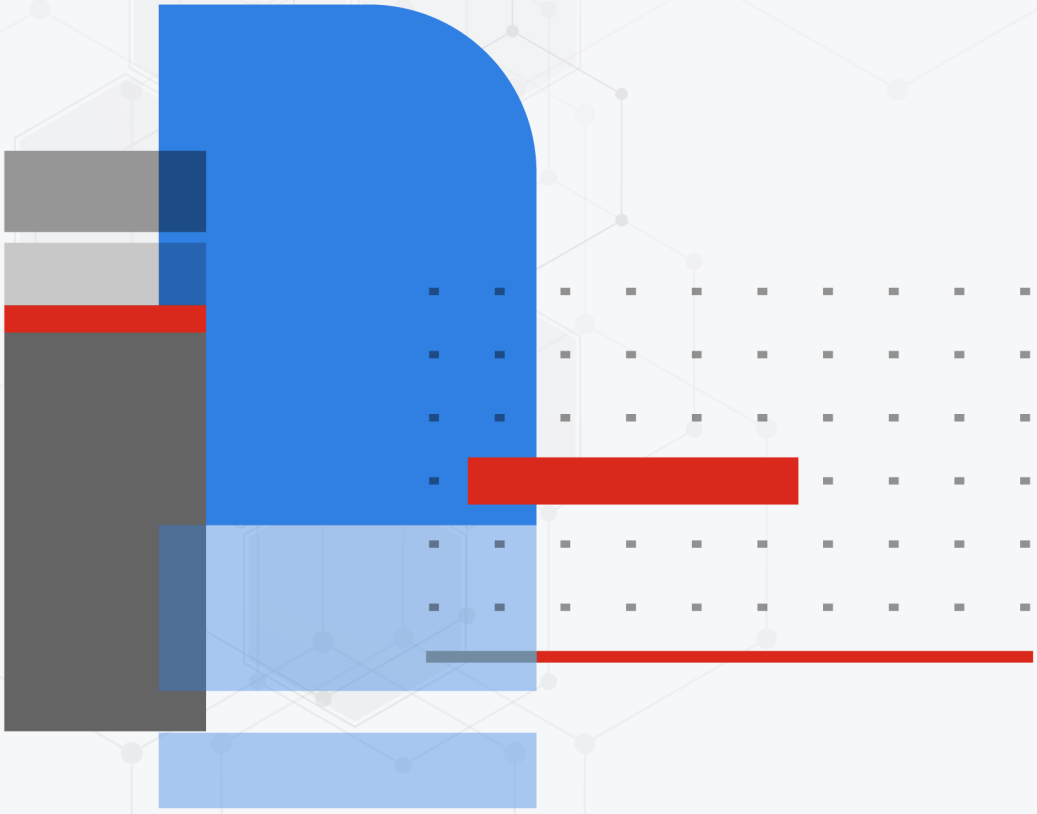
Proxmox Administration Guide

Fortinet 7.6



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November 22, 2024
Fortinet 7.6 Proxmox Administration Guide
01-76-1099944-20241122

TABLE OF CONTENTS

Change log

Date	Change description
2024-11-22	Initial release.

About FortiGate-VM on Proxmox

FortiGate-VMs allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. They also allow you to rapidly provision security infrastructure whenever and wherever it is needed. FortiGate-VMs feature all the security and networking services common to hardware-based FortiGate appliances. You can deploy a mix of FortiGate hardware and VMs, operating together and managed from a common centralized management platform.

This document describes how to deploy a FortiGate-VM in a Proxmox environment.

FortiGate-VM models and licensing

FortiGate-VM offers perpetual licensing (normal series and v-series) and annual subscription licensing. See VM license for details.

After you submit an order for a FortiGate-VM, Fortinet sends a license registration code to the email address that you entered on the order form. Use this code to register the FortiGate-VM with Customer Service & Support, then download the license file. After you upload the license to the FortiGate-VM and validate it, your FortiGate-VM is fully functional.

FortiGate-VM evaluation license

The Fortinet permanent trial license requires a FortiCare account. This trial license has limited features and capacity. See Permanent trial mode for FortiGate-VM for details.

FortiGate-VM virtual licenses and resources

The primary requirement for provisioning a FortiGate-VM may be the number of interfaces it can accommodate rather than its processing capabilities. In some cloud environments, options with a high number of interfaces tend to have high numbers of vCPUs.

FortiGate-VM licensing does not restrict whether the FortiGate can work on a VM instance in a public cloud that uses more vCPUs than the license allows. The number of vCPUs that the license indicates does not restrict the FortiGate from working, regardless of how many vCPUs the virtual instance includes. However, only the licensed number of vCPUs process traffic and management tasks. The FortiGate-VM does not use the rest of the vCPUs.

License	1 vCPU	2 vCPU	4 vCPU	8 vCPU	16 vCPU	32 vCPU
FGT-VM08	OK	OK	OK	OK	The FortiGate-VM uses 8 vCPUs for traffic and management and does not use the rest.	

You can provision a VM instance based on the number of interfaces you need and license the FortiGate-VM for only the processors you need.

Public compared to private clouds

The behavior differs between private and public clouds:

- Private clouds (VMware ESXi/KVM/Xen/Microsoft Hyper-V/Proxmox): both licensed vCPUs and RAM are affected. Fortinet does not have licensed RAM size restrictions. However, the minimum recommended RAM size is 2 GB for all versions.
- Public clouds (AWS/Azure/GCP/OCI/AliCloud): only licensed vCPU is affected.

For example, you can activate FG-VM02 on a FGT-VM with 4 vCPUs and there is no limit on the RAM size when running on a private VM platform.

Likewise, you can activate FG-VM02 on a FGT-VM c5.2xlarge EC2 instance with 8 vCPUs running on AWS. Only 2 vCPU is consumable, and there is no limit on the RAM size. You can refer to licenses for public clouds as bring your own license.

Deploying a FortiGate-VM into Proxmox

This guide describes how to deploy a FortiGate-VM into a Proxmox hypervisor.

Assumptions

1. You already have Proxmox installed and know the basics of accessing and using the Proxmox GUI and CLI. This tutorial uses Proxmox 8.1.5.
2. You have Fortinet Support Portal access and can download the appropriate firmware images. FortiOS 7.0.14 is used for this tutorial, but the steps below can be applied to any version.

Workflow

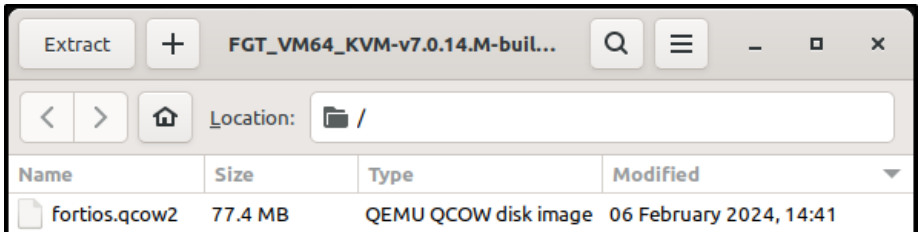
Downloading FortiGate KVM image files and copying them to Proxmox

1. Login to the Fortinet Support Portal and choose *Support* > *Firmware Download* from the menu at the top.
2. Ensure *FortiGate* is selected in the dropdown list. Click the *Download* tab and then go to the desired FortiOS version.
3. At this point, you should see a long list of downloadable firmwares for the various models of FortiGate hardware appliances and VM platforms. Scroll down until you see the FGT_VM64_KVM builds. You should see two entries as shown below: FGT_VM64_KVM-v7.6.X.M-buildXXXX-FORTINET.out and **FGT_VM64_KVM-v7.6**.X.M-buildXXXX-FORTINET.out.kvm.zip. Note the differences in file extensions, i.e., .out versus .kvm.zip.

   You can use your browser's built-in find feature to quickly find the files you need. Use `Ctrl+F` or `CMD+F` and search for `VM64_KVM`.

4. The FGT_VM64_KVM-v7.6.X.M-buildXXXX-FORTINET.out file is an actual firmware file that you would use to upgrade an already instantiated FortiGate VM to v7.6.X. The one you need is the FGT_VM64_KVM-v7.6.X.M-buildXXXX-FORTINET.out.kvm.zip file. Click the *HTTPS* link of the FGT_VM64_KVM-v7.6X.M-buildXXXX-FORTINET.out.kvm.zip entry to download this file.
5. Extract the contents of the FGT_VM64_KVM-v7.6.X.M-buildXXXX-FORTINET.out.kvm.zip to a folder. You should see a fortios.qcow2 file. This is the image file that we need to copy over to Proxmox.



6. There are various methods to copy the fortios.qcow2 onto a Proxmox node. Typically, SCP (Secure Copy) is used. In the example below, the `scp fortios.qcow2 root@pve-hp-03.skwire.net:/root/fortios.qcow2` command is used to copy the fortios.qcow2 file to the Proxmox node at `pve-hp-03.skwire.net`. Of course, change your node address to match your Proxmox environment. This could be a simple IP address or a FQDN as in the example. Furthermore, this tutorial assumes you are using the root user and copying the file to the root user home directory at /root.

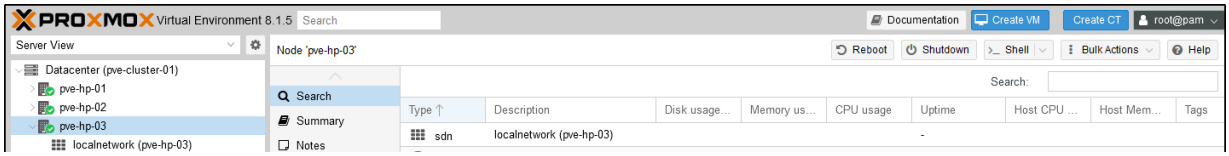
```
me@my-laptop:~/Desktop$ ls
fortios.qcow2
me@my-laptop:~/Desktop$ scp fortios.qcow2 root@pve-hp-03.skwire.net:/root/fortios.qcow2
root@pve-hp-03.skwire.net's password:
fortios.qcow2                                                                 100%   74MB
109.8MB/s   00:00
me@my-laptop:~/Desktop$
```

As mentioned above, there are various methods to get a QCOW2 image onto a Proxmox node. In the example, commandline SCP is used. However, you could also use a GUI SCP client like WinSCP on Windows or Forklift on Mac. Finally, if you have FTP set up on your Proxmox node, you could use that as an alternative. Use whatever method you're comfortable with.

