Dell EMC VSI for VMware vSphere Web Client

Version 7.4

Product Guide

P/N 302-000-051

REV 18

DELL EMC

Published July 2018

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

CHAPTER 1

Introduction

This chapter includes the following topics:

About this document

This document provides installation and configuration instructions for the Dell EMC Virtual Storage Integrator (VSI) for VMware Web Client plug-in. It also includes information about managing, provisioning, and viewing storage arrays using the VSI plug-in.

Audience

This solution was designed for VMware administrators who manage shared NFS or VMFS storage through a web interface.

After the storage administrator has planned and implemented the storage environment, the VMware administrator sets up the VMware virtual environment and loads Dell EMC VSI for VMware vSphere Web Client. This software enables VMware administrators to provision and manage datastores, virtual machines, and RDMs on the supported Dell EMC storage systems without the direct involvement of the storage administrator.

Scope

This document describes how to install, configure, and use Dell EMC VSI for VMware vSphere Web Client.

Related documentation

The following documents contain additional information and are available on Dell EMC Online Support:

- *Dell EMC VSI for VMware vSphere Web Client Release Notes*
- *Dell EMC SMI-S Provider Release Notes*
- Dell EMC storage system documentation
- Dell EMC AppSync™ documentation
- Dell EMC PowerPath™ Management Appliance documentation
- Dell EMC RecoverPoint™ documentation

Product Overview

The Dell EMC Virtual Storage Integrator (VSI) for VMware vSphere Web Client is a plug-in for VMware vCenter. It enables administrators to view, manage, and optimize storage for VMware ESX/ESXi servers and hosts, and then map that storage to the hosts.

VSI consists of a graphical user interface and the Dell EMC Solutions Integration Service (SIS), which provides communication and access to the storage systems.

Depending on the platform, tasks that you can perform with VSI include:

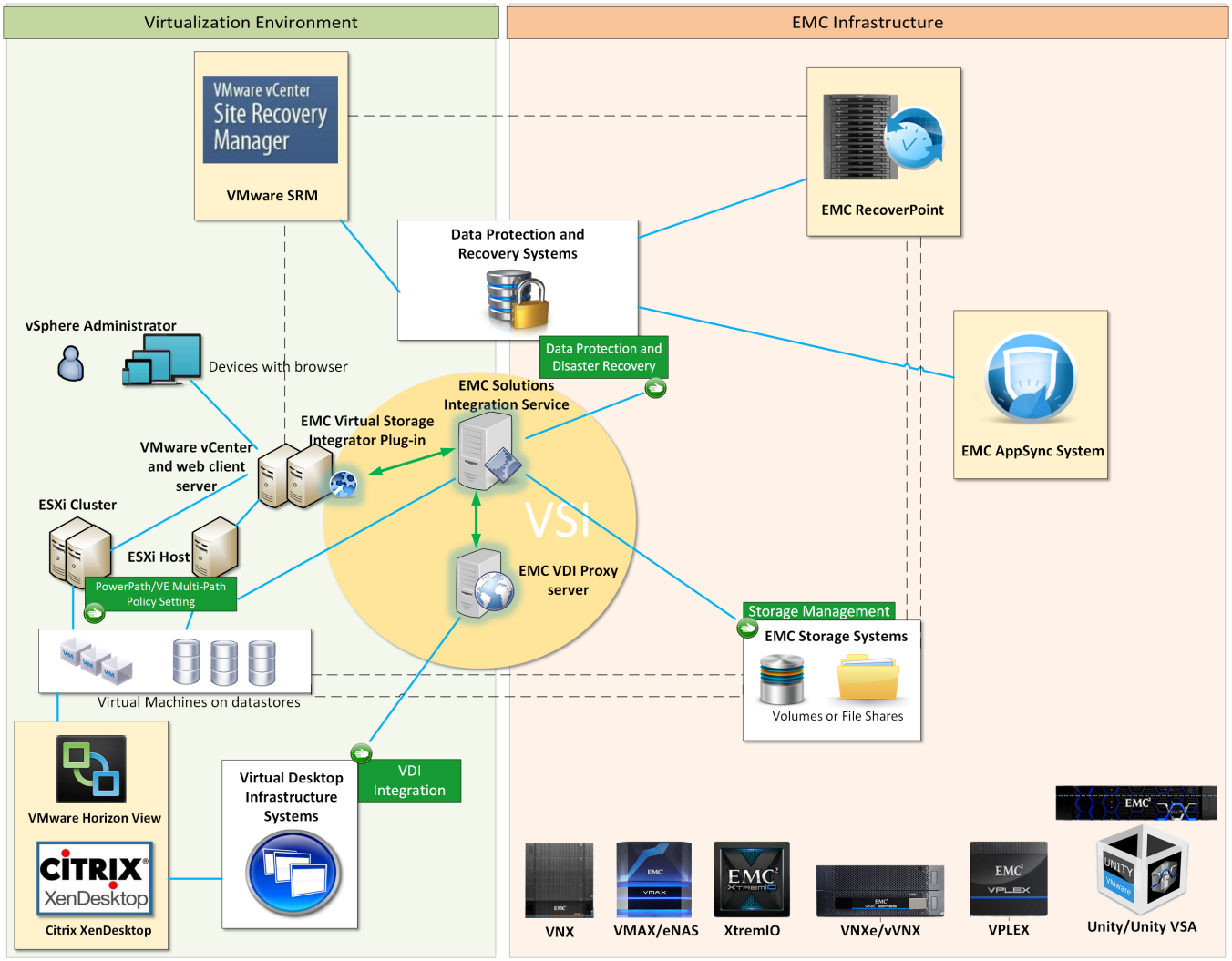
- Storage provisioning
- Setting multipathing policies
- Cloning
- Block deduplication

- Compression
- Storage mapping
- Capacity monitoring
- Virtual desktop infrastructure (VDI) integration
- Data protection using Dell EMC AppSync or Dell EMC RecoverPoint

Using the Solutions Integration Service, a storage administrator can enable virtual machine administrators to perform management tasks on a set of storage pools.

Dell EMC Simple Support Matrix lists supported versions of Dell EMC storage systems and software.
The following figure depicts the architecture of a typical deployment of VSI for VMware vSphere Web Client.

Figure 1 VSI deployment architecture



CHAPTER 2

Installing VSI and Setting Up the Environment

This chapter includes the following topics:

Overview

This chapter provides instructions for installing and upgrading the VSI plug-in, deploying the Solutions Integration Service, and using the Solutions Integration Service to register VSI and enable the VSI features.

Chapter 3 discusses additional functions of the Solutions Integration Service.

Software prerequisites

Learn where to find the software requirements for this product.

The supported environment and software requirements for the VSI for VMware vSphere Web Client are listed in the Dell EMC Simple Support Matrix.

This version of VSI supports multiple vCenters (Linked Mode, Enhanced Linked Mode and no Linked Mode). You must deploy the VSI Plug-in to all vCenters, even in the Linked Mode.

Upgrading VSI

The Solutions Integration Service OVA package contains the VSI plug-in. To upgrade to a newer version of VSI, download the latest OVA package from Dell EMC Online Support, and then follow the instructions in this section to migrate the database.

Before you begin

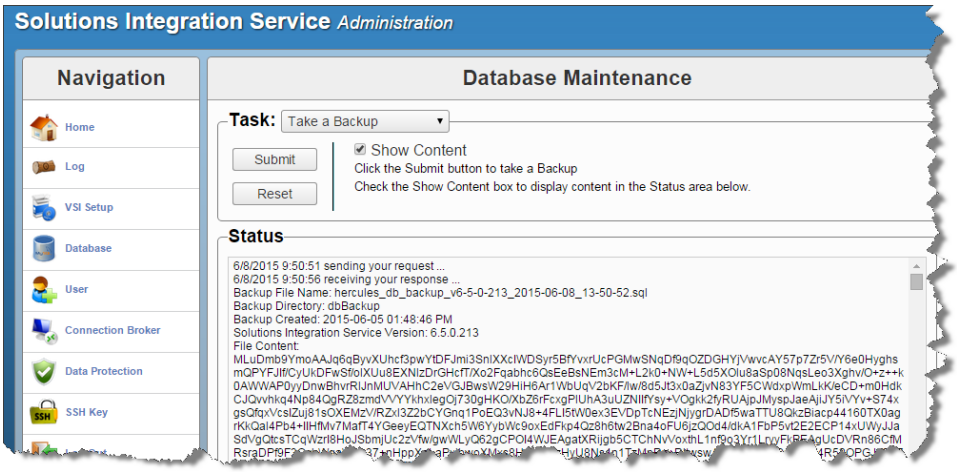
During the upgrade, VSI automatically removes registration information related to VMAX2 and vVNX arrays, as they are not supported in version 6.9.2 or later. However, VSI cannot remove reclaim schedules for Dell EMC VMAX2 or Dell EMC vVNX and you must remove them manually. Dell EMC recommends that you remove them before you upgrade.

Procedure

1. Log in to your current version of the Solutions Integration Service, click **Database** and select **Take a Backup** to create a backup of the existing database, and save the backup to a secure location.

   The backup file includes the Solutions Integration Service version number, as shown in the example below.

Figure 2 Creating a backup of the Solutions Integration Service database



2. Deploy the new Solutions Integration Service OVA file.

   Follow the instructions in Deploying the Solutions Integration Service on page 15.

3. Log in to the new Solutions Integration Service, click **Database** and select **Take a Backup** to create a backup of the new Solutions Integration Service database, and save the backup to a secure location.

Note

When migrating data from the previous version, you must complete the following steps immediately after the new version is deployed. If you use the new version (for example, to grant storage system access control) before migrating the data, the migration could fail and you must then provision everything manually.

---

4. Select **Data Migration.**
5. Click **Choose File** and locate the file you created in step 1 (the backup of the previous version).
6. Click **Submit**.
7. Verify the migration is complete:
   - If the migration is successful, deactivate the previous version of the Solutions Integration Service (if not already done). All Solutions Integration Service data for the previous version are moved to the new version, including users, storage systems, and access control information.
   - If the migration fails:
     a. Restore the new Solution Integration Service database from the backup file you created in step 3 on page 13.
     b. Manually provision all required elements.
8. Register the VSI plug-in, as described in Registering the VSI plug-in on page 17.

Installing VSI

Read this section if you are installing VSI for VMware vSphere Web Client for the first time.

Procedure

1. Install the VMware vSphere Web Client using the VMware documentation at www.vmware.com.

   Required environment and system requirements are listed on the Dell EMC Simple Support Matrix.

2. Download the Solutions Integration Service OVA file:

   a. From Dell EMC Online Support, search for **`VSI for VMware vSphere Web Client`**.

   b. Click the **VSI for VMware vSphere Web Client 7.3** download link.

   The downloaded file name is `emc_solutions_integration_service_v73_x86_64_OVF10.ova`.

Configuring the environment

To deploy the Solutions Integration Service and enable the VSI plug-in, you must identify parameter values, deploy the Solutions Integration Service, register the VSI plug-in, and set up port assignments. The following sections detail the steps to complete these tasks.

Identifying parameter values

Gather and record the required parameter values described in this section.

Table 1 Required parameter values

Item	Component	Description	Value
1	vSphere Web Client	URL/IP address and port number of the VMware vSphere Web Server (example: https://192.168.0.1:9443)	
		Login credentials (administrator username and password)	
2	vCenter server where the OVF/OVA is to be deployed	vCenter server IP address (example: 192.168.0.2)	
		vCenter login credentials (username and password)	
3	Solutions Integration Service OVA file location	URL or a folder location on your local drive Example: `(C:)\\Users\username\Downloads`	

Table 1 Required parameter values (continued)

Item	Component	Description	Value
4	Deployment destination for the Solutions Integration Service	Path and folder name on the VMware vCenter server where the service is to run	
5	Compute resource	A cluster, host, or resource pool	
6	Source network	The name and IP address format of the network where the service is to be deployed	
7	Custom properties/IP addresses	• Public network IP address • Default gateway • DNS servers (if needed) • Netmask IP address	

Deploying the Solutions Integration Service

Follow the steps in this section to install and configure the Solutions Integration Service.

Use the values in Table 1 on page 14 to complete the following steps.

Procedure

1. Log in to the vSphere Web Client (Item 1).
2. Select **Home** > **Hosts and Clusters**.

   Optionally, expand the directory to select a specific folder or datastore.
3. Right-click the vCenter, cluster, or host storage device (Item 2) and select **Deploy OVF Template.**

   The following message appears: `This site is using the VMware Client integration Plug-In. Do you want to allow it to access your operating system?`
4. Click **Allow**.

   The Deploy OVF Template wizard appears.
5. In **Select source**, enter the location of the Solutions Integration Service OVA file (Item 3), and then click **Next**.
6. On the **Review details** screen, verify that the information is correct and click **Next**.
7. Accept the **End User License Agreement (EULA)** and click **Next.**
8. In **Select name and folder**, type a name for the destination folder or accept the default.
9. Select the folder or datacenter location (Item 4) where you want to save the Solutions Integration Service OVA file and click **Next**.
10. For **Select a resource**, select the compute resource (Item 5) and click **Next**.
11. For **Select storage**:

a. Select an appropriate disk format.

b. Select the datastore for the deployed OVF/OVA for the project.

c. Click **Next**.

12. For **Setup network**, use the values in Item 6 to:

    a. Select a network.

    b. Select the IP address format IPV4 for the Solutions Integration Service.

13. For the **Customize Template** properties, enter the following details (Item 7):

    - **Public network IP address**
    - **Default gateway**
    - **DNS servers**
    - **Netmask IP address**

14. Click **Next**.

15. In the **Ready to Complete** dialog box:

    a. Verify the details.

    b. If you want the Solutions Integration Service to power on immediately after the OVF/OVA deployment, select the check box in the **Ready to Complete** dialog box. Otherwise, you can power it on manually.

    c. Click **Finish**.

16. Right-click the name of the virtual machine with the newly deployed EMC Solutions Integration Service and select **Power On**.

17. Wait for the deployment to finish and for the Solutions Integration Service to be operational.

18. Verify the REST web service as follows:

    a. Log in as follows:
    `https://`*`Solutions Integration Service IP Address`*`:8443/vsi_usm/`

    For example: `https://192.168.0.3:8443/vsi_usm/`

    b. Accept all certificates or add them to exceptions.

19. To change the root password, login to the vSphere console with the default username **`root`** and password **`root`**. The operating system will prompt for a password change and you will need to set a new, secure password for the root user.

20. To enable SSH on the machine, log in to the vSphere and type **`systemctl enable sshd`** and **`systemctl start sshd`**. The SSH service is now enabled.

Results

The **Welcome to the Dell EMC VSI Solutions Integration Service** screen appears and the Dell EMC VSI Solutions Integration Service is ready for use.

Registering the VSI plug-in

You must register the VSI plug-in to download and enable the VSI plug-in extensions.

Procedure

1. Using a browser, go to the Solutions Integration Service Administrator web page. Log in with the Solutions Integration Service credentials as follows: `https://<Solutions Integration Service IP Address>:8443/vsi_usm/admin`

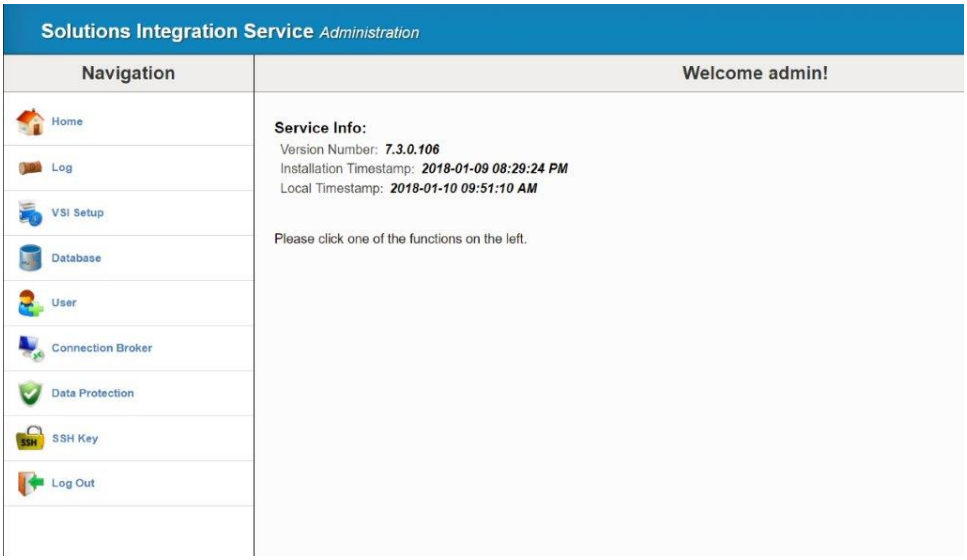
   For example: `https://192.168.0.3:8443/vsi_usm/admin`

   Note

   If this is the first time that you are logging in, see Logging in to the Solutions Integration Service on page 25.

   The Solutions Integration Service Administration Home screen appears, as shown in the example below.

   Figure 3 Solutions Integration Service Administration Home screen

2. Click **VSI Setup**.
3. Enter the values for the following parameters and click **Register.**
   - **vCenter IP/Hostname**: The IP address that contains the VSI plug-in package.
     This is the IP address of the vCenter to which you are registering the VSI plug-in. If you are using the vCenter hostname, ensure that DNS is configured.
   - **vCenter Username**: The username that has administrative privileges.
   - **vCenter Password**: The administrator's password.
   - **Admin Email (Optional)**: The email address to which notifications should be sent.
4. Browse to the vSphere Web Client address using the information from Table 1 on page 14.

After you log in, the VSI plug-in is downloaded and deployed.

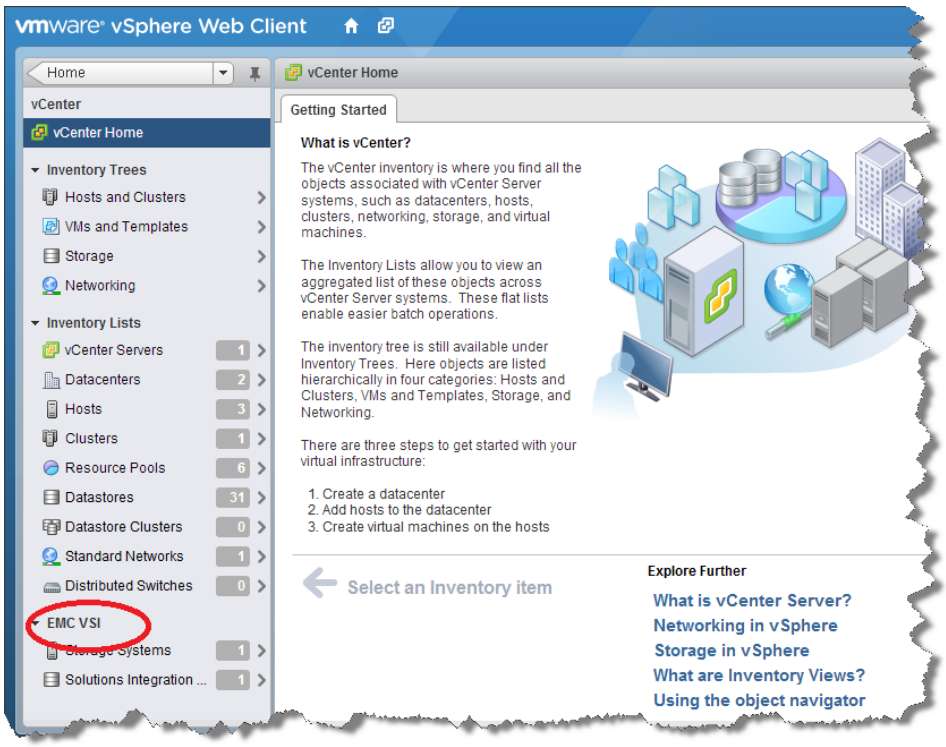
Note

The download takes several minutes.

If you have installed previous versions of the VSI plug-in, clear your browser cache to ensure that you use the newest version of VSI.

5. In the **vSphere Web Client** window, select **vCenter** in the navigation pane to verify that **Dell EMC VSI** is listed, as shown below.

Figure 4 Verifying that Dell EMC VSI is installed



Default port assignments

Review the default port assignments.

The default port assignments for communication on the storage and data protection systems as shown in the following table.

Table 2 Port assignments

System	Request type	Source	Destination	Default port
All storage arrays	VSI requests sent to Solutions Integration Service (SIS)	VSI	SIS	8443
All storage arrays	SIS requests sent to vCenter SDK	SIS	vCenter	443
Dell EMC VNX arrays	SIS file requests sent to control station (CS)	SIS	CS	22
VNX arrays	SIS DHSM requests sent to Data Movers	SIS	Data Mover	5080

Table 2 Port assignments (continued)

System	Request type	Source	Destination	Default port
VNX arrays	SIS block requests sent to storage processors (SP)	SIS	SP	443
Dell EMC VMAX3 and Dell EMC VMAX All Flash arrays	SIS requests sent to SMI-S Provider	SIS	SMI-S	HTTP: 5988, HTTPS: 5989
VMAX3 and VMAX All Flash eNAS	SIS file requests sent to control station (CS)	SIS	CS	22
	SIS DHSM requests sent to Data Movers	SIS	Data Mover	5080
Dell EMC XtremIO™ arrays	SIS requests sent to XMS	SIS	XtremIO XMS	443
Dell EMC AppSync™ data protection	SIS requests sent to AppSync server	SIS	AppSync server	8445
Dell EMC RecoverPoint™ data protection	SIS requests sent to RecoverPoint server	SIS	RecoverPoint server	7225
Site Recovery Manager (SRM) data protection	SIS requests sent to SRM server	SIS	SRM server 5.8 SRM server 6.0	9007 9086

Uninstalling VSI

Follow the steps in this section to uninstall VSI.

Procedure

1. Log in to the Solutions Integration Service, click **Maintain Database** and select **Take a Backup** and save to a secure location.
2. Unregister VSI.

   You can use the **VSI Setup** feature of the Solutions Integration Service or see Unregistering or refreshing the Solutions Integration Service on page 24.
3. Power off the Solutions Integration Services virtual machine in the hosting vCenter.
4. Delete the SIS disk in the hosting vCenter.

CHAPTER 3

Dell EMC Solutions Integration Service

This chapter includes the following topics:

Dell EMC Solutions Integration Service roles

The Solutions Integration Service enables administrators to view log files, register the VSI plug-in, provide access to storage administrators and users, and back up and restore configurations.

The Solutions Integration Service defines the following three roles:

- *Admin*: A preconfigured user in the distributed Solutions Integration System who can create Storage Administrator (Storage Admin) and User roles and perform the functions described in Solutions Integration Service functions on page 26.
- *Storage Admin*: A role created by the Admin who can perform the functions described in Managing storage administrator tasks on page 39.

  Note

  vSphere administrators must register at least one storage system on vSphere to be able to manage storage access in the Solutions Integration Service.

- *User*: A role created by the Admin, which gives the user access to storage in the VSI Web Client.

Configuring the Solutions Integration Service

Learn how to configure the Solutions Integration Service.

The Solutions Integration Service provides the communication between the storage system and VMware vSphere, as shown in Figure 1 on page 9. Before you can use VSI, you must configure access to the Solutions Integration Service by registering the service with the appropriate credentials.

Registering the Solutions Integration Service

Registering the Solutions Integration Service enables it to communicate with one or more vCenters.

Note

You can register only one Solutions Integration Service. For a VSI upgrade or to use a different server, you must first unregister the current service. Unregistering or refreshing the Solutions Integration Service on page 24 provides more information.

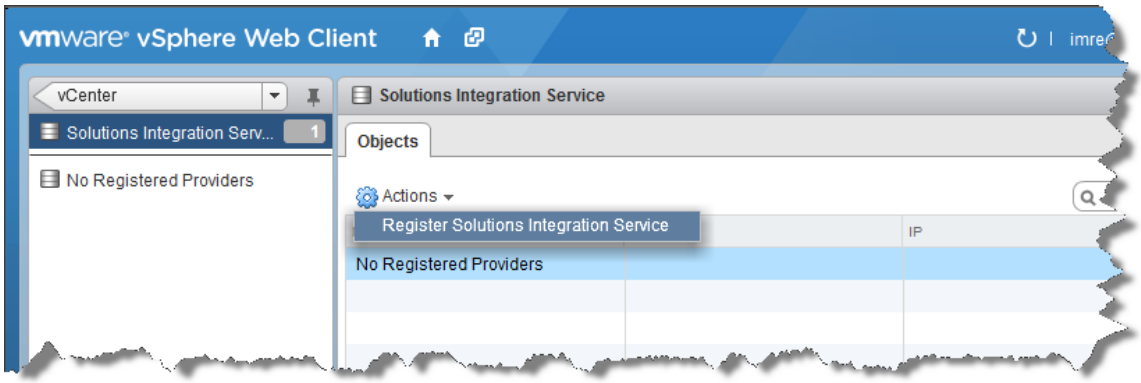
Procedure

1. Log in to the vSphere Web Client with the IP address and port number.

   For example, https://192.168.0.1:9443/vsphere-client

2. Select **Home** > **vCenter** > **Dell EMC VSI** > **Solutions Integration Service.**
3. Under **Actions** select **Register Dell EMC Solutions Integration Service**, as shown below.

Figure 5 Registering the Solutions Integration Service



4. In the **Register Dell EMC Solutions Integration Service** wizard, enter values for the following parameters:
   - **Dell EMC Solutions Integration Service IP / Hostname**: The IP address of the Solutions Integration Service virtual appliance (vApp).
   - **Dell EMC Solutions Integration Service Password**: The Solutions Integration Service administrator password.
   - **Existing SIS User** (checkbox): Select to enable login without reentering your Solutions Integration Service password.
   - **Confirm Solutions Integration Service Password**: (First-time login only) Retype your Solutions Integration Service password.
   - **vCenter IP(s) / Hostnames(s)**: Select the appropriate IP address if vCenter is configured with more than one IP address.
   - **vCenter Password**: The password for the specified vCenter User Name.

   Values for the following parameters are automatically provided and cannot be changed:
   - **EMC Solutions Integration Service User Name**: Determined by the system.
   - **vCenter IP(s)/Hostname(s)**: The IP address(es) of the vCenter or linked vCenters.
   - **vCenter User Name**: The username that you used to log in to the vCenter. This can be different from your login username.
5. Click **OK**.

Results

The Dell EMC Solutions Integration Service is registered and you can now register storage systems. See Registering and removing storage systems on page 50.

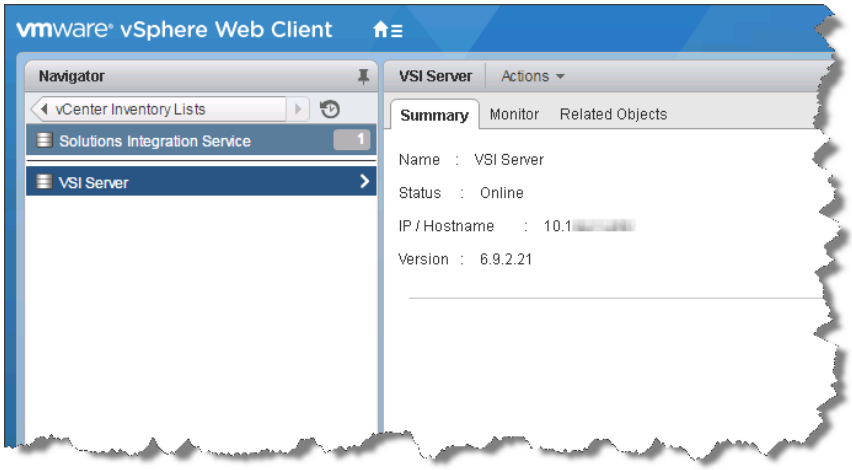
Viewing Solutions Integration Service details

Learn how to find details about the Solutions Integration Service (SIS).

Procedure

1. Select **Home** > **vCenter** > **Dell EMC VSI** > **Solutions Integration Service.**
2. Click **VSI Server** to view the name, status, version and IP address of the Solutions Integration Service, as shown below.

Figure 6 Viewing VSI server Summary information



Status definitions are:

- **Online**: The Solutions Integration Service is connected and functional.
- **Unreachable**: The Solutions Integration Service is unreachable or shut down.
- **Unable to Login**: The Solutions Integration Service is not connected. Do one of the following:
  - Unregister and then register the Solutions Integration Service.
  - Select **Rescan** under the **Actions** menu for the Solutions Integration Service to activate it.

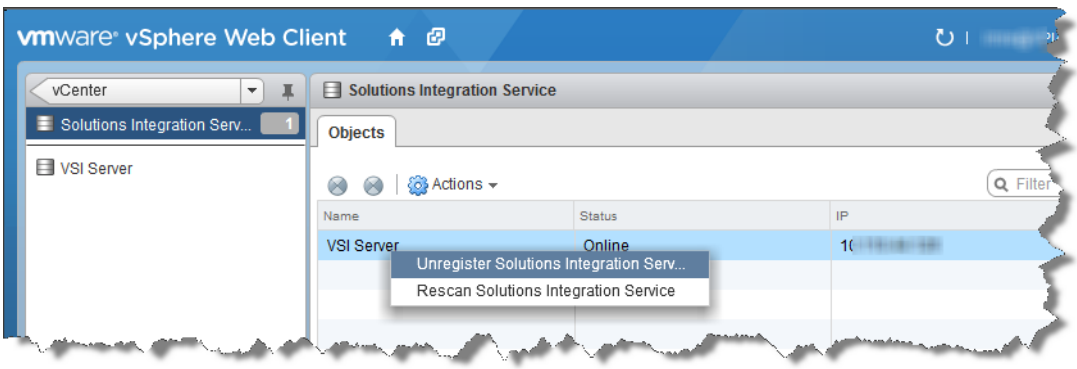
Unregistering or refreshing the Solutions Integration Service

You can register only one Solutions Integration Service. To upgrade VSI or use a different server, you must unregister the current service. If the service is registered but the summary indicates `Unable to log in`, refresh the window to activate it.

Procedure

1. Select **Home** > **vCenter** > **Dell EMC VSI** > **Solutions Integration Service.**
2. Under **Actions** select **Unregister Dell EMC Solutions Integration Service**, as shown below.

Figure 7 Unregistering or refreshing the Solutions Integration Service



- Select **Unregister Solutions Integration Service** to disable communication with the Solutions Integration Service.
- Select **Rescan Solutions Integration Service** to refresh the Solutions Integration Service window.

Logging in to the Solutions Integration Service

Learn how to log in to the Solutions Integration Service using the default password and how to change the password.

Note

The first time you log in to the Solutions Integration Service, you must change your password. After the Solutions Integration Service password is changed, it cannot be modified. If the password is lost, you must redeploy the Solutions Integration Service and use the default login ID and password to log in.

Procedure

1. In your web browser, type the following IP address: `https://<Solutions_Integration_Service_IP_Address>:8443/vsi_usm`

   For example: `https://10.110.44.126:8443/vsi_usm`

2. Click **Administration**.
3. For the login ID type **`admin`** and for the password type **`ChangeMe`**.
4. Type a new password, and then click **Change**.

   Ensure that you save your new password in a secure location.

   The password change confirmation message appears with the following information:

   - **Version Number**: The version of the Solutions Integration Service
   - **Installation Timestamp**: The time at which the Solutions Integration Service was deployed
   - **Local Timestamp**: The current time on the Solutions Integration Service

Solutions Integration Service functions

Learn about the functions that you can perform as *Administrator* and as *Storage Administrator*.

- Logging in to the Solutions Integration Service with *administrator* credentials enables the features described in **Administrator functions** and in Managing administrator tasks on page 27.
- Logging in with *storage administrator* credentials enables you to manage storage systems, as described in **Storage administrator functions** and in Managing storage administrator tasks on page 39.

Table 3 Administrator functions

Menu item	Function	Reference
Home	Displays version and timestamp information.	
Log	Displays Solutions Integration Service log files.	Viewing log files on page 27
VSI Setup	• Provides fields for entering the information needed to register the VSI plug-in. • Provides VDI proxy setup functions.	• Registering the VSI plug-in on page 17 • Installing the VDI web service proxy on page 32
Database	Provides the functionality to view, create, and restore a database backup and to migrate the database when you are upgrading to a new version of VSI.	Maintaining the Solutions Integration Service database on page 29
User	Enables you to add or delete storage administrators and users and view vCenters to which users have access.	Managing users on page 30
Connection Broker	Enables you to add connection brokers for VDI servers.	Installing the VDI web service proxy on page 32
Data Protection	Enables you to add or modify data protection systems.	Managing data protection on page 35
SSH Key	Enables you to add, view, delete, or update Host Public Keys.	Managing Host SSH keys on page 39
Log Out	Logs you out of the **Solutions Integration Service Administration** window.	

