

TECHNOLOGY PARTNER PROGRAM

- 1. Deployment of Palo Alto Networks VM-Series Next-Generation Firewall with Nutanix Calm
- 2. Applying Microsegmentation with Nutanix Flow and Palo Alto Networks VM-Series

Author: Nutanix and Palo Alto Networks



Contents

Partner Information	4
Use cases for integration into Palo Alto Networks Next-Generation Security Operating Platform	4
Use Case No. 1: Micro-Segmentation	4
Use Case No. 2: Virtual Desktop Infrastructure	4
Palo Alto Networks Products for Integration	4
Integration Benefits	5
Integration Diagram	6
Palo Alto Networks Configuration	6
Bootstrap ISO	6
Generate VM-Auth-Code	6
Bootstrap ISO Image Creation	7
Create ISO Image	8
Register the VM-Series Firewall with Auth Codes	9
Download VM-Series KVM Base Image	10
Create Panorama Admin Account for Nutanix Calm	10
Partner Product Configuration	13
Upload VM-Series Image and Bootstrap ISO Image	13
Create a Project	16
Import and Configure Calm Blueprint	19
Deploy Palo Alto Networks VM-Series Application from Calm Blueprint	37
Verify PAN-OS XML API Configuration Settings	42
Verify VM-Series Virtual Machines Provisioning	43
Apply Microsegmentation Policy via Nutanix Flow and VM-Series	45
Deploy Additional VM-Series via Calm Scale Out	51
Troubleshooting Resources & Documentation	54
Nutanix	54
Palo Alto Networks	54
Technical Details	55
Nutanix	55
Palo Alto Networks	56

Partner Information

Partner information			
Date	September 27, 2019		
Partner Name	Nutanix and Palo Alto Networks		
Web Site	https://www.nutanix.com & https://www.paloaltonetworks.com		
Product Name	Nutanix Calm & Flow, Palo Alto Networks Panorama & VM-Series		
Partner Contact	alliances@nutanix.com; nutanix@paloaltonetworks.com		
Support Contact	https://www.nutanix.com/support-services/product-support		
Product Description	Automated deployment of Palo Alto Networks VM-Series Next-Generation Firewall and Microsegmentation		

Use cases for integration into Palo Alto Networks Next-Generation Security Operating Platform

Use Case No. 1: Micro-Segmentation

- **Challenge:** Virtual applications running on the same host are difficult to selectively segment without complex network design and configuration, often requiring hairpinning 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 No. 2: 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

- Panorama (8.1 & 9.0)
- PAN-OS for VM-Series KVM Image (8.1 & 9.0)

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	Nutanix Versions
AutoFocus			
Cortex XDR			
Cortex XDR Analytics			
MineMeld			
NGFW			
Panorama		PAN-OS 8.1 & PAN-OS 9.0	Prism Central 5.10.6 AOS 5.10.6 with AHV Calm 2.7.0 -or- Prism Central 5.11 AOS 5.11 with AHV Calm 2.7.1
Prisma Access			
Prisma Cloud			
Prisma SaaS			
Traps			
VM-Series		8.1 & 9.0	Prism Central 5.10.6 AOS 5.10.6 with AHV Calm 2.7.0 -or- Prism Central 5.11 AOS 5.11 with AHV Calm 2.7.1
WildFire			
Other			

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.

Integration Diagram



Palo Alto Networks Configuration

Bootstrap ISO

To provide a zero-touch configuration of the Next-Generation Firewall VM-Series instances, which includes automatic licensing and subscription to a Panorama centralized management server, the Bootstrap ISO image provides the configuration elements necessary.

The contents of the Bootstrap ISO image consist of four directories off the root of the ISO filesystem – within two of the four directories are files containing the requisite configuration data. While other configuration elements are possible, they are outside the scope of this guide and are not required for deploying VM-Series with Nutanix Calm.

