Active System Manager
Version 7.6 Quick Installation Guide

Notes, Cautions, and Warnings

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

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2014 - 06

Rev. A00

Contents

1

Overview

Active System Manager (ASM) is Dell's unified management product that provides a comprehensive infrastructure and workload automation solution for IT administrators and teams. ASM simplifies and automates the management of heterogeneous environments, enabling IT to respond more rapidly to dynamic business needs.

IT organizations today are often burdened by complex data centers that contain a mix of technologies from different vendors and cumbersome operational tasks for delivering services while managing the underlying infrastructure. These tasks are typically performed through multiple management consoles for different physical and virtual resources, which can dramatically slow down service deployment.

The new ASM features an enhanced user interface that provides an intuitive, end-to-end infrastructure and workload automation experience through a unified console. This speeds up workload delivery and streamlines infrastructure management, enabling IT organizations to accelerate service delivery and time to value for customers.

This document contains information about virtual appliance and software requirements of ASM, and the resources supported by ASM such as chassis, servers, storage, network switches, and adapters

About this Document

This document version is updated for ASM, version 7.6.

What is New in this Release

- Support for Hyper-V Compellent (Fibre Channel).
- VMs and Application support for Hyper-V or SCVMM.
- Support for ESXi NetApp Storage.
- Ability to clone a configuration of a server and apply it to another server.
- iSCSI and Fibre Channel boot support for Windows and Linux.
- iSCSI and Fibre Channel boot service migration support for Windows and Linux.
- Support for Windows 2008 R2 deployment.
- Ability to clone Hyper-V and VMware Virtual Machine from virtual machine or template.
- Template updates including new template for SQL Server Windows 2012 Support.
- Service Mobility — Capability to migrate server's BIOS, NICs, storage connectivity, and assigned identity information to another server in a designated server pool.
- Flexible Configurations — Provides multiple implementation choices for both network card and fabric configuration.

- Service Lifecycle Enhancements supports:
  - Ability to scale up storage, hosts, and virtual machines.
  - Ability to retry and deploy a failed service.

Accessing Online Help

ASM online help system provides context-sensitive help available from every page in ASM user interface.

After you log in to ASM user interface, you can access the online help in any of the following ways:

- To open context-sensitive online help for the active page, click **?**, and then click **Help**.
- To open context-sensitive online help for a dialog box, click **?** in the dialog box.

Additionally, in the online help, use the **Enter search items** option in the **Table of Contents** to search for a specific topic or keyword.

Other Documents You May Need

Go to http://www.dell.com/asmdocs for additional supporting documents such as:

- *Dell Active System Manager version 7.6 User's Guide*
- *Dell Active System Manager version 7.6 Release Notes*
- *Dell Active System Manager version 7.6 Quick Installation Guide*

For more information about best practices, Dell solutions, and service, see Dell Active System Manager page on Dell Techcenter:

http://en.community.dell.com/techcenter/converged-infrastructure/w/wiki/4318.dell-active-system-manager.aspx

Licensing

ASM licensing is based on the total number of managed resources, except for the VMware vCenter and Windows SCVMM instances

ASM 7.6 supports following license types:

- Trail License — A Trial license can be procured though the account team and it supports up to 25 resources for 90 days.
- Standard License — A Standard license grants full access.

You will receive an e-mail from customer service with the instructions of downloading ASM. The license file is attached to that email.

If you are using ASM for the first time, you must upload the license file through the **Initial Setup** wizard. To upload and activate subsequent licenses, click **Settings** → **Virtual Appliance Management.**

After uploading an initial license, subsequent uploads replace the existing license.

Important Note

Engaging support requires that all prerequisites are fulfilled by customer or deployment team. Third party hardware support is not provided by Dell services. Discovery, inventory and usage of third party hardware must be in the expected state as described in the prerequisites and configuring sections of this guide.

ASM Port and Protocol Information

The following ports and communication protocols used by ASM to transfer and receive data.

Table 1. ASM Port and Protocol Information

Ports	Protocols	Port Type	Direction	Use
22	SSH	TCP	Inbound / Outbound	I/O Module
23	Telnet	TCP	Outbound	I/O Module
53	DNS	TCP	Outbound	DNS Server
67, 68	DHCP	UDP	Outbound	DHCP Server
69	TFTP	UDP	Inbound	Firmware Updates
80, 8080	HTTP	TCP	Inbound / Outbound	HTTP Communication
123	NTP	UDP	Outbound	Time Synchronization
162, 11620	SNMP	UDP	Inbound	SNMP Synchronization
443	HTTPS	TCP	Inbound / Outbound	Secure HTTP Communication
443, 4433	WS-MAN	TCP	Outbound	iDRAC and CMC Communication
129, 445	CIFS	TCP	Inbound / Outbound	Back up program date to CIFS share
2049	NFS	TCP	Inbound / Outbound	Back up program data to NIFS share

2

Installation and Quick Start

The following sections provide installation and quick start information, including step-by-step instructions for deploying and configuring ASM in VMware vSphere Client or SCVMM. Only one instance of ASM should be installed within a network environment. Exceeding this limit can cause conflicts in device communication.

Information Prerequisites

Before you begin the installation process:

- Gather TCP/IP address information to assign to the virtual appliance.
- If you want to deploy the ASM virtual appliance on VMware vCenter, make sure that VMware vCenter Server and VMware vSphere Client are currently running.
- If you want to deploy the ASM virtual appliance on Windows Hyper-V, make sure SCVMM Instance is up and running and Hyper-V host on which ASM virtual appliance deployed is already installed on SCVMM.
- Download ASM appliance file, which contains either the virtual appliance .ovf file for (VMware) or the virtual appliance virtual hard drive .vhd (Hyper-V).
- Determine the host on which the ASM virtual appliance will be installed. You can use any host managed by VMware vCenter or Hyper-V manager that has network connectivity with your out-of-band (OOB), management, and potentially iSCSI networks. This is required for discovery to complete successfully.

⚠ **CAUTION: The ASM virtual appliance functions as a regular virtual machine. Therefore, any interruptions or shut downs affects the overall functionality.**

Installing Active System Manger

Before you begin, make sure that systems are connected and VMware vCenter Server, VMware vSphere Client, and SCVMM are running.