The following table lists the features that are available to storage administrators.

Table 4 Storage administrator functions

Menu item	Function	Reference
Home	Displays version and timestamp information.	
Log	Displays Solutions Integration Service log files.	Viewing log files on page 27
vCenter	Displays the vCenters available to the current logged-in user.	Viewing vCenters for storage administrators on page 40
Schedules	Enables you to view and optionally delete active schedules.	Managing schedules on page 40

Table 4 Storage administrator functions (continued)

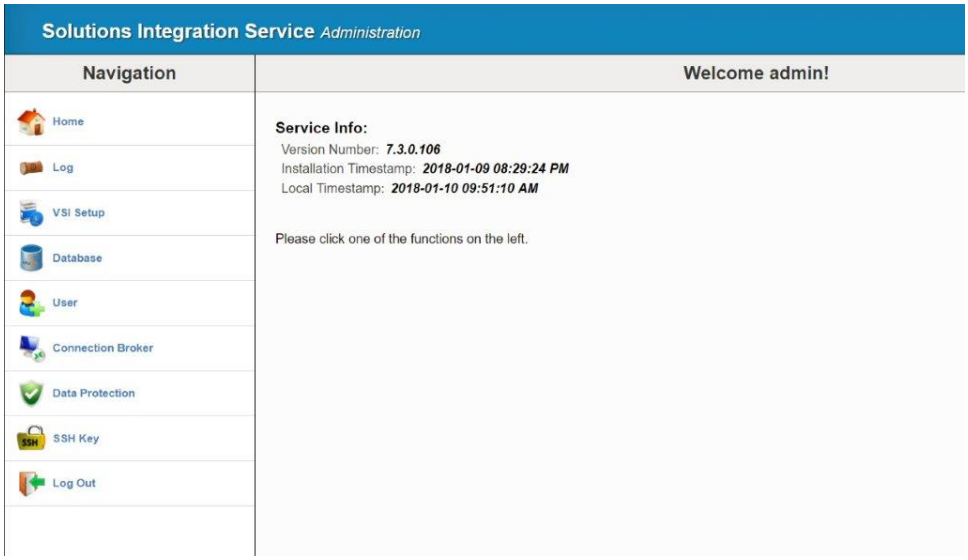
Menu item	Function	Reference
Storage Access	Enables you to view active storage system information, add storage systems, and manage storage systems that you own.	Managing storage access on page 40
Storage Settings	Enables you to add or modify VNX storage system models.	Managing VNX storage settings on page 47
Log Out	Logs you out of the **Solutions Integration Service Administration** window.	

Managing administrator tasks

Learn which tasks you can perform when logged in as *Administrator*.

Log in to the Solutions Integration Service with administrator credentials to access the features shown below.

Figure 8 Solutions Integration Service Administration: Home screen



Viewing log files

The Solutions Integration Service log files provide activity and configuration information about the Solutions Integration Service database that can help troubleshoot or restore settings after a failure event.

Procedure

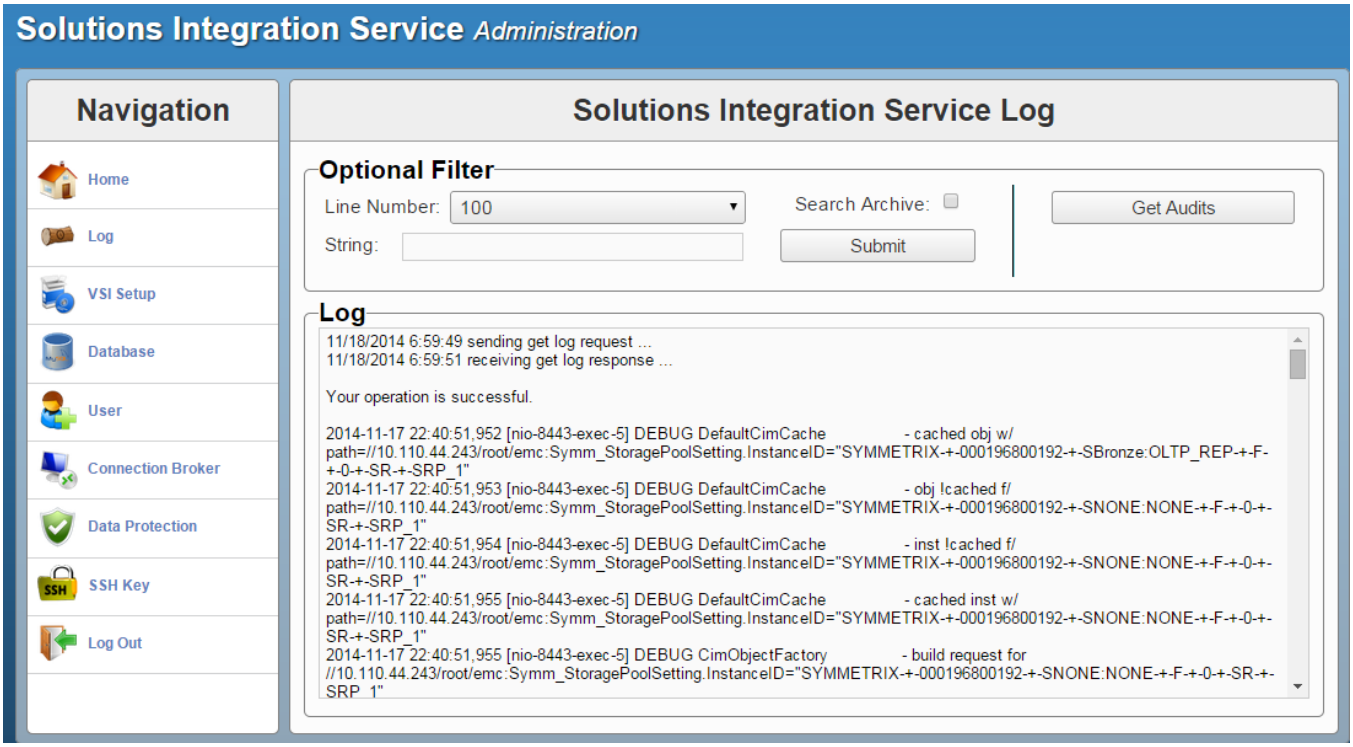
1. From the **Solutions Integration Service Administration** window, click **Log** to display Solutions Integration Service log files.
2. Select any of the following **Optional Filters**:
   - **Line Number**: Specifies the number of lines that you want to display.
   - **String**: Specifies information that you want to find.

- **Search Archive**: Searches all previous logs.
- **Change Log Level**: Changes the type of information to be captured in the log file (for example, which parameters to save in the controller logs, service logs, domain class logs, grails logs, and third party logs.) You must have administrator credentials to change the log level.

3. Click **Submit**.

   The log files are displayed, as shown below.

Figure 9 Viewing the Solution Integration Service Log



Viewing audit logs

Audit logs provide information about important changes to the Storage Information System, including user creation and deletion, storage assignments, and parameter changes.

Procedure

1. In the **Solutions Integration Service Log** window, click **Get Audits**.
2. In the **Audit Table** window, click **Refresh**.

   The **Audit Table** lists the following information for each log file:

   - **Name**: The name of the action taken
   - **Owner**: The module the action affected
   - **Description**: A description of the action
   - **Timestamp**: The time the action took place
3. Click **Cancel** to return to the **Solutions Integration Service Log** window.

Maintaining the Solutions Integration Service database

The Solutions Integration Service database resides on the Solutions Integration Service vApp and contains active configurations, system information, and user setup information.

The Solutions Integration Service has a backup mechanism to protect the system from data loss or data corruption. For example, if a storage administrator accidentally deletes or incorrectly modifies the configuration data, the Solutions Integration Service administrator can restore it from a safe backup.

You can use the Database feature to view a list of available database backups, create new database backups, restore the database from an available backup, and migrate the database when upgrading to a new version of VSI.

Procedure

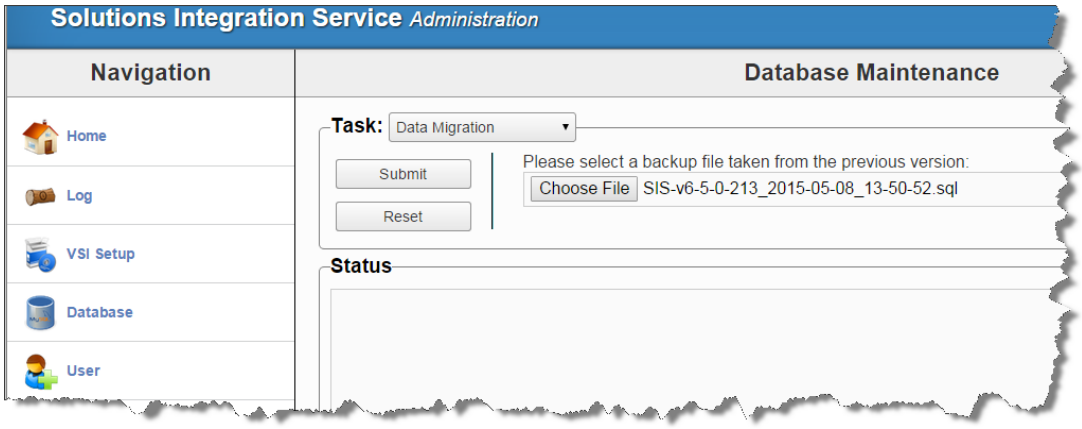
1. Log in to the Solutions Integration Service with system administrator credentials.
2. Click **Database**.
3. Select one of the following operations:
   - **Do nothing**: No action will be taken.
   - **View Backup Files**: Shows a list of backups that were created.
   - **Take Backup**: Creates a backup of the Solutions Integration Service database and saves it to a local system location, for example, your `Downloads` folder.
   - **Restore from Backup**: Restores the database from the local copy on your computer.

     To choose the file to restore, click **Choose File** and navigate to the backup file you want to use. Backup files have the following naming format:

     `hercules_db_backup_v1-0-0-52_2013-08-08_15-16-17.sql`
   - **Data Migration**: Migrates the database from a previous version of the Solutions Integration Service to the currently deployed version. Click **Choose File** to locate the backup database file for the previous version.
4. Click **Submit**.

   The following figure shows a Data Migration example.

Figure 10 Migrating database files from a previous version of the Solutions Integration Service



Managing users

Learn about adding users and managing users' access to storage.

The Solutions Integration Service administrator can use the Users feature to add or delete storage administrators and users. The storage administrator can grant or deny storage system access to this list of users, and control their access to specific types of storage within those storage systems. Managing storage access on page 40 provides more information about the storage administrator's role.

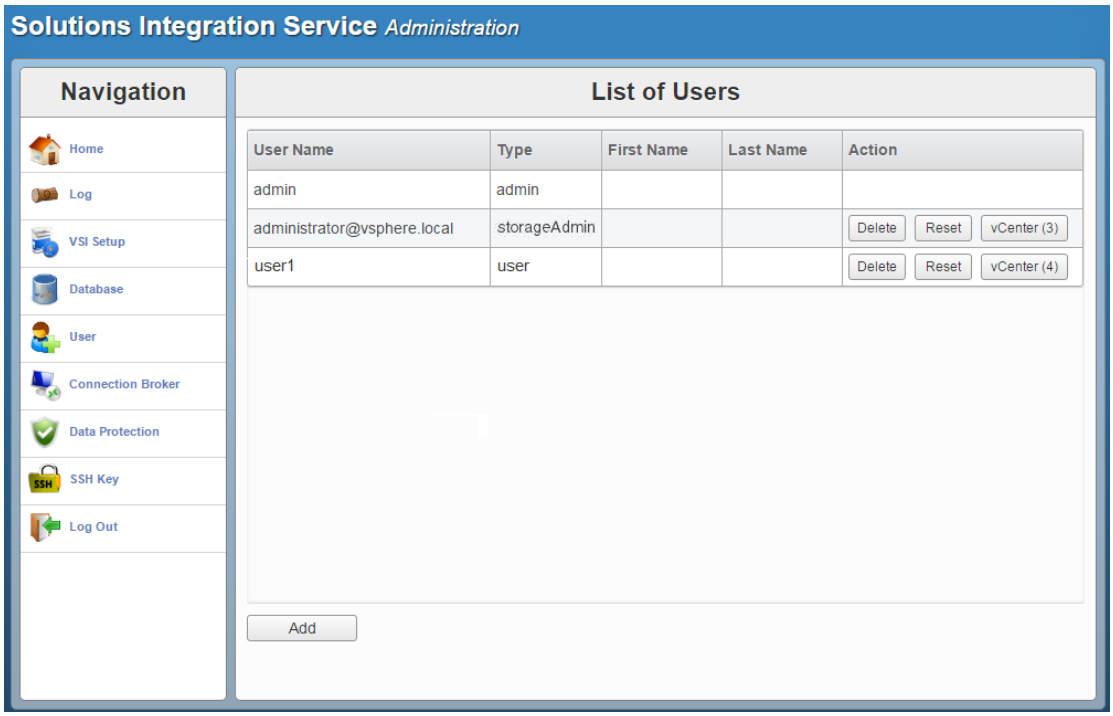
Adding a new user or storage administrator

The *Administrator* role can add users and storage administrators using the Solutions Integration Service.

Procedure

1. Log in to the Solutions Integration Service with system administrator credentials.
2. Click **Users**.
3. The table displays all existing users, as shown below.

Figure 11 Viewing the Solutions Integration Service List of Users



4. Click **Add**.
5. From the **User Type** list box, select **User** or **Storage Admin**.
6. Type the values for the following parameters:
   - **User Name**
   - **First Name**
   - **Last Name**
   - **User Password**
   - **Confirm Password**
7. Click **Save**.
8. Click **OK**.

Viewing vCenters for a user

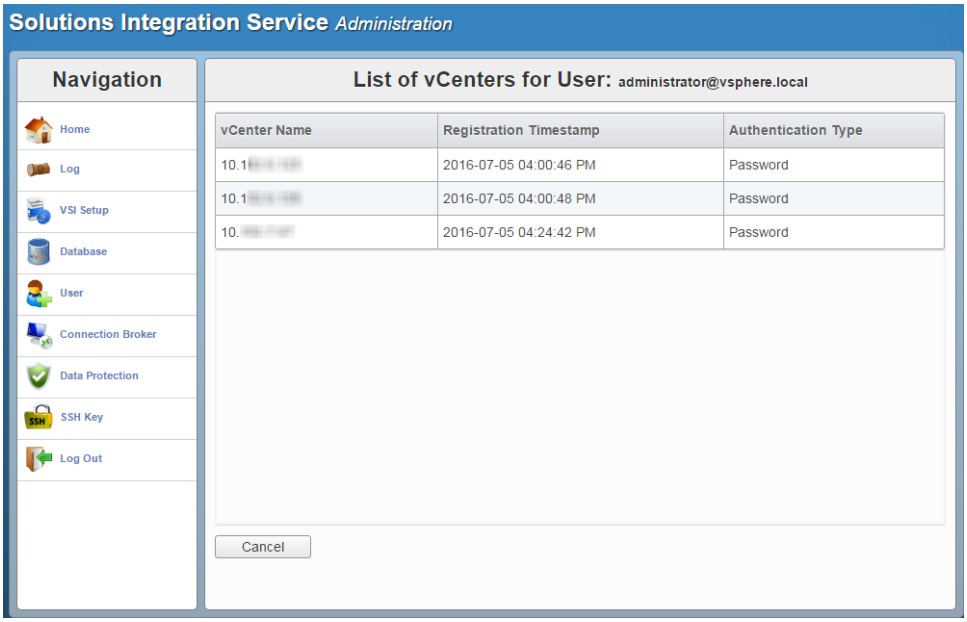
The Solutions Integration Service administrator can view the vCenters that are accessible to each user.

Procedure

1. Log in to the Solutions Integration Service with system administrator credentials.
2. Click **Users**.
3. In the **List of Users** table, click the **vCenter** button next to a user.

   The **List of vCenters for User** table appears, as shown below.

Figure 12 Viewing vCenters for a user



Deleting a user or storage administrator

The *Administrator* role can delete users and storage administrators from the Solutions Integration System.

Note

Before deleting storage administrators, ensure that they have deleted all the storage systems they own. These storage systems can not be managed from the Solutions Integrations Service after the storage administrator is deleted.

Procedure

1. Log in to the Solutions Integration Service with system administrator credentials.
2. Click **Users**.

   The **List of Users** window is displayed.
3. Next to the user that you want to delete, click **Delete**.
4. Click **OK**.

Installing the VDI web service proxy

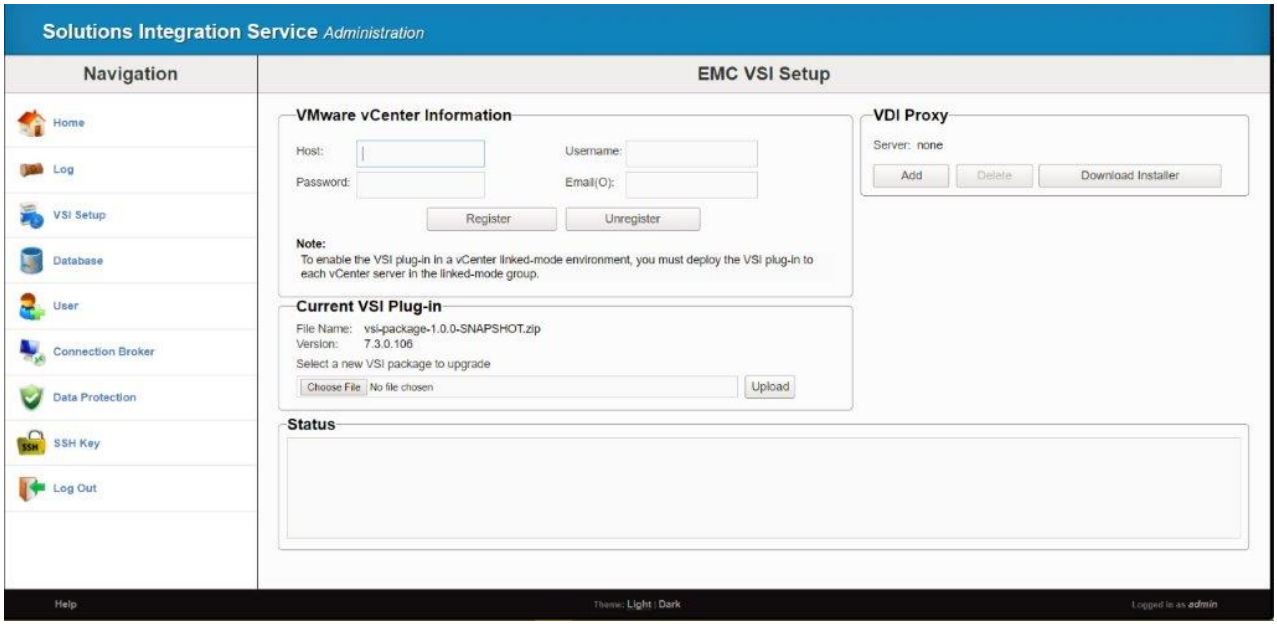
The VDI proxy application enables the provisioning of connection brokers by Solution Integration Service administrators using the Connection Broker feature or by storage users using the VSI Web Client.

Procedure

1. Log in to the Solutions Integration Service with system administrator credentials.
2. Click **VSI Setup**.

   The following figure shows the **Dell EMC VSI Setup** window.

Figure 13 Dell EMC VSI Setup window



3. Under **VDI Proxy**, click **Download Installer** to download the `EmcVdiWebApi.zip` file.
4. Ensure that the web server meets the following requirements:
   - Windows 2012 or later is installed.
   - Internet Information Services (IIS) 8 with all features is installed.
   - Microsoft Web Deploy 3.5 is installed.
   - The web server is connected to the server running VMware Horizon View or Citrix XenDesktop.
5. Install the file as a new web service:
   a. Copy the Zip file to the destination web server.
   b. From the IIS manager, click **Sites** > **Default Web Site**.
   c. Delete any existing site named emcvdi.
   d. Right-click **Default Web Site** and select **Deploy** > **Import Application**.
   e. Click **Browse** to select the Zip file you copied in step a.
   f. Continue with the wizard, accepting the default settings and clicking **Next**.
   g. Select **Yes, ...** to overwrite existing files.
   h. Click **Finish**.
6. Set up the VDI Proxy:
   a. Under VDI Proxy, click **Add**.
   b. Type host name or IP address for the VDI Proxy server.
   c. Click **Save** to test the connection and save the settings.

After you finish

Note

To add a connection broker, the user must have full permission on the IIS web service. To edit permissions, right-click the IIS web service, click **Edit Permissions**, and select **Security**.

Deleting the VDI proxy settings

All users lose the ability to provision new clones to the broker from VSI Web Client.

Procedure

1. Log in to the Solutions Integration Service with system administrator credentials.
2. Click **VSI Setup**.
3. Under **VDI Proxy**, click **Delete**.

Managing connection brokers

The Connection Broker feature enables Solutions Integration Service administrators to integrate XtremIO virtual machines with VDIs like VMware Horizon View and Citrix XenDesktop.

Note

For Citrix XenDesktop, add XenDesktop to your trusted hosts list on the VDI proxy server before you register it in VSI or in the Solutions Integration Service, otherwise the registration fails. Use the following command:

```
Set-Item wsman:localhost\\client\\trustedhosts -value * -force
```

Setting up VDI connection brokers

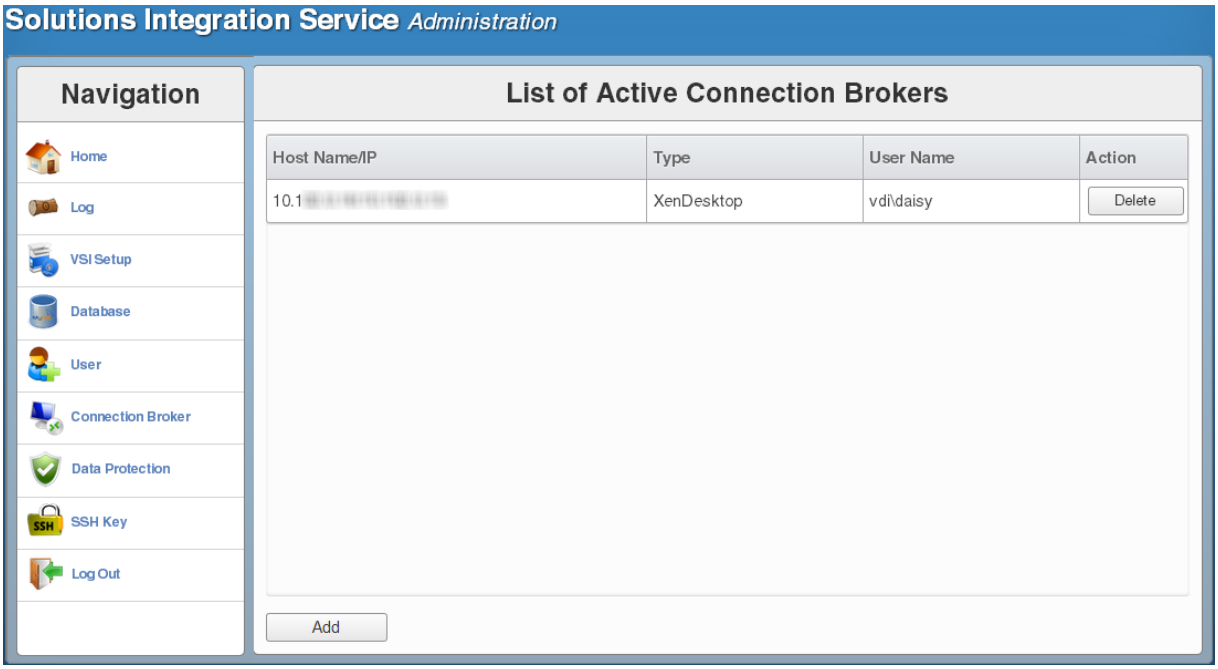
Learn to set up a VDI connection broker for Citrix XenDesktop or VMware Horizon View.

Procedure

1. Log in to the Solutions Integration Service with system administrator credentials.
2. Click **Connection Broker**.

   The following figure shows the **List of Active Connection Brokers** window.

Figure 14 List of Active Connection Brokers window



When connection brokers are defined, the **List of Active Connection Brokers** window provides the following functions:

- **Delete**—Delete the associated connection broker.
- **Add**—Add a new connection broker.

Adding a connection broker

Learn how to add a VMware View Manager or Citrix XenDesktop Manager connection broker.

Procedure

1. In the **List of Active Connection Brokers** window, click **Add**.
2. In the **Create a Connection Broker** window, provide the following information for the new connection broker:
   - **Broker Type**: **VMware View Manager** or **Citrix XenDesktop Manager**
   - **Host Name/IP**
   - **User Name**
   - **User Password**
   - **Confirm Password**
   - For XenDesktop: **vCenter name** or **IP address**.
3. Click **Save** to test the connection and save the settings.

Managing data protection

The Data Protection feature enables the system administrator to add or modify the following data protection systems:

- AppSync—Used to administer service plans and datastore copies directly from the vSphere Client and to assign an AppSync system to a user

- RecoverPoint—Used to administer protection groups and consistency groups from the vSphere Client and to assign a RecoverPoint system to a user.

Viewing data protection systems

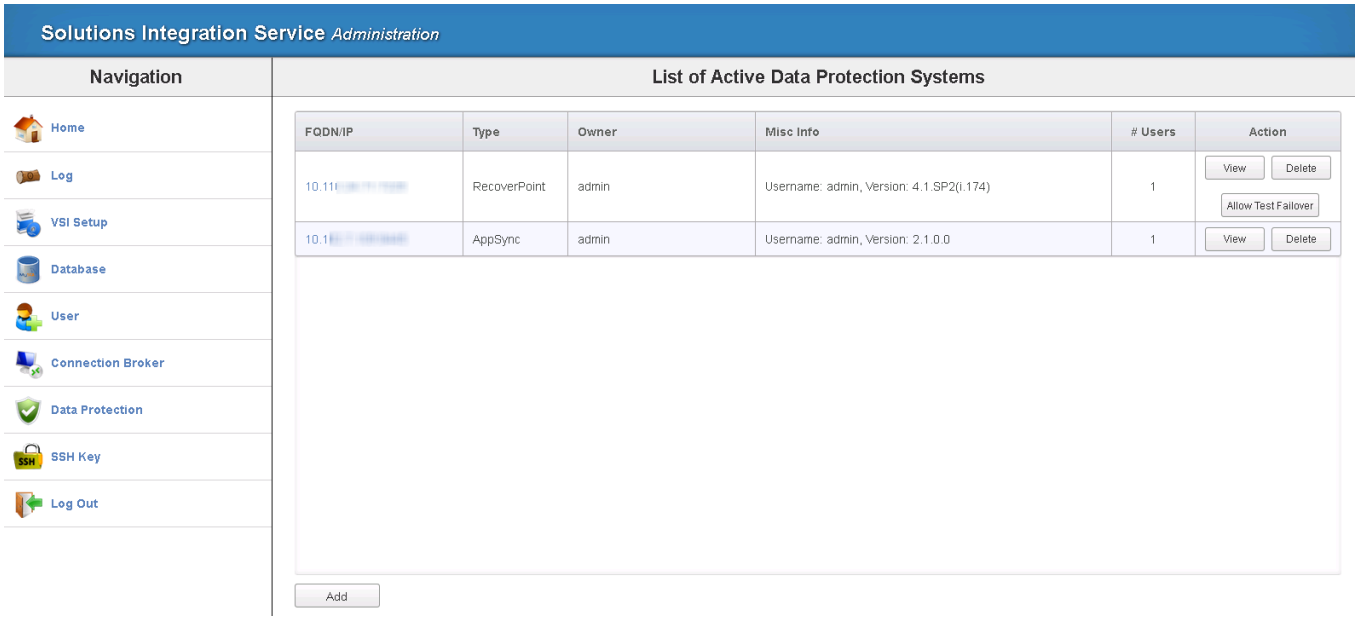
Learn what you can do with data protection systems that you own.

Procedure

1. Log in to the Solutions Integration Service with system administrator credentials.
2. Click **Data Protection**.

   All registered data protections systems are listed, as shown below.

   Figure 15 Viewing active data protection systems



3. You can perform the following actions for the data protection systems that you own:
   - **View**: View data protection system details and manage access for users. Refer to Managing data protection access on page 36 in the next section.
   - **Delete**: Unregister a data protection system. Refer to Unregistering a data protection system on page 38.
   - **Allow Test Failover**: Allow test failover on EMC RecoverPoint systems. Refer to Allowing test failover on RecoverPoint systems on page 38.
   - **Add**: Register a data protection system Refer to Registering a data protection system on page 38.

Managing data protection access

Learn how to enable users to access data protection.

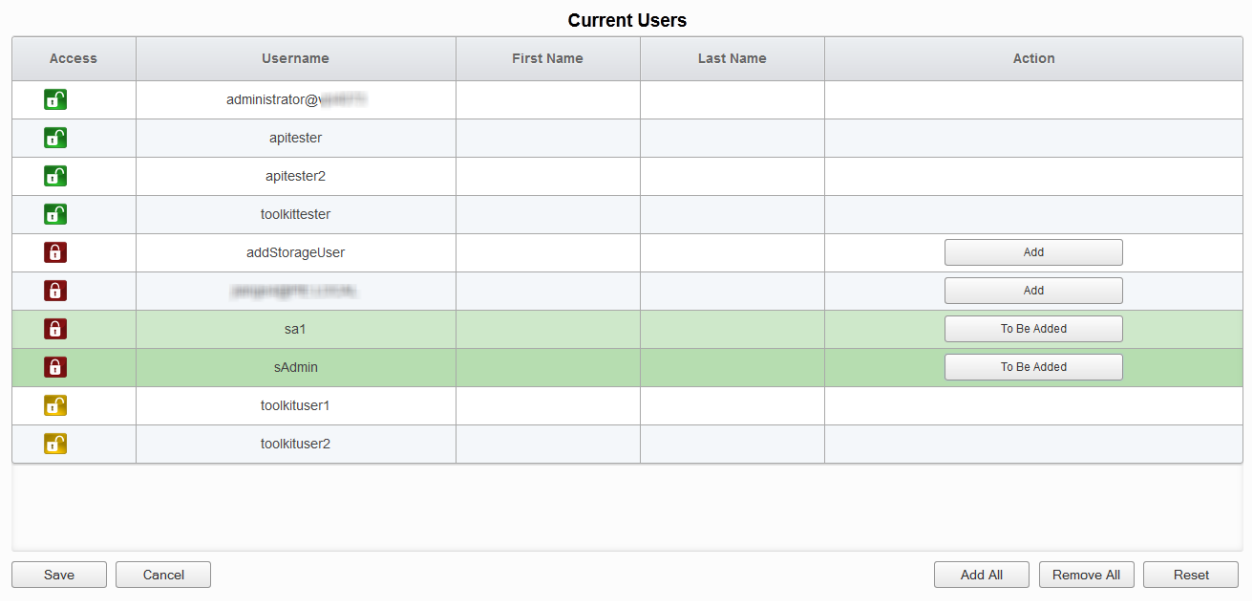
Procedure

1. Log in to the Solutions Integration Service with system administrator credentials.

2. Click **Data Protection**.
3. Click **View** in the record of the system for which you want to grant or remove access for users.

   The current users are listed, as shown below.

   Figure 16 Managing data protection system access



   The icons in the **Access** column are defined as follows:

   - Green—The user already has access to the selected data protection system and the Remove button is available to remove user access.

     Note

     If the user is a system administrator, the **Remove** button is unavailable and access cannot be removed.

   - Red—The user does not have access to any data protection system of the same type and the **Add** button is available to grant user access.
   - Yellow—The user has access to another AppSync data protection system. The **Add** button is not available because a normal user can have access to only one AppSync system.