Deploying the FortiGate-VM into Proxmox

To deploy the FortiGate-VM into Proxmox:

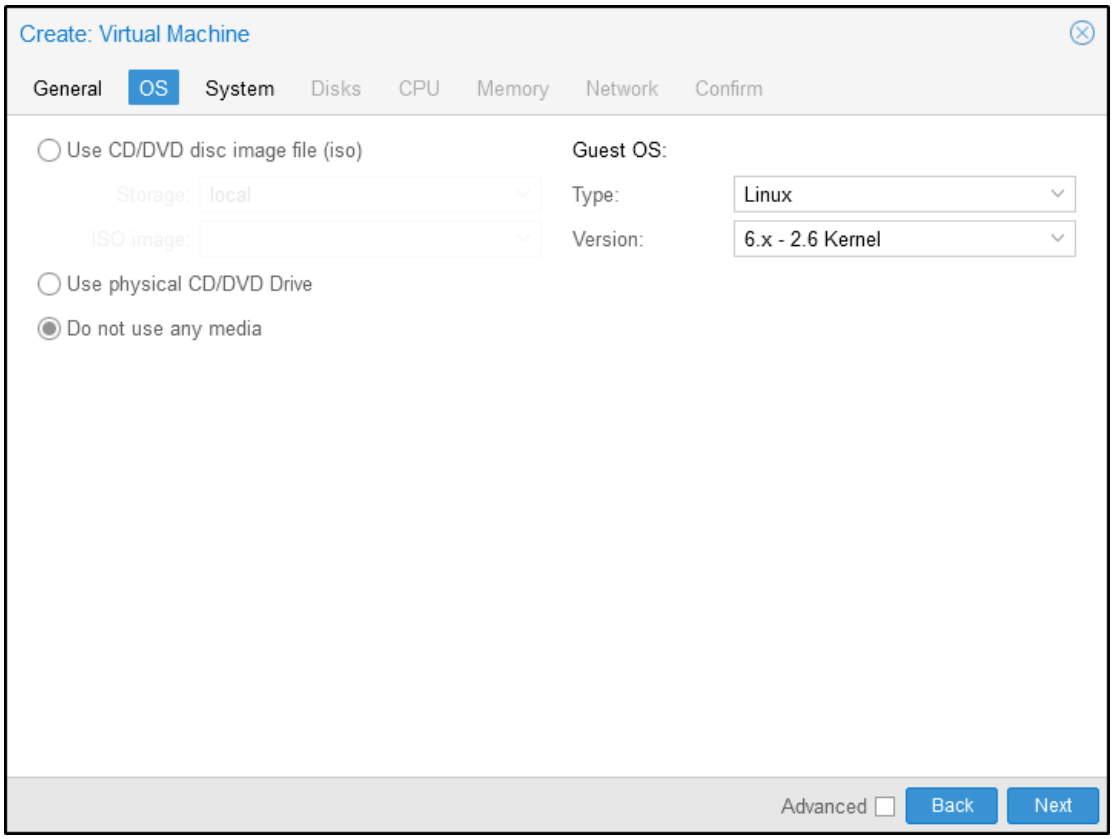
1. In the Proxmox GUI, highlight the node you copied the FortiOS image to and click the *Create VM* button in the upper right. The *Create: Virtual Machine* dialog appears.



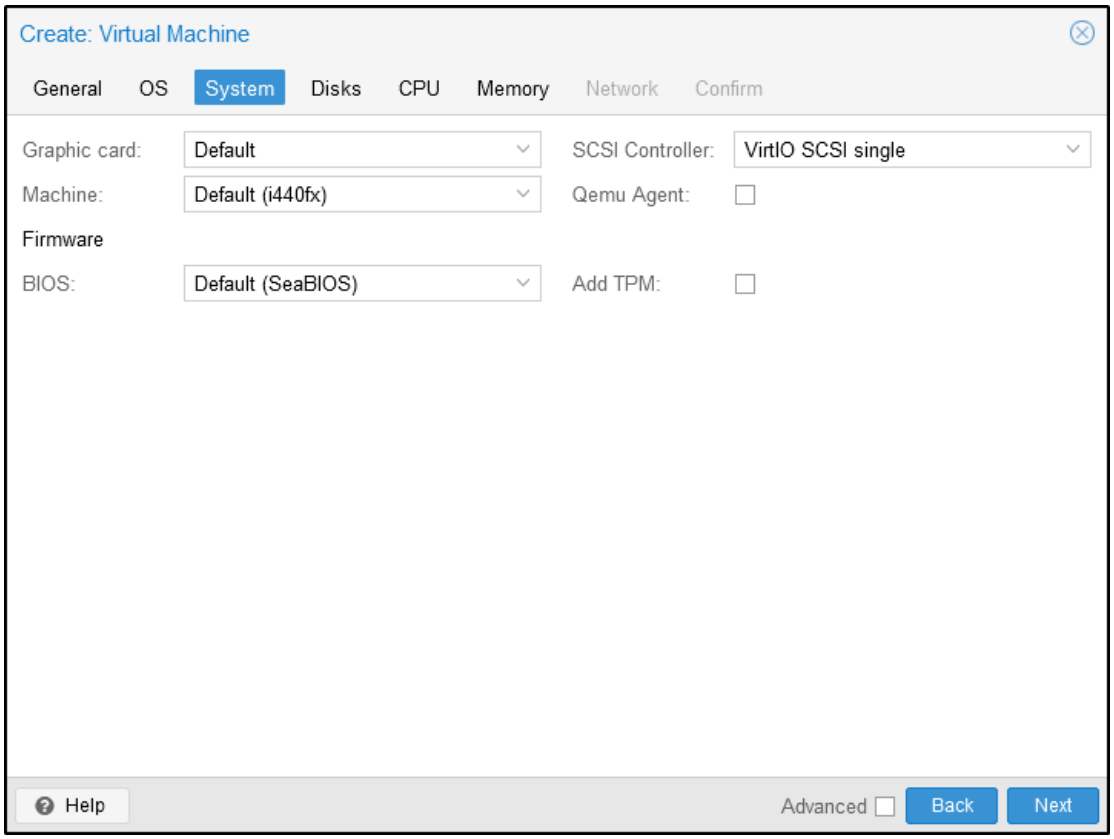
2. In the *Create: Virtual Machine* dialog's *General* tab, change the *VM ID* value, if desired. Make a mental note of this ID value as you will use it later. In the *Name* field, give the virtual machine a useful name. Click *Next* to move to the *OS* tab.

You might find it useful to add the FortiOS version number to the end of your virtual machine name.

3. In the *OS* tab, select the *Do not use any media*. Leave the *Type* and *Version* options at their defaults of *Linux* and *6.x - 2.6 Kernel*, respectively. Click *Next* to move to the *System* tab.



4. In the *System* tab, leave everything at their defaults and click *Next* to move to the *Disks* tab.



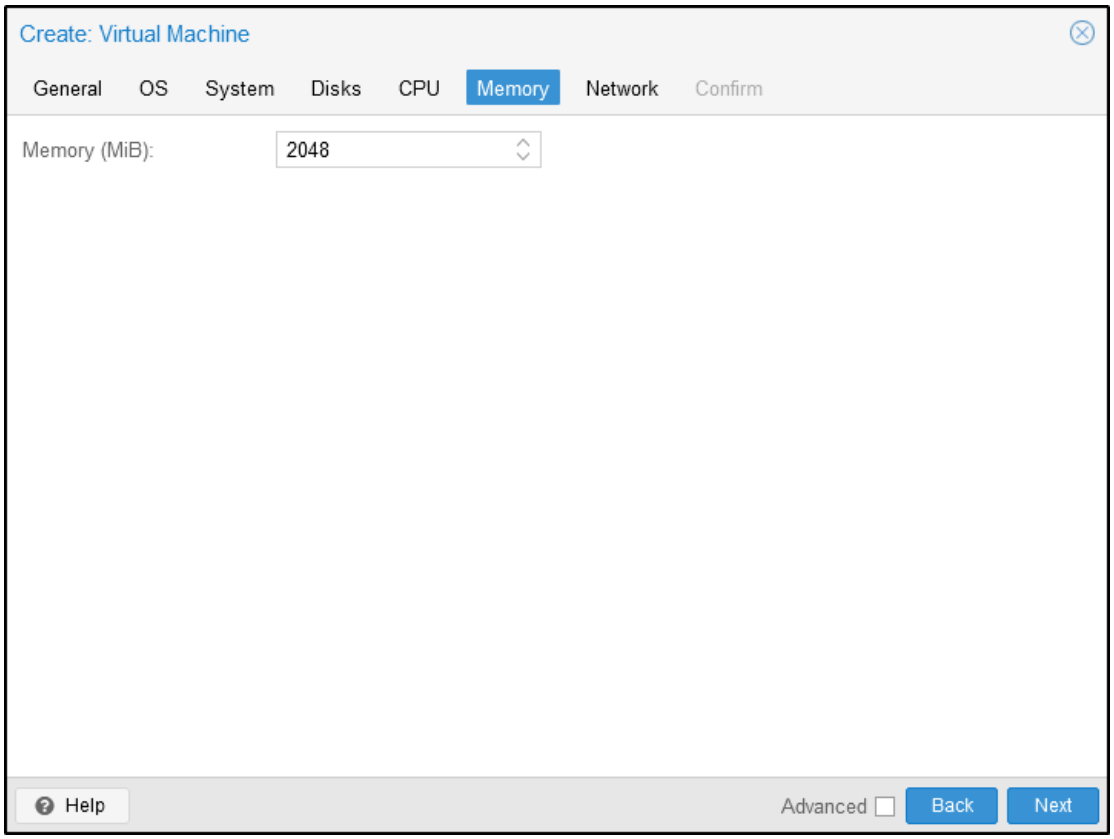
5. In the *Disks* tab, by default, you should see an entry for one SCSI disk named *scsi0*. Click the small trashcan icon to delete this disk. You should now see *No Disks* displayed. Click *Next* to move to the *CPU* tab.

We add disks in a later step.

6. For the purposes of this tutorial, we leave the *CPU* tab values at their defaults. If you have a valid FortiGate VM license (VM02, VM04, VM08, etc), feel free to increase the values to match your license. Click *Next* to move to the *Memory* tab.

A few years ago, Fortinet changed their free VM license from a 14-day trial period to a permanent free trial period with limitations. See here for more information.

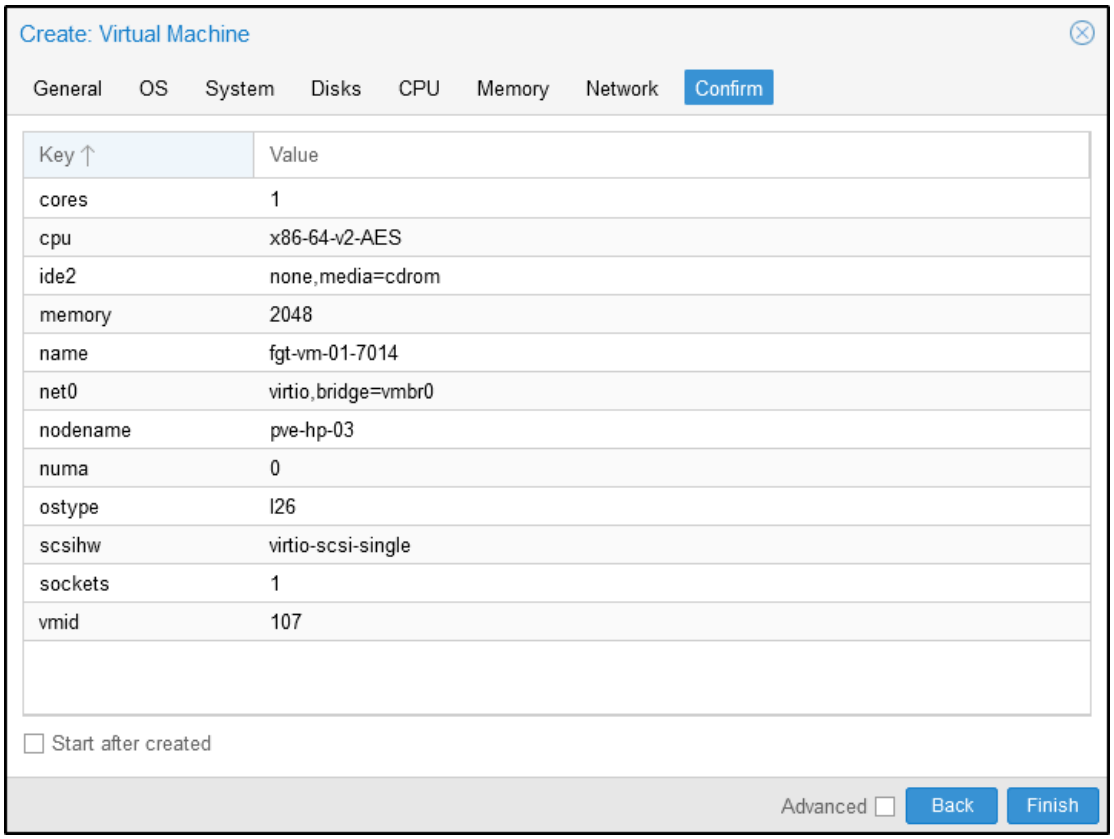
7. For the purposes of this tutorial, we leave the *Memory* tab values at their defaults. If you have a valid FortiGate VM license (VM02, VM04, VM08, etc), there is no memory limit, so feel free to increase the memory value as desired. Click *Next* to move to the *Network* tab.