Generate VM-Auth-Code

Prior to creating the Bootstrap ISO image, you must first generate the VM-Auth-Code. Log into Panorama via the command-line interface (CLI), and issue the following command:

request bootstrap vm-auth-key generate lifetime <1-8760>

For example, to generate a key that is valid for 24 hours, enter the following:

request bootstrap vm-auth-key generate lifetime 24

VM auth key 755036225328715 generated. Expires at: 2019/12/29 12:03:52

Bootstrap ISO Image Creation

Create a new folder called *bootstrap* on your computer. Within that folder, create four folders as follows:

		•		
config				
	init-cfg.txt	(case-sensitive t	text file)	
content				
	Empty			
license				
	<i>authcodes</i> extension)	(case-sensitive f	text file with no fil	le
software				
	Empty			
	Image: Image	Manage DVD Drive (E:) Bootstrap Drive Tools		
	A Name	^ Date modified	Type	
	A Quick access	8/19/2019 12:4	4 AM File folder	
	Desktop *	t 10/14/2016 5:5	4 AM File folder	
	Documents 🖈 🔤 softwa	re 8/19/2019 12:4 re 8/19/2019 12:4	4 AM File folder 4 AM File folder	
	Pictures 🖈			
	Cleanup			
	Desktop			
	Nutanix Blueprir			
	This PC			
	3D Objects			

Use a text editor to create the init-cfg.txt and authcodes text files listed above and place them in their respective directory:

init-cfg.txt

```
type=dhcp-client
op-cmd-dpdk-pkt-io=off
ip-address=
default-gateway=
netmask=
ipv6-address=
ipv6-default-gateway=
hostname=
```

```
vm-auth-key=VM AUTH KEY VALUE
panorama-server=IP ADDRESS OF PANORAMA SERVER
panorama-server-2=
tplname=
dgname=
dns-primary=IP ADDRESS OF PRIMARY DNS
dns-secondary=IP ADDRESS OF SECONDARY DNS
op-command-modes=multi-vsys,jumbo-frame
dhcp-send-hostname=no
dhcp-accept-server-hostname=no
dhcp-accept-server-domain=no
```

← → ~ ↑ 📙 > Th	is PC > DVD Drive (E:) Bo	otstrap → config			
A Quick access Desktop Downloads Documents Pictures Pictures	Name		Date modified 8/19/2019 12:57 AM	Type Text Document	Size 1 K
Cleanup Cleanup Desktop Creative Cloud Fil This PC 3 D Objects		6			

authcodes

A123456789 enter the value for the auth code as provided by Palo Alto Networks





Create ISO Image

Use the 'mkisofs' utility to create the ISO image containing the files and corresponding directory structure above:



mkisofs -J -R -v -V "Bootstrap" -A "Bootstrap" -ldots -l -allow-lowercase -allow-multidot -o bootstrap.iso bootstrap/

Register the VM-Series Firewall with Auth Codes

Prior to deployment of VM-Series, your auth codes must be activated on the Palo Alto Networks support site otherwise, the automated licensing process will not complete successfully.

Using your web browser, go to:

https://support.paloaltonetworks.com

Navigate to Assets -> VM-Series Auth Codes



Follow the instructions as documented on the Palo Alto Networks TechDocs site to register the auth codes:

https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/license-the-vm-series-firewall/register_ -the-vm-series-firewall/register-the-vm-series-firewall-with-auth-code.html

Download VM-Series KVM Base Image

To deploy VM-Series on your Nutanix cluster, download the VM-Series KVM Base Image from the Palo Alto Networks Support Site:

https://support.paloaltonetworks.com

1. Navigate to Assets -> Software Updates



- 2. In the Filter By drop-down select PAN-OS for VM-Series KVM Base Images
- 3. Download the most recent version by selecting the link containing the filename as denoted below.

oftware	Updates				
ilter By: PAN	-OS for VM-Series KV	M Base Im 👻			
Version	Release Date 🔻	Release Notes	Download	Size	Checksum
V PAN-OS	for VM-Series KV	/M Base Images		_	
9.0.1	04/09/2019	Release Notes	PA-VM- KVM-9.0.1.qcow2	3.0 GB	Checksum
8.0.15	03/04/2019	Release Notes	PA-VM- KVM-8.0.15.qcow2	2.3 GB	Checksum

Create Panorama Admin Account for Nutanix Calm

Not only does the Nutanix Calm Blueprint for VM-Series deploy instances across your Nutanix AHV cluster, it also leverages the PAN-OS XML API to automate the configuration of several key elements within Panorama. While it is possible to use an administrative account with Super User privileges, the principle of least-privilege dictates that you should always use administrative accounts with only the permissions necessary to carry out the required functions.