4. In the **Current Users** table, do one of the following:
   - Click **Add** in the row for each user for whom you want to grant access.
   - Click **Add All** to add all listed users who do not currently have access.
   - Click **Remove** in the row for each user for whom you want to remove access.
   - Click **Remove All** to remove all current users who do not own the system.
   - Click **Reset** to abandon your changes.
5. Click **Save**.
6. Click **OK** in the confirmation dialog box.

Registering a data protection system

To use a data protection system, you must first register it.

Procedure

1. Log in to the Solutions Integration Service with system administrator credentials.
2. Click **Data Protection**.
3. In the **List of Active Data Protection Systems** window, click **Add**.
4. Provide the values for the following parameters:
   - **Data Protection Type**: AppSync or RecoverPoint
   - **FQDN/IP**: The fully qualified domain name (FQDN) or IP address of the data protection server.

     Note

     The FQDN or IP address must be accessible from the Solutions Integration Service server or the connection will fail.
   - **Port**: 8445 is the default port for AppSync; 7225 is the default port for RecoverPoint.
   - **User Name**: User name required for access to the server.
   - **User Password**: Password required for access to the server.
   - **Confirm Password**: Confirm the password.
5. Click **Save**, and then click **OK** in the confirmation dialog box.

Unregistering a data protection system

You can unregister a data protection system that is no longer needed.

Procedure

1. Log in to the Solutions Integration Service with system administrator credentials.
2. Click **Data Protection**.
3. Click **Delete** next to the system that you want to unregister.
4. Click **OK** to confirm the deletion.

Allowing test failover on RecoverPoint systems

Learn how to set RecoverPoint systems to allow test failover.

Procedure

1. Log in to the Solutions Integration Service with system administrator credentials.
2. Click **Data Protection**.
3. In the **List of Active Data Protection Systems**, click **Allow Test Failover** for the appropriate RecoverPoint system.
4. Click **OK** in each of the confirmation dialog boxes.

Managing Host SSH keys

Using the SSH Key function, the system administrator can view, delete, update, and add host public keys.

Viewing, modifying, or deleting SSH keys

Learn how to manage SSH keys.

Procedure

1. Log in to the Solutions Integration Service with system administrator credentials.
2. Click **SSH Key**.

   The **List of SSH Keys** is displayed.

3. Next to the host name that you want to modify, click the button for the function you want to perform.
   - **View**—View the information and then click **Cancel**.
   - **Update**—Type the new public key, and then click **Save**.
   - **Delete**—Click **OK** to confirm that you want to delete the key.

Adding an SSH key

Administrators can add SSH keys.

Procedure

1. Log in to the Solutions Integration Service with system administrator credentials.
2. Click **SSH Key**.

   The **List of SSH Keys** is displayed.

3. Click **Add**.
4. In the **Add Public Key** dialog box, type the values for the following:
   - **Hostname**
   - **Host IP**
   - **Public Key**
5. Click **Save**.

Managing storage administrator tasks

Learn about the tasks the *Storage Administrator* can perform.

Logging in to the Solutions Integration Service as a storage administrator enables you to perform the tasks listed in Table 4 on page 26. The following sections provide the procedures for each task.

Viewing vCenters for storage administrators

As a storage administrator, you can view the vCenters accessible to you.

Procedure

1. Log in to the Solutions Integration Service as a storage administrator.
2. Click **vCenters**.

Results

The **vCenters for User** table lists the details of the vCenters to which you have access.

Managing schedules

Learn to manage schedules.

Note

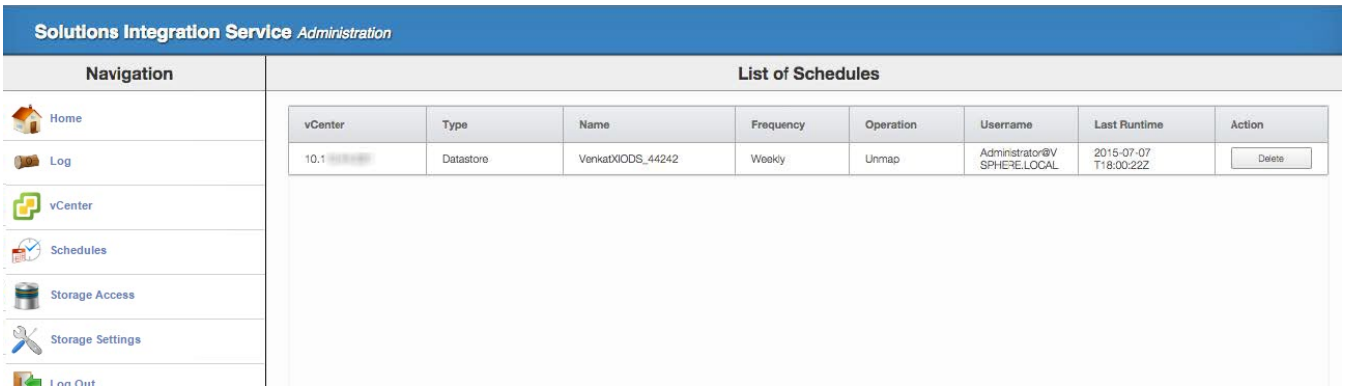
To delete a schedule on XtremIO datastores, the storage administrator must first register the vCenter.

Procedure

1. Log in to the Solutions Integration Service with storage administrator credentials.
2. Click **Schedules**.

   The **List of Schedules** shows all active schedules, as shown below.

   Figure 17 Managing schedules



3. (Optional) To delete a schedule, click **Delete** in the **Action** column, and then click **OK** in the confirmation dialog box.

Managing storage access

Learn about the tasks you can perform in the **Storage Access** window.

Note

vSphere administrators must register at least one storage system on vSphere to be able to manage storage access in the Solutions Integration Service.

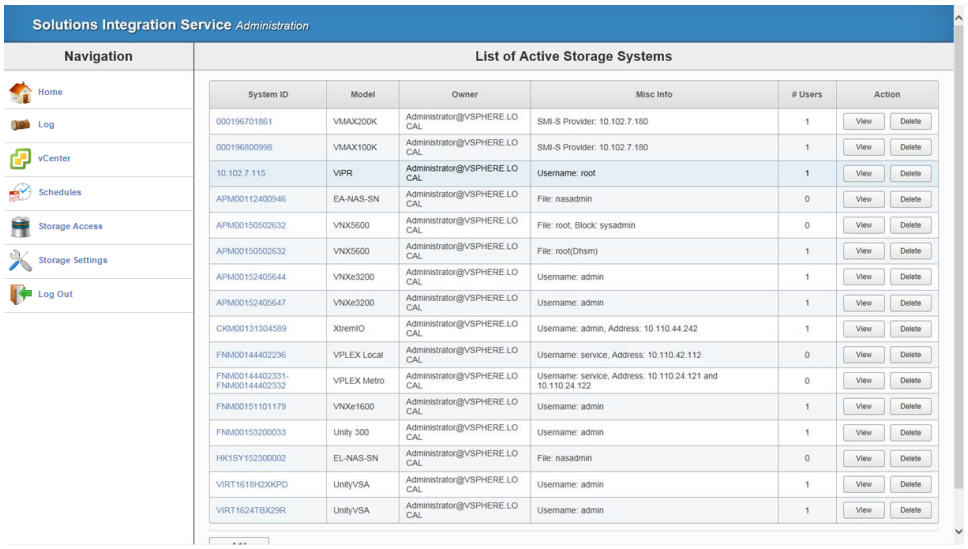
Logging in to the Solutions Integration Service as a storage administrator enables you to perform the following actions:

- On eNAS: Create and delete eNAS storage systems, add and delete users to/from storage systems and storage pools.
- On EMC Unity™ and EMC UnityVSA: Create block and file storage and add or remove users to/from storage pools
- On VNX: Create block and file storage, register DHSM users for compression and cloning on EMC storage systems, add or remove users to/from storage pools, and add or modify VNX storage system models
- On VNXe1600: Create block storage and add or remove users
- On VNXe3200: Create block and file storage and add or remove users to/from storage pools
- On VMAX3 and VMAX All Flash: Create storage arrays and manage user access
- On EMC VPLEX™: Create storage arrays
- On XtremIO: Create and delete storage systems and add and remove users to/from storage systems

To use the Storage Access feature, log in to the Solutions Integration Service with storage administrator credentials and click **Storage Access**.

The **List of Active Storage Systems** is displayed, as shown below.

Figure 18 Storage Access window



Note

Action items appear only for the storage systems that you own.

From the **Storage Access** window, you can view active storage system information, add storage systems, and perform the following actions for the storage systems that you own:

- **View**: View storage system details and manage users.
  For Unity, UnityVSA, VNXe3200, eNAS, VNX, VMAX3, and VMAX All Flash systems, you can manage storage pools for a particular system. Clicking **View** displays the **Storage System Details** page where you can grant or remove individual file or block storage pool access. Granting storage access to users on page 43 provides details.

- **Delete**: Delete a storage system.
- **Add**: Create storage systems. Steps for adding storage systems are provided in the following section.

Adding storage systems

Storage administrators can add the storage systems listed in this section.

- eNAS
- Unity
- UnityVSA
- VMAX3
- VMAX All Flash
- VNX (File and Block)
- VNXe1600
- VNXe3200
- VPLEX
- XtremIO

Creating storage on eNAS, Unity, UnityVSA, VMAX3, VMAX All Flash, VNXe, VPLEX, and XtremIO systems

Use this procedure to create storage on all systems except VNX.

Procedure

1. Log in to the Solutions Integration Service with storage administrator credentials.
2. From the **Storage Access** window, click **Add**.

   The **Create a Storage System** window appears.

3. From **Storage System Type** list select the storage type.
4. Type the credentials for the system.

   For eNAS, the DHSM username and password is required to enable compression and deduplication on a datastore.

5. For VMAX3 and VMAX All Flash arrays only:
   a. Type or select values for the following parameters:
      - **Protocol** (HTTP, HTTPS).
      - **SMI-S Provider Address**
      - **Default Port** (change if necessary).
      - **SMI-S Provider User Name** (username with administrative credentials)
      - **SMI-S Provider Password**
      - **Max device size (GB)**—(Optional; “0” means unlimited device size).

   b. Click **Retrieve Arrays**.
   c. From the list, select an array to be registered.
6. Click **Save**, and then click **OK** in the confirmation dialog box.

Creating storage on VNX arrays

You can create access credentials for block storage, file storage, or both on VNX arrays with the Storage Access feature.

You can grant any user, other than the storage array owner, only one access credential on a VNX array. The credential can be file only, block only, or block plus file. Users who already have access to the array are designated with a yellow check mark  in the **Status** column of the **Current Users** list. To modify the credential, delete the current credential and create a new access credential.

Procedure

1. From the **Storage Access** window, click **Add**.

   The **Create a Storage System** window appears.

2. For **Storage System Type** select **VNX**.
3. To create block storage:
   a. Under **Block (VMFS, RDM) Storage**, select **Register**.
   b. For **Unisphere Scope**, select **Global**, **Local**, or **LDAP**.
   c. Type the values for the following parameters:
      - **Storage Processor IP**
      - **Unisphere User Name**
      - **Unisphere Password**
4. To create file storage:
   a. Under **File (NFS) Storage**, select **Register**.
   b. Type the values for the following parameters:
      - **Control Station IP**
      - **Control Station User Name**
      - **Control Station Password**
5. To register a DHSM username for compression and cloning, select **Register** and type the DHSM user name and password in the text boxes provided.
6. Click **Save**.
7. Click **OK**.

Granting storage access to users

The Storage Access feature enables storage administrators to grant read-only or read/write access to users for storage systems that they own.

When the user logs in to the vSphere Web Client, the changes appear under **EMC VSI** > **Storage Systems**.

Managing users and storage pools

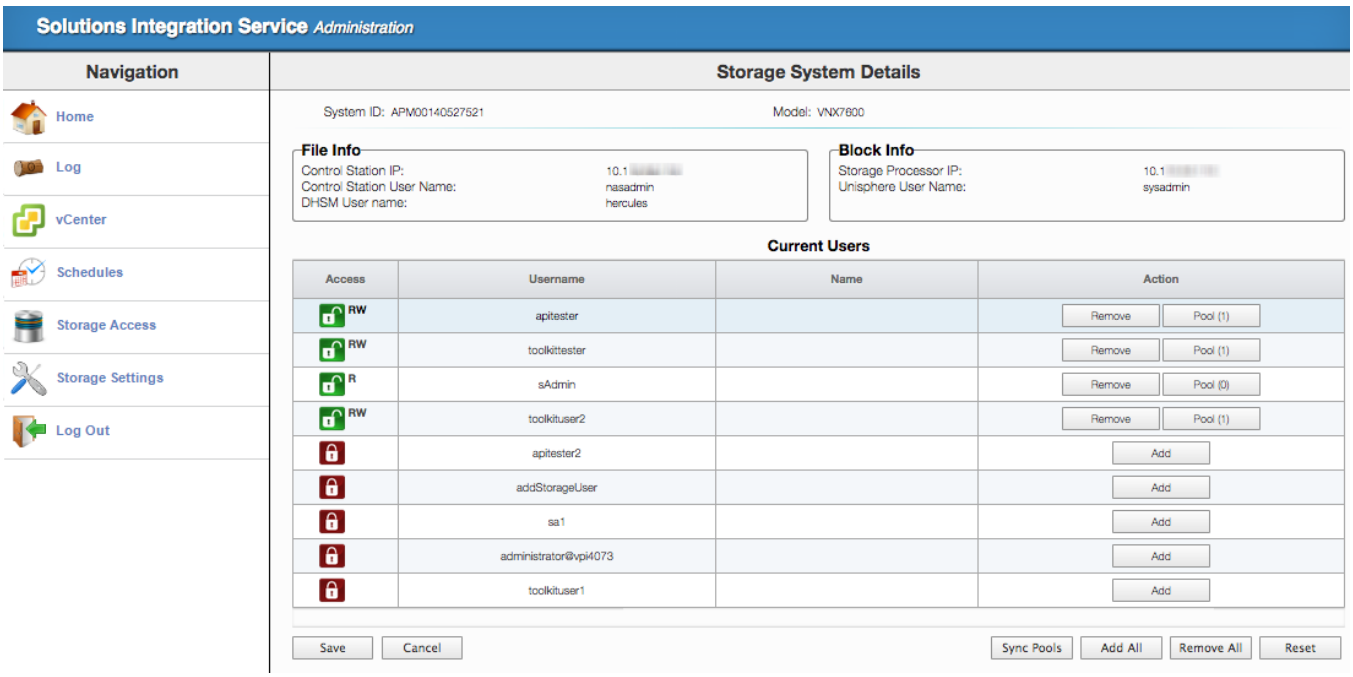
Learn about the actions you can perform using the SIS Storage Access component.

Procedure

1. Log in to the Solutions Integration Service with storage administrator credentials and click **Storage Access.**
2. Click **View** next to the storage system that you want to manage.

   The **Storage System Details** window appears, displaying system information and a list of current users. The following figure shows a sample VNX system.

   Figure 19 Viewing Storage System Details for a VNX system



You can perform the following actions for the storage system:

- Remove access to the storage system: Click **Remove** next to the user name. Click **Remove All** to remove all current users.
- Grant read access: Click **Add** next to the user name. Click **Add All** to grant read-only access to all displayed users.
- Grant write access for eNAS or VNX storage pools: Click **Pool** next to the user name. In the **Storage Pools** list, click **Add** for each pool that you want to assign to that user.

The buttons at the bottom of the window enable you to perform the following actions:

- **Save**—Saves your settings. When the user logs in to the vSphere Web Client, the changes appear in the available storage pool list during provisioning.
- **Cancel**—Returns you to the Storage System Details page without saving any changes.
- **Sync Pools** (eNAS, VNX, Unity, UnityVSA, and VNXe only)—Synchronizes the storage pool changes for the registered storage system. Available GB is updated to reflect the latest usage on the pool.

- **Add All**—Adds all displayed users to the storage system.
- **Remove All**—Removes all displayed users from the storage system.
- **Reset**—Resets all pending storage operations on the storage system to their previous settings.

3. Click **Save**.

Managing VMAX3 and VMAX All Flash maximum device size and user quotas

For VMAX3 and VMAX All Flash storage systems, you can use the **Storage System Details** window to update the maximum device size and to specify the total amount of storage users can provision.

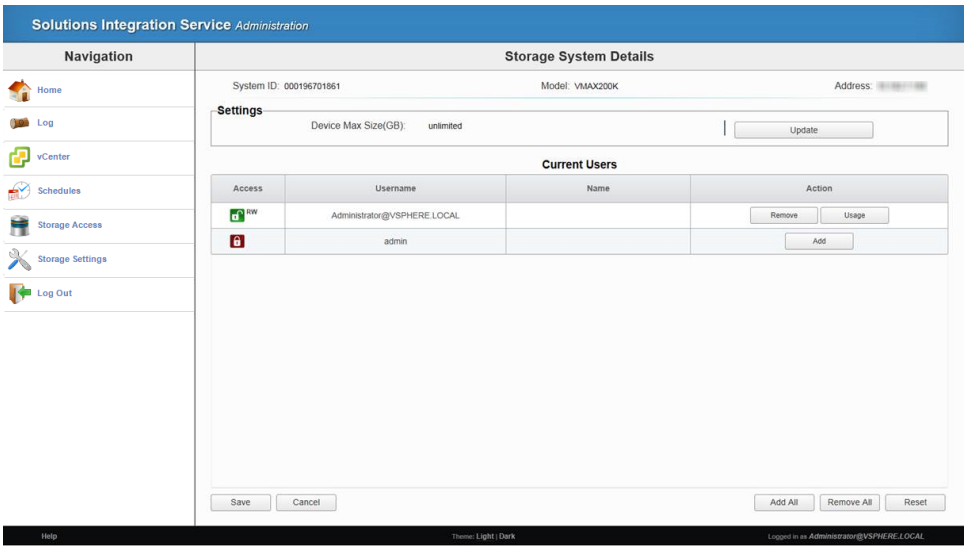
Procedure

1. Log in to the Solutions Integration Service with storage administrator credentials and click **Storage Access.**
2. Click **View** next to the storage system that you want to manage.

   The **Storage System Details** window appears, displaying system information and a list of current users.

   The following figure shows a sample VMAX3/VMAX All Flash system.

   Figure 20 Viewing VMAX3 or VMAX All Flash storage system details



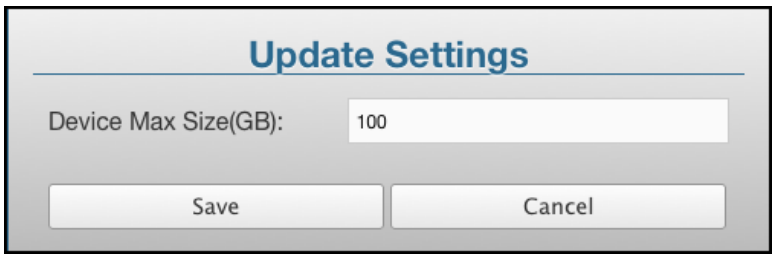
Managing maximum device size

You can change the maximum device size for VMAX3 and VMAX All Flash arrays.

Procedure

1. In the **Settings** box, click **Update**, as shown in Figure 20 on page 45.
2. In the **Update Settings** dialog box, shown below, type the new size, and then click **Save**.

Figure 21 Updating maximum device size.



Results

The maximum device size is updated.

Setting storage provisioning limits

Learn to manage the amount of storage available to users.

The information and functions available on the **Storage System Usage** page are shown in the following figure and described in the following table.

Figure 22 Viewing Storage System Usage

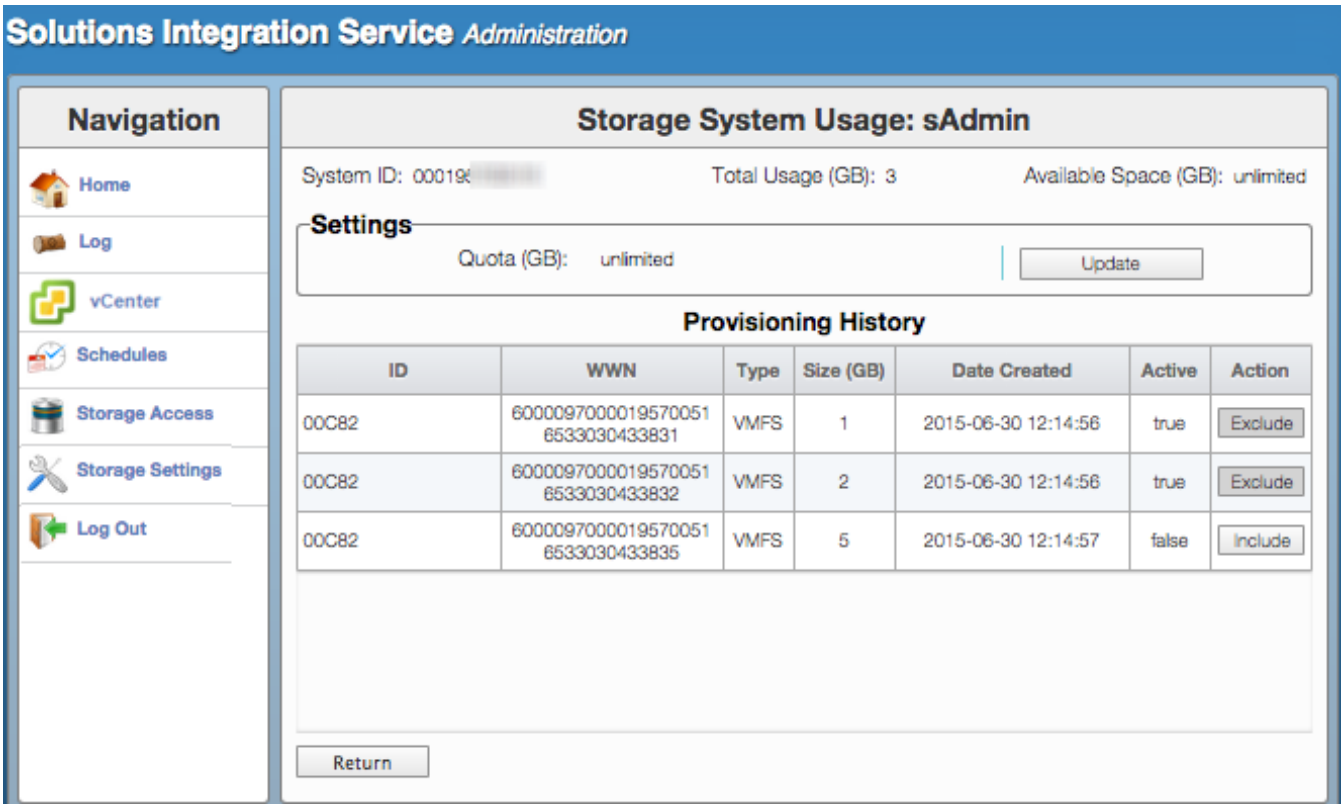


Table 5 Storage System Usage GUI elements

Field	Description
System ID	The system ID of the selected VMAX system.
Total Usage	The amount of space that has been allocated to all users.

Table 5 Storage System Usage GUI elements (continued)

Field	Description
Available Space	The total amount of space available on the array to all users. When this number is zero, no more space can be provisioned on the array.
Quota	The total amount of space the selected user can provision.
Update	Displays the **Update Settings** dialog box to change the user quota. Entering 0 or leaving it blank saves the quota as unlimited (no quota).
Provisioning History	Contains a history of all VMAX storage that was successfully provisioned using the current Solutions Integration Service. Device sizes include total usage. Any provisioning that was done either before VSI version 6.6 or outside of VSI are not tracked here. For example, if a storage administrator deletes a LUN directly from the VMAX storage array, the history of that LUN is still visible here.
Action column	Exclude/Include—Includes or excludes the **Provisioning History** entry. **Note** Normally, the history does not need to be modified, but the storage administrator can use the Exclude or Include button to modify the entry for the purpose of calculating total usage. Once a history is excluded, its device size will not be counted towards the user's total usage. Note that this operation does not make any change to the actual storage LUNs.

Procedure

1. Open the **Storage System Details** page, as shown in Figure 20 on page 45.
2. In the **Current Users** list, click **Usage** next to the user name that you want to modify.
3. In the **Settings** box, click **Update**.
4. In the **Update Settings** dialog box, type a number for **User Quota**, and then click **Save**.

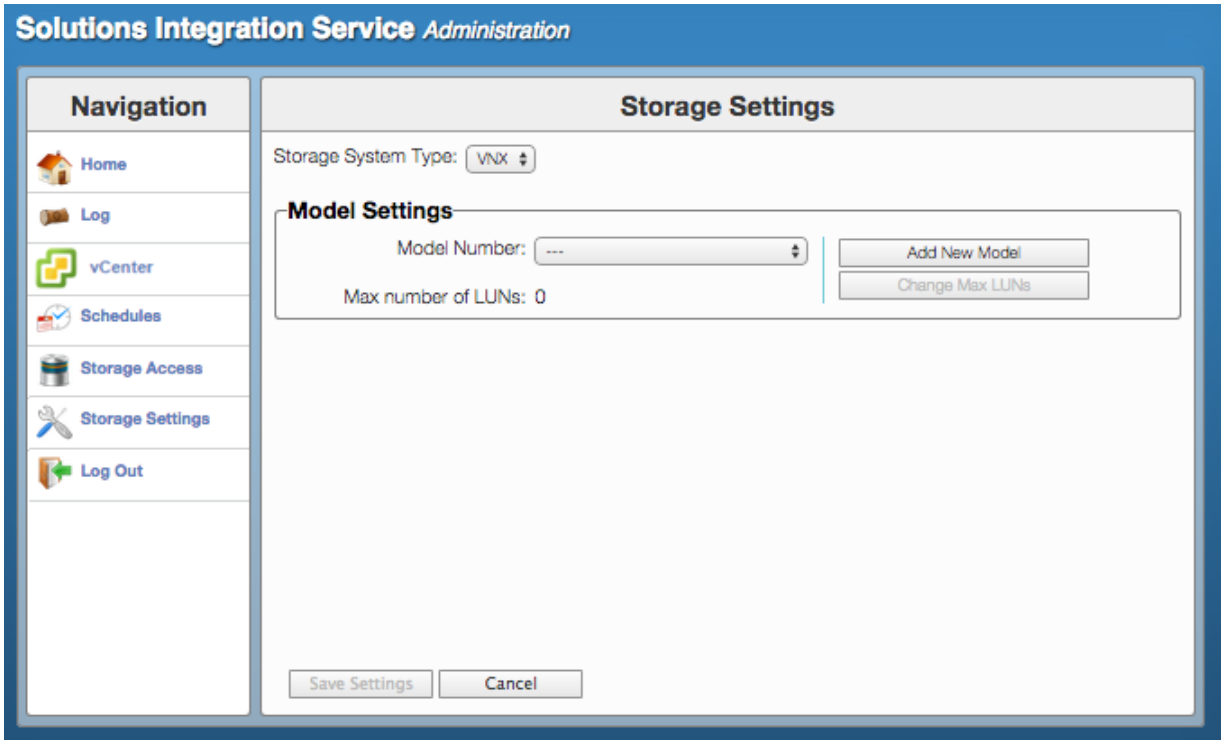
   The quota for that user is updated.

Managing VNX storage settings

The Storage Settings feature enables storage administrators to add or modify storage system settings and set up the maximum number of LUNs for a specific VNX model.

To use the Storage Setting feature, log on to the Solutions Integration Service with storage administrator credentials. The **Storage Settings** window is shown below.

Figure 23 Storage Settings window



Adding a new VNX model

Procedure

1. Click **Add new Model**.
2. Enter the model number and the maximum number of LUNs in the appropriate text boxes.
3. Click **Save Settings**.

Changing the maximum number of LUNs

Procedure

1. Select the VNX model from the **Model Number** list.
2. Click **Change Max LUNs**.
3. In the **Max number of LUNs** text box, type the maximum number of LUNS supported by the storage system.

CHAPTER 4

Using VSI to View and Manage Storage

This chapter includes the following topics:

Registering and removing storage systems

After enabling the Solutions Integration Service, the storage systems that you want to view and manage with VSI must be registered. If the storage systems were not registered and assigned to you by the Solutions Integration Services storage administrator, you can use the procedures in the following sections to register Unity, UnityVSA, VMAX3, VMAX All Flash, VNX, VNXe, VPLEX, XtremIO, and eNAS storage systems.

Registering storage systems

Use this procedure to register Unity, UnityVSA, VMAX3, VMAX All Flash, VNXe1600, VNXe3200, VPLEX, XtremIO, and eNAS storage.

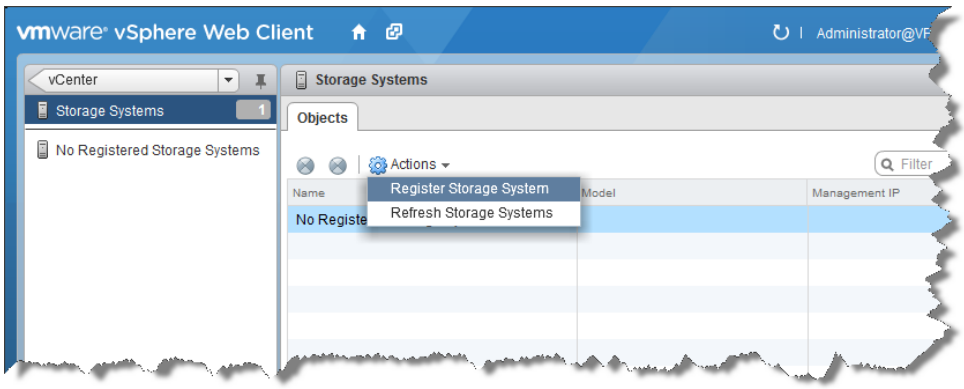
Procedure

1. Select **Home** > **vCenter Inventory Lists** > **EMC VSI** > **Storage Systems**.

   The list shows the storage systems that are accessible from the Solutions Integration Service.

2. Select **Actions** > **Register Storage Systems, as shown in** the following figure.

   Figure 24 Registering a storage system



3. In the **Register EMC Storage System** window, for **Storage System type**, select the storage system type to register.

   The GUI displays the required parameters for the storage type.

4. Complete one of the following options:

   - To register Unity, UnityVSA, VNXe1600, VNXe3200, VPLEX, and XtremIO storage types, in the designated text boxes, type the name or IP address of the storage system, account username, and account password and click **OK**.
   - To register eNAS storage, specify the **Control Station IP**, **Control Station username**, and **Control Station Password**. To use LDAP authentication, type the username in this format: *username@domain_name*. Type the **DHSM Username** and **DHSM Password**, if required.
   - To register VMAX3 or VMAX All Flash storage types complete step 5.

5. For VMAX or VMAX All Flash only:

a. Select the protocol (HTTP, HTTPS) from the drop-down menu, type the SMI-S Provider IP address, and change the default port if required (optional).

b. Type the username and password of the SMI-S provider.

c. Enter a number (in GB) for the maximum device size. A blank or 0 value means that there is no maximum device size, therefore, it is unlimited.

d. Click **Retrieve** > **Arrays.** All VMAX3 and VMAX All Flash storage arrays that are connected to the SMI-S provider are listed.

e. Select the array that you want to add and click **OK**.

Results

A confirmation dialog box appears, indicating the owner of the storage system, that is, the user who first registered it. The owner controls the storage system credentials. Registering the storage system can take several minutes. When the registration is complete, the system appears in the storage list.

Registering VNX storage

You can register a VNX storage system as block, file, or both block and file.

Note

If both block and file credentials are specified, both credentials must point to the same VNX (with the same serial number). If the block and file credentials are valid but do not point to the same VNX system, you cannot register for both block and file.

Procedure

1. Select **Home** > **vCenter Inventory Lists** > **EMC VSI** > **Storage Systems.**

   The list shows the storage systems that are accessible from the Solutions Integration Service.

2. Select **Actions** > **Register Storage Systems**.
3. In the **Register EMC Storage System** window, for **Storage System type**, select the storage system type to register.

   The GUI displays the required parameters for the storage type.

4. To register as Block storage, specify the following parameters:

   a. Select **Register as block (VMFS, RDM) storage**.

   b. Type the storage processor IP address, VNX block username, VNX block password.

   c. Select a scope (Global, Local, or LDAP) for VNX block access.

