



# Nutanix and Palo Alto Networks Service Chain Integration Guide

Author: Nutanix & Palo Alto Networks

Deploying Palo Alto Networks VM-Series Next-Generation Firewall

Enforcing Microsegmentation with Nutanix Flow and Palo Alto Networks VM-Series Next-Generation Firewall

# Table of Contents

Nutanix and Palo Alto Networks Service Chain Integration Guide	1
Use cases for integration into Palo Alto Networks VMSeries	3
Use Case: Micro-Segmentation	3
Use Case: Virtual Desktop Infrastructure	3
Palo Alto Networks Products for Integration	3
Integration Benefits	4
Partner Information	5
Prerequisite Validation	6
Deploy Palo Alto Networks Panorama	8
Prepare Panorama for Logging	17
Deploy VM SERIES	19
Initial Configuration for VM Series	24
Panorama Configuration	27
NUTANIX Service Chain Configuration	38
Direct Traffic to Network Function Chain	47
Configure Dynamic Address Groups	55
Create Custom Application for NUTANIX	61
Best Practices	68
References	69

## Use cases for integration into Palo Alto Networks VM-Series

### Use Case: Micro-Segmentation

**Challenge:** Virtual applications running on the same host are difficult to selectively segment without complex network design and configuration, often requiring hair pinning traffic and negatively impacting performance. This may lead to increased threat exposure or vulnerabilities in your virtualized environments.

**Answer:** Micro-segmentation helps reduce the attack surface by preventing lateral movement across your east-west traffic. This is accomplished by deploying VM-Series integrated with Nutanix Flow. Use the Nutanix Calm blueprint to create service chains and deploy VM-Series on every AHV host. With Nutanix Flow, specific traffic can be transparently directed to the VM-Series firewall in the service chain for deep packet inspection based on the user-defined Nutanix Flow policy.

### Use Case: Virtual Desktop Infrastructure

**Challenge:** Virtual desktops are growing in popularity but hosting all of these desktops within your core data center also dramatically increases your attack surface without the proper protections in place. The dynamic nature of these desktops can also make security management challenging.

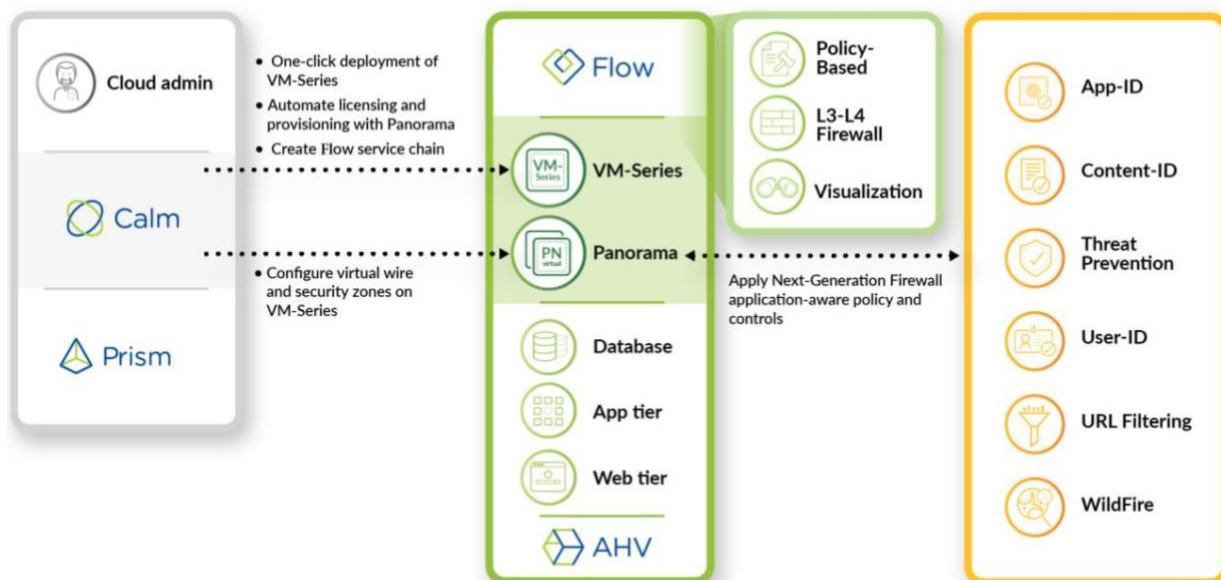
**Answer:** To address this concern, Nutanix Flow can isolate groups of virtual desktops with a simple security policy and work with VM-Series on AHV to inspect and enforce Layer 7 controls as well as block threats across the virtual desktop infrastructure.

## Palo Alto Networks Products for Integration

Palo Alto Networks Products	Integration Status	Palo Alto Networks Versions Tested	Nutanix Versions
Panorama	Complete	Panorama 8.1.11 Panorama 9.0.4 Panorama 9.0.6 Panorama 9.1.2	AOS 5.19 (20190916.360) NCC (3.10.1.2) Foundation 4.62 LCM 2.3.4.2
VM-Series	Complete	PAN-OS 8.1.1 PAN-OS 9.x and above	AOS 5.19 (20190916.360) NCC (3.10.1.2) Foundation 4.62 LCM 2.3.4.2

## Integration Benefits

When integrated with Palo Alto Networks VM-Series next-generation virtual firewalls, Flow's ability to control traffic is augmented with industry-leading threat prevention capabilities. While micro-segmentation can help reduce the attack surface of a Nutanix environment, VM-Series threat prevention services ensure that threats attempting to penetrate the perimeter, move laterally across legitimate network connections, or exfiltrate data are detected and stopped. Real-time threat intelligence feeds arm VM-Series with the latest threat signatures detected across the entire Palo Alto Networks install-base to protect Nutanix environments from the latest zero-day threats.



## Partner Information

Partner Information	
Date	June 4, 2021
Partner Name	Nutanix and Palo Alto Networks
Web Site	<a href="https://www.nutanix.com">https://www.nutanix.com</a> & <a href="https://www.paloaltonetworks.com">https://www.paloaltonetworks.com</a>
Product Name	Nutanix Calm Nutanix Flow Palo Alto Networks Panorama & VM-Series Next-Generation Firewall
Partner Contact	<a href="mailto:alliances@nutanix.com">alliances@nutanix.com</a> <a href="mailto:nutanix@paloaltonetworks.com">nutanix@paloaltonetworks.com</a>
Support Contact	<a href="https://www.nutanix.com/support-services/product-support">https://www.nutanix.com/support-services/product-support</a> <a href="https://support.paloaltonetworks.com">https://support.paloaltonetworks.com</a>
Product Description	Automated deployment of Palo Alto Networks VM-Series Next Generation Firewall and Microsegmentation on Nutanix AHV

## Prerequisite Validation

Prior to deploying the VM-Series firewalls confirm you have all the prerequisites in place.

The below Nutanix hypervisor (AHV) version is based off of our testing, please refer to the compatibility matrix to confirm the supported version for your deployment scenario.

<https://docs.paloaltonetworks.com/compatibility-matrix/vm-series-firewalls/vms-series-hypervisor-support.html>

### Nutanix Components:

- Prism Central (Management Console)
  - Flow license enabled
- Nutanix Hypervisor (AHV)
  - AOS 5.19 (20190916.360)

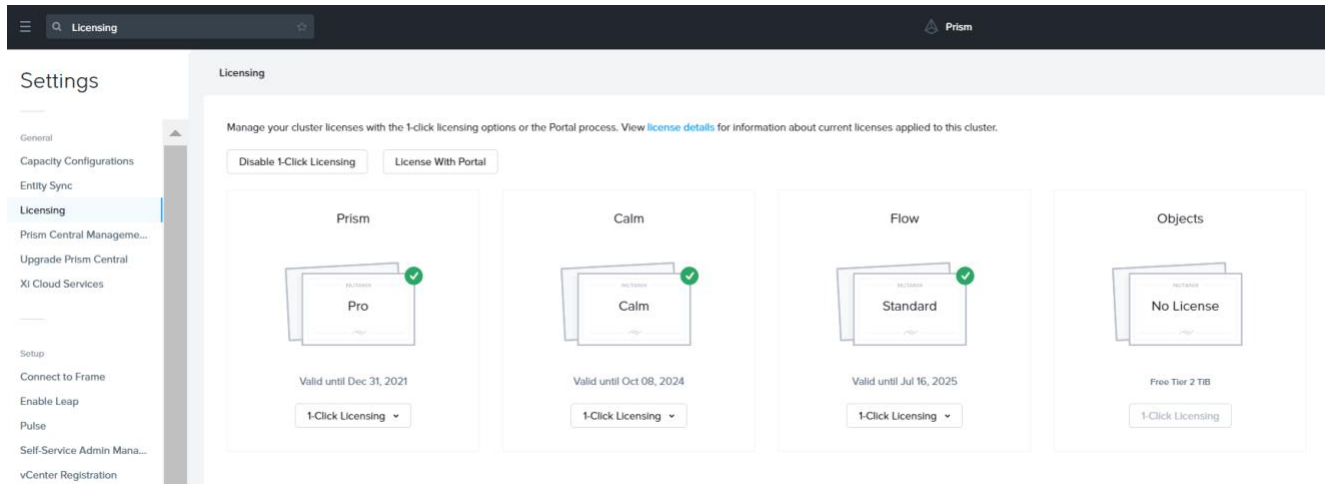
### PAN-OS Supported

9.x and above

## Validation

Flow License Installed (allow for East-West integration)

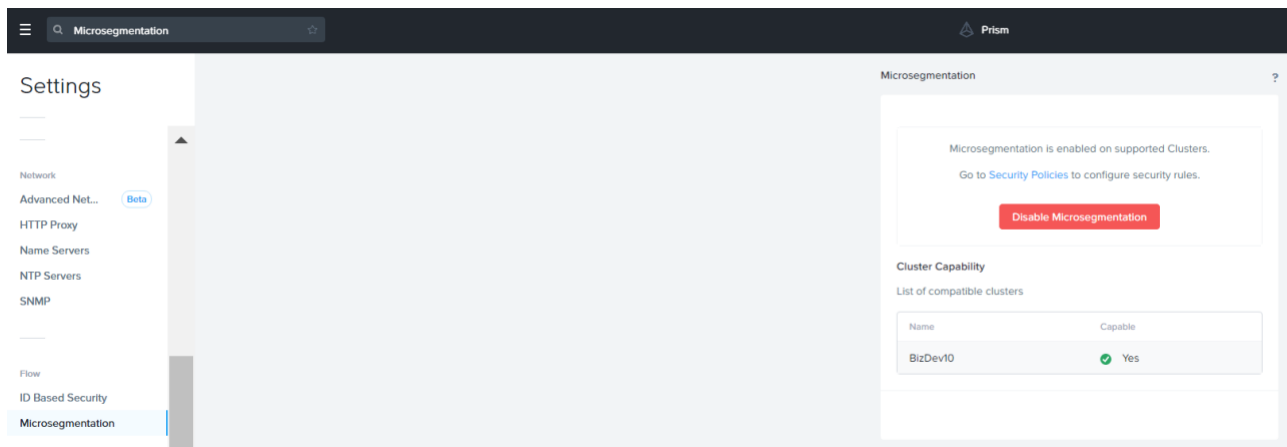
Prism Central -> Prism Central Settings -> Licensing



Nutanix Prism Central Settings - Licensing - Flow License Enabled

Microsegmentation License Installed

Prism Central -> Prism Central Settings -> Microsegmentation



Nutanix Prism Central Settings - Microsegmentation License Enabled

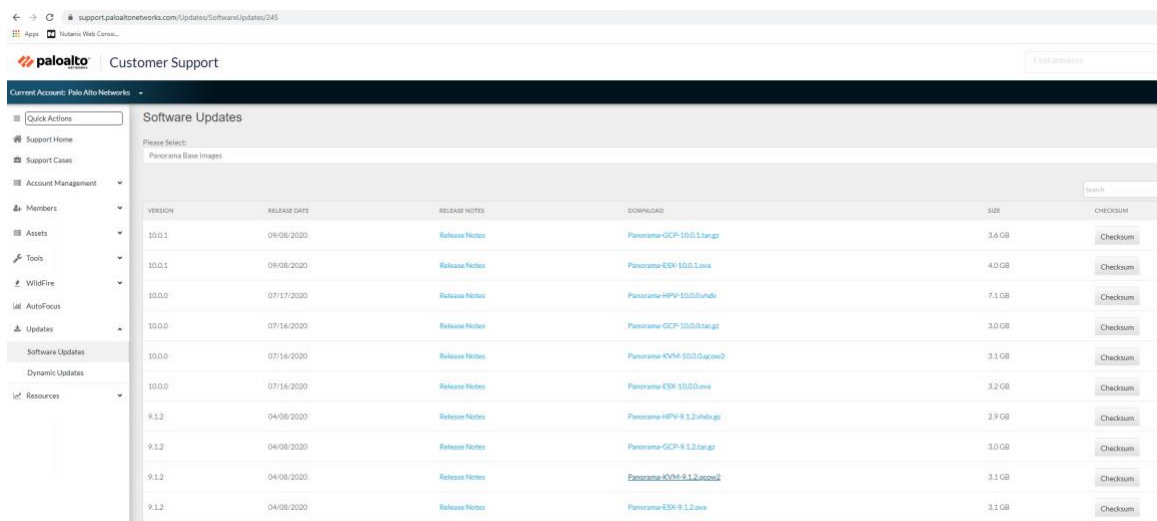
# Deploy Palo Alto Networks Panorama

You can now deploy Panorama and a Dedicated Log Collector on Nutanix AHV. Panorama deployed on AHV is Bring Your Own License (BYOL), supports all deployment modes (Panorama, Log Collector, and Management Only), and shares the same processes and functionality as the M-Series hardware appliances.

## 1. Download Panorama Base Image

URL: <https://support.paloaltonetworks.com/Updates/SoftwareUpdates/245>

Filename: Panorama-KVM-9.1.2.qcow2



VERSION	RELEASE DATE	RELEASE NOTES	DOWNLOAD	SIZE	CHECKSUM
10.0.1	09/08/2020	<a href="#">Release Notes</a>	<a href="#">Panorama-GCP-10.0.1.tar.gz</a>	3.6 GB	<a href="#">Checksum</a>
10.0.1	09/08/2020	<a href="#">Release Notes</a>	<a href="#">Panorama-ESX-10.0.1.ova</a>	4.0 GB	<a href="#">Checksum</a>
10.0.0	07/17/2020	<a href="#">Release Notes</a>	<a href="#">Panorama-HPV-10.0.0.ova</a>	7.1 GB	<a href="#">Checksum</a>
10.0.0	07/16/2020	<a href="#">Release Notes</a>	<a href="#">Panorama-GCP-10.0.0.tar.gz</a>	3.0 GB	<a href="#">Checksum</a>
10.0.0	07/16/2020	<a href="#">Release Notes</a>	<a href="#">Panorama-KVM-10.0.0.qcow2</a>	3.1 GB	<a href="#">Checksum</a>
10.0.0	07/16/2020	<a href="#">Release Notes</a>	<a href="#">Panorama-ESX-10.0.0.ova</a>	3.2 GB	<a href="#">Checksum</a>
9.1.2	04/08/2020	<a href="#">Release Notes</a>	<a href="#">Panorama-HPV-9.1.2.vhdx.gz</a>	2.9 GB	<a href="#">Checksum</a>
9.1.2	04/08/2020	<a href="#">Release Notes</a>	<a href="#">Panorama-GCP-9.1.2.tar.gz</a>	3.0 GB	<a href="#">Checksum</a>
9.1.2	04/08/2020	<a href="#">Release Notes</a>	<a href="#">Panorama-KVM-9.1.2.qcow2</a>	3.1 GB	<a href="#">Checksum</a>
9.1.2	04/08/2020	<a href="#">Release Notes</a>	<a href="#">Panorama-ESX-9.1.2.ova</a>	3.1 GB	<a href="#">Checksum</a>

## Palo Alto Networks Customer Support Portal - Updates - Software Updates

## 2. Create a Nutanix Image Configuration by going to **Prism Central -> Virtual Infrastructure -> Images -> Add Image**



Add Images

---

1 Select Image 2 Select Location

---

Image Source

☒ Image File ☐ URL

+ Add File

---

Cancel Next

## Prism Central - Virtual infrastructure - Images - Add Images

Add Images

---

1 Select Image 2 Select Location

---

Image Source

☒ Image File ☐ URL

+ Add File

Source: [LOCAL]Panorama-KVM-9.1.2.qcow2 Remove

Image Name Image Type

Panorama-KVM-9.1.2.qcow2 Disk

Image Description

PA-VM-Panorama-9.1.2

Checksum

7a2ccd99228dcd2a5177a1830f88729a52dbd4 SHA-256

---

Cancel Next

## Prism Central - Virtual infrastructure - Images - Add Images - upload QCOW2

Checksum can be added to validate that the QCOW2 is not corrupted but is not mandatory for the upload.

When adding the image make sure to identify which cluster you would like to upload the image to.

Add Images

1 Select Image

2 Select Location

Placement Method

☒ Place image directly on clusters

This option is good for smaller environments. The image will be placed on all selected clusters below.

☐ Place image using Image Placement policies

This option is good for larger environments. It requires you to first set up Image Placement policies between categories assigned to clusters and categories assigned to images. From there on, you only need to associate a relevant category to an image while uploading it here.

