Active System Manager Release 8.3 Installation Guide

Notes, Cautions, and Warnings

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

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.

2016 - 09

Rev. A01

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. 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 release 8.3.

What’s New in this Release

Active System Manager 8.3 is focused on expanding capabilities around workload deployment, adding new capabilities around managing existing environments, and improving the granularity of information shown around the current state of environments under management.

The highlights of Active System Manager release 8.3 include the following:

Support for Dell Hybrid Cloud for Virtualization that includes a new plug-in for compatibility with vRealize Orchestrator 7.0 and 7.1. Customers can create workflow that automates the deployment of ASM service templates created in ASM.

This release also includes compatibility support for the following:

- Support for SUSE Linux Enterprise Server 11 SP4 that enables Dell's SAP HANA Cloud Solution to leverage ASM's hardware compatibility list to offer ASM automation capabilities to customers.
- Support for PowerEdge R630, PowerEdge R730, PowerEdge R730XD hybrid and flash configurations, PowerEdge FC430, PowerEdge FC630, and PowerEdge FX2- All flash configurations. Customers can leverage ASM capabilities to discover, deploy and manage the VSAN ready nodes on Virtual SAN 6.2.

Accessing Online Help

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

Log in to the ASM user interface with the user name **admin** and then enter password **admin**, and press Enter.

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.

Also, 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

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

- *Active System Manager Release 8.3 User's Guide*
- *Active System Manager Release 8.3 Release Notes*
- *Active System Manager Release 8.3 Compatibility Matrix*
- *Active System Manager Release 8.2 SDK Reference Guide*
- *Active System Manager Integration for VMware vRealize Orchestrator user's Guide*
- *Active System Manager Release 8.3 API Reference Guide*

You can also see http://www.dell.com/asmtechcenter for how-to videos, white papers, blogs, and support forums.

www.dell.com/asmtechcenter

Contacting Dell Technical Support

To contact Dell Technical Support, make sure that the Active System Manager Service Tag is available.

- Go to the tech direct portal https://techdirect.dell.com
- Log in using your existing account or create an account if you do not have an account.
- Create a case for your incident.
- Add your Active System Manager service tag.
- Select **Active System Manager** as the Incident type.
- Type the relevant information in the Problem Details, and add attachments or screen shots if necessary.
- Fill in contact information and submit the request.

Licensing

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

ASM 8.3 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 receive an email from customer service with instructions for downloading ASM and your license.

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

1. Under the **License Management** section, on the **Virtual Appliance Management** page, click **Add**. The **License Management** window is displayed.
2. Click **Browse** beside **Upload License** and select an evaluation license file, and then click **Open**.

   The **License Management** window with the license type, number of resources, and expiration date of the uploaded license is displayed.
3. Click **Save** to apply the evaluation license.

4. After uploading the license file, the following information about the license is displayed:
    - License Type
    - Number of Resources
    - Number of Used Resources
    - Number of Available Resources
5. To replace the evaluation license with standard license, click **Add** under **License Management** section, click **Browse** beside **Upload License** and select a regular standard license file, and then click **Open**.

    You get information regarding license type, number of resources and expiration date of the uploaded license on License Management window.
6. Click **Save** to apply the standard license.

    It replaces the evaluation license with standard license.

After uploading the license file, the following information about the license is displayed:

- License Type
- Number of Resources
- Number of Used Resources
- Number of Available Resources

You can add multiple standard licenses. After uploading multiple licenses, all the licenses are aggregated together and displayed as one under **License Management** section.

NOTE: If you try to upload the same standard license second time, you get an error message stating that License has already been used.

Important Note

Engaging support requires that all pre-requisites 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 pre-requisites 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
7	Echo	TCP/UDP	Inbound/Outbound	IP address conflict resolution
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

Ports	Protocols	Port Type	Direction	Use
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 Pre-requisites

Before you begin the installation process:

- Gather the TCP/IP address information to assign to the virtual appliance.
- Ensure that the VMware vCenter server and VMware vSphere client are running, if you are deploying the ASM virtual appliance in a VMware vSphere environment.
- Deploying the ASM virtual appliance to a Microsoft Windows virtualization environment requires that the Hyper-V host on which ASM is 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) or the qcow2 file for KVM installation.
- Determine the host on which the ASM virtual appliance is 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 Manager

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

NOTE: All switches must have SSH connectivity enabled.

