Active System Manager
Version 8.0 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.

Copyright © 2014 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Dell™ and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

2014 - 11

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 8.0.

What is New in this Release

- Infrastructure firmware compliance and updates
- Wizard based chassis, server and IO onboarding with advanced configuration
- 13th generation server support.
- Streamlined installation experience
- FCoE support with Brocade, Dell s5000, and Cisco Nexus
- Resource health monitoring
- Enhanced role-based access control
- Service Lifecycle Improvements including scheduling a service deployment and scaling down a running 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 8.0 User's Guide*
- *Dell Active System Manager version 8.0 Release Notes*
- *Dell Active System Manager version 8.0 Compatibility Matrix 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 8.0 supports following license types:

- Trial License — A Trial license can be procured through 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 for 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 or Microsoft virtualization environment. 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.
- Deploying the ASM virtual appliance to a VMware vSphere environment requires that both VMware vCenter Server and VMware vSphere Client be running.
- Deploying the ASM virtual appliance to a Microsoft Windows virtualization environment requires that the hyper-v host on which ASM will be deployed is installed on a running instance of 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: 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.

Specification	Prerequisite
	• The virtual appliance is able to communicate with the PXE network in which the appliance is 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.
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. • 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.

Specification	Prerequisite
	• 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 PowerEdge M I/O Aggregator	• 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.
Dell Networking MXL 10/40GbE blade switch	• Any VLAN which is dynamically provisioned by ASM must exist on the switch. • Server facing ports must be in hybrid mode.. • Server facing ports must be configured for spanning tree portfast. • Server facing ports must be configured for spanning tree portfast. • Make sure DCB settings are configured on each port.
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. • Virtual ports must be enabled on compellent. • Follow Compellent best-practices for storage configuration.
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.

Specification	Prerequisite
	• Appropriate licenses are deployed on the VMware vCenter.
System Center Virtual Machine Manager (SCVMM)	• See System Center Virtual Machine Manager (SCVMM) Prerequisites.
PXE Setup	• Either use Active System Manager as the PXE responder by configuring through ASM user interface, by **Getting Started** page or follow instructions in Configuring ASM Virtual Appliance as PXE Responder.

Prerequisites for M1000e (with MXL), S5000, and Compellent

The following table describes the prerequisites for the FCoE solution offered using M1000e (with MXL), S5000, and Compellent. For more information, see http://en.community.dell.com/techcenter/extras/m/white_papers/20387203

Resource	Prerequisites
MXL	• DCB needs to be enabled. • VLT needs to be disabled. • FIP Snooping feature needs to be enabled on the MXL. `Conf` `Feature fip-snooping` • Port-channel member interfaces needs to have below configuration. `interface range tengigabitethernet 0/33 – 36` `port-channel-protocol lacp` `port-channel 128 mode active` `exit` `protocol lldp` `no advertise dcbx-tlv ets-reco` `dcbx port-role auto-upstream` `no shut` `exit` • Port-channel connecting S5000 switch needs to have following configuration. `interface port-channel 128` `portmode hybrid` `switchport` `fip-snooping port-mode fcf` • Server facing ports need to have following configuration.. `portmode hybrid` `switchport`

Resource	Prerequisites
	protocol lldp dcbx port-role auto-downstream no shut exit
S5000	Following is the prerequisite for S5000. • Enable Fibre Channel capability and Full Fabric mode. feature fc fc switch-mode fabric-services • Enable FC ports connecting to Compellent storage array and FC ports connecting to other S5000 switch via ISL links. interface range fi 0/0 - 7 no shut • Create DCB Map. dcb-map SAN_DCB_MAP priority-group 0 bandwidth 60 pfc off priority-group 1 bandwidth 40 pfc on priority-pgid 0 0 0 1 0 0 0 0 exit • Create a FCoE VLAN. fcoe-map default_full_fabric fabric-id <FCoE VLAN ID> vlan <FCoE VLAN Id> fc-map <FC MAP> exit NOTE: Following is the process of generating the FC MAP. For generating the fc-map use below ruby code. Here VLAN ID is FCoE VLAN ID. fc_map = vlanid.to_i.to_s(16).upcase[0..1] fc_map.length == 1 ? fc_map = "0EFC0#{fc_map}" : fc_map = "0EFC#{fc_map}"
Compellent	Fault domain need to be created as per Compellent best practices.