This is easily accomplished through the creation of an Admin Role and Administrator account in Panorama.

1. Log into the Panorama admin UI and navigate to the Panorama tab, then select Admin Roles



2. Create a new Admin Role by clicking Add at the bottom of the page (api-admin-role)



3. Deselect every option on the Web UI tab by clicking on each green checkmark. They will change to red Xs as you proceed through the list



4. Change to the *XML/REST API* tab and repeat the process, this time changing every red X to a green checkmark



5. No changes are necessary on the Command Line tab as no permissions are granted by default

			pi-admin-role							
Desci	ription	Restrict ac	cess to API							
	Role	Panorar	na 🔘 Device Group	and Template						
Web UI	XML/I	REST API	Command Line							
None										

- 6. Click *OK* to save the changes
- 7. Select the Administrators menu, then click Add to create a new account provide a username (nutanixadmin) and password and confirm the password. Change the Administrator Type drop-down select from Dynamic to Custom Panorama Admin, then select the newly created role in the next drop-down select

paloalto		Dashboar	d ACC	Monitor Pan	norama	Administrator		0
Context Panorama						Name	nutanixadmin	
Setup • · · · · · · · · · · · · · · · · · ·	^					Authentication Profile	None Use only client certificate authentication (Web)	*
Config Audit Managed WildFire Clusters Managed WildFire Appliances		Name	Role	Authentication Profile	Password Pr	Password Confirm Password	••••••	
Administrators		admin	Superuser			Administrator Type	Use Public Key Authentication (SSH) Custom Panorama Admin	-
Access Domain Authentication Profile						Profile Password Profile	api-admin-role None	~
Addrenication Sequence User Identification Managed Devices Summary							Can	cel

8. Click OK to save the new account. Select *Commit -> Commit to Panorama* then click the *Commit* button to apply the newly defined role and account



Partner Product Configuration

Upload VM-Series Image and Bootstrap ISO Image

Begin the deployment process by uploading the PAN-OS for VM-Series KVM Base Image and Bootstrap ISO to Prism Central.

		x	🐥 🧿 🔘 🕄 📍 admin 🗸
Main Dashboard			Reset Dashboard + Add Widgets
Impacted Cluster	Cluster Quick Access	Cluster Storage	Tasks
Ntnx-Cluster	Ntnx-Cluster	CLUSTER USED STORAGE DATA REDU	View All Task(s) DETAILS
Per Cap Conf Ava Sys		Ntnx-Cluster 1.09 : 1	Resolve Alert: 0 out of 3 alerts successfully Failed O updated
Anomalies (last 24 hours)			Resolve Alert: 0 out of 3 alerts successfully Failed •
Runway 365 days Inefficient VMs 51			Acknowledge Alert: 0 out of 3 alerts Failed O
Cluster Runway	Cluster CPU Usage	VM Efficiency ×	Cluster Latency
Ntnx- CPU 365+ days	Ntnx- Cluster 16.7%	32 19 Overprovisioned Inactive	Ntnx- Cluster 5.8 ms
	Cluster Memory Usage	1 0	Controller IOPS
	Ntnx- Cluster 60.07%	Constrained Bully	Ntnx- 261 Cluster IOPS
		View All Inefficient VMs	
		Reports	
		2 0 Total Reports Scheduled Reports	

1. From the Prism Central menu, navigate to Virtual Infrastructure -> Images



2. Click Add Image

⊒ Q Images	☆
Images 7 Total Images	□ • Add Image ↓ → Type name to filter by
	► Name