Deployment pre-requisites

Table 2. Deployment pre-requisites

Specification	Pre-requisite
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 OS Installation network in which the appliance is deployed. It is recommended to configure the virtual appliance directly on the OS Installation network, and not on the external network. • The virtual appliance is able to communicate with the hypervisor management network.

Specification	Pre-requisite
	• The DHCP server is fully functional with appropriate PXE settings to PXE boot images from ASM in your deployment network.
vCenter	Ensure that the **Virtual SAN Default Storage Policy** is set to the following default values: • Number of failures to tolerate: 0 • Number of disks stripes per disk: 1 • Force Provisioning: No • Object space reservation: 0% • Flash read cache reservation: 0.000% **NOTE: To view or update the storage policy, on the VMware vSphere Web Client, click Home → Policies and Profiles → VM Storage Policies → Virtual SAN Default Storage Policy.**
Brocade for Dell Compellent	Alias needs to be created having Dell Compellent fault domain WWPN accessible on Brocade switch. Create a single alias including the virtual ports for the Dell Compellent fault domain, WWPN accessible on Brocade switch. ASM automates the creation of each additional zone for the server objects and place them into a zone config. **NOTE: Ensure that the single alias is listed first in the list of aliases.**
Brocade for EMC VNX	Alias needs to be created having EMC VNX WWPN accessible on Brocade switch. Create a single alias in the Brocade switches including WWPN accessible on Brocade switch. ASM automates the creation of each additional zone for the server objects and place them into a zone config.
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 Fibre Channel which are listed as C: in boot order or PXE and iSCSI, which are listed as NICs in the boot order. ASM enables the supporting device connectivity and adjusts the boot order, but cannot enable or disable device names in the boot order. • Before performing Fibre Channel boot from SAN, a server must be configured with the QLogic Fibre Channel card, which is configured with the appropriate scan selection. To verify this in the BIOS and QLogic device settings, press F2 for System Set up, and then go to **Device Settings → <Target QLogic Fibre Channel adapter name> → Fibre Channel Target Configuration → Boot Scan**, and then select **First LUN**. The **First LUN** setting needs to be disabled for deployments other than Boot from SAN. **NOTE: For all servers prior to ASM discovery, make sure that the RAID controller is enabled.** After updating these devices setting, you should restart the server to ensure that Lifecycle Controller system inventory is updated. • Server facing ports must be configured for spanning tree portfast. • Ensure that the **Non-RAID Disk Mode** option is selected in the system BIOS to configure non-RAID disks. **NOTE: You can also set the non-RAID mode, by setting the RAID controller to the default settings.**
C-Series Server	• Network and BIOS configuration cannot be done using appliance. You need to do it manually. • Hard Disk should be available for server to install OS. • You need to set single NIC to PXE boot. This should be set as first boot device and hard disk should be set as second boot device.

Specification	Pre-requisite
	• Network must be configured on top-of-rack (ToR) switch which is connected to C-Series server. • Necessary VLAN must be configured on the service facing port of that top of rack switch. **NOTE: You need to place PXE VLAN-untagged for any kind of OS deployment. If it is Windows and Linux bare metal OS installation, you need to set workload network and you need to set Hypervisor management network for ESXi deployment.**
Cisco Servers	• Network and BIOS configuration cannot be done using appliance. You need to do it manually.
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 configured for spanning tree portfast. • If DCB settings are used, it must be properly configured on the switch for converged traffic. • Switches have SSH connectivity enabled. • Ensure that lacp ungroup is not set to vlt on your switches.
N-Series Switches	• The management IP address is configured for the switches. • ASM creates the virtual machine (VM) traffic VLANs dynamically. • You have access to the switches with passwords enabled. • Switches have SSH connectivity enabled. • Server facing ports must be in hybrid mode. • Server facing ports must be in switch port 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 PowerEdge M I/O Aggregator	If ASM is used to perform the initial configuration of credentials and IPs on the IOM in the blade chassis, you must to make sure, no enabled password is configured on the switches. **NOTE: ASM supports only standalone and PMUX mode.**
Dell Networking MXL 10/40GbE blade switch	• Any VLAN which is dynamically provisioned by ASM must exist on the switch. • Make sure that DCB settings are configured on each port. • If ASM is used to perform the initial configuration of credentials and IPs on the IOM in the blade chassis, you need to make sure, no enabled password is configured on the switches. • Switches have SSH connectivity enabled.
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 an SNMP community name set to "public".
Dell Compellent Storage Array	• The management IP address is configured for the Storage Array. • All storage array members are added to the group. • Virtual ports must be enabled on Dell Compellent.

