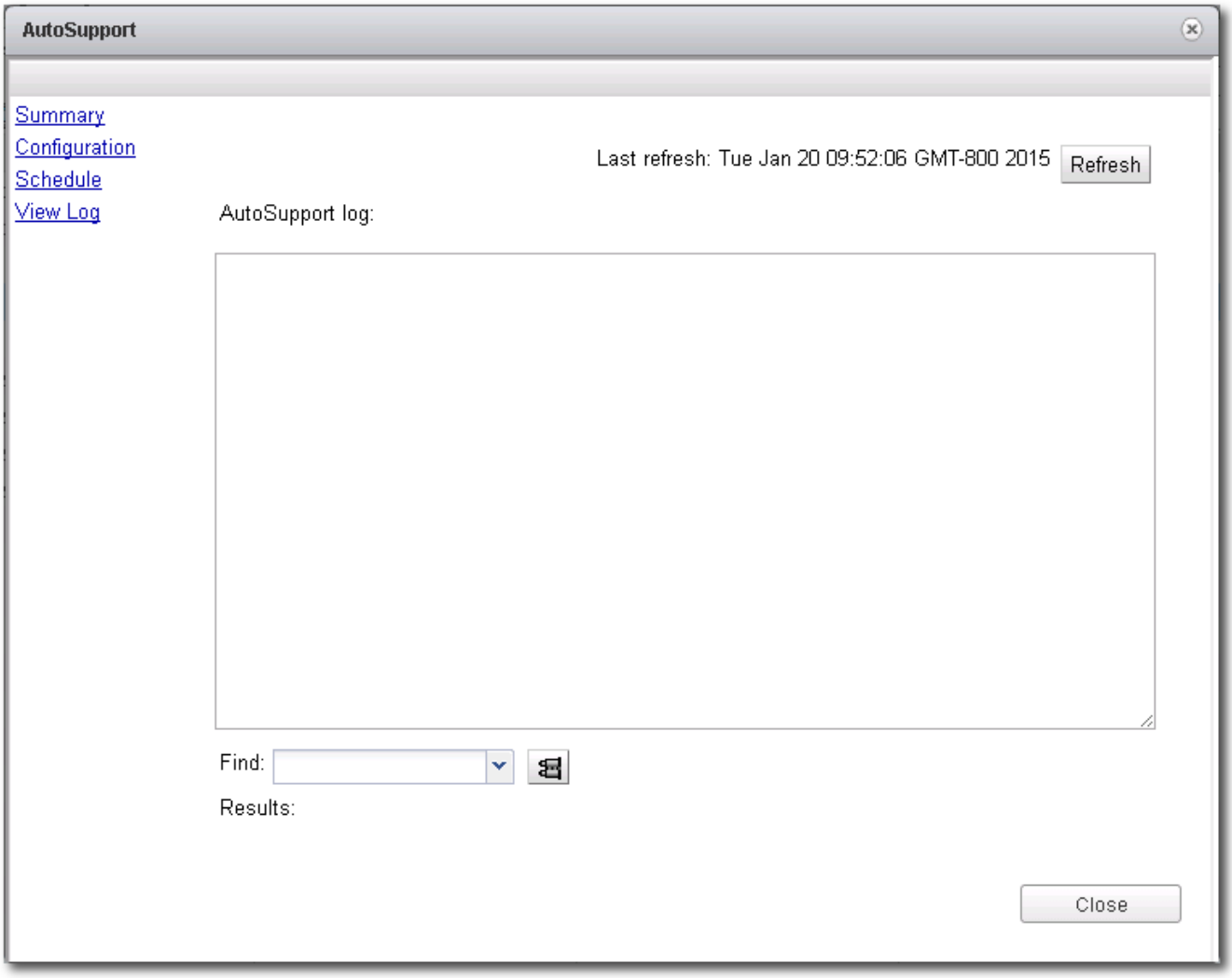
4. From the Schedule page, you have the option to enable schedule transmissions of the AutoSupport information and to configure when the transmissions will occur using the **Edit** option.

Figure 28) AutoSupport Schedule Wizard



5. The View Log page displays a list of past transmissions and their status.

Figure 29) AutoSupport View Log Wizard

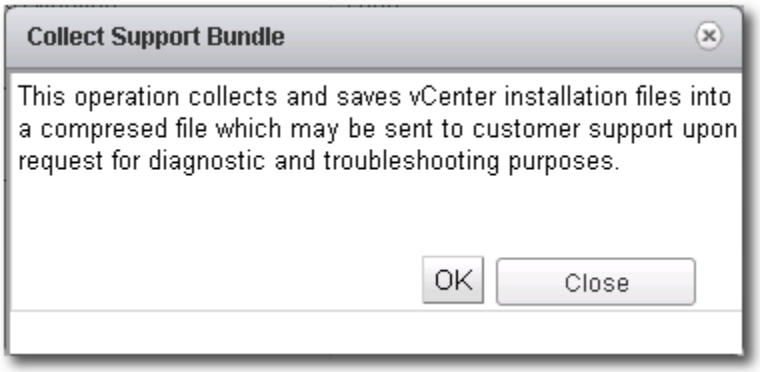


Collect Support Bundle

The collect support bundle option performs an automatic collection of logs and configuration information on your environment to be used by technical support to assist in problem resolution. To generate a support bundle, perform the following:

1. Select the target storage array in the right pane (table list).
2. Click the **Collect Support Bundle** icon (be patient, this may take some time).
3. Your default browser should open a file save dialog.
4. Accept and complete the file download depending on your browser's settings.
5. Click **Close** to finish the operation.

Figure 30) Collect Support Bundle Dialog Box.

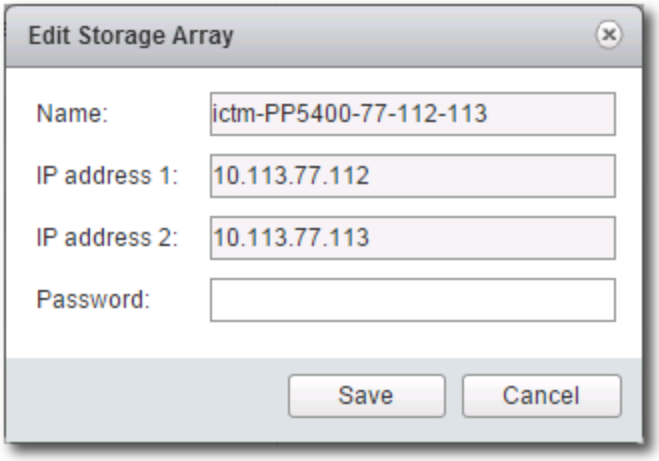


Once the file has been downloaded to your system, named **vcpsupport_<*date*>.zip**, you may then send it to NetApp technical support upon request.

Edit Storage Array

The **Edit Storage Array** option provides the ability to modify the selected storage array. Select the storage array to modify and click the **Edit Storage Array** icon. You will then have the ability to modify the settings for the selected array.

Figure 31) Edit Storage Array Dialog Box.

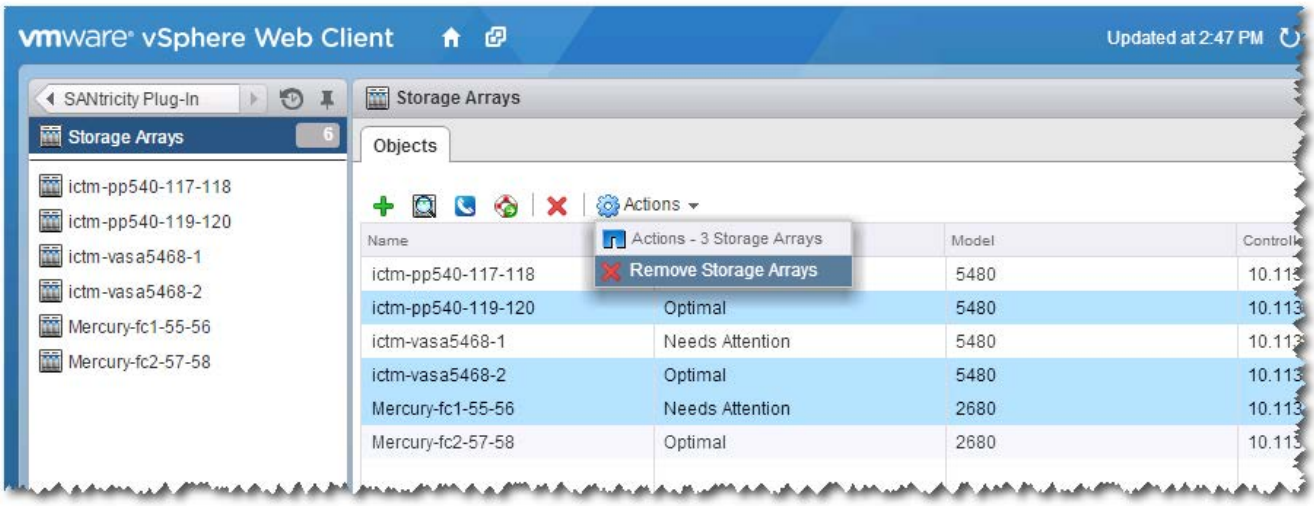


Remove Storage Arrays

Storage arrays may be removed by either selecting an individual storage array in the Objects view or by selecting multiple storage arrays.

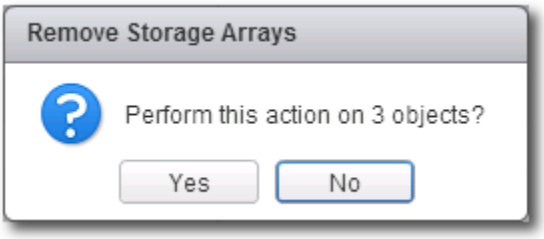
1. In the Web Client Storage Arrays Objects tab, **select** the Storage Arrays to be removed.
2. Click the Remove Storage Arrays icon.

Figure 32) Remove Multiple Storage Arrays Window.



The Remove Storage Arrays confirmation box appears.

3. Select **Yes** to verify removal of selected arrays.



Storage Array Save Configuration

The NetApp plug-in supports storage array configuration backups to script files that can be applied to a storage array from the NetApp SANtricity ES Storage Manager software. These script files facilitate the restoration of the storage array configuration, such as storage array name, volume group configurations, volume names, and volume capacities.

CAUTION: The NetApp plug-in does not back up data residing on the storage array. You must use a standard backup strategy to recover user data that resides on the volumes.

The NetApp plug-in Automatic Save Configuration feature performs a save configuration of the storage array after a configuration event has occurred on the storage array, either from the NetApp plug-in or from the storage management software.

CAUTION: Only the configuration information for the storage array is saved during a save configuration operation. Data stored on the volumes is not saved.

Note: Only the base storage array configuration information is saved. Objects such as snapshots, volume copies, and remote mirrors are not saved to the script file.

A storage array modification event starts a four-minute timer, on the application server, at the time of the event on the storage array. If within that four-minute time window, no other configuration events have occurred on the storage array, a save configuration occurs. If another modification event occurs within the four-minute time window, the timer is reset to four minutes. When no modification events are detected on the storage array within the four-minute

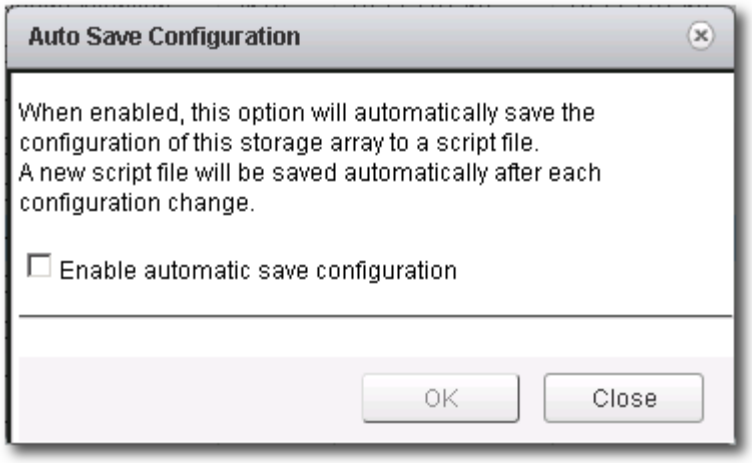
time window, a save configuration is performed. Automatic Save Configuration maintains the last 15 save configuration script files.

Enabling 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. Select the target storage array from the list of managed storage arrays.
2. Click the **Auto Save Config** icon.

Figure 33) Auto Save Configuration dialog box.



3. Select the **Enable automatic save configuration** checkbox.
4. Click **OK**.
5. Click **Close**.

Note: After automatic configuration backups are enabled, they are persisted between restarts of the NetApp application server and vCenter Server. To disable automatic save configuration, clear the check box in the **Automatically Save Configuration** dialog box.

Note: The automatic backup script files are located in the following directory: **`C:\Program Files\NetApp\SANtricity Plug-in for VMware vCenter\jetty\working\savecfg.`** The files are name *<storage_array_name>_<date_time_stamp>*`.cfg`.

Performing a Manual Save Configuration

To perform a manual save configuration, perform these steps from Storage Arrays Objects tab:

1. In the right pane, click the name of the storage array.
2. Click the Manually Save Configuration icon.

The Manual Save Configuration dialog box appears.

3. Click **OK**.

Note: You may receive a security alert informing you are about to leave a secure Internet connection. Select **Yes** to continue.

Note: If you receive an error message stating your current security settings do not allow this file to be downloaded, you must add the secured http address for your application server to the trusted sites list inside of Internet Explorer.

The **File Download** dialog box appears.

4. Click **Save**.
5. Click **Close** to complete the action.

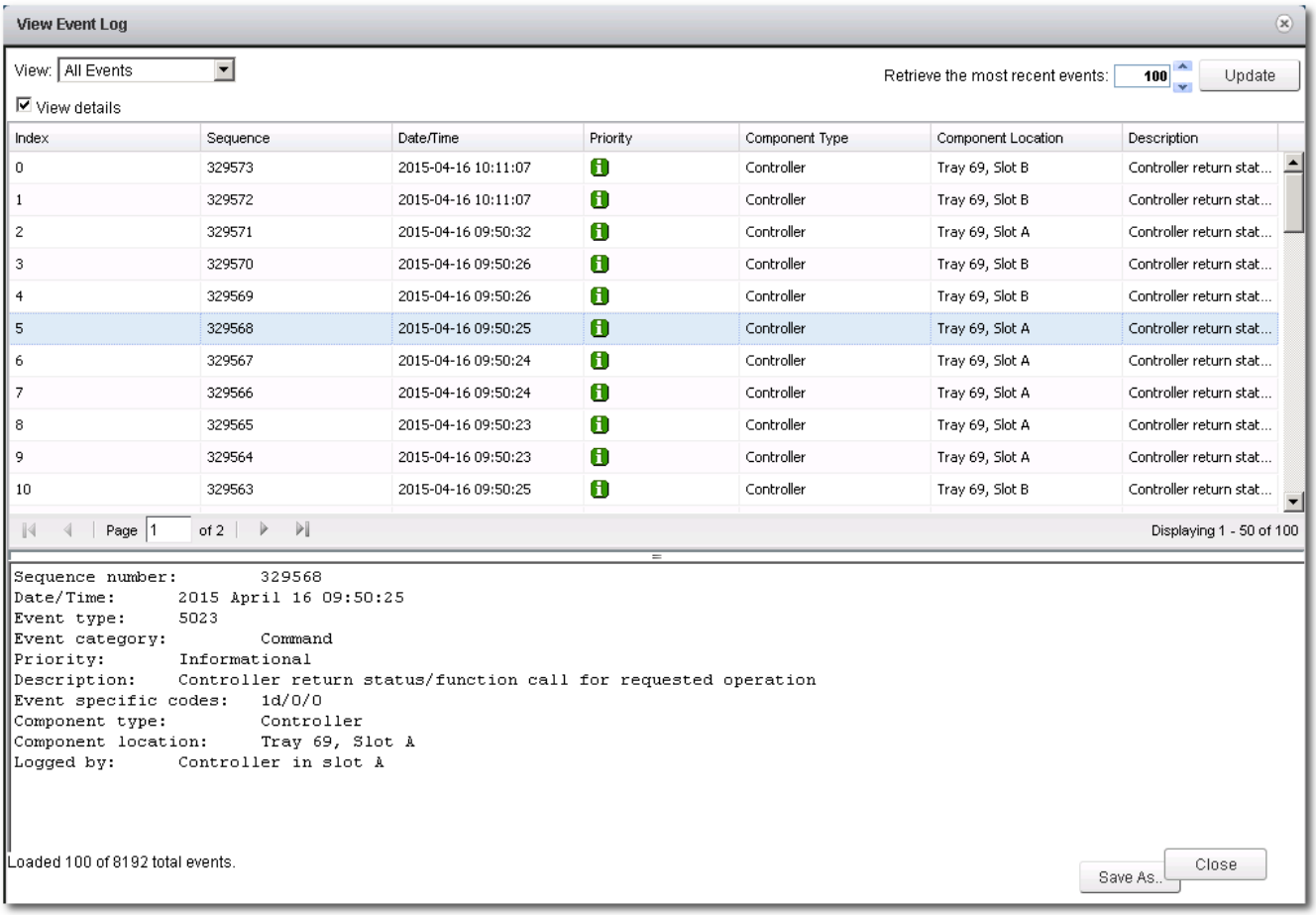
View Event Log

The View Event Log utility provides access to the selected storage array's major event log. To access a storage array's major event log, perform the following:

1. **Select** a storage array from the list of managed arrays.
2. Click the **View Event Log** icon, or **View Event Log** option from the Actions drop-down menu.

The View Event Log utility is displayed.

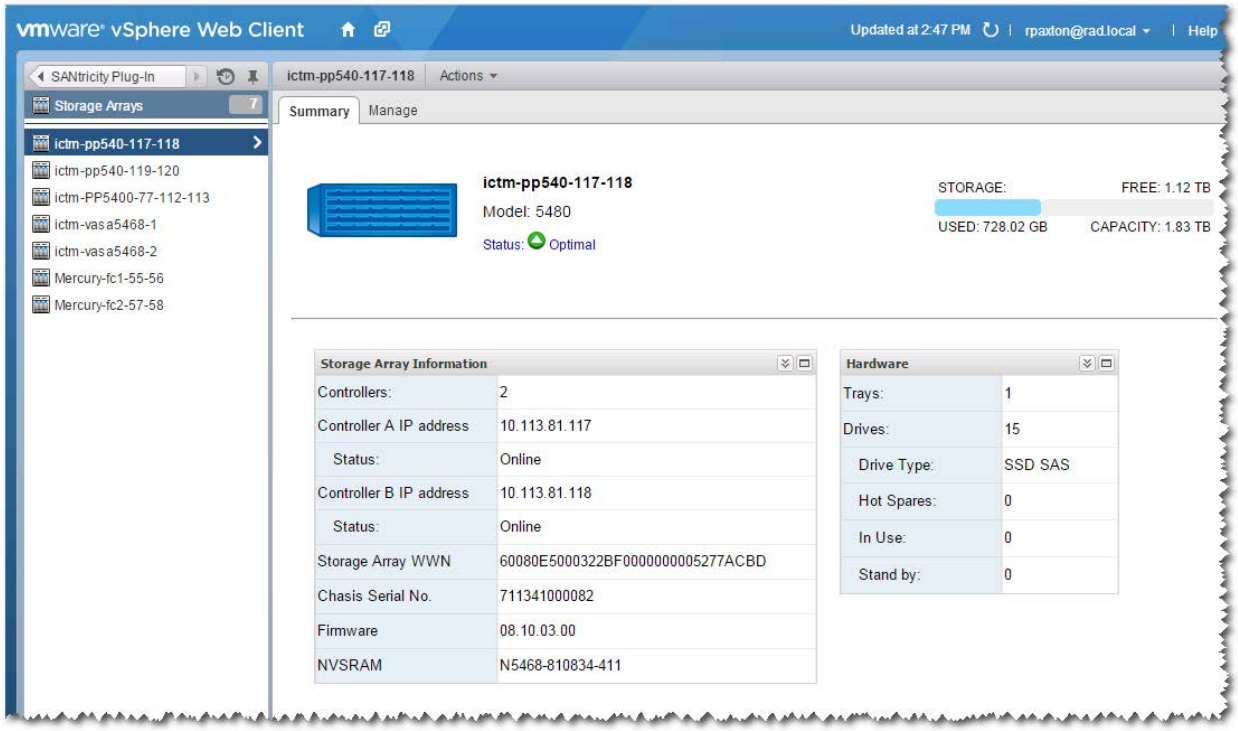
Figure 34 - View Event Log display.



SELECTED STORAGE ARRAY SUMMARY TAB

Clicking on a storage array from the Storage Arrays list displays a summary of the selected storage array. This includes information on the status of the storage array, the number of controllers, their status, their IP addresses, the storage array WWN, the chassis serial number, firmware and NVSRAM versions, along with drive information. The storage array Summary tab also provides access to the Recovery Guru information, if the storage array is non-optimal; a Needs Attention link will be activated detailing the issues with the current storage array.

Figure 35) Storage Array Summary Tab.



