



FortiADC - VM Installation - Xen Project

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 - Xen Project

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 Xen Project	12
Installation overview	12
Step 1: Bridge to one of the Xen server physical network interfaces	13
Step 2: Create the VM instance logical volume	14
Step 3: Deploy the VM image file	15
Deploying via Virtual Machine Manager	15
Deploying via dom0 command line	22
Step 4: Configure access to the web UI & CLI	26
Step 5: Upload the license file	27
What's next?	29

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

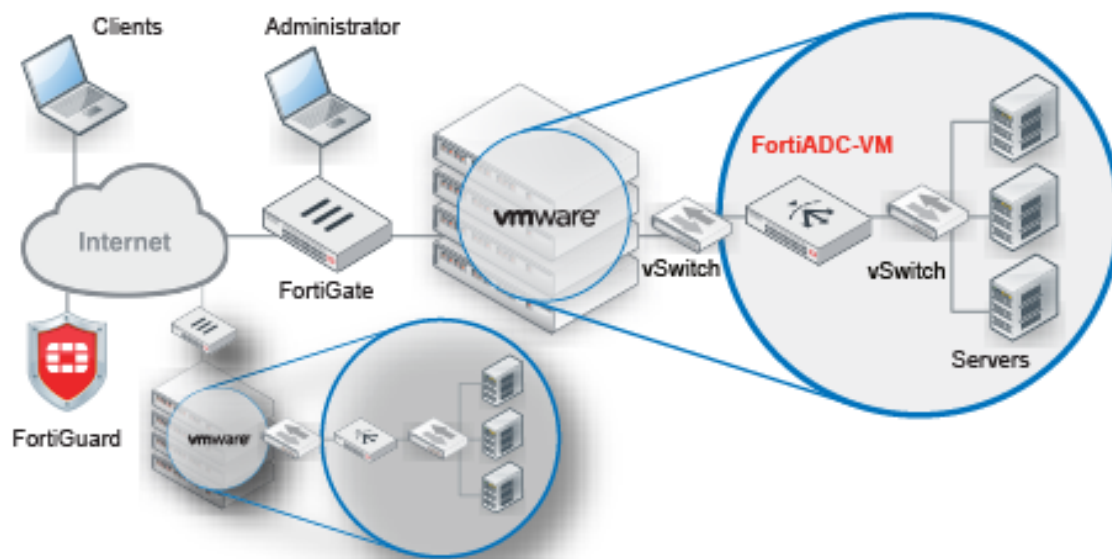
Welcome, and thank you for selecting Fortinet Technologies, Inc. products for your network. The FortiADC D-series family of Application Delivery Controllers (ADC) optimizes the availability, user experience, performance and scalability of enterprise application delivery.

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

The screenshot shows the Fortinet Customer Service & Support website. The top navigation bar includes the Fortinet logo, a 'Home' button, and links for 'Asset', 'Assistance', 'Download', and 'Feedback'. A 'LOG OUT' button is visible in the top right corner. The main content area is divided into several sections:

- Asset**: Contains three main options:
 - Register/Renew**: Register HW/Virtual appliance or software; Activate service contract or license on your registered product. (This option is highlighted with a red box in the original image.)
 - Manage Products**: Search, update or generate report for your registered products. Like product entitlement, description, location, entitlement and reseller etc.
 - Purchase Services**: Extend your expiring services at our on-line renewal store.
- Download**: Contains four options:
 - Service Updates
 - Firmware Images**: (This option is highlighted with a red box in the original image.)
 - Firmware Checksums
 - HQIP Images
- Quick Links**: Contains two columns of links:
 - TAC Forti-Companion
 - RMA Forti-Companion
 - Tickets Creation Guide
 - Product Life Cycle
 - FortiCare Terms & Conditions
 - Help Documents
- Resources**: Contains a list of links:
 - Knowledge Base
 - Fortinet Video Library
 - Fortinet Document Library
 - Discussion Forums
 - Training & Certification
- FortiGuard**: Contains a list of links:
 - Advisories & Reports
 - FortiGuard Blog
 - FortiGuard Services
 - Global Threat Level
 - Security Tools
 - Resources Library
- Programs**: Contains a list of links:
 - Support Offerings
 - Premium Support
 - Premium RMA
 - Professional Services
 - Beta Program

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

FortiADC

Release Notes

Download

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

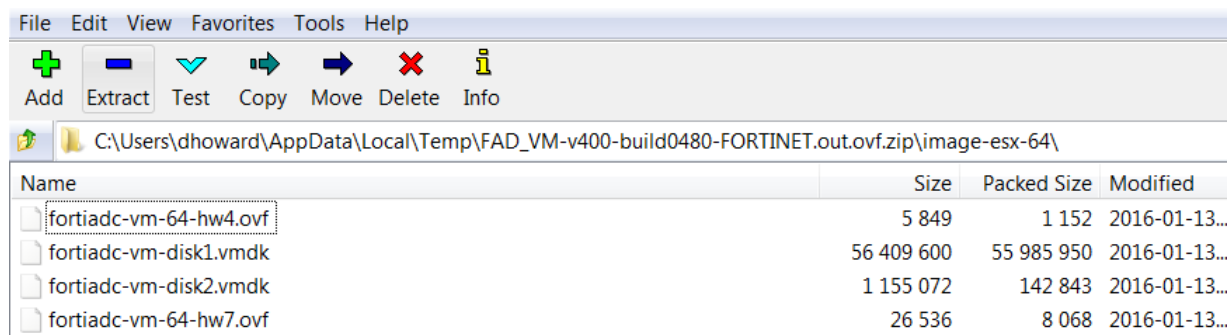
Name	Size (KB)	Date Created	Date Modified
 FAD_1500D-v400-build0480-FORTINET.out	59,537	2016-01-15 12:01:51	2016-01-15 12:01:51
 FAD_2000D-v400-build0480-FORTINET.out	58,830	2016-01-15 12:01:13	2016-01-15 12:01:13
 FAD_200D-v400-build0480-FORTINET.out	56,078	2016-01-15 12:01:47	2016-01-15 12:01:47
 FAD_300D-v400-build0480-FORTINET.out	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.

- 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 fortiaadc-vm-64-hw4.ovf file is a VMware virtual hardware version 4 image that supports ESXi 3.5.</p> <p>The fortiaadc-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	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.
KVM	The kvm.zip download file contains the boot.qcow2 and data.qcow2 files you use for the installation.
Citrix Xen	The xenserver.zip download file contains the fortiaadc-vm-xen.ovf file you use for the installation.
Xen Project	The xenopensource.zip download file contains the fortiaadc.hvm, bootdisk.img, and logdisk.img files you use for the installation.