- 3. Click +Add File and browse to the PAN-OS for VM-Series KVM Base Image, then click OK
- 4. Input a name in the *Image Name* field or accept the default value, a description (optional), leave the *Image Type* set to *Disk*, and click *Save*

Add In	nages
Image Source	
Image File O URL	
+ Add	I File
Source: [LOCAL]\PA-VM-KVM-9.0	1.qcow2 Remove
Image Name	Image Type
VM-Series-9.0.1-Base-KVM-	Disk ~
Image Description	
Palo Alto Networks VM-Series	9.0.1 Disk Image
	Cancel Save

- 5. Click Add Image
- 6. Click +Add File and browse to the Bootstrap ISO, then click OK

Image File OURL			
	+ Add F	ile	
Source: [LOCAL]\VN	1-Series Bootstra	ap.iso	Remove
Image Name VM-Series Bootst	rap.iso	ISO	
Image Description			
VM-Series Bootst	rap ISO		

7. Input a name in the *Image Name* field or accept the default value, provide a description (optional), choose *ISO* from the *Image Type* drop-down select, and click *Save*

Create a Project

If you already have an existing Nutanix Project defined, that can be used to deploy the Calm Blueprint in lieu of creating a new project. Otherwise, follow the steps in this section to create a new Nutanix Project.

1. Navigate to Administration -> Projects



2. Click Create Project

a Projects		×
Projects O Total Projects	Create Project	

3. Provide a *Name* and *Description*, then choose the *AHV Cluster* on which you want to deploy the VM-Series instances

Create Project		
General Settings Project Name Palo Alto Networks VM-Series Deployment Description Deploy VM-Series on Nutanix		General Settings Cluster Users, Groups and Role Network Quotas (Optional)
Cluster		
Ntnx-Cluster	•	

4. Click the *+Users* button then select either *User* or *User Group* in the drop-down select – type in the first few letters of the desired *User* or *User Group* and auto-complete will provide a list of options to select and choose the *Project Admin* role, then click *Save*

elect users and active directo	ry groups.	+ User
NAME	ROLE	ACTIONS
User ↓ Nutanix Admin	Project Admin	✓ Save · Cancel

Collaboration enables users in this project to see and interact with each other's VMs, Apps, etc. The role given to a user determines the extent to which they can interact with entities that belong to other users in this project.

Network

Select the networks that will be accessible to this project.

5. Select the checkbox next to the *Network* to associate with the Management interface on each VM-Series instance

	Create Project		
C client_vw	0	슙	
cognitiveclient	0	☆	General Settings
cognitiveserver	0	☆	Users, Groups and Roles
container	22	☆	Network Quotas (Optional)
□ 12	0	☆	
L2ClientVlan30	30	☆	
L2ServerVlan40	40	습	
g mgmt-network	0	☆	
prismnet	156	습	

6. Scroll down and click *Save* to finish configuring the *Project*

vwire200	200	۲ ۲
vwire_vlan_301	301	<u>ث</u>
vwire_vlan_302	302	Ó

Cancel

Save

Quotas (Optional)

Import and	Configure	Calm	Blueprint

^{1.} Navigate to Services -> Calm



2. Choose the Blueprints menu and click on Upload Blueprint



3. Browse to the Calm Blueprint JSON file and select the Project created in the last section and click Upload

Upload Blueprint	×
Blueprint Name	
Palo Alto Networks - VM-Series - Calm Blueprint	
Project	
Palo Alto Networks VM-Series Deployment	×v
	Upload Cancel

NOTE: As you proceed through the remaining steps, ensure you only modify the settings in the Value fields – do not modify any text in the Name fields

