Aruba Mobility Master

Installation Guide

a Hewlett Packard
Enterprise company

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
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Contents

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 02	The following sections were updated: • Adding Licenses on page 26 • System Requirements on page 8 • Configuring the Initial Setup on page 23
Revision 01	Initial release.

This guide describes the Installation, Configuration and Troubleshooting steps for the Aruba Mobility Master.

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`	This fixed-width font depicts the following: • Sample screen output • System prompts • Filenames, software devices, and specific commands when mentioned in the text
`Commands`	In the command examples, this bold font depicts text that you must type exactly as shown.
<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.
`[Optional]`	Command examples enclosed in brackets are optional. Do not type the brackets.
`{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*

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	licensing.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

The Aruba Mobility Master provides a 64-bit virtualized software-based managed platform on VM architecture.

Mobility Master is the centralized management platform for deployment in a virtualized network infrastructure. The Mobility Master operates on VM platforms in VMware environments and can reside with other virtualized appliances.

Aruba does not recommend over subscription of processors, memory, and NIC ports on the virtual machine.

Listed below are some of the advantages of switching to a Mobility Master:

- The Mobility Master 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 Mobility Master, refer to the *ArubaOS 8.0.x Quick Start Guide* for steps to setup the network.

System Requirements

Listed below are the minimum hypervisor host system requirements for ArubaOS to run as a guest virtual machine (VM) and the resources required for the VM to be functional:

- Quad-core Core i5 1.9 GHz processors with hyper threading enabled
- 8 GB RAM
- Minimum 2 physical NICs on the ESXi host

ArubaOS VM Requirement

Listed below are the minimum resources required for the ArubaOS VM to function:

- 3 vCPUs
- 4 GB memory
- 10 GB disk space. For information on increasing the flash size, see Increasing Flash Size on page 9.
- 4 virtual NICs

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 ArubaOS. In instances where more than one VM is setup in a hypervisor, then:

- The number of logical processors reported on the ESXi (vSphere client) should be higher or equal to the sum of vCPUs allocated to each of the VMs setup in that host.
- The sum of the memory allocated to each VM should not exceed the overall host memory capacity reported.

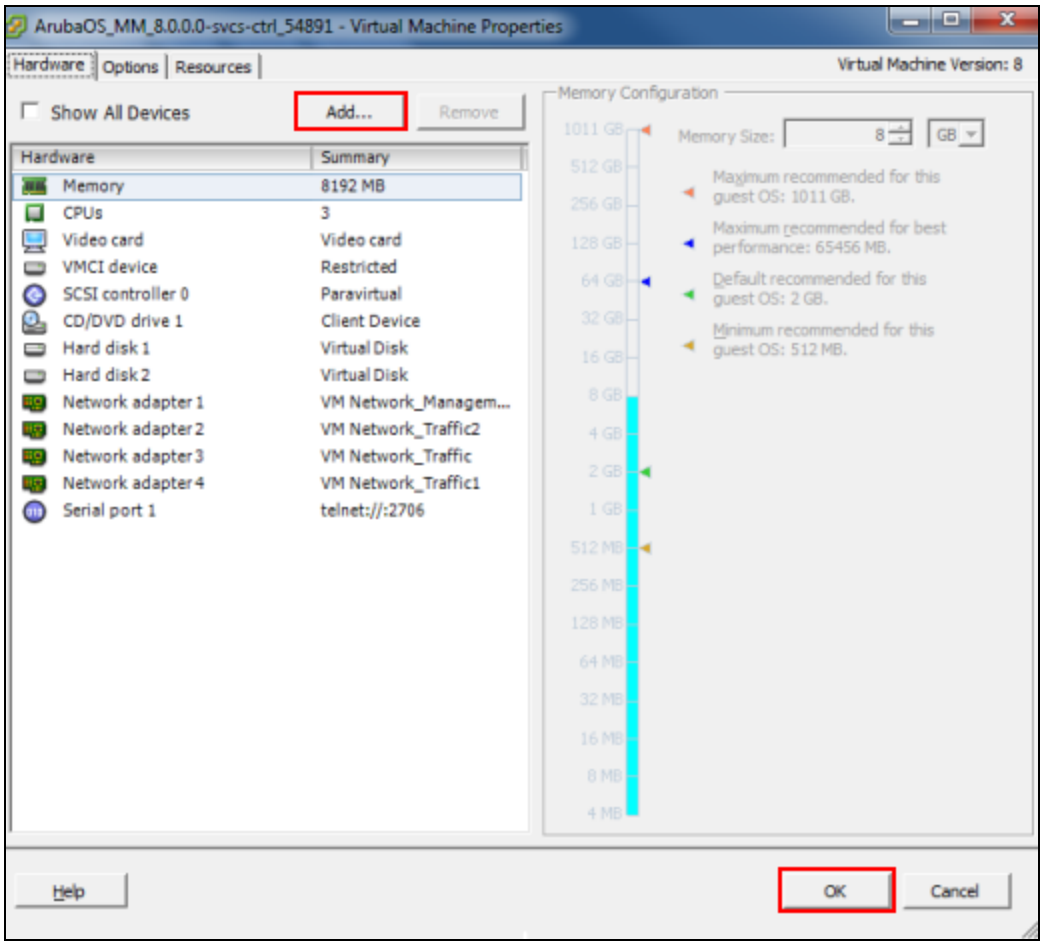
- The total CPU utilization, memory usage, and network throughput should not exceed 80% of the host capacity.
- One NIC is shared with ESXi Management and the second is reserved for datapath.

Increasing Flash Size

ArubaOS 8.0 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.

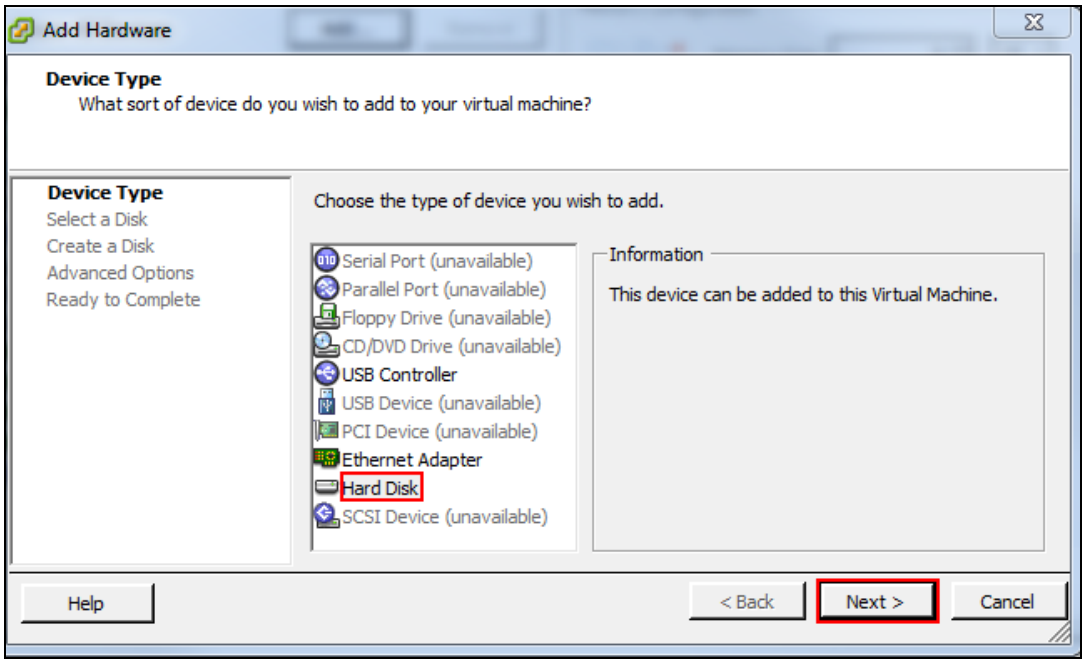
1. Power down the VM.
2. Right click the VM in the vSphere client and click **Edit Settings**.
3. Click **Add** in the **Virtual Machine Properties** window.