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 Xen Project

This chapter provides procedures for FortiADC-VM on Xen Project. It includes the following information:

Installation overview	12
Step 1: Bridge to one of the Xen server physical network interfaces	13
Step 2: Create the VM instance logical volume	14
Step 3: Deploy the VM image file	15
Deploying via Virtual Machine Manager	15
Deploying via dom0 command line	22
Step 4: Configure access to the web UI & CLI	26
Step 5: Upload the license file	27
What's next?	29



Before upgrading the image to v5.1.0, increase the size of the bootdisk.img to 2 GB.

The size of the bootdisk.img was less than 2G before v5.1.0. If you deploy an ADC after v5.1.0, bootdisk.img is 2GB by default.

How to resize the boot disk

1. Power off the ADC
2. Go to KVM host machine, entering the ADC installation directory.
3. Execute the following command: `qemu-img resize bootdisk.img +1G`

Installation overview

FortiADC-VM is deployed as a fully virtualized `domU` virtual machine.

To deploy FortiADC-VM on an open source Xen Project hypervisor/XAPI cloud, you can use either the `dom0` virtual machine's:

- command line or
- desktop environment, such as GNOME or KDE

Once FortiADC-VM is deployed, however, either your Xen server itself or your management computer must have a desktop environment.

`sudo xm console <domain_int>` using an alias to `/dev/pty` does not succeed. Instead, VNC is required to connect to FortiADC-VM's virtual local console.

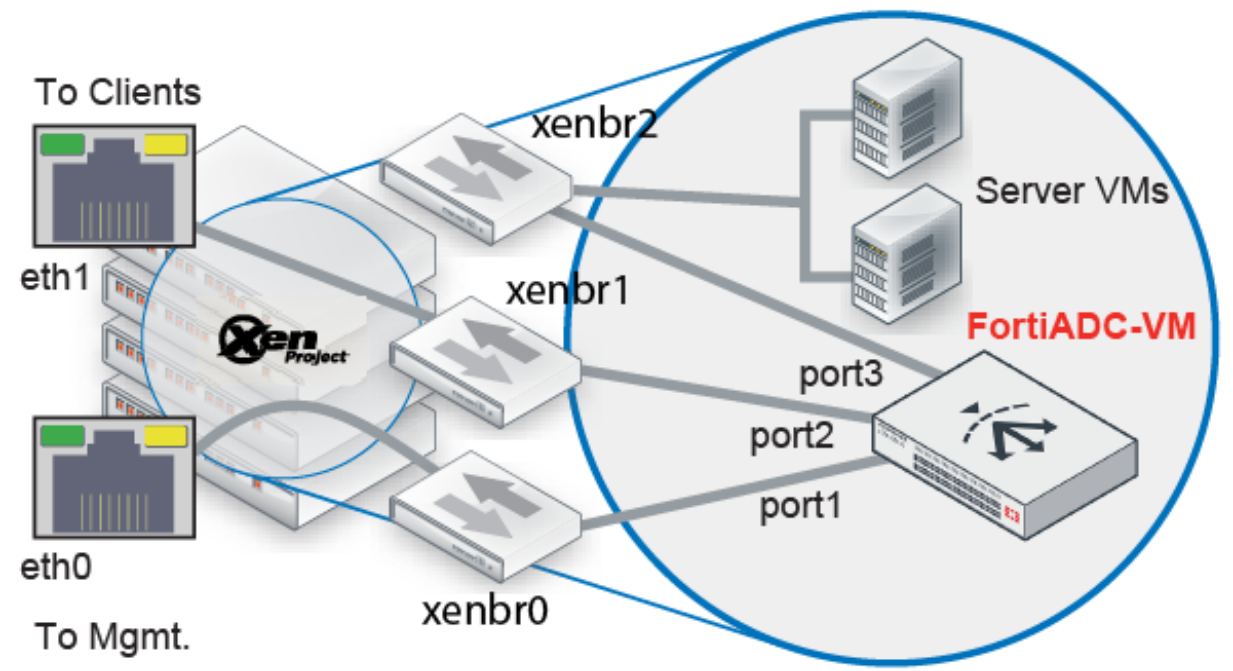
Step 1: Bridge to one of the Xen server physical network interfaces

If you have not yet installed the network bridge utilities required by Xen in order to bridge the virtual machine vNICs to the hypervisor network connection, you must do that by installing the bridge network utilities and then editing the network interface configuration.

```
sudo apt-get install bridge-utils
sudo nano /etc/network/interfaces
```

When editing the network interface configuration, usually you should bind the bridge (in the `vif` examples, the bridge is `xenbr0`) to one of your network interfaces (e.g. `eth0`) in `/etc/network/interfaces`. Depending on the number of physical interfaces on the server and how you will map them to vNetworks, you may need to create multiple bridges.

The following table provides an example of how vNICs could be mapped to the physical network ports on a server with two physical NICs.



Example: Network mapping for reverse proxy mode

Xen Project		FortiADC-VM	
Physical Network Adapter	Network Mapping (vSwitch Port Group)	Virtual Network Adapter for FortiADC-VM	Network Interface Name in Web UI/CLI

Xen Project			FortiADC-VM
eth0	xenbr0	Management	port1
eth1	xenbr1	External	port2
	xenbr2	Internal	port3

Below is a configuration example assuming the server has only one physical NIC, eth0:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet manual

auto xenbr0
iface xenbr0 inet static
address 192.0.2.10
netmask 255.255.255.0
gateway 192.0.2.1
```

Step 2: Create the VM instance logical volume

You must create the logical volume that FortiADC-VM will use to store its vDisks. In this case, the logical volume is on the Xen server's local disk, but usually it is preferable to store it on an NFS or CIFS share.

To create a local logical volume:

1. Connect to the command line in dom0 on the Xen server where you will deploy FortiADC-VM (for example, via an SSH client such as PuTTY).
2. Find the name of your dom0 logical volume group. (Volume group is highlighted below in bold).

```
xenuser@LabXen:~$ sudo pvs
[sudo] password for xenuser:
PV VG Fmt Attr PSize PFree
/dev/sda5 LabXen-vg lvm2 a- 698.39g 673.45g
```

3. Create a logical volume. In this case, the logical volume is on the Xen server's local disk, but you could store it on an NFS or CIFS share.