Summary View General Information

The Summary view tab provides general information for the select storage array within the Storage Array Information portlet. The details displayed in this area include:

- Number of controllers
- Controller IP addresses
- Controller status
- Storage array WWN
- Storage array chassis serial number
- Storage array firmware version
- Storage array NVSRAM version

The Summary view tap also provides general information on the selected storage array's drive configuration under the Hardware portlet, which include:

- Number of drive trays
- Number of drives
- Type of drives used
- Number of hot spares defined
- Number of hot spares in-use
- Number of hot spares in stand-by

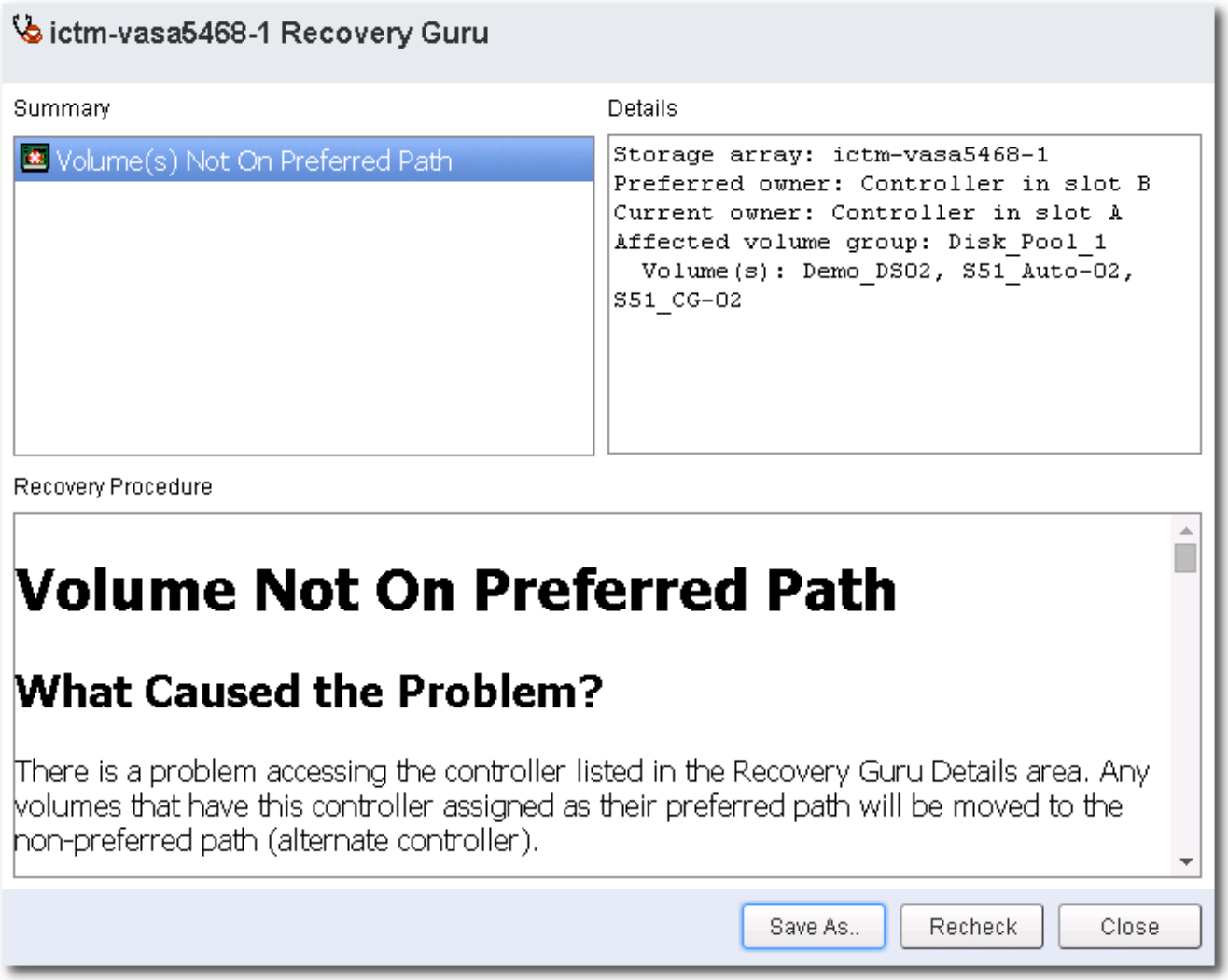
Recovery Guru Information

The Recovery Guru information displays information on issues that are currently affecting the selected storage array. These include the following:

- Summary of issue(s)
- Detail of issue(s)
- Recovery Procedures

Note: The recovery procedures are written to be applied from within NetApp SANtricity Storage Manager and may not be available within the NetApp plug-in. Some issues may be resolved from within the plug-in, but most will have to be applied from the SANtricity Storage Manager.

Figure 36) Recovery Guru Information Window.

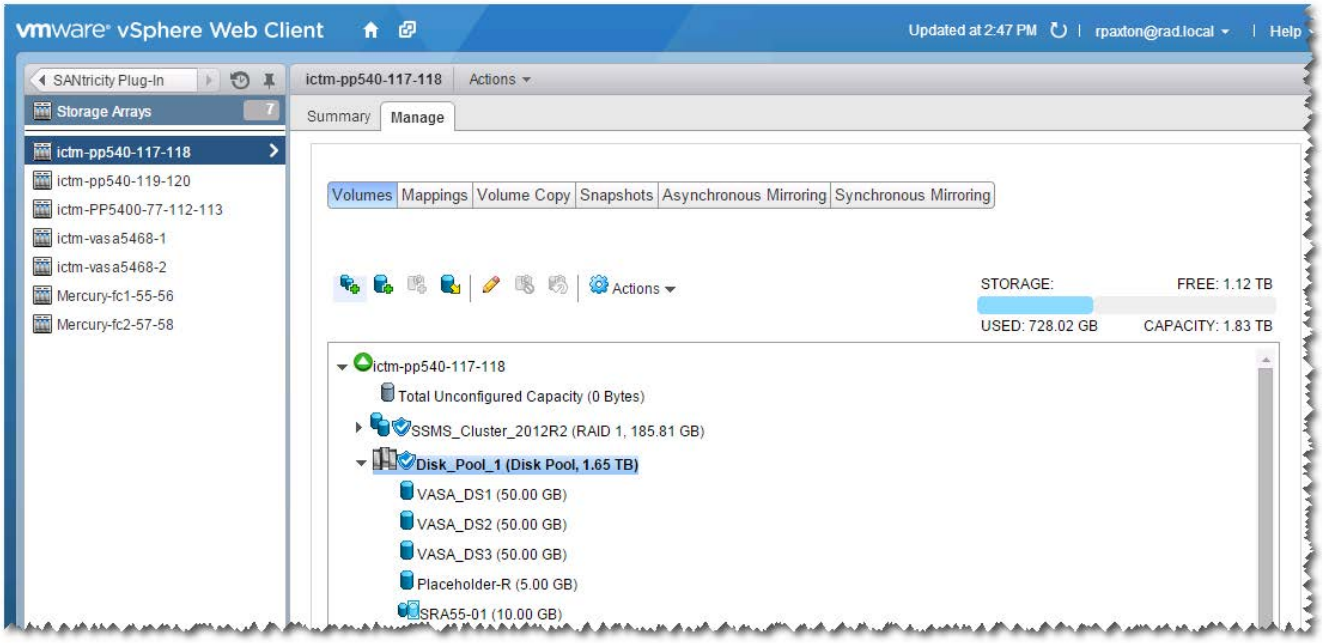


SELECTED STORAGE ARRAY MANAGE TAB

The Manage tab provides for management of the selected storage array. From this tab, you can select one of the following views to work with:

- Volumes
- Mappings
- Volume Copy
- Snapshots
- Asynchronous Mirroring
- Synchronous Mirroring

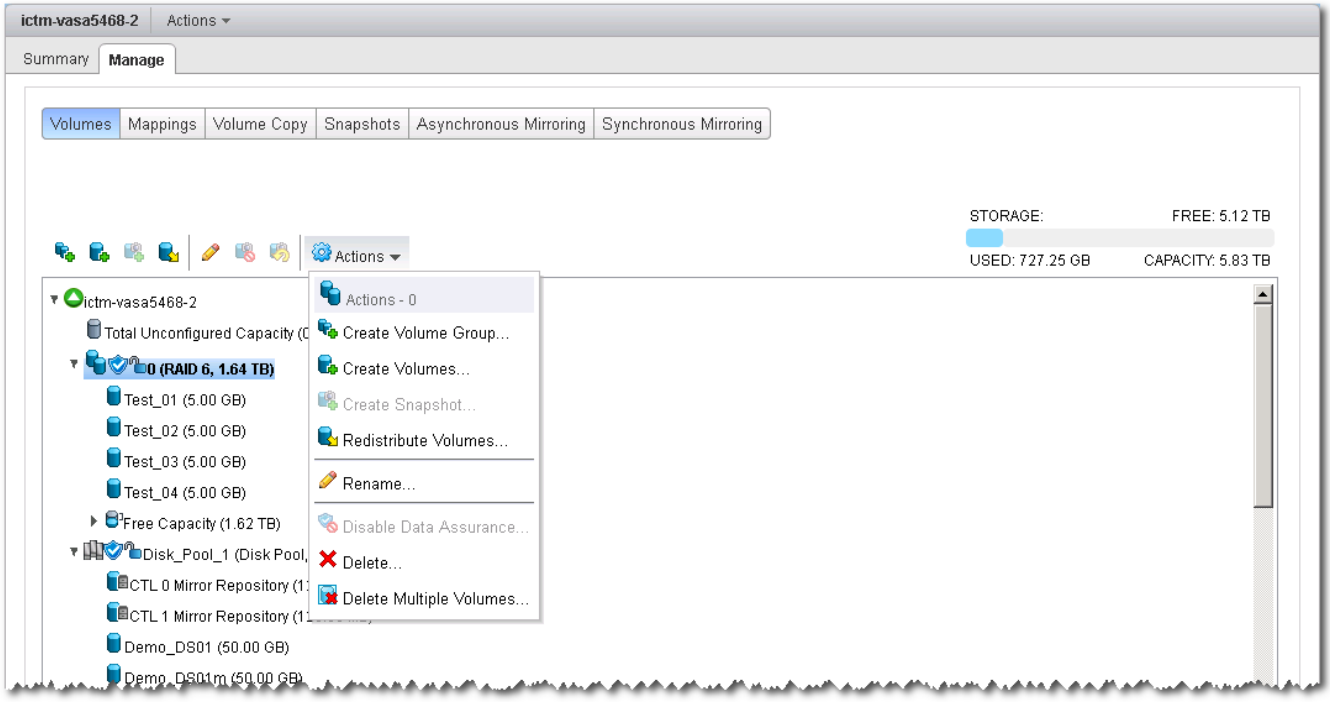
Figure 37) Manage View Tab.



Volumes View Features

Selecting the **Volumes** button shows a logical view of the storage array that displays how storage capacity is allocated. This view allows you to create dynamic disk pools, legacy volume groups, and volumes. This view also provides the ability to manage existing disk pools, volume groups, and volumes along with creating legacy snapshots of volumes. New volumes can be created on either a dynamic disk pool or on a volume group.

Figure 38) Storage Array Volumes View.



- Create Volume Group....
- Create Volumes….
- Create Snapshot….
- Redistribute Volumes….
- Rename….
- Disable Snapshot….
- Recreate Snapshot….

Additional options available from the Actions menu include:

- Disable Data Assurance....
- Delete....
- Delete Multiple Volumes....

Create Volume Group

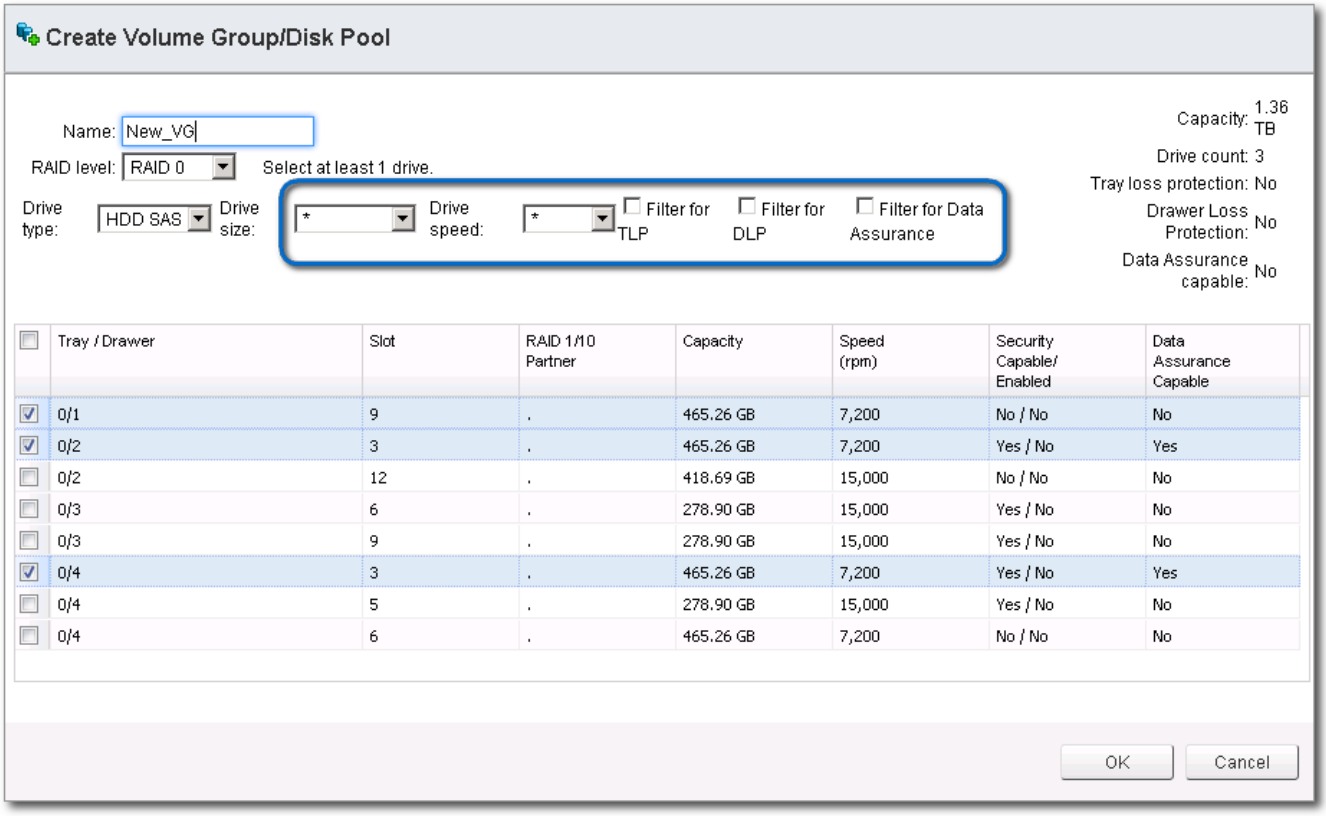
The **Create Volume Group** command launches a wizard to walk you through creating a new volume group. During this process, you must select the available free drives, the drives that will make up the new volume group, and the RAID level.

The volume group wizard has five filtering options to help guide the creation of a new volume group. The first filter allows filtering drives by capacity. This drop-down will display a list of all drive capacities within the storage array. Select the size of the drive to filter by. The second filter option is to filter by drive speed (RPM). This drop-down

will display a list of all drive speeds detected within the storage array. Select the drive speed of the new volume group to apply filter.

The other three filter options allow for enforcement of tray loss protection (TLP), drawer loss protection (DLP), and Data Assurance (DA). By selecting these options, the list of available drives is reduced to allow for TLP, DLP, or DA during the volume group creation process. TLP and DLP allow for a complete drive tray or complete drawer failure without failing the volume(s) within the volume group. DA provides data integrity checking between the controller to the physical drive, ensuring data is written to disk correctly.

Figure 39) Create Volume Group Dialog Box.



Selecting drives in the table view will update the Capacity information in the upper right corner of the display showing the final capacity for the new volume group or disk pool.

Note: Please review Defining Volumes for vSphere and Volume Decision-Making Schemes to best configure the NetApp SANtricity storage for VMware vSphere environments.

Create Disk Pool

Dynamic Disk Pools (DDPs) are a feature of firmware versions 7.83 and later that provide for highly redundant and scalable RAID architecture, also known as Controlled, Scalable, Decentralized Placement of Replicated Data (CRUSH). This technology is used in place of traditional volume groups. Release 3.0 supports creation, management, and deletion of DDPs on the NetApp SANtricity storage arrays. DDP volumes are represented with the icon.

To create a new DDP, click the **Create Volume Group** icon and select Disk Pool in the RAID level dropdown box. Then select the drives to include for the disk pool.

NOTE: A minimum of 11 physical drives must be selected for the creation of a Dynamic Disk Pool.

Create Volume(s)

Before creating a volume useable by vSphere, you must select an existing disk pool with free capacity, select an existing volume group with free capacity, create a new volume group from unconfigured capacity, or create a new disk pool from unconfigured capacity.

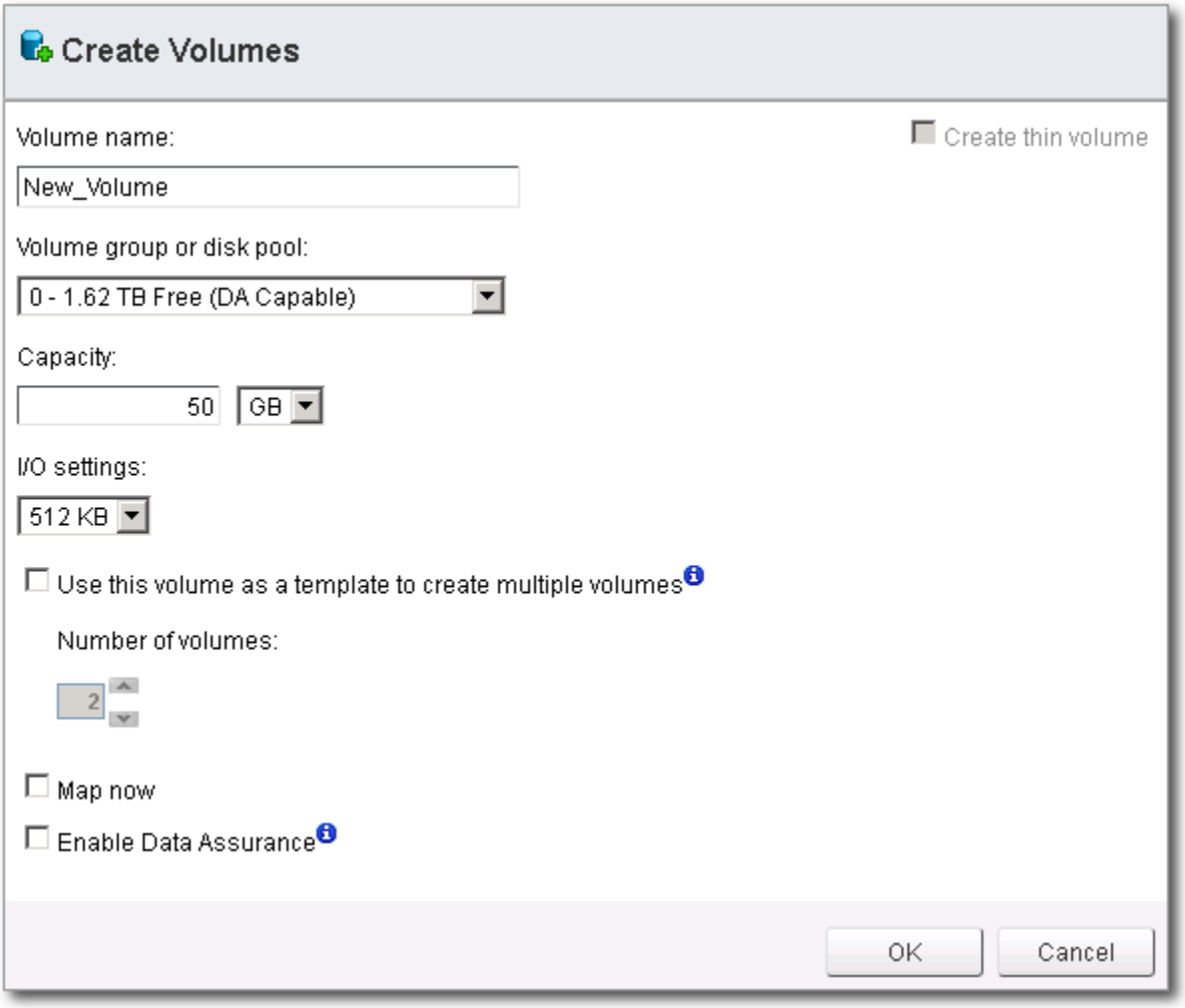
To create a new volume or volumes, click on the icon and perform the following steps:

New Volume on a Volume Group

1. Click **Create Volume** icon.

The **Create Volume** wizard appears.

Figure 40) Create Volume Dialog Box.



2. In the Name text box, type the **Volume Name**.
3. From the Volume Group drop-down list, select a **Volume Group** to use for the new volume.
4. In the **Capacity** text box, type the **size** of the new volume, and select the modifier from the drop-down list.
5. In the **I/O Settings** area, select the segment size for the new volume.
6. (Optional) Select the checkbox if multiple volumes are desired and then select the number of volumes to create.