Figure 1 *Virtual Machine Properties*



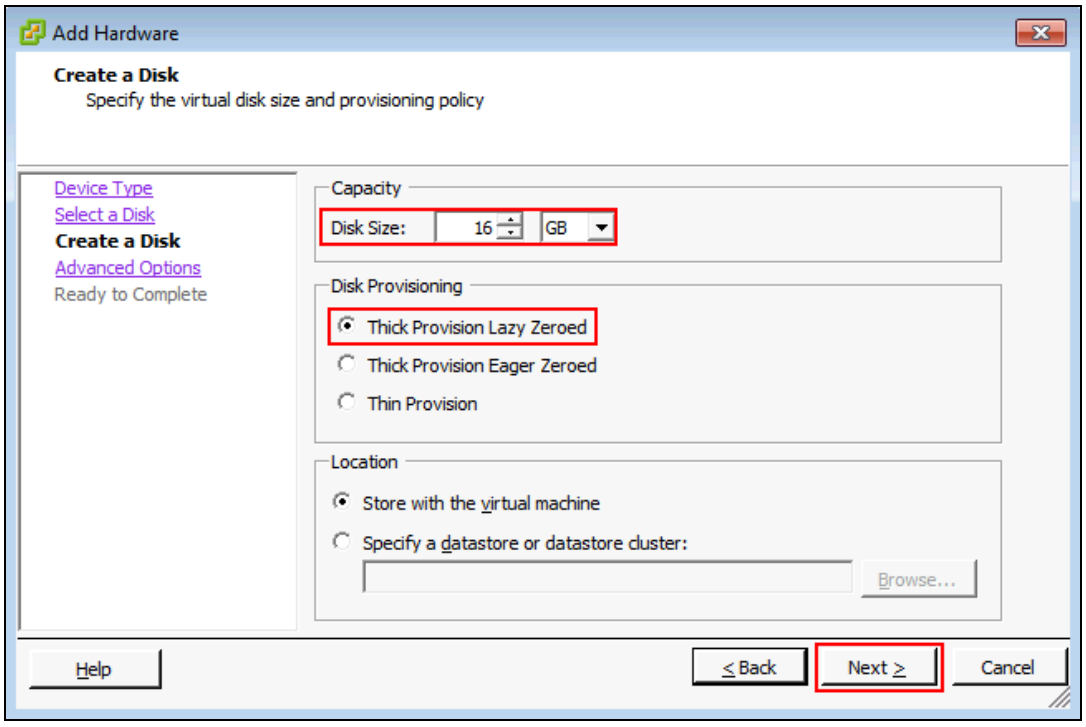
4. Click **Hard Disk** in the **Add Hardware** window and click **Next**.

Figure 2 *Selecting the Device Type*



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 3 *Create Disk*



7. Click **Next** in the **Advanced Options** window and click **Finish**.

Prerequisites

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

- vSphere Client/vCenter 5.1 or 5.5 is installed on a Windows machine.
- vSphere Hypervisor 5.1 or 5.5 is installed on the server that hosts the Mobility Master as a guest.
- OVF template is obtained from an Aruba representative and accessible from vSphere Client/vCenter.

Logging Into ESXi Host Using vSphere Client

NOTE

This section describes the configuration of the VM using the vSphere Windows client, if vCenter infrastructure is available the same can be achieved through the web interface provided by vCenter.

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

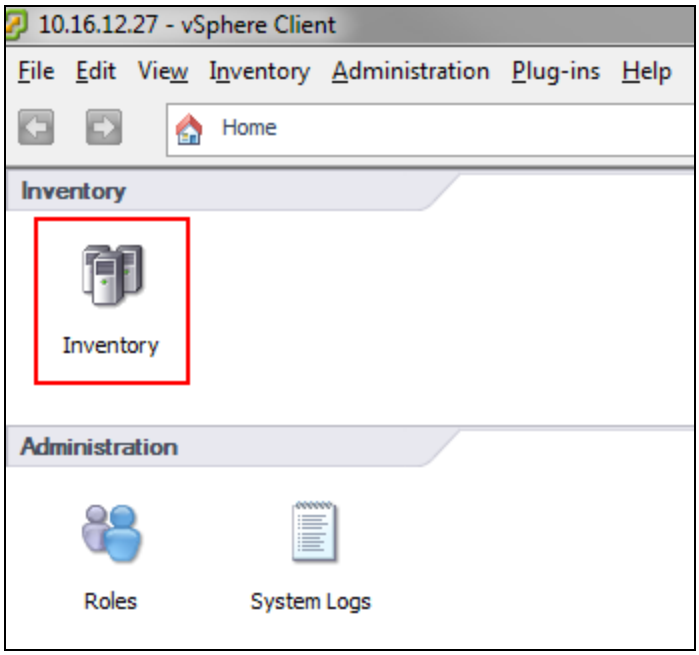
1. Open the vSphere Client.
2. Enter the IP address or name of the vSphere Hypervisor in the **IP address / Name** field.
3. Enter the user name in the **User name** field.
4. Enter the password in the **Password** field.
5. Click **Login**.
   The **vSphere Client** page is displayed.

Creating A VM Network For Management

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

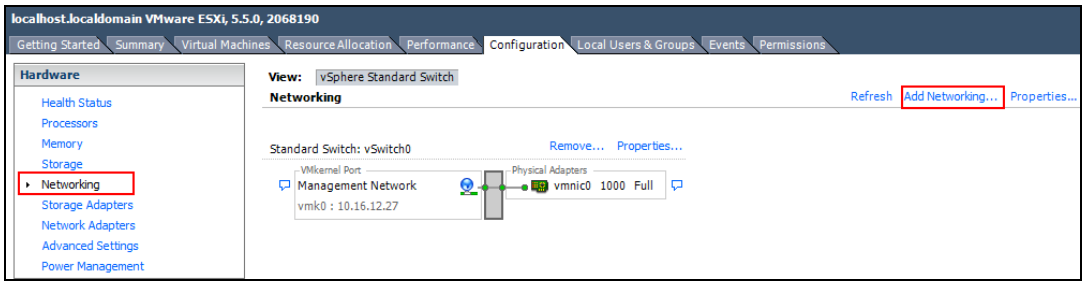
1. Log in to the vSphere ESXi Host using vSphere Client. For additional information, see Logging Into ESXi Host Using vSphere Client.
2. From the vSphere Client page, click **Inventory**.

Figure 4 *Inventory Button*



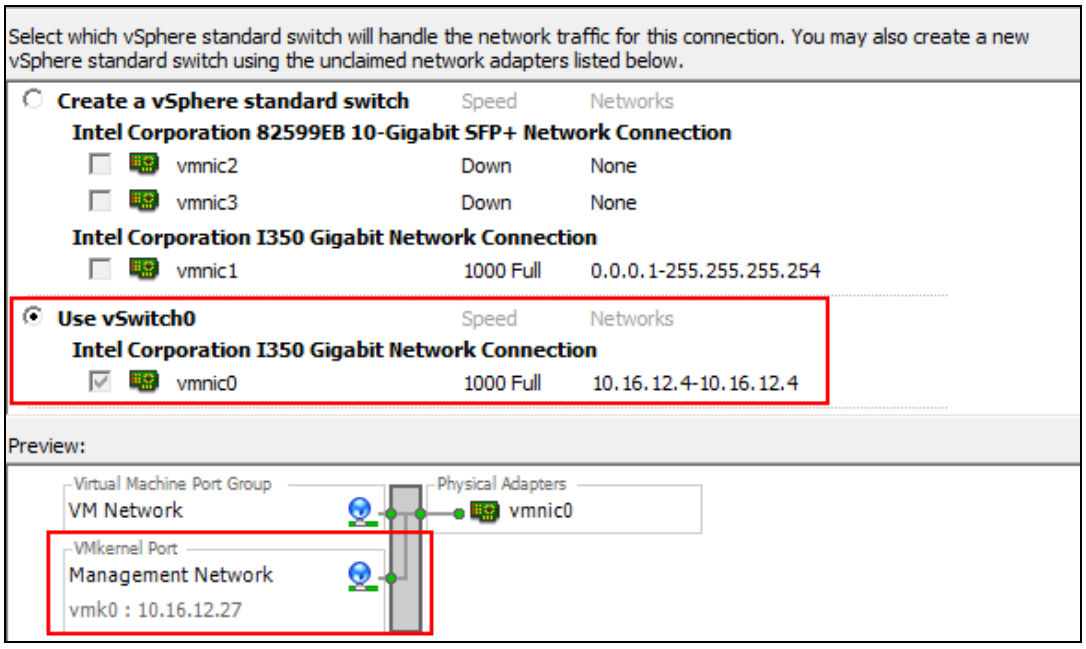
3. Click **Configuration** tab.
4. Click **Networking** from the **Hardware** menu.
5. Click **Add Networking.**
   The **Add Network Wizard** is displayed.