Prerequisites for Rack Server, S5000, and Compellent

The following table describes the prerequisites for the FCoE solution offered using Rack Server, S5000, and Compellent. For more information, see http://en.community.dell.com/techcenter/extras/m/white_papers/20387203

Resource	Prerequisites
S5000	• DCB needs to be enabled. • VLT needs to be disabled. • Enable Fibre Channel capability and Full Fabric mode. `feature fc` `fc switch-mode fabric-services` • Enable FC ports connecting to Compellent storage array and FC ports connecting to other S5000 switch via ISL links. `interface range fi 0/0 - 7` `no shut` • Create DCB Map. `dcb-map SAN_DCB_MAP` `priority-group 0 bandwidth 60 pfc off` `priority-group 1 bandwidth 40 pfc on` `priority-pgid 0 0 0 1 0 0 0 0` `exit` • Create a FCoE VLAN. `interface vlan <VLAN ID> [Create VLAN for FCoE]` `exit` • Create FCoE Map. `fcoe-map default_full_fabric` `fabric-id <FCoE VLAN ID> vlan <FCoE VLAN Id>` `fc-map <FC MAP>` `exit`
Compellent	Fault domain need to be created as per Compellent best practices.

Prerequisites for M1000e (with MXL), S5000, Brocade, and Compellent

The following table describes the prerequisites for the FCoE solution offered using M1000e (with MXL), S5000, Brocade, and Compellent. For more information, see http://en.community.dell.com/techcenter/extras/m/white_papers/20387203

Resource	Prerequisites
MXL	• DCB needs to be enabled. • VLT needs to be disabled. • FIP Snooping feature needs to be enabled on the MXL. `conf` `Feature fip-snooping` • Port-channel member interfaces needs to have below configuration. `interface range tengigabitethernet 0/33 – 36` `port-channel-protocol lacp` `port-channel 128 mode active` `exit` `protocol lldp` `no advertise dcbx-tlv ets-reco` `dcbx port-role auto-upstream` `no shut` `exit` • Port-channel connecting S5000 switch needs to have following configuration. `interface port-channel 128` `portmode hybrid` `switchport` `fip-snooping port-mode fcf` • Server facing ports needs to below configuration `portmode hybrid` `switchport` `protocol lldp` `dcbx port-role auto-downstream` `no shut` `exit`
S5000	Below configuration is prerequisite for S5000. • Enable Fibre Channel capability and Full Fabric mode. `feature fc` • Enable FC ports connecting to Compellent storage array and FC ports connecting to other S5000 switch via ISL links. `interface range fi 0/0 – 7` `no shut` • Create DCB Map `dcb-map SAN_DCB_MAP` `priority-group 0 bandwidth 60 pfc off` `priority-group 1 bandwidth 40 pfc on` `priority-pgid 0 0 0 1 0 0 0 0` `exit`

Resource	Prerequisites
	• Create a FCoE VLAN `interface vlan <VLAN ID> [Create VLAN for FCoE]` `exit` • Create FCoE Map `fcoe-map default_full_fabric` `fabric-id <FCoE VLAN ID> vlan <FCoE VLAN Id>` `fc-map <FC MAP>` `exit` • Apply FCoE MAP to interface `interface fibrechannel 0/0` `fabric default_full_fabric` `no shutdown` **NOTE:** Below is the process of generating the FC MAP For generating the fc-map use below ruby code. Here VLAN ID is FCoE VLAN ID `fc_map = vlanid.to_i.to_s(16).upcase[0..1] fc_map.length == 1 ? fc_map = "0EFC0#{fc_map}" : fc_map = "0EFC#{fc_map}"`
Brocade	Alias needs to be created having Compellent fault domain WWPN accessible on Brocade switch.
Compellent	Nothing specific for ASM

Prerequisites for Rack Server, S5000, Brocade and Compellent

The following table describes the prerequisites for the FCoE solution offered using Rack Server, S5000, Brocade and Compellent. For more information, see http://en.community.dell.com/techcenter/extras/m/white_papers/20387203