Save 🕆 Publish 🛓 Do	ownload 🕨 La	unch	?
Application AHV	n Profile Name		
Variables 🥐	Variables 🕐		Ð
COUNT: 1 Type: String		ズ	:
Panorama_IP: 192.1 Type: String	68.1.1	Ř	:
Panorama_Usernan Type: String	ne: admin	ř	:
Panorama_Passwor Type: String	rd: ******	×	:
Panorama_DeviceG	Group: Calm	×	:
Panorama_Templat Type: String	e: Calm-Templ	ž	:
Panorama_Templat Type: String	eStack: Calm	ž	:
Panorama_Zone: C. Type: String	ALM-VWIRE-Z	×	:
Panorama_Vwire: d	lefault-vwire	X	:

4. Input a numeric value in the *COUNT* section to represent the number of VM-Series instances you want to deploy

COUNT: 2	×	1.848.0
Name		
COUNT		
Data Type (i)		
String	*	
Multiple Input (Array)		
Input Type		
Simple	*	
Value		
2]
Secret ()		
Label (Optional)		
Palo Alto Networks VM-Series Count		
Description (Optional)		
No of palo alto VMs to be provisioned in AHV cluster.	/	
	.1	
Mark this variable private		L
Private variables are hidden from users. They a	re not	

5. Provide the IP address for your Panorama server

Panorama_IP: 10.3.6.97	S.
Name	
Panorama_IP	
Data Type 🕕	
String	*
Multiple Input (Array)	
Input Type	
Simple	•
Value	
10.3.6.97	
Secret ()	
Label (Optional)	
IP Address of Panorama	
Description (Optional)	5
14	

6. Supply the username for the Panorama delegated Administrator account (nutanixadmin) created earlier

F	Panorama_Username: nutanixad 🕉
Nā	ime
F	anorama_Username
Da	ita Type 🕕
	5tring 👻
	Multiple Input (Array)
Inj	but Type
	5imple 👻
Va	lue
1	nutanixadmin
	Secret ()
La	bel (Optional)
ι	Jsername for Panorama API Administrator
De	scription (Optional)
(Credential used to make api operations for panorama configuration
	Mark this variable private
Pri sho	vate variables are hidden from users. They are not own at launch or in app. So, they cannot be marke ntime

7. Enter the corresponding password for the delegated Administrator account in the Value field

Panorama_Password: ******	x
Name	
Panorama_Password	
Data Type (i)	
String	Ŧ
Multiple Input (Array)	
Input Type	
Simple	*
Value	ø
Secret ()	
Label (Optional)	
Password for Panorama API Admir	nistrator
Description (Optional)	
Description (Optional) Credential used to make api opera	ations for
Description (Optional) Credential used to make api oper panorama configuration	ations for

8. Accept the default Panorama Device Group name (CALM) or supply your own in the Value field

Panorama_DeviceGroup: Nutanix 🕉
Name
Panorama_DeviceGroup
Data Type ()
String
Multiple Input (Array)
Input Type
Simple
Value
Nutanix_Device_Group
Secret ()
Label (Optional)
Device Group for Palo Alto VMs
Description (Optional)
Device group created on panorama for palo alto VMs
Private variables are hidden from users. They are not
shown at launch or in app. So, they cannot be marked runtime
Mark this variable mandatory

9. Accept the default Panorama Template name (Calm_Template) or supply your own in the Value field

Name	
Panorama_Template	
Data Type 🧻	
String	-
Multiple Input (Array)	
Input Type	
Simple	•
Value	
Nutanix_Template	
Secret ()	
Label (Optional)	
Template for Palo Alto VMs	
Description (Optional)	
Template created on panorama for palo VMs.	alto
Mark this variable private	
Private variables are hidden from users. The	ey are not
shown at launch or in app. So, they cannot l runtime	be marked
Mark this variable mandatory	
Mandatory variables will have to be filled by	the
consumers while launching the application	

10. Accept the default Panorama Template Stack (Calm_Stack) or supply your own in the Value field

Name	
Panorama_TemplateStack	
Data Type (i)	
String	Ŧ
Multiple Input (Array)	
Input Type	
Simple	*
Value	
Nutanix_Template_Stack	
Secret ()	
Label (Optional)	
Template Stack for Pars Alto VMs	
Description (Optional)	
Template stack created on panorama for alto VMs.	palo
Mark this variable private	
Private variables are hidden from users. The	y are not
shown at launch or in app. So, they cannot b runtime	e marke
Mark this variable mandatory	
Mandatery wariables will have to be filled by	the