Figure 5 *Adding A Network*



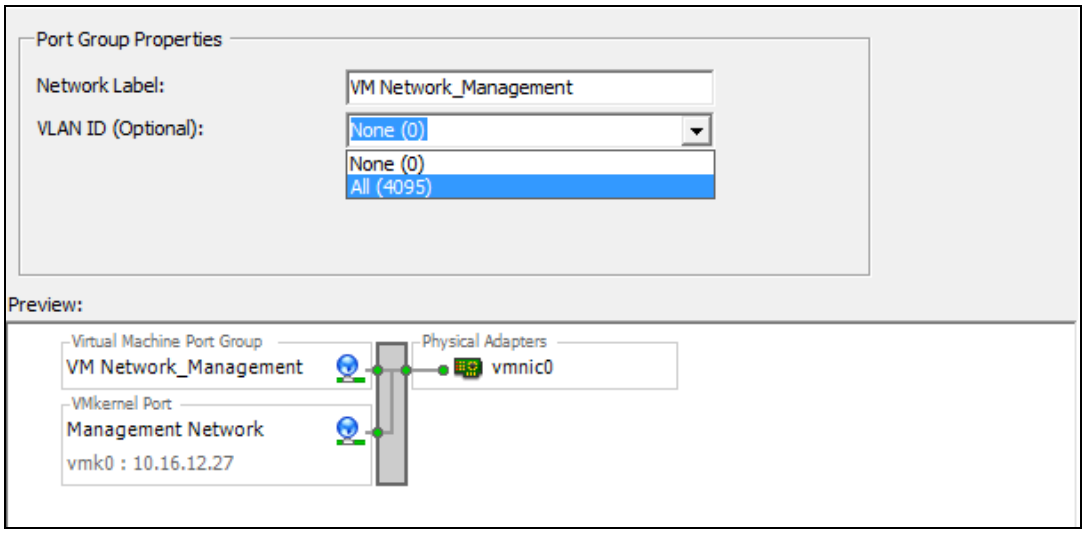
6. Select the **Virtual Machine** option and click **Next**.
7. Select the **vSwitch** that has **VMkernel** port mapped for ESXi management network and click **Next**.

Figure 6 *Selecting A Network Adapter For Management*



8. 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**.

Figure 7 *Selecting Port Group Properties*



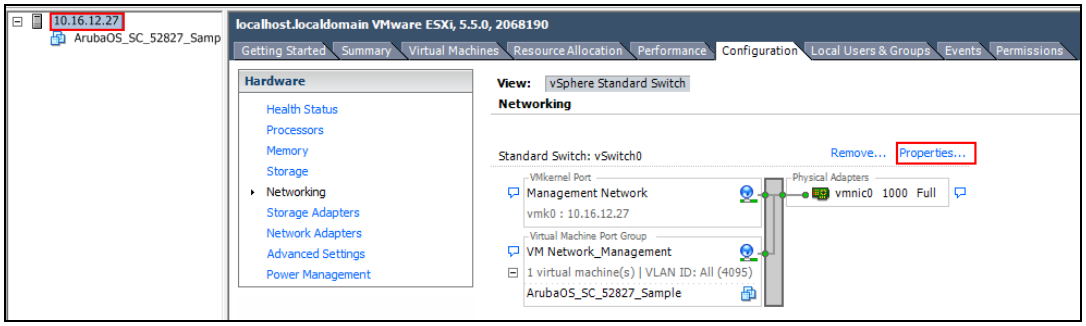
9. Click **Finish**.

NOTE

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

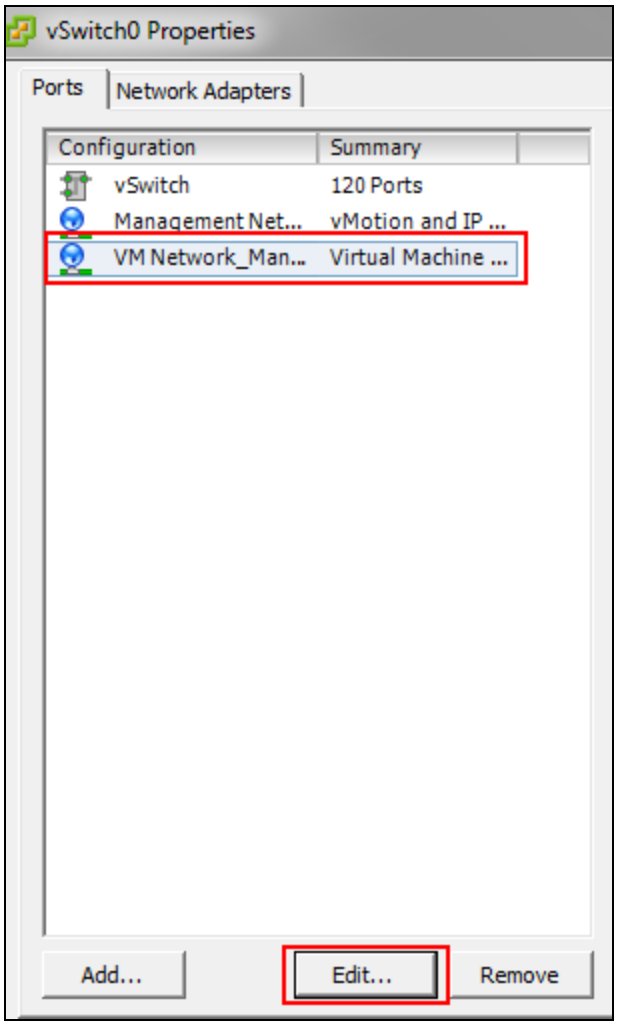
10. Click the ESXi host IP address.
11. Click the **Configuration** tab.
12. Click **Networking** from the **Hardware** section.
13. Click **Properties** of the **VM Network_Management**.

Figure 8 *VM Network Properties_Management*



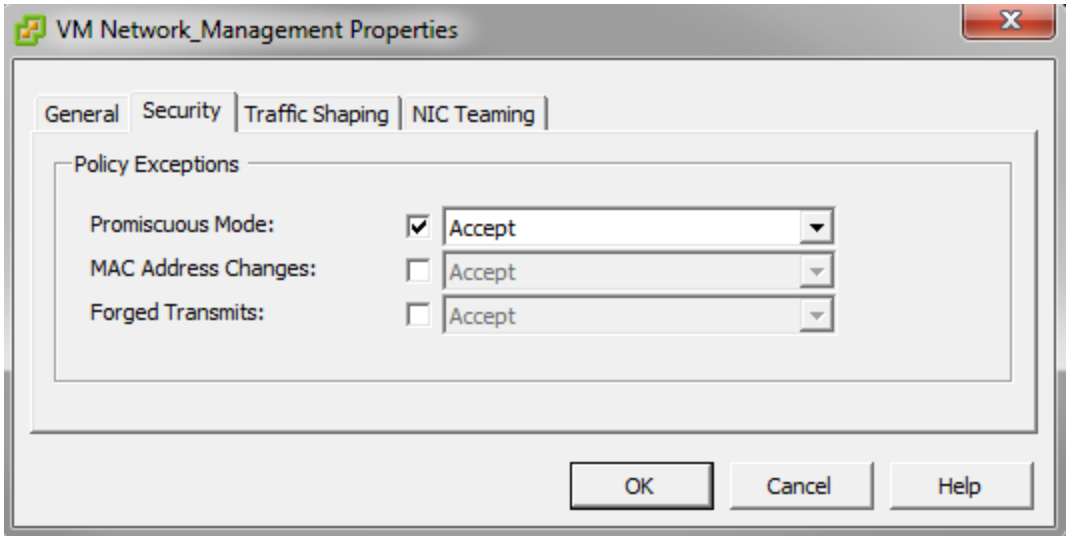
14. Select the port that was created earlier and click **Edit**.