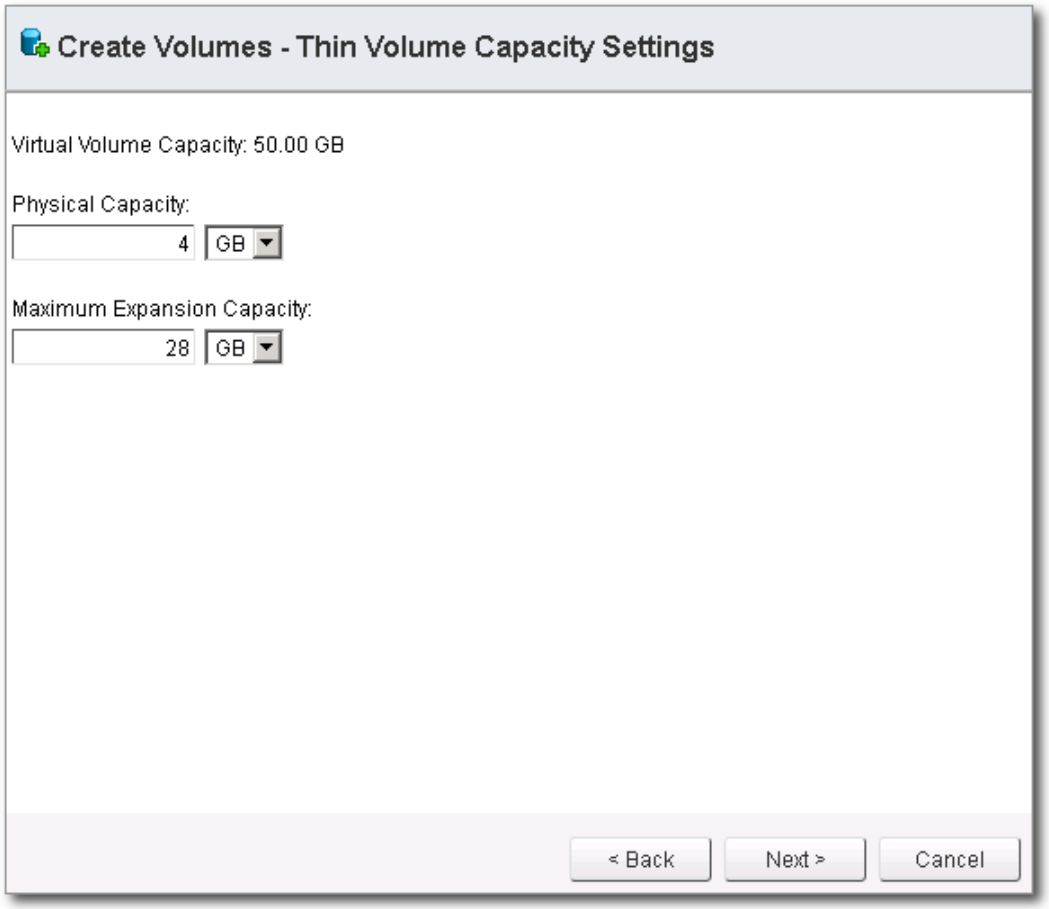
7. (Optional) Select the **Map now** checkbox if the new volumes should be mapped immediately to a host or host group.
8. (Optional) Select the **Enable Data Assurance** checkbox to enable DA for the new volume(s).
9. Click **OK** to create the volume.

New Volume on a Disk Pool

Creating volumes on a disk pool is similar to creating on a legacy volume group, except I/O settings are dictated by the DDP. Also creation of thin provisioned volumes is allowed on DDPs. To create a fat provisioned volume, repeat steps for New Volume on a Volume Group, skipping I/O settings. To create a thin provisioned volume, perform the following steps:

1. Click Create Volume icon.
2. In the **Name** text box, type the volume name.
3. From the **Volume Group or Disk Pool** drop-down list, select a disk pool to use for the new volume.
4. In the **Size** text box, type the size of the new volume, and select the rate from the drop-down list.
5. Click the **Create thin volume** checkbox.
6. (Optional) check the **Map now** checkbox.
7. (Optional) check the **Enable Data Assurance** checkbox.
8. Click **Next**.

Figure 41) Create Thin Volume Dialog Box.



9. In the **Physical Capacity** textbox, type the initial physical size for the thin provisioned volumes (multiple of 4 GB).
10. In the **Maximum Expansion Capacity** textbox, type the maximum physical size desired for the thin provisioned volume.
11. Click **Finish** or **Next** if **Map now** option was selected.

Legacy Snapshots

When the Snapshot premium feature is enabled on the storage array and a valid base volume is selected, the **Create Snapshot** option is enabled. This feature allows you to create a legacy snapshot of the base volume that is selected. To create a new version snapshot, using point-in-time copy, see the Snapshots View section.

Note: Legacy snapshots are not allowed on thin provisioned volumes.

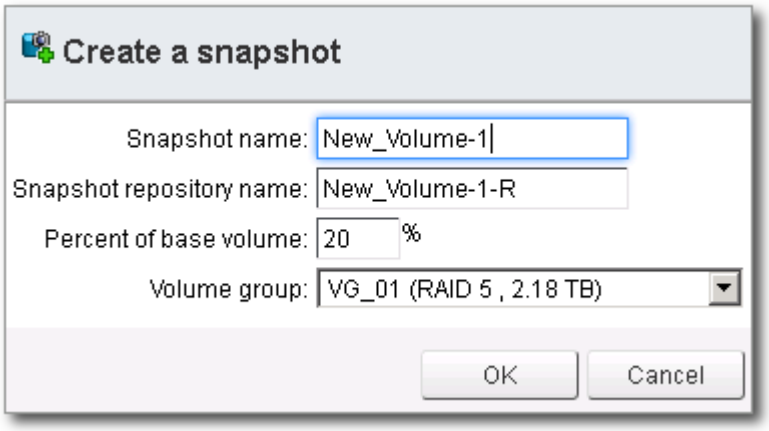
Note: Legacy snapshots are not supported on volumes residing on a DDP; see the Snapshots View section to create a point-in-time snapshot of these volumes.

Create Snapshot

The snapshot commands within the **Volumes** view allow for management of the legacy snapshot feature. To create a legacy snapshot, perform the following:

1. Highlight the base volume, and click **Create Snapshot** icon.
2. The **Create a snapshot** wizard appears.

Figure 42) Create a snapshot Dialog Box.



- **Snapshot name** -- the name of the new snapshot volume.
- **Snapshot repository name --** the name of the new repository volume.
- **Percent of base volume --** the percentage of the base volume to use for the repository.
- **Volume group --** the name of the volume group in which to place the repository volume.

3. Enter the parameters to be used for the snapshot within the **Create a snapshot** wizard dialog.
4. Select the volume group to be used for the snapshot repository from the drop-down box.
5. Click **OK** to complete the process.

Note: When the size of the snapshot exceeds the percentage of the base volume, the snapshot fails. The snapshot is no longer available for use until it is reestablished by recreating it (see Recreate Snapshot).

Disable Snapshot

To temporarily deactivate a snapshot so that it can be used again later, highlight the snapshot volume in the Volumes tree, and click **Disable Snapshot** icon. The snapshot process stops, but the relationship remains between the snapshot, the base volume, and the repository volumes.

Recreate Snapshot

To reestablish a deactivated snapshot or refresh an existing snapshot, click **Recreate Snapshot** icon and click the **OK** button to confirm the operation. A new snapshot of the base volume is created.

Note: Recreating a snapshot disables the original snapshot before the new snapshot is created.

Redistribute Volumes

The NetApp SANtricity Plug-in for VMware vCenter supports redistribution of storage array volumes based on their preferred controller ownership. Typically during ESXi rescan operations, volume ownership is transferred to the non-preferred controller causing the storage array to become non-optimal. By redistributing the volumes to their preferred controller owner, this will resolve the non-optimal condition and balance the I/O loads across the storage array controllers. If all the storage array volumes are already located on their preferred controller, then the **Redistribute Volumes** icon will be greyed out and unavailable.

Rename

The **Rename** feature allows for renaming the selected object from the **Volumes** tree view.

1. Select the object to be renamed and click on the **Rename** icon.
2. Enter the new name for the object.
3. Click **OK** to apply the change.

Disable Data Assurance

The **Disable Data Assurance** allows for disabling data assurance (T10 PI) on the selected volume. Data Assurance (DA) can only be disabled on volumes residing within a volume group and not on volumes residing within a disk pool. Select the volume to deactivate DA on and click the **Disable Data Assurance** icon from the Actions dropdown menu. No confirmation window is displayed during this operation.

Note: Once DA has been deactivated on a volume, it cannot be re-enabled. The volume must be recreated to enable DA.

Note: You can only disable DA on a volume without dependencies such as legacy snapshots or remote volume mirror relationships.

Delete

The **Delete** command provides the ability to delete the selected object (volume, volume group, disk pool, or snapshot). Only objects that are not participating in asynchronous mirror groups, snapshot groups, or remote volume mirrors may be deleted.

1. Select the object to be deleted and click the Delete command from the Actions dropdown menu.

The **Delete Volume** confirmation box is displayed.

2. Click OK to confirm deletion of the object (click Cancel to abort deletion of object).

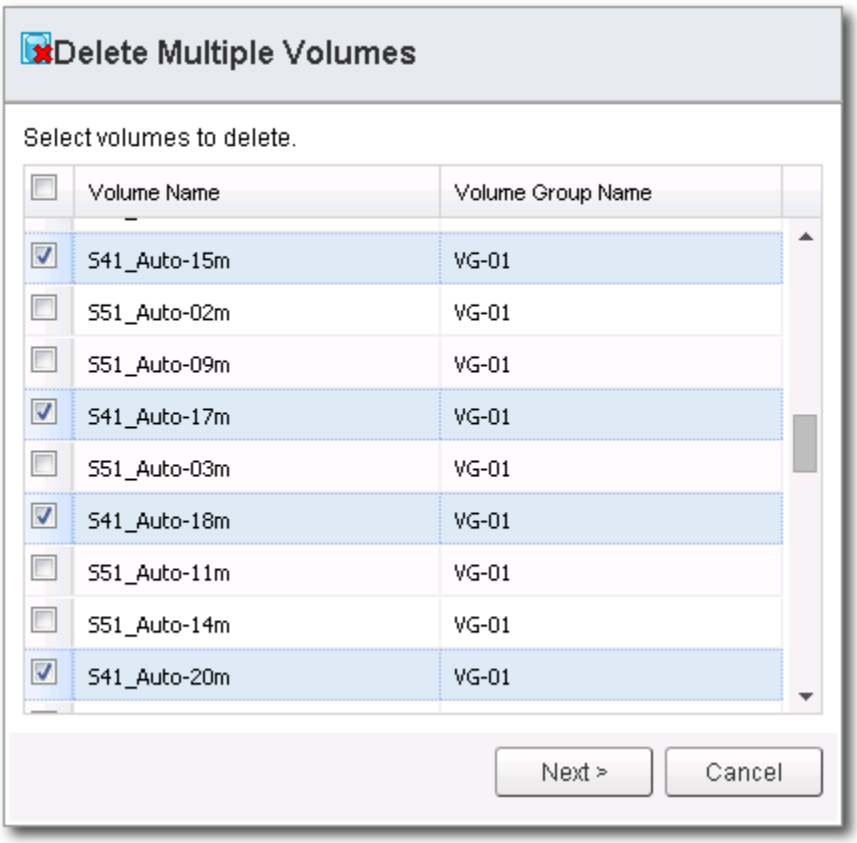
Note: Some object may not be deleted until all child objects are deleted first; such as DDPs or volumes in a mirrored relationship. Delete or remove member objects before deleting base volume, volume group, or disk pool.

Delete Multiple Volumes

The **Delete Multiple Volumes** command allows for deleting multiple volumes at one time. To use this feature perform the following:

1. Select the storage array object from the volume tree view.
2. Select **Delete Multiple Volumes** command from the Actions dropdown menu.

A Delete Multiple Volumes wizard is then displayed.



3. **Select** the volumes to be deleted by placing a checkmark in the checkbox next to the volume name.
4. Click **Next** once all volumes are selected and a confirmation dialog box is displayed.
5. If the displayed volumes to be deleted looks correct click **Finish** to delete the selected volumes.

Note: Due to a limitation of the SDK, a limit of 80 volumes at a time can be deleted with this command.

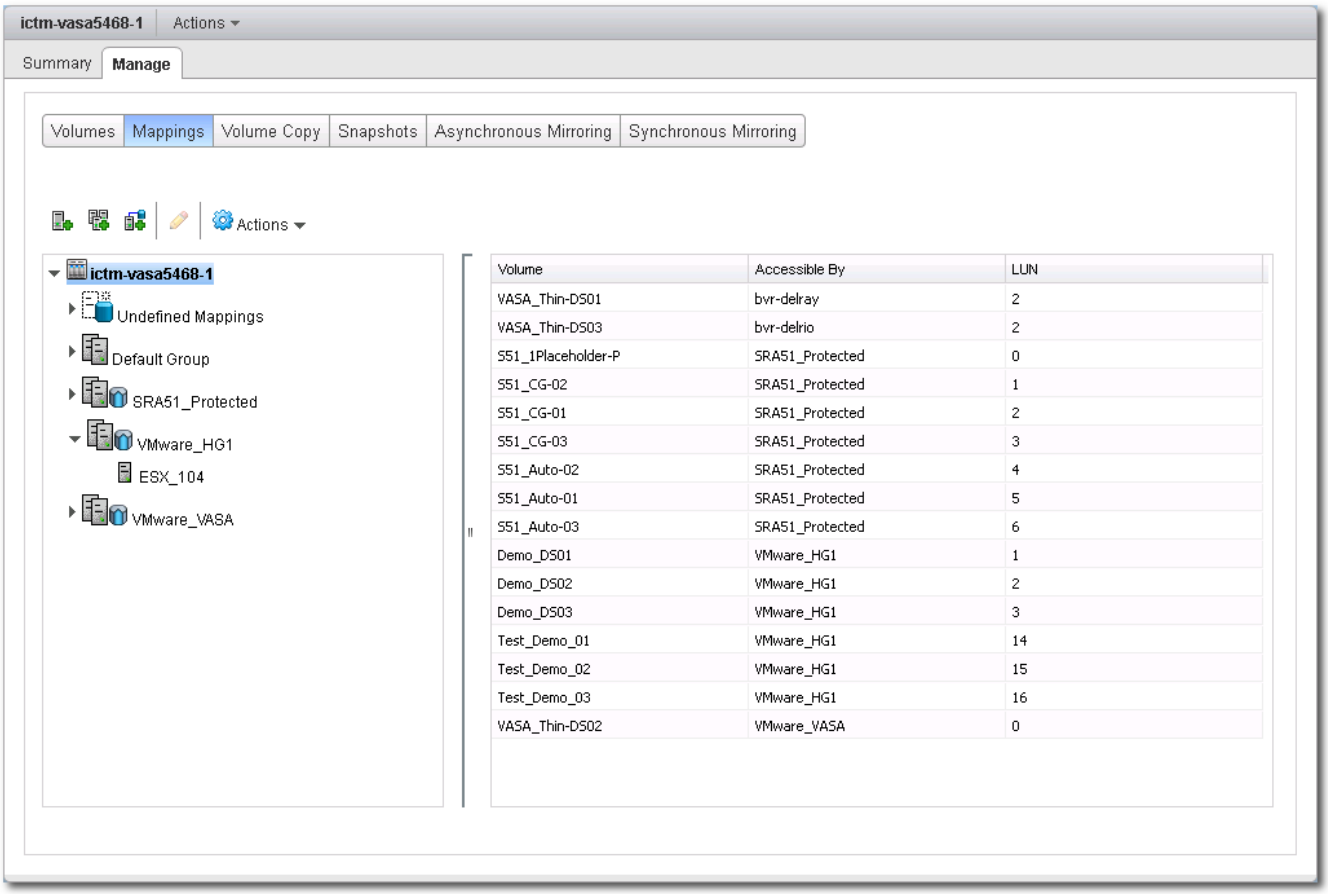
Note: Volumes participating in mirror relationship must be removed from the AMG before they can be deleted.

Mappings View Features

The **Mappings** view provides the ability to manage how storage array volumes are present to the ESXi hosts. This view also provides the ability to manage hosts and host groups on the selected storage array. The following commands are available from this view:

- Add Host....
- Add Host Group....
- Add Mapping....
- Rename....
- Remove.... (Only available from the Actions dropdown menu.)

Figure 43) Storage Array Mappings View.



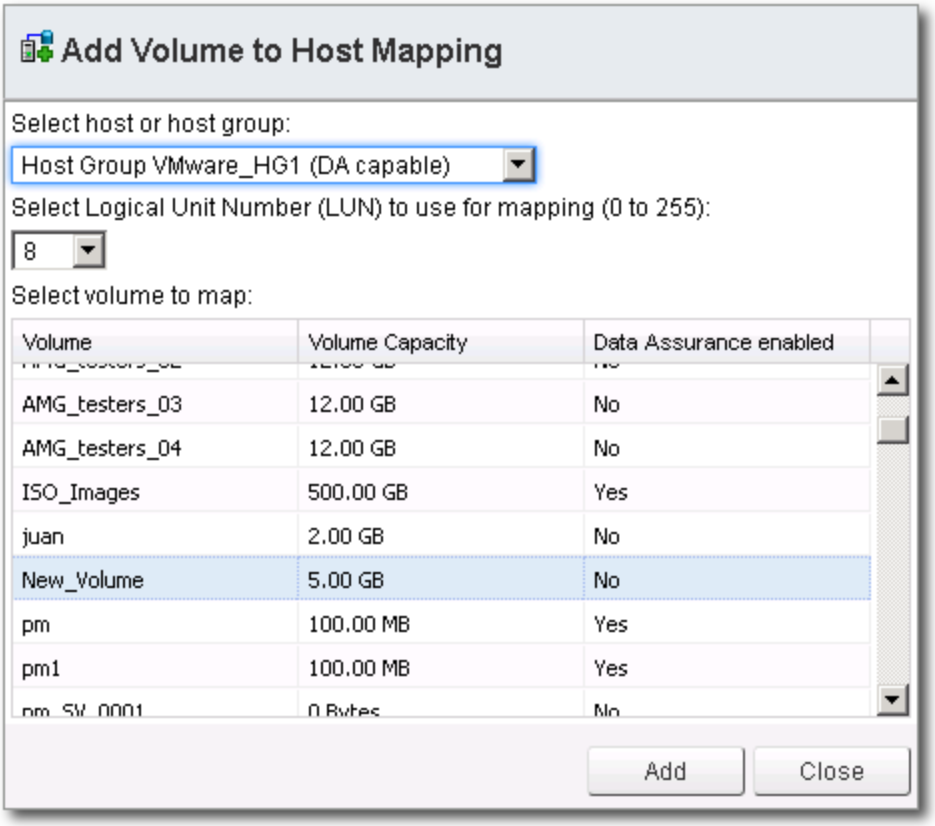
Add Mapping

To present a volume to an ESXi host or host group:

1. Click the Add Mapping icon.

The **Add Volume to Host Mapping** wizard is displayed.

Figure 44) Add Volume to Host Mapping.



2. **Select** host or host group the volume will be presented to from the dropdown box.
3. Accept the default logical unit number (LUN) or change to desired LUN number for the new mapping.
4. **Select** the volume to be mapped.
5. Click **Add**.
6. **Repeat** steps 3 through 5 for additional volumes to present or click **Close** to finish.

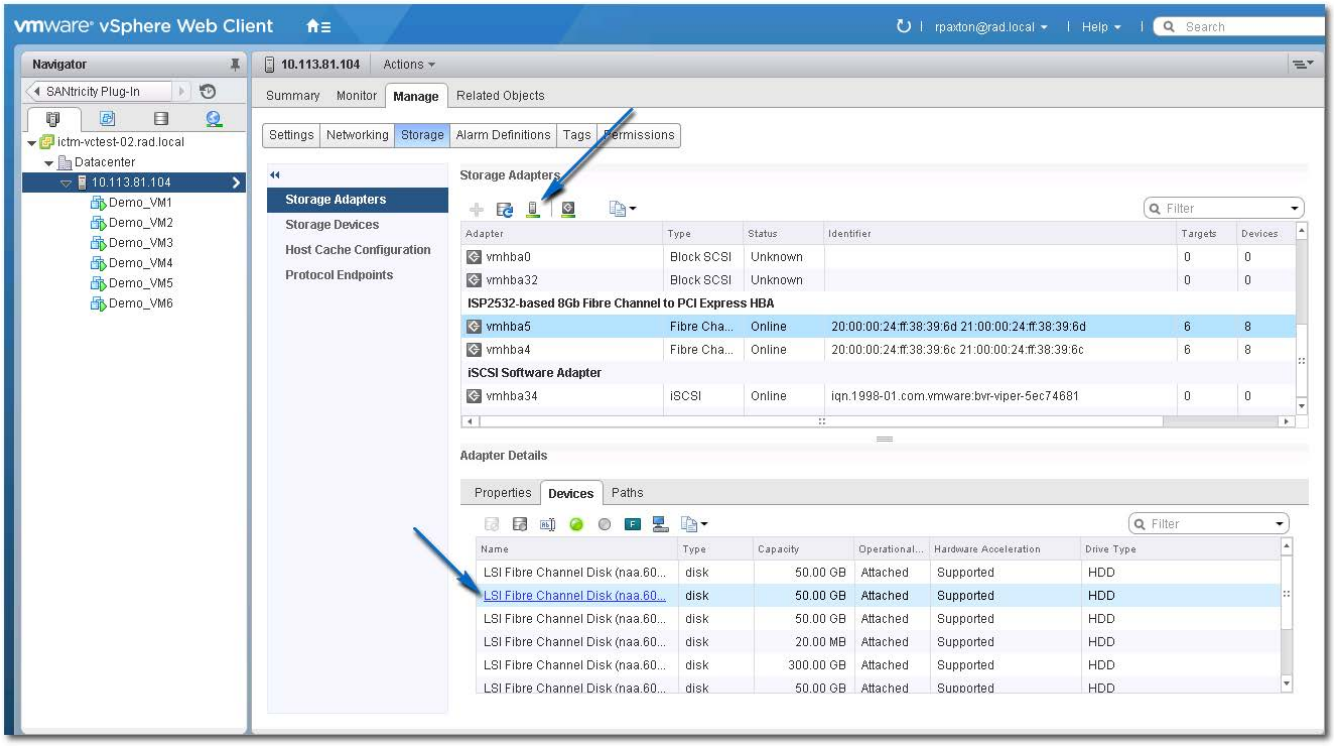
Note: When your storage array uses multiple groups of HBAs per ESXi host, the new volumes should be balanced across all hosts/host groups. Do not add all the volumes to a single host/host group; no I/O balancing can occur in this case.

Rescan Storage Adapters

After the volumes have been mapped to the ESXi host(s), the storage adapters on the ESXi host must be rescanned to detect the new storage volumes. This action is accomplished under the **Manage** tab in the **Hosts and Clusters** view. Select **Storage** for the ESXi host being configured and then click the rescan all storage adapters icon.

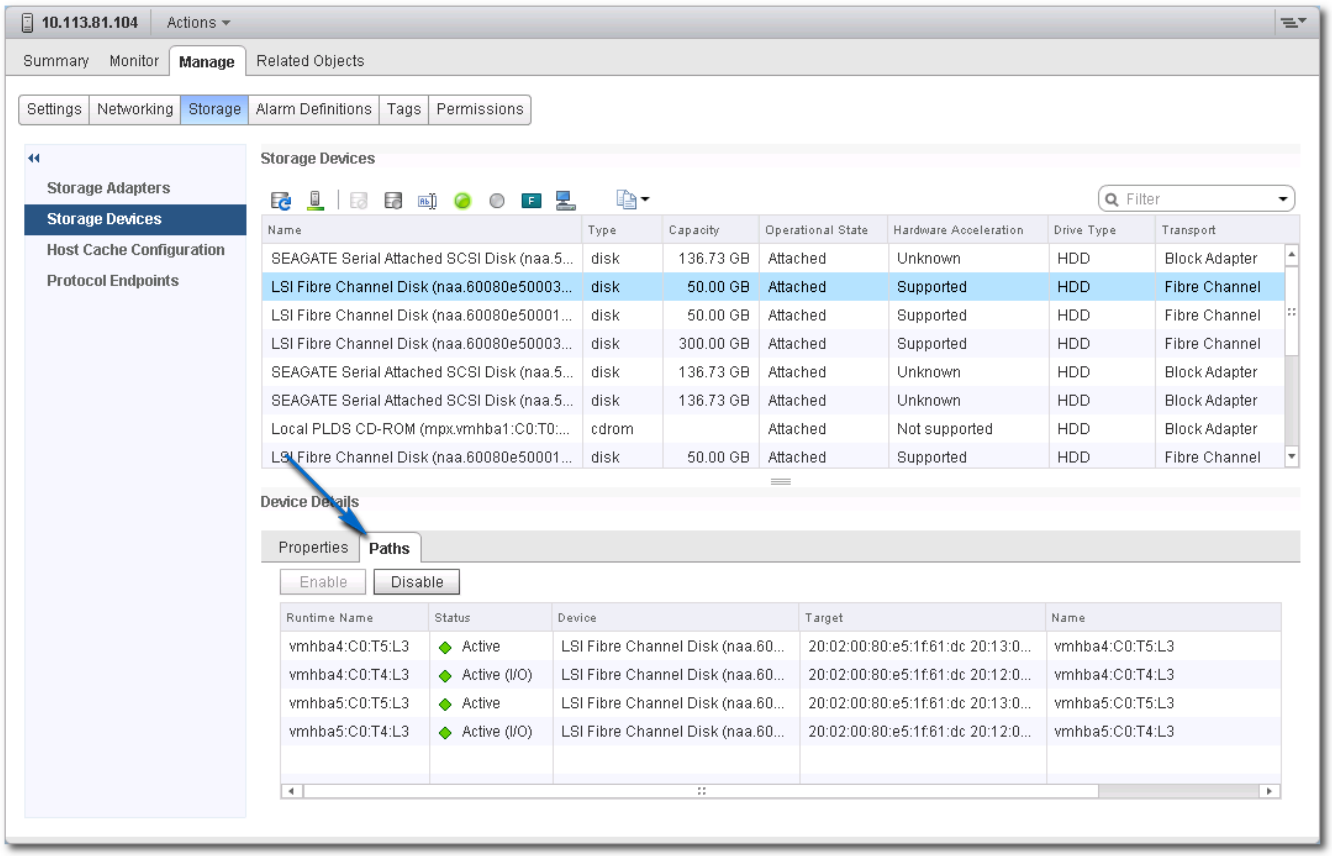
Note: You may need to run the Rescan, from vCenter, twice to detect all of the new storage volumes that have been mapped to the ESXi host.

Figure 45) Storage Adapters Rescan.



From this view, the user can also verify that the correct number of paths have been configured by clicking on one of the devices listed under the storage adapter. This should then display the Storage Devices view. Select the Paths tab to view the details of the selected device. For round robin PSP, you should see four active connections with two denoting I/O. For most recently used PSP, you should see either four active connections with one channel showing I/O or two active connections and two standby connections and one of the active channels showing I/O. To change the PSP method for a device, select the Properties tab under Device Details pane, scroll down to the Edit Multipathing button. Click the button and select the path selection policy to apply to the device from the drop-down box. Click OK to apply.

Figure 46) Device Details Paths view.

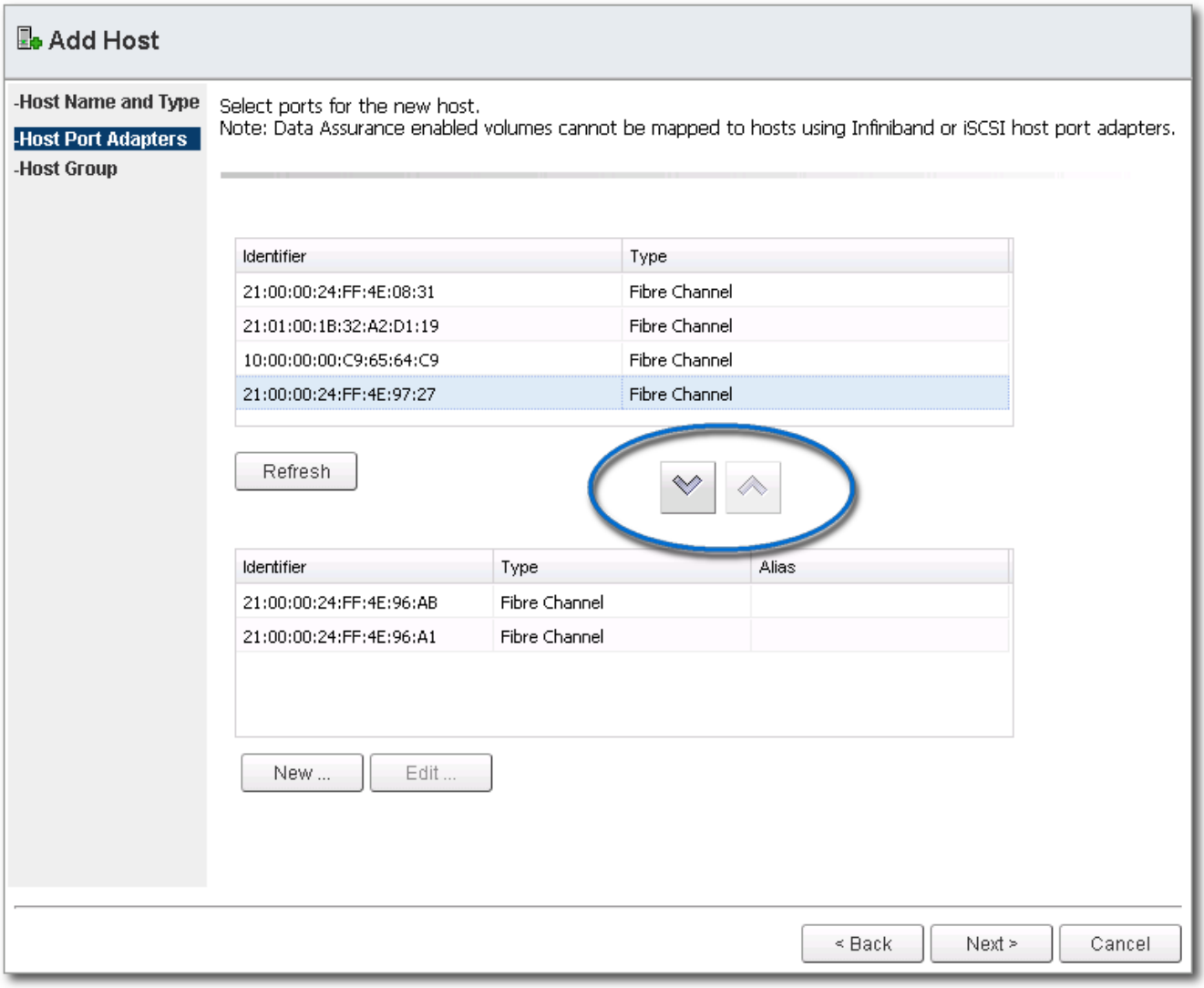


Add Host

The **Add Host** command allows for defining hosts used to present volumes to. To add a new host:

1. Select a host group to add a new host to and click the **Add Host** icon.
2. Enter the name for the new host.
3. Select the host type (VmwTPGSALUA for ESXi host) from the drop-down box.
4. Select the interface type and click **Next**.
5. Select the available host port adapters' identifiers for the new host to be added.
6. Click the **down arrow** to move the host port identifier to the lower window (Repeat for dual port configuration).

Figure 47) Host Port Adapters Wizard.



Note: Only unconfigured host port identifiers are displayed within the top window of the **Add Host** wizard.

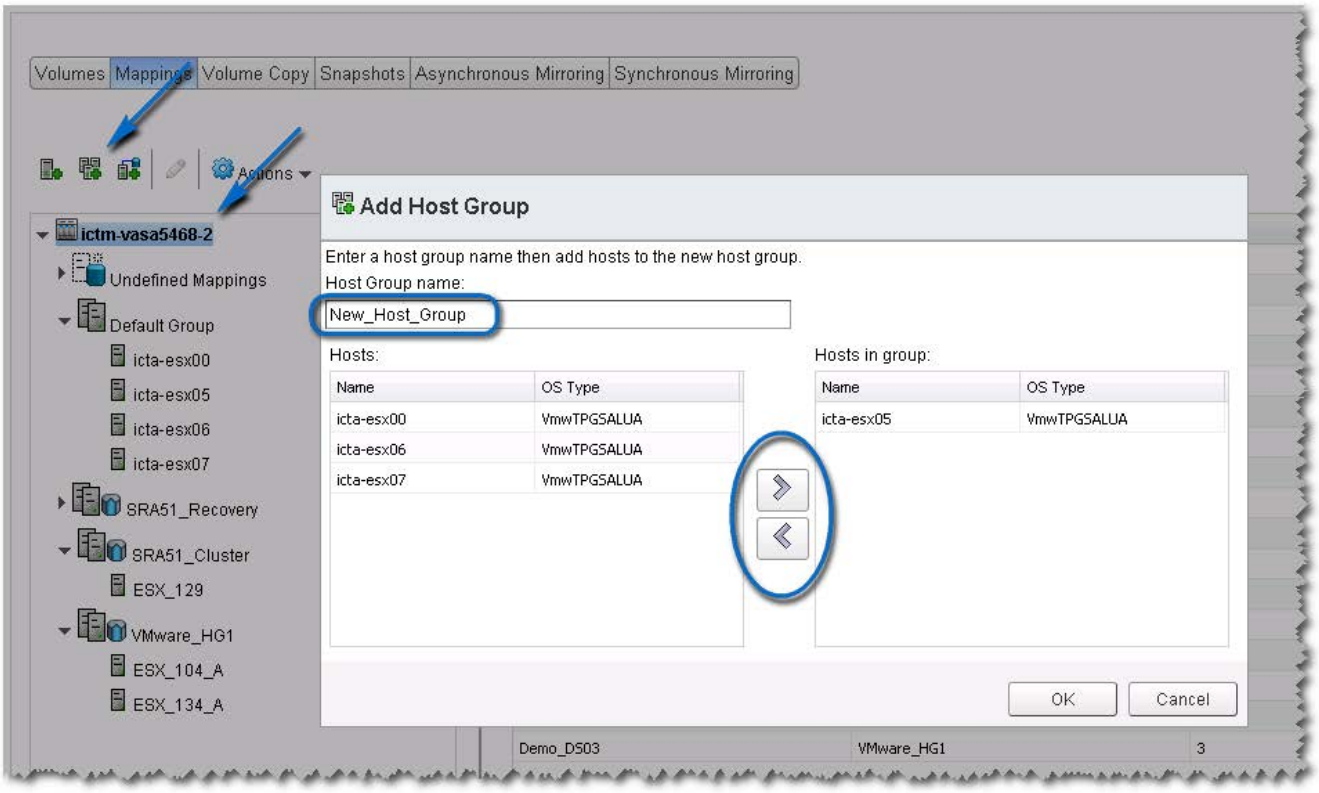
7. Click **Next**.
8. Select the radio button to choose if this host will be added to a host group (shared volume mappings).
9. If the host will be added to a host group, choose the radio button for either a new host group or existing host group.
10. Enter a new host group name or select an existing host group from the drop-down box.
11. Click **Finish**.

Add Host Group

To create a new host group, to share LUN mappings between hosts:

1. Click **Add Host Group** icon.

Figure 48) Add Host Group Wizard.



2. Enter the name for the new host group.
3. Select the name(s) of the host(s) to be added to the new host group.

Note: Only hosts that are currently in the default host group will be listed in the available hosts list.

4. Click the right arrow to add the host(s) to the new host group.
5. (Optional) Repeat steps 3 and 4 for additional hosts.
6. Click **OK** once all hosts have been added to the new host group.

Rename

The **Rename** command allows for renaming a host or host group. Select the host or host group to be renamed and click the **Rename** icon. Enter a new name for the object and click **OK**.

Remove

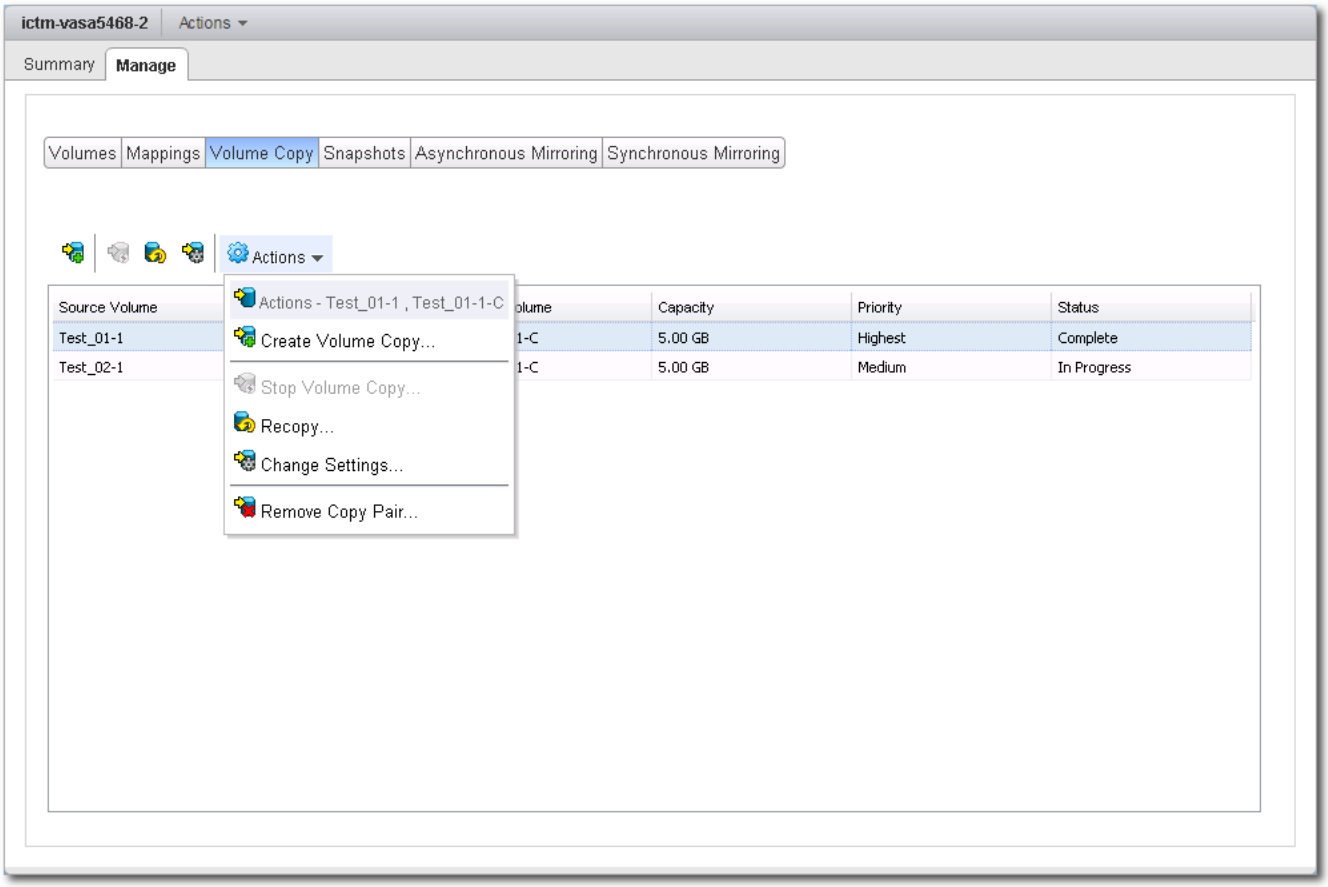
The **Remove** command allows for removing the selected object (host or host group) from the storage array. Select the host or host group to remove and click the **Remove** icon from the **Actions** menu dropdown.

Volume Copy View Features

The **Volume Copy** view provides management of volume copies on the selected storage array. This tab also displays existing volume copy pairs along with their current status. Volume copy provides a method to copy all existing data from a source volume to a target volume. Unlike snapshot, the target volume, once completed, does not rely on data from the source volume; it contains all data from the original volume and may be mapped to alternate host(s) for data mining or recovery purposes without affecting the source volume data. The following commands are available from this view:

- Create Volume Copy....
- Stop Volume Copy....
- Recopy....
- Change Settings....
- Remove Copy Pair....

Figure 49) Volume Copy View Tab.

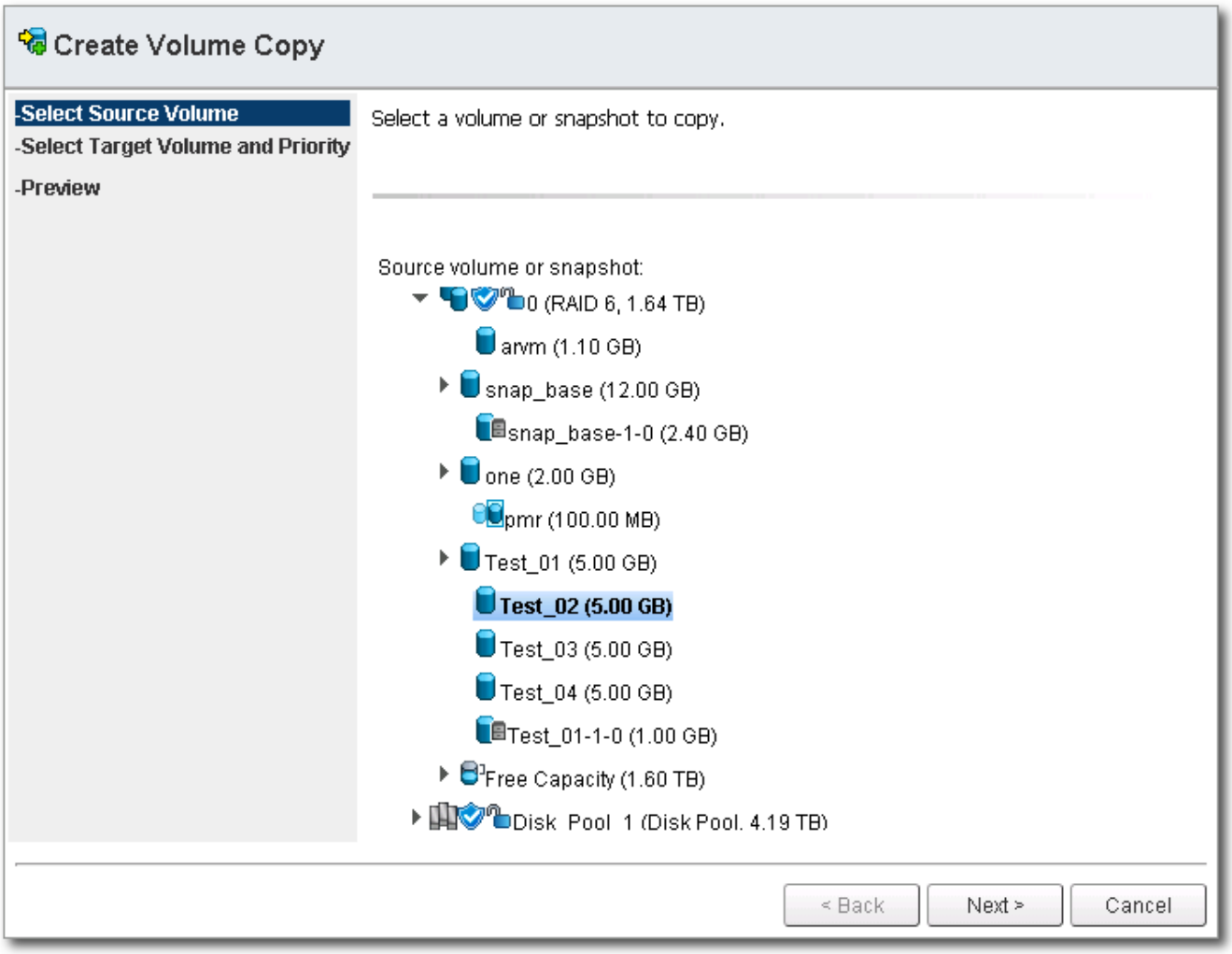


Create Volume Copy

1. To create a new volume copy, click **Create Volume Copy** icon.

The **Create Volume Copy** wizard is then displayed.

Figure 50) Select Source Volume.

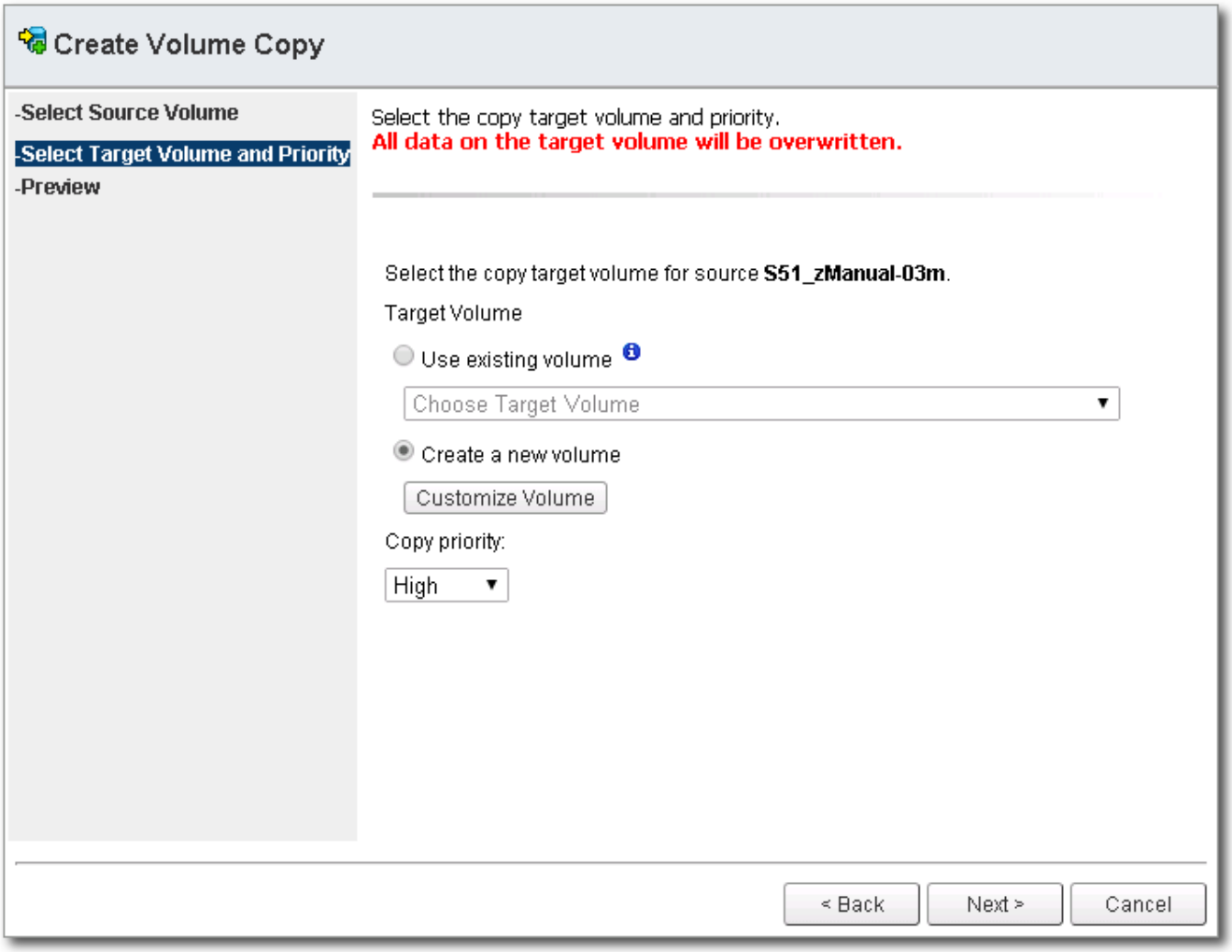


Note: While the volume copy is being established, a snapshot of the source volume is created which is used to create the volume copy from. This ensures that the data is consistent at the time the volume copy was initiated and continued read-write access to the source volume during the copy operation.

Note: Snapshots for volumes residing on a disk pool are not supported in this release. Any volume copy using volumes on a disk pool will be read-only to the host until the copy process completes.

2. Select the source volume and click **Next**.
3. Choose either Use existing volume or Create a new volume radio button.

Figure 51) Select Target Volume and Priority.



4. **Select** the copy priority to use while establishing the new volume copy.
5. Click **Next**.
6. Review and verify the volume copy settings and click **Finish** to start the volume copy.

Stop Volume Copy

The **Stop Volume Copy** command will stop the current volume copy operation for the selected copy pair. Select a copy pair that is in-progress and click the **Stop Volume Copy** icon. A confirmation dialog will appear, select **OK** to stop the operation.

Recopy

The **Recopy** command will recopy all data from the source volume to the target volume, overwriting any existing data on the target volume, for the selected volume copy pair.

CAUTION: All data residing on the target volume will be overwritten with this option.

1. **Select** the volume copy pair to use for the recopy.
2. Click Recopy icon.
3. Verify the information within the **Recopy** dialog and choose **OK** or **Cancel**.

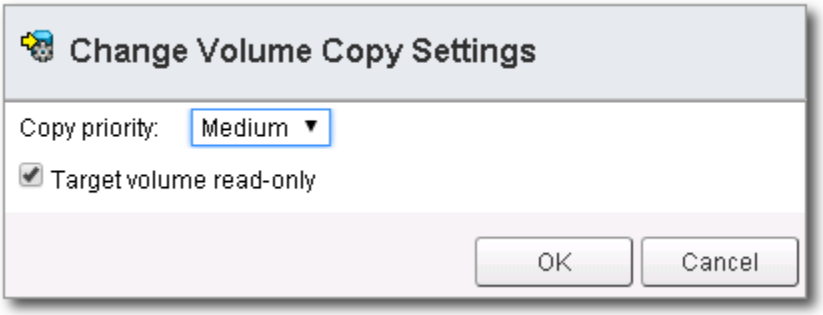
Change Settings

If you would like to change the target volume to read-write or change the modification priority, perform the following steps:

1. **Select** an existing volume copy pair from the list.
2. Click the **Change Settings** icon.

The **Change Volume Copy Settings** dialog box is displayed.

Figure 52) Change Volume Copy Settings.



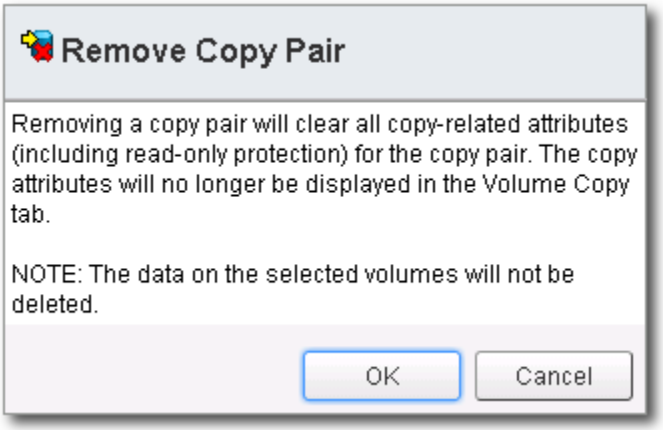
3. From the Copy Priority drop-down box, select the new priority for the volume copy.
4. Uncheck the Target Volume Read-Only box to allow for read-write of the target volume copy.
5. Click **OK**.

Remove Copy Pair

The **Remove Copy Pair** command removes the relationship of the source and target of a volume copy pair. This does not remove the target volume or the data residing on the target volume. To remove a volume copy pair relationship:

1. **Select** the volume copy pair to be removed.
2. Click **Remove Copy Pair** icon from the **Actions** dropdown menu.
3. Click **OK** to remove the volume copy pair or **Cancel** to abort, within the Remove Copy Pair dialog box.

Figure 53) Remove Copy Pair dialog box.

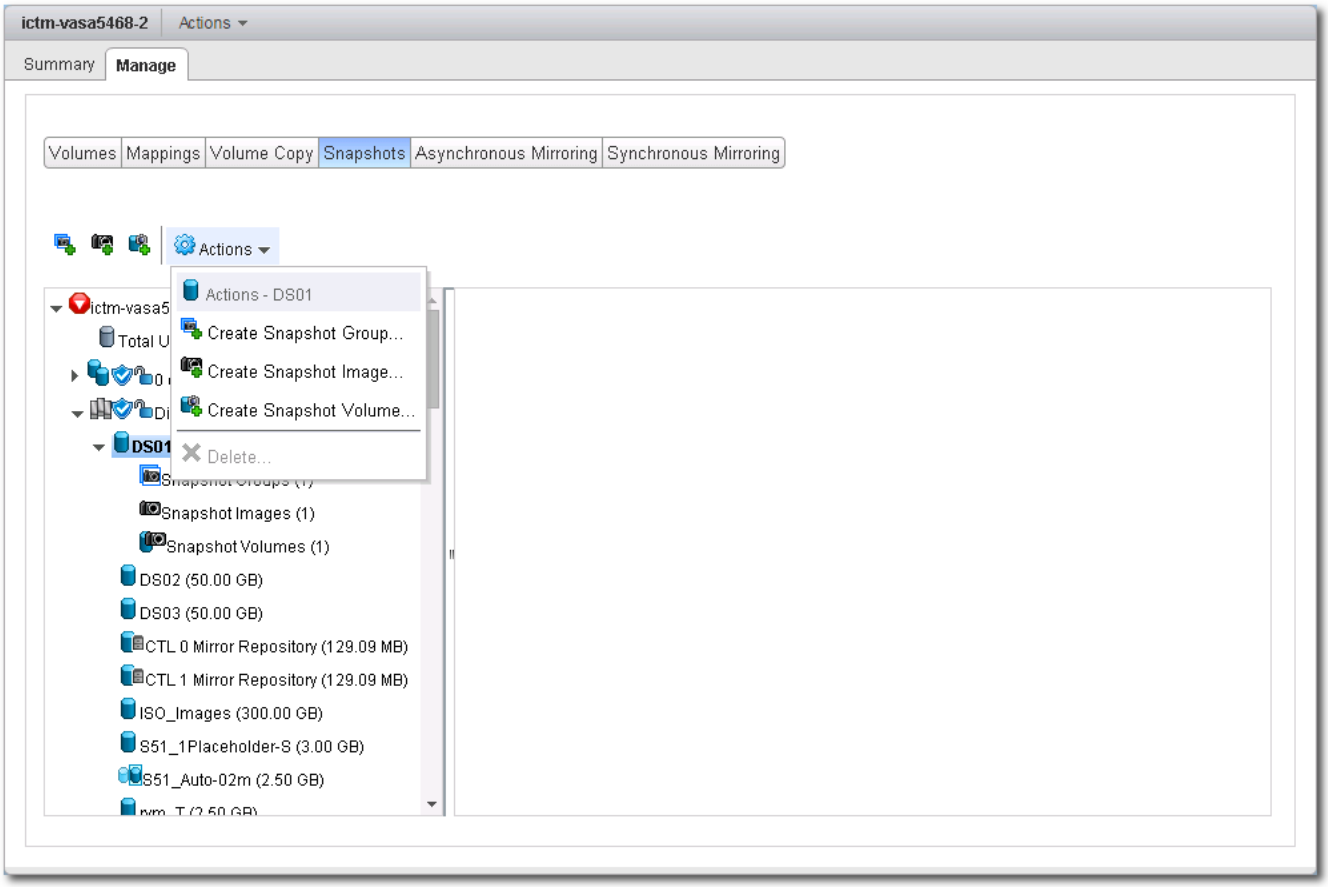


Snapshots View Features

NetApp E-Series and EF-Series storage arrays with firmware 7.84 and later support Point-in-Time (PiT) based snapshots. These snapshots provide a PiT image of the base volume that may be used to revert back to, or presented to an alternate host as read-only or read-write volume. The following commands are available from this view:

- Create Snapshot Group....
- Create Snapshot Image....
- Create Snapshot Volume....
- Delete....

Figure 54) Snapshots View.



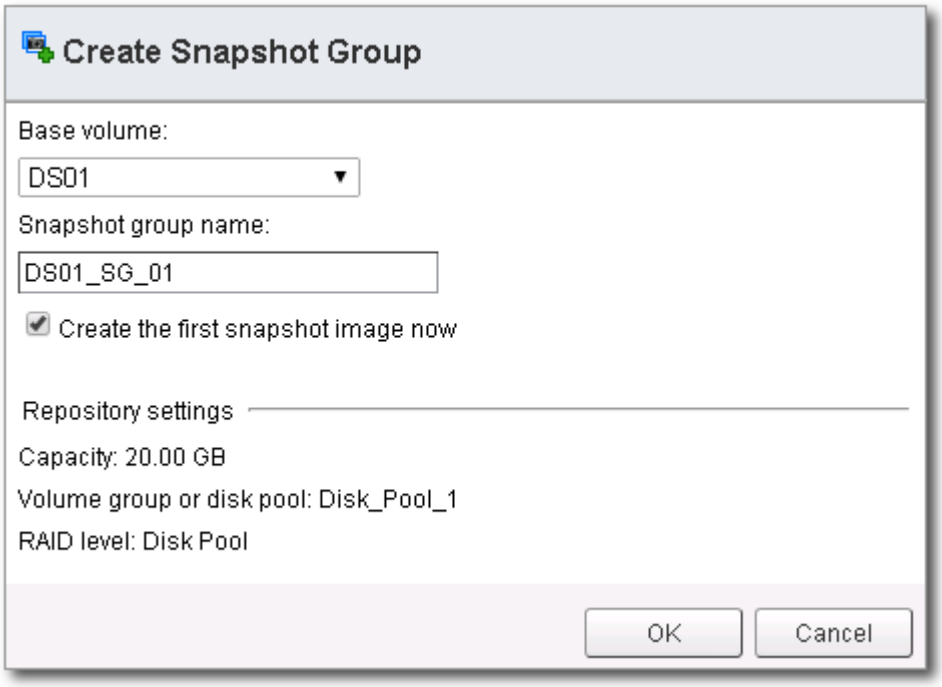
Note: To rollback a snapshot image to the base volume, you must use SANtricity Storage Manager; image rollback is not currently supported within the NetApp Plug-in. Additionally, SANtricity Storage Manager may also be used to setup scheduled snapshot images automatically.

Create Snapshot Group

A snapshot group is used to hold snapshot images of a storage array volume. To create a new snapshot group, perform the following steps:

1. **Select** the base volume from the Volumes tree window.
2. Click Create Snapshot Group icon.

Figure 55) Create Snapshot Group dialog box.



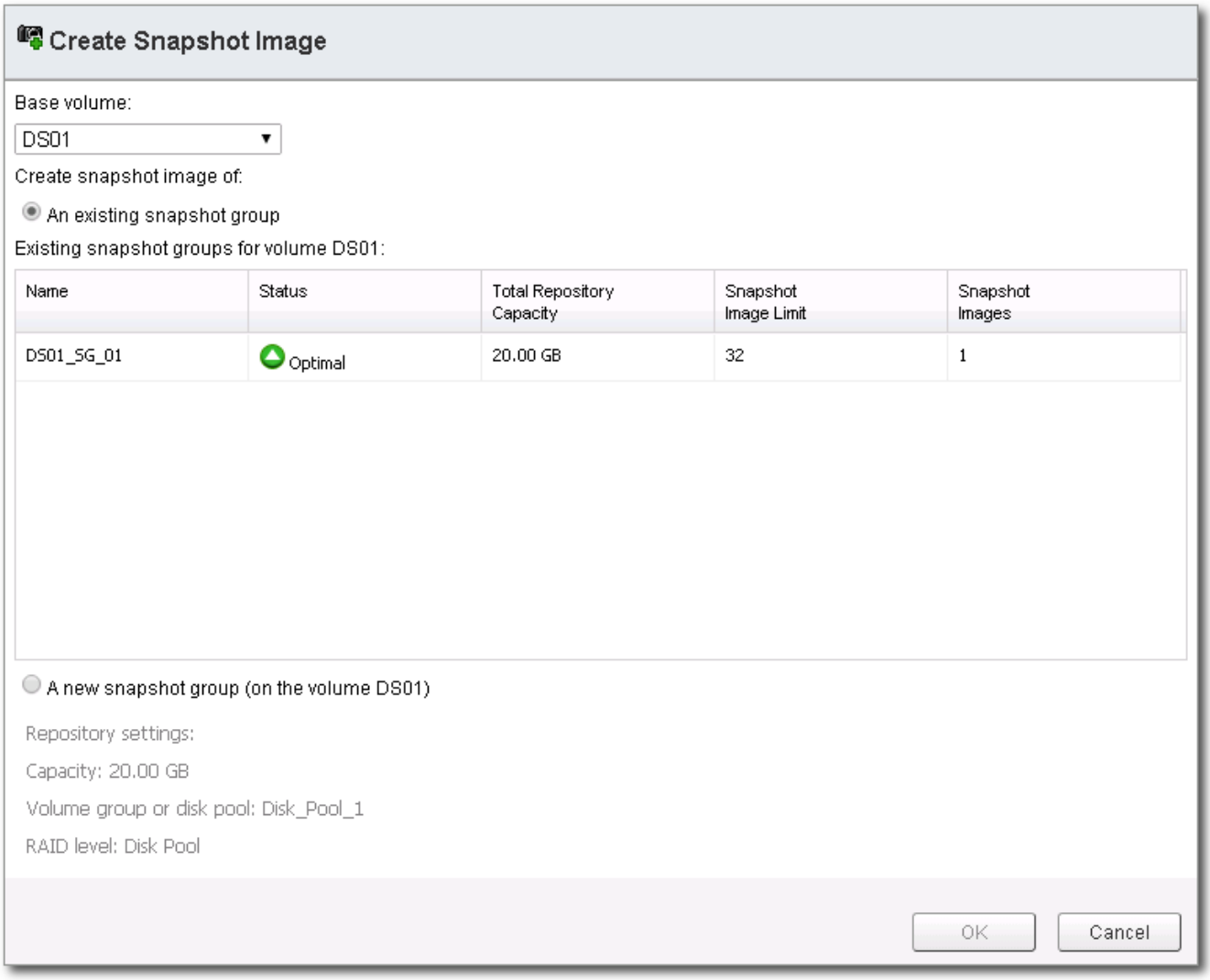
3. **Modify** the displayed parameters as necessary.
4. Click **OK**.

Create Snapshot Image

A snapshot image is a point-in-time copy of the base volume. Once an image is created, it may be used to roll-back the base volume to or it may be used to create a volume from. To create an image, perform the following steps:

1. **Select** the base volume from the volumes tree window.
2. Click Create Snapshot Image icon.

Figure 56) Create Snapshot Image Dialog Box.



3. In the Base volume dropdown box, **select** the base volume of the snapshot image.
4. **Select** an existing snapshot group to use for the new image.

Note: If this is the first snapshot image for the base volume, a new snapshot group will be created if not already manually created.

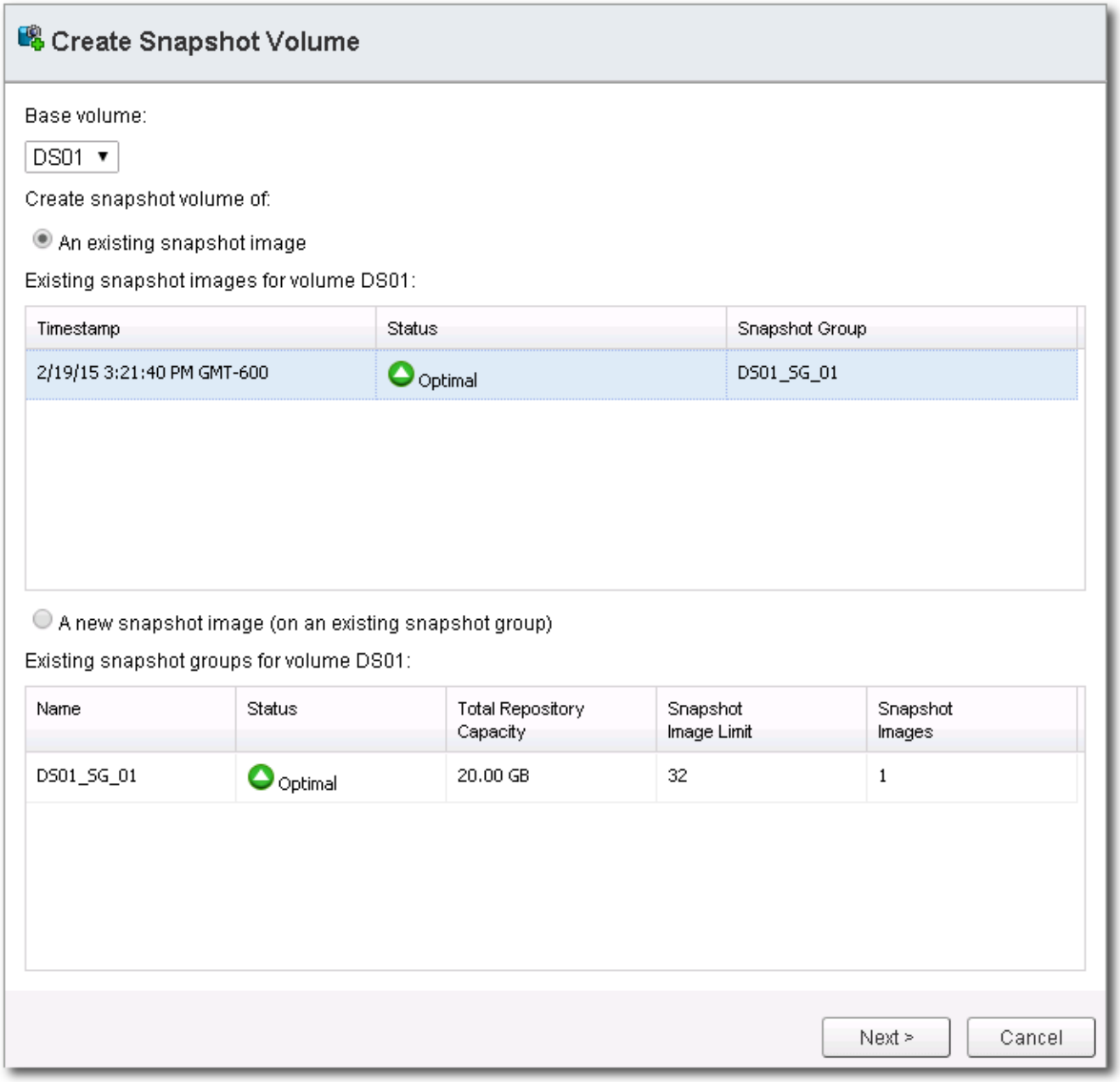
5. Click **OK**.