Resource	Prerequisites
S5000	• DCB needs to be enabled. • VLT needs to be disabled. • Enable Fibre Channel capability and Full Fabric mode. `feature fc`

Resource	Prerequisites
	• Enable FC ports connecting to Compellent storage array and FC ports connecting to other S5000 switch via ISL links. `interface range fi 0/0 - 7` `no shut` • Create DCB Map. `dcb-map SAN_DCB_MAP` `priority-group 0 bandwidth 60 pfc off` `priority-group 1 bandwidth 40 pfc on` `priority-pgid 0 0 0 1 0 0 0 0` `exit` • Create a FCoE VLAN. `interface vlan <VLAN ID> [Create VLAN for FCoE]` `exit` • Create FCoE Map. `fcoe-map default_full_fabric` `fabric-id <FCoE VLAN ID> vlan <FCoE VLAN Id>` `fc-map <FC MAP>` `exit`
Brocade	Alias needs to be created having Compellent fault domain WWPN accessible on Brocade switch.
Compellent	Fault domain need to be created as per Compellent best practices.

Prerequisites for M1000e (with MXL), Cisco Nexus, and Compellent

The following table describes the prerequisites for the FCoE solution offered using M1000e (with MXL), Cisco Nexus, and Compellent. For more information, see http://en.community.dell.com/techcenter/extras/m/white_papers/20387203

Resource	Prerequisites
MXL	• DCB needs to be enabled. • VLT needs to be disabled. • FIP Snooping feature needs to be enabled on the MXL. `conf` `Feature fip-snooping` • Port-channel member interfaces needs to have below configuration. `interface range tengigabitethernet 0/33 - 36`

Resource	Prerequisites
	`` port-channel-protocol lacp port-channel 128 mode active exit protocol lldp no advertise dcbx-tlv ets-reco dcbx port-role auto-upstream no shut exit ``` • Port-channel connecting Cisco Nexus switch needs to have following configuration. ``` interface port-channel 128 portmode hybrid switchport fip-snooping port-mode fcf ``` • Server facing ports needs to have following configuration. ``` portmode hybrid switchport protocol lldp dcbx port-role auto-downstream no shut exit ```
Cisco Nexus	Following is the prerequisite for Cisco Nexus. • Enable required features. ``` feature fcoe feature npiv feature lacp ``` • Create a new VSAN - instantiate it in the VSAN database. ``` conf vsan database vsan <vsan id> ``` • Configure regular ethernet VLANs, and then the FCoE VLAN is created with an assignment to its respective VSAN. ``` vlan <fcoe vlan> fcoe vsan <vsan> ``` • Instantiate but do not configure the upstream port-channel (LAG) to the core /aggregation switch. • Instantiate but do not configure the downstream port-channel (LAG) to the IOA4. • Create the VFC interface to bind to the servers CNA FIP MAC address. This can be located in the CMC WWN table or the IDRAC page for the server.

Resource	Prerequisites
	Example `interface vfc101` `bind mac-address 5C:F9:DD:16:EF:07` `no shutdown` `interface vfc102` `bind mac-address 5C:F9:DD:16:EF:21` `no shutdown` • Move back into the VSAN database and create entries for the new VFC just created and create entries for the FC port(s) that will be used. vsan database vsan 2 interface vfc101 vsan 2 interface vfc102 vsan 2 interface fc2/1 vsan 2 interface fc2/2 NOTE: All the Compellent ports needs to part of the same VSAN.
Compellent	Create fault domain as per Compellent best practices.

Prerequisites for Rack Server, Cisco Nexus, and Compellent

The following table describes the prerequisites for the FCoE solution offered using Rack Server, Cisco Nexus and Compellent. For more information, see http://en.community.dell.com/techcenter/extras/m/white_papers/20387203

Resource	Prerequisites
Cisco Nexus	Following is the prerequisite for Cisco Nexus. • Enable required features. `feature fcoe` `feature npiv` `feature lacp` • Create a new VSAN - instantiate it in the VSAN database. `conf` `vsan database` `vsan <vsan id>` • Configure regular ethernet VLANs, and then the FCoE VLAN is created with an assignment to its respective VSAN. `vlan <fcoe vlan>` `fcoe vsan <vsan>`