Figure 9 *Edit Network Properties_Management*



15. Select the **Promiscuous Mode** check box and **Accept** from the drop-down list.

Figure 10 *Selecting Promiscuous Mode*



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

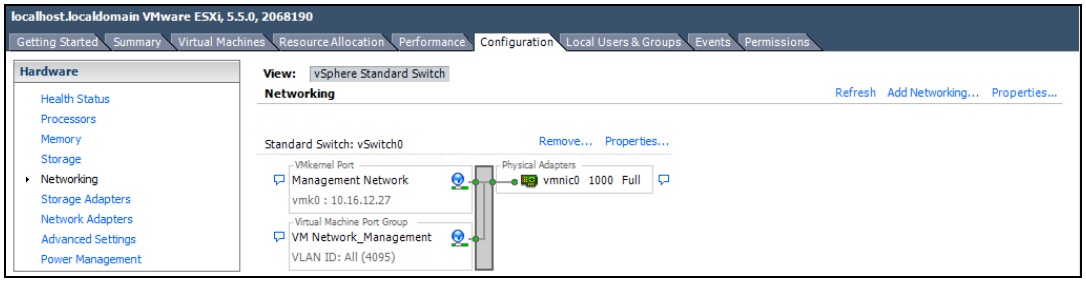
Creating VM Networks For Traffic

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.**

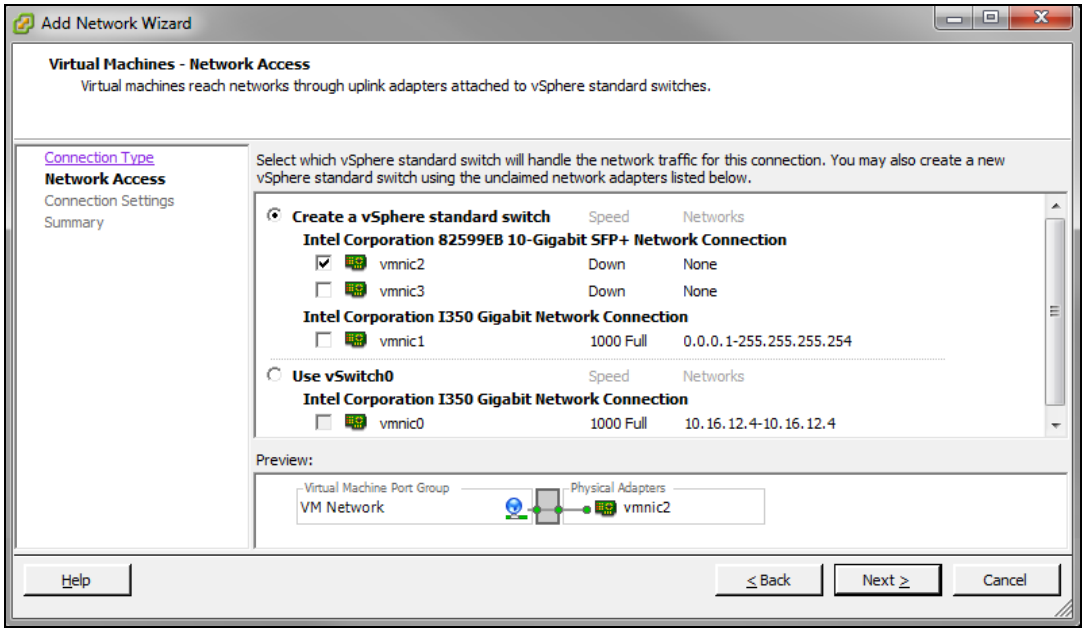
   The **Add Network Wizard** is displayed.

Figure 11 *Adding A Network For Traffic*



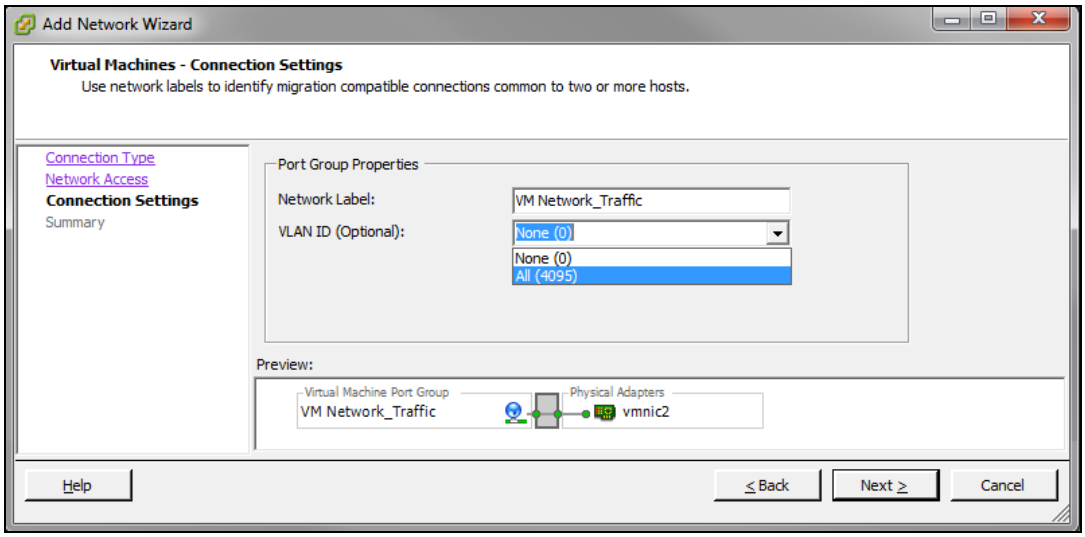
3. Select the **Virtual Machine** option and click **Next**.
4. Select a **vSwitch** that will handle the network traffic and click **Next**.

Figure 12 *Selecting A Network Adapter For Traffic*



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**.

Figure 13 *Selecting Port Group Properties*



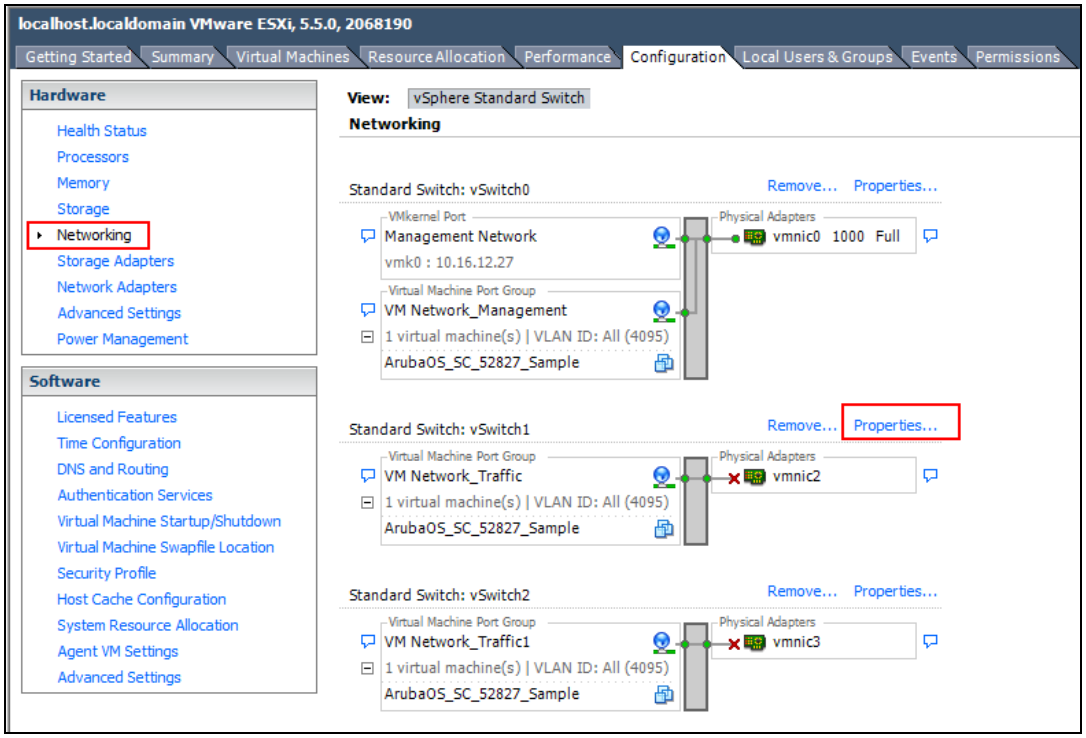
6. Click **Finish**.