```
sudo lvcreate -L 100G -n fortiadc-vm /dev/LabXen-vg
```

where you would replace:

- 100G — The amount of disk space to allocate to FortiADC-VM's vDisk in gigabytes.
- fortiadc-vm — The name of your virtual machine, as it appears in Virtual Machine Manager or when you use the `xm` command to create the virtual machine.
- LabXen-vg — The name of your dom0 volume group according to the output of the `sudo pvs` command.

Step 3: Deploy the VM image file

This section describes two options for deploying the VM image file:

- [Deploying via Virtual Machine Manager](#)
- [Deploying via dom0 command line](#)

Deploying via Virtual Machine Manager

If you have not yet installed a graphical centralized management tool for Xen on your management computer, begin by installing it. Multiple clients exist for managing Xen Project servers. In these instructions, we use Virtual Machine Manager.

On Debian-related Linux distributions, to install Virtual Machine Manager, open a terminal and enter:

```
sudo apt-get install virt-manager
```

On Red Hat-related Linux distributions, the command is :

```
sudo yum virt-manager
```

This centralized manager includes a Xen client for connecting to a remote Xen Project hypervisor to deploy FortiADC-VM. It also includes a built-in VNC client that you will need later in order to connect to FortiADC-VM's local console and configure its network connection. When the download and installation is complete, if you are not already logged into your desktop environment (GNOME, KDE, xfce, etc.), start X Windows and log in.

To enable Virtual Machine Manager to connect to your Xen server, you must also modify the **server's** configuration file (usually `/etc/xen/xend-config.sxp`). Un-comment these lines (remove the hash (`#`) from the beginning) and change 'no' to 'yes':

```
(xend-unix-server yes)
(xend-unix-path /var/lib/xend/xend-socket)
```

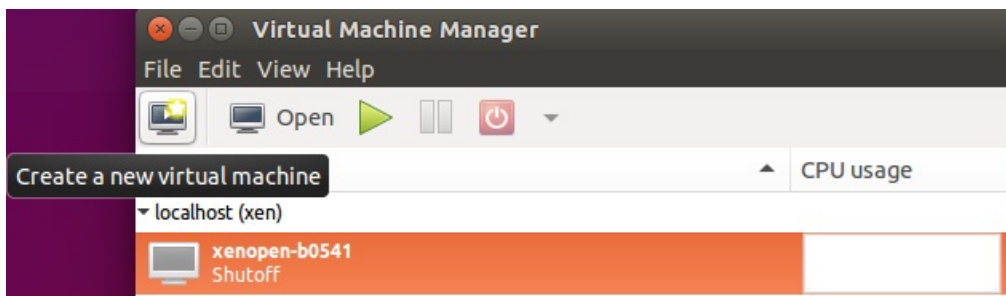
To deploy the VM image using Virtual Machine Manager:

1. On your management computer, open a terminal application and enter the command to extract the package to a folder, then start Virtual Machine Manager:

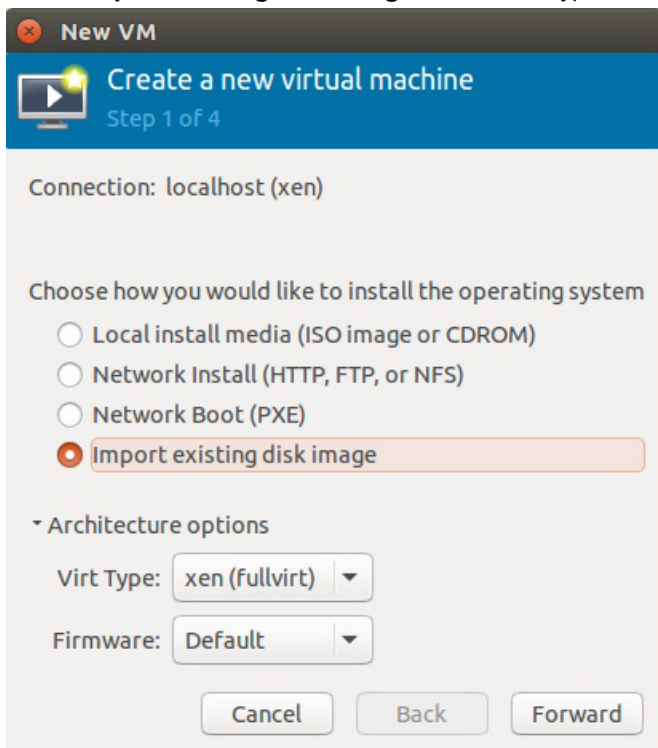
```
unzip FAD_XENOPEN-v400-build0547-FORTINET.out.xenopensesource.zip
sudo virt-manager
```

The application will open in your desktop environment, so its appearance might vary slightly.

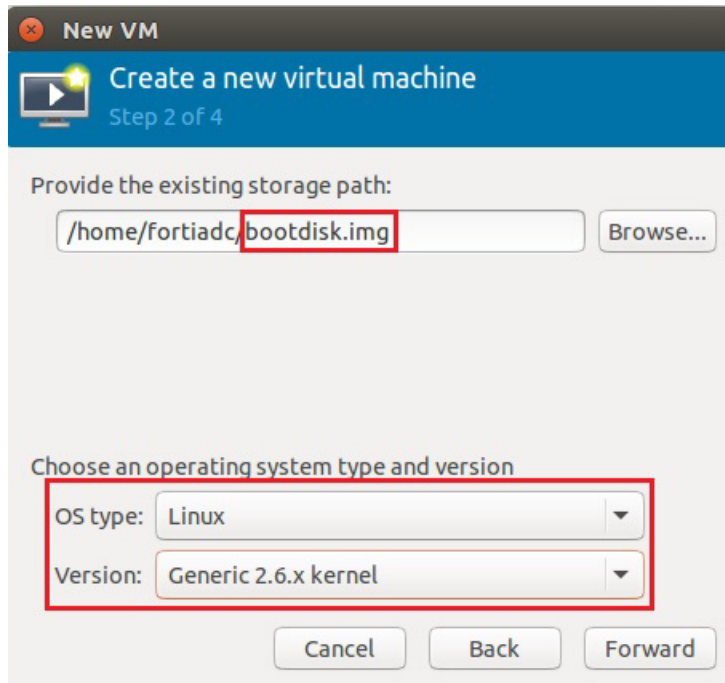
2. Go to File > Add Connection and connect to the Xen server where you will deploy the VM.
3. Click the **New** icon to open the wizard for a new virtual machine.



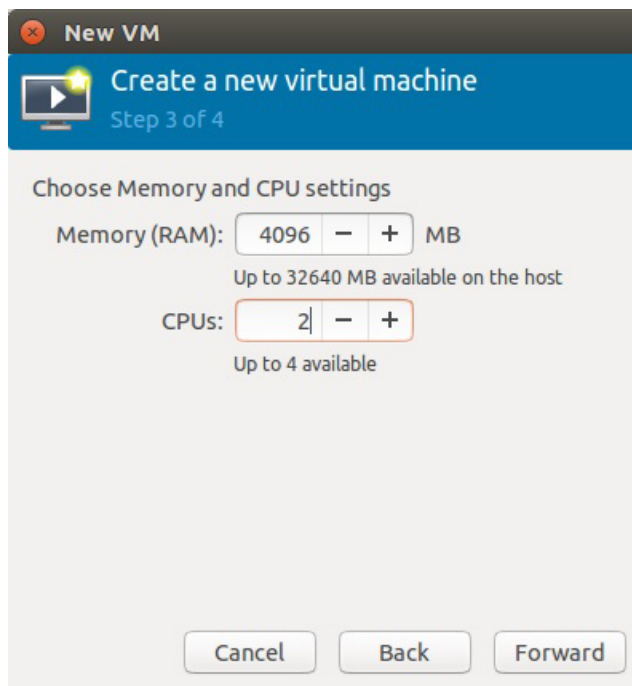
4. Select **Import existing disk image**, select Virt Type **xen (fullvirt)**, and then click **Forward**.



5. Click **Browse** and locate the `bootdisk.img` file. In OS type, select **Linux**, then in Version, expand the list to show all distributions, then select **Generic 2.6.x kernel**, and click **Forward**.

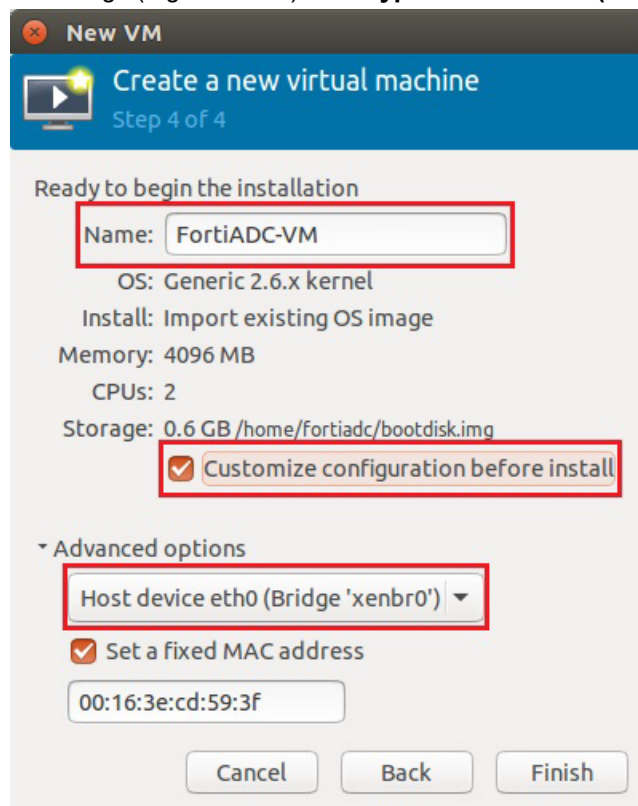


