



FortiADC - VM Installation - VMWare VMSphere

Version 5.4.0

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



February 19, 2020

FortiADC 5.4.0 VM Installation - VMWare VMSphere

01-540-600000-20200219

TABLE OF CONTENTS

Change Log	4
Getting Started	5
Introduction	5
Basic network topology	5
System requirements	6
Downloading software & registering with support	7
Licensing	9
Evaluation license	10
License sizes	10
License validation	10
About this document	11
Deploying FortiADC-VM on VMware vSphere	12
Installation overview	12
Step 1: Deploy the OVF file	13
Step 2: Configure virtual hardware settings	17
Resizing the virtual disk (vDisk)	18
Configuring the number of virtual CPUs (vCPUs)	19
Configuring the virtual RAM (vRAM) limit	21
Mapping the virtual NICs (vNICs) to physical NICs	23
HA Configuration	25
config drive (vmware)	26
Step 3: Power on the virtual appliance	27
Step 4: Configure access to the web UI & CLI	28
Step 5: Upload the license file	29
What's next?	30
Upgrading the number of VM CPUs	31
Upgrading the virtual hardware	32
Cloud-init using config drive	32
FortiADC-VM license file	33
FortiADC configuration script	33
Create the Config Drive ISO	34
Results and verification	38

Change Log

Date	Change Description
2020-04-07	Add "Cloud-init using config drive" section to Chapter 2
2020-02-18	Add "config drive (vmware)" section to Chapter 2, Step 2.
2019-10-29	Fourth release
2019-04-17	Third release
2019-02-22	Second release
2017-08-23	<ul style="list-style-type: none">• Initial release.• Changed "n < 60,000 — 2 GB vRAM; 60,001 < n < 140,000 — 4 GB vRAM" to "1 < n < 140,000 — 4 GB vRAM". See p. 26.• Changed minimum vRAM from "1 GB" to "2 GB". See p. 26.

Getting Started

This chapter includes the following information:

Introduction	5
Basic network topology	5
System requirements	6
Downloading software & registering with support	7
Licensing	9
Evaluation license	10
License sizes	10
License validation	10
About this document	11

Introduction

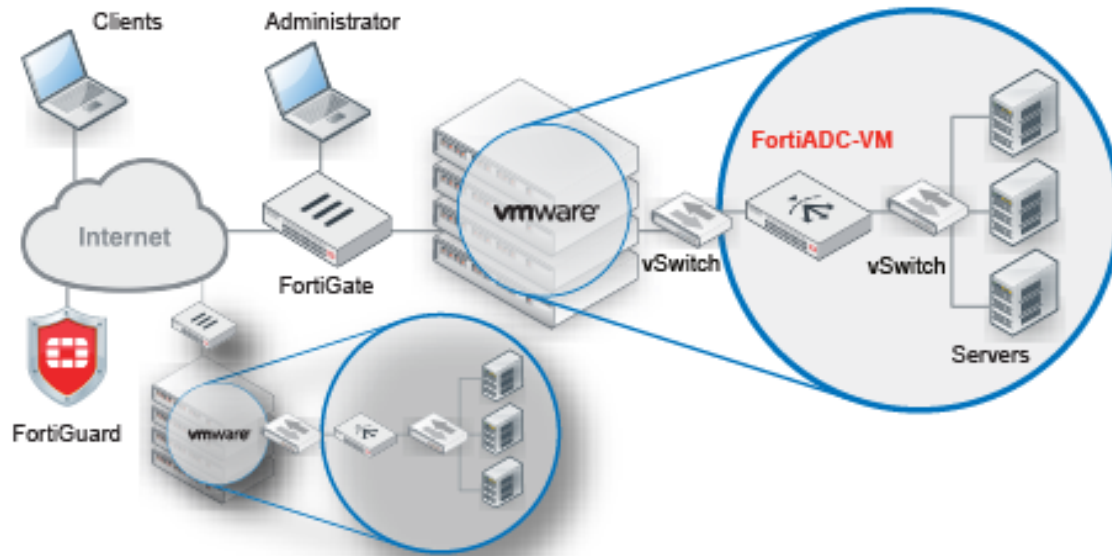
Welcome, and thank you for selecting Fortinet Technologies, Inc. products for your network. The FortiADC D-series family of Application Delivery Controllers (ADC) optimizes the availability, user experience, performance and scalability of enterprise application delivery.

The FortiADC D-series family includes physical appliances and virtual appliances. FortiADC-VM is a virtual appliance version of FortiADC. FortiADC-VM is suitable for small, medium, and large enterprises.

Basic network topology

[FortiADC-VM network topology on page 5](#) shows the network topology when the FortiADC-VM is deployment in a virtual machine environment such as VMware vSphere.

FortiADC-VM network topology



FortiADC intercepts incoming client connections and redistributes them to your servers. FortiADC has some firewall capability. However, because it is designed primarily to provide application availability and load balancing, it should be deployed behind a firewall that focuses on security, such as FortiGate.

In deployments that use the FortiADC global server load balancing feature, each hosting location should have its own FortiADC. For example, if you had server clusters located in New York, Shanghai and Bangalore, you deploy three FortiADC appliances: one in New York, one in Shanghai, and one in Bangalore.

Once the virtual appliance is deployed, you can configure FortiADC-VM via its web UI and CLI, from a web browser and terminal emulator on your management computer.

In the initial setup, the following ports are used:

- DNS lookup — UDP 53
- FortiGuard licensing — TCP 443

System requirements

VM environment	Tested Versions
VMware	ESXi 3.5, 4.x, 5.0, 5.1, 5.5, 6.0, 6.5
Microsoft Hyper-V	Windows Server 2012 R2
KVM	Linux version 3.19.0 qemu-img v2.0.0, qemu-img v2.2
Citrix Xen	XenServer 6.5.0
Xen Project Hypervisor	4.4.2, 4.5



For best performance, install FortiADC-VM on a “bare metal” hypervisor. Hypervisors that are installed as applications on top of a general purpose operating system (Windows, Mac OS X or Linux) host have fewer computing resources available due to the host OS’s own overhead.

Hardware-assisted virtualization (VT) must be enabled in the BIOS.

Downloading software & registering with support

When you purchase a FortiADC-VM, you receive an email that contains a registration number. This is used to download the software, your purchased license, and also to register your purchase with Fortinet Customer Service & Support so that your FortiADC-VM will be able to validate its license with Fortinet.

Many Fortinet customer services such as firmware updates, technical support, and FortiGuard services require product registration. For more information, see the Fortinet Knowledge Base article [Registration Frequently Asked Questions](#).

[Fortinet Customer Service & Support on page 7](#) shows the Fortinet Customer Service & Support website.

Fortinet Customer Service & Support

To register & download FortiADC-VM and your license:











1. Log into the Fortinet Customer Service & Support web site:
<https://support.fortinet.com/>
2. Under Asset, click **Register/Renew**.
3. Provide the registration number that was emailed to you when you purchased the software. Registration numbers are a hyphenated string of 25 numbers and characters in groups of 5, such as:
TLH5R-NUNDP-MC6T7-0DNWA-AP45ZA
A registration form appears.
4. Use the form to register your ownership of FortiADC-VM.
After completing the form, a registration acknowledgment page appears.
5. Click the **License File Download** link.
Your browser will download the `.lic` file that was purchased for that registration number.
6. Click the **Home** link to return to the initial page.
7. Under Download, click **Firmware Images**.
8. Click the FortiADC link and navigate to the version that you want to download.

Select Product

Release Notes

Download

Image File Path
[/ FortiADC/ v4.00/ 4.4/ 4.4.0/](#)
Image Folders/Files
[Up to higher level directory](#)

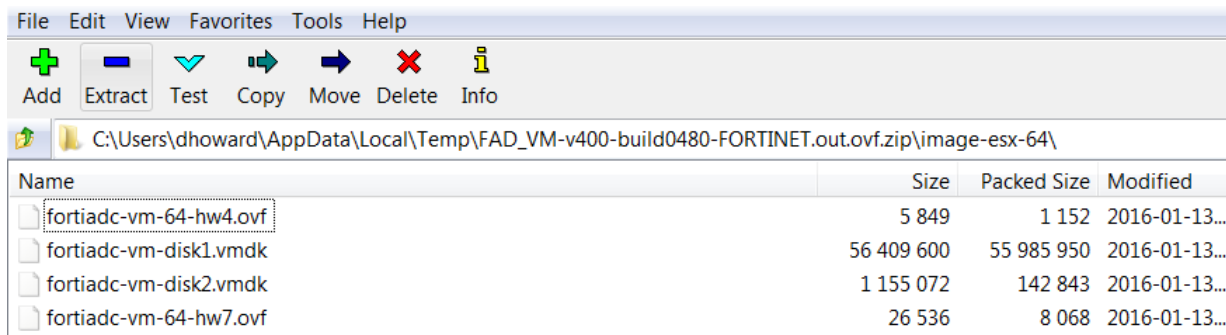
Name	Size (KB)	Date Created	Date Modified
 FAD_1500D-v400-build0480-FORTINET.out	59,537	2016-01-15 12:01:51	2016-01-15 12:01:51
 FAD_2000D-v400-build0480-FORTINET.out	58,830	2016-01-15 12:01:13	2016-01-15 12:01:13
 FAD_200D-v400-build0480-FORTINET.out	56,078	2016-01-15 12:01:47	2016-01-15 12:01:47
 FAD_300D-v400-build0480-FORTINET.out	58,829	2016-01-15 12:01:36	2016-01-15 12:01:36
 FAD_4000D-v400-build0480-FORTINET.out	58,838	2016-01-15 12:01:28	2016-01-15 12:01:28
 FAD_400D-v400-build0480-FORTINET.out	58,862	2016-01-15 12:01:01	2016-01-15 12:01:01
 FAD_700D-v400-build0480-FORTINET.out	58,856	2016-01-15 12:01:00	2016-01-15 12:01:00
 FAD_VM-v400-build0480-FORTINET.out	54,953	2016-01-15 12:01:37	2016-01-15 12:01:37
 FAD_VM-v400-build0480-FORTINET.out.ovf.zip	54,824	2016-01-15 12:01:24	2016-01-15 12:01:24
 FortiADC-4_4_0-Release-Note-for-D-Series-Models.pdf	375	2016-01-15 12:01:18	2016-01-15 12:01:18

9. Download the `.zip` file. You use the VM installation files contained in the `.zip` file for *new* VM installations. (The `.out` image files are for upgrades of existing installations only, and cannot be used for a new installation.)



Files for FortiADC-VM have a `FAD_VM` filename prefix. Other prefixes indicate that the file is for hardware versions of FortiADC such as FortiADC 200D. Such other files cannot be used with FortiADC-VM.

10. Extract the .zip file contents to a folder. The following figure shows the contents of the package for VMware. Refer to the table that follows for details on packages for supported VM environments.



VM environment	Download package
VMware	<p>The ovf.zip download file contains multiple ovf files.</p> <p>The fortiadc-vm-64-hw4.ovf file is a VMware virtual hardware version 4 image that supports ESXi 3.5.</p> <p>The fortiadc-vm-64-hw7.ovf file is a VMware virtual hardware version 7 image that supports ESXi 4.0 and above.</p> <p>Refer to the VMware support site for information about VMware virtual hardware versions and ESXi versions.</p>
Microsoft Hyper-V	<p>The hyperv.zip download file contains multiple files you use for the installation. Extract all the files to a directory you can access when you perform the installation. When you do the installation, you select the folder that contains the unzipped files.</p>
KVM	<p>The kvm.zip download file contains the boot.qcow2 and data.qcow2 files you use for the installation.</p>
Citrix Xen	<p>The xenserver.zip download file contains the fortiadc-vm-xen.ovf file you use for the installation.</p>
Xen Project	<p>The xenopensource.zip download file contains the fortiadc.hvm, bootdisk.img, and logdisk.img files you use for the installation.</p>

Licensing

This section describes licensing. It includes the following information:

- [Evaluation license](#)
- [License sizes](#)

- [License validation](#)

Evaluation license

FortiADC-VM can be evaluated with a free 15-day trial license that includes all features except:

- HA
- FortiGuard updates
- Technical support

You do not need to manually upload the trial license. It is built-in. The trial period begins the first time you start FortiADC-VM. When the trial expires, most functionality is disabled. You must purchase a license to continue using FortiADC-VM.

License sizes

FortiADC-VM licenses are available at the following sizing levels.

FortiADC-VM sizes

	License/model					
	VM01	VM02	VM04	VM08	VM16	VM32
Virtual CPUs (vCPUs)	1	2	4	8	16	32
Virtual RAM (vRAM)	4 GB	4 GB	8 GB	16 GB	32 GB	64 GB

Maximum IP sessions varies by license, but also by available vRAM, just as it does for hardware models. For details, see the maximum configuration values in the [FortiADC Handbook](#).

License validation

FortiADC-VM must periodically re-validate its license with the Fortinet Distribution Network (FDN). If it cannot contact the FDN for 24 hours, access to the FortiADC-VM web UI and CLI are locked.

By default, FortiADC-VM attempts to contact FDN over the Internet. If the management port cannot access the Internet (for example, in closed network environments), it is possible for FortiADC-VM to validate its license with a FortiManager that has been deployed on the local network to act as a local FDS (FortiGuard Distribution Server).

