Palo Alto Networks VM-Series for Nutanix Acropolis Hypervisor (AHV)

NUTANIX

Table of Contents

The VM-Series firewall is distributed using the QCOW2 format, which is one of the disk image formats supported by Nutanix AHV. This can be installed on any hardware that is capable of running Nutanix Acropolis Hypervisor.

For a list of hardware platform choices for Nutanix AHV, refer to the below link:

https://www.nutanix.com/products/hardware-platforms/

In order to deploy a VM-Series firewall on Nutanix AHV, you should be familiar with Nutanix Prism Element/Central, Image Service, AHV Networking and Configuration and VM guest deployment.

For more details refer : http://nutanixbible.com/#anchor-part-iv.-book-of-ahv-109

SYSTEM REQUIREMENTS

See VM-Series System Requirements for minimum hardware requirements for your VM-Series Model. The KVM Hypervisor requirements will hold good for Nutanix AHV as well.

https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/about-the-vm-series-firewall/vm-series-models/vm-series-system-requirements.html

Nutanix Cluster Requirements

Recommended Nutanix AOS (Acropolis Operating System) Version – 5.5.4 and above (LTS)
Recommended Nutanix AHV (Acropolis Hypervisor) Version – 20170830.156 and above (LTS)

Supported Deployments on Nutanix AHV

The VM-Series virtual appliance can be deployed on any node of Nutanix Cluster running AHV as the hypervisor. The supported configuration is L3 mode. vWire, and L2 modes will be supported in later releases of AOS/AHV integrated with Nutanix Flow.

SR-IOV, IPv6 is not supported by AHV at the time of writing this document.

Palo Alto Panorama Virtual Appliance is not supported on Nutanix AHV as of this release.

NOTE: Panorama virtual appliance running on a Nutanix ESXi cluster or Non-Nutanix ESXi cluster will be able to manage VM-Series virtual appliance running on AHV.

NUTANIX

VM-Series Limitations on AHV

DPDK mode in VM-Series 8.1.2

The PANOS versions 8.1.2 is supported on Nutanix AHV with dpdk mode disabled. On the VM-Series firewall, DPDK is enabled by default.

Disabled dpdk on vm-series using any of the below methods.

Method 1: PANOS CLI

- Download PANOS 8.1.0 qcow2 from Palo Alto Networks support site.
- Import it on AHV using image services, create a VM with this image and with 1 NIC attached.
- Power Up the VM and allow it to successfully boot up.
- Login to PANOS CLI and execute the command: set system setting dpdk-pkt-io off
- Reboot the VM for the changes to take effect.

Method 2: Bootstrap ISO

More details on VM-Series Firewall Bootstrap Workflow:
https://www.paloaltonetworks.com/documentation/81/virtualization/virtualization/bootstrap-the-vm-series-firewall/vm-series-firewall-bootstrap-workflow.html

The following link describes the fields in init-cfg.txt file:
https://www.paloaltonetworks.com/documentation/81/virtualization/virtualization/bootstrap-the-vm-series-firewall/create-the-init-cfgtxt-file/init-cfgtxt-file-components.html

In addition to the fields mentioned in the above link include the following to disable dpdk at first boot op-cmd-dpdk-pkt-io=off

Sample init-cfg.txt with dpdk disabled

```
type=dhcp-client
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=PAN
vm-auth-key=297791969289142
panorama-server=
panorama-server-2=
tplname=
dgname=
dns-primary=
dns-secondary=
op-command-modes=multi-vsys,jumbo-frame
dhcp-send-hostname=yes
```

dhcp-send-client-id=yes
dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=yes
op-cmd-dpdk-pkt-io=off

NOTE: this method does not require a reboot and dpdk mode is disabled on first boot.

Verify bootstrap completion

Execute the command : show system bootstrap status

```
admin@PANBS> show system bootstrap status

Bootstrap Phase              Status         Details
==============               ======         =======
Media Detection              Success        Media detected successfully
Media Sanity Check           Success        Media sanity check successful
Operational Commands         Success        Operational command set jumbo mode completed successfully; Operational command
set dpdk-pkt-io off completed successfully
Parsing of Initial Config    Successful
License Install              Successful     Successfully installed license key using authcode [redacted]
Auto-commit                  Successful
```

Pass criteria: “Media Detection”, “Media sanity check”, “Parsing of Initial Config”, “License install” and “auto commit status” are successful from “show system bootstrap status” output.

Execute the command: show system setting dpdk-pkt-io

```
admin@PANBS> show system setting dpdk-pkt-io

Device current Packet IO mode:                  Packet MMAP
Device DPDK Packet IO capable:                  yes
Device default Packet IO mode:                  DPDK
```

Pass criteria: “Device current Packet IO mode” is set to Packet MMAP mode.

NOTE: PANOS 8.1.3 release will have a fix that will support dpdk mode on Nutanix AHV.

Virtual Interfaces – Delete & Adding

PANOS Virtual Appliances deployed on Nutanix AHV do not support deleting and adding Interfaces at the same time. This is a limitation on AHV due to incorrect interface mac mapping with PCI-ID when deleting an existing virtual interface and adding new interfaces. This issue is an open item on Nutanix AHV which is targeted to be addressed in future releases.

For example, below is a PANOS VM with 12 virtual interfaces connected to it on Nutanix AHV. The interface mac to PCI-ID can be viewed using the following command from PAN CLI:

admin@PA-VM> debug show vm-series interfaces all

```
Interface_name       Base-OS_port       Base-OS_MAC             PCI-ID         Driver
        mgt                  eth0          50:6b:8d:bc:bb:8d                      virtio_net
        Ethernet1/1          eth1          50:6b:8d:43:0b:80       0000:00:04.0   rte_virtio_pmd
```

```
        Ethernet1/2             eth2          50:6b:8d:85:3c:83       0000:00:05.0   rte_virtio_pmd
        Ethernet1/3             eth3          50:6b:8d:39:12:d7       0000:00:09.0   rte_virtio_pmd
        Ethernet1/4             eth4          50:6b:8d:19:13:dd       0000:00:0a.0   rte_virtio_pmd
        Ethernet1/5             eth5          50:6b:8d:83:94:2f       0000:00:0b.0   rte_virtio_pmd
        Ethernet1/6             eth6          50:6b:8d:06:55:b1       0000:00:0c.0   rte_virtio_pmd
        Ethernet1/7             eth7          50:6b:8d:c7:64:89       0000:00:0d.0   rte_virtio_pmd
        Ethernet1/8             eth8          50:6b:8d:ac:83:7e       0000:00:0e.0   rte_virtio_pmd
        Ethernet1/9             eth9          50:6b:8d:e5:34:c3       0000:00:0f.0   rte_virtio_pmd
        Ethernet1/10            eth10         50:6b:8d:d0:68:7a       0000:00:10.0   rte_virtio_pmd
        Ethernet1/11            eth11         50:6b:8d:4f:0d:57       0000:00:13.0   rte_virtio_pmd
        Ethernet1/12            eth12         50:6b:8d:e2:18:da       0000:00:14.0   rte_virtio_pmd
```

Deleting Ethernet 1/9 (from the above config) and adding 2 new interfaces and a reboot of the PANOS VM results in the mac to PCI-ID mapping to change. See the below output of the above command after the interface/s are deleted and added.

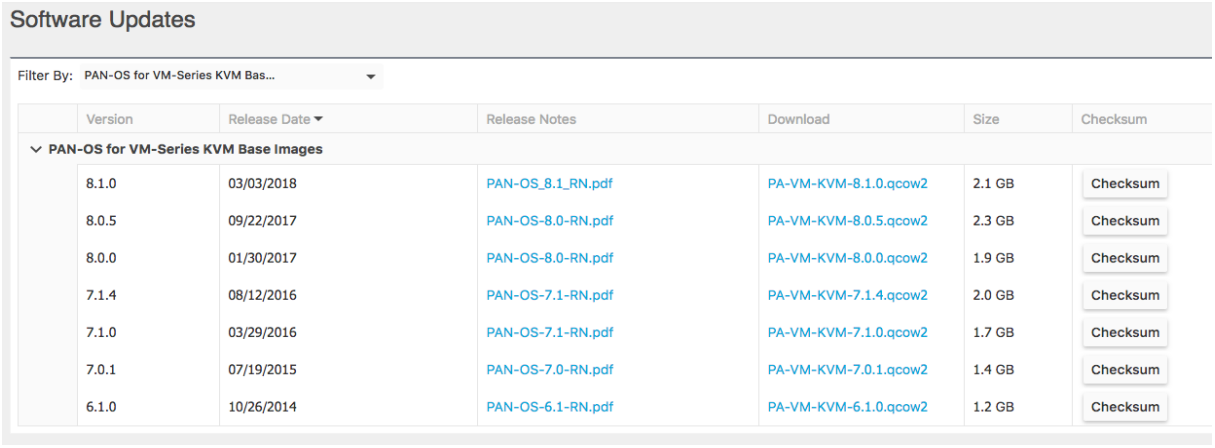
```
admin@PA-VM> debug show vm-series interfaces all
    Interface_name       Base-OS_port       Base-OS_MAC             PCI-ID         Driver
    mgt                     eth0          50:6b:8d:bc:bb:8d                     virtio_net
    Ethernet1/1             eth1          50:6b:8d:43:0b:80       0000:00:04.0   rte_virtio_pmd
    Ethernet1/2             eth2          50:6b:8d:85:3c:83       0000:00:05.0   rte_virtio_pmd
    Ethernet1/3             eth3          50:6b:8d:39:12:d7       0000:00:09.0   rte_virtio_pmd
    Ethernet1/4             eth4          50:6b:8d:19:13:dd       0000:00:0a.0   rte_virtio_pmd
    Ethernet1/5             eth5          50:6b:8d:83:94:2f       0000:00:0b.0   rte_virtio_pmd
    Ethernet1/6             eth6          50:6b:8d:06:55:b1       0000:00:0c.0   rte_virtio_pmd
    Ethernet1/7             eth7          50:6b:8d:c7:64:89       0000:00:0d.0   rte_virtio_pmd
    Ethernet1/8             eth8          50:6b:8d:ac:83:7e       0000:00:0e.0   rte_virtio_pmd
    Ethernet1/9             eth9          50:6b:8d:d0:68:7a       0000:00:10.0   rte_virtio_pmd
    Ethernet1/10            eth10         50:6b:8d:b1:f6:31       0000:00:11.0   rte_virtio_pmd.(Newly
    added)
    Ethernet1/11            eth11         50:6b:8d:9e:3c:f9       0000:00:12.0   rte_virtio_pmd.(Newly
    added)
    Ethernet1/12            eth12         50:6b:8d:4f:0d:57       0000:00:13.0   rte_virtio_pmd
    Ethernet1/13            eth13         50:6b:8d:e2:18:da       0000:00:14.0   rte_virtio_pmd
```

From the above, it shows the previous Ethernet1/10 (from step 1) has now moved to Ethernet1/9 (in Step 2) and the two new interfaces have been assigned Ethernet1/10 & 1/11. This creates a security loophole as PAN assigns security policies to Zones. Zones are a collection of the interfaces for which the Admin wants to apply a security policy. This way if an interface which was in untrusted zone goes into trusted zone and Network admin has to reconfigure it from PAN every time they delete and add new interfaces.

NUTANIX

Set Up a VM-Series Firewall on a Nutanix Acropolis Hypervisor Cluster

Download VM-Series qcow2 image from Pala Alto Networks support site - https://support.paloaltonetworks.com/Support/Index