NOTE

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

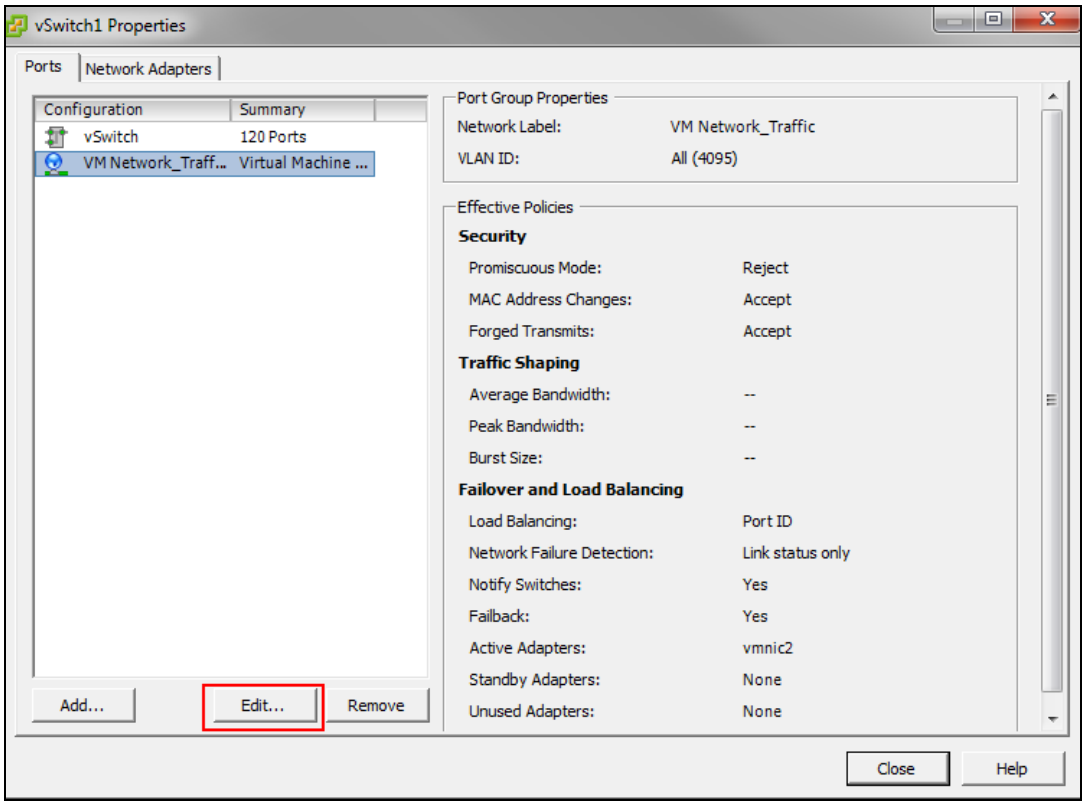
7. Click the ESXi host IP address.
8. Click the **Configuration** tab.
9. Click **Networking** from the **Hardware** section.
10. Click **Properties** of the vSwitch to edit.

Figure 14 *VM Network Properties_Traffic*



11. Select the port that was created earlier and click **Edit**

Figure 15 *Edit Network Properties_Traffic*



12. Select the **Promiscuous Mode** check box and **Accept** from the drop-down list.
13. Click **OK**.
14. Click **Close**.

Repeat the steps to enable Promiscuous mode on the other two networks.

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 Logging Into ESXi Host Using vSphere Client.
2. Click **File > Deploy OVF Template**.
   The **Deploy OVF Template Wizard** is displayed.

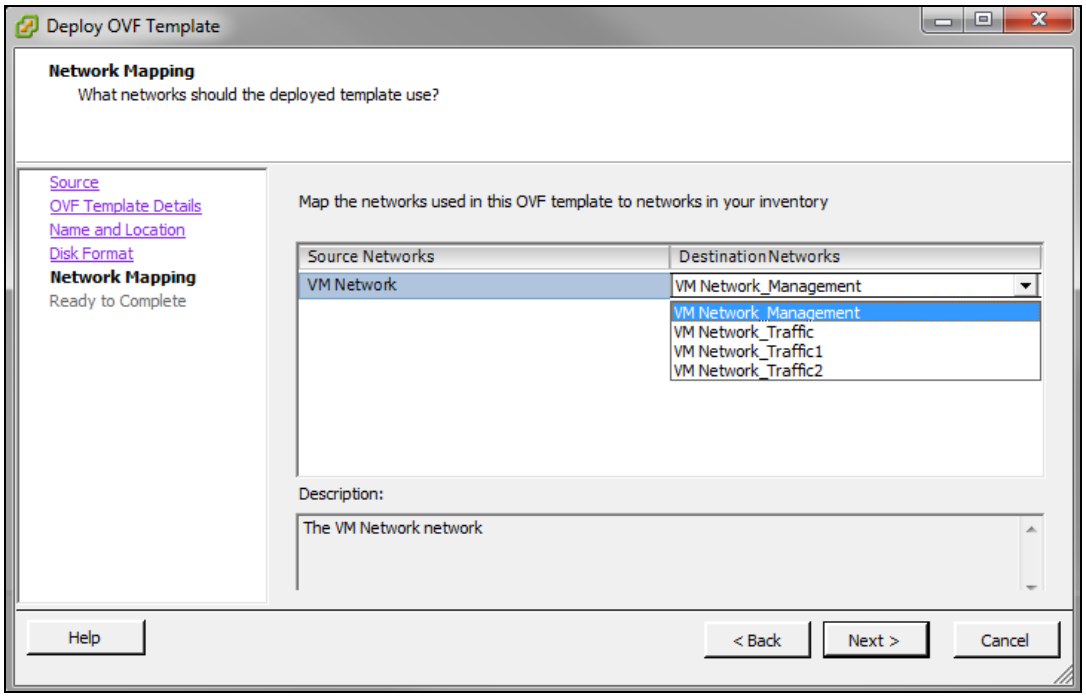
NOTE

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 in the left pane is displayed.
4. Click **Next**.
   The **Name and Location** option in the left pane is displayed.
5. In the **Name** field, enter a name for the OVF template and click **Next**.
   The **Disk Format** option in the left pane is displayed.
6. Select **Thick Provision Lazy Zeroed** option and click **Next**.
   The **Network Mapping** option in the left pane is displayed.

7. Select **VM Network_Management** from the Network Label drop-down list and click **Next**.
   The **Ready to Complete** option in the left pane is displayed.

Figure 16 *Network Mapping*



Review your preferences before clicking **Finish**.

NOTE

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.

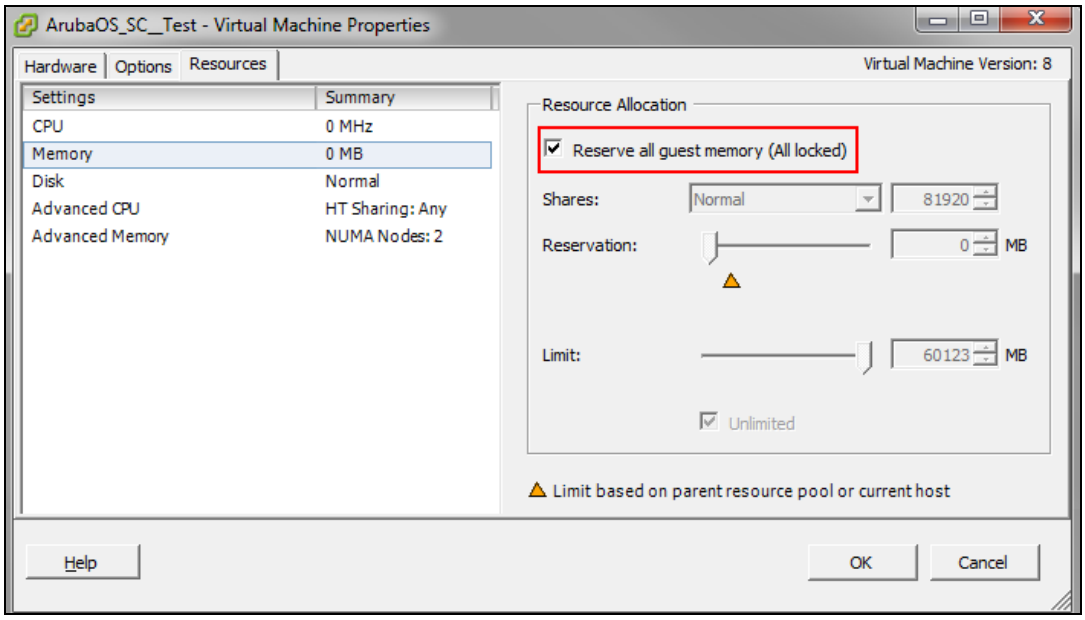
9. Click **OK**.
10. Click **Close**.