Select Clusters

Select the set of clusters to use for placement

☒ All clusters

Name

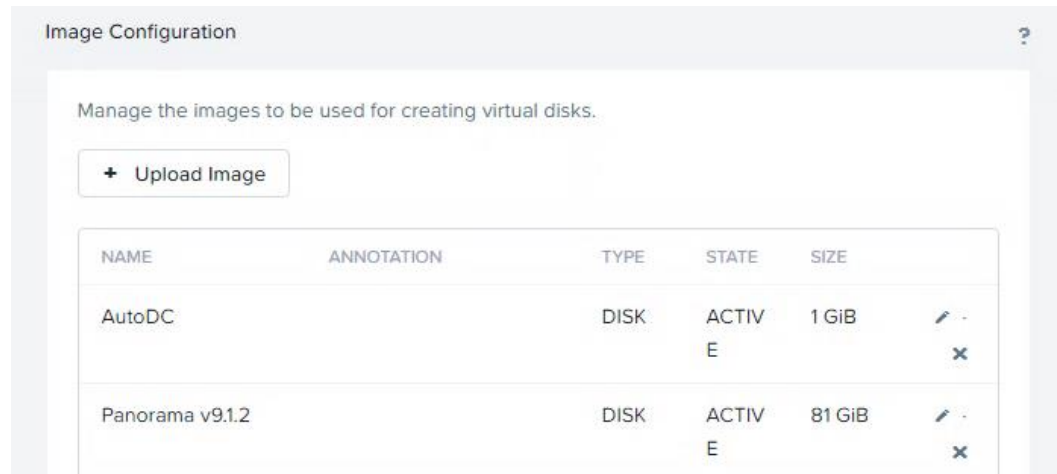
☐ BizDev10

Back

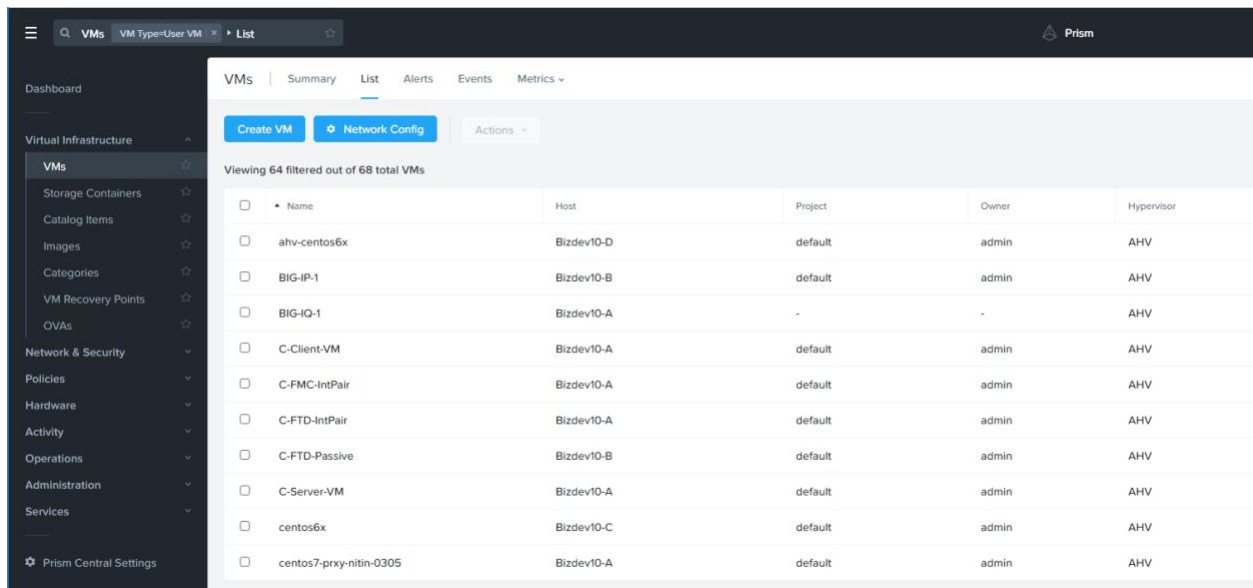
Save

Prism Central - Virtual infrastructure - Images - Add Images - cluster selection

Wait for Image State to become **Active**.



3. Navigate to the Virtual Infrastructure tab on Prism. Create a new VM by selecting the VM tab and clicking on the **Create VM** button.



Ref: <https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/set-up-panorama/setup-the-panorama-virtual-appliance/setup-prerequisites-for-the-panorama-virtual-appliance.html>

Refer to the following table for VM deployment values.

Panorama Virtual Appliance Configurations	
Compute Details	
vCPU(s)	1
Number of Cores per vCPU	16
Memory	32
Boot Configuration	
Legacy BIOS	DISK (scsi.0)
Disks	
scsi.0	81GB (From Image)
scsi.1	2000GB
Network Adapters (NIC)	
NIC 1 - VLAN ID	0

Create VM

Compute Details

vCPU(s)  
1

Number Of Cores Per vCPU  
16

Memory ?  
32 GiB

Boot Configuration

Legacy BIOS

Set Boot Priority

DISK (scsi.0)

Only the selected disk will be used for boot. (No fallback to other disks)

UEFI ?

Cancel

Save

Add Disk

Type  
DISK

Operation  
Clone from Image Service

Bus Type  
SCSI

Image ?  
Panorama-KVM-10.0.4.qcow2

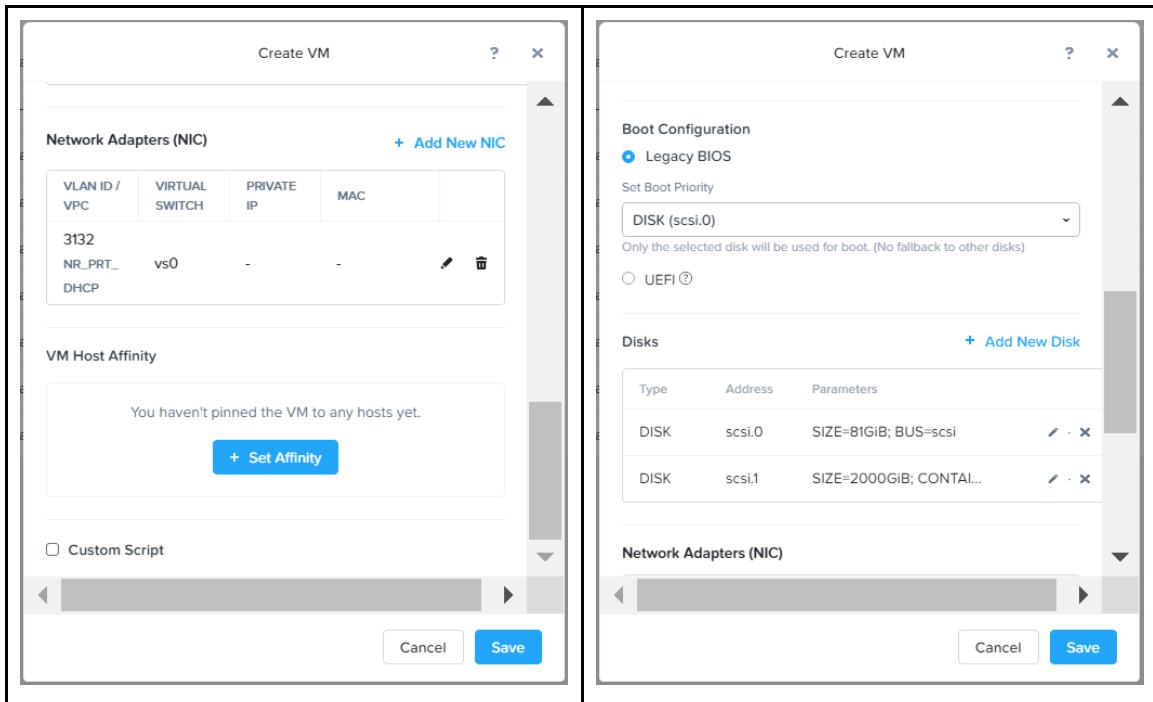
Size (GiB) ?  
81  
Please note that changing the size of an image is not allowed.

Index  
Next Available

Cancel

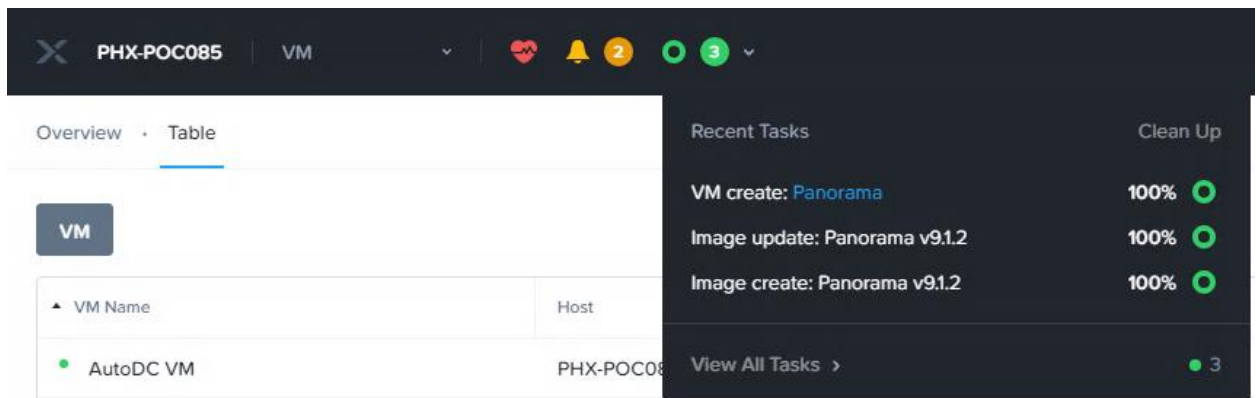
Add

Prism Central - Virtual infrastructure - VM - Create VM (1)



Prism Central - Virtual infrastructure - VM - Create VM (2)

- Once the VM has been provisioned, click **Save** and the VM will automatically deploy. Monitor **Recent Tasks** to ensure the VM deployed successfully.



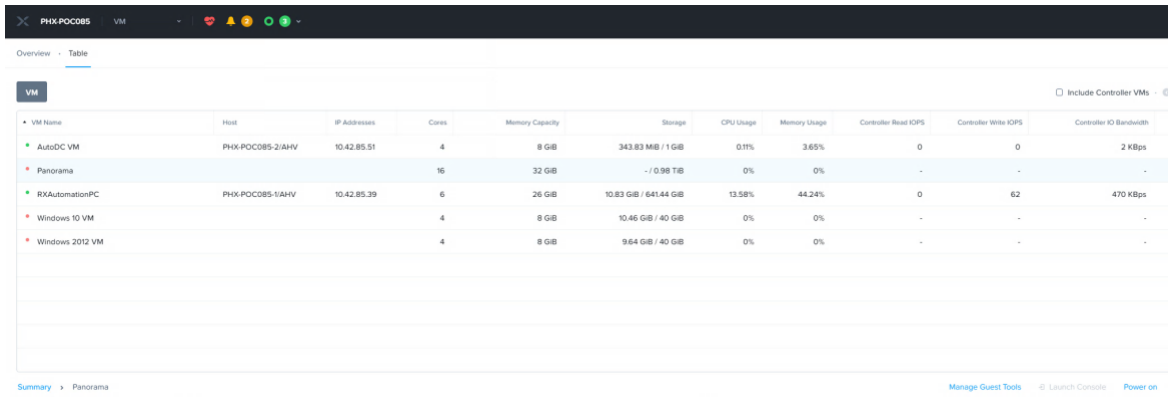
- The default boot behavior of Panorama or a VM-Series firewall will get stuck on the bootloader. This is because PAN-OS is looking for a serial port during the boot process; however, Nutanix does not automatically add serial ports during deployment. Login to any CVM via SSH. Run the following command to complete this step.

acli vm.serial\_port\_create “VM Name” type=kServer index=0

```
** SSH to CVM via 'nutanix' user will be restricted in coming releases. **
** Please consider using the 'admin' user for basic workflows. **
nutanix@NTNX-13SM36500024-A-CVM:10.42.85.29:~$ acli vm.serial_port_create Panorama type=kServer index=0
VmUpdate: pending
VmUpdate: complete
nutanix@NTNX-13SM36500024-A-CVM:10.42.85.29:~$
```

Once a serial port has been assigned to the Panorama VM, proceed to the next step.

6. On the Prism Element Web-UI, navigate to the Panorama VM and click **Power On**. After a few seconds, the Launch Console button will appear. Click on **Launch Console** to access the Panorama CLI.

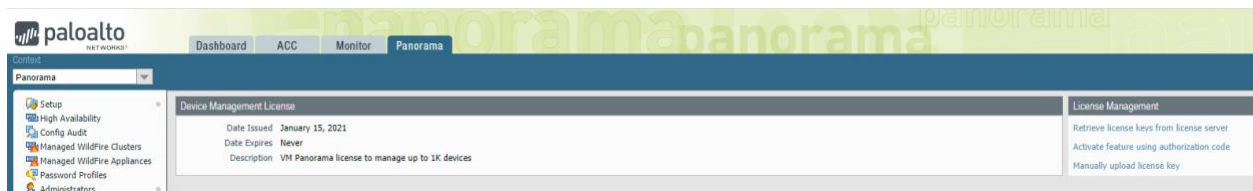


VM Name	Host	IP Addresses	Cores	Memory Capacity	Storage	CPU Usage	Memory Usage	Controller Read KPS	Controller Write KPS	Controller IO Bandwidth
AutoDC VM	PHX-POC085-2/AHV	10.42.85.51	4	8 GiB	343.83 MiB / 1 GiB	0.11%	3.65%	0	0	2 Kbps
Panorama	PHX-POC085-1/AHV	10.42.85.39	6	32 GiB	~ / 0.98 TiB	0%	0%	-	-	-
RXAutomationPC	PHX-POC085-1/AHV	10.42.85.39	6	26 GiB	10.83 GiB / 641.44 GiB	13.58%	44.24%	0	62	470 Kbps
Windows 10 VM			4	8 GiB	10.46 GiB / 40 GiB	0%	0%	-	-	-
Windows 2012 VM			4	8 GiB	9.64 GiB / 40 GiB	0%	0%	-	-	-

7. Login to Panorama with the factory default account of admin/admin. Panorama will force you to update the default password so proceed forward by changing the default password. You must also update the Panorama VM Management Interface settings so that the Web-UI can be accessed. Run the following commands to complete this step replacing network values with those of your environment.

```
> configure (enter configuration mode)
# set deviceconfig system ip-address 10.1.1.2 netmask 255.255.255.0 default-gateway
10.1.1.1 dns-setting servers primary 4.2.2.2
# commit
```

8. After the commit is complete, launch your browser and navigate to the newly assigned IPv4 address of the Panorama Virtual Appliance.
9. Verify that the Panorama Serial Number shows under **Panorama > Setup > Management > General Settings**. If the Serial Number is unknown, manually enter the Serial Number provided in the order fulfillment email.
10. Verify that the Panorama Virtual Appliance is able to pull a license under **Panorama > Licenses**. Click on **Retrieve license keys from license server** if appliance is not licensed.





## Prepare Panorama for Logging

After you Install Panorama on Nutanix AHV, add virtual logging disks to the Panorama virtual appliance instance to provide storage for logs generated by managed firewalls. You can add virtual disks to a local log Collector for a Panorama virtual appliance in Panorama mode or for a Dedicated Log Collector. The Panorama virtual appliance on AHV supports only 2TB logging disks and, in total, supports up to 24TB of log storage. You cannot add a logging disk smaller than 2TB or a logging disk of a size that is not evenly divisible by 2TB because the Panorama virtual appliance partitions logging disks in to 2TB partitions.

1. Log in to the Panorama CLI. Enter the following command to view the disks on the Panorama virtual appliance.

```
# show system disk details
```

2. Enter the following command and confirm the request.

```
# request system disk add sdb
```

3. Enter the following command to verify the status of the disk addition.

```
# show system disk details
```

```
admin@Panorama> show system disk details

Name    : sdb
State   : Present
Size    : 2048000 MB
Status  : Available
Reason  : Admin enabled
```

4. Log in to the Panorama web interface.

5. Create a Log Collector by navigating to **Panorama > Managed Collectors > Add**. On the **General** tab, add the S/N for Panorama. Select **Disks** and **Add** each newly added disk. Click **OK** and **Commit** changes.

Collector

General

Disks

Collector S/N

0007EV30347

Inbound Certificate for Secure Syslog

None

Warning: Only MGT interface is supported for all functions on collectors running PAN-OS 6.0 or earlier.

OK

Cancel

Collector

General

Disks

1 item

→

×

<input type="checkbox"/>	ENABLED DISKS
<input type="checkbox"/>	Disk A

+

 Add 

-

 Delete

OK

Cancel

The configuration status should now show **In Sync**.