On the FortiADC-VM, specify the FortiManager IP address for the "override server" in the FortiGuard configuration:

```
FortiADC-VM # config system fortiguard
    set override-server-status enable
    set override-server-address <fortimanager_ip>:8890
end
```

where <fortimanager_ip> is the IP address. (TCP port 8890 is the port where the built-in FDS feature listens for requests.)

For more information on the FortiManager local FDS feature, see the [FortiManager Administration Guide](#).

Note: Although FortiManager can provide FortiGuard security service updates to some Fortinet devices, for FortiADC, its FDN features can provide license validation only.

About this document

This document describes how to deploy a FortiADC virtual appliance disk image onto a virtualization server, and how to configure the virtual hardware settings of the virtual appliance. It assumes you have already successfully installed a virtualization server on the physical machine.

This document does *not* cover initial configuration of the virtual appliance itself, nor ongoing use and maintenance. After deploying the virtual appliance, see the [FortiADC Handbook](#) for information on initial appliance configuration.

Deploying FortiADC-VM on VMware vSphere

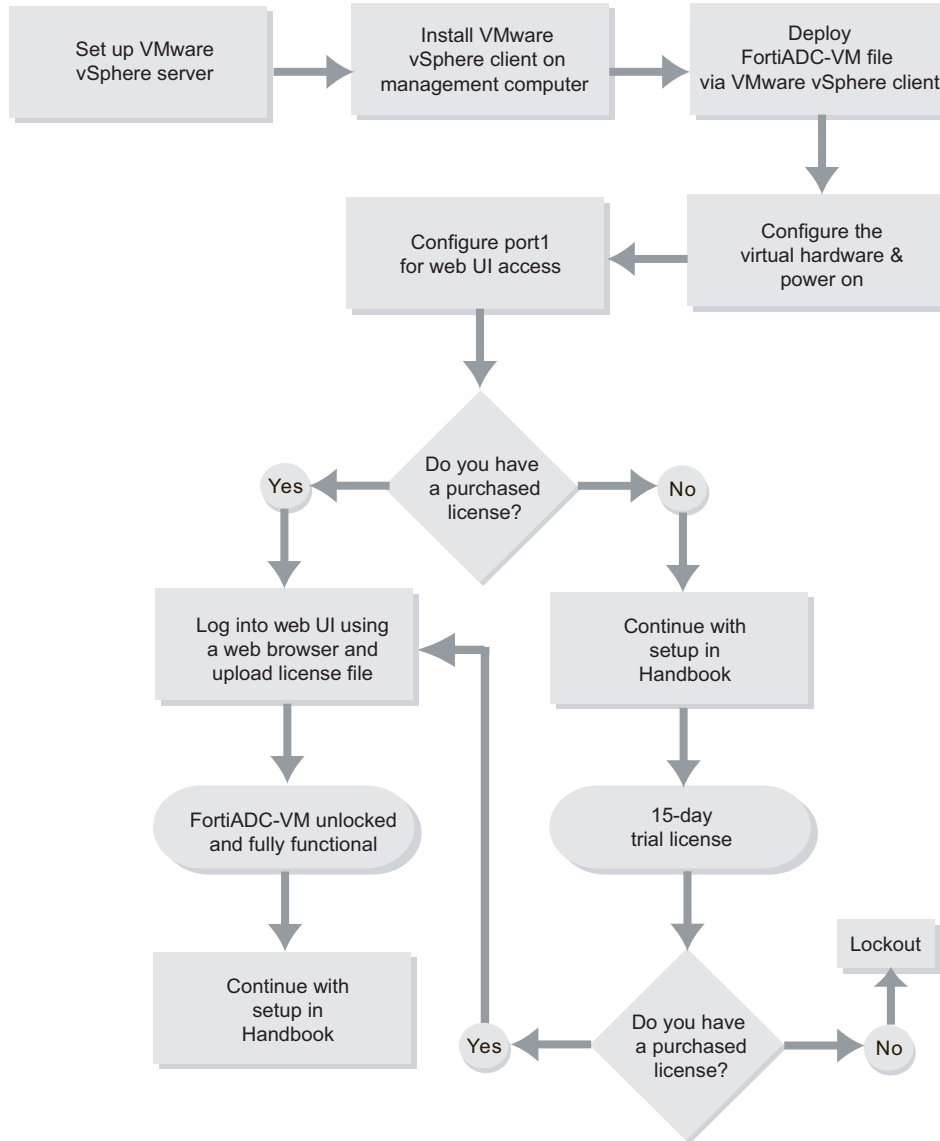
This chapter provides procedures for deploying FortiADC-VM on VMware vSphere. It includes the following information:

Installation overview	12
Step 1: Deploy the OVF file	13
Step 2: Configure virtual hardware settings	17
Resizing the virtual disk (vDisk)	18
Configuring the number of virtual CPUs (vCPUs)	19
Configuring the virtual RAM (vRAM) limit	21
Mapping the virtual NICs (vNICs) to physical NICs	23
HA Configuration	25
config drive (vmware)	26
Step 3: Power on the virtual appliance	27
Step 4: Configure access to the web UI & CLI	28
Step 5: Upload the license file	29
What's next?	30
Upgrading the number of VM CPUs	31
Upgrading the virtual hardware	32
Cloud-init using config drive	32
FortiADC-VM license file	33
FortiADC configuration script	33
Create the Config Drive ISO	34
Results and verification	38

Installation overview

The diagram below gives an overview of the process for installing FortiADC-VM on VMware vSphere, which is described in the subsequent text.

Basic steps for installing FortiADC-VM (VMware)

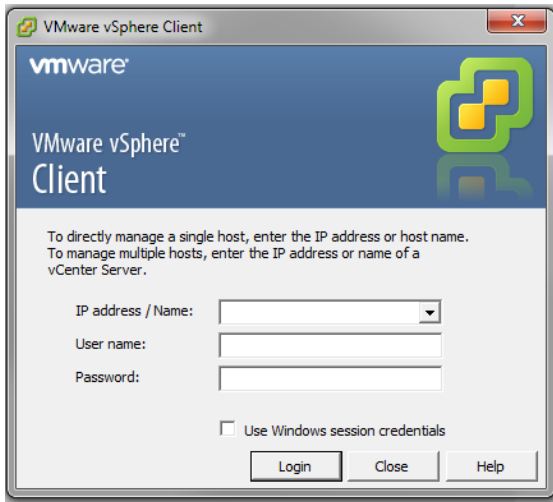


Step 1: Deploy the OVF file

You must first use VMware vSphere Client to deploy the FortiADC-VM OVF package.

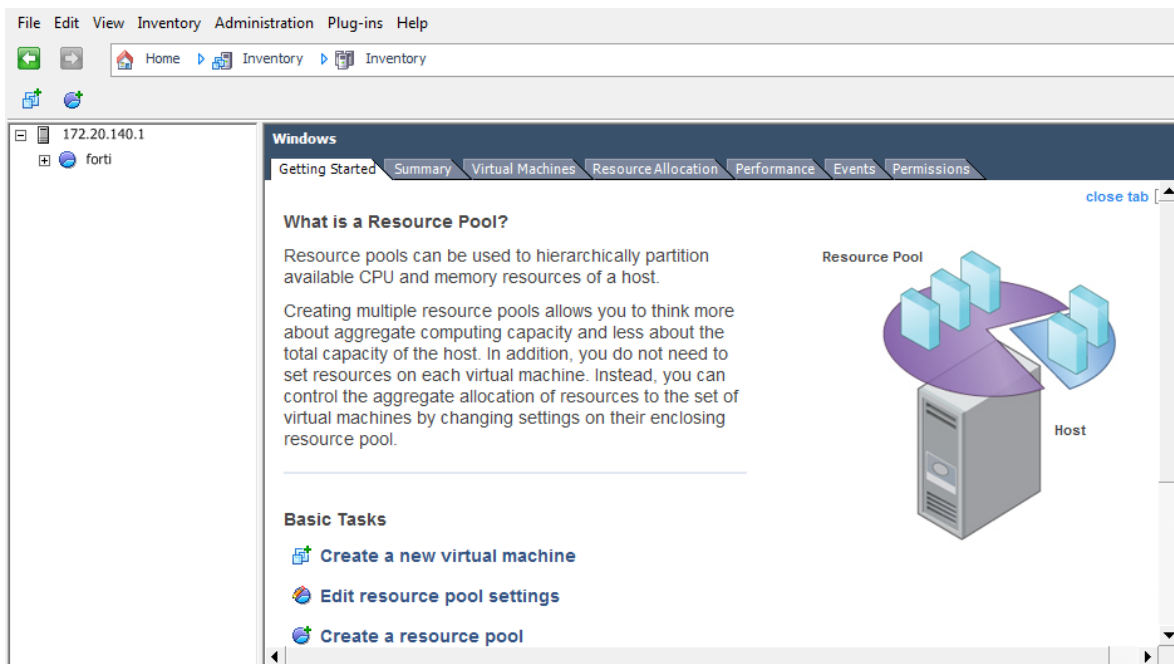
To deploy the virtual appliance:

1. Use the VMware vSphere client to connect to VMware vSphere server:
 - a. On your management computer, start the VMware vSphere Client.

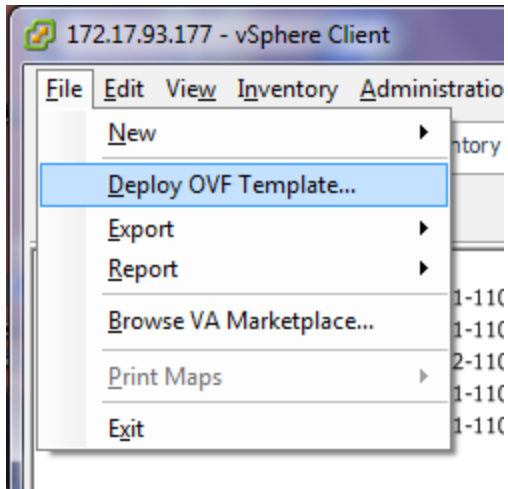


- b. In IP address / Name, type the IP address or FQDN of the VMware vSphere server.
 - c. Enter the username and password, and click **Login**.

When you successfully log in, the vSphere Client window appears.



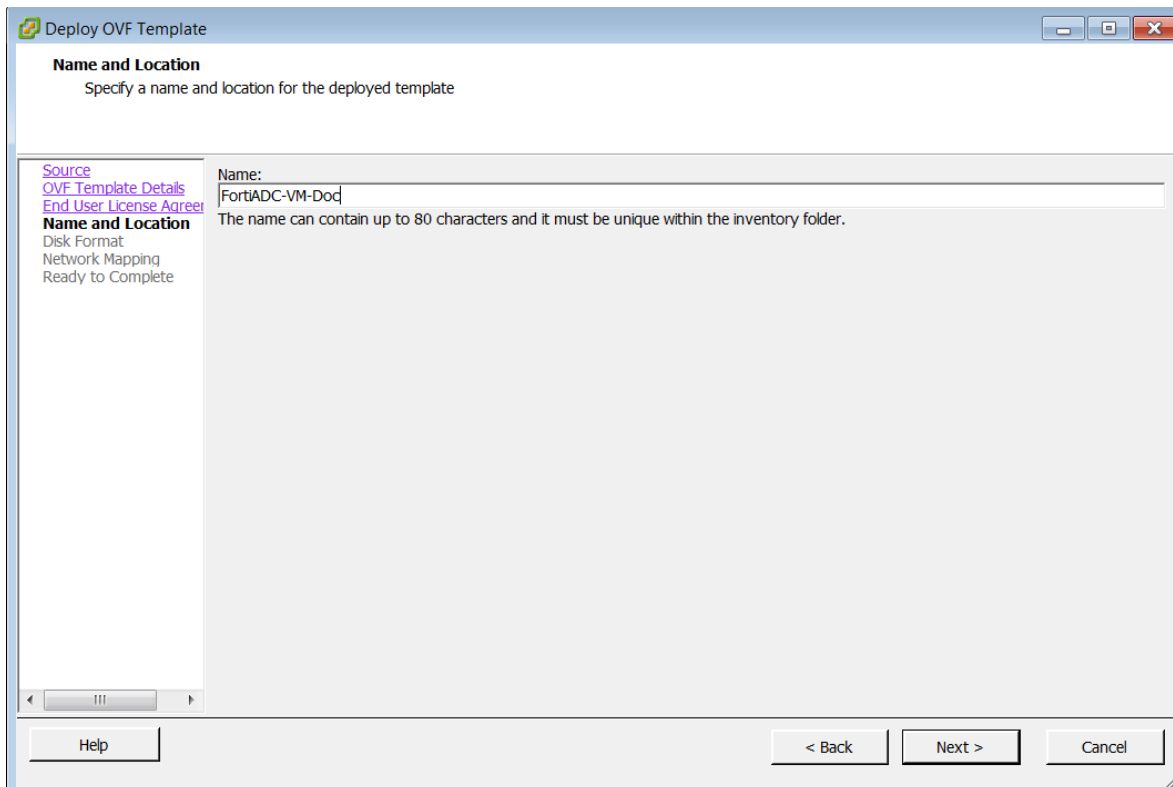
2. Go to File > Deploy OVF Template.



A deployment wizard window appears.

3. In the Deploy OVF Template window, click **Browse** and then locate and select the FortiADC-VM OVF file.
4. Click **Next** twice.
5. On the Name and Location page, type a unique descriptive name for this instance of FortiADC-VM and then then click **Next** to continue.