6. Adjust the vRAM and vCPU settings to be appropriate for your deployment. Fortinet recommends a minimum of 4096 MB vRAM and 1 vCPU. Valid vCPU values range from 1 to 32, depending on your FortiADC-VM license. Click **Forward**.



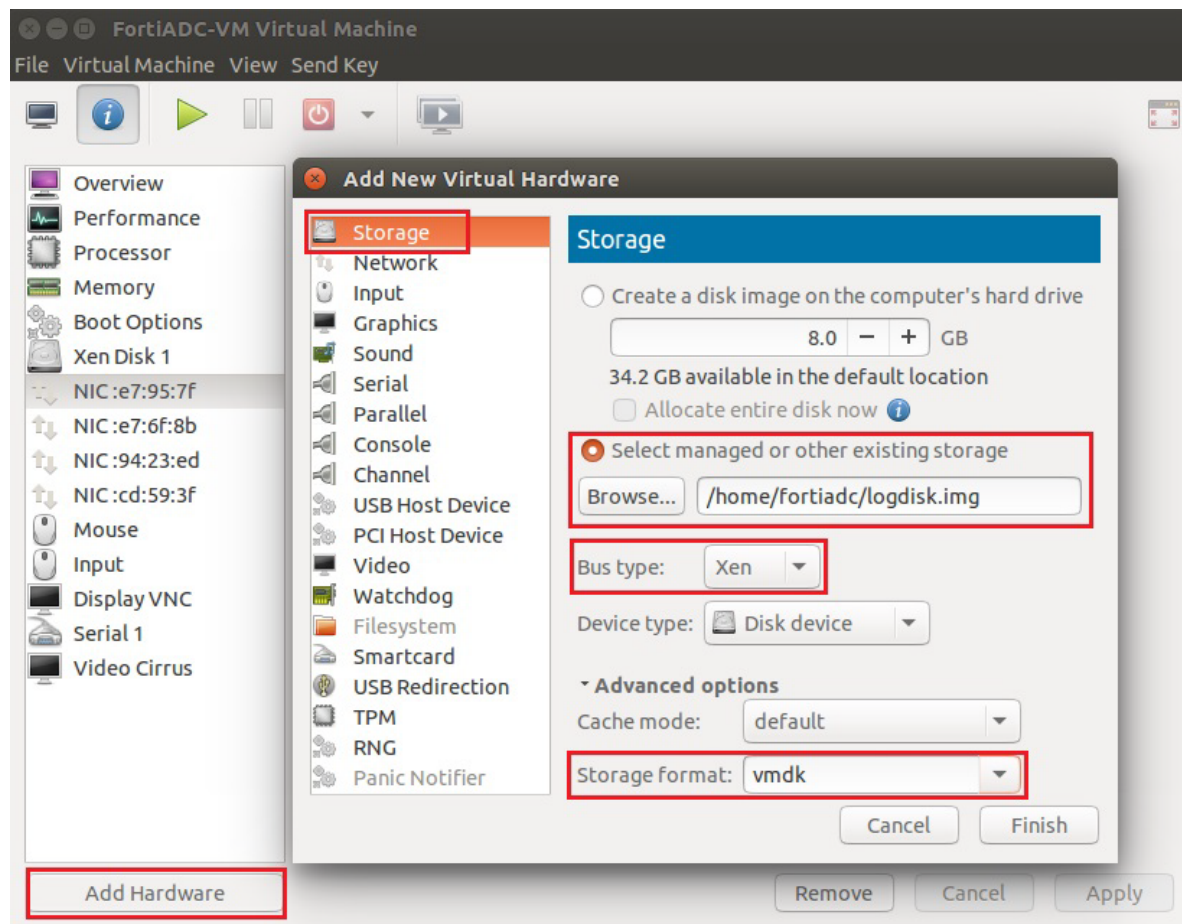
7. In Name, type a unique descriptive name for this instance of FortiADC-VM as it will appear in Virtual Machine Manager's inventory, such as FortiADC-VM. If you will deploy multiple instances of this file, consider a naming scheme that will make each VM's purpose or IP address easy to remember. (This name will not be used as the host name, nor will it appear within the FortiADC-VM web UI.) Mark the **Customize configuration before install** check box. Also click to expand **Advanced options**, then click the drop-

down menu to change NAT to **Specify shared device name** and in Bridge name, enter the name of the Xen bridge (e.g. `xenbr0`). **Virt Type** should be **xen (fullvirt)**. Click **Finish**.

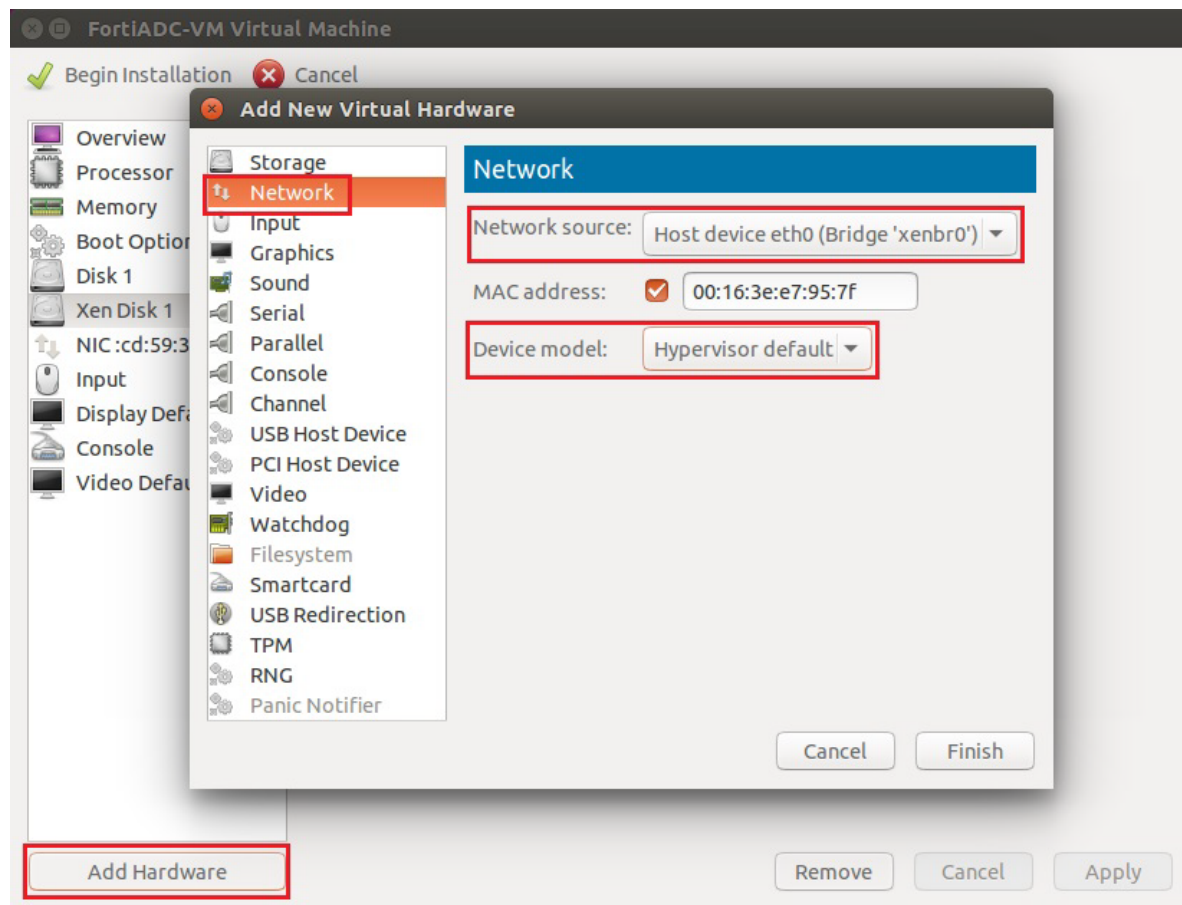


A new dialog will appear where you can add the other vDisk and vNICs.

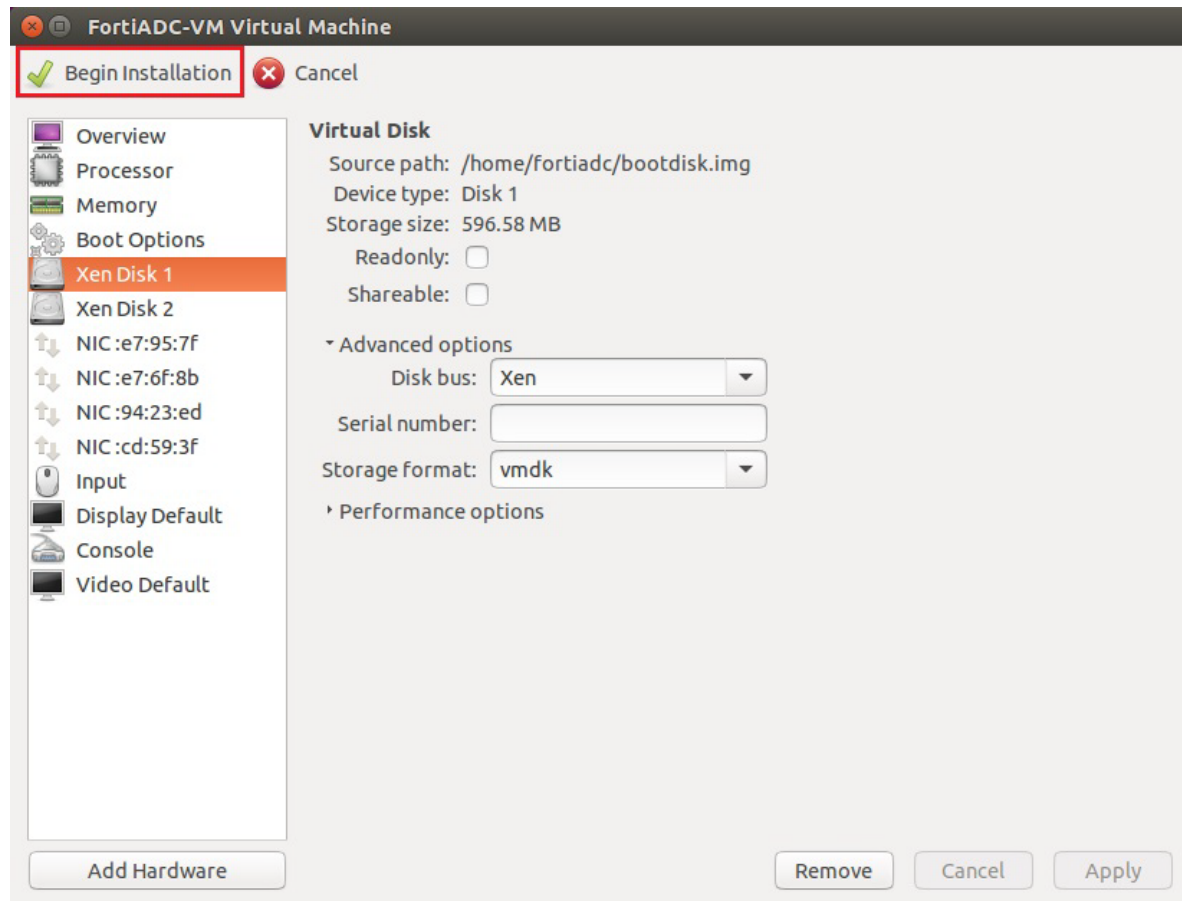
8. In the menu on the left, select the virtual disk. In Advanced options, configure `boot.disk` to be a virtual disk (VMDK). Then click the **Add Hardware** button virtual disk (VMDK). Then click the Add Hardware button and add the `logdisk.img` file also as a VMDK.



9. In the menu on the left, click **Add Hardware** and add another virtual network adapter that is bound to the bridge.
Repeat this step again until you have 4 vNICs, then click **Apply**.



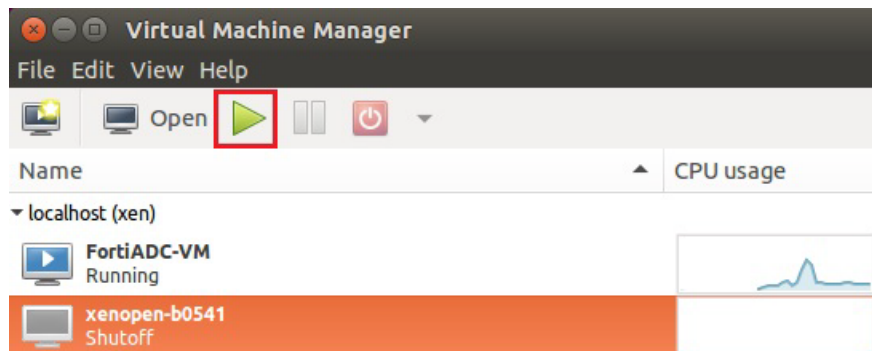
10. Click **Begin Installation** to send the FortiADC-VM image and its VM settings to the Xen server.



The client connects to the VM environment, and deploys the image to it. Time required depends on your computer's hardware speed and resource load, and also on the file size and speed of the network connection, but might take 15 minutes to complete.

When complete, the deployment should appear in the list of deployed VMs for that Xen server, in the pane on the left side of Virtual Machine Manager.

11. To power on the VM, click the **Play** button.



Deploying via dom0 command line

Connect to the command line of your `dom0` guest. For example, you may be able to use PuTTY to make an SSH connection to the Xen server's IP address, or you may use a local GNOME Terminal application.

Next, unpack the file that you downloaded from Fortinet, and open the configuration file in a plain text editor such as `nano`.