Specification	Pre-requisite
	• Follow Dell Compellent best-practices for storage configuration. • Storage Centers needs to be added to the Enterprise Manager before initiating the Element Manager discovery in ASM. • Fault Domain and IP Address configuration of iSCSI controllers needs to be done before discovery Element Manager in ASM. • Discovery of EM needs to be done with same credentials which are used for add storage center in Element Manager. • Enable SNMP on Dell Compellent to enable ASM to monitor the device. For more information on creating alias, see **Brocade for Dell Compellent** section in this topic.
Dell Compellent iSCSI on MXL with Hyper V	• Enable LLDP and its corresponding attributes. • DCB (with no PFC option) on the participating interfaces (Server Facing and Port-Channel Members). Since DCB is globally enabled, the PFC should be turned off individually in those interfaces. • Link Level Flow control (LLFC) must be Rx ON and Tx OFF on the respective interfaces. • MTU must be set to 9216 on respective interfaces. **Sample server facing interface configuration** FTOSA1#show running-config interface tengigabitethernet 0/15 ! interface TenGigabitEthernet 0/15 no ip address mtu 9216 portmode hybrid switchport flowcontrol rx on tx off spanning-tree 0 portfast spanning-tree pvst edge-port dcb-map DCB_MAP_PFC_OFF ! protocol lldp advertise management-tlv management-address system-name dcbx port-role auto-downstream no shutdown **Sample port-channel member interface configuration** FTOSA1#show running-config interface tengigabitethernet 0/41 !

Specification	Pre-requisite
	interface TenGigabitEthernet 0/41 no ip address mtu 9216 dcb-map DCB_MAP_PFC_OFF ! port-channel-protocol LACP port-channel 1 mode active ! protocol lldp advertise management-tlv management-address system-name no advertise dcbx-tlv ets-reco dcbx port-role auto-upstream no shutdown FTOSA1#
VMware vCenter 5.1, 5.5 or 6.0	• VMware vCenter 5.1, 5.5 or 6.0 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.
OS Installation	• 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.
Dell PowerEdge M1000e chassis	**NOTE: Prior to deployment of M1000e server, you need to disable FlexAddress every server in the chassis.** To disable FlexAddress, follow the path:**CMC** > **Server Overview** > **Setup** > **FlexAddress**. You need to turn off server to disable FlexAddress. This should be done prior discovering the server. This setting applies to the chassis and the servers in the chassis, not to the IOM switches such as MXL or IOA.
Dell PowerEdge FX2 chassis	**NOTE: Prior to deployment of FX2 server, you need to disable FlexAddress every server in the chassis.** To disable FlexAddress, follow the path: **CMC** > **Server Overview** > **Setup** > **FlexAddress**. You need to turn off server to disable FlexAddress. This should be done prior discovering the server. This setting applies to the chassis and the servers in the chassis, not to the IOM switches such as MXL or IOA.

Specification	Pre-requisite
EMC storage	- VNX alias must be created in the Brocade switches. For more information on creating alias, see **Brocade for EMC VNX** section in this topic. **NOTE: Select the Thin LUN option only to create thin volumes.**

Pre-requisites for System Center Virtual Machine Manager (SCVMM)

ASM manages resource on Microsoft System Center Virtual Machine Manager through Windows Remote Management (WinRM). Windows RM must be enabled on the SCVMM server and 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 tear 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 Hyper-V 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 the Microsoft knowledge base article 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 that 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 on VMware vSphere

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 is displayed.
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 is stored. Click **Next** to continue.
7. Depending on the vCenter configuration, one of the following options are displayed:
   - **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 preallocate 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.

NOTE: When deploying Virtual Machines to an existing vCenter cluster using an ASM template, make sure that all OS Installation or Public or Private LAN networks (which are used on the Virtual Machine) are defined as Networks in ASM. The name parameter of the Networks in ASM should match with the name of the port groups on the ESXi hosts.

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-8.3-.vhd

    d. Under the **Select library server and destination for imported resources** section, click **Browse**. Select the destination folder in which ASM install VHD is located (for example, My_SCVMM -> MSCVMMLibrary -> VHDs), and then click **OK**.

    e. Click **Import**.
3. To deploy ASM virtual appliance:

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

    b. Click **Create Virtual Machine**.

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

    d. From the list of sources, select VHD -> Dell-ActiveSystemManager-8.3- <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 **4**, and then in the **Memory** section, change the memory value to 16 GB.