Resource	Prerequisites
	• Instantiate but do not configure the upstream port-channel (LAG) to the core /aggregation switch. • Instantiate but do not configure the downstream port-channel (LAG) to the IOA4. • Create the VFC interface to bind to the servers CNA FIP MAC address. This can be located in the CMC WWN table or the IDRAC page for the server. For Example `interface vfc101` `bind mac-address 5C:F9:DD:16:EF:07` `no shutdown` `interface vfc102` `bind mac-address 5C:F9:DD:16:EF:21` `no shutdown` • Move back into the VSAN database and create entries for the new VFC just created and create entries for the FC port(s) that will be used. vsan database vsan 2 interface vfc101 vsan 2 interface vfc102 vsan 2 interface fc2/1 vsan 2 interface fc2/2 **NOTE:** All the Compellent ports needs to part of the same VSAN.
Compellent	Create fault domain as per Compellent best practices.

Prerequisites for M1000e (with MXL), Cisco Nexus, Brocade, and Dell Compellent

The following table describes the prerequisites for the FCoE solution offered using M1000e (with MXL), Cisco Nexus, Brocade, and Dell Compellent. For more information, see http://en.community.dell.com/techcenter/extras/m/white_papers/20387203

Resource	Prerequisites
MXL	• DCB needs to be enabled. • VLT needs to be disabled. • FIP Snooping feature needs to be enabled on the MXL. `conf` `Feature fip-snooping`

Resource	Prerequisites
	• Port-channel member interfaces needs to have following configuration. `interface range tengigabitethernet 0/33 – 36` `port-channel-protocol lacp` `port-channel 128 mode active` `exit` `protocol lldp` `no advertise dcbx-tlv ets-reco` `dcbx port-role auto-upstream` `no shut` `exit` • Port-channel connecting Cisco Nexus switch needs to have following configuration. `interface port-channel 128` `portmode hybrid` `switchport` `fip-snooping port-mode fcf` • Server facing ports needs to have following configuration. `portmode hybrid` `switchport` `protocol lldp` `dcbx port-role auto-downstream` `no shutdown` `exit`
Cisco Nexus	Following is the prerequisite for Cisco Nexus: • Enable “npv” feature on the switch. This requires switch reboot and old configuration will be wiped off. (Ensure to backup the configuration before enabling the feature) `conf` `feature npv` • Enable required features . `feature fcoe` `feature npiv` `feature lacp` • Create new VSAN — instantiate it in the VSAN database. `conf` `vsan database` `vsan <vsan id>` • Configure regular Ethernet VLANs, and then the FCoE VLAN is created with an assignment to its respective VSAN `vlan <fcoe vlan>` `fcoe vsan <vsan>`

Resource	Prerequisites
	• Instantiate but do not configure the upstream port-channel (LAG) to the core /aggregation switch. • Instantiate but do not configure the downstream port-channel (LAG) to the IOA4. • Create the VFC interface to bind to the servers CNA FIP MAC address. This can be located in the CMC WWN table or the iDRAC page for the server. For Example `interface vfc101` ` bind mac-address 5C:F9:DD:16:EF:07` ` no shutdown` `interface vfc102` ` bind mac-address 5C:F9:DD:16:EF:21` ` no shutdown` • Move back into the VSAN database and create entries for the new VFC just created and create entries for the FC ports that are used. vsan database vsan 2 interface vfc101 vsan 2 interface vfc102 vsan 2 interface fc2/1 vsan 2 interface fc2/2 NOTE: All the Dell Compellent ports need to part of the same VSAN.
Brocade	Alias needs to be created having Dell Compellent fault domain WWPN accessible on Brocade switch.
Dell Compellent	Nothing specific for ASM.