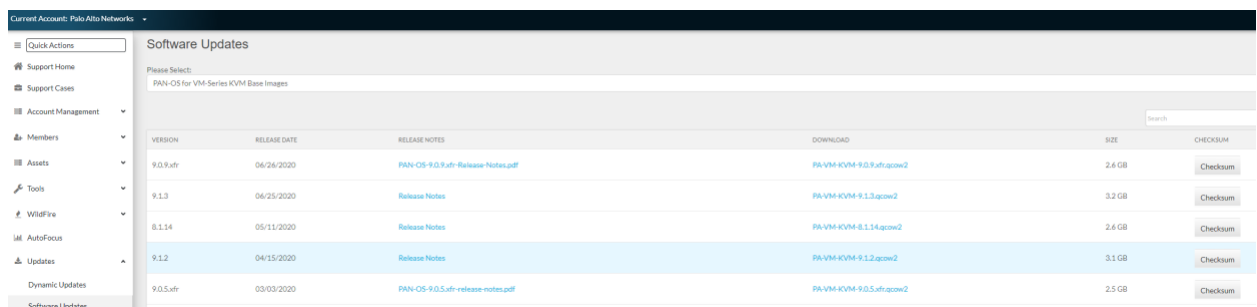
# Deploy VM SERIES

The VM-Series firewall for Nutanix AHV allows you to deploy the VM-Series firewall on AHV. The VM-Series firewall is distributed using the QCOW2 format, which is one of the disk image formats supported by Nutanix AHV. (Note: in this case a VM-Series 300 was used)

1. Download VM-Series qcow2 image from Palo Alto Networks support site.

URL: <https://support.paloaltonetworks.com/Support/Index>

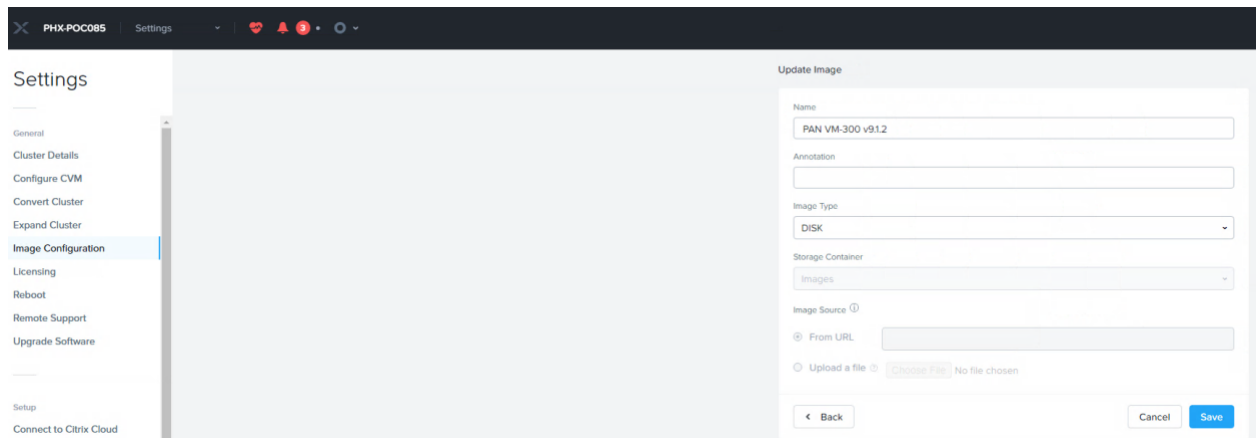
Filename: PA-VM-KVM-9.1.2.qcow2



The screenshot shows the 'Software Updates' page in the Palo Alto Networks management interface. A sidebar on the left contains navigation links: Quick Actions, Support Home, Support Cases, Account Management, Members, Assets, Tools, WildFire, AutoFocus, Updates, Dynamic Updates, and Software Updates. The main content area is titled 'Software Updates' and includes a search bar. Below the search bar is a table with columns: VERSION, RELEASE DATE, RELEASE NOTES, DOWNLOAD, SIZE, and CHECKSUM. The table lists several updates, with version 9.1.2 highlighted in blue.

VERSION	RELEASE DATE	RELEASE NOTES	DOWNLOAD	SIZE	CHECKSUM
9.0.8.vfr	06/26/2020	<a href="#">PAN-OS-9.0.8.vfr-Release-Notes.pdf</a>	<a href="#">PA-VM-KVM-9.0.8.vfr.qcow2</a>	2.6 GB	<a href="#">Checksum</a>
9.1.3	06/25/2020	<a href="#">Release Notes</a>	<a href="#">PA-VM-KVM-9.1.3.qcow2</a>	3.2 GB	<a href="#">Checksum</a>
8.1.14	05/11/2020	<a href="#">Release Notes</a>	<a href="#">PA-VM-KVM-8.1.14.qcow2</a>	2.6 GB	<a href="#">Checksum</a>
9.1.2	04/15/2020	<a href="#">Release Notes</a>	<a href="#">PA-VM-KVM-9.1.2.qcow2</a>	3.1 GB	<a href="#">Checksum</a>
9.0.5.vfr	03/03/2020	<a href="#">PAN-OS-9.0.5.vfr-release-notes.pdf</a>	<a href="#">PA-VM-KVM-9.0.5.vfr.qcow2</a>	2.5 GB	<a href="#">Checksum</a>

2. Create a Nutanix Image Configuration by going to **Settings > Image Configuration > Create Image**.



The screenshot shows the 'Settings' page in the Nutanix management interface. The left sidebar contains navigation links: General, Cluster Details, Configure CVM, Convert Cluster, Expand Cluster, Image Configuration (highlighted), Licensing, Reboot, Remote Support, Upgrade Software, Setup, and Connect to Citrix Cloud. The main content area is titled 'Update Image' and contains a form with the following fields: Name (PAN VM-300 v9.1.2), Annotation, Image Type (DISK), Storage Container (Images), Image Source (From URL), and Upload a file (Choose File). The form also includes 'Back', 'Cancel', and 'Save' buttons.

- Wait for Image State to become **Active**.

Name	Format	State	Size
bootstrap.iso	ISO	ACTIVE	15.59 MiB
PA-VM-KVM-9.1.6....	DISK	INACTIVE	-
PAN Panorama-V...	DISK	ACTIVE	81 GiB
PAN VM-300 v9.1.2	DISK	ACTIVE	60 GiB

- Navigate to the VM tab on Prism. Create a new VM by selecting the VM tab and clicking on the **Create VM** button.

Ref: <https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/set-up-the-vm-series-firewall-on-nutanix-ahv.html>

VM-Series Virtual Appliance Configurations	
Compute Details	
vCPU(s)	1
Number of Cores per vCPU	4
Memory	16
Boot Configuration	
Legacy BIOS	DISK (scsi.0)
Disks	

scsi.0	60GB (From Image)
Network Adapters (NIC)	
NIC 1 - VLAN ID	0 (Management VLAN)

Create VM ? x

General Configuration

Name

Nutanix-PaloAltoNetworks-FW

Description

VM-series firewalls 10.0.4 Release Testing

Timezone

(UTC) UTC

☐ Use this VM as an agent VM

Compute Details

vCPU(s)

1

Number Of Cores Per vCPU

Cancel

Save

Create VM ? x

Compute Details

vCPU(s)

1

Number Of Cores Per vCPU

4

Memory ?

16

GiB

Boot Configuration

☒ Legacy BIOS

Set Boot Priority

DISK (scsi.0)

Only the selected disk will be used for boot. (No fallback to other disks)

☐ UEFI ?

Cancel

Save

Prism Central - Virtual infrastructure - VM - Create VM (1)

Add Disk

Type

DISK

Operation

Clone from Image Service

Bus Type

SCSI

Image

PA-VM-KVM-10.0.4.qcow2

Size (GiB)

60

Please note that changing the size of an image is not allowed.

Index

Next Available

Cancel

Add

Create VM

Disks

+ Add New Disk

Type	Address	Parameters	
DISK	scsi.0	SIZE=60GiB; BUS=scsi	✎ ✕

Network Adapters (NIC)

+ Add New NIC

VLAN ID / VPC	VIRTUAL SWITCH	PRIVATE IP	MAC	
0	vs0	-	-	✎ ✕
NR_PRO				
D_DHCP				

VM Host Affinity

You haven't pinned the VM to any hosts yet.

Cancel

Save

### Prism Central - Virtual infrastructure - VM - Create VM (2)

- Repeat step 21 until you have exactly 1 VM-Series firewall deployed for every Nutanix AHV Host in the environment. Additional NICs for each VM will be provisioned later.
- Prior to turning on each VM-Series firewall, attach a serial port to each VM to prevent the bootloader process from hanging. Login to any CVM host via SSH and perform the following command.
 

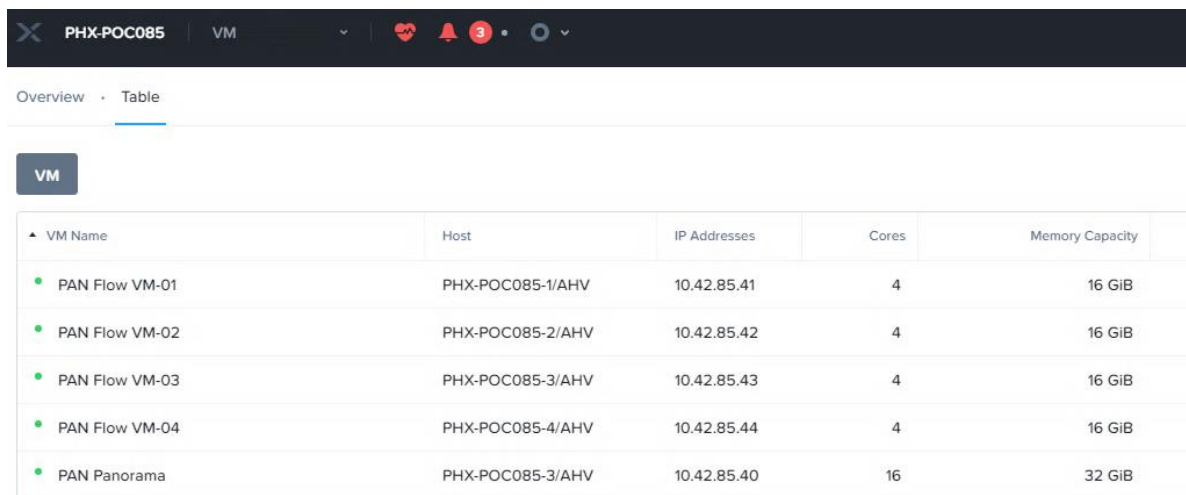
```
acli vm.serial_port_create "VM Name" type=kServer index=0
```
- On the Prism Element Web-UI, navigate to each of the VM-Series Firewall and click **Power On**. After a few seconds, the Launch Console button will appear. Click on **Launch Console** to access the VM-Series Firewall CLI.

8. Login to each VM-Series Firewall with the factory default account of admin/admin. PAN-OS will force you to update the default password so proceed forward by changing the default password. You must also update the VM Management Interface settings so that the Web-UI can be accessed. Run the following commands to complete this step replacing network values with those of your environment.

```
> configure (enter configuration mode)
# set deviceconfig system ip-address 10.1.1.3 netmask 255.255.255.0 default-gateway
10.1.1.1 dns-setting servers primary 4.2.2.2
# commit
```

**Note:** The time to login to the VM-Series firewalls UI can take a few minutes to load after the initial deployment.

9. After the commit is complete, verify the IPv4 configs on the **Prism > VM > Table** screen. Launch your browser and navigate to the newly assigned IPv4 address of the Panorama Virtual Appliance.



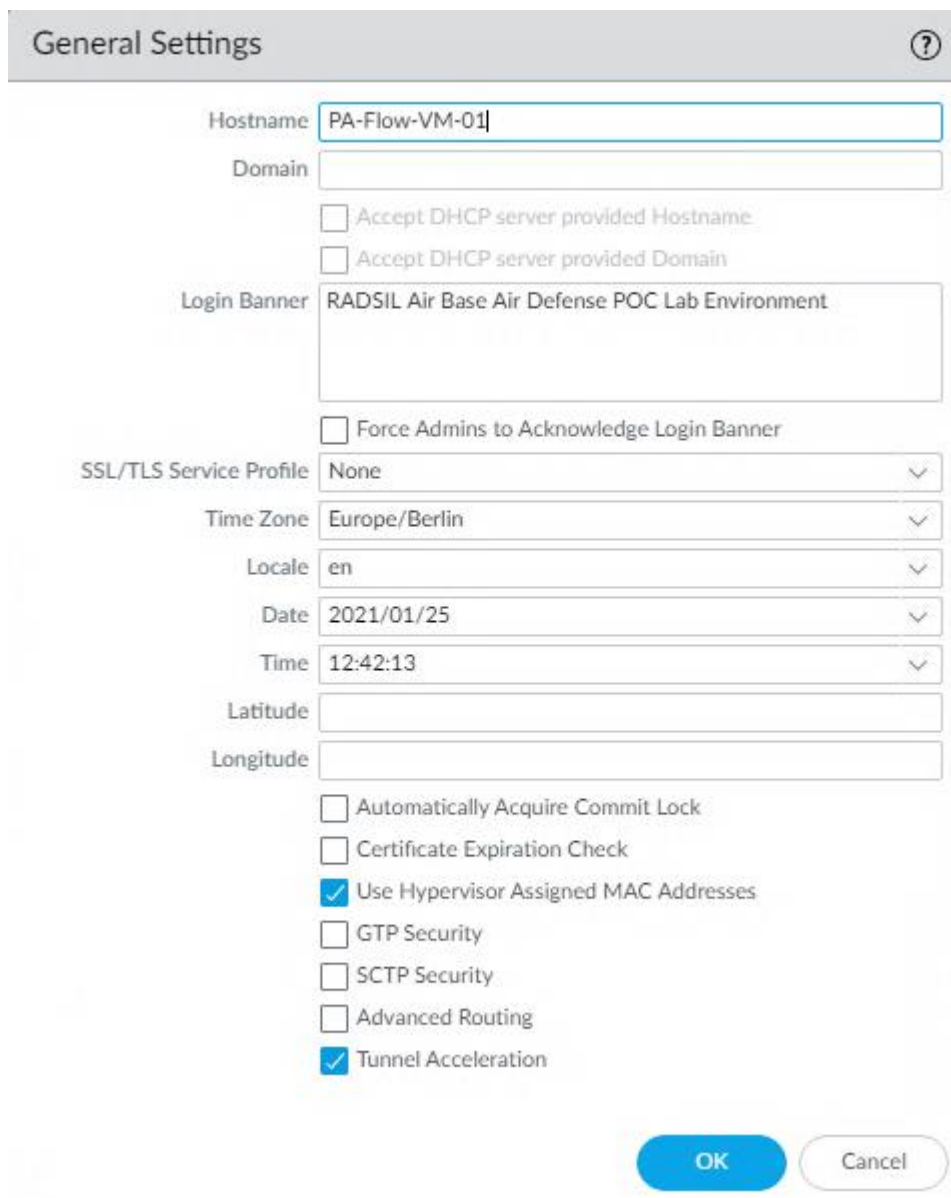
The screenshot shows the Palo Alto Networks VM-Series management interface. At the top, there is a navigation bar with the text "PHX-POC085" and "VM". Below this, there are tabs for "Overview" and "Table", with "Table" being the active tab. A "VM" button is visible on the left. The main content area displays a table with the following columns: VM Name, Host, IP Addresses, Cores, and Memory Capacity. The table lists five VMs: PAN Flow VM-01, PAN Flow VM-02, PAN Flow VM-03, PAN Flow VM-04, and PAN Panorama. Each VM has a green status indicator, a host name, an IP address, 4 cores, and 16 GiB of memory capacity, except for PAN Panorama which has 16 cores and 32 GiB of memory capacity.

VM Name	Host	IP Addresses	Cores	Memory Capacity
PAN Flow VM-01	PHX-POC085-1/AHV	10.42.85.41	4	16 GiB
PAN Flow VM-02	PHX-POC085-2/AHV	10.42.85.42	4	16 GiB
PAN Flow VM-03	PHX-POC085-3/AHV	10.42.85.43	4	16 GiB
PAN Flow VM-04	PHX-POC085-4/AHV	10.42.85.44	4	16 GiB
PAN Panorama	PHX-POC085-3/AHV	10.42.85.40	16	32 GiB

## Initial Configuration for VM-Series

Each VM-Series Firewall will be setup to have Panorama push a majority of network, object, and policy configurations. However, there are a few items to cover on each VM-Series firewall individually prior to managing each VM under Panorama.

1. On the VM-Series Web-UI, navigate to **Device > Setup > Management**. Configure the device **Hostname** and **Time Zone** under **General Settings**.



The screenshot shows the 'General Settings' configuration page. The 'Hostname' field is set to 'PA-Flow-VM-01'. The 'Domain' field is empty. There are two unchecked checkboxes: 'Accept DHCP server provided Hostname' and 'Accept DHCP server provided Domain'. The 'Login Banner' field contains the text 'RADSIL Air Base Air Defense POC Lab Environment'. There is an unchecked checkbox for 'Force Admins to Acknowledge Login Banner'. The 'SSL/TLS Service Profile' is set to 'None'. The 'Time Zone' is set to 'Europe/Berlin'. The 'Locale' is set to 'en'. The 'Date' is set to '2021/01/25'. The 'Time' is set to '12:42:13'. The 'Latitude' and 'Longitude' fields are empty. There are several unchecked checkboxes: 'Automatically Acquire Commit Lock', 'Certificate Expiration Check', 'GTP Security', 'SCTP Security', and 'Advanced Routing'. There are two checked checkboxes: 'Use Hypervisor Assigned MAC Addresses' and 'Tunnel Acceleration'. At the bottom right, there are 'OK' and 'Cancel' buttons.

Field	Value
Hostname	PA-Flow-VM-01
Domain	
Accept DHCP server provided Hostname	<input type="checkbox"/>
Accept DHCP server provided Domain	<input type="checkbox"/>
Login Banner	RADSIL Air Base Air Defense POC Lab Environment
Force Admins to Acknowledge Login Banner	<input type="checkbox"/>
SSL/TLS Service Profile	None
Time Zone	Europe/Berlin
Locale	en
Date	2021/01/25
Time	12:42:13
Latitude	
Longitude	
Automatically Acquire Commit Lock	<input type="checkbox"/>
Certificate Expiration Check	<input type="checkbox"/>
Use Hypervisor Assigned MAC Addresses	<input checked="" type="checkbox"/>
GTP Security	<input type="checkbox"/>
SCTP Security	<input type="checkbox"/>
Advanced Routing	<input type="checkbox"/>
Tunnel Acceleration	<input checked="" type="checkbox"/>



- On the **Device > Setup > Management** tab, configure the Panorama Settings to include the IPv4 Address of the Panorama Server. Ensure Panorama **Policy and Objects** and Panorama **Device and Networks** Templates are enabled.

The screenshot shows the 'Panorama Settings' window. At the top, there's a header 'Panorama Settings' with a help icon. Below it, the 'Panorama Servers' section has a text input field containing '10.42.85.40'. To the right of this field is a checkbox labeled 'Enable pushing device monitoring data to Panorama', which is checked. Below this, there are three input fields: 'Receive Timeout for Connection to Panorama (sec)' with value '240', 'Send Timeout for Connection to Panorama (sec)' with value '240', and 'Retry Count for SSL Send to Panorama' with value '25'. Further down, there's another checkbox labeled 'Enable automated commit recovery', which is also checked. Below this checkbox are two more input fields: 'Number of attempts to check for Panorama connectivity' with value '1', and 'Interval between retries (sec)' with value '10'. At the bottom of the window, there are four buttons: 'Disable Panorama Policy and Objects', 'Disable Device and Network Template', 'OK', and 'Cancel'.

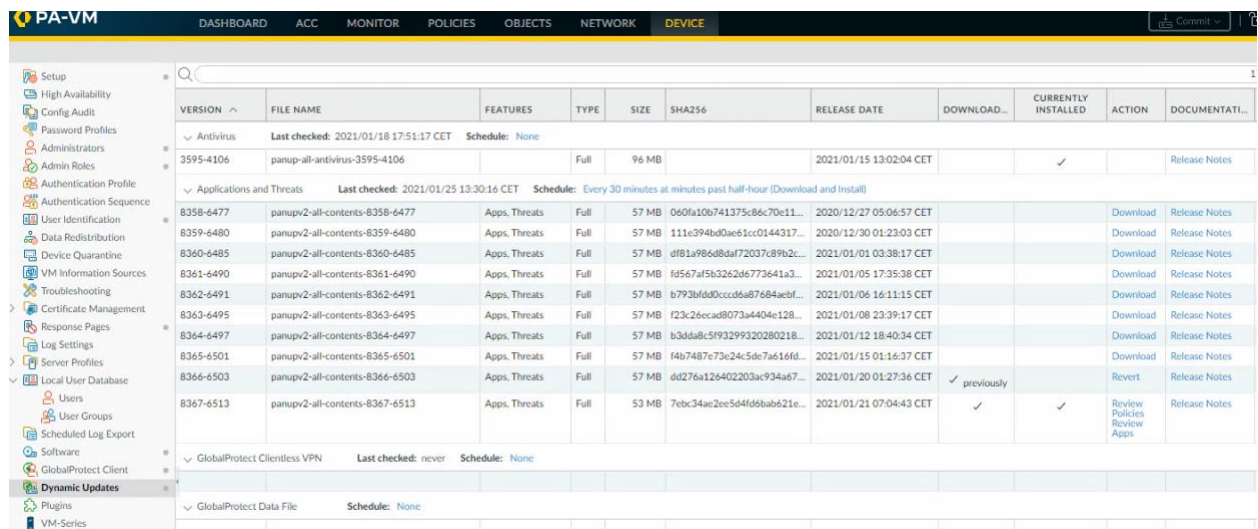
- On the **Device > Setup > Services** tab, configure the primary and secondary **DNS** and **NTP** server settings.

The screenshot shows the 'Services' configuration window. On the left, there's a sidebar with a tree view under 'Setup'. The 'Services' tab is selected in the top navigation bar. The main content area is titled 'Services' and contains several settings. Under 'Update Server', the value is 'updates.paloaltonetworks.com'. Below that, 'Verify Update Server Identity' is checked. Under 'DNS Servers', the 'Primary DNS Server' is '10.42.194.10' and the 'Secondary DNS Server' is empty. Below that, 'Minimum FQDN Refresh Time (sec)' is '30' and 'FQDN Stale Entry Timeout (min)' is '1440'. Under 'Proxy Server', the 'Primary NTP Server Address' is '0.pool.ntp.org', 'Primary NTP Server Authentication Type' is 'None', 'Secondary NTP Server Address' is '1.pool.ntp.org', and 'Secondary NTP Server Authentication Type' is 'None'. At the bottom, there's a section titled 'Services Features' with a link to 'Service Route Configuration'.

- On the **Device > Licenses** tab, verify that all licenses have pulled down successfully. If not, click on **Retrieve license keys from license server**. This will prompt a reboot of the Virtual Appliance. Upon reboot, check the License tab again.



- On the **Device > Dynamic Updates** tab, click on **Check Now**. You should now see multiple dynamic update packages to install. **Download** and **install** the latest Applications and Threats package.



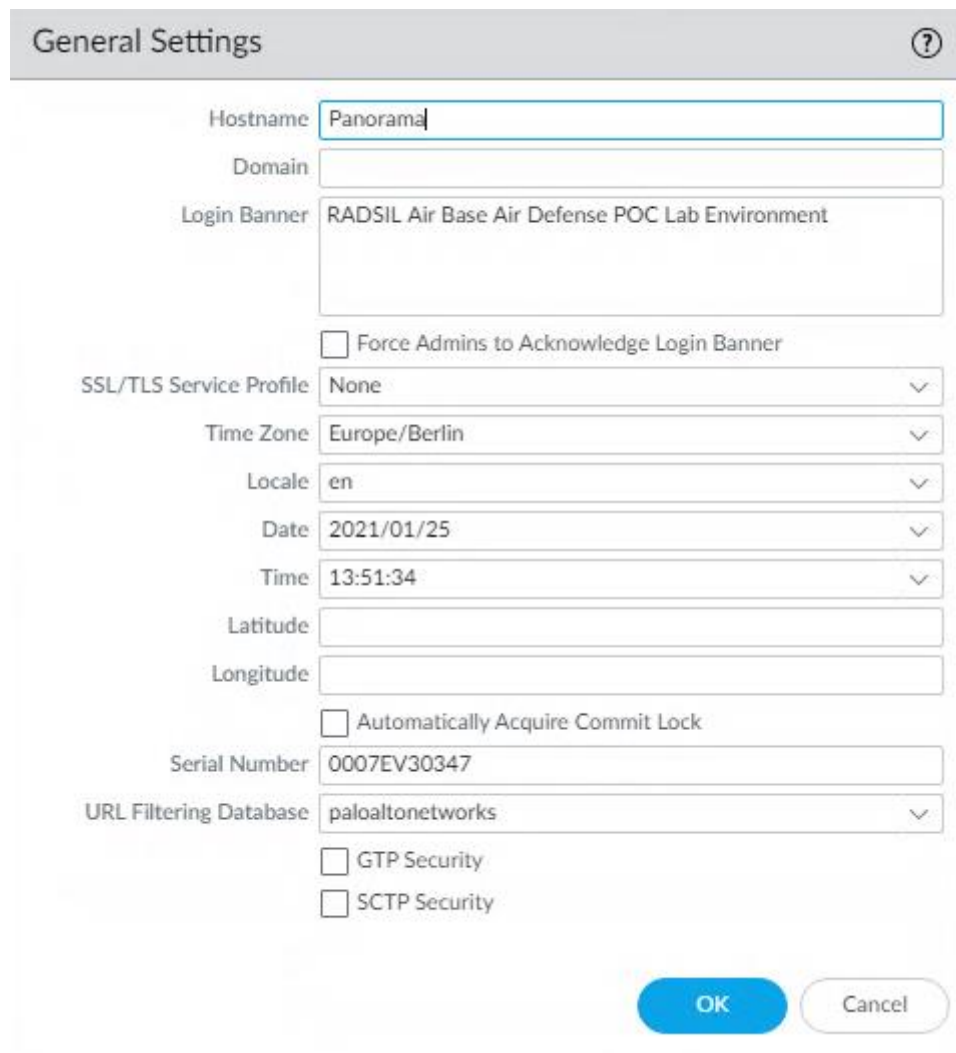
- RECOMMENDED** – On the **Device > Software** tab, click on **Check Now**. You should now see multiple software versions available for download and installation. Upgrade your VM to the latest version release.

- Repeat** steps 27-31 on each VM-Series firewall.

## Panorama Configuration

Now that each VM-Series firewall is up and running, the next steps outline the initial configuration of Panorama and how-to setup templates and device groups for central management of each VM-Series.

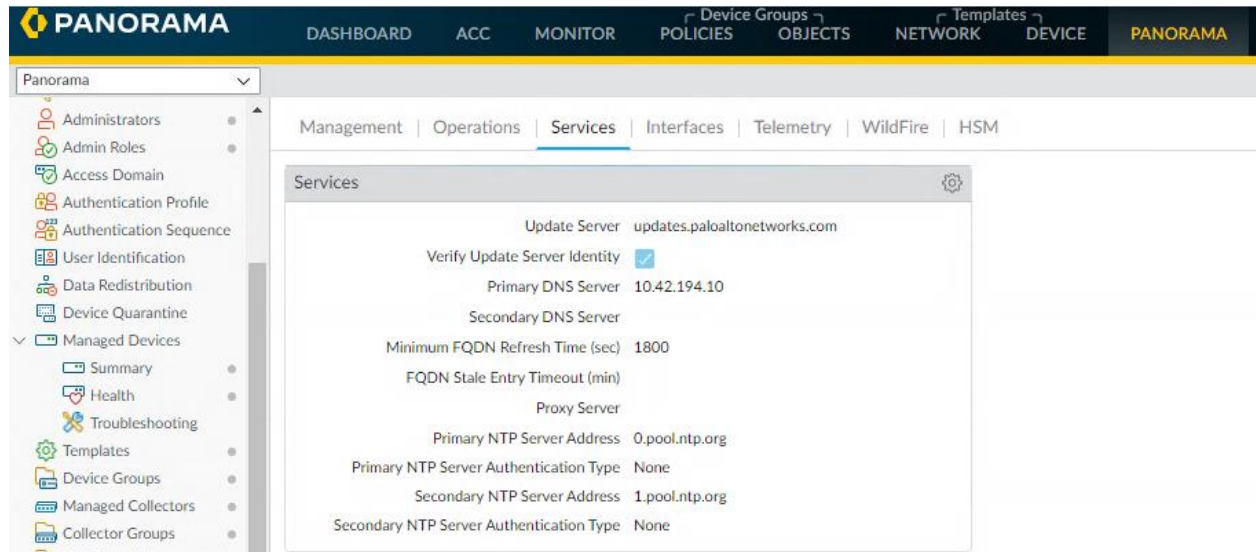
1. On the Panorama Web-UI, navigate to **Panorama > Setup > Management**. Configure the device **Hostname** and **Time Zone** under **General Settings**.



The screenshot shows the 'General Settings' configuration page in the Panorama Web-UI. The page has a grey header with the title 'General Settings' and a help icon. The settings are organized into a form with various input fields, dropdown menus, and checkboxes. The 'Hostname' field is highlighted with a blue border and contains the text 'Panorama'. The 'Domain' field is empty. The 'Login Banner' field contains the text 'RADSIL Air Base Air Defense POC Lab Environment'. There is a checkbox for 'Force Admins to Acknowledge Login Banner' which is unchecked. The 'SSL/TLS Service Profile' dropdown is set to 'None'. The 'Time Zone' dropdown is set to 'Europe/Berlin'. The 'Locale' dropdown is set to 'en'. The 'Date' dropdown is set to '2021/01/25'. The 'Time' dropdown is set to '13:51:34'. The 'Latitude' and 'Longitude' fields are empty. There is a checkbox for 'Automatically Acquire Commit Lock' which is unchecked. The 'Serial Number' field contains the text '0007EV30347'. The 'URL Filtering Database' dropdown is set to 'paloaltonetworks'. There are two checkboxes at the bottom: 'GTP Security' and 'SCTP Security', both of which are unchecked. At the bottom right of the form are two buttons: 'OK' (blue) and 'Cancel' (grey).

Field	Value
Hostname	Panorama
Domain	
Login Banner	RADSIL Air Base Air Defense POC Lab Environment
Force Admins to Acknowledge Login Banner	<input type="checkbox"/>
SSL/TLS Service Profile	None
Time Zone	Europe/Berlin
Locale	en
Date	2021/01/25
Time	13:51:34
Latitude	
Longitude	
Automatically Acquire Commit Lock	<input type="checkbox"/>
Serial Number	0007EV30347
URL Filtering Database	paloaltonetworks
GTP Security	<input type="checkbox"/>
SCTP Security	<input type="checkbox"/>

2. On the **Panorama > Setup > Services** tab, configure the primary and secondary **DNS** and **NTP** server settings.



3. On the **Panorama > Licenses** tab, verify that all licenses have pulled down successfully. If not, click on **Retrieve license keys from license server**. This will prompt a reboot of the Virtual Appliance. Upon reboot, check the License tab again.



- On the **Panorama > Dynamic Updates** tab, click on **Check Now**. You should now see multiple dynamic update packages to install. **Download** and **install** the latest Applications and Threats package.

PANORAMA

DASHBOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICEPANORAMA

Panorama

Setup

High Availability

Config Audit

Managed WildFire Clusters

Managed WildFire Appliances

Password Profiles

Administrators

Admin Roles

Access Domain

Authentication Profile

Authentication Sequence

User Identification

Data Redistribution

Device Quarantine

Managed Devices

Templates

Device Groups

Managed Collectors

Collector Groups

Certificate Management

Log Ingestion Profile

Log Settings

Server Profiles

Scheduled Config Export

Software

Dynamic Updates

Plugins

Nutanix

Setup

Monitoring Definition

Licenses

Support

VERSION

FILE NAME

FEATURES

TYPE

SIZE

SHA256

RELEASE DATE

DOWNLOAD...

CURRENTLY INSTALLED

ACTION

Antivirus

Last checked: 2021/01/25 13:03:11 CET

Schedule: Every hour (Download and Install)

3596-4107

panup-all-antivirus-3596-4107

Full

97 MB

972a58afb7...

2021/01/16 13:00:02 CET

Download

3597-4108

panup-all-antivirus-3597-4108

Full

97 MB

57b1daaab...

2021/01/17 13:00:02 CET

Download

3598-4109

panup-all-antivirus-3598-4109

Full

97 MB

5e8729fd63...

2021/01/18 13:00:03 CET

Download

3599-4110

panup-all-antivirus-3599-4110

Full

97 MB

99621464f9...

2021/01/19 13:03:02 CET

Download

3600-4111

panup-all-antivirus-3600-4111

Full

98 MB

c986193d1a...

2021/01/20 13:00:03 CET

Download

3601-4112

panup-all-antivirus-3601-4112

Full

98 MB

0b981de04...

2021/01/21 13:03:03 CET

✓

Install

3602-4113

panup-all-antivirus-3602-4113

Full

98 MB

ec7465eba4...

2021/01/22 13:03:03 CET

✓

Install

3603-4114

panup-all-antivirus-3603-4114

Full

98 MB

856ebc3b3b...

2021/01/23 13:02:02 CET

✓

Install

3604-4115

panup-all-antivirus-3604-4115

Full

98 MB

8c4d5823bf...

2021/01/24 13:00:04 CET

✓ previously

Revert

3605-4116

panup-all-antivirus-3605-4116

Full

97 MB

77be56b3c3...

2021/01/25 13:00:03 CET

✓

✓

Applications and Threats

Last checked: 2021/01/25 13:30:24 CET

Schedule: Every 30 minutes at minutes past half-hour (Download and Install)

8358-6477

panupv2-all-apps-8358-6477

Apps

Full

49 MB

f1e4d6ebb4...

2020/12/27 05:06:36 CET

Download

8359-6480

panupv2-all-apps-8359-6480

Apps

Full

49 MB

ecbc3a9363...

2020/12/30 01:22:42 CET

Download

8360-6485

panupv2-all-apps-8360-6485

Apps

Full

49 MB

db3ef380f3...

2021/01/01 03:38:40 CET

Download

8361-6490

panupv2-all-apps-8361-6490

Apps

Full

49 MB

d87b617f7f...

2021/01/05 17:35:59 CET

Download

8362-6491

panupv2-all-apps-8362-6491

Apps

Full

49 MB

c1783c4716...

2021/01/06 16:11:33 CET

Download

8363-6495

panupv2-all-apps-8363-6495

Apps

Full

49 MB

9c1c0f691a...

2021/01/08 23:38:55 CET

Download

8364-6497

panupv2-all-apps-8364-6497

Apps

Full

49 MB

e8cb7892d4...

2021/01/12 18:40:14 CET

Download

8365-6501

panupv2-all-apps-8365-6501

Apps

Full

49 MB

dc3f22988...

2021/01/15 01:16:59 CET

✓

Install

8366-6503

panupv2-all-apps-8366-6503

Apps

Full

49 MB

2869bada72...

2021/01/20 01:28:02 CET

✓ previously

Revert

8367-6513

panupv2-all-apps-8367-6513

Apps

Full

44 MB

f2b023d86c...

2021/01/21 07:05:02 CET

✓

✓

Review Policies Review Apps

- RECOMMENDED** – In order for Panorama to successfully manage devices, it must at a minimum match the same PAN-OS version as what is installed on other VM-Series devices. On the **Device > Software** tab, click on **Check Now**. You should now see multiple software versions available for download and installation. Upgrade your VM to the latest version release.

- On the **Panorama > Managed Devices > Summary** tab, click **Add** and enter the Serial Number of each VM-Series firewall. Click **OK**.

Add Device

Serial

007254000155104  
007254000155105  
007254000155106  
007254000155107

Please enter one or more device serial numbers. Enter one entry per row, separating the rows with a newline.

☒ Associate Devices

Import

OK

Cancel

- Give Panorama a few moments to connect to each VM-Series firewall and pull them in.  
You will see **Connected** under the **Device State** column once finished.

PANORAMA

DASHBOARD

ACC

MONITOR

POLICIES

OBJECTS

NETWORK

DEVICES

PANORAMA

Panorama

Setup

High Availability

Config Audit

Managed WildFire Clusters

Managed WildFire Appliances

Password Profiles

Administrators

Admin Roles

Access Domain

Authentication Profile

Authentication Sequence

User Identification

Data Redistribution

Device Quarantine



8. On the **Panorama > Device Groups** tab, click **Add** to create a new Device Group. Name the group and add each VM-Series firewall. Click **OK**.

Device Group

Name

NTNX-DeviceGroup

Description

REFERENCE TEMPLATES

+ Add

- Delete

Devices

FILTERS

Device State

Connected (5)

Platforms

PA-VM (5)

Templates

NTNX-Stack (4)

Tags

NAME

☒ PA-Flow-VM-01

☒ PA-Flow-VM-02

☒ PA-Flow-VM-03

☒ PA-Flow-VM-04

☐ PA-VM-300

Select All

Deselect All

☐ Group HA Peers

☐ Filter Selected (4)

5 items

→

×

Parent Device Group

Shared

Master Device

None

The master device is the firewall from which Panorama gathers user ID information for use in policies.

OK

Cancel

9. On the **Panorama > Templates** tab, click **Add** to create a Template. Click **OK**.

Template

Name

NTNX-Template

Default VSYS

vsys1

Description

The default virtual system template configuration is pushed to firewalls with a single virtual system.

OK

Cancel

10. On the **Panorama > Templates** tab, click **Add Stack** to create a Template Stack. Add the previously created **Template** and all **Devices** under the previously created Device Group and click **OK**.