      To use LDAP authentication, type the username and select LDAP from the list box. Do not type the domain name as part of the username.

5. To register as File storage, specify the following parameters:

   a. Select **Register as file (NFS) storage**.

   b. Specify the **Control Station IP**, **VNX Control Station username**, and **Control Station Password**.

To use LDAP authentication, type the username in this format: <username>@<domain_name>

c. Select **Register file access to compression and cloning**.

d. Type the DHSM username and DHSM password in the designated boxes.

6. Click **OK**.

Results

A confirmation dialog box appears, indicating the owner of the storage system, that is, the user who first registered it. The owner controls the storage system credentials. Registering the storage system can take several minutes. When the registration is complete, the system appears in the storage list.

Unregistering a storage system

You can unregister storage systems that are no longer needed.

Procedure

1. Select **Home** > **vCenter Inventory Lists** > **EMC VSI** > **Storage Systems**.
2. Select the array that you want to unregister.
3. Select **Actions** > **Unregister Storage System**.

Viewing storage systems and storage system objects

You can view the properties for storage systems and storage objects, including datastores, virtual machines, and RDM disks.

Viewing system properties

You can view properties for registered storage systems.

Procedure

1. Select **Home** > **vCenter Inventory Lists** > **EMC VSI** > **Storage Systems**.
2. Select a storage system from the inventory list.

   The **Summary** tab displays the fully qualified domain name, model, management IP address, and other information about the storage system.

Viewing host properties

You can view consolidated datastore information on a host for registered storage systems.

Procedure

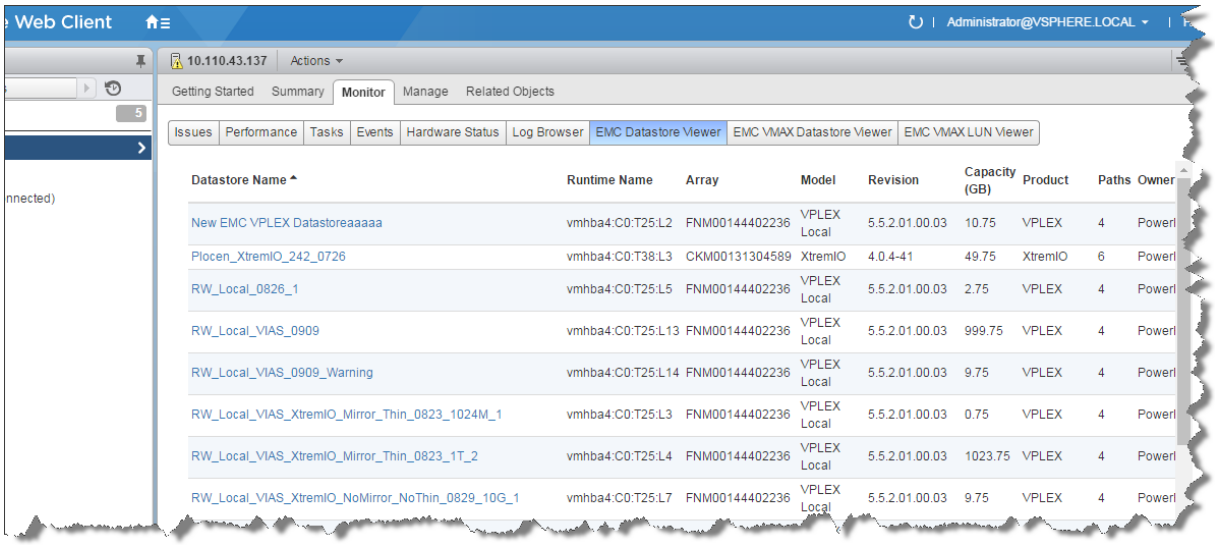
1. Select **Home** > **Inventory Lists** > **Hosts**.
2. Select a host from the inventory list and select **Monitor** > **EMC Datastore Viewer**.

   The datastore table appears, as shown below. Click the column header to sort columns.

Note

VMAX objects are listed on the **EMC VMAX Datastore Viewer** and **EMC VMAX LUN Viewer** tabs.

Figure 25 Viewing datastores on a host



3. Click the link in the **Datastore Name** column to view property details.

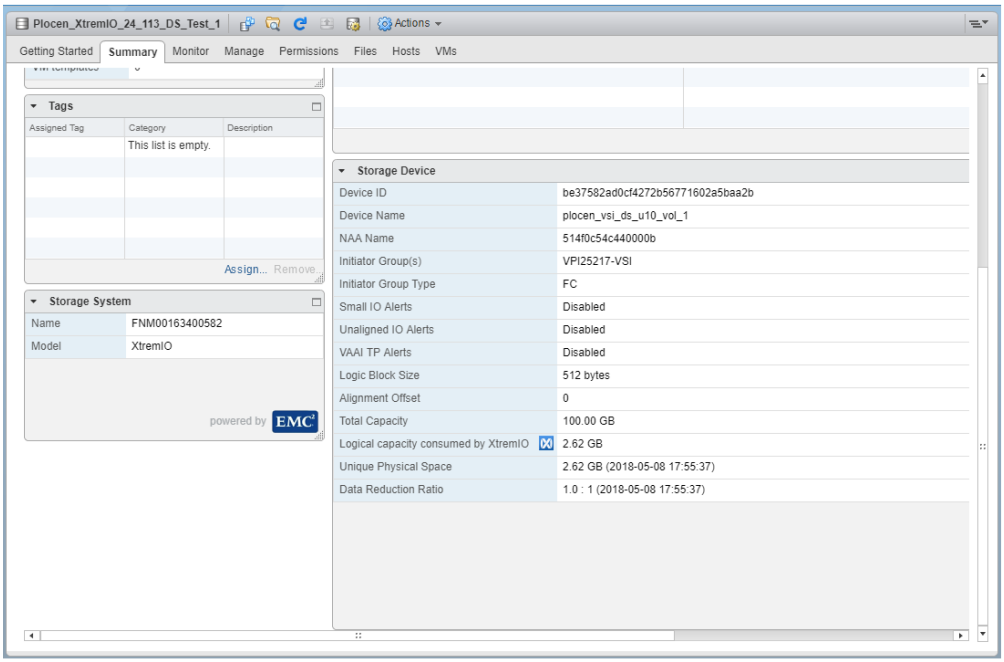
Viewing NFS or VMFS datastore properties

Use the **Summary** tab to view datastore properties in vSphere.

Procedure

1. Ensure that the storage array used by the datastore or RDM disk has been registered.
2. Select **Home** > **vCenter Inventory Lists** > **Datastores**.
3. Select the datastore name.
4. Click **Summary** to view the **Storage System**, **Details**, and **Storage Device** panes, as shown in the following figure:

Figure 26 Viewing datastore properties



Note

This release introduces new fields **Unique Physical Space** and **Data Reduction Ratio** under **Storage Device**. By default, these fields are blank before calculation. VSI queries the XtremIO Management Server (XMS) to retrieve these values. The calculation must be run from the XMS.

Note

For VMFS datastores on thin pool LUNs, the VSI properties show a different amount of used and free space than VMware shows in the **Storage Used** graphic on the right of the GUI window. This VMware UI component has no awareness of the added metadata stored on the pool with the LUN. VSI properties display the same numbers as EMC Unisphere™ does on a VNX array.

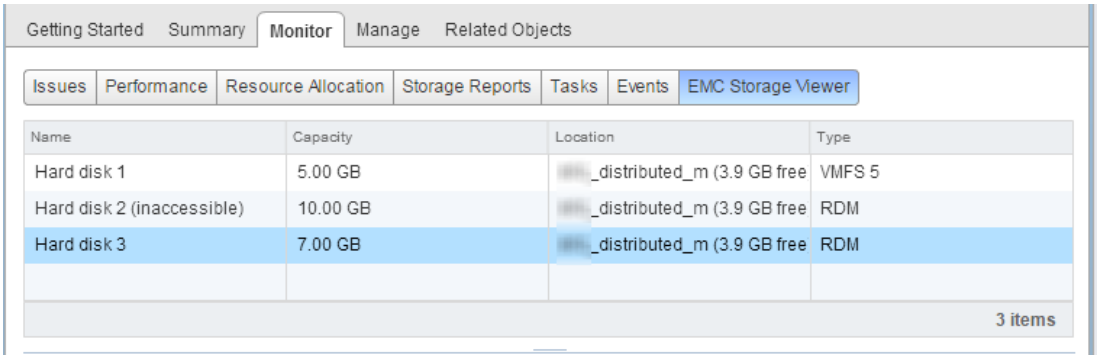
Viewing RDM disk properties

Use the **Monitor** tab to view RDM disk properties in vSphere.

Procedure

1. Select **Home** > **vCenter Inventory Lists** > **Virtual Machines**.
2. Expand the directory and select the appropriate virtual machine.
3. Select **Monitor** > **EMC Storage Viewer**.
4. Select the RDM disk, as shown below.

Figure 27 Viewing properties of an RDM disk



Viewing VMAX datastores at host level or cluster level

View EMC VMAX datastores created on a host or cluster.

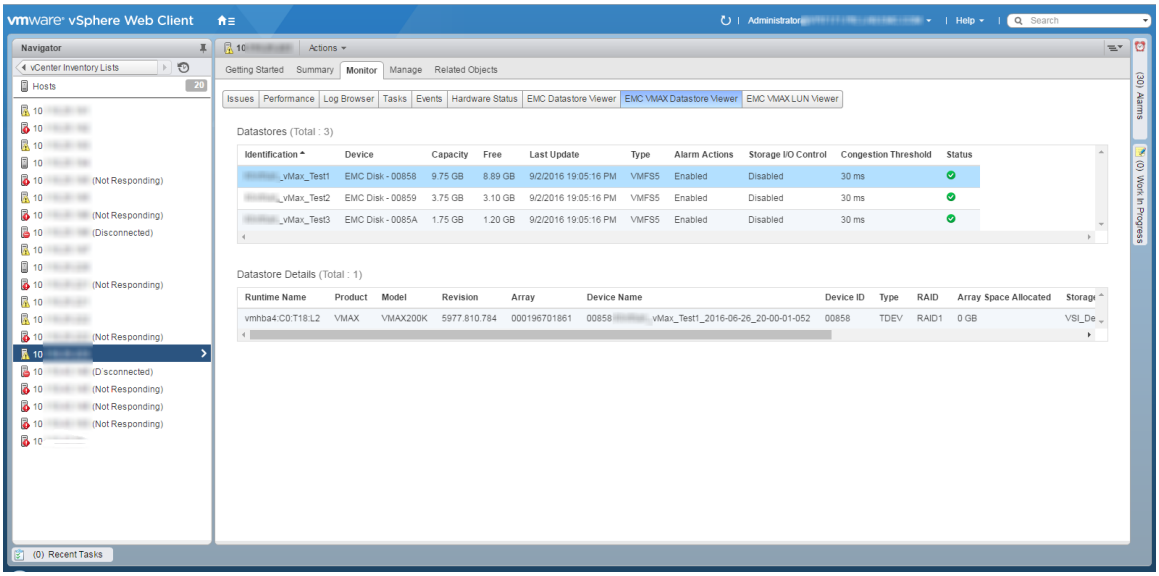
Before you begin

Ensure that a VMAX array is registered in the Solutions Integration Service.

Procedure

1. Select **Home** > **vCenter Inventory Lists**, and then select **Hosts** or **Clusters**.
2. Select a host or cluster and select **Monitor** > **EMC VMAX Datastore Viewer**.
3. Select a row in the **Datastores** table to view the **Datastore Details**, as shown below.

Figure 28 Viewing VMAX datastore details at host level



Viewing VMAX LUNs at host level or cluster level

View EMC VMAX LUNs created on a host or cluster.

Before you begin

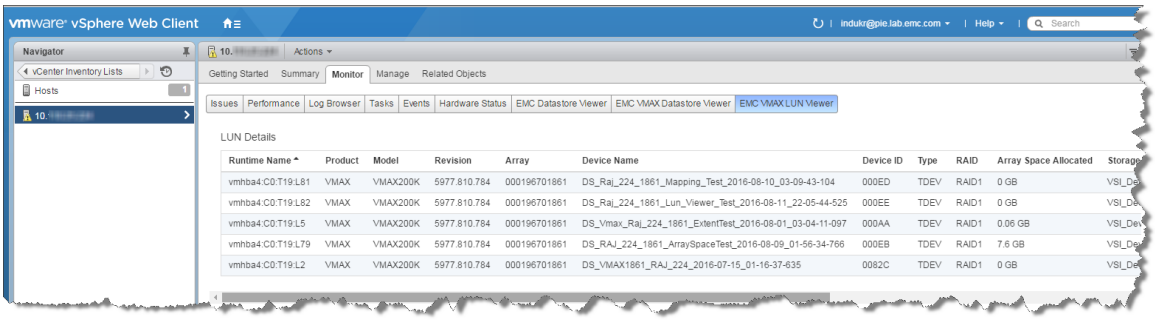
Ensure that a VMAX array is registered in the Solutions Integration Service.

Procedure

1. Select **Home** > **vCenter Inventory Lists**, and then select **Hosts** or **Clusters**.
2. Select a host or cluster and select **Monitor** > **EMC VMAX LUN Viewer**.

   Details are displayed in the LUN Details table, as shown below.

   Figure 29 Viewing VMAX LUN details at host level



Viewing virtual machine clone properties

You can view virtual machine clone properties using the **Summary** tab.

Procedure

1. Select **Home** > **VMs and Templates**.
2. Select the object name.
3. Click **Summary** to view Storage Device and Storage System details.

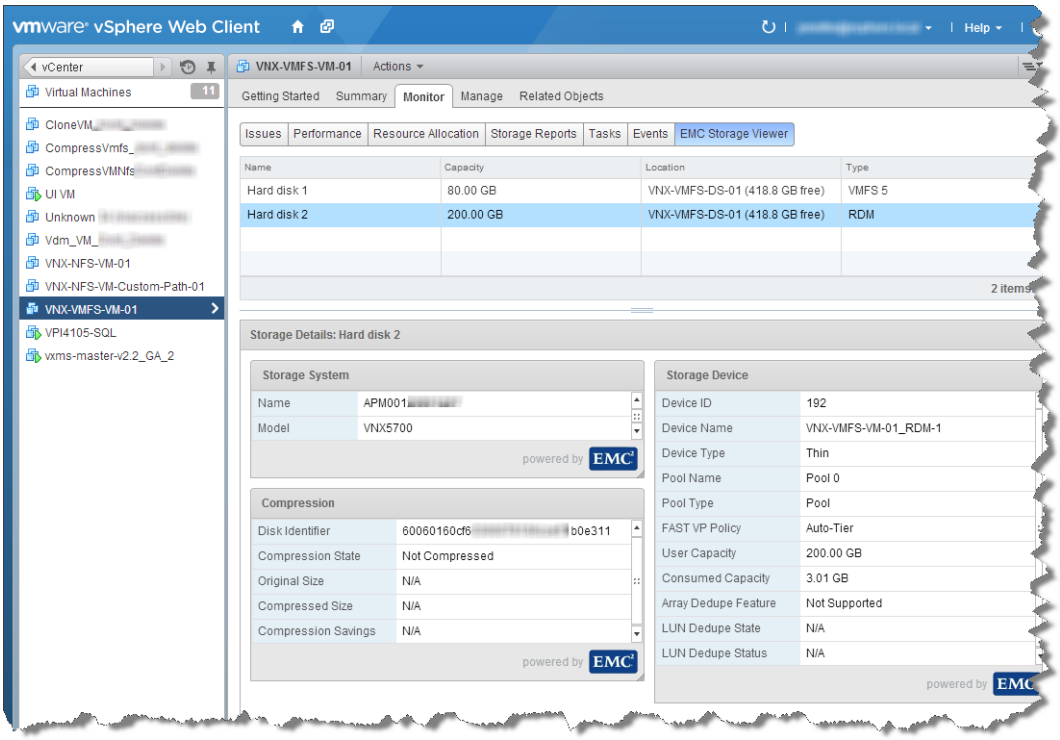
Viewing compression properties

Use the **Monitor** tab to view compression properties.

Procedure

1. Select **Home** > **VMs and Templates**.
2. Select the object name.
3. Click **Monitor**.
4. Select **EMC Storage Viewer**, as shown below.

Figure 30 Viewing VNX RDM volume properties with EMC Storage Viewer



Note

If a virtual machine is compressed, the VSI properties show a different amount of used and free space than VMware reports, since it has no awareness of the compression savings. VSI properties display the same compression savings as Unisphere does on the VNX.

5. To see virtual machine properties, including compression properties, select the first virtual disk on the list.
6. To see RDM volume properties, select the appropriate subsequent virtual disk.

Managing connection brokers

You can use VSI to manage connection brokers for VMware Horizon View and Citrix XenDesktop.

Registering a connection broker with VSI

Use this procedure to register a VMware View Manager or Citrix XenDesktop Manager connection broker.

Procedure

1. Click **Home** > **vCenter** > **Inventory Lists** > **EMC VSI** > **Connection Broker**.
2. Right-click **Connection Broker** and select **Register Connection Broker**.
3. In the **Register Connection Broker** dialog box, select the **Connection Broker** (**VMware View Manager** or **Citrix XenDesktop Manager**) and type the required server credentials.

4. Click **OK**.

Unregistering a connection broker

Use this procedure to unregister a connection broker.

Procedure

1. Click **Home** > **vCenter** > **Inventory Lists** > **EMC VSI** > **Connection Broker**.
2. Right-click **Connection Broker** and select **Unregister Connection Broker**.

Refreshing a connection broker

You can refresh a connection broker using this procedure.

Procedure

1. Click **Home** > **vCenter** > **Inventory Lists** > **EMC VSI** > **Connection Broker**.
2. Right-click **Connection Broker** and select **Refresh Connection Broker**.

Managing multipathing policies

This version of VSI automatically registers EMC PowerPath/VE and enables you to set multipathing policies for all devices using the VMware Native Multipathing Plug-in (NMP) or EMC PowerPath/VE. The following resources provide more information about installing the PowerPath license:

- https://support.emc.com/downloads/1800_PowerPath-VE-for-VMware/Documentation
- *PowerPath Management Appliance Installation and Configuration Guide* available on support.emc.com

Modifying multipathing policies

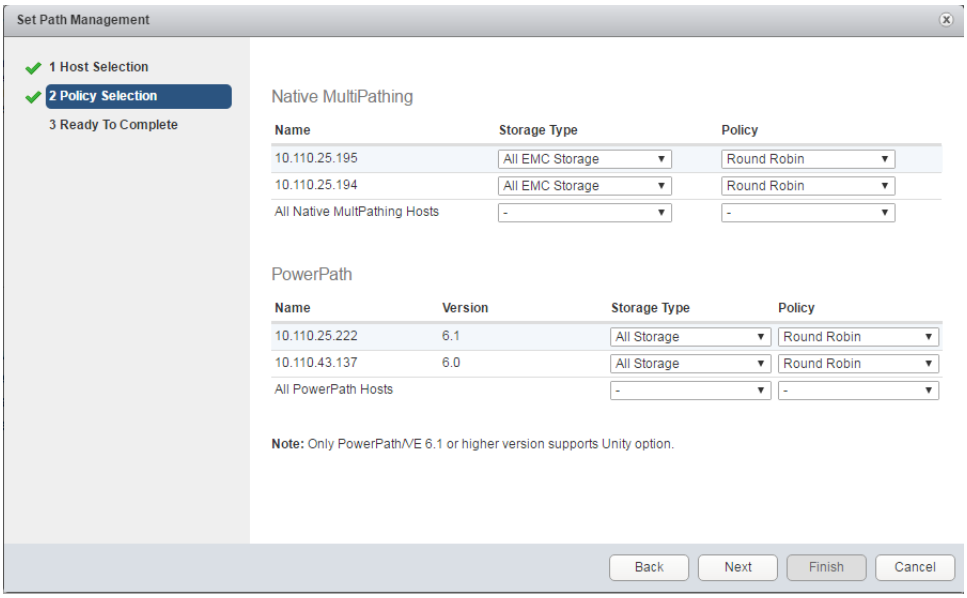
You can modify multipathing policies for datacenters, clusters, folders, and hosts using the **Path Management** wizard.

Procedure

1. Click **Home** > **vCenter Inventory Lists** and expand the inventory tree if necessary.
2. Right-click a datacenter, cluster, folder, or host and select **Set Path Management**.

   The **Path Management** wizard appears showing the hosts that are available for modification and their current policy.
3. For **Host Selection**, select the hosts you want to modify.
4. Click **Next**.
5. For **Policy Selection**, select a storage option and a corresponding policy for the host or, optionally, for all hosts in the group, as shown below.

Figure 31 Policy Selection



The following table shows the available options. Policy options depend on the storage type selected.

Table 6 Available choices for storage types and policies

Native multipathing		PowerPath/VE	
Storage types	**Available policies**	**Storage types**	**Available policies**
All Storage	• Most Recently Used • Round Robin • Fixed	All Storage	• Least Blocks • Least I/O • Stream I/O • Symmetrix Optimization • CLARiiON Optimization • Adaptive
All EMC Storage		All EMC Storage	
All Symmetrix		All Symmetrix	
All Unity		All Unity (requires PowerPath/VE v 6.1 or later)	
All VPLEX		All VPLEX	
All VNX		All VNX	
All VNXe3200		All XtremIO	
All XtremIO			

6. Click **Next**.
7. In the **Ready to Complete** dialog box, click **Finish**.

   You can monitor progress in the **Tasks** list.

Applying recommended host settings on VMAX

Set Round Robin path switching frequency according to best practices for EMC VMAX devices.

Before you begin

A VMAX array must be registered in the Solutions Integration Service.

Procedure

1. In the vSphere Navigator, right-click a host name and select **All EMC VSI Plugin Actions** > **ESXi Host Settings**.

   The **ESXi Host Recommended Settings** wizard appears.
2. Select **VMAX3 / VMAX All Flash**.

   Note

   If XtremIO storage is also presented to the ESXi host, refer to the EMC topic noted in the wizard for further instructions.
3. Select the options, **Round Robin path switching frequency - 1 I/O packet** and **Add claim rule for Round Robin path switching frequency-1 I/O packet**, and then click **Next**.
4. Type the **Username**, **Password**, and **Port** number for the host and click **Next**.
5. Review the settings and click **Finish**.
6. Review the log messages in the Solutions Integration Service to ensure that the settings were applied.

Setting host parameters on XtremIO arrays

From the host, cluster, or folder level, you can apply recommended settings for EMC XtremIO devices.

Before you begin

- Ensure that all hosts under the selected cluster or folder use the same credentials for host settings. If not, the task fails.
- Ensure that the SSH connection is enabled on all hosts.

The settings you can change include:

- **Disk Settings**
  - **SchedNumReqOutstanding**

    Note

    1. For ESXi version 6.0 or earlier, **SchedNumReqOutstanding** is set to 256. For ESXi version 6.5 or later, **SchedNumReqOutstanding** is set to LUN queue depth.
    2. Set the LUN queue depth before you set **SchedNumReqOutstanding**.
  - **SchedQuantum**
  - **DiskMaxIOSize**
- **Native Multipathing Settings (Round Robin)**
- **LUN queue depth** (Host must be restarted for changes to take effect.)

  Note

  For QLogic, LUN queue depth will be set to 256 as recommended. For Cisco UCS FNIC and Emulex, LUN queue depth will be set to 128 as recommended.

- **Optimal settings for cloning to XtremIO volumes**

Note

When the ESXi host connects to XtremIO X1 only, the **OptimalMaxHwTransferSize** is set to 256. When the ESXi host connects to XtremIO X2 only or to both XtremIO X1 and X2, the **OptimalMaxHwTransferSize** is set to 4096.

Procedure

1. From the vSphere Web Client, select **Home** > **vCenter** > **Hosts**.
2. Select a host in the inventory list to display the available objects. To set a property on multiple hosts, choose a cluster or folder.
3. Right-click the object you want to modify, and select **All EMC VSI Plugin Actions** > **ESXi Host Settings**.
4. In the **ESXi Host Recommended Settings** dialog box, select **XtremIO**, and then select the settings that you want to modify.
5. Click **Next**
6. If the SSH connection to the host is required, type the ESX host credentials and click **Next**.
7. Click **Finish**.
8. If you have changed the HBA queue depth setting, manually restart the host.

Setting space reclamation

Using the space reclamation feature in VSI, you can reclaim unused storage on datastores, hosts, clusters, folders, and storage folders on Unity, UnityVSA, VMAX3, VMAX All Flash, VNX, VNXe, VPLEX, and XtremIO storage arrays.

Note

VMware vSphere 6.5 or later provides automatic unmapping for VMFS 6 datastores. You can still use VSI to manuallly reclaim space for VMFS 5 and VMFS 6 datastores.

Because scheduled reclaim tasks are created per-datastore, scheduling from the host, cluster, folder, or storage folder level results in one scheduled task per datastore under the target object. Only one scheduled reclaim task can exist for each datastore.

When setting a schedule with the reclaim wizard:

- At the cluster, host, folder, or storage folder level, a **Schedule new job** task is created for each datastore under the target.
- At the datastore level, a single **Schedule new job** task is created for the target datastore.
- At the host level, the task is performed serially—that is, one at a time on each datastore.
- If you schedule the task on separate datastores at the same time, the tasks run in parallel. This option is not recommended because it causes heavy I/O operations.

Note

For vSphere version 5.5 or earlier, ensure that all hosts under the selected cluster or folder use the same credentials for host settings. If not, the task fails.

Procedure

1. From the vSphere Web Client, select **Home** > **vCenter Inventory Lists** > **Hosts**.
2. Select a cluster, host, folder, or storage folder in the inventory list to display the available objects.
3. Right-click the object you want to modify, and select **All EMC VSI Plugin Actions** > **Reclaim Unused Storage**.
4. In the **Reclaim Unused Storage** wizard, type the host username and password, and then click **Test Connection**.
5. Under **Reclamation Schedule**, set the following as appropriate, and then click **Next**.
   - In the Schedule list, select **Run Now**, **Daily**, **Weekly**, **Monthly**, or **Unschedule** (available only if a schedule exists), and then click **Next**. Selecting **Daily**, **Weekly**, or **Monthly** sets the schedule based on the current time, day, and/or date. Existing schedules for single datastores are displayed as the default value.

     Selecting **Unschedule** deletes the existing schedule.
   - For **Start Date/Time**, select the date and time to set a custom start time for the schedule.

     Note

     All scheduled dates and time stamps are determined by the time zone specified on the Solutions Integration Service server.
6. In **Ready to Complete**, review the details, and then click **Finish**.

Deleting reclamation schedules

You can delete schedules that you have created.

Procedure

1. Select **Home** > **vCenter Inventory Lists** > **vCenter Servers**.
2. Expand a vCenter Server and Datacenter list and select a datacenter.
3. Select **Manage** or **Configure** > **EMC VSI Schedule Management**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.
4. Select a schedule and click **Delete**.
5. Click **OK** to delete the schedule.

CHAPTER 5

Provisioning EMC Storage with VSI

This chapter includes the following topics:

Introduction

This chapter describes EMC storage system requirements and how to provision datastores and RDM disks on EMC storage systems.

EMC storage system requirements

Learn about the EMC storage systems that are supported with VSI and related system requirements.

The EMC Simple Support Matrix provides the supported storage system version numbers for this release. To obtain the required software, contact EMC Customer Support.

Table 7 EMC storage system requirements

EMC storage system	Requirements
eNAS	• Network ports are configured. • Network connectivity exists between one or more Data Movers and ESX/ESXi servers. • Network connectivity exists between the Control Station and vSphere Client on port 22 (required to provision NFS storage). • Network connectivity exists between the vCenter Server and vSphere Client.
Unity and UnityVSA	• A supported Unity OE software version is installed. • Network ports are configured. • Network connectivity exists between Unity and ESX/ESXi servers. • Network connectivity exists between vCenter Server and vSphere Web Client. • Unity File maximum file system size is 64 TB; minimum file system size is 3 GB. • Unity Block maximum LUN size is 256 TB; minimum LUN size is 10 GB. • A storage pool is created.
VMAX3 and VMAX All Flash	• A supported HYPERMAX OS and SMI-S Provider versions are installed. • A masking view has been created. • An array is connected to the host using FC or iSCSI. • The SMI-S Provider has discovered the target VMAX3/VMAX All Flash system.
VNX for File	• All VNX Data Movers have a supported VNX OE for File version installed. • NFS license is enabled. • Network ports are configured. • Network connectivity exists between one or more Data Movers and ESX/ESXi servers. • Network connectivity exists between the Control Station and vSphere Client on port 22 (required to provision NFS storage). • Network connectivity exists between one or more Data Movers and vSphere Client on port 5080 (required to compress and clone virtual machines). • Network connectivity exists between the vCenter Server and vSphere Client.

Table 7 EMC storage system requirements (continued)

EMC storage system	Requirements
	• DHSM is set up to use the compression and cloning features. • VNX for file maintains the following limit: Maximum file system size = 16 TB.
VNX for Block	• A supported VNX OE for Block version is installed. • A storage pool or RAID group is created. • Network ports are configured. • Network connectivity exists between one or more storage processors and ESX/ESXi servers. • Network connectivity exists between one or more storage processors and the vSphere Client on port 443 (required for provisioning VMFS datastores and RDM disks and for setting tiering policies). • Network connectivity exists between the vCenter Server and vSphere Client. • Each ESX/ESXi host that will access block storage is connected to a storage group on the array.
VNXe1600 (Block only)	• A supported VNXe OE software version is installed. • iSCSI license is enabled (to provision block storage). • Network ports are configured. • Network connectivity exists between VNXe1600 and ESX/ESXi servers. • Network connectivity exists between the vCenter Server and vSphere Web Client. • VNXe for Block maximum LUN size is 16 TB; minimum LUN size is 10 GB. • A storage pool or RAID group is created.
VNXe3200	• A supported VNXe OE software version is installed. • NFS license is enabled (to provision file storage). • Network ports are configured. • Network connectivity exists between VNXe3200 and ESX/ESXi servers. • Network connectivity exists between vCenter Server and vSphere Web Client. • VNXe for file maximum file system size is 16 TB; minimum file system size is 1 GB. • VNXe for block maximum LUN size is16 TB; minimum LUN size is 10 GB. • A storage pool or RAID group is created. • iSCSI license is enabled (to provision block storage).
VPLEX	The supported VPLEX version is installed. **Note** VPLEX Local and VPLEX Metro are supported. VPLEX GEO is not supported.
XtremIO	• A supported XtremIO version is installed. • One or more initiator groups exist.

Table 7 EMC storage system requirements (continued)

EMC storage system	Requirements
	• FC or iSCSI connection exists between the ESX/ESXi host and the array. • XMS is configured for the XtremIO array.

Registering a storage provider

To provision virtual volumes on a VVol-enabled storage system, you must first register a storage provider.

Procedure

1. Select **Home** > **vCenter Inventory Lists** > **vCenter Servers** and select a vCenter.
2. Select **Manage** or **Configure** > **Storage Providers**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

3. Click **Add** (green plus sign) and provide the following credentials for the storage provider you are creating:

   Name: A meaningful name for the new storage provider
   URL: The URL for the new storage provider in the format `https://storage_system_IP:8443/vasa/version.xml`, where *storage_system_IP* is the IP address of a VVol-enabled storage system in your environment
   User name: The storage array username
   Password: The storage array password

4. Click **OK** to register the storage provider.

Results

The storage provider status is **Online** and it includes at least one active storage system.

Provisioning NFS datastores

You can provision NFS datastores in datacenters, folders, clusters, or hosts on the following storage arrays: eNAS, Unity, UnityVSA, VNX, and VNXe3200.

Note

For eNAS, Unity, UnityVSA, VNX, and VNXe3200 arrays, you can provision a new NFS datastore or create an NFS datastore from an existing export.

Procedure

1. Select **Home** > **vCenter Inventory Lists** > **Hosts** and expand the inventory tree if necessary.

2. Right-click the object name.
3. Select **All EMC VSI Plug-in Actions** > **New EMC Datastore**.

   The **New EMC Datastore** wizard appears.

4. For **Name and location**, specify a unique name for the datastore and click **Next**.

   Note

   Valid names can include alphanumeric characters, hyphen (-), underscore (_), open parenthesis ((), and close parenthesis ()). All other characters are invalid.