Deployment Prerequisites

Specification	Prerequisite
Connection Requirements	• The virtual appliance is able to communicate with the out-of-band management network and any other networks from which you want to discover the resources. • The virtual appliance is able to communicate with the PXE network in which the appliance is

Specification	Prerequisite
	deployed. It is recommended to configure the virtual appliance directly on the PXE network, and not on the external network. • The virtual appliance is able to communicate with the hypervisor management network. • The DHCP server is fully functional with appropriate PXE settings to PXE boot images from ASM in your deployment network.
Firmware and BIOS Requirements	Make sure all the resources are configured with the firmware versions listed in the section Supported Resources
PowerEdge M1000e Chassis, blade server, and IO aggregators	• Chassis Management Controller (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.
Dell PowerEdge Hypervisor Servers	Server iDRAC is configured and has the out-of-band IP address and login credentials.
Dell PowerEdge Servers	• Dell PowerEdge Servers are configured and have the management IP address and login credentials assigned. NOTE: The user name (root) and password required. • Any device being used in the boot order, such as C: Drive or NICs, must already be enabled in the boot order. This applies when booting to SD Card, Hard Disk, or FC, which are listed as C: in boot order or PXE and iSCSI, which are listed as NICs in the boot order. ASM will enable the supporting device connectivity and adjust the boot order, but cannot enable/disable device names in the boot order. • Before performing Fibre Channel boot from SAN, a server must be configured with the QLogic fiber channel card, which is configured with the appropriate scan selection. To verify this in the BIOS and QLogic device settings, press F2 for System Setup, and then go to **Device Settings** → **<Target QLogic Fibre Channel adapter name>** → **Fibre Channel Target Configuration** → **Boot Scan**, and then select "*First LUN*".
Dell PowerConnect 7024 switches	• The management IP address is configured for the switches. • ASM creates the virtual machine (VM) traffic VLANs dynamically.

Specification	Prerequisite
	• Users have access to the switches with passwords enabled.. • Switches have SSH connectivity enabled.
Dell Force10 S4810 switches (Top-of-Rack [ToR])	• The management IP address is configured for the ToR switches. • Any VLAN which is dynamically provisioned by ASM must exist on the ToR switch. • Server facing ports must be in hybrid mode. • Server facing ports must be in switchport mode. • Server facing ports must be configured for spanning tree portfast. • If DCB settings are used, it must be properly configured on the switch for converged traffic.
Dell 8 | 4 I/O modules	• The management IP address is configured for the Brocade switches.
EqualLogic Storage Array	• The management and group IP addresses are configured for Storage Array. • All storage array members are added to the group. NOTE: The Equallogic management interface must be configured to enable dedicated management network. • EqualLogic array must have a SNMP community name set to "public".
Compellent Storage Array	. • The management IP address is configured for Storage Array • All storage array members are added to the group.
VMware vCenter 5.1 or 5.5	• VMware vCenter 5.1 or 5.5 is configured and accessible through the management and hypervisor management network. • Appropriate licenses are deployed on the VMware vCenter.
System Center Virtual Machine Manager (SCVMM)	• See System Center Virtual Machine Manager (SCVMM) Prerequisites.
PXE Setup	• The details of PXE setup is described in the Configuring ASM Virtual Appliance as PXE Boot Responder section.

System Center Virtual Machine Manager (SCVMM) Prerequisites

ASM manages resource on Microsoft System Center Virtual Machine Manager through Windows Remote Management (WinRM). Windows RM must be enabled on the SCVMM server. ASM requires Windows RM to utilize default port and basic authentication. To enable these settings, on the SCVMM server, open a Windows PowerShell interface with administrator permissions and run the following commands:

```
winrm set winrm/config/client/auth '@{Basic="true"}'
winrm set winrm/config/service/auth '@{Basic="true"}'
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
```

The default amount of memory allocated for WinRM processes is limited to 150 MB. To avoid out of memory errors, increase the memory size to 1024:

```
winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="1024"}'
```

NOTE: There is a known issue with WMF 3.0. The MaxMemoryPerShellMB configuration may be ignored. For more information, see KB2842230. The fix for Windows 8/Windows 2012 x64 (non R2) is available at the following link. The fix is not necessary for Windows 2012 R2.

Make sure SCVMM has time synchronized with a time server. If SCVMM time is off from deployed Hyper-V hosts then you may not be able to add hosts and create clusters in SCVMM.

Deploying ASM from VMware vSphere Client

1. Extract the .zip file to a location accessible by VMware vSphere Client. It is recommended to use a local drive or CD/DVD, because installing from a network location can take up to 30 minutes.
2. In vSphere Client, select **File** → **Deploy OVF Template**. The Deploy OVF Template wizard displays.
3. On the **Source** page, click **Browse**, and then select the OVF package. Click **Next** to continue.
4. On the **OVF Template Details** page, review the information that is displayed. Click **Next** to continue.
5. On the **End User License Agreement** page, read the license agreement and click **Accept**. To continue, click **Next**.
6. On the **Name and Location** page, enter a name with up to 80 characters and then, select an **Inventory Location** where the template will be stored. Click **Next** to continue.
7. Depending on the vCenter configuration, one of the following options display:

   - **If resource pools are configured** — On the **Resource Pool** page, select the pool of virtual servers to deploy the appliance virtual machine.
   - **If resource pools are NOT configured** — On the **Hosts/Clusters** page, select the host or cluster on which you want to deploy the appliance virtual machine.

   Click **Next** to continue.
8. If there is more than one datastore available on the host, the **Datastore** page displays. Select the location to store virtual machine (VM) files, and then click **Next** to continue.
9. On the **Disk Format** page, choose one of the following options:

   - To allocate storage space to virtual machines. as required, click **thin provisioned format**.
   - To pre-allocate physical storage space to virtual machines at the time a disk is created, click **thick provisioned format**.

   Click **Next** to continue.
10. On the **Ready to Complete** page, review the options you selected on previous pages and click **Finish** to run the deployment job. A completion status window displays where you can track job progress.