Template Stack

Name

NTNX-Stack

Default VSYS

vsys1

The default virtual system template configuration is pushed to firewalls with a single virtual system.

Description

☐ TEMPLATES

☐ NTNX-Template

+ Add

- Delete

↑ Move Up

↓ Move Down

The Template at the top of the Stack has the highest priority in the presence of overlapping config

Devices

FILTERS

✓ ☐ Platforms

☐ PA-VM (5)

✓ ☐ Device Groups

☐ NTNX-DeviceGroup (4)

☐ Tags

☐ HA Status

Q

5 items

→

×

☒ PA-Flow-VM-01

☒ PA-Flow-VM-02

☒ PA-Flow-VM-03

☒ PA-Flow-VM-04

☐ PA-VM-300

Select All

Deselect All

☐ Group HA Peers

☐ Filter Selected (4)

OK

Cancel



11. On the **Panorama > Collector Groups** tab, click **Add** to create a new Log Collector Group.

On the **General** tab, name the group and click **Add** under the Collectors section and select **Panorama Server** from the drop down. On the Device Log Forwarding tab, click **Add** and select each VM-Series firewall as a device and Panorama as a collector. Click **OK** and **OK**.

The image shows two screenshots of the Panorama web interface for configuring a Log Collector Group.

**Top Screenshot: General Tab**

- Collector Group** (Title bar)
- General** | Monitoring | Device Log Forwarding | Collector Log Forwarding | Log Ingestion (Tabs)
- Name:** Panorama Log Collector Group
- Log Storage:** Total: 1.53 TB, Free: 75.30 GB
- Min Retention Period (days):** [1 - 2000]
- Collector Group Members:** 1 item → ×
  - ☒ **COLLECTORS** ^
  - ☒ Panorama(0007EV30347)
- Buttons:** + Add - Delete
- Options:**
  - ☐ Enable log redundancy across collectors
  - ☐ Forward to all collectors in the preference list
  - ☐ Enable secure inter LC Communication
- Footer:** Log collector on local panorama is using the secure client configuration from 'Panorama -> Secure Communication Settings'
- Buttons:** OK Cancel

**Bottom Screenshot: Device Log Forwarding Tab**

- Collector Group** (Title bar)
- General** | Monitoring | **Device Log Forwarding** | Collector Log Forwarding | Log Ingestion (Tabs)
- Log Forwarding Preferences:** 1 item → ×

DEVICES	COLLECTORS
<input checked="" type="checkbox"/> PA-Flow-VM-02 PA-Flow-VM-03 PA-Flow-VM-04 PA-VM-300 PA-Flow-VM-01	Panorama
- Buttons:** + Add - Delete
- Buttons:** OK Cancel

12. **Commit to Panorama** to save your progress.

13. On the **Device > Log Settings** tab, ensure that the previously created **Template** is selected at the top of the screen. Add log settings for each of the rows on this tab and ensure to check to box for **Panorama**. Click **OK**.

PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE** PANORAMA

Panorama Template: NTNX-Template View by: Device Mode: Single VSYS: Normal Mode; VPN Enabled

System

NAME	DESCRIPTION	FILTER	PANORAMA/CORTEX DATA LAKE
<input checked="" type="checkbox"/> System Logs		All Logs	<input checked="" type="checkbox"/>

+ Add - Delete Clone PDF/CSV

Configuration

NAME	DESCRIPTION	FILTER	PANORAMA/CORTEX DATA LAKE
<input checked="" type="checkbox"/> Configuration Logs		All Logs	<input checked="" type="checkbox"/>

+ Add - Delete Clone PDF/CSV

14. On the **Network > Interfaces** tab, click **Add Interface** and add ethernet 1/1 and ethernet 1/2 as a Virtual Wire. Click **OK**.

PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS **NETWORK** DEVICE PANORAMA

Panorama Template: NTNX-Template View by: Device Mode: Single VSYS: Normal Mode; VPN Enabled

Interfaces Ethernet VLAN Loopback Tunnel SD-WAN

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE
Slot 1							
ethernet1/1	Virtual Wire		none	none	Untagged	NTNX-Flow-Vwire	NTNX-Flow-Zone
ethernet1/2	Virtual Wire		none	none	Untagged	NTNX-Flow-Vwire	NTNX-Flow-Zone

15. On the **Network > Zones** tab, click **Add** to create a new zone. Add both interfaces that you just created. Click **OK**.

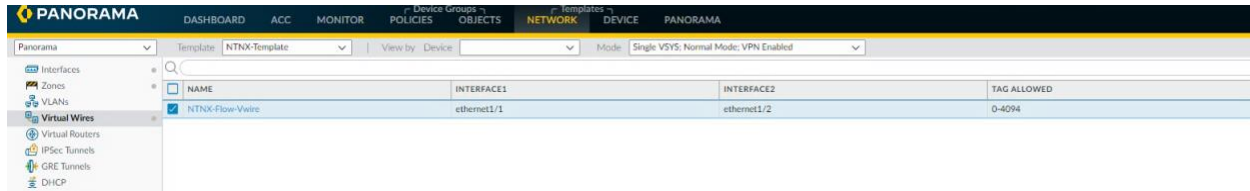
PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS **NETWORK** DEVICE PANORAMA

Panorama Template: NTNX-Template View by: Device Mode: Single VSYS: Normal Mode; VPN Enabled

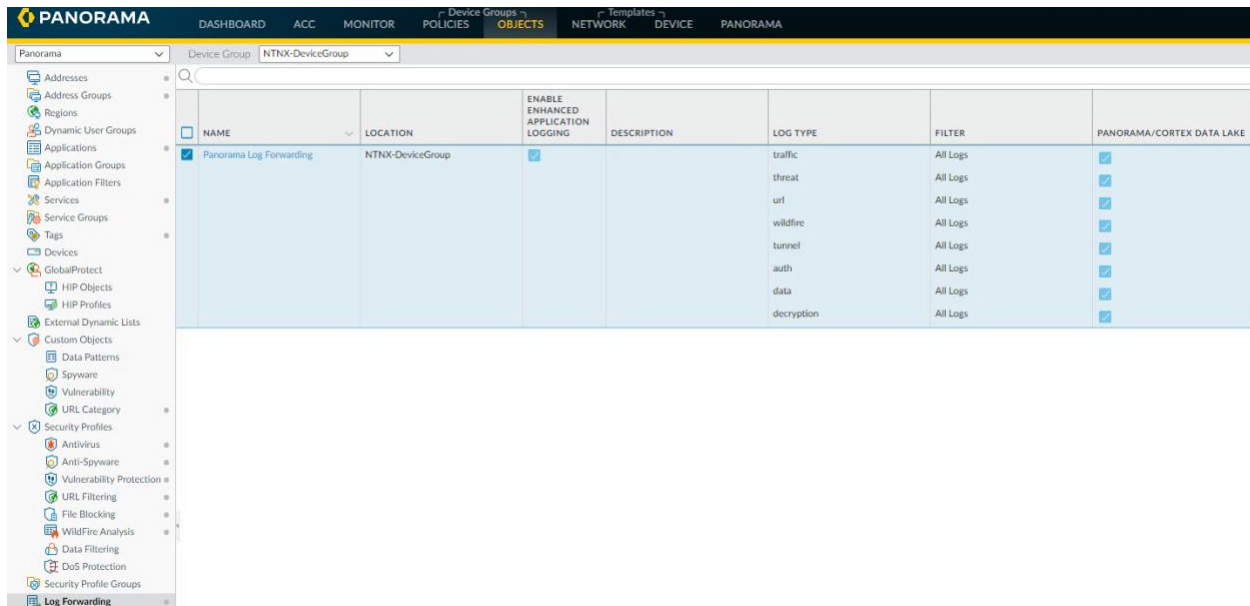
Zones

NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION
<input checked="" type="checkbox"/> NTNX-Flow-Zone	virtual-wire	ethernet1/1 ethernet1/2		<input checked="" type="checkbox"/>

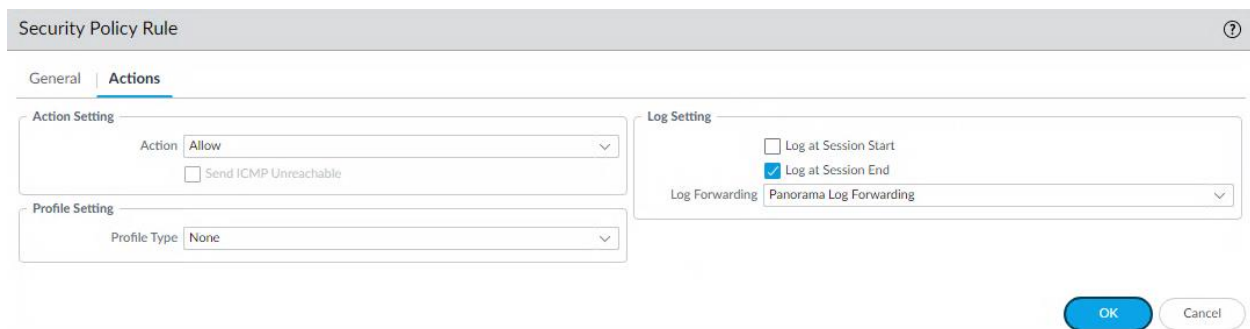
16. On the **Network > Virtual Wires** tab, click **Add** to create a new virtual wire. Select ethernet 1/1 and ethernet 1/2 and set **Tag Allowed** to **0-4094**. Check the boxes for both **Link State Pass Through** and **Multicast Firewalling**. Click **OK**.



17. On the **Objects > Log Forwarding** tab, click **Add** to create a new log forwarding profile. Name the profile and Add in each log type to send to **Panorama**. Click **OK**.



18. On the **Policies > Security > Default Rules** tab, modify the **intrazone-default** rule to log to **Panorama**. Click **OK**.



19. On the upper right corner of the Panorama Web-UI, select **Commit > Commit and Push**.  
Verify the **Commit** and **Push Scopes**. Click **Commit and Push**.

Commit and Push

Doing a commit will overwrite the Panorama running configuration with the commit scope.

Commit All Changes

Commit Changes Made By:1 admin

COMMIT SCOPE	LOCATION TYPE
NTNX-DeviceGroup	Device Groups
NTNX-Template	Templates

Preview Changes

Change Summary

Validate Commit

Group By Location Type

PUSH SCOPE	LOCATION TYPE ^	ENTITIES
NTNX-DeviceGroup	Device Groups	PA-Flow-VM-03, PA-Flow-VM-04, PA-Flow-VM-02, PA-Flow-VM-01
NTNX-Stack	Templates	PA-Flow-VM-03, PA-Flow-VM-04, PA-Flow-VM-02, PA-Flow-VM-01

Edit Selections

Remove Selections

Validate Device Group Push

Validate Template Push

Group By Location Type

Note: By default, devices that are associated with the entities in the commit scope are selected, however you may customize the selection.

Enter a description

Commit And Push

Cancel

20. Navigate to the **Task Manager** and verify the last Commit All succeeded.

Task Manager - All Tasks (Panorama)

145

TYPE	STATUS	START TIME	MESSAGES	ACTION
Download	Completed	01/25/21 14:53:05	File successfully downloaded	
Commit All	Completed	01/25/21 14:53:02	commit to template NTNX-Stack	
Commit All	Completed	01/25/21 14:53:02	commit to device group	
Commit and Push				

Download

Download

Download

Download

Download

Download

Download

Download

Show All Tasks

Job Status - commit to template NTNX-Stack

4 items

FILTERS

Status

Commit Succeeded (4)

Platforms

PA-VM (4)

Device Groups

NTNX-DeviceGroup (4)

Templates

NTNX-Stack (4)

Tags

HA Status

DEVICE NAME	STATUS	HA STATUS
PA-Flow-VM-02	commit succeeded	
PA-Flow-VM-03	commit succeeded	
PA-Flow-VM-04	commit succeeded	
PA-Flow-VM-01	commit succeeded	

Summary

Progress 100%

Result Succeeded 4

Result Pending 0

Result Failed 0

Details

This operation may take several minutes to complete

21. On the **Panorama > Managed Devices > Summary** tab, the **Shared Policy** and **Templates** columns should now show a status of **In Sync**.

PANORAMA

DASHBOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICEPANORAMA

Panorama

SetupHigh AvailabilityConfig AuditManaged WildFire ClustersManaged WildFire AppliancesPassword ProfilesAdministratorsAdmin RolesAccess DomainAuthentication ProfileAuthentication SequenceUser IdentificationData RedistributionDevice Quarantine

NTNX-DeviceGroup (4/4 Devices Connected): Shared > NTNX-DeviceGroup

PA-Flow-VM-03

PA-VM

007254000155...

10.42.85.43

Create

NTNX-Stack

Connected

None

N/A

In Sync

In Sync

PA-Flow-VM-04

PA-VM

007254000155...

10.42.85.44

Create

NTNX-Stack

Connected

None

N/A

In Sync

In Sync

PA-Flow-VM-02

PA-VM

007254000155...

10.42.85.42

Create

NTNX-Stack

Connected

None

N/A

In Sync

In Sync

PA-Flow-VM-01

PA-VM

007254000155...

10.42.85.41

Create

NTNX-Stack

Connected

None

N/A

In Sync

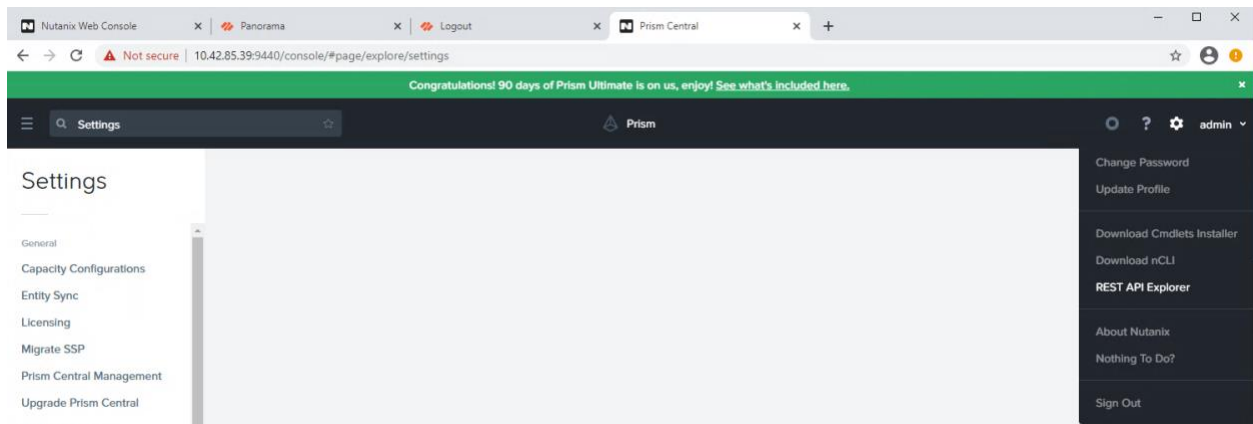
In Sync

22. The VM-Series firewalls are now ready to accept and log traffic once the service chain is configured.

# NUTANIX Service Chain Configuration

Service Chain configuration must be created using REST API in current AOS and can be done from the Prism Central Web-UI leveraging the built-in API explorer tool. Service chains are used to direct traffic of each VM to a configured Network Function Chain that points to the Palo Alto Networks VM-Series firewalls. There is a blueprint available on the Nutanix marketplace that automates this process; however, these steps are outlined here to guide the manual creation of both the network service and the network service chain.

1. Open a new web browser tab and navigate to the Prism Central Web-UI API explorer by going to [https://Prism\\_Central\\_IP:9440](https://Prism_Central_IP:9440) and login. On the right, select the drop down from the login name and select **REST API Explorer**.



- ```
{
  "kind": "cluster"
}
```

[Try it out!](#) [Hide Response](#)

3. Scroll through the Response Body and find the **uuid** for the cluster. Write this down or copy the string to a text file for later reference when building the service chain.

Response Body

```
{
  "external_subnet": "10.42.85.0/255.255.255.128",
  "external_data_services_ip": "10.42.85.38",
  "name_server_ip_list": [
    "10.42.194.10"
  ],
  "internal_subnet": "192.168.5.0/255.255.255.128"
},
{
  "metadata": {
    "last_update_time": "2021-01-16T02:13:13Z",
    "kind": "cluster",
    "uuid": "0005b8f0-6855-b10d-0000-00000000280d",
    "spec_version": 2,
    "creation_time": "2021-01-16T02:13:13Z",
    "categories_mapping": {},
    "categories": {}
  },
  {
    "status": {
      "state": "COMPLETE",
      "name": "Unnamed",
    }
  }
}
```

4. Scroll through the Response Body and find the **name** for the cluster. Write this down or copy the string to a text file for later reference when building the service chain.

Response Body

```
{
  "spec": {
    "name": "PHX-POC085",
    "resources": {
      "config": {
        "software_map": {
          "NCC": {
            "status": "INSTALLED",
            "version": "ncc-4.0.0.1",
            "software_type": "NCC"
          }
        }
      }
    }
  }
}
```



5. Create a category in Prism Central for the Network Function with the key ***network\_function\_provider*** value. The value of this key will act as labels on the Network Function VMs that identifies them as the instances of the Network Function on each host. This name ***network\_function\_provider*** must never be changed. On the Prism Central homepage, navigate to ***Virtual Infrastructure > Categories***. Click on the New Category button at the top and fill in the ***Name, Purpose*** and ***Values*** field showcased below. Click ***Save***.

### Create Category

#### General

Name ?

Purpose ?

Values ?



Cancel

Save

6. Create a Network Function Chain in the Cluster using the Cluster Name and UUID from steps 57 and 58 and the network\_function\_provider value from step 59. On the Prism Central *REST API Explorer*, select *network\_function\_chains* > *POST*. Under the *get\_entities\_request* parameters, type the following code and click *Try it out*. Make sure to double and triple check the values in red for accuracy!

```
{
  "spec": {
    "name": "PANOS_CHAIN",
    "resources": {
      "network_function_list": [
        {
          "network_function_type": "INLINE",
          "category_filter": {
            "type": "CATEGORIES_MATCH_ALL",
            "params": {"network_function_provider": ["PaloAlto"]}
          }
        }
      ]
    },
    "cluster_reference": {
      "kind": "cluster",
      "name": "PHX-POC085",
      "uuid": "0005b8f0-6855-b10d-0000-00000000280d"
    }
  },
  "api_version": "3.1.0",
  "metadata": {
    "kind": "network_function_chain"
  }
}
```

POST /network\_function\_chains

Create a new Network Function Chain

### Implementation Notes

Given an Intentful spec, creates a network function chain with associated metadata.

### Response Class (Status 202)

[Model](#) [Model Schema](#)

```
{
  "status": {
    "description": "string",
    "state": "string",
    "message_list": [
      {
        "message": "string",
        "reason": "string",
        "details": {}
      }
    ]
  }
}
```

### Response Content Type

application/json

### Parameters

| Parameter | Value                                                                                                                                            | Description | Parameter Type | Data Type                                                                                                                                                                                                                                                                                                                                                                          |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------|-------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| body      | <pre>"spec": {   "name": "PANOS_CHAIN",   "resources": {     "network_function_list": [       {         "network_function_type": "INLINE",</pre> |             | body           | <a href="#">Model</a> <a href="#">Model Schema</a> <pre>{   "spec": {     "name": "string",     "description": "string",     "resources": {       "network_function_list": [         {           "network_function_type": "string",           "category_filter": {             "kind_list": [               "string"             ]           }         ]       ]     }   } }</pre> |

Parameter content type:

application/json

[Click to set as parameter value](#)

### Response Messages

| HTTP Status Code | Reason         | Response Model                                                                                                                                                                                                                                       | Headers |
|------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| default          | Internal Error | <a href="#">Model</a> <a href="#">Model Schema</a> <pre>{   "kind": "network_function_chain",   "code": 0,   "message_list": [     {       "message": "string",       "reason": "string",       "details": {}     }   ]   "state": "string", }</pre> |         |

Try it out!

7. Verify that the chain is created by selected ***network\_function\_chains/list*** > ***POST***. Under the ***get\_entities\_request*** parameters, type the following and click ***Try it out***.

```
{  
  "kind": "network_function_chain"  
}
```

Response Body

```
{  
  "entities": [  
    {  
      "status": {  
        "state": "COMPLETE",  
        "name": "PANOS_CHAIN",  
        "resources": {  
          "network_function_list": [  
            {  
              "network_function_type": "INLINE",  
              "category_filter": {  
                "type": "CATEGORIES_MATCH_ALL",  
                "params": {  
                  "network_function_provider": [  
                    "PaloAlto"  
                  ]  
                }  
              }  
            }  
          ]  
        }  
      }  
    }  
  ],  
  "execution_context": {  
    "task_uuids": [  
      "6dc31354-6c77-4eec-a0bc-96ee72ab22d7"  
    ]  
  }  
}
```

8. While on the ***network\_function\_chains/list*** page, record the Network Function Chain UUID from the Response Body for reference later.

Response Body

```
{  
  }  
}  
}  
},  
"name": "PANOS_CHAIN",  
},  
"metadata": {  
  "last_update_time": "2021-01-18T16:10:27Z",  
  "kind": "network_function_chain",  
  "uuid": "d96be965-a42f-4acc-be53-d344c69ff6d1",  
  "spec_version": 0,  
  "creation_time": "2021-01-18T16:10:26Z",  
  "categories_mapping": {},  
  "owner_reference": {  
    "kind": "user",  
    "uuid": "fa5c3932-9155-55d9-b84f-e9e5b657f383",  
    "name": "nutanixadmin@diablo.ntnx"  
  },  
  "categories": []  
}  
}  
}  
}
```

9. Create Ingress and Egress virtual NICs on each VM-Series firewall and assign each VM as a Nutanix Agent VM. Power off each VM-Series firewall prior to running the CLI commands below. SSH to a CVM and run the following commands. Run these commands in order and repeat this step for each VM-Series firewall deployed. Ensure to change the IPv4 address on the final command each time to set different affinity values to each VM-Series firewall.

```
accli vm.update "VM-01" agent_vm=true extra_flags=is_system_vm=true
accli vm.nic_create "VM-01" type=kNetworkFunctionNic network_function_nic_type=kIngress
accli vm.nic_create "VM-01" type=kNetworkFunctionNic network_function_nic_type=kEgress
accli vm.affinity_set "VM-01" host_list=x.x.x.x
```

10. On the Prism Central Web-UI, assign each VM-Series firewall to the ***network\_function\_provider:PaloAlto*** category. Navigate to ***Virtual Infrastructure > VMs***. Select each VM-Series VM and select ***Actions > Manage Categories***. In the Search for a category, look for ***network\_function\_provider*** and select the category and then click ***Save***.

☰

VMs

VM Type=User VM

List

☆

VMs

13 Filtered VMs out of 17

1 Filter(s) Applied

Summary

List

Alerts

Events

Metrics

Create VM

⚙️

Actions

🔖

1 selected out of 13 filtered VMs

☐

Name

☐

Domain Controller

☐

Domain Controller

☒

PAN Flow VM-01

☐

PAN Flow VM-02

☐

PAN Flow VM-03

☐

PAN Flow VM-04

☐

PAN Panorama

☐

PAN VM-300

☐

Prism Central

☐

Windows 10 VM-01

☐

Windows 10 VM-02

☐

Windows 10 VM-03

Update

Delete

Clone

Launch console

Hard Power Off

Soft Shutdown

Disable Efficiency Measurement

Disable Anomaly Detection

Protect

Unprotect

Create Recovery Point

Migrate

Add to Recovery Plan

Run Playbook

Manage Categories

Manage VM Categories

Set Categories

You have selected **PAN Flow VM-01**.  
Selected categories will be applied to the VM.

network\_function\_provider: P... ⊖

Search for a category 🔍 ⊕

Possible Associated Policies

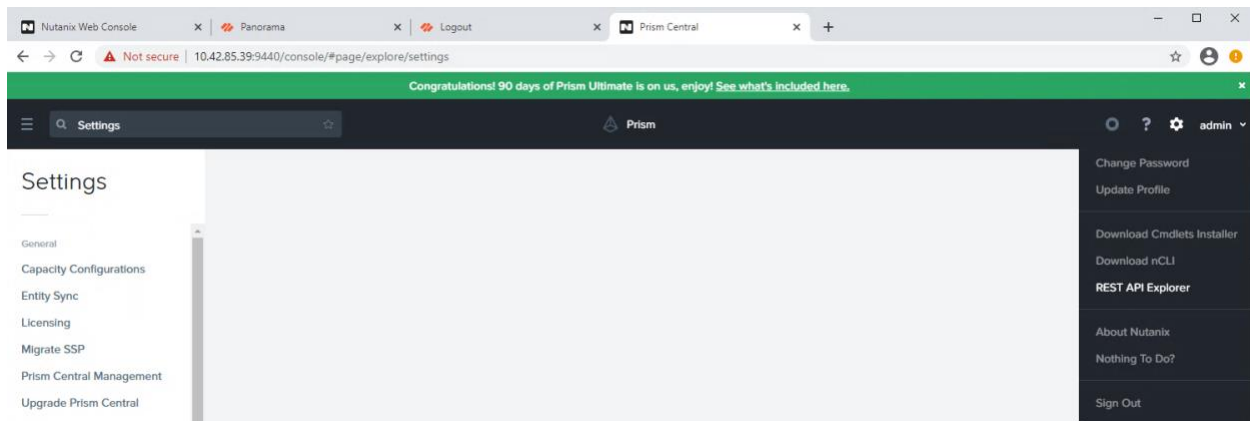
For all categories associated with a policy, please go to the policy page.

| POLICY TYPE   | POLICY NAME | APPLIES BECAUSE OF                     |
|---------------|-------------|----------------------------------------|
| Service Chain | PANOS_CHAIN | network_function_provider;<br>PaloAlto |

## Direct Traffic to Network Function Chain

Now that the network function VMs are added to a network function chain, there are a number of ways to direct traffic to the chain. This preferred method directs specific application, VM or infrastructure flows from the AHV network through the chain by attaching the network function chain to each subnet through Prism Central REST API Explorer. This method does require Prism Central but does not require a Flow license or microsegmentation; however, the same results are achieved.

1. Open a new web browser tab and navigate to the Prism Central Web-UI API explorer by going to [https://Prism\\_Central\\_IP:9440](https://Prism_Central_IP:9440) and login. On the right, select the drop down from the login name and select **REST API Explorer**.



2. Navigate to **Subnets/list** and click on **POST**. Under the **get\_entities\_request** parameters, type the following and click **Try it out**.

```
{  
  "kind": "subnet"  
}
```

POST

/subnets/list

Get a list of existing subnets

**Implementation Notes**  
This operation gets a list of subnets, allowing for sorting and pagination. Note: Entities that have not been created successfully are not listed.

Response Class (Status 200)

[Model](#) [Model Schema](#)

```
{
  "entities": [
    {
      "status": {
        "name": "string",
        "state": "string",
        "availability_zone_reference": {
          "kind": "availability_zone",
          "name": "string",
          "uuid": "string"
        }
      }
    }
  ]
}
```

Response Content Type

application/json

Parameters

| Parameter            | Value                                                                                         | Description | Parameter Type | Data Type                                                                                                                                                                                                                                                                          |
|----------------------|-----------------------------------------------------------------------------------------------|-------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| get_entities_request | <div>{<br/>  "kind": "subnet"<br/>}</div> <div>Parameter content type: application/json</div> |             | body           | <div><a href="#">Model</a> <a href="#">Model Schema</a></div> <div>{<br/>  "kind": "subnet",<br/>  "sort_attribute": "string",<br/>  "filter": "string",<br/>  "length": 0,<br/>  "sort_order": "string",<br/>  "offset": 0<br/>}</div> <div>Click to set as parameter value</div> |

Response Messages

| HTTP Status Code | Reason         | Response Model                                                                                                                                                                                                                                                                               | Headers |
|------------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| default          | Internal Error | <div><a href="#">Model</a> <a href="#">Model Schema</a></div> <div>{<br/>  "kind": "subnet",<br/>  "code": 0,<br/>  "message_list": [<br/>    {<br/>      "message": "string",<br/>      "reason": "string",<br/>      "details": []<br/>    }<br/>  ],<br/>  "state": "string",<br/>}</div> |         |

Try it out!

[Hide Response](#)



3. Scroll through the Response Body and find the **uuid** for the subnet. Write this down or copy the string to a text file for later reference when redirecting traffic to the network function chain.

Response Body

```
{
  "vswitch_name": "vbr",
  "subnet_type": "VLAN",
  "virtual_switch_uuid": "e83f18e8-9a4b-4174-8fbb-6b9bdd99ed6e",
  "vlan_id": 0,
  "network_function_chain_reference": {
    "kind": "network_function_chain",
    "uuid": "d96be965-a42f-4acc-be53-d344c69ff6d1"
  },
  "name": "Rx-Automation-Network"
},
{
  "metadata": {
    "last_update_time": "2021-01-18T18:04:31Z",
    "kind": "subnet",
    "uuid": "3cf73816-4916-41b8-b4da-a86fe1d578b9",
    "spec_version": 3,
    "creation_time": "2021-01-16T17:08:15Z",
    "categories_mapping": {},
    "owner_reference": {
      "kind": "user",
      "uuid": "fa5c3932-9155-55d9-b84f-e9e5b657f383",
      "name": "nutanixadmin@diablo.ntnx"
    },
    "categories": {}
  }
}
```

4. Get the subnet details using the subnet UUID. Navigate to **Subnet/{uuid}** and click on **GET**. Paste the **subnet UUID** in the **Parameters section** and click **Try it out**.

GET

/subnets/{uuid}

Get a existing subnet

**Implementation Notes**  
 This operation gets a existing subnet.

**Response Class (Status 200)**  
[Model](#) [Model Schema](#)

```

{
  "status": {
    "name": "string",
    "state": "string",
    "availability_zone_reference": {
      "kind": "availability_zone",
      "name": "string",
      "uuid": "string"
    },
  },
  "message_list": [
    {

```

**Response Content Type**

application/json

**Parameters**

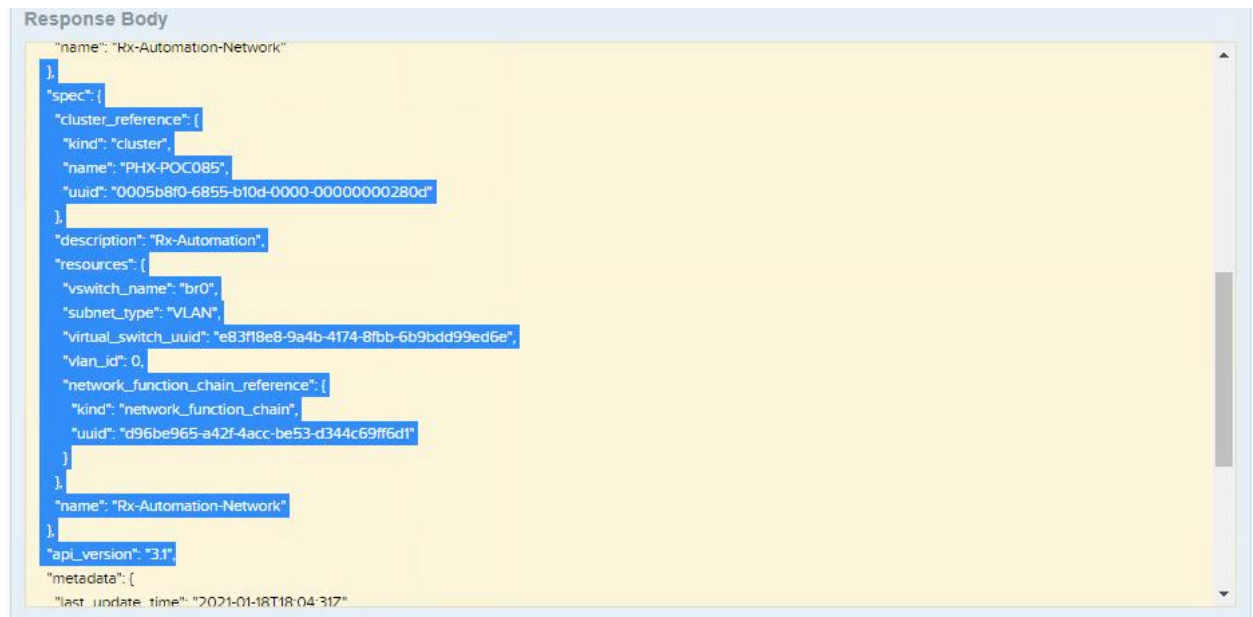
| Parameter | Value                                | Description             | Parameter Type | Data Type |
|-----------|--------------------------------------|-------------------------|----------------|-----------|
| uuid      | 3cf73816-4916-41b8-b4da-a86fe1d578b9 | The UUID of the entity. | path           | string    |

**Response Messages**

| HTTP Status Code | Reason                | Response Model                                                                                                                                                                                                                        | Headers |
|------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| 404              | Invalid UUID provided | <a href="#">Model</a> <a href="#">Model Schema</a> <pre> {   "kind": "subnet",   "code": 0,   "message_list": [     {       "message": "string",       "reason": "string",       "details": []     }   ],   "state": "string", </pre> |         |
| default          | Internal Error        | <a href="#">Model</a> <a href="#">Model Schema</a> <pre> {   "kind": "subnet",   "code": 0,   "message_list": [     {       "message": "string",       "reason": "string",       "details": []     }   ],   "state": "string", </pre> |         |

Try it out!

- Copy the response starting at spec for use in the next step. Copied contents should be as follows.



6. Modify the code as follows and copy it for the next step.

**NOTE:** This is sample code only!

```
{
  "spec": {
    "name": "2381",
    "resources": {
      "vswitch_name": "br0",
      "network_function_chain_reference": {
        "kind": "network_function_chain",
        "uuid": "d96be965-a42f-4acc-be53-d344c69ff6d1"
      },
      "subnet_type": "VLAN",
      "ip_config": {
        "default_gateway_ip": "10.21.238.129",
        "dhcp_server_address": {
          "ip": "10.21.238.254"
        }
      },
      "pool_list": [
        {
          "range": "10.21.238.170 10.21.238.200"
        }
      ],
      "prefix_length": 25,
      "subnet_ip": "10.21.238.128",
      "dhcp_options": {
```

```
        "domain_name_server_list": [
            "10.21.253.10",
            "10.20.0.10"
        ]
    },
    "vlan_id": 2381
},
"cluster_reference": {
    "kind": "cluster",
    "name": "SPECIALTY03",
    "uuid": "000553bb-3957-e293-0000-00000000165dc"
}
},
"api_version": "3.1",
"metadata": {
    "last_update_time": "2018-11-06T14:49:28Z",
    "kind": "subnet",
    "uuid": "6fbb6a17-a068-47c0-8e15-236b5ef15a8b",
    "creation_time": "2018-11-06T14:10:16Z",
    "spec_version": 3,
    "owner_reference": {
        "kind": "user",
        "uuid": "335db0ad-6b3f-5b61-9098-bc63c9132305",
        "name": "username"
    },
    "categories": {}
}
}
```

7. Navigate to **Subnet/{uuid}** and click on **PUT**. Paste the **subnet UUID** in the **Parameters** section. In the **body**, paste the modified code from step 70 and click **Try it out**.

PUT

/subnets/{uuid}

Update a existing subnet

**Implementation Notes**  
This operation submits a request to update a existing subnet based on the input parameters.

**Response Class (Status 202)**  
[Model](#) [Model Schema](#)

```
{
  "status": {
    "name": "string",
    "state": "string",
    "availability_zone_reference": {
      "kind": "availability_zone",
      "name": "string",
      "uuid": "string"
    },
    "message_list": [
      {

```

Response Content Type

application/json

**Parameters**

| Parameter | Value                                | Description             | Parameter Type | Data Type |
|-----------|--------------------------------------|-------------------------|----------------|-----------|
| uuid      | 3cf73816-4916-41b8-b4da-a86fe1d578b9 | The UUID of the entity. | path           | string    |

**body**

```
},
"spec": {
  "cluster_reference": {
    "kind": "cluster",
    "name": "PHX-POC085",
    "uuid": "0005b8f0-6855-b10d-0000-00000000280d"
  }
}
```

Parameter content type: application/json

**body**

[Model](#) [Model Schema](#)

```
{
  "spec": {
    "name": "string",
    "availability_zone_reference": {
      "kind": "availability_zone",
      "name": "string",
      "uuid": "string"
    },
    "description": "string",
    "resources": {
      "subnet_type": "string",

```

Click to set as parameter value

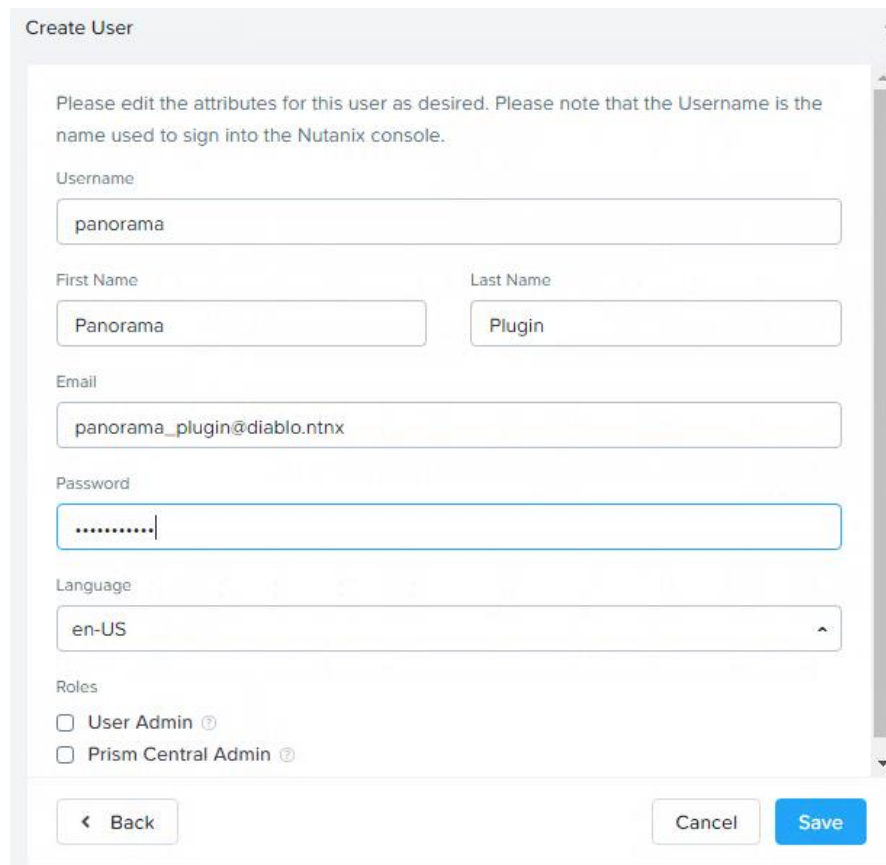
8. Check to ensure each VM-Series firewall is now receiving traffic. Login to Panorama Web-UI and navigate to **Monitor > Logs > Traffic**. Ensure that all VM-Series firewalls are reporting logs to Panorama correctly.

| PANORAMA                     |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
|------------------------------|--|--------------------------------------------------------|---------------|-------------------|----------------|----------------|-------------|----------------|------------------------------|-------------|-----------------------------------|---------|-------------|--------|--------------------------|
| DASHBOARD                    |  | ACC                                                    | MONITOR       | Device Groups (1) |                | Templates (1)  |             | POLICIES       |                              | OBJECTS     | NETWORK                           | DEVICE  | PANORAMA    |        |                          |
| Panorama                     |  | Device Group                                           |               | All               |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Logs                         |  | / device in 10.42.85.40 and / add src in 10.42.85.0/24 |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Traffic                      |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Threat                       |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| URL Filtering                |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Wildfire Submissions         |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Data Filtering               |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| HIP Match                    |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| GlobalProtect                |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| IP-Tag                       |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| User-ID                      |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Decryption                   |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Tunnel Inspection            |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Configuration                |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| System                       |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Authentication               |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Unified                      |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| External Logs                |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Traps ESX                    |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Threat                       |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| System                       |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Policy                       |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Config                       |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Agent                        |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Automated Correlation Engine |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
| Predefined Policies          |  |                                                        |               |                   |                |                |             |                |                              |             |                                   |         |             |        |                          |
|                              |  | GENERATE TIME                                          | DEVICE NAME   | TYPE              | FROM ZONE      | TO ZONE        | SOURCE      | SOURCE USER    | SOURCE DYNAMIC ADDRESS GROUP | DESTINATION | DESTINATION DYNAMIC ADDRESS GROUP | TO PORT | APPLICATION | ACTION | RULE                     |
|                              |  | 01/25 17:34:21                                         | PA-Flow-VM-03 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.42 | diablogpan_svc |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:34:20                                         | PA-Flow-VM-02 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.42 | diablogpan_svc |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:34:20                                         | PA-Flow-VM-04 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.44 | diablogpan_svc |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:34:20                                         | PA-Flow-VM-03 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.44 | diablogpan_svc |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:34:19                                         | PA-Flow-VM-03 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.41 | diablogpan_svc |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:34:18                                         | PA-Flow-VM-03 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.43 | diablogpan_svc |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:34:18                                         | PA-Flow-VM-03 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.45 |                |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:34:18                                         | PA-Flow-VM-01 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.41 | diablogpan_svc |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:34:17                                         | PA-Flow-VM-04 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.45 |                |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:33:16                                         | PA-Flow-VM-03 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.42 | diablogpan_svc |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:33:15                                         | PA-Flow-VM-04 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.44 | diablogpan_svc |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:33:15                                         | PA-Flow-VM-02 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.42 | diablogpan_svc |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:33:15                                         | PA-Flow-VM-03 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.44 | diablogpan_svc |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:33:14                                         | PA-Flow-VM-03 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.41 | diablogpan_svc |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |
|                              |  | 01/25 17:33:13                                         | PA-Flow-VM-01 | end               | NTN0-Flow-Zone | NTN0-Flow-Zone | 10.42.85.41 | diablogpan_svc |                              | 10.42.85.40 |                                   | 3978    | incomplete  | allow  | PAN - Panorama - Inbound |

## Configure Dynamic Address Groups

The Panorama plugin for Nutanix facilitates the use of dynamic address groups by monitoring virtual machines in your Nutanix environment. Prism Central groups entities in your Nutanix environments by categories, made up by a key value pair. Panorama creates tags based on categories in Prism Central. When a virtual machine is placed in a category Panorama applies the corresponding tag to the virtual machine's IP address. You can then create a security policy by using the categories from Nutanix (tags within Panorama) as match criteria for dynamic address groups in Panorama.

1. On the Prism Central Web-UI, navigate to **Prism Central Settings > Local User Management**. Click on **New User**. Fill in all required fields and click **Save**.



Create User

Please edit the attributes for this user as desired. Please note that the Username is the name used to sign into the Nutanix console.

Username  
panorama

First Name  
Panorama

Last Name  
Plugin

Email  
panorama\_plugin@diablo.ntnx

Password  
.....

Language  
en-US

Roles

☐ User Admin ⓘ

☐ Prism Central Admin ⓘ

< Back Cancel Save

- On the **Virtual Infrastructure > Categories** tab, click **New Category** and fill in the fields. Click **Save**. You may create as many categories as you want to leverage as dynamic address groups on Panorama.

Create Category

---

**General**

Name ?

ClientVM

Purpose ?

Client Virtual Machines Group

Values ?

ABAD\_clientVM +

Cancel Save

- On the **Virtual Infrastructure > VMs** tab, check the box next to the VMs you want to apply a category to and select **Actions > Manage Categories**. Find the category you want to apply to the VM and click **Save**.

Manage VM Categories

---

**Set Categories**

You have selected **Windows 10 VM-03**.  
Selected categories will be applied to the VM.

Client Q +

**ClientVM: ABAD**

**Possible Associated Policies**

For all categories associated with a policy, please go to the policy page.

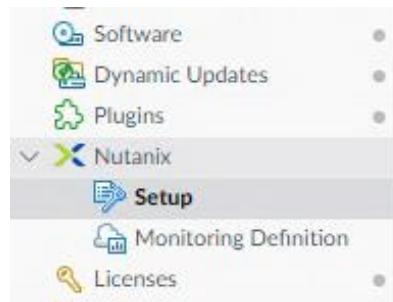
Select one or more categories, and a summary of their current usage will be displayed here.



- On the Panorama Web-UI, navigate to **Panorama > Plugins**. Click on **Check Now** and locate the **Nutanix-1.0.0** plugin. **Download** the file and select **Install** from the Actions column.

| FILE NAME                           | VERSION | RELEASE DATE        | SIZE | DOWNLOADED | CURRENTLY INSTALLED | ACTIONS                  |
|-------------------------------------|---------|---------------------|------|------------|---------------------|--------------------------|
| Name: ips_signature_converter-1.0.0 |         |                     |      |            |                     |                          |
| ips_signature_converter-1.0.0       | 1.0.0   | 2020/07/21 16:40:58 | 3M   |            |                     | Download                 |
| Name: kubernetes-1.0.0              |         |                     |      |            |                     |                          |
| kubernetes-1.0.0                    | 1.0.0   | 2020/07/17 12:03:06 | 4M   |            |                     | Download                 |
| Name: kubernetes-1.0.1              |         |                     |      |            |                     |                          |
| kubernetes-1.0.1                    | 1.0.1   | 2020/11/05 15:43:48 | 4M   |            |                     | Download                 |
| Name: nutanix                       |         |                     |      |            |                     |                          |
| nutanix-1.0.0                       | 1.0.0   | 2019/12/02 10:03:31 | 41M  | ✓          | ✓                   | Remove Config  Uninstall |
| Name: sd_wan-1.0.0                  |         |                     |      |            |                     |                          |
| sd_wan-1.0.0                        | 1.0.0   | 2019/12/16 14:52:32 | 858K |            |                     | Download                 |
| Name: sd_wan-1.0.1                  |         |                     |      |            |                     |                          |
| sd_wan-1.0.1                        | 1.0.1   | 2020/02/20 09:39:21 | 876K |            |                     | Download                 |
| Name: sd_wan-1.0.2                  |         |                     |      |            |                     |                          |
| sd_wan-1.0.2                        | 1.0.2   | 2020/04/27 09:51:47 | 974K |            |                     | Download                 |
| Name: sd_wan-1.0.3                  |         |                     |      |            |                     |                          |
| sd_wan-1.0.3                        | 1.0.3   | 2020/06/24 17:16:18 | 987K |            |                     | Download                 |
| Name: sd_wan-1.0.4                  |         |                     |      |            |                     |                          |
| sd_wan-1.0.4                        | 1.0.4   | 2020/08/06 10:27:41 | 994K |            |                     | Download                 |

- A **Nutanix** tab will now show under the Panorama tab. Select **Setup**.



- On the Nutanix Plugin **General** tab, check the box for **Enable Monitoring**.

General | Notify Groups | Nutanix Prism Central

General

Enable Monitoring ☒

Monitoring Interval (sec) 60

7. On the Nutanix Plugin **Notify Groups** tab, click **Add** and add the existing Device Group. Click **OK**.

General | **Notify Groups** | Nutanix Prism Central

Notify Group

1 item → ×

| <input type="checkbox"/>            | NAME             | DEVICE GROUP     |
|-------------------------------------|------------------|------------------|
| <input checked="" type="checkbox"/> | NTNS-DeviceGroup | NTNX-DeviceGroup |

+ Add - Delete

8. On the Nutanix Plugin **Nutanix Prism Central** tab, click **Add** and enter the **Prism Central IP/Port** and **Username/Password** information from step 73. Click **Validate** to ensure the service account with Prism Central works. Click **OK**.

PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE **PANORAMA**

Panorama

General | **Notify Groups** | Nutanix Prism Central

Nutanix Prism Central Info

1 item → ×

| <input type="checkbox"/>            | NAME          | PRISM CENTRAL IPS | USERNAME | DESCRIPTION |
|-------------------------------------|---------------|-------------------|----------|-------------|
| <input checked="" type="checkbox"/> | Prism_Central | 10.42.85.39:9440  | panorama |             |

+ Add - Delete

Nutanix Prism Central Info

Name: Prism\_Central

Description:

Prism Central IP/FQDN:PORT: 10.42.85.39:9440

Username: panorama

Password: .....

Confirm Password: .....

Validate OK Cancel

9. **Commit and Push** changes.

10. Navigate to **Objects > Address Groups**. Click **Add** to add a dynamic address group. Name the group and select **Dynamic** under Type. Click **Add Match Criteria** and locate the category/categories you want to create dynamic address groups with. Click **OK**.

The screenshot shows the 'Address Group' configuration window. At the top, the title bar says 'Address Group' with a help icon and a close icon. The form contains the following fields and options:

- Name:** A text input field containing 'Client VM DAGs'.
- Shared:** An unchecked checkbox.
- Disable override:** An unchecked checkbox.
- Description:** An empty text input field.
- Type:** A dropdown menu set to 'Dynamic'.
- Match:** A large text area containing the text 'intnx.PC-Prism\_Central.CL-PHX-POC085.ClientVM.ABAD'.
- Tags:** A dropdown menu with a plus icon and the text 'Add Match Criteria'.

At the bottom right, there are two buttons: a blue 'OK' button and a grey 'Cancel' button.

11. On the **Objects > Address Groups** tab, select **more...** under the addresses column for the dynamic address group you just created. You should see objects that have been pulled in from Prism Central.

**PANORAMA** DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE PANORAMA

Device Group: **NTNX-DeviceGroup**

Addresses

**Address Groups**

| NAME                                               | LOCATION         | MEMBERS COUNT | ADDRESSES |
|----------------------------------------------------|------------------|---------------|-----------|
| <input checked="" type="checkbox"/> Client VM DAGs | NTNX-DeviceGroup | dynamic       | more...   |
| <input type="checkbox"/> Domain Controller DAGs    |                  |               | more...   |
| <input type="checkbox"/> NTNX CVMs                 |                  |               |           |
| <input type="checkbox"/> PAN VM Firewalls          |                  |               |           |

**Address Groups - Client VM DAGs** 2 items → X

| ADDRESS     | TYPE          | ACTION          |
|-------------|---------------|-----------------|
| 10.42.85.52 | registered-ip | Unregister Tags |
| 10.42.85.53 | registered-ip | Unregister Tags |

NTNX-CVM-A-10.42.85.29  
NTNX-CVM-B-10.42.85.30  
NTNX-CVM-C-10.42.85.31  
NTNX-CVM-D-10.42.85.32  
PAN-VM01-10.42.85.41  
PAN-VM02-10.42.85.42  
PAN-VM03-10.42.85.43  
PAN-VM04-10.42.85.44

12. These Dynamic Address Groups can now be leveraged in security policy and will automatically update when changes to VMs tied to these categories change, thus automating policy without requiring a new security policy push.

**PANORAMA** DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE PANORAMA

Device Group: **NTNX-DeviceGroup**

Security

**Pre Rules**

| NAME                                  | LOCATION         | TAGS                   | TYPE      | ZONE           | Source                 | USER | Destination                           |
|---------------------------------------|------------------|------------------------|-----------|----------------|------------------------|------|---------------------------------------|
|                                       |                  |                        |           |                | ADDRESS                |      | ADDRESS                               |
| 1 PAN - Panorama - Inbound            | NTNX-DeviceGroup | PAN Management         | universal | NTNX-Flow-Zone | any                    | any  | NTNX-Flow-Zone PAN-Panorama-10.4...   |
| 2 PAN - Panorama - Outbound           | NTNX-DeviceGroup | PAN Management         | universal | NTNX-Flow-Zone | PAN-Panorama-10.42...  | any  | NTNX-Flow-Zone any                    |
| 3 PAN - NGFW - Inbound                | NTNX-DeviceGroup | PAN Management         | universal | NTNX-Flow-Zone | any                    | any  | NTNX-Flow-Zone PAN VM Firewalls       |
| 4 PAN - NGFW - Outbound               | NTNX-DeviceGroup | PAN Management         | universal | NTNX-Flow-Zone | PAN VM Firewalls       | any  | NTNX-Flow-Zone any                    |
| 5 PAN - Panorama Plugin               | NTNX-DeviceGroup | PAN Management         | universal | NTNX-Flow-Zone | PAN-Panorama-10.42...  | any  | NTNX-Flow-Zone NTNX-PC-10.42.85.39    |
| 6 NTNX - Prism Central - Inbound      | NTNX-DeviceGroup | NTNX Management        | universal | NTNX-Flow-Zone | any                    | any  | NTNX-Flow-Zone NTNX-PC-10.42.85.39    |
| 7 NTNX - Prism Central - Outbound     | NTNX-DeviceGroup | NTNX Management        | universal | NTNX-Flow-Zone | NTNX-PC-10.42.85.39    | any  | NTNX-Flow-Zone any                    |
| 8 NTNX - CVM Access to PC             | NTNX-DeviceGroup | NTNX Management        | universal | NTNX-Flow-Zone | NTNX CVMs              | any  | NTNX-Flow-Zone NTNX-PC-10.42.85.39    |
| 9 NTNX - PC Access to CVM and PE      | NTNX-DeviceGroup | NTNX Management        | universal | NTNX-Flow-Zone | NTNX-PC-10.42.85.39    | any  | NTNX-Flow-Zone NTNX CVMs              |
| 10 ABAD - Active Directory - Inbound  | NTNX-DeviceGroup | Active Directory Rules | universal | NTNX-Flow-Zone | Client VM DAGs         | any  | NTNX-Flow-Zone Domain Controller D... |
| 11 ABAD - Active Directory - Outbound | NTNX-DeviceGroup | Active Directory Rules | universal | NTNX-Flow-Zone | Domain Controller DAGs | any  | NTNX-Flow-Zone any                    |
| 12 ABAD - Active Directory - Protect  | NTNX-DeviceGroup | Active Directory Rules | universal | NTNX-Flow-Zone | any                    | any  | NTNX-Flow-Zone Domain Controller D... |
| 13 Test Office 365                    | NTNX-DeviceGroup | none                   | universal | NTNX-Flow-Zone | Client VM DAGs         | any  | NTNX-Flow-Zone any                    |

## Create Custom Application for NUTANIX

Nutanix AOS uses a non-standard port for SSL connections for management. This port will be categorized as SSL via PAN-OS App-ID; however, since TCP 9440 falls outside the realm of traditional SSL traffic, setting a rule to leverage Application-Default will result in this traffic bypassing the rule and instead, this traffic will live on the intrazone-default rule. We can create a custom application on Panorama to identify this traffic and assign this custom application in policy so that we can properly apply granular policy to these connections.