Prerequisites for Rack Server, Cisco Nexus, Brocade, and Dell Compellent

The following table describes the prerequisites for the FCoE solution offered using Rack Server, Cisco Nexus, Brocade, and Dell Compellent. For more information, see http://en.community.dell.com/techcenter/extras/m/white_papers/20387203

Resource	Prerequisites
Cisco Nexus	Following is the prerequisite for Cisco Nexus: • Enable “npv” feature on the switch. You need to reboot the switch and delete the old

Resource	Prerequisites
	configuration. (Ensure to back up the configuration before enabling the feature). `conf` `feature npv` • Enable required features. `feature fcoe` `feature npiv` `feature lacp` • Create VSAN-instantiate it in the VSAN database. `conf` `vsan database` `vsan <vsan id>` • Configure regular Ethernet VLANs, and then the FCoE VLAN is created with an assignment to its respective VSAN. `vlan <fcoe vlan>` `fcoe vsan <vsan>` • Instantiate but do not configure the upstream port-channel (LAG) to the core /aggregation switch. • Instantiate but do not configure the downstream port-channel (LAG) to the IOA4. • Create the VFC interface to bind to the servers CNA FIP MAC address. This can be located in the CMC WWN table or the iDRAC page for the server. For Example: `interface vfc101` ` bind mac-address 5C:F9:DD:16:EF:07` ` no shutdown` `interface vfc102` ` bind mac-address 5C:F9:DD:16:EF:21` ` no shutdown` • Move back into the VSAN database and create entries for the new VFC just created and create entries for the FC ports that are used. vsan database vsan 2 interface vfc101 vsan 2 interface vfc102 vsan 2 interface fc2/1 vsan 2 interface fc2/2

Resource	Prerequisites
	NOTE: All the Dell Compellent ports need to part of the same VSAN.
Brocade	Alias needs to be created having Compellent fault domain WWPN, accessible on Brocade switch.
Dell Compellent	Create fault domain as per Dell Compellent best practices.

Prerequisites for M1000e (with MXL and FC FlexIOM), Brocade, and Dell Compellent

The following table describes the prerequisites for the FCoE solution offered using M1000e (with MXL and FC FlexIOM), Brocade, and Dell Compellent. For more information, see http://en.community.dell.com/techcenter/extras/m/white_papers/20387203

Resource	Prerequisites
MXL	• DCB needs to be enabled. • VLT needs to be disabled. • FC feature needs to be enabled on the MXL. Remove "fip-snooping" feature if enabled on the MXL. `conf` `feature fc` • Port-channel member interfaces needs to have following configuration. `interface range tengigabitethernet 0/33 – 36` `port-channel-protocol lacp` `port-channel 128 mode active` `exit` `protocol lldp` `no advertise dcbx-tlv ets-reco` `dcbx port-role auto-upstream` `no shut` `exit` • Server facing ports needs to have following configuration. `portmode hybrid` `switchport` `protocol lldp` `dcbx port-role auto-downstream` `no shut` `exit`
Brocade	Alias needs to be created having Dell Compellent fault domain WWPN accessible on Brocade switch.

Resource	Prerequisites
Dell Compellent	Create fault domain as per Dell Compellent best practices.

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 as well as on Active Directory and DNS servers used in SCVMM/HyperV deployments. ASM deployments support Active Directory and DNS servers which exist on the same machine. If Active Directory and DNS servers exist on separate machines, some manual tare-down may be required to remove host entries from the DNS server. ASM requires Windows RM to utilize default port and basic authentication. To enable these settings, on the SCVMM server and on the Active Directory and DNS server used in HyperV deployments, 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"}'
```

For Windows 2008:

```
winrm quickconfig
```

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 the SCVMM has its time synchronized with time of the associated timer server. If the SCVMM timer is set to 'off' mode by using the deployed Hyper-V hosts, you cannot 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-8.0-.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-8.0- <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 ASM VM. 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.

NOTE:

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 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 ASM virtual appliance on the Hyper-V host.
9. After ASM virtual appliance is deployed, right-click 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 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 ASM virtual appliance.

Configuring ASM Virtual Appliance as PXE Boot Responder

ASM requires both PXE and DHCP network services to function. ASM may be configured to act as the DHCP server and PXE responder on a PXE network if one is not present in the environment. This can be configured through the Getting Started menu for appliance setup in the ASM user interface. If an external DHCP or PXE server is used for the PXE network, follow the instructions in the section Configuring DHCP or PXE on External Servers.

4

Customizing Virtual Machine Templates for VMware and Hyper-V

ASM supports cloning virtual machines (VM) or virtual machine templates in VMware, and cloning virtual machine templates in Hyper-V. For ASM virtual machine or virtual machine template cloning, the virtual machine or virtual machine templates must be customized to make sure virtual machine or virtual machine templates have a unique identifier and can communicate back to the ASM appliance upon completion of the cloning process. This requires several customizing steps that depends on virtual machine which is needed to be cloned.

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

ASM can clone existing virtual machines and virtual machine templates in vCenter, or virtual machine templates in Hyper-V. The source virtual machines and virtual machine templates must be customized according to the instructions provided in this section. After customization, you must shut down the virtual machine and you cannot restart the virtual machine. For VMware virtual machines or virtual machine templates, cloning is supported as long as you are cloning within the same datacenter. For SCVMM the virtual machine templates must exist in the SCVMM library. Cloning virtual machines directly is not currently supported for Hyper-V.

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

The following customization is required only for VMware virtual machines:

Install VMWare Tools on the virtual machine:

- If the virtual machine being used does not have a DVD drive, you must add one. To do this, edit the settings of the virtual machine and add a DVD drive through your VMware management console.
- Once a DVD drive is available, right-click the virtual machine and select Guest-> Install/Upgrade VMware Tools. This will mount the media for VMware tools.
- Log into the operating system of the virtual machine and run the VMware tools installer within the OS running on the virtual machine. See VMware documentation for further information on installing VMware tools.

The following customization is required for both VMWare and Hyper-V virtual machine

Install the puppet agent on the virtual machine:

- If the virtual machine being used was successfully created by ASM, the puppet agent will already be installed.

- To install the puppet agent on the virtual machine, copy the puppet agent install files to the virtual machine. The puppet agent is available on the ASM appliance for both Windows and Linux

  in /var/lib/razor/repo-store directory. If the virtual machine being customized has network access to the ASM appliance, you can connect to this same directory as a network share directory using the address: **\\<ASM appliance hostname or IP>\razor\puppet-agent** .

  Depending on your operating system, the installer may require additional packages (.rpms) which are dependencies and you must install it first. If the installer reports such dependencies, use the correct method for your operating system to find and install the dependencies, and then retry installation of the 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 virtual machines, this must be done by viewing the services and setting the puppet agent service to "automatic".

  – For Linux virtual machines, verify whether or not the puppet agent is enabled by running the following command and checking the value of "enable" is set to true:

  ```
  Puppet resource service puppet
  ```

  – If the service is not set to true as noted above, run the following puppet command as administrator:

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

- Time must be synchronized between the ASM appliance and the virtual machine being cloned to ensure proper check in upon completion of cloning. Make sure NTP is configured on the virtual machine. Follow the appropriate instructions for your operating system to synchronize the virtual machine with an NTP server.
- 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" in Linux or "C:\windows\system32\driver\etc\hosts" in Windows.
- Configure the puppet.conf file to use "dellasm" as a server. To configure the puppet.conf file, perform the following:

  – Identify the location of the puppet.conf file. To do this, run the following command as "administrator" in Windows or "root" in Linux which will display the directory of the puppet.conf file.

  ```
  puppet config print config
  ```

  – Open the puppet.conf file by using a text editor and add the line "server = dellasm" to the [main], [master], and [agent] section. If any of these sections does not exist, create them. A sample resulting puppet.conf file may look similar to the following:

  ```
  [main]
  server=dellasm
  [master]
  server=dellasm
  [agent]
  server=dellasm
  ```

NOTE: Additional lines may be present in the puppet.conf file for your system. It is not necessary to delete any information from this file. You just need to ensure the previously noted section is present in the file.

Customizing Linux Template

Perform the following task to customize Linux template:

1. Ensure all instructions have been completed for VMware or Hyper-V virtual machines as noted in the previous section.
   a. Install VMware tools (VMware only)
   b. Install puppet agent and ensure it is configured to run on startup
   c. Make sure ASM appliance and virtual machine time are synchronized by NTP.
   d. Make sure DNS is configured for "dellasm" to resolve.
   e. Make sure `puppet.conf file` has updated configuration to point to "`dellasm`" as server.
2. Copy puppet `certname` scripts `puppet_certname.sh` and `puppet_certname.rb` to the virtual machine.
   a. You can find the puppet certificate name scripts for Linux (`puppet_certname.sh` and `ppet_certname.rb`) in /opt/asm-deployer/scripts on ASM appliance. You can move these files to /var/lib/razor/repo-store. The ASM appliance location /var/lib/razor/repo-store is a share that can be mounted to your virtual machine if the virtual machine has network connectivity to the ASM appliance

      NOTE: The INI file version in the puppet certificate name script must be 2.0.2.

   b. On a Linux virtual machine, you must copy these scripts to /usr/local/bin. Make sure the permissions are set on these scripts to at least read and execute. To do this, run the following commands:

      ```
      chmod 755 /usr/local/bin/puppet_certname.sh
      chmod 755 /usr/local/bin/puppet_certname.rb
      ```
3. Make sure the virtual machine has access to the internet, as this will be required to download and install the necessary ruby gem files. If your virtual machine will not have access to the internet, then download the ruby gem files for "inifile" and "hashie" and place them in the /usr/local/bin directory where you copied the `puppet certname` scripts.
4. You must update the Network Interfaces so that it will not be associated with the base virtual machine MAC address (varies based on OS, examples below). To update it, run the following:

   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
   ```
5. Configure **`cronjob`** to execute the **puppet_certname.sh** script and restart or start the puppet service.