            NOTE: The number of "big" processes that can be executed in parallel by default is set to the number of processors assigned to a VM. For example, if you give your appliance 8 processors, it executes eight processes at once instead of the default 4 processes.
        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 necessary.

    k. On the **Select networks** page, select your OS Installation 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 **Create**.

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**.

Rectifying mounting errors during Hyper–V deployment

For Hyper-V Cluster deployment, if the cluster configuration fails to mount the disk and create the cluster storage volume:

Error 01

SCVMM reports DNS error during mounting of the available storage on SCVMM cluster. This is due to intermittent network failure during the mounting operation.

Resolution

Retry the deployment, so that ASM can retry to mount the volumes.

Error 02

SCVMM reports DNS error during mounting of the available storage on SCVMM cluster. Trying to reuse an existing volume used in another Hyper-V cluster.

Resolution

Hyper-V or SCVMM does not allow mounting a volume which is used in another cluster (Active / Inactive). ASM does not format already formatted volume to avoid any data loss.

In case an existing volume is used for cluster configuration, ASM fails the cluster deployment to avoid the data loss. To configure the volume to be used in this cluster, do the following:

This volume needs to be formatted manually from one of the servers that needs to be added to the cluster.

1. RDP to the Server using local administrator account.
2. Select **Server Manager → Tools → Computer Management → Disk Management**.
3. Select the volume that is failing
4. Select **Online → Initialize disk (Partition Style MBR)**.
5. Create Simple Volume. Ensure to clear the drive letter.

6. On SCVMM, refresh the host and the cluster
7. Retry the deployment from ASM.

Deploying the ASM appliance as Kernel-based Virtual Machine (KVM)

Before you begin deploying the ASM appliance as KVM, ensure that you have the following minimum connection requirements for the hypervisor:

- An ethernet interface that uses a static IP to connect to the operating system.
- An ethernet interface that is bound to the bridge device.

1. Extract the .zip file and copy the qcow2 file to /var/lib/libvirt/images/ on your Linux KVM hypervisor.
2. Run the following command:

   ```
   virt-install -n [vm name]--ram [size]--connect qemu:///system --network bridge=[name of
   network bridge interface]--os-type linux --os-variant rhel6 --disk /dev/
   sda,path=/var/lib/libvirt/images/[qcow2 file name],device=disk,format=qcow2,bus=scsi --
   vcpus [number of vcpus]--noautoconsole--import --graphics vnc, listen=0.0.0.0
   ```
3. To view the port the VNC console session is listening on, run the following command:

   ```
   virsh vncdisplay [vm name]
   ```

   For more information on accessing the appliance console using a VNC application, see Configuring ASM Virtual Appliance.

   NOTE: To destroy the virtual machine, run the following command:

   ```
   virsh destroy [vm name]
   ```

   NOTE: To remove the virtual machine from the list, run the following command:

   ```
   virsh undefine [vm name]
   ```

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

Changing Dell Administrator Password

To change the Dell administrator default password:

1. In VMware Sphere, click the **Console** tab to open the console of the virtual appliance.
2. Log in to the console with the default user name *delladmin* and password *delladmin* and press Enter.
3. Click **I Agree** for EULA.
4. On the **Initial Appliance Configuration** user interface, click **Change Admin Password**.
5. Enter the Current Password, New Password, Confirm New Password, and click **Change Password**.

Accessing the Initial Appliance Configuration

To access the Initial Appliance Configuration after the first run:

1. In VMware Sphere, click the Console tab to open the console of the virtual appliance or use the SSH protocol to connect to ASM virtual appliance IP (ssh needs to be enabled on the appliance).
2. Log in to the console with the default user name *delladmin* and password and press **Enter**.
3. Enter the command **asm_init_shell** at the command prompt.

   NOTE: If you use the ASM 8.3 User interface, to log in you need to use the username as *admin* with the default password as *admin*.

Configuring Static IP Address in the Virtual Appliance

1. In VMware Sphere, click the **Console** tab to open the console of the virtual appliance or use the SSH protocol to connect to ASM virtual appliance IP (ssh needs to be enabled on the appliance).
2. Log in to the console with the user name *delladmin*, enter current password, and then press **Enter**.

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

3. At the command line interface, run the command **asm_init_shell**.
4. In the Appliance Configuration 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.

Configuring Virtual Appliance with Two NICS

If the OS Installation network is not routed, you must add an extra vNIC to the ASM appliance to make it communicate and respond to TFTP requests on the OS Installation network.

1. In VMware vSphere, select the Virtual Appliance and select “Power Off”.
2. Select Virtual Appliance and select “Edit Settings”.
3. Select “Add” in the properties page and choose “Ethernet Adapter”. Select Adapter Type as “VMXNET3”.
4. Select the PXE port group name that needs to be associated with the new network.
5. Select “Next” and then “OK” to ensure that the settings are updated on the Virtual Appliance.
6. Assign static IP address on the new network using the steps provided in section “Configuring Static IP Address in the Virtual Appliance”.

Configuring ASM Virtual Appliance as PXE Boot Responder

ASM may be configured to act as the DHCP server and PXE responder on an OS Installation 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 OS Installation network, follow the instructions in the section Configuring DHCP or PXE on External Servers.

NOTE: Ensure that your DHCP scope has enough IP addresses. The installation process can temporarily consume between 4-8 IPs during the initial PXE boot process. This is based on interface card configuration and the number of physical interfaces on the server. These IPs only used temporarily during server configuration and installation.

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 and in Red Hat Enterprise Linux. For ASM virtual machine or virtual machine template cloning, the virtual machine or virtual machine templates must be customized to make sure that 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 depend on virtual machine which is needed to be cloned.

While cloning a virtual machine running Red Hat Enterprise Linux, you must ensure the following:

- On base virtual machines with one NIC:
  - Network adapter — Network Adapter 1 is added to the virtual machine.
  - Device ID is set to default. For example, eno16780032.
- On base virtual machines with two NICs:
  - Network adapters — Network Adapter 1 and Network Adapter 2 are added to the virtual machine.
  - Device ID is set to default. For example, eno16780032 and eno33559296.
- The network device files present in the **/etc/sysconfig/network-scripts/ifcfg-<device id>** directory contain the correct device ID information.
- MAC address information is not present in the device ID files in the base virtual machine.

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 data center. For SCVMM the virtual machine templates must exist in the SCVMM library. Cloning virtual machines directly is not currently supported for Hyper-V.

NOTE: Before cloning VMware and Hyper-V VMs, ensure that the virtual machine used for cloning is defined with a DHCP configuration in the operating system.

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 mounts the media for VMware tools.

- Log in to the operating system of the virtual machine and run the VMware tools installer within the OS running on the virtual machine. For more information on installing VMware tools, see VMware documentation.

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

Customizing Linux Template

Perform the following task to customize Linux template:

1. Ensure that 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 that it is configured to run on startup
   c. Make sure that ASM appliance and virtual machine time are synchronized by NTP.
   d. Make sure that 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 following command needs to be run from the /var/lib/razor/repo-store directory or will fail.

      ```
      sudo find win2012 -print0 | sudo xargs -0 chown razor:razor
      ```

      NOTE: The version of the INI file in puppet certificate script should be specified as 2.0.2. To verify this, open the puppet_certname.sh file and check that the INI file version is specified as 2.0.2 or not.
   b. On a Linux virtual machine, you must copy these scripts to /usr/local/bin. Make sure that 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 that the virtual machine has access to the Internet, as this is required to download and install the necessary ruby gem files. Download the required gem files from https://rubygems.org/ and move the gem files to the appropriate place on the host you are preparing. 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.

   NOTE: The `puppet_certname.sh` script that runs on startup of the VM clone attempts to install the ruby “inifile” and “hashie” gems from the Internet. If there is no internet connection, it generates error messages to communicate with rubygems.org.
4. It would be less error-prone to require the user to install the gems in the source VM rather than having them installed when the clone VM starts up. To do this, you need to:
   - Remove the gem install lines from `puppet_certname.sh`.
   - Manually run the gem installs either with the instructions on how to set a proxy or how to install the gems by downloading them directly.
5. 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
   ```

   RHEL 7

   Remove MAC Address from the interface configuration file. For example,

   ```
   sed -i "/^HWADDR/d" /etc/sysconfig/network-scripts/ifcfg-ens192
   ```

   NOTE: While setting up the base clone virtual machine, ensure that:
   - The eth0 interface is available on the virtual machine and configured for DHCP.
   - You remove any persistent hardware information by using only the eth0 interface.
   - You convert the virtual machine to use eth0 as the network interface manually. This is important because virtual machines deployed using ASM may use eth1 as their network interface.

NOTE: Interface naming on RHEL 7 VM depends on the various factors provided at https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/ch-Consistent_Network_Device_Naming.html#sec-Naming_Schemes_Hierarchy

Debian/Ubuntu:

```
rm /lib/udev/rules.d/75-persistent-net-generator.rules
```

6. 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
      ```

      RHEL 7

      ```
      @reboot /usr/local/bin/puppet_certname.sh
      ```

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

      ```
      crontab -l
      ```

7. 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, do the following:

   - 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.
   - Delete the ssl directory located at /var/lib/puppet/ssl for Linux VMs and C:\ProgramData\PuppetLabs\puppet\etc\ssl for Windows VM.
   - Remove the certname entry from puppet_conf file.

Customizing Windows Template

Perform the following task to customize Windows 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 version of the INI file in puppet certificate script should be specified as 2.0.2. To verify this, open the puppet_certname.sh file and check that the INI file version is specified as 2.0.2 or not.

   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. Download the required gem files from https://rubygems.org/ and move the gem files to the appropriate place on the host you are preparing. 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 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, turn 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, do the following:

    - 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.
    - Delete the ssl directory located at /var/lib/puppet/ssl for Linux VMs and C:\ProgramData\PuppetLabs\puppet\etc\ssl for Windows VM.
    - Remove the certname entry from puppet_conf file.

    NOTE: Ensure that the VM template is not created using the Microsoft System Preparation Tool (sysprep) to avoid any failure during unattended operating system installation.

Preparing a vCenter Image for Cloning

The following topic covers the steps that you must follow to prepare a vCenter guest operating system to clone and create templates in vCenter using ASM. After you have prepared the image, you can select the template to quickly deploy the VMware template on target clusters in your infrastructure.

Pre-Requisites

Before you begin creating the image, ensure that you have:

- A vCenter system with a guest operating system — Microsoft Windows
- Internet access to download ruby gems from **https://rubygems.org.**
- Knowledge of Windows Task Scheduler
- Access to the ASM Virtual appliance using CIFS or NFS
- Network access from the targeted cluster to ASM appliance

Customizing the vCenter Windows Template

NOTE: Ensure that you have met the pre-requisites before you begin customizing the template.

1. Install the VMware tools on the guest operating system.
2. Install the puppet agent and ensure that you configure the puppet agent to run at startup.
    - You can install the puppet agent by accessing the agent on the ASM appliance using the CIFS connection on the guest operating system or at the following path in the local system \\dellasm\razor.
    - Move the puppet agent directory to a default location on the system with the guest operating system.

    NOTE: It is recommended that you install the puppet agent version 3.6.2.
3. Run the agent 3.2.1 msi file on the system with the guest operating system. Perform this step using an administrator access.
4. Ensure that the ASM appliance and virtual machine time are synchronized using the Network Time Protocol (NTP).

5. Ensure that DNS is configured for **dellasm** to resolve. Creating an entry in DNS with forward and lookup pointers enables you to pull and resource your ASM appliance instance.
6. Ensure that the file on the system with the guest operating **puppet.conf** system is updated to include dellasm as the server for each of the entries.
7. Open the **puppet.conf** file in a text editor with administrator privileges and include the following:

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

   NOTE: The puppet.conf file is available at the following location on the system with the guest operating system that you preparing: C:\ProgramData\PuppetLabs\puppet\etc.

8. Update the etc host file on the system with the guest operating system to ensure that the guest operating system is able to resolve dellasm.

   NOTE: The etc file is at C:\Window\System32\drivers\etc.

   To edit the etc host file, perform the following steps:

   a. Open Notepad using the Start menu.
   b. Right-click and click **Run as administrator**.
   c. Click **File** → **Open**.
   d. Navigate to the location of the etc host file and open the file.
   e. Add the following to the host file: `<Your ASM IP> dellASM # Dell ASM Virtual Appliance`

9. Navigate to the **/opt/asm-deployer/scripts** folder on your ASM appliance and move the following files or scripts to **/var/lib/razor/repo-store** location on the system with the guest operating system:
   - **Puppet_certname.bat**
   - **Puppet_certname.rb**

   NOTE: On a systems running Windows operating system, you can access these files using ssh or WinSCP client.

   You can also use the following command to move the files: `$sudo mv puppet_certname.bat puppet_certname.rb /var/lib/razor/repo-store`

   This command moves the files to the \\dellasm\razor folder. You can access the files using CIFS from the system with the guest operating system.

10. Move the files to the C: drive on the system with your guest operating system.
11. Download the latest version of the following files from **https://rubygems.org** to the C: drive on your guest operating system.
    - hashie
    - inifile

Setting up the Windows Task Scheduler

This topic provides information on setting up the Windows task scheduler to run a script that generates a unique certificate for the system with the guest operating system and run the puppet agent.

Perform the following steps to set up the Windows Task Scheduler:

1. Click **Start** → **Control Panel** → **Administrative Tools** → **Task Scheduler**.

   The **Task Scheduler** window is displayed.
2. Right-click **Puppet CertName** and click **Create New Task**.

   The **Puppet CertName** properties window is displayed.
3. Update the following on the **General** tab:
   - Type the Name in the **Name** field.

- Select the **Run whether user is logged on or not** option.
- Select the **Run with highest privileges** option.
- Type the operating system name in the **Configure for** field.

  NOTE: Ensure that the operating system you select aligns with the guest operating system you are preparing.

4. Click **OK**.
5. Click **Triggers.**
6. On the **Triggers** page, select **At startup** and click **Edit**.
7. On the **Edit Trigger** window, update the following:
   - Select **At startup** from the **Begin the task:** drop-down menu.
   - Select **Enabled** under **Advanced Settings** section.
8. Click **OK**.
9. Click **Actions**.
10. On the **Actions** page, click **New**.
11. Select **Start a program** from the **Action:** drop-down menu.
12. Click **Browse** navigate to C: drive and select the **puppet_certname.bat** script.
13. Click **OK**.
14. Click **Conditions**.
15. Ensure that following options under the **Power** section are selected:
    - **Start the task only if the computer is on AC power**
    - **Stop if the computer switches to battery power**
16. Click **OK**.
17. Click **Settings**.
18. Ensure that the following options are selected:
    - **Allow task to be run on demand**
    - **Stop the task if it runs longer than:**
    - **If the running task does not end when requested, force it to stop**
    - **Stop is the existing instance** is selected **If the task is already running, then the following rule applies:** drop-down menu.
19. Click **OK**.
20. Click **OK** to complete the set up.

    After completing all the tasks, you can create a template in vCenter with guest operating system and utilize the template as a clone.

    Click **Run Inventory** in ASM on the vCenter instance to ensure that up-to-date information is available in ASM.

    After you deploy the template, you can test the guest operating system by running the following command:

    ```
    >puppet agent -t
    ```

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 that 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 Release 8.3 User's Guide*.
- Configure the NetApp Storage Component. For more information, see Configuring the NetApp Storage Component.
- Configure the fileshare Network on the server component. For More information, see *Active System Manager Release 8.3 User's Guide*.

Adding NetApp Ruby SDK to ASM Virtual Appliance

NetApp Manageability SDK files are available to download directly from NetApp. You need a **NetApp NOW** account to download the SDK. These files are DfmErrno.rb, NaElement.rb, NaErrno.rb, and NaServer.rb

The NaServer.patch file is available on the ASM appliance at location /etc/puppetlabs/puppet/modules/netapp/files/NaServer.patch You will need the above files to proceed further. Contact your administrator for any additional patch files, or updates.

1. Log in to the ASM Appliance.
2. Download and copy the NetApp SDK Ruby lib files to the ASM Appliance /tmp/*.
3. Copy these Ruby libs files from /tmp to /etc/puppetlabs/puppet/modules/netapp/lib/puppet/util/network_device/netapp

   ```
   # sudo cp /tmp/*.rb /etc/puppetlabs/puppet/modules/netapp/lib/puppet/util/network_device/netapp
   ```
4. Copy any patch file(s) to the ASM Appliance /tmp directory, currently there is NaServer.patch

   ```
   # sudo cp /etc/puppetlabs/puppet/modules/netapp/files/NaServer.patch /tmp
   ```
5. Apply the patch(es) to update the NetApp SDK Ruby files.

   ```
   # sudo patch /etc/puppetlabs/puppet/modules/netapp/lib/puppet/util/network_device/netapp/NaServer.rb </tmp/NaServer.patch
   ```
6. 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/*
   ```
7. 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/*
   ```

Enabling 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 Release 8.3 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

Installing Plug-ins for EMC to Support Volume Provisioning

To support volume provisioning on a EMC VNX 5300 and VNX 5400 storage array, ensure that you install the plug-ins on a storage array.

To install the Software Enabler feature:

1. Start **Unisphere Service Manager** (USM).
2. Log in to the storage array.
3. Copy the enabler (.ena file) to the c:\emc\repository\Downloads\VNX folder on the windows host where you installed USM. Create the folder in case the folder does not exist. The file is available on the disks that shipped with your storage array.
4. In the **System** window, click **Software** → **System Software** → **Prepare for Installation**.
5. Click **Software** → **System Software** → **Install Software** to proceed with the installation.
6. Select **Install VNX OE** for block and/or enablers option and follow the instructions on the screen.

   The controllers reboot after the feature is installed. This process may take up to 45 minutes for each Service Processor (SP).
7. When the installation is complete, click **Finish**.

Perform the following steps to verify if the feature is installed:

1. Log in to EMC Unisphere.
2. Click **All System** → **System List**.
3. Right-click the storage array and select **Properties**.
4. Click the **Software** tab.

   A list of enabled features is displayed.

   NOTE: Ensure that Thin Provisioning is listed under Packages. If not, follow the steps to add the feature.

7

Completing Initial Configuration

Log in to ASM using the appliance IP address, After logging in to ASM, you need to complete the basic configuration setup in the Initial Setup wizard. After that you get four other wizards that allow you to define Networks, discover resources, configure resources, and publish template. For more information, see the *Active System Manager Release 8.3 User's Guide*.

NOTE: If you use the ASM 8.3 User interface, to log in you need to use the username as `admin` with the default password as `admin`.

Installing Windows ADK 8.1 for OS Prep for Windows

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

NOTE: You should use Microsoft ADK 8.1 installed in the default location. Make sure to install all options during ADK installation process.

1. Create a Windows .iso that has been customized for use with ASM using ADK and build-razor-winpe.ps1 script. You 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 is 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 allows 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 that the build directory has space available for the working build files, and 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

   NOTE: Approximately four times the .iso size space (approximately 25 GB) is required to perform .iso processing on the ADK machine.

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 to 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 or QLogic 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.

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 8.3 or 8.3 installed in the default location.
4. The build-razor-winpe script supports an ASM appliance that uses an external DHCP/PXE server, or using the ASM appliance as your DHCP PXE server. This command to run this script has the following structure:

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

If ASM does not act as the DHCP/PXE server, that is your DHCP/PXE server is external, you run the script and provide the ASM appliance IP as input.

For example,

