Technical Guide

Virtual AMF Appliance on VMWare vSphere for AMF Cloud-based Network Management

Installation and Technical Guidelines

Introduction

AMF Cloud™ allows your Allied Telesis Management Framework (AMF) Master and/or Controller to be virtual appliances, rather than integrated into an Allied Telesis switch or firewall. Enjoy AMF's comprehensive suite of features that combine to simplify network management across all supported network equipment from the core to the edge, and also take advantage of the additional powerful benefits that the cloud affords.

Deployment is more flexible with private or public cloud installation—use your own local server, or deploy fully online with Amazon web services. This guide describes how to deploy AMF Cloud using your own server, by installing the Virtual AMF Appliance (VAA) onto VMWare vSphere.

What is AMF virtualization?

AMF is a suite of features that combine to simplify network management across all supported network equipment from the core to the edge.

AMF provides simplified device recovery and firmware upgrade management. The primary function of AMF is to reduce the management and maintenance overhead on a network, while improving on responsiveness and handling of equipment failures within the network.

AMF Controller/Master functionality can be provided by a Allied Telesis Switch/Router device, or by a Virtual Machine. The Virtual Machine option allows the AMF network to be managed from either a local server, or from the Cloud.

This gives greater flexibility with regard to where the AMF management devices can physically reside, as they can be in remote locations away from other parts of the network.

AMF virtualisation has many other benefits common to virtual machines, such as excellent disaster recovery and rapid deployment.

The AlliedWare Plus software for the virtual machine is known as the Virtual AMF Appliance, or VAA. The VAA is an ISO image that

is loaded onto the virtual machine at boot up time. Once the VAA has loaded, the familiar AlliedWare Plus command-line interface (CLI) is available and network engineers can then use this CLI to configure and manage the virtual AMF Controller/Master.

Audience for this guide

This guide is intended for computer system administrators and network engineers. Moderate expertise in the field of hypervisors and virtual machine (VM) creation and configuration is highly recommended, at least to the level where the installer already knows how to create virtual machines.

This guide describes how to create a virtual machine for AMF Virtualisation. For further documentation of AMF configuration, including examples and command references, please see the links provided in the "Related documents" section below.

Related documents

The following documents give more information about AMF:

- AMF Feature Overview and Configuration Guide
- AMF Datasheet

These documents are available from the links above or on our website at alliedtelesis.com

Contents

How do I Obtain a VAA and Configure it?

To obtain and configure a VAA you need to:

Step 1: **Install a Hypervisor, the Operating System that Virtual Machines run on.**

Prerequisites and installation of the Hypervisor is described in "Prerequisites" on page 4.

Step 2: **Create and configure the Virtual Machine on a Hypervisor.**

Configuring a virtual machine is detailed in "Configuring a VAA Using VMware vSphere" on page 5.

Step 3: **License the VAA**

Licensing the VAA is detailed in "Obtaining and Installing the VAA Software License" on page 16.

Providing the Hypervisor that the VAA Runs On

Prerequisites

Allied Telesis' VAA supports the VMware hypervisor **VMware vSphere v6.0** or above to create and configure virtual machines (VMs) and manage virtual infrastructures.

This guide assumes that the customer knows either how to install VMware vSphere, or already has a host ready to install virtual machines for a VAA.

Physical Ethernet ports

One Ethernet port on the host machine will be configured for access from the VM Client. The addition of network interface cards (NICs) for VAA networking is recommended.

Hypervisor clock

Virtual machines are synced to the main hypervisor clock by default. As the VAA licenses are time-based, it is critical that the hypervisor clock is synchronized to UTC.

Memory and disk space

Each virtual machine for a VAA has a minimum set of hardware requirements. This implicates how large the physical RAM and physical hard drive storage space needs to be on the host machine.

For each VM, Allied Telesis recommends that you allocate:

- 1GB physical disk space for storage
- 1GB physical RAM

Configuring a VAA Using VMware vSphere

Uploading the Virtual AMF Appliance ISO image

Before you begin, you will first need to upload the VAA ISO image to a data store on your ESXi server. For the complete set of instructions on uploading a VAA ISO image, please refer to the VMware vSphere 6.0 Documentation Centre.

You can obtain the ISO image from the Allied Telesis Download Centre.

Creating a VAA virtual machine

Using **VMware vSphere client 6.0**, follow these steps:

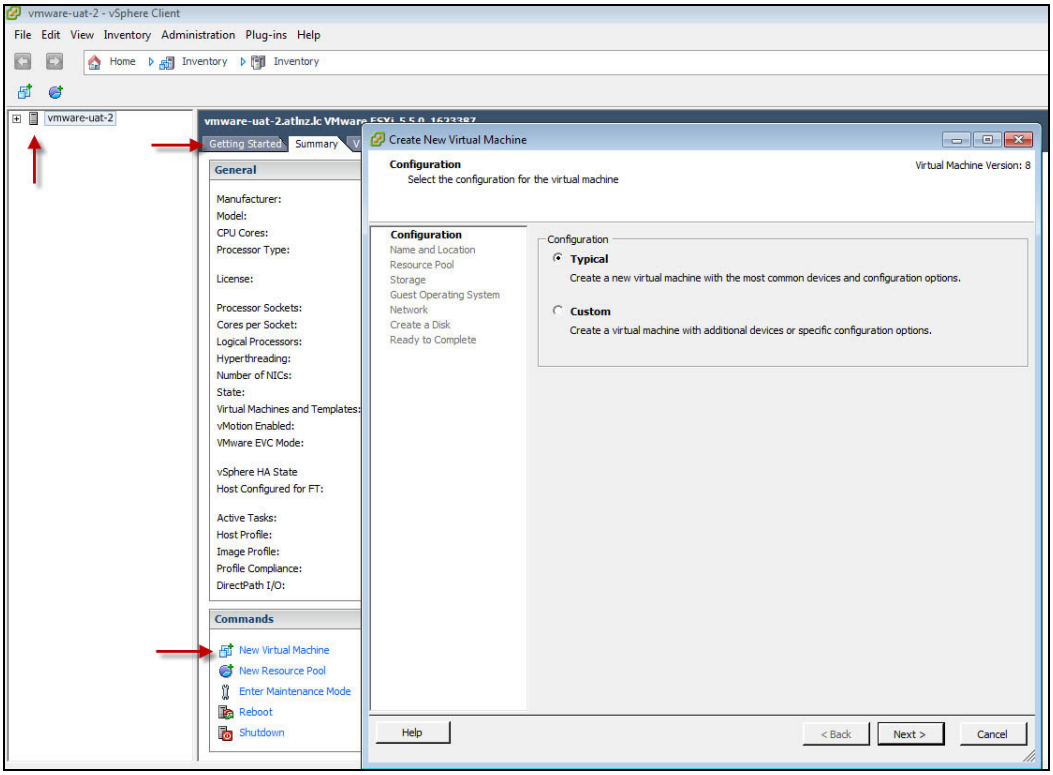
1. Select your **ESXi server** in the list on the left.
2. Select the **Getting Started** tab.
3. Click on the **Create New Virtual Machine** link.

This opens a configuration wizard, that guides you through the following process:

Configuration

In the **Configuration** window:

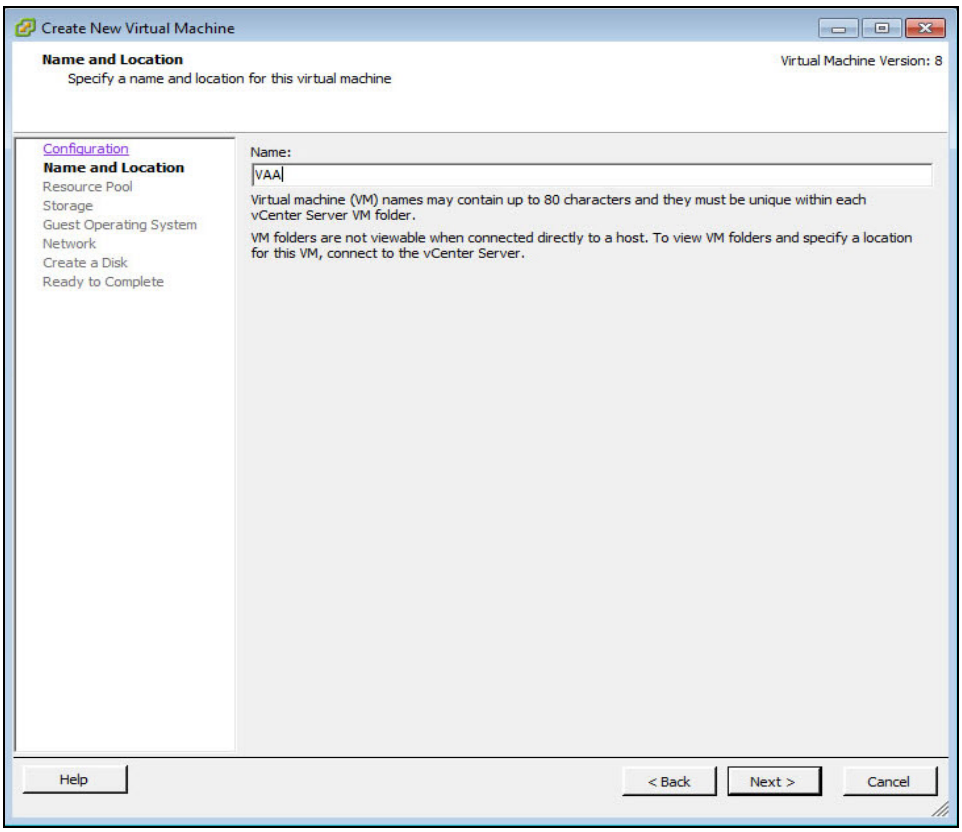
- Select **Typical**
- Click **Next >**



Name and Location

In the **Name and Location** window:

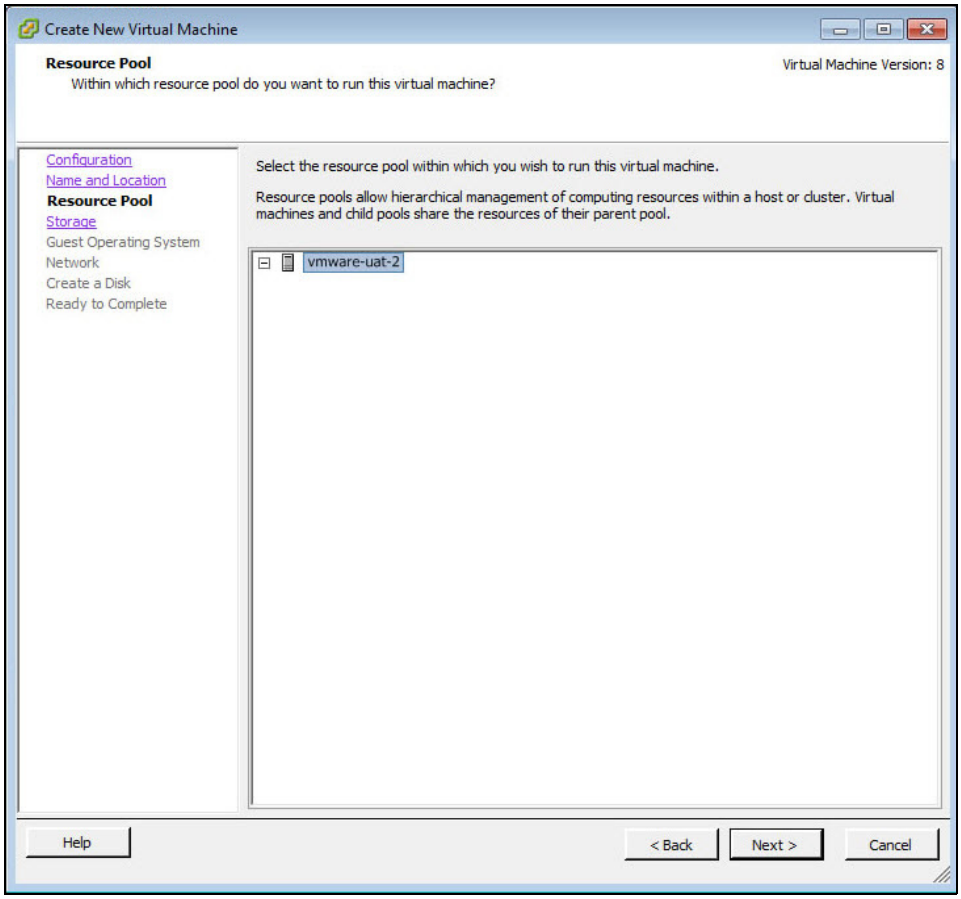
- Enter a **Name** of your choosing.
- Click **Next >**



Resource Pool

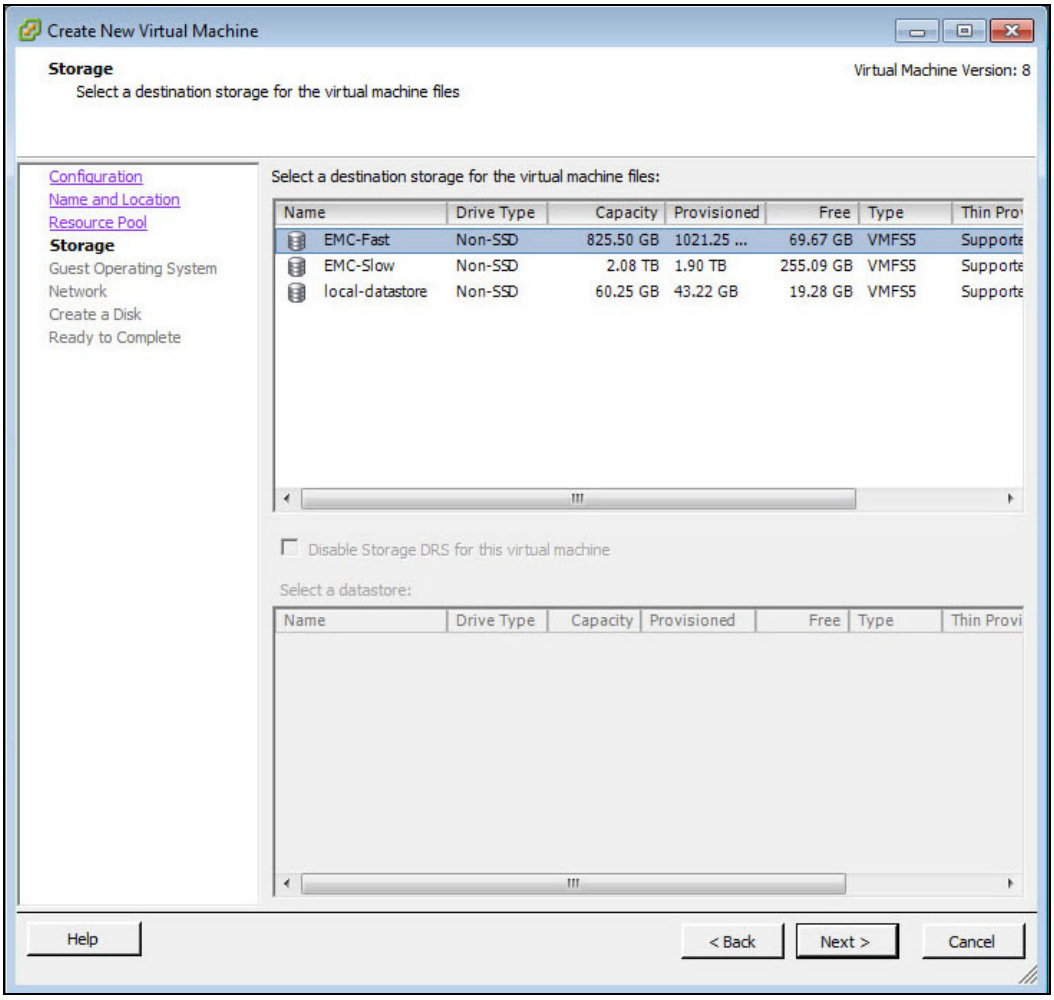
In the **Resource Pool** window:

- Select the **HostGroup** to run on.
- Click **Next>**



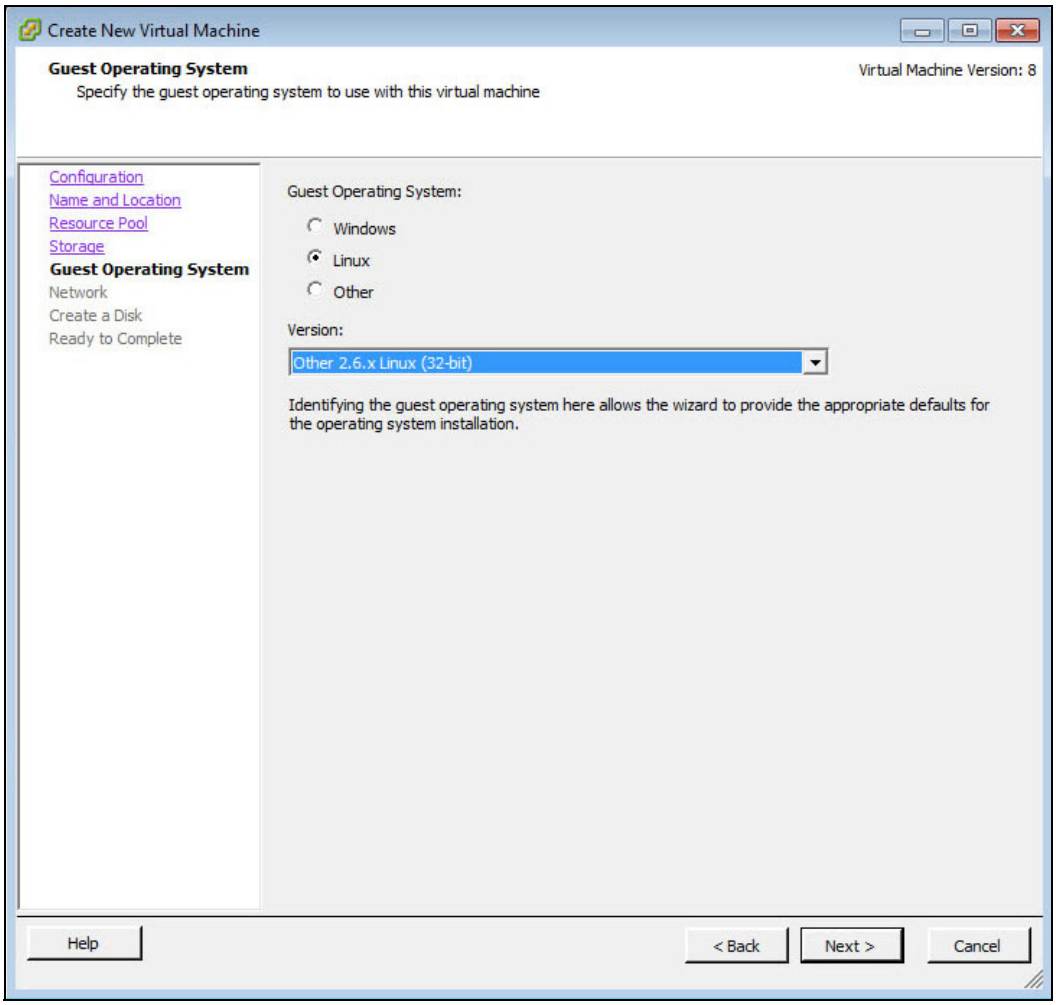
Storage

Select an appropriate destination data store for the virtual machine files. The appropriate choice depends on your specific ESXi configuration.



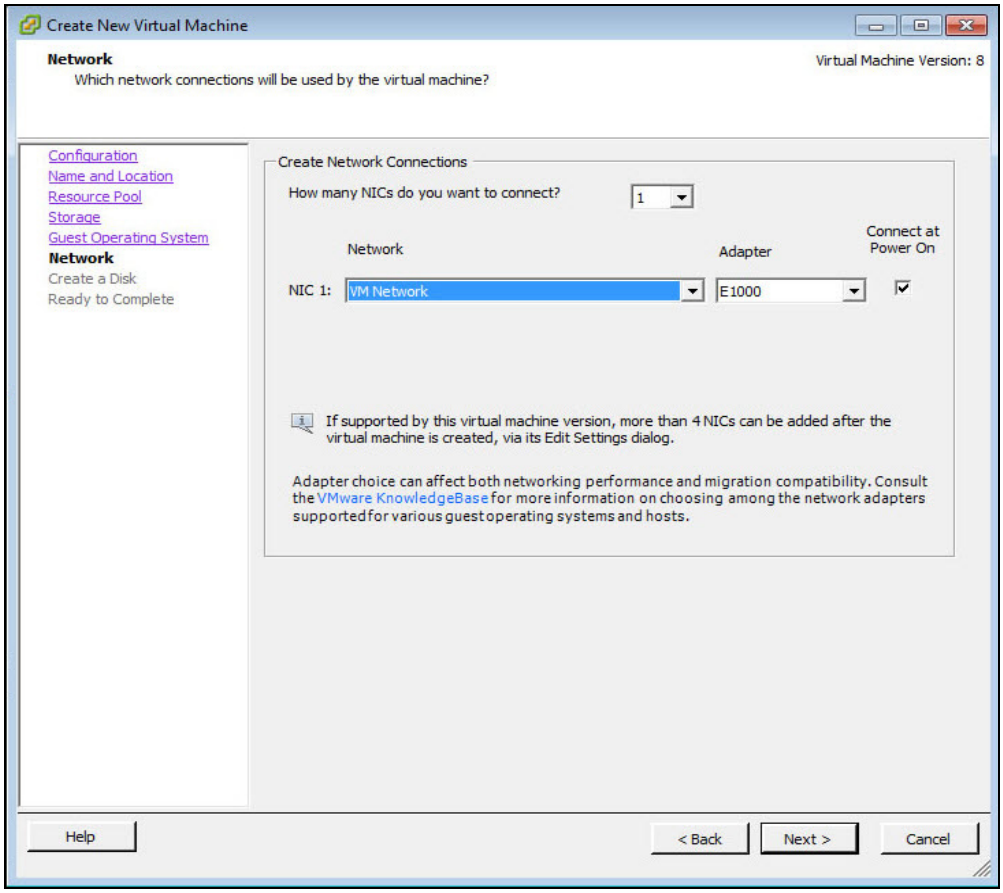
- Click **Next >**

Guest Operating System



- Select the **Linux** radio button.
- Select **Version** Other 3.x Linux (32-bit). If this version is not available, such as on earlier versions of vSphere, you should select Other 2.6x Linux (32-bit).
- Click **Next >**

Network



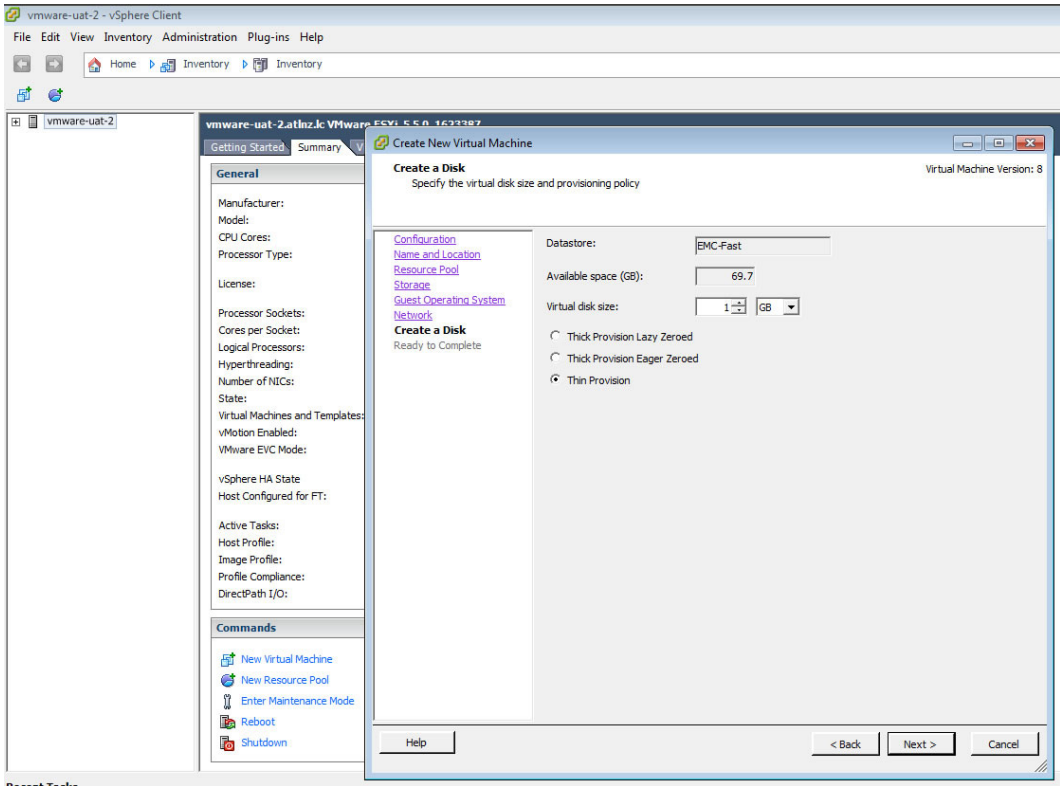
- Specify the number of interfaces the VAA will require, one interface for every VMware network you need to connect to.
- For each NIC select the appropriate network.
- **Adapter** type can be E1000 or VMXNET3, with VMXNET3 possibly offering better performance.
    - For information on the E1000 or VMXNET3, please see the VMware Knowledge Base article: Choosing a network adapter for your virtual machine (1001805).
- Ensure **Connect at Power On** is ticked.
- Click **Next >**

VLAN configuration

We recommend that you create an AMF specific network using either a VLAN, or a dedicated NIC.

If you wish to use VLAN sub-interfaces in the Virtual AMF Appliance, you will need to set "VLAN ID: All (4095)" in the VMware port group settings. This in effect tags a port to allow all VLAN IDs to pass through it.

Create a Disk

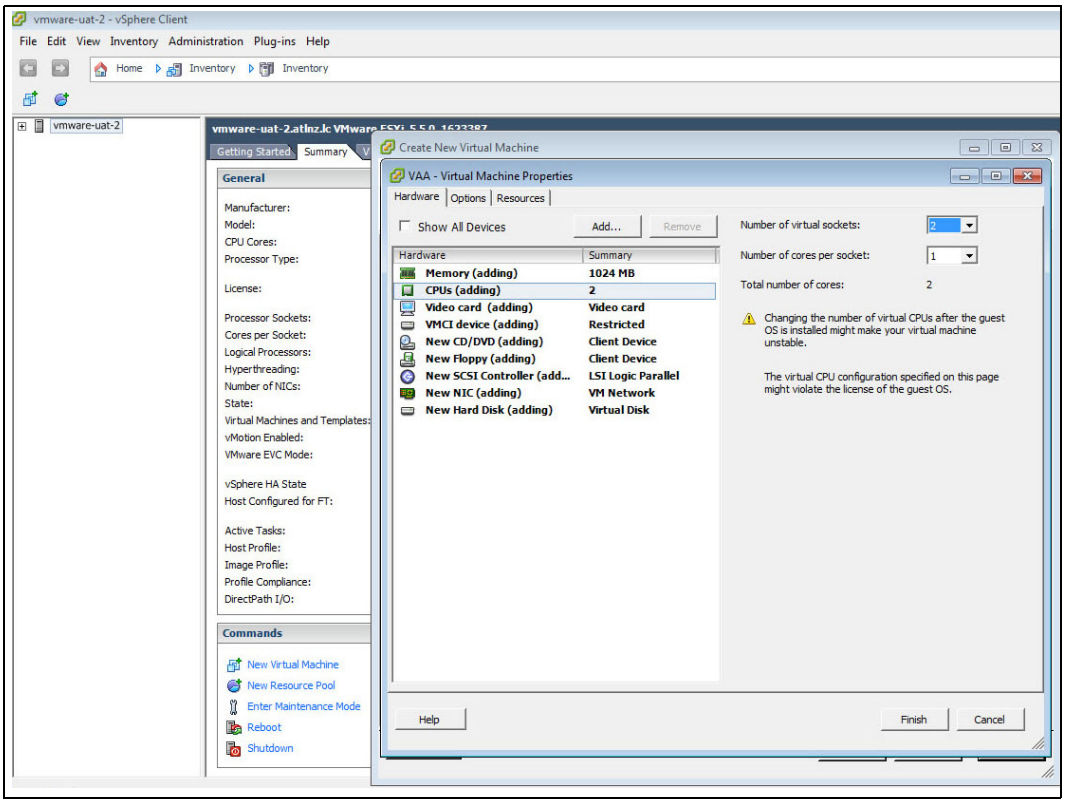


- Virtual disk size must be between 1GB and 2TB, **32GB** is recommended.
- Click **Next >**

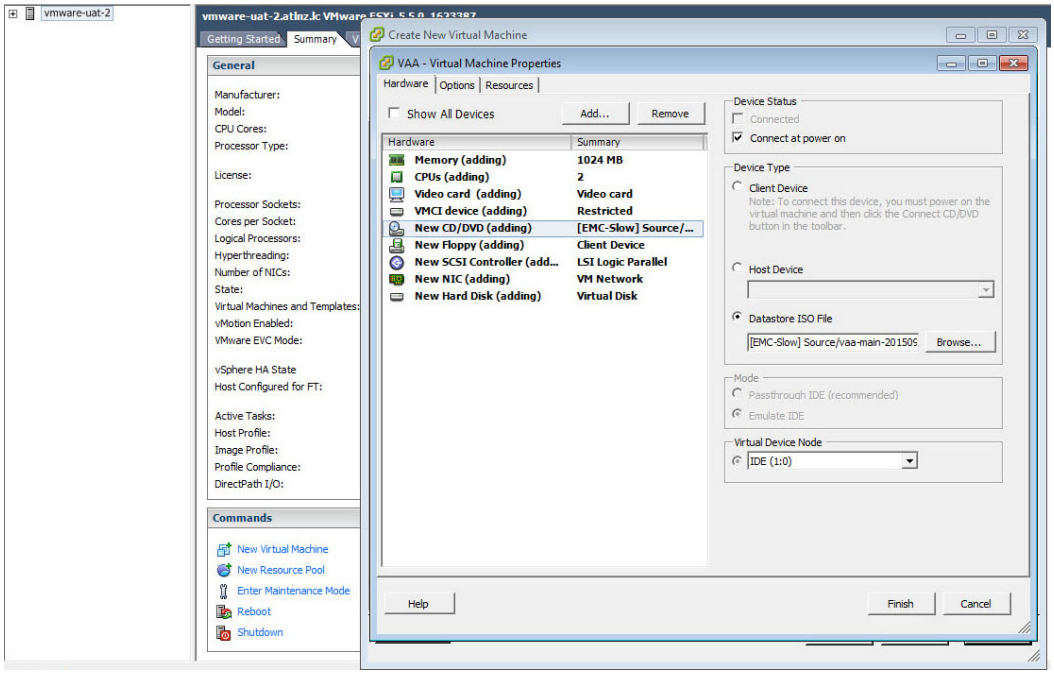
Ready to Complete

- Double check the virtual-machine configuration is correct.
- Tick the **Edit virtual machine settings before completion** check-box.
- Click **Finish**

Virtual Machine Properties



- Select the **Memory** item and set memory to **1024 MB**
- Select the **CPUs** item and set the number of CPUs to **2**
- Select the **CD/DVD** Drive 1 item.



- Ensure that **Connect at power on** check-box is ticked.
- Select the **Datastore ISO File** radio button.

- **Browse** for the VAA ISO image you uploaded earlier.
- Click **Finish**.

This completes the set-up and you can now use the VAA.

Starting the VAA on vSphere

In the vSphere Client:

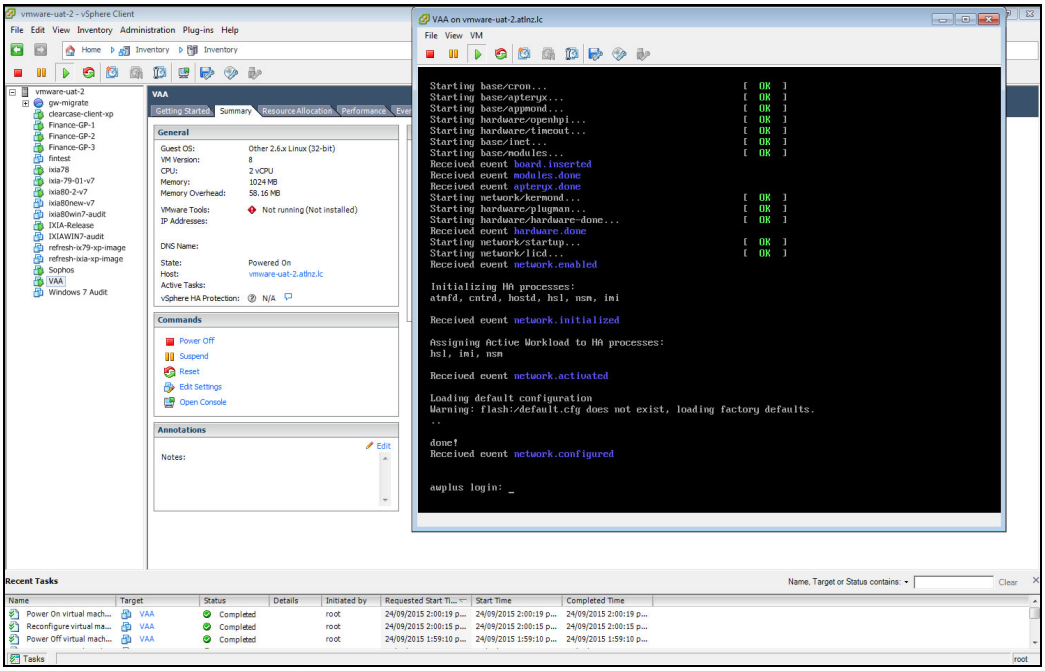
- Select **VAA** from the inventory list on the left.
- **Right click** the virtual appliance, opening the context menu.
- In the **Commands** sub-menu, click **Power On**.

View Console

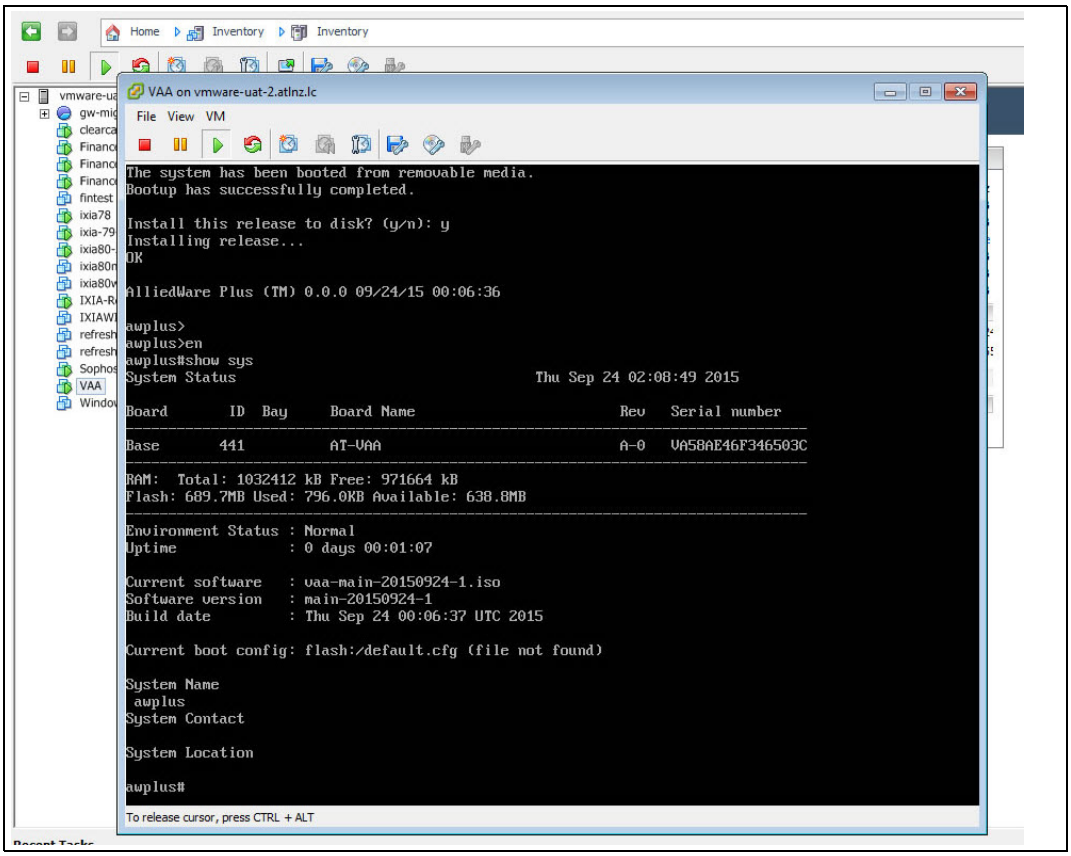
- Select **VAA** from the inventory list on the left side of vSphere Client.
- **Right click** the virtual appliance, opening the context menu.
- Click **Open Console**

Install

- The install login prompt displays: *Do you want to install this release to disc?*
- Type in **Yes** to Install.



The following screenshot shows the first run.



Stopping the VAA on vSphere

- Select **VAA** from the inventory list on the left side of vSphere Client.
- **Right click** the virtual appliance, opening the context menu.
- In the **Power** sub-menu, click **Power Off**.

Upgrading and downgrading the software of a VAA on vSphere

First upload the new VAA ISO image to a data store, as detailed in "Configuring a VAA Using VMware vSphere" on page 5. To upgrade or downgrade the current installed image, you will need to change the current.iso software image in the virtual-machine configuration, then reboot the virtual-machine.

To change the current .iso software image:

- Power off the virtual-machine you wish to upgrade/downgrade.
- Edit the settings of the virtual-machine.
- Select CD/DVD Drive 1 item
- Ensure that **Connect at power on** check-box is ticked.
- Select the **Datastore ISO File** radio button.
- **Browse** for the desired VAA iso image.

Now start the virtual machine. During boot you will see a menu that looks like this:

```
Alliedware+
Boot from CD
```

- Select the **Boot from CD** option.

Note: You will only have 5 seconds to select "Boot from CD" before the boot continues with the previously installed release.

This will boot using the new .iso software image, and next time you login using the console you will be presented with the "*Install this release to disk? (y/n)*" option. Enter y.

Migrating a running VAA to a different physical host

If you need to take a host offline for maintenance, you can move the virtual machine to another host. Migration with vMotion™ allows virtual machine processes to continue working throughout a migration. Refer to the VMotion documentation for instructions.

Requirements: Both physical hosts must have:

- the same network configuration.
- access to the same network(s) to which the interfaces of the VAA are mapped.
- access to the data-store that the VAA uses.

Accessing the CLI of the VAA

When the VAA is powered on, and is being viewed via the console, and has completed its bootup sequence, it will offer a login prompt. Login with the default username of **manager** and password of **friend**.

You now have access to the familiar AlliedWare Plus CLI, and can configure the AMF Master/Controller as described in the AMF Feature Overview and Configuration Guide.

Obtaining and Installing the VAA Software License

Licensing for a VAA is subscription-based. The type of license will depend on how extensive the network is that you need to manage.

Network engineers in charge of managing AMF need to consider how many:

- AMF Masters throughout the network are linked to an AMF Controller
- nodes in each AMF Area are linked to the area's AMF Master.

Each VAA acting as an AMF Controller or AMF Master will need its own unique license file that is based on the unique serial number of the VAA. License files are a binary file called a Capability Response File (CRF) with a .bin file extension. This is a binary-encoded file that defines the number and type of nodes allowed throughout the AMF network.

To obtain and activate a license, perform the following steps.

1. Start the VAA and log into the AlliedWare Plus command line using the default username of **manager** and password of **friend**.
2. Use the command **show system** to obtain the VAA serial number, as shown in bold in the following output example.

```
awplus>show system
System Status                                  Tue Feb 07 09:53:21 2017

Board       ID  Bay     Board Name                          Rev   Serial number
-------------------------------------------------------------------------------
Base       441          AT-VAA                              A-0   VF6234FC78713007
-------------------------------------------------------------------------------
RAM:  Total: 512672 kB Free: 456484 kB
Flash: 7.5GB Used: 17.4MB Available: 7.0GB
-------------------------------------------------------------------------------
...
```

3. Contact your authorized Allied Telesis distributor or reseller to purchase the appropriate subscription license. You will need to supply the VAA's serial number. Once your purchase has been successfully processed, the CRF .bin file containing the license will be available in the Allied Telesis Download Center.

4. To automatically download and install the license onto the VAA, first make sure your VAA is able to contact the Allied Telesis Download Center. To do this, confirm that it can successfully ping alliedtelesis.flexnetoperations.com. If it cannot, you may need to configure your firewall to allow outbound DNS lookups and HTTPS connections. Then download and install the license, by using the following command in priveleged exec mode:

```
awplus#license update online
```

5. If your VAA is unable to access the Allied Telesis Download Center, you can download the CRF .bin file from the Download Center (or your Allied Telesis support center may email it to you). Once you have obtained the file, copy it onto the VAA so that it is visible on the virtual Flash. Then install the file manually, by using the following command:

```
awplus#license update file <filename.bin>
```

6. Confirm the license has been applied, by using the command **show license external**, as shown in the following output example.

```
awplus#show license external
Licensed features:

AMF Master
       Start date                    : 05-Nov-2016 12:00AM
       Expiry date                   : 03-Nov-2017 11:59PM
       Total Nodes Allowed           : 20
```

AMF license expiry

AMF licenses on VAA are time based. Warnings of a pending license expiry will be displayed in the log at the following times: 28 days, 21 days, 14 days, 7 days and 1 day prior to a license expiring. You can set up appropriate syslog monitoring to look for these messages.

Configuring and Monitoring the VAA

The AMF command set available within the VAA is very similar to that available within a physical switch running AlliedWare Plus.

The commands like **atmf working-set**, **atmf select-area** and **atmf remote-login** all work in the same manner on the VAA as they do on a physical switch.

Similarly, scripts can be created within the VAA, and triggers created that will run these scripts.

Configuring interfaces and links

The chief differences between configuring the VAA and configuring a physical AlliedWare Plus device are:

- The VAA just has **eth** interfaces, these are called eth0, eth1, ...
- VLANs cannot be created on the VAA command-line. Instead 802.1q sub-interfaces need to be configured on the eth0 interface.
- The only AMF links that the VAA supports are virtual links.

So, a typical configuration on the VAA, to connect the VAA eth1 to switches in VLAN11 and VLAN12 would be:

```
interface eth1
encapsulation dot1q 12
encapsulation dot1q 11
!
interface eth1.11
ip address 192.168.11.1/24
!
interface eth1.12
ip address 192.168.12.1/24
atmf network-name AKL-Central
atmf master
atmf virtual-link id 11 ip 192.168.11.1 remote-id 11 remote-ip
192.168.11.2
atmf virtual-link id 12 ip 192.168.12.1 remote-id 12 remote-ip
192.168.12.2
```

Remote connection to the VAA

SSH into the VAA is supported. The full VAA CLI is available via SSH connections.

Backups and storage

By default, the VAA will store backups to Flash. The Flash available to the VAA is actually memory in the VM host, that has been configured as virtual flash for the VAA virtual machine. The amount of Flash made available to the virtual machine is defined during the installation process, see "Create a Disk" on page 11.

To see the status of backups, use the **show atmf backup** command.

```
vaa_top# show atmf backup area
Scheduled Backup ..... Enabled
Schedule ............. 1 per day starting at 03:00
Next Backup Time .... 20 May 2016 03:00
Backup Bandwidth ..... Unlimited
Backup Media ......... INTERNAL (Total 1951.8MB, Free 1843.3MB)
Current Action ........ Idle
Started .............. -
Current Node ........ -
Area Name Node Name Date Time Status
------------------------------------------------------------------------
Canterbury green 19 May 2016 13:41:42 Good
```

Also, the VAA can be configured to store backups on remote file servers, in the same way a physical AMF master or controller can.

```
vaa_top#show atmf backup
Scheduled Backup ..... Enabled
Schedule ............. 1 per day starting at 03:00
Next Backup Time .... 19 May 2016 03:00
Backup Bandwidth ..... Unlimited
Backup Media ......... FILE SERVER 1 (Total 56193.0MB, Free 27492.0MB)
Server Config .........
1 ................... Configured (Mounted, Active)
Host ............... 192.168.56.1
Username ........... janeb
Path ............... /tftpboot/vaa_file_server
Port ............... -
2 ................... Unconfigured
Current Action ........ Idle
Started .............. -
Current Node ........ -
------------------------------------------------------------------------
Node Name Id Date Time In ATMF On Media Status
------------------------------------------------------------------------
blue 1 06 May 2016 14:27:49 No Yes Good
green 1 06 May 2016 14:27:55 No Yes Good
vaa_top 1 15 May 2016 03:00:00 Yes Yes Good
```