Create Snapshot Volume

A snapshot volume allows for a snapshot image to be mapped to a host or host group for data access. To create a snapshot volume, perform the following steps:

1. **Select** a base volume in the volumes tree window that has an existing snapshot group.
2. Click **Create Snapshot Volume** icon.

Figure 57) Create Snapshot Volume dialog.



3. **Select** a snapshot image from the available list of images or select **A new snapshot image** option and click **Next**.
4. In the Snapshot volume name text box, **enter a name** for the new snapshot volume.
5. Select the **access mode** for the snapshot volume.

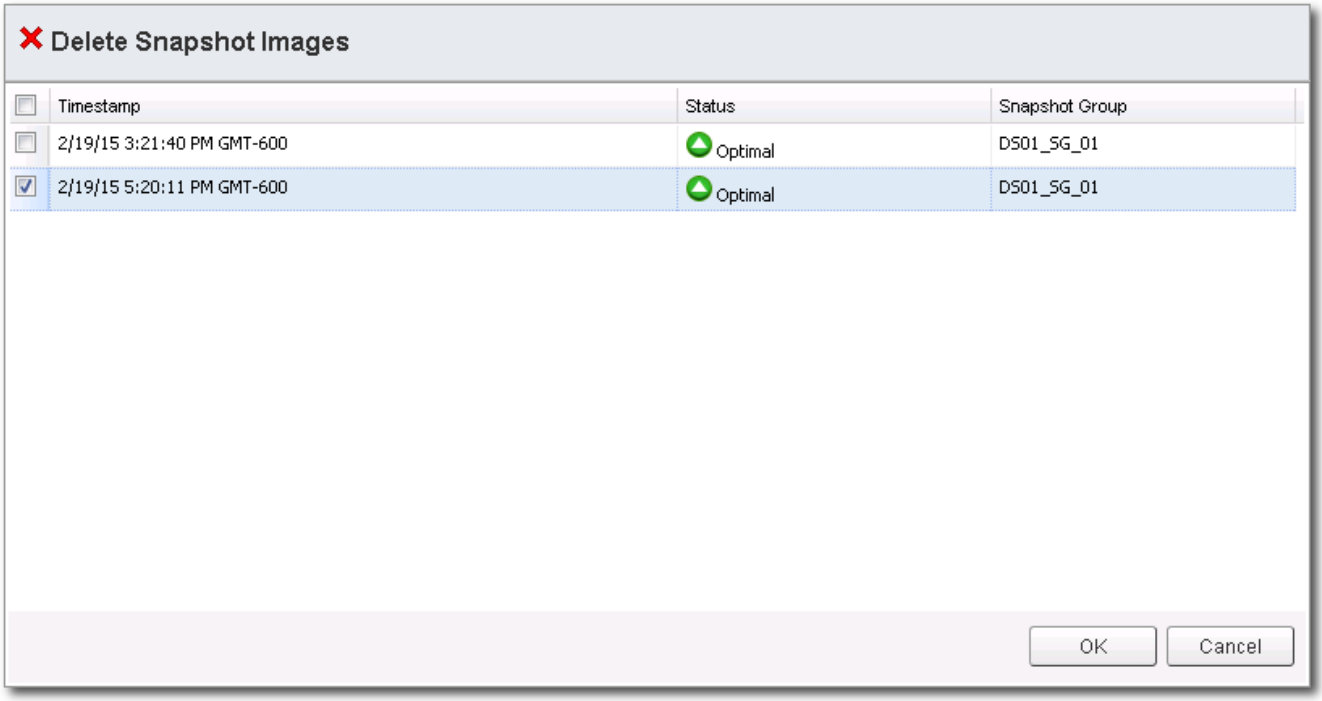
6. Click **Finish**.

Delete

The **Delete** command allows for removal of snapshot volumes, snapshot images, or snapshot groups depending on the object select. The delete option will open a dialog box of the selected object displaying the leafs of that object. To delete a snapshot object, perform the following:

1. **Expand** the base volume from the volumes tree window.
2. Select the Snapshot Groups, Snapshot Images, or Snapshot Volumes object.
3. Click **Delete** command.

Figure 58) Delete Snapshot Objects.



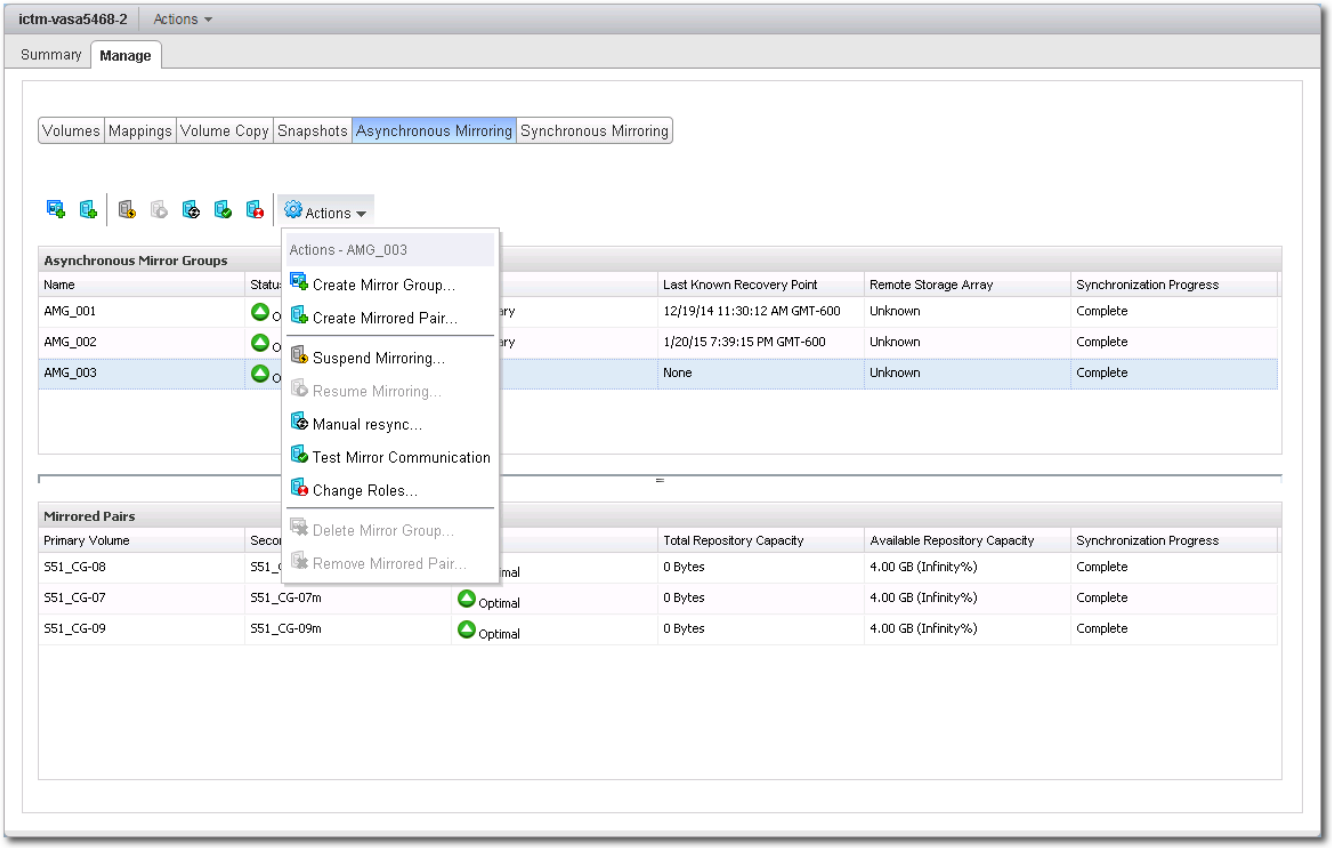
4. **Select** the checkbox next to the leaf objects to be deleted.
5. Click **OK**.
6. Click **OK** in the Warning dialog box to delete the object or **Cancel** to abort the operation.

Asynchronous Mirroring View Features

The **Asynchronous Mirroring** view tab allows for management of Asynchronous Remote Volume Mirrors (aRVM). aRVMs are available on NetApp E-Series and EF-Series storage arrays with firmware 7.84 and later. The following commands are available on the **Asynchronous Mirroring** view tab:

- Create Mirror Group....
- Create Mirrored Pair....
- Suspend Mirroring....
- Resume Mirroring....
- Manual Resync....
- Test Mirror Communication....
- Change Roles....
- Delete Mirror Group....
- Remove Mirrored Pair....

Figure 59) Asynchronous Mirroring View.



Asynchronous Remote Volume Mirroring Details

The aRVM feature is similar to RVM by allowing source volumes from a primary storage array to be replicated to a target volume on a remote storage array. However, aRVM supports both iSCSI and fibre channel connections between the storage arrays and utilizes point-in-time replication strategy. aRVM enables you to manage the synchronization process of creating a consistent data set on a remote storage array.

An asynchronous mirror group (AMG) may contain several mirrored pairs that you can manage as one entity. A mirrored pair consists of a primary volume and a secondary volume. Both volumes contain identical copies of the

same data. Write operations are performed to the primary volume and then replicated to the secondary volume based on the AMG synchronization settings.

An AMG defines the synchronization settings for all mirrored pairs within the group. Each mirrored pair in an AMG shares the same synchronization settings, primary and secondary role, and write mode. You can synchronize all mirrored pairs in the AMG at the same time.

An asynchronous mirror group is associated with the local storage array and remote storage array in the mirrored pair.

- The local storage array performs the primary role in the asynchronous mirror group. All volumes added to the asynchronous mirror group on the local storage array perform the primary role in the mirror relationship.
- The remote storage array performs the secondary role in the asynchronous mirror group. All volumes added to the asynchronous mirror group on the remote storage array perform the secondary role in the mirror relationship.

Create Mirror Group

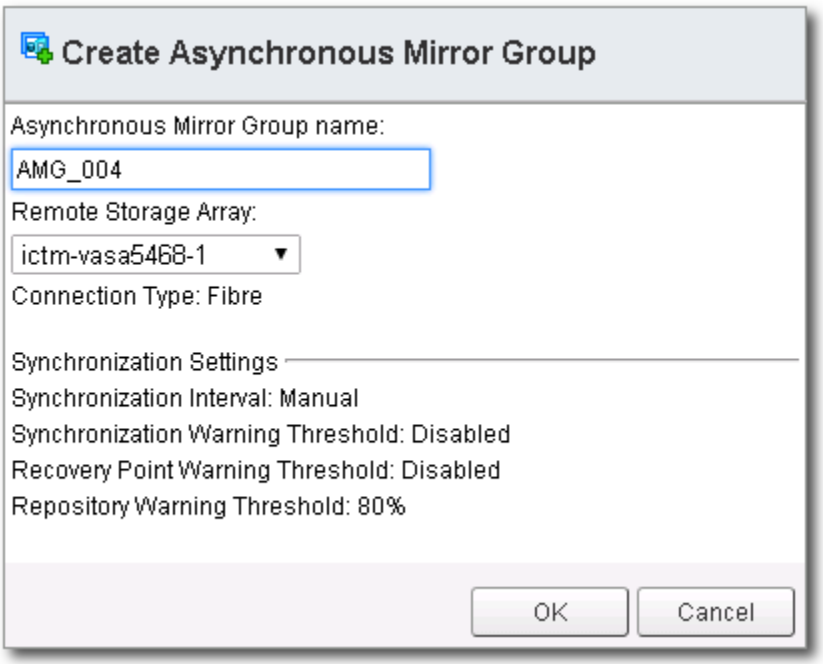
An AMG is used to group mirrored pairs as a single entity and control replication settings for all members of the AMG. A mirrored pair may only reside in a single AMG. There is a limit of 4 AMGs per storage array. To create a new AMG, perform the following:

Note: To configure asynchronous mirrors within the NetApp Plug-in, both arrays (local array and remote array) must be added to the NetApp Plug-in Array Manager. If either array is removed from the Array Manager, any AMGs configured between the two arrays will not be displayed in the plug-in.

1. Click Create Mirror Group icon.

The Create Asynchronous Mirror Group dialog box appears.

Figure 60) Create Asynchronous Mirror Group dialog box.



2. In the Asynchronous Mirror Group Name text box, **type** a unique name for the AMG.
3. **Select** the remote storage array for the AMG from the Remote Storage Array dropdown list.

Note: The Remote storage array dropdown list shows only the storage arrays that support selection as the remote storage array.

4. Click **OK**.

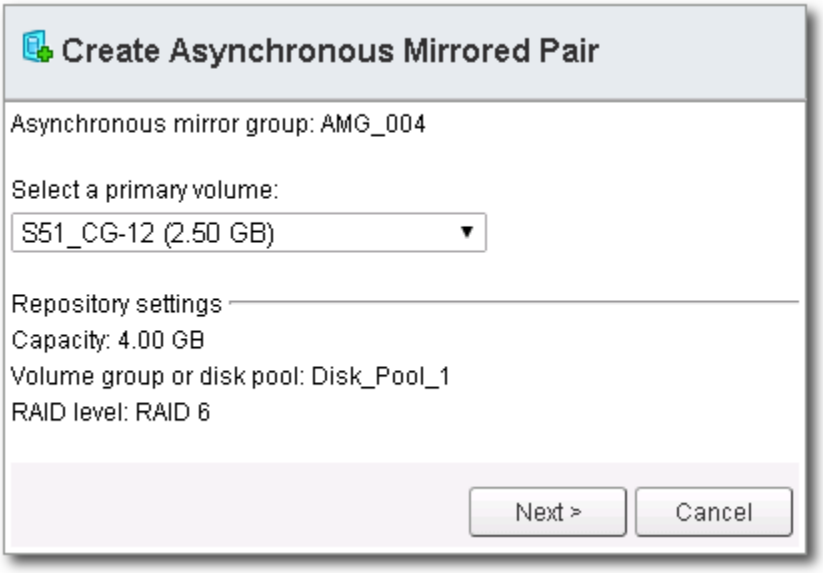
Create Mirrored Pair

The **Create Mirrored Pair** option allows for creating a mirror pair relationship between a primary volume on the primary array and a secondary volume on the secondary array. To create a new mirrored pair, perform the following:

1. In the Asynchronous Mirror Groups table, **select** an AMG (with primary role) in which to create a mirrored pair.
2. Click **Create Mirrored Pair** icon.

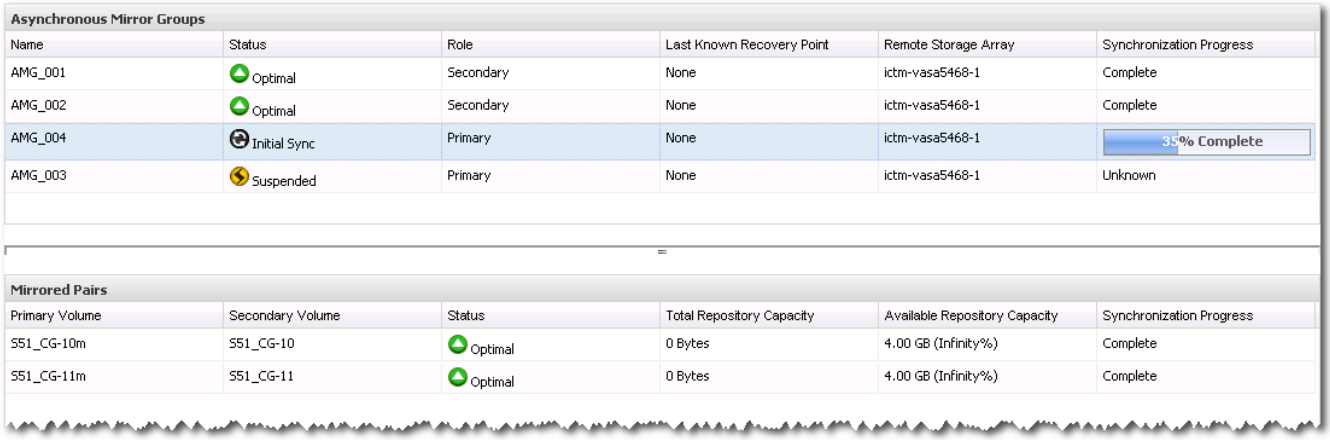
The Create Asynchronous Mirrored Pair dialog box appears.

Figure 61) Create Asynchronous Mirrored Pair Dialog Box.



3. On the Select a primary volume dropdown list, **select** the primary volume for the mirrored pair.
4. Click **Next**.
5. On the Select a secondary volume dropdown list, **select** the secondary volume for the mirrored pair.
6. Click **Finish**.

Figure 62) Initial Sync Status Asynchronous Mirror Groups Table and Mirrored Pairs Table.



Asynchronous Mirror Groups

Name	Status	Role	Last Known Recovery Point	Remote Storage Array	Synchronization Progress
AMG_001	Optimal	Secondary	None	ictm-vasa5468-1	Complete
AMG_002	Optimal	Secondary	None	ictm-vasa5468-1	Complete
AMG_004	Initial Sync	Primary	None	ictm-vasa5468-1	35% Complete
AMG_003	Suspended	Primary	None	ictm-vasa5468-1	Unknown

Mirrored Pairs

Primary Volume	Secondary Volume	Status	Total Repository Capacity	Available Repository Capacity	Synchronization Progress
S51_CG-10m	S51_CG-10	Optimal	0 Bytes	4.00 GB (Infinity%)	Complete
S51_CG-11m	S51_CG-11	Optimal	0 Bytes	4.00 GB (Infinity%)	Complete

Suspend Mirroring

When mirroring is suspended, the volumes in the mirrored pairs cannot synchronize data. The suspend-mirroring operation must be performed by the storage array in the primary role for the AMG. To suspend mirroring, do the following:

1. **Select** the AMG from the Asynchronous Mirror Groups window.
2. Click Suspend Mirroring icon.
3. Select **Yes**, I wish to perform the operation.
4. Click **OK**.

Resume Mirroring

Mirroring can be resumed only when all members of the asynchronous mirror group are in the **Optimal** status. The resume operation can be performed only by the storage array that has the primary role for the AMG. To resume mirroring, do the following:

1. **Select** the suspend AMG from the Asynchronous Mirror Groups window.
2. Click Resume Mirroring icon.
3. Select **Yes**, I wish to perform the operation.
4. Click **OK**.

Manual Resync

The **Manual Resynchronization** operation forces the immediate resynchronization of the data on all mirrored pairs within the AMG. A manual resynchronization must be performed by the storage array that has the primary role for the AMG.

Note: You cannot perform a manual resynchronization until the minimum wait time (10 minutes) between synchronizations has elapsed.

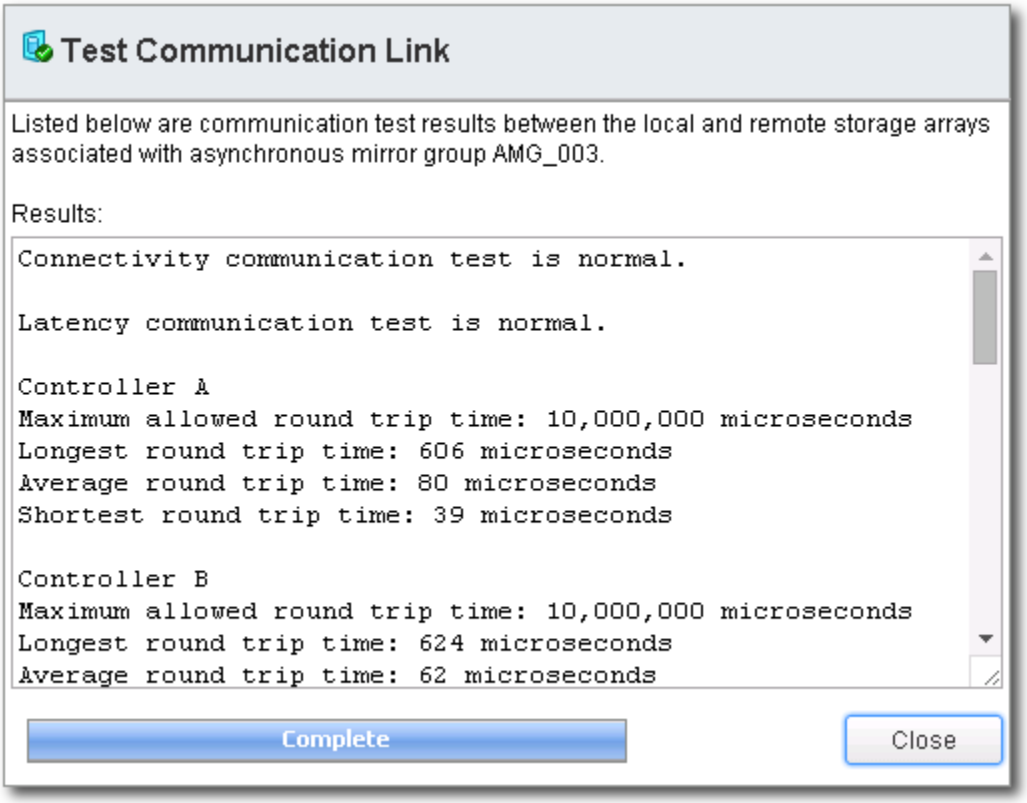
To manually synchronize an AMG, do the following:

1. **Select** an AMG from the Asynchronous Mirror Groups window.
2. Click **Manual resync** icon.
3. Select **Yes**, I wish to perform the operation.
4. Click **OK**.