```
powershell -executionpolicy bypass -file build-razor-winpe.ps1
192.168.2Windows2012r2.iso ASMWindows2012r2.iso
```

If ASM acts as the DHCP/PXE server you run the script and provide the input “DHCP” instead of the ASM appliance IP.

For example:

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

NOTE: This step takes some time to complete. After completion, it creates a Windows .iso file which is customized for using with ASM. You must go to repositories and upload .iso file.

NOTE: If the build script fails or is stopped during execution, it may be necessary to clean up files in the build directory before running again. Sometimes, 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 running 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. On the home page, 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, type the name of the repository.

   b. From the **Image Type** drop-down menu, select the appropriate image type.

c. In the **Source File** or **Path Name** box, type the path of the OS Image file name in a file share.

d. If using a CIFS share, type 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

NOTE: Ensure that your DHCP scope has enough IP addresses. The installation process can temporarily consume between 4-8 IPs during the initial PXE boot process. This is based on interface card configuration and the number of physical interfaces on the server. These IPs only used temporarily during server configuration and installation.

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

Creating 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, type the following information and click **OK** to create a user class.
    a. In the **Display Name** box, type *iPXE*.

       NOTE: The binary for the output of the ASCII “iPXE” is (69 50 58 45).

    b. In the **Description** box, enter *iPXE Clients*.
    c. In the data pane, under **ASCII**, enter *iPXE*.
5. Click **Close**.

Creating the DHCP Policy

1. Open the Windows 2012 DHCP Server DHCP Manager.
2. In the console tree, expand the scope that services your ASM OS Installation 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**.

Creating the Boot File Scope Option

1. Open the Windows 2012 DHCP Server DHCP Manager.
2. In the console tree, expand the scope that services your ASM OS Installation 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 OS Installation network)
   - **006 Name Server** (DNS server IP address)

Configuring 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

Creating 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 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*.

   NOTE: The binary for the output of the ASCII “iPXE” is (69 50 58 45).

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

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

Creating 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 services ASM PXE environment.
3. In the **Scope Options** dialog box, click the **Advanced** tab, select the **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.

Creating 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 services 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. Also, in the right pane, based on your 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 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 OS Installation network.
- **filename "bootstrap.ipxe"**

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

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 information, 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 enables / 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;
#  }
#}
```