Pre-Allocating Memory in Aruba Mobility Master

Follow the steps below to pre-allocate memory in Aruba Mobility Master:

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 17 *Editing Memory Settings*



NOTE

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

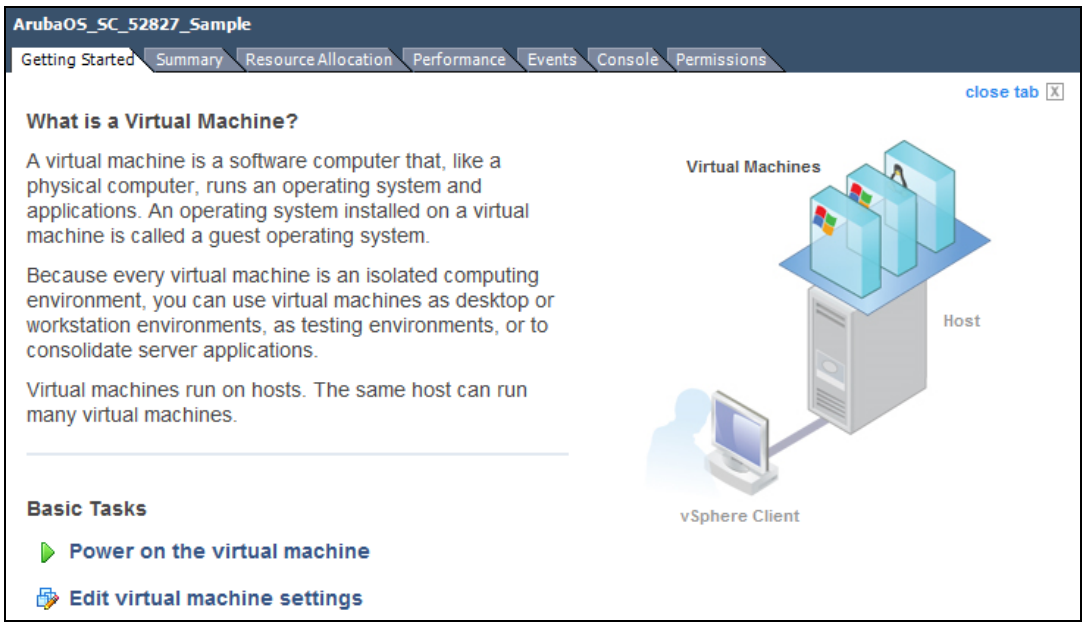
Assigning Network Connections

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:

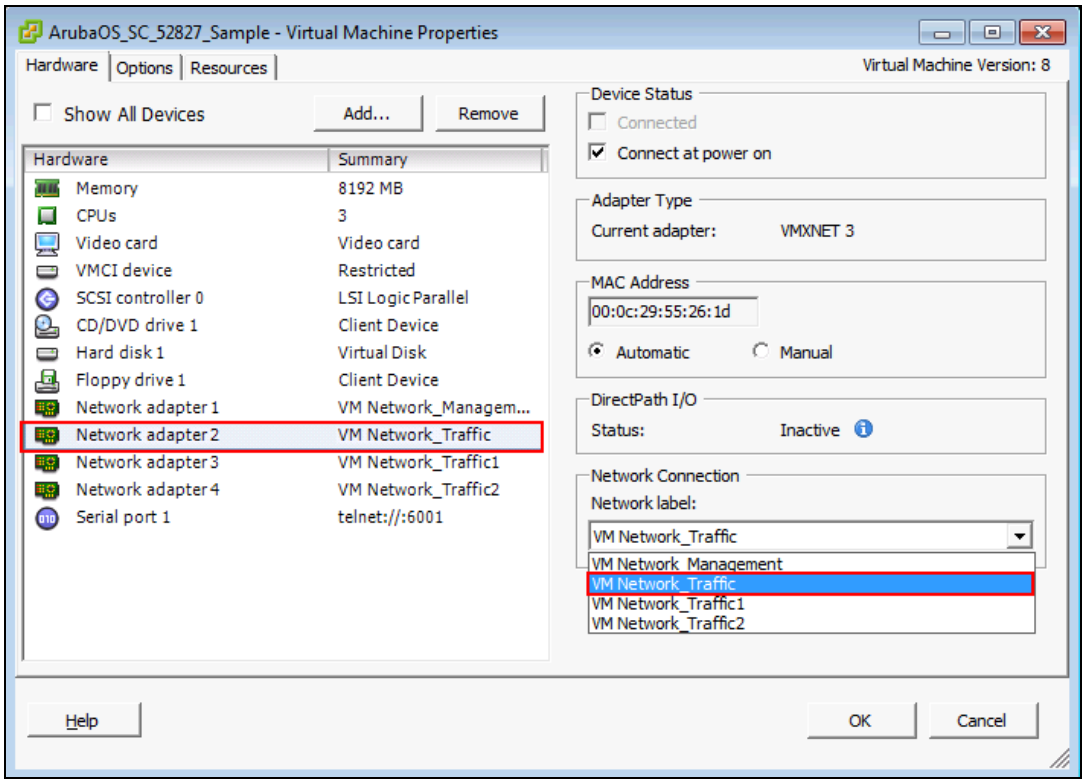
1. Click **Edit virtual machine settings**.

Figure 18 *Virtual Machine Settings*



2. Select **Network adapter2** and select **VM Network_Traffic** from the **Network label** drop-down list.

Figure 19 *Assigning A Network*



3. Repeat the steps and assign:
   a. **Network adapter3** to **VM Network_Traffic1**
   b. **Network adapter4** to **VM Network_Traffic2**
4. Click **OK**.

NOTE

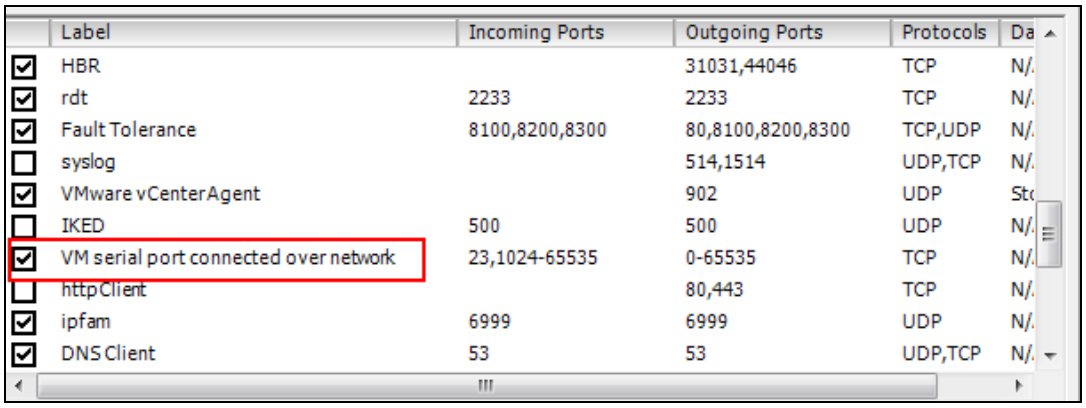
The Mobility Master does not support more than four interfaces.

Enabling Security Profile Configuration

Before configuring the serial console for the VM ensure the security profile configuration is enabled to allow serial port communication over 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. Scroll down to **VM serial port connected over network** and ensure that the check box is selected.

Figure 20 *Enabling VM Serial Port Connected Over Network*



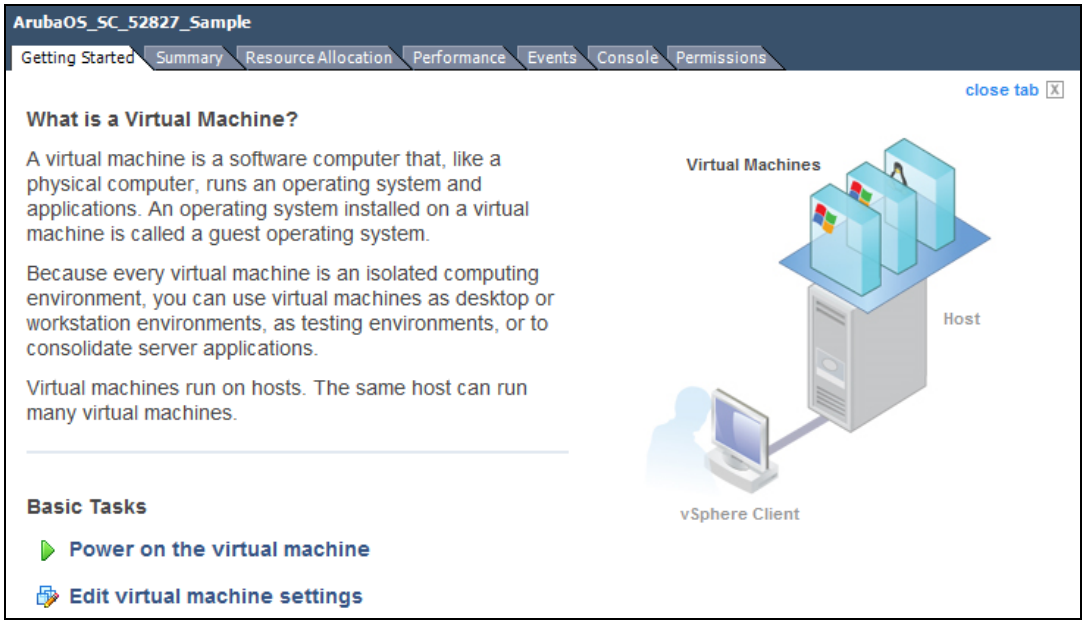
6. Click **OK**.