Test Mirror Communication

The **Test Mirror Communication** option displays statistics between the two storage arrays configured for the AMG. Select the AMG to obtain information and then click the **Test Mirror Communication** icon. The **Test Communication Link** results are then displayed.

Figure 63) Test Communication Link results.



Change Roles

A **Change Roles** option promotes the current secondary mirror group to the primary role and demotes the current primary mirror group to the secondary role. After roles are changed, hosts mapped to the former primary volumes in the AMG no longer have write access to the mirrored volumes. Hosts in the AMG that was promoted to the primary role now have write access to the mirrored volumes.

Note: If the AMG is not resynchronized, data written to primary volumes after the last synchronization is lost and cannot be recovered.

To change roles, do the following:

1. **Select** the AMG within the Asynchronous Mirror Groups window.
2. Click **Change Roles** icon.

- The Confirm Change dialog box appears
- The **Resynchronize mirror group now** check box is selected by default. To prevent the resynchronization, clear the check box.
- Select **Yes, I wish to perform this operation**.
- Click **OK**.

The Asynchronous Mirror Groups window shows the role change for the AMG. In the Mirrored Pairs window, the primary and secondary volumes in the AMG have switched roles.

Delete Mirror Group

Asynchronous mirror groups can only be deleted once all mirrored pairs have been removed from the AMG. Once all the mirrored pairs have been removed, select the **Delete Mirror Group** option from the **Actions** dropdown menu.

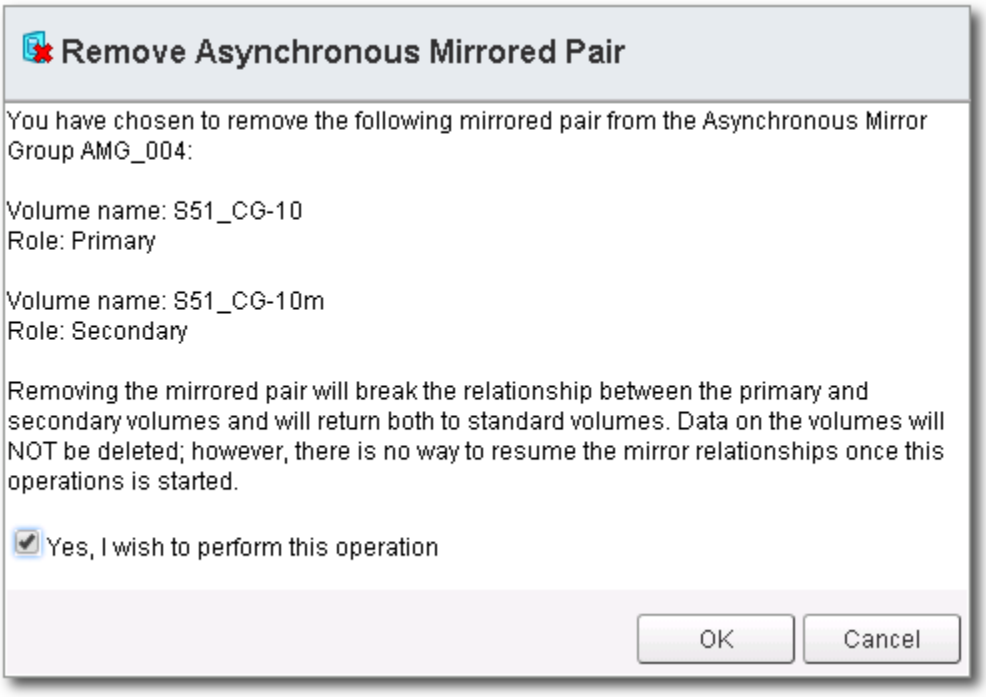
Remove Mirrored Pair

Removing a mirrored pair breaks the relationship between the primary volume and the secondary volume. Both volumes are return to standard volume status. No data is deleted from either the source volume or the target volume. To remove a mirrored pair, perform the following:

1. In the **Asynchronous Mirror Groups** table, **select** the asynchronous mirror group from which to remove the mirrored pair.
2. **Select** the mirrored pair to be removed from the **Mirrored Pairs** table.
3. Click **Remove Mirrored Pair** command from the **Actions** dropdown menu.

The Remove Asynchronous Mirrored Pair dialog box appears.

Figure 64) Remove Asynchronous Mirrored Pair dialog box.



4. Select **Yes**, I wish to perform the operation.
5. Click **OK**.

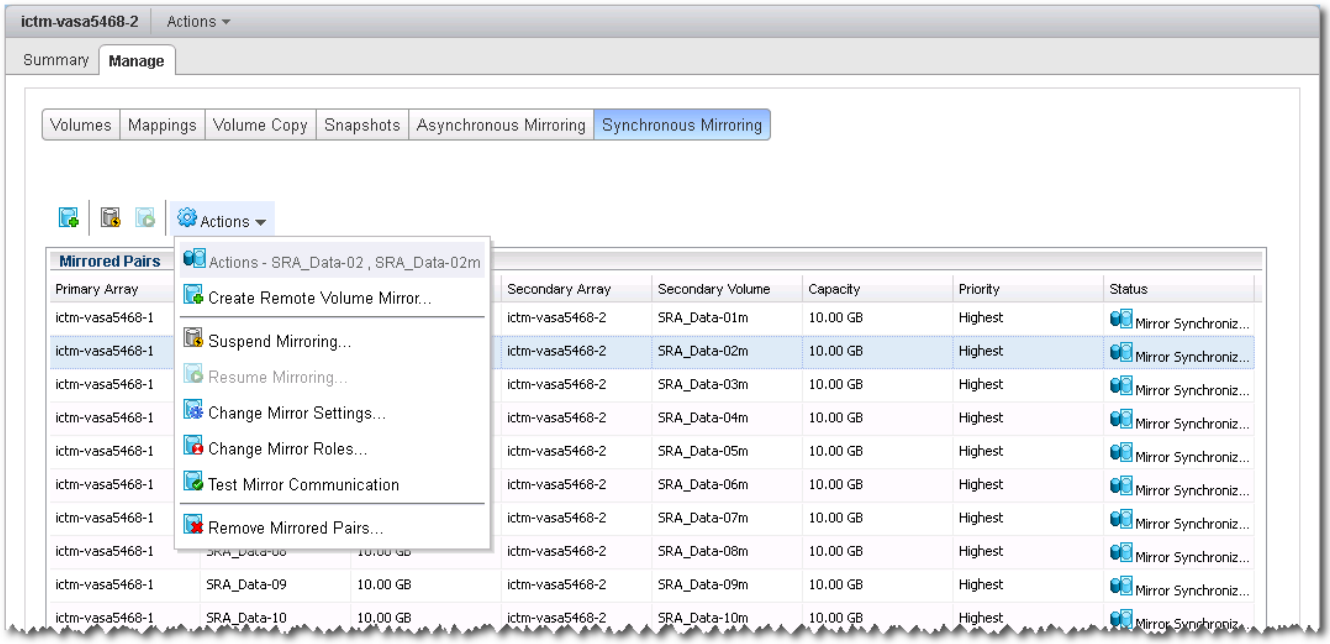
The mirrored pair is removed from the **Mirrored Pairs** table.

Synchronous Mirroring View Features

When the Synchronous Mirroring premium feature is enabled on the storage array, the **Synchronous Mirroring** tab appears within the NetApp plug-in. From this tab, existing synchronous mirror pairs are displayed along with the Commands area, which allows for the following commands:

- Create Remote Volume Mirror....
- Suspend Mirroring....
- Resume Mirroring....
- Change Mirror Settings....
- Change Mirror Roles....
- Test Mirror Communication
- Remove Mirrored Pairs....

Figure 65) Synchronous Mirroring View.



Create Remote Volume Mirror

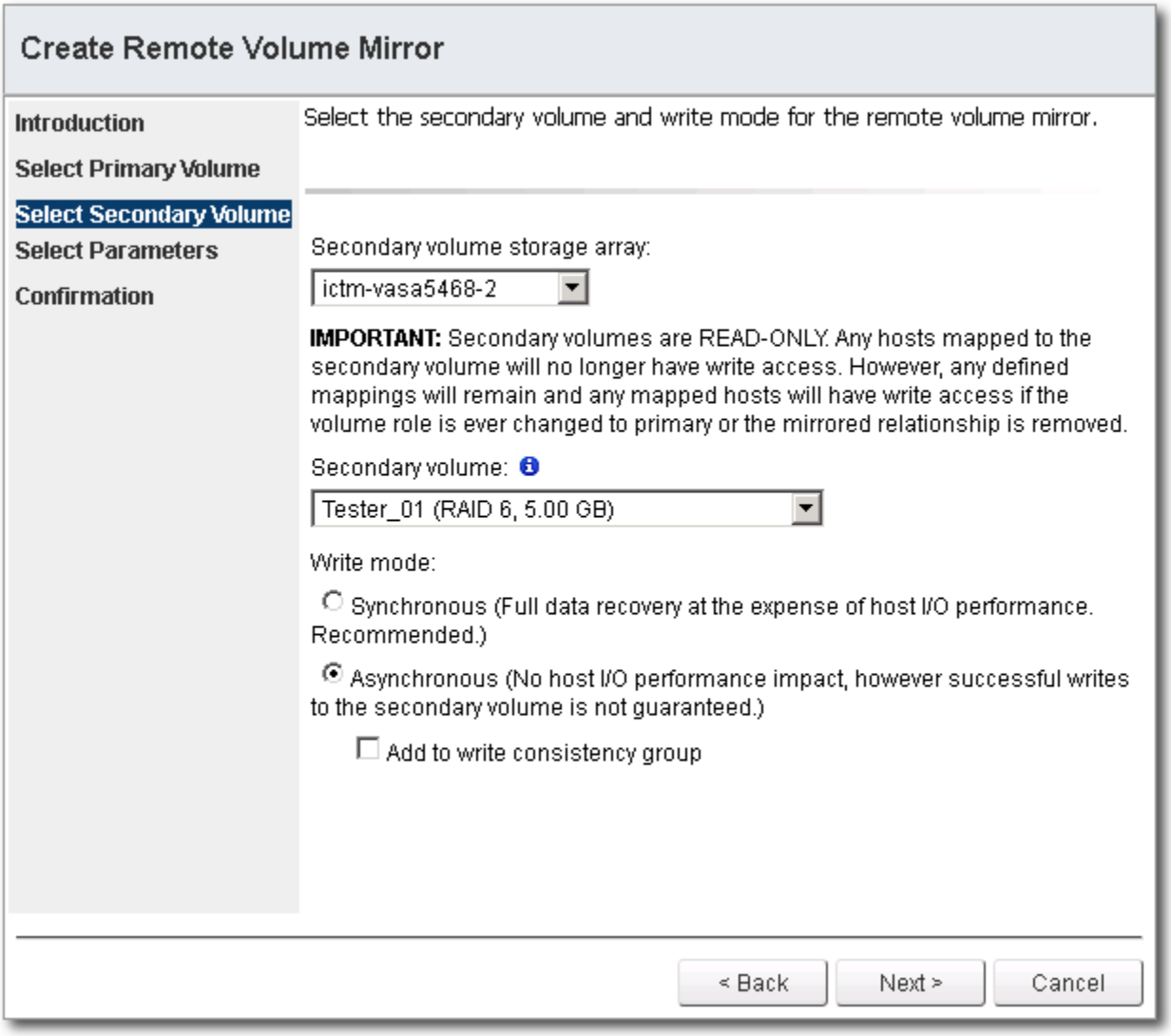
The **Create Remote Volume Mirror** command is used to establish a remote volume mirror between two storage arrays connected via fibre channel. To establish a new remote volume mirror, perform the following:

Note: To create a synchronous mirror, both the local and the remote storage arrays must be added to the Array Manager view.

1. Click the Create Remote Volume Mirror command.
2. Review the **Introduction** wizard instructions and click **Next**.
3. Select the primary volume for the mirror relationship and click **Next**.
4. From the drop-down list, **select** the remote storage array for the mirror.
5. From the drop-down list, **select** the secondary volume to be the target of the primary volume.
6. Select the write mode for the remote mirror and click **Next**.
7. **Choose** resynchronization method to use.
8. From the drop-down list, **select** the synchronization priority for the mirror and click **Next**.

9. Review the **Confirmation** page, and click **Finish** to establish the mirror relationship.

Figure 66) Create Remote Volume Mirror Dialog Box.



Suspend Mirroring

To suspend synchronous mirroring of a mirrored pair:

1. **Select** the mirrored pair from the Mirrored Pairs window.
2. Click Suspend Mirroring icon.
3. Click **OK** to suspend the selected mirror pair or **Cancel** to abort the operation.

The I/O between the mirrored pairs is suspended, but the mirrored association is maintained.

Resume Mirroring

To resume mirroring of a suspended mirror pair:

1. **Select** the suspended mirror pair from the Mirrored Pairs window.
2. Click Resume Mirroring icon.
3. Choose **OK** to resume mirroring of the selected mirror pair or **Cancel** to about the operation.

The I/O between the mirrored pairs resumes, and out-of-sync data is resynchronized.

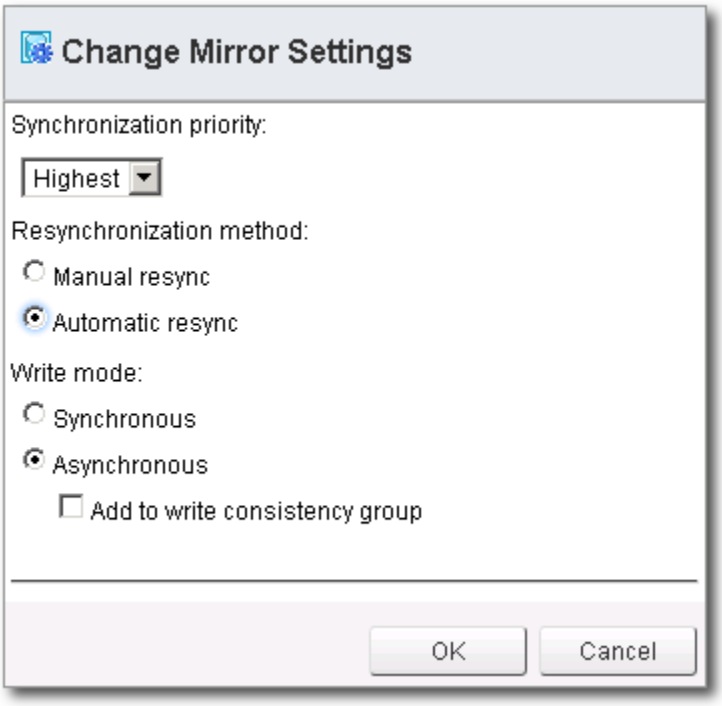
Note: This option is available only for mirrored pairs that have been suspended.

Change Mirror Settings

To modify the parameters of a mirrored pair, such as the synchronization priority, the resynchronization method, or the write mode, perform these steps:

1. **Select** the mirrored pair to modify.
2. Click **Change Mirror Settings** command from the **Actions** dropdown menu.

Figure 67) Change Volume Copy Parameters.



3. **Modify** the displayed parameters as needed.
4. Click **OK**.

Change Mirror Roles

Changing mirror roles makes the following role changes in the mirrored pair:

- Promotes the secondary volume to the primary volume and allows read-write access to the volume from the remote location.
- Demotes the primary volume to the secondary volume and disables writes to the volume from the primary site.

To change mirror roles:

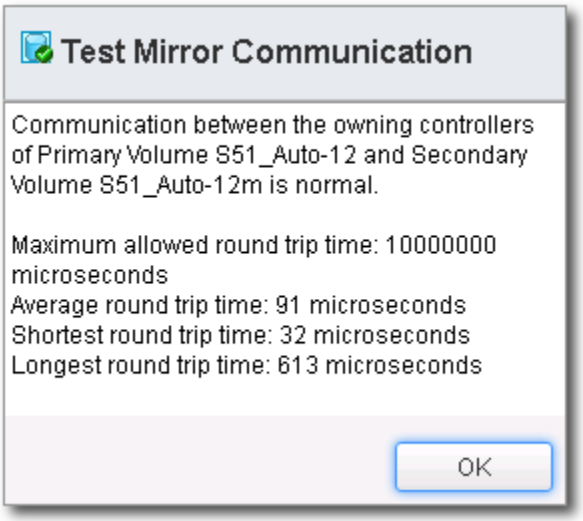
1. **Select** the mirrored pair from the **Mirrored Pairs** window.
2. Click **Change Mirrored Roles** command from the **Actions** dropdown menu.
3. Choose **OK** to change the mirror roles or **Cancel** to abort the operation.

Test Mirror Communication

Testing mirrored communication displays the round-trip times between the volumes in the mirrored pair. The times are displayed as average round-trip times, shortest round-trip times, and longest round-trip times.

To test mirrored communication, click **Test Mirrored Communication** command from the **Actions** dropdown menu. Click **OK** to close the dialog box after reviewing the information display.

Figure 68) Test Mirror Communication results.



Remove Mirrored Pairs

Removing a mirrored pair breaks the mirroring association between the volume at the primary site and the volume at the secondary site. After the operation completes, the mirroring status between the volumes is lost. For mirroring to be re-established between the volumes, a full resynchronization must occur. To remove a mirrored pair relationship, perform the following steps:

1. **Select** an existing mirrored pair from the **Mirrored Pairs** window.
2. Click **Remove Mirrored Pairs** command from the **Actions** dropdown menu.
3. Click **OK** to remove the mirrored pair or **Cancel** to about the process within the **Remove Mirrored Pairs** dialog box.

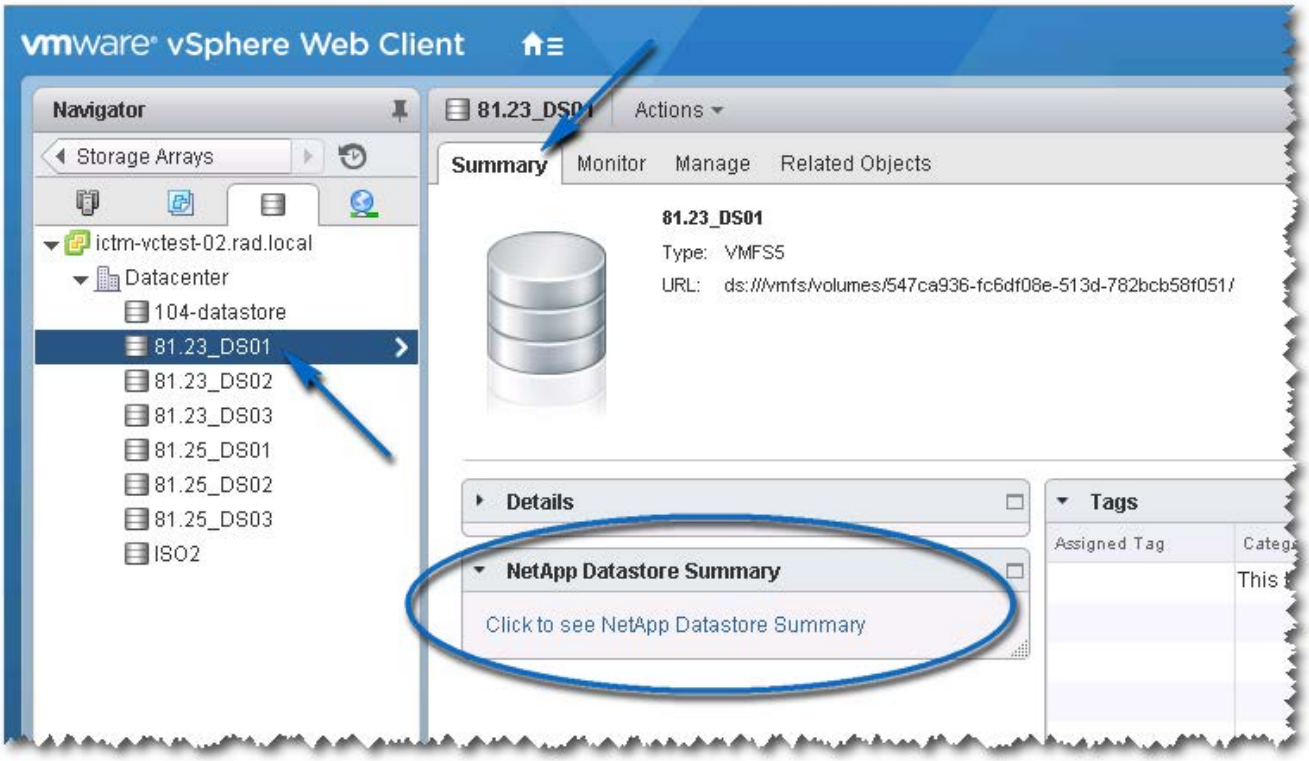
Note: The remove action will not remove the secondary volume from the remote array or remove the existing data on the secondary volume.