The name is the string that appears in the vSphere Client inventory, such as `FortiADC-VM-Doc`. If you plan to deploy multiple instances of this file, consider a naming scheme that makes each VM's purpose or IP address easy to remember. (This name is *not* used as the hostname, nor does it appear within the FortiADC-VM web UI.)



6. On the Disk Format page, select one of the following options and then click **Next** to continue:

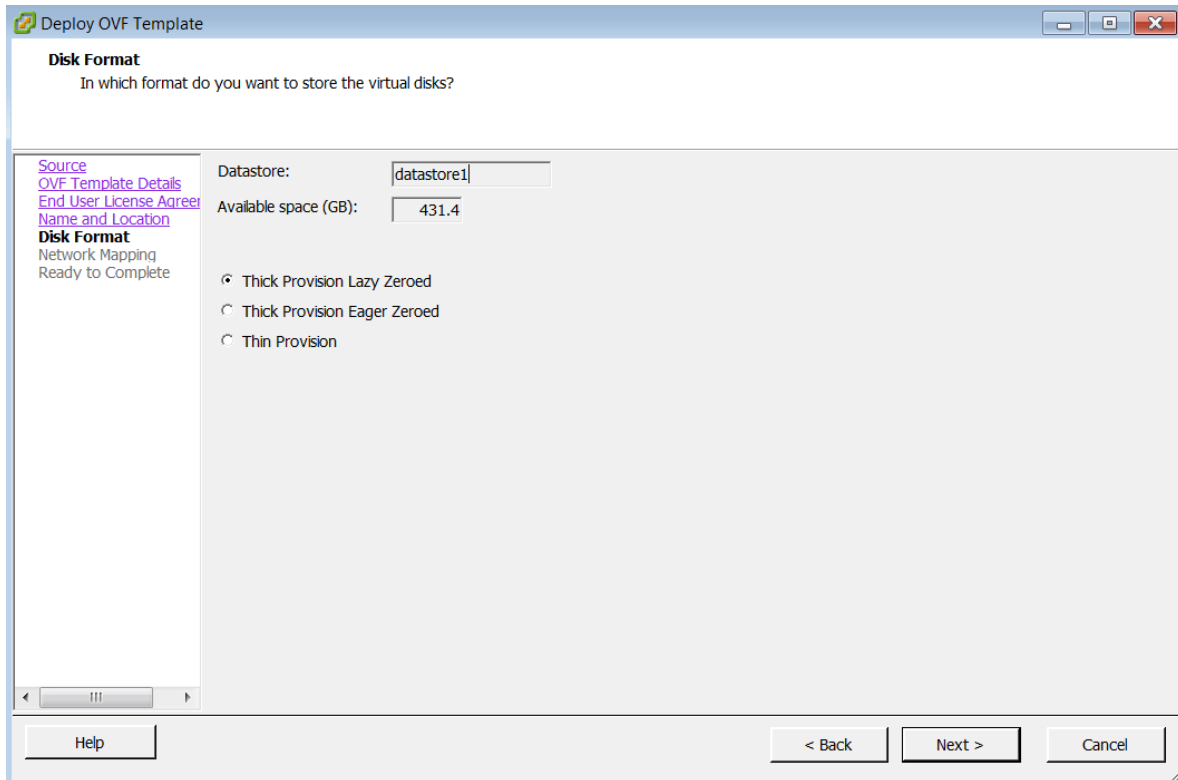
- **Thick provision**— Immediately allocate disk space (specifically 32 GB) for the storage repository.
- **Thin provision**— Allocate more disk space on demand, if the storage repository uses a VMFS3 or newer file system.



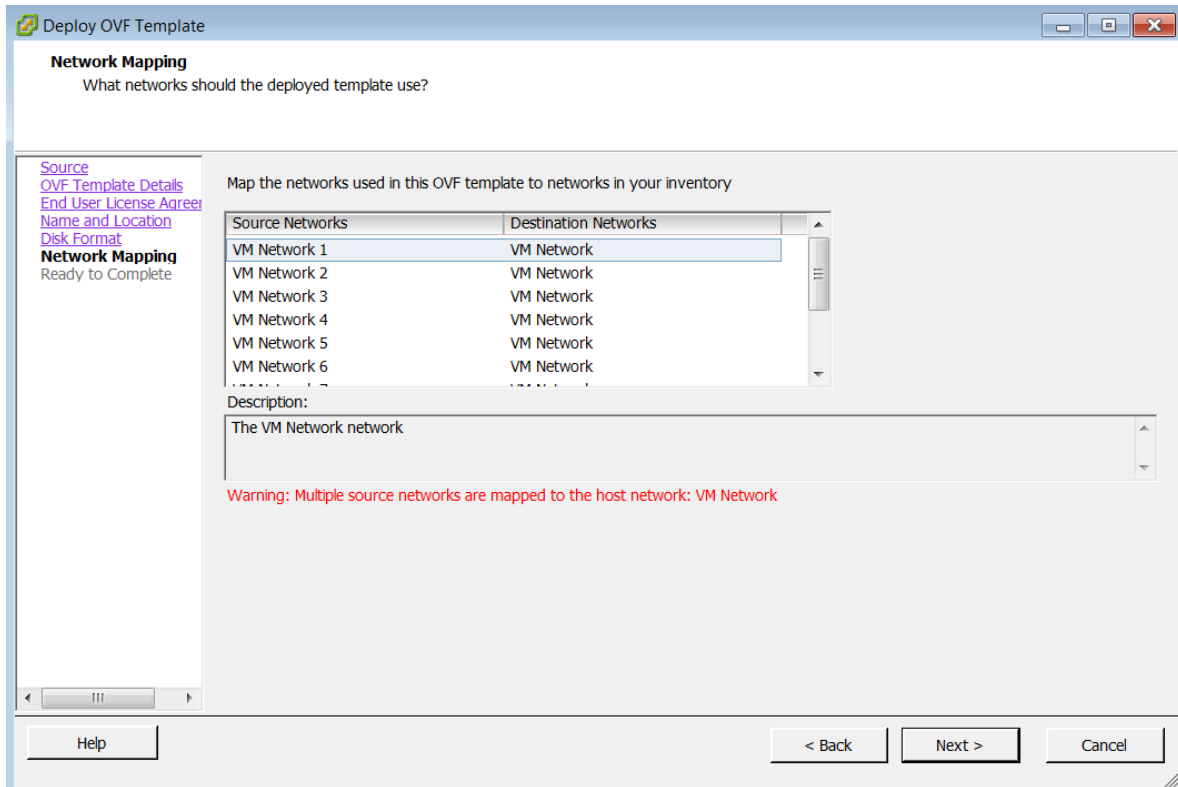
Regardless of your choice here, you must later either allocate or make available at least 40 GB of disk space. 30 GB is only the default minimum value, and is not recommended.

7.

8.



9. On the Network Mapping page, if the hypervisor has more than one possible network mapping for its vSwitch, select the row for the network mapping that FortiADC-VM should use and then then click **Next** to continue.



10. Click **Finish** to close the wizard.

The client connects to the VM environment and deploys the OVF to it. When the operation is complete, the vSphere Client window reappears. The list of virtual machines in the left navigation pane should include your new instance of FortiADC-VM.

Do not power on the virtual appliance until you have completed the following steps:

- Resize the virtual disk (VMDK).
- Set the number of vCPUs.
- Set the vRAM on the virtual appliance.
- Map the virtual network adapter(s).

These settings must be configured in the VM environment, not the FortiADC OS.

Step 2: Configure virtual hardware settings

After deploying the FortiADC-VM image and before powering on the virtual appliance, log into VMware vSphere and configure the virtual appliance hardware settings to suit the size of your deployment.

[Virtual hardware settings on page 17](#) summarizes the defaults that are set in the default image and provides rough guidelines to help you understand whether you need to upgrade the hardware before you power on the virtual appliance. For more precise guidance on sizing, contact your sales representative or Fortinet Technical Support.

Virtual hardware settings

Component	Default	Guidelines
Hard disk	32 GB	32 GB is insufficient for most deployments. Upgrade the hard disk before you power on the appliance. After you power on the appliance, you must reformat the FortiADC OS log disk with the following command: <code>execute formatlogdisk</code> Before you use this command you must upload a license file.
CPU	1 CPU	1 CPU is appropriate for a VM01 license. Upgrade to 2, 4, 8, 16, 32 CPU for VM02, VM04, and VM08, VM16, VM32 licenses, respectively.
RAM	4 GB	4 GB is the minimum. See the section on vRAM for guidelines based on expected concurrent connections.
Network interfaces	10 bridging vNICs are mapped to a port group on one virtual switch (vSwitch).	Change the mapping as required for your VM environment and network.

Resizing the virtual disk (vDisk)

If you configure the virtual appliance storage repository to be internal (i.e. local, on its own vDisk), resize the vDisk before powering on the VM appliance.



This step is not applicable if you set up the virtual appliance to use external network file system datastores (such as NFS).

The FortiADC-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files. However, they are only 32 GB, which is not large enough for most deployments. You must resize the vDisk before powering on the virtual machine.

Before doing so, make sure that you understand the effects of the vDisk settings. These options affect the possible size of each vDisk.

1 MB block size — 256 GB maximum file size

2 MB block size — 512 GB maximum file size

4 MB block size — 1024 GB maximum file size

8 MB block size — 2048 GB maximum file size

For example, if you have an 800 GB datastore which has been formatted with 1 MB block size, you cannot size a single vDisk greater than 256 GB.

Consider also that, depending on the size of your network, you might require more or less storage for logs, reports, and other data.

For more information on vDisk sizing, see:

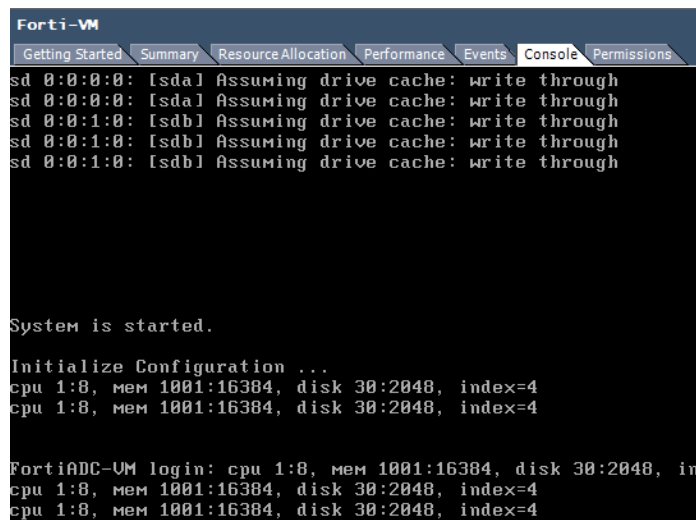
<https://communities.vmware.com/docs/DOC-11920>

To resize the vDisk:

1. Use the VMware vSphere client to connect to VMware vSphere server.
2. Turn off the power of your VMware.
3. Right click and click **Edit Settings**. Under Hard disk, **resize** the logdisk.

Note: If you have resized logdisk (*not* bootdisk), after booting FortiADC and uploading a license file, you should execute the following command: `execute formatlogdisk`. Executing this command will clear all statistics and logs etc.

Important: If you upgrade the vDisk size, the vDisk size and FortiADC-VM log partition size likely do not match, and you will see the disk errors shown in the following figure when you attempt to log into the console.



To fix this:

1. Press Enter repeatedly until you see the login prompt.
2. At the login prompt, type `admin` and no password to log in.
3. Enter the following command to fix the disk issue:

```
execute formatlogdisk
```

Configuring the number of virtual CPUs (vCPUs)

By default, the virtual appliance is configured to use 1 vCPU. Depending on the FortiADC-VM license that you purchased, you can allocate 1, 2, 4, 8, 16, or 32 vCPUs.