Deploying ASM using SCVMM

To deploy ASM using SCVMM:

1. Extract the .zip file for ASM build to a local folder on your SCVMM appliance <ASM_INSTALLER_ROOT_DIR>.
2. To add ASM to the Library of Physical Library Objects in SCVMM, do the following:
   a. In the left pane, click **Library**.
   b. In the **Home** tab, click **Import Physical Resource**.
   c. Click the **Add Resource** button. Browse to the location of ASM .vhd file: <ASM_INSTALLER_ROOT_DIR>\Virtual Hard Disks\Dell-ActiveSystemManager-7.6-.vhd
   d. Under the **Select library server and destination for imported resources** section, click the **Browse** button. Select the destination folder in which ASM install VHD is located (for example, My_SCVMM -> MSCVMMLibrary -> VHDs), and then click **OK**.
   e. Click the **Import** button.

3. To deploy ASM virtual appliance:

    a. In the left pane, click **VMs and Services**.

    b. Click the **Create Virtual Machine** button.

    c. Select **Use an existing virtual machine, VM template, or virtual hard disk**, and then click the **Browse** button

    d. From the list of sources, select VHD -> Dell-ActiveSystemManager-7.6- <bulid>.vhd, and then click **OK**.

    e. Click **Next**.

    f. In the **Virtual machine name** text box, type the virtual machine name for your appliance, and then click **Next**.

    g. On the **Configure Hardware** page, do the following:

        1. In the **Compatibility** section, set **Cloud Capability Profile** to **Hyper-V**.
        2. In the **Processors** section, change the processor value to **2**, and then in the **Memory** section, change the memory value to 8 GB.
        3. In the **Network Adapter 1** section, assign the adapter to your PXE VM Network.
        4. Click **Next**.

    h. On the **Select Destination** page, select the destination host group that contains the Hyper-V server where you want to deploy the ASM virtual machine. Click **Next**.

    i. On the **Select Host** page, select the host on which you want to deploy ASM, and then click **Next**.

    j. On the **Configuration Settings** page, make the changes for your environment, if required.

    k. On the **Select networks** page, select your PXE network and configure it appropriately.

    l. On the **Add Properties** page, set to **Always turn on the Virtual Machine** and the OS as **CentOS Linux (64 bit)**, and then click **Next**.

    m. Review the summary, select the **Start Virtual machine after deploying it** option, and then click the **Create** button.

Deploying ASM on Hyper-V host

To deploy ASM on Hyper-V host:

1. Open Hyper-V Manager in the Windows 2012 host. The Windows 2012 host should be displayed under Hyper-V Manager.
2. Select the host and select **Action → Import Virtual Machine**.
3. Select the folder containing the ASM virtual appliance including snapshots, virtual hard disks, virtual machines, and import files. Click **Next**.
4. On the **Select Virtual Machine** page, select the virtual machine to import (there is only one option available), and then click **Next**.
5. On the **Choose Import Type** page, select **Copy the virtual machine**, and then click **Next**.
6. On the **Choose Destination** page, retain the default values or select the location of the virtual machine, snapshot, and smart paging, and click **Next**.
7. On the **Choose Storage Folders** page, retain the default values or click **Browse** and select the location of virtual hard disks, and then click **Next**.
8. On the **Summary** page, review the options you selected on earlier pages, and then click **Finish** to deploy the ASM virtual appliance on the Hyper-V host.

9. After ASM virtual appliance is deployed, right-click the ASM virtual appliance, and then click **Settings**.
10. In the **Settings** wizard, to enable the virtual switch, select **VM-Bus Network Adapter**. Optionally, provide a VLAN ID, if the host is tagged on a particular network, and then click **OK**.
11. Select the ASM virtual appliance, and then click **Start under Actions**.

3

Configuring ASM Virtual Appliance

You must configure the following settings in the virtual appliance console before you start using ASM:

- Change Dell administrator password. For detailed information, see Changing Delladmin Password
- Configure static IP Address in the virtual appliance. For detailed information, see Configuring Static IP Address in the Virtual Appliance
- Configure ASM Virtual Appliance as PXE boot responder. For detailed information, see Configuring ASM Virtual Appliance as PXE Boot Responder
- Import Windows ISO on the virtual appliance. For detailed information, see Deploying WinPE on the Virtual Appliance
- Deploy the WinPE image file to the virtual appliance. For detailed information, see Deploying WinPE on the Virtual Appliance

Changing Dell Administrator Password

To change “delladmin” password:

1. You must use the SSH protocol to connect to ASM virtual appliance IP.
2. Log in to the console with the user name *delladmin* and password *delladmin* and press `Enter`.
3. At the command line interface, run the command `passwd`. Follow the prompts to update the password.
4. To log in using the new password, at the command line interface, enter the old credentials and the new password.

Configuring Static IP Address in the Virtual Appliance

1. In VMware Sphere, click the **Console** tab to open the console of the virtual appliance.
2. Log in to the console with the user name *delladmin*, enter current *delladmin* password, and then press `Enter`.

   NOTE: The default password for delladmin account is *delladmin*.

3. At the command line interface, run the command *sudo su -* and then enter the current delladmin password.
4. In the **Properties** dialog box, click **Network Configuration.**
5. In the **Network Connections** dialog box, click **Wired** → **Auto eth0**, and then click **Edit**.
6. In the **Editing Auto eth0** dialog box, click **IPv4 Settings** tab.
7. Select **Manual** from the **Method** drop-down list.
8. In the **Addresses** table, type the static IP address, subnet mask, gateway, and then click **Add**.
9. Click **Apply** to set the static IP address of the appliance.
10. For Hyper-V only, reboot the ASM virtual appliance.

Configuring ASM Virtual Appliance as PXE Boot Responder

ASM requires both PXE and DHCP network services to function. ASM virtual appliance contains a PXE service that is used to register resources with ASM so that workloads can be deployed. ASM virtual appliance must be deployed directly on the network configured for the PXE service.

The PXE service requires a DHCP server configured to provide boot server (TFTP PXE server) information and specific start-up file information. ASM PXE implementation uses the iPXE specification so that the configuration details include instructions to allow legacy PXE servers and resources to boot properly to this iPXE implementation.

This section provides information about configuring DHCP on the following servers. The information includes only the basic configuration options and declarations required for an iPXE environment. These details should be used as a cumulative addition to the settings currently used in your DHCP implementation (if you already have a DHCP environment).

