# AOS-W 8.7.0.0 Virtual Appliance



#### **Copyright Information**

© Copyright 2020 Hewlett Packard Enterprise Development LP.

#### **Open Source Code**

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company 6280 America Center Drive San Jose, CA 95002 USA

#### **Copyright Information**

Alcatel-Lucent and the Alcatel-Lucent Enterprise logo are trademarks of Alcatel-Lucent. To view other trademarks used by affiliated companies of ALE Holding, visit:

#### https://www.al-enterprise.com/en/legal/trademarks-copyright

All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. (2020)

#### **Open Source Code**

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses.

Contents	
Revision History	
About this Guide	
Important	
Conventions	
Contacting Support	
Alcatel-Lucent Mobility Master Virtual Appliance	
What's New	
AOS-W VM Requirements	10
Installing AOS-W Using vSphere Hypervisor	13
Logging Into ESXi Host Using vSphere Client	
Creating A VM Network For Management	
Creating VM Networks For Traffic	
Deploying the OVF Template	
Pre-Allocating Memory	
Assigning Network Connections	
Enabling Security Profile Configuration	
Configuring Serial Console for the VM	
Installing AOS-W Using vSphere Hypervisor ESXi 6.5	
Overview of Procedures	
Logging Into ESXi Host Using vSphere Hypervisor 6.5	25
Creating VM Networks	
Enabling Security Profile Configuration	
Configuring Serial Console for the VM	
Installing AOS-W Using vSphere Hypervisor	
Installing AOS-W OVA Using vCenter	29
Adding a Serial Port	
Installing AOS-W ISO Using vCenter	
Create a New VM	
Installing the ISO on the VM	35
Installing AOS-W Using KVM Hypervisor	
Prerequisites	
Configuring the Virtual Network Computing Server	41
Creating a VM and Installing AOS-W	
Enabling Serial Console Over Telnet	
Installing AOS-W Using Windows Hyper-V	52
Prerequisites	52
Installing AOS-W on Windows Server Hyper-V	
Configuring the New VM	

Creating a Network Adapter	
Configuring Trunk Ports	5/
Post-Installation Procedures	58
Configuring the Initial Setup	
Management Interface	
Troubleshooting	61
Connectivity Issues	61
DHCP Address	61
ARP Issues	
MAC Address Collision in a Network	
Characters Repeating In Remote Console	
Networks Cards Not Detected	
HP Proliant DL580 Running ESXi 5.5 Is Not Powered On Due To Memory Leaks	62
Network Interfaces Are Not In The Correct Order	
Connectivity Issues Observed When Using Multiple vSwitches	62
Appendix	1
Recommendations for NIC Teaming on a vSwitch	1
Configuring ReversePathFwdCheckPromisc	
Creating a Distributed vSwitch Using vCenter with LACP Configuration	7
Increasing the Flash Size on a vSphere Hypervisor	15
Backing up and Restoring Critical Data	18
Implementing Management Interface	20
Datapath Debug Commands	
Upgrading a Switch	
Gracefully Shutting Down AOS-W VMs	
Jumbo Frame Support	26

### **Revision History**

The following table lists the revisions of this document.

#### Table 1: Revision History

Revision	Change Description
Revision 01	Initial release.

# Chapter 1 About this Guide

This guide describes the steps to install, configure, and deploy the Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance on:

- vSphere Hypervisor
- Kernel-Based Virtual Machine (KVM) Hypervisor
- Windows Hyper-V

The steps to deploy a Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance as a standby Switch or managed device are the same.

For information related to licensing, refer to the *Alcatel-Lucent Mobility Master Licensing Guide*.

### Important

The following sections of the guide have references to configuration changes that need to be made when installing a Mobility Controller Virtual Appliance or Mobility Master Virtual Appliance:

- AOS-W VM Requirements
- Assigning Network Connections

### Conventions

The following conventions are used throughout this document to emphasize important concepts:

Table 2: Typographical Conventions	
------------------------------------	--

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
System items	<ul> <li>This fixed-width font depicts the following:</li> <li>Sample screen output</li> <li>System prompts</li> <li>Filenames, software devices, and specific commands when mentioned in the text</li> </ul>
Commands	In the command examples, this bold font depicts text that you must type exactly as shown.
<arguments></arguments>	In the command examples, italicized text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: # send <text message=""> In this example, you would type "send" at the system prompt exactly as shown, followed by the text of the message you wish to send. Do not type the angle brackets.</text>
[Optional]	Command examples enclosed in brackets are optional. Do not type the brackets.



OTE

NOTE

Type Style	Description
{Item A   Item B}	In the command examples, items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.

#### The following informational icons are used throughout this guide:



Indicates helpful suggestions, pertinent information, and important things to remember.



Indicates a risk of damage to your hardware or loss of data.



Indicates a risk of personal injury or death.

### **Contacting Support**

 Table 3: Contact Information

Contact Center Online	
Main Site	https://www.al-enterprise.com
Support Site	https://businessportal2.alcatel-lucent.com
Email	ebg_global_supportcenter@al-enterprise.com
Service & Support Contact C	Center Telephone
North America	1-800-995-2696
Latin America	1-877-919-9526
EMEA	+800 00200100 (Toll Free) or +1(650)385-2193
Asia Pacific	+65 6240 8484
Worldwide	1-818-878-4507

The Alcatel-Lucent Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance provide a 64bit virtualized software-based managed platform on virtual machine (VM) architecture. The Alcatel-Lucent Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance operate on x86 platforms in a hypervisor environment and can reside with other virtualized appliances. The Alcatel-Lucent Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance are centralized management platforms for deployment in a virtualized network infrastructure. Some of the key security features offered by the Alcatel-Lucent Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance are:

- Authentication
- Encryption Support
- Security Policy
- Rogue Detection and Suppression
- Security Firewall

Listed below are few advantages of switching to Alcatel-Lucent Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance environment:

- Reduces the number of devices occupying rack space and the overheads associated with managing and servicing products from different vendors.
- Multiple services are consolidated on a common platform, thereby reducing the cost and optimizing the infrastructure by providing consolidated services.
- Additional devices can be deployed remotely, increasing hardware selection option and flexibility.
- By eliminating a single point failure, you can create a reliable and high-performance networking system.

On successfully installing the Alcatel-Lucent Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance, refer to the *AOS-W 8.6.0.0 Getting Started Guide* for steps to setup the network.



Ensure the number of CPU sockets is always 1 and the value of the cores is the same as the required CPUs.

Storage vMotion is not supported in the Alcatel-Lucent Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance environment.

### What's New

This section lists the new features and enhancements released in this version of the installation guide.

### **AOS-W VM Requirements**

Listed below are the minimum resources required for AOS-W VM to function:



If the prescribed vCPU and Memory values are not configured during the initial setup the following error message is displayed "**Minimum 4GB memory (actual 3GB) or minimum 3 CPU (actual 2 CPU) requirement not met**"



For the Alcatel-Lucent Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance to function as expected on a VMware ESXi server with NIC teaming, LACP should be configured and enabled between the VMware ESXi host and upstream switch.

SKUs	Total vCPU (hyper threaded)	Memory (GB)	Flash/Disk (GB)	Total Supported Interfaces
MM-VA- 50	3	6	6	2 data ports (0/0/0, 0/0/1), 1 mgmt port
MM-VA- 500	6	8	8	2 data ports (0/0/0, 0/0/1), 1 mgmt port
MM-VA- 1K	8	32	32	2 data ports (0/0/0, 0/0/1), 1 mgmt port
MM-VA- 5K	10	64	64	2 data ports (0/0/0, 0/0/1), 1 mgmt port
MM-VA- 10K	16	128	128	2 data ports (0/0/0, 0/0/1), 1 mgmt port

Table 4: Memory and CPU Allocation	- Mobility Master	Virtual Appliance
------------------------------------	-------------------	-------------------

**NOTE:** Alcatel-Lucent recommends using Intel Xeon E5-2650 v4 @ 2.2GHz enterprise grade CPUs for optimum performance.



If your deployment is using a MM-VA 50 SKU and the topology is configured for Layer-2 redundancy, note that the standby Mobility Master will be counted as one Mobility Controller against the capacity and license count.

#### **Table 5:** Memory and CPU Allocation - Mobility Controller Virtual Appliance

SKUs	Total vCPU (hyper threaded)	Memory (GB)	Flash/Disk (GB)	Total Supported Interfaces
MC-VA- 10	3	4	6	3 data ports (0/0/0, 0/0/1, 0/0/2), 1 mgmt port
MC-VA- 50	4	6	6	3 data ports (0/0/0, 0/0/1, 0/0/2), 1 mgmt port
MC-VA- 250	5	8	8	3 data ports (0/0/0, 0/0/1, 0/0/2), 1 mgmt port
MC-VA- 1K	6	16	16	3 data ports (0/0/0, 0/0/1, 0/0/2), 1 mgmt port
MC-VA- 4K	12	48	48	3 data ports (0/0/0, 0/0/1, 0/0/2), 1 mgmt port
MC-VA- 6K	14	64	64	3 data ports (0/0/0, 0/0/1, 0/0/2), 1 mgmt port

**NOTE:** Alcatel-Lucent recommends using Intel Xeon E5-2670 v3 @ 2.3GHz enterprise grade CPUs for optimum performance.



MC-VA-4K and MC-VA-6K are not orderable SKUs. However, you can scale up by installing multiple instances of MC-VA-1K. For example to deploy 4K APs on a single Mobility Controller Virtual Appliance, you need to add four MC-VA-1K licenses.

The hypervisor host should not be oversubscribed in terms of number of VMs configured on a host as it adversely impacts the functionality and performance of AOS-W. In instances where more than one VM is setup in a hypervisor, then:

- The number of logical processors reported on the hypervisor should be higher or equal to the sum of vCPUs allocated to each VM setup in that host.
- The sum of the memory allocated to each VM should not exceed the overall host memory capacity reported.
- The total CPU utilization, memory usage, and network throughput should not exceed 80% of the host capacity.



Ensure the number of sockets and threads is always one and the value of cores is the same as the current allocation.

Ensure that the following prerequisites are addressed before starting the installation:

- vSphere Hypervisor 5.1, 5.5, 6.0, 6.5, or 6.7 is installed on the server that hosts the Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance as a guest.
- vSphere Client/vCenter is installed on a Windows machine.
- OVF/ISO template is obtained from an Alcatel-Lucent representative and accessible from vSphere Client/vCenter.

# Logging Into ESXi Host Using vSphere Client

Follow the steps to log in to the vSphere ESXi Host:

- 1. Open the vSphere Client.
- 2. Enter the IP address or name of the vSphere Hypervisor in the IP address / Name field.
- 3. Enter the user name in the **User name** field.
- 4. Enter the password in the **Password** field.
- 5. Click Login.

The **vSphere Client** page is displayed.

### **Creating A VM Network For Management**

Follow the steps below to create a VM network for management:

1. Log in to the vSphere ESXi Host using vSphere Client. For additional information, see <u>Logging Into ESXi</u> <u>Host Using vSphere Client</u>.

- 2. From the vSphere Client page, click **Inventory**.
- 3. Click **Configuration** tab.
- 4. Click **Networking** from the **Hardware** menu.
- 5. Click Add Networking.

The Add Network Wizard is displayed.

#### Figure 1 Adding A Network

loca	lhost.localdomain VMware ESXi, 5.5	.0, 2068190				
Ge	ting Started Summary Virtual Mach	ines Resource Allocation Performance Configu	ration Local Users & Groups Events Permissions			
Ha	rdware	View: vSphere Standard Switch				la u
	Health Status Processors Memory	Networking Standard Switch: vSwitch0	Remove Properties	Refresh	Add Networking	Properties
ŀ	Storage Networking Storage Adapters Network Adapters Advanced Settings Power Management		ical Adapters			

- 6. Select the Virtual Machine radio button and click Next.
- 7. Select the **vSwitch** that has **VMkernel** port mapped for ESXi management network and click **Next**.



Intel Corporation I350 Gigabit Network Connection         Image: Within the port Group       1000 Full       10.16.12.4-10.16.12.4         Virtual Machine Port Group	Create a vSphere standard switch	Speed	Networks
Image: With the second seco	Intel Corporation 82599EB 10-Giga	bit SFP+ Net	work Connection
Intel Corporation I350 Gigabit Network Connection          wmnic1       1000 Full       0.0.0.1-255.255.255.254         Use vSwitch0       Speed       Networks         Intel Corporation I350 Gigabit Network Connection       Networks         w:       1000 Full       10.16.12.4-10.16.12.4	mnic2	Down	None
Image: Wind Characterization with the point of the p	🔲 📟 vmnic3	Down	None
Use vSwitch0     Speed     Networks       Intel Corporation I350 Gigabit Network Connection     Image: Network Connection       Image: Vmnic0     1000 Full     10.16.12.4-10.16.12.4	Intel Corporation I350 Gigabit Netw	vork Connect	ion
Intel Corporation I350 Gigabit Network Connection         Image: Within the port Group       1000 Full       10.16.12.4-10.16.12.4         Within the Port Group	Vmnic1	1000 Full	0.0.0.1-255.255.255.254
Image: write         1000 Full         10.16.12.4-10.16.12.4           Virtual Machine Port Group         Physical Adapters	Use vSwitch0	Speed	Networks
Virtual Machine Port Group	Intel Corporation 1350 Gigabit Netw	vork Connect	ion
Virtual Machine Port Group	Vmnic0	1000 Full	10.16.12.4-10.16.12.4
	iew: Virtual Machine Port Group VM Network	· ·	
	Management Network 👳 🔶		
Management Network 🧕 🚽			

8. In the **Port Group Properties** section, provide a name for the management network in the **Network Label** field and select **All (4095)** from the **VLAN ID (Optional)** drop-down list. Click **Next**.

Figure 3 Selecting Port Group Properties

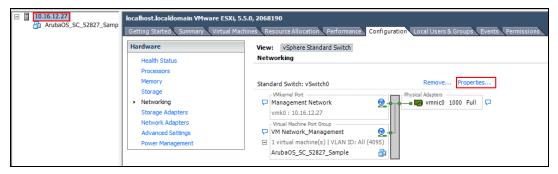
Network Label:	VM Network_Management		
VLAN ID (Optional):	None (0)	-	
	None (0)		
	All (4095)		
eview:			
Virtual Machine Port Group —	Physical Adapters		
Virtual Machine Port Group – VM Network_Managemer	it 👲 🖼 vmnic0		
- Virtual Machine Port Group			

#### 9. Click **Finish**.

The VM network name is set to VM Network\_Management and is used as an example in all configuration procedures.

- 10. Click the ESXi host IP address.
- 11. Click the **Configuration** tab.
- 12. Click **Networking** from the **Hardware** section.
- 13. Click **Properties** of the **VM Network\_Management**.

Figure 4 VM Network Properties\_Management



14. Select the VM network that was created for management and click Edit.

Figure 5 Edit Network Properties\_Management

2	vSwitch0 Properties				
P	orts	Network Adapters			
	Con	figuration	Summary		
	1	vSwitch	120 Ports		
	Θ	Management Net	vMotion and IP		
	0	VM Network_Man	Virtual Machine	]	
	A	dd	Edit Rer	nove	

- 15. Click the **Security** tab.
- 16. Select the **Promiscuous Mode** check box select **Accept** from the drop-down list.
- 17. Select the Forged Transmits check box and select Accept from the drop-down list.

NOTE

Forged Transmits should be enabled for VRRP to function.

18. Select the MAC Address Changes check box and select Accept from the drop-down list.

19. Click **OK**.

20. Click Close.

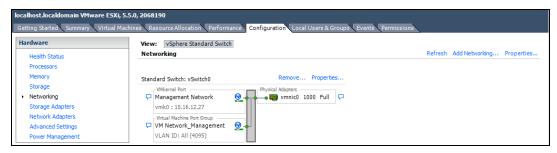
# **Creating VM Networks For Traffic**

Follow the steps below to create a VM network for traffic:

- 1. Repeat steps 1 to 4 of Creating A VM Network For Management.
- 2. Click Add Networking.

The Add Network Wizard is displayed.

Figure 6 Adding A Network For Traffic

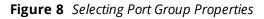


- 3. Select the Virtual Machine option and click Next.
- 4. Select a **vSwitch** that will handle the network traffic and click **Next**.

Figure 7 Selecting A Network Adapter For Traffic

🕢 Add Network Wizard				_ <b>D</b> X
Virtual Machines - Netw Virtual machines reach	work Access h networks through uplink adapters attached to vSphe	ere standard sv	vitches.	
Connection Type Network Access	Select which vSphere standard switch will handle vSphere standard switch using the unclaimed ne			ite a new
Connection Settings Summary	• Create a vSphere standard switch	Speed	Networks	*
Summary	Intel Corporation 82599EB 10-Giga	bit SFP+ Net	work Connection	
	Vmnic2	Down	None	
	vmnic3	Down	None	
	Intel Corporation 1350 Gigabit Netv	vork Connect	tion	=
	Vmnic1	1000 Full	0.0.0.1-255.255.255.254	
	O Use vSwitch0	Speed	Networks	
	Intel Corporation I350 Gigabit Netv	vork Connect	tion	
	vmnic0	1000 Full	10.16.12.4-10.16.12.4	-
	Preview:			
	Virtual Machine Port Group VM Network	Physical Adapters		
<u>H</u> elp	3		≤Back Next ≥	Cancel

5. In the **Port Group Properties** section, provide a name for **Network Label** and select **All (4095)** from the **VLAN ID (Optional)** drop-down list. Click **Next**.



Add Network Wizard					
Virtual Machines - Connection Settings Use network labels to identify migration compatible connections common to two or more hosts.					
Connection Type Network Access	Port Group Properties				
Connection Settings	Network Label:	VM Network_Traffic			
Summary	VLAN ID (Optional):	None (0) None (0) All (4095)	×		
	Preview:				
	-Virtual Machine Port Group VM Network_Traffic	Physical Adapters			
Help			<u>≤</u> Back Next	t <u>Cancel</u>	

6. Click Finish.



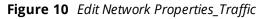
Ensure that the Management VM network and the Traffic VM network is isolated to avoid a network loop.

- 7. Click the ESXi host IP address.
- 8. Click the **Configuration** tab.
- 9. Click **Networking** from the **Hardware** section.
- 10. Click **Properties** of the vSwitch to edit.

Figure 9 VM Network Properties\_Traffic

localhost.localdomain VMware ESXi, 5.5.0, 2068190 Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions				
Hardware Health Status Processors	View: vSphere Standard Switch Networking			
Memory Storage • Networking Storage Adapters	Standard Switch: vSwitch0 -Wikemel Port Management Network vmk0 : 10.16.12.27	Remove Properties Physical Adapters wmnic0 1000 Full		
Network Adapters Advanced Settings Power Management	Virtual Machine Port Group ✓ VM Network_Management ☑ 1 virtual machine(s)   VLAN ID: All (4095) ArubaOS_SC_52827_Sample			
Licensed Features Time Configuration DNS and Routing Authentication Services Virtual Machine Startup/Shutdown Virtual Machine Swapfile Location	Standard Switch: vSwitch1 Virtual Machine Port Group VM Network_Traffic 1 virtual machine(s)   VLAN ID: All (4095) Aruba0S_SC_52827_Sample	Remove Properties		
Virtual Machine Swapine Education Security Profile Host Cache Configuration System Resource Allocation Agent VM Settings Advanced Settings	Standard Switch: vSwitch2 -Virtual Machine Port Group VM Network_Traffic1 I virtual machine(s)   VLAN ID: All (4095) ArubaOS_SC_52827_Sample	Remove Properties		

11. Select the VM network that was created for traffic and click **Edit** 



vSwit	tch1 Properties				
orts	Network Adapters				
	figuration	Summary	Port Group Properties	VM Network_Traffic	
	vSwitch VM Network_Traff	120 Ports Virtual Machine	VLAN ID:	All (4095)	
			Effective Policies		
			Security		
			Promiscuous Mode:	Reject	
			MAC Address Changes:	Accept	
			Forged Transmits:	Accept	
			Traffic Shaping		
			Average Bandwidth:		
			Peak Bandwidth:		
			Burst Size: Failover and Load Balan		
			Load Balancing:	Port ID	
			Network Failure Detection		
			Notify Switches:	Yes	
			Failback:	Yes	
			Active Adapters:	vmnic2	
			Standby Adapters:	None	
Ac	id	Edit Remove	Unused Adapters:	None	
				Close	e Help

- 12. Click the **Security** tab.
- 13. Select the **Promiscuous Mode** check box select **Accept** from the drop-down list.
- 14. Select the Forged Transmits check box and select Accept from the drop-down list.



Forged Transmits should be enabled for VRRP to function.

15. Select the MAC Address Changes check box and select Accept from the drop-down list.

- 16. Click **OK**.
- 17. Click Close.

Create two additional networks for traffic and repeat the steps to enable Promiscuous mode and Forged transmits.



The Mobility Master Virtual Appliance supports three network interfaces and Mobility Controller Virtual Appliance supports four network interfaces. For more information, see <u>Alcatel-Lucent Mobility Master Virtual Appliance on</u> page 10.

If the vSwitch or Distributed vSwitch is configured to use NIC teaming please refer to the <u>Recommendations</u> for NIC Teaming on a vSwitch on page 1 in the Appendix for validated configuration settings.

### **Deploying the OVF Template**

Follow the steps below to deploy the Open Virtual Format (OVF) template:

1. Log in to the vSphere ESXi Host using vSphere Client. For additional information, see <u>Logging Into ESXi</u> <u>Host Using vSphere Client</u>.

2. Click File > Deploy OVF Template.

#### The Deploy OVF Template Wizard is displayed.



It is recommended to copy the template to the client machine before importing the OVF template.

3. Click **Browse** and navigate to the location of the OVA file and click **Next**.

The **OVF Template Details** option is highlighted.

4. Click Next.

The Name and Location option is highlighted..

5. In the **Name** field, enter a name for the OVF template and click **Next**.

The **Disk Format** option is highlighted.

6. Select Thick Provision Lazy Zeroed option and click Next.

The **Network Mapping** option is highlighted.

7. Select VM Network\_Management from the Destination Networks drop-down list and click Next. The Ready to Complete option is highlighted.

Figure 11 Network Mapping

🕗 Deploy OVF Template				
Network Mapping What networks should the	deployed template use?			
Source OVF Template Details Name and Location	Map the networks used in this OVF template to networks in your inventory			
Disk Format	Source Networks	DestinationNetworks		
Network Mapping	VM Network	VM Network_Management	-	
Ready to Complete		VM Network_Management VM Network_Traffic VM Network_Traffic1 VM Network_Traffic2		
	Description:			
	The VM Network network		*	
Help		< Back Next >	Cancel	

Review your preferences before clicking Finish.

Do not select Power on after deployment check box in the Ready to Complete window.

#### 8. Click Finish.

The OVF template is deployed.



NOTE

Since the deployment of the OVF template is time consuming, it is highly recommended that the client is on the same VLAN as the Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance.

9. Click **OK**.

10. Click Close.

### **Pre-Allocating Memory**

Follow the steps below to pre-allocate memory in the Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance:

1. Right-click the VM and select **Edit Settings** or click **Edit virtual machine settings** from the **Getting Started** tab.

- 2. From the **Resources** tab select **Memory.**
- 3. Select the **Reserve all guest memory (All locked**) check box.
- 4. Click **OK**.

#### Figure 12 Editing Memory Settings

ArubaOS_SC_Test - Virtual Machine Properties				
Hardware Options Resources		Virtual Machine Version: 8		
Settings	Summary	Resource Allocation		
CPU	0 MHz			
Memory	0 MB	Reserve all guest memory (All locked)		
Disk Advanced CPU	Normal HT Sharing: Any	Shares: Normal v 81920 -		
Advanced Memory	NUMA Nodes: 2	Reservation:		
		Limit: 60123 + MB		
		Limit based on parent resource pool or current host		
Help		OK Cancel		

Repeat the steps to pre-allocate memory for other AOS-W VMs.

For more information on memory and CPU allocation refer to sizing tables in <u>Alcatel-Lucent Mobility Master</u> Virtual Appliance on page 10.

### **Assigning Network Connections**

By default the management network is assigned to all network adapters.

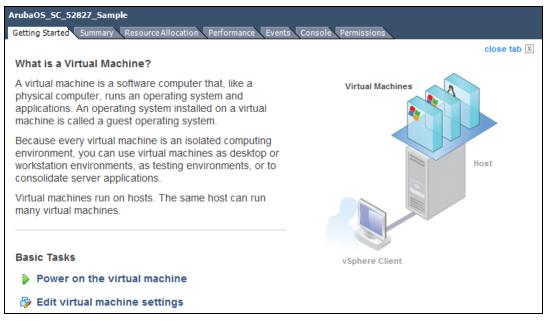


If different networks are not assigned to different adapters it will result in a network loop.

Follow the steps below to assign different networks to different adapters:

1. Click Edit virtual machine settings.

#### Figure 13 Virtual Machine Settings



2. Select Network adapter2 and select VM Network\_Traffic from the Network label drop-down list.

#### Figure 14 Assigning A Network

rdware Options Resources		Virtual Machine Version:
Show All Devices	Add Remove	Device Status
lardware	Summary	Connect at power on
Memory CPUs Video card VMCI device SCSI controller 0 CD/DVD drive 1 Hard disk 1 Floppy drive 1 Network adapter 1	8192 MB 3 Video card Restricted LSI Logic Parallel Client Device Virtual Disk Client Device VM Network_Managem	Adapter Type Current adapter: VMXNET 3 MAC Address 00:0c:29:55:26:1d C Automatic C Manual DirectPath I/O Status: Inactive 1
<ul> <li>Network adapter 2</li> <li>Network adapter 3</li> <li>Network adapter 4</li> <li>Serial port 1</li> </ul>	VM Network_Traffic VM Network_Traffic1 VM Network_Traffic2 telnet://:6001	Network_Traffic VM Network_Traffic VM Network_Traffic VM Network_Traffic VM Network_Traffic VM Network_Traffic1 VM Network_Traffic2
Help		OK Cancel

- 3. Repeat the steps and assign:
  - a. Network adapter3 to VM Network\_Traffic1
  - b. Network adapter4 to VM Network\_Traffic2
- 4. Click **OK**.

#### Table 6: Network Adapter Mapping

Adpater	Mapping
Network Adapter 1	Out-of-band management
Network Adapter 2	Gigabit ethernet 0/0/0
Network Adapter 3	Gigabit ethernet 0/0/1
Network Adapter 4	Gigabit ethernet 0/0/2



The Mobility Master Virtual Appliance does not support more than three network interfaces, but Mobility Controller Virtual Appliance supports four interfaces.

### **Enabling Security Profile Configuration**

This is an optional step and should be used only if serial console redirection is required. To enable security profile configuration you need to Telnet over the network.

- 1. Click the ESXi host IP address.
- 2. Click the **Configuration** tab.
- 3. In the **Software** section, click **Security Profile**.
- 4. In the **Firewall** section, click **Properties**.
- 5. Select the VM serial port connected over network check box.

Figure 15 Enabling VM Serial Port Connected Over Network

	Label	Incoming Ports	Outgoing Ports	Protocols	Da 🔺
$\mathbf{\nabla}$	HBR		31031,44046	TCP	N/.
$\mathbf{\nabla}$	rdt	2233	2233	TCP	N/.
$\mathbf{\nabla}$	Fault Tolerance	8100,8200,8300	80,8100,8200,8300	TCP,UDP	N/.
	syslog		514,1514	UDP,TCP	N/.
$\mathbf{\nabla}$	VMware vCenterAgent		902	UDP	St(
	IKED	500	500	UDP	N/. =
$\mathbf{\nabla}$	VM serial port connected over network	23,1024-65535	0-65535	TCP	N/
Г	http Client		80,443	TCP	N/.
$\mathbf{\nabla}$	ipfam	6999	6999	UDP	N/.
$\mathbf{\nabla}$	DNS Client	53	53	UDP,TCP	N/. +
•					•

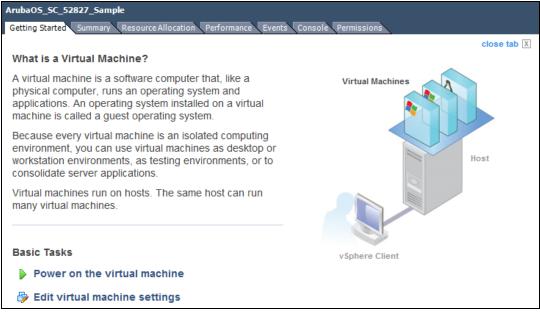
6. Click **OK**.

### **Configuring Serial Console for the VM**

Follow the steps below to configure serial console for the VM:

- 1. Select the VM machine that was created.
- 2. Click Edit virtual machine settings.

#### Figure 16 Edit Virtual Machine Settings



- 3. On the **Hardware** tab, click **Add**.
- 4. Select Serial Port and click Next.
- 5. Select Connect via Network and click Next.

#### Figure 17 Configuring Serial Console

Add Hardware				
Device Type What sort of device do	you wish to add to your virtual machine	e?		
Device Type Select Port Type Select Output File Ready to Complete	Choose the type of device you w Serial Port Parallel Port CD/DVD Drive CD/DVD Drive USB Controller USB Device (unavailable) PCI Device (unavailable) CD/DVD Drive USB Device (unavailable) Ethernet Adapter Hard Disk SCSI Device (unavailable)	vish to add. Information This device can be added to this Virtual Machine.		
Help		≤ Back Next ≥ Cancel		

#### 6. Select Server (VM Listens for connection) and enter telnet://:6001 in the Port URI field.

#### Figure 18 Connecting The Serial Via Network

🔗 Add Hardware	
Network Serial Port Setting How should this serial port of	
Device Type Select Port Type Select Network Backing Ready to Complete	Network Backing         © Server (VM listens for connection)         © Client (VM initiates connection)         Port URI:         telnet://:6001         Use Virtual Serial Port Concentrator         vSPC URI:         Device Status         Image: Connect at power on         I/O Mode         Image: Vield CPU on poll         Allow the guest operating system to use this serial port in polled mode rather than in interrupt mode.
Help	≤ Back Next ≥ Cancel

#### 7. Click **Next > Finish > OK**.

To enable serial console redirect refer to <u>Configuring the Initial Setup on page 58</u>.



If there are multiple VMs on the same ESXi host ensure they are connected to different serial ports.

To access the VM console you must telnet to the IP address of the ESXi host.

Ensure that the following prerequisites are addressed before starting the installation:

- vSphere Hypervisor 6.5 is installed on the server that hosts the Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance as a guest.
- OVF/ISO template is obtained from an Alcatel-Lucent representative and accessible from vSphere Client/vCenter.



Support is available for vSphere Web Client from ESXi 6.0 onwards.

### **Overview of Procedures**

Listed below are the steps to install AOS-W using vSphere Hypervisor ESXi 6.5:

- Logging Into ESXi Host Using vSphere 6.5
- Creating a VM Network
- Enabling Serial Console Access
- <u>Configuring Serial Console for the VM</u>

### Logging Into ESXi Host Using vSphere Hypervisor 6.5

To log in to the vSphere ESXi host:

- 1. Enter the IP address of the vSphere Hypervisor in a Web browser.
- 2. Enter the user name and password.
- 3. Click **Login**. The vSphere Web Client page is displayed.

### **Creating VM Networks**



Create two VM networks, one for management and the other for network traffic.

### **Creating VM Network For Management**

To create a VM network for management:

- 1. Log in to the vSphere 6.5 Web client.
- 2. Click **Networking** in the **Navigator** menu. The networking wizard is displayed.
- 3. Click Add port group.
- 4. In Add port group New port group:
- Enter a name in the for the new port group.
- Enter 4095 in the VLAN ID field.
- Select vSwitch0 from the Virtual switch drop-down list.

- 5. Click Add.
- 6. Select the newly created port group from the networking wizard and click **Edit settings**.
- 7. Click the **Security** tab.
- 8. Select Accept for Promiscuous mode, MAC address changes, and Forged transmits.
- 9. Click **Save**.

### **Creating VM Networks For Traffic**

To create a VM network for traffic:

1. In the vSphere 6.5 Web client navigate to **Navigator > Networking**. The networking wizard is displayed.

- 2. Click the Virtual Switches tab.
- 3. Click Add standard virtual switch.
- 4. In the Add standard virtual switch New switch
- Enter a name in the for the new virtual switch.
- From the **Uplink1** drop-down list select a vmnic that will handle the network traffic.
- 5. Click Add.
- 6. Click **Port groups** in the networking wizard.
- 7. Click Add port group.
- 8. In Add port group New port group:
- Enter a name in the for the new port group. For example **Traffic**.
- Enter **4095** in the **VLAN ID** field.
- Select the virtual switch that was created for traffic.
- 9. Click the **Security** tab.
- 10. Select Accept for Promiscuous mode, MAC address changes, and Forged transmits.
- 11. Click Add.

# **Enabling Security Profile Configuration**

This is an optional configuration and should be used only if serial console redirection is required. To enable security profile configuration you need to Telnet over the network.

- 1. In the vSphere 6.5 Web client navigate to **Navigator > Networking**.
- 2. Click the Firewall rules tab.
- 3. Select VM Serial port connected over network.
- 4. Click **Actions** and select **Enable**.

### **Configuring Serial Console for the VM**

To configure serial console for the VM:

1. In the vSphere 6.5 Web client navigate to **Navigator > Virtual Machines**. A list of VMs are displayed.

- 2. Click the Virtual Switches tab.
- 3. Right click the VM in which you want to configure serial console and click **Edit settings**.
- 4. In the **Edit standard virtual switch <virtual switch name>** window:
- Click Add other device and select Serial Port.

- Click the **New Serial Port** tab and select **Use network** from the drop-down list.
- Select **Server** from the drop-down list for **Direction**.
- Enter **telnet://:6001** in Port URL field.
- 5. Click **Save**.

# Chapter 5 Installing AOS-W Using vSphere Hypervisor

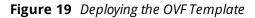
Ensure that the following prerequisites are addressed before starting the installation:

- vSphere Hypervisor 5.1, 5.5, 6.0, 6.5, or 6.7 is installed on the server that hosts the Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance as a guest.
- vSphere Client/vCenter is installed on a Windows machine.
- OVF/ISO template is obtained from an Alcatel-Lucent representative and accessible from vSphere Client/vCenter.

Follow the steps below to deploy the Open Virtual Format (OVF) template using vCenter:

1. Login to vCenter.

2. Right-click the ESXi host where the ovf will be deployed and click **Deploy OVF Template**. This action can also be done through the **Actions > Deploy OVF Template**.



vmware <sup>®</sup> vSphere Web Client		New vApp
Navigator	-	New Resource Pool
	1	Deploy OVF Template
Back		Connection •
		Maintenance Mode
✓ I vcsa.qavm.com		Power •
▶ 🛅 Amol		Certificates
▼ 🛄 SSP		
SSP-DC		Storage
✓ International Platform-DC	٠	Add Networking
🔻 🔂 10.16.13.239	-	Add Diagnostic Partition
🚰 ArubaOS_MM_60512-sha1-n	-	Host Profiles
MM-8.2-stdby		Host Promes
🚰 srini-sample-del (orphaned)		Edit Default VM Compatibility
▼ 📱 10.16.9.20		Export System Logs
ArubaOS_MM_60512-MM1		
ArubaOS_MM_8.1.0.0_59206		Reconfigure for vSphere HA
ArubaOS_MM_8.1.0.2_60417	-	Assign License
ArubaOS_MM_8.1.0.2_60858		Settings
ArubaOS_VMC_8.1.0.0_5920		Move To
ArubaOS_VMC_8.1.0.2_6041		Tags & Custom Attributes
MMui		rags a custom Autoutes
primary		Add Permission
🔁 secondary		Alarms
		Remove from Inventory
▼ 10.16.9.25	Б	Disassociate Host
ArubaOS_MM_8.0.1.0_57204		
ArubaOS_MM_8.1.0.2_60858		All vCenter Orchestrator plugin Actions
ArubaOS_VMC_8.1.0.2		Update Manager 🔹 🕨
Windows 2012_10.16.9.26	0-2	
Windows 2012_10.10.9.20		
ap mildows b		

- 3. Select Local file and click Browse.
- 4. Navigate to the location of the ova template, select the file, click **Open**.
- 5. Click Next.

6. Provide a name for the VM deployment and select the data center that contains the ESXi host. Click **Next**.

Figure 20 Selecting the Name and Location

🎓 Deploy OVF Template		? »
<ul> <li>1 Select template</li> <li>2 Select name and location</li> <li>3 Select a resource</li> <li>4 Review details</li> <li>5 Select storage</li> <li>6 Ready to complete</li> </ul>	Select name and location         Enter a name for the OVF and select a deployment location.         Name       ArubaOS_VMC_8.2.0.0_60872         Filter       Browse         Select a datacenter or folder.         Vesa.qavm.com         > aruble         SSP         > Platform-DC	
	Back Next Finish Car	icel

- 7. Select the ESXi host to run the deployment. Click **Next**.
- 8. Review the details of the deployment and click **Next**.

9. In the **Select storage** window ensure **Select Thick Provision Lazy Zeroed** option and click **Next**.

10. In the **Select network** window you can either add a standard vSwitch or distributed vSwitch to the source network. Click **Next** and **Finish**.



🍞 Deploy OVF Template		() H
<ul> <li>1 Select template</li> <li>2 Select name and location</li> </ul>	Select networks Select a destination network for each source	e network.
✓ 3 Select a resource	Source Network	Destination Network
<ul> <li>4 Review details</li> </ul>	VM Network	Platform_DPortGroup
✓ 5 Select storage		Platform_DPortGroup
6 Select networks		Dummy
7 Ready to complete		200_network
		VM Network 3
	_	VM Network
		Browse
	Description - VM Network	
	The VM Network network	
	IP Allocation Settings	
	IP protocol: IPv4	IP allocation: Static - Manual 0
		Back Next Finish Cancel

### **Adding a Serial Port**

Follow the steps below to add a serial port to be configured for serial access.

- 1. Right-click the ESXi where the OVA is displayed and click **Edit Settings**.
- 2. In the Virtual Hardware tab select Serial Port from the New device drop down and click Add,
- 3. Make the following changes:
  - a. For New Serial Port select Use Network.

- b. For **Direction** select **Server**.
- c. For **Port URL** enter telnet://:<esxi ip address>:<port number>.
- 4. Click **OK** and power on the OVA.

The following steps summarize the flow of steps to be followed to complete the installation:

- 1. Download the ISO file.
- 2. Create a VM running Red Hat Enterprise Linux 6 (64-bit).
- 3. Edit memory, HDD, network settings, and SCSI controller logic.
- 4. Edit the VM to force BIOS and use this to change the OS boot from CD.
- 5. Connect the ISO as CD/DVD from Datastore or local machine.
- 6. Boot the VM. The VM detects AOS-W from the CD and installs AOS-W.

### **Create a New VM**

1. Download the ISO file from Alcatel-Lucent website and upload the file to the VMware vSphere ESXi hypervisor datastore.

2. Right-click the ESXi host where the VM will be created and click **New Virtual Machine > New Virtual Machine**.

3. In the **Select a create type** window select **Create a new virtual machine**.

4. In the **Select a name folder** window enter a name for the new VM and select a location. Click **Next**.

Figure 22 Name and Location of New VM

1 New Virtual Machine		? >>
<ul> <li>1 Select creation type</li> <li>1 a Select a creation type</li> </ul>	Select a name and folder Specify a unique name and target location	
2 Edit settings	Enter a name for the virtual machine.	
2a Select a name and folder	New Virtual Machine_Tpubs <	
2b Select a compute resource	Virtual machine names can contain up to 80 characters and the	ey must be unique within each vCenter Server VM folder.
2c Select storage	Select a location for the virtual machine.	
2d Select compatibility	Q Search	
2e Select a guest OS	▼ 🗗 vcsa.qavm.com	
2f Customize hardware	▶ 🚍 Amol	
3 Ready to complete	▶ ☐ SSP     ♥       ▷ ☐ Platform-DC	Select a datacenter or VM folder to create the new virtual machine in.
		Back Next Finish Cancel

5. In the **Select a compute resource** window select the location of the host for installation. Click **Next**.

6. In the **Select storage** window select the datastore to store the configuration and disk files. Click **Next**.

1 Select creation type 1a Select a creation type	Select storage Select the datastore in which to store the configuration and disk files					
2 Edit settings 2a Select a name and folder 2b Select a compute resource	The following datastores	store Default are accessible from the de tion files and all of the virtu:		it you selected. Select	the destination d	atastore for the
2c Select storage	Name	Capacity	Provisioned	Free	Туре	Cluster
2d Select compatibility	datastore1 (1)	924.00 GB	76.35 GB	874.77 GB	VMFS 5	
2e Select a guest OS						
2f Customize hardware						
3 Ready to complete						
	4					
	Compatibility					
	Compatibility checks	s succeeded.				

Figure 23 Select Datastore

7. In the **Select compatibility** window, from the drop-down box select the ESXi version running on the vSphere. Click **Next**.

8. In the **Select a guest OS** screen, select **Guest OS Family** as Linux and **Guest OS version** as Red Hat Enterprise Linux 6 (64-bit). Click **Next**.

Figure 24 Select Guest Operating System

<b>*</b>	New Virtual Machine				?	) H
	1 Select creation type	Select a guest OS Choose the guest C	IS that will be installed on the virtual machine			
-	1a Select a creation type 2 Edit settings	, , , ,	t operating system here allows the wizard to provide the appropriate defa	ults for	the operating system	
<b>~</b>	2a Select a name and folder	installation.				
<b>~</b>	2b Select a compute resource					
<b>~</b>	2c Select storage	Guest OS Family:	Linux	•		
<b>~</b>	2d Select compatibility	Guest OS Version:	Red Hat Enterprise Linux 6 (64-bit)	•		
~	2e Select a guest OS					
	2f Customize hardware					
:	3 Ready to complete					
			Compatit	ility: E	SXi 6.0 and later (VM version 1	1)
			Back	Nex	t Finish Cance	<u>اا</u>

- 9. In the **Customize hardware** screen make the following changes:
  - a. Change the CPU value to 6.

Alcatel-Lucent recommends increasing the Cores for CPU and keeping the Socket value always at 1.

- b. Click the CPU drop-down and change **Cores per Socket** to 6.
- c. Change the **Memory** from 2048 MB to 8192 MB.



1	New Virtual Machine			? ₩
>	1 Select creation type 1a Select a creation type	Customize hardware Configure the virtual machine hard	dware	
	2 Edit settings	Virtual Hardware VM Options	SDRS Rules	
> >	2a Select a name and folder 2b Select a compute resource	-	6	*
~	2c Select storage	Cores per Socket (*)	6 Sockets: 1	
~	2d Select compatibility	CPU Hot Plug	Enable CPU Hot Add	::
~	2e Select a guest OS	Reservation	0 <b>v</b> MHz <b>v</b>	
	2f Customize hardware	Limit	Unlimited	
	3 Ready to complete	Shares	Normal - 6000 -	
		CPUID Mask	Expose the NX/XD flag to guest	
		Hardware virtualization	Expose hardware assisted virtualization to the guest 🚯	
		Performance Counters	Enable virtualized CPU performance counters	
		Scheduling Affinity	0	
		CPU/MMU	Automatic 🚽 🚯	*
		New device:	Select Add	
			Compatibility: ESXi 6.0 and later (VM	version 11)
			Back Next Finish	Cancel

- d. Change the **New SCSI controller** type to **LSI Logic Parallel**.
- e. From the New device drop down select New Hard Disk. Click Add.

f. From the **New device** drop down select **Network** and click **Add**. Add another network for the installation.

The following steps for configuring a serial port is optional:

a. From the **New device** drop down select **Serial Port**. Click **Add**.

b. From the **New Serial Port** drop down select **Use Network** and for **Connection** change **Direction** to **Server**.

c. Configure the Port URI to telnet://:<esxi ip address>:<port number>

#### Figure 26 Other Modifications

Customize hardware Configure the virtual mach	nine hardw	/are				
Virtual Hardware VM 0	Options	SDRS Rules	]			
▶ 🚐 New Hard disk	1	16	* *	GB	•	
👻 🛃 New SCSI controll	er L	SI Logic Paral	lel			
SCSI Bus Sharing	1	None			• 0	
Change Type	l	LSI Logic Para	allel		• 🗲	
▶ 飅 New Network	1	VM Network			•	Connect
▶ 🝥 New CD/DVD Drive	e 🤇	Client Device			•	Connect
🕨 🗖 New Floppy drive	(	Client Device			•	Connect
▶ 📃 Video card	5	Specify custor	n settings		•	
VMCI device						
Mew SATA Control	ler					
▶ Other Devices						
▶ 🔜 New Hard disk	1	16	* *	GB	•	
▼ ID *New Serial port	l	Use Network			- <	
Status	$\checkmark$	Connect At F	ower On			
Connection	<b>&gt;</b> D	)irection	Server			-
_	→ P	Port URI: te	elnet://10.16.1	3.239:333	3	
			Use Virtual	Serial Port	t Conce	ntrator
	VS	SPC URI:				
I/O Mode	-	Yield CPU o	n poll			
New device:		oo Serial	Port	•	Add	

# Installing the ISO on the VM

- 1. Navigate to the ESXi host where the VM was installed.
- 2. Right click and select **Edit Settings**.
- 3. Click the VM Options tab and select Boot Options.
- 4. Select Force Boot Options and Failed Boot Recovery. Click OK.

#### Figure 27 Boot Options

🗗 New VM_TPubs_iso - Edit Setti	ings	? ••
Virtual Hardware VM Options	SDRS Rules VApp Options	
▶ General Options	VM Name: New VM_TPubs_iso	1
VMware Remote Console Options	Lock the guest operating system when the last remote user disconnects	
VMware Tools	Expand for VMware Tools settings	
<ul> <li>Power management</li> </ul>	Expand for power management settings	
Firmware	Choose which firmware should be used to boot the virtual machine:	
	BIOS (recommended)	<u>]</u> .[
	Changing firmware might cause the installed guest operating system to become unbootable.	
Boot Delay	Whenever the virtual machine is powered on or reset, delay the boot order for:	
	0 milliseconds	
Force BIOS setup (*) 🗲	The next time the virtual machine boots, force entry into the BIOS setup screen	
Failed Boot Recovery (*) 🗲	When the virtual machine fails to find a boot device, automatically retry boot after:	
	10 seconds	
▹ Encryption	Expand for encryption settings	•
Compatibility: ESXi 6.0 and later (VI	I version 11) OK Cano	el

5. Click **Power on the virtual machine**. The BIOS prompt is displayed.

6. In the **Boot** option change **CD-ROM Drive** to first boot option and **Hard Drive** as the second boot option. Press **F10** to save changes and exit.

Main Adva		PhoenixBIOS ecurity	<mark>Setup</mark> Boot	Utility Exit	
CD DOM D	•				Item Specific Help
UMware UMware -Removable Legacy Network bo Network bo	e ble Add-in e Virtual S e Virtual S	CSI Hard Dr CSI Hard Dr ives ware VMXNET ware VMXNET	ive (0:: 3 3 #2		Keys used to view or configure devices: <enter> expands or collapses devices with a + or - <ctrl+enter> expands all &lt;+&gt; and &lt;-&gt; moves the device up or down. <n> May move removable device between Hard Disk or Removable Disk <d> Remove a device that is not installed.</d></n></ctrl+enter></enter>
F1 Help ↑↓ Esc Exit ↔	Select It Select Me			Values ► Sub-Me	-

7. Navigate to the ESxi host where the VM was installed. Click the **Summary** tab.

8. In the VM Hardware section, select CD/DVD drive 1 > Connect to CD/DVD image on a datastore.

Figure 29 Connect the CD/DVD Image on Datastore

New VM_TPubs_iso		🛓 🛛 🙆 Action:	e _				
New VM_1Pubs_iso			5 *				
Getting Started Summ	nary Monitor Configu	ire Permissio	ons Snapshots	Datastores	Networks	Update Manag	er
New VM_TPubs_iso         Guest OS:       Red Hat Enterprise Linux 6 (64-bit)         Compatibility:       ESXi 6.0 and later (VM version 11)         VM ware Tools:       Not running, not installed         More info       DNS Name:         IP Addresses:       Host:         10.16.13.239							
🔥 VMware Tools is n	ot installed on this virtual	machine.					
<ul> <li>VM Hardware</li> </ul>			▼ VM Storage	Policies			
▶ CPU	6 CPU(s), 143 MHz use	d	VM Storage Poli	icies			
▶ Memory	8192 MB, 2539 MB n	nemory active	VM Storage Poli	icy Compliance			
▶ Hard disk 1	16.00 GB		Last Checked E	Date			
▶ Hard disk 2	32.00 GB				Che	ck Compliance	
▶ Network adapter 1	VM Network 3 (connec	ted)	▼ Tags				
▶ Network adapter 2	VM Network (connecte	d)	Assigned Tag	Category	Des	aription	
▶ Network adapter 3	VM Network (connecte	d)		This list is en	npty.		
OD/DVD drive 1	Disconnected	_µ <sup>gr</sup> - <b>0</b>					
🔚 Floppy drive 1	Disconnected		o host CD device		.  -		
Video card	8.00 MB	B Connect to CD/DVD image on a datastore					
▶ Other	Additional Hardware	Connect to	i i i i i i i i i i i i i i i i i i i	a Content Library			

9. Browse to the location of the ISO file in the datastore, select the ISO file and click **OK**. Verify if the CD/DVD drive is connected in the **Summary** tab.

The installation will be initiated and once the installation is complete the system will be halted.

### Figure 30 System Halt

New VM_TPubs_iso	Enforce US Keyboard Layout	View Fullscreen	Send Ctrl+Alt+Delete
Unmounting partitions			
Boot		[ 0K ]	
Image0			
Image1 License		С ОК Ј С ОК Ј	
Dummy1			
<b>Вимму2</b>		с ок ј	
Flash		[ 0K ]	
Installing Bootloader		сок ј	
ArubaOS installation completed s	uccessfully		
Please remove the installation m	edium		
System will be halted in 5 secon	ds		
The system is going down NOW!			
Sent SIGTERM to all processes			
Sent SIGKILL to all processes			
Requesting system halt [ 150.205797] reboot: System ha	lted		
1 150.2057571 Febbull: System Ha	Iteu		

10. Power off the VM and ensure the ISO is removed from the CD/DVD drive in the **Summary** tab.

11. Power on the system.

# Prerequisites

Ensure that the following prerequisites are addressed before starting the installation:

- Enabling Intel VT virtualization hardware extensions in BIOS.
- Installing CentOS 7.2 on the x86 hardware.



Issue the **ethtool -K ethX gro off** command to ensure **generic receive offload** is disabled for all Ethernet ports that are mapped to the AOS-W VM for datapath traffic on KVM Hypervisor as root.

### **Supported Versions**

QEMU 2.0



The host kernel should be running version 4.6 or above and QEMU verision 2.7.0 for optimum crypto throughput performance with AOS-W in the KVM infrastructre. Libvrt should support passing of poll-us configuration option from VM xmlspecification to QEMU.

### **Enabling Intel VT Virtualization Hardware Extensions in the BIOS**

Follow the steps below to enable Intel IT virtualization hardware extensions in the BIOS:

- 1. Power on the machine and access the **BIOS Settings**.
- 2. Navigate to the **Processor** submenu. Processor settings menu may be hidden in **Chipset**, **Advanced CPU Configuration**, or **Northbridge**.
- 3. Enable Intel Virtualization Technology.

### **Installing CentOS 7.2**

Follow the steps below to install CentOS 7.2 on your system:

- 1. Connect a DVD or bootable USB stick to install CentOS 7.2.
- 2. Select Virtualization Host in Software Selection and select all Add-Ons for the installation.
- 3. Click Done.
- 4. Navigate to the location of the CentOS 7.2 file and select the destination folder.
- 5. Click Begin Installation.
- 6. Create a new user and a root password for the CentOS 7.2 installation during the installation process.
- 7. Reboot the server after the installation is complete.
- 8. Login to the newly installed CentOS 7.2 and configure the network and connect the server to the Internet.

A connection to the Internet is required to validate the installation and to install other packages.

a) Check for cpu virtualization support by executing the following command:

[root@localhost ~]# cat /proc/cpuinfo | grep -i vmx flags : ........vmx ......

b) Check for KVM mode support in the Kernel. If kvm\_intel is not listed, manually load kvm\_intel using the

```
modprobe kvm_intel command.
  [root@localhost ~]# lsmod | grep -i kvm
  kvm_intel 162153 0
  kvm 525259 1 kvm_intel
  [root@localhost ~]#
```



If the **Operation not supported** error message is displayed, ensure that Intel Virtualization technology is enabled in the BIOS.

9. Install the following packages:

- yum install qemu-kvm-tools.x86\_64 qemu-kvm.x86\_64 qemu-kvm-common.x86\_64
- yum install virt-manager.noarch virt-manager-common.noarch
- yum install virt-install.noarch
- yum groupinstall "GNOME Desktop"
- yum install tigervnc-server xorg-x11-fonts-Type1

Follow the steps below to install the AOS-W Mobility Master Virtual Appliance or a Mobility Controller Virtual Appliance on a KVM hypervisor:

- 1. Configuring the Virtual Network Computing (VNC) Server.
- 2. Creating a new VM and installing AOS-W.
- 3. Deploying the Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance.

# **Configuring the Virtual Network Computing Server**

Follow the steps below to configure the Virtual Network Computing (VNC) server and open up the firewall port to access the server remotely:

# 1. Start the VNC Server and configure a password for your CentOS server by executing the following command:

```
[root@localhost ~]# vncserver.You will require a password to access your desktop.
Password:
Verify:
xauth: file /root/.Xauthority does not exist
New 'localhost.localdomain:1 (root)' desktop is localhost.localdomain:1
Creating default startup script /root/.vnc/xstartup
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/localhost.localdomain:1.log
```

2. Open the firewall port on the CentOS server to ensure the CentOS server can be accessed using vncviewer.

```
[root@localhost ~]# netstat -ntap | grep vnc
tcp 0 0 0.0.0.0:5901 0.0.0.0:* LISTEN 14318/Xvnc
tcp 0 0 0.0.0.0:5902 0.0.0.0:* LISTEN 5242/Xvnc
tcp 0 0 10.16.9.130:5902 10.20.102.206:51576 ESTABLISHED 5242/Xvnc
tcp6 0 0 :::5901 :::* LISTEN 14318/Xvnc
tcp6 0 0 :::5902 :::* LISTEN 5242/Xvnc
[root@localhost ~]#
[root@localhost ~]# firewall-cmd --permanent --zone=public --add-port=5901/tcp
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]#
```

3. Download the AOS-W ISO image file from **support.esd.alcatel-lucent.com** to your CentOS server. The following are examples of ISO image files:

- AOS-W\_MM\_8.2.0.0\_57113.iso.
- AOS-W\_VMC\_8.2.0.0\_57113.iso.

## Creating a VM and Installing AOS-W

Follow the steps below to access the CentOS server through the VNC and start the virt manager to create the VM to be used by AOS-W:

- 1. Access the terminal and type **virt-manager** to start the **Virtual Machine Manager**.
- 2. Access the Virtual Machine Manager tab.
- 3. Click on File > New Virtual Machine. The New VM dialog box is displayed.

Figure 31 New Virtual Machine

	Virtual Ma	chine Manager	_ 0 ×
File Edit View Help			
<u>A</u> dd Connection		-	
<u>N</u> ew Virtual Machine		CPU usage	Host CPU usage
<u>C</u> lose	Ctrl+W	ci o couge	
<u>Q</u> uit	Ctrl+Q		
Running			
Suchin-MM Running			
Suchin-VMC Running		· · · · ·	
VS-MM1 Running			
VS-VMC-250AP Running			

- 4. Select Choose Local Install Media and click Forward.
- 5. Select Use ISO image and click Browse.
- 6. Navigate to the location of the iso image and click **Choose Volume**.

Ensure that Automatically detect operating system based in install media is not selected.

7. Select **OS type** as **Linux** and **Version** as **Redhat Enterprise Linux 7.2** from the drop-down lists and click **Forward**.

8. Change the Memory (RAM) to 8192 and CPUs to 6 and click Forward.

AOS-W 8.7.0.0 Virtual Appliance | Installation Guide

For Mobility Controller Virtual Appliance the RAM can be setup as 4096 (4 GB) and 3 CPUs. For more information on memory and CPU allocation refer to sizing tables in the <u>Alcatel-Lucent Mobility Master</u> <u>Virtual Appliance on page 10</u> section.

9. Select **Enable Storage for this VM** and change the value in **Create a disk image on the computer's hard drive** to 4 GB. Click **Forward**.

Figure 32 Enabling Storage on the VM

New VM					
Create a new virtual machine Step 4 of 5					
<ul> <li>Enable storage for this virtual machine</li> <li>Create a disk image on the computer's hard drive</li> </ul>					
4.0 – + GiB					
845.0 GiB available in the default location <ul> <li>Allocate entire disk now</li> <li>Select managed or other existing storage</li> </ul>					
Browse					
Cancel Back Forward					

The size of this disk needs to be at least 4 GB for Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance.

10. Provide a name for the VM and select **Customize configuration before install**. Click **Finish**.

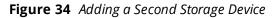
Figure 33 Beginning the Installation

	New VM				
	Create a new virtual machine Step 5 of 5				
Ready to be	gin the installation				
Name:	ArubaMM_KVM				
OS:	Red Hat Enterprise Linux 7.2				
Install:	Local CDROM/ISO				
Memory:	8942 MiB				
CPUs:	6				
Storage:	4.0 GiB				
	<ul> <li>Customize configuration before install</li> </ul>				
▼ Network selection					
Virtual network 'default' : NAT 🔻					
	Cancel Back Finish				

11. Select VirtIO Disk 1 and click on Advanced Options and make sure the Disk bus option is VirtIO.

12. Click **Add Hardware** and add another 8 GB storage device. (should be greater than half the size of RAM configured for the Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance).

13. Select VirtIO from the Bus type drop-down list. Click Finish.



		Add New Virtual Hardware
🚽 Begin Installation 🛛 💥 C:	Storage	Storage
Overview         Processor         Memory         Boot Options         IDE CDROM 1         IDE CDROM 2         Video QXL         IDE CONTOller USB         IDE USB Redirector 1         IDE USB Redirector 2	<ul> <li>Controller</li> <li>Network</li> <li>Input</li> <li>Graphics</li> <li>Sound</li> <li>Serial</li> <li>Parallel</li> <li>Console</li> <li>Channel</li> <li>USB Host Device</li> <li>PCI Host Device</li> <li>Video</li> <li>Watchdog</li> <li>Filesystem</li> <li>Smartcard</li> <li>USB Redirection</li> <li>TPM</li> <li>RNG</li> </ul>	<ul> <li>Create a disk image on the computer's hard drive</li> <li>6.0 - + GiB</li> <li>6.9 GiB available in the default location</li> <li>Allocate entire disk now S</li> <li>Select managed or other existing storage</li> <li>Browse</li> <li>Device type: Disk device </li> <li>Bus type: VirtIO </li> <li>Advanced options</li> </ul>
	ංజ RNG ൟ Panic Notifier	
Add Hardware		Cancel Finish

### **Creating Bridge Entries**

Create bridge entries to map all three network adapters that you will create in the steps below:

Ensure that you create a fourth bridge entry when configuring Mobility Controller Virtual Appliance.

#### 1. Login to CentOS and create three bridges and map three physical interfaces to these bridges.

```
[root@localhost ~]# brctl addbr br1
[root@localhost ~]# brctl addif br1 eno1
[root@localhost ~]# ifconfig br1 up
[root@localhost ~]# brctl addbr br2
[root@localhost ~]# ifconfig br2 up
[root@localhost ~]# brctl addbr br3
[root@localhost ~]# brctl addif br3 eno3
[root@localhost ~]# ifconfig br3 up
```

2. To make these bridge entries persistent across reboots, create a file in **/etc/sysconfig/network-scripts/** for all bridges.

```
[root@localhost ~]#vi /etc/sysconfig/network-scripts/ifcfg-br1
DEVICE=br1
STP=no
TYPE=Bridge
IPV6INIT=yes
```

IPV6 AUTOCONF=no IPV6 DEFROUTE=yes IPV6 FAILURE FATAL=no NAME=br1 UUID=a65be46d-a32a-4dca-bd00-f8acf9a356e5 ONBOOT=yes IPV6 PRIVACY=no [root@localhost ~]# [root@localhost ~]# cat /etc/sysconfig/network-scripts/ifcfg-br2 DEVICE=br2 STP=no TYPE=Bridge IPV6INIT=yes IPV6 AUTOCONF=no IPV6\_DEFROUTE=yes IPV6 FAILURE FATAL=no NAME=br2 UUID=19cf4539-9633-40aa-a4c5-606849b6e3db ONBOOT=yes IPV6\_PRIVACY=no [root@localhost ~]# [root@localhost ~]# cat /etc/sysconfig/network-scripts/ifcfg-br3 DEVICE=br3 STP=no TYPE=Bridge IPV6INIT=yes IPV6 AUTOCONF=no IPV6 DEFROUTE=yes IPV6 FAILURE FATAL=no NAME=br3 UUID=cb9a8df9-aa37-4346-8993-9e3739a9b0ce ONBOOT=yes IPV6\_PRIVACY=no

3. Click **Network Interface** and enter the following values:

- Network Source: Specify shared device name.
- Bridge name: br1
- Device model: virtio

Figure 35 Creating Bridge Entries

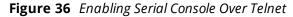
test_techpubs Virtual Machine					
🖋 Begin Installation 🛛 💥	Cancel Installation				
🖳 Overview	Virtual Network In	terface			
Processor	Network source:	Specify shared device n	name 🔻		
Memory		Bridge name: br1			
👺 Boot Options					
VirtIO Disk 1	Device model:	virtio	•		
IDE CDROM 1	MAC address:	52:54:00:f1:38:93			
NIC :f1:38:93	MAC address.	52.54.00.11.58.55			
🖉 Tablet					
💻 Display Spice					
述 Sound: ich6					
🚵 Console					
🚵 Channel qemu-ga					
🚵 Channel spice					
🖳 Video QXL					
📑 Controller USB					
WSB Redirector 1					
USB Redirector 2					
Add Hardware	]		Remove Cancel App	oly	

- 4. Click Add Hardware to add two more network interfaces.
- 5. Map bridge interfaces (**br2** and **br3**) to these network interfaces.
- 6. Click Add Hardware to add serial console.

### **Enabling Serial Console Over Telnet**

Follow the steps below to enable serial console over telnet. This procedure is optional.

- 1. Remove the existing Serial 1 device and click **Add Hardware**.
- 2. Select **Serial** on the left pane.
- 3. Select **TCP net Console** from the **Device Type** drop-down list.
- 4. Add the CentOS Server IP in the **Host** field and change the port number.
- 5. Select the **Use Telnet** check box and click **Finish**.



π	Add New Virtual Hardware _ 🗆 ×						
	Storage Controller	Serial Devi	ce				
	Network	Device Type:	TCP net console (tcp)		•		
	Input Graphics	Host:	10.16.34.34	Port:	<b> 4560</b>	- +	
	Sound Serial	Mode:	Server mode (bind)	-			
	Parallel	Use Telnet:					
	Console						
	Channel						
08 08	USB Host Device PCI Host Device						
<u> </u>	Video						
	Watchdog						
A	Filesystem						
	Smartcard						
	USB Redirection TPM						
	RNG						
ŝ	Panic Notifier						
				😮 Car	ncel	🔿 Finish	

6. Execute the following command to ensure the host firewall permits access to port number for serial console.

```
[root@localhost ~]# firewall-cmd --permanent --zone=public --add-port=4560/tcp
success
[root@localhost ~]# firewall-cmd --reload
success
```

NOTE

Enable serial console redirection from the AOS-W CLI after AOS-W boots up by executing the following command serial console redirection enable.

- 7. Select **VNC server** as the Spice Server from the **Type** drop-down list.
- 8. Select **Copy local keymap** from the **Kepymap** drop-down list and click **Apply**.
- 9. Select CPUs and make select the Copy host CPU configuration option.
- 10. Select the Manually set CPU topology option from the Topology drop down list.

11. Ensure the number of **Sockets** and **Threads** is always 1 and the value of **Cores** is the same as the value of **Current allocation**.

rhel7.0 on QEMU/KVM File Virtual Machine View Send Key 10 o X. 5 D ð, CPUs Overview Logical host CPUs: 24 OS information Current allocation: 3 + \_ Performance Maximum allocation: 3 CPUs Memory Configuration Boot Options Copy host CPU configuration VirtIO Disk 1 - Topology VirtIO Disk 2 Manually set CPU topology IDE CDROM 1 Sockets: 1 + NIC :51:db:08 Cores: + 3 NIC :e4:64:54 NIC :24:49:70 Threads: 1 + NIC :07:d0:73 Tablet 1 Mouse Keyboard Display VNC Sound: ich6 Add Hardware Cancel O Apply

Figure 37 Configuring CPU Values

#### 12. Click Begin Installation and select Install AOS-W.

Once the installation is complete the system will be halted after configuring the Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance.

#### Figure 38 System Halt

💻 😵   🖻 🗉 💌	10					. 0
Unmounting partitions						
Boot		1				
ImageO		1				
Image 1		1				
License			OK			
Dummy1 Dummy2			OK			
Flash			Öĸ			
Installing Bootloader		1	ΟK	1		
ArubaOS installation com	mpleted successfully					
Please remove the instal	llation medium					
System will be halted in	n 5 seconds					
The system is going down Sent SIGTERM to all proc Sent SIGKILL to all proc Requesting system halt	Cesses					
[ 26.572173] reboot: 5	System halted					

13. Force reset the VM to boot AOS-W and access to first boot dialogue.

#### Important

• Ensure you open the firewall port from CentOS terminal and restart the firewall.

```
[root@localhost ~]# firewall-cmd --permanent --zone=public --add-port=7001/tcp
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]#
```

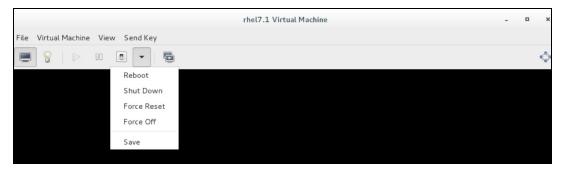
### **Configure Multiple Datapath CPUs**

To configure multiple datapath CPU's additional configuration is required both in host and guest. The guest changes cannot be made using virt-manager and hence you need to use the **virsh edit** command.



Ensure that the VM is gracefully shut down by using either the **Reboot** or **Shut Down** option before editing the VM xml specification.

### Figure 39 Graceful Shutdown



### **Changes in Host**

### On the KVM server, load the **vhost\_net module**

	'		_	
[root@localhost	~]#	lsmod   g:	rep	vhost
[root@localhost	~]#	modprobe v	vho	st_net
[root@localhost	~]#	lsmod   g:	rep	vhost
vhost_net		18152	0	
vhost		33338	1 .	vhost_net
macvtap		22363	1 .	vhost_net
tun		27141	3 ,	vhost_net

### XML Changes in Guest

Use the **virsh edit <name of the VM>** command in the KVM server and add the **<driver name='vhost' queues='y'/>"** tag, where y = total number of CPU's allocated to the VM.

For example, for a VM with six VCPU's and three NIC's of type Virtio, edit the xml and add **<driver** name='vhost' queues='6'> " tag for each NIC interface.

```
aruba@ubuntu-server-16x:~$ virsh list --all

Id Name State

5 centos6.5 running

- vmm-500dev shut off

[root@localhost ~]# virsh edit vmm-500dev
```

Domain vmm-500dev XML configuration edited.

Add **<driver name='vhost' queues='6'/>** after **"model type='virtio"** in the bridge config to ensure the values for the number of queues for the vhost and CPUs for the VM are the same.

The following snippet is an example of multi-queue XML specification for a single NIC interface. The same tag needs to be added for all Mobility Master Virtual Appliance NIC interfaces.

```
</controller>
<interface type='bridge'>
<mac address='52:54:00:d3:4a:3c'/>
```

```
<source bridge='br1'/>
<target dev='vnet10'/>
<model type='virtio'/>
<driver name='vhost' queues='6'/>
<alias name='net0'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
</interface>
<interface type='bridge'>
<mac address='52:54:00:49:7a:c6'/>
<source bridge='br2'/>
<target dev='vnet11'/>
<model type='virtio'/>
<driver name='vhost' queues='6'/>
<alias name='net1'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
</interface>
<interface type='bridge'>
<mac address='52:54:00:d3:55:7d'/>
<source bridge='br3'/>
<target dev='vnet12'/>
<model type='virtio'/>
<driver name='vhost' queues='6'/>
<alias name='net2'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
</interface>
```

```
[root@localhost ~]# virsh edit vmm-500dev
```

#### Domain vmm-500dev XML configuration edited.

[root@localhost ~]# virsh dumpxml vmm-500dev | grep queues <driver name='vhost' queues='6'/> <driver name='vhost' queues='6'/> [root@localhost ~]#

#### Reboot the VM and once the VM boots up you should see three CPUs as indicated in the example

(mm) [mynode] #show datapath utilization Datapath Network Processor Utilization +----+ Cpu | Cpu utilization during past | 1 | Type | Id | 1 Sec 4 Secs 64 Secs | +----+ 

 SP |
 1 |
 0% |
 0% |

 FP |
 2 |
 0% |
 0% |

 FP |
 3 |
 0% |
 0% |

 0% | 08 | 08 | Datapath CPU Allocation Summary Slow Path (SP) : 1, Slow Path Gateway (SPGW) : 0 Fast Path (FP) : 2, Fast Path Gateway (FPGW) : 0 DPI : 0, Crypto (CRYP) : 0 (mm) [mynode] #

#### VM memory locking xml tag

```
<name>VMC_50</name>
<uuid>4f5aaac7-7c3c-4565-8bf3-1b1492945cdc</uuid>
<memory unit='KiB'>6291456</memory>
<currentMemory unit='KiB'>6291456</currentMemory>
<memtune>
<hard_limit unit='G'>8</hard_limit>
</memtune>
<memoryBacking>
<locked/>
</memoryBacking>
```

# Prerequisites

Ensure that the following prerequisites are addressed before starting the installation:

- Hyper-V Version Windows Server 2012 R2
- Hyper-V Version Windows Server 2016



The following procedure can be used to deploy a Mobility Controller Virtual Appliance or a Mobility Master Virtual Appliance on Windows Hyper-V.

# Installing AOS-W on Windows Server Hyper-V

- 1. Log into the Windows server.
- 2. Open the Hyper-V manager.
- 3. Select the Hyper-V host machine from the navigation pane.
- 4. Right-click on the host machine and click **New > Virtual Machine**. Click **Next**.

#### Figure 40 Creating a New VM

File Action View Hel			
🔶 🌒 🔽 🔝			
🔡 Hyper-V Manager			
WIN-6VM9II90K1P	Virtual Machie	100	Manual Manufacture
	New	,	Virtual Machine
	Import Virtual Machine		Hard Disk
	Hyper-V Settings		Floppy Disk
	Virtual Switch Manager		Off
	Virtual SAN Manager		Off
	Edit Disk		
	Inspect Disk		
	Stop Service		
	Remove Server		
	Refresh		
	View	•	
	Help		

5. Enter a name for the VM in **Specify Name and Location** screen. If you want to store the machine in a location different from the default one, select the **Store the virtual machine in a different location** checkbox.

6. Select **Generation 1** as generation for this VM. Click **Next**.

7. Allocate 4096 MB as the startup memory. Click **Next**.

8. Click **Next** on the **Configure Network** screen. Network will be configured in later steps.

9. Enter a name for the first virtual disk. A second virtual disk will be added in later steps. Click **Next**.

10. Select Install an operating system from a bootable CD/DVD-ROM.

11. Select **Image file (.iso)** and click **Browse** to navigate to the location of the iso file. Select the iso file and click **Next**.

12. Click Finish.

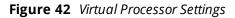
Figure 41 Completing the Installation

30	New Virtual Machine Wizard
Completing	the New Virtual Machine Wizard
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine. Description:          Name:       New Virtual Machine_Test         Generation:       Generation 1         Memory:       4096 MB         Network:       Not Connected         Hard Disk:       C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\VMC Disk1_Test.vhdx (VH         Operating System:       Will be installed from C:\Users\Administrator\Desktop\ArubaOS_MM_8.2.0.0-mm-
	<     III       To create the virtual machine and dose the wizard, dick Finish.

### Configuring the New VM

1. Right-click on the new VM and click **Settings**.

2. Select **Processor** from the **Hardware** pane and set the **Number of virtual processors** based on your requirement. For more information see, <u>Alcatel-Lucent Mobility Master Virtual Appliance on page</u> <u>10</u>.



New Virtual Machine_Test	~	
<ul> <li>★ Hardware</li> <li>★ Add Hardware</li> <li>★ BIOS Boot from CD</li> <li>■ Memory 4096 MB</li> <li>■ Processor</li> <li>■ IDE Controller 0</li> <li>■ Hard Drive VMC Disk1_Test.vhdx</li> <li>■ IDE Controller 1</li> <li>● DVD Drive ArubaOS_MM_8.2.0.0-mm</li> <li>SCSI Controller</li> <li>■ Network Adapter Not connected</li> <li>♥ COM 1 None</li> <li>♥ COM 2 None</li> <li>♥ COM 2 None</li> <li>♥ Diskette Drive None</li> <li>★ Management</li> <li>Integration Services Some services offered</li> <li>♥ Checkpoint File Location C:\ProgramData\Wicrosoft\Win</li> <li>♥ Smart Paging File Location C:\ProgramData\Wicrosoft\Win</li> <li>♥ Start Action</li> </ul>	Ш	Processor         You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.         Number of virtual processors:       1         Resource control         You can use resource controls to balance resources among virtual machines.         Virtual machine reserve (percentage):       0         Percent of total system resources:       0         Virtual machine limit (percentage):       100         Percent of total system resources:       5         Relative weight:       100
Restart if previously running	~	

3. Click **IDE Controller 0**. Select **Hard Drive** and click **Add** to add a second hard drive.

For increased performance it is recommended to use a SCSI controller/Disk instead of IDE controller.

4. Click New.

Figure 43 Adding a Second Virtual Disk

New Virtual Machine_Test	or New Virtual Machine_Test on WIN-6VM9II90K1P
<ul> <li>★ Hardware</li> <li>★ Add Hardware</li> <li>▲ BIOS Boot from CD</li> <li>■ Memory 4096 MB</li> <li>■ Processor</li> </ul>	Hard Drive You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting. Controller: Location: IDE Controller 0      I (in use)     V
3 Virtual processors IDE Controller 0 Image: Arrow VMC Disk1_Test.vhdx Image: Arrow VMC Disk1_Test.vhdx Image: Arrow Arr	Media You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file. Virtual hard disk:
IDE Controller 1  DVD Drive ArubaOS_MM_8.2.0.0-mm  SCSI Controller  Network Adapter Not connected  COM 1 None  COM 2	<ul> <li>If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.</li> </ul>
None Diskette Drive None Management Name New Virtual Machine_Test Integration Services Some services offered Checkpoint File Location	To remove the virtual hard disk, dick Remove. This disconnects the disk but does not delete the associated file.  Remove
C: \ProgramData \Microsoft \Win Smart Paging Fle Location C: \ProgramData \Microsoft \Win	V OK Cancel Apply

- 5. Click **Next** in the **New Virtual Hard Disk Wizard** window.
- 6. Select **VHDX** as the disk format and click **Next**.
- 7. Select **Dynamically expanding** as the disk type. Click **Next**.
- 8. Specify a name and location for the new VM and click **Next**.

9. The size of the new VM should be at least the size of the RAM. For more information on the size of the hard disk, see <u>Alcatel-Lucent Mobility Master Virtual Appliance on page 10</u>. Click **Next > Finish**.



In the **Hardware > Processor** section of the VM ensure the **Maximum number of processors** and the **Maximum amount of memory** on a single virtual NUMA node in the NUMA topplogy should always be more than the values configured for the Mobility Master. If the number of processors or memory allocated to the Mobility Master is more than what is configured under the NUMA configuration, the number of NUMA nodes and sockets will automatically increase and Mobility Master will not boot up.

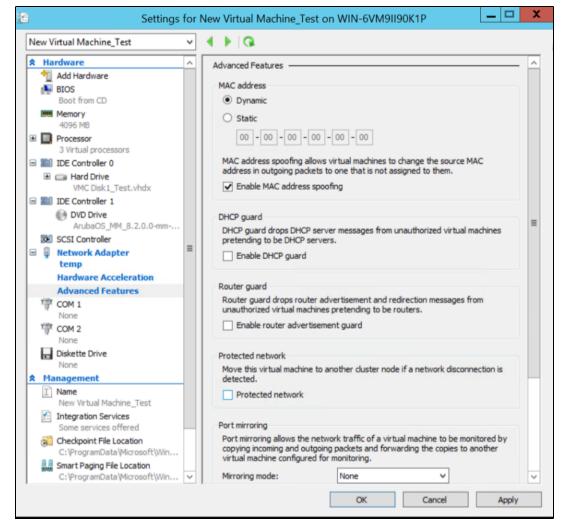
### **Creating a Network Adapter**

- 1. Select **Add Hardware** from the **Hardware** pane.
- 2. Select Network Adapter and click Add.
- 3. Select a virtual switch from the drop-down list.

4. Select Hardware Acceleration and ensure that Enable virtual machine queue and Enable IPsec task offloading check-boxes are cleared.

- 5. Select **Advanced Features** and complete the following steps:
  - a. Check the **Enable MAC address spoofing** checkbox.
  - b. Disable Protected Network.

Figure 44 Advanced Features



### 6. Click Apply > OK.



Create 3 network adapters for deploying a Mobility Master Virtual Appliance and 4 network adapters for deploying Mobility Controller Virtual Appliance.

### 7. Right-click the new VM and click **Start**.

8. Turn off the VM after the installation is complete and remove the installation ISO from DVD Drive. Restart the VM.

Figure 45 Restart the VM

Name 📩	State	CPU Usage	Assigned Memory	Uptime	Status		
mm-8.2	Off						
New Virtual Mac <sup>hie</sup>	Connect	0.%	4096 MB	00:03:35			
ubuntu-16.04-2	Settings						
VMC	Turn Off						
	Shut Down						
	Save						
	Pause						
	Reset						
Checkpoints	Checkpoint						
	Move						
	Export		The selecte	d virtual machine	has no checkpoints.		
	Rename						
	Enable Replication						
	Help						



To configure remote serial console for the VM, use a third party TCP proxy tool.

## **Configuring Trunk Ports**

Run the following **PowerShell** commands to configure trunk ports:

Remove all network adapters from the VM:

Remove-VMNetworkAdapter -vmname VMC

Add mgmt interface:

```
Add-VMNetworkAdapter -VMName VMC -Name mgmt
Set-VMNetworkAdapter -VMName VMC -Name mgmt -IPsecOffloadMaximumSecurityAssociation 0
-VmqWeight 0 -NotMonitoredInCluster $true
```

Add data interfaces:

```
Add-VMNetworkAdapter -VMName VMC -Name p1
Set-VMNetworkAdapter -VMName VMC -Name p1 -IPsecOffloadMaximumSecurityAssociation 0 -
VmqWeight 0 -NotMonitoredInCluster $true -MacAddressSpoofing on
Set-VMNetworkAdapterVlan -VMName VMC -VMNetworkAdapterName p1 -Trunk -
AllowedVlanIdList "1-4094" -NativeVlanId 0
```



Repeat the commands to create 2 virtual NICs if the device used is a Mobility Master Virtual Appliance or 3 virtual NICs if the device is a Mobility Controller Virtual Appliance.

These interfaces can then be added to virtual switches added through UI.

Once the installation is complete, follow these post-installation procedures to complete the deployment.

# **Configuring the Initial Setup**

Follow the steps below to configure initial setup:

- 1. Click Power on the virtual machine.
- 2. Enter values for the following first boot parameters in the console:
- System name
- Switch role
- IP type to terminate IPsec tunnel
- Master switch IP address or FQDN
- Is this a VPN concentrator for managed device to reach Master switch
- This device connects to Master switch via VPN concentrator
- Master switch Authentication method
- IPsec Pre-shared Key
- Uplink Vlan ID
- Uplink port
- Uplink port mode
- Native VLAN ID [1]
- Uplink Vlan IP assignment method
- Uplink Vlan Static IP address
- Uplink Vlan Static IP netmask
- IP default gateway
- DNS IP address
- IPV6 address on vlan
- Port-channel
- Port-channel id
- Uplink Vlan Static IPv6 address
- Uplink Vlan interface IPV6 prefix length
- IPv6 default gateway
- Country code
- Time Zone
- Time in UTC
- Date
- Password for admin login
- Re-type password for admin login

### The choices you entered in the first boot dialog are displayed.



Enter a static IP as the management IP in VLAN as part of the Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance setup. This should be a routable IP in an accessible subnet that the user can use to access the Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance via CLI (SSH) or Web GUI (HTTP) after VM setup is complete.

#### Enter **<Ctrl P>** to make changes to the first boot parameters.

3. Enter **Yes** to accept the changes. The Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance reboots and displays the log in prompt.

- 4. Log in with user name as admin and the password set in Step 2.
- 5. Execute the **enable** command.

6. Power on the Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance and execute the following command to enable the serial console.

Serial console redirect requires the vSphere Enterprise Plus license. When you enable serial console redirect, the vSphere console host window will be blank.

(host) #serial console redirect enable

Execute the following command to see the status of the serial console.

(host)	#show s	serial	console	rec	liı	rect
	Serial	Consol	e Redir	rect	:	Enabled

Execute the following commands to disable and view the status of the serial console.

(host) #serial console redirect disable
(host) #show serial console redirect
 Serial Console Redirect : Disabled

Reboot the Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance to access the serial console after enabling the serial console redirect.

To access the serial console telnet the IP address of the serial console followed by the serial port configured. For example: telnet 10.16.12.27 6001.

### **Management Interface**

The Mobility Master Virtual Appliance/Mobility Controller Virtual Appliance is a VM instance and access to the console is dependent on the deployment environment. If access through the serial port is denied you can alternatively access the console through the Management Interface. After an IP is assigned, the management interface can be accessed from anywhere in the network. To implement this change a separate routing table is assigned with its own default gateway for managing the IP that is introduced. This ensures the management traffic is routed to the right interface.

The initial implementation of this feature covers IPv4, IPv6, and manual configuration of a static IP for management interface from the console.



This feature cannot be configured using the WebUI.

Execute the following commands to configure an IP on the management interface:

IPv4:

```
(host) [mynode] \# \mbox{configure terminal} Enter Configuration commands, one per line. End with \mbox{CNTL}/\mbox{Z}
```





(host) [mynode] (config) #interface mgmt
(host) [mynode] (config-submode)#no shutdown
(host) [mynode] (config-submode)#ip address 10.16.9.203 255.255.255.0

### IPv6:

(host) [mynode] (config) #interface mgmt
(host) [mynode] (config-submode)#ipv6 address 2014::184/64

Execute the following commands to configure a default gateway for the management interface traffic and to segregate the management traffic from the normal data traffic on datapath ports:

#### IPv4:

(host) [mynode] (config) #ip default-gateway mgmt 10.16.9.2

#### IPv6:

(host) [mynode] (config) #ipv6 default-gateway mgmt 2014::1

# **Connectivity Issues**

Users experience wireless client connectivity issues when Mobility Master Virtual Appliance and Mobility Controller Virtual Appliance is used with NIC teaming and without configuring LACP. To resolve this issue refer to in the Appendix.

# **DHCP Address**

Clients connected to the Alcatel-Lucent Mobility Controller Virtual Appliance are unable to get a DHCP address. This issue is resolved by implementing NIC teaming on vSwitch or Distributed vSwitch. For more information refer to the Appendix.

# **ARP** Issues

ARP issue occurs when Promiscuous Mode is not enabled and all VLANs are disallowed on vSwitch.

### Instructions

Enable Promiscuous Mode and allow all VLANs on vSwitch.

To enable Promiscuous Mode, perform the following steps:

- 1. Log in to vSphere ESXi Host.
- 2. Switch to **Configuration** tab.
- 3. Select Networking under Hardware section.
- 4. Click **Properties** for a configured vSwitch.
- 5. Click Edit under Ports tab of vSwitch Properties window.
- 6. Switch to **Security** tab in **vSwitch Properties** window.
- 7. Select Accept from the Promiscuous Mode drop-down list.



Enable Promiscuous Mode on all ports attached to the VM. If a single port is used in AOS-W, Promiscuous Mode need not be enabled.

### 8. Click **OK**.

To allow all VLANs on vSwitch, perform the following steps:

- 1. Log in to the vSphere ESXi Host.
- 2. Click the **Configuration** tab.
- 3. Select Networking under Hardware section.
- 4. Click **Properties** for a configured vSwitch.
- 5. Select a configured VM network under **Ports** tab of **vSwitch Properties** window.
- 6. Click Edit under Ports tab of vSwitch Properties window.
- 7. Select All (4095) from the drop-down list against VLAN ID (Optional).

# **MAC Address Collision in a Network**

A user notices MAC address collision in a network due to duplicate MAC entries. When the duplicate MAC entry is detected by AOS-W, connectivity to the Mobility Controller Virtual Appliance is lost. To resolve this issue, refer to the following KB article. Once the issue is resolved reboot all VMs.

https://kb.vmware.com/selfservice/microsites/search.do?language=en\_US&cmd=displayKC&externalId=1024025

# **Characters Repeating In Remote Console**

The user notices unintended keystrokes when typing into a remote console. To resolve this issue, refer to the following KB article:

http://kb.vmware.com/selfservice/microsites/search.do?language=en\_ US&cmd=displayKC&externalId=196

# **Networks Cards Not Detected**

When a new network card is added to the ESXi/ESX host the following symptoms might be displayed:

- The new network card is not recognized by the system.
- The new network card is not listed when you run the command **esxcfg-nics -I**.

To resolve this issue, refer to the following KB article:

http://kb.vmware.com/selfservice/microsites/search.do?language=en\_US&cmd=displayKC&externalId=1034782

### HP Proliant DL580 Running ESXi 5.5 Is Not Powered On Due To Memory Leaks

HP Proliant DL580 running ESXi 5.5 will not be powered on due to memory leaks. To resolve this issue, refer to the following KB article:

http://kb.vmware.com/selfservice/microsites/search.do?language=en\_%20US&cmd=displayKC&externalId =2085618

# **Network Interfaces Are Not In The Correct Order**

Adding a fifth network adapter that uses **vmxnet3** devices changes the PCI bus IDs and also the order of network interfaces. To resolve this issue, refer to the following KB article:

https://communities.vmware.com/thread/443600

# **Connectivity Issues Observed When Using Multiple vSwitches**

Connectivity issues observed when multiple vSwitches in a VM network. To resolve this issue, refer to the following KB article:

https://communities.vmware.com/thread/460582

This chapter details additional information required in the current version of the Mobility Master. Click the following links for more information:

- Recommendations for NIC Teaming on a vSwitch
- Increasing the Flash Size on a vSphere Hypervisor
- Increasing the Flash Size on a KVM Hypervisor
- Backing up and Restoring Critical Data
- Datapath Debug Commands
- Implementing Management Interface
- Upgrading a Controller
- Jumbo Frame Support

### **Recommendations for NIC Teaming on a vSwitch**

When creating a vSwitch on the ESXi host, two or more NICs (network adapters) can be configured in the same vSwitch. To balance the traffic from the VM host to the uplink device since there is more than one NIC configured, ESXi provides the following configuration options:

- Route based on originating port ID.
- Route based on IP hash.
- Route based on source MAC hash.
- Explicit failover order.

### **Configuring NIC Teaming**

Login to the vSphere ESXi host using WebUI or a vSphere client. This following example is configured through the WebUI.

1. Login to the ESXi host.

2. Navigate to **Networking > Virtual Switches > Add standard virtual switch** or right click **Networking** and select **Add standard vSwitch**.

Figure 46 Adding a Standard Virtual Switch

vmware <sup>-</sup> ESXi <sup></sup>					
"E Navigator		🧕 localhost.localdom	ain - Networking		
✓ ☐ Host Manage			rtual switches Physical NICs VMkernel NI		
Monitor	5	Add standard virt	tual switch 🖪 Add uplink 🧪 Edit settings   🧲		v Uplinks
E Storage		wSwitch0		2	1
🧕 🔮 Networking	3	wSwitch1		1	0
	Networking Add port gr			1	2
	Add poir gi				
	Add VMker	rnel NIC			

3. In the **Add standard virtual switch - New switch** window enter the following details: a. **vSwitch Name**  b. Add the required number of uplinks from the **Uplink 1** drop-down menu.

c. Under **Security**, click the **Accept** radio button for **Promiscuous mode** and **Mac address** changes.

4. Click **Add**. A new vSwitch is created.

#### Figure 47 New vSwitch

🧕 localhost.localdomain - Networking			
Port groups Virtual switches Physical NICs VMkernel N	ICs TCP/IP stacks Firewall rules		
🏝 Add standard virtual switch 🛛 💻 Add uplink 🥒 Edit settings   🧲	Refresh   🔅 Actions		Q Search
Name	Port groups	Uplinks ~	Туре ~
m vSwitch0	2	1	Standard vSwitch
m vSwitch1	1	0	Standard vSwitch
m vSwitch2	1	2	Standard vSwitch
m test vSwitch	0	1	Standard vSwitch
			4 items "

### **Creating a Port Group**

1. Navigate to **Networking > Port groups > Add port group** or right click **Networking** and select **Add port group**.

Figure 48 Adding Port Group

<b>/m</b> ware <sup>,</sup> ESXi <sup>-</sup>					
🖥 Navigator 🛛	Second Se				
✓ ☐ Host Manage Monitor	Port groups         Virtual switches         Physical NICs <u>2</u> Add port group <u>2</u> Edit settings <u>2</u> Refresh <u>4</u>	VMkernel NICs TCP/IP stacks	Firewall rules		
> 🔁 Virtual Machines 🛛 5	Name	✓ Active ports	VLAN ID V	Туре	~ vSwitch
E Storage	Q VM Network	1	0	Standard port group	wSwitch0
🔮 Networking 🔬 Network	and the ptwork	1	0	Standard port group	wSwitch0
		0	51	Standard port group	wSwitch1
	indard vSwitch	1	51	Standard port group	svSwitch2
🐜 Add Vh	Ikernel NIC				

- 2. Provide a name for the new port group.
- 3. Add the virtual switch that was configured with NIC teaming to this port group.

4. Ensure the **Accept** radio button is selected for **Promiscuous mode**, **MAC address changes**, and **Forged transmits** under **Security**.

5. Click **Add**. A new port group is created.

### Figure 49 New Port Group

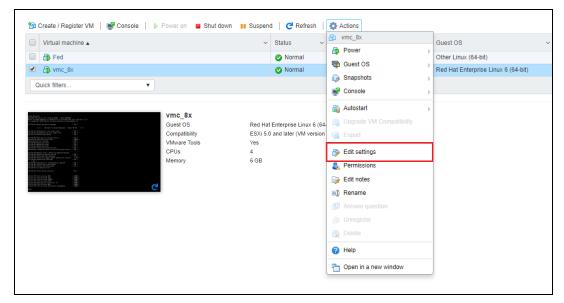
🔮 Add port group - test port group	
Name	test port group
VLAN ID	0
Virtual switch	test vSwitch
✓ Security	
Promiscuous mode	Accept Reject Inherit from vSwitch
MAC address changes	Accept Reject Inherit from vSwitch
Forged transmits	● Accept ○ Reject ○ Inherit from vSwitch
	Add Cancel

### Adding the Port Group to a VM Host

To add the port group to an host, edit the host setting of the Mobility Master Virtual Appliance or Mobility Controller Virtual Appliance.

- 1. From the **Navigator** window select **Virtual Machines**. The list of VMs are displayed.
- 2. Right-click the VM and select **Edit settings** or select the VM and click **Actions** > **Edit settings**.





3. Add the new port group that was created to the VM host.

Figure 51 Adding Port Group

🚯 Edit settings - vmc_8x (ESXi 5.0 virtua	I machine)	
Virtual Hardware VM Options		
🔜 Add hard disk 🛛 🎫 Add network ada	pter 🔄 Add other device	
CPU	4 🔻 🚺	
Memory	6144 MB 🔻	
Hard disk 1	4 GB •	0
Hard disk 2	6 GB <b>v</b>	0
► K SCSI Controller 0	LSI Logic Parallel	•
Network Adapter 1	VM Network	▼  Connect  ©
► ■■ Network Adapter 2	test port group	▼ Connect ⊗
Network Adapter 3	VM Network	▼  □ Connect
► ■■ Network Adapter 4	VM Network	▼  □ Connect
Floppy drive 1	Use existing floppy image	•
► i CD/DVD Drive 1	Host device	•
▶ 🕎 Video Card	Specify custom settings	٣
		Save Cancel

4. Click **Save**.

### **Preventing Dropping or Looping Broadcast/Multicast Packets**

To achieve this you need to make some changes to the NIC teaming policy.

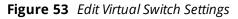
- 1. From the **Navigator** window select **Networking** > **Port Groups**.
- 2. Select the new port group that was created and click **Edit settings**.

Figure 52 Edit Port Group Settings

vmware <sup>®</sup> ESXi <sup>®</sup>		
Ravigator	🧕 localhost.localdomain - Networking	
✓ ☐ Host Manage	Port groups Virtual switches Physical NICs VMkerne	el NICs TCP/IP stacks
Monitor	2 Add port group 🥒 Edit settings C Refresh   🎄 Actions	
> 🗗 Virtual Machines 🛛 2	Name ~	Active ports ~
Storage	🧕 VM Network	2
- 🔮 Networking 🛛 🗾 5	Management Network	1
test v Switch	<u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>	0
More networks	<u> </u>	0
	🧕 test port group	1
	👰 vmnic4PG	1
	test port group	
	Accessible: Yes Virtual machines: 1	
		est vSwitch
	VLAN ID: 0	
	Active ports: 1	

3. Click **Security** and select the **Accept** radio option to enable **Promiscuous mode**, **MAC address changes**, and **Forged transmits**.

- 4. Click **NIC teaming** and make the following changes:
  - a. Load balancing option to Use explicit failover order.
  - b. Network failover detection option to Link status only.
  - c. Select the **Yes** radio button for **Notify switches** and **Failback**.
  - d. Select **No** for **Override failover order**.



Add uplink			
MTU	1500		
Uplink 1	vmnic5	,	6
Uplink 2	vmnic3	,	6
Link discovery	Click to expand		
Security			
Promiscuous mode	Accept OReject	t	
MAC address changes	Accept OReject	t	
Forged transmits	Accept OReject	t	
NIC teaming			
Load balancing	Use explicit failove	r order	▼
Network failover detection	Link status only		•
Notify switches	● Yes ○ No		
Failback	O Yes 💿 No		
Failover order	Mark standby	≣† Move up 🛛 ≣∎ Move down	
	Name	Speed	Status
	vmnic5	Link down	Active
	vmnic3	1000 Mbps, full duplex	Active
Traffic shaping	Click to expand		

5. Click **Save**.

# Configuring ReversePathFwdCheckPromisc

### In the WebUI

- 1. From the Navigator window select **Manage** > **System** > **Advanced settings**.
- 2. Scroll down or use the search bar to go to the **Net.ReversePathFwdCheckPromisc** option.
- 3. Select Net.ReversePathFwdCheckPromisc and click Edit option.
- 4. In the **Edit option Net.ReversePathFwdCheckPromisc** window update the **New value** field to 1 and click **Save**.



The **Net.ReversePathFwdCheckPromisc** option is not enabled by default and making changes to this option will be globally applicable on the ESXi.

### In the CLI

```
[host:] esxcfg-advcfg /Net/ReversePathFwdCheckPromisc
Value of ReversePathFwdCheckPromisc is 0
```

```
[host:] esxcfg-advcfg -s 1 /Net/ReversePathFwdCheckPromisc
Value of ReversePathFwdCheckPromisc is 1
[host:]
```



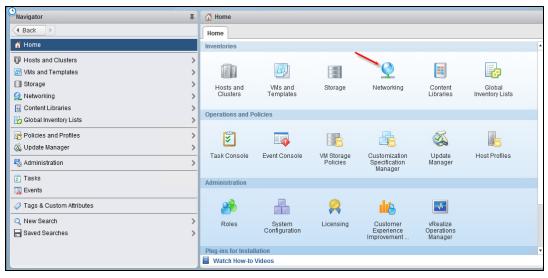
If the value of the ReversePathFwdCheckPromisc configuration option is changed when the ESXi instance is running, you need to enable or re-enable the promiscuous mode for the change in the configuration to take effect.

# Creating a Distributed vSwitch Using vCenter with LACP Configuration

Follow the steps below to create a distributed vSwitch:

- 1. Log in to the vSphere web client.
- 2. From the Home screen, select Networking.

Figure 54 Navigating to the Networking Icon



3. Right-click the data center and click **Distributed Switch > New Distributed Switch**.

Figure 55 New Distributed Switch

Navigator	Ĭ	h Plat	tform-DC	11	智 놆	🔁   🎯 Acti	ions 👻															
A Back		Getting	g Started	Summary	Monitor	Configure	Permissions	Hosts & Clusters	VMs	Datastores	Networks	Update Manag	jer									
Q 🙆 🗉	2																					
🔫 🚰 vcsa.qavm.com		What is a Datacenter?																				
Amol				the primary																		
SSP     SP     Platform-DC		inventory objects such as hosts and virtual machines. From the datacenter, you can add																				
200_network	Actions - Platform-DC	d nosts, folders, and clusters to a																				
O Dummy	Add Host	tacenter.																				
G test	1 New Cluster	enter Server can contain multiple																				
🔮 VM Network	New Folder	> ta	acenters. Large companies might use																			
Q VM Network 2	Distributed Switch			istributed Sv		-	2		Н	ost												
Q VII Network 2-19:     New Virtual Machine       Q VII Network 3     New vicp from Library       Q VII Network 4     Deploy OVF Template       → □ Platform-DSWITC     Storage       ▲ Platform-DSW     Edit Default VM Compatibility			Emport Distributed Switch																			
											Datacenter     vCenter Server     vSphere Client											
			🙉 Migrate VMs to Another Network																			
				Move To	- 1	ic Tasks				Funlara Fr										ethor		
				Rename	sic Tasks Explore Further																	
	Tags & Custom Attributes	- • I											_									
TRecent Objects Add Permission																						
Viewed Crea	Alarms	- • I																				
Platform-DC	🗙 Delete		Target		S	tatus		Initiator		Queued For	SI	art Time	1 •									
A Platform_DPortGroup	All vCenter Orchestrator plugin Actio	ns 🕨	🕜 vc	sa.qavm.con	n 🗸	Complete	d	VMware vSpher	re Up	2	263 ms 8	/13/2017 10:29:01	f									
10.16.9.25 Update Manager		•																				

4. Enter a name for the new switch in the **Name and location** window. Click **Next**.

### 5. Select **Distributed switch:6.0.0**. Click **Next**.

Select the exact version that is running on the ESXi host for the distributed switch. In this example we are selecting Distributed switch:6.0.0, as the setup uses vCenter 6.5 managing ESXi hosts running 6.0.

6. Select the required number of uplink ports Edit Settings page.

### Figure 56 Edit Settings

Len New Distributed Switch		(?) <b>}</b>
<ul> <li>1 Name and location</li> <li>2 Select version</li> <li>3 Edit settings</li> <li>4 Ready to complete</li> </ul>	Edit settings Specify number of uplinks: Number of uplinks: Network I/O Control: Default port group: Port group name:	k ports, resource allocation and default port group.          Image: style="text-align: center;">Image: style="text-align: center;"/>Image: style="text-align: center;"///Image: style="text-align: center;"///Image: style="text-al
		Back Next Finish Cancel

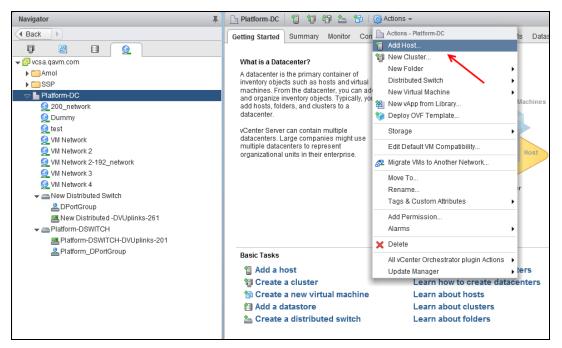
- 7. Click **Next** and review your selections.
- 8. Click Finish.

### Adding ESXi Hosts to the Distributed Switch

Follow the steps below to add ESXi hosts to the newly created distributed switch. These steps will enable vCenter to add physical ports to the distributed switch.

- 1. Right-click the newly created distributed switch and select **Add and Manage Hosts.** Click **Next**.
- 2. In the Select task window select Add hosts. Click Next.

### Figure 57 Add Hosts



3. Click **New Hosts** to add new ESXi hosts for the distributed switch configuration.

#### 4. Select the host from the **Select new hosts** window and click **OK**.

NOTE

Select **Configure identical network settings on multiple hosts (template mode)** to enable similar network configurations on multiple hosts.

Select new hosts		
Incompatible Hosts		Q Filter -
✓ Host	Host State	Cluster
10.16.13.239	Connected	N/A
M Q Find -		1 items 🕒 Copy -
		OK Cancel

### Figure 58 Select New Hosts

5. Click **Next**. In the **Select template host** window select a template host to apply its configuration to other hosts on the switch.

This step will enable you to add physical ports on the ESXi hosts to the distributed switch. Click **Next**.

6. In the **Manage physical network adapters** window select a physical network adapter.

#### 7. Click Assign uplink. The Select an Uplink for vmnic1 window is displayed.

#### 8. Select **Uplink 1 for vmnic1** and click **OK**. Click **Next**.

E			-	
			7	
Ν	0	т	Е	

In this example we have selected three uplinks when creating the distributed switch. Repeat these steps for the other vmnic2 and vmnic3.

9. Click **Apply to all** to apply the physical network adapter assignments to all hosts on the switch.

#### Figure 59 Selecting an Uplink for the Physical Adapter

	🖟 Add and Manage Hosts							
> >	1 Select task 2 Select hosts	Select network adapter tasks Select the network adapter tasks to perform.						
	3 Select network adapter tasks         4 Manage physical network adapters         5 Manage VMkernel network adapters         6 Analyze impact	<ul> <li>Manage physical adapters</li> <li>Add physical network adapters to the distributed switch, assign them to uplinks, or remove existing ones.</li> <li>Manage VMkernel adapters</li> <li>Add or migrate VMkernel network adapters to this distributed switch, assign them to distributed port groups, configure VMkernel adapter settings, or remove existing ones.</li> </ul>						
	7 Ready to complete	Migrate virtual machine networking Migrate VM network adapters by assigning them to distributed port groups on the distributed switch. Sample distributed switch						
		Manage VMkernel adapters VMkernel port group VMkernel ports www. VM port group VIrtual Machines Wm on the second s						
		Back Next Finish Canc	el					

- 10. Click Next in the Manage VMkernel network adapters page.
- 11. Click **Next** in the **Analyze impact** page and **Ready to complete** page. Click **Finish**.

### **Editing Security Properties on the Distributed Port Group**

Follow the steps below to modify the security settings on the distributed port group:

- 1. Select the distributed port group that is created under the distributed switch.
- 2. Select the **Configure** tab and click **Edit**.
- 3. Select **Accept** from the **Promiscuous mode**, **MAC address changes**, and **Forged transmits** drop down lists. Click **OK**.

Figure 60 Modify Security Settings

A DPortGroup_TestTP - Edit Setting	S			?
General Advanced Security Traffic shaping VLAN Teaming and failover Monitoring Traffic filtering and marking Miscellaneous	Promiscuous mode: MAC address changes: Forged transmits:	Accept Accept Accept	•	
				OK Cancel

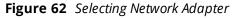
4. Navigate to **Hosts and clusters**.

5. Right-click the AOS-W VM that is running on the ESXi hosts to which the distributed switch is configured and select **Edit Settings**.

Figure 61 Mapping Uplink Ports

✓ I vcsa.qavm.com	
▶ 🔁 Amol	
▼ SSP	
SSP-DC	
▼ In Platform-DC	Demonstration (1)
▼ 🔂 10.16.13.239	🕨 Powered On 🔅
ArubaOS_MM_60512-sha1-newovatool	5_5
MM-8.2-stdby	-
🔂 srini-sample-del (orphaned)	
▼ 10.16.9.20	► VM Hardware
ArubaOS_MM_60512-MM1	Actions - ArubaOS_MM_60512-MM1
ArubaOS_MM_8.1.0.0_59206	Power
ArubaOS_MM_8.1.0.2_60417-july14	Guest OS
ArubaOS_MM_8.1.0.2_60858-11	Snapshots
ArubaOS_VMC_8.1.0.0_59206	P Open Console
ArubaOS_VMC_8.1.0.2_60417-july14	- Open Console
🗗 MMui	🖶 Migrate
🗗 primary	Clone •
🔂 secondary	Template •
wvmcui	Fault Tolerance
▼	VM Policies
ArubaOS_MM_8.0.1.0_57204	
ArubaOS_VMC_8.1.0.2	Compatibility •
ArubaOS_VMC_8.1.0.2_60858-2	Export System Logs
Windows 2012_10.16.9.26	🊂 Edit Resource Settings
🚯 Windows 8	🚱 Edit Settings <
	Move To
	Rename
	Edit Notes
	Tags & Custom Attributes
	Add Permission
	Alarms
	Remove from Inventory
	Delete from Disk
	All vCenter Orchestrator plugin Actions
	Update Manager 🕨 🕨

6. Select the distributed port group that was created in the earlier steps as Network Adapter 2.



ArubaOS_MM_60512-M	1M1 - Edit Settings		(?) ▶
Virtual Hardware VM Opt	ions SDRS Rules	vApp Options	
F 🔲 CPU	6	• 0	
▶ 🏧 Memory	8192	▼ MB ▼	
▶ 🚍 Hard disk 1	4	GB V	
▶ 🛄 Hard disk 2	6	GB V	
▶ ☑ SCSI controller 0	LSI Logic Parallel		
Metwork adapter 1	VM Network	🚽 🗹 Connecte	d
▶ m *Network adapter 2	DPortGroup_TestTP	(DSwitch_Tesť 🕞 🗹 Connecte	d
Network adapter 3	Dummy	🚽 🗆 Connecte	d
▶ <ul> <li>▶ OD/DVD drive 1</li> </ul>	Client Device	🗸 🗌 Connecte	d
Floppy drive 1	Client Device	Connecte	d
Video card	Specify custom setti	ngs 🚽	
VMCI device			
▶ Other Devices			
▶ Upgrade	Schedule VM Com	patibility Upgrade	
New device:	Select	Add	
Compatibility: ESXi 5.0 and	later (VM version 8)		OK Cancel

Connectivity will be restored with correct uplink switch configuration.

## **Configuring LACP Between the Distributed Switch and Uplink Switch**

Follow the steps below to configure LACP between the distributed and uplink switch:

- 1. From vCenter dashboard, click **Networking** and select the new distributed switch.
- 2. Click the **Configure** tab, and select **LACP**.

🖴 DSwitch_TestTP 🛛 🙎 🤱 🕼	s² 🦗 🍥	Actions 👻			
Getting Started Summary Monito	r Configure	Permission	s Ports H	osts VMs	Networks
	LACP				
▼ Settings	The enhance	ed LACP sup	port on a vSph	ere distribut	ed switch lets you connect ESXi hosts to physical switches by using dynamic link aggregation.
Properties Migrating network traffic to LAGs					
Topology LACP LAG Name Ports Mode VLAN					
	LAG Name	Ports	Mode	VLAN	
Private VLAN					This list is empty.
NetFlow Port mirroring					
Health check					
Resource Allocation					
System traffic					

- 3. Click + to add a LAG.
- 4. In the **New Link Aggregation Group** window update the following and click **OK**.
  - a. Name Name for the new LAG
  - b. Number of Ports 3
  - c. Mode Active
- 5. Select the new distributed port group configuration.



By default, uplink ports 1,2, and 3 will be selected for communication as active uplinks. This should be replaced with the LACP configuration.

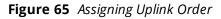
6. In the distributed port group page, click the **Configure** tab and select **Edit**.

Figure 64	Edit Port Group	Settings
-----------	-----------------	----------

🚨 DPortGroup_TestTP 🛛 🤰 🥘 Ad	ctions 👻	=*
Getting Started Summary Monitor	Configure Permissions Ports	Hosts VMs
<ul> <li>✓ Settings</li> </ul>	Properties	Edit
Properties	General	Λ
Properties	Name:	DPortGroup_TestTP
Policies	Port binding:	Static binding
► More	Port allocation:	Elastic
	Number of ports:	8
	Network resource pool:	(default)
	Advanced	
	Configure reset at disconnect:	Enabled
	Override port policies	
	Block ports:	Allowed
	Traffic shaping:	Disabled
	Vendor configuration:	Disabled
	VLAN:	Disabled
	Uplink teaming:	Disabled
	Security policy:	Disabled
	NetFlow:	Disabled
	Traffic filtering and marking:	Disabled

7. Select Teaming and failover.

8. Using the up and down arrow button move **Uplink 1**, **Uplink 2**, and **Uplink 3** to **Unused uplinks** and **lag1\_MM1\_test** to **Active uplinks**. Click **OK**.

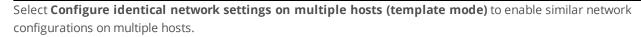


A DPortGroup_TestTP - Edit Setting	S			?
DPortGroup_TestTP - Edit Setting     General     Advanced     Security     Traffic shaping     VLAN     Teaming and failover     Monitoring     Traffic filtering and marking     Miscellaneous	s Load balancing: Network failure detection: Notify switches: Failback: Failback: Failover order Active uplinks Image and	Route based on originating virtual port Link status only Yes Yes		•
	Uplink 1 Uplink 2 Uplink 3 Select active and standby up	plinks. During a failover, standby uplinks acti	vate ir	n the order specified above.
				OK Cancel

### **Mapping LACP Port with Physical NICs**

Follow the steps below to map LACP with physical NICs.

- 1. Right-click the newly created distributed switch and select **Add and Manage Hosts.** Click **Next**.
- 2. In the Select task window select Manage host networking. Click Next.
- 3. Click **Attached hosts** and add ESXi hosts to the LACP configuration. Click **Next**.



#### Figure 66 Add and Manage Hosts

	Add and Manage Hosts			?
>	1 Select task 2 Select hosts	Select hosts Select hosts to manage their networking on this distributed switch.		
	Select network adapter	Attached hosts 🛛 🗙 Remove		
	<sup>4</sup> tasks	Host	Host Status	
	5 Manage physical network adapters (template mode)	10.16.9.20	Connected	
	6 Manage VMkernel network adapters (template mode)	10.16.9.25	Connected	
	7 Analyze impact			
	8 Ready to complete			
		Configure identical network settings on multiple hosts (template	e mode). 🕕	
			Back Next Finish Canc	el J

4. In the **Select template host** window select a template host to apply its configuration to other hosts on the switch. Click **Next**.

This step will enable you to add physical ports on the ESXi hosts for LACP. Click **Next**.

5. In the **Select network adapter tasks** window select **Manage physical network adapters.** Click **Next**.

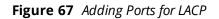
6. In the **Manage physical network adapters** window select a physical network adapter.

7. Click **Assign uplink**. The **Select an Uplink for vmnic1** window is displayed.

8. Select **lag\_MM1\_test0** for vmnic1 and click **OK**.



9. Click **Apply to all** to apply the physical network adapter assignments to all hosts on the switch. Click **Next**.



		a mada)		
	Manage physical network adapters (templat Add or remove physical network adapters to the			
2 Select hosts				
3 Select template host	<ol> <li>Configure or review physical network ada</li> </ol>	apter assignments for the template hos	t in this switch.	
4 Select network adapter tasks	🔚 Assign uplink 🗙 Unassign adapter 🐚	Reset changes 🚯 View settings		
5 Manage physical network adapters (template mode)	Host/Physical Network Adapters	1 🛦 In Use by Switch	Uplink	Uplink Port Group
6 Analyze impact	- 🗐 10.16.9.20 (template)			
	<ul> <li>On this switch</li> </ul>			
7 Ready to complete	对 vmnic1 (Reassigned)	DSwitch_TestTP	lag1_MM1_test-0	DSwitch_TestTP-DVUplinks
	飅 vmnic2 (Reassigned)	DSwitch_TestTP	lag1_MM1_test-1	DSwitch_TestTP-DVUplinks
	飅 vmnic3 (Reassigned)	DSwitch_TestTP	lag1_MM1_test-2	DSwitch_TestTP-DVUplinks
	<ul> <li>On other switches/unclaimed</li> </ul>			
	💌 vmnic0	vSwitch0	-	-
	🐥 Apply to all 🝙 Reset all 🚯 View setting			
	Host/Physical Network Adapters	1 🛦 In Use by Switch	Uplink	Uplink Port Group
	▼ 10.16.9.25			
	<ul> <li>On this switch</li> </ul>			
	vmnic1 (Reassigned)	DSwitch_TestTP	lag1_MM1_test-0	DSwitch_TestTP-DVUplinks
	飅 vmnic2 (Reassigned)	DSwitch_TestTP	lag1_MM1_test-1	DSwitch_TestTP-DVUplinks
	vmnic3 (Reassigned)	DSwitch_TestTP	lag1_MM1_test-2	DSwitch_TestTP-DVUplinks
	<ul> <li>On other switches/unclaimed</li> </ul>			
	🐖 vmnic0	vSwitch0	-	-
			Back	Next Finish Car

10. Click **Next** in the **Analyze impact** screen. There should be no impact in this window.

# Increasing the Flash Size on a vSphere Hypervisor

AOS-W enables you to increase the size of your flash to ensure that the flash is hosted on a separate disk. By doing this you can move to a hard disk with higher storage capacity for flash with minimal impact. Follow the steps below to increase the size of the flash on the Mobility Master Virtual Appliance.

- 1. Power down the VM.
- 2. Right click the VM in the vSphere client and click **Edit Settings**.
- 3. Click Add in the Virtual Machine Properties window.

Figure 68 Virtual Machine Properties

🕖 10.16.9.238 - vSphere C	lient
File Edit View Invento	ry Administration Plug-ins Help
🖸 🖾 🚯 Home	🕨 🛃 Inventory 🎐 🗊 Inventory
<ul> <li>III</li> <li>IIII</li> <li>III</li> <li>III</li></ul>	a 13 e 🗟 🗞
□ □ 10.16.9.238 □ AOS_SC-1 □ ArubaOS_MM	ArubaOS_MM_8.0.0.0_55647
<ul> <li>ArubaOS_SC_</li> <li>ControllerSim_</li> <li>ControllerSim_</li> <li>Fedora 20 5.1</li> <li>Mahesh_SC_N</li> </ul>	Guest Snapshot Open Console
Migration Too	Edit Settings
	Add Permission Ctrl+P
	Report Performance
	Rename
	Open in New Window Ctrl+Alt+N Remove from Inventory Delete from Disk

4. Click Hard Disk in the Add Hardware window and click Next.

Figure 69 Selecting the Device Type

Add Hardware		Manager State		X
Device Type What sort of device do	you wish to add to your virtual machine?			
Device Type Select a Disk Create a Disk Advanced Options Ready to Complete	Choose the type of device you wish to add.			
Help		<u>≤</u> Back	Next >	Cancel

5. Select **Create a new virtual disk** and click **Next**.

6. Enter a value of the desired disk size and select **Thick Provision Lazy Zeroed**. Click **Next**.

#### Figure 70 Create Disk

🕗 Add Hardware		Manager State	X
Create a Disk Specify the virtu	al disk size and provisioning policy		
Device Type Select a Disk Create a Disk Advanced Options Ready to Complete	Capacity Disk 16 GB C Disk Provisioning C Thick Provision Lazy Zeroed Thick Provision Eager Zeroed Thin Provision Location Store with the virtual machine Specify a datastore or datastore cluster:		
Help	Browse.	Cat	ncel

- 7. Click **Next** in the **Advanced Options** window and click **Finish**.
- Figure 71 New Hard Disk

Show Al Devices       Add       Remove       Memory Configuration         Hardware       Summary       1011 GB       Memory Size:       8         Image: CPUs       3       1011 GB       Memory Size:       8         Image: CPUs       3       128 GB       Maximum recommended for       111 GB       128 GB         Image: CPUs       3       128 GB       Maximum recommended for       113 GB       113 GB         Image: CD/DVD drive 1       Client Device       64 GB       Maximum recommended for       115 GB         Image: CD/DVD drive 1       Client Device       64 GB       Maximum recommended for       108 GB         Image: Hard disk 2       Virtual Disk       32 GB       Image: COS: 2 GB.       Minimum recommended for         Image: Hard disk 3       Virtual Disk       16 GB       Image: COS: 2 GB.       Minimum recommended for         Image: Hard disk 3       Virtual Disk       16 GB       Image: COS: 512 MB.       Image: COS: 512 MB.         Image: Proverse adapter 1       VM Network 2       4 GB       Image: COS: 512 MB.       Image: COS: 512 MB.         Image: Serial port 1       telnet://:6004       2 GB       Image: COS: 512 MB.       Image: COS: 512 MB.         Image: Serial port 1       telnet://:6004       2 GB	Hardware Options Resources	1		Virtual Machine Version:	: 8
Hardware       Summary       Memory       8192 MB       S12 GB       Memory Stze:         Memory       8192 MB       512 GB       Memory Stze:       Maximum recommended for         Video card       Video card       128 GB       Maximum recommended for         VMCI device       Restricted       128 GB       Maximum recommended for         SSSI controller 0       LSI Logic Parallel       64 GB       Maximum recommended for         CD/DVD drive 1       Client Device       64 GB       Maximum recommended for         Hard disk 1       Virtual Disk       32 GB       Default recommended for         Hard disk 2       Virtual Disk       16 GB       Minimum recommended for         Hard disk 3       Virtual Disk       16 GB       Minimum recommended for         Hard disk 3       Virtual Disk       16 GB       Minimum recommended for         Hard disk 3       Virtual Disk       16 GB       Minimum recommended for         Network adapter 1       VM Network 2       4 GB       Minimum recommended for         Network adapter 3       VM Network 3       2 GB       Minimum recommended for         Serial port 1       tehnet://:6004       2 GB       1 GB         St2 MB       256 MB       256 MB       256 MB <th>Show All Devices</th> <th>Add</th> <th>1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 -</th> <th></th> <th></th>	Show All Devices	Add	1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 -		
64 MB 32 MB 16 MB 8 MB	Memory CPUs Video card VMCI device SCSI controller 0 CD/DVD drive 1 Hard disk 1 Hard disk 2 Hard disk 3 Floppy drive 1 Network adapter 1 Network adapter 2 Network adapter 3	8192 MB 3 Video card Restricted LSI Logic Parallel Client Device Virtual Disk Virtual Disk Virtual Disk Client Device VM Network VM Network 2 VM Network 3	512 68 - 296 68 - 128 68 - 32 68 - 32 68 - 8 68 - 8 68 - 1 68 -	Memory Size: Maximum recommended for this guest OS: 1011 GB. Maximum recommended for best performance: 130964 MB. Default recommended for this guest OS: 2 GB. Minimum recommended for this	8

8. Power on the VM and AOS-W will migrate data from the old hard disk to the new one.

#### Figure 72 Migrating Data

Aruba Networks ArubaOS Version 8.0.0.0-sucs-ctrl (build 0000 × label Built by srini@localhost.localdomain on 2016-05-04 at Copyright (c) 2002-2016, Aruba, a Hewlett Packard Ente	13:11:48 IST (gcc version 4.7.2)
	Е ОК ] Е ОК ]
	СОК ] СОК ]
<	a MM >>>>>
	E NOT FOUND ] E ok j

9. Confirm if the newly added **Hard disk 3** is used by AOS-W. The **Hard disk 3** will be listed as **/dev/sdc1** and if old hard disk is in use, it will be listed as **/dev/sdb1**. If the OVF file only contains a single hard disk it be listed as **/dev/sda3**.

10. If the new **Hard disk 3** is working as expected, the older hard disk can be removed from the VM and deleted from disk of the vSphere server.

Figure 73 Removing a Hard Disk

Hardware Options Resource	47 - Virtual Machine Properties	Virtual Machine Version: 8
Show All Devices	Add Restore	This device has been marked for removal from
Hardware Memory CPUs Video card Video card SCSI controller 0 CD/DVD drive 1 Hard disk 1 Hard disk 2 (removing) Hard disk 3 Floppy drive 1 Network adapter 1 Network adapter 2 Network adapter 3 Serial port 1	Summary         8192 MB         3         Video card         Restricted         LSI Logic Parallel         Client Device         Virtual Disk         Removed         Virtual Disk         Client Device         VM Network         VM Network 2         VM Network 3         telnet://:6004	To cancel the removal, click the Restore button.  Removal Options  Remove from virtual machine  Remove from virtual machine and delete
Help		OK Cancel



AOS-W supports only 3 disks and the size of the new disk that is added should be more than the current disk size.

# **Backing up and Restoring Critical Data**

It is important to frequently back up all critical configuration data and files on the compact flash file system to an external server or mass storage device. Ensure the following files are backed up regularly:

- Configuration data
- WMS database
- Local user database

- Licensing database
- Floor plan JPEGs
- Custom captive portal pages
- x.509 Certificates
- Switch Logs

## Back Up and Restore Compact Flash in the WebUI

The WebUI provides the easiest way to back up and restore the entire compact flash file system. The following steps describe how to back up and restore the compact flash file system using the WebUI on the Mobility Master:

1. Click on the **Configuration** tab.

2. Click **Pending Configuration** and then **Deploy Changes**. **Pending Changes** is visible only when there changes to be saved, if this option is not visible skip this step.

3. Navigate to the **Diagnostics > Technical Support > Backup Flash** page.

4. Click **Create Backup** to back up the contents of the compact flash file system to the flashbackup.tar.gz file.

5. Click **Copy Backup** to copy the file to an external server.

You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Diagnostics > Technical Support > Copy Files** page.

6. To restore the backup file to the compact flash file system, navigate to the **Diagnostics > Technical Support > Restore Flash** page. Click **Restore**.

## Back Up and Restore Compact Flash in the CLI

The following steps describe the backup and restore procedure for the entire compact flash file system using the Switch's command line:

1. Enter **config** mode in the CLI on the Switch, and enter the following command:

(host) [mynode] (config) #write memory

2. Use the backup command to back up the contents of the compact flash file system to the **flashbackup.tar.gz file**.

(host) [mynode] (config)# backup flash
Please wait while we tar relevant files from flash...
Please wait while we compress the tar file...
Checking for free space on flash...
Copying file to flash...
File flashbackup.tar.gz created successfully on flash.

3. Use the copy command to transfer the backup flash file to an external server or storage device:

(host) [mynode] (config) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername>
<ftpuserpassword> <remote directory>

(host) [mynode] (config) copy flash: flashbackup.tar.gz usb: partition <partition-number>

You can later transfer the backup flash file from the external server or storage device to the compact flash file system with the copy command:

(host) [mynode] (config) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
(host) [mynode] (config) # copy usb: partition <partition-number> <filename> flash:
flashbackup.tar.gz

4. Use the restore command to untar and extract the flashbackup.tar.gz file to the compact flash file system:

(host) [mynode] (config) # restore flash

## **Back Up and Restore Configuration in the CLI**

The following steps describe the backup and restore procedure for the configuration file system using the Switch's command line:

1. Enter **config** mode in the CLI on the Switch, and execute the following command:

(host) [mynode] (config) #write memory

2. Use the backup command to back up the contents of the configuration file system to the **configbackup.tar.gz** file.

(host) [mynode] (config) # backup config
Please wait while we take the config backup.....
File configbackup.tar.gz created successfully on flash.
Please copy it out of the controller and delete it when done.

3. Use the copy command to transfer the backup configuration file system to an external server or storage device:

(host) [mynode] (config) copy flash: configbackup.tar.gz ftp: <ftphost> <ftpusername>
<ftpuserpassword> <remote directory>
(host) [mynode] (config) copy flash: configbackup.tar.gz usb: partition <partitionnumber>

You can later transfer the backup configuration file from the external server or storage device to the compact flash file system with the copy command:

(host) # copy tftp: <tftphost> <filename> flash: configbackup.tar.gz
(host) # copy usb: partition <partition-number> <filename> flash: configbackup.tar.gz

4. Use the restore command to untar and extract the **configbackup.tar.gz** file to restore the configuration:

```
(host) [mynode] (config) # restore config
Please wait while we restore the config backup.....
Config restored successfully.
Please reload (reboot) the controller for the new config to take effect.
```

## Snapshot

A VMware snapshot is a copy of the virtual machine's disk file (VMDK) at a given point in time. Snapshots provide a change log for the virtual disk and are used to restore a VM to a particular point in time when a failure or system error occurs.

A snapshot preserves the state and data of a VM at a specific point in time. A VM provides several operations for creating and managing snapshots and snapshot chains. These operations let you create snapshots, revert to any snapshot in the chain, and remove snapshots. For additional information about snapshots refer to the VMware kb article

https://kb.vmware.com/selfservice/microsites/search.do?language=en\_ US&cmd=displayKC&externalId=1015180.

# **Implementing Management Interface**

This sections discusses implementation of the management interface on the Mobility Master. It includes the following:

- Assigning the IP address to the management interface from the CLI
- Ensuring management bound traffic uses the correct interfaces and a default gateway specific to the management interface
- Protecting the management interface against unwanted traffic and DOS attacks

Once the IP is assigned (manual or dynamic) we should be able to reach the management interface from anywhere in the network. This requires that we have a default gateway for the management interface. But this default gateway should not be used for the data routing table of the Switch. So the inherent problem is that we need to have two default gateways; one for the management interface and the other for the data traffic and the management traffic should be via the management interface only. This is solved by the use of the iproute2 utility and having a separate routing table with its own default gateway for the management IP. With this we can ensure that the management traffic does not leak onto unwanted interfaces.

The management interface is mapped to eth0 and is a Linux interface. It is not a part of SOS and does not have access to the SOS firewall to protect itself. Since the management interface is susceptible to attacks it is imperative that we should firewall this interface. For this we use the iptables firewall present in Linux. We allow only ssh (22), telnet(2323) ,tftp(69) and HTTPS(443,4343) traffic on the management interface and also rate limit traffic to protect Switch from unwanted traffic flood over the network. Initially phase of this feature is implemented for manually configuring a static IP for management interface from the console. It covers both IPv4 and IPv6 implementation. Most of the functional behavior and implementation are same for IPv4 and IPv6. This feature can be extended for obtaining IP dynamically from DHCP server in the network in future.

# **Datapath Debug Commands**

Listed below are the commands to view the system statistics of your Switch:

Execute the show datapath frame [counters] command to view statistics of the data traffic processed. This command displays the frame statistics that are received and transmitted from the datapath of the Switch. Allocated frames indicate buffers allocated at any given point of time. A constant increment in the buffer indicates a buffer leak.

The following example displays statistics of data traffic processed.

• Execute the **show port stats** command to view the traffic received/transmitted through gigabit ports using the datapath.

The following example displays the port statistics.

```
GE 0/0/0 6179766 46516 1192249262 3446810 0 0 0 0
GE 0/0/1 179 166996 14782 5019706 0 0 0 0
GE 0/0/2 0 0 0 0 0 0 0 0
```

Execute the **show datapath heartbeat stats** command to monitor the health of the systems. Heartbeats are sent from the control plane to the datapath every second. The packets pass through the datapath CPUs and return to the control plane in one second. If the load on the system increases or there is a CPU lock there is a possibility of the heartbeat being missed. If this recurs 30 times consecutively the Switch reboots. The heartbeat probe introduced in this release, sends out a probe when two consecutive heartbeats are missed and also measures the actual time taken for the packets to pass through the datapath CPUs and return to the control plane.

The following example displays the heartbeat statistics.

```
(host) #show datapath heartbeat stats
Sibyte HeartBeat Stats:
  Total HB sent: 42686
  Total HB send errors: 0
  Current HB send errors: 0 (max:30)
  HB send errors high water-mark: 0
Sibyte Probe Stats:
  Total probes sent: 0
  Last probe sent @ 0:00:00.000
```

Last probe rcvd @ 0:00:00.000

 Execute the show datapath dpdk [mempool-stats | ring-stats] command to view the DPDK mempool and ring statistics. Since the size of the mempool and ring may vary based on the system template this command identifies the size of the structures used.

The following example displays DPDK mempool and ring statistics.

```
(host) #show datapath dpdk mempool-stats
DPDK Memory Pool Statistics Table
mPoolName mPoolAddr Flags phyAddr Size hdrSize eltSize tSize priDataSize success bulk
success objs fail bulk fail objs cPoolCount
log history 0x2aaaaa802080 0 0x0xa9002080 512 64 2048 0 0 0 0 0 479
mbuf pool 0x2aaa36200000 0 0x0xa9400000 65536 64 4032 0 0 0 0 0 0 62935
msg 0x7fecd6700080 0 0x0x24700080 1024 64 40 24 0 0 0 0 1024
(host) #show datapath dpdk ring-stats
DPDK Ring Statistics Table
____ ____
Flags: Flag - set for single producer or consumer
Used - number of entries in a ring
Freed - number of free entries in a ring
QThreshold - Enqueque Threshold
nQSuccessBulk - Successful enqueues number
nQSuccessObjs - Objects successfully enqueued
nQFailBulk - Failed enqueues number
nQFailObjs - Objects that failed to be enqueued
dQSuccessBulk - Sucessful dequeues number
```

```
dQSuccessObjs - Objects successfully dequeued
dQFailBulk - Failed dequeues number
dQFailObjs - Objects that failed to be dequeued
RingName RingAddr Flag Used Freed QThreshold nQSuccessBulk nQSuccessObjs nQFailBulk
nQFailObjs dQSuccessBulk dQSuccessObjs dQFailBulk dQFailObjs
_____ ___ ____
                                                ___ _____
MP log history 0x2aaaaa800000 0 479 544 0 0 0 0 0 0 0 0 0
MP mbuf pool 0x7fecd6600000 0 62908 68163 0 0 0 0 0 0 0 0 0
core-0-low 0x2aaaaa98a5c0 2 0 1023 0 0 0 0 0 0 0 0 0
core-0-high 0x2aaaaa98c640 2 0 1023 0 0 0 0 0 0 0 0 0
core-1-low 0x2aaaaa98e6c0 2 0 1023 0 0 0 0 0 0 0 0 0
core-1-high 0x2aaaaa990740 2 0 1023 0 0 0 0 0 0 0 0 0
core-2-low 0x2aaaaa9927c0 2 0 1023 0 0 0 0 0 0 0 0 0
core-2-high 0x2aaaaa994840 2 0 1023 0 0 0 0 0 0 0 0 0
```

- MP\_msg 0x2aaaaa9968c0 0 1024 1023 0 0 0 0 0 0 0 0 0
- Execute the **show datapath utilization** command to view the CPU utilization of all the datapath CPUs (SP/FP).

The following example displays datapath CPU utilization statistics.

If the CPU speed is more than 2.1 GHz, data displayed under the **64 Secs** option is invalid, but valid only for **1 Sec** and **4 Sec** options. Counter inconsistency is only for CPUs with speed more than 2.1 GHz.

```
(host) #show datapath utilization
Datapath Network Processor Utilization
-----+
| Cpu utilization during past |
Cpu | 1 Sec 4 Secs 64 Secs |
-----+
1 | 0% | 0% | 0% |
2 | 0% | 0% | 0% |
```

• Execute the **show cpuload [current]** command to view the Switch's CPU load for application and system processes. Use the current option to check the output of the top two UNIX commands.

The following example shows that the majority of the Switch's CPU resources are not being used by either the application (user) or system processes.

(host) #show cpuload user 6.9%, system 7.7%, idle 85.4%

The following example displays the summary of system (CPU) load. When the current option is used, it displays detailed information of the CPU load for each process.

```
(host) #show cpuload [current]
top2 - 05:09:29 up 2 days, 9 min, 0 users, load average: 0.00, 0.01, 0.05
Tasks: 132 total, 2 running, 130 sleeping, 0 stopped, 0 zombie
Cpu(s): 2.5%us, 1.5%sy, 0.0%ni, 96.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 7915932k total, 2817304k used, 5098628k free, 2744k buffers
Swap: 0k total, 0k used, 0k free, 193244k cached
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
3462 root 20 0 2134m 16m 7772 S 26 0.2 744:48.18 sos.shumway.elf
```

```
3654 root 20 0 56112 5856 4732 S 4 0.1 40:48.87 gsmmgr
3503 root 20 0 0 0 0 R 2 0.0 63:24.05 kni single
1 root 20 0 8340 676 572 S 0 0.0 0:00.92 init
2 root 20 0 0 0 0 S 0 0.0 0:00.00 kthreadd
3 root 20 0 0 0 0 S 0 0.0 0:00.22 ksoftirqd/0
5 root 20 0 0 0 0 S 0 0.0 0:02.02 kworker/u:0
6 root RT 0 0 0 0 S 0 0.0 0:00.00 migration/0
7 root RT 0 0 0 0 S 0 0.0 0:00.00 migration/1
8 root 20 0 0 0 0 S 0 0.0 0:01.94 kworker/1:0
9 root 20 0 0 0 0 S 0 0.0 0:07.79 ksoftirgd/1
10 root 20 0 0 0 0 S 0 0.0 0:01.26 kworker/0:1
11 root RT 0 0 0 0 S 0 0.0 0:00.00 migration/2
12 root 20 0 0 0 0 S 0 0.0 0:01.08 kworker/2:0
13 root 20 0 0 0 0 S 0 0.0 0:05.80 ksoftirqd/2
14 root 0 -20 0 0 0 S 0 0.0 0:00.00 cpuset
15 root 0 -20 0 0 0 S 0 0.0 0:00.00 khelper
16 root 0 -20 0 0 0 S 0 0.0 0:00.00 netns
...
```

# **Upgrading a Switch**

Follow the steps below to upgrade the Switch. You can upgrade the OS on the Switch either through WebUI or through the CLI. The following methods can be used to upgrade the OS on the Switch:

- TFTP
- FTP
- SCP
- Local File (This option is available while upgrading through WebUI)

Be sure to back up the Switches as described in <u>Backing up and Restoring Critical Data</u>.

In the WebUI:

1. In the Mobility Master node hierarchy, navigate to **Configuration > Upgrade > Software Management.** 

- 2. Choose the upgrade method.
- 3. If you are using TFTP, FTP, or SCP for upgrade enter the server IP address.
- 4. Enter the image file name.
- 5. Choose the partition to upgrade.
- 6. Select Yes to Reboot Controller After Upgrade.
- 7. Select Yes to Save Current Configuration Before Reboot.
- 8. Click Upgrade.

In the CLI:

Execute the following commands on the CLI to upgrade the OS:

For TFTP: (host) [mynode] (config)# copy tftp: <TFTP server IP address> <image file name>
system: partition <0 or 1>

For FTP: (host) [mynode] (config) # copy ftp: <FTP server IP address> <username> <image file
name> system: partition <0 or 1>

For SCP: (host) [mynode] (config) # copy scp: <SCP host IP address> <username> <image file
name> system: partition <0 or 1>

Once the image is uploaded in the flash, save the configuration and reload the Switch.

If the following error message is displayed, follow the steps above to reload the OS on both partitions.

## **Gracefully Shutting Down AOS-W VMs**

It is important to gracefully shutdown the guest AOS-W VM's to avoid database corruptions and other related issues. The following steps describe the process to perform a graceful shutdown in the VMware ESXi and KVM hypervisor.

### In the VMware ESXi Hypervisor

- 1. Right click the VM in the vSphere client.
- 2. Click **Power > Shut Down** Guest or **Power > Restart Guest**.

Figure 74 Graceful Shutdown in VMware ESXi Hypervisor

ArubaOS_MM_8.0.1.0-svcs-ctrl ArubaOS_VMC_55647_serial		Power	•	Pow	er On	Ctrl+B
ArubaOS_VMC_8.0.0.0_55647 Centos 6.5-dev-opt mig_fix clova_new_img_test tool_ova		Guešť Snapshot Open Console Edit Settings	•	Susp Rese	rer Off bend et t Down Guest	Ctrl+E Ctrl+Z Ctrl+T Ctrl+D
		Add Permission Ctrl+	Ρ	Rest	art Guest	Ctrl+R
		Report Performance		by creating a new		
		Rename				
		Open in New Window Ctrl+Alt+ Remove from Inventory Delete from Disk	N	pre-built v oftware alr an operat	eady	

## In the KVM Hypervisor

In the KVM hypervisor peform a graceful shutdown by either clicking click **Shut Down** or **Reboot**.

Figure 75 Graceful Shutdown in KVM Hypervisor

rhel7.1 Virtual Machine		×
File Virtual Machine View Send Key		
		¢
Reboot Shut Down Force Reset Force Off		
Save		

# Jumbo Frame Support

Jumbo frames are the data frames that are larger than 1500 bytes and includes the Layer 2 header and frame check sequence. Jumbo frames functionality can be configured on the following and can support up to 9216 bytes of payload:

- OmniAccess Mobility Controllers (OAW-40xx SeriesSwitches, OAW-4x50 SeriesSwitches, and Mobility Controller Virtual Appliances.
- Mobility Master (Mobility Master Virtual Appliance and hardware Mobility Master)

In centralized deployments, frames that are more than 1500 bytes in size are generated from the AP to the managed device during encryption and enabling AMSDU. Therefore, whenever the AP associates to the managed device, jumbo frames are used to get the highest network performance. If this functionality is not supported, the data frames gets fragmented, which reduces the overall throughput of the network and makes the network slow.



AOS-W supports jumbo frames between 11ac APs, OAW-40xx Series, OAW-4x50 Series Switches, and x86 platforms such as Mobility Controller Virtual Appliances, Mobility Master (Mobility Master Virtual Appliances, and hardware Mobility Masters.

Jumbo frames are not supported on Mobility Controller Virtual Appliances and Mobility Master Hardware Appliances running on Windows Hyper-V.

You can enable the jumbo frame support in the following scenarios:

- Tunnel node: In a tunneled node deployment, the wired clients connected on the tunneled nodes can send and receive the jumbo frames.
- L2 or L3 GRE tunnels: When you establish a GRE tunnel between two managed devices, the clients on one managed device can send and receive jumbo frames from the clients on the other managed device on enabling jumbo frames.
- **Between wired clients**: In a network where clients connect to the managed device with jumbo frames enabled ports can send and receive the jumbo frames.
- Wi-Fi tunnel: A Wi-Fi tunnel can support an AMSDU jumbo frame for an AP (the maximum MTU supported is up to 9216 bytes).



AMSDU is not supported on x86 platforms.

## **Limitations for Jumbo Frame Support**

This release of AOS-W does not support the jumbo frames for the following scenarios:

- IPsec, IPIP, and xSec.
- IPv6 fragmentation or reassembly.

## **Configuring Jumbo Frame Support**

You can use the CLI to configure the jumbo frame support.

To enable the jumbo frame support globally and to configure the MTU value:

(host) [mynode] (config) #firewall jumbo mtu <1789-9216>

You can configure the MTU value between 1789-9216. The default MTU value is 9216.

To enable jumbo frame support on a port channel:

(host) [mynode] (config) #interface port-channel <id> jumbo

#### To enable jumbo frame support on a port:

(host) [mynode] (config) #interface gigabitethernet <slot>/<module>/<port> jumbo



## Viewing the Jumbo Frame Support Status

Execute the following command to view the global status of the jumbo frame support: (host-vmc) [mynode] #show firewall

Execute the following command to view the jumbo frame status on a port:

(host-vmc) [mynode] #show interface gigabitethernet <slot>/module>/<port>

Execute the following command to view the jumbo frame status on a port channel:

(host-vmc) [mynode] #show interface port-channel <id>

### Enable/disable Jumbo Frame Support Globally and Configure MTU Value

(host) [mynode] (config) #firewall

(host) [mynode] (config-submode)#jumbo ?
mtu MTU of Jumbo frames on this platform (when enabled)
<cr>

(host) [mynode] (config-submode)#jumbo mtu ?
<1789-9216> MTU for Jumbo frames
(host-vmc) [mynode] (config-submode)#jumbo mtu 9216
(host-vmc) [mynode] (config-submode)#no jumbo

#### Enable/disable Jumbo Frame Support on a Port

(host-vmc) [mynode] (config) #interface gigabitethernet 0/0/0 (host-vmc) [mynode] (config-submode)#jumbo (host-vmc) [mynode] (config-submode)#no jumbo

#### Enable/disable Jumbo Frame Support on a Port Channel

(host-vmc) [mynode] (config) #interface port-channel 0 (host-vmc) [mynode] (config-submode)#jumbo (host-vmc) [mynode] (config-submode)#no jumbo