   Type the following commands:

   ```
   crontab –e
   ```

   a. Add the following line to this file and then save and exit the 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
```

6. After completing customization, turn off the virtual machine. To create a virtual machine template, follow the appropriate steps for virtualization environment.

   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 Windows Template

Perform the following task to customize Linux template.

1. Make sure all instructions have been completed for VMware or Hyper-V virtual machines as noted in the previous section.
   a. Install VMware tools (VMware only)
   b. Install puppet agent and ensure it is configured to run on startup
   c. Make sure ASM appliance and virtual machine time are synchronized by NTP.
   d. Make sure DNS is configured for “dellasm” to resolve.
   e. Make sure puppet.conf file has updated configuration to point to “dellasm” as server
2. Copy puppet certname scripts `puppet_certname.bat` and `puppet_certname.rb` to the virtual machine.
   a. You can find the puppet certificate name scripts for Windows (puppet_certname.bat and ppet_certname.rb) in /opt/asm-deployer/scripts on ASM appliance. You can move these files to /var/lib/razor/repo-store. The ASM appliance location /var/lib/razor/repo-store is a share that can be mounted to your virtual machine if the virtual machine has network connectivity to the ASM appliance.

      NOTE: The INI file version in the puppet certificate name script must be 2.0.2.

   b. On a Windows virtual machine, you must copy these scripts to “`C:\`”
3. Make sure the virtual machine has access to the internet, as this is required to download and install the necessary ruby gem files. If your virtual machine will not have access to the Internet, then download the ruby gem files for "inifile" and "hashie" and place them in the "C:\" directory where you copied the puppet certname scripts.
4. Launch Windows Task Scheduler and create a new task.
5. Specify that task runs the script “`C:\puppet_certname.bat.`”
6. Specify that the task run in the “C:\” directory, this is an optional parameter but is required for ASM clone customization.
7. Make sure the task can run even you are not logged in and you must be able to run it with highest privilege.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 whether user is logged on or not.
8. Ensure that the check box is selected in the scheduled task settings for "If the running task does not end when requested, force it to stop." and select "Stop the existing instance" drop-down menu.
9. In addition, make sure the task is configured for the correct operating system at the bottom of General Settings.
10. Specify that the trigger for the task is to execute on startup.
11. After completing customization, turned off the virtual machine. To create a virtual machine template, follow the appropriate steps for your virtualization environment at this time.

NOTE: To create a virtual machine template in SCVMM, make sure the virtual machine template OS Configuration has an administrator password and if necessary, a Windows product key set. To do this, right click the virtual machine template and select "Properties", then select "OS Configuration" and enter a password in **Admin Password** and a product key in **Product Key** settings.

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.

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 8.0 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 8.0 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 8.0 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 logging into ASM, you need to complete the basic configuration setup in the Initial Setup wizard. For more information about completing the initial setup, see the *Active System Manger Version 8.0 User's Guide*.

A

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 .iso that has been customized for use with ASM using ADK and build-razor-winpe.ps1 script. You will need to locate the appropriate drivers for your server hardware or virtual machines for the operating system you are trying to install. For Dell hardware, drivers can be obtained from support.dell.com. For other vendors such as VMware, follow the instructions from the manufacturer to locate the correct drivers. During .iso customization it will be updated to include the drivers required for VMware virtual machine VMXnet3 NICs, any other drivers specific to your hardware, and customizations for use with ASM. This will allow you to support operating system deployment through ASM of Windows 2008 R2, Windows 2012, or Windows 2012 R2 to virtual machines or bare-metal servers. For more information see, Creating WinPE Image and Updating Install Media for Windows 2008 R2, Windows 2012 and Windows 2012 R2