5. For **Type**, select **NFS** and click **Next**.
6. For **Array Selection**, select from the list of file-capable arrays that are accessible to the VSI client that you specified and click **Next**.
7. Provide values for the remaining parameters in the wizard and click **Next** after each wizard step.

   The following tables provide details about particular NFS datastore parameters for each storage system:

   - Table 8 on page 67: eNAS, VNX
   - Table 9 on page 68: Unity, UnityVSA, VNXe3200

8. In the **Ready to Complete** dialog box, review the parameters and click **Finish**.

   When the tasks are completed, a checkmark appears next to **Create NAS datastore** under **Recent Tasks**.

   Note

   To refresh the task frame, click **My Tasks**, and then select **All Users Tasks**.

Results

The new datastore appears under **Home** > **vCenter Inventory Lists** > **Datastores** > **Summary**.

Table 8 Required parameters for provisioning an NFS datastore on eNAS and VNX

Wizard step	Parameter	Description
Data Mover Selection	**Select Data Mover**	Select from the list of Data Movers that are available on the array.
	Select Interface	Select the IP address that you want to use.
	Select the hosts that require access to the datastore	vCenter determines the host IP address that can be selected. Select a host IP address or domain name. You must select at least one.
Provisioning Action		You can create a new NFS export or create a datastore from an existing NFS export. Select **Create new NFS Export** or **Map Existing NFS Export**.
	Create new NFS Export	Select this option to create a new NFS export.

Table 8 Required parameters for provisioning an NFS datastore on eNAS and VNX (continued)

Wizard step	Parameter	Description
	• **Pool Selection**	Select from the storage pools that are available on the selected array.
	• **NFS Export Properties**	• **Initial capacity** • **Thin enabled**: Specifies that storage is allocated on a just-enough and just-in-time basis. • **Maximum capacity**: Specify the maximum capacity for the virtual pool. If **Thin enabled** is selected, **Maximum Capacity** is unavailable. • **Advanced**: Optionally, set the following parameters: ▪ **Export path** ▪ **Highwater mark** ▪ **Direct Writes Enabled** ▪ **No Prefetch** ▪ **Virus Checking Enabled** ▪ **Export to Subnet** ▪ **Set Timeout Setting**
	Map Existing NFS Export	Select this option to create a datastore from an existing NFS export.
	• **Existing NFS Export**	• **NFS Export Name**: Select an NFS export. • Optionally, click **Advanced** to set advanced NFS export properties.

Table 9 Required parameters for provisioning an NFS datastore on Unity, UnityVSA, and VNXe3200

Wizard step	Parameter	Description
Provisioning Action		You can create a new NFS export or create a datastore from an existing NFS export. Select **Create new NFS Export** or **Map Existing NFS Export**.
	Create new NFS Export	Select this option to create a new NFS export.
	• **Choose Storage Pool**	Select from the storage pools that are available on the selected array.
	• **New NFS Export**	Specify the parameters for the virtual pool: • **NAS server**. • **Tiering Policy**. • **Size**: Specify the capacity. • **Thin**: Select **Enabled**.

Table 9 Required parameters for provisioning an NFS datastore on Unity, UnityVSA, and VNXe3200 (continued)

Wizard step	Parameter	Description
		Note Unity and UnityVSA support only thin provisioning. • **Hosts**: Select the hosts that require access to the datastore.
	Map Existing NFS Export	Select this option to create a datastore from an existing NFS export.
	• **Existing NFS Export**	• **NAS Server**. • **Export path**: Select the export path of an existing NFS datastore. • **Select the hosts that require access to the datastore**: Select the required hosts. **Note** If you launched the wizard from a specific host, only that host is displayed. If you launched the wizard at the cluster level, all the hosts within that cluster are available for selection.

Provisioning VMFS datastores

You can provision VMFS datastores in datacenters, folders, clusters, or hosts on the following storage arrays: Unity, UnityVSA, VMAX3, VMAX All Flash, VNX, VNXe1600, VNXe3200, VPLEX, and XtremIO.

Note

You can provision VMFS-6 datastores if you are using vCenter and ESXi version 6.5 or later. You can provision VMFS-5 datastores on vCenter and ESXi version 6.0 or later.

Procedure

1. Select **Home** > **vCenter Inventory Lists** > **Hosts** and expand the list, if necessary, to view nested items.
2. Right-click the host or cluster name.
3. Select **All EMC VSI Plug-in Actions** > **New EMC Datastore.**
4. In the **New EMC Datastore** wizard, specify a value for each of the following parameters:
   - **Name and location**: Type a name for the datastore.

Note

Valid names can include alphanumeric characters, hyphen (-), underscore (_), open parenthesis ((), and close parenthesis ()). All other characters are invalid.

- **Type**: Select **VMFS**.
- **Array Selection**: Select from the list of block-capable arrays that are accessible to this client. The **More Info** column provides capacity information for XtremIO arrays and other details to help you choose an appropriate array.

5. Provide values for the remaining parameters in the wizard and click **Next** after each wizard step. The following tables provide details about particular VMFS datastore parameters for each storage system:
   - Table 10 on page 70: VMAX3 and VMAX All Flash
   - Table 11 on page 70: VNX
   - Table 12 on page 71: Unity, UnityVSA, VNXe1600, VNXe3200
   - Table 13 on page 72: VPLEX
   - Table 14 on page 73: XtremIO
6. In the **Ready to Complete** dialog box, review the parameters and click **Finish**.

Results

When the tasks are completed, a checkmark appears next to the new datastore.

The new datastore appears under **Home** > **vCenter Inventory Lists** > **Datastores**.

Table 10 Required parameters for provisioning a VMFS datastore on VMAX3 and VMAX All Flash

Wizard step	Parameter	Description
Storage Resource Pool	**Volumes**	Type the number of volumes to create.
	Volume capacity	Type a number and select the measurement.
	Storage Resource Pool	Select a pool.
	Storage Groups	Select a storage group from the table.

Table 11 Required parameters for provisioning a VMFS datastore on VNX

Wizard step	Parameter	Description
Pool Selection		Select from the storage pools that are available on the selected array.
VMFS Version	• **VMFS-6** • **VMFS-5**	Select the version. **Note** Available VMFS versions depend on your version of vCenter and ESXi.
Datastore Details	**Preferred LUN ID**	

Table 11 Required parameters for provisioning a VMFS datastore on VNX (continued)

Wizard step	Parameter	Description
	Default Owner	
	Capacity	The maximum allowed capacity for a new export is the greater of the available capacity in the virtual pool or the maximum capacity of the VMFS version.
	Thin	Select for thin provisioning. **Thin** is not available if you selected a RAID group in **Pool Selection** or if FAST is not installed on the array. The maximum capacity changes if **Thin** is selected. **Note** If the virtual pool does not specify the available capacity, `Max: unknown` is displayed.
	Advanced	Select the Tiering Policy: • **Start High then Auto-Tier (Recommended)** • **Auto-tier** • **Highest Available Tier** • **Lowest Available Tier**

Table 12 Required parameters for provisioning a VMFS datastore on Unity, UnityVSA, VNXe1600, and VNXe3200

Wizard step	Parameter	Description
Pool Selection		Select from the storage pools that are available on the selected array.
VMFS Version	• **VMFS-6** • **VMFS-5**	**Note** Available VMFS versions depend on your version of vCenter and ESXi.
Datastore Details (Unity, UnityVSA, and VNXe3200 only)	**Capacities**	The maximum allowed capacity for a new datastore is the smallest of the following amounts: the available capacity in the virtual pool, the maximum allowed LUN size, or the maximum capacity of the VMFS version: • VMFS-5 and VMFS-6 support a maximum volume size of 64 TB. • VMFS-5 and VMFS-6 support a maximum LUN capacity of 256 TB. If the virtual pool does not specify the available capacity, `Max: unknown` is displayed. **Thin** is selected by default. Clear the check box for thick provisioning.

Table 12 Required parameters for provisioning a VMFS datastore on Unity, UnityVSA, VNXe1600, and VNXe3200 (continued)

Wizard step	Parameter	Description
		Note Unity and UnityVSA support thin provisioning only. **Compression**: This checkbox is available for Extreme Performance pools only on Unity 4.1.0 or later arrays. Select it to enable compression on the new datastore.
	Advanced (Unity, UnityVSA, VNXe3200 only)	Select the Tiering Policy.
	Multiple Volumes	Type the number of volumes you want to create.
Datastore Details (VNXe1600 only)	**Capacity**	Type the amount of storage you want to provision.
	Thin	Select this option for thin provisioning.

Table 13 Required parameters for provisioning a VMFS datastore on VPLEX

Wizard step	Parameter	Description
VMFS Version	• **VMFS-6** • **VMFS-5**	**Note** Available VMFS versions depend on your version of vCenter and ESXi.
Consistency Group Selection	**Add storage to an existing consistency group**	Select this option to add to an existing consistency group. You can use the filter list to narrow the list and select a local or global consistency group from the table.
	Create a new consistency group	Select this option to create a new consistency group.
Consistency Group Name		Required only if you are creating a new consistency group. Type a name for the new consistency group.
Select Consistency Group Type Required only if you are creating a new consistency group.	**Local**	• Select a cluster from the list. • Global Visibility: Local consistency groups are synchronous and visible only to the local cluster unless you select this option. • Select a **Detach Rule** from the list.
	Distributed	• Synchronous and visible to all clusters. You can add only distributed Virtual Volumes. • Select a **Detach Rule** from the list.
Protection Options Selection	**Source Cluster**	Select the location for the new datastore.
	High Availability Options	Select **Enable Mirroring**.
	Synchronization Options	Available only if you selected the distributed consistency group type.

Table 13 Required parameters for provisioning a VMFS datastore on VPLEX (continued)

Wizard step	Parameter	Description
		• **Synchronize Data**—Synchronizes data from the source storage volume to the target storage volume. Select this option to mirror existing data to another cluster. • **Do Not Synchronize Data**—Select this option only if you are sure that host-based volume initialization will resolve any inconsistencies between the underlying storage volumes. Otherwise, select **Synchronize Data**.
Storage Selection	• **Source Storage** • **Target Storage**	Specify the Source and Target IP addresses. The data on the source storage volume will be copied to the target storage volumes.
Second Storage Selection Required only if you selected a Distributed consistency group type.	• **Source Storage** • **Target Storage**	Specify the Source and Target IP addresses. The data on the source storage volume will be copied to the target storage volumes.
Storage Views Selection		Select the storage to expose to hosts through storage views.

Table 14 Required parameters for provisioning a VMFS datastore on XtremIO

Wizard step	Parameter	Description
Initiator Group Selection		Select initiator groups from the list.
VMFS Version	• **VMFS-6** • **VMFS-5**	• VMFS-5 and VMFS-6 support a maximum LUN capacity of 64 TB. **Note** Available VMFS versions depend on your version of vCenter and ESXi.
Datastore Details	**Maximum capacity**	Value depends on the VMFS version selected and the remaining available XtremIO capacity. The smaller value is displayed.
	Type	Logical block size (auto filled).
	• **Small IO Alerts** • **Unaligned IO Alerts** • **VAAI TP Alerts**	Select **Enable** or **Disable**. Default is **Disable**.
	Multiple Volumes	Type a value for **Volume Count**.

Provisioning Unity and UnityVSA Virtual Volume datastores

You can provision Virtual Volume datastores on Unity and UnityVSA storage systems.

Before you begin

To provision virtual volumes on a Unity storage system, you must first register a storage provider. Refer to Registering a storage provider.

Procedure

1. Select **Home** > **Hosts and Clusters** and expand the inventory tree if necessary.
2. Right-click the object name.
3. Select **All EMC VSI Plug-in Actions** > **New EMC VVOL Datastore**.

   The **New EMC VVOL Datastore** wizard appears.
4. For **Datastore Type**, select **VVol (Block)** or **VVol (File)** and click **Next**.
5. For **Datastore Name**, specify a unique name for the datastore and click **Next**.

   Note

   Valid names can include alphanumeric characters, space, hyphen, underscore, open parenthesis, and close parenthesis. All other characters are invalid.
6. For **Array Selection**, select from the list of Virtual Volume-capable arrays that are accessible to the VSI client that you specified and click **Next**.

   Note

   This page shows only Unity/UnityVSA storage systems that have a VMware VASA/VVols license installed.
7. For **Capability Profile Selection**, do one of the following:
   - Use an existing profile: Select the checkbox of an existing capability profile to enable the row, specify the **Datastore Size** in the last column, and click **Next**.

     Note

     You can select multiple capability profiles for each VVol datastore and configure a maximum size for each profile. The datastore size will be the sum of the sizes for each capability profile selected.
   - Create a new profile: Click **Add New Capability Profile**. In the **New Capacity Profile** wizard, specify the **Name**, **Description**, **UsageTag**, and **Storage Pool**, and click **Save**.

     The selections are not mutually exclusive. You can select multiple capability profiles, existing profiles, and newly created profiles.

     A new capability profile is added into the bottom of capability profile table. Specify the **Datastore Size** in the last column.

Note

A new capability profile is created in Unity/UnityVSA only after you specify the datastore size and click **Finish** on the **Summary** page in the last step.

8. For **Host Selection**, select the hosts that require access to the datastore and click **Next**.
9. In the **Ready to Complete** dialog box, review the parameters and click **Finish**.

Results

When the tasks are completed, a checkmark appears next to **CreateVvolLun** under **Recent Tasks**.

Note

To refresh the task frame, click **My Tasks**, and then select **All Users Tasks**.

Extending datastores

When NFS and VMFS datastores start to run out of free space, you can add more storage space by extending them. You can extend datastores on the following EMC storage systems: VNX, VNXe1600, VNXe3200, and XtremIO.

You can extend any NFS datastore. You can extend VMFS datastores that meet the following criteria:

- The datastore is on a thick or thin LUN.
- The datastore does not span multiple extents.
- The datastore is not provisioned from a RAID group.
- The datastore is not an RDM volume.
- The datastore is not on a metaLUN or striped metaLUN.

Procedure

1. Select **Home** > **vCenter Inventory Lists** > **Datastores**.
2. Right-click the datastore to be extended, and select **All EMC VSI Plugin Actions** > **Extend Storage**.
3. In the **Extend Storage** wizard, under **Capacity Details**, in **Additional Device Capacity**, type the additional capacity to add to the datastore and select a unit of measure from the list box.
4. Click **Next**.
5. In **Ready to Complete**, review your selections and click **Finish**.

Note

When extending a striped volume, a meta volume of type BCV+TDEV is created. This volume is a backup of the datastore that is currently being extended. Verify that the extend operation completes successfully without data loss, and then delete this volume manually.

Extending virtual volume datastores

When virtual volume (VVol) datastores start to run out of free space, you can add more storage space by extending them. You can extend datastores on EMC Unity storage systems.

Procedure

1. Select **Home** > **vCenter Inventory Lists** > **Datastores**.
2. Right-click the datastore to be extended, and select **All EMC VSI Plugin Actions** > **Extend VVol Datastore**.
3. In the **Extend VVol Datastore** wizard, under **Array Details**, select the array that contains the datastore and click **Next**.
4. In **Capability Profile Selection**, select one or more profiles to be extended and type a number for the new **Datastore Size**.
5. In **Ready to Complete**, review your selections and click **Finish**.

Provisioning RDM disks

You can provision RDM disks at the virtual machine level on the following EMC storage systems: Unity, UnityVSA, VMAX3, VMAX All Flash, VNX, VNXe1600, VNXe3200, VPLEX, and XtremIO. Provisioning of RDM disks is not supported on Unity VVOL systems.

Procedure

1. Select **Home** > **vCenter Inventory Lists** > **Hosts**.
2. Right-click the appropriate virtual machine name and select **All EMC VSI Plug-in Actions** > **New EMC RDM Disk.**
3. For **Array Selection**, from the list of arrays, select a storage array for the type of RDM disk you want to provision and click **Next**.
4. Provide values for the parameters in the wizard and click **Next** after each wizard step. The following tables provide details about particular RDM disk parameters for each storage system:
   - Table 15 on page 76: Unity, UnityVSA, VMAX3, VMAX All Flash, VNX, VNXe1600, and VNXe3200
   - Table 17 on page 79: VPLEX
   - Table 16 on page 79: XtremIO
5. In the **Ready to Complete** dialog box, review the parameters and click **Finish**.

Results

When the tasks are completed, a checkmark appears next to the new RDM disk.

Table 15 Required parameters for provisioning an RDM disk on Unity, UnityVSA, VMAX3, VMAX All Flash, VNX, VNXe1600, and VNXe3200

Wizard step	Parameter	Description
Storage Pool Selection (Unity,		Select a storage pool for the new volume.

Table 15 Required parameters for provisioning an RDM disk on Unity, UnityVSA, VMAX3, VMAX All Flash, VNX, VNXe1600, and VNXe3200 (continued)

Wizard step	Parameter	Description
UnityVSA, VNX, VNXe1600, VNXe3200 only)		**Note** The list shows only storage pools that you have access to. Refer toManaging users and storage pools on page 44 for details.
Hard Disk Settings	**Location**	Select the location for the new RDM disk.
	Compatibility mode	• **Physical** (default): Allows the guest operating system to access the hardware directly. Physical compatibility is useful if you are using SAN-aware applications on the virtual machine. However, a virtual machine with a physical compatibility RDM cannot be cloned, converted to a template, or migrated if the migration involves copying the disk. • **Virtual**: Allows the RDM to behave like a virtual disk, which enables features such as creating snapshots, cloning, and so on. When you clone the disk or make a template from it, the contents of the LUN are copied into a VMDK virtual disk file. When you migrate a virtual compatibility mode RDM, you can migrate the mapping file or copy the contents of the LUN to a virtual disk.
	Shares	Select the shares value. The shares value is the relative metric for controlling disk bandwidth. The values **Low**, **Normal**, **High**, and **Custom** are the sum of all shares of all the virtual machines that are on the host.
	Limit - IOPS	Enter the upper limit of IOPS to allocate to the virtual machine, or select **Unlimited**.
	Virtual Device Node	Select any unassigned node or multiple nodes and move them to the box on the right.
	Disk Mode	If you selected **Virtual** for the **Compatibility mode**, select the appropriate disk mode: • **Dependent**: Disks are included in snapshots. • **Independent - persistent**: Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode is written permanently to the disk. • **Independent - nonpersistent**: Changes to disks in nonpersistent mode are discarded when you turn off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you turn off or reset the virtual machine.

Table 15 Required parameters for provisioning an RDM disk on Unity, UnityVSA, VMAX3, VMAX All Flash, VNX, VNXe1600, and VNXe3200 (continued)

Wizard step	Parameter	Description
Storage Pool Selection (VMAX3, VMAX All Flash only)	**Volume capacity**	Type a number and select the measurement.
	Storage Resource Pool	Select a pool.
	Storage Groups	Select a storage group from the table.
Volume Properties (VNX only)	**Preferred LUN ID**	
	Default Owner	• Auto • SP A • SP B
	Capacity	Specify the amount of storage. The maximum allowed capacity for the new RDM is the available capacity in the virtual pool. If the virtual pool does not specify the available capacity, Max-unknown is displayed.
	Thin	Select the option for thin provisioning.
	Advanced	Select the Tiering Policy: • **Start High then Auto-Tier (Recommended)** • **Auto-Tier** • **Highest Available Tier** • **Lowest Available Tier**
Volume Properties (Unity, UnityVSA, VNXe3200 only)	**Capacities**	The amount of storage you want to provision. The maximum allowed capacity for the new RDM is the smaller of the available capacity in the virtual pool or the maximum allowed LUN size. If the virtual pool does not specify the available capacity, `Max: unknown` is displayed.
	Thin	Select this option for thin provisioning. **Note** Unity and UnityVSA support only thin provisioning.
	Tiering Policy	• **Start High then Auto-Tier (Recommended)** • **Auto-Tier** • **Highest Available Tier** • **Lowest Available Tier**
Volume Properties (VNXe1600 only)	**Capacity**	The amount of storage you want to provision.
	Thin	Select this option for thin provisioning.

Table 16 Required parameters for provisioning an RDM disk on XtremIO

Wizard step	Parameter	Description
Initiator Group Selection		Select one or more initiator groups to which the new volume will be mapped.
Cluster IG Selection (optional)		Select the initiator groups to which the new volume can be mapped. These initiator groups are associated with the hosts under one cluster, which includes the host behind the virtual machine. The purpose of this configuration is to allow new RDM disks to be visible at the cluster level. **Note** This dialog box lists only the initiator groups that are not listed in the **Initiator Group Selection** dialog box.
Hard Disk Settings	**Location**	Select a location for the new RDM disk.
	Compatibility Mode	• **Physical**: Allows the guest operating system to access the hardware directly. Cannot be cloned or copied. • **Virtual**: Allows the RDM to behave as a virtual disk, allowing cloning and other virtual disk features.
	Shares	Select the shares value. The shares value is the relative metric for controlling disk bandwidth. The values **Low**, **Normal**, **High**, and **Custom** are the sum of all shares of all the virtual machines that are on the host.
	Limit-IOPS	Select the upper limit of I/O operations per second (IOPS) allocated to the virtual disk.
	Virtual Device Node	Select any unassigned node or multiple nodes and move them to the box on the right using the arrows or drag and drop.
	Disk Mode	(Available if you selected virtual compatibility mode.) Select **Dependent** (persistent) or **Independent** (nonpersistent).
Volume Properties	**Capacity**	Specify the amount of storage to be allocated for the new volume. Maximum is 64 TB.
	• **Small IO Alerts** • **Unaligned IO Alerts** • **VAAI TP Alerts**	Select **Enable** or **Disable**. The default setting is **Disable**.

Table 17 Required parameters for provisioning an RDM disk on VPLEX

Wizard step	Parameter	Description
Consistency Group Selection	**Add storage to an existing consistency group**	Select this option to add to an existing consistency group. You can use the filter list to narrow the list and select a local or global consistency group from the table.
	Create a new consistency group	Select this option to create a new consistency group.

Table 17 Required parameters for provisioning an RDM disk on VPLEX (continued)

Wizard step	Parameter	Description
Consistency Group Name (For new consistency group only)		Type a name for the new consistency group.
Select Consistency Group Type (for new consistency group only)	**Local**	• Select a cluster from the list. • **Global Visibility**: Local consistency groups are synchronous and visible only to the local cluster unless you select this option. • Select a **Detach Rule** from the list.
	Distributed	• Synchronous and visible to all clusters. You can add only distributed Virtual Volumes. • Select a Detach Rule from the list.
Protection Options Selection	**Source Cluster**	Select the location for the new datastore.
	High Availability Options	Select **Enable Mirroring**.
	Synchronization Options	Available only if you selected the distributed consistency group type. • **Synchronize Data**: Synchronizes data from the source storage volume to the target storage volume. Select this option to mirror existing data to another cluster. • **Do Not Synchronize Data**: Select this option only if you are sure that host-based volume initialization will resolve any inconsistencies between the underlying storage volumes. Otherwise, select Synchronize Data
Storage Selection	• **Source Storage** • **Target Storage**	Specify the **Source** and **Target IP** addresses. The data on the source storage volume will be copied to the target storage volumes.
Second Storage Selection Required only if you selected a Distributed consistency group type.	• **Source Storage** • **Target Storage**	Specify the **Source** and **Target IP** addresses. The data on the source storage volume will be copied to the target storage volumes.
Storage Views Selection		Select the storage to expose to hosts through storage views.
Hard Disk Settings	**Location**	Select the location for the new RDM disk.
	Compatibility mode	• **Physical** (default): Allows the guest operating system to access the hardware directly. Physical compatibility is useful if you are using SAN-aware applications on the

Table 17 Required parameters for provisioning an RDM disk on VPLEX (continued)

Wizard step	Parameter	Description
		virtual machine. However, a virtual machine with a physical compatibility RDM cannot be cloned, converted to a template, or migrated if the migration involves copying the disk. • **Virtual**: Allows the RDM to behave like a virtual disk, which enables features such as creating snapshots, cloning, and so on. When you clone the disk or make a template from it, the contents of the LUN are copied into a VMDK virtual disk file. When you migrate a virtual compatibility mode RDM, you can migrate the mapping file or copy the contents of the LUN to a virtual disk.
	Shares	Select the shares value. The shares value is the relative metric for controlling disk bandwidth. The values **Low**, **Normal**, **High**, and **Custom** are the sum of all shares of all the virtual machines that are on the host.
	Limit - IOPS	Enter the upper limit of IOPS to allocate to the virtual machine, or select **Unlimited**.
	Virtual Device Node	Select any unassigned node or multiple nodes and move them to the box on the right.
	Disk Mode	If you selected **Virtual** for the **Compatibility mode**, select the appropriate disk mode: • **Dependent**: Disks are included in snapshots. • **Independent - persistent**: Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode is written permanently to the disk. • **Independent - nonpersistent**: Changes to disks in nonpersistent mode are discarded when you turn off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you turn off or reset the virtual machine.

Provisioning VMFS datastores using VPLEX VIAS

You can provision VMFS datastores using VPLEX VIAS in datacenters, folders, clusters, or hosts.

Procedure

1. Select **Home** > **vCenter Inventory Lists** and expand the list to view nested items.
2. Right-click the host (cluster, data center, or folder) name and select **All EMC VSI Plug-in Actions** > **New EMC Datastore by VPLEX VIAS**.

3. Complete the wizard, clicking **Next** and **Finish**.

   The required parameters as follows:

   - **Name and Location**—Type a unique name for the datastore. The length of the name cannot exceed 64 bits and must begin with a letter. Valid characters are letters, numbers, hyphen, underscore, and space.
   - **Array Selection**—Select a **VPLEX Local** or **VPLEX Metro** storage system.
   - **VMFS Version**—Select **VMFS 5** or **VMFS 6**.
   - **Consistency Group**—Select a consistency group from the list. Type in the text box to filter the list by name or type.
   - **Volume Options**—Type the required **Volume Capacity**. Limits are 512 MB to 32 TB.
   - Select **High Availability** options to enable mirroring.
   - **Storage**—For each storage object, select a **Storage Array**, a **Storage Pool**, and a **Storage Group**. For VMAX only, select policy and workload filters. For storage pools that support thin volumes, the **Create thin virtual volume** checkbox is enabled.

     Note

     VPLEX provisions thin storage volumes on the target array, and then creates thin virtual volumes using the newly provisioned thin storage volumes.

   - **Storage Views**— Select a storage view from each list, which is grouped by cluster name.

4. Under **Ready to Complete**, review the summary information and click **Finish**.

CHAPTER 6

Managing Compression and Deduplication

This chapter includes the following topics:

Introduction

You can use the vCenter menu to enable or disable compression and deduplication on EMC VNX series, eNAS, and EMC VNXe3200 storage systems. For EMC Unity and UnityVSA storage systems, you can enable or disable inline compression when you create a VMFS datastore.

Viewing compression properties

Use the procedure in this topic to view compression properties for virtual machines created on eNAS datastores.

Note

- You can view compression properties for VMAX3 storage groups in the **New EMC Datastore** wizard when you create a VMFS datastore.
- You can view compression properties for a selected Unity 4.0.1 or later datastore in the **Summary** tab.

Procedure

1. Select **Home** > **vCenter Inventory Lists** > **Virtual Machines** and select a virtual machine from the list.
2. Select **Monitor** > **EMC Storage Viewer.**
3. Select a virtual disk in the list to view virtual machine properties, including compression properties.

Managing compression and deduplication on VNX and eNAS storage systems

You can enable and disable compression and deduplication on VNX and eNAS storage systems.

You can perform the following actions:

- Enable or disable file compression and deduplication on NFS datastores and on vCenter objects that contain NFS datastores.
- Enable and disable block compression on VMFS datastores and on vCenter objects that contain VMFS datastores.
- Enable and disable block deduplication on VNX VMFS datastores and on vCenter objects that contain VMFS datastores.

You can compress and decompress the system objects listed the following table.

Table 18 Results of compressing objects in vSphere

Object	Result
Virtual machine	The virtual machine is compressed.
Host	All virtual machines on the host are compressed.

Table 18 Results of compressing objects in vSphere (continued)

Object	Result
Cluster	All virtual machines in the cluster are compressed.
Pool	All virtual machines in the pool are compressed.
Datastore	All virtual machines in the datastore are compressed.
Folder	All virtual machines and datastores in the folder are compressed.
Datacenter	All virtual machines in the datacenter are compressed.

Limitations for compression and deduplication on file systems

Certain limitations and characteristics apply to compression and deduplication on file systems.

Familiarize yourself with the following:

- The compression and deduplication operation fails if you do not have valid file and DHSM credentials for the VNX or eNAS array. Managing storage access on page 40 and Registering and removing storage systems on page 50 provide more information about registering storage. Creating a DHSM user and service on a data mover on page 86 provides instructions for creating a DHSM user name.
- You can compress and deduplicate any virtual machine disk that resides on VNX file or eNAS storage that is registered to VSI with DHSM credentials, as long as the virtual machine is neither a fast clone nor a fast clone parent.
- When you add a virtual disk to a compressed and deduplicated virtual machine, the new disk is not automatically compressed and deduplicated, because the compression and deduplication operation occurred before you added the new disk. Repeat the compression and deduplication operation on the virtual machine to compress and deduplicate only new virtual disks.
- For best performance, enable caching on the file system where you are performing compression and deduplication operations.
- If compression and deduplication is disabled for the datastore on which the operation is executed, VSI automatically sets compression and deduplication to the suspended mode. The suspended mode allows individual compression and deduplication operations to execute, but does not compress and deduplicate the other objects on the datastore.
- You can use virtual machine compression and deduplication when archiving gold image virtual machines. However, you cannot compress and deduplicate a virtual machine that has or has had working fast clones. You will need to create a copy of the virtual machine by cloning the master virtual machine so that you can compress and deduplicate it, and then archive it.
- Compressing and deduplicating a virtual machine decreases its size on the disk. If you compress and deduplicate a host, cluster, folder, datastore, or datacenter, then the NAS platform compresses and deduplicates the VMDK files associated with all virtual machines within the selected object. The feature does not compress and deduplicate VSWP files.
- To compress and deduplicate or decompress and reduplicate a virtual machine, it must meet the following criteria:

- Hard Disk 1 is stored on an NFS datastore that resides on a VNX or eNAS array.
- The NFS datastore is on a registered VNX or eNAS array that includes valid file and DHSM credentials.
  An error message `Operation not supported for selected virtual machine` is displayed if you try to compress and deduplicate a virtual machine that does not meet these criteria.

Creating a DHSM user and service on a data mover

To enable compression and deduplication on file storage, you must create a DHSM user, and then register the storage with DHSM credentials. You also need DHSM credentials to use VSI to clone and view properties of NFS datastores and to compress and decompress virtual machines.

Use an SSH client tool to run the commands in the following procedure.

Note

The commands in the following procedure set the DHSM on all data movers. To set the DHSM on a specific data mover, replace **ALL** with the data mover name in the commands.

Procedure

1. Create a DHSM user on the data mover:

   Type **# /nas/sbin/server_user ALL -add -md5 -passwd *dhsm_user***, where *dhsm_user* is the user name you want to create.

   Type the responses at the prompts as shown:

```
Creating new user dhsm_user
User ID: 525
Group ID: 525
Home directory:
Changing password for user dhsm_user
New passwd:
Retype new passwd:
```

2. Enable digest authentication:

   Type **# /nas/bin/server_http ALL -modify dhsm -authentication digest -users *dhsm_user***

```
server_2 :
DHSM FACILITY CONFIGURATION
  Service name       : EMC File Mover service
  Comment            : Service facility for getting DHSM
attributes
  Active             : False
  Port               : 5080
  Threads            : 16
  Max requests       : 300
  Timeout            : 60 seconds
  ACCESS CONTROL
    Allowed IPs        : any
    Authentication     : digest ,Realm : DHSM_Authorization
    Allowed user       : dhsm_user
  SSL CONFIGURATION
    Mode               : OFF
    Persona            : default
```

```
    Protocol           : default
    Cipher             : default
```

If the preceding command failed with the error `NAS_DB environment not defined`,
add **`NAS_DB=/nas`** to the beginning of your command. For example:

`NAS_DB=/nas /nas/bin/server_http ALL -modify dhsm -authentication digest -users`

3. Start the DHSM service on data movers:

   Type **`# /nas/bin/server_http ALL -service dhsm -start`**

```
server_2 : done
DHSM FACILITY CONFIGURATION
  Service name       : EMC File Mover service
  Comment            : Service facility for getting DHSM
attributes
  Active             : True
```

Enabling file compression and deduplication

Learn to enable file compression and deduplication.