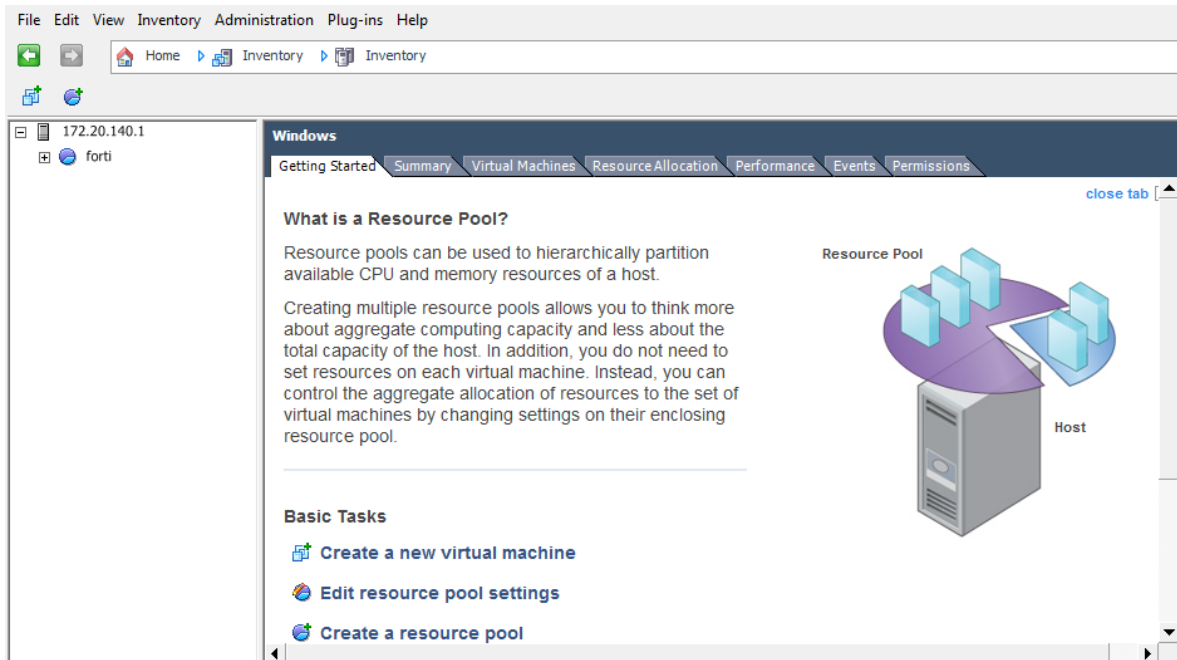
For more information on vCPUs, see the VMware vSphere documentation:

<https://www.vmware.com/support/vsphere-hypervisor.html>

To change the number of vCPUs:

1. Use the VMware vSphere client to connect to VMware vSphere server.

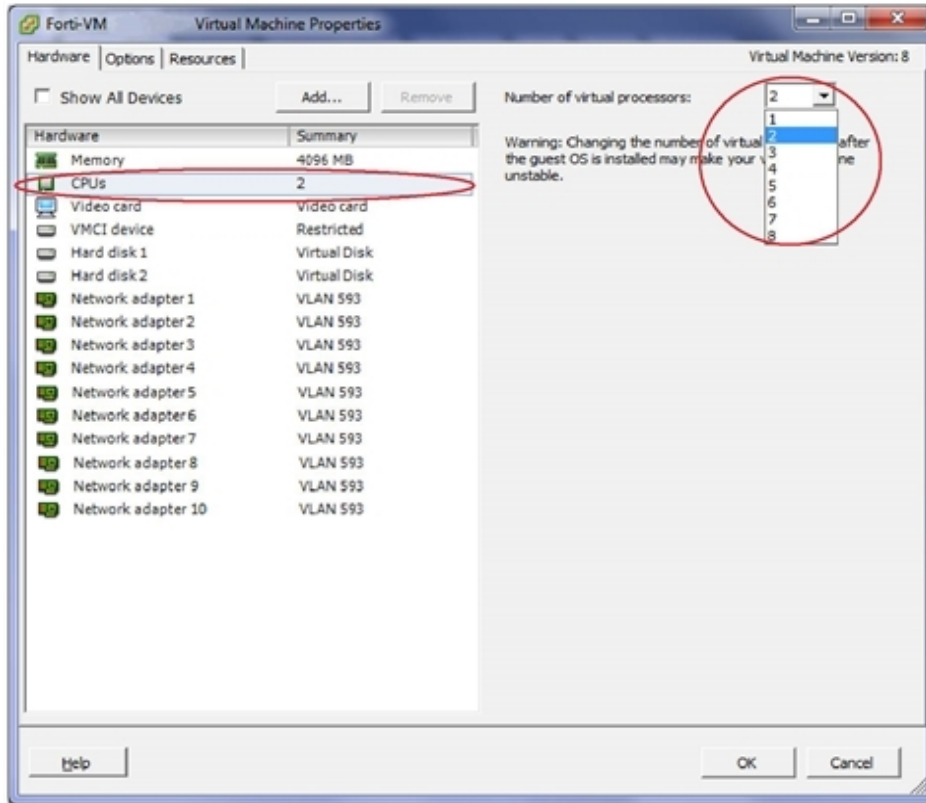
The following figure shows the vSphere client manager window.



2. In the left pane, right-click the name of the virtual appliance, such as **FortiADC-VM-Doc**, then select **Edit Settings**.

The virtual appliance properties dialog appears.

3. In the list of virtual hardware on the left side of the dialog, click **CPUs**.



4. In Number of virtual processors, specify the maximum number of vCPUs to allocate. Valid values range from 1 to 8.
5. Click **OK**.

Configuring the virtual RAM (vRAM) limit

The FortiADC-VM image is pre-configured to use 4 GB of vRAM. We recommend at least 4GB memory for all VM deployments. You can change this value. Appropriate values are suggested as follows, according to the number (n) of Layer-7 transactions that will be handled simultaneously by FortiADC-VM:

$1 < n < 140,000$ — 4 GB vRAM

$140,001 < n < 300,000$ — 8 GB vRAM

$300,001 < n < 600,000$ — 16 GB vRAM

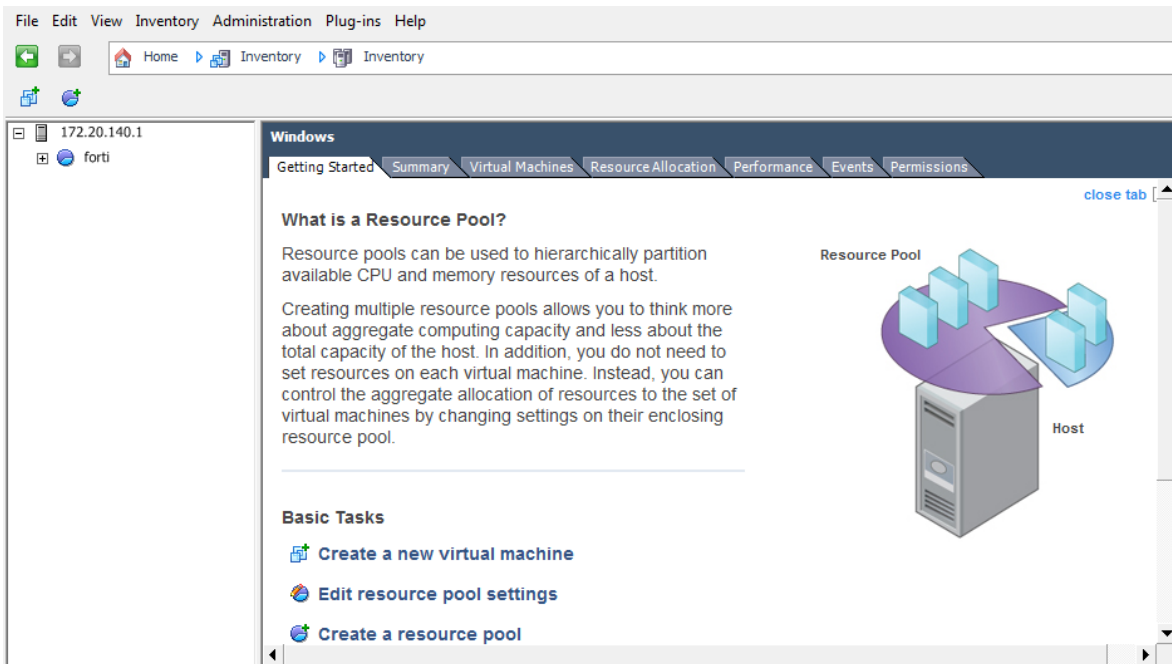
Also, sizing should be adjusted if the FortiADC-VM will be handling Layer-4 connections, or a mixture of Layer-4 and Layer-7 connections.



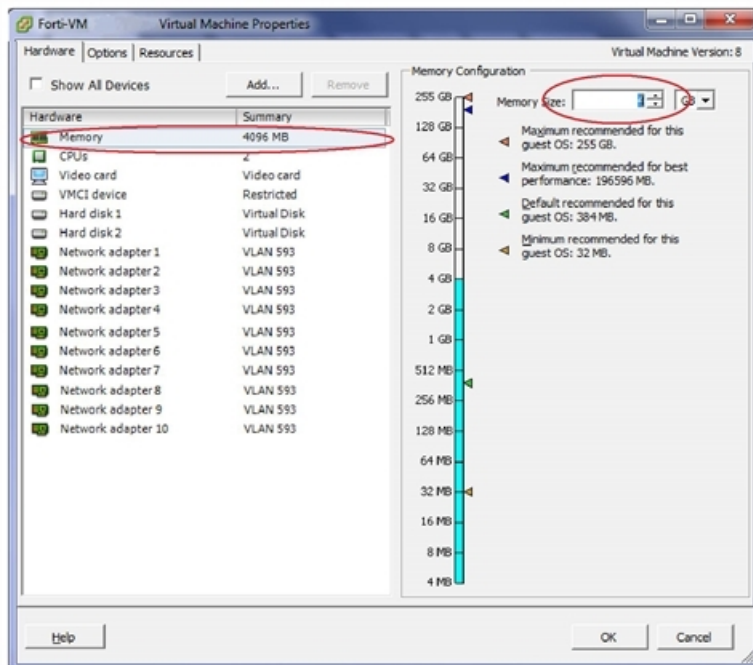
It is possible to configure FortiADC-VM to use less vRAM, such as 2 GB. However, for performance reasons, it is not recommended.

To change the amount of vRAM:

1. Use the VMware vSphere client to connect to VMware vSphere server. The following figure shows the vSphere client manager window.



2. In the left pane, right-click the name of the virtual appliance, such as **FortiADC-VM-Doc**, then select **Edit Settings**. The virtual appliance properties dialog appears.
3. In the list of virtual hardware on the left side of the dialog, click **Memory**.



4. In Memory Size, type the maximum number in gigabytes (GB) of the vRAM to allocate.
5. Click **OK**.

Mapping the virtual NICs (vNICs) to physical NICs

When you deploy the FortiADC-VM package, 10 bridging vNICs are created and automatically mapped to a port group on one virtual switch (vSwitch) within the hypervisor. Each of those vNICs can be used by one of the 10 network interfaces in FortiADC-VM. (Alternatively, if you prefer, some or all of the network interfaces can be configured to use the same vNIC.) vSwitches are themselves mapped to physical ports on the server.

You can change the mapping, or map other vNICs, if your VM environment requires it.

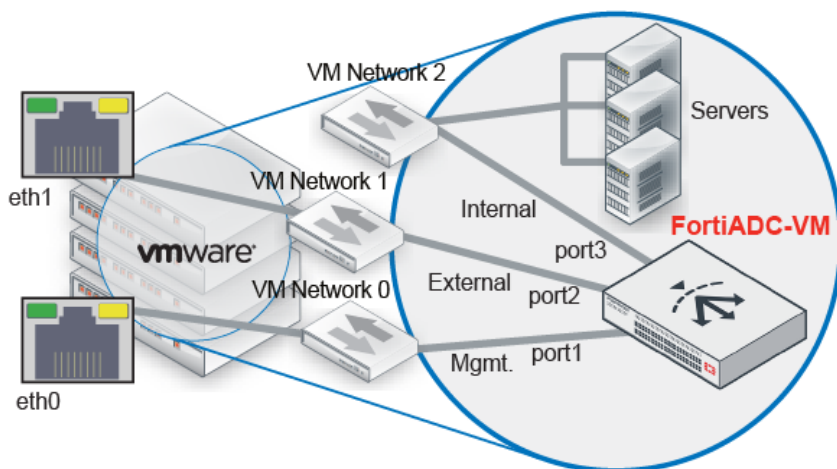
The appropriate mappings of the FortiADC-VM network adapter ports to the host computer physical ports depends on your existing virtual environment.



Often, the default bridging vNICs work, and do not need to be changed. If you are unsure of your network mappings, try bridging first before trying non-default vNIC modes such as NAT or host-only networks. The default bridging vNIC mappings are appropriate where each of the host's guest virtual machines have their own IP addresses on your network. The most common exceptions to this rule are for VLANs.

Example: Network mapping on page 23 illustrates how vNICs could be mapped to the physical network ports on a server.