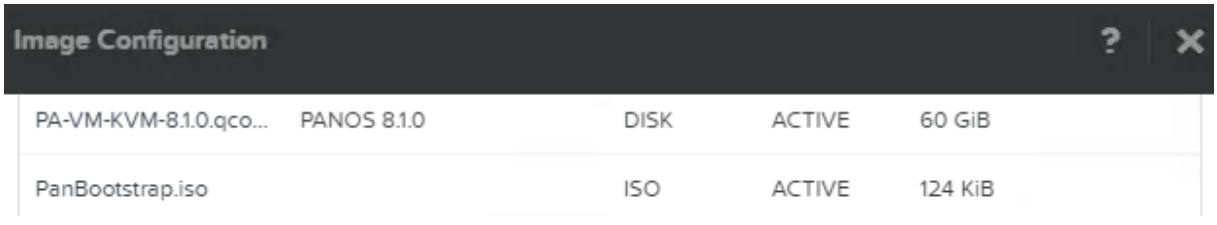
Version	Release Date	Release Notes	Download	Size	Checksum
PAN-OS for VM-Series KVM Base Images					
8.1.0	03/03/2018	PAN-OS_8.1_RN.pdf	PA-VM-KVM-8.1.0.qcow2	2.1 GB	Checksum
8.0.5	09/22/2017	PAN-OS-8.0-RN.pdf	PA-VM-KVM-8.0.5.qcow2	2.3 GB	Checksum
8.0.0	01/30/2017	PAN-OS-8.0-RN.pdf	PA-VM-KVM-8.0.0.qcow2	1.9 GB	Checksum
7.1.4	08/12/2016	PAN-OS-7.1-RN.pdf	PA-VM-KVM-7.1.4.qcow2	2.0 GB	Checksum
7.1.0	03/29/2016	PAN-OS-7.1-RN.pdf	PA-VM-KVM-7.1.0.qcow2	1.7 GB	Checksum
7.0.1	07/19/2015	PAN-OS-7.0-RN.pdf	PA-VM-KVM-7.0.1.qcow2	1.4 GB	Checksum
6.1.0	10/26/2014	PAN-OS-6.1-RN.pdf	PA-VM-KVM-6.1.0.qcow2	1.2 GB	Checksum

Download “PA-VM-KVM-8.1.0.qcow2” from the list of “PAN-OS for VM-Series KVM Base Images”

Upload the base image to Nutanix AHV cluster using Prism Image Services. Follow the steps as mentioned in Nutanix Support Portal - https://portal.nutanix.com/#/page/docs/details?targetId=Prism-Central-Guide-Prism-v55:mul-image-add-pc-t.html

Upgrade the VM-Series PAN-OS to 8.1.2 or 8.1.3 as per the procedure defined here: https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/upgrade-to-pan-os-81/upgrade-the-firewall-to-pan-os-81

For PAN-OS 8.1.2, create a Bootstrap ISO file using the steps mentioned in the earlier section and upload the ISO file to Nutanix image service. Upon successful upload the Prism image service should display the files as “Active” as shown below:

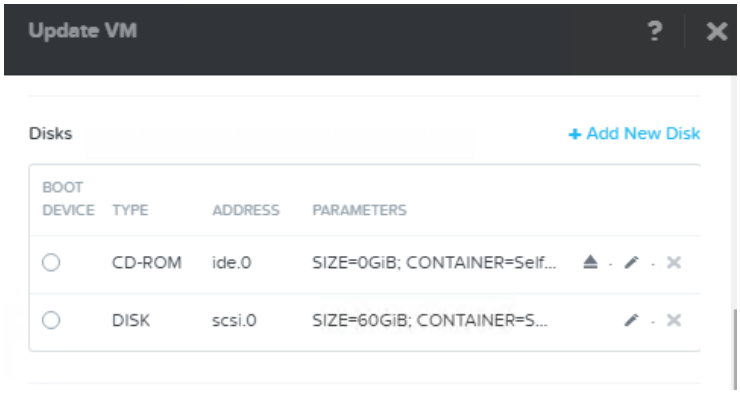


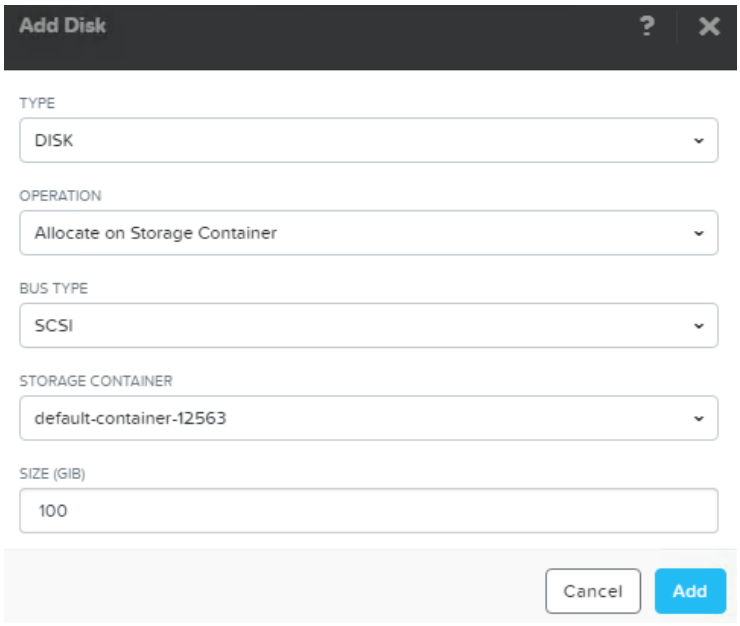
Create a VM from the above images using Prism UI. The “Create VM” option in Prism Element provide the options to set “Name”, virtual resources like – vcpu, memory and attach, vDisk and ISO and also configure network interfaces. Please follow the steps mentioned here:

https://portal.nutanix.com/#/page/docs/details?targetId=Prism-Central-Guide-Prism-v55:mul-vm-create-acropolis-pc-t.html#ntask_hmj_fzt_zt

NOTE: The ISO file is attached to the VM using an IDE bus and the disk image is attached to the VM using a SCSI bus type.

Add an additional disk to the VM for logging.





Also, login to CVM of the cluster and disable bridge chaining on AHV/AOS running 5.5.x. This will not be required in AHV/AOS releases 5.8 and above.

$ manage_ovs disable_bridge_chain

Power on the PANOS VM and allow it to boot up successfully.

NUTANIX

Verify deployment of VM-Series on Nutanix AHV

1. Verify Hypervisor is identified – Pass criteria “show system info” output reports the vm-mode as ‘KVM’

```
admin@PANBS> show system info

hostname: PANBS
ip-address: [redacted]
public-ip-address: [redacted]
netmask: 255.255.240.0
default-gateway: [redacted]
ip-assignment: dhcp
ipv6-address: unknown
ipv6-link-local-address: fe80::526b:8dff:fe5f:29f1/64
ipv6-default-gateway:
mac-address: 50:6b:8d:5f:29:f1
time: Mon Aug 13 00:45:33 2018
uptime: 0 days, 0:02:40
family: vm
model: PA-VM
serial: 007254000050672
vm-mac-base: D4:1D:71:E7:A2:00
vm-mac-count: 256
vm-uuid: 77251E2F-F4D7-46F7-B4AD-A51BD7380807
vm-cpuid: KVM:610F0000FFFB8B0F
vm-license: VM-300
vm-mode: KVM
cloud-mode: non-cloud
sw-version: 8.1.2
global-protect-client-package-version: 0.0.0
app-version: 769-4439
app-release-date:
av-version: 0
av-release-date:
threat-version: 0
threat-release-date:
wf-private-version: 0
wf-private-release-date: unknown
url-db: paloaltonetworks
wildfire-version: 0
wildfire-release-date:
url-filtering-version: 0000.00.00.000
global-protect-datafile-version: unknown
global-protect-datafile-release-date: unknown
global-protect-clientless-vpn-version: 0
global-protect-clientless-vpn-release-date:
logdb-version: 8.1.8
platform-family: vm
vpn-disable-mode: off
multi-vsys: off
operational-mode: normal
```

2. Verify Dataplane is ready – Pass criteria “show chassis-ready” output reports ‘yes’

```
admin@PANBS> show chassis-ready

yes

admin@PANBS>
```

3. Verify additional disk for logging is identified – Verify the disk in “show system disk-space”. Also, login to the UI and verify that the Log Storage capacity accurately displays the new disk capacity in Device → Setup → Management under Logging and Reporting Settings.

```
admin@PANBS> show system disk-space

Filesystem            Size  Used Avail Use% Mounted on
/dev/sda3             6.9G  2.4G  4.3G  36% /
/dev/sda5              16G  1.5G   14G  10% /opt/pancfg
/dev/sda6             7.9G  1.3G  6.2G  18% /opt/panrepo
tmpfs                 4.8G  4.0G  837M  83% /dev/shm
/dev/sr0              124K  124K     0 100% /mnt/cdrom
/dev/sdb1              99G  200M   94G   1% /opt/panlogs
tmpfs                  12M     0   12M   0% /opt/pancfg/mgmt/lcaas/ssl/private
```