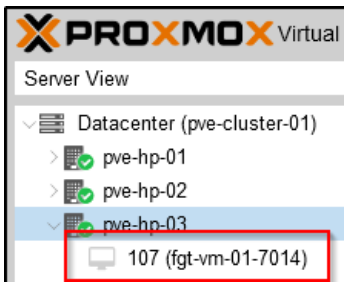
8. In the *Network* tab, deselect the *Firewall* option and leave the rest of the options at their defaults. Click *Next* to move to the *Confirm* tab.

We add more network interfaces in a later step.

9. In the *Confirm* tab, ensure the *Start after created* option is unselected. Again, note the *vmid* value as you will use it later. Click *Finish* to build the VM.



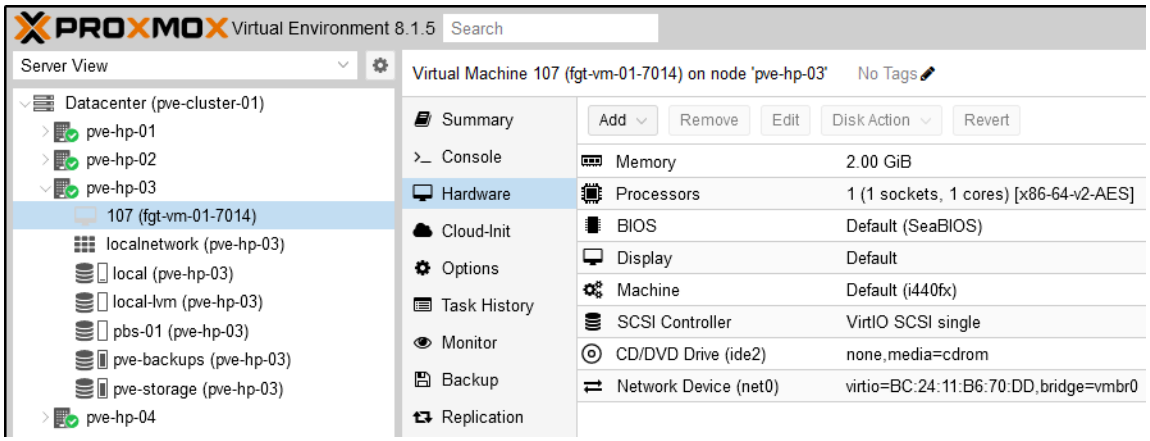
After some seconds, you should see the new VM in the left sidebar with the VMID and name chosen in the previous steps.



Importing the QCOW2 image into the FortiGate-VM

To import the QCOW2 image into the FortiGate-VM:

1. In the Proxmox GUI, highlight the newly created VM in the left sidebar and click *Hardware* in the middle sidebar. Note the presence of one network interface named *net0* and the lack of disks.



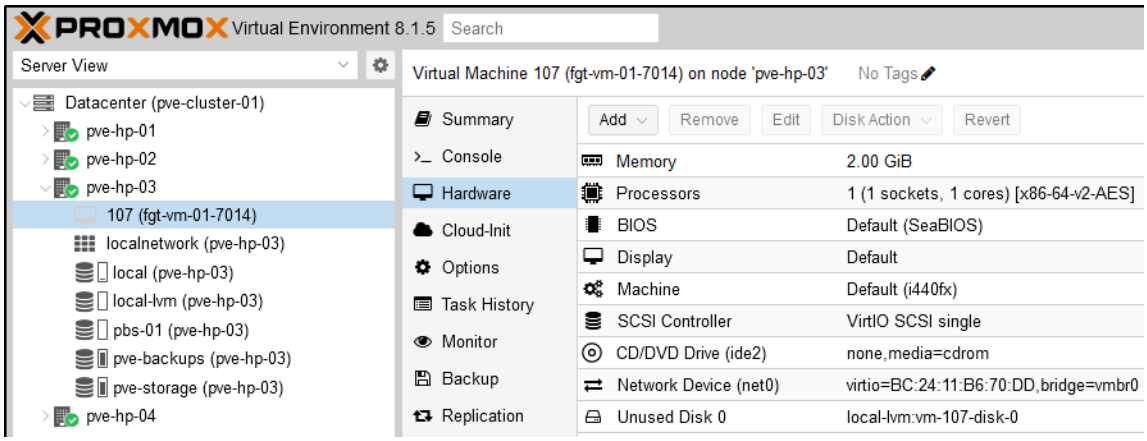
2. Highlight the Proxmox node in the left sidebar and click the *Shell* entry in the middle sidebar. After the shell appears, type `pwd` to ensure are in the `/root` folder and then type `ls` to display the contents of the directory. You should see the fortios.qcow2 image file we copied over earlier.

```
root@pve-hp-03:~# pwd
/root
root@pve-hp-03:~# ls
fortios.qcow2
root@pve-hp-03:~#
```

3. To import the fortios.qcow2 image into your newly created VM, you use the `qm disk import` command: `qm disk import <vmid> fortios.qcow2 <storage device name>`. You will need to adjust the command to match your *vmid* created earlier and *storage device name* of choice. By default, Proxmox creates a local and local-lvm storage device when it is installed. In the example below, we use a vmid of 107 and the local-lvm storage device. Take note of the disk name when the command is finished. In the example below, it's: `unused0:local-lvm:vm-107-disk-0`

```
root@pve-hp-03:~# qm disk import 107 fortios.qcow2 local-lvm
importing disk 'fortios.qcow2' to VM 107 ...
  Logical volume "vm-107-disk-0" created.
transferred 0.0 B of 2.0 GiB (0.00%)
transferred 24.4 MiB of 2.0 GiB (1.19%)
transferred 50.6 MiB of 2.0 GiB (2.47%)
[...]
transferred 2.0 GiB of 2.0 GiB (98.21%)
transferred 2.0 GiB of 2.0 GiB (99.91%)
transferred 2.0 GiB of 2.0 GiB (100.00%)
Successfully imported disk as 'unused0:local-lvm:vm-107-disk-0'
root@pve-hp-03:~#
```

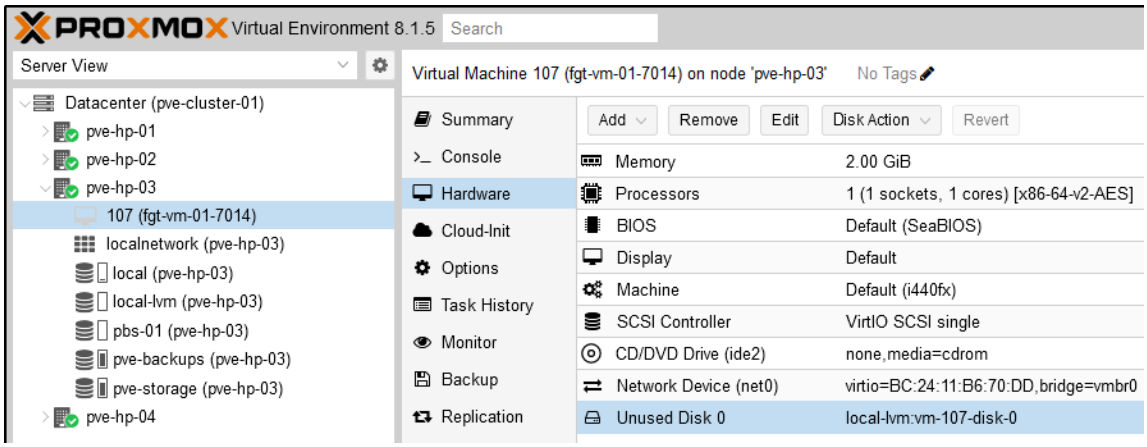
4. Select the FortiGate VM in the left sidebar and click *Hardware* in the middle sidebar. Note the newly imported disk . At this point, it shows as *Unused Disk 0*.



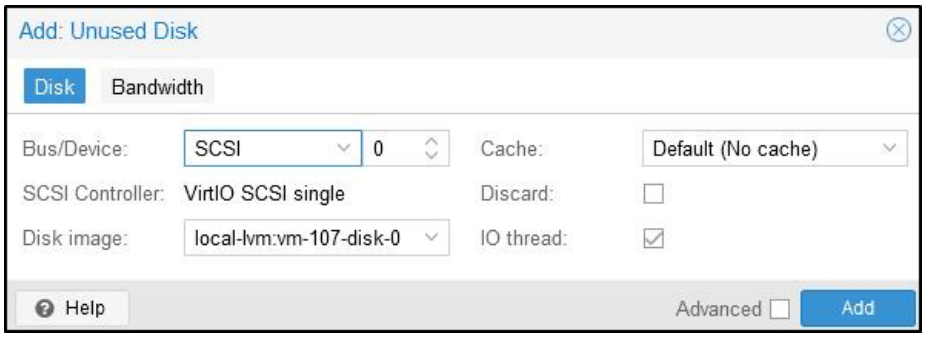
Adding a boot disk to the FortiGate-VM

To add a boot disk to the FortiGate-VM:

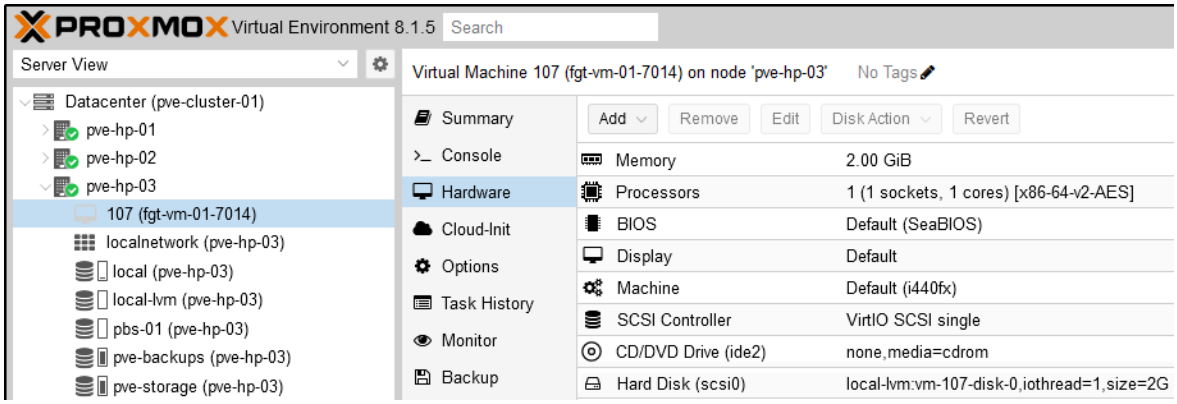
1. Highlight the *Unused Disk 0* entry and click the *Edit* button.



2. The *Add: Unused Disk* dialog appears. Accept the defaults and click the *Add* button.



3. Note the newly added *Hard Disk (scsi0)* is now mapped to the *local-lvm:vm-107-disk-0* created earlier.

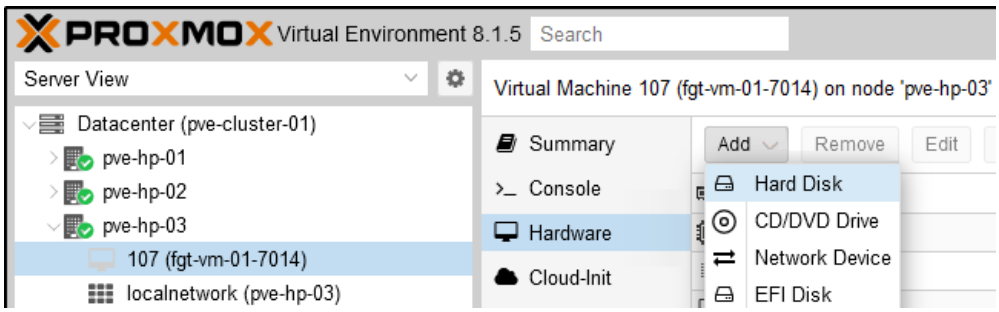


Optional: Adding a logging disk

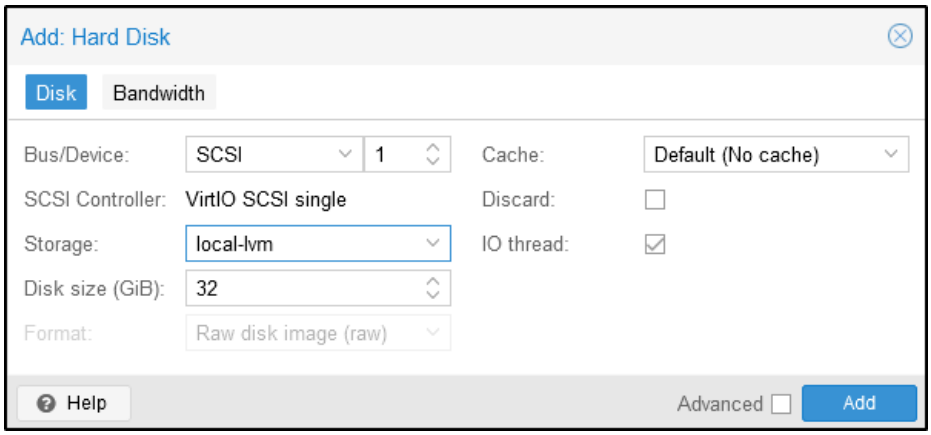
FortiGate hardware model numbers that end in a "1" have an extra storage device on-board for logging or the WAN optimization feature, i.e, FG-61F, FG-101F, FG-1801F, etc. You can duplicate that functionality on a FortiGate VM by adding a virtual logging disk.

To add a logging disk:

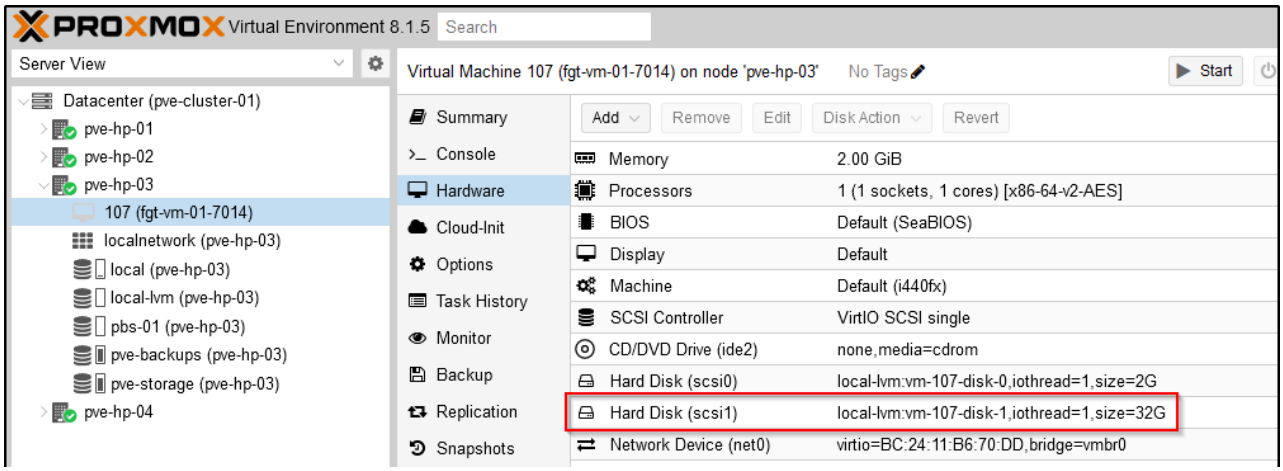
1. To add a logging disk, select the FortiGate-VM in the left sidebar and click *Hardware* in the middle sidebar. Click the *Add* button and select *Hard Disk* from the dropdown menu.



2. The *Add: Hard Disk* dialog appears. Select *local-lvm* from the *Storage* dropdown. You can leave the *Disk size (GiB)* value at 32 or change it as desired. Leave all other fields at their defaults and click *Add* to add the new disk.



Note the newly added *Hard Disk (scsi1)* with a size of *32G*. This disk will be formatted by FortiOS when you first boot the VM.

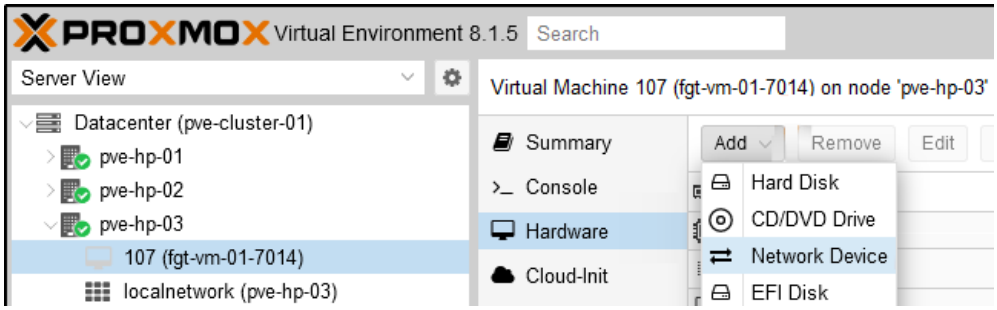


Optional: Adding additional network interfaces

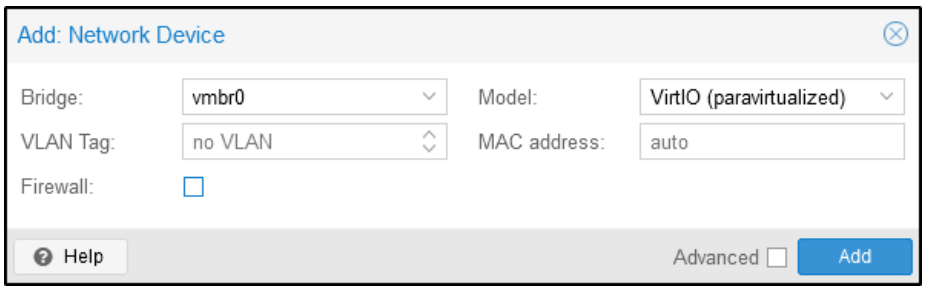
With the free, unlicensed, FortiGate VM, a maximum of three network interfaces are supported. With a fully licensed FortiGate VM, a maximum of twelve interfaces are supported.

To add additional network interfaces:

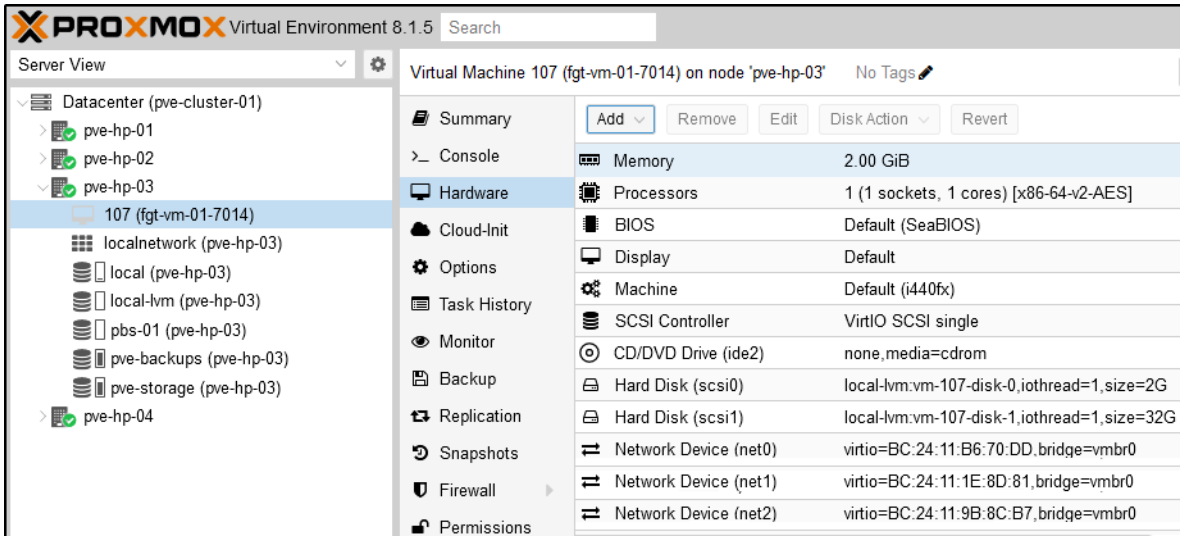
1. To add additional network interfaces, select the FortiGate-VM in the left sidebar and click *Hardware* in the middle sidebar. Click the *Add* button and select *Network Device* from the dropdown menu.



2. The *Add: Network Device* dialog appears. If there are additional bridges configured on your Proxmox node, you can select it from the *Bridge* dropdown. If not, the default vmbr0 will suffice. Ensure the *Firewall* checkbox is unselected. Click the *Add* button to add the new network interface to the VM. Repeat the steps to add a third network interface to the VM.



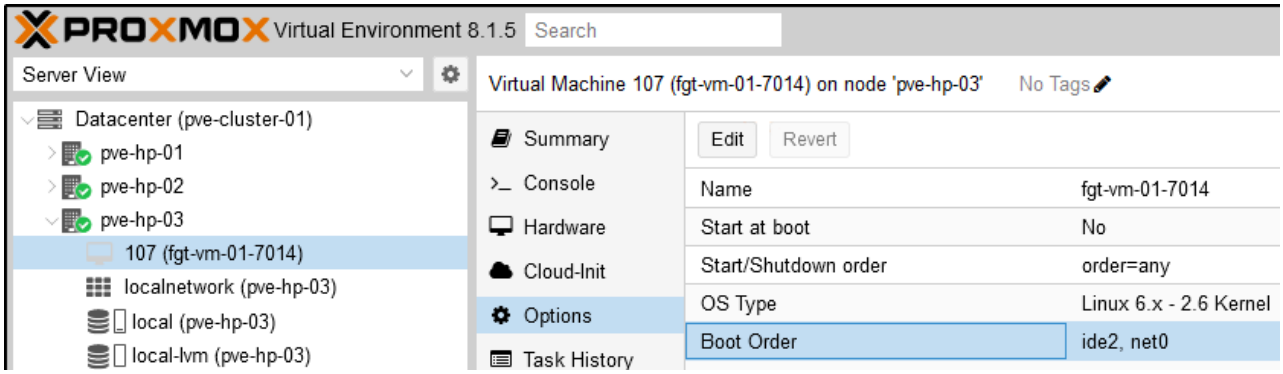
Note the newly added network *Network Device (net1)* and *Network Device (net2)* interfaces.



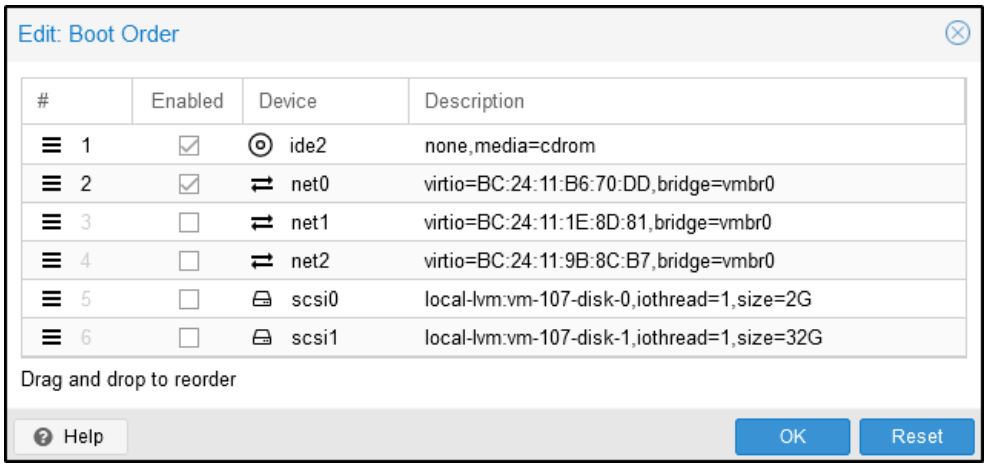
Verifying the Boot Order

To verify the boot order:

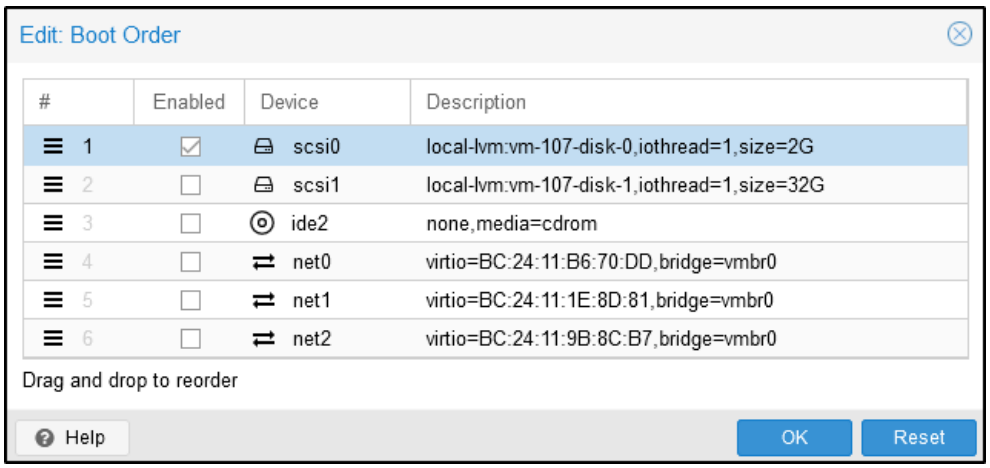
1. To verify the boot order, select the FortiGate VM in the left sidebar and click *Options* in the middle sidebar. Select the *Boot Order* entry and click the *Edit* button. Alternately, you can simply double-click the *Boot Order* entry.



2. The *Edit: Boot Order* dialog appears.



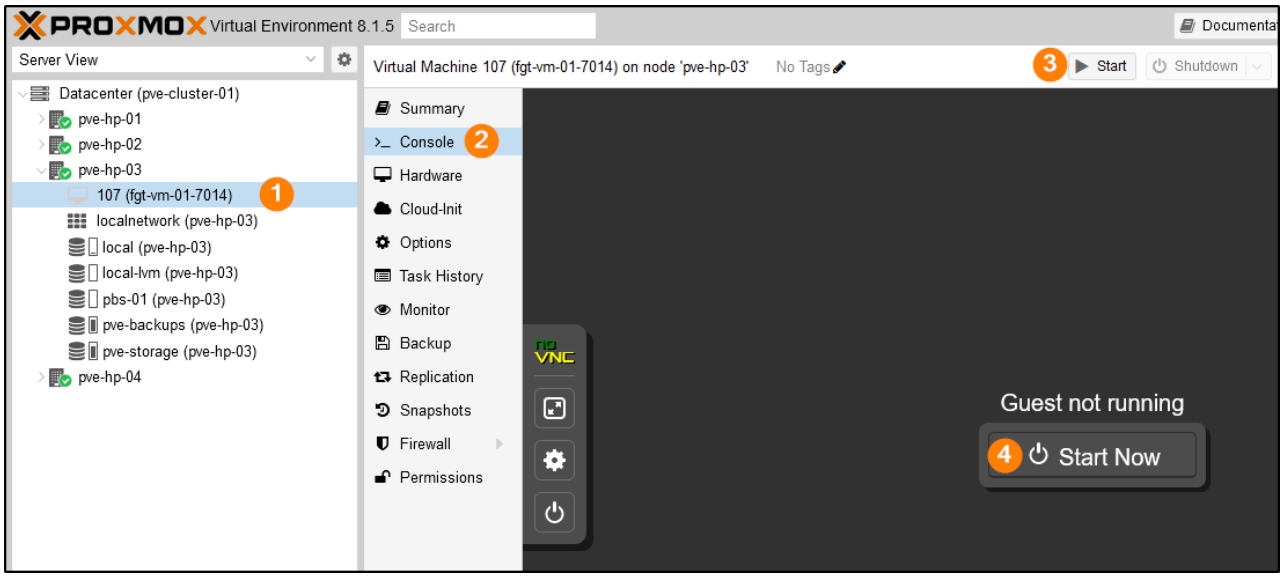
Use the selector icons to drag and drop the *scsi0* disk to the top of the list and ensure the *Enabled* checkbox for that entry is unselected. For neatness, drag the *scsi1* entry to the second position. Uncheck the *Enabled* boxes for the *ide2* and *net0* entries. Click the *OK* button when finished.



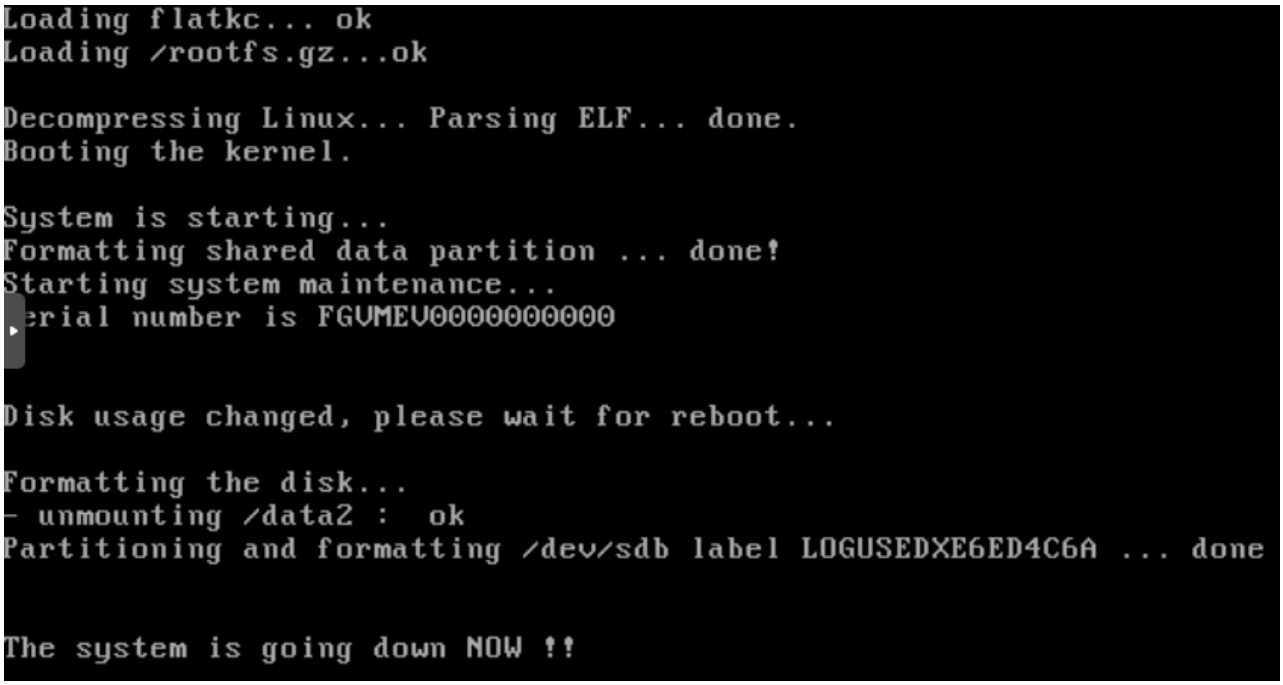
Booting the FortiGate-VM

To boot the FortiGate-VM:

1. Select the FortiGate-VM in the left sidebar and select >_ *Console* in the middle sidebar. Click the *Start* button at the top or the *Start Now* button in the middle of the console.



The FortiGate VM starts to boot, detects the logging disk, formats it, and reboots.



2. After the reboot, the standard FortiGate login prompt is displayed. Login with a username of **admin** and no password. You are prompted to enter a password, verify it, and then presented with the standard FortiOS CLI prompt.

```
Loading flatkc... ok
Loading /rootfs.gz...ok

Decompressing Linux... Parsing ELF... done.
Booting the kernel.

System is starting...
Serial number is FGVMEV0000000000

FortiGate-VM64-KVM login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

FortiGate-VM64-KVM #
```

3. On a FortiGate VM, `port1` is set to `dhcp` mode. Assuming DHCP is running on the vmbr0 bridge segment, enter the `get system interface physical` command to see which IP was received on the `port1` interface of the FortiGate. In the screenshot below, you can see this FortiGate VM received an IP of `192.168.0.19` on the `port1` interface. The two additional interfaces you added previously map to `port2` and `port3` on the FortiGate VM. Note that additional interfaces, by default, are set to `static` mode.

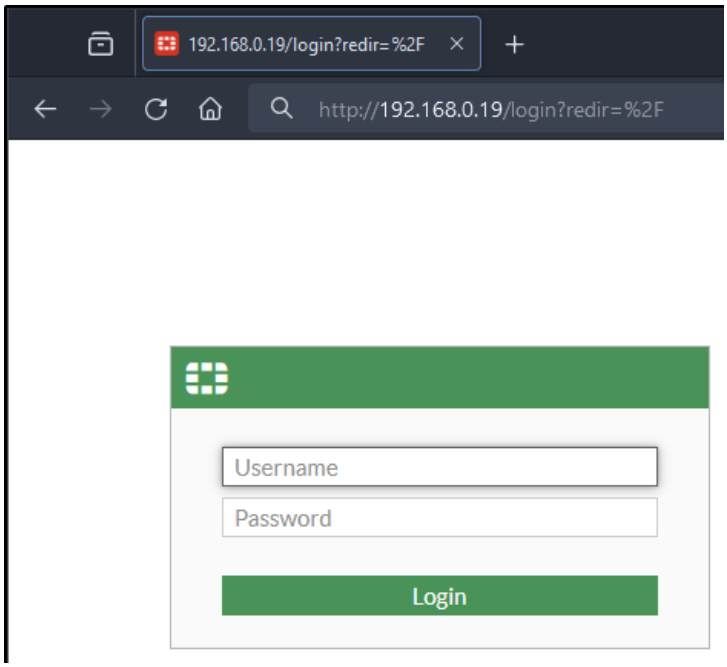
```
FortiGate-VM64-KVM # get system interface physical
== [onboard]
        ==[port1]
                mode: dhcp
                ip: 192.168.0.19 255.255.255.128
                ipv6: ::/0
                status: up
                speed: 10000Mbps (Duplex: full)
                FEC: none
                FEC_cap: none
        ==[port2]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: up
                speed: 10000Mbps (Duplex: full)
                FEC: none
                FEC_cap: none
        ==[port3]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: up
                speed: 10000Mbps (Duplex: full)
--More--
```

4. Enter the `show system interface port1` to verify which services are available on this interface. By default, `ping`, `https`, `ssh`, `http`, and `fgfm` are allowed. Ping, HTTP, HTTPS, and SSH are probably familiar to you. FGFM

is the protocol that FortiManagers and FortiGates use to communicate with each other.

```
                ipv6: ::/0
                status: up
                speed: 10000Mbps (Duplex: full)
                FEC: none
                FEC_cap: none
        ==[port3]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: up
                speed: 10000Mbps (Duplex: full)
                FEC: none

FortiGate-VM64-KVM # show system interface port1
config system interface
    edit "port1"
        set vdom "root"
        set mode dhcp
        set allowaccess ping https ssh http fgfm
        set type physical
        set snmp-index 1
    next
end
```

5. Using a web browser, you can now access the FortiOS GUI interface.



Deploying a FortiGate-VM into Proxmox using cloud-init and a FortiFlex token

This guide describes how to use cloud-init, along with a FortiFlex token, to automatically provision and license a FortiGate-VM on a Proxmox hypervisor.

Cloud-init: What is it?

Cloud-init is the industry standard method by which cloud instances (think VMs) can be provisioned at initial boot-up. From a FortiGate perspective, cloud-init can automatically apply a supplied config and license to a newly deployed FortiGate-VM. Fortinet's usage of cloud-init relies on the creation and use of an ISO file containing the configuration and license information.

Fortinet's cloud-init with a FortiFlex token uses slightly different ISO contents than Fortinet's cloud-init with a full license method.

Assumptions

1. You already have Proxmox installed and know the basics of accessing and using the Proxmox GUI and CLI. This tutorial uses Proxmox 8.1.4.
2. You already know how to deploy a basic FortiGate VM into Proxmox. If you do not know how, please refer to the Deploying a FortiGate VM into Proxmox tutorial. This tutorial uses FortiOS 7.0.14, but the steps below can be applied to any version.
3. You are familiar with Fortinet's FortiFlex product, have created a Flex Entitlement, and have a valid, unused FortiFlex token ready to use.
4. You are at least somewhat familiar with Fortinet's usage of cloud-init.

Workflow

Creating the config and license files

There are various methods to create the config and license files and get them onto a Proxmox node. You can create them locally on your computer and then SCP them to the node using command-line SCP or a GUI SCP client like WinSCP. You can also create them directly on the Proxmode node if you are comfortable with Linux and text editors such as nano or vi. Use whichever method works best for you.

The config file contains standard FortiOS config lines. For the purposes of this tutorial, we simply change the hostname. That said, you could add as many, or as few, configuration lines as desired. Instead of a typical FortiGate VM license file, FortiFlex uses a single token value to generate entitlement.

In the example below, two files have been created: config.txt and license.txt. The config.txt contains the lines necessary to change the hostname of the FortiGate VM. The license.txt file contains a single line with the FortiFlex token value. Of course, substitute the token value with your own valid token.

```
root@pve-hp-01:~# pwd
/root

root@pve-hp-01:~# ls
config.txt  license.txt

root@pve-hp-01:~# cat config.txt
config system global
set hostname my-fortigate-vm
end

root@pve-hp-01:~# cat license.txt
LICENSE-TOKEN: 4F83B7E8D79DC8FA06B3

root@pve-hp-01:~#
```

Creating the multipart MIME file

Use the `write-mime-multipart -o user_data config.txt license.txt` command to create a multipart MIME file from the config.txt and license.txt files. Ensure the output file is named user_data.

The write-mime-multipart program is part of the cloud-image-utils package and can be installed using the `apt-get install cloud-image-utils` command in your Proxmox node.

```
root@pve-hp-01:~# write-mime-multipart -o user_data config.txt license.txt

root@pve-hp-01:~# cat user_data
Content-Type: multipart/mixed; boundary="===============06943020547569871 48=="
MIME-Version: 1.0

----------------0694302054756987148==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="config.txt"

config system global
set hostname my-fortigate-vm
end

----------------0694302054756987148==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="license.txt"
```

```
LICENSE-TOKEN: 4F83B7E8D79DC8FA06B3

--================0694302054756987148==--

root@pve-hp-01:~#
```

Creating the cloud-init config-drive ISO

A standard cloud-init config-drive ISO follows a specific folder structure as follows:

```
root@pve-hp-01:~# tree -F
./
├── config-drive/
│           └── openstack/
│               ├── content/
│               │           └── 0000 <-- License data file
│               └── latest/
│                   └── user_data <-- Configuration data file
```

When using a FortiFlex token, the format is slightly different because both the configuration data and license data are contained within the single multipart MIME file.

```
root@pve-hp-01:~# tree -F
./
├── config-drive/
│           └── openstack/
│               ├── content/
│               └── latest/
│                   └── user_data <-- Multipart MIME file with both configuration and license
data
```

In your Proxmox node, create the directory structure above and copy your user_data file into the latest folder.

```
root@pve-hp-01:~# mkdir -p config-drive/openstack/content
root@pve-hp-01:~# mkdir -p config-drive/openstack/latest
root@pve-hp-01:~# cp user_data config-drive/openstack/latest/
```

Use the `mkisofs -R -r -o config-drive.iso config-drive/` command to create an ISO file.

If you do not have mkisofs on your Proxmox node, you can install it with the `apt-get install mkisofs` command.

```
root@pve-hp-01:~# ls
config-drive  config.txt  license.txt  user_data

root@pve-hp-01:~# mkisofs -R -r -o config-drive.iso config-drive
I: -input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 890
Total directory bytes: 6144
Path table size(bytes): 56
Max brk space used 1b000
179 extents written (0 MB)
```

```
root@pve-hp-01:~# ls
config-drive  config-drive.iso  config.txt  license.txt  user_data

root@pve-hp-01:~#
```

For simplicity, we copy the `config-drive.iso` file to the `local` storage device on the Proxmox node using the `cp config-drive.iso /var/lib/vz/template/iso/` command.

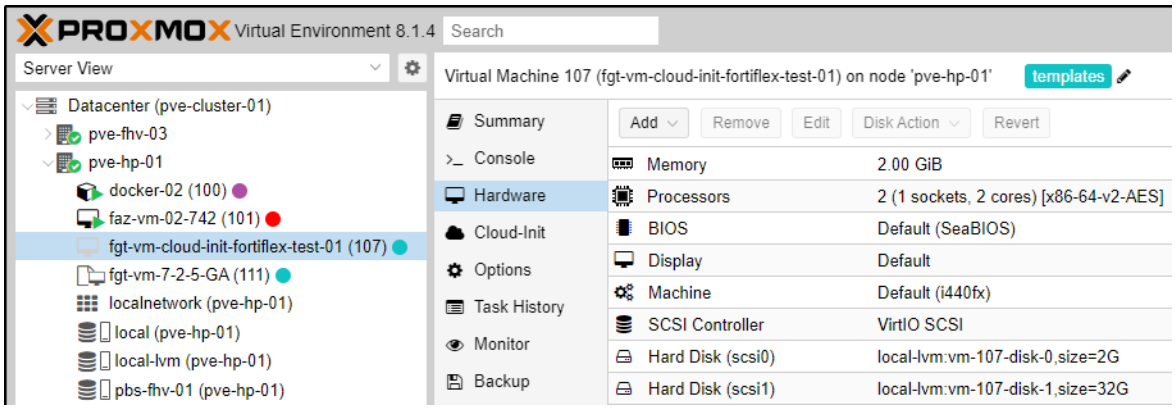
```
root@pve-hp-01:~# cp config-drive.iso /var/lib/vz/template/iso/

root@pve-hp-01:~# ls /var/lib/vz/template/iso/
config-drive.iso

root@pve-hp-01:~#
```

You can copy the config-drive.iso file to any Proxmox storage device capable of storing ISO files.

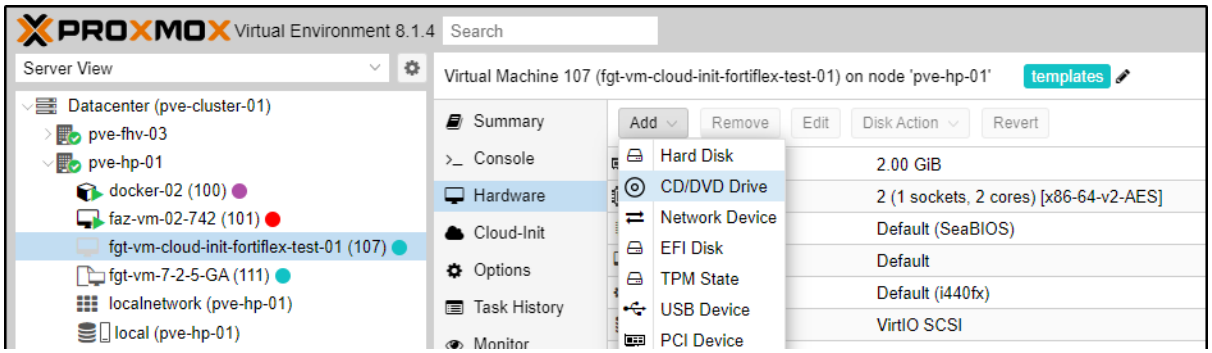
Deploying a FortiGate-VM and attaching the config-drive.iso

To deploy a FortiGate-VM and attach the config-drive.iso:

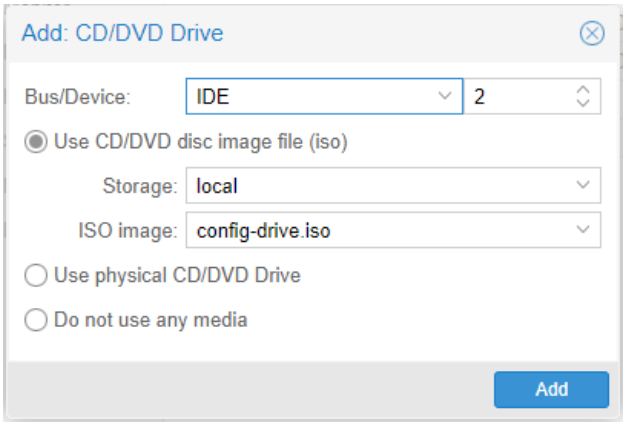
1. Deploy a base FortiGate VM as Deploying a FortiGate-VM into Proxmox on page 7 describes. Ensure that you do not start the VM.
2. Select the newly created VM in Proxmox in the left sidebar and then select the *Hardware* entry in the middle sidebar.



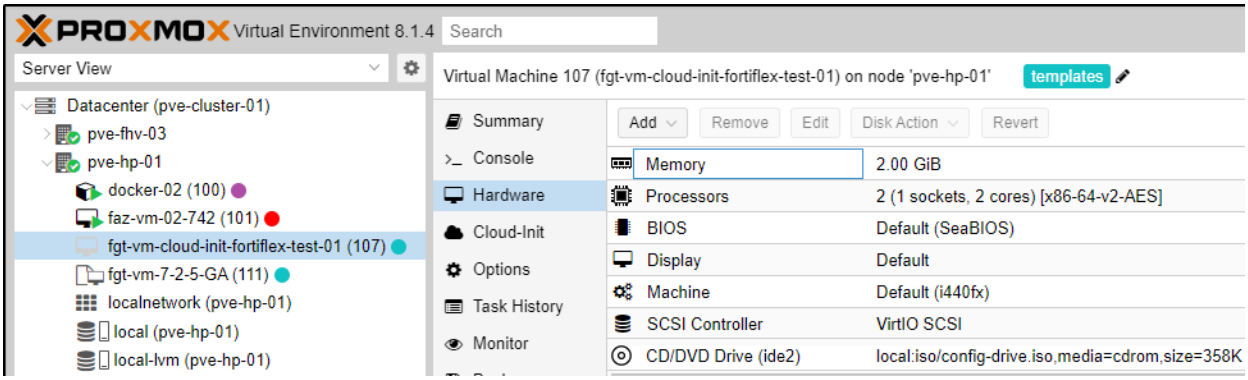
3. Click the *Add* dropdown and choose *CD/DVD Drive* from the options.



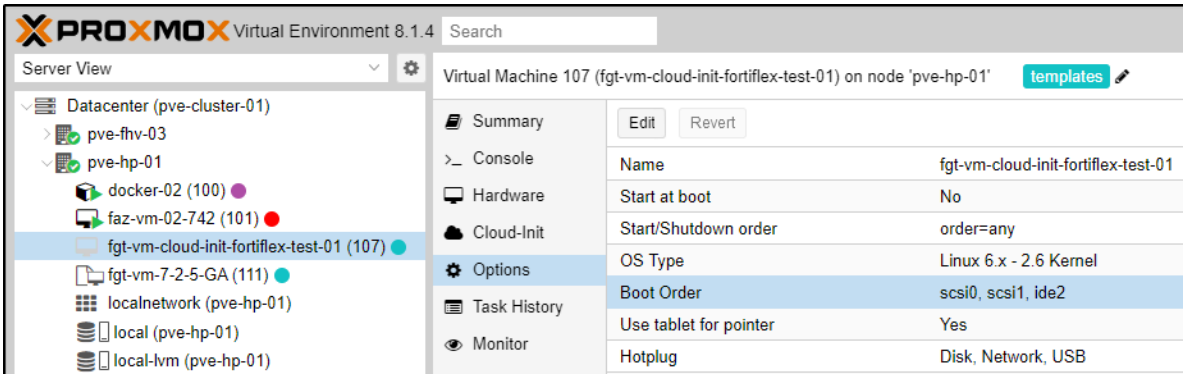
4. The *Add: CD/DVD Drive* dialog appears. Ensure the *Use CD/DVD disc image file (iso)* option is selected. In the *Storage* field, choose *local*. In the *ISO image* field, choose *config-drive.iso*. Click *Add* when finished.



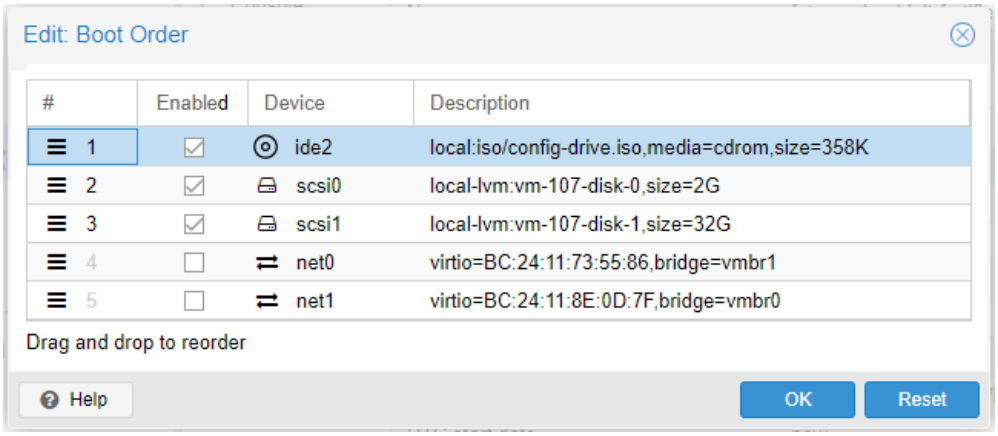
5. Ensure you see the newly added CD/DVD Drive.



6. In the middle sidebar, choose *Options*, highlight the *Boot Order* entry and click *Edit*.

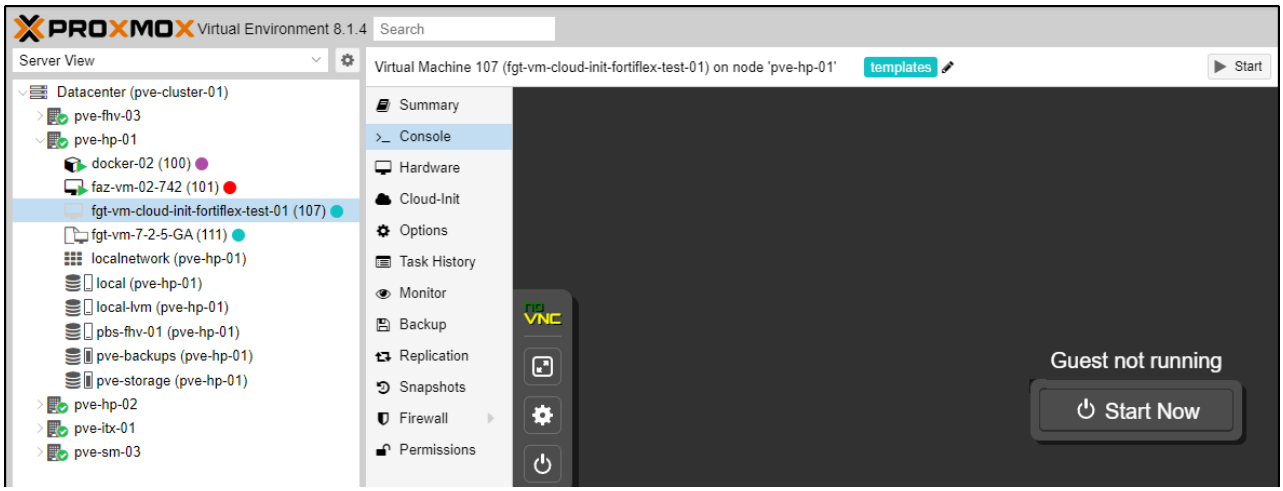


7. The *Edit: Boot Order* dialog appears. Using the selector icons, click and drag the *ide2* entry to the top of the list and verify that it is *Enabled* with a checkmark. Ensure that the *scsi0* and *scsi1* entries are *Enabled* with checkmarks and any *net#* drives are unselected. Click *OK* when done.



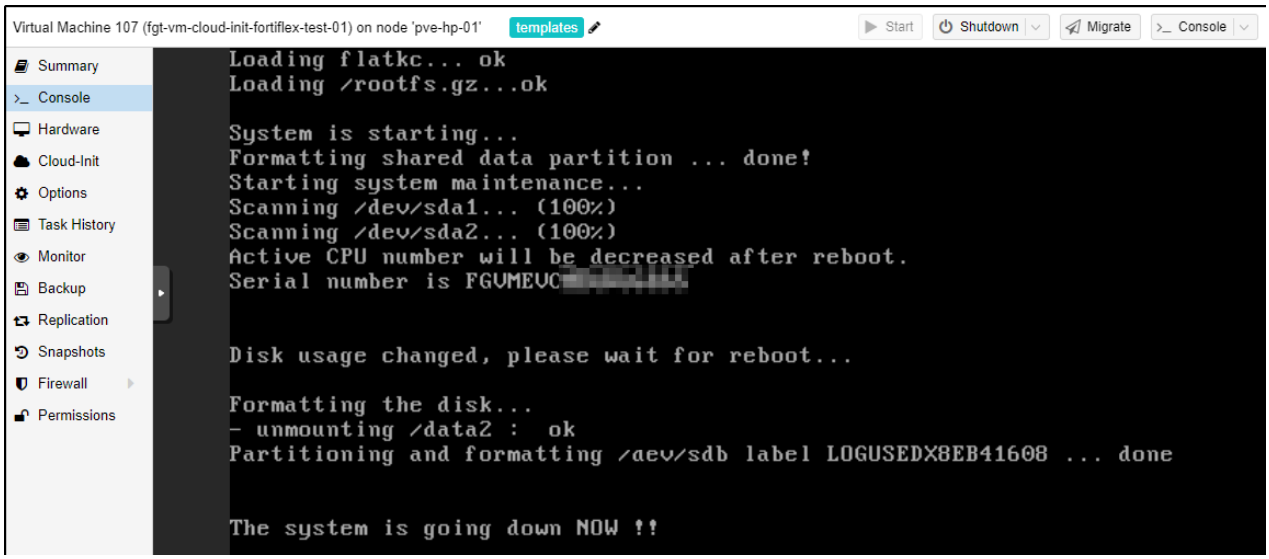
Depending on how you deployed your FortiGate-VM, you may not have a *scsi1* device, and the number of *net#* interfaces you have might differ from the screenshots.

8. In the middle sidebar, choose *Console* and click the *Start Now* button.

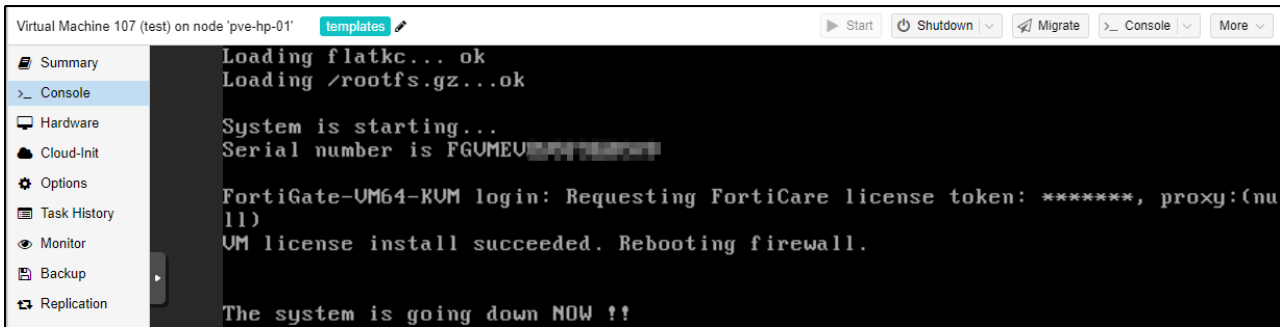


For cloud-init to properly entitle the FortiGate, it must have internet access when it boots. Typically, this is accomplished by the port1 interface getting an address via DHCP.

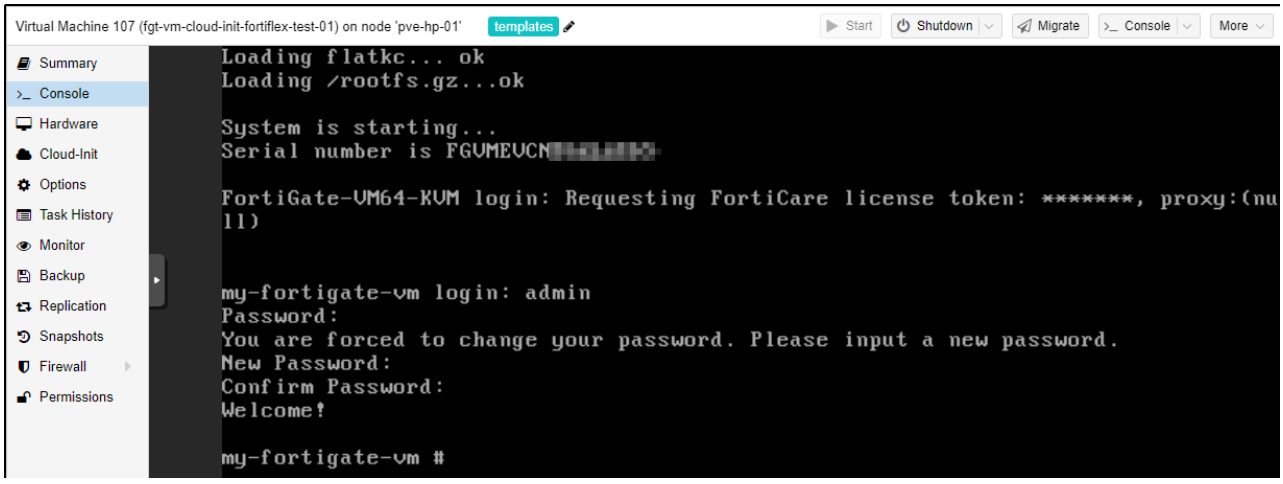
9. The VM starts to boot, generates a serial number, detects and formats any extra logging drives it finds, and reboots.



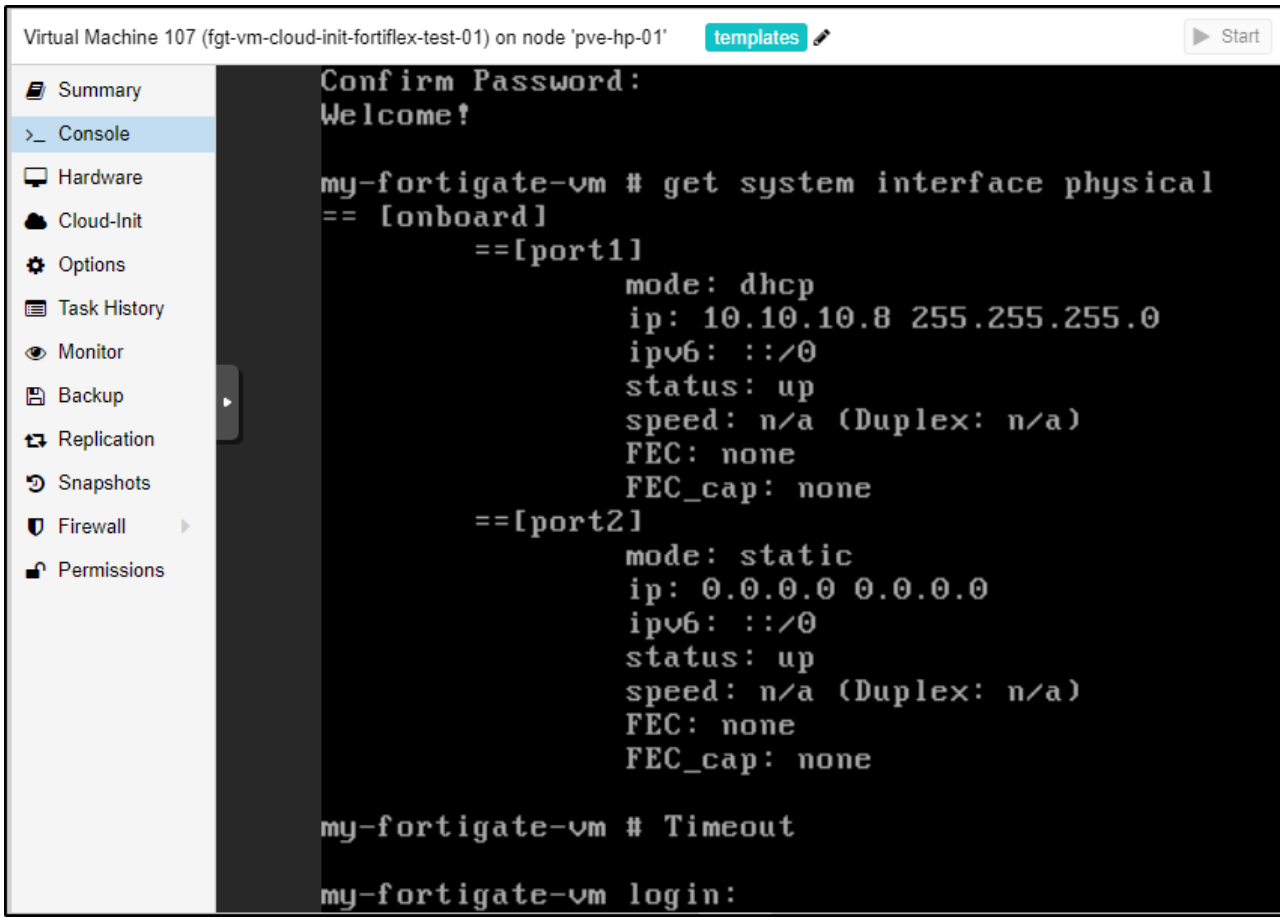
10. Allow 20-30 seconds after reboot for FortiGate to communicate with the FortiCloud servers to allow proper entitlement of the VM via the FortiFlex token. If all goes well, you should see the following FortiCloud messages automatically appear, followed by another automatic reboot.



11. After the reboot, notice the prompt change to the `my-fortigate-vm` we specified in the config. Log in with *admin* (no password) and change the password when requested.



12. Issue the `get system interface physical` command to see what address port1 received from DHCP.



Verifying cloud-init operation

There are a few commands you can use to verify cloud-init worked properly.

Enter the `get system status | grep License` command to verify the license's validity and expiration date.

```
my-fortigate-vm # get system status | grep License
License Status: Valid
License Expiration Date: 2024-05-09
```

Enter the `diagnose debug cloud-init show` command to show the result of the cloud-init boot log. This command is also a useful troubleshooting command when cloud-init does not work properly.

```
my-fortigate-vm # diagnose debug cloudinit show
 >> Checking metadata source config drive
 >> Unable to open disk /dev/ram5, No such file or directory
 >> Unable to open disk /dev/ram6, No such file or directory
 >> Unable to open disk /dev/ram7, No such file or directory
 >> Unable to open disk /dev/ram8, No such file or directory
 >> Unable to open disk /dev/ram9, No such file or directory
 >> Unable to open disk /dev/ram10, No such file or directory
 >> Unable to open disk /dev/ram11, No such file or directory
 >> Unable to open disk /dev/ram12, No such file or directory
 >> Unable to open disk /dev/ram13, No such file or directory
```

```
 >> Unable to open disk /dev/ram14, No such file or directory
 >> Unable to open disk /dev/ram15, No such file or directory
 >> Found config drive /dev/sr0
 >> Successfully mount config drive
 >> MIME parsed preconfig script
 >> MIME parsed VM token
 >> Found metadata source: config drive
 >> Run preconfig script
 >> FortiGate-VM64-KVM $  config system global
 >> FortiGate-VM64-KVM (global) $  set hostname my-fortigate-vm
 >> FortiGate-VM64-KVM (global) $  end
 >> Finish running preconfig script
 >> Trying to install vmlicense ...
 >> License-token: 4F83B7E8D79DC8FA06B3
 >> Config script not found in config drive
 >> Config script is not available
my-fortigate-vm #
```

Enter the `diagnose deb vm-print-license` command to reveal more detailed license information.

```
my-fortigate-vm # diagnose debug vm-print-license
SerialNumber: FGVMELTM24002814
CreateDate: Sun Mar 10 23:30:06 2024
License expires: Thu May  9 17:00:00 2024
Default Contract:
FMWR:6:20240310:20240510,ENHN:20:20240310:20240510,COMP:20:20240310:20240510,AVDB:6:20240310
:20240510,NIDS:6:20240310:20240510,FURL:6:20240310:20240510,SPAM:6:20240310:20240510,ISSS:6:
20240310:20240510,PBDS:6:20240310:20240510,FCSS:10:20240310:20240510,FGSA:6:20240310:2024051
0,SWNM:6:20240310:20240510,VMLS:6:20240310:20240510:2,SOAR:6:20240310:20240510,IOTH:6:202403
10:20240510,AFAC:6:20240310:20240510
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: EL (20)
CPU: 2 (subscription:2)
MEM: 2147483647
VDOM license:
  permanent: 2
  subscription: 0
my-fortigate-vm #
```

Another useful troubleshooting command is `diagnose hardware sysinfo vm full`.

```
my-fortigate-vm # diagnose hardware sysinfo vm full
UUID:     a32396a9db66444c89254f991bf250f5
valid:    1
status:   1
code:     200
warn:     0
copy:     0
received: 4294941305
warning:  4294941305
recv:     202403102331
dup:
my-fortigate-vm #
```

www.fortinet.com