Example: Network mapping



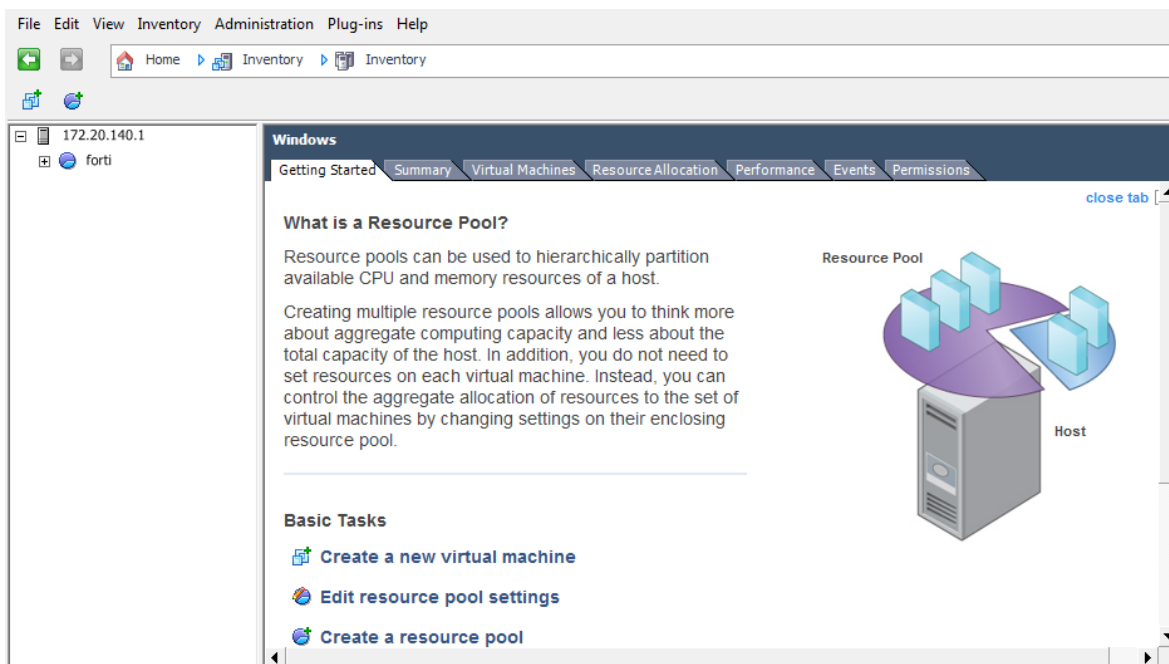
Example: Network mapping

VMware vSphere			FortiADC-VM
Physical Network Adapter	Network Mapping (vSwitch Port Group)	Virtual Network Adapter for FortiADC-VM	Network Interface Name in Web UI/CLI
eth0	VM Network 0	Management	port1

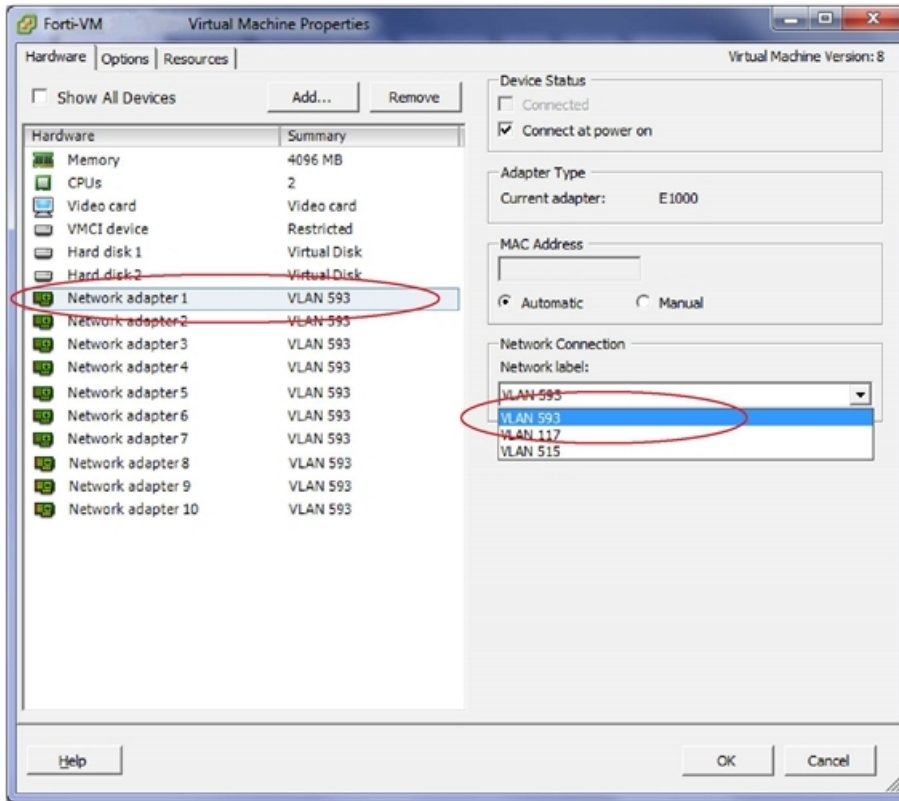
VMware vSphere Physical Network Adapter	Network Mapping (vSwitch Port Group)	Virtual Network Adapter for FortiADC-VM	FortiADC-VM Network Interface Name in Web UI/CLI
eth1	VM Network 1	External	port2
	VM Network 2	Internal	port3
			port4
			port5
			port6
			port7
			port8
			port9
			port10

To map network adapters:

1. Use the VMware vSphere client to connect to VMware vSphere server. The following figure shows the vSphere client manager window.



2. In the left pane, right-click the name of the virtual appliance, such as **FortiADC-VM-Doc**, then select **Edit Settings**. The virtual appliance properties dialog appears.
3. In the list of virtual hardware on the left side of the dialog, click the name of a virtual network adapter to see its current settings.

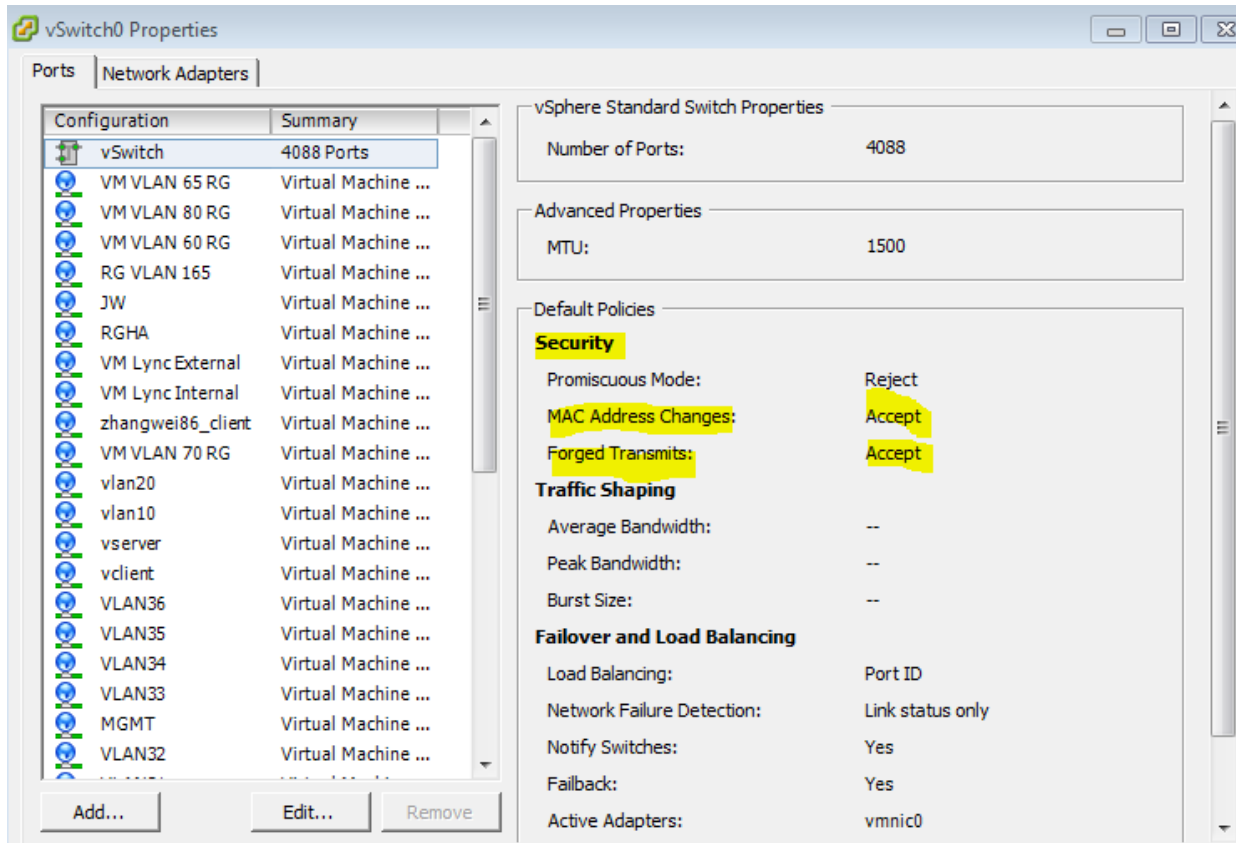


4. From the Network Connection drop-down menu, select the virtual network mapping for the virtual network adapter.
The correct mapping varies by the virtual environment network configuration. In the example illustration above, the vNIC **Network adapter 1** is mapped to the virtual network (vNetwork) named **VLAN 593**.
5. Click **OK**.

HA Configuration

When configuring HA on FortiADC appliances using VMware VMs, ensure that the vSwitch can accept MAC Address Changes and Forced Transmits on the HA Heartbeat VLAN. For more information, see the [FortiADC D-Series Handbook](#).

The illustration below shows what the vSwitch Properties page looks like with these settings enabled



config drive (vmware)

Mount ISO to get metadata, userdata, and license

License

```
config-drive/openstack/content/0000
```

```
-----BEGIN FAD VM LICENSE-----
```

```
.....
```

```
-----END FAD VM LICENSE-----
```

Userdata

```
config-drive/openstack/latest/user_data
config system global
set hostname Test
end
```

Metadata

```
config-drive/openstack/latest/meta_data.json
{
  "public_keys":{
```

```

    "key": "ssh-rsa xxxxxxxxxxxx"
  }
}

```

Do ISO image

```
xorriso -as mkisofs -V config-2 -o Drive.iso config-drive/
```

Mount ISO to get file, set license, ssh-key, and run script

Step 3: Power on the virtual appliance

After the virtual appliance software has been deployed and its virtual hardware configured, you can power on the virtual appliance.

Before you begin:

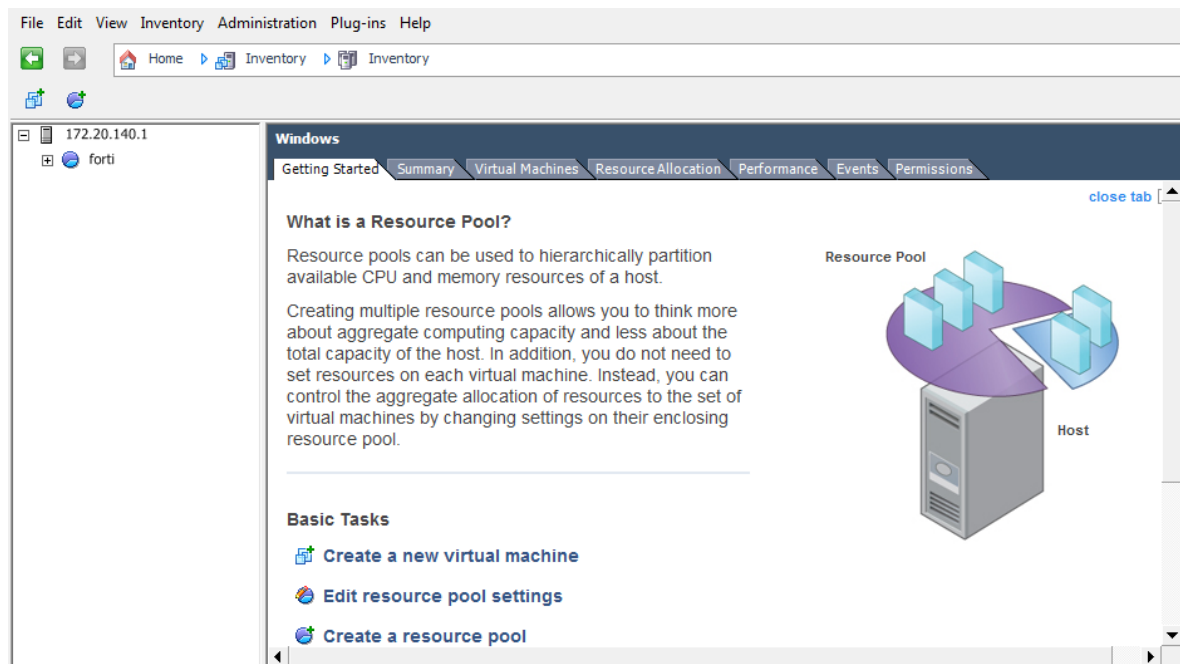
- You must have resized the disk (VMDK).
- You must have resized the CPUs and RAM, if necessary.
- You must have mapped the virtual network adapters if the defaults are not appropriate.

These settings must be configured in virtual machine environment. You do not configure them in the FortiADC OS.

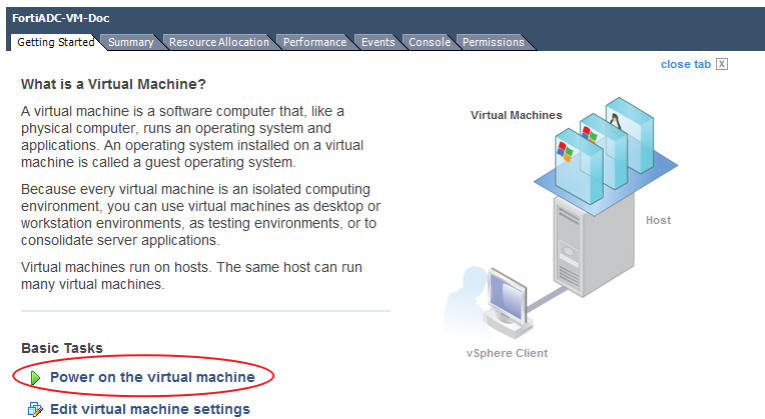
To power on FortiADC-VM:

1. Use the VMware vSphere client to connect to VMware vSphere server.

The following figure shows the vSphere client manager window.



2. In the left pane, click the name of the virtual appliance, such as **FortiADC-VM-Doc**.
3. Click the **Getting Started** tab.



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

Step 4: Configure access to the web UI & CLI

Once it is powered on, you must log into the FortiADC-VM command-line interface (CLI) via the VMware vSphere console and configure basic network settings so that you can connect to the web UI and/or CLI of the appliance through your management computer's network connection.