2. Create a Windows repository and copy Windows installation media (customized Windows .iso from step 1) on ASM appliance. **Ensure the build directory has space available for the working build files, as well as the final .iso file that is created. It is recommended to have enough space available for approximately three times the size of the .iso file.** For more information, see Adding OS Image Repositories

Creating WinPE Image and Updating Install Media for Windows 2008 R2, Windows 2012 and Windows 2012 R2

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.

To create customized Windows.iso image for Windows 2008 R2, Windows 2012 and Windows 2012 R2:

1. Create a build folder on your ADK machine. For example, ADK machine build directory may be “c:\buildpe”.
2. Within this build folder create a directory called “Drivers”.

NOTE:

- If any additional drivers are required, add the drivers under the “Drivers” folder in the build directory you created on your ADK machine. 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. To obtain the VMware Windows drivers: Install VMware tools on a running Windows 2012 or Windows 2012 R2 and on the virtual machine. Go to the C:\Program Files\Common Files\VMware\Drivers directory. Copy the contents in the Drivers folder to the directory that contains your WinPE build scripts.
- If you deploy Windows 2012 or 2012 R2 to an M420 server, drivers for Broadcom network adapters must be added to the image, as they are not included in Windows. 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 drivers on the files system and copy them to the “Drivers” folder. These drivers typically start with "b57".
- Native driver support for Dell server components in Windows 2008 R2 is limited, so obtain the latest NIC and RAID drivers for Windows 2008 R2 from Dell.com
- If you deploy Cisco servers, make sure to obtain appropriate device drivers for the operating system you are trying to deploy from Cisco.

3. Log in to the ASM virtual appliance and obtain the script “build-razor-winpe.ps1” from the /opt/razor-server/build-winpe directory and copy this to the build directory created in step 1 on your machine with ADK 8.0 or 8.1 installed in the default location.
4. Using a command line tool for PowerShell with administrator rights, go to the directory containing your build script, Drivers folder, and windows .iso image. This directory should contain these files only. To run the build script, run the command:

   ```
   powershell -executionpolicy bypass -file build-razor-winpe.ps1 [ASM appliance IP] [Your Windows .iso name] [New Windows .iso name]
   ```

   For example:

   ```
   powershell -executionpolicy bypass -noninteractive -file build-razor-winpe.ps1 192.168.0.1 Windows2012r2.iso ASMWindows2012r2.iso
   ```

   NOTE: This step takes some time to complete. After completion, it creates new Windows .iso file which is customized for use with ASM. This .iso will be copied to your ASM appliance.

   NOTE: If the build script fails or is stopped during execution it may be necessary to clean up files in the build directory before executing again. In some cases, directories may still be mounted and require cleanup. To clean up, delete all files other than the necessary script, starting .iso, and Drivers folder. If any files cannot be deleted, try executing the following commands from a command prompt in the build folder location:`C:\buildpe>dism /cleanup-wim`

Adding OS Image Repositories

You can add one or more OS image repositories in ASM GUI.

To add an OS image repository, perform the following tasks in the ASM GUI:

1. In the left pane, click **Settings > Repositories**.
2. On the **Repositories** page, click **OS Image Repositories** tab, and then click **Add**.
3. In the **Add OS Image Repository** dialog box, perform the following actions:

a. In the **Repository Name** box, enter the name of the repository.
b. In the **Image Type** box, enter the image type.
c. In the **Source File** or **Path Name** box, enter the path of the OS Image file name in a file share.
d. If using a CIFS share, enter the User Name and Password to access the share. These fields are only enabled when entering a CIFS share.

For more information about firmware repositories, see *ASM Online Help*.

B

Configuring DHCP or PXE on External Servers

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;
#  }
#}
```