NETAPP DATASTORE SUMMARY INFORMATION

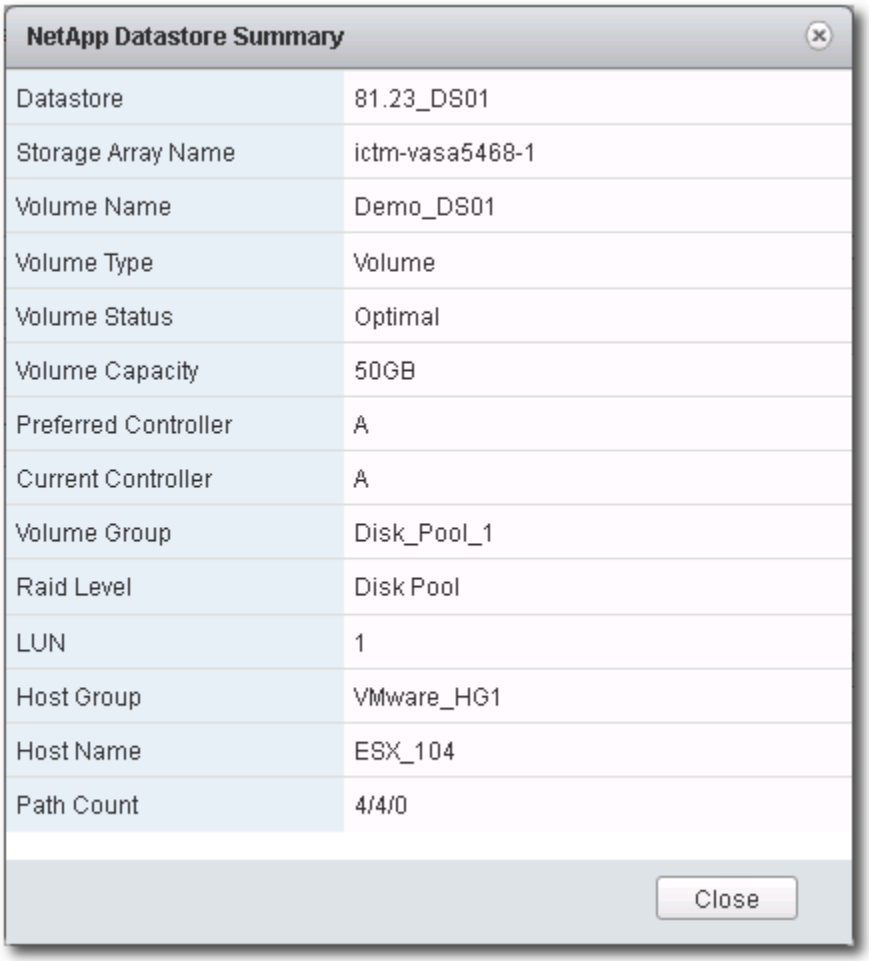
Datastore summary information may also be displayed by performing the following:

1. Navigate to the **Storage** view from the home button .
2. Select the Datastore to view from the Navigator list.
3. Click the **NetApp Datastore Summary** link.

Figure 69) VMware vCenter Storage Summary view.



The summary information for the selected datastore is then displayed. This includes storage array specific information on the underlying volumes servicing the selected datastore.



BEST PRACTICES

This section provides best practices for using NetApp E-Series storage arrays within VMware vSphere environments.

Defining Volumes for vSphere

Before you provision volumes for VMFS datastores, you must plan how to set up storage for the ESXi systems, including deciding on the number of volumes to use and the size of the volumes.

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

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

Volume Decision-Making Schemes

When the storage characterization for a VM is not available, you can use either the predictive scheme or the adaptive scheme to decide on the volume size and number of volumes to use.

Using the Predictive Scheme to Make Volume Decisions

1. Create several volumes with different storage characteristics.
2. Build a VMFS Datastore on each volume. Label each datastore according to its characteristics.
3. Allocate volumes to contain the data for VM applications in the VMFS datastores built on volumes with the appropriate RAID level for the applications' requirements.
4. Use disk shares to distinguish high-priority VMs from low-priority virtual machines.

Note: Disk shares are relevant only within a given host. The shares assigned to VMs on one host have no effect on VMs on other hosts.

5. Run the applications to determine whether VM performance is acceptable.

Using the Adaptive Scheme to Make Volume Decisions

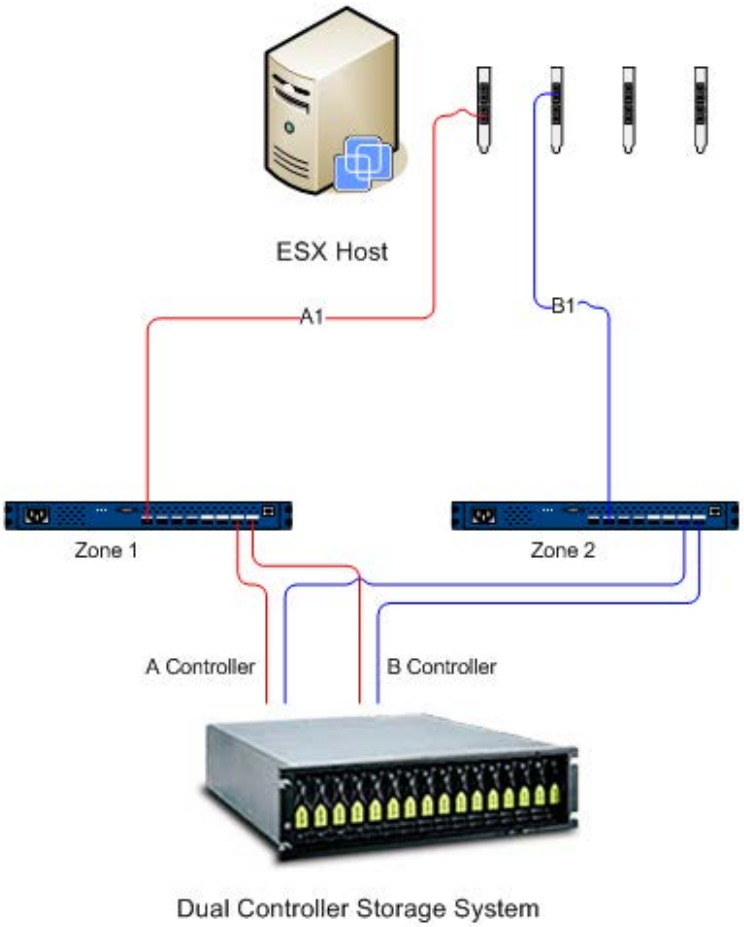
1. Create a large volume, such as RAID 1+0 or RAID 5, and enable write caching.
2. Build a VMFS datastore on that volume.
3. Place four or five volumes on the VMFS datastore.
4. Run the applications to determine whether disk performance is acceptable.

- If performance is acceptable, you can place additional volumes on the VMFS datastore.
- If performance is not acceptable, create a new, larger volume, and repeat the process. You can use a different RAID level. Use migration so that you do not lose VMs when you re-create the volume.

VMware ESXi Host Fibre Channel Configuration

The NetApp plug-in allows an ESXi host to be automatically configured to use a NetApp E-Series storage array by detecting the installed host bus adapters (HBAs) within the ESXi host and configuring new hosts on the storage array with the World Wide Names (WWNs) of the HBAs from the ESXi host. The default ESXi multipathing mode NetApp for E-Series Fibre Channel storage arrays is Most Recently Used (MRU). To ensure optimum performance for the ESXi host with more than two HBAs, the ESXi host should be configured to use the storage array in pairs of HBAs. This method allows for the maximum I/O throughput from the ESXi host to the storage array. Using this method requires proper SAN configuration and balancing of LUNs between hosts/host groups. Figure 70 shows a properly configured two-HBA port, ESXi host, SAN configuration utilizing two fabric switches and a dual-controller storage array.

Figure 70) Dual Port HBA Configuration.



This example shows a fully redundant fabric configuration. If a Fibre Channel (FC) switch or HBA fails, the alternate switch still connects to both storage controllers in the storage array. If a storage controller also fails, the ESXi host can still access the remaining controller, and all volumes fail over to that controller. A complete loss of access to storage occurs if any other element fails.

Figure 71) Single Failure.

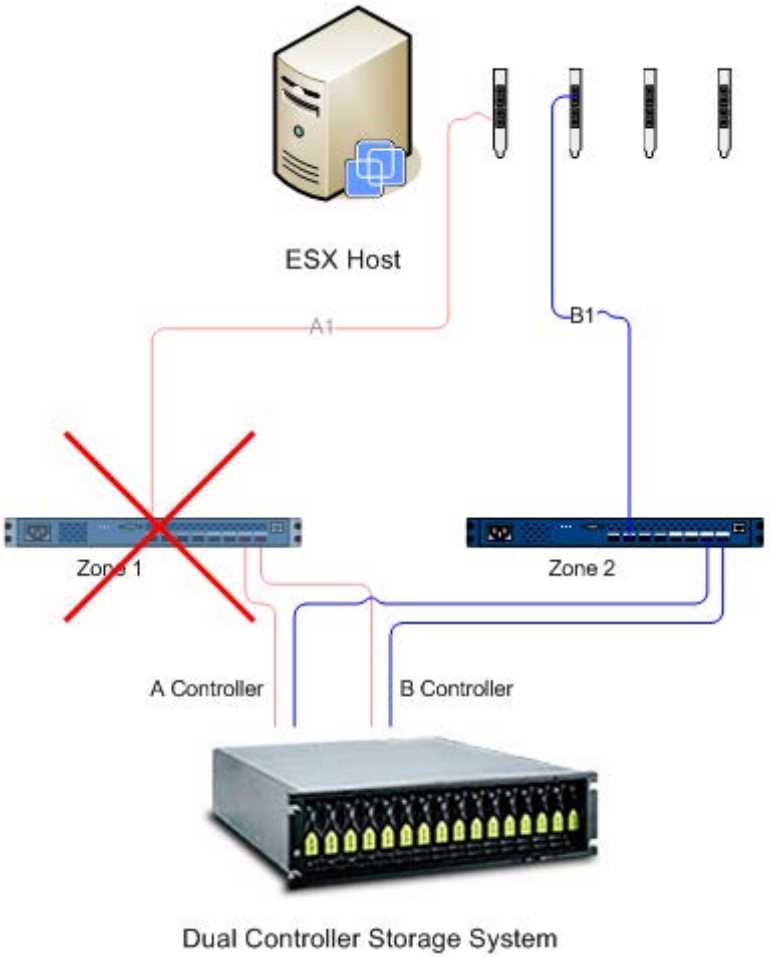
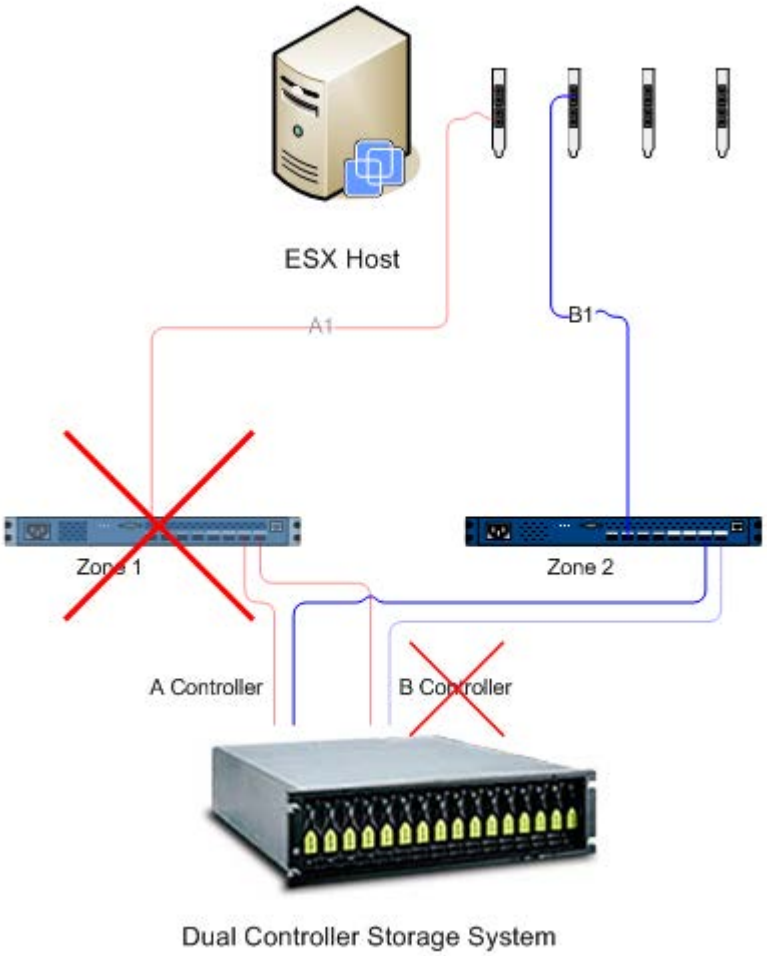
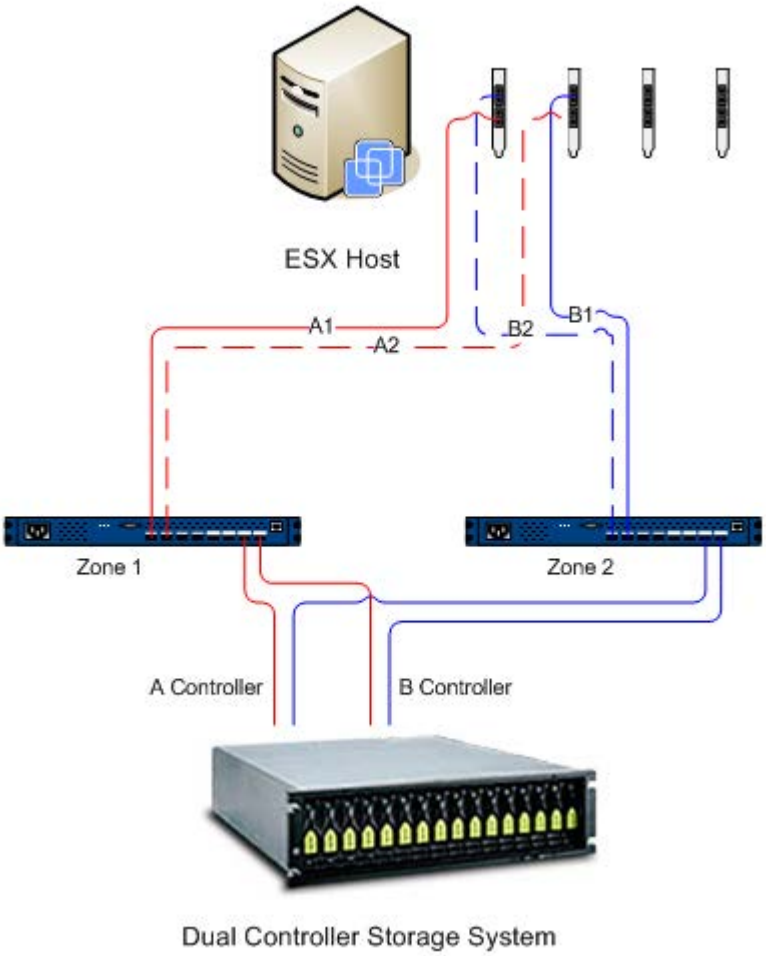


Figure 72) Double Failure.



This method works well to maintain access to the data in case of a hardware failure; however, MRU only maintains one active path for each HBA group. Therefore, if you have an ESXi host with four HBAs, only one HBA is active at a time. To achieve higher I/O throughput from the ESXi 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. From the storage array, the second pair of HBAs is defined as a separate host, and volumes 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 FC bandwidth between all HBA groups. When this method is used in the array, the Automatic ESXi Host Configuration utility cannot determine which HBAs are configured to each zone in the fabric, and the user must verify that a single HBA is connected to both fabric zones for each HBA pair group.

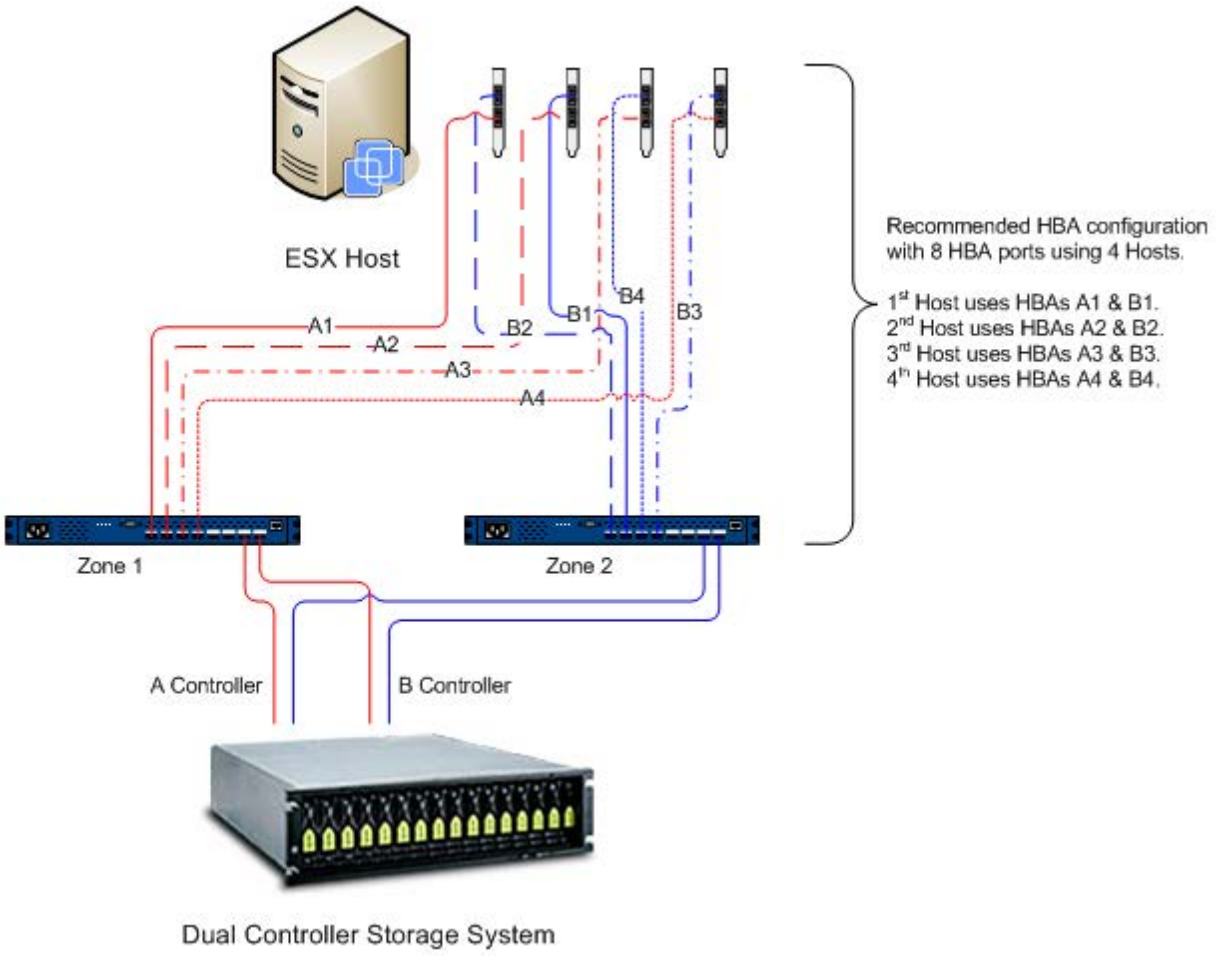
Figure 73) Quad Port Configuration.



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 74 shows how an 8-port HBA configuration can be configured.

Figure 74) 8 HBA Port Configuration.



APPENDICES

Current Restrictions

This section describes known issues and available workarounds with NetApp plug-in version 3.0.

ID: 200627833 – Multiple Item Delete Restricted to Less Than 80 Objects

Issue: When using multiple array delete or multiple volume delete, you must limit the number of selected objects to less than 80 per invocation of the command. This is due to the addressing space allowed by the SDK.

Work Around: Run the multiple delete action repeatedly selecting less than 80 objects per invocation.

Note: Microsoft Internet Explorer browsers are limited to less than 40 objects per invocation.

ID: 200702748 – ESXi Host to Storage Array Wizard Usability Issues

Issue:

1. The "Add Host Group..." button should be greyed-out on the initial loading of the manual configuration page.
2. After creating an object under the parent item in the tree of the manual configuration page, the visual representation of being selected (blue background on the label) on the parent is not displayed. The font of the label stays bold.
3. The Rename dialogs for the Host Group and Host do not have titles.
4. After staging the objects to be created and you are on the Review Changes page, if you click on the back button your items that were staged are no longer displayed.

Work Around: There is no real workaround for these issues.

ID: 200716368 – vSphere 6.0 SAS Datastore View

Issue: When using vSphere 6.0, SAS Datastore volumes are not displayed in the Plug-in Datastores view portlet.

Work Around: There is no workaround for this issue at this time.

Configuration Worksheet

vCenter server Name: _____

DNS Name: _____

IP Address: _____

vCenter server Administrator Name: _____

Password: _____

Application Server Name: _____

DNS Name: _____

IP Address: _____

Storage Administrator User ID: _____

Security Level: Read-Only _____ or Read-Write _____

Storage Administrator User ID: _____

Security Level: Read-Only _____ or Read-Write _____

Storage Array 1 Name: _____

IP Address(es): _____/_____

Password: _____

Storage Array 2 Name: _____

IP Address(es): _____/_____

Password: _____

Storage Array 3 Name: _____

IP Address(es): _____/_____

Password: _____

Storage Array 4 Name: _____

IP Address(es): _____/_____

Password: _____

Trademark information

Copyright information

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277


NetApp