To configure basic network settings:

1. Use the VMware vSphere Client to log into the vSphere server.
2. In the left pane, select the name of the virtual appliance, such as **FortiADC-VM-Doc**.
3. Click the **Console** tab to open the console of the FortiADC-VM virtual appliance.
4. At the login prompt, type `admin` and no password to log in.
5. Configure the management interface, static route, and DNS server so you can access the system from a secure management network. Use the following command syntax:

```
config system interface
  edit port1
    set ip <address/mask>
    set allowaccess {http https ping snmp ssh telnet}
  end
config router static
  edit 1
    set gateway <gateway_address>
  end
config system dns
  set primary <dns_address>
  set secondary <dns_address>
end
```

where:

- `<address/mask>` is either the IP address and netmask assigned to the network interface, such as `192.168.1.99/24`; the correct IP will vary by your configuration of the vNetwork.

- `<gateway_address>` is IP address of the next hop router for port1.
- `<dns_address>` is the IP address of a DNS server

You should now be able to connect via the network from your management computer to `port1` of FortiADC-VM using:

- a web browser for the web UI (e.g. If `port1` has the IP address 192.168.1.1, go to `https://192.168.1.1/`).
- an SSH client for the CLI (e.g. If `port1` has the IP address 192.168.1.1, connect to 192.168.1.1 on port 22).

Step 5: Upload the license file

When you purchase a license for FortiADC-VM, Technical Support provides a license file that you can use to convert the 15-day trial license to a permanent, paid license.

You can upload the license via a web browser connection to the web UI. No maintenance period scheduling is required: it will not interrupt traffic, nor cause the appliance to reboot.

To upload the license via the web UI:

1. On your management computer, start a web browser.
Your computer must be connected to the same network as the hypervisor.
2. In your browser's URL or location field, enter the IP address of port1 of the virtual appliance, such as:
`https://192.168.1.99/`.
3. Use the username `admin` and no password to log in.
The system presents a self-signed security certificate, which it presents to clients whenever they initiate an HTTPS connection to it.
4. Verify and accept the certificate, and acknowledge any warnings about self-signed certificates.
The web UI opens to the dashboard.
5. In the System Information portlet, use the **update** link and the **Browse** button to upload the license file (.lic).

After the license has been validated, the System Information widget indicates the following:

- License row: The message: Valid: License has been successfully authenticated with registration servers.
- Serial Number row: A number that indicates the maximum number of vCPUs that can be allocated according to the FortiADC-VM software license, such as `FADV0100000028122` (where "V01" indicates a limit of 1 vCPUs).

If logging is enabled, this log message will also be recorded in the event log:

```
"VM license has been updated by user admin via GUI(192.0.2.40)"
```

If the update did not succeed, on FortiADC, verify the following settings:

- time zone & time
- DNS settings
- network interface up/down status
- network interface IP address
- static routes

On your computer, use `nslookup` to verify that FortiGuard domain names are resolving (VM license queries are sent to `update.fortiguard.net`).

```
C:\Users\username>nslookup update.fortiguard.net
Server: google-public-dns-a.google.com
Address: 8.8.8.8
```

```
Non-authoritative answer:
Name: fds1.fortinet.com
Addresses: 209.66.81.150
209.66.81.151
208.91.112.66
Aliases: update.fortiguard.net
```

On FortiADC, use `execute ping` and `execute traceroute` to verify that connectivity from FortiADC to the Internet and FortiGuard is possible. Check the configuration of any NAT or firewall devices that exist between the FortiADC appliance and the FDN or FDS server override.

```
FortiADC # exec traceroute update.fortiguard.net
traceroute to update.fortiguard.net (209.66.81.150), 32 hops max, 84 byte packets
 1 192.0.2.2 0 ms 0 ms 0 ms
 2 209.87.254.221 <static-209-87-254-221.storm.ca> 4 ms 2 ms 3 ms
 3 209.87.239.161 <core-2-g0-3.storm.ca> 2 ms 3 ms 3 ms
 4 67.69.228.161 3 ms 4 ms 3 ms
 5 64.230.164.17 <core2-ottawa23_POS13-1-0.net.bell.ca> 3 ms 5 ms 3 ms
 6 64.230.99.250 <tcore4-ottawa23_0-4-2-0.net.bell.ca> 16 ms 17 ms 15 ms
 7 64.230.79.222 <tcore3-montreal01_pos0-14-0-0.net.bell.ca> 14 ms 14 ms 15 ms
 8 64.230.187.238 <newcore2-newyork83_so6-0-0_0> 63 ms 15 ms 14 ms
 9 64.230.187.42 <bxX5-newyork83_POS9-0-0.net.bell.ca> 21 ms 64.230.187.93 <BX5-
    NEWYORK83_POS12-0-0_core.net.bell.ca> 17 ms 16 ms
10 67.69.246.78 <Abovenet_NY.net.bell.ca> 28 ms 28 ms 28 ms
11 64.125.21.86 <xe-1-3-0.cr2.lga5.us.above.net> 29 ms 29 ms 30 ms
12 64.125.27.33 <xe-0-2-0.cr2.ord2.us.above.net> 31 ms 31 ms 33 ms
13 64.125.25.6 <xe-4-1-0.cr2.sjc2.us.above.net> 82 ms 82 ms 100 ms
14 64.125.26.202 <xe-1-1-0.er2.sjc2.us.above.net> 80 ms 79 ms 82 ms
15 209.66.64.93 <209.66.64.93.t01015-01.above.net> 80 ms 80 ms 79 ms
16 209.66.81.150 <209.66.81.150.available.above.net> 83 ms 82 ms 81 ms
```

If the first connection had not succeeded, you can either wait up to 30 minutes for the next license query, or reboot.

```
execute reboot
```

If after 4 hours FortiADC still cannot validate its license, a warning message will be printed to the local console.

What's next?

At this point, the FortiADC virtual appliance is running, and it has received a license file, but its operating system is almost entirely unconfigured. See the [FortiADC Handbook](#) for information on getting started with feature configuration.

Upgrading the number of VM CPUs

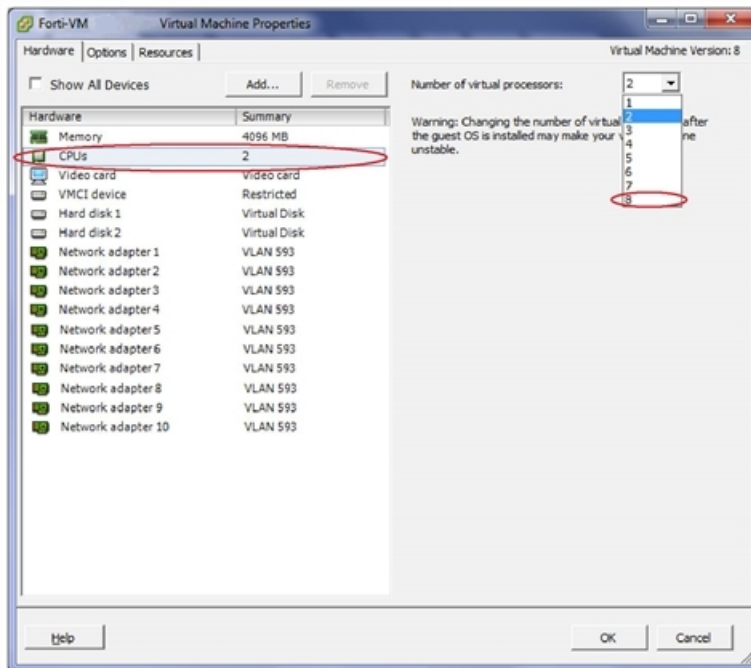
FortiADC-VM is licensed for either 1, 2, 4, 8, 16 or 32 CPUs. If you start with one license and outgrow it, you can upgrade.

Before you begin:

- You must purchase the new license and copy the license file to your management computer.
- Be aware that you must shut down FortiADC and power off the virtual machine to perform the upgrade.

To allocate more vCPUs:

1. In the FortiADC web UI, go to System > Status > Dashboard.
2. Upload the new license. For details, see [Uploading the license](#).
3. In the System Information widget, click **Shut Down**.
The virtual appliance will flush its data to its virtual disk, and prepare to be powered off. If you skip this step and immediately power off FortiADC-VM, you might lose buffered data.
4. On your management computer, log into the vSphere server.
5. In the left pane, click the name of the virtual appliance, such as **FortiADC-VM-Doc**.
6. Click the **Getting Started** tab.
7. Click **Power off the virtual machine**.
8. Increase the vCPU allocation. For details, see [Configuring the number of virtual CPUs \(vCPUs\)](#).



9. Power on the virtual appliance again.

Upgrading the virtual hardware

By default, the FortiADC-VM `fortiadc-vm-64-hw7.ovf` image uses VMware virtual hardware version 7. If you have a VMware ESXi 5.1 environment that supports virtual hardware version 9, and you want to provide version 9 feature support such as backups, you can update the virtual hardware.

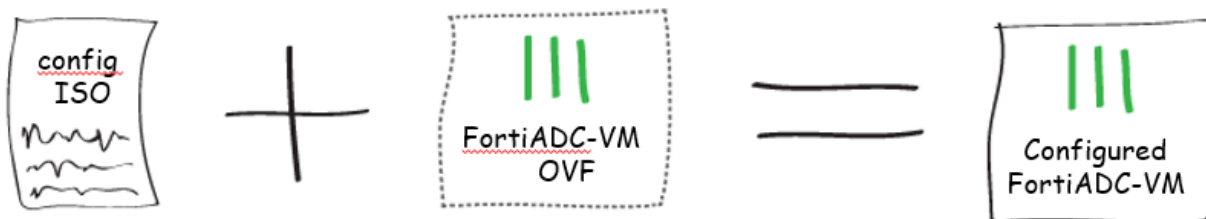
For more information on virtual hardware, see:

<http://kb.vmware.com/selfservice/documentLinkInt.do?micrositeID=&popup=true&languageId=&externalID=1010675>

To upgrade the virtual hardware:

1. Shut down FortiADC-VM. To do this, you can enter the CLI command:
`execute shutdown`
2. In VMware vCenter, right-click the VM and select **Power > Power Off**.
3. After it has been powered off, right-click the VM and select the option to upgrade the virtual hardware.
4. When the upgrade is complete, power on FortiADC-VM.

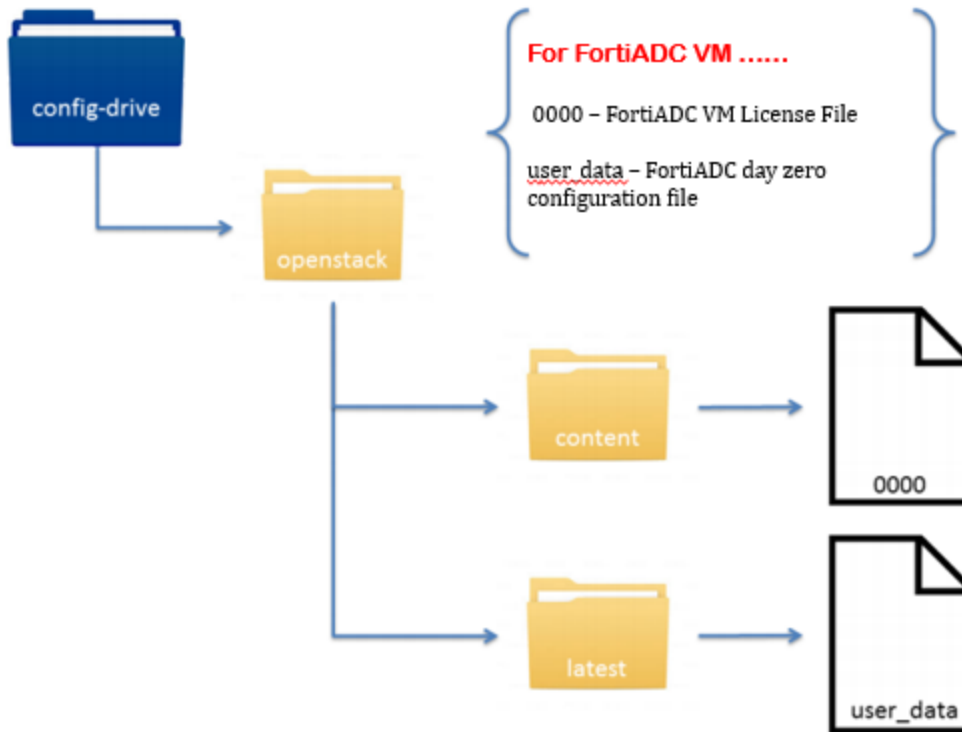
Cloud-init using config drive



This section describes how to bootstrap a FortiADC-VM in VMware vCenter using config drive. Use this guide if you are deploying VMs on VMware vCenter or standalone ESX and would like to preconfigure the FortiADC-VM so that it boots with a predetermined configuration, and a valid license.

Verify that the config drive functionality is available for your FortiADC-VM version in the release notes. FortiADC-VM supports version 2 of the config-drive capabilities. [Cloud-Init config drive](#) was initially created for OpenStack and other cloud environments and is a capability available on the FortiADC-VM even when booting within a VMware vCenter or standalone ESX environment. Config drive also allows the administrator to pass both day zero configuration scripts and FAD-VM licenses to the FortiADC on initial boot.

To pass a config drive to the FortiADC-VM, first you must create a directory structure, and place the license file and configuration script file in the appropriate places. Here is the directory structure you will need:



FortiADC-VM license file

The contents of the FAD-VM license file go into the 0000 file. Generally one would cat the license file and redirect the output into the config-drive/openstack/content/0000 file.

```
fad-user@ubuntu:/var/tmp$ cat config-drive/openstack/content/0000
-----BEGIN FAD VM LICENSE-----
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-# #-REDACTED-
  REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-# #-REDACTED-
  REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-#
-----END FAD VM LICENSE-----
fad-user@ubuntu:/var/tmp$
```

FortiADC configuration script

The configuration script for a FortiADC-VM uses standard FortiADC CLI syntax. Here is a simple example, where the hostname is Example-Day0 and port1 is configured to use your designated IP address:

```
fad-user@ubuntu:/var/tmp$ cat config-drive/openstack/latest/user_data
config system global
set hostname Example-Day0
end

config system interface
edit port1
set mode static
set ip 10.106.170.53/24
set allowaccess https ssh ping
```

```
end
fad-user@ubuntu:/var/tmp$
```

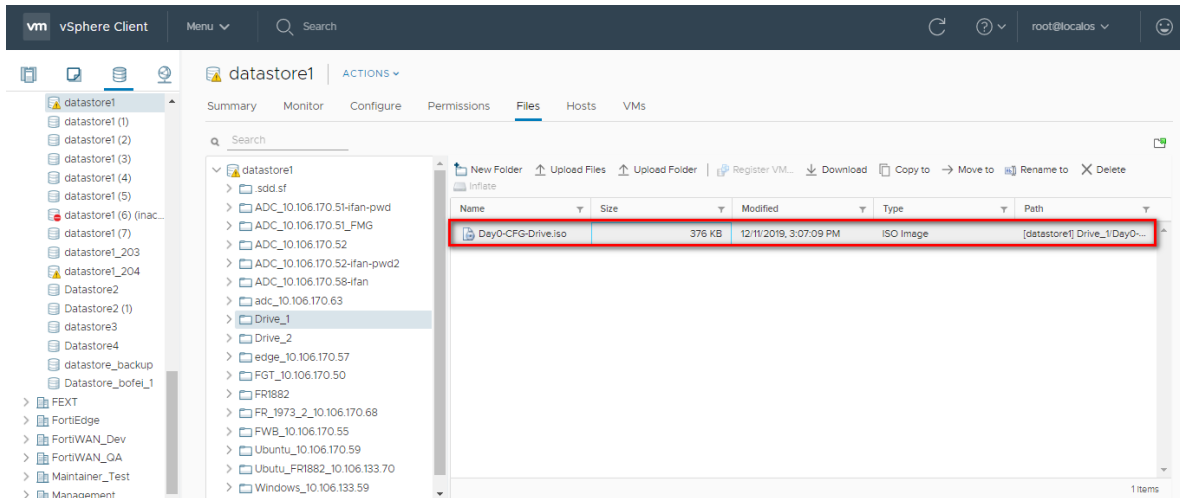
Create the Config Drive ISO

1. Create the config-drive ISO using a utility such as xorriso (other utilities can also be used to create ISOs, such as mkisofs). Using xorriso, this example refers to the config-drive directory created above with the relevant license file and configuration script. Here is an example of creating a config-drive ISO on an Ubuntu host:

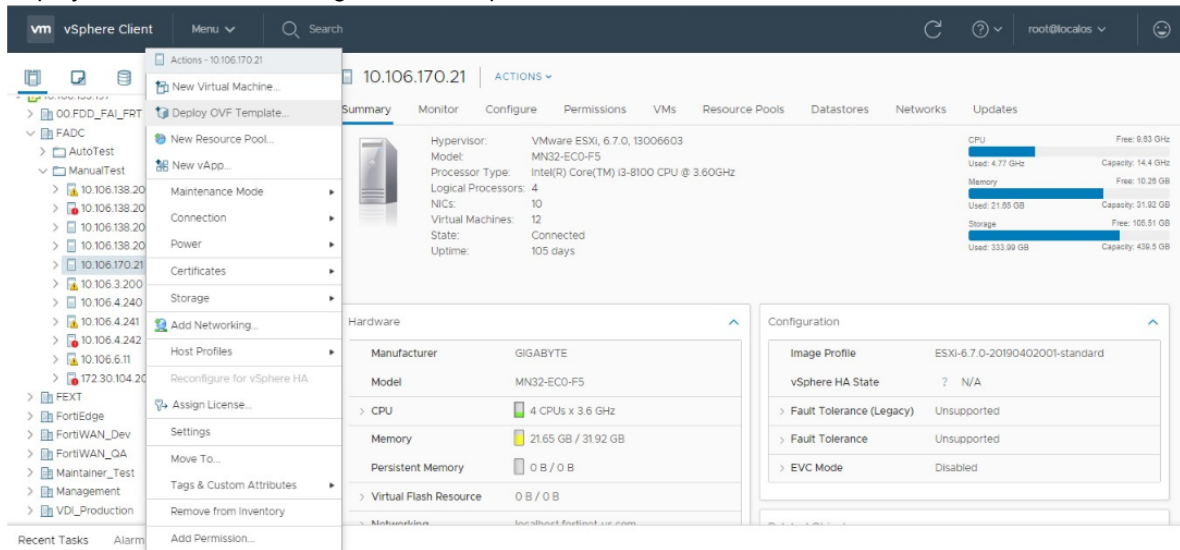
```
xorriso -as mkisofs -V config-2 -o Day0-CFG-Drive.iso config-drive/
xorriso 1.3.2 : RockRidge filesystem manipulator, libburnia project.
Drive current: -outdev 'stdio:Day0-CFG-Drive.iso'
Media current: stdio file, overwriteable
Media status : is blank
Media summary: 0 sessions, 0 data blocks, 0 data, 14.3g free
xorriso : WARNING : -volid text does not comply to ISO 9660 / ECMA 119 rules
Added to ISO image: directory '/'='/var/tmp/config-drive'
xorriso : UPDATE : 5 files added in 1 seconds
xorriso : UPDATE : 5 files added in 1 seconds
ISO image produced: 185 sectors
Written to medium : 185 sectors at LBA 0
Writing to 'stdio:Day0-CFG-Drive.iso' completed successfully.

ls -l Day0-CFG-Drive.iso
-rw-rw-r-- 1 fad-user fad-user 378880 Apr 2 13:32 Day0-CFG-Drive.iso
```

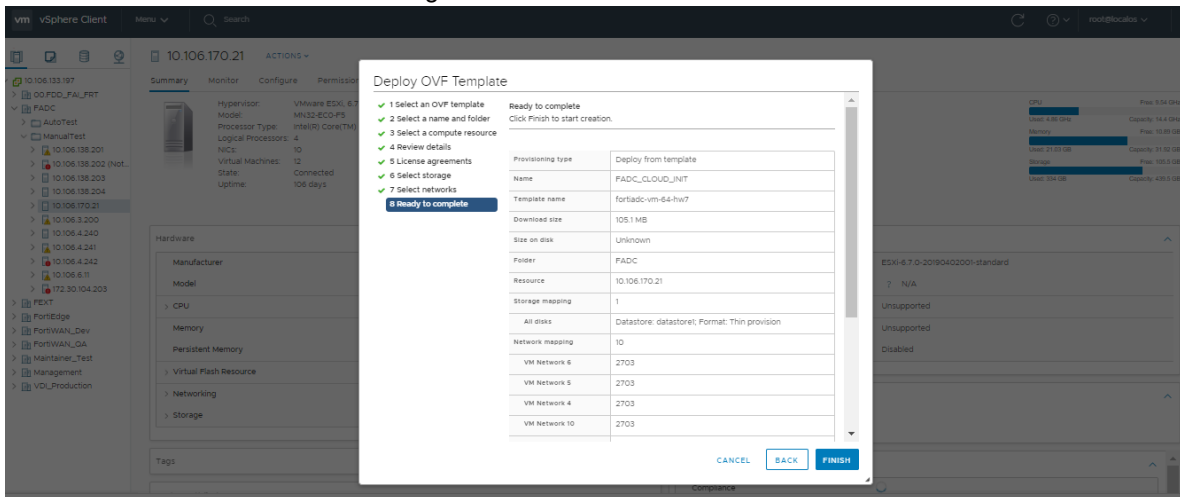
2. Now that the configuration drive has been created, place the ISO on the data store so that it can be used with FortiADC-VMs.



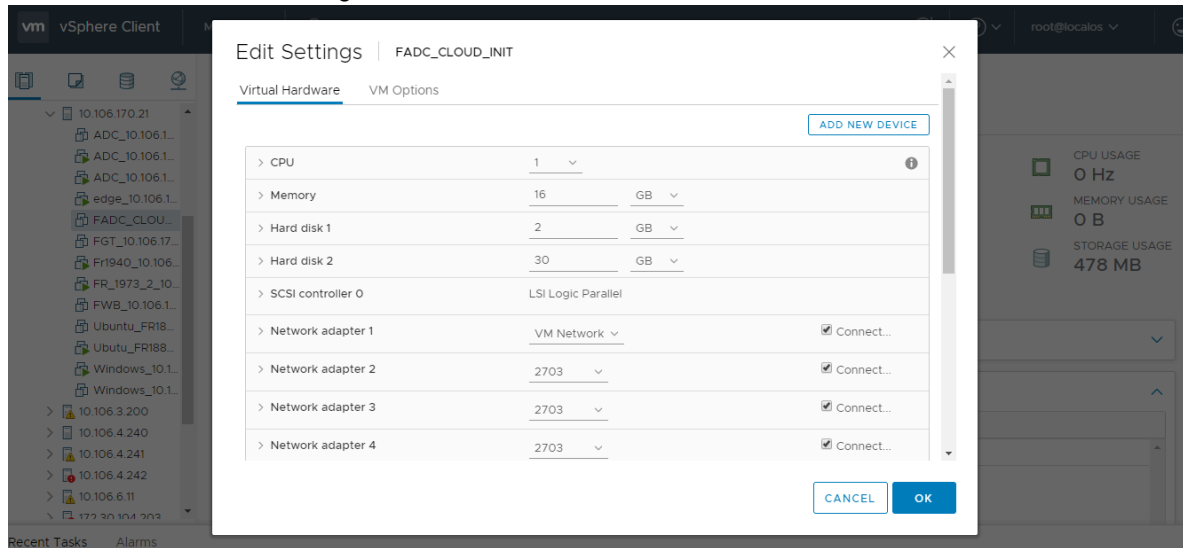
3. Deploy the FortiADC-VM using an OVF template.



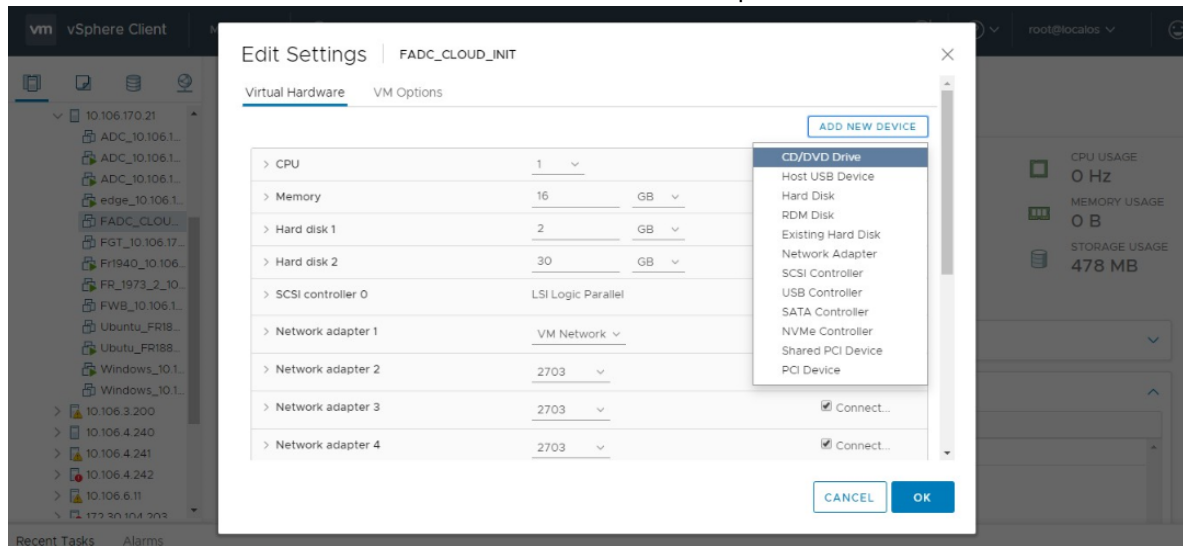
4. Once you reach the end of the OVF template deployment Ensure to deselect Power on after deployment if has. This is so we can attach our config-drive ISO as a cdrom device before initial boot.