- Microsoft Windows 2012 Server. See Configure DHCP on Windows 2012 DHCP Server
- Microsoft Windows 2008 Server R2. See Configure DHCP on Windows 2008 DHCP Server
- Linux DHCPd (ISC DHCP). See Configuring DHCP for Linux

Configure DHCP on Windows 2012 DHCP Server

To configure the DHCP on Windows 2012 DHCP Server, perform the following tasks:

1. Create DHCP User Class
2. Create DHCP Policy
3. Create Boot File scope option

For additional information, see http://ipxe.org/howto/msdhcp

Create the DHCP User Class

You must create the user class for the DHCP server before creating the DHCP Policy.

1. Open the Windows 2012 DHCP Server DHCP Manager.
2. In the console tree, navigate to **IPv4**. Right click **IPv4**, and then click **Define User Classes** from the drop-down menu.
3. In the **DHCP User Classes** dialog box, click **Add**.
4. In the **New Class** dialog box, enter the following information and click **OK** to create a user class.

    a. In the **Display Name** box, enter *iPXE*

    b. In the **Description** box, enter *iPXE Clients*

    c. In the data pane, under **ASCII**, enter *iPXE*
5. Click **Close**.

Create the DHCP Policy

1. Open the Windows 2012 DHCP Server DHCP Manager.
2. In the console tree, expand the scope that will service your ASM PXE network. Right-click **Policies** and select **New Policy**.

   The DHCP Policy Configuration Wizard is displayed.
3. Next to **Policy Name**, type *iPXE* and enter the description as *iPXE Client.* Click **Next**.
4. On the **Configure Conditions for the policy** page, click **Add**.
5. In the **Add/Edit Condition** dialog box, perform the following actions, and then click **OK**.
   - Select **User Class** from the **Criteria** list.
   - Select **iPXE** from the list of **Values** and click **Add**.
6. On the **Configure Conditions for the policy** page, select the **AND** operator and click **Next**.
7. On the **Configure settings for the policy** page, select the **AND** operator and click **Next**.
   - If you want to use only the portion of the DHCP scope for PXE, click **Yes**, and then enter the IP address range to limit the policy.
   - If you do not want to use the portion of the DHCP scope for PXE, click **No**.
8. For PXE service to function properly, under **Available Options**, select **067 Bootfile Name**, and enter the string value as *bootstrap.ipxe.*
9. Click **Next**, and then click **Finish**.

Create the Boot File Scope Option

1. Open the Windows 2012 DHCP Server DHCP Manager.
2. In the console tree, expand the scope that will service your ASM PXE network. Right click **Scope Options** and select **Configure Options**.
3. In the right pane, enter the following information:
   - Click **066 Boot Server Host Name** and enter the IP address or DNS name of ASM server in the **Value** column.
   - For PXE service to function properly, click **067 Bootfile Name** and enter *undionly.kpxe* in the **Value** column.
4. In the right pane, configure the following based on your network settings:
   - **003 Router** (default gateway that is on the PXE network)
   - **006 Name Server** (DNS server IP address)

Configure DHCP on Windows 2008 DHCP Server

To configure the DHCP on Windows 2008 DHCP Server, perform the following tasks:

1. Create DHCP User Class
2. Create DHCP Policy
3. Create Boot File Scope Option

For additional information, see http://ipxe.org/howto/msdhcp

Create the DHCP User Class

You must create the user class for the DHCP server before creating the DHCP Policy.

1. Open the Windows 2008 DHCP Server DHCP manager.
2. In the console tree, navigate to **IPv4**. Right click **IPv4**, and then click **Define User Classes** from the drop-down menu.
3. In the **DHCP User Class** dialog box, click **Add** to create a new user class.
4. In the **New Class** dialog box, enter the following information and click **OK** to create a user class.

    a. In the **Display Name** box, enter *iPXE*.

    b. In the **Description** box, enter i*PXE Clients*.

    c. In the data pane, under **ASCII**, enter *iPXE*.
5. Click **Close**.

Create the DHCP Policy

Use the new User Class to create a DHCP policy scope option.

1. Open the Windows 2008 DHCP Server DHCP manager.
2. Add a scope option to the DHCP scope that will service ASM PXE environment.
3. In the **Scope Options** dialog box, click the **Advanced** tab, select **067 Bootfile Name** check box, and in the **String value** box, enter *bootstrap.ipxe* .

    NOTE: For PXE service to function properly, you must enter *bootstrap.ipxe* for the **067 Bootfile Name**.
4. Select **DHCP Standard Options** from the **Vendor** class drop-down list.
5. Select **iPXEclass** from the **User Class** drop-down list.
6. Click **OK** to save the scope option.

The policy is created by utilizing the new User Class with a scope option.

Create the Boot File Scope Option

The Boot File option is created for the DHCP scope that services your ASM PXE.

1. Open the Windows 2008 DHCP Server DHCP Manager.
2. In the console tree, expand the scope that will service your ASM PXE network. Right click **Scope Options** and select **Configure Options**.
3. In the right pane, enter the following information:
    - Click **066 Boot Server Host Name** and enter the IP address or DNS name of ASM server in the **Value** column.
    - For PXE service to function properly, click **067 Bootfile Name** and enter *undionly.kpxe* in the **Value** column.
4. Additionally, in the right pane, based on you network settings, configure the following:
    - **003 Router** (default gateway that is on the PXE network)
    - **006 Name Server** (DNS server IP address)

Configuring DHCP for Linux

You can manage the configuration of the Linux DHCPD service by editing the **dhcpd.conf** configuration file. The **dhcpd.conf** is located at **/etc/dhcp** directory of most Linux distributions. If the DHCP is not installed on your Linux server, install the Network Infrastructure Server or similar services.

Before you start editing the **dhcpd.conf** file, it is recommended to back up the file. After you install the appropriate network services, you must configure the **dhcpd.conf** file before you start the DHCPD service.

The DHCP configuration must include the following options:

- **next-server <IP address>**

  Indicates the IP address of the PXE server. That is, the IP address of ASM appliance vNIC that exists on the PXE network.
- **filename "bootstrap.ipxe"**

  NOTE: For PXE service to function properly, you must specify *bootstrap.ipxe* for the file name.

The PXE service uses iPXE service. You must use two different bootstrap files for the PXE environment, one for the initial PXE boot, which starts up the system to the final iPXE boot file.

To run this operation, add the following code to the **dhcpd.conf** file:

```
        if exists user-class and option user-class = "iPXE" {
              filename "bootstrap.ipxe";
        } else {
                 filename "undionly.kpxe";
        }
```

Secondly, add the following code to the subnet declaration within your **dhcpd.conf** file. This code instructs a legacy PXE server to boot to a legacy boot file, and then directs to the iPXE boot file. For more details, see the Sample DHCP Configuration

The configuration file must contain the following information:

```
# dhcpd.conf
# Sample configuration file for ISC dhcpd
next-server 192.168.123.21;# IP address of ASM Server
default-lease-time 6000;
max-lease-time 7200;
authoritative;
log-facility local7;

subnet 192.168.123.0 netmask 255.255.255.0 {
            range 192.168.123.24 192.168.123.29;
            option subnet-mask 255.255.255.0;
            option routers 192.168.123.1;
            if exists user-class and option user-class = "iPXE" {
                            filename "bootstrap.ipxe";
                            } else {
                            filename "undionly.kpxe";
                            }
            }
```

After you modify the **dhcpd.conf** file based on your environment, you need to start or restart your DHCPD service. For more information, see http://ipxe.org/howto/dhcpd

Sample DHCP Configuration

```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
#option definitions common to all supported networks...
#option domain-name "example.org";
#option domain-name-servers 192.168.203.46;


#filename "pxelinux.0";
next-server 192.168.123.21;# IP address of ASM Server


default-lease-time 6000;
max-lease-time 7200;


# Use this to enble / disable dynamic dns updates globally.
#ddns-update-style none;


# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;


# Use this to send dhcp log messages to a different log file (you also
have to hack syslog.conf to complete the redirection.
log-facility local7;


# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.


#subnet 192.168.123.0 netmask 255.255.255.0 {
#}


# This is a very basic subnet declaration.


subnet 192.168.123.0 netmask 255.255.255.0 {
range 192.168.123.24 192.168.123.29;
option subnet-mask 255.255.255.0;
option routers 192.168.123.1;
if exists user-class and option user-class = "iPXE" {
    filename "bootstrap.ipxe";
  } else {
    filename "undionly.kpxe";
  }
}


# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.
```

```
#subnet 10.254.239.32 netmask 255.255.255.224 {
#range dynamic-bootp 10.254.239.40 10.254.239.60;
#option broadcast-address 10.254.239.31;
#option routers rtr-239-32-1.example.org;
#}


#A slightly different configuration for an internal subnet.
#subnet 10.5.5.0 netmask 255.255.255.224 {
#range 10.5.5.26 10.5.5.30;
#option domain-name-servers ns1.internal.example.org;
#option domain-name "internal.example.org";
#option routers 10.5.5.1;
#option broadcast-address 10.5.5.31;
#default-lease-time 600;
#max-lease-time 7200;
#}


# Hosts which require special configuration options can be listed in
# host statements.   If no address is specified, the address will be
# allocated dynamically (if possible), but the host-specific information
# will still come from the host declaration.


#host passacaglia {
#  hardware ethernet 0:0:c0:5d:bd:95;
#  filename "vmunix.passacaglia";
#  server-name "toccata.fugue.com";
#}


# Fixed IP addresses can also be specified for hosts.   These addresses
# should not also be listed as being available for dynamic assignment.
# Hosts for which fixed IP addresses have been specified can boot using
# BOOTP or DHCP.   Hosts for which no fixed address is specified can only
# be booted with DHCP, unless there is an address range on the subnet
# to which a BOOTP client is connected which has the dynamic-bootp flag
# set.
#host fantasia {
#  hardware ethernet 08:00:07:26:c0:a5;
#  fixed-address fantasia.fugue.com
#}


# You can declare a class of clients and then do address allocation
# based on that.   The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.

#class "foo" {
#  match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
#}

#shared-network 224-29 {
#subnet 10.17.224.0 netmask 255.255.255.0 {
#option routers rtr-224.example.org;
#  }
#  subnet 10.0.29.0 netmask 255.255.255.0 {
#    option routers rtr-29.example.org;
#  }
#   pool {
#     allow members of "foo";
#     range 10.17.224.10 10.17.224.250;
#   }
#   pool {
#     deny members of "foo";
#     range 10.0.29.10 10.0.29.230;
#   }
#}
```

Deploying WinPE on the Virtual Appliance

You need to perform the following configuration tasks before using ASM to deploy Windows OS.

NOTE: You should use Microsoft ADK 8.1 or ADK 8.0 installed in the default location..

1. Create a Windows repository with Windows installation media on the ASM appliance. For more information, see Create a repository with Windows installation media on ASM Appliance
2. Create a WinPE image to support Windows 2008 R2, Windows 2012 or Windows 2012 R2 deployment for bare metal or a VMware virtual machine, and update install media for Windows 2008, Windows 2012 or Windows 2012 R2 to include drivers and necessary updates to support ASM. For more information, see Creating WinPE Image and Update Install Media for Windows 2008, Windows 2012 and Windows 2012 R2
3. Copy WinPE, install media to the ASM repository, and update permissions for all files in the repository. For more information, see Copying WinPE and Install Media to ASM Repository and Updating Permissions

Create a Repository with Windows Installation Media on ASM Appliance

1. Log in to the virtual appliance with the user name *delladmin*.
2. Copy the **Windows.iso** file to the directory **/var/lib/razor/repo-store/**
3. Using a text editor, create a **/tmp/windows_repo.json** file with the following content:

   ```
   {
       "name": "<your windows repo name>",
       "iso-url": "file:///var/lib/razor/repo-store/<windows_ISO_name>.iso"
   }
   ```
4. To register the **.iso** file, run the following command. At command line interface, you have to enter your delladmin password.

   ```
   "sudo razor create-repo --json /tmp/windows_repo.json"
   ```
5. To verify whether or not the repository is created, run the following command:

   ```
   "sudo razor repos"
   ```
6. Run the following commands to extract the **.iso file** from the directory **/var/lib/razor/repo-store** to the directory **/var/lib/razor/repo-store/< your window repo name>**. Make sure that your Windows **.iso file** is available in **“repo-store”** directory where you run the following commands.

   ```
   "sudo mount -o loop /var/lib/razor/repo-store/<windows_ISO_name>.iso /mnt"
   "sudo rsync -av /mnt/ /var/lib/razor/repo-store/<your Windows repo name>"
   "sudo umount /mnt"
   ```
7. Update permissions for the directory, by running the command:

   ```
   "sudo find <your Windows repo name> -print0 | sudo xargs -0 chown
   razor:razor"
   ```

Creating WinPE Image and Updating Install Media for Windows 2012 and Windows 2012 R2

To create WinPE Image and update Install Media for Windows 2008, Windows 2012 and Windows 2012 R2:

1. Log in to the ASM virtual appliance and copy the scripts **build-razor-winpe.ps1** and **razor-client.ps1** from the **/opt/razor-server/build-winpe** directory to a folder created in the ADK machine. For example, ADK machine directory may be **c:\buildpe**.
2. In the **razor-client.ps1** file, replace `${server}` with the IP address of your ASM virtual appliance in the following code:

   ```
   $baseurl = http://${server}:8080/svc
   ```

   After completing this task, the following line is displayed.

   ```
   $baseurl = http://192.168.0.17:8080/svc
   ```

   You should have Windows Assessment and Deployment toolkit that contains the Windows PE environment used to automate the Windows installer installed in the DEFAULT location on a Windows machine. Licensing for Windows PE requires that you build your own customized WinPE WIM image containing the required scripts.

   NOTE:

   - If any additional drivers are required, add the drivers under the **drivers** folder. The drivers are installed into the Windows image, if applicable. The drivers that do not apply to the OS being processed are ignored.
   - If you want deploy Windows to VMWare VMs, the WinPE drivers for the VMXNET3 virtual network adapter from VMWare required. The instructions for obtaining a VMXNET3 driver from VMWare are listed below.
   - If you deploy Windows to an M420 server, drivers for Broadcom network adapters must be added to the image, as they are not included in Windows. The instructions for including these drivers are listed below. Obtain these device drivers from Dell.com.
   - Native driver support for Windows 2008 is limited, so obtain the latest NIC and RAID drivers for Windows 2008 from Dell.com
   - If you deploy Cisco servers, make sure to obtain appropriate device level from Cisco for the OS, which you are trying to deploy.

   The install scripts require the default location for the ADK. This package is obtained from Microsoft.
3. Copy the **build-razor-winpe.ps1** and **razor-client.ps1** scripts created to a directory on your machine with ADK 8.0 or 8.1 installed in the default location as described in step 1.
4. Obtain a copy of the Broadcom Drivers for an m420 server from dell.com and install the driver package on a Windows 2012 or 2012 R2 machine. Locate the Windows install drivers on the files ystem and copy them to the **Drivers** folder created in the step 3. These drivers typically start with "b57".

5. Obtain a copy of the VMware Windows drivers for the VMXNET 3 adapter from VMware. To obtain the VMware Windows drivers:

    a. Install VMware tools on a running Windows 2012 or Windows 2012 R2 and on the virtual machine.

    b. Go to the **C:\Program Files\Common Files\VMware\Drivers** directory.

    c. Copy the contents in the **Drivers** folder to the directory that contains your WinPE build scripts.

6. Copy the files **boot.wim** and **install.wim** from the ASM virtual appliance to the directory on your ADK machine. The **boot.wim** and **install.wim** files can be found in the **/var/lib/razor/repo-store/<your Windows repo>/SOURCES** directory.
7. Using a command line tool for PowerShell, go to the directory containing your build scripts, **Drivers** folder, and **boot.wim** and **install.wim** files. This directory should contain these files only.
8. To run the build script, run the command:

    ```
    powershell -executionpolicy bypass -noninteractive -file build-razor-
    winpe.ps1
    ```

    NOTE: This step takes some time to complete. After completion, it creates a directory with the name `razor-winpe` under the current working directory. The final custom WinPE image, **bootmgr.exe** (for Windows 2012 R2 repositories), **boot.wim**, and **install.wim** are copied to this directory.

9. For Windows 2008 installs, some additional fonts must be copied from the ADK machine to the repository folder on the ASM appliance. Go to the directory on your 8.1 ADK machine **C:\Program Files (x86)\Windows Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\Media\Boot\Fonts** and copy all **.ttf** type files to your Windows 2008 repository under **<Windows 2008 repo name>/boot/fonts**

Copying WinPE and Install Media to ASM Repository and Updating Permissions

To copy WinPE, install media to ASM repository, and update permissions for all files in the repository:

1. Copy the new **boot.wim** and **install.wim** files to the ASM virtual appliance under **/var/lib/razor/repo-store/<your Windows repo>/Sources**
2. Make sure you update the permissions on the **boot.wim** and **install.wim** files on the ASM virtual appliance. Therefore, you can run the files. To perform this task, run the following commands:

    ```
    "sudo chmod 755 /var/lib/razor/repo-store/<your windows repo>/Sources/
    boot.wim"
    "sudo chmod 755 /var/lib/razor/repo-store/<your windows repo>/Sources/
    install.wim"
    ```

3. Rename the new WinPE image file that you have created in the earlier section to **razor-winpe.wim**, and then copy the file to the root of your Windows repository created using the steps described in the section Create a repository with Windows installation media on ASM appliance.
4. If you are deploying Windows 2008 or Windows 2012 R2, you should also copy the latest **bootmgr.exe** file to the root of your Windows repository created using the steps described in the section Create a repository with Windows installation media on ASM appliance. This file is available in the output directory when you create your customized WinPE image as specified in the earlier section.
5. For Windows 2008 R2 installations, additional fonts are required to support WinPE 4.0 or WinPE 5.0. On your ADK machine, locate the following directory **C:\Program Files (x86)\Windows Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation Environment\amd64\Media\Boot\Fonts**, and copy all the **.ttf** type files to your Windows 2008 repository into the directory **/var/lib/razor/repo-store/<your Windows 2008 directory>//boot/fonts/**

6. Make sure that the right privileges are granted to the repository files.

   ```
   "sudo chmod 755 /var/lib/razor/repo-store/<your windows repo>/bootmgr.exe"
   "sudo chmod 755 /var/lib/razor/repo-store/<your windows repo>/razor-
   winpe.wim"
   "sudo find <your windows repo> -print0 | sudo xargs -0 chown razor:razor"
   “sudo setsebool -P samba_export_all_ro 1”
   ```

Importing Linux ISOs on the Virtual Appliance for Operating System Deployment

The following steps provide instructions to import Red Hat Enterprise Linux 6.5 ISO on the ASM virtual appliance for Operating System Deployment.

1. Log in to virtual appliance with the user name *delladmin*.
2. Copy the ISO file to the directory **/var/lib/razor/repo-store/**.
3. To create a Red Hat Enterprise Linux 6.5 repository, create a **/tmp/rhel65_repo.json** file with the following content:

   ```
   {
   “name”: “<your rhel repo name>”,

   “iso-url”: file:///var/lib/razor/repo-store/<Red Hat ISO name>.iso

   }
   ```

4. To register the **.iso** file, run the following command using the content file created in step 3. The example here uses the **rhel65_repo.json** file created in the earlier step.

   ```
   sudo razor create-repo --json /tmp/rhel65_repo.json
   ```

5. To verify whether or not the repository is created, run:

   ```
   sudo razor repos
   ```

6. Change directory to **/var/lib/razor/repo-store/rhel65** directory. If the operating system files are already available, continue to Step 7. Otherwise, run the following commands to extract the **.iso** file from the directory **/var/lib/razor/repo-store** to the directory **/var/lib/razor/repo-store/rhel65**. Make sure that the Linux **.iso** file is available in “repo-store” directory where you run the following commands.

   ```
   “sudo mount -o loop /var/lib/razor/repo-store/<RHEL ISO NAME>.iso /mnt”

   “sudo rsync -av /mnt/* /var/lib/razor/rep-store/<your rhel repo name>”

   “sudo umount /mnt”
   ```

7. Make sure that the correct privileges are granted to the repository files.

   ```
   “sudo find <your rhel repo name> -print0 | sudo xargs -0 sudo chown
   razor:razor”
   ```

8. ASM uses a default kickstart file to automate the installation of Linux. If you want to customize while installing the operating system, you can customize the kickstart file template “kickstart.erb” used to automate the installation.

   Use the `sudo` command to edit the **kickstart.erb** file available in the following directory **/opt/razor-server/installers/redhat**, and then enter the necessary customizations for the install. For more information about editing kickstart files for Linux install automation, refer to Linux documentation.

   NOTE: Currently, only one kickstart version is supported for Linux. Changes here affect both CentOS and Red Hat OS installations.

4

Customizing Virtual Machine Templates for VMware and Hyper-V

For ASM virtual machine (VM) cloning to work in conjunction with application components, you must customize the virtual machine and virtual machine templates, install the puppet agent, and then install the appropriate startup scripts.

Customizing Virtual Machine Templates or Virtual Machines for VMware or Hyper-V

ASM can clone existing virtual machines and virtual machine templates in vCenter as long as they exist in the same vCenter datacenter. The source virtual machines and virtual machine templates must be customized according to the instructions provided in the section. After customization, you must shut down the virtual machine and you cannot restart the virtual machine. You can clone virtual machine templates that exist in the library for SCVMM by using ASM. However, the source virtual machine templates are must be created according to the instructions provided in the section.

NOTE: After customization, if you restart the virtual machines, the template will no longer valid for cloning, and in that case, the verification file must be deleted. See later in this section about deleting the verification file.

To customize VMware virtual machines and virtual machine templates, you must install the following components:

- For VMware tools: If ASM has deployed the virtual machine being used for customizing the virtual machine for cloning, you must add a DVD drive to install VMware tools. In this case, the puppet agent is already installed on the virtual machine.
- Additional components that need to be included in virtual machine and virtual machine templates are same for both Hyper-V and VMware:
  - Puppet certificate name scripts – You can find the puppet certificate name script in **/opt/asm-deployer/scripts** on the ASM appliance. You can move the file to **/var/lib/razor/repo-store** and access it through the network share on the appliance by the following instruction:
  - On a windows virtual machine, you must copy the script to **"C:\"**
  - On a Linux virtual machine, you must copy these scripts to /usr/local/bin.
  - Verify wheather or not the permissions are set on these scripts to at least read and execute.
  - run the command to verify:

```
chmod 755 /usr/local/bin/puppet_certname.sh
chmod 755 /usr/local/bin/puppet_certname.rb
```

- Puppet Agent — You must install the puppet agent on the virtual machine. The puppet agent is available on the appliance for both Windows and Linux in **/var/lib/razor/repo-store** directory. If the virtual machine being customized and that has access to the ASM appliance, and then you can connect to the same razor shared by connecting to **\\<ASM appliance hostname or IP>\razor\puppet-agent**

> **NOTE:** The puppet agent version should be greater than 3.0.0 and lower than 3.4.

After you install the puppet agent, make sure the puppet agent service is enabled to run on system start. For Windows, this must be done by viewing the services and setting the puppet agent service to "automatic".

  - To verify whether or not the puppet agent is enable, run the following command:

    ```
    puppet resource service puppet
    ```

    You are able to see whether or not the service “enable” is set to “true” or “false”.

  - If the service is not set to true from the above command, enable the puppet agent service, run the following puppet command as administrator:

    ```
    puppet resource service puppet enable=true
    ```

- Make sure the NTP is configured based on virtual machine. The virtual machine and ASM appliance must have synchronized time.
- Configure the **puppet.conf** file to use "**dellasm**" as a server. To configure the **puppet.config** file, perform the following:

  - Run the following command as administrator in Windows and root in Linux to identify the location of puppet.config file:

    ```
    puppet config print config
    ```

  The command displays the directory of the puppet.config file.

- Open the **puppet.config** file by using the text editor and add the following line to the [**main**],[**master**], and [**agent**] section. If any of these sections does not exist, create them:

  server = dellasm

  - Make sure the ASM appliance hostname dellasm can be resolved by using DNS. Either add the appropriate CNAME record in DNS* or add the appropriate host entries to /etc/hosts or C:\windows

    `\system32\driver\etc\hosts based on your operating system.`

- Make sure the puppet agent does not contain any existing SSL certificates. The directory listed by the following command should be empty (remove all files in the directory if it exists).To verify run the following command for this.

  ```
  puppet config print ssldir
  ```

> **NOTE:** After preparing the base virtual machine, in case the virtual machine is restarted, the puppet verification file will need to be deleted from system. This file can be found in Windows at `C:\ProgramData\puppet_verification_run.txt or in Linux at /var/lib/puppet_verification_run.txt.`

Customizing Linux Template

Perform the following task to customize Linux template.

1. You must update the Network Interfaces so that they will not be associated with the base virtual machine MAC address (varies based on OS, examples below). To update, run the following command:

   ```
   RHEL/CentOS:
   rm /etc/udev/rules.d/70-persistent-net.rules
   rm/lib/udev/rules.d/75-persistent-net-generator.rules
    sed -i "/^HWADDR/d" /etc/sysconfig/network-scripts/ifcfg-eth0
   Debian/Ubuntu:
   rm /lib/udev/rules.d/75-persistent-net-generator.rules
   ```

2. Configure cronjob to execute the puppet_certname.sh script and restart or start the puppet service.

   ```
   crontab –e
   ```

   The puppet restart should be set up in the crontab addition.

   a. Add the following line to this file

      ```
      @reboot /usr/local/bin/puppet_certname.sh; /etc/init.d/puppet restart
      ```

   b. Run the following command, and ensure that you see the above line, to verify the crontab is updated as expected or not,

      ```
      crontab -l
      ```

Customizing Windows Template

Perform the following steps to make sure windows schedules tasks on startup.

1. Launch Windows Task Scheduler and create a new task.
2. The task runs C:\puppet_certname.bat.
3. Make sure the task can run even if the user is not logged in. To enable this option, right-click the puppet_certname.bat and click **Properties**. In the puppet_certname properties dialog box, under **Security** options, select **Run only when user is logged on**.
4. Specify the start in directory same as the script location (c:\).

5

Configuring ASM Virtual Appliance for NetApp Storage Support

For ASM to support NetApp, perform the following tasks:

- Add NetApp Ruby SDK libraries to the appliance. For more information about adding SDK libraries, see Adding NetApp Ruby SDK
- Enable HTTP/HTTPs for the NFS share. For more information, see Enabling HTTP or HTTPs for NFS Share

  Make sure license is enabled for NFS on NetApp. To obtain and install the license, refer *NetApp documentation*.
- Create the credentials to access NetApp Storage. For creating credential, see *Active System Manager version 7.6 User's Guide*.
- Configure the NetApp Storage Component. For more information, see Configuring the NetApp Storage Component
- Configure the the fileshare Network on the server component. For More information, see *Active System Manager version 7.6 User's Guide*

Adding NetApp Ruby SDK

NetApp Manageability SDK is available to download directly from NetApp. You need a NetApp NOW account to download the SDK.

NaServer.patch file is available on the ASM appliance at location /etc/puppetlabs/puppet/module/netapp/files/NaServer.patch

1. Log in to virtual appliance.
2. Copy the NetApp SDK Ruby lib files (..\lib\ruby\NetApp\*) to the virtual appliance /tmp/*
3. Copy ruby libs from SDK to /etc/puppetlabs/puppet/modlues/netapp/lib/puppet/util/network_device/netapp
4. Copy ruby libs from SDK to /etc/puppetlabs/puppet/modlues/netapp/lib/puppet/util/network_device/netapp
5. Sudo cp /tmp/*.rb /etc/puppetlabs/puppet/modules/netapp/lib/puppet/util/network_device/netapp/
6. Copy NaServer.patch to appliance in /tmp/ directory
7. Run patch:

   ```
   sudo patch /etc/pupetlabs/puppet/modules/netapp/lib/puppet/util/
   network_device/netapp/NaServer.rb < /tmp/NaServer.patch
   ```

8. Update the permissions on the NetApp module. To update the permissions, run the following command:

   ```
   sudo chmod 755 /etc/puppetlabs/puppet/modules/netapp/lib/puppet/util/
   network_device/netapp/*
   ```

9. Change the owner of the files. To change the owner of the files, run the following command:

   ```
   sudo chown pe-puppet:pe-puppet /etc/puppetlabs/puppet/modules/netapp/lib/
   puppet/util/network_device/netapp/*
   ```

Enable HTTP or HTTPs for NFS share

Connect to the NetApp Filer using ssh and run the `option http`command to see the current settings. If the property `httpd.admin.ssl` is set to off, then run the command `option httpd.admin.ssl.enable on` to enable HTTPS.

```
ADC-NetApp01> options http
httpd.access  legacy
httpd.admin.access  legacy
httpd.admin.enable  on
httpd.admin.hostsequiv.enable on
httpd.admin.max_connections  512
httpd.admin.ssl.enable  on
httpd.admin.top-page.authentication on
httpd.autoindex.enable  on
httpd.bypass_traverse_checking on
httpd.enable   on
httpd.ipv6.enable  off
httpd.log.format  common(value might be overwritten in takeover)
httpd.method.trace.enable  off
httpd.rootdir  /vol/vol0/home/http
httpd.timeout 300(value might be overwritten in takeover)
httpd.timewait.enable  off(value might be overwritten in takeover
ADC-NetApp01>
```

Configuring NetApp Storage Component

The following settings must be configured in the NetApp storage component.

For more information about NetApp Storage Component, see *Active System Manager version 7.6 User's Guide*.

- Target NetApp
- Storage Value
- New Volume Name
- Storage Size
- Aggregate Name
- The Space Reservation Mode
- Snapshot percentage
- The Percentage of Space to Reserve for Snapshot
- Auto-increment

- Persistent
- NFS Target IP

6

Completing Initial Configuration

Log in to ASM using the appliance IP address after completing the steps in this guide,

After logging into ASM, you need complete the basic configuration setup in the **Initial Setup** wizard. For more information about completing the initial setup, see the *Active System Manger Version 7.6 User's Guide*.