1. On the Panorama Web-UI, navigate to Monitor > Logs > Traffic and locate connections based on destination port TCP 9440.

Detailed Log View

General

Session ID

41537

Action

allow

Action Source

from-policy

Host ID

Application

ssl

Rule

intrazone-default

Rule UUID

9cc24362-5433-4eec-9b5e-92b12fc21ff1

Session End Reason

tcp-rst-from-server

Category

any

Device SN

007254000155107

IP Protocol

tcp

Log Action

Panorama Log Forwarding

Generated Time

2021/01/19 20:59:32

Start Time

2021/01/19 20:58:19

Receive Time

2021/01/19 20:59:50

Elapsed Time(sec)

44

Tunnel Type

N/A

Source

Source User

Source

10.42.85.31

Source DAG

Country

10.0.0.0-10.255.255.255

Port

36120

Zone

NTNX-Flow-Zone

Interface

ethernet1/2

X-Forwarded-For IP

0.0.0.0

Destination

Destination User

Destination

10.42.85.39

Destination DAG

Country

10.0.0.0-10.255.255.255

Port

9440

Zone

NTNX-Flow-Zone

Interface

ethernet1/1

Flags

Captive Portal

☐

Proxy Transaction

☐

Decrypted

☐

Packet Capture

☐

Client to Server

☐

Server to Client

☐

Symmetric Return

☐

Mirrored

☐

Tunnel Inspected

☐

Details

Type

end

Bytes

40055

Bytes Received

10872

Bytes Sent

29183

Repeat Count

1

| PCAP | RECEIVE TIME        | TYPE | APPLICAT... | ACTION | RULE              | RULE UUID | BYT... | SEVERITY | CATEG... | URL CATEG... LIST | VERDICT | URL | FILE NAME |
|------|---------------------|------|-------------|--------|-------------------|-----------|--------|----------|----------|-------------------|---------|-----|-----------|
|      | 2021/01/19 20:59:50 | end  | ssl         | allow  | intrazone-default | 9cc243... | 400... |          | any      |                   |         |     |           |
|      | 2021/01/19 20:59:50 | end  | ssl         | allow  | intrazone-default | 9cc243... | 400... |          | any      |                   |         |     |           |

Close

2. Login to the VM-Series Firewall where this traffic was observed from. Navigate to **Monitor > Packet Capture**. Select **Manage Filters**.

The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. On the left is a sidebar menu with 'Logs' expanded, showing various log types like Traffic, Threat, URL Filtering, etc., and 'Packet Capture' at the bottom. The main content area is titled 'Configure Filtering' and includes a 'Manage Filters' link and a status '[1/4 Filters Set]'. Below this are toggle switches for 'Filtering' (ON) and 'Pre-Parse Match' (OFF). The 'Configure Capturing' section has a 'Packet Capture' toggle (OFF) and a search bar. A table below the search bar has two columns: 'STAGE' and 'FILE'. One row is visible with 'firewall' in both columns.

3. On the **Packet Capture Filter** screen, click **Add** and include items from the log in step 85 that can be used to filter on the traffic. This will help keep the PCAP file clean for further analysis. Click **OK**.

The screenshot shows the 'Packet Capture Filter' configuration screen. It features a table with columns: ID, INGRESS INTERFACE, SOURCE, DESTINATION, SRC PORT, DEST PORT, PROTO, NON-IP, and IPV6. One filter is listed with ID 1, INGRESS INTERFACE ethernet1/1, SOURCE 10.42.85.31, and DESTINATION 10.42.85.39. Below the table are buttons for '+ Add', '- Delete', and a link 'Set Selected Packet Capture Filter'. At the bottom right are 'OK' and 'Cancel' buttons.

| <input type="checkbox"/>            | ID | INGRESS INTERFACE | SOURCE      | DESTINATION | SRC PORT | DEST PORT | PROTO | NON-IP  | IPV6                     |
|-------------------------------------|----|-------------------|-------------|-------------|----------|-----------|-------|---------|--------------------------|
| <input checked="" type="checkbox"/> | 1  | ethernet1/1       | 10.42.85.31 | 10.42.85.39 |          | 9440      |       | exclude | <input type="checkbox"/> |



- On the **Configure Capturing** section, click **Add** to create a capture stage file for PCAP collection. Select firewall for the stage and name the file. Click **OK**.

Packet Capture Stage

Stage

firewall

File

firewall

File name should begin with a letter and can have letters, digits, ".", "\*", "\_", and "%".

Packet Count

[1 - 209715200]

Byte Count

[1 - 209715200]

OK

Cancel

- Set both the **Filter** and **Packet Capture** to **ON**. Wait a few moments to make sure that traffic is successfully captured and then toggle the Packet Capture to **OFF**.

PA-VM

DASHBOARDACC**MONITOR**POLICIESOBJECTS

Logs

Traffic

Threat

URL Filtering

WildFire Submissions

Data Filtering

HIP Match

GlobalProtect

IP-Tag

User-ID

Decryption

Tunnel Inspection

Configuration

Configure Filtering

Manage Filters

[1/4 Filters Set]

Filtering

ON

Pre-Parse Match

OFF

Configure Capturing

Packet Capture

ON

Q

| <input type="checkbox"/> | STAGE    | FILE     |
|--------------------------|----------|----------|
| <input type="checkbox"/> | firewall | firewall |

6. After you turn the Packet Capture OFF, a file will appear under Captured Files.

| Captured Files                     |                     |          |
|------------------------------------|---------------------|----------|
| <input type="text"/>               |                     |          |
| <input type="checkbox"/> FILE NAME | DATE                | SIZE(MB) |
| <input type="checkbox"/> firewall  | 2021/01/24 23:40:03 | 0.379249 |

7. Download the file and open the PCAP file in Wireshark. Find a full TCP session by pulling up TCP Streams. Custom Applications in PAN-OS require us to identify a common pattern to use for App-ID deep-packet inspection. Since SSL traffic is encrypted, the only readable data can be derived from the server certificate. The PCAP below shows the server certificate has a commonName of **\*.nutanix.local**. We will use this to build our custom application.

The image shows a Wireshark packet capture of a TLS handshake. The packet list at the top shows a sequence of packets: a TCP Reset (RST) from 10.42.85.39 to 10.42.85.30, followed by a TLSv1.2 Server Hello and Certificate exchange. The packet details pane for the selected packet (Frame 79) shows the TLSv1.2 Record Layer: Handshake Protocol: Certificate. The certificate details show a commonName of \*.nutanix.local.

```
> Frame 79: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Nutanix_e2:2b:c2 (50:0b:8d:e2:2b:c2), Dst: Nutanix_c4:f4:67 (50:0b:8d:c4:f4:67)
> Internet Protocol Version 4, Src: 10.42.85.39, Dst: 10.42.85.30
> Transmission Control Protocol, Src Port: 9440, Dst Port: 58644, Seq: 1, Ack: 191, Len: 1460
> Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Server Hello
  > TLSv1.2 Record Layer: Handshake Protocol: Certificate
    > Certificate: 308203bf308202a7a0030201020209002640000073a9c35300000092a064000f7000101... (id-at-commonName=*.nutanix.local,id-at-organizationalUnitName=Manageability,id-at-organizationName=Nutanix Inc.,id-at-localityName=San Jose,id-at-stateOrProvinceName=CA,id-at-countryName=US)
      > signedCertificate
        > version: v3 (2)
        > serialNumber: 0x0012640000073a9b5
        > signature (sha256withRSAEncryption)
          > issuer: rdnSequence (0)
          > rdnSequence: 6 items (id-at-commonName=*.nutanix.local,id-at-organizationalUnitName=Manageability,id-at-organizationName=Nutanix Inc.,id-at-localityName=San Jose,id-at-stateOrProvinceName=CA,id-at-countryName=US)
          > validity
            > subject: rdnSequence (0)
            > subjectPublicKeyInfo
              > extensions: 3 items
            > algorithmIdentifier (sha256withRSAEncryption)
              > padding: 0
            > encrypted: 8500d4b6260000f4197859ef0eca81e0ac6885c5d2073cbd7d36c34931746472c90ca444...
```



8. On the Panorama Web-UI, navigate to **Objects > Applications** and click **Add** at the bottom.
- On the **Application > Configuration** tab, provide the App with a name, description and define appropriate properties for the applications behavior.

Application (Read Only) ?

Configuration

Advanced

Signatures

General

Name

Nutanix-SSL

Description

Nutanix Prism Web Console

Properties

Category

networking

Subcategory

encrypted-tunnel

Technology

browser-based

Parent App

ssl

Risk

1

Characteristics

☒ Capable of File Transfer

☐ Excessive Bandwidth Use

☒ Tunnels Other Applications

☐ Has Known Vulnerabilities

☐ Used by Malware

☐ Evasive

☐ Pervasive

☐ Prone to Misuse

☐ Continue scanning for other Applications

Tag

Edit

OK

Cancel

9. On the **Application > Advanced** tab, select **Port** under Defaults and click **Add** to provide **Port** and **Protocol** information.

Application (Read Only) ?

Configuration

Advanced

Signatures

Defaults

☒ Port

☐ IP Protocol

☐ ICMP Type

☐ ICMPv6 Type

☐ None

PORT

tcp/9440

+ Add

- Delete

Enter each port in the form of [tcp|udp]/[dynamic|0-65535] Example: tcp/dynamic or udp/32

Timeouts

Timeout

[0 - 604800]

TCP Timeout

[0 - 604800]

UDP Timeout

[0 - 604800]

TCP Half Closed

[1 - 604800]

TCP Time Wait

[1 - 600]

Scanning (activated via Security Profiles)

☐ File Types

☐ Viruses

☐ Data Patterns

OK

Cancel

10. On the **Application > Signatures** tab, click **Add**. Give the signature a name and select **Session** for the Scope. Click **Add And Condition**. Build a pattern based on the **ssl-rsp-certificate** context and write the pattern out in **REGEX** format. Click **OK** three times to save the custom application.

Signature

Signature Name

Nutanix-SSL

Comment

Scope

Transaction

Session

☐ Ordered Condition Match

| <input type="checkbox"/> | AND CONDITION   | COND...          | OPERATOR      | CONTEXT             | PATTERN            |
|--------------------------|-----------------|------------------|---------------|---------------------|--------------------|
| And Condition 1          |                 |                  |               |                     |                    |
| <input type="checkbox"/> | And Condition 1 | Or Condi...<br>1 | pattern-match | ssl-rsp-certificate | \*\..nutanix\..loc |

+

 Add Or Condition 

+

 Add And Condition 

-

 Delete 

↑

 Move Up 

↓

 Move Down

OK

Cancel

Or Condition

Operator

Pattern Match

Context

ssl-rsp-certificate

Pattern

\\*\..nutanix\..local

0 items

| <input type="checkbox"/> | QUALIFIER | VALUE |
|--------------------------|-----------|-------|
|--------------------------|-----------|-------|

+

 Add 

-

 Delete

OK

Cancel

12. On the **Monitor > Logs > Traffic** tab, you can now observe **Nutanix-SSL** traffic hitting our custom application accordingly.

| PANORAMA                                                                                                                                    |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
|---------------------------------------------------------------------------------------------------------------------------------------------|--|----------------------|---------|----------|--|---------|---------|--------|----------|--|--|--|--|--|--|--|
| Dashboard                                                                                                                                   |  | ACC                  | Monitor | Policies |  | Objects | Network | Device | Panorama |  |  |  |  |  |  |  |
| Panorama                                                                                                                                    |  | Device Group         |         | All      |  |         |         |        |          |  |  |  |  |  |  |  |
| Logs                                                                                                                                        |  | 1 app 22 Nutanix-SSL |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Traffic                                                                                                                                     |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Threat                                                                                                                                      |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| URL Filtering                                                                                                                               |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| WebFilter Submissions                                                                                                                       |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Data Filtering                                                                                                                              |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| HTTP Match                                                                                                                                  |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| GlobalProtect                                                                                                                               |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| IP Tag                                                                                                                                      |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| User-ID                                                                                                                                     |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Decryption                                                                                                                                  |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Tunnel Inspection                                                                                                                           |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Configuration                                                                                                                               |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| System                                                                                                                                      |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Authentication                                                                                                                              |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Unified                                                                                                                                     |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| External Logs                                                                                                                               |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Raps ESM                                                                                                                                    |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Threat                                                                                                                                      |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| System                                                                                                                                      |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Policy                                                                                                                                      |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Config                                                                                                                                      |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Agent                                                                                                                                       |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Automated Correlation Engine                                                                                                                |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Correlation Objects                                                                                                                         |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Correlated Events                                                                                                                           |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| App Scope                                                                                                                                   |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| Summary                                                                                                                                     |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:44 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.31 1042.85.39 9440 Nutanix-SSL allow NTHK - Pktn Central - Inbound  |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:43 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.31 1042.85.39 9440 Nutanix-SSL allow NTHK - Pktn Central - Inbound  |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:43 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.32 1042.85.39 9440 Nutanix-SSL allow NTHK - Pktn Central - Inbound  |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:34 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.29 1042.85.39 9440 Nutanix-SSL allow NTHK - Pktn Central - Inbound  |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:24 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.39 1042.85.31 9440 Nutanix-SSL allow NTHK - Pktn Central - Outbound |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:22 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.32 1042.85.39 9440 Nutanix-SSL allow NTHK - Pktn Central - Inbound  |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:20 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.30 1042.85.39 9440 Nutanix-SSL allow NTHK - Pktn Central - Inbound  |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:19 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.29 1042.85.39 9440 Nutanix-SSL allow NTHK - Pktn Central - Inbound  |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:16 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.40 1042.85.39 9440 Nutanix-SSL allow PAN - Panorama - Outbound      |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:16 PA-Flow-VMM-03 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.40 1042.85.39 9440 Nutanix-SSL allow PAN - Panorama - Outbound      |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:14 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.31 1042.85.39 9440 Nutanix-SSL allow NTHK - Pktn Central - Inbound  |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:13 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.32 1042.85.39 9440 Nutanix-SSL allow NTHK - Pktn Central - Inbound  |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:13 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.39 1042.85.37 9440 Nutanix-SSL allow NTHK - Pktn Central - Outbound |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:06 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.30 1042.85.39 9440 Nutanix-SSL allow NTHK - Pktn Central - Inbound  |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/25 22:24:04 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.30 1042.85.39 9440 Nutanix-SSL allow NTHK - Pktn Central - Inbound  |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |
| 01/24 22:59:48 PA-Flow-VMM-01 end NTHK-Flow-Zone NTHK-Flow-Zone 1042.85.36 1042.85.37 9440 Nutanix-SSL allow NTHK - Pktn Central - Outbound |  |                      |         |          |  |         |         |        |          |  |  |  |  |  |  |  |

## Best Practices

### PAN-OS Maintenance

Nutanix AOS currently does not have a way to monitor the health or status of a VM attached to a Service Chain. This means that when any NGFW Virtual Appliance attached to the Service Chain is offline, all internal VM traffic will fail on the Nutanix Host with the offline NGFW Virtual Appliance.

When performing any maintenance function that requires a reboot of the NGFW Virtual Appliance such as a software upgrade to PAN-OS, it is recommended to migrate all VM's off by placing the Nutanix Host in maintenance mode. Once all Virtual Machines are migrated off the Nutanix Host, it is safe to reboot the NGFW Virtual Appliance. Once the NGFW Virtual Appliance maintenance is complete, the Nutanix Host may be placed out of maintenance mode.

# References

1. Install Panorama Virtual Appliance on Nutanix AHV  
<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/set-up-panorama/set-up-the-panorama-virtual-appliance/install-the-panorama-virtual-appliance/install-panorama-on-kvm.html>
2. Initial Panorama Virtual Appliance Configuration  
<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/set-up-panorama/set-up-the-panorama-virtual-appliance/perform-initial-configuration-of-the-panorama-virtual-appliance.html>
3. Configure Panorama as a Local Log Collector  
<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-log-collection/configure-a-managed-collector.html>
4. Configure Log Forwarding to Panorama  
<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-log-collection/configure-log-forwarding-to-panorama.html>
5. Complete the Panorama Virtual Appliance Setup  
<https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/set-up-panorama/set-up-the-panorama-virtual-appliance/complete-the-panorama-virtual-appliance-setup.html>
6. Configure the Panorama Plugin for Nutanix  
<https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/set-up-the-vm-series-firewall-on-nutanix-ahv/vm-monitoring-on-nutanix/configure-the-panorama-plugin-for-nutanix>
7. Install VM-Series Firewall on Nutanix AHV  
<https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/set-up-the-vm-series-firewall-on-nutanix-ahv.html>
8. Initial VM-Series Firewall Configuration  
<https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/set-up-the-vm-series-firewall-on-kvm/install-the-vm-series-firewall-on-kvm/install-the-vm-series-firewall-using-virt-manager/perform-initial-configuration-on-the-vm-series-on-kvm.html>
9. Nutanix REST API  
<https://portal.nutanix.com/page/documents/details?targetId=Prism-Element-Data-Protection-Guide-v511:man-rest-api-c.html>
10. Create a Service Chain using REST APIs on Nutanix  
<https://portal.nutanix.com/page/documents/kbs/details?targetId=kA00e000000LleICAG>