Procedure

1. Select **Home** > **vCenter** > **Inventory Lists** > and expand the directory.
2. Right-click the object for which you want to enable compression and deduplication.
3. Select **All EMC VSI Plug-in Actions** > **Enable File Compression and Deduplication**.

Disabling file compression and deduplication:

Learn to disable file compression and deduplication.

Procedure

1. Select **Home** > **vCenter** > **Inventory Lists** > and expand the directory.
2. Right-click the object for which you want to disable compression and deduplication.
3. Select **All EMC VSI Plug-in Actions** > **Disable File Compression and Deduplication**.

Enabling and disabling compression on block datastores

You can enable and disable block compression on VMFS datastores and vCenter objects that contain VMFS datastores.

Enabling block compression

Learn to enable compression on block datastores.

Procedure

1. Select **Home** > **vCenter** > **Inventory Lists** and expand the directory.
2. Right-click the object and select **All EMC VSI Plugin Actions** > **Enable Block Compression**.

Disabling block compression

Learn to disable compression on block datastores.

Procedure

1. Select **Home** > **vCenter** > **Inventory Lists** and expand the directory.
2. Right-click the object and select **All EMC VSI Plugin Actions** > **Disable Block Compression**.

Enabling and disabling deduplication on block datastores

VSI supports block deduplication on VNX2 systems. You can enable or disable block deduplication at the feature, pool, or LUN level on a VNX array. The following actions are available:

- **Enable block deduplication**: Applies deduplication to all virtual machines, one by one, that reside on the selected object.
- **Disable block deduplication**: Disables block deduplication on all virtual machines, one by one, that reside on the selected object.

The following restrictions apply:

- Deduplication is available only for pool LUNs on a system that has the deduplication feature enabled.
- You can enable either deduplication or compression, but not both.
- If you enable or disable deduplication on a pool LUN that has VNX snapshots associated with it, all snapshots are deleted when the operation is completed.
- You cannot set tiering policies for a deduplicated LUN.
- You can report savings from deduplication at the pool level but not at the LUN level.

Completing deduplication prerequisites

Before you can enable deduplication, prepare the environment.

Procedure

1. Create a VNX block storage array.
2. Create a datastore by provisioning storage on a host:
   - **Storage Type**: LUN
   - **Storage Array**: *array created in Step 1*
   - **Storage Pool**: Pool
   - **File System Version**: VMFS-5 or VMFS-6
   - **Datastore Type**: VMFS
3. Create the virtual machine by selecting the datastore that you created in Step 2.

Enabling block deduplication

You can enable deduplication on various objects, including datastores, virtual machines, hosts, host clusters, datacenters, and folders.

Procedure

1. Right-click the object and select **All EMC VSI Plugin Actions** > **Enable Block Deduplication**.
2. In the confirmation dialog box, click **Yes** to acknowledge that any array-based snapshots will be deleted.

   This action applies deduplication on all virtual machines, one by one, that reside the selected object.

Disabling block deduplication

You can disable deduplication as follows on various objects, including datastores, virtual machines, hosts, host clusters, datacenters, and folders.

Procedure

1. Right-click the object and select **All EMC VSI Plugin Actions** > **Disable Block Deduplication**.
2. In the confirmation dialog box, click **Yes**.

Results

This action applies reduplication to all virtual machines, one by one, that reside on the selected object.

Managing file compression and deduplication on VNXe3200 storage systems

You can enable or disable file compression and deduplication on NFS datastores and on virtual machines, hosts, clusters, and datacenters that contain NFS datastores.

Enabling file compression and deduplication

Learn to enable file compression and deduplication on VNXe3200 storage systems.

Procedure

1. Select **Home** > **vCenter** > **Inventory Lists** and expand the directory.
2. Right-click the object for which you want to enable compression and deduplication.
3. Select **All EMC VSI Plug-in Actions** > **Enable File Compression and Deduplication**.

Disabling file compression and deduplication

Learn to disable file compression and deduplication on VNXe3200 storage systems.

Procedure

1. Select **Home** > **vCenter** > **Inventory Lists** and expand the directory.

2. Right-click the object for which you want to disable compression and deduplication.
3. Select **All EMC VSI Plug-in Actions** > **Disable File Compression and Deduplication**.

CHAPTER 7

Managing Clones and Snapshots

This chapter includes the following topics:

Cloning virtual machines on VNX storage arrays

This section describes the fast clone and full clone operations for virtual machines.

- Cloning a virtual machine with fast clone operations: Creates a file-based snapshot of a virtual machine that maintains a relationship with its parent virtual machine
- Cloning a virtual machine with full clone operations: Creates a complete and independent copy of a virtual machine

About fast clones

Fast clone is a NAS feature that creates a file-based snapshot of a virtual machine that maintains a relationship with its parent virtual machine.

The following limitations exist for fast clones:

- Once a virtual machine has fast clones, it can no longer be compressed. Fast clones are created in the same NFS datastore as the parent virtual machine.
- You can create fast clones only from uncompressed virtual machines. VSI automatically decompresses a compressed virtual machine before creating the fast clone.
- The fast clone operation fails if the storage administrator does not provide DHSM credentials.
- You cannot create a fast clone of a virtual machine that is a fast clone itself.
- You can create fast clones of a gold image virtual machine only when it is on the same file system. Fast cloning across file systems is not supported.
- You cannot delete a gold image virtual machine that has fast clones. If you use the Delete from Disk option in vCenter on a gold image virtual machine the virtual machine is removed from inventory. The VMDK file associated with the virtual machine is retained, but all other files (for example SWAP, VMX, and so on) are deleted.
- You cannot compress a master virtual machine that has fast clones.
- You cannot create a fast clone on a compressed virtual machine. If you do so, VSI decompresses the virtual machine before continuing with the cloning operation.

About full clones

The full clone feature creates a complete and independent copy of a virtual machine.

The following limitations exist for creating full clones:

- The full clone operation fails if the storage administrator does not provide DHSM credentials.
- You can create full clones only to file systems that are on the same Data Mover.

Creating clones of virtual machines

You can create clones of certain virtual machines.

Cloning is available only for virtual machines that meet the following criteria:

- The virtual machine has only one virtual disk.
- The virtual machine is on an NFS datastore that resides on a registered VNX array with valid file and DHSM credentials.

Procedure

1. Select **Home** > **vCenter** > **Inventory Lists** > **Virtual Machines**.
2. Expand the directory to find the appropriate server.
3. Right-click the virtual machine name.
4. Select **All EMC VSI Plug-in Actions** > **EMC Clone**.
5. In the **EMC Clone Existing Virtual Machine** dialog box, for **Select the base name and folder**:
   a. Type a base name for the clone.
   b. Select a destination folder or a virtual machine for the cloned virtual machine.
   c. Click **Next**.
6. For **Select a compute resource**: You must select a valid compute resource. If the source datastore is not available on the selected hosts, the following warning message appears: `Fast clone option for this virtual machine is not available on the selected compute resource's datastores.` See the **Compatibility** frame to help determine the problem.
7. Specify the details for **Select Clone Options**:
   - **Clone Count**: Select the number of clones to be created.
     Max is the maximum number of clones that can be created and is determined by the number of CPU cores that are on the selected destination.
     The default is 12 virtual machines per core.

     Note

     If you create one clone, the name is the clone name you specify. If you create multiple clones, they are numbered. For example, if you specified four digits on the index, virtual machine X would have clones called X0001, X0002, X0003, and so on.
   - **Clone type**: Select fast clone or full clone.

     Note

     If the compute resource does not have access to the datastore that is hosting the source virtual machine, you can create only full clones.
   - **Generated Clone Name**: Automatically generated name for the clone.
   - **Add Leading Zeroes to Index**: Indicate whether the clones will have leading zeroes in the file names.
   - **Number of Digits in Index**: Specify the total number of digits to append to the end of the clone name.
   - **Customization Specification**: Select customized definitions from the customization specifications manager.
   - **Power on virtual machines after creation**: Select to automatically power on the virtual machine clones.
8. Do one of the following:
   - For fast clones, go to step #GUID-B304B540-485A-49D3-B4AE-BEBAC31F505C/ID-165-0000148C on page 94.

- For full clones, in **Select storage**, specify the datastore for the full clone. The datastore that you select must meet the following criteria:
  - The destination datastore must have available space that is larger than the number of clones multiplied by the size of the source virtual machine's files.
  - The destination datastore must reside on the same array and Data Mover as the source datastore.

9. Click **Next**.
10. In the **Ready to complete** dialog box, verify the details, and then click **Finish**.

Creating native clones on XtremIO VMFS datastores

The Native Clone feature uses the VMware Native Clone API to create a clone of a virtual machine in a VMFS datastore.

Note

Native clones from Eager Zeroed Thick Provisioned virtual machines are faster than clones from other types of virtual machines.

Procedure

1. Right-click the virtual machine to be cloned and select **All EMC VSI Plug-in Actions** > **EMC Clone**.

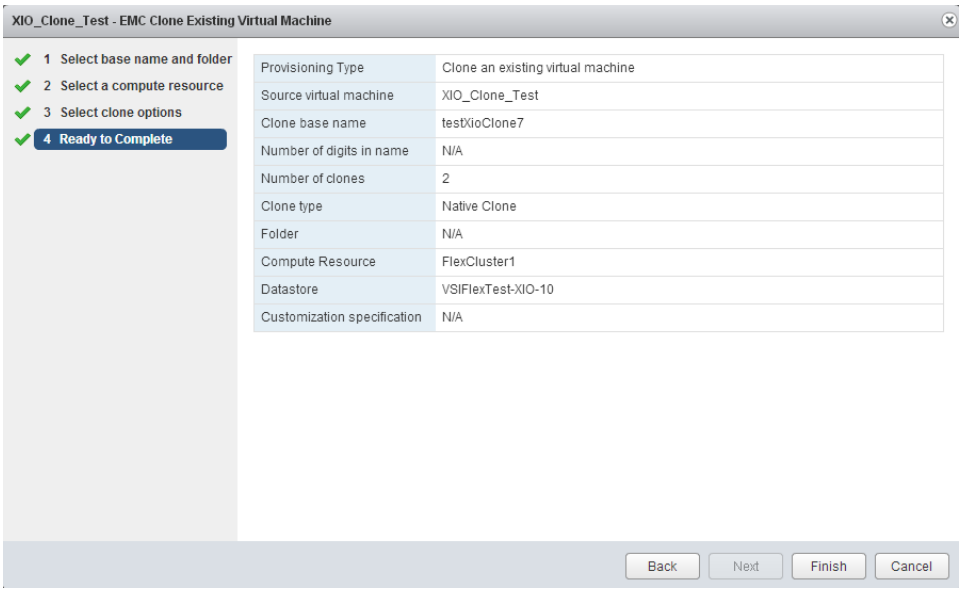
   Note

   If the **EMC Clone** menu option is not available, check the SIS registration step to ensure that **Enable scheduling for reclaim operation and XtremIO Cloning** is selected and the vCenter password is provided.

2. In **Select base name and folder**, type a name for the clone, select the destination folder, and then click **Next**.
3. In **Select a compute resource**, select a cluster, host, vApp, or resource pool to run the virtual machine clones, and then click **Next**.
4. In **Select clone options**, complete the following information:
   - **Clone count**: Type the number of clones you want to create.
   - **Generated clone name**:
     - **Add leading zeros to index used to generate names**: Select to add leading zeroes to the index numbers in the file names.
     - **Number of digits in index**: Specify the total number of digits to append to the end of the clone name.
   - **Customization specification**: List of all customized definitions from the customization specifications manager.
   - **Select destination datastore**: The target to store the clones. Select an existing XtremIO datastore or select **New** to create a new datastore.
   - **Power on virtual machines after creation**: Select to automatically power on the virtual machine clone.
5. In **Ready to Complete**, review your selections, and then click **Finish**.

The following figure shows a sample XtremIO cloning summary.

Figure 32 Cloning an existing virtual machine on an XtremIO array



Working with XtremIO snapshots

Learn the actions available for XtremIO snapshots.

You can perform the following actions for XtremIO snapshots:

- Create and name snapshots of XtremIO datastores
- View XtremIO snapshots generated for virtual machine restore
- Mount a datastore from a snapshot
- For XtremIO 4.x snapshots only:
  - Create and name a writable or read-only snapshot
  - Create and manage snapshot schedules
  - Restore virtual machines and datastores from XtremIO snapshots

Note

Ensure that the XtremIO XMS time setting is accurate, because this time is used for snapshots and schedules.

Creating a snapshot

You can create snapshots for datastores with a single extent whose underlying storage is an XtremIO volume.

Procedure

1. In the datastore inventory list, right-click the XtremIO datastore you want to copy and select **All EMC VSI Plugin Actions** > **Take Snapshot**.
2. Type a name for the snapshot or accept the default name.
3. Depending on the XtremIO version, do one of the following:

- For XtremIO 3.x datastores, click **OK** to create the snapshot.
- For XtremIO 4.x datastores, in the **Take Snapshot** dialog box, select the **Snapshot Type**: **Writable** or **Read-only**, and then click **OK**.

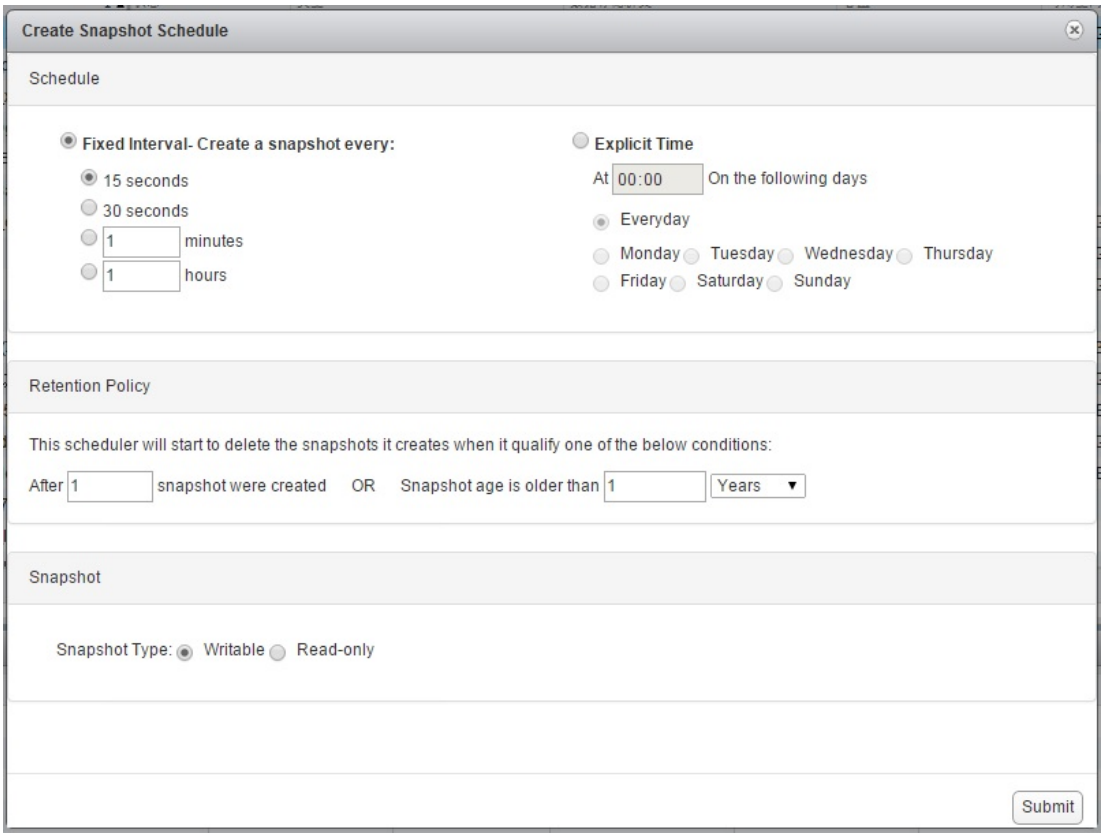
Creating snapshot schedules

You can create snapshot schedules for datastores with a single extent whose underlying storage is an XtremIO 4.0.x volume.

Procedure

1. In the **Datastore inventory** list, right-click the datastore for which you want to create a snapshot schedule and select **All EMC VSI Plugin Actions** > **Create Snapshot Schedule**.
2. In the **Create Snapshot Schedule** dialog box, set the **Schedule**, **Retention Policy**, and **Snapshot Type**, as shown below.

   Figure 33 XtremIO Create Snapshot Schedule wizard



3. Click **Submit**.
4. In the confirmation dialog box, click **OK**.

Viewing snapshots and schedules

On the **Snapshot Management** tab, you can view snapshots of virtual machines and datastores. On the **Scheduler Management** tab, you can view schedules for datastores that are based on XtremIO 4.0.x volumes.

Procedure

1. Select an XtremIO datastore or virtual machine from the inventory list.

2. Select **Manage** or **Configure** > **XtremIO Management**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

   - Details of all snapshots for the selected datastore or virtual machine are displayed on the **Snapshot Management** tab. Click a column header to sort the table.
   - Details of all snapshot schedules for the selected datastore are displayed on the **Scheduler Management** tab.

Managing snapshot schedules

You can suspend, resume, modify, or remove snapshot schedules for datastores based on an XtremIO 4.0.x volume.

Procedure

1. From the inventory list, select a datastore.
2. Select **Manage** or **Configure** > **XtremIO Management** > **Scheduler Management**.

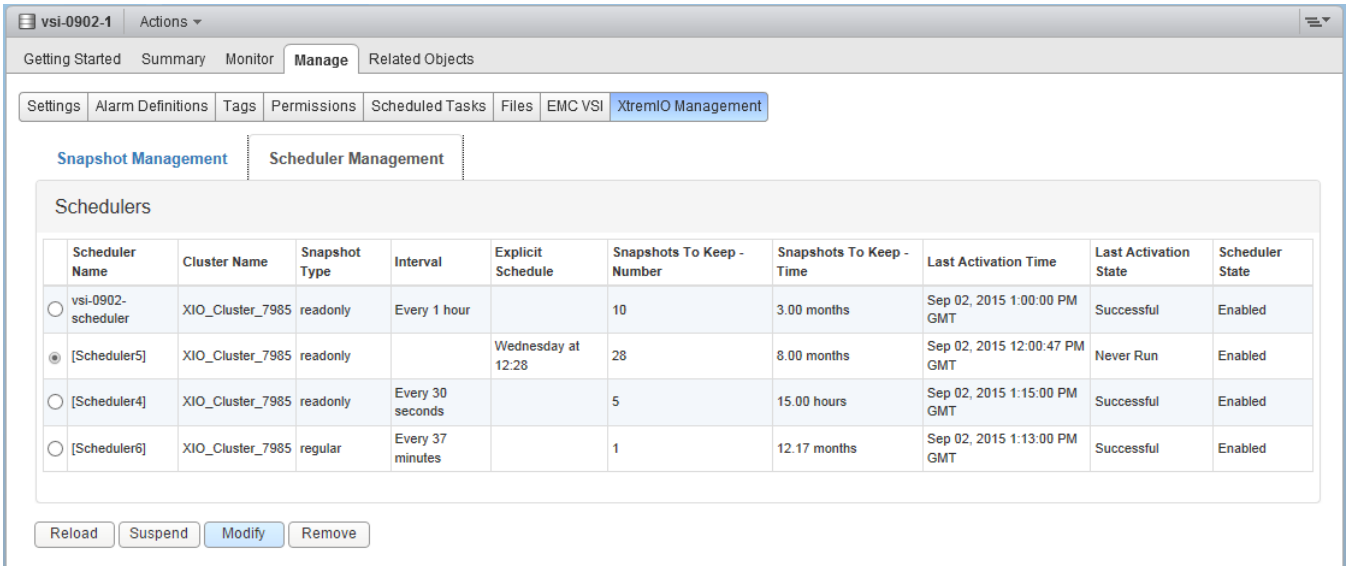
   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

3. Select the schedule that you want to change.

   The following figure shows the **Scheduler Management** tab for vSphere Web Client versions earlier than 6.5.

   Figure 34 Scheduler Management tab



4. Click the appropriate button for the action you want to perform:
   - **Reload**: Refreshes the data
   - **Suspend**: Suspends an active schedule

- **Resume**: Resumes a suspended schedule
- **Modify**: Opens the Snapshot Scheduler for modification
- **Remove**: Removes the schedule

5. In the confirmation dialog box, click **OK** or **Submit**.

Restoring virtual machines from an XtremIO snapshot

When a qualified virtual machine is selected, details of XtremIO snapshots, which are restorable points in time for virtual machines, are listed under **XtremIO Management**. These snapshots are on the XtremIO volume that is the backend LUN of the datastore hosting the selected virtual machine. You can use any of these snapshots to restore the selected virtual machine.

Note

- A *qualified* virtual machine has only one disk that is based on a datastore resident on an XtremIO volume.
- The available snapshots are ordered by virtual machine creation time. There is no specific vSphere API approach that can retrieve this property, therefore, the actual value calculated by VSI might not be exact in certain cases.

Procedure

1. Select a virtual machine from the inventory list.
2. Select **Manage** or **Configure** > **XtremIO Management** > **Snapshot Management**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

3. Select the snapshot to use for the virtual machine restore and click **Restore**.
4. In the confirmation dialog box, click **OK**.

Restoring a datastore from an XtremIO snapshot

You can restore a datastore from an XtremIO 4.0.x or later volume.

Procedure

1. From the inventory list, select a datastore based on an XtremIO 4.0.x or later volume.
2. Select **Manage** or **Configure** > **XtremIO Management** > **Snapshot Management**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

3. Select the snapshot to use for the restore and click **Restore**.
4. In the confirmation dialog box, click **OK**.

Mounting datastores from snapshots

Learn to mount datastores from snapshots.

Note

A snapshot can be mounted only once, but you can use these workarounds:

- To mount the data from a single snapshot to multiple datastores, take a snapshot on a mounted datastore and mount the new snapshot as a new datastore.
- Unmount a datastore but do not delete it. After unmounting, right click the inaccessible datastore and click **Mount Datastore**.

Procedure

1. Select a datastore in the inventory list.
2. Select **Manage** or **Configure** > **XtremIO Management** > **Snapshot Management**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

3. Select a snapshot to mount and click **Mount**.
4. In the **XtremIO Snapshot Mount Settings** dialog box, select a host on which to mount the snapshot and click **OK**.

   The snapshot is mounted. You can monitor the task status in **My Tasks** in the **Recent Tasks** panel.

Viewing mounted datastores

Learn how to view mounted datastores.

Procedure

1. Select **Home** > **vCenter** > **Hosts** and select the appropriate host.
2. Select **Related Objects** > **Datastores**.

CHAPTER 8

Managing Virtual Desktop Infrastructure

This chapter includes the following topics:

Integrating XtremIO clones with VDI

You can integrate XtremIO virtual machines with a VMware Horizon View or Citrix XenDesktop virtual desktop infrastructure (VDI).

Procedure

1. Use the Solutions Integration Service to create a new VDI service (see Installing the VDI web service proxy on page 32).
2. Register a connection broker by doing one of the following:
   - Use the Solutions Integration Service (see Managing connection brokers on page 34).
   - Use VSI (see Registering a connection broker with VSI on page 57).
3. Follow the steps in the appropriate section:
   - Integrating clones with VMware Horizon View in a new pool on page 102
   - Integrating clones with VMware Horizon View in an existing pool on page 103
   - Integrating clones with Citrix XenDesktop in a new or existing pool on page 103

Integrating clones with VMware Horizon View in a new pool

After you create native clones, use this procedure to integrate them with Horizon View in a new pool.

Procedure

1. Complete steps 1 through 4 in Creating native clones on XtremIO VMFS datastores on page 94.
2. Under **Connection Broker Information**, select **Integrate with VMware View**, and then click **Next**.
3. For **Pool Choice**, select a VMware View Server from the list. Select **Add VMs to a new Pool**, and click **Next**.
4. For **Pool Name**, type a unique ID, display name, and optional description in the boxes provided, and select an option for **Desktop Persistence**.
5. For **Pool Settings**, select the appropriate values for the following options:
   - **When VM is not is use**
   - **Automatic logoff after disconnect**
   - **Allow users to reset their desktop**
   - **Default display protocol**
   - **Adobe Flash quality**
   - **Adobe Flash throttling**
6. In **Ready to Complete**, review your selections, and then click **Finish**.

Integrating clones with VMware Horizon View in an existing pool

After you create native clones, use this procedure to integrate them with Horizon View in an existing pool.

Procedure

1. Complete the steps in Creating native clones on XtremIO VMFS datastores on page 94.
2. Under **Connection Broker Information**, select **Integrate with VMware View**, and then click **Next**.
3. For **Pool Choice**, select a VMware View Server from the list. select **Add VMs to an existing Pool**, select a pool from the list, and click **Next**.
4. For **Ready to Complete**, review your selections, and then click **Finish**.

Integrating clones with Citrix XenDesktop in a new or existing pool

After you create native clones, use this procedure to integrate them with Horizon View.

Note

Add XenDesktop to your trusted hosts list on the VDI proxy server before you register it in VSI or in the Solutions Integration Service, otherwise the registration fails. Use the following command: `Set-Item wsman:localhost\\client\\trustedhosts -value * -force`

Procedure

1. Complete steps 1 through 4 in Creating native clones on XtremIO VMFS datastores on page 94.
2. Under **Connection Broker Information**, select **Integrate with XenDesktop**, and then click **Next**.
3. For **DesktopGroup Choice**, provide the values for the following parameters:
   - **XenDesktop Controller**: Select the appropriate IP address from the list.
   - **New/Existing Machine Catalog**:
     - **Add VMs to a New Machine Catalog**: Opens the **Set up a New Machine Catalog** dialog box. Type a name and description for the new machine catalog.
     - **Add VMs to an Existing Machine Catalog**: Select from the list.
   - **New/Existing Desktop Group**:
     - **Add VMs to a New Desktop Group**: Opens the **Set up a New Desktop Group** dialog box. Type a name, display name, and description for the new desktop group.
     - **Add VMs to an Existing Desktop Group**: Select from the list.
4. In **Ready to Complete**, review your selections and click **Finish**.

CHAPTER 9

Managing AppSync Data Protection with VSI

This chapter includes the following topics:

About EMC Data Protection Services

The AppSync data protection feature enables VMware administrators to manage service plans and datastore copies, restore virtual machines, and view and modify the settings for AppSync server directly from the vSphere Web Client.

The versions of EMC AppSync that are supported with this release are listed in the EMC Simple Support Matrix.

Managing AppSync server credentials

You must have valid AppSync server credentials (an address and an account with adequate privileges) to manage AppSync from VSI. Using the Actions menu, you can register, edit, or unregister a data protection system.

Before you can use VSI to manage AppSync, you must either be assigned an AppSync system by an administrator using the Solutions Integration System GUI or you must register an AppSync system in vSphere.

Note

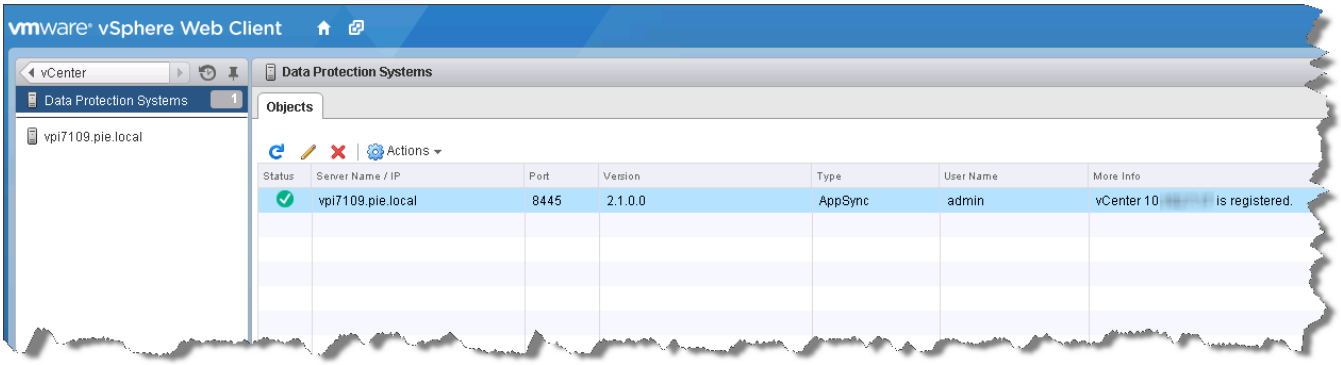
A user can be granted access to only one AppSync system and can register only one AppSync system on a vSphere Web Client.

Registering a new AppSync system

This procedure also registers the current vCenter to the AppSync server, if it is not already registered, and triggers the AppSync server to discover the current vCenter (or vCenters in the current linked-mode group) immediately.

The new item appears in the **Objects** tab under **Data Protection Systems**, as shown below. All vCenters are listed and the **Status** column indicates whether or not they are registered.

Figure 35 Viewing a registered AppSync server in vSphere



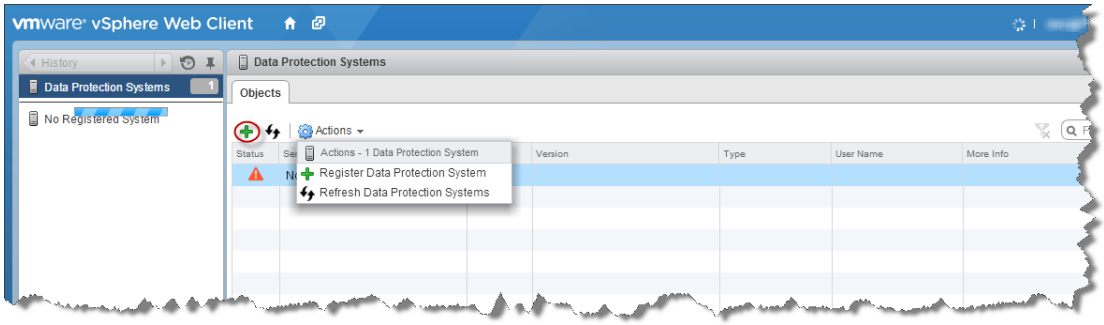
Procedure

1. Select **Home** > **vCenter Inventory Lists** > **EMC VSI** > **Data Protection Systems**.

   The **Data Protection Systems** list displays the data protection systems that are accessible from the Solutions Integration Service.

2. Click **Actions** > **Register Data Protection System** or click **+**, as shown below.

Figure 36 Adding a data protection system



3. In the **Register EMC Data Protection System** dialog box, provide the following information for the server on which you want to add AppSync:
   - **Protection System Type**: **AppSync (default)**
   - **FQDN or IP**: Type the fully qualified domain name (FQDN) or IP address of the AppSync server.

     Note

     The FQDN or IP address must be accessible from the Solutions Integration Service server or the connection will fail.

   - **Port**: 8445 is the default port.
   - **User name**: Type the username (a user account name that has the appropriate privileges) as configured on the AppSync server.
   - **Password**: Type the password.
   - **vCenter Name(s) / IP(s)**: The current vCenter or all vCenters in linked mode are listed.
4. Click **Test** to verify the credentials and test the connection to the AppSync server.

   The status of the test is displayed. If the test fails, correct the problem (invalid credentials, connection failure, and so forth) and try again.
5. If the test is successful, click **OK** to complete the registration.
6. Click **OK** in the confirmation dialog box.

Modifying AppSync credentials

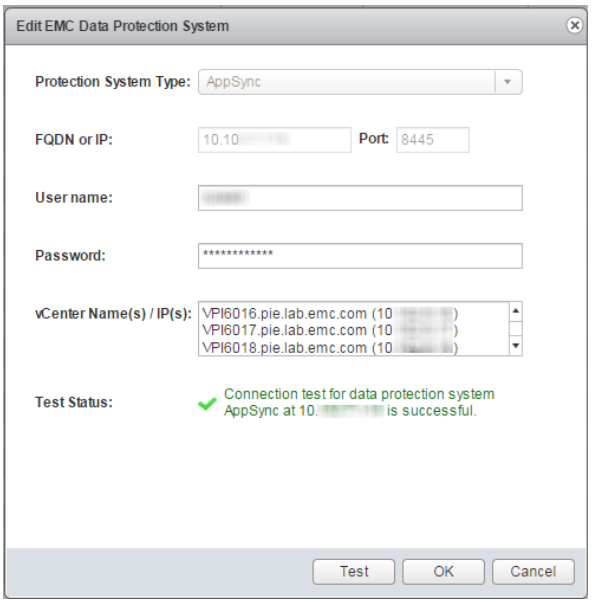
Using this procedure, you can edit the credentials or re-register the current vCenter that has been unregistered on the AppSync server.

Procedure

1. Select **Home** > **vCenter** > **Data Protection Systems** > **Actions** > **Edit Data Protection System**.

   The current data appears in the **EMC Protection System** dialog box, as shown below.

Figure 37 Viewing Data Protection System credentials



2. You can modify the user name and password by typing the new information in the appropriate text boxes.
3. Click **Test** to ensure that the information is valid, and then click **OK**.

Unregistering an AppSync system

Use this procedure to unregister an AppSync system that is no longer needed.

Procedure

1. Select **Home** > **vCenter** > **Data Protection Systems** and select an AppSync system from the list.
2. Click **Actions** > **Unregister Data Protection System**.
3. Click **Yes** to confirm that you want to unregister the system.

Results

The server credentials are unregistered from the current user.

Rediscovering the vCenter server

If a registered vCenter server becomes unavailable to AppSync, use this procedure to rediscover it.

Procedure

1. Select **Home** > **vCenter** > **Inventory Lists** > **vCenter Servers**.
2. Right-click the vCenter server and select **All EMC VSI Plugin Actions** > **AppSync vCenter Rediscover**.
3. Click **Yes** to run the discovery.
4. Click **Yes** in the confirmation dialog box.

Managing service plans

This section describes how to view, create, subscribe, unsubscribe, modify, and run service plans.

Viewing service plans

Use this procedure to view AppSync service plans.

Procedure

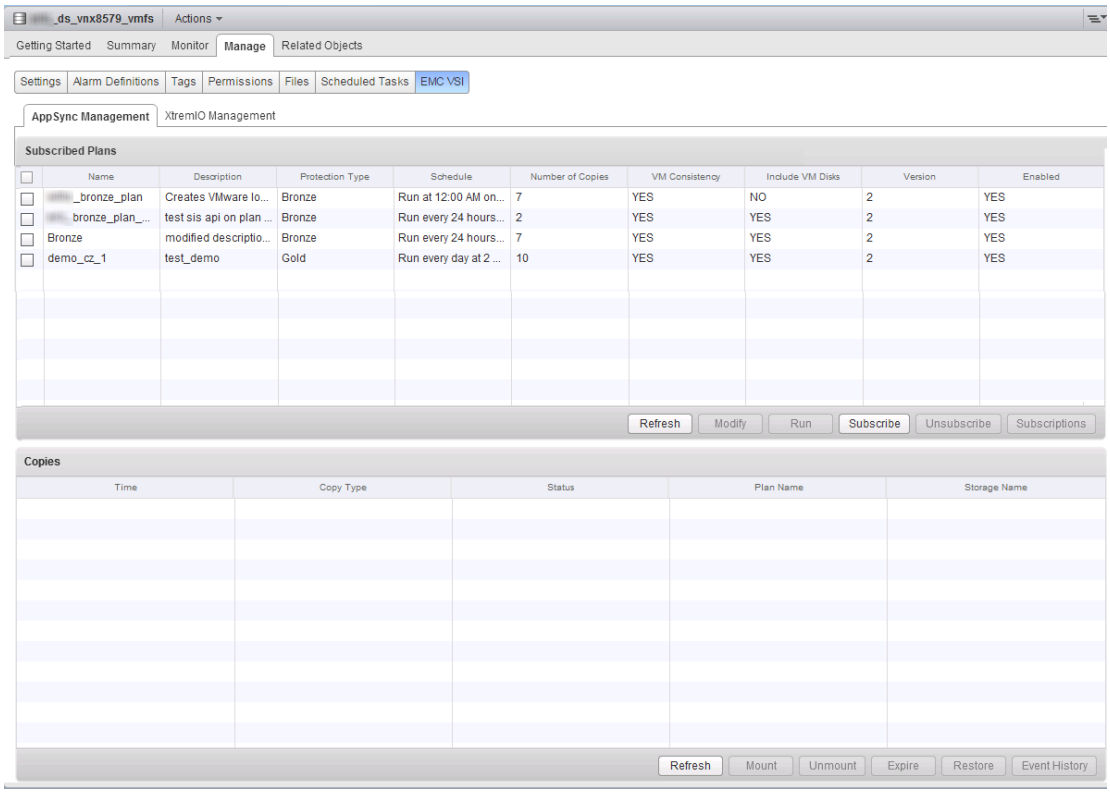
1. Select **Home** > **vCenter** > **Inventory Lists** > **Datastores** and select a datastore from the inventory list.
2. Click **Manage** or **Configure** > **EMC VSI** > **AppSync Management**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

   The currently subscribed plans for the selected datastore are listed with the details shown below.

Figure 38 Viewing AppSync service plans



Creating and subscribing to new service plans

This procedure enables you to create a new service plan based on an existing one and subscribe to it. You also have the option to configure the settings of the mount phase in the service plan when the wizard completes.

Procedure

1. Select **Home** > **vCenter** > **Inventory List** > **Datastores** and select a datastore from the inventory list.
2. Click **Manage** or **Configure** > **EMC VSI** > **AppSync Management**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

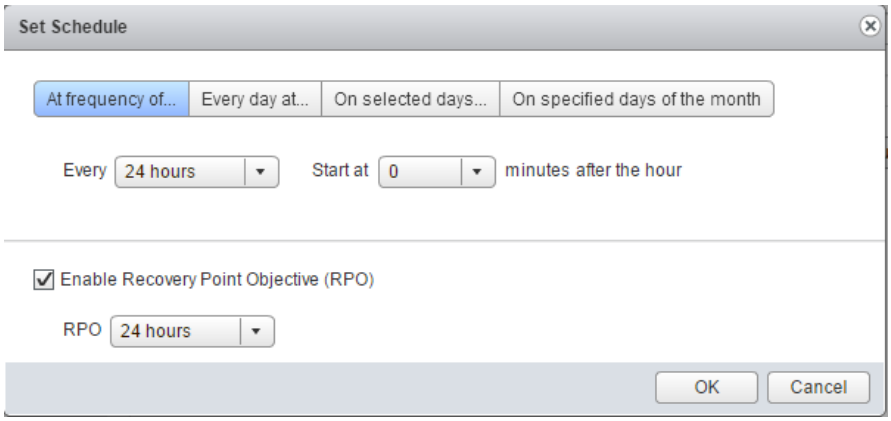
   The subscribed plans are listed.
3. Click **Subscribe**.
4. In the wizard, click **Create and Subscribe**.
5. Click **Next**.

   All service plans for VMware VMFS and NFS datastores in the registered AppSync server are listed.
6. In **Base of Service Plan**: From the **Available Service Plans** list, select the plan you want to use as a template, and then click **Next**.

   Ensure that the selected service plan is aligned with your datastore protection type:

   - For local protection, choose **Bronze**.
   - For remote protection, choose **Silver**.
   - For local and remote protection, choose **Gold** or choose **Bronze and Silver**.
7. In **Basic Settings**, provide the following information:
   - **Plan Name**: Type a unique name for the plan.
   - **Description** (optional): Type a description.
   - **Protection Type**: (Predefined according to the base service plan).
   - **Schedule**: Click **Set Schedule**.
     In the **Set Schedule** dialog box, click the appropriate buttons to modify the settings for the new schedule, as shown in the following figure, and then click **OK**.

Figure 39 Set Schedule dialog box



- **Copy Consistency**: Provide the following parameter values as required:

  Note

  Refer to the AppSync documentation for details about these parameters.

  - VM Consistent
  - Crash Consistent
  - Minimum Simultaneous VM Snapshots
  - Include VM Disks

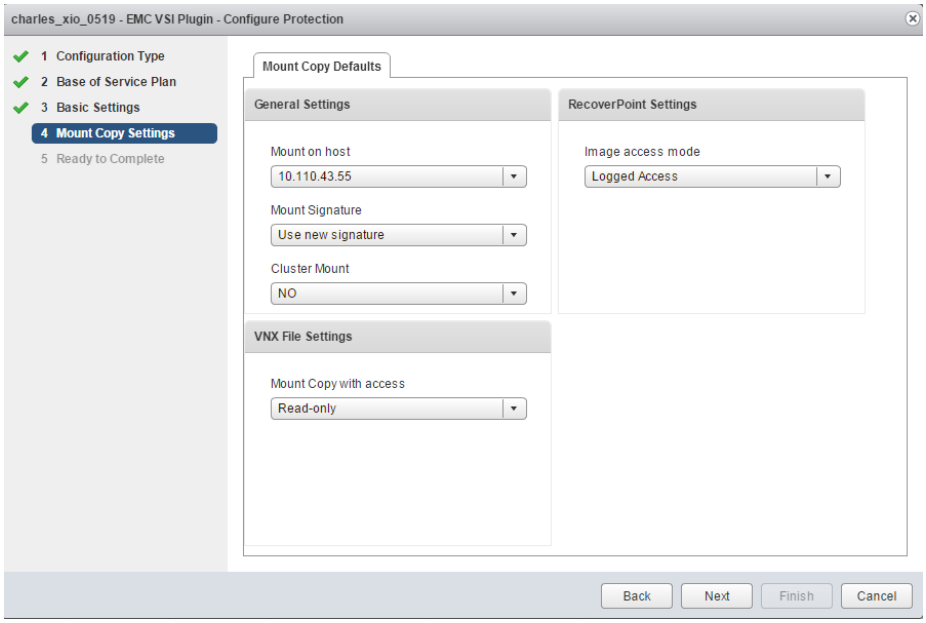
- Set the **Number of Copies**.
- In **Mount Settings**, optionally select **Unmount Previous Copy** and/or **Mount Copy** to perform these functions when the wizard completes.

8. Click **Next**.
9. If you selected **Mount Copy**, provide the settings for the following parameters, as shown in Figure 40 on page 112:
   - Under **General Settings**:
     - **Mount on host**: Select from the available hosts.
     - **Mount Signature**: Select **Use original signature** or **Use new signature**.
     - **Use new signature**: (applicable for VMware VMFS datastores only) Resignatures the VMFS volume on mounting.
     - **Cluster Mount**: Select **Yes** or **No**.
   - Under **RecoverPoint Settings** > **Image access mode**, select from the following options:
     - **Logged Access**: Use this mount option if the integrity check requires the scanning of large areas of the replicated volumes.
     - **Virtual Access with Roll**: Provides nearly instant access to the copy, but also updates the replicated volume in the background. When the replicated volumes are at the requested point in time, the RPA transparently switches to direct replica volume access, allowing heavy processing.
     - **Virtual Access**: Provides nearly instant access to the image but it is not intended for heavy processing.

When the selected base plan type is **Gold**, under **Copy to Mount**, select **local** or **remote** (not shown in Figure 40 on page 112).

- Under **VNX File Settings** (available only for VMware VNX File datastores) > **Mount Copy with access**, select **Read-only** or **Read-write**.
  When the selected base plan type is **Gold**, under **Copy to Mount**, select **local** or **remote** (not shown in in the following figure).

Figure 40 Selecting Mount Copy properties



10. Click **Next**.
11. Review your selections in the **Ready to Complete** dialog box, and then click **Finish**.
12. Click **OK** in the confirmation dialog box.
13. Click **Refresh** to view the new plan in the **Subscribed Plans** list.

Subscribing to existing service plans

Use this procedure to subscribe to existing plans.

Procedure

1. Select **Home** > **vCenter** > **Datastores** and select a datastore from the inventory list.
2. Click **Manage** or **Configure** > **EMC VSI** > **AppSync Management**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

   The subscribed plans are listed.
3. Click **Subscribe**.
4. In the wizard, select **Subscribe**, and then click **Next**.

   Existing Service Plan lists the service plans that are not currently subscribed.

5. Select a service plan to subscribe, and then click **Next**.
6. Review your selections in the **Ready to Complete** dialog box, and then click **Finish**.
7. Click **OK** in the confirmation dialog box.

Unsubscribing service plans

Use this procedure to unsubscribe service plans.

Procedure

1. Select **Home** > **vCenter** > **Datastores** and select a datastore from the inventory list.
2. Click **Manage** or **Configure** > **EMC VSI** > **AppSync Management**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

   The subscribed plans are listed.
3. Select the service plan to unsubscribe, and then click **Unsubscribe**.
4. In the confirmation dialog box, click **Yes** to unsubscribe the plan.

Running a service plan on demand

Use this procedure to run a service plan immediately.

Procedure

1. Select **Home** > **vCenter** > **Datastores** and select a datastore from the inventory list.
2. Click **Manage** or **Configure** > **EMC VSI** > **AppSync Management**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

   The subscribed plans are listed.
3. Select the service plan to run, and then click **Run**.
4. Click **Yes** to run the plan.
5. Click **OK** in the confirmation dialog box.
6. Click **Refresh** under the **Copies** table to verify that the new copy exists.

Modifying a service plan

Procedure

1. Select **Home** > **vCenter** > **Datastores** and select a datastore from the inventory list.
2. Click **Manage** or **Configure** > **EMC VSI** > **AppSync Management**.

Note

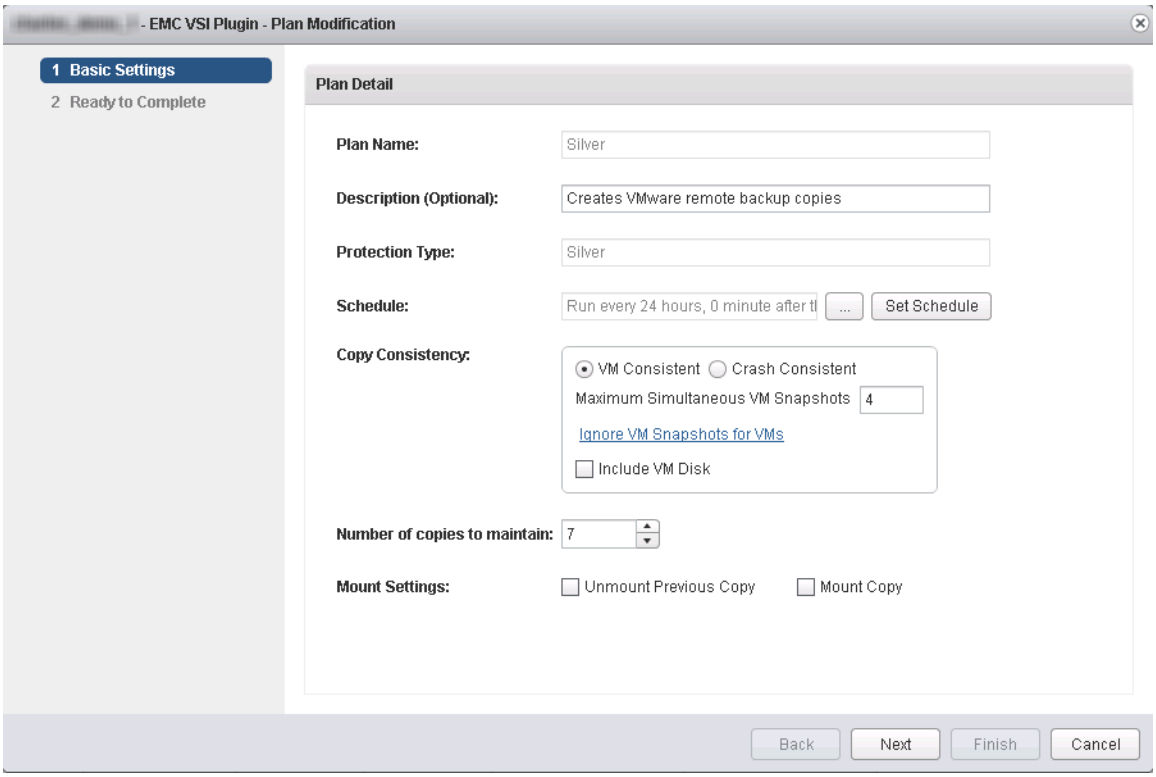
For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

The subscribed plans are listed.

3. Select the service plan to modify and click **Modify**.

   The **Plan Modification** wizard appears, as shown below.

Figure 41 Plan Modification wizard - Basic Settings



4. (Optional) In **Basic Settings**, modify the following parameters:
   - **Description**: Type a description.
   - Under **Schedule** click **Set Schedule**. In the **Set Schedule** dialog box, click the appropriate buttons to modify the settings for the new schedule, as shown in Figure 39 on page 111, and then click **OK**.
   - **Copy Consistency**: Provide the following parameter values as required.

     Note

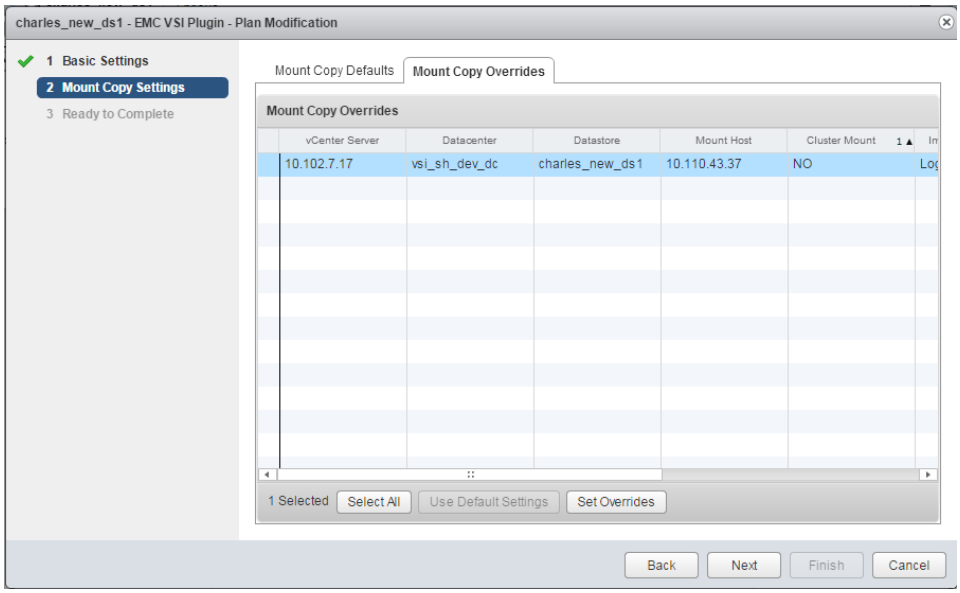
     Refer to the AppSync documentation for details about these parameters.

     - **VM Consistent**
     - **Crash Consistent**
     - **Minimum Simultaneous VM Snapshots**
     - **Ignore VM Snapshots for VMs**—Click this link to open the **Ignore VM Snapshot List** where you can select the snapshots to ignore.
     - **Include VM Disks**

- **Number of Copies**: Set the number of copies.
- **Mount Settings**: Select **Unmount Previous Copy** and/or **Mount Copy** to perform these functions when the wizard completes.

5. Click **Next**.
6. If you selected **Mount Copy**, you can modify the **Mount Copy Defaults** as described in step 9 on page 111.
7. Click **Mount Copy Overrides**, as shown below.

Figure 42 Mount Copy Overrides tab

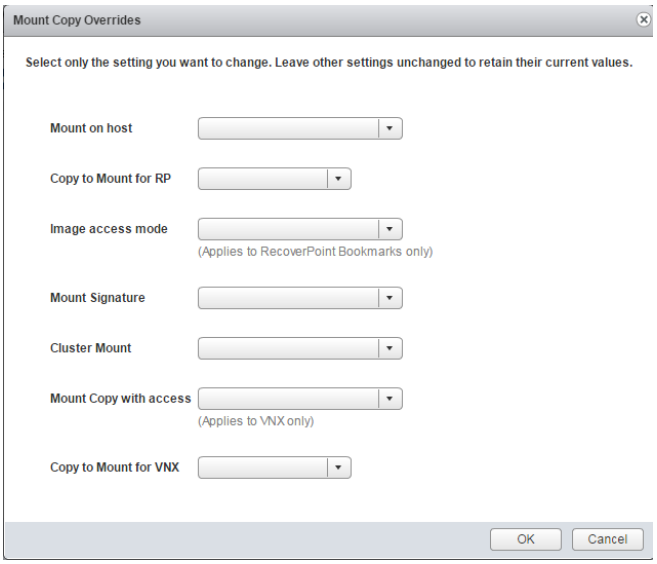


8. Select a protected datastore and click **Set Overrides.**
9. In the **Mount Copy Overrides** dialog box, shown below, select the required values for the settings you want to change.

Note

Refer to the AppSync documentation for details on these parameters.

Figure 43 Mount Copy Overrides dialog box



10. Click **OK**, and then click **Next**.
11. For **Ready to Complete**, review the settings, and then click **Finish**.

Managing AppSync datastore copies

You can view and manage datastore copies that are generated as a result of service plan subscriptions at the datastore level or datacenter level. Use the datacenter level to restore protected datastores that were previously deleted.

Restoring a previously-deleted datastore

From the datacenter level, you can restore a previously-deleted datastore that was protected by AppSync.

Procedure

1. Select **Home** > **Inventory Lists** and select a datacenter.
2. Click **Manage** or **Configure** > **EMC VSI** > **AppSync Management** > **Datastore Protection**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

3. In the **Protected Datastores** list, select the datastore to be restored and click **Get Copies**.

   The list appears in the **Copies** pane.
4. Select the copy that you want to use to restore the datastore and click **Restore**.

   The **Restore** wizard opens.
5. Complete the wizard using the guidance in Restoring datastore copies on page 118.

Viewing datastore copies

View datastore copies generated as a result of service plan subscriptions.

Procedure

1. Select **Home** > **vCenter** > **Datastores** and select a datastore from the inventory list.
2. Click **Manage** or **Configure** > **EMC VSI** > **AppSync Management**.

   Note

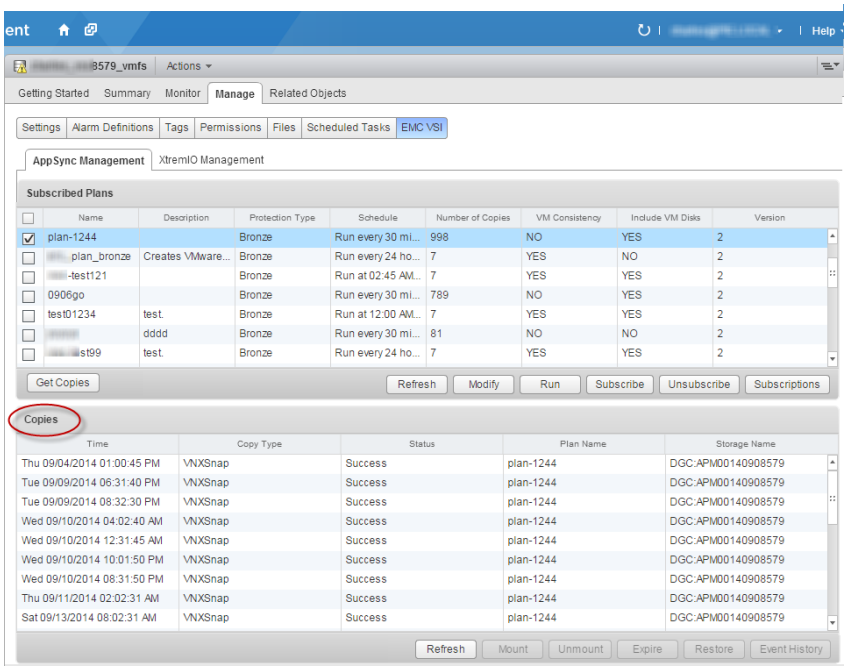
   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

3. Select one or more service plans, and then click **Get Copies**.

Results

The copies are displayed, as shown below.

Figure 44 Viewing AppSync datastore copies



Expiring datastore copies

Expire datastore copies generated as a result of service plan subscriptions.

Procedure

1. Select **Home** > **vCenter** > **Datastores** and select a datastore from the inventory list.
2. Click **Manage** or **Configure** > **EMC VSI** > **AppSync Management**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

3. Under **Copies**, select the copy to be expired.
4. Click **Expire**, and then click **OK** in the confirmation dialog box.

   Copies that were generated at the same time with the same copy type under the same plan are expired at the same time.

5. Click **Refresh** below the copies table.

Results

The expired copy is removed from the table.

Restoring datastore copies

Use this procedure to restore a datastore from a copy.

Procedure

1. Select **Home** > **vCenter** > **Datastores** and select a datastore from the inventory list.
2. Click **Manage** or **Configure** > **EMC VSI** > **AppSync Management**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

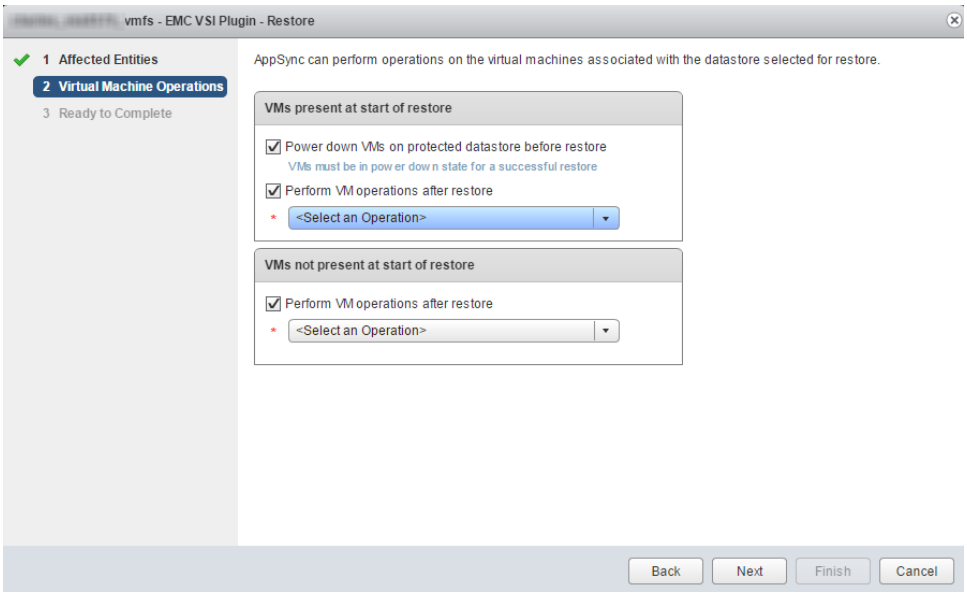
3. Select one or more service plans, and then select **Get Copies**.
4. Select a copy to restore, and then click **Restore**.

   The **Restore** wizard appears.
5. In **Select a copy** (displayed only if you selected a RecoverPoint copy):
   - **Continue to restore the selected datastore copy**: Select a copy to be restored.
   - **Select a point in time**: Select the **Day** and **Time**.
   - **Location**: Available if both local and remote copies exist.
6. Click **Next**.

   If the datastore that you selected is defined in a consistency group, a warning is displayed listing the affected datastores.
7. For **Affected Entities** (displayed only if at least one datastore is affected), select **I understand that the above items will be restored with my previous selections**.
8. Click **Next**.

   The wizard displays the **Virtual Machine Operations** options, as shown below.

Figure 45 Restore Datastore wizard - Virtual Machine Operations



9. For **Virtual Machine Operations**, select the appropriate operations for the following:
   - For **VMs present at start of restore**:
     - **Power down VMs on protected datastore before restore**: Powers off any virtual machines that are present before starting the restore operation.
     - **Perform VM operations after restore**: Select one of the following:
       - **Return VMs back to state found at start of restore**
       - **Register all virtual machines**
       - **Register and power up all virtual machines**
   - For **VMs not present at start of restore**, select one of the following options:
     - **Register all virtual machines**
     - **Register and power up all virtual machines**
10. Click **Next**.
11. In the **Ready to Complete** dialog box, review your selections, and then click **Finish**.
12. Click **OK** in the confirmation dialog box.

Mounting datastore copies

Use this procedure to mount AppSync datastore copies.

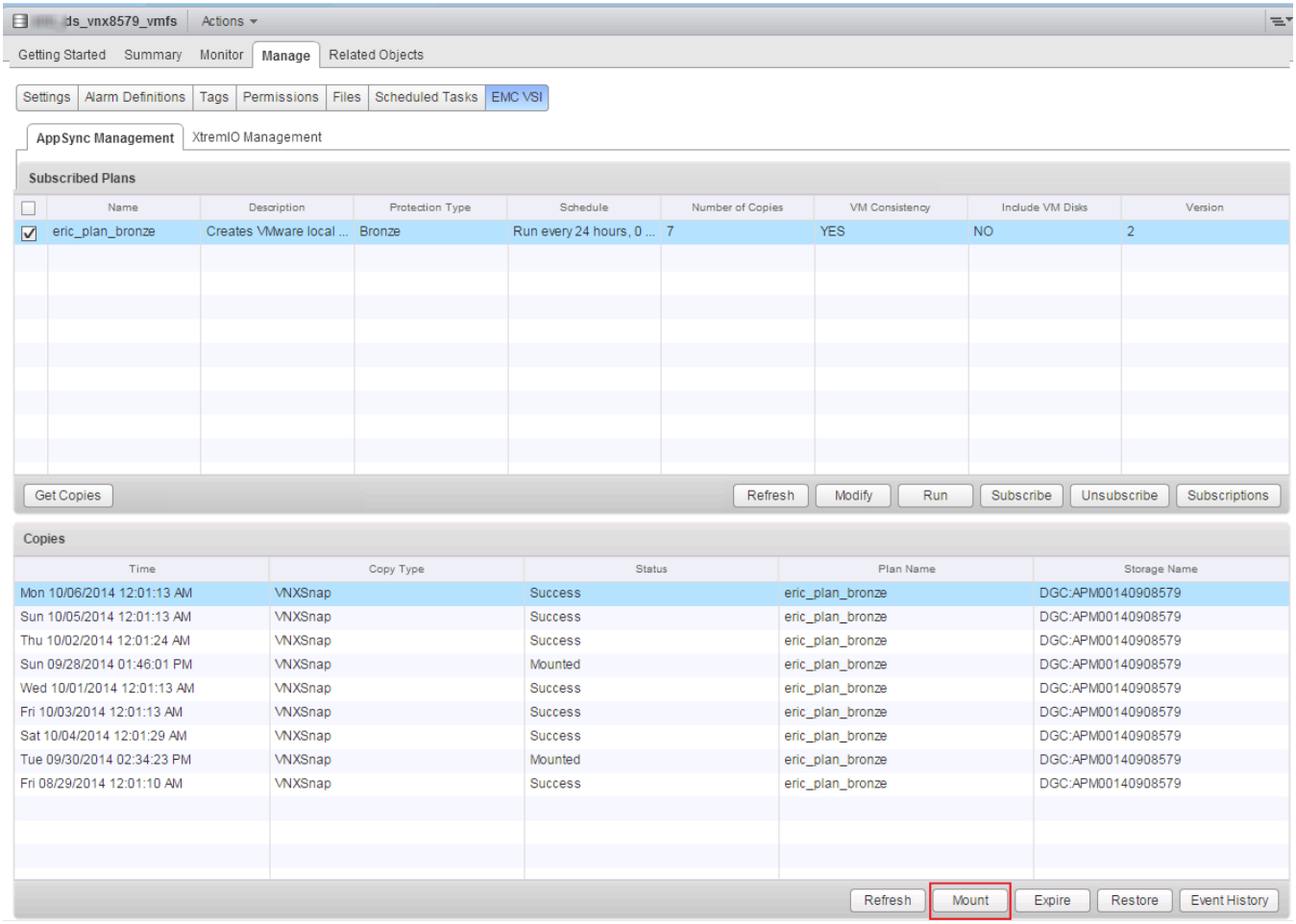
Procedure

1. Select **Home** > **vCenter** > **Inventory List** > **Datastores** and select a datastore.
2. Select **Manage** or **Configure** > **EMC VSI** > **AppSync Management**, as shown below.

Note

For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

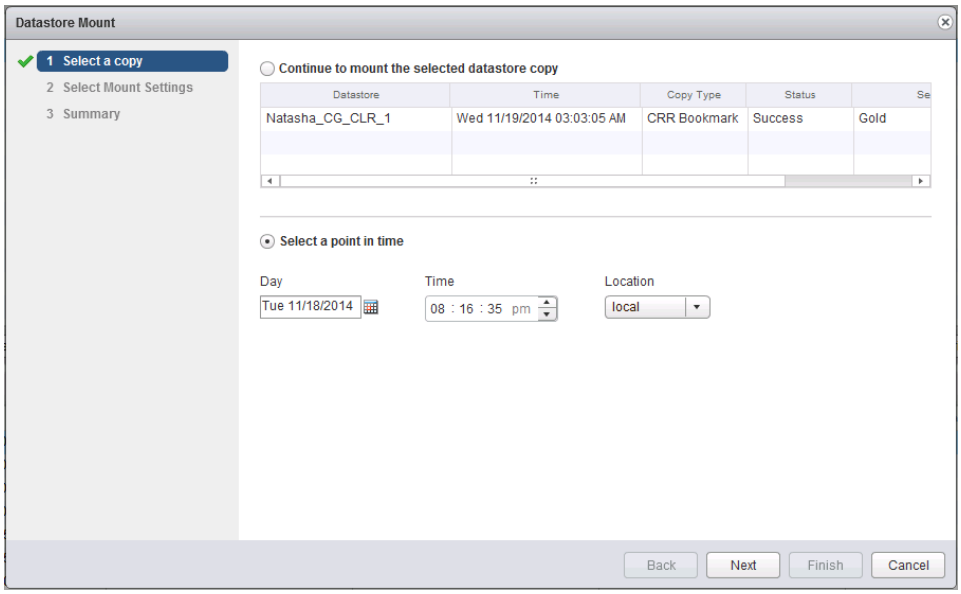
Figure 46 Mounting an AppSync datastore copy



3. Under **Subscribed Plans**, select a service plan and under **Copies**, select the copy that you want to mount.
4. Click **Mount**.

   The **Datastore Mount** wizard appears, as shown below.

Figure 47 Datastore Mount wizard



5. **Select a copy** is displayed only if you select a RecoverPoint copy. Depending on the copies available, you have the following options:
   - **Continue to mount the selected datastore copy**.
   - **Select a point in time**: Use the **Date** and **Time** selectors to select a point-in-time copy.
   - **Location**: Available if both local and remote copies exist.
6. **Mount Additional Copies** is displayed only if other datastore copies are available. Copies that were generated at the same time with the same copy type under the same plan are listed. Optionally, select additional datastore copies to restore.
7. In **Select Mount Settings**, provide the following parameters:
   - **Mount on host**: The IP address of the host on which to mount the datastore copy.
   - **Image access mode**: Enabled only when the datastore copy type is **RP**.
   - **Mount Copy with access**: Enabled only when the datastore copy type is **VNXFileSnap**.
   - **Mount Signature**: Enabled only when the datastore copy type is not **VNXFileSnap**.
   - **Cluster Mount**: Enabled only when the selected host in **Mount on host** is in a cluster.
8. In **Summary**, review your selections and click **Finish**.

Unmounting datastore copies

Use this procedure to unmount AppSync datastore copies.

Note

Copies that are mounted together must be unmounted together.

Procedure

1. Select **Home** > **vCenter Inventory List** > **Datastores** and select a datastore.
2. Select **Manage** or **Configure** > **EMCVSI** > **AppSync Management**, as shown in Figure 46 on page 120.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

3. Under **Subscribed Plans**, select a service plan and under **Copies**, select a copy for which the **Status** is **Mounted**.
4. Click **Unmount**.
5. Click **Yes** to confirm the unmount operation.
6. Click **OK** in the confirmation dialog box.

Viewing event history

Use this procedure to view AppSync copy history.

Procedure

1. Select **Home** > **vCenter** > **Datastores** and select a datastore from the inventory list.
2. Click **Manage** or **Configure** > **EMCVSI** > **AppSync Management**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

3. Under **Copies**, select a copy and click **Event History**.

   The time, type, and message are displayed for each event.
4. Click **OK** to close the **Event History** list.

Managing datacenter alerts

You can set up email notifications that are triggered by alerts generated at the AppSync server.

Procedure

1. Select **Home** > **vCenter** > **Inventory Lists**.
2. Select a datacenter and select **Manage** or **Configure** > **EMC AppSync Management** > **Settings.**

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

3. In the **Alert Subscription** dialog box, click **Subscribe**.
4. In the **Send Alerts** dialog box, enter one or more email addresses separated by commas.
5. Click **OK** in the confirmation dialog box.

6. Clicking **Unsubscribe** enables you to cancel the alerts for the subscribed email addresses.

Managing virtual machine copies

Using VSI, you can view and manage virtual machine copies at datacenter level and virtual machine level, as described in this section. At the datacenter level, you can restore previously deleted virtual machines that were protected by AppSync.

Restoring a previously-deleted virtual machine

From the datacenter level, you can restore a previously-deleted virtual machine that was protected by AppSync.

Procedure

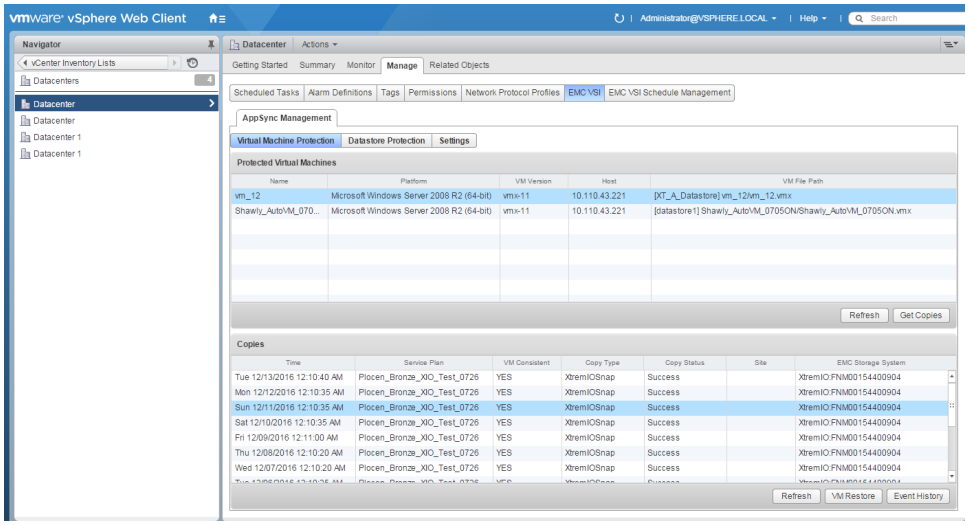
1. Select **Home** > **Inventory Lists** and select a datacenter.
2. Click **Manage** or **Configure** > **EMC VSI** > **AppSync Management** > **Virtual Machine Protection**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

   The list of protected virtual machines for the selected datacenter appears.
3. Select a protected virtual machine from the list and click **Get Copies**.
4. Select an item from the **Copies** list, as shown below.

Figure 48 Datacenter view of virtual machine copies



5. Optionally, click the associated button to perform any of the following operations for the selected copy:
   - **Refresh**: Refreshes the list.
   - **VM Restore**: Opens the **Granular VM Restore** Wizard. Restoring virtual machines on page 124 provides instructions for this operation.

- **Event History**: Opens the **Event History** dialog box, displaying the time, type, and message for each event.

Restoring virtual machines

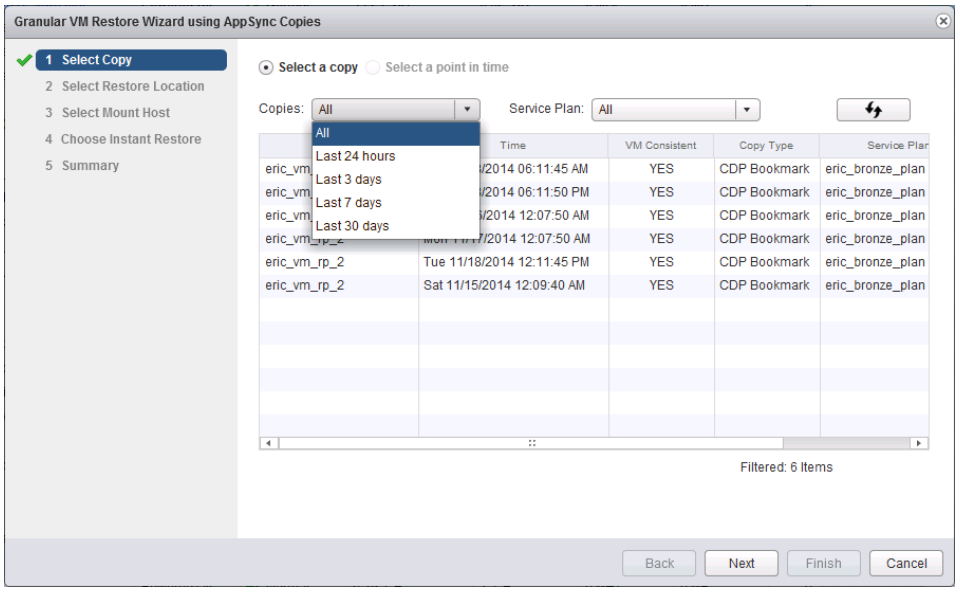
Use this procedure to restore virtual machines using AppSync copies.

Procedure

1. Select **Home** > **vCenter** > **Inventory Lists** > **Virtual Machines**.
2. Right-click the virtual machine you want to restore and select **All EMC VSI Plugin Actions** > **AppSync VM Restore**.

   The **Granular VM Restore Wizard** opens, as shown below.

   Figure 49 Restoring a virtual machine



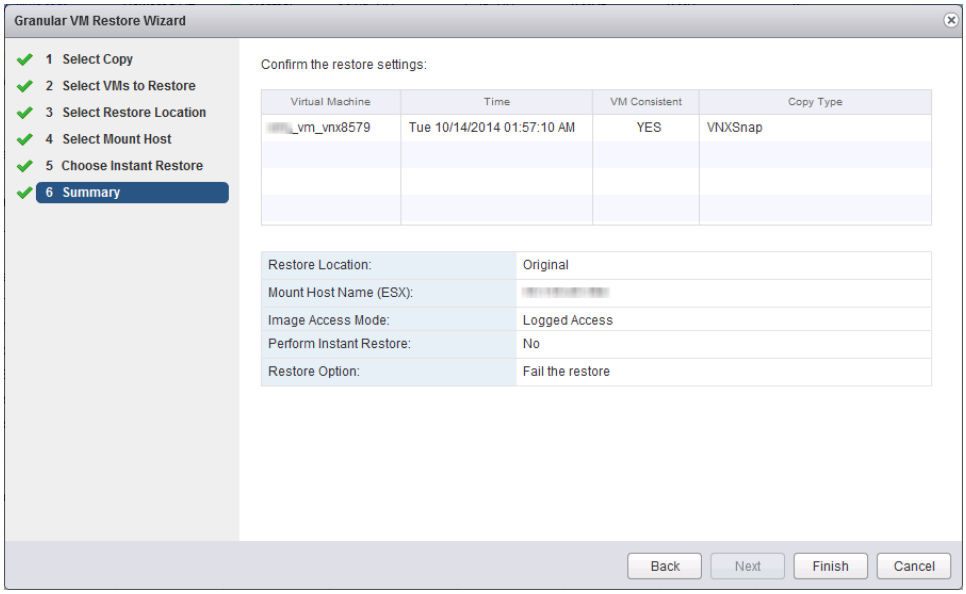
3. For **Select Copy**: Select one of the folloiwng:
   - **Select a Copy**:
     - Filter the available copies using the **Copies** list, which filters by time, or the **Service Plan** list.
     - Select a copy to restore from and click **Next**.
   - **Select a point in time**: (available only when the datastore is protected by RecoverPoint technology).
     - Select the **Day** and **Time**.
     - **Location**: Available if both local and remote copies exist.
4. If affected virtual machines are listed, for **Select VMs to Restore**, select one of the following:
   - **Continue to restore the selected virtual machine only**
   - **View and/or select the other VMs for restore**
     The **Other Virtual Machines** list is displayed. Optionally, select one or more virtual machines from the list.
5. Click **Next**.

6. For **Select Restore Location**, select **Original location** or **Alternate location**.
7. If you selected **Alternate location**, provide the following information from the lists:
   - **vCenter Server IP address**
   - **Datacenter**
   - **Host**
   - **Datastore**
8. Select one of the following actions for **If the VM being restored already exists in the restore location**:
   - **Fail the restore**
   - **Create a new virtual machine**
   - **Unregister the virtual machine**
   - **Delete from disk before performing restore**
   - **Delete from disk after performing restore**
9. Click **Next**.
10. For `Select Mount Host`:
    a. Select the **Mount host name (ESX)** from the list.
    b. If the copy is a RecoverPoint copy, select the **Image access mode**.
    c. Click **Next**.
11. For **Choose Instant Restore**, select whether you want to perform an instant restore.

    If there are multiple virtual machine copies to restore, optionally, change the default number (2) in **Maximum number of simultaneous virtual machines to be restored**, and then click **Next**.
12. Review the **Summary** information, and then click **Finish**.

    The following figure shows a sample **Summary** screen.

Figure 50 Reviewing the Summary information for restoring a virtual machine from a copy.



13. Click **OK** in the confirmation dialog box.

Required configurations and known issues

When restoring a virtual machine using AppSync, the following configurations are required:

- For EMC RecoverPoint, when the ESXi host that you selected to mount to in the **VM Restore** wizard is under a cluster containing several hosts, ensure that the replica LUN of the datastore on which the virtual machine resides is visible to all the hosts in the cluster.
- For VNX Snapshot, when the ESXi host that you selected to mount to in the **VM Restore** wizard is under a cluster containing several hosts, put all of these ESXi hosts into one Storage Group and add the replica volume to this consolidated storage group, otherwise the VM Restore operation fails.
- For VNX SnapSure™, when the ESXi host that you selected to mount to in the **VM Restore** wizard is in a cluster containing several hosts, ensure that the replica file system is visible to all of the ESXi hosts in the cluster.
- For VMAX, when the ESXi host that you selected to mount to in the **VM Restore** wizard is in a cluster containing several hosts, put all of these ESXi hosts in one masking view and add the replica volume to this consolidated masking view, otherwise the VM Restore operation fails.
- For VNX SnapSure and Replicator, the VM Restore operation fails because of an AppSync known issue.

CHAPTER 10

Managing RecoverPoint Data Protection with VSI

This chapter includes the following topics:

About EMC RecoverPoint

This release of VSI supports EMC RecoverPoint for data protection. The RecoverPoint integration in VSI enables VMware administrators to:

- View and configure consistency groups
- Modify the settings for RecoverPoint server directly from the vSphere Web Client
- View protection groups for a VMware SRM server that is using RecoverPoint for data protection

Refer to the EMC RecoverPoint documentation for a list of supported EMC storage systems.

Managing RecoverPoint systems

To manage RecoverPoint from VSI, you must have valid RecoverPoint server credentials (an address and an account with adequate privileges). Using the Actions menu, you can register, edit, or unregister a data protection system.

Before you can use VSI to manage RecoverPoint, you must either be assigned a RecoverPoint system by an administrator using the Solutions Integration System GUI or you must register a RecoverPoint system in vSphere.

Registering a new RecoverPoint system

You must register RecoverPoint before you can use it for data protection.

Procedure

1. Select **Home** > **vCenter** > **EMC VSI** > **Data Protection Systems**.

   The **Data Protection Systems** list displays the data protection systems that are accessible from the Solutions Integration Service.
2. Click **Add** (**+**).
3. In the **Register EMC Data Protection System** wizard, provide the following information for the server on which you want to add RecoverPoint:
   - **Protection System Type**: **RecoverPoint**
   - **FQDN or IP**: Type the fully qualified domain name (FQDN) or IP address of the RecoverPoint server.

     Note

     The FQDN or IP address must be accessible from the Solutions Integration Service server or the connection will fail.
   - **Port**: 7225 is the default port.
   - **User name**: Type the username (a user account name that has the appropriate privileges) as configured on the RecoverPoint server.
   - **Password**: Type the password.
4. Click **Test** to verify the credentials and test the connection to the RecoverPoint server.

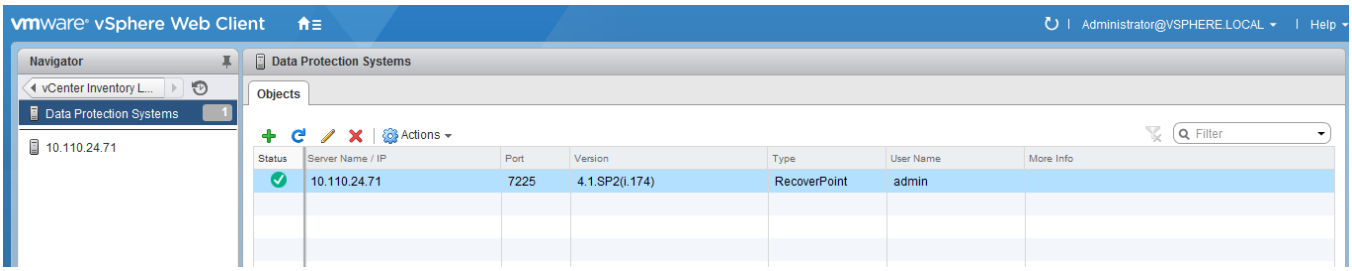
   The status of the test is displayed. If the test fails, correct the problem (invalid credentials, connection failure, and so forth) and try again.

5. If the test is successful, click **OK** to complete the registration.
6. Click **OK** in the confirmation dialog box.

Results

The new item appears in the **Objects** tab under **Data Protection Systems**, as shown below.

Figure 51 Viewing a registered RecoverPoint server in vSphere



Modifying RecoverPoint credentials

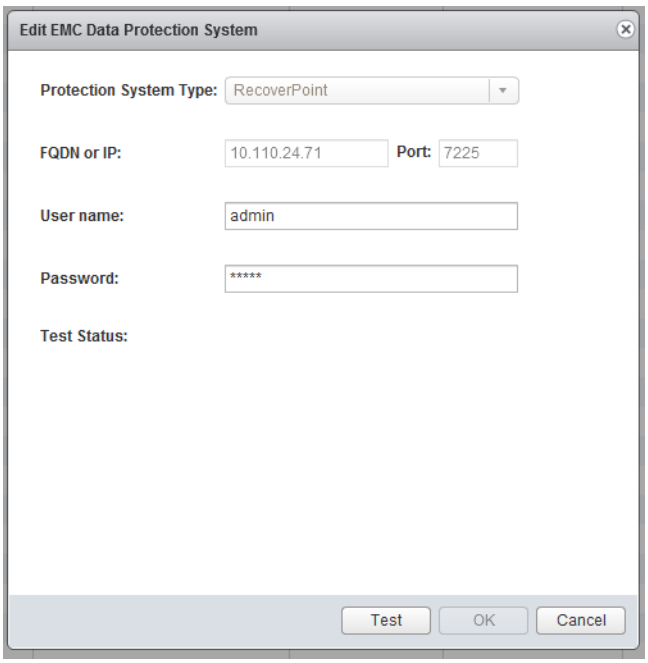
Using this procedure, you can edit the RecoverPoint server credentials.

Procedure

1. Select **Home** > **vCenter** > **Data Protection Systems** > **Actions** > **Edit Data Protection System**.

   The current data appears in the **EMC Protection System** dialog box, as shown below.

   Figure 52 Editing Data Protection System credentials



2. You can modify the user name and password by typing the new information in the appropriate text boxes.
3. Click **Test** to ensure that the information is valid, and then click **OK**.

Unregistering a RecoverPoint system

Use this procedure to unregister a RecoverPoint system.

Procedure

1. Select **Home** > **vCenter** > **Data Protection Systems** and select a RecoverPoint system from the list.
2. Click **Actions** > **Unregister Data Protection System**.
3. Click **Yes** to confirm that you want to unregister the system.

Results

The server credentials are unregistered from the current user.

Allowing Test Failover on RecoverPoint systems

Use this procedure to allow test failover on RecoverPoint systems.

Procedure

1. Select **Home** > **vCenter** > **Data Protection Systems** and select a RecoverPoint system from the list.
2. Click **Actions** > **Allow Test Failover**.
3. Click **OK** in the confirmation dialog boxes.

Configuring consistency groups

A consistency group is a logical entity used to configure protection policies, and set recovery point objective (RPO) and recovery time objective (RTO) policies according to specific resource allocation and prioritization. Use consistency groups to failover to, recover production from, and test any replica defined in the group.

Procedure

1. Select **Home** > **vCenter** > **Virtual Machines** and select a virtual machine.
2. Select **Management** > **EMC VSI** > **RecoverPoint Management** > **Consistency Groups**.

   The table lists the details of the corresponding consistency groups for the LUNs that are protected by RecoverPoint and are behind the data store in which the virtual machine resides. The consistency group is listed if the virtual machine has RDM disk that is protected by consistency groups in RecoverPoint.

   Note

   Only consistency groups that are configured to be externally managed by Site Recovery Manager are listed.

   From this window, you have the following options:

   - **Change policy**:

     Click > **Change Policy** > **Allow testing failover while clusters are disconnected** > **OK** > **OK**.
   - **Set expiry time**:

     Click **Set Expiry Time**, Set the date and time, and then click **OK**, **OK**.

- **Clear Point in Time and expiry time of a consistency group**:

  Click **Clear PiT**, click **OK** to confirm that you want to remove the selected snapshot from the consistency group, and click **OK**.
- **View details of consistency group snapshots**:

  Click **Snapshots** at the bottom of the **Consistency Groups** table.
- **Apply a Point in Time to a consistency group**:

  Select a consistency group, select the applicable snapshot, click **Apply** at the bottom of the **Snapshots** table, click **OK** to apply the selected snapshot to the selected consistency group, and click **OK**.
- **View protected virtual machines**:

  Select a consistency group, select **Virtual Machines** at the bottom of the **Consistency Groups** table.

Managing VMware vCenter Site Recovery Manager credentials

Use the following procedures to register or unregister vCenter Site Recovery Manager (SRM) credentials.

Registering a system

Only one Site Recovery Manager (SRM) server can be registered for each vCenter.

Before you begin

Ensure that you have registered the Solutions Integration Service using the vCenter password. Otherwise, registration of the SRM will fail.

Procedure

1. Select **Home** > **vCenter** > **EMC VSI** > **Data Protection Systems**.

   The data protection systems that are accessible from the Solutions Integration Service are listed.
2. Click **Add** (**+**).

   The **Register EMC Data Protection System** wizard appears.
3. For **Protection System Type** select **SRM**.
4. For **vCenter Name/IP**, select the protected vCenter to register.

   By default, the SRM server is installed on the same host as vCenter server. The default setting for the associated parameters will be the same as the vCenter credentials. Select the check box to customize the IP address and Port if SRM is installed on another host.
   The default port for SRM 5.8 is 9007; for SRM 6.0 the default is 9086.
5. Click **Test** to verify the credentials.
6. Click **OK**.
7. Click **OK** in the confirmation dialog box.

Unregistering a Site Recovery Manager system

Use this procedure to unregister a Site Recovery Manager system.

Procedure

1. Select **Home** > **vCenter** > **EMC VSI** > **Data Protection Systems**.

   The data protection systems that are accessible from the Solutions Integration Service are listed.

2. Select **Actions** > **Unregister Data Protection System**.
3. Click **Yes** to confirm the action.

Viewing protection groups and related consistency groups

A protection group can be viewed only on the production site. It cannot be viewed on the recovery site, even after test failover.

Procedure

1. Select **Home** > **vCenter** > **Virtual Machines** and select a virtual machine.

   Note

   The virtual machine must be protected by SRM systems that are registered in VSI.

2. Select **Manage** or **Configure** > **EMC VSI** > **Recover Point Management** > **Protection Groups**.

   Note

   For vSphere 6.5 Web Client, the **Manage** tab has been changed to **Configure**.

   The table lists details of the protection groups for the selected virtual machine.
3. Select a protection group to view related consistency groups.

CHAPTER 11

Managing XtremIO Native Replication with VSI

This chapter includes the following topics:

About XtremIO Native Replication

The XtremIO native replication feature enables VMware administrators to:

- View protected consistency groups
- View protected consistency group session details
- View available recovery points of a protected consistency group
- View all the scheduled tasks
- Set and clear the SRM recovery points of a consistency group.

View Protected Consistency Groups and Details

You can view the protected consistency groups and the details of the consistency groups, including session details and available recovery points.

Viewing Protected Consistency Groups

You can view the protected consistency groups associated with a virtual machine.

Procedure

1. Select **Home** > **VMs and Templates**.
2. Select the virtual machine.
3. Click **Configure** > **EMC VSI** > **XtremIO Native Replication**.

   The protected consistency groups are displayed.

View Protected Consistency Group Session Details

You can view session details of the protected consistency group associated with a virtual machine.

Procedure

1. Select **Home** > **VMs and Templates**.
2. Select the virtual machine.
3. Click **Configure** > **EMC VSI** > **XtremIO Native Replication**.

   The protected consistency groups are displayed.
4. Select the protected consistency group and to view the session details of the protected consistency group, click on **Session Details**.

View Available Recovery Points of a Protected Consistency Group

You can view all the available recovery points of a protected consistency group associated with a virtual machine.

Procedure

1. Select **Home** > **VMs and Templates**.
2. Select the virtual machine.
3. Click **Configure** > **EMC VSI** > **XtremIO Native Replication**.

   The protected consistency groups are displayed.

4. Select the protected consistency group and to view all the available recovery points, click **Available Recovery Points**.

   Note

   To update the available recovery points, click **Refresh**.

View Scheduled Tasks

You can view all the scheduled tasks of the expiring SRM recovery points.

Procedure

1. Select **Home** > **Hosts and Clusters**.
2. Select the Datacenter.
3. Click **Configure** > **EMC VSI Schedule Management**.

   All the scheduled tasks are displayed.

Set SRM Recovery Point

You can set the SRM recovery point of a protected consistency group associated with a virtual machine.

Procedure

1. Select **Home** > **VMs and Templates**.
2. Select the virtual machine.
3. Click **Configure** > **EMC VSI** > **XtremIO Native Replication**.

   The protected consistency groups are displayed.

4. Select the protected consistency group and to view all the available recovery points, click **Available Recovery Points**.

   Note

   To update the available recovery points, click **Refresh**.

5. Select any recovery point, click **Set as SRM Recovery Point**. A dialog box is displayed with the details of the selected consistency group and the recovery point. Click `OK` to set the SRM recovery point, or click `Cancel` to exit.

   Note

   The SRM recovery point expires in 3 hours and VSI creates a scheduled task to achieve this.

6. On clicking `OK`, a progress bar is displayed to show that the new recovery point is being set and once the process is done, a success dialog box is displayed. Click `OK`, the recovery point is set to the new one.

Clear SRM Recovery Point

You can clear the SRM recovery point of a protected consistency group associated with a virtual machine.

Procedure

1. Select **Home** > **VMs and Templates**.
2. Select the virtual machine.
3. Click **Configure** > **EMC VSI** > **XtremIO Native Replication**.

   The protected consistency groups are displayed.
4. Select the protected consistency group and to view all the available recovery points, click **Available Recovery Points**.

   Note

   To update the available recovery points, click **Refresh**.
5. Select a recovery point that is set to be the SRM recovery point, click **Clear SRM Recovery Point**. A dialog box is displayed with the details of the selected consistency group and the recovery point. To clear the SRM recovery point, Click `OK`, or click `Cancel` to exit.

   Note

   You can clear a SRM recovery point only after you set a recovery point.
6. On clicking `OK`, a progress bar is displayed to show that the selected recovery point is being cleared. Once the process is done, a success dialog box is displayed. Click `OK`, the recovery point is cleared.

CHAPTER 12

Troubleshooting

This chapter includes the following topics:

Known problems and limitations

Learn where to find known issues for this release of VSI.

A list of known problems and limitations for this product is documented in the current version of the *EMC VSI for VMware vSphere Web Client Release Notes*.

Viewing log files

Use the log files to help determine the cause of failures. You can view the VSI or Solutions Integration Service log files using either the vSphere Web Client or the vSphere Client for Windows.

Viewing log files with the Solutions Integration Service
Refer to Managing administrator tasks on page 27.

Viewing log files with the web client
Refer to Viewing log files with the web client on page 138.

Accessing log files when the VSI Plugin is not available
Refer to Accessing log files when the VSI plug-in is not available on page 139.

Viewing log files with the web client

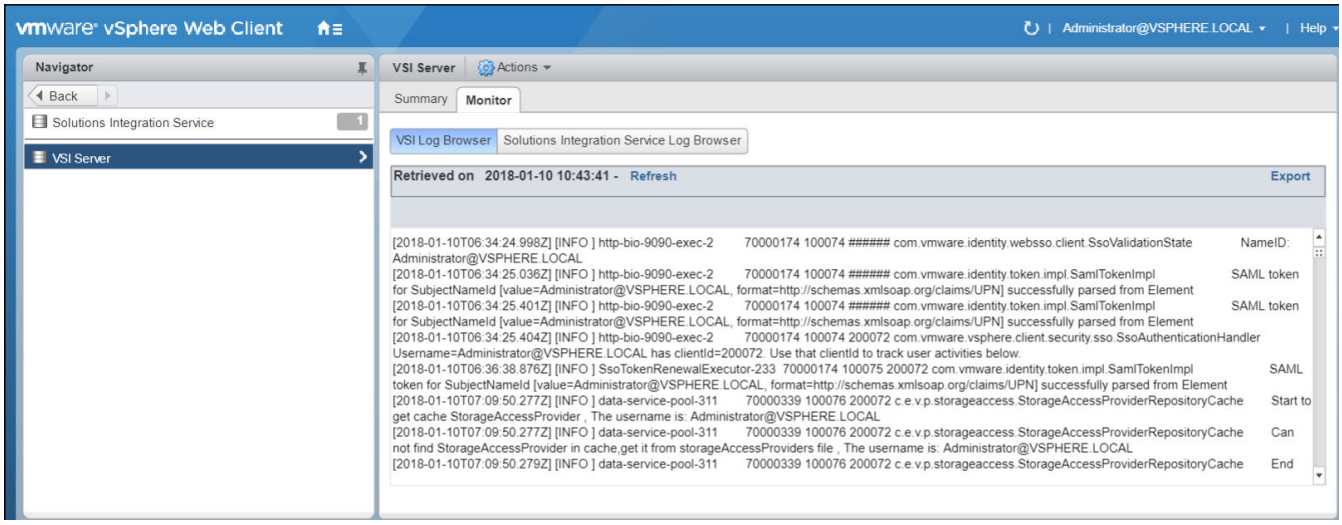
You can use the vSphere Web Client to view VSI log files.

Procedure

1. From the vSphere Web Client, select **Home** > **vCenter** > **EMC VSI** > **Solutions Integration Service.**
2. Click **VSI Server.**
3. Select **Monitor**.
4. Select **VSI log browser** or **Solutions Integration Service browser**.

   The following figure shows an example of the VSI Log Browser.

   Figure 53 Viewing VSI Log files



5. Click **Refresh** to view the log entries.

6. To save the log file, click **Export**.

Accessing log files when the VSI plug-in is not available

If the VSI plug-in is unavailable, use this procedure to access the log files for the EMC Solutions Integration Service and VSI plug-in.

Procedure

1. Log in to the vSphere Web Client.
2. Select **Home** > **Inventory Lists** > **Virtual Machines.**
3. Expand the navigation tree in the left pane, right-click the Solutions Integration Service virtual machine, and select **Open Console**.

   Note

   To release the cursor from the Console window, press Ctrl–Alt.

4. Click inside the console window and press Enter.
5. Enter the user ID and password (default: root/root).

   Note

   On first login, you must change the root password.

6. After you have logged in, type `cd` to change to the `/var/log/` folder.
7. Open the `vsi_usm.log` file and copy the contents.

   You can use any text editor, such as vi or emacs.

8. Using Remote Desktop, log in to the Windows virtual machine that is hosting the vSphere Web Client web service.
9. Open Windows Explorer and navigate to the `C:\ProgramData\VMware \vSphere Web Client\serviceability\logs\` folder.
10. Open the `vsphere_client_virgo.log` file.