Configuring Serial Console for the VM

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

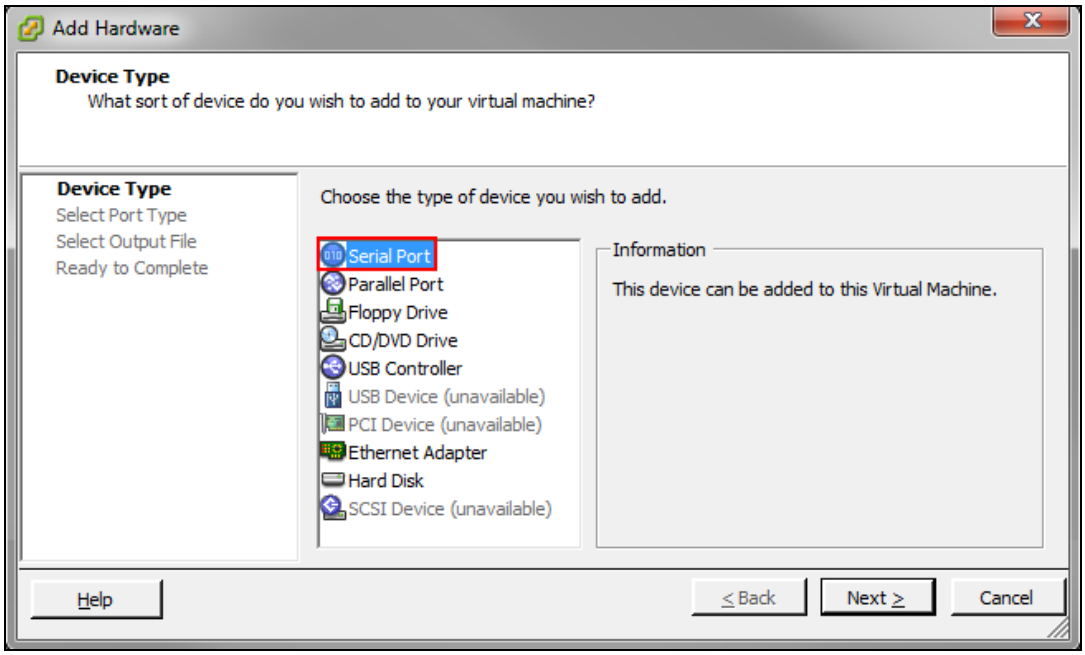
1. Click **Edit virtual machine settings**.

Figure 21 *Edit Virtual Machine Settings*



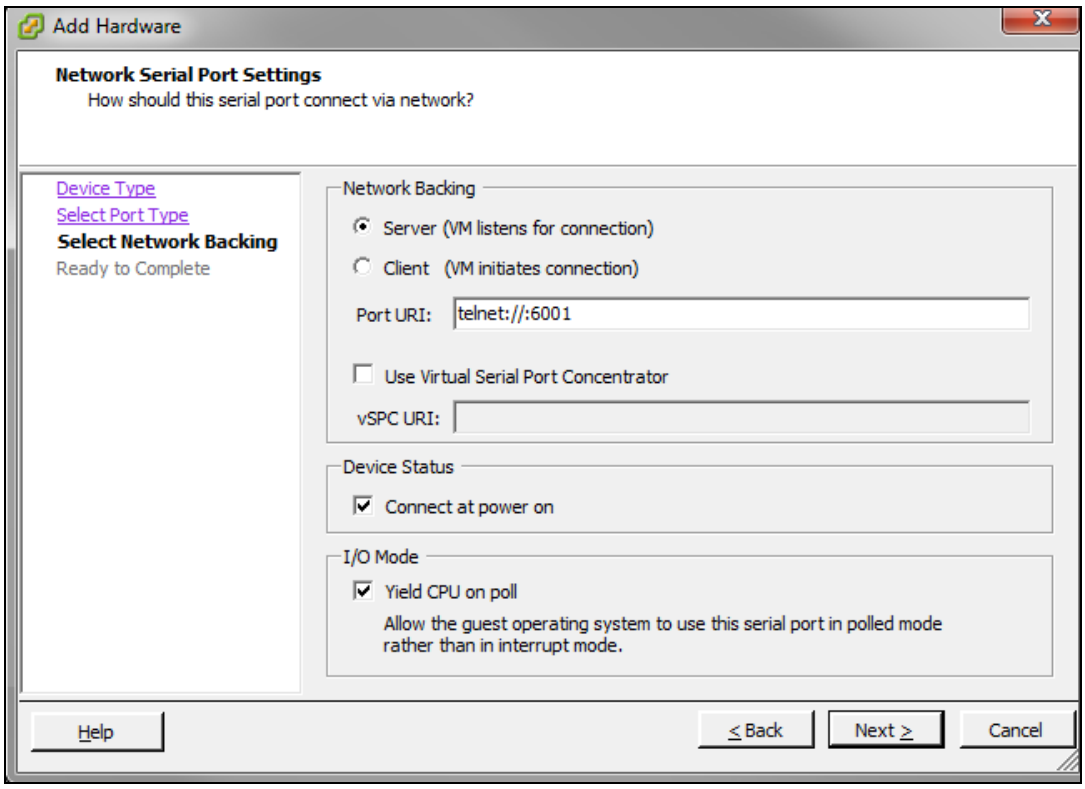
2. On the **Hardware** tab, click **Add**.
3. Select **Serial Port** and click **Next**.
4. Select **Connect via Network** and click **Next.**

Figure 22 *Configuring Serial Console*



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

Figure 23 *Connecting The Serial Via Network*



6. Click **Finish > OK**.

NOTE

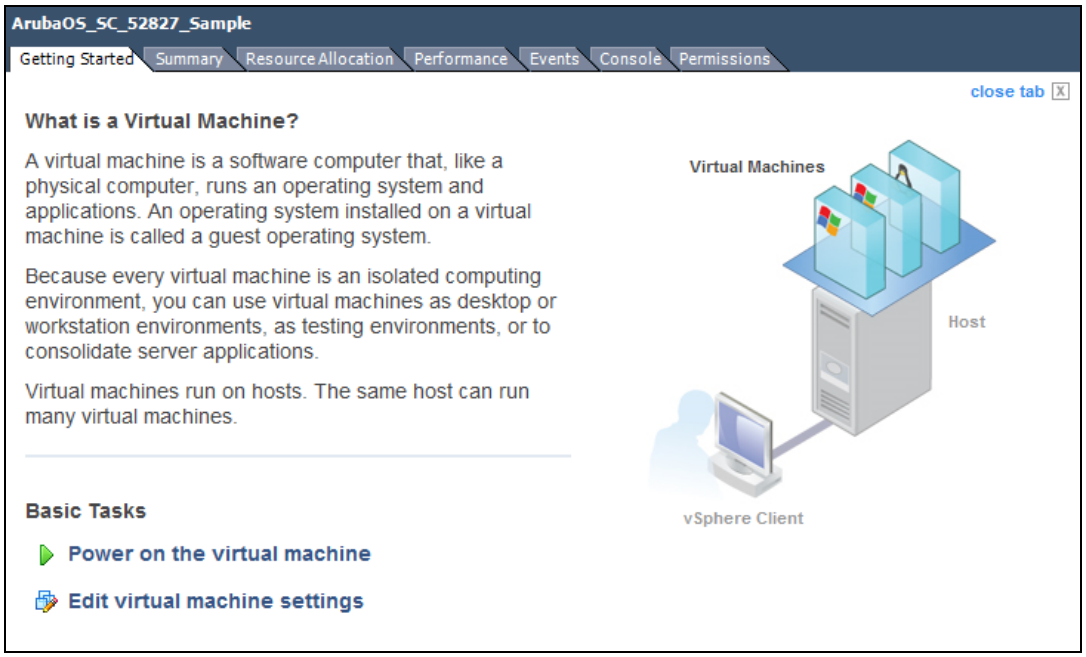
If more than one virtual machine is present, ensure that it is not connected to the same port.

Configuring the Initial Setup

Follow the steps below to configure initial setup:

1. Click **Power on the virtual machine**.

Figure 24 *Switching On The Virtual Machine*



2. Click the **Console** tab.
   The first boot dialogue is displayed.
3. Enter the following first boot parameters:
   - 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
   - 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
   - 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 setup. This should be a routable IP in an accessible subnet that the user can use to access the Mobility Master via CLI (SSH) or Web GUI (HTTP) after VM setup is complete.

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

4. Enter **Yes** to accept the changes. The Mobility Master reboots and displays the log in prompt.
5. Log in with user name as admin and the use password set in Step 3.
6. Execute the **enable** command.
7. Power on the Mobility Master and execute the following command to enable the serial console.

```
(host) #serial console redirect enable
```

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

```
(host) #show serial console redirect
               Serial Console Redirect : 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 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 Aruba Mobility Master 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.

Seamless Logon

The Seamless Logon feature enables you to login from the Mobility Master to a managed device without entering a password. The user can remotely login from a centralized location (Mobility Master) to any managed device and execute any show commands.

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

IPv4:

```
(ArubaMM) [mynode] #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
(ArubaMM) [mynode] (config) #interface mgmt
(ArubaMM) [mynode] (config-submode)#ip address 10.16.9.203 255.255.255.0
```

IPv6:

```
(ArubaMM) [mynode] (config) #interface mgmt
(ArubaMM) [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

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

IPv6:

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

Syntax

Parameter	Description
<cost>	Distance metric for the specified route.
mgmt	Specify the nexthop to indicate that the default gateway is for management interface.

Troubleshooting

Listed below are the commands to troubleshoot issues that occur with management interface:

Execute the **show interface mgmt** command to view the management IP address and default gateway.

```
(ArubaMM) [mynode] (config) #show interface mgmt
```

Execute the **show log errorlog all** command to view the log files for the configuration errors in routes and firewall rules.

```
(ArubaMM) [mynode] (config) #show log errorlog all
```

The Aruba licensing system is controller based. The license key is a combination of unique alphanumerical strings and special characters generated using the controller's serial number and is valid only for that controller. This section describes how to generate and install the licenses using the CLI and WebUI.

Aruba Mobility Master does not support adding the serial number or generating a passphrase from the WebUI.

In the CLI

1. Execute the **show inventory** command to obtain the passphrase.

```
(ArubaMM) [mynode] #show inventory

Mgmt Port HW MAC Addr           : 00:0C:29:CC:7B:70
HW MAC Addr                     : 00:0C:29:CC:7B:7A
Product key#                    : MMDCC7B70
Activate license                : Not applicable
Supported device type           : MM
Active device type              : MM
```

2. Access the Aruba License Management System (LMS), using your login credentials.
3. Navigate to **Activate Certificates** tab. Select **Mobility Controller** from the **ProductType** drop-down list.
4. Enter the following information in the respective fields:

- Virtual Mobility Serial Number
- Passphrase
- Certificate IDs
- Location (optional)

  Add all the certificates required for the Aruba Mobility Master.

5. Select the **Yes** option to acknowledge the **End-User Software License Agreement**.

To add another controller click **Another Controller**.

6. Click **Activate Certificates.**

   You will receive an email with the activation key and other license keys that were requested.
7. Install the Aruba Mobility Master capability license (for example, LIC-ASC-xx) using **license add** command.

```
(ArubaMM) [mynode] (config) #license add kNpWMoKA-AfP5H6GZ-G/OtC323-08mqBGaP-GuiXfnIG-
bw6JYM0W-Hq5a7BDG-8/Dk0Nyi-0z7AiBy0-a5s
```

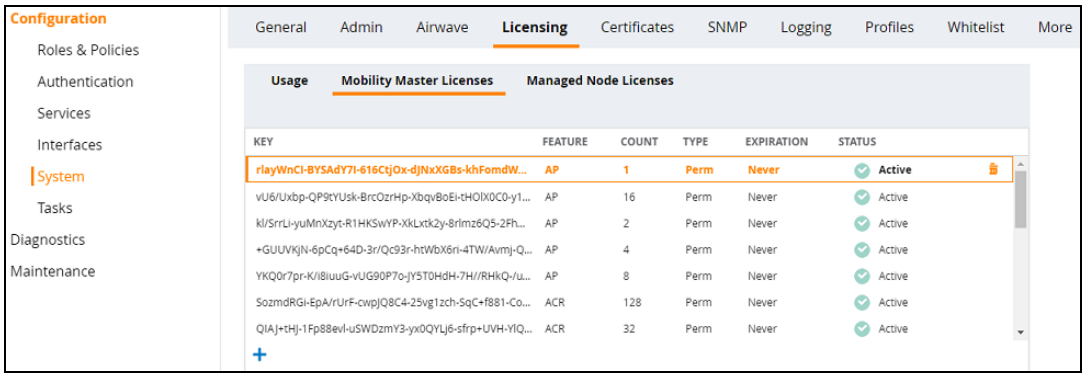
8. Reload the Aruba Mobility Master for the new service key to take effect.
9. Install the license using **license add** command.
10. Install the remote licenses using **license add remote** command.

In the WebUI

Follow the steps below to install licenses using the WebUI:

1. Access the Aruba login page and enter the **User** and **Password** details.
2. In the **Managed Network** node hierarchy, navigate to **Configuration > System > Licensing** tab.
3. Click **Mobility Master Licenses**.
4. Click the **+** symbol.

Figure 25 *Installing Licenses*



5. Enter the license key in the space provided.
6. Click **OK**.
7. Click **Submit**.
8. Click **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy changes.**

ARP Issues

Scenario

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.

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).
8. Click **OK**.

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 -l**.

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:

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
- Controller 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 controller's command line:

1. Enter **config** mode in the CLI on the controller, 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 config file system using the controller's command line:

1. Enter **config** mode in the CLI on the controller, and execute 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 **configbackup.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 configbackup.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: configbackup.tar.gz ftp: <ftphost> <ftpusername>
<ftpuserpassword> <remote directory>
(host) [mynode] (config) copy flash: configbackup.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) # 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 virtual machine at a specific point in time. A virtual machine 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 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 controller. 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 mgmt. interface and also rate limit traffic to protect controller 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 controller:

- 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 controller. 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.

```
(host) #show datapath frame counters
+----+------+-----------------------------------------------------+
|SUM/| | | |
|CPU | Addr | Description Value |
+----+------+-----------------------------------------------------+
| | [00] | Allocated Frames 3155 |
| | [03] | Unknown Unicast 127 |
| | [04] | IPv6 Unknown Unicast 5 |
+----+------+-----------------------------------------------------+
| | | |
| G | [00] | BPDUs Received 28 |
```

```
+----+------+-----------------------------------------------------+
```

- 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.

```
(host) #show port stats
Port Statistics
---- --------- ---------- ------- -------- --------------- ---------------- --------- -----
---
Port PacketsIn PacketsOut BytesIn BytesOut InputErrorBytes OutputErrorBytes CRCErrors
RxNoMbuf
---- --------- ---------- ------- -------- --------------- ---------------- --------- -----
---
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 controller 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 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 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
MP_mbuf_pool 0x7fecd6600000 0 62908 68163 0 0 0 0 0 0 0 0
core-0-low 0x2aaaaa98a5c0 2 0 1023 0 0 0 0 0 0 0 0
core-0-high 0x2aaaaa98c640 2 0 1023 0 0 0 0 0 0 0 0
core-1-low 0x2aaaaa98e6c0 2 0 1023 0 0 0 0 0 0 0 0
core-1-high 0x2aaaaa990740 2 0 1023 0 0 0 0 0 0 0 0
core-2-low 0x2aaaaa9927c0 2 0 1023 0 0 0 0 0 0 0 0
core-2-high 0x2aaaaa994840 2 0 1023 0 0 0 0 0 0 0 0
MP_msg 0x2aaaaa9968c0 0 1024 1023 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 controller'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 controller'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 ksoftirqd/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 Controller

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

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

Be sure to back up the controllers as described in Backing up and Restoring Critical Data.

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 controller.

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

```
(host) [mynode] (config)# show image version
Ancillary image stored on flash is not for this release
**********************************************************************
* WARNING:  An additional image upgrade is required to complete the *
* installation of the AP and WebUI files. Please upgrade the boot   *
* partition again and reload the controller.                        *
**********************************************************************
```