```
unzip FAD_XENOPEN-v400-build0547-FORTINET.out.xenopensesource.zip
cd FAD_XENOPEN-v400-build0547-FORTINET.out.xenopensesource
nano fortiadc.hvm
```

Then edit these lines in `fortiadc.hvm` file:

```
memory = 4096
vcpus = 2
vif = [ 'type=netfront, bridge=xenbr0', 'type=netfront, bridge=xenbr0', 'type=netfront,
        bridge=xenbr0', 'type=netfront, bridge=xenbr0', ]
disk = [ 'file:<disk image path>/bootdisk.img,xvda,w','file:<logdisk image
        path>/logdisk.img,xvdb,w' ]
```

As an alternative to locally stored disk images, you can reference an NFS or CIFS share:

```
#Mount point on the server's local file system
root = "/dev/nfs"
nfs_server = '192.0.2.100'
#Root directory on the NFS server
nfs_root = '/path/to/directory'
```

Configure virtual hardware settings to allocate appropriate resources for the size of your deployment before powering on the virtual appliance. For details, see the documentation for the [open source Xen Hypervisor](#).

Change the value if necessary to allocate enough vCPUs for the size of your deployment. Valid vCPU values range from 1 to 32, depending on your FortiADC-VM license.

Similarly, FortiADC-VM for Xen Project comes pre-configured to use 4 GB of vRAM (`memory`). However, this is not enough for most deployments. Change this value to be appropriate for your deployment. The valid range is from 4 GB to 64 GB.

If you configure the virtual appliance's storage to be internal (that is, local, on its own vDisk), resize the vDisk before powering on. 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. Resize the vDisk before powering on the virtual machine.



This step is not applicable if the virtual appliance will use external network file system (such as NFS or CIFS) datastores.

Depending on your Xen `dom0` platform, you may also need to reconfigure `fortiadc.hvm` with the path to your `hvmloader`. For example, this may be correct for CentOS or Red Hat Linux:

```
kernel = "/usr/lib/xen/boot/hvmloader"
```

but this is required by Ubuntu 12.0.4 LTS:

```
kernel = "/usr/lib/xen-4.1/boot/hvmloader"
```

Apply the changes by rebooting or restarting networking. (In some cases rebooting is required: `sudo /etc/init.d/networking restart` may not delete your old IP address from `eth0` and therefore not correctly bring up all interfaces.)

Run these commands to deploy the VM, power it on, and show its Xen domain ID number (highlighted below in bold):

```
xenuser@LabXen:/$ sudo xm create fortiadc.hvm
xenuser@LabXen:/$ sudo xm list
Name ID Mem VCPUs State Time(s)
Domain-0 0 5877 4 r----- 1556.9
fortiadc-vm 2 2048 2 -b---- 126.8
```

If your `dom0` is Ubuntu 12.04 and/or when creating the VM, you receive this error:

Error: Domain 'fortiadc-xen' does not exist.



and if `/var/log/xen/qemu-dm-fortiadc-xen.log` contains this line:
Could not read keymap file: '/usr/share/qemu/keymaps/en-us'

then the key mapping is not in its expected location. Enter this line:

```
sudo ln -s /usr/share/qemu-linaro /usr/share/qemu
```

then retry the command to create FortiADC-VM.

Since VNC listening port numbers are dynamically allocated to guest VMs, use the domain ID number in the output from the previous command to run this command to show the current VNC listening port number and IP address for FortiADC-VM:

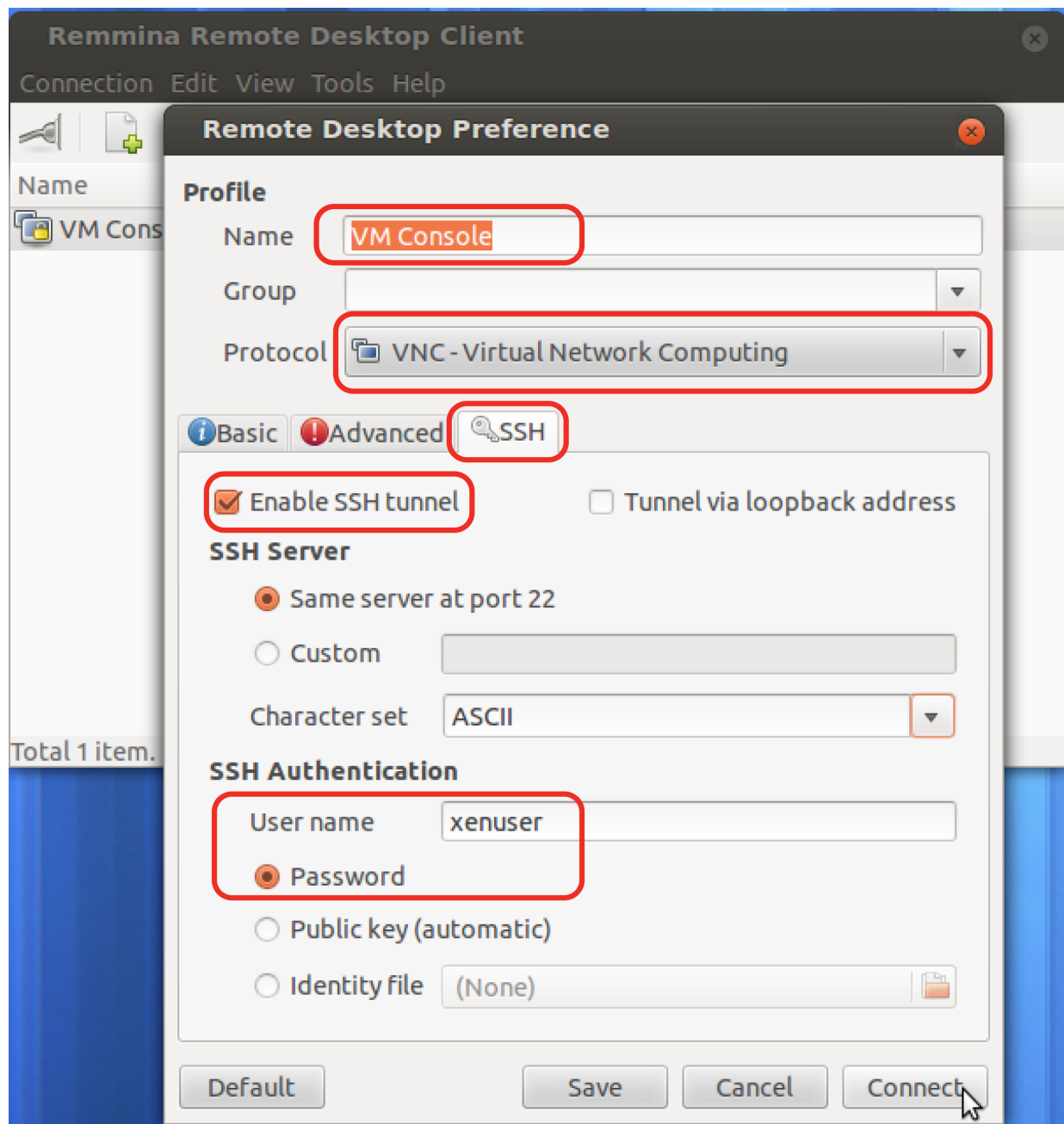
```
xenuser@LabXen:/$ sudo xenstore-ls /local/domain/2/console
port = "4"
limit = "1048576"
type = "ioemu"
vnc-port = "5900"
vnc-listen = "127.0.0.1"
tty = "/dev/pts/5"
```

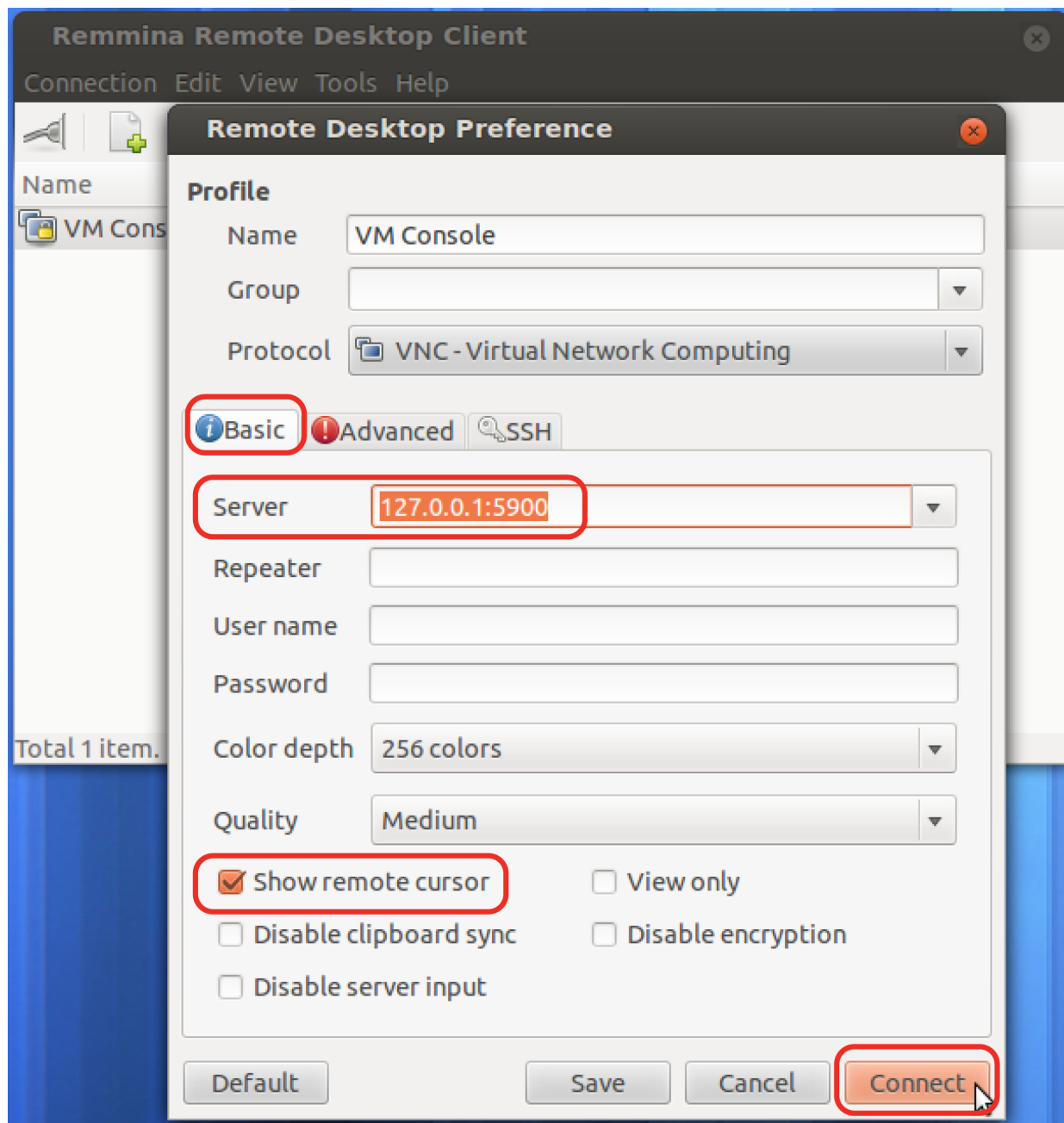
Finally, on your management computer, install and start a VNC viewer and connect to the Xen server's IP address and listening port number for VNC. (In the images below, the VNC viewer is installed in `dom0` on the Xen server that is hosting FortiADC-VM, so the VNC viewer connects to 127.0.0.1. If connecting from your management computer, replace this with the IP address of your Xen server.) For example, on a Debian or Ubuntu Linux management computer, you could use these commands:

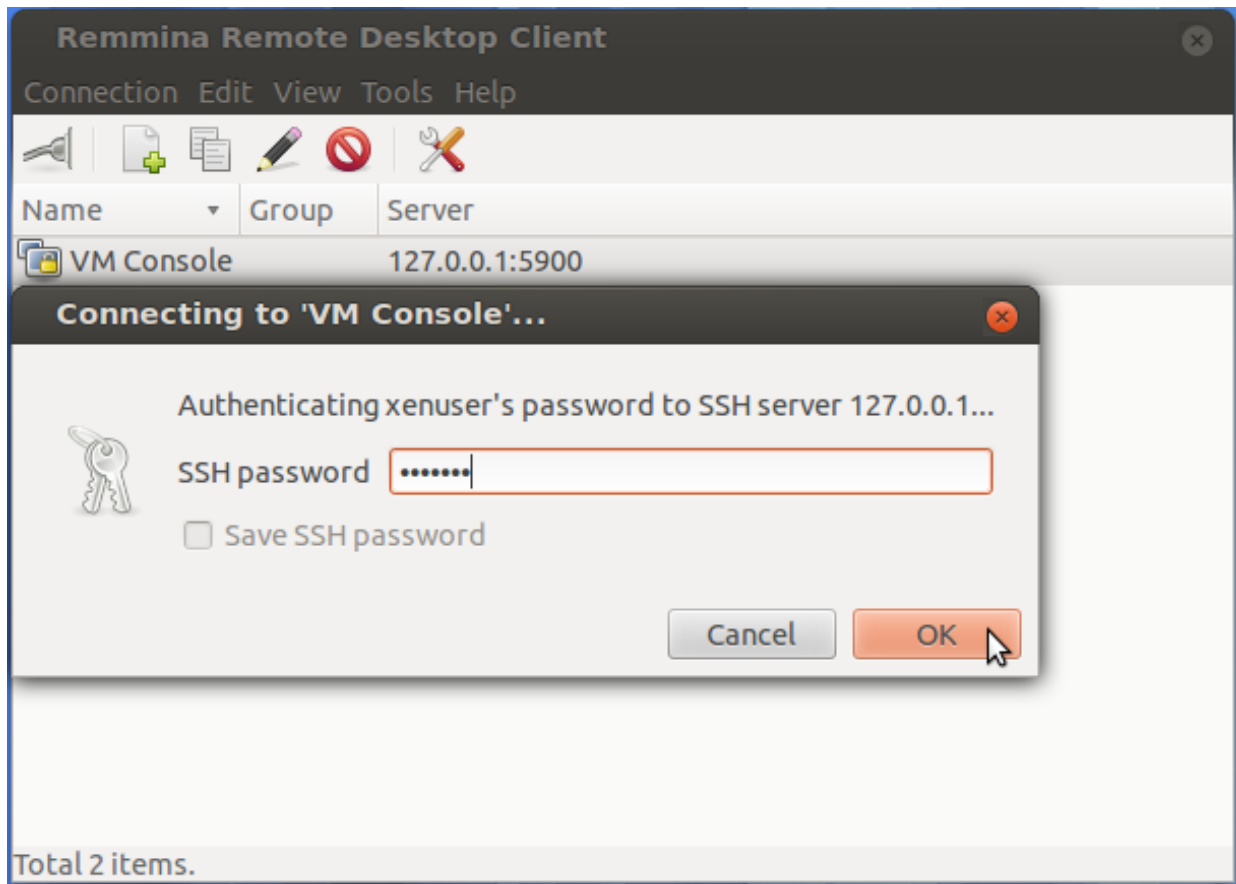
```
sudo apt-get install remmina
remmina
```



You **must** run this command from a terminal with an X Windows environment such as GNOME Terminal in order for it to be able to open the VNC viewer window.







Step 4: Configure access to the web UI & CLI

Once it is powered on, you must log in to the FortiADC-VM command-line interface (CLI) via the 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 in FortiADC-VM:

1. Open the Xen Project Virtual Manager.
2. In the left pane, select the name of the virtual appliance and click **Open**.
3. At the login prompt, type `admin` and no password to log in.
4. 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/`.
The web UI login page appears.
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
```

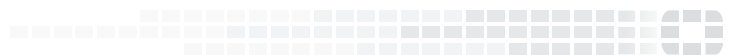
If after 4 hours FortiADC still cannot validate its license, a warning message will be printed to the local console.

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.



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.