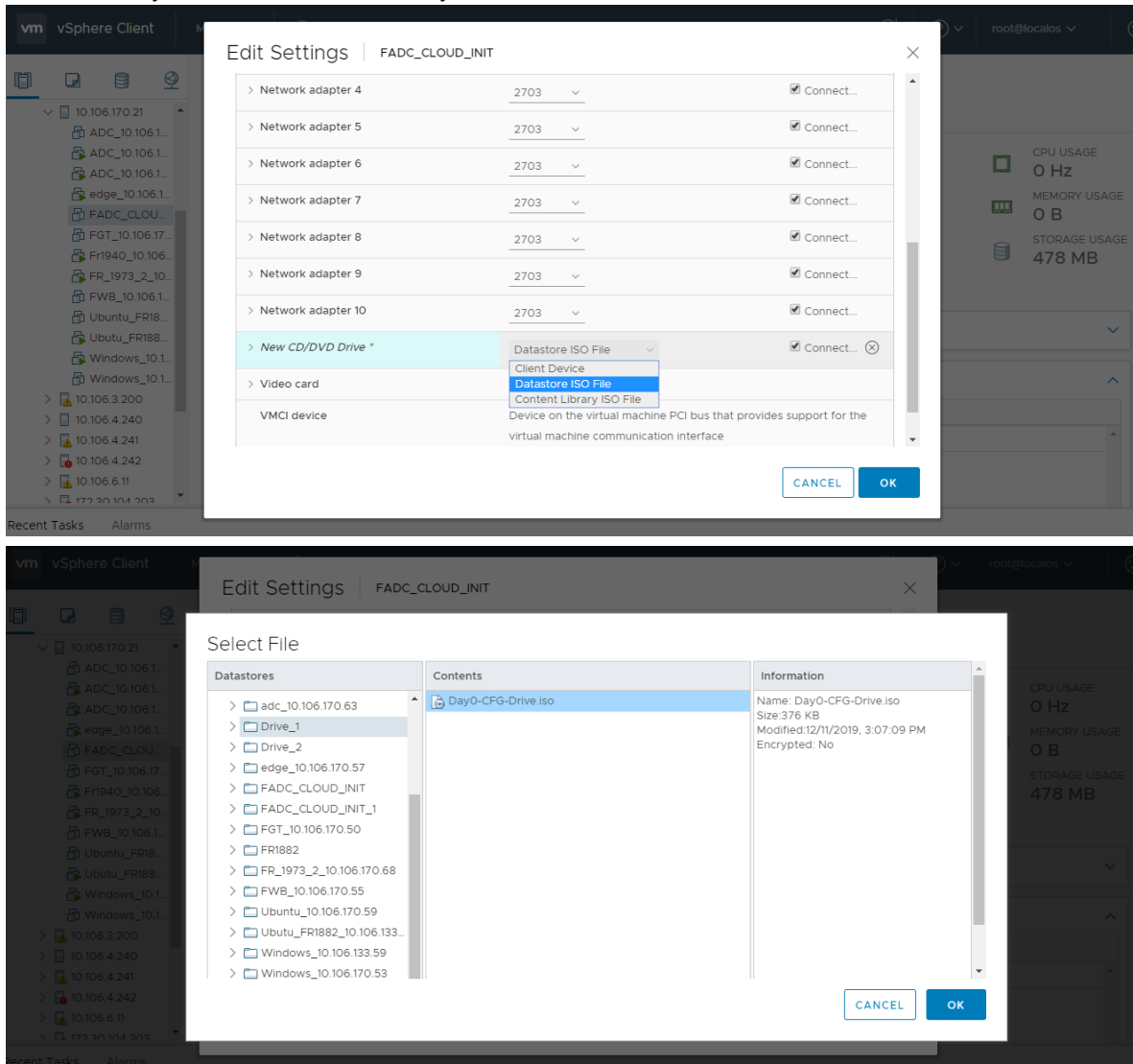
5. Edit the virtual machine settings.



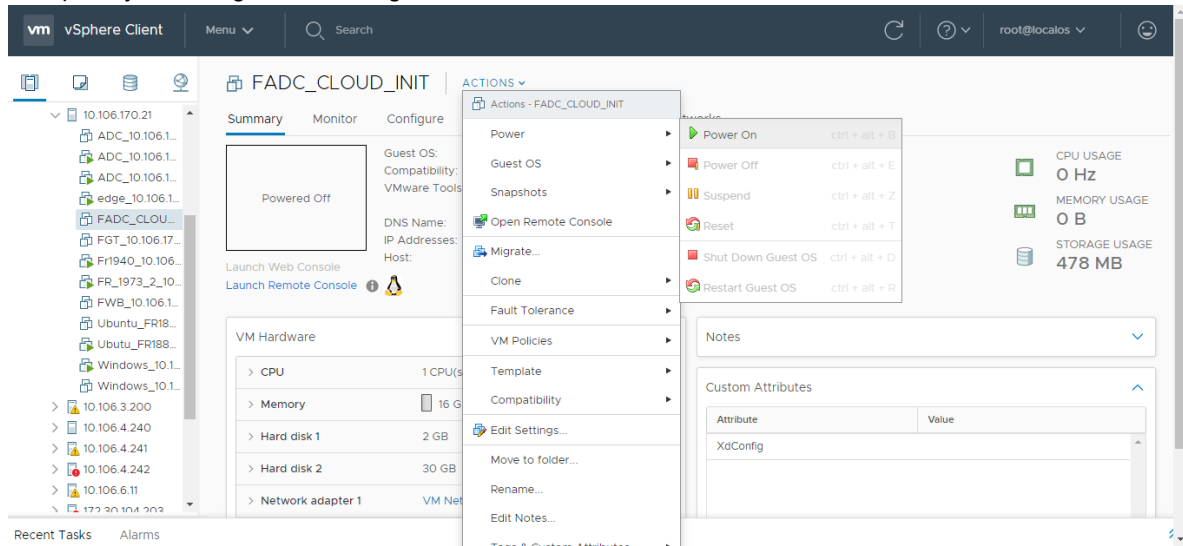
6. Add a new device: CD/DVD drive and Ensure to select Connect at power on.



7. Attach the Day0-CFG-Drive.iso ISO that you created earlier.



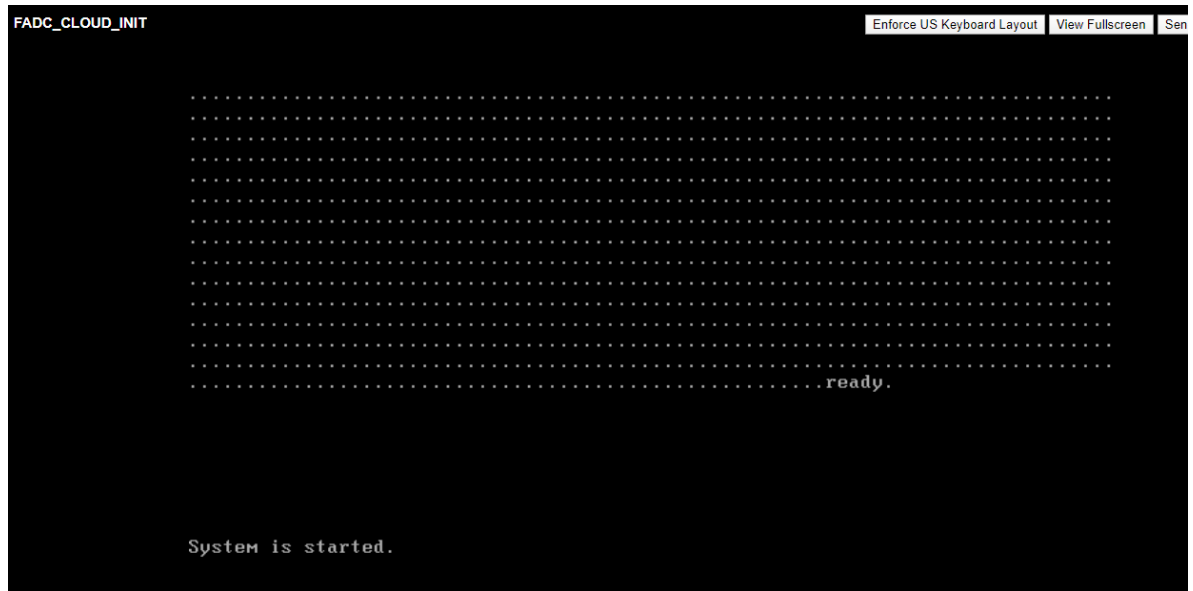
8. Complete your changes, then navigate to the VM to boot it.



Results and verification

Boot the FortiADC-VM and open the console to verify that the VM is booting and utilizing the license file and day zero configuration file that was provided. Follow these verifications steps:

1. Power on the VM.



- Go to the Console. Verify that you see the Configuration and VM license installed message and the subsequent reload.

```
FADC_CLOUD_INIT Enforce US Keyboard Layout | View Fullscreen | Send Ctrl+Alt+Delete
.....
.....
.....ready.

System is started.

FortiADC-UM login:
Initialize from config drive
Configuration applied
License installed.
Remove old status failed 2
Serial Number: FADU000000184361

Ready to reload system.
```

- Upon completion of the boot sequence, you can verify that the FortiADC-VM hostname changed to ExampleDay0. Also verify that the license file is verified and the license registration status changed to VALID.

```
Remove old status failed 2
Serial Number: FADU000000184361

Ready to reload system.

The system is reloading.....

FortiADC-UM login: admin
Password:
You are forced to change your password, please input a new password.
New Password: *****
Confirm Password: *****
Welcome!

Example-Day0 #
```

- After logging in, use the get system status command to verify that the license is upload.

```
FADC_CLOUD_INIT Enforce US Keyboard Layout | View Fullscreen | Send Ctrl+Alt+Delete

System Time: Thu Apr 02 16:57:03 PDT 2020

Example-Day0 # get system status
Version: FortiADC-UM v5.4.1.build0728.200331
UM Registration: Valid: License has been successfully authenticated with registration servers.
UM License File: License file and resources are valid.
UM Resources: 1 CPU/8 allowed, 15915 MB RAM, 29 GB Disk
Serial-Number: FADU000000184361
WAF Signature DB: 00001.00026 (Expire: 2020-4-13)
IP Reputation DB: 00004.00636 (Expire: 2020-4-13)
Geography IP DB: 00002.00050
Geography Regions: 00002.00024 (CN)
Web Filter: (Expire: 2020-4-13)
Credential Stuffing DB: 00000.00000
Regular Virus DB: 00001.00123 (Expire: 2020-4-13)
Extended Virus DB: 00000.00000 (Expire: 2020-4-13)
Extreme Virus DB: 00000.00000 (Expire: 2020-4-13)
AV Engine: 00006.00006 (Expire: 2020-4-13)
IPS-DB: 00006.00741 (Expire: 2020-4-13)
IPS-ETDB: 00000.00000 (Expire: 2020-4-13)
IPS Engine: 00004.00021 (Expire: 2020-4-13)
Bootloader Version: n/a
Hard Disk: Capacity 29 GB, Used 83 MB ( 0.28%), Free 29 GB
```

5. Use the get system interface port1 to verify that port1 is configured.

```

FADC_CLOUD_INIT
Example-Day0 #
Example-Day0 #
Example-Day0 #
Example-Day0 # get system interface port1
type                : physical
dedicate-to-mgmt    : disable
mode                : static
vdom                : root
redundant-master    :
ip                  : 10.106.170.53/23
ip6                 : ::0
allowaccess         : https ping ssh
mtu                 : 1500
speed               : auto
status              : up
retrieve_physical_hwaddr : disable
mac-addr            : 00:50:56:a9:77:a3
flow-sniffer        : disable
wccp                : disable
secondary-ip        : disable
ha-node-secondary-ip : disable
traffic-group       :
floating            : disable
Example-Day0 #

```

ESXi cloud init reference

For ESXi the utility xorriso is used on a Linux host to create the ISO used to boot the VM. The directory structure used to create the ISO is described below.

After the ISO is created you must upload it to your datastore of choice and attach it to the FortiADC-VM after deploying the OVF but before booting it up for the first time.

ls -lR config-drive/

```

config-drive/: total 4
drwxrwxr-x 4 fad-user fad-user 4096 Apr 2 11:59 openstack

```

config-drive/openstack:

```

total 8
drwxrwxr-x 2 fad-user fad-user 4096 Apr 2 12:07 content
drwxrwxr-x 2 fad-user fad-user 4096 Apr 2 12:06 latest

```

config-drive/openstack/content:

```

total 4
-rw-rw-r-- 1 fad-user fad-user 287 Apr 2 11:00 0000

```

config-drive/openstack/latest:

```

total 4
-rw-r--r-- 1 fdc-user fdc-user 172 Apr 2 11:06 user_data

```

cat config-drive/openstack/content/0000

```

-----BEGIN FAD VM LICENSE-----
#-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-# #-REDACTED-
  REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-# #-REDACTED-
  REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-REDACTED-#
-----END FAD VM LICENSE-----

```

cat config-drive/openstack/latest/user_data

```

config system global
set hostname Example-Day0
end
config system interface

```



```
edit port1
set mode static
set ip 10.106.170.53/24
set allowaccess https ssh ping
end
```

```
xorriso -as mkisofs -V config-2 -o Day0-CFG-Drive.iso config-drive/
xorriso 1.3.2 : RockRidge filesystem manipulator, libburnia project.
Drive current: -outdev 'stdio:Day0-CFG-Drive.iso' Media current: stdio file,
overwriteable
Media status : is blank
Media summary: 0 sessions, 0 data blocks, 0 data, 14.3g free
xorriso : WARNING : -volid text does not comply to ISO 9660 / ECMA 119 rules Added to
ISO
image:
directory '/'='/var/tmp/config-drive'
xorriso : UPDATE : 5 files added in 1 seconds xorriso : UPDATE : 5 files added in 1
seconds
ISO
image produced: 185 sectors
Written to medium : 185 sectors at LBA 0
Writing to 'stdio:Day0-CFG-Drive.iso' completed successfully.
```

```
ls -l Day0-CFG-Drive.iso
-rw-rw-r-- 1 fad-user fad-user 378880 Apr 2 11:32 Day0-CFG-Drive.iso
```



FORTINET[®]



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.