11. In the *Panorama_Zone* section, accept the default *PAN-OS Security Zone Name* (*CALM-VWIRE-ZONE*) or supply your own in the *Value* field

blama	
Name	
Panorama_Zone	
Data Type 🧻	
String	v
Multiple Input (Arrey)	
Input Type	
Simple	Ŧ
Value	
Microsegment_Zone	
Secret ①	
Label (Optional)	
Zone for Palo Alto VMs	
Description (Optional)	
Zone created on panorama for palo alto V	'Ms
Mark this usualable subjects	
mark this variable private Private variables are hidden from users. They	v are not
shown at launch or in app. So, they cannot b	e marke
unioning .	
Mark this variable mandatory	
Mark this variable mandatory Mandatory variables will have to be filled by	the

12. In the *Panorama_Vwire* section, accept the default name for the *PAN-OS Virtual Wire* object (*default-vwire*) or supply your own in the *Value* field

Panorama_Vwire	В
Data Type 🚺	
String	· · · · · · · · · · · · · · · · · · ·
Multiple Input	(Array)
Input Type	
Simple	
Value	
Nutanix_vWire	
Secret (1)	
Label (Optional)	
Virtual wire for Pa	alo Alto VMs
Description (Optio	nal)
Virtual wire creat VMs	ted on panorama for palo alto
Mark this varia	ble private
Private variables an	e hidden from users. They are no
untime	in app. 50, they cannot be marke
	2
✓ Mark this varia	pre mandatory
consumers while la	unching the application
LUIISUIICIS WITHE IN	

13. Scroll up to the top and click Save



14. You will see an error message displayed – this is expected behavior



15. Click the *Credentials* link

Q Calm	*	×	🐥 🕄 🔘 <mark>?</mark> 💠 admin v
Palo Alto Networks - VM-Series - Calm Blueprint	9	Configure Credentials	✓ I Save ⊕ Publish
			Variables ?

16. Expand the *Credentials* section by clicking the > next to the username *admin*



17. Input the default PAN-OS admin password (*admin* – all lowercase) and click *Save* – this time the changes apply without any error message – click the *Back* button

Credentials	
Credentials 😛	
✓ ₽ admin	
Credential Name	
admin	
Username	Ř
admin	
Secret Type	
Password	•
Password	Ř
•••••	•
	Reset Clear
Is used as the default credential	?



18. In the lower left-hand corner, click the word *PaloAlto* in the box labeled *Service* – a new set of configuration settings will open on the righthand side of the page



19. The names of the *Virtual Machines* are dynamically created based on the value defined in the *VM Configuration* section

vin comgututo	
@@(calm_array_ @@(calm_time)@ a unique VM nar prepend a custo identification.	index)@@ and I@ have been added to ensure ne. You can append or m string to this value for
VM Name VM-Series-@@(NU	<i>オ</i> JM)@@
IMAGES (2)	ズ 🕂
IMAGES (2)	ズ 🛨 : (1)
IMAGES (2) Image Device Bootable Ima	
IMAGES (2) Image Device Bootable Ima Image	ې € (۱) ge cannot be deleted ۲

The default text PaloAlto-@@{NUM}@@ will create Virtual Machines in the following format:

PaloAlto-1 PaloAlto-2 ... PaloAlto-X

To change the name of the Virtual Machines, only replace the text up to @@{NUM}@@

20. Modify the drop-down select for *Image Device (1)* to reflect the *PAN-OS for VM-Series KVM Base Image* you imported earlier – **do not uncheck** checkbox next to *Bootable* – the *PAN-OS for VM-Series KVM Base Image* is the default boot volume and the VM will not boot if the checkbox is unchecked

/M-Series-@@(NUM)@@	
MAGES (2)	Ř
Image Device (1)	
Bootