Active System Manager Solution Guide
Active System 800

Version A01
April 2013

February 2013| Rev 1.0

Contents

Tables

Figures

1 Introduction to the Active System 800 Solution

Today, many IT organizations are missing deadlines or cannot respond fast enough to customer demands, have insufficient IT budgets, or have to manage trade-offs. In response, convergence in the data center has emerged as a trend in IT to address the growing needs for agility, efficiency, and quality. IT organizations are rapidly adopting converged infrastructure solutions to lower the cost of running critical workloads, enable faster infrastructure deployments, and drive simplicity and speed of management.

Below are some high-level solutions for the Dell™ Active System (AS) 800:

- **Rapid and Simple Scalability**—The Dell AS 800 is a part of the Active Infrastructure family, which includes fully pre-integrated converged infrastructure solutions. As one of the pre-integrated solutions offered, the Dell Active System 800 is a scalable blade server and storage infrastructure designed to support private cloud infrastructures. Able to add compute and storage capacity as needed in a non-disruptive manner, the Active System 800 offers many different configuration options for varying business conditions and sizes for a highly utilized IT infrastructure.
- **Quick and Easy Provisioning**—The Dell Active System 800 allows for more rapid application deployments through minimized design, test, procurement, integration, and configuration phases. One key feature of the Active System 800 is the Active System Manager, which offers streamlined, automated processes, as well as a quick response to dynamic business needs through template-based, modular infrastructure provisioning. This allows IT infrastructures to achieve higher efficiencies and more accurate delivery of IT services. A single IT generalist can manage most common tasks via the streamlined and automated processes delivered through the Active System Manager.
- **Automated and Efficient**—The Dell Active System 800 enables your data center to reach its maximum potential, and reduces the complexity and amount of time spent manually managing storage functions through automation for a more efficient and simplified management. This allows the Dell Active System 800 to support the efficient, agile delivery of applications and IT services made possible by a private cloud infrastructure, delivering true IT as a Service through private cloud benefits such as self-service portals and chargebacks.

This document describes the deployment and management of Active System Manager 7.0 on Active System 800 infrastructures.

1.1. Audience

IT administrators and IT managers — who have purchased, or are planning to purchase an Active System configuration—can use this document to understand the design elements, hardware and software components, and the overall architecture of the solution

1.2. Support

Contact Dell technical Support by visiting the Dell web site at www.dell.com/support/softwarecontacts.

1.3. Technical Documentation

The Dell Active System Manager documentation enables you to better understand your current Active Infrastructure, its deployment, and management software.

For this release, we recommend that you familiarize yourself with the following documentation:

- Active System 800 Spec Sheet
- Active System 800 VMware ESX 5.x Reference Architecture
- Active System Manager 7.0 User Guide
- Active System Manager 7.0 Web Interface User Guide

To access the latest Active System Manager documentation for Version 7.0:

1. Navigate to www.dell.com/support/manuals and click **Choose** from a list of all Dell products.
2. Click **Software, Monitors, Electronics & Peripherals** > **Software** > **Enterprise System Management** > **Dell Active System Manager v7.0**.

1.4. Overview

This section provides a high-level product overview of VMware vSphere, Dell PowerEdge blade servers, Dell PowerEdge M I/O Aggregator, Dell Force10 S4810 switch, Dell Force10 S55 switch, and Dell EqualLogic Storage.

VMware vSphere 5.1 Hypervisor
- vMotion, Storage vMotion
- VMware HA and DRS

Dell PowerEdge Blade Servers for Compute Cluster
- Energy efficient PowerEdge M1000e enclosure
- 12th generation M620 blade server
- Flex Address
- CMC and iKVM for enclosure management

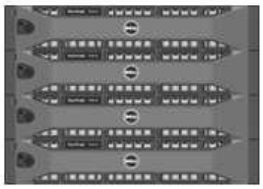
Dell PowerEdge M I/O Aggregator
- Highest Performance in a Blade Switch
- Highest Density in a Single Blade Switch
- Stackable for Simplified Management
- Scalability & Modular to Fit Your Business
- Support for converged networking with Data Center Bridging (DCB)

Dell PowerEdge Rack Servers for Management Cluster
- 12th generation R620 rack servers
- Concentrated computing power in 1U form factor
- Large memory and I/O capacity
- Powerful systems management with Dell iDRAC and Lifecycle Controller

Dell Force10 S4810 Switches for Converged Network
- High-density 48-port 10 GbE switch with four 40 GbE uplinks
- Ultra-low-latency, non-blocking, cut-through switch for line-rate L2 and L3 performance
- Integrated network automation and virtualization tools via the Open Automation Framework
- Support for converged networking with Data Center Bridging (DCB)

Dell Force10 S55 Switch for Management
- High-density 48-port 1/10 GbE scalable switch
- Low-latency, non-blocking switch for line-rate L2 and L3 performance
- Integrated network automation and virtualization tools via the Open Automation Framework

Dell EqualLogic Storage
- 10GbE iSCSI SAN arrays with SFP+ and 10GBase-T support
- Thin Provisioning and Storage Tiering
- Support for converged networking with Data Center Bridging (DCB)
- Integration with VMware



Integrated Management
- Dell Active System Manager
- VMware vCenter Server
- Dell Management plug-in for VMware vCenter
- Dell OpenManage Essentials
- Dell EqualLogic Virtual Storage Manager (VSM) for VMware
- Dell EqualLogic SAN HeadQuarters (HQ)
- Dell Repository Manager

Cloud Enablement
- VMware vCloud Connector for Dell vCloud connectivity

Table 1 lists the Active System Manager solution for the Active System 800-supported components.

Table 1. Active System 800-Supported Components

Component	Details
VMware vSphere 5.1 Hypervisor	Up to 2x Dell PowerEdge M1000e chassis with up to 32x Dell PowerEdge M620 Blade Servers and embedded VMware vSphere 5.1
Converged Fabric Switch	• 2xDell Force10 S4810 • 2x Dell PowerEdge M I/O Aggregator in each Dell • PowerEdge M1000e chassis
Storage	• Up to 8x Dell EqualLogic PS6110 series arrays
Management Infrastructure	• 2x Dell PowerEdge R620 servers with embedded VMware vSphere 5.1 hosting management VMs. • 1x Dell Force10 S55 used as a 1Gb out-of-band management switch
Management components hosted in the management infrastructure	• Dell Active System Manager • VMware vCenter Server • Dell Management Plug-in for VMware vCenter • Dell OpenManage Essentials • Dell EqualLogic Virtual Storage Manager (VSM) for VMware • Dell EqualLogic SAN Headquarters (HQ) • VMware vCloud Connector • Dell Repository Manager

1.5. Active System 800-Supported Configurations

Table 2 lists the Active System Manager solution for the Active System 800-supported configurations.

Table 2. Active System 800-Supported Configurations

Configuration	Support
M1000e chassis and supported blade types (M620)	**Support firmware images as per the Active System Manager solution for** Active System 800
Dell Force10 Top-of-Rack (ToR) S4810 switches	Supported FTOS and base configuration will be packaged in the virtual appliance. The base configuration should be updated for management IP and virtual LAN (VLAN) per data center deployment need.
Dell EqualLogic PS6110 Storage Array	Supported firmware versions will be packaged in the virtual appliance.
VMware vCenter 5.1 for virtual machine (VM) workloads	Supported ESXi 5.1 image will be bundled in the virtual appliance
ESXi 5.1 installation support on blade servers	

1.6. Deployment Options

The Active System Manager solution for Active System 800 is packaged as a virtual appliance and is made available for VMware vCenter 5.1 and the Windows Server 2012 System Center Virtual Machine Manager (SCVMM); see Table 3:

- Open Virtualization Format (OVF) for VMware—The disk format is VMware virtual machine disk (VMDK).
- Hyper-V virtualization environment—The disk format is virtual hard disk (VHD) for Hyper-V.

Table 3. Deployment Options

Virtual Appliance Filenames	Platform
Dell-ActiveSystemManager-7.0.0.xyztp_VMware.zip	VMware vCenter 5.1
Dell-ActiveSystemManager-7.0.0.xyztp_Microsoft.zip	Microsoft Server 2012 with Hyper-V

1.7. Deployment Prerequisites

Before using the Active System Manager solution for end-to-end provisioning of Active System 800 components, ensure that the prerequisites listed in Table 4 are in place.

Table 4. Deployment Prerequisites

Specification	Prerequisite
Active System 800 **units connected per the** Active System 800 ***Reference Architecture and Design Guidelines***	
Management server is configured per the Active System 800 ***Reference Architecture and Design Guidelines***	
Firmware and BIOS Requirements	All equipment must be configured with firmware versions as listed in section Appendix C—Firmware and Software Base Lineup
For the Active System 800 **chassis, blade server, and IO aggregators:**	• CMC for M1000e chassis is configured and has the management IP address and login credentials assigned • Server iDRAC and IOA is configured and has the management IP address and login credentials assigned using CMC Management interface. The username (**root**) and password for CMC, IOA, and iDRAC must be identical.
Force10 S4810 switches (Top-of-Rack [ToR])	• The management IP address is configured for the ToR switches. • The A800 base configuration is applied on both switches. • VLANs are created on the switches per the Active System 800 deployment specification. • The virtual machine (VM) traffic VLANs will be created dynamically by Active System Manager.
EqualLogic Storage Array	• The group IP and management IP are configured for Storage Array. • All storage array members are added to the group.
VMware vCenter 5.1	• vCenter 5.1 is configured and accessible via the management and hypervisor management network. • Appropriate licenses are deployed on the vCenter.
PXE Setup for server deployment	Details for deploying PXE Server is listed in section Appendix G—PXE Setup Requirements. This setup is needed for PXE boot of the servers only.

2 Active System Manager Deployment

2.1 Deploying OVF

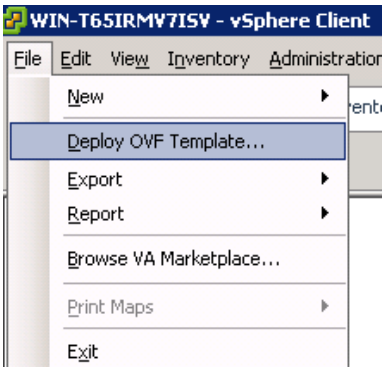
The Active System Manager Open Virtualization Format (OVF) can be imported on to an ESXi host using the VMware OVF import process. When booted, the Active System Manager VM get its IP address from an existing DHCP server. If the DHCP server is not configured, then assign the IP address manually to the appliance.

2.1.1 Importing OVF from the vSphere Client

To import OVF from the vSphere Client, perform the following steps:

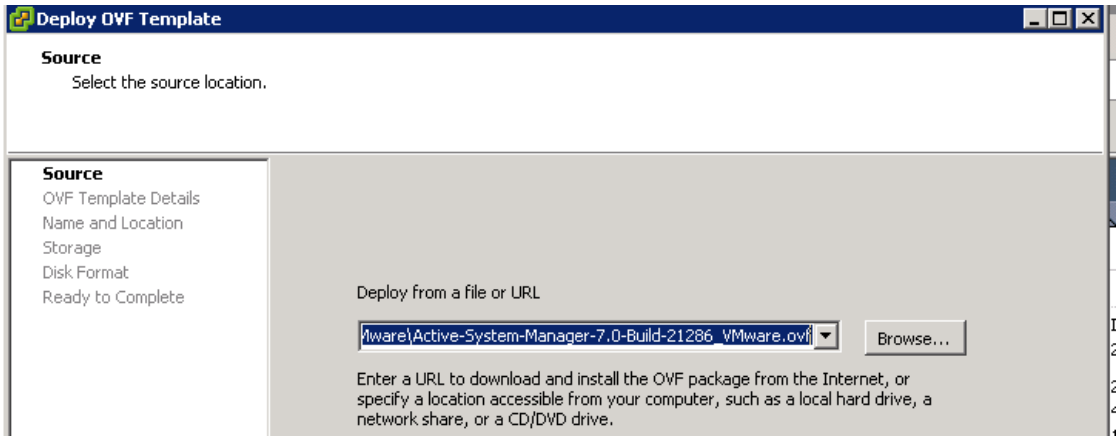
1. On the vSphere Client menu, click **File** > **Deploy OVF Template**.

   Figure 1. Deploy OVF Template Menu Option

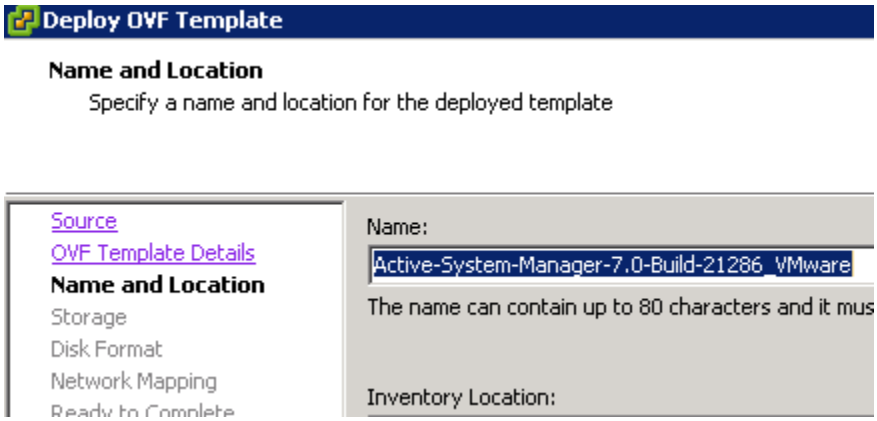
2. Browse the OVF file and select **Next**.

   Figure 2. Deploy OVF Template Source File Location

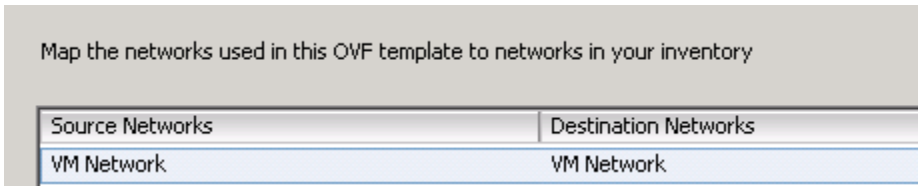
3. In the **Name** field, enter the VM name and click **Next**.

Figure 3. Name and Location of the Deployed Template



4. Select the appropriate datastore name where the VM must be hosted.
5. Select the disk format. (Thin provisioning is supported and recommended.)
6. Select the network name. The VM must be mapped to the Hypervisor Management Network. All networks (for example, OOB, Hypervisor Management, vMotion, iSCSI, and VM workloads) are expected to be accessible from the appliance.

Figure 4. Mapping the Networks Used in the OVF Template



7. Table 5 lists the necessary key access credentials to use.

Table 5. Key Access Credentials

VM Access Credentials	Username/Password
Active System Manager server installation login	**delladmin/delladmin**
Active System Manager server root	**root/Dell@123**
Active System Manager application	**admin/admin**

2.2 Deploying VHD

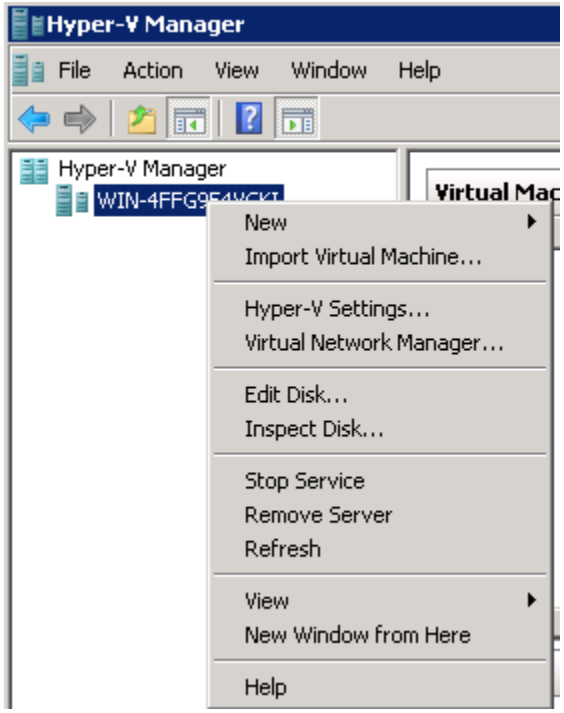
The Active System Manager Open Virtualization Format (VHD) can be imported on to a Hyper-V host using the **Hyper-V Manager** > **Import Virtual Machine** option. When booted, the Active System Manager VM gets its IP address from an existing DHCP server. If a DHCP server is not configured, manually assign the IP address to the appliance.

2.2.1. Importing the VHD Using Hyper-V Manager

To import the VHD from the Hyper-V Manager, perform the following steps:

1. On the Hyper-V Manager dialog box, select a host, right-click and select **Import Virtual Machine**.

   Figure 5. Hyper-V Manager > Import Virtual Machine



2. Click **Browse**, navigate to the location where the VDH is available in the extracted format, and click **Import**.

Figure 6. Import Virtual Machine

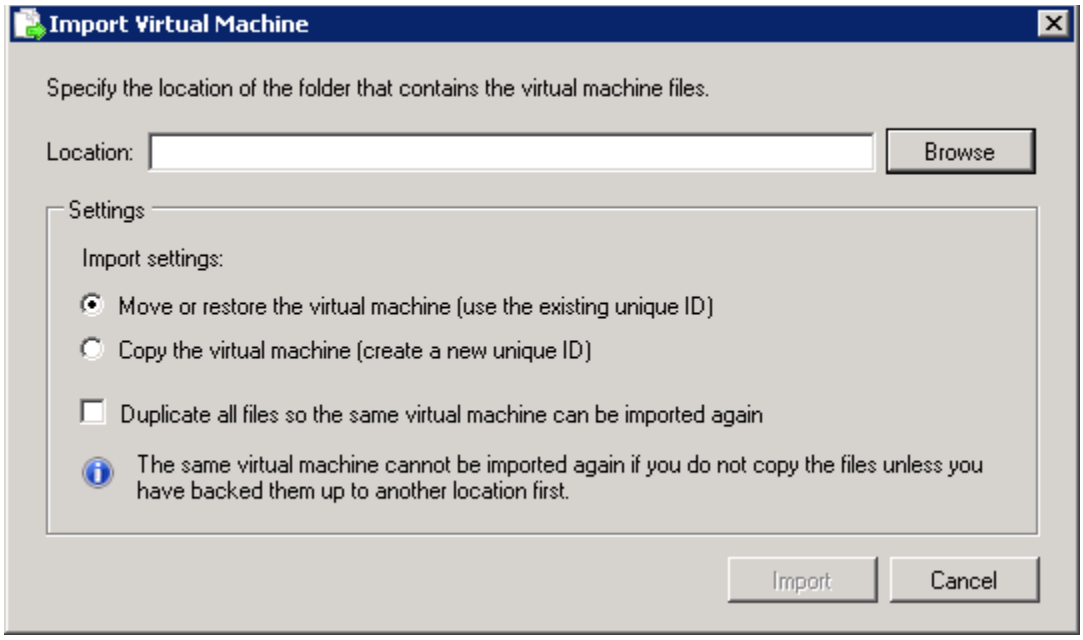
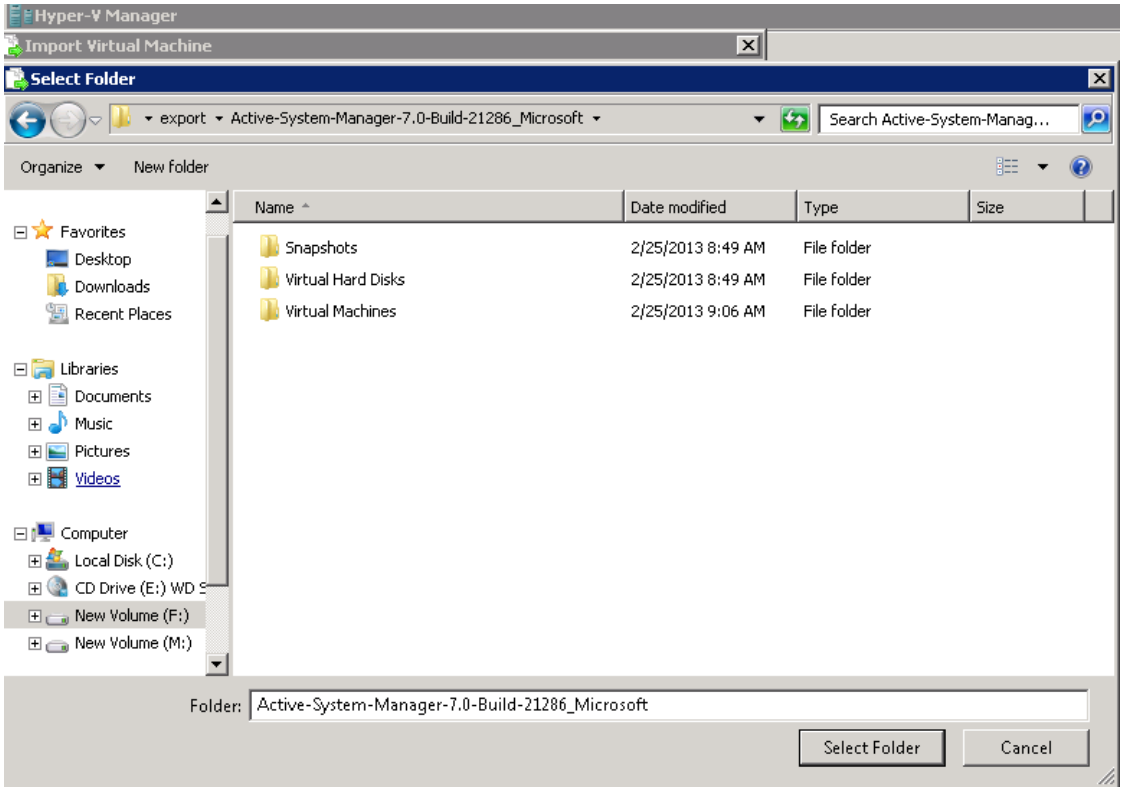
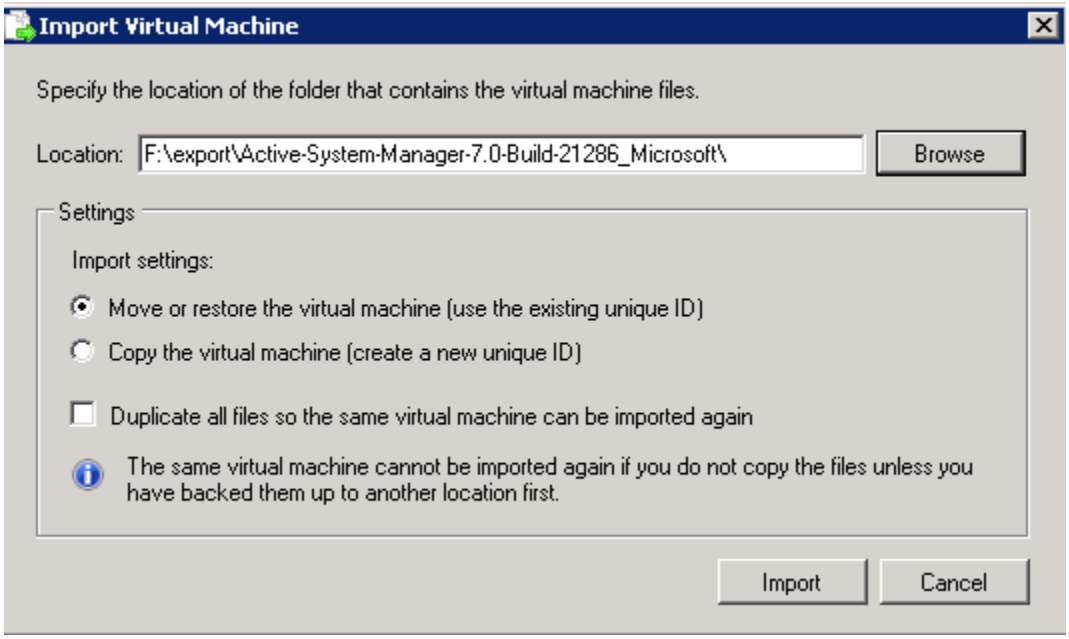


Figure 7. Select Folder Option



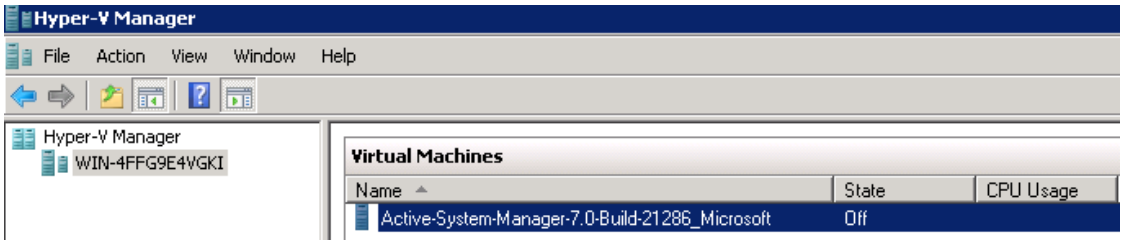
3. Select a folder to house the VHD and click **Select Folder**.

Figure 8. Import Settings



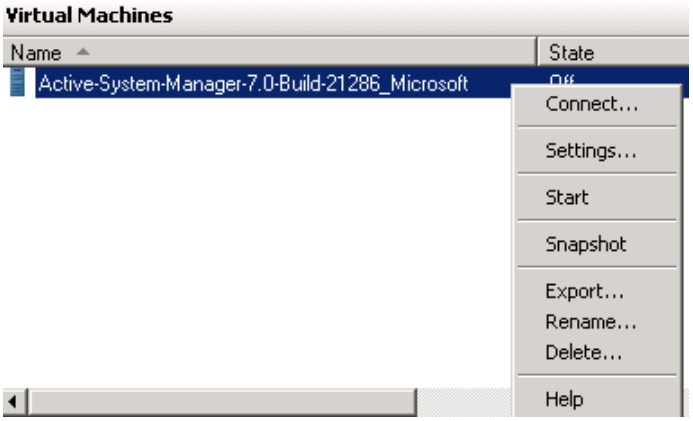
4. Verify the location that contains the virtual machine files and click **Import**.

Figure 9. Newly-Imported VM Displayed on the Hyper-V Manager



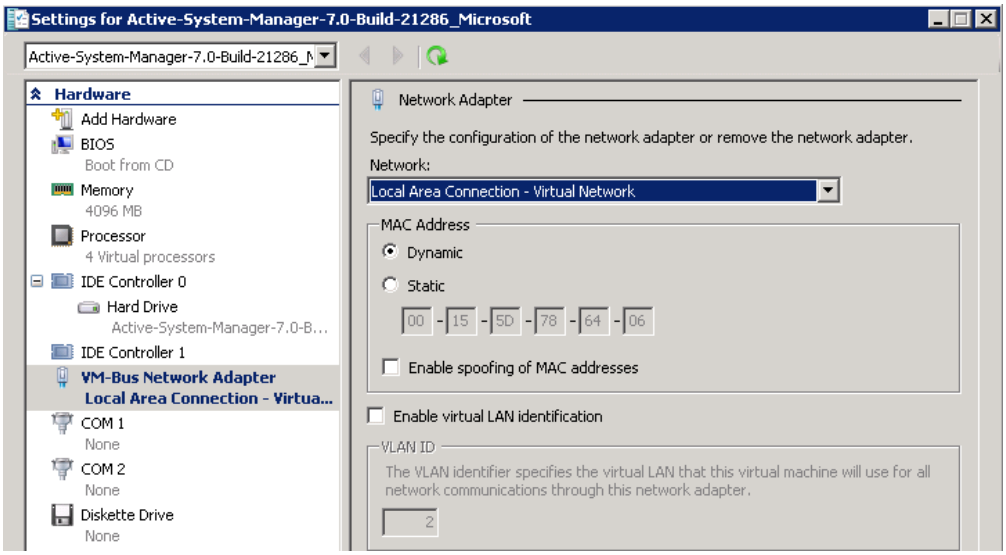
5. Select the VM and click **Start** to power on the VM.

Figure 10. Starting the VM



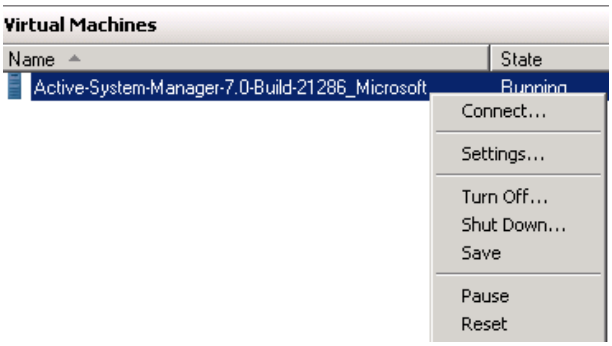
6. Select the network. The VM should be mapped to the Hypervisor Management Network. All the networks (for example, OOB, Hypervisor Management, vMotion, iSCSI, and VM workloads) are expected to be accessible from the appliance.

Figure 11. Selecting the Network



7. Click **Connect** to launch the console.

Figure 12. Connecting to Launch the Console

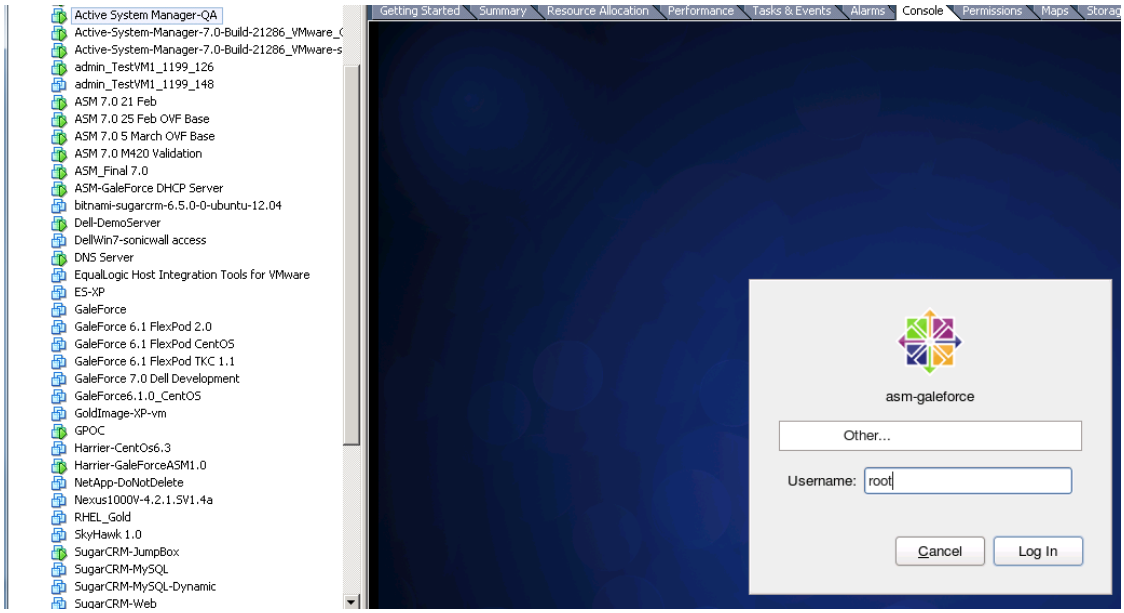


2.3 Assigning IP Address to the Active System Manager

To assign the IP Address to the Active System Manager appliance, perform the following steps:

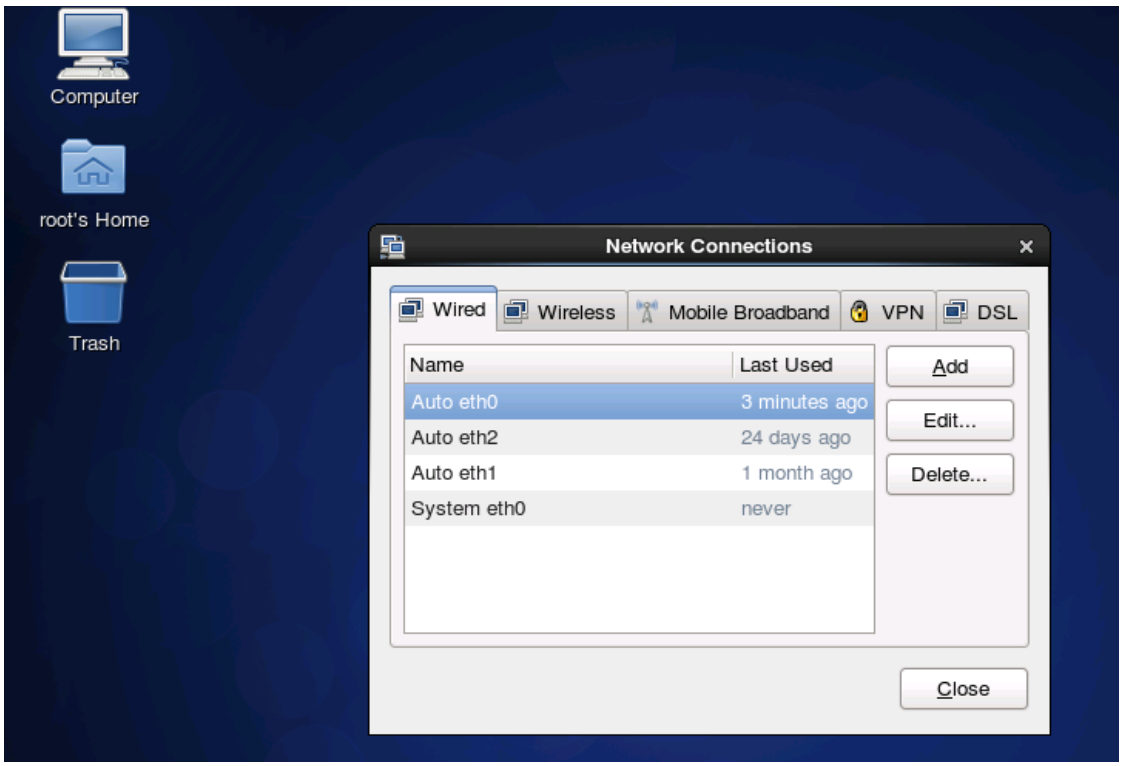
1. On the vSphere or Hyper-V Manager client, select the deployed **Active System Manager** appliance and open its console.

Figure 13. Logging In to the Active System Manager



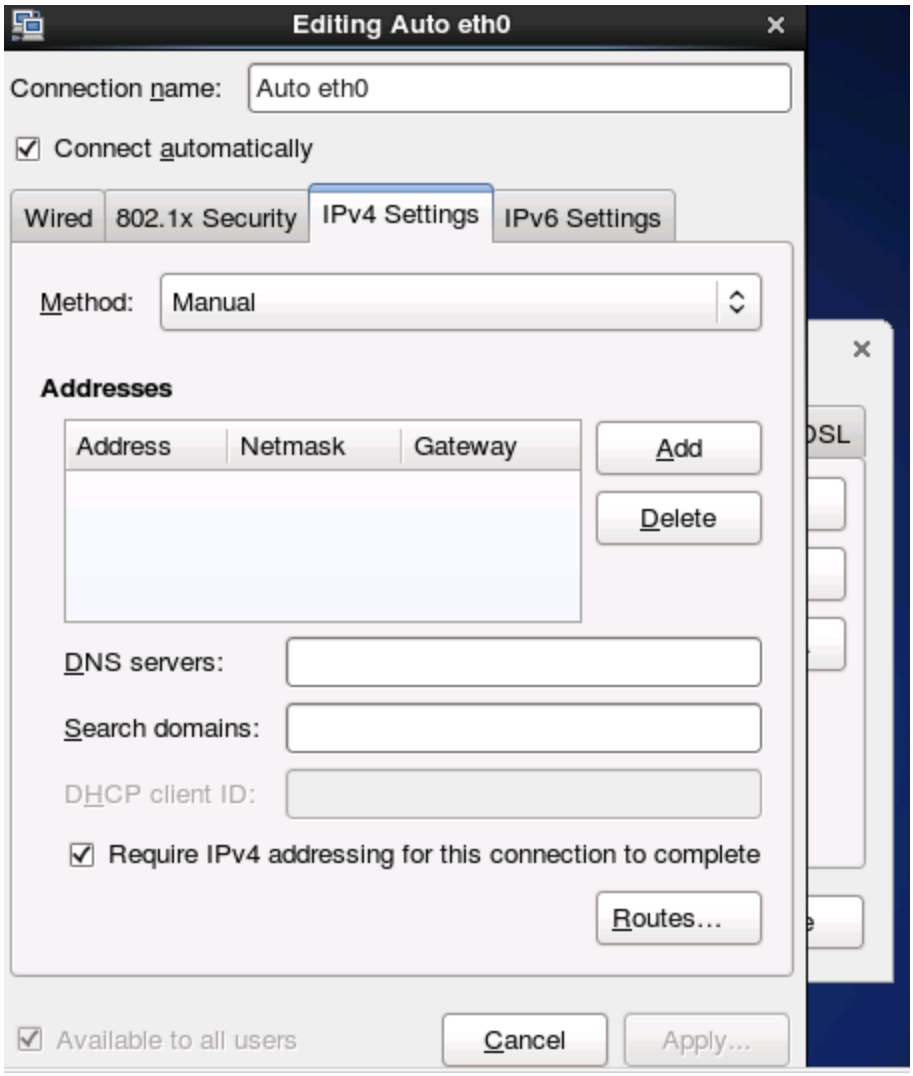
2. Log in as the **root** user. Root user credentials are given Key Access Credentials.
3. Navigate to **System** >**Preferences** >**Network Connections** to launch the Network Connections wizard.

Figure 14. Network Connections Wizard



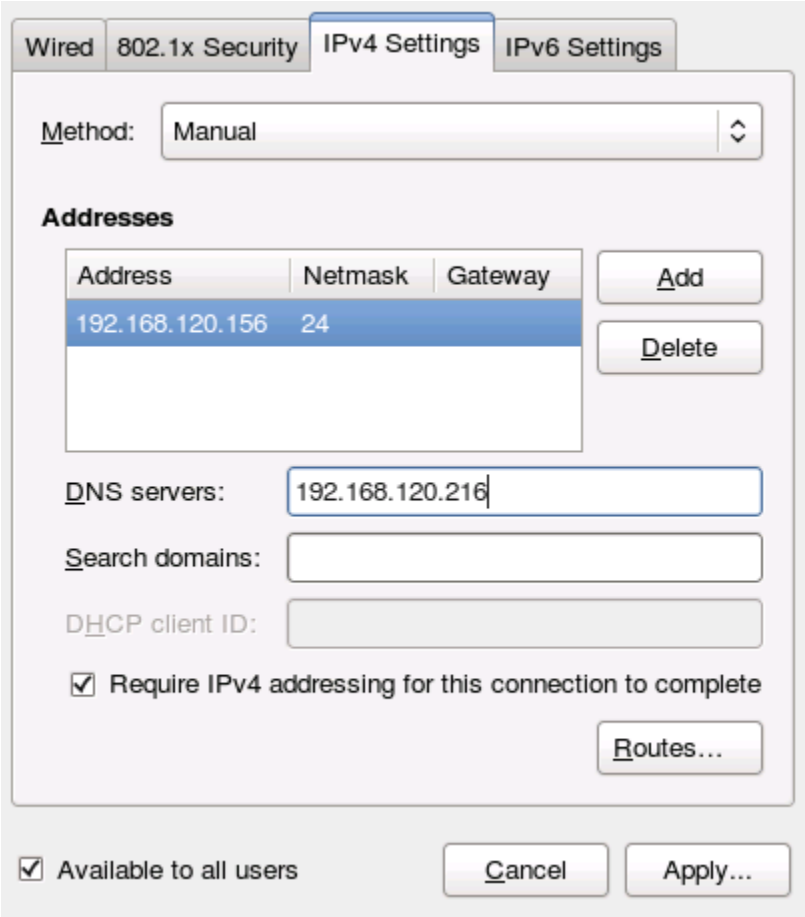
4. Select the network interface card (NIC) appliance on which IP address should be configured manually and click **Edit**.
5. When the Editing dialog box displays (see figure below) update the IP address: select the IPv4 settings, click the **Method** drop-down list and select **Manual**.

Figure 15. Editing



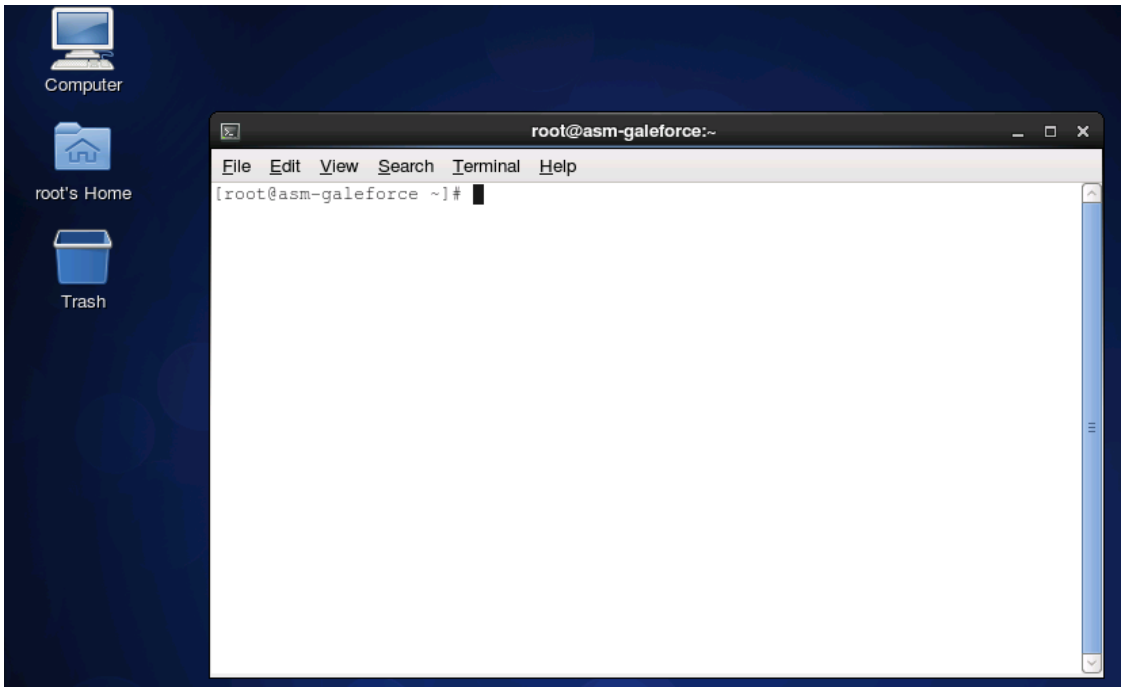
6. Click **Add** to provide the IP address and other networking details (for example, DNS), as shown in the next figure.

Figure 16. Adding IP Addresses



7. Click **Apply**. Once this is done, open the terminal by clicking **Applications** > **System Tools** > **Terminal**.

Figure 17. Terminal Console



8. Execute the **/etc/init.d/network restart** command.
9. Log in to the appliance with the newly configured IP address. This will ensure that IP address is configured correctly on appliance.

2.4 Installing the Active System Manager License

To install the Active System Manager license via the web client, perform the following steps:

1. Close all Active System Manager clients (web client and thick RCP client) connected to the Active System Manager server. (The RCP client installation details are provided in the subsequent sections.)
2. Log in to the Active System Manager Services as the **delladmin/delladmin** user.
3. If the **license.lic** file already exists, create a backup available under **$HOME/asm-galeforce/gf/common/etc/license.lic**.
4. Copy the new license file as **license.lic** in the **$HOME/asm-galeforce/gf/common/etc** directory.

2.5 Configuring Active System Manager Services

2.5.1 Starting Services

Appliance is configured to start Active System Manager services during start-up. Following are the steps for starting the appliance manually.

1. Log in as the **delladmin** user. The password is listed in the 2.1 Deploying OVF section.
2. Execute the following command:

```
cd $HOME/asm-galeforce/gf/sbin
./startGF.sh
```

Note:

The Active System Manager services must not be started by the **root** user.

2.5.2 Stopping Services

Following are the steps for stopping the services manually.

1. Log in as the **delladmin** user. The password is listed in the 2.1 Deploying OVF section.
2. Execute the following command:

```
cd $HOME/asm-galeforce/gf/sbin
./stopGF.sh
```

2.5.3 Verifying Service Status

To verify that all Active System Manager services are up and running, perform the following steps:

1. Log in as the **delladmin** user. The password is listed in the 2.1 Deploying OVF section.
2. Run the following script to display the current status of all services, including the Oracle database status:

```
cd asm-galeforce/gf/sbin
./gfstatus.sh
```

Below is sample output:

```
                    Active System Manager Services Status


Installation
----------------
Release Version: 7.0
Build Number: 21286

Database
----------------
```

```
Vendor: Oracle (Ver: 11.2.0.1.0)
Host: asm-galeforce Port: 1521
Service name: DB11G
Status: Running

Active System Manager Service
---------------------------------
Host: asm-galeforce Port: 40500 Secure Port: 50500
Enterprise: Dell
Lab: DEMO
Status: Running

Domain Services
---------------
1. Domain     : System (Id: 1)
   Description:
   ------------------------------------------------------
   Session server
      Host: asm-galeforce  Port: 40500  Secure Port: 50500
      Status: Running
```

2.6 Installing the Active System Manager Client

You can install the Active System Manager Client on the following platforms:

- 2.6.1 Installing Active System Manager Client Software on Windows
- 2.6.2 Installing the Active System Manager Client Software on Mac
- 2.6.3 Installing the Active System Manager Client Software on Linux

2.6.1 Installing Active System Manager Client Software on Windows

To install the Active System Manager Client software on a Microsoft Windows OS, perform the following steps:

1. Download the Active System Manager installer, x64 version should be downloaded for x64 OS and x32 should be downloaded for x32 based OS
2. On your desktop, click **Start** > **Run** > **Browse**, navigate to the **setup.exe** file, and click **OK**. Alternatively, from your Windows Explorer window, navigate to the **setup.exe** file and double-click it.

   A Security Warning window prompts you to run the file.
3. Click **Run** to enable the installation wizard to guide you through the installation process.

Note:

If an existing version of the client is on the client machine, invoking the installer prompts you to select to uninstall the existing version already on the system. Once selected, the installer uninstalls the existing version and then exits. You must perform the originally intended install after uninstalling the previous version as a single step.

4. Click **Finish** to complete the installation process.

2.6.2 Installing the Active System Manager Client Software on Mac

To install the Active System Manager Client software on a Mac OS, perform the following steps:

1. Download the **ActiveSystemManager-macosx.x86_64_7.0.0_xyzt.zip** file.
2. Unzip the file into a specific folder destination on your hard drive.
3. Create the Active System Manager folder and move the file contents to this location.
4. Execute the **Active System Manager.app** file.

2.6.3 Installing the Active System Manager Client Software on Linux

To install the Active System Manager Client software on Linux, perform the following steps:

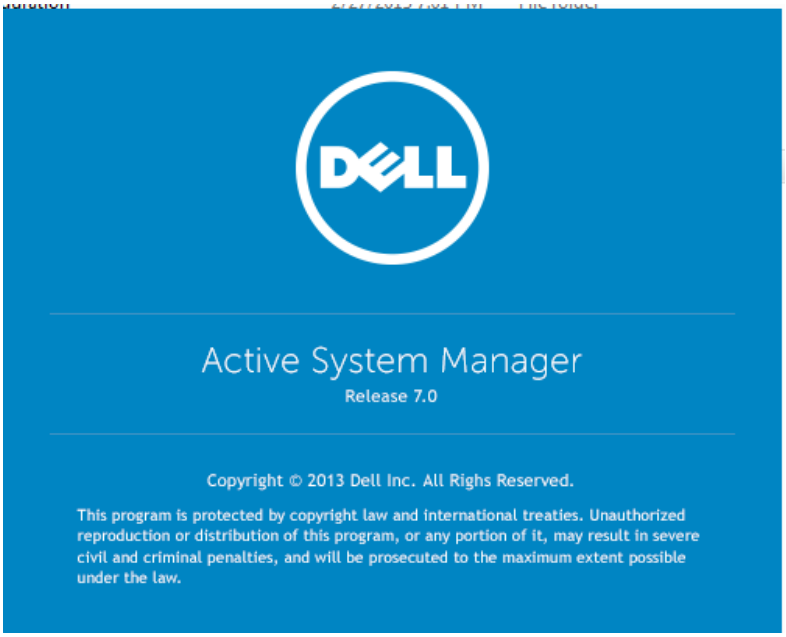
1. Download the **ActiveSystemManager-linux.gtk.x86_7.0.0_xyzt.zip** file.
2. Unzip the file into a specific folder destination on your hard drive.
3. Create the Active System Manager folder and move the file contents to this location.
4. In the console, execute the **Active System Manager** file.

2.6.4 Accessing Active System Manager Using the Windows Client Software

To access the Active System Manager software using the Windows Client software, perform the following steps:

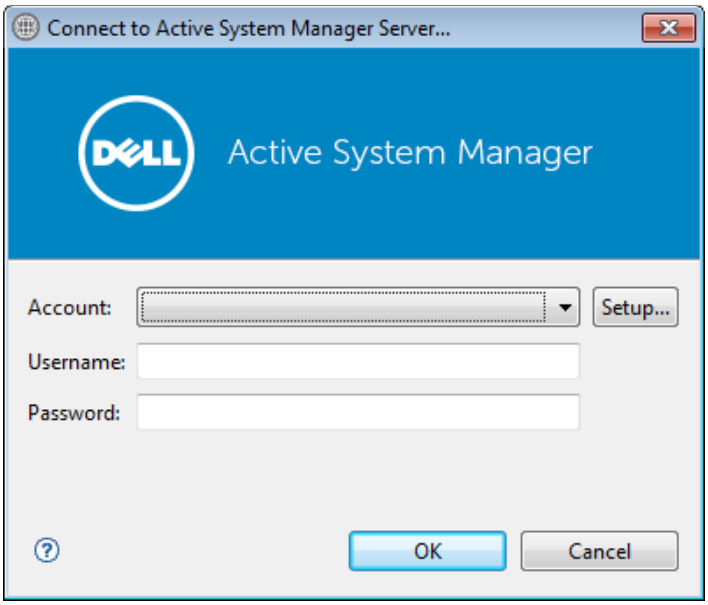
1. Launch the client software application.

Figure 18. Launching the Active System Manager Client Software



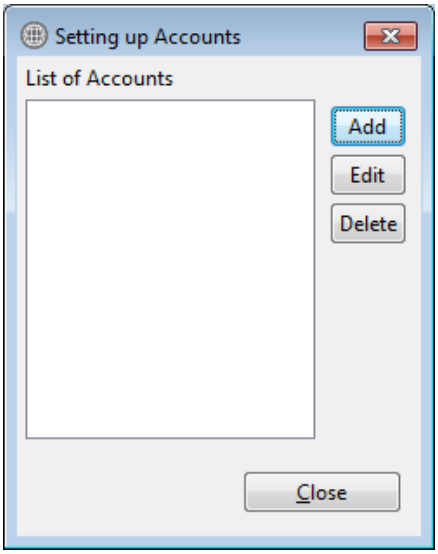
2. Click **Setup** to create the account setup.

Figure 19. Connecting to the Active System Manager Server



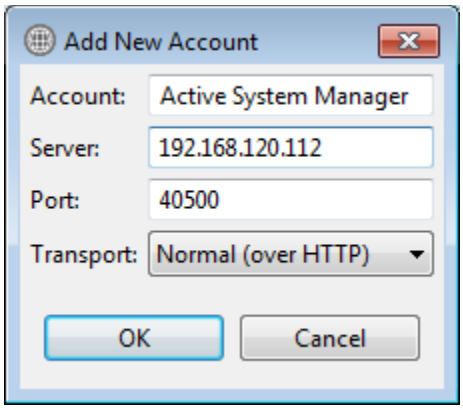
3. On the Setting Up Accounts dialog box, click **Add**. Name the account as the connection to the Active System Manager appliance.

Figure 20. Setting Up Accounts



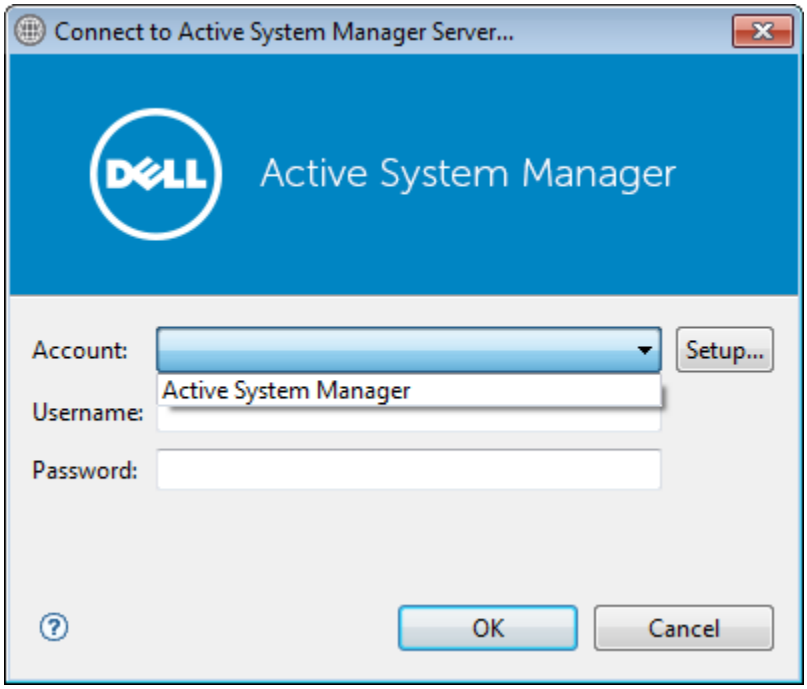
4. Provide the name of the connection and IP address of the appliance. The name of the connection can be any descriptive as shown in the following figure.

Figure 21. Adding New Account



5. Click **OK** and close the Setting Up Account dialog box.
6. Select the account created in earlier step 4.

Figure 22. Logging In to the Active System Manager



7. Provide the username and the password for the appliance. The default username and password is **admin**/**admin**. Click **OK** to launch the Active System Manager application.

3 Active System Manager Setup

This section captures the sequence of steps which should be followed within Active System Manager for managing deploying the blade servers in the Active System 800.

3.1 User and Group Management

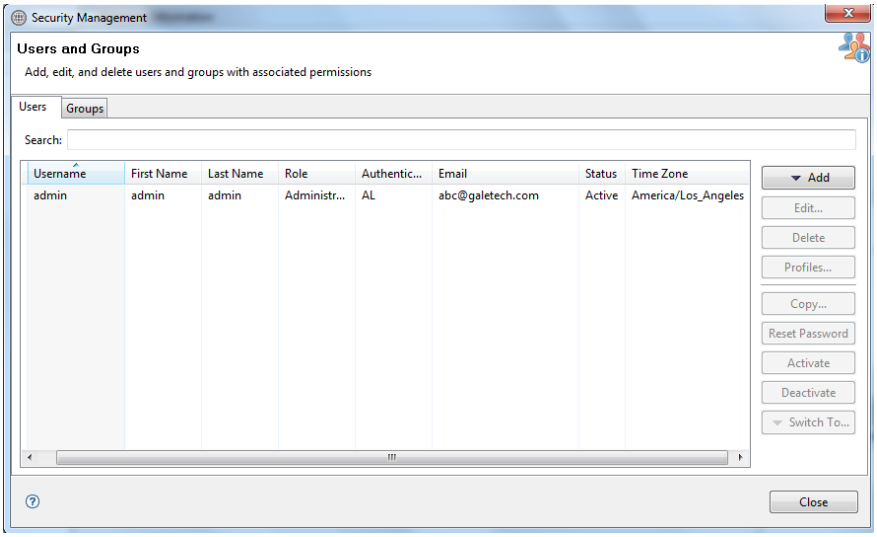
You can manage users and groups within the Active System Manager either directly (by entering the values for individual users and groups from the Windows Client graphical user interface [GUI]), or by importing users from an external repository, such as Lightweight Directory Access Protocol (LDAP), Active Directory (AD), or Network Information Service (NIS).

For user management, log in to the Windows client and navigate to **Tools** > **User and Groups**. The **Security Management—Users and Groups** dialog box displays.

Note:

Set the time zone to match the time on the workstation that the Active System Manager client is installed.

Figure 23. Security Management—Users and Groups



For details on user and group administration, see the “User Profile Management” chapter in the *Active System Manager User Guide*, which is downloadable from the Active System Manager 7.0 web portal (**Help** menu) or from the Thick client(Eclipse-based).

3.2 Discovering Active System 800 Components

Discovery of the Active System 800 components includes:

- Dell M1000e Chassis
- Dell M620 Blade servers
- Dell PowerEdge M I/O Aggregators
- Force10 Top-Of-Rack (ToR) S4810 switches
- Dell EqualLogic Storage Array
- VMware vCenter Server components

3.2.1 Initiating Discovery

To initiate the Discovery process, perform the following tasks in this order:

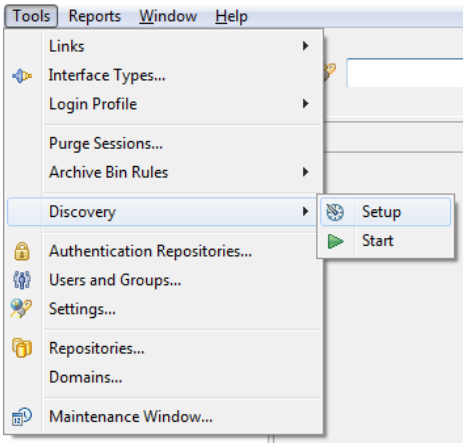
- 3.2.1.1 Configuring Discovery Setup
- 3.2.1.2 Adding Details for the Active System
- 3.2.1.3 Adding vCenter System Properties
- 3.2.1.4 Starting the Discovery Process

3.2.1.1 Configuring Discovery Setup

To configure Discovery settings, perform the following steps:

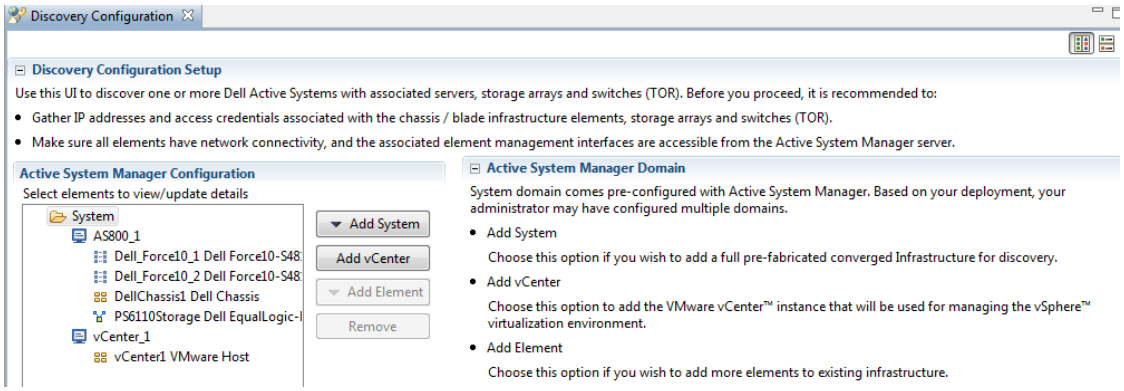
1. Connect to the Active System Manager Client using user credentials with Administrator privileges.
2. Select **Tools** >**Discovery** >**Setup**.

Figure 24. Discovery Menu Options



The Discovery Configuration Setup page displays.

Figure 25. Discovery Configuration Setup

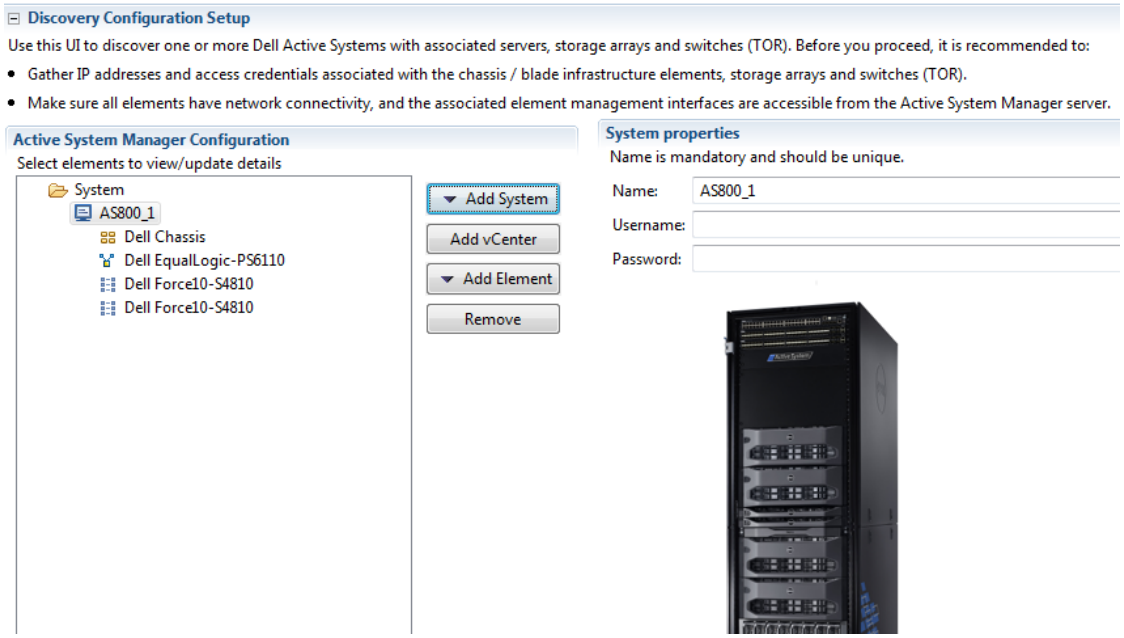


3.2.1.2 Adding Details for the Active System 800 Unit

To add details for the Active System 800 unit, click **Add System**. This feature displays names for Active System 800 components that will be discovered; for example:

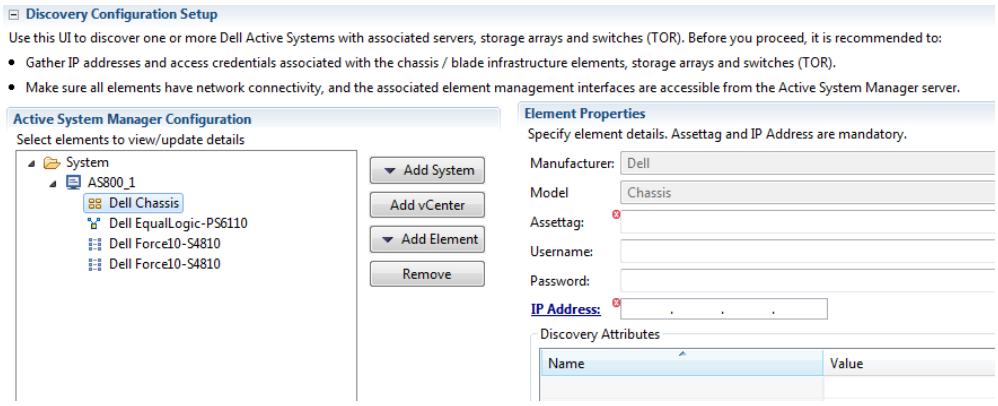
- Dell Chassis
- Dell EqualLogic Storage Array
- Dell Force10

Figure 26. Adding System Details



3. Select the individual components and provide the required IP address/login credentials per the figure.

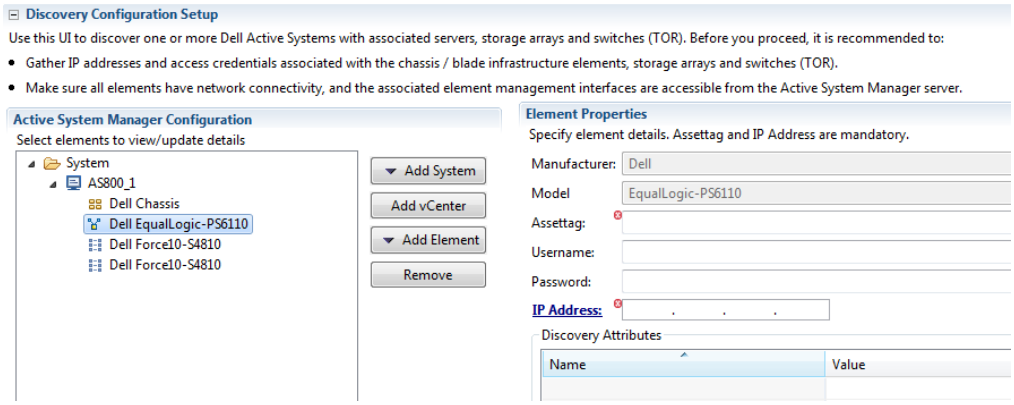
Figure 27. Dell Chassis Element Properties



- **Assettag**—Required. Unique key or name used to import or identify the Dell M1000e Chassis within Active System Manager. For example Assettag Dell_Chassis_001 (a unique name) can be used to track the chassis in Active System Manager
- **Username**—Username to access and manage the Dell M1000e Chassis.
- **Password**—Password to access and manage the Dell M1000e Chassis.
- **IP Address**—Required. IP address for the Dell M1000e Chassis CMC. The CMC should be IP reachable from the Active System Manager server.

4. Provide the following element properties for the Dell EqualLogicStorageArray system (Figure 7):

Figure 28. EqualLogicStorayArray Element Properties



- **Assettag**—Required. Unique key or name for the EqualLogic Storage Array, which is used to import or identify an EqualLogic Storage Array in the Active System Manager. For example, Assettag Dell_EqualLogic_PS6100_1 (a unique name) can be used to track the EqualLogic array in Active System Manager.
- **Username**—Group username to access and manage the EqualLogic Storage Array.
- **Password**—Group password to access and manage the EqualLogic Storage Array.
- **IP Address**—Required. Group Management IP address for the EqualLogic Storage Array. Group Management IP should be reachable (via ping to test) from the ASM server Group IP of the EqualLogic Array should be IP reachable from the Active System Manager server.

The following figure displays an example of how to edit to the /etc/hosts file and how it should be saved: Save file > press **Esc** > type **:wq!** > press **Enter**.

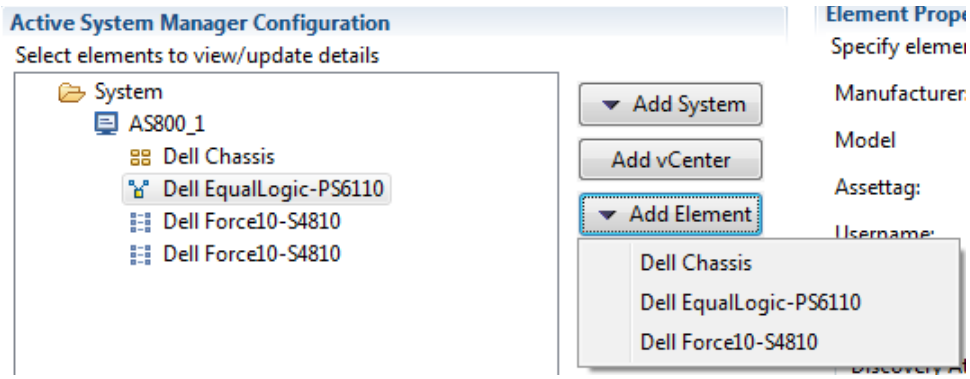
Figure 29. Editing and Saving the /etc/hosts File

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1       asm-galeforce localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6
YourIPHere      hostname.domain.com     # manual entry for ASM7.0
~
~
~
~
```

Note:

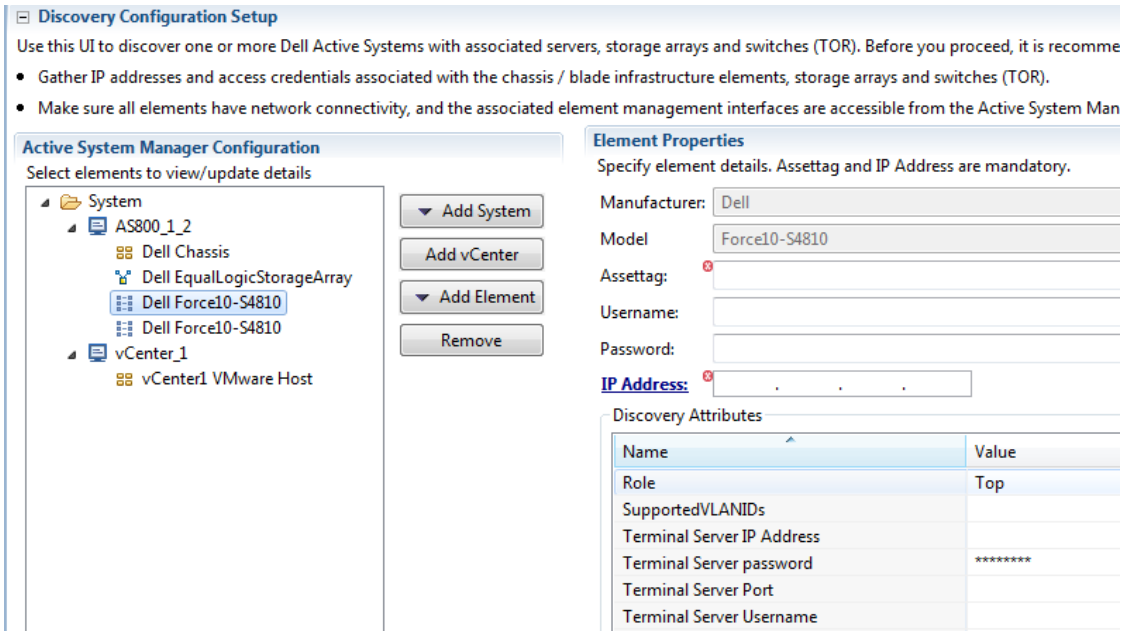
Ifthere are multiple storage groups, there should be an entry for each of the Storage Group in the Discovery Configuration Setup view. For adding a new element in an existing Active System 800 unit, click **Add Element**, select **Dell EqualLogicStorageArray**, and provide required details to initiate discovery.

Figure 30. Adding the Dell EqualLogicStorageArray Element



5. For Dell Force10 Switch (ToR) discovery, provide the following element properties and discovery attributes:

Figure 31. Dell Force10 Element Properties and Discovery Attributes



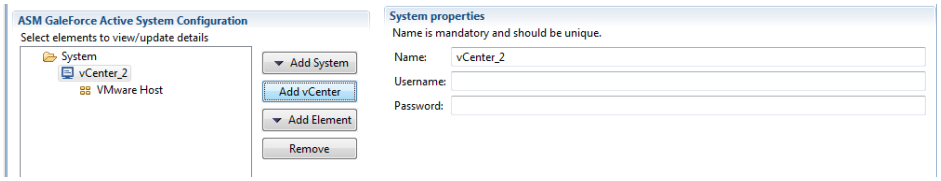
- **Assettag**—Required. Unique key or name for Dell Force10 Switch which is used to import or identify the Force10 Switch in Active System Manager. For example, Assettag Dell_Force10-S4810_1 (a unique name) can be used to track the Force10 Switch in Active System Manager
- **Username**—Username to manage the Force10 switch.
- **Password**—Password to manage the Force10 switch.
- **IP Address**—Required. Management IP address for the Force10 switch. This should be IP reachable from the Active System Manager server.
  - **Role**—(Optional) Top / Bottom.
  - **SupportedVLANIDs**—VLAN IDs that could be provisioned on the Top-Of-Rack (ToR) switch. Sample input format (2..1024); the switch supports a VLAN range from 2 to 1,024.
  - **Terminal Server IP Address**—Optional. Required if switch to managed using the Terminal Server port.
  - **Terminal Server Port**— Optional. Required if switch to managed using Terminal Server port.
  - Terminal Server Username—Optional. Terminal Server username (if configured)
  - Terminal Server Password—Optional. Terminal Server password (if configured)

3.2.1.3 Adding vCenter System Properties

To add vCenter system properties, perform the following steps:

1. On the Active System Manager > **System** > **vCenter** configuration, click **Add vCenter**.
2. For VMware vCenter discovery, provide the following system properties:

Figure 32. Adding vCenter System Properties



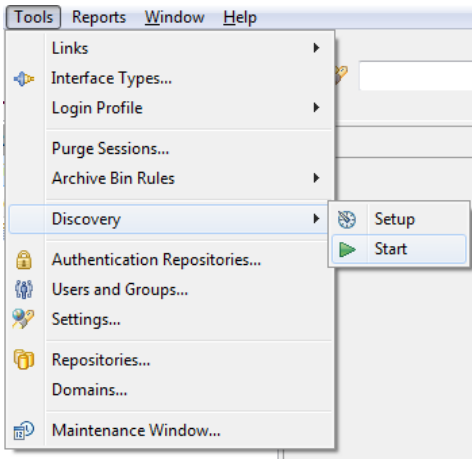
- **Name**—Unique key or name for VMware vCenter which is used to import or identify vCenter in the Active System Manager.
- **Username**—Username to access and manage the vCenter. This user must have full administrator rights to the vCenter. If the vCenter Server is part of a Windows Domain, then enter the username as **username@domain**.
- **Password**—Password to access and manage the vCenter.
- **IP Address**—IP address for the vCenter application. This must be IP reachable from the Active System Manager server.

3.2.1.4Starting the Discovery Process

To start the Discovery process, perform the following steps:

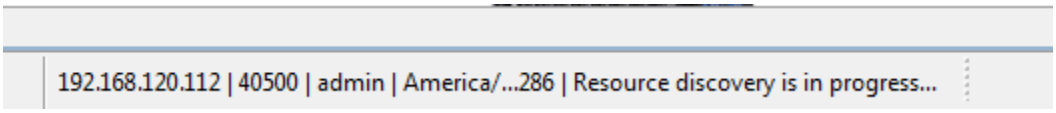
1. Connect to the Active System Manager Client using user credentials with Administrator privileges.
2. On the menu bar, click **Tools** >**Discovery** >**Start**, which initiates the discovery process for components that were set up during the discovery configuration setup.

Figure 33. Tools > Discovery > Start



Note:

- You can view the discovery progress indication at the task bar shown in the bottom of the client.

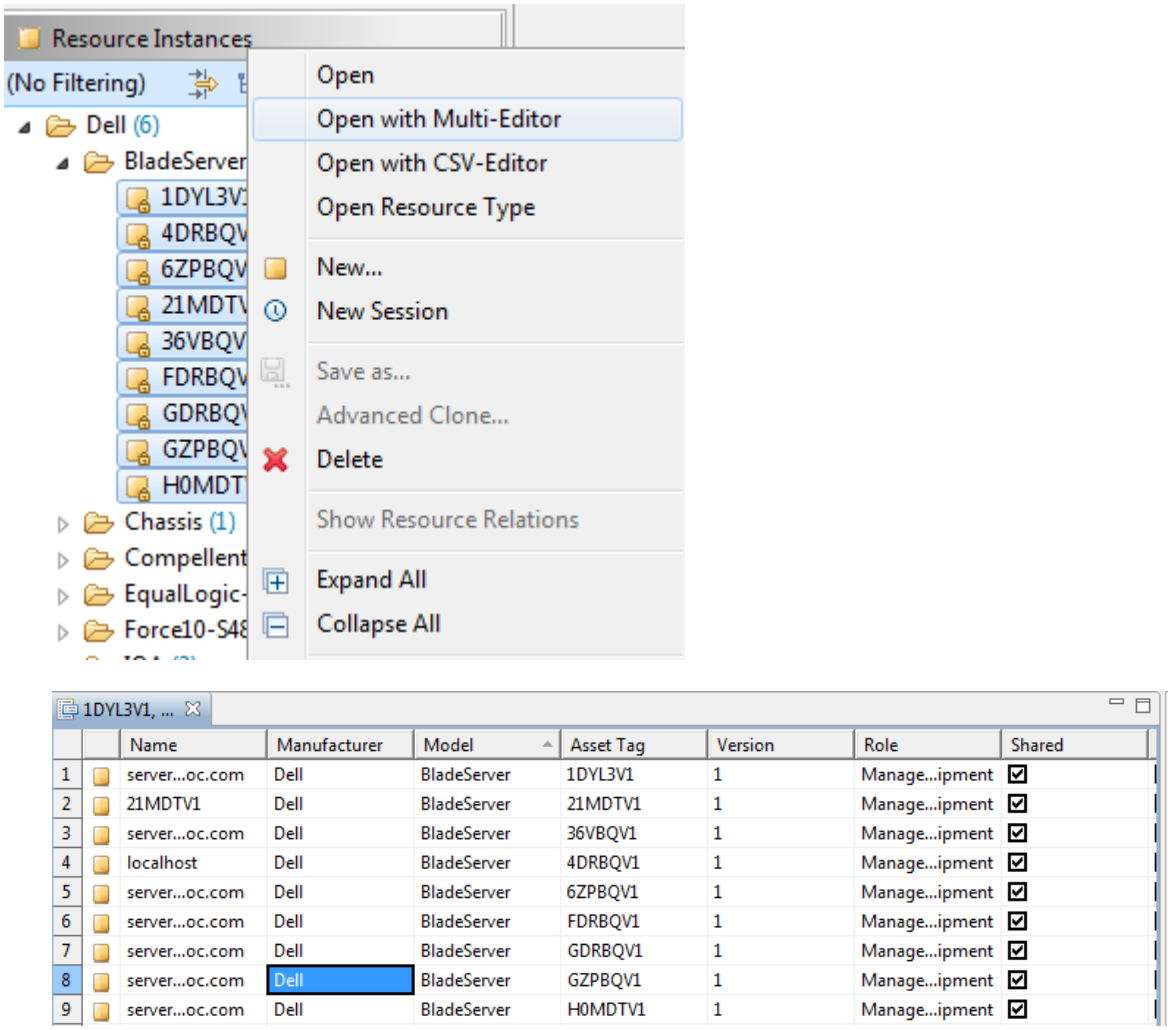


- Ifdiscovery progress is initiated again when a discovery process is already in progress, the Active System Manager user is prompted with a message, indicating the same.

3. After completing the Active System 800 components discovery, update the following information manually in the Active System Manager for all blade servers. These parameters will be used for configuring the ESXi Server with appropriate IP Address, hostname, iSCSI IP Address etc.

   This information can be updated by using the multi-editor feature or by opening individual server instances. You can launch the multi-editor by selecting multiple server instances and then clicking **Open with Multi-Editor**.

Figure 34. Open with Multi-Editor



The following parameters must be updated:

- **ISCSIvNICIPAddresses**—Space-separated list of IP addresses to be assigned to iSCSI virtual network interface cards (vNICs). For example, for updating information for “vmnic6 vmnic7” using the Update Port Group with iSCSI VLAN operation, the value can be in the 192.168.120.XX 192.168.120.YY format. as an example and will depend on the environment subnet range. The IP Addresses needs to be separated by a space “ “
- **iSCSIChapUsername**—iSCSI Chap username used to access volume of EqualLogic Storage Array
- **iSCSIChapSecret**—iSCSI Chap secret corresponding to iSCSI Chap username.
- **ServerHostname**—Hostname to be assigned to the ESXi server.
- **ServerDomainName**—Domain name to be assigned to the ESXi server.
- **ServerNameServer**—Name server to be assigned to the ESXi server. If there are multiple name servers, a comma “,” separated valued should be provided.

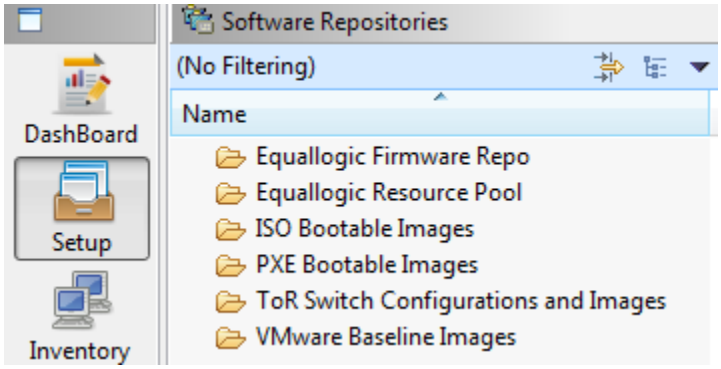
- **ServerGateway**—Gateway for the ESX server.
- **ServerNetmask**—Netmask for the management NIC of ESX server.
- **ServerIPAddress**—IP address that must be assigned to management NIC of the ESX server. Ifthe hypervisor must retrieve an IP address from the DHCP server, leave this parameter blank.
- **ServerPassword—**Server root password to be assigned during unattended installation.
- **vMotionIPAddress—**TBD
- vMotionSubnet (netmask)—TBD

3.3 Software Repositories Available in the Active System Manager Virtual Appliance

The following repositories are pre-packaged and available in the Active System Manager virtual appliance:

- Applicable for Dell Servers—"PXE bootable images", where the repository has the ESXi PXE bootable installer image already configured and "ISO bootable images" where the ESXi ISO bootable installer image is available.
- Applicable for Dell EqualLogic Storage—EqualLogic Storage Firmware.
- The repository has EqualLogic firmware images configured (EqualLogic Storage Resource Pools)
- ToR Switch Configurations and Images—The repository has switch images and a base configuration configured.
- VMware ESXi images

Figure 35. Software Repositories



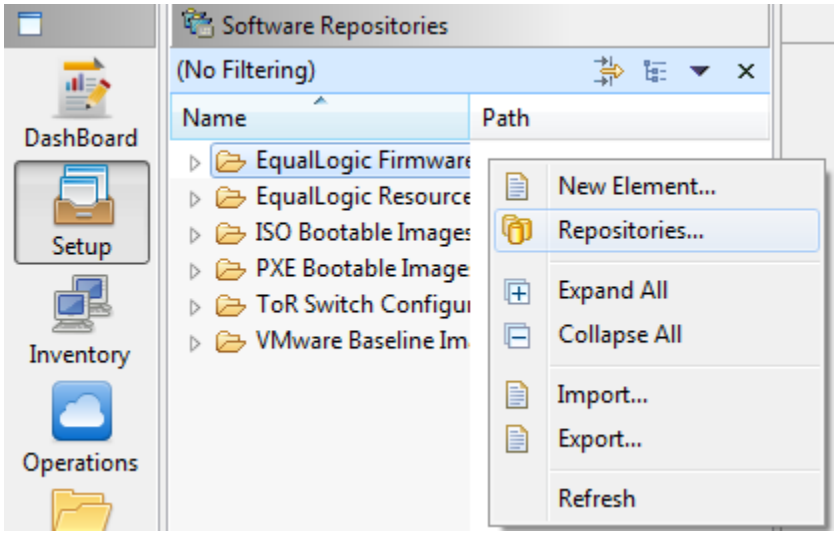
3.3.1 Updating Repository Elements for Firmware Images on EqualLogic Firmware Repo

The EqualLogic StorageArray repository contains firmware images to be used for updating the firmware on EqualLogic Storage Arrays.

To update these repository elements, perform the following steps:

1. Open the **Software Repositories** view in the setup perspective by clicking **Setup** > **Software Repositories** on the client.

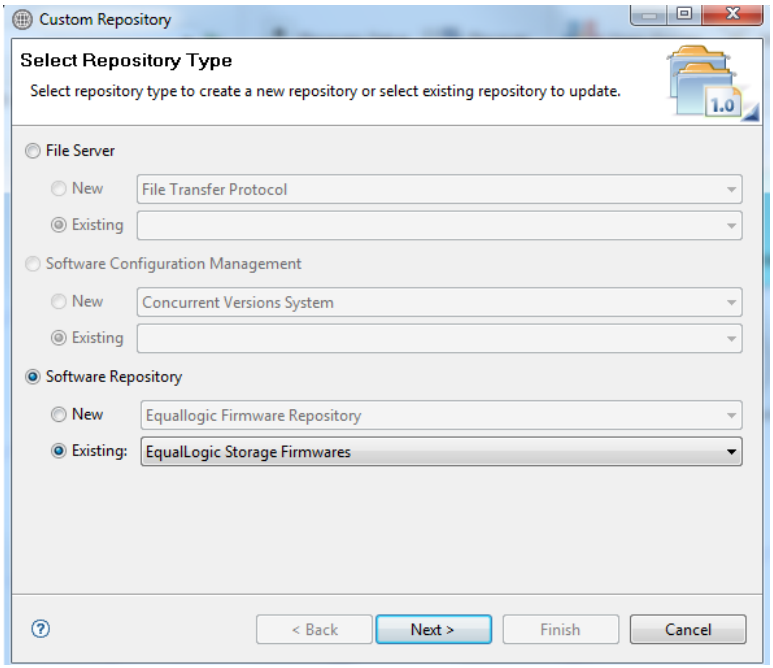
   Figure 36. Software Repositories View

2. Right-click the view and select **Repositories**.

   The **Custom Repository—Select Repository Type** dialog box displays.

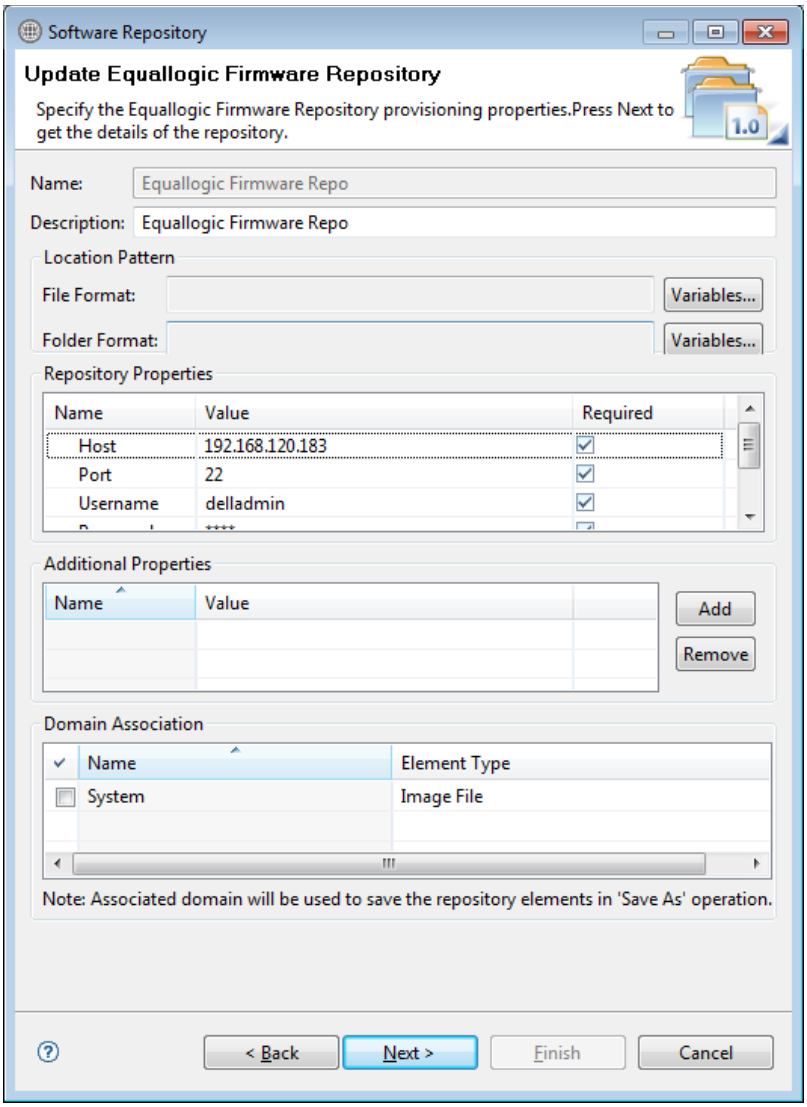
Figure 37. Selecting Repository Type to Update



3. Click the **Software Repository** > **Existing** radio buttons.
4. Using the drop-down menu, select the Repository Type and click **Next**.
5. Update the IP address, username, password, and base directory (location on the server where the firmware images are present, it can be the access information for the Active System Manager appliance as appliance is shipped with latest firmware images; otherwise, it can the access information for the remote server having the firmware images residing on it, the server should be SSH reachable from the Active System Manager appliance) for the image server, and click **Next**.

   The **Custom Repository—Update EqualLogic Firmware Repository** dialog box displays; see Figure 19.

Figure 38. Update EqualLogic Firmware Repository

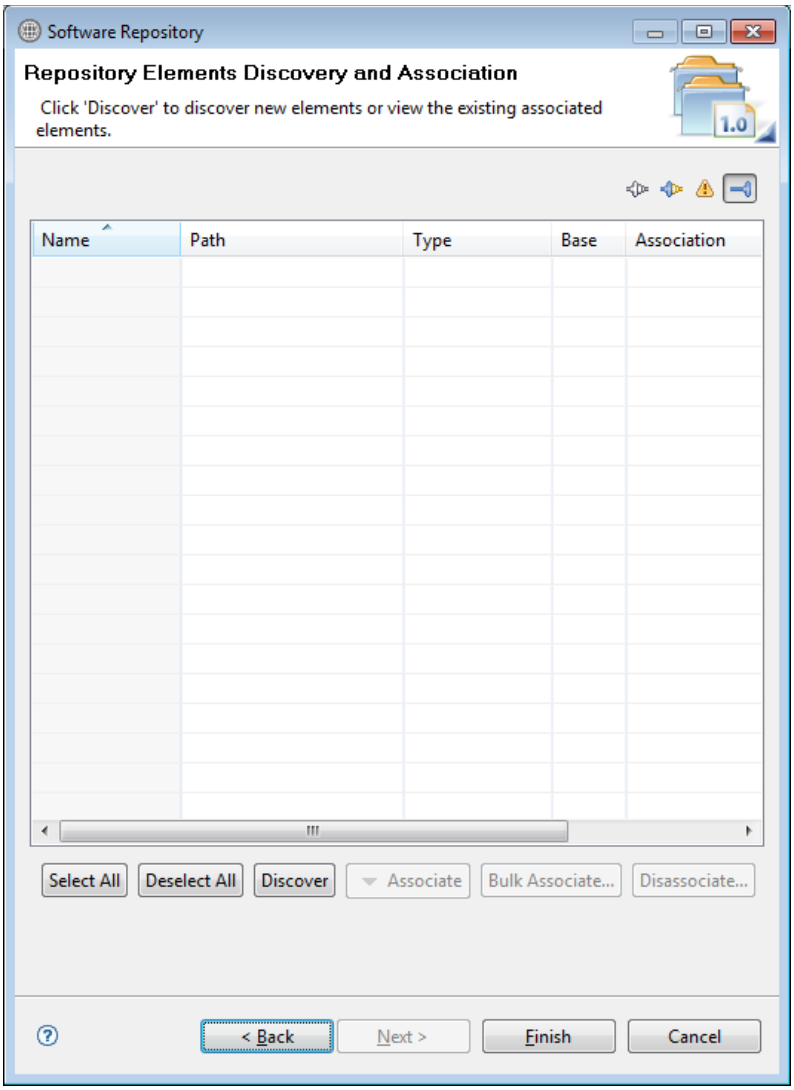


6. Click **Finish**.

Note:

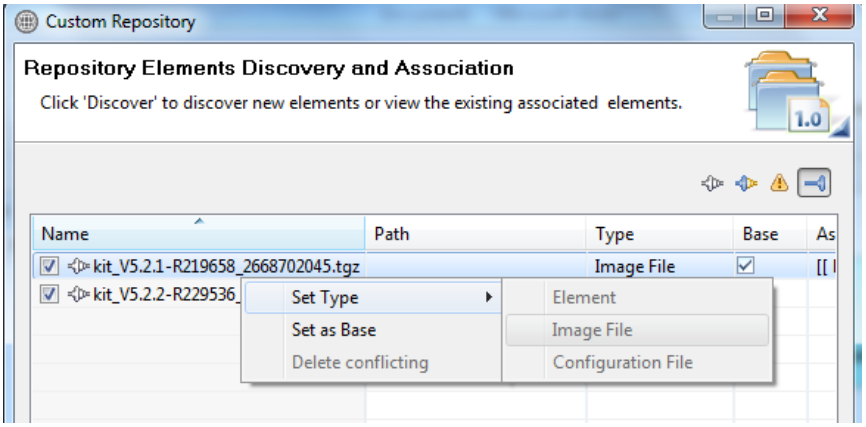
Ifa new image is added to the appliance, skip this step.

Figure 39. Repository Elements Discovery and Association



7. Click **Discover** to display all the firmware images available on the image server.

Figure 40. Repository Elements Discovery and Association



8. Click **Associate** to associate the image file with the required Resource Types (Dell EqualLogic Storage Array and EqualLogic Storage Pool).

Figure 41. Associating Resource Types

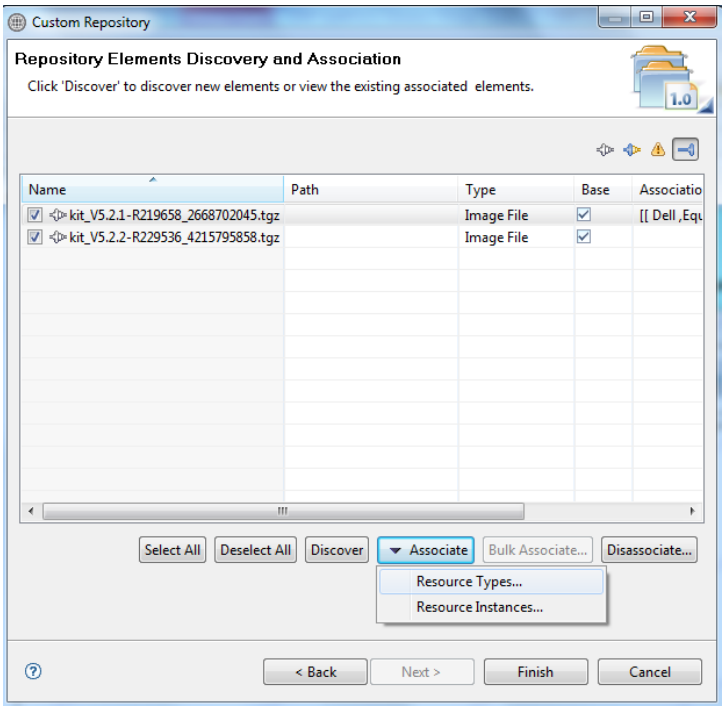
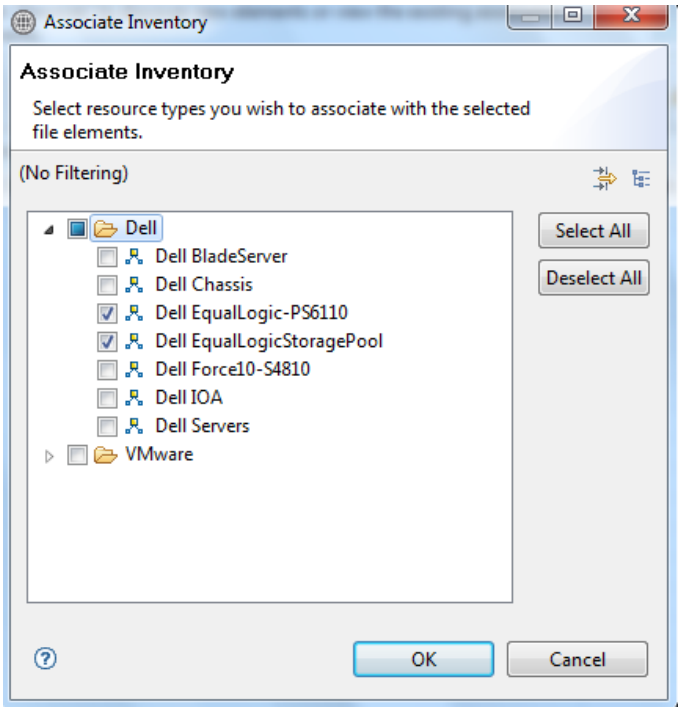


Figure 42. Associating Inventory



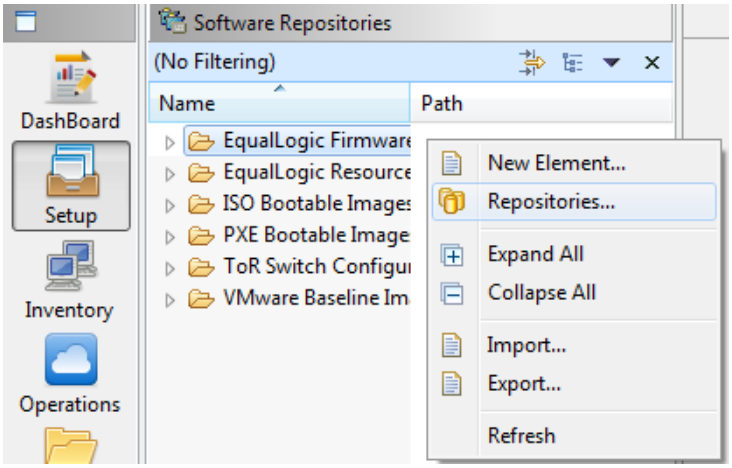
9. Select resource types and click **OK**.

3.3.2 Updating Repository Elements for EqualLogic Storage Resource Pools

The EqualLogic Storage Resource Pool repository contains the information of the Storage Pools available on EqualLogic Storage Arrays.

To update these repository elements, perform the following steps:

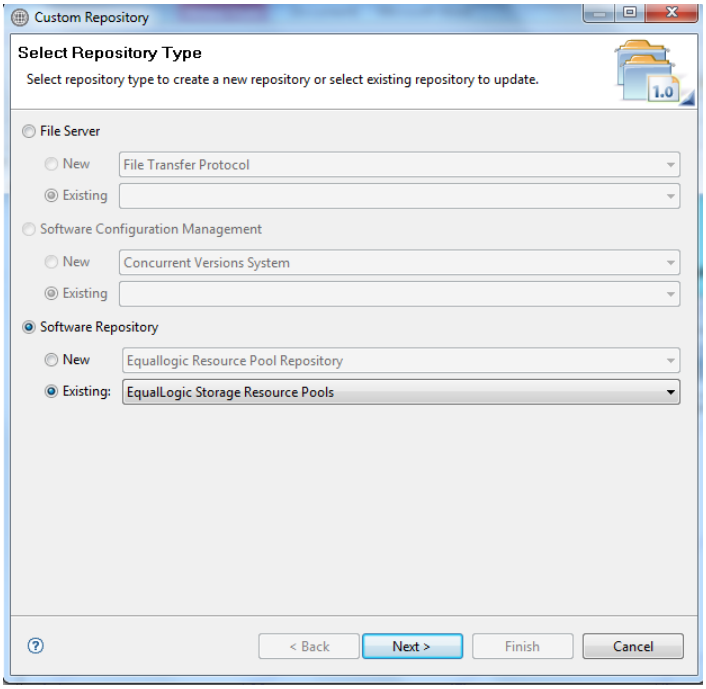
1. Open the **Software Repositories** view in the setup perspective.



2. Right-click the view and select **Repositories**.

   The **Custom Repository—Select Repository Type** dialog box displays.

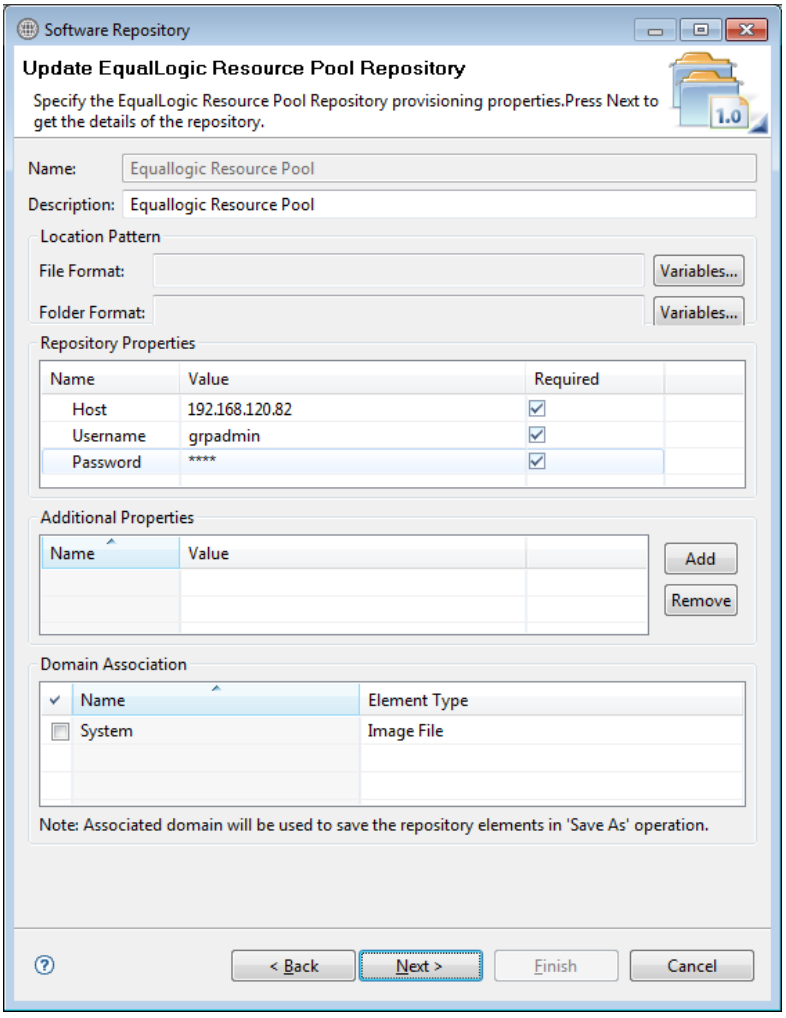
Figure 43. Selecting Repository Type to Update



3. Click the **Software Repository** > **Existing** radio buttons.
4. Using the drop-down menu, select **EqualLogic Storage Resource Pools** and click **Next**.

The **Software Repository—Update EqualLogic Resource Pool Repository** dialog box displays.

Figure 44. Update EqualLogic Resource Pool Repository



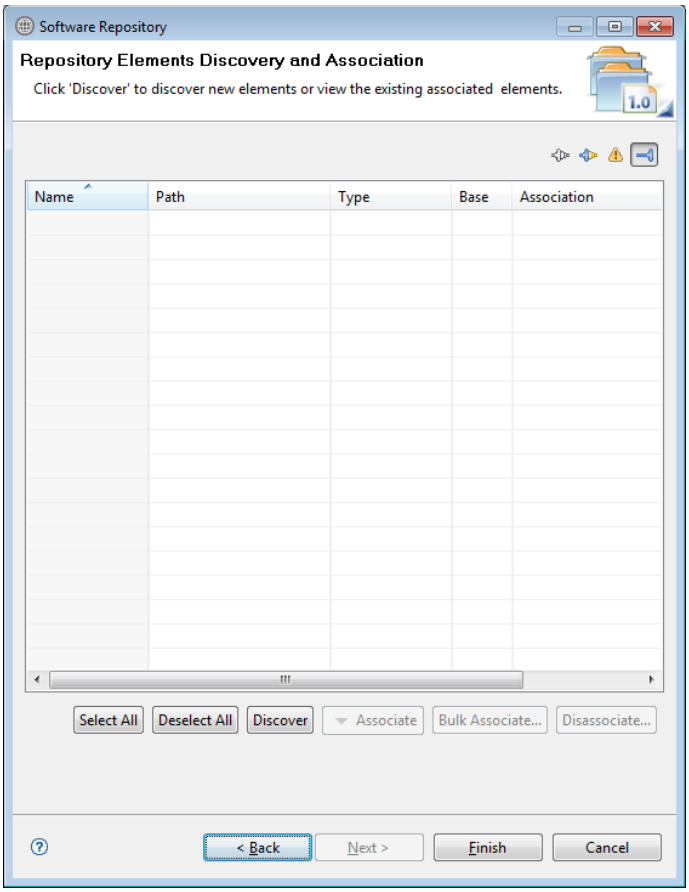
5. Update the **Host**, **Username**, and **Password** parameters. These parameters correspond to storage group Management IP address, group username, group password respectively, and click **Next**.
6. Click **Finish**.

Note:

Ifa new resource pool is added and information needs to be updated, skip this step.

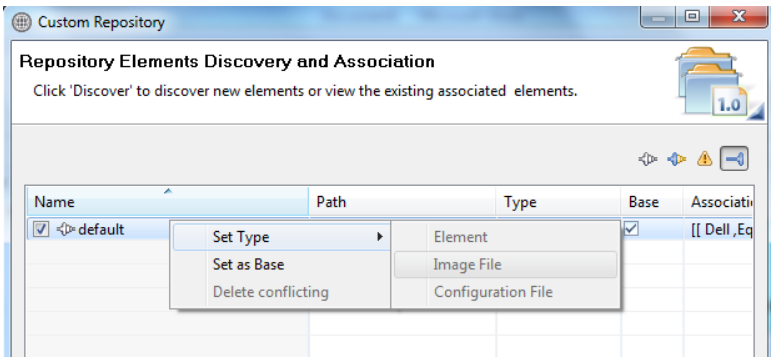
7. Click **Discover** to display all the storage pools available on the Storage Array.

Figure 45. Discovering New Elements



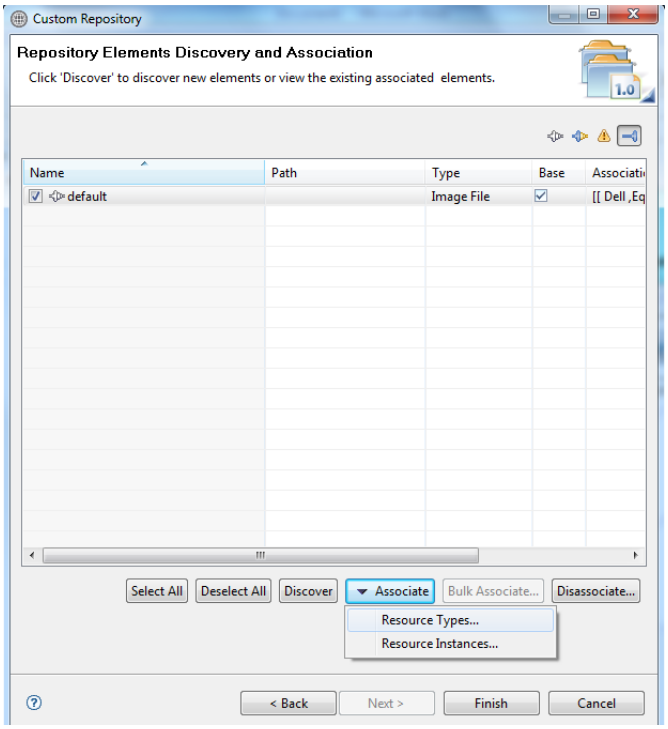
8. Right-click the selected Resource Pool and update the Type to **Image File**, and click **Finish**.

Figure 46. Repository Elements Discovery and Association



9. Click **Associate** to associate the storage pools with the required Resource Types (Dell EqualLogic-PS6110 and EqualLogic Storage Pool), and click **Finish**.

Figure 47. Associating Resource Types

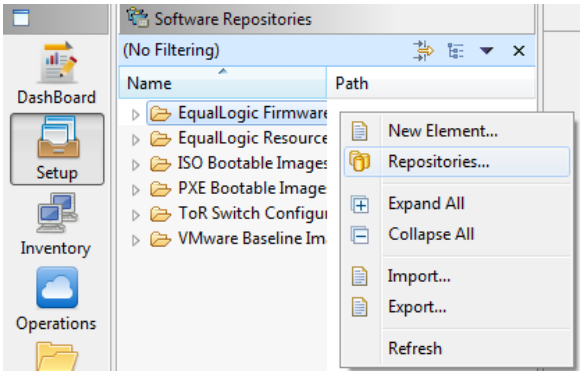


3.3.3 Updating Repository Elements for PXE Bootable Images

To update these repository elements, perform the following steps:

1. Open the **Software Repositories** view in the Setup perspective.

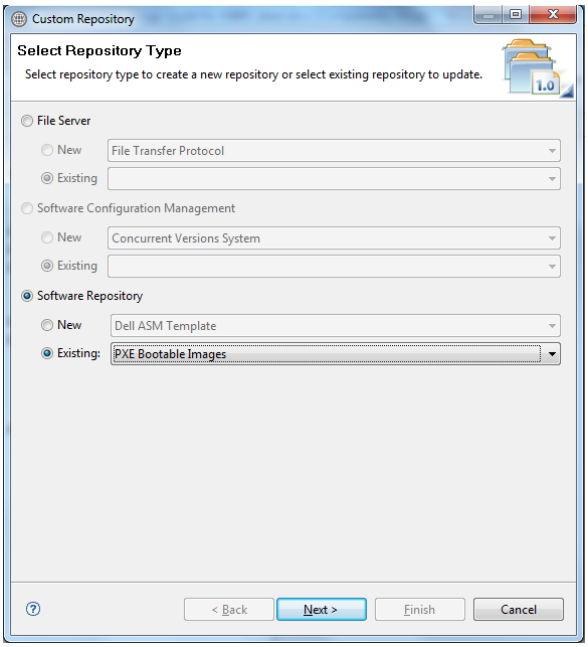
Figure 48. Software Repositories View



2. Right-click the view and select **Repositories**.

   The **Custom Repository—Select Repository Type** dialog box displays.

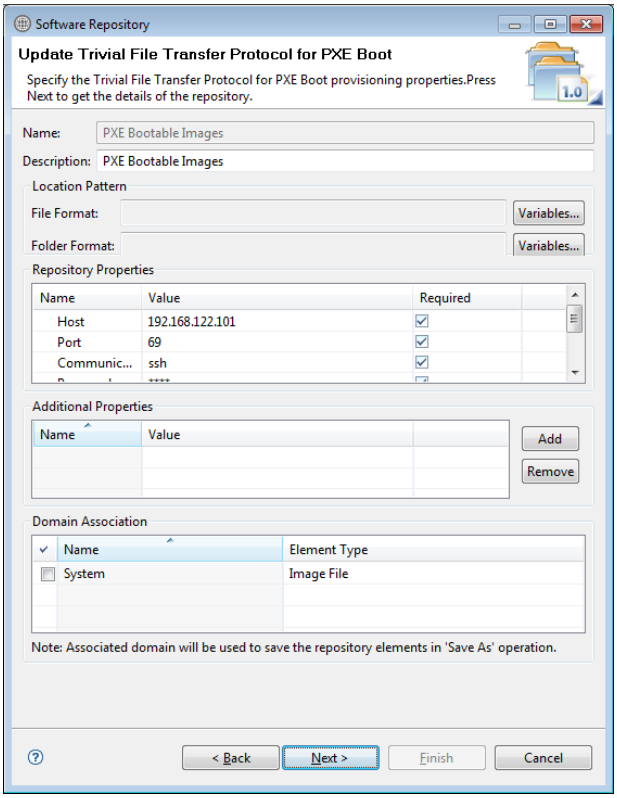
Figure 49. Selecting Repository Type to Update



3. Click the **Software Repository** > **Existing** radio buttons.
4. Using the drop-down menu, select **PXE Bootable Images** and click **Next**.

   The **Update Trivial File Transfer Protocol for PXE Boot** dialog box displays.

Figure 50. Update TFTP for PXE Boot

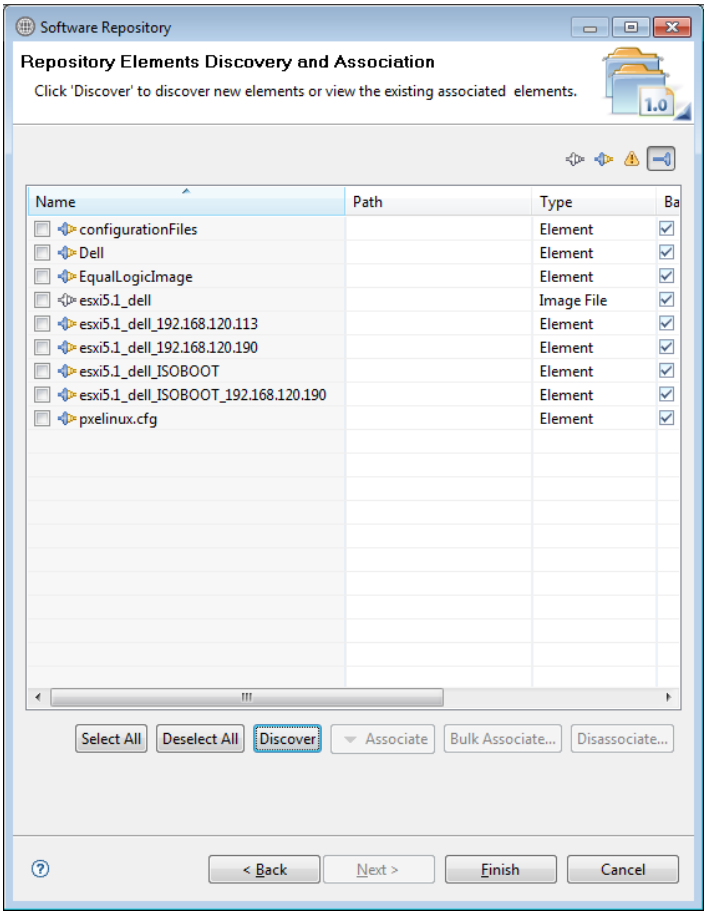


5. Update the **Host** attribute value with the IP address of the Active System Manager appliance.
6. The Username and Password are configured with default appliance username and password. These needs to be updated Ifthe default username/password is updated.
7. Click **Next** to display the list of repository files.
8. Click **Finish**.

Note:

Ifa new resource pool is added and information needs to be updated, skip this step.

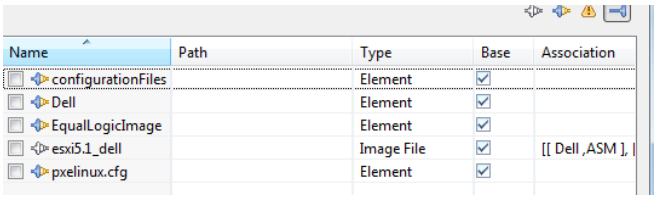
Figure 51. Discovering New Elements



9. Click **Discover** to initiate the discovery of the repository files. This step is required only if a new image is added to the repository.

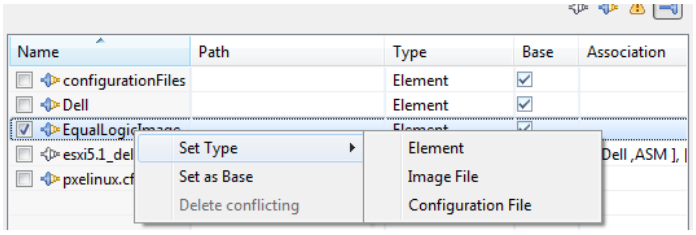
   This will list the discovered element in the repository.

Figure 52. List of Repository Files



10. Right-click the selected discovered elements and update the Type to **Image File**, and click **Finish**.

Figure 53. Updating Discovered Elements Type to Image File

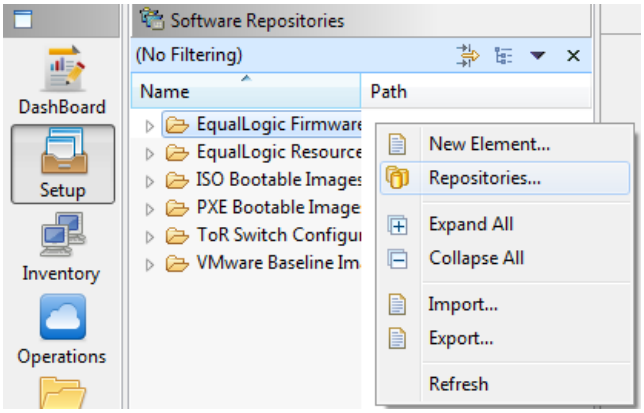


3.3.4 Updating Repository Elements for ISO Bootable Images

To update these repository elements, perform the following steps:

1. Open the **Software Repositories** view in the Setup perspective.

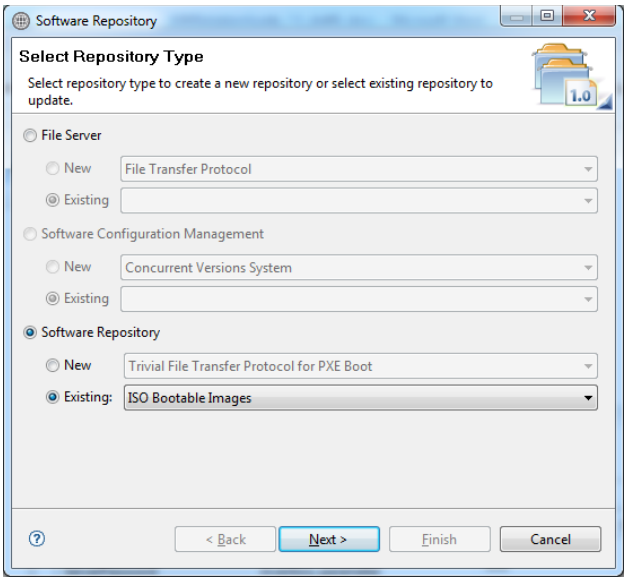
Figure 54. Software Repositories View



2. Right-click the view and select **Repositories**.

   The **Custom Repository—Select Repository Type** dialog box displays.

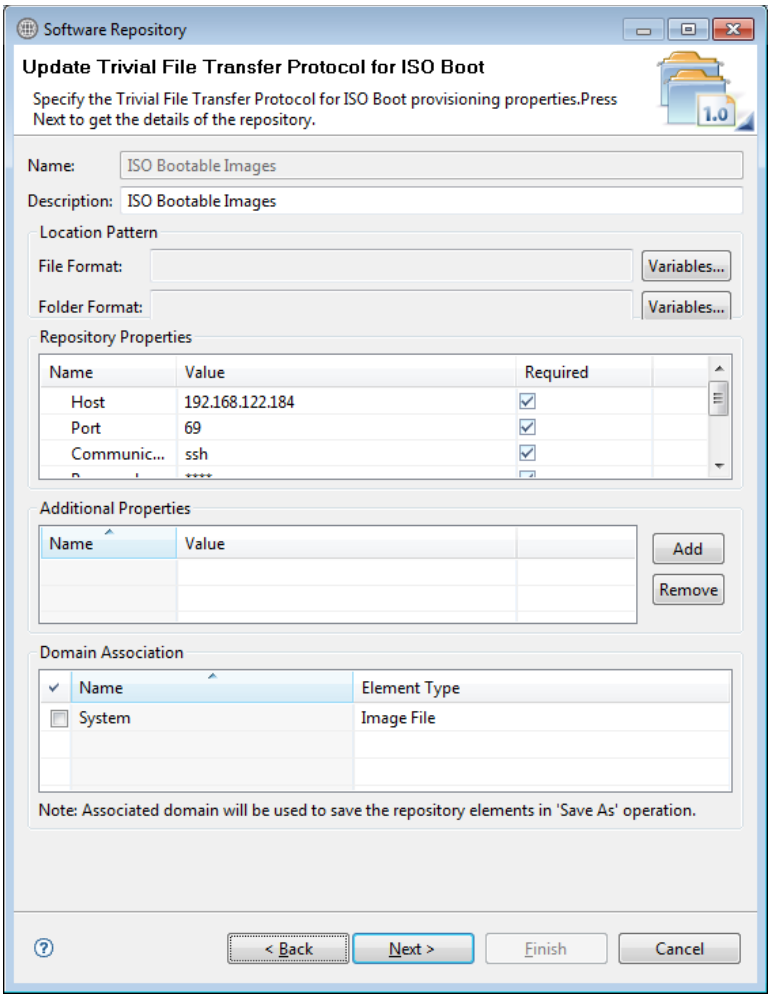
Figure 55. Selecting Repository Type to Update



3. Click the **Software Repository** > **Existing** radio buttons.
4. Using the drop-down menu, select **ISO Bootable Images** and click **Next**.

   The **Update Trivial File Transfer Protocol for ISO Boot** dialog box displays.

Figure 56. Update TFTP for PXE Boot



5. Update the **Host** attribute value with the IP address of the Active System Manager appliance.
6. The Username and Password are configured with default appliance username and password. These needs to be updated if the default username/password is updated.
7. Click **Next** to display the list of repository files.
8. Click **Finish**.

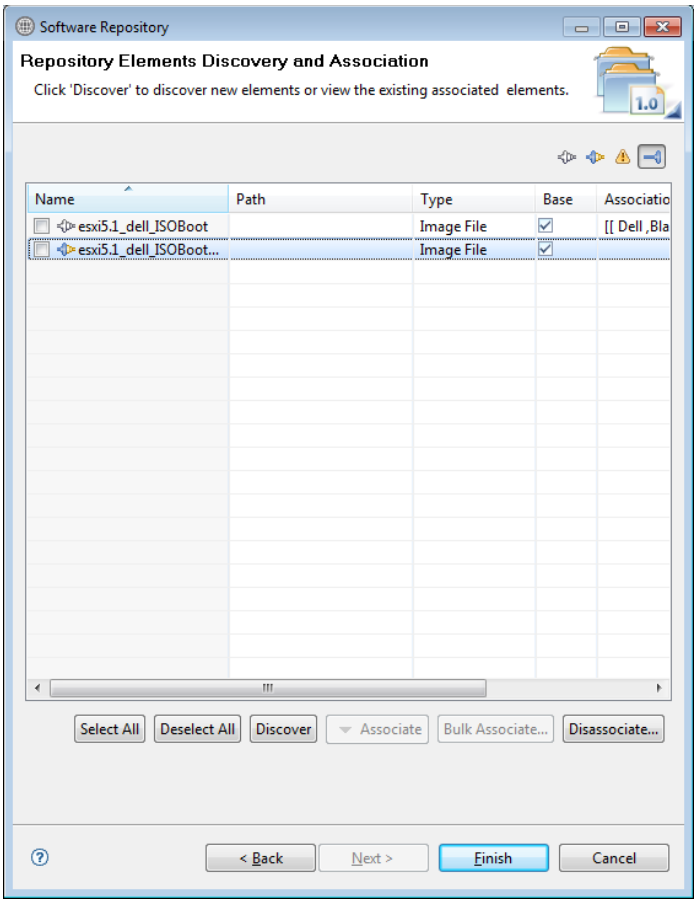
Note:

If a new resource pool is added and information needs to be updated, skip this step.

9. Click **Discover** to initiate the discovery of the repository files. This step is required only ifa new ISO image is added to the appliance.

   This will list the discovered element in the repository.

Figure 57. List of Repository Files



10. Right-click the selected discovered elements and update the Type to **Image File**, and click **Finish.**

Figure 58. Updating Discovered Elements Type to Image File

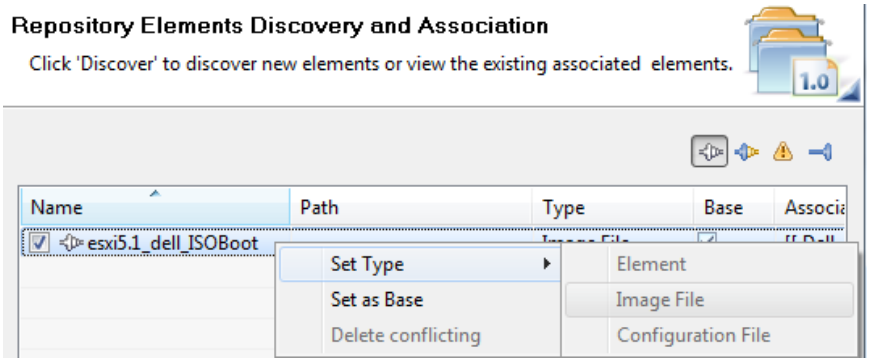
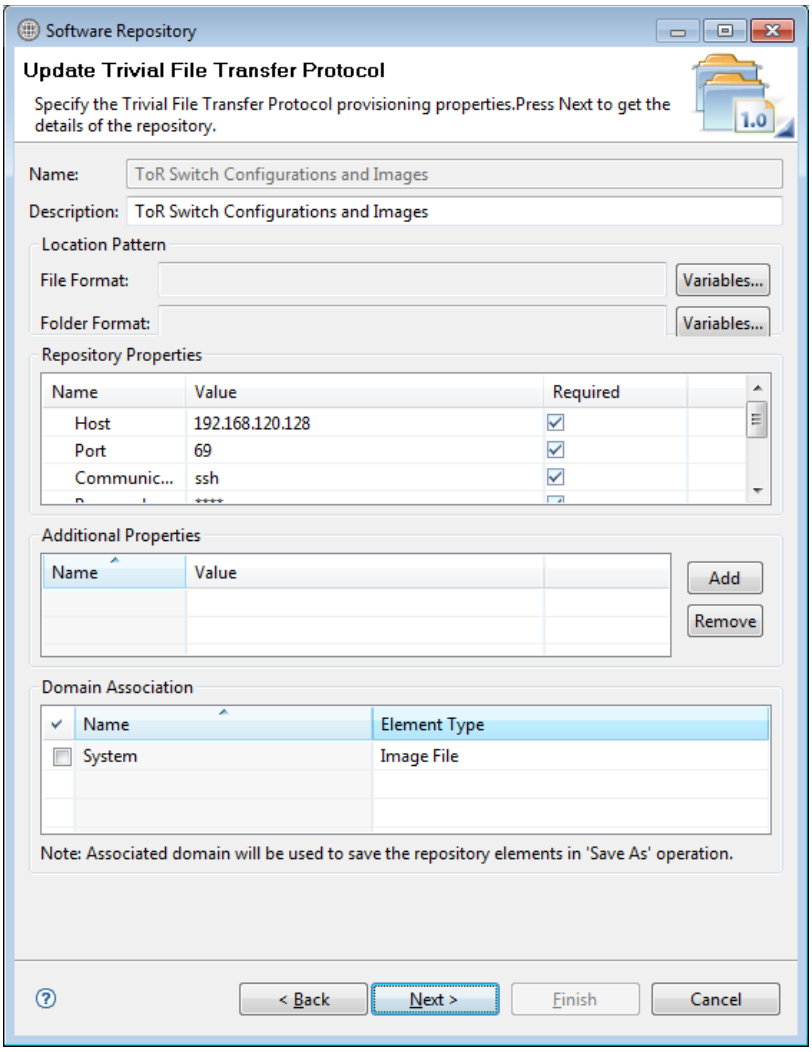


Figure 59. Repository Properties

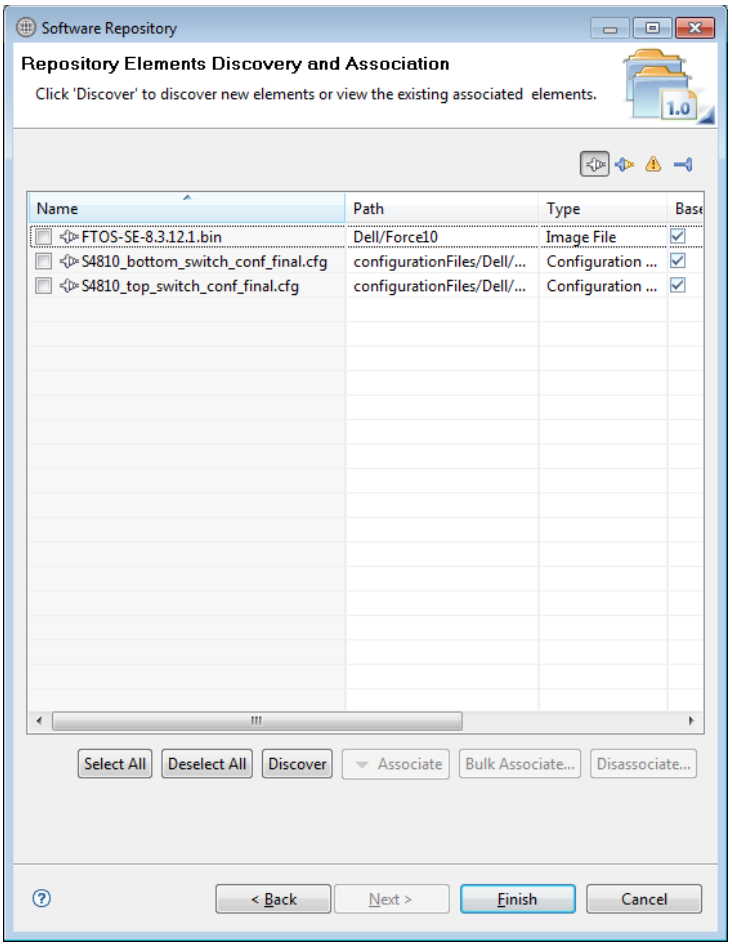


11. Update the **Host** attribute with the IP address of the VM appliance.
12. Click **Next** to display the list of repository files.
13. Click *Finish*.

Note:

Ifa new resource pool is added and information needs to be updated, skip this step.

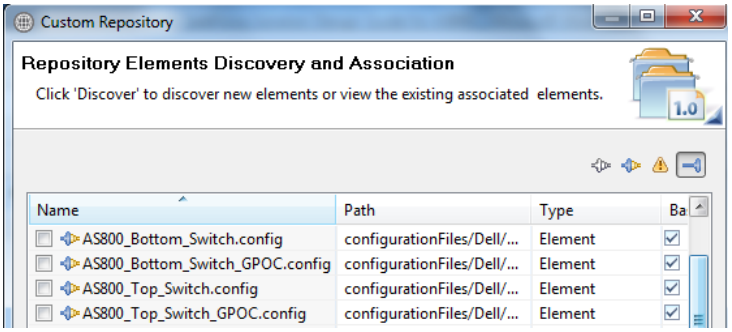
Figure 60. Discovering New Elements



14. Click **Discover** to initiate the discovery of the repository files.

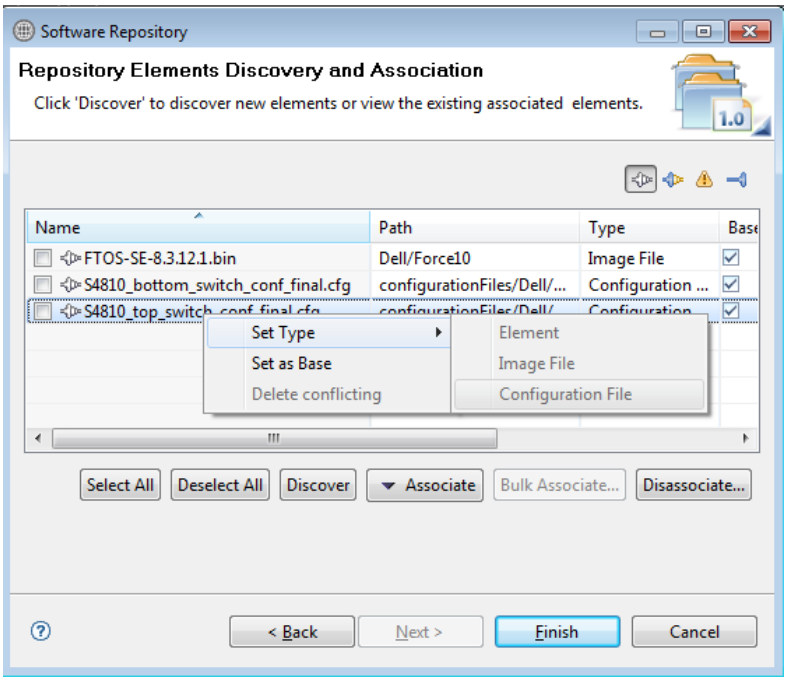
    The list of discovered elements in the repository displays.

Figure 61. List of Repository Files



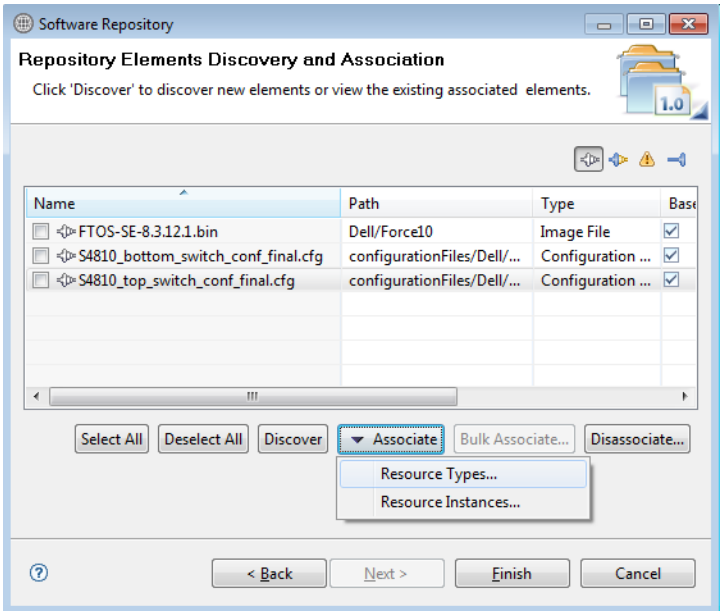
15. Right-click the selected discovered elements, update the Type to **Configuration File**, and click **Finish**.

Figure 62. Updating Discovered Elements Type to Configuration File



16. Click **Associate** to associate the selected element with the **Dell Force10** resource type and click **Finish**.

Figure 63. Associating Resource Types



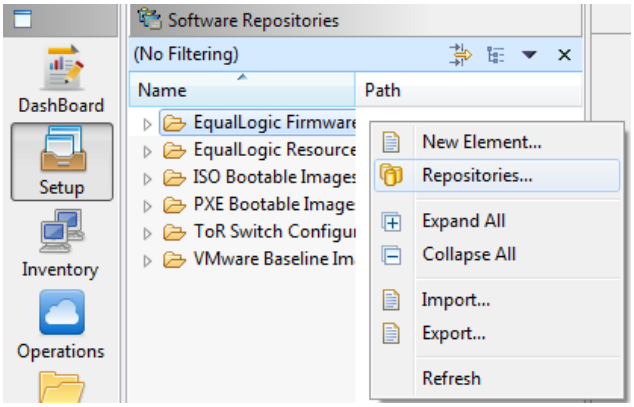
3.3.5 Updating Repository Elements for VMware Baseline Images

This repository contains VMware baseline images for creating VM clones.

To update the repository elements for VMware baseline images, perform the following steps:

1. Open the **Software Repositories** view in the Setup perspective.

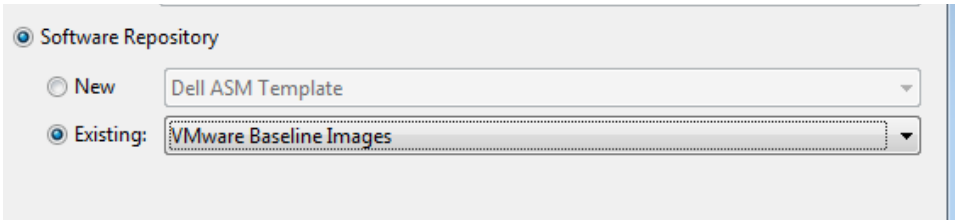
   Figure 64. Software Repositories View



2. Right-click the view and select **Repositories**.

   The **Custom Repository—Select Repository Type** dialog box displays.

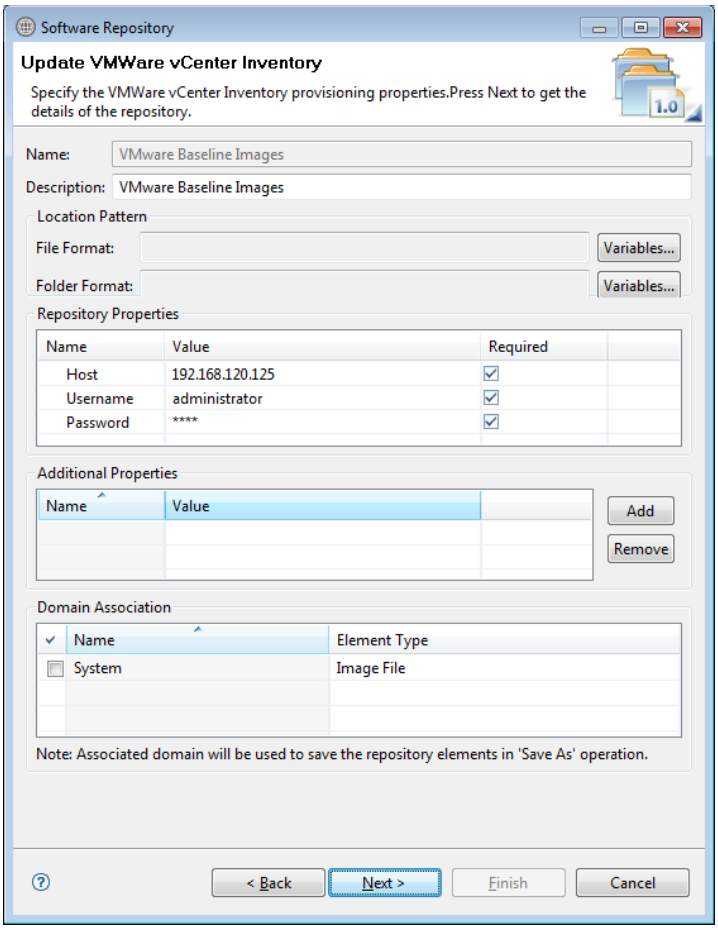
   Figure 65. Selecting VMware Baseline Images Repository



3. Click the **Software Repository** > **Existing** radio buttons.
4. Using the drop-down menu, select **VMware Baseline Images,** and click **Next**.

   The **Repository Properties** dialog box displays.

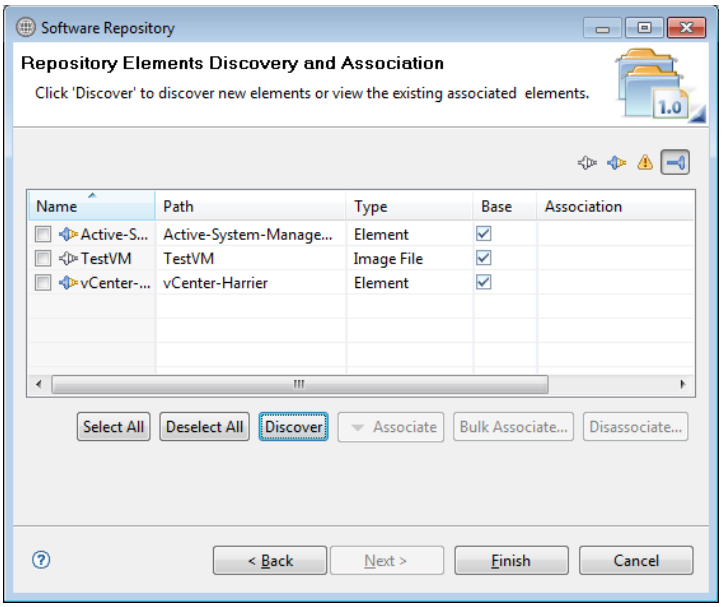
Figure 66. Repository Properties



5. Update the VMware vCenter host (IP address), username, and password.
6. Click **Next** to display the list of repository files.
7. Click **Discover** to initiate the discovery of the repository files.

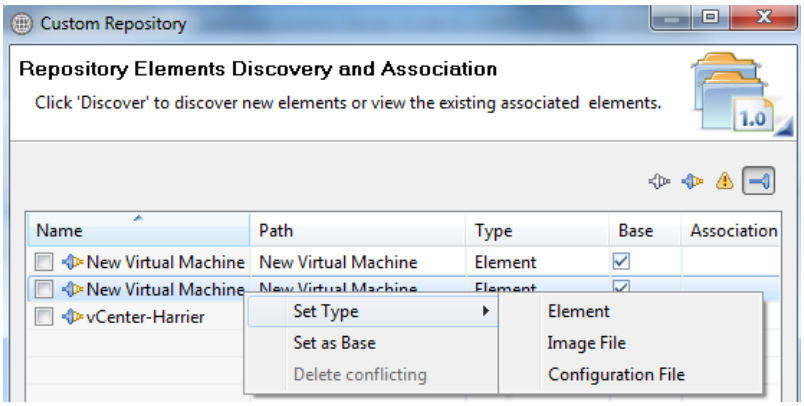
   The list of VMs managed by the vCenter displays.

Figure 67. List of Repository Files



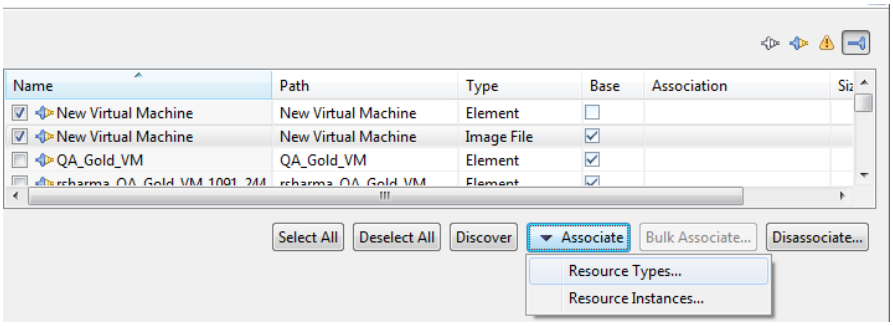
8. Right-click the selected discovered element, select **Set Type** > **Image File**, and click **Finish**.

Figure 68. Updating Discovered Elements Type to Image File



9. Click **Associate** to associate the selected element with the **VMware VM** resource type and click **Finish**.

Figure 69. Associating Resource Types

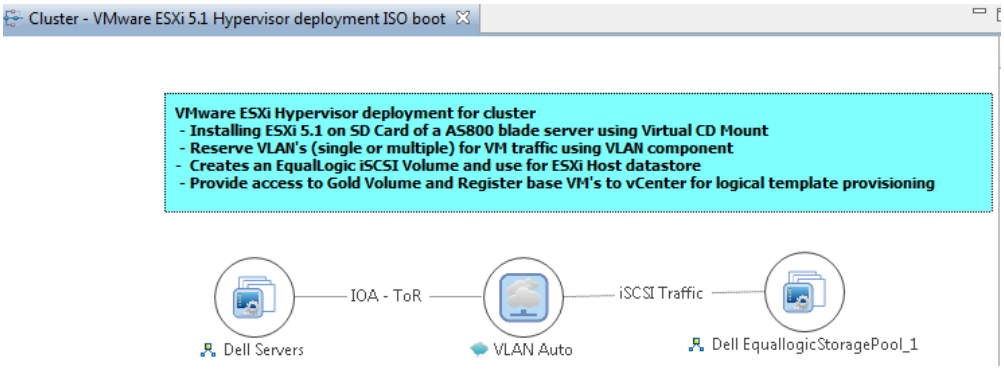


4 Physical Templates and Orchestration

4.1 Multiple Blade Server for Cluster Provisioning

Template '*Cluster - VMware ESXi 5.1 Hypervisor deployment ISO boot' and 'Cluster - VMware ESXi 5.1 Hypervisor deployment PXE boot'* can be used for installing ESXi 5.1 on an SD card/hard disk, respectively, using PXE / ISO Boot. You can specify one or more blade servers using this template for creating a cluster.

Figure 70. Multiple Blade Server for Cluster Provisioning



When this template is scheduled, this template performs the following sequence of operations:

1. Reserves single or multiple VLANs for VM traffic using a VLAN component. Ifthe VLAN reserved in the session is not already configured on the ToR switches, then the VLANs are created and tagged to appropriate port-channels.
2. IOA Configuration
    a. The VLAN IDs provided for Network1, Network2, Network4, and VLAN component in the physical template are created on the IOA server facing interfaces as Tagged VLANs.
    b. The Native VLAN ID provided for Network1 is added as Un-Tagged VLAN on the server facing interface.
    c. The Native VLAN ID is mandatory for PXE boot scenario.
3. NIC Partitioning
    a. NIC Partitioning is enabled on the CAN.
    b. NIC Partitioning is only supported Broadcom CNA.
4. Set NIC Attributes
    a. Configure the Min and Max Bandwidth
    b. Enable / Disable iSCSI Offload on the NIC Partitions
    c. Enable LAN Mode
    d. Enable the Legacy boot protocol for PXE Boot scenario

5. Create the ISO files for each server dynamically based on the Server IP Address, Hostname, Name server values provided in the database.
6. Mount the ISO using iDRAC Virtual Media on all the Servers and initiate the installation process.
7. Configure the vSwitch configuration
    a. Create the vSwitch and port-groups based on Active System 800 deployment specification
    b. Tag the port-groups with appropriate VLANs as specified in the template
    c. Create iSCSI Port-groups and install / configure the MEM VIBs
8. Create a volume of the EqualLogic Storage Array
    a. The new volume is created per physical session based on the size specified in the Orchestration input.
    b. The authentication of the new volume is configured based on the Chap username and secret key specified in the inventory database of the servers.
9. Create vCenter Cluster / Datacenter (if not already exists) on the specified vCenter. The cluster is created with default settings (DRS - On, HA - On, EVC - Disabled).

    Note: The cluster name passed as an argument must not be the Management cluster.
10. Add hosts to the vCenter cluster.
11. The datastore created in the orchestration is used for provisioning the VM in the logical workload templates. Provides access to Gold volume and using Gold volume, creates base VMs.
12. Installs EqualLogic MEM modules. The MEM package is transferred to the volume created in the above step to enable the installation.
13. Registers base VMs to the vCenter for logical template provisioning.

Note:

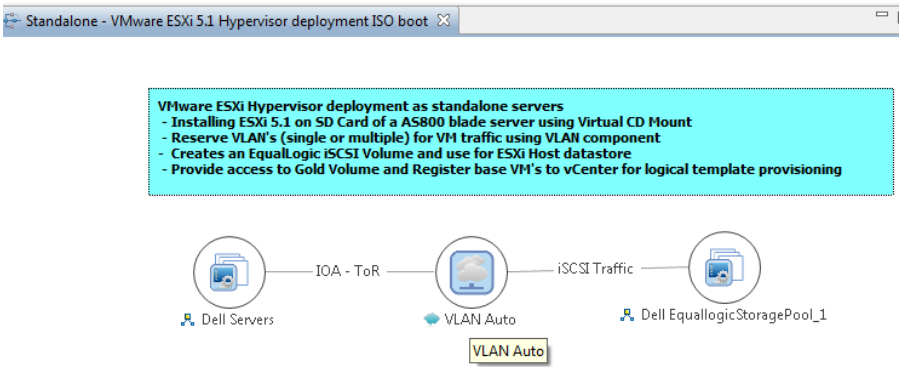
You should update the template for necessary inputs before scheduling this template for cluster provisioning. For details, see the

4.5 Updating Physical Templates section.

4.2 Single Blade Server for Standalone ESX Host Provisioning

Template *'Standalone—VMware ESXi 5.1 Hypervisor deployment with SD Card with vSwitch' and 'Standalone - VMware ESXi 5.1 Hypervisor deployment with HDD with vSwitch'* can be used for installing ESXi 5.1 on an SD card/hard disk, respectively, using PXE / ISO Boot. User could specify one or more blade servers for standalone ESXi host provisioning.

Figure 71. Single Blade Server for Standalone ESX Host Provisioning



When this template is scheduled, this template performs the following sequence of operations:

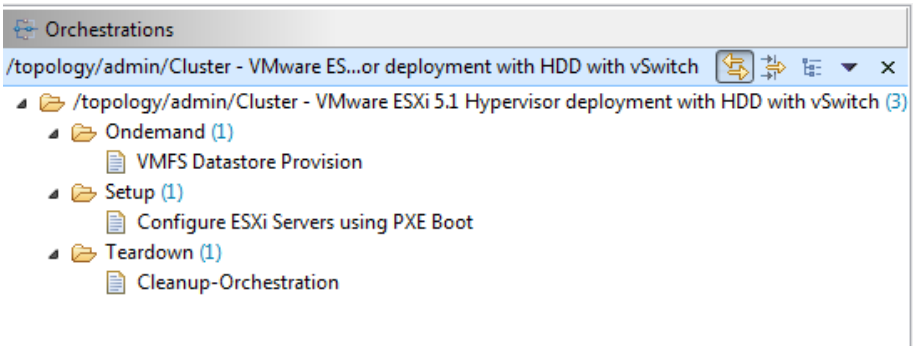
1. Reserves single or multiple VLANs for VM traffic using a VLAN component. Ifthe VLAN reserved in the session is not already configured on the ToR switches then the VLAN are created and tagged to appropriate port-channels.
2. IOA Configuration
    a. The VLAN IDs provided for Network1, Network2, Network4 and VLAN component in the physical template are created on the IOA server facing interfaces as Tagged VLANs.
    b. The Native VLAN ID provided for Network1 is added as Un-Tagged VLAN on the server facing interface.
    c. The Native VLAN ID is mandatory for PXE boot scenario.
3. NIC Partitioning
    a. NIC Partitioning is enabled on the CAN.
    b. NIC Partitioning is only supported Broadcom CNA.
4. Set NIC Attributes
    a. Configure the Min and Max Bandwidth
    b. Enable / Disable iSCSI Offload on the NIC Partitions
    c. Enable LAN Mode
    d. Enable the Legacy boot protocol for PXE Boot scenario
5. Create the ISO files for each server dynamically based on the Server IP Address, Hostname, Name server values provided in the database.
6. Mount the ISO using iDRAC Virtual Media on all the Servers and initiate the installation process.

7. Configure the vSwitch configuration
    a. Create the vSwitch and port-groups based on Active System 800 deployment specification
    b. Tag the port-groups with appropriate VLANs as specified in the template
    c. Create iSCSI Port-groups and install / configure the MEM VIBs
8. Create a volume of the EqualLogic Storage Array
    a. The new volume is created per physical session based on the size specified in the Orchestration input.
    b. The authentication of the new volume is configured based on the Chap username and secret key specified in the inventory database of the servers.
9. Add hosts to the vCenter at datacenter level.
10. The datastore created in the orchestration is used for provisioning the VM in the logical workload templates. Provides access to Gold volume and using Gold volume, creates base VMs.
11. Installs EqualLogic MEM modules. The MEM package is transferred to the volume created in the above step to enable the installation.
12. Registers base VMs to the vCenter for logical template provisioning.

4.3 Associated Orchestrations with Cluster and Standalone Host Templates

Each physical template has three orchestrations associated with it:

Figure 72. Orchestrations



1. **On-demand**—*VMFS Datastore Provision* TBD Per Jerry Ness, need more detail around the missing task that a VMFS datastore LUN for the GOLD images must be initially created on the storage before the logical templates can be run.

   This orchestration can be executed on-demand when the session is in a Running state.

2. **Setup**—*Configures the ESXi Servers using PXE Boot*

   This orchestration executes when template provisioning starts and the session is in the Setting Up state.

3. **Teardown**—*Cleanup-Orchestration*

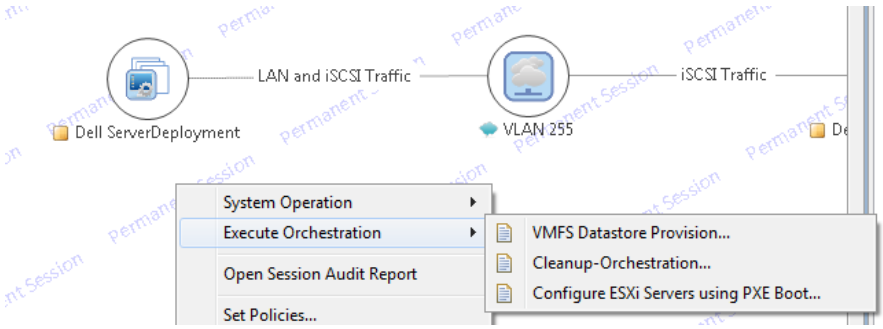
   This orchestration executes when template provisioning start and session is in Setting-up state.

4.4 Additional Storage for Cluster or Host

For additional VMFS storage or datastore need on a cluster or standalone ESXi host reserved through the Active System Manager, you can execute on-demand orchestration from a Running session.

For executing the on demand orchestration, open the session by double-clicking it. On the session, right click and select the **VMFS Datastore Provisioning** orchestration for execution.

Figure 73. VMFS Datastore Provision



When executed, orchestration performs the following sequence of operations:-

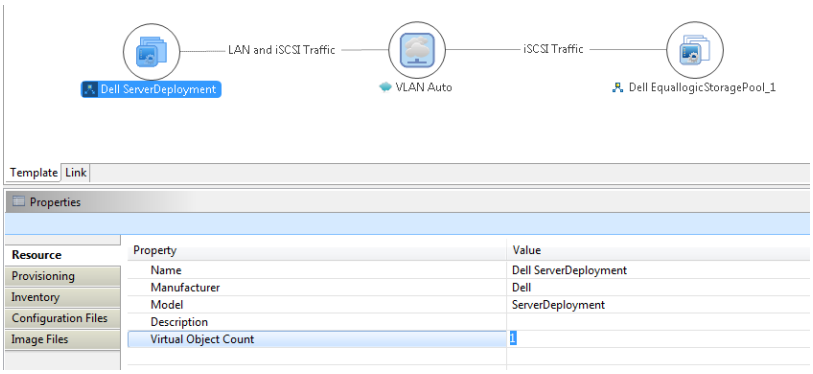
- Creates a new volume on EqualLogic storage.
- Allows access to specific cluster or standalone ESXi hosts, as applicable.
- Creates a VMFS datastore on a cluster or standalone ESXI hosts, as applicable.

4.5 Updating Physical Templates

To update cluster and standalone templates that require specific data before scheduling a template for cluster provisioning, perform the following steps:

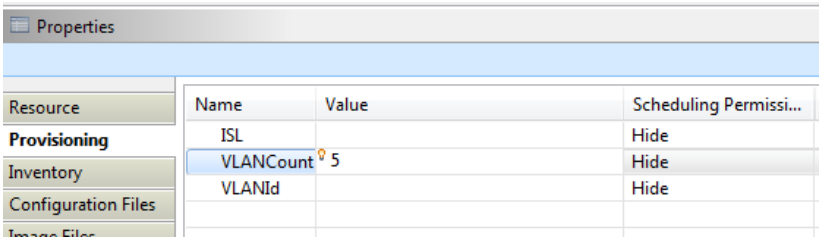
1. Update the template for a blade server. (Updates the blade server count for cluster provisioning.)

Figure 74. Updating Template for Blade Server



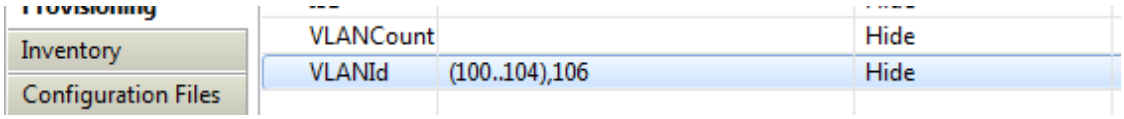
2. Save the template by **Ctrl**+**S** or by selecting the save icon on the thick client after making the changes.
3. Update the template for VLANs.

Figure 75. Updating Template for VLANs



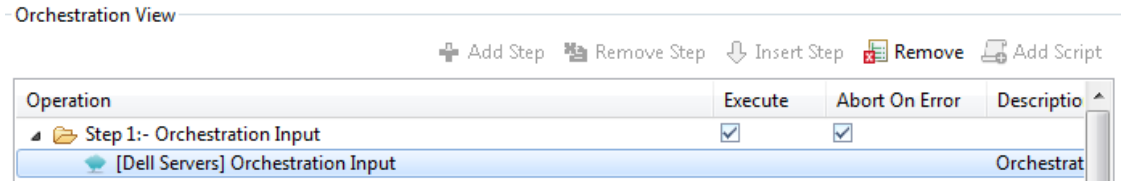
4. Select the **VLAN Component**, click the **Inventory** tab, and update the **VLANCount** with the number of VLANs to be provisioned.
5. Update the VLAN ID range, as applicable, and update the *VLANId* parameter.

Figure 76. Updating VLAN ID Range and Parameter



6. Save the template.
7. Provide input to the orchestration using one of two methods.

Figure 77. Orchestration Input



a. Double-click the **Configure ESXi Server using PXE Boot** orchestration to open it.

b. Double-click the **Orchestration Input** method to provide other inputs to orchestration.

Figure 78. Orchestration Input

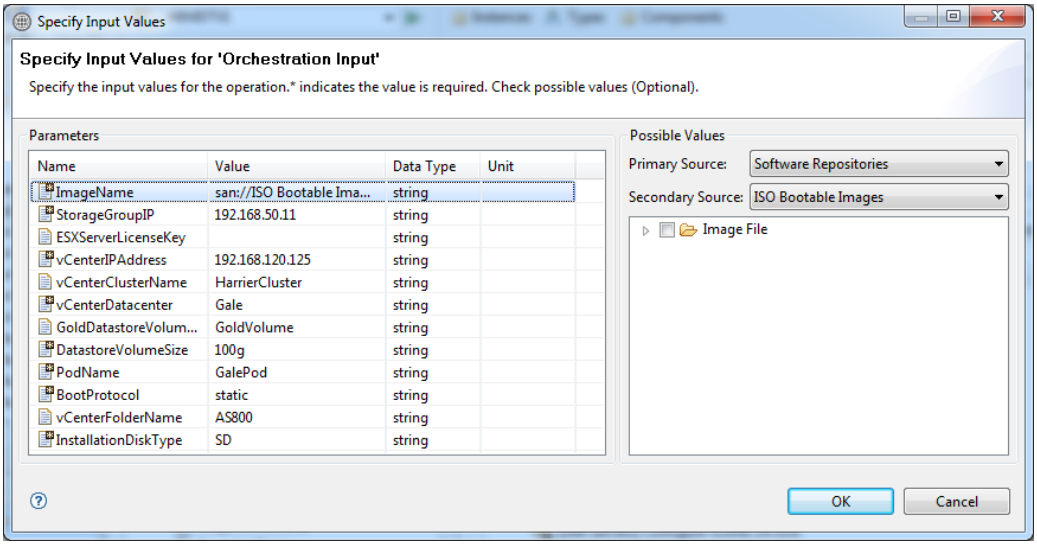


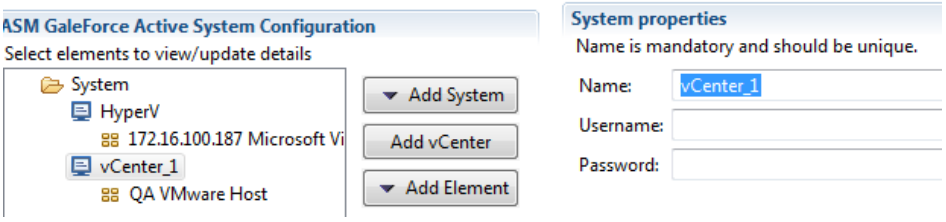
Table 6 lists and defines the available Orchestration Input parameters.

Table 6. Orchestration Input Parameters

Parameter	Description
ImageName	Selects the ESXi image from the repository. The orchestration is already mapped with an existing ESXi image available on the appliance.
ESXServerLicenseKey	License key for the VMware ESXi hosts that will be provisioned by the orchestration.
vCenterIPAddress	vCenter IP Address as provided in the Discovery Setup configuration.
vCenterClusterName	vCenter cluster name that will be provisioned by the orchestration. **Note: The cluster name passed as an argument must not be the Management cluster.**

Parameter	Description
vCenterDatacenter	vCenter data center to be used for provisioning.
GoldDatastoreVolumeName	Volume name consisting of baseline VM images that will be used for cloning new VMs.
DatastoreVolumeSize	Size in GB of the datastore to be provisioned on servers or a cluster.
StoragePoolName	Name of the pool on which the volume should be created for provisioning the datastore. This input should be provided from the EqualLogic Resource Pool repository.
BootProtocol	DHCP/Static. Default is static. If the IP address of the server is expected to come from DHCP server.
vCenterFolderName	(optional) The vCenter folder where the ESXi hosts needs to be provisioned during the orchestration
InstallationDisk	**SD** (the default) | **HDD**. If the installation must be performed on the server HDD, then value needs to be updated. *Note: The BIOS boot order needs to be updated manually*

Figure 79. vCenter_1 System Properties

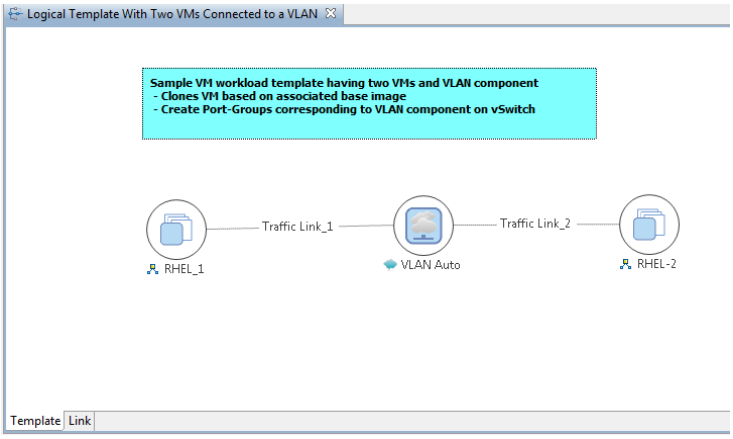


5 Workload Provisioning Using Logical Templates

5.1 Two VMs with a VLAN

The *Two virtual machine with a VLAN* Logical template can be used to create VM workloads by scheduling a logical template over existing physical resources sessions, to consume the compute and storage resources of specific physical components.

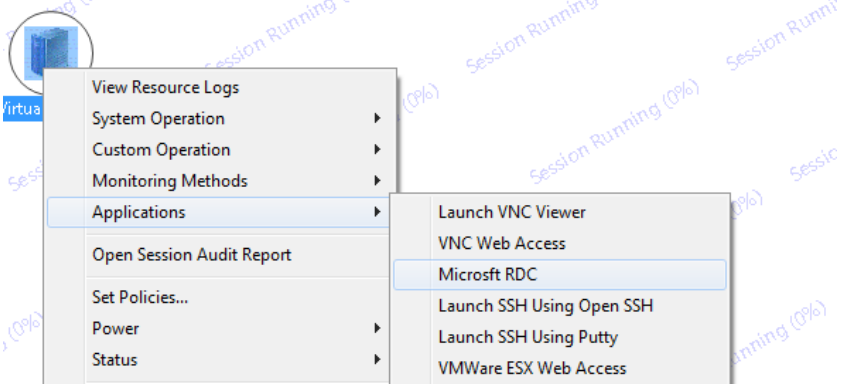
Figure 80. Two VMs Connected to a VLAN



When scheduled, this template performs the following sequence of operations:

- Clones and powers on two VMware VMs based on the Gold VM Image associated in the template.
- Creates port-groups corresponding to VLAN component on vSwitch, as can also be seen in the annotation in the template screenshot below.
- Once the VMs are provisioned the user can also launch custom applications as applicable using custom methods from Active System Manager- Windows client.
- For Application launch,
- Select a VM in a session
- Right click on the VM
- Select the Applications
- Select the Application to be launched

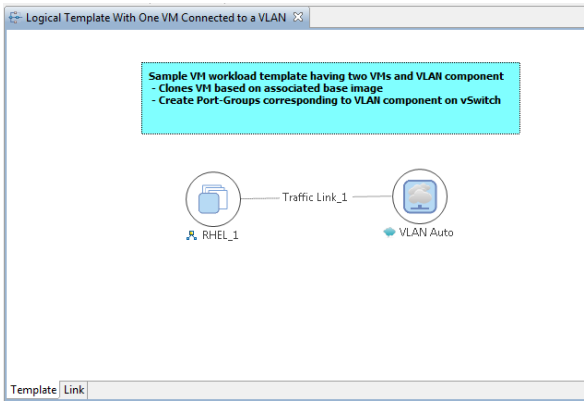
Figure 81. Applications > Microsoft RDC



5.2 Single Virtual Machine with VLAN

The *Single virtual machine with a VLAN* Logical template can be used to create VM workloads by scheduling logical template over existing physical resources session, to consume the compute and storage resources of specific physical components.

Figure 82. Single VM Connected to a VLAN



When scheduled, this template performs the following sequence of operations:-

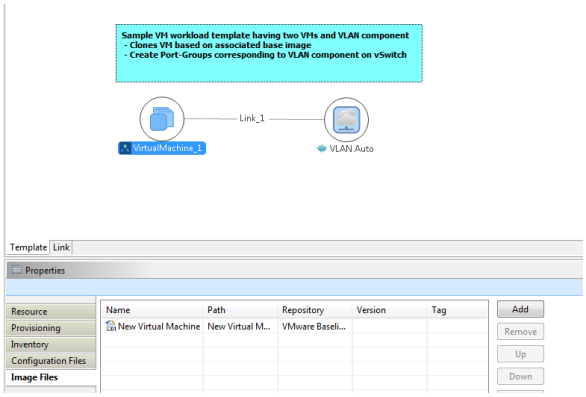
- Clones and powers on a single VMware VMs based on the Gold VM image associated in the template.
- Creates port-groups corresponding to a VLAN component on the vSwitch (see Figure 55).
- Once the VMs are provisioned, you can also launch custom applications using custom methods from the Active System Manager Windows client.

5.3 Updating a Baseline VM Image on Logical Templates

To update the baseline VM image associated with the VM object in the template, perform the following steps:

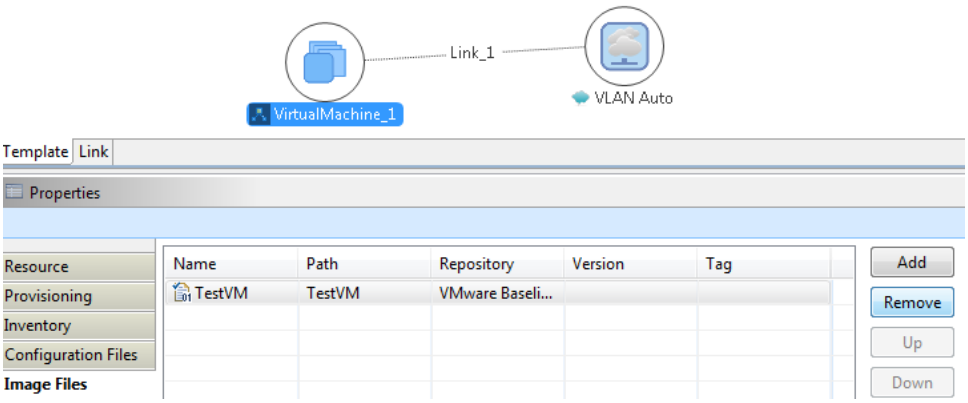
1. Select the VM object in the template and click the **Image Files** tab.

Figure 83. Image Files Properties



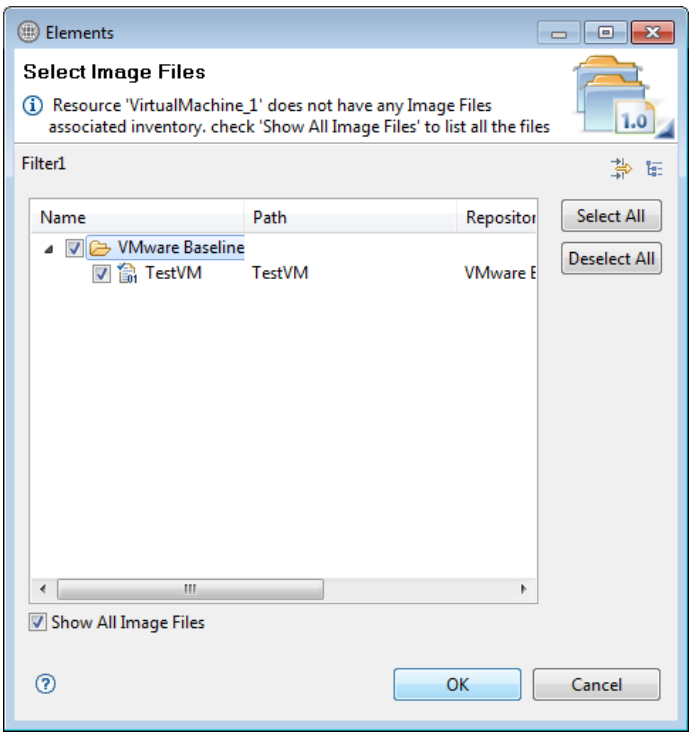
2. Select the already associated image file and click **Remove** to remove the existing association.

Figure 84. Remove the Association



3. Click **Add** and select the gold VM image to be associated with the VM object.

Figure 85. Select Gold VM Image File



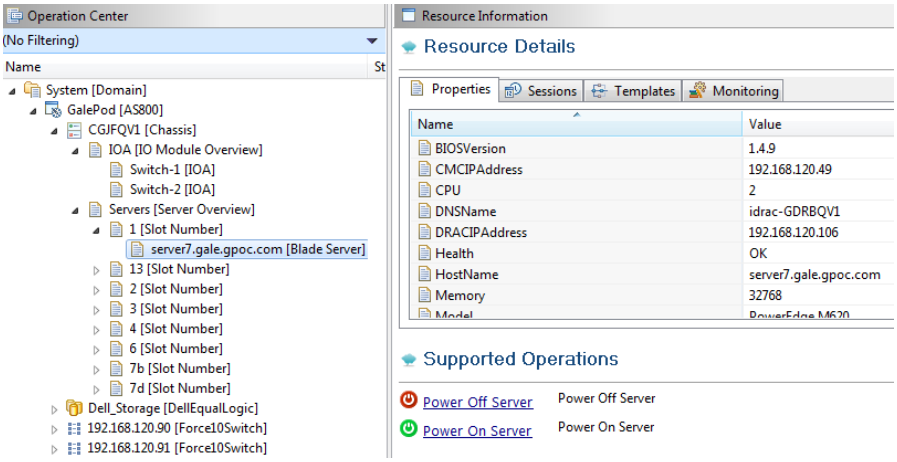
6 Operation Center View—Administrative Operations

6.1 Managing Blades

The following operations are provided on the Active System Manager Server Operation Center view to perform administrative tasks:

- Power On Server—Used to power on the blade server using server iDRAC.
- Power Off Server—User to power off the blade server using server iDRAC. The migration of the VMs running on the server will be taken care by the VMware vMotion capability.

Figure 86. Supported Operations



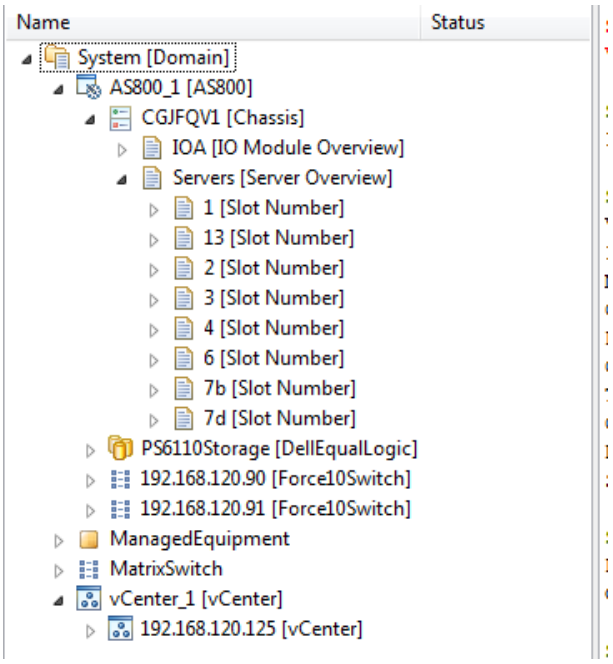
6.2 Managing vCenter Objects

This section describes the following VMware vCenter managed objects:

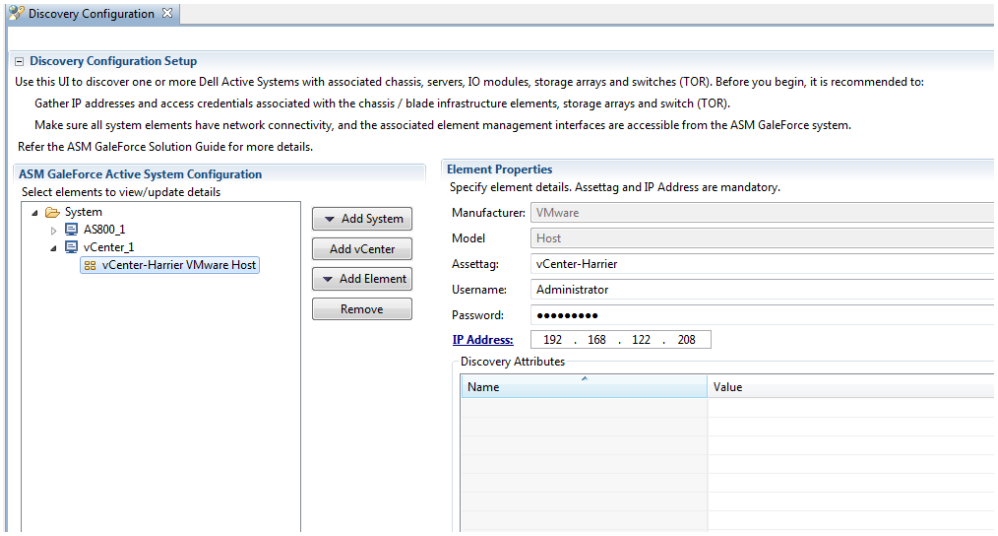
- 6.2.1 Clusters and Hosts
- 6.2.2 VMware vSwitches
- 6.2.3 VMware Datastores

Specifically, this section describes how these managed objects can be directed through Active System Manager—Operation Center view. The vCenter discovery can be initiated using the Active System Manager Discovery facility, which populates the Operation Center view of the Active System Manager.

Figure 87. Operation Center View



To initiate the discovery of a VMware vCenter, various discovery elements and their corresponding attributes can be provided as shown below in the Discovery Configuration Setup wizard; steps for configuring the Discovery setup for a vCenter are detailed in the Discovery Configuration Setup section.



6.2.1 Clusters and Hosts

Clusters and hosts, along with their attributes, are discovered and populated in the Active System Manager Operation Center view. This view enables methods to be executed on clusters and hosts for on demand provisioning, as required.

Figure 88. Clusters and Hosts (Example 1)

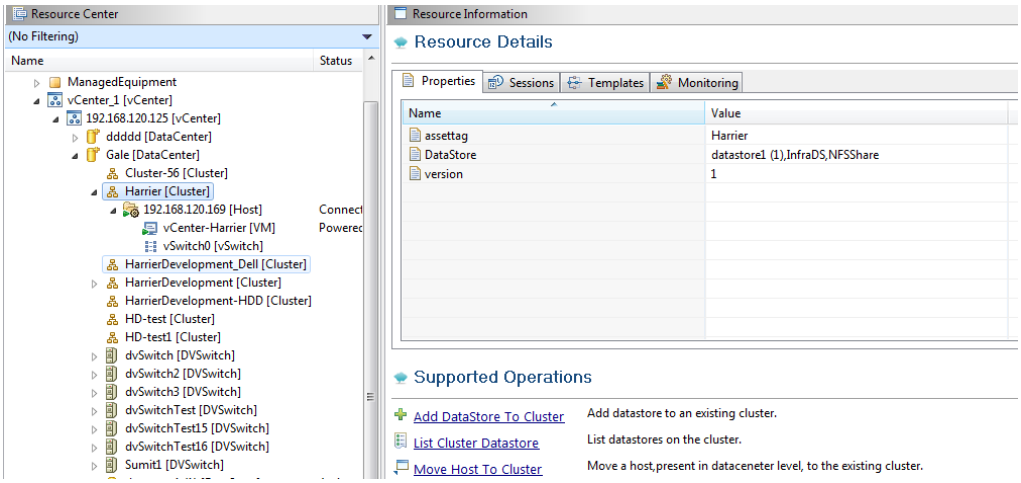
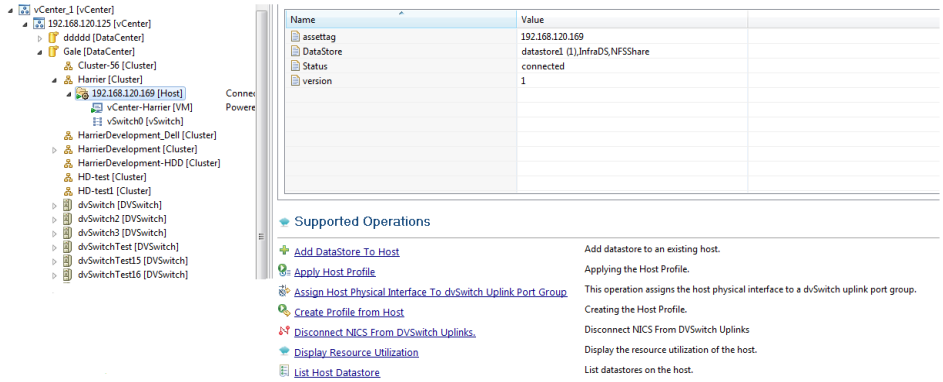


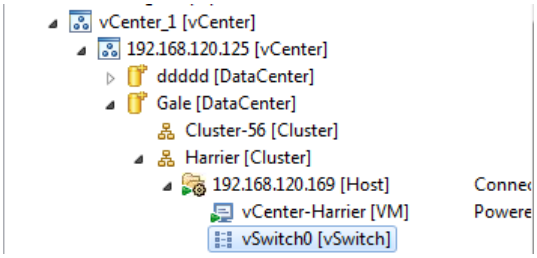
Figure 89. Clusters and Hosts (Example 2)



6.2.2 VMware vSwitches

Hosts vSwitches are also discovered and populated in the Operation Center view as part of the vCenter Discovery process.

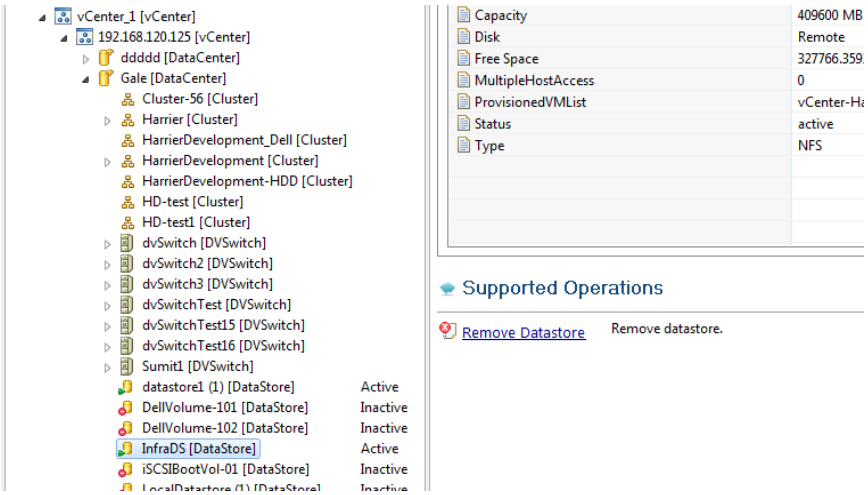
Figure 90. VMware vSwitches



6.2.3 VMware Datastores

Datastores are one of the most important components of the VMware-based virtualized infrastructure. The Active System Manager supports the discovery of datastores managed by the vCenter. The various attributes of a datastores are also discovered and populated in the Operation Center view.

Figure 91. VMware Datastores



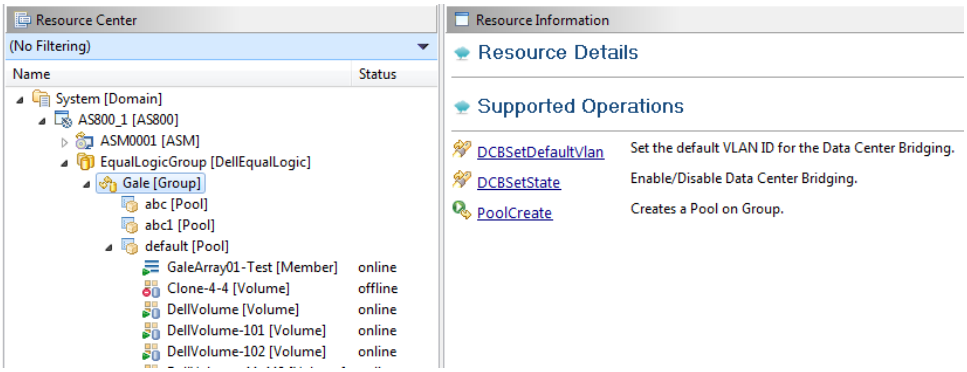
6.3 Managing EqualLogic Storage

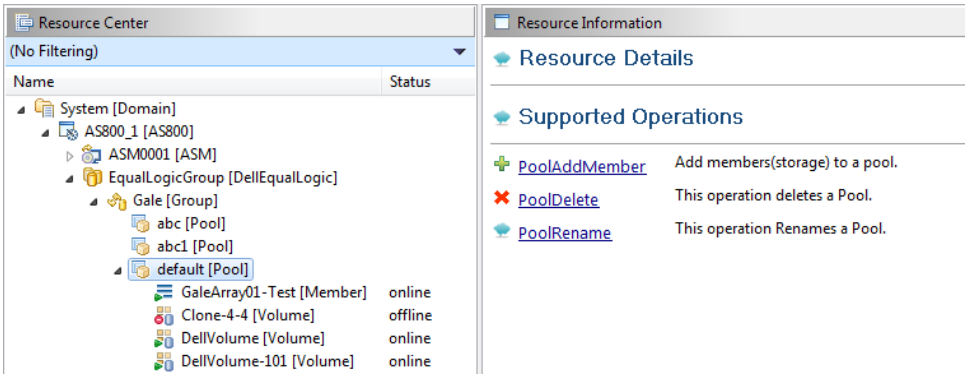
Table 7 lists and defines the members provided in the Active System Manager EqualLogic Storage Operation Center view.

Table 7. EqualLogic Group Members

Operation	Description
PoolCreate	Creates a new Storage Pool on an EqualLogic Storage Array.
PoolAddMember	Adds a Storage Array to a given Storage Pool on an EqualLogic Storage Array.
PoolDelete	Deletes a Storage Pool present on an EqualLogic Storage Array.
PoolRename	Renames an existing Storage Pool present on an EqualLogic Storage Array.

Figure 92. EqualLogic Group Members





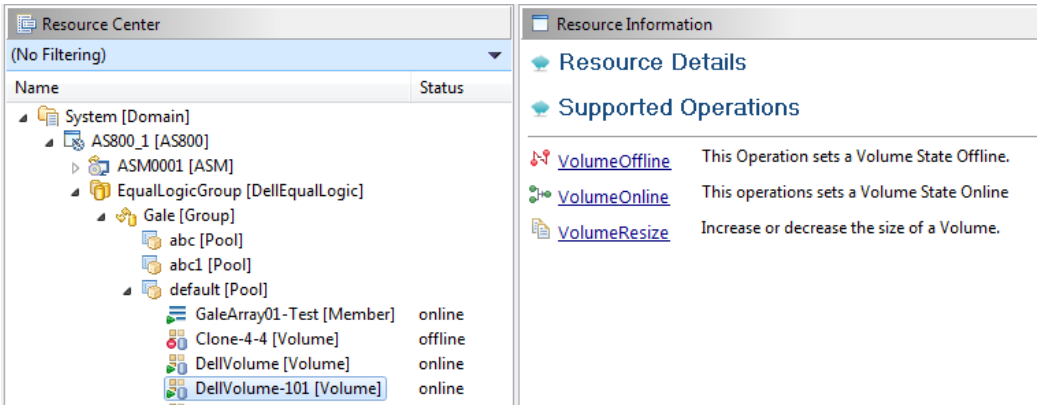
6.4 Managing Volume

Table 8 lists and defines the operations provided in the Active System Manager EqualLogic Storage Operation Center view. The figure displays an example of EqualLogic group members.

Table 8. EqualLogic Group Members

Operation	Description
VolumeOffline	Offlines a volume present on an EqualLogic Storage Array.
VolumeOnline	Onlines a volume present on an EqualLogic Storage Array.
VolumeResize	Resizes a volume present on an EqualLogic Storage Array

Figure 93. EqualLogic Group Members



6.5 Setting Up Storage

The following operations are provided on the Active System Manager EqualLogic Storage Operation Center view for performing administrative tasks:

- Storage group-level supported operations
- Storage member-level supported operations

Figure 94. Storage Group-Level Supported Operations

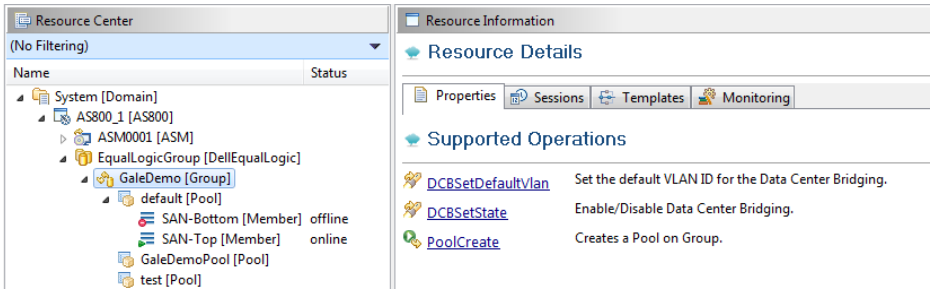


Table 9. Storage Group-Level Supported Operations

Operation	Description	Input Parameter
DCBSetDefaultVlan	Sets a default VLAN ID for Data Center Bridging (DCB) on an EqualLogic Storage Array	*vLanId*—Default vLanId for dcb
DCBSetState	Enables or disables DCB on an EqualLogic Storage Array.	*dcbState* {**enable** | **disable**}
PoolCreate	Creates a new storage pool in the storage group.	*poolName*—Storage pool name

Figure 95. Storage Member-Level Supported Operations

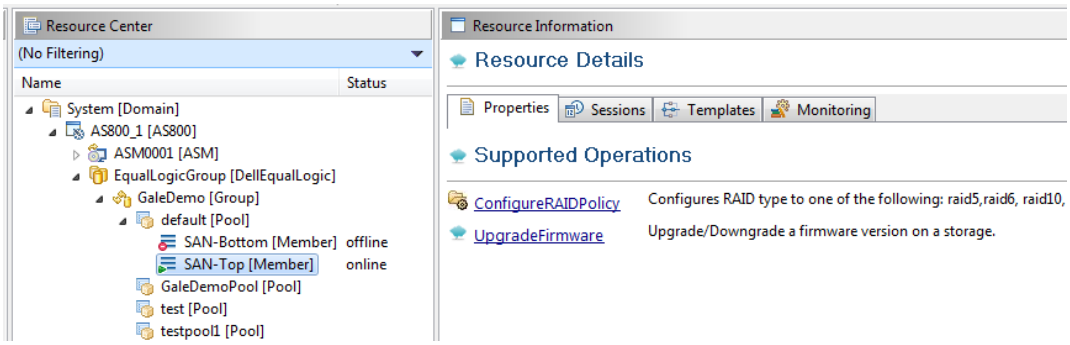


Table 10. Storage Member-Level Supported Operations

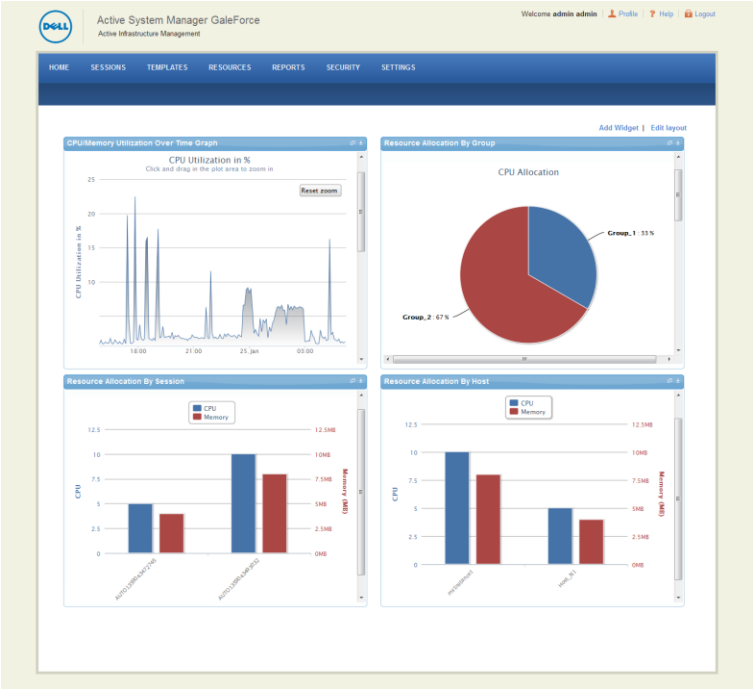
Operation	Description	Input Parameter
ConfigureRAIDPolicy	Configures the required redundant array of independent disks (RAID) level on an EqualLogic Storage Array.	*raidType* {**raid6** | **raid10** | **raid50**}
UpgradeFirmware	Upgrades the firmware image on an EqualLogic Storage Array.	*imageName*—Image from repository. *delayInMinutesAfterRestart*—Introduce wait once the firmware is installed and the member storage device is restarted, the RA connects the storage after this defined delay (in minutes) after the restart parameter.

7 Dashboard Reports

7.1 Resource Allocation by Sessions Report

This report provides resource allocation data for sessions which are in a Running state. This report displays CPU and memory allocations grouped by Active System Manager sessions, and can be used to view the CPU and memory allocation in a data center environment at that particular instant. The figure displays an example of a Resource Allocation by Sessions report.

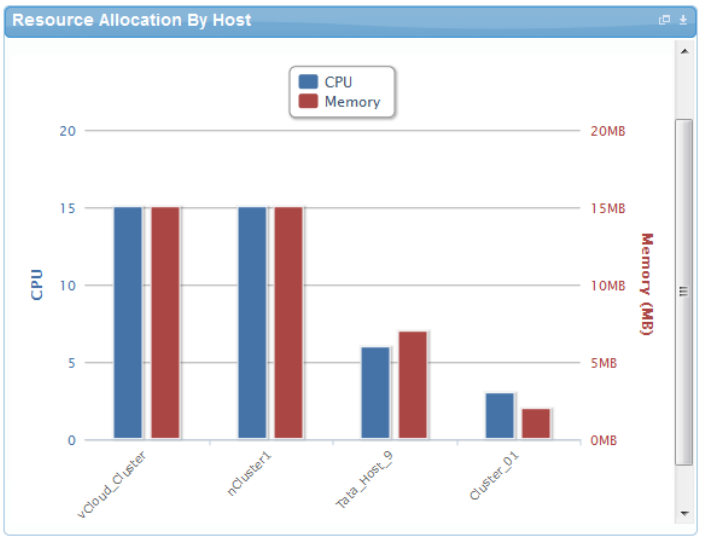
Figure 96. Resource Allocation by Sessions Report



7.2 Resource Allocation by Hosts Report

This report provides resource allocation data for hosts on which some virtual resources are provisioned in running sessions. This report displays CPU and memory allocations grouped by hosts, and can be used to view a current usage of the CPU and memory allocation per host for a data center. The figure displays an example of a Resource Allocation by Hosts report.

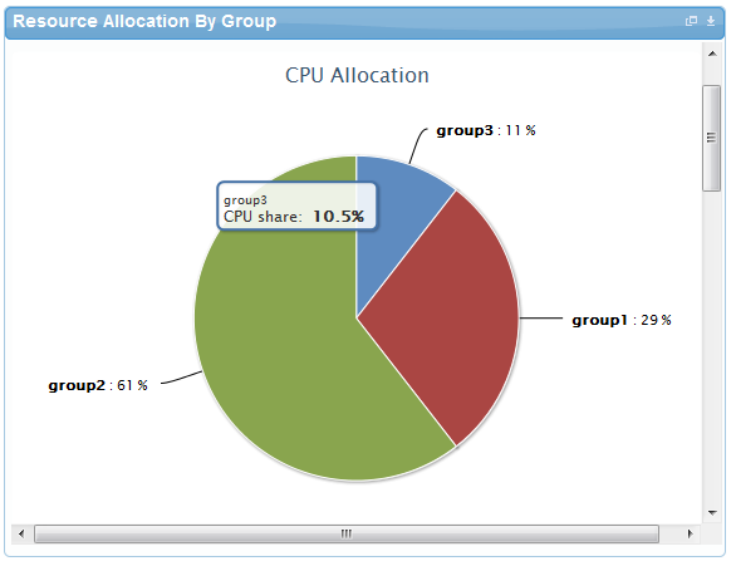
Figure 97. Resource Allocation by Hosts Report



7.3 Resource Allocation by Groups Report

This report provides resource allocation data for virtual resources that are utilized in sessions owned by members of a group (grouped by group name). This report also captures the current allocation by groups and works for CPU and memory allocation. The figure displays an example of a Resource Allocation by Groups report.

Figure 98. Resource Allocation by Groups Report



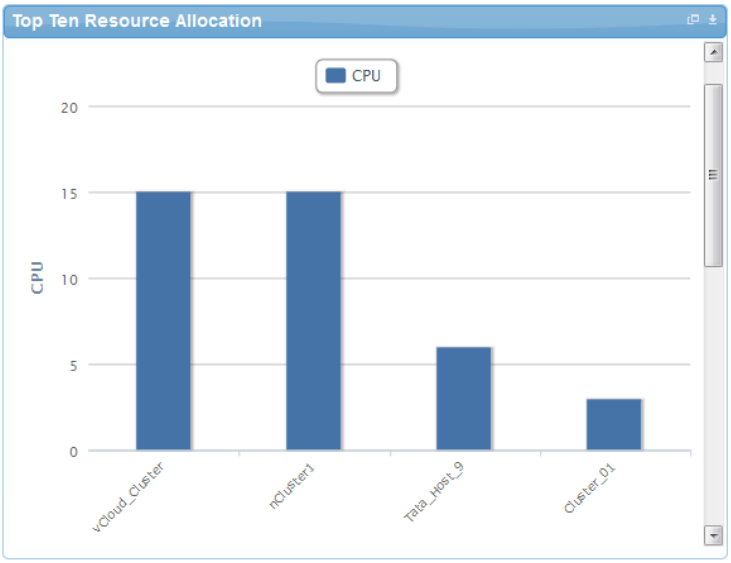
7.4 Top Ten Resource Allocation Report

This report includes three sub-options for different groupings:

- **By Host**—Lists top ten hosts which are currently in use and have allocated maximum CPU and memory attributes.
- **By User**—Displays the list of top 10 users who are currently consuming the maximum number of CPUs and memory.
- **By Group**—Similar to “By User”, but consolidated at the group level.

The figure displays an example of a Top Ten Resource Allocation report.

Figure 99. Top Ten Resource Allocation Report



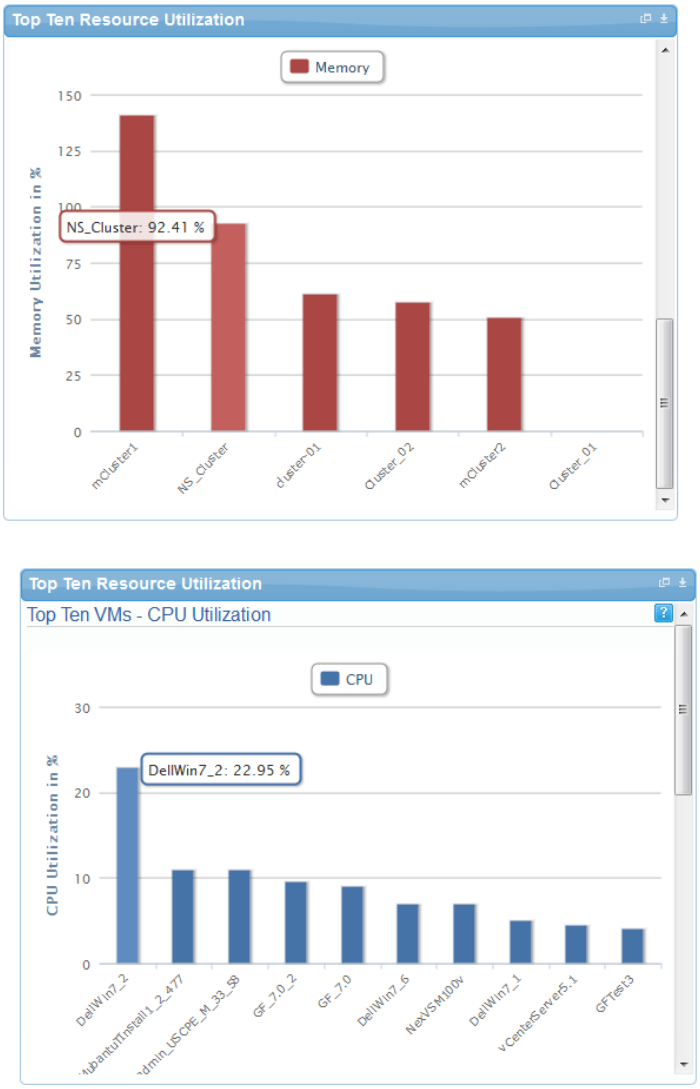
7.5 Top Ten Resource Utilization Report

This report is similar to the Top Ten Resource Allocation report; however, this report provides utilization data as opposed to allocation. The required data is made available using a monitoring method that continuously keeps polling the device, VM, or cluster for current utilization data. The data is persisted in the database and the last polled data is provided to the user. This report can be grouped by the following:

- VMs
- Hosts
- Clusters
- Storage

The figure displays an example of a Top Ten Resource Utilization report.

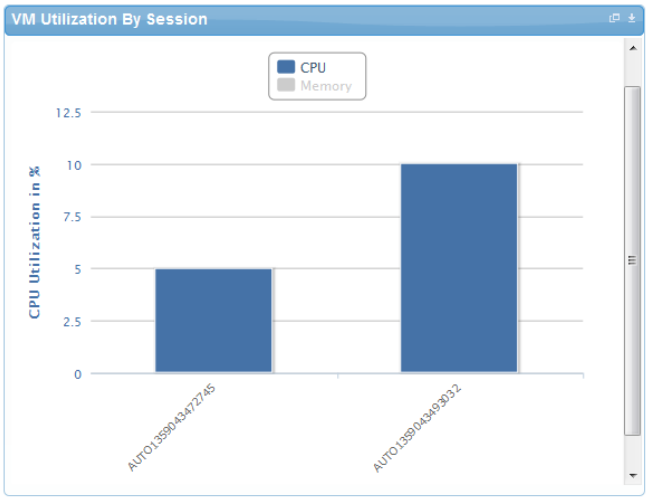
Figure 100. Top Ten Resource Utilization Report



7.6 VM Utilization by Session Report

This report provides the most recent data for CPU and memory utilized on any VM, grouped by sessions. This data is available in terms of percentage with respect to the allocated limits. The figure displays an example of a VM Utilization by Session Report.

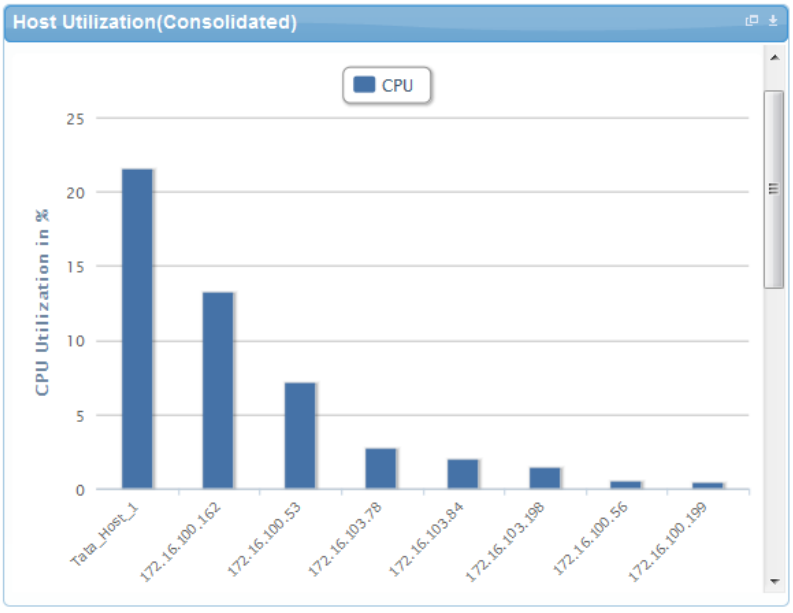
Figure 101. VM Utilization by Session Report



7.7 Host Utilization (Consolidated) Report

This report displays information about how much capacity is being utilized on a host by all running VMs, with respect to the allocated capacity. This report is available for CPU and memory attributes. The figure displays an example of a Host Utilization (Consolidated) report.

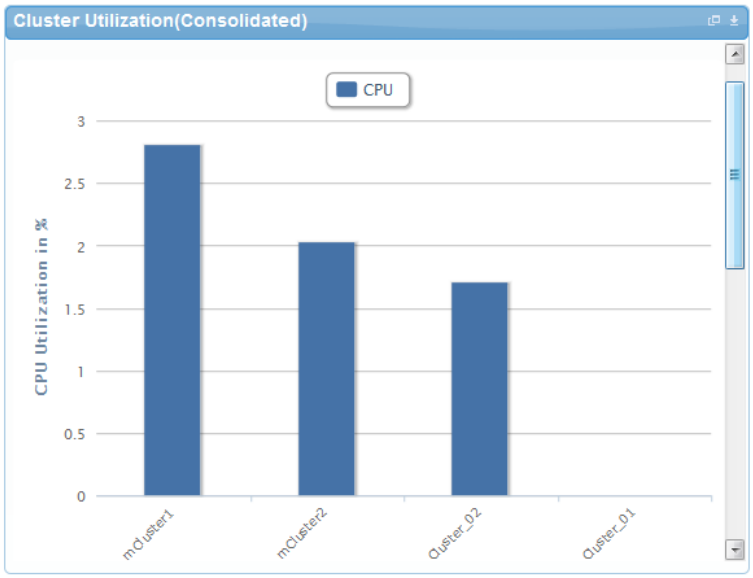
Figure 102. Host Utilization (Consolidated) Report



7.8 Cluster Utilization (Consolidated) Report

This report is similar to the Host Utilization (Consolidated) report, except that it works for clusters. The figure displays an example of a Cluster Utilization (Consolidated) report.

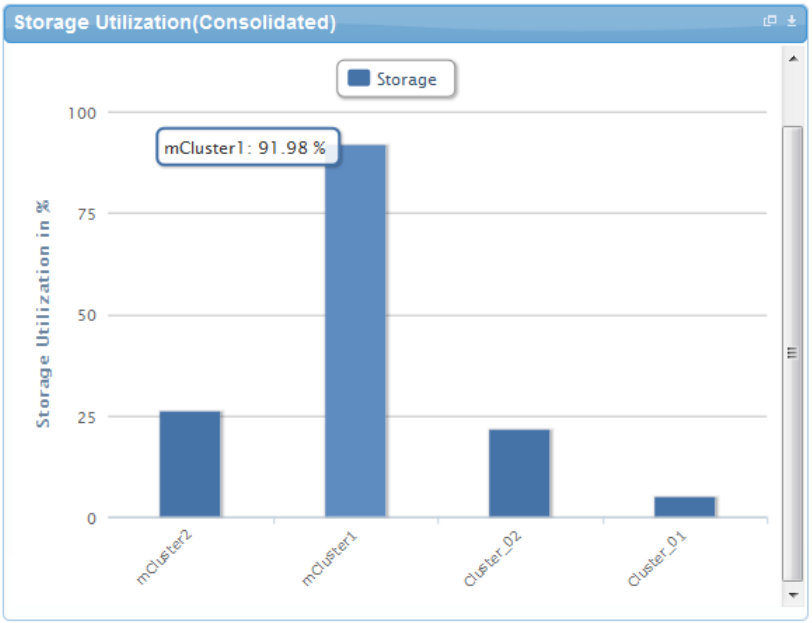
Figure 103. Cluster Utilization (Consolidated) Report



7.9 Storage Utilization (Consolidated) Report

This report provides storage utilization as a percentage of allocated storage for clusters. The figure displays an example of a Storage Utilization (Consolidated) Report.

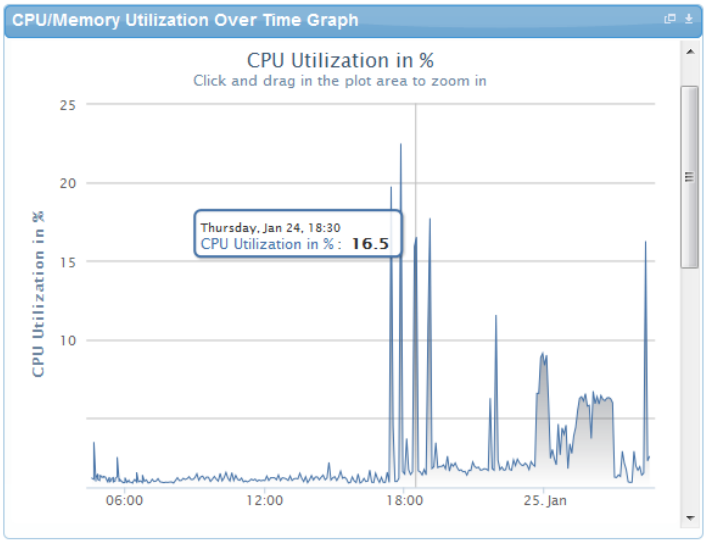
Figure 104. Storage Utilization (Consolidated) Report



7.10 CPU and Memory Utilization Showback Report

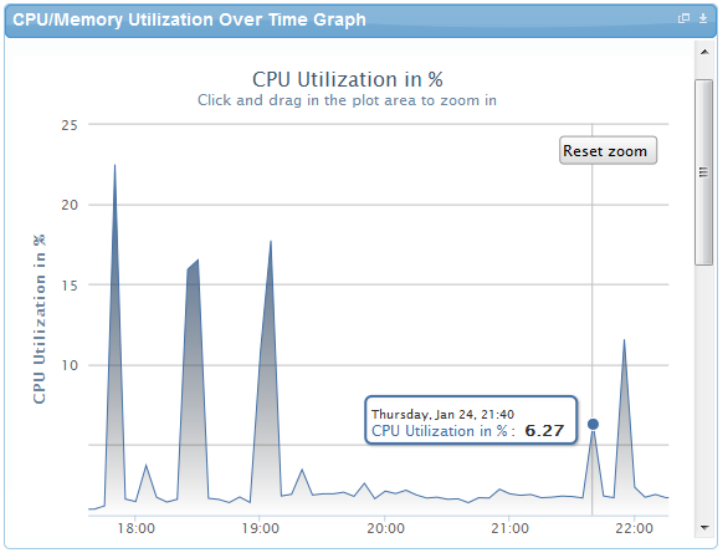
This report provides CPU and memory utilization of Hosts in percentage over a period of given time (e.g. Weekly, Daily, and Hourly). The figure displays an example of a CPU and Memory Utilization Showback report.

Figure 105. CPU & Memory Utilization Showback Report



You can view the data for a specific time interval (with a minimum time interval limit of ten minutes between two data points). To view the specific time interval data, select a point and drag the mouse to a desired data point; this will show the data for the specific time interval. You can rest the time interval to default by clicking **Reset Zoom**.

Figure 106. Reset Zoom



A Appendix A—Deployment Activities

A.1 Verifying Active System Manager Services

To verify that all Active System Manager services are up and running, perform the following steps:

1. Log in as the user who installed the services.
2. Run the following script to display the current status of all services, including the Oracle database status:

```
cd asm-galeforce/gf/sbin
./gfstatus.sh
```

Below is sample output:

```
                    Active System Manager Services Status


Installation
----------------
Release Version: 7.0
Build Number: 21286

Database
----------------
Vendor: Oracle (Ver: 11.2.0.1.0)
Host: asm-galeforce Port: 1521
Service name: DB11G
Status: Running

Active System Manager Service
---------------------------------
Host: asm-galeforce Port: 40500 Secure Port: 50500
Enterprise: Dell
Lab: DEMO
Status: Running

Domain Services
----------------
1. Domain     : System (Id: 1)
   Description:
   ------------------------------------------------------
   Session server
      Host: asm-galeforce  Port: 40500  Secure Port: 50500
      Status: Running
```

B Appendix B—Build of Materials

Table 11 displays a list of build of materials, grouped by Resource Adapters.

Table 11. Build of Material—Resource Adapters

Vendor	Model	Description
Dell	Chassis	Dell Chassis resource adapter using WSMAN and RACADM CLI used for discovery operations
Dell	Servers	Dell Servers resource adapter using WSMAN and RACADM CLI used for provisioning the servers
Dell	IOA	Management of IO Aggregator
Dell	EqualLogicPS6110	Management of EqualLogic storage
Dell	EqualLogicStoragePool	Management of EqualLogic storage pool
Dell	Force10-S4810	Management of ToR switches
Template	VMwareLib	VMware Host Provisioning on Blades
VMware	Host	VMware vCenter Management
VMware	Virtual Machine	VMware Virtual Machine Instance Management

Table 12 displays a list of build of materials, grouped by templates.

Table 12. Build of Material—Templates

ID	Description	Workflows
1—Physical	Cluster - VMware ESXi 5.1 Hypervisor deployment ISO boot	Configure ESXi Servers using ISO Boot, Cleanup-Orchestration, and VMFS Datastore Provision.
2—Physical	Cluster - VMware ESXi 5.1 Hypervisor deployment PXE boot	Configure ESXi servers using PXE Boot, Cleanup-Orchestration, and VMFS Datastore Provision.
3-Physical	Standalone - VMware ESXi 5.1 Hypervisor deployment PXE boot	Configure ESXi servers using PXE Boot, Cleanup-Orchestration, and VMFS Datastore Provision.
4-Physical	Standalone - VMware ESXi 5.1 Hypervisor deployment ISO boot	Configure ESXi servers using ISO Boot, Cleanup-Orchestration, and VMFS Datastore Provision.
5—Logical	Logical template with one VM connected to a VLAN	Built-in orchestration.

ID	Description	Workflows
6—Logical	Logical template with two VMs connected to a VLAN	Built-in orchestration.

C Appendix C—Firmware and Software Base Lineup

Table 13 displays a list of firmware and software base lineups, grouped by Hypervisor blades.

Table 13. Firmware and Software Base Lineup—Hypervisor Blades

Resource	Active System Manager 7.0
BIOS	1.6.0
CPLD	1.0.5
iDRAC7 Enterprise	1.35.35
LCC (Life Cycle Controller) 2	1.1.1.18
Network Controller Broadcom FW	7.4.8
EqualLogic MEM	1.1.1
VMware ESXi	5.1(799733) A02
Microsoft Hyper-V	NA

Table 14 displays a list of firmware and software base lineups, grouped by management blades.

Table 14. Firmware and Software Base Lineup

Resource	Active System Manager 7.0
BIOS	1.5.0
iDRAC7 Enterprise	1.35.35
LCC (Life Cycle Controller) 2	1.1.1.18
Network Controller Broadcom FW	7.2.20
EqualLogic MEM	1.1.1
VMware ESXi	5.1(799733) A02

Table 15 displays a list of firmware and software base lineups, grouped by chassis, storage, and switches.

Table 15. Firmware and Software Base Lineup—Chassis, Storage, Switches

Resource	Active System Manager 7.0
CMC	4.31
PowerEdge M I/O Aggregator 8.3.17.2	8.3.17.3
Force10 S4810 (LAN)	8.3.12.1
Force10 S55 (OOB)	8.3.5.3
EqualLogic PS Arrays	6.0.2 (R305616)

Table 16 displays a list of firmware and software base lineups, grouped by management VMs and software.

Table 16. Firmware and Software Base Lineup

Resource	Active System Manager 7.0
CMC	NA
PowerEdge M I/O Aggregator 8.3.17.2	NA
Force10 S4810 (LAN)	8.3.12.1
Force10 S55 (OOB)	8.3.5.3
EqualLogic PS Arrays	6.0.2 (R305616)

Table 17 displays a list of firmware and software base lineups, grouped by management VMs and software.

Table 17. Firmware and Software Base Lineup—Management VMs and Software

Resource	Active System Manager 7.0
Windows Server 2008 R2 Standard	N/A
VMware vCenter Server	5.1.0 (799731)
Dell EqualLogic Virtual Storage Manager (VSM)	3.5 EPA

Resource	Active System Manager 7.0
Dell OpenManage Plug-in for vCenter	1.6.0.33
Dell SAN HQ	2.5 EPA
VMware vCloud Connector	1.5
Dell OpenManage Essentials	1.1
Dell OpenManage Repository Manager	1.4.113

D Appendix D—Adding New ESXi PXE Images

This appendix describes the following topics related to adding new ESXi images:

- Preparing the VMware ESXi 5.x Installation Media
- Modifying the ESXi boot.cfg Configuration File
- Configuring the HTTP ServerCreating a Kickstart Configuration File

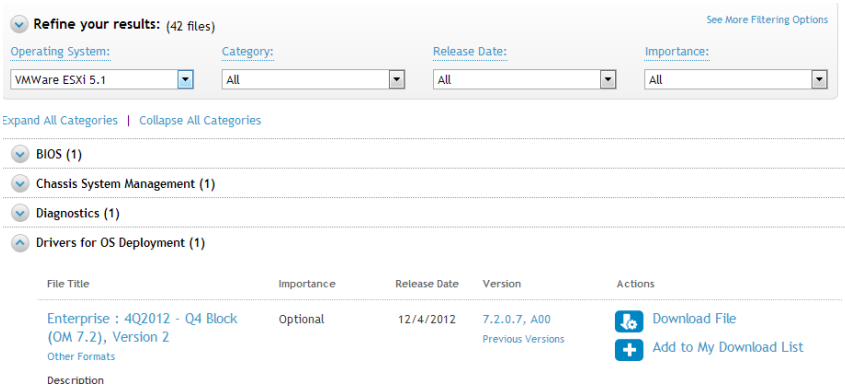
D.1 Preparing the VMware ESXi 5.x Installation Media

To prepare the VMware ESXi 5.x installation media, perform the following steps:

1. Log in to www.dell.com.
2. Open the support and driver page (http://www.dell.com/support/drivers/us/en/04/ProductSelector/Select?rquery=fkey-e-Drivers_PS)
3. Select **Server > Storage & Networking**.
4. Select **PowerEdge**.
5. Select **PowerEdge M620**.
6. Select **VMware ESXi 5.1**.

The image will be listed in the “Drivers for OS Deployment” section

Figure 107. Downloading the ISO Image



7. On your Trivial File Transfer Protocol (TFTP) server, simply extract the contents of the installation ISO into a new directory using the following commands (as the **root** user):

```
# mkdir /tmp/dellISO
# mkdir /tftpboot/esxi5.1_dell

# mount -o loop VMware-VMvisor-Installer-5.1.0-799733.x86_64-
Dell_Customized_RecoveryCD_A00.iso tmp/dellISO
# cp -fr /tmp/dellISO/* /var/lib/tftpboot/esxi5.1_dell/
# chmod +w /tftpboot/esxi5.1_dell/*
```

D.2 Modifying the ESXi boot.cfg Configuration File

To confirm that the installation source is not in the root of the TFTP server, perform the following steps:

1. Remove all slashes (/) from the **boot.cfg** file so that relative paths are used (vi :%s#/##g).
2. Add a "prefix" directive to the **boot.cfg** file to specify the proper subdirectory, from the perspective of the TFTP root:

```
# cat boot.cfg
bootstate=0
title=Loading ESXi installer
kernel=tboot.b00
kernelopt=ks=http://xx.xx.xx.xx/esxi5.1_dell/ks.cfg
modules=b.b00 --- useropts.gz --- k.b00 --- chardevs.b00 --- a.b00 --- user.b00
--- s.v00 --- misc_cni.v00 --- net_bnx2.v00 --- net_bnx2.v01 --- net_cnic.v00 -
-- net_tg3.v00 --- scsi_bnx.v00 --- scsi_bnx.v01 --- net_bna.v00 ---
scsi_bfa.v00 --- ima_be2i.v00 --- scsi_be2.v00 --- net_igb.v00 --- scsi_mpt.v00
--- ima_qla4.v00 --- net_qlcn.v00 --- scsi_qla.v00 --- ata_pata.v00 ---
ata_pata.v01 --- ata_pata.v02 --- ata_pata.v03 --- ata_pata.v04 ---
ata_pata.v05 --- ata_pata.v06 --- ata_pata.v07 --- block_cc.v00 ---
ehci_ehc.v00 --- weaselin.t00 --- esx_dvfi.v00 --- xlibs.v00 --- ipmi_ipm.v00 -
-- ipmi_ipm.v01 --- ipmi_ipm.v02 --- misc_dri.v00 --- net_be2n.v00 ---
net_e100.v00 --- net_e100.v01 --- net_enic.v00 --- net_forc.v00 ---
net_ixgb.v00 --- net_nx_n.v00 --- net_qlge.v00 --- net_r816.v00 ---
net_r816.v01 --- net_s2io.v00 --- net_sky2.v00 --- net_vmxn.v00 ---
ohci_usb.v00 --- sata_ahc.v00 --- sata_ata.v00 --- sata_sat.v00 ---
sata_sat.v01 --- sata_sat.v02 --- sata_sat.v03 --- sata_sat.v04 ---
```

```
scsi_aac.v00 --- scsi_adp.v00 --- scsi_aic.v00 --- scsi_fni.v00 ---
scsi_hps.v00 --- scsi_ips.v00 --- scsi_lpf.v00 --- scsi_meg.v00 ---
scsi_meg.v01 --- scsi_meg.v02 --- scsi_mpt.v01 --- scsi_mpt.v02 ---
scsi_rst.v00 --- uhci_usb.v00 --- tools.t00 --- scsi_qla.v01 --- dell_con.v00 -
-- xorg.v00 --- imgdb.tgz --- imgpayld.tgz
build=
updated=0
# chmod +w /var/lib/tftpboot/esxi5.1_dell/*
```

D.3 Adding a PXE Menu Entry

Create a file named “pxe.cfg” inside the image directory on the TFTP server. The content of the file displays as follows:

```
DEFAULT menu.c32
MENU TITLE ESXi-5.1 Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
  KERNEL esxi5.1_dell/mboot.c32
  APPEND -c /esxi5.1_dell/boot.cfg ks=http://KSFILEPATH +++
  MENU LABEL ESXi-5.1 ^Installer
LABEL hddboot
  LOCALBOOT 0x80
  MENU LABEL ^Boot from local disk
```

Note:

The value of **`KSFILEPATH`** will be replaced dynamically by the Resource Adapter with the TFTP IP address value defined for the “PXE Repo” repository (assuming the TFTP server and the web server are running on the same machine). Ifdynamic replacement is not required, place the of the IP address (or hostname) value of the web server where the ks.cfg file is located.

D.4 Configuring the HTTP Server

HTTP services are enabled, by default, on the appliance.

D.5 Creating a Kickstart Configuration File

To create a kickstart configuration file, perform the following steps:

1. Create the image directory on the HTTP server base location:

```
# cd /var/www/html
# mkdir esxi5.1_dell
```

Note:

The name of the directory needs to be same as the image directory created on the TFTP server.

2. Create a file named “ks_template.cfg” inside the image directory on the HTTP server.

   The content of the file will as shown below:

```
# Sample scripted installation file
# Accept the VMware End User License Agreement
vmaccepteula
# Set the root password for the DCUI and ESXi Shell
rootpw <PASSWORD>

clearpart --firstdisk=<FIRSTDISK> --overwritevmfs

# Install on the first local disk available on machine
install --firstdisk=<FIRSTDISK> --overwritevmfs

# Set the network to DHCP on the first network adapater, use the specified
hostname and do not create a portgroup for the VMs
<NETWORKCONTENT>
# reboots the host after the scripted installation is completed
reboot

%firstboot --interpreter=busybox
<FIRSTBOOTDATA>
```

Notes:

- The value of `<PASSWORD>` will be replaced with the password string defined in the Resource Adapter configuration file. The default value is **iforgot**.
- The value of `<FIRSTDISK>` will be replaced by `local/usb`, depending on the boot sequence defined in the deployment template.
- The value of `<NETWORKCONTENT>` will be replaced for the DHCP or static IP address configuration. The default configuration is **dhcp**. If the value of the IP address, subnet mask, and name-server is provided in the inventory, then the static IP address configuration will be applied on the server.
- The value of `<FIRSTBOOT>` will be replaced by the network configuration template file, available inside the Resource Adapter package. The configuration is based on the specifications for the Active System 800VMware Deployment document.
- The `<FIRSTBOOT>` configuration also includes:
  - iSCSI initiator configuration
  - ESXi license Key. The value is added if the license key information is available in the resource adapter configuration file.
  - Name of the Local datastore

D.6 Adding the New Image to the Software Repositories

If the new image is added by replacing the earlier image directory, then no change is required.

If the new image is added with a new name/directory then the “PXE Bootable Image” repository must be updated, as described in 3.3.3 Updating Repository Elements for PXE Bootable Images section.

E Appendix E—Adding New ESXi ISO Images

This appendix describes the following topics related to adding new ESXi images:

- Preparing the VMware ESXi 5.x Installation Media
- Modifying the ESXi boot.cfg Configuration File
- Configuring the HTTP ServerCreating a Kickstart Configuration File

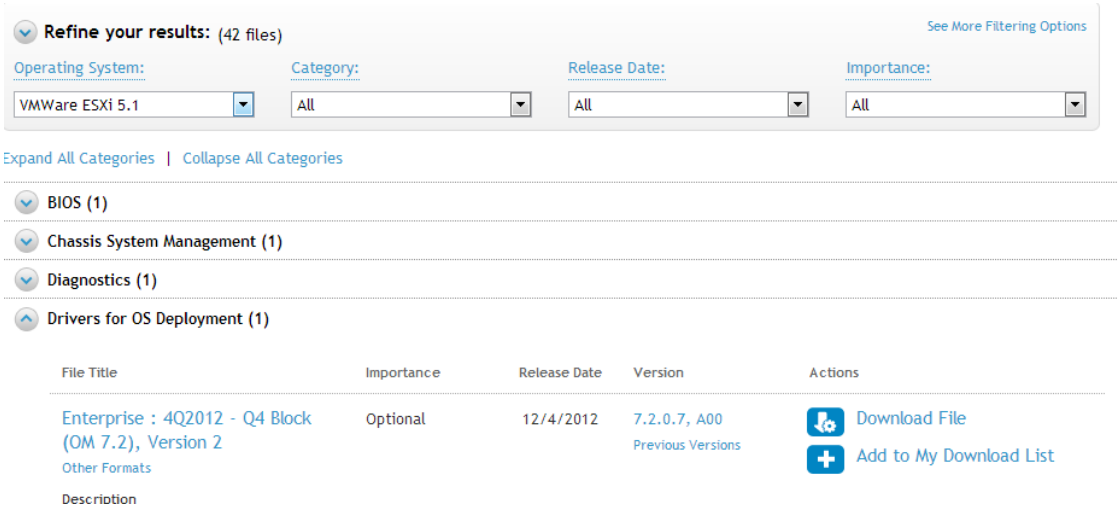
E.1 Preparing the VMware ESXi 5.x Installation Media

To prepare the VMware ESXi 5.x installation media, perform the following steps:

3. Log in to www.dell.com.
4. Open the support and driver page (http://www.dell.com/support/drivers/us/en/04/ProductSelector/Select?rquery=fkey-e-Drivers_PS)
5. Select **Server > Storage & Networking**.
6. Select **PowerEdge**.
7. Select **PowerEdge M620**.
8. Select **VMware ESXi 5.1**.

The image will be listed in the "Drivers for OS Deployment" section.

Figure 108. Drivers for OS Deployment



9. On your Active System Manager appliance server, simply extract the contents of the installation ISO into a new directory using the following commands (login as the **root** user") :

```
# mkdir /tmp/dellISO
# mkdir /home/delladmin/ISOBootImages/esxi5.1_dell_ISOBoot_New

# mount -o loop VMware-VMvisor-Installer-5.1.0-799733.x86_64-
Dell_Customized_RecoveryCD_A00.iso /tmp/dellISO
# cp -fr /tmp/dellISO /home/delladmin/ISOBootImages/esxi5.1_dell_ISOBoot_New
```

```
# chmod +w /home/delladmin/ISOBootImages/esxi5.1_dell_ISOBoot_New/*
```

Note:

If the newly added image need to replace the existing image, then execute following commands:

```
mv /home/delladmin/ISOBootImages/esxi5.1_dell_ISOBoot_New
/home/delladmin/ISOBootImages/esxi5.1_dell_ISOBoot
```

E.2 Modifying the ESXi boot.cfg Configuration File

To confirm that the installation source is not in the root of the TFTP server, perform the following steps:

1. Update the **kernelopt** parameter to point the kickstart file to the CD-ROM:

```
# cat boot.cfg
bootstate=0
title=Loading ESXi installer
kernel=/tboot.b00
kernelopt=ks=cdrom:/KS.CFG
modules=/b.b00 --- /useropts.gz --- /k.b00 --- /chardevs.b00 --- /a.b00 ---
/user.b00 --- /s.v00 --- /misc_cni.v00 --- /net_bnx2.v00 --- /net_bnx2.v01 ---
/net_cnic.v00 --- /net_tg3.v00 --- /scsi_bnx.v00 --- /scsi_bnx.v01 ---
/net_bna.v00 --- /scsi_bfa.v00 --- /ima_be2i.v00 --- /scsi_be2.v00 ---
/net_igb.v00 --- /scsi_mpt.v00 --- /ima_qla4.v00 --- /net_qlcn.v00 ---
/scsi_qla.v00 --- /ata_pata.v00 --- /ata_pata.v01 --- /ata_pata.v02 ---
/ata_pata.v03 --- /ata_pata.v04 --- /ata_pata.v05 --- /ata_pata.v06 ---
/ata_pata.v07 --- /block_cc.v00 --- /ehci_ehc.v00 --- /weaselin.t00 ---
/esx_dvfi.v00 --- /xlibs.v00 --- /ipmi_ipm.v00 --- /ipmi_ipm.v01 ---
/ipmi_ipm.v02 --- /misc_dri.v00 --- /net_be2n.v00 --- /net_e100.v00 ---
/net_e100.v01 --- /net_enic.v00 --- /net_forc.v00 --- /net_ixgb.v00 ---
/net_nx_n.v00 --- /net_qlge.v00 --- /net_r816.v00 --- /net_r816.v01 ---
/net_s2io.v00 --- /net_sky2.v00 --- /net_vmxn.v00 --- /ohci_usb.v00 ---
/sata_ahc.v00 --- /sata_ata.v00 --- /sata_sat.v00 --- /sata_sat.v01 ---
/sata_sat.v02 --- /sata_sat.v03 --- /sata_sat.v04 --- /scsi_aac.v00 ---
/scsi_adp.v00 --- /scsi_aic.v00 --- /scsi_fni.v00 --- /scsi_hps.v00 ---
/scsi_ips.v00 --- /scsi_lpf.v00 --- /scsi_meg.v00 --- /scsi_meg.v01 ---
/scsi_meg.v02 --- /scsi_mpt.v01 --- /scsi_mpt.v02 --- /scsi_rst.v00 ---
/uhci_usb.v00 --- /tools.t00 --- /scsi_qla.v01 --- /dell_con.v00 --- /xorg.v00
--- /imgdb.tgz --- /imgpayld.tgz
build=
updated=0

# chmod +w /home/delladmin/ISOBootImages/esxi5.1_dell_ISOBoot_New/*
```

E.3 Creating a Kickstart Configuration File

To create a kickstart configuration file, perform the following steps:

1. Create the image directory on the HTTP server base location:

```
# cd /home/delladmin/ISOBootImages/esxi5.1_dell_ISOBoot_New
```

Note:

The name of the directory needs to be same as the image directory created on the TFTP server.

2. Create a file named “ks.cfg” inside the image directory.

   The content of the file will as shown below:

```
# Sample scripted installation file
# Accept the VMware End User License Agreement
vmaccepteula
# Set the root password for the DCUI and ESXi Shell
rootpw <PASSWORD>

clearpart --firstdisk=<FIRSTDISK> --overwritevmfs

# Install on the first local disk available on machine
install --firstdisk=<FIRSTDISK> --overwritevmfs

# Set the network to DHCP on the first network adapter, use the specified
hostname and do not create a portgroup for the VMs
<NETWORKCONTENT>
# reboots the host after the scripted installation is completed
reboot

%firstboot --interpreter=busybox
<FIRSTBOOTDATA>
```

Notes:

- The value of `<PASSWORD>` will be replaced with the password string defined in the Resource Adapter configuration file. The default value is **iforgot**.
- The value of `<FIRSTDISK>` will be replaced by `local/usb`, depending on the boot sequence defined in the deployment template.
- The value of `<NETWORKCONTENT>` will be replaced for the DHCP or static IP address configuration. The default configuration is **dhcp**. If the value of the IP address, subnet mask, and name-server is provided in the inventory, then the static IP address configuration will be applied on the server.
- The value of `<FIRSTBOOT>` will be replaced by the network configuration template file, available inside the Resource Adapter package. The configuration is based on the specifications for the Active System 800VMware Deployment document.
- The `<FIRSTBOOT>` configuration also includes:
  - iSCSI initiator configuration

- ESXi license Key. The value is added if the license key information is available in the resource adapter configuration file.

Name of the Local datastore

3. Copy the ks.cfg file to the HTTP Server base location.

```
mkdir -p /var/www/html/esxi5.1_dell_ISOBoot_New/

cp /home/delladmin/ISOBootImages/esxi5.1_dell_ISOBoot_New/ks.cfg
/var/www/html/esxi5.1_dell_ISOBoot_New/ks.cfg
```

If the existing image directory is replaced, skip the above commands and execute the following:

```
mkdir -p /var/www/html/esxi5.1_dell_ISOBoot

cp /home/delladmin/ISOBootImages/esxi5.1_dell_ISOBoot/ks.cfg
/var/www/html/esxi5.1_dell_ISOBoot/ks.cfg
```

4. Update the file permission on the newly added image:

```
chown -R delladmin:delladmin /home/delladmin/ISOBootImages
chmod -R +w  /home/delladmin/ISOBootImages/
```

E.4 Adding the New Image to the Software Repositories

If the new image is added by replacing the earlier image directory, then no change is required.

If the new image is added with a new name/directory then “ISO Bootable Image” repository must be updated, as described in 3.3.4 Updating Repository Elements for ISO Bootable Images section.

F Appendix F— Planning Worksheet

Table 18. Out of Band Management IP Address Configuration

Equipment	IP Address	Subnet Mask	Gateway	Username	Password
Chassis 1 CMC					
Chassis 2 CMC					
iDRAC for all M620					
Force10 S4810 Switch1					
Force10 S4810 Switch2					
EqualLogic Storage Array Group Management					
EqualLogic Storage Array Group on iSCSI Network					
Active System Manager Appliance					
vCenter					

F.1 ESXI Server IP Configuration

The following parameters for each server are required:

- **ISCSIvNICIPAddresses—**Space-separated list of IP addresses to be assigned to iSCSI virtual network interface cards (vNICs). For example, for updating information for "vmnic6 vmnic7" using the **Update Port Group with iSCSI VLAN** operation, the value will be in the `192.168.120.XX 192.168.120.YY` format. The IP Addresses needs to be separated by a space " "
- **ISCSINetmask – iSCSI subnet mask of the iSCSI virtual network interface cards (vNICs)**
- **iSCSIChapUsername** – iSCSI Chap username used to access volume of EqualLogic Storage Array
- **iSCSIChapSecret** – iSCSI Chap secret corresponding to iSCSI Chap username.
- **ServerHostname**—Hostname to be assigned to the ESXi server.
- **ServerDomainName** – Domain name to be assigned to the ESXi server.
- **ServerNameServer** – Name server to be assigned to the ESXi server.
- **ServerGateway**—Gateway for the ESX server.
- **ServerNetmask**—Netmask for the ESX server.
- **ServerIPAddress**—IP address that must be assigned to the ESX server. If the hypervisor must retrieve an IP address from the DHCP server, leave this parameter blank.
- **ServerPassword** – Server password to be assigned during unattended installation.

F.2 VLAN for IOA Configuration

Traffic Type	VLAN
Management	
vMotion	
VM Workload(s)	
iSCSI Management / Traffic	

VMware Workloads

1. Administrator needs to create a volume on EqualLogic storage array manually
2. This volume needs to contain the base line VMs that will be used for creating the VM workloads

Note:

The base line VMs needs to have VMware Tools installed.

G Appendix G—PXE Setup Requirements

Considerations before creating the DHCP Server:

- The PXE Network must be separate from the Management Network.
- Active System Manager must have a network interface with same subnet as the TFTP Server. Appliance uses ARP entries for identifying the IP Address assigned to the ESXi Servers by the DHCP Server.
- The Active System Manager VM appliance has pre-defined templates for installing ESXi 5.1 on the Dell blade servers using PXE boot. For enabling the Preboot Execution Environment (PXE) boot, the following additional services are configured on the appliance:

G.1 TFTP Server

TFTP services are enabled and deployed at **/var/lib/tftpboot** on the appliance. The ESXi Dell customized image is embedded within the appliance.

G.2 HTTP Server

HTTP services are enabled on the appliance.

G.3 DHCP Server

DHCP services are disabled on the appliance to avoid any issue with an existing DHCP server that may already be running on the same customer network. For the PXE setup requirement, the DHCP services should be running on the same network as the PXE. The DHCP server is configured to use Eth1 on the appliance

The VM appliance is created with one vNIC. The vNIC needs to be in the Hypervisor Management Network.

G.4 Configuring PXE Setup with Embedded DHCP Server

The DHCP Services needs to be enabled on separate network interface on the appliance. Before configuring the DHCP Services, add a new Virtual NIC on the appliance using the VMware vSphere client and restart the appliance.

G.4.1 Configuring the DHCP Server

To configure the DHCP server, perform the following steps:

1. Connect to the VM appliance console using the **root** user credentials through either the VMware vSphere Client VM console or the Hyper-V VM console.
2. Assign a static IP address on the **eth1** interface. This IP Address must belong to the hypervisor Management subnet.
3. Edit file /etc/sysconfig/dhcpd and add following content to the file.

```
# Command line options here
DHCPDARGS=”eth1”
```

4. Edit the **/etc/dhcp/dhcpd.conf** file.
5. Update the values of the IP address ranges and subnets per the customer environment.
6. Update the value of the next server with the VM appliance IP address on the same subnet as the DHCP server (**eth0** IP address). The “next-server” represents the TFTP Server where the image is hosted.

```
# DHCP Server for Hypervisor management network
# Uncomment following lines with appropriate IP Address range

subnet 192.168.122.0  netmask 255.255.255.0 {
    range 192.168.122.102 192.168.122.230;
    allow booting;
    allow bootp;
    filename “pxelinux.0”;
    next-server 192.168.122.101;
# --- default gateway
    option routers                  192.168.122.1;
    option subnet-mask              255.255.255.0;
    option domain-name-servers      192.168.122.1;

       option netbios-node-type 2;
    default-lease-time 28800;
    max-lease-time 28800;
}
```

G.4.2 Configuring the TFTP Server

The ESXi 5.1 customized image is embedded inside the appliance at `/var/lib/tftpboot/esxi51._dell`. The image is configured to create a kickstart file dynamically based on the IP address provided in the Active System Manager inventory.

If the ESXi host is configured to learn the IP address through DHCP (configured through orchestration), and then there is no need to update the Server IP Address information in the Active System Manager inventory. The IP Address configured on the hosts by the DHCP server will be updated automatically during the server installation.

If a new image is required to be added to the appliance, follow the steps available in Appendix C—Firmware and Software Base Lineup.

To start the DHCP services, execute the **/etc/init.d/dhcpd restart** command.

G.5 Configuring the PXE Setup with the Existing DHCP Server

If the DHCP server already exists on the Hypervisor Management Network, perform the following steps:

1. Update the appliance's DHCP settings to support the Bootstrap Protocol (BOOTP).
2. Edit the **/etc/dhcpd/dhcpd.conf** file.
3. Update the next-server to point to the Active System Manager appliance IP address; the images are hosted on the appliance.

```
allow booting;
allow bootp;
filename "pxelinux.0";
next-server 192.168.122.101;
```

H Appendix H—FAQs

Q1 Volumes on EqualLogic Array are not removed for cancelled sessions. This wastes storage space and consumes iSCSI connections.

A1 User should manually cleanup the unused volumes on the EqualLogic storage array and iSCSI connections after session is canceled.

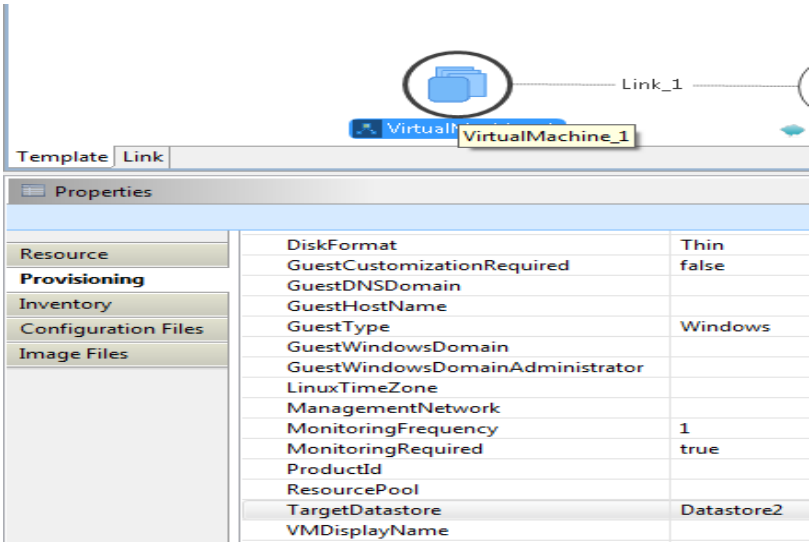
Q2 The orchestrations assume that Port Channel 2 is configured on the switches. If not, you get a failure indicated by red links on the session.

A2 The list of port-channels are configurable, based on the environment this list could be controlled by updating the "portChannelList" in the "ssi.properties" file under "$HOME/asm-galeforce/gf/common/integrations/Dell/Force10-S4810"

Q3 Where is the VM created? Is there way to specify which Datastore gets created?

A3 User can specify on which datastore the VM will be created by providing the value of "TargetDatastore" provisioning parameter of the VM in the template as shown in the screenshot below. If there is no value provided for "TargetDatastore" , the RA chooses the best available datastore for VM creation.

Figure 109. Provisioning Properties



Q4 Is there a way to revert a template or import the original template?

A4 The original templates are available on the appliance under folder $HOME/DefaultTemplates

Also as best practice:

a. You should make a copy of the template and make the required modification in the cloned template.

b. Keep the copy of the original templates by exporting them locally on a client machine and importing it back as needed.

Q5 What is the difference between synchronize and discovery

A5 TBD.

Q6 SSI properties will be overwritten when upgrading the RA.

A6 Yes upgrading the RA will override the ssi.properties file. As best practice, before upgrading the RA, backup RA directory by following the steps given below –

- Login the Active System Manager server as “delladmin” user
- cd $HOME/asm-galeforce/gf/common/integrations
- cp –r <manufacturer>/<model> <manufacturer>/<model>_<CurrentDate>

Q7 How Gold Volumes on EqualLogic storage array are secured?

A7 Gold volume is secured by creating the access rights for the chap users.

Steps to create the Gold Volume –

1. Create a volume of appropriate size on EqualLogic Storage array.
2. Associate the chap account and associate it with the newly created volume.
3. Connect to the management host and configure the newly created datastore.

Q8 What about images and firmwares released after this release of Active System Manager 7.0?

A8 Images and firmware versions that are released after Active System Manager 7.0 should work but this should be validated with the solution.

Q9 What is base level configuration and what is consists of for Dell Force10 switches?

A9 Base level configuration is the minimal set of configuration running on the switches so as to bring them to an operational state. Additional details of these configurations can be found in the embedded files.

Q10 Is it required to create pools on Dell EqualLogic storage array?

A10 Creating pool is optional. If there are no user-defined pools on the EqualLogic Storage array, then a newly created volume becomes part of the default storage pool. Pools can be created by executing the **PoolCreate** method on the EqualLogic group object in the Operation Center View.

Q11 Is HTTPS supported for connecting to Active System Manager?

A11 Yes, HTTPS is supported on Active System Manager.

Q12 Is terminal server connectivity required for Dell Force10 switches?

A12 Terminal server connectivity to Dell Force10 switches is optional.

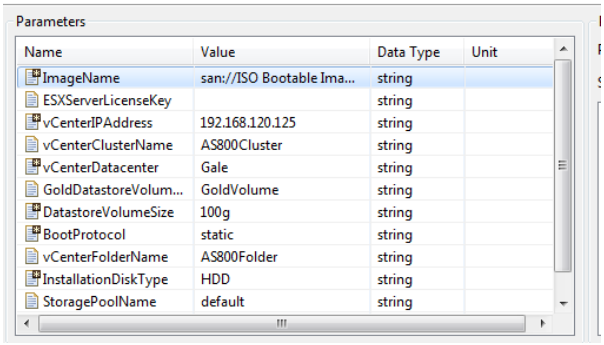
Q13 Does the default password of the Active System Manager appliance get updated?

A13 The appliance login password can be changed. If the password is changed, Software repositories that are configured on Active System Manager Appliance should be modified with the new password.

Q14 How would a user know what's the optional parameters in an orchestration step method?

A14 Parameters with the * sign suffixed in front of them are mandatory and the ones without * sign are optional. See figure for exampls.

Figure 110. Parameters



Q15 When do I add new images and firmware versions in the appliance?

A15 TBD

Q16 If a customer is not going to use PXE deployments, are they still required to configure this?

A16 PXE setup is optional if a customer is not going to use PXE deployment. They can use ISO boot solution of Active System Manager 7.0

Q17 Do you want to show Hyper-V? These are all only VMware specific.

A17 Active System Manager 7.0 supports VMware ESXi server imaging and workload provisioning for VMware VM. Microsoft Hyper-V is not supported with Active System Manager 7.0.

Q18 How to change the hostname of the Active System Manager Server?

A18 Steps to change hostname of the Active System Manager server –

a. Log in to the Active System Manager as the **root** user.

b. Open the **/etc/sysconfig/network** file and update the "HOSTNAME" field value with the new hostname.

c. Also update the hostname in the **/etc/hosts** file.

d. Reboot the server by executing the **reboot** command.

e. Once the server is up and running, log in to the server as the **delladmin** user.

f. Verify that the hostname is updated to the new hostname by executing the **hostname** command.

g. Ensure that all Active System Manager services are stopped first:

cd $HOME/asm-galeforce/gf/sbin

h. Execute the **./updateHostName.sh** file and follow the instructions to update the hostname in the Active System Manager installation.

i. Start the Active System Manager Services. Details on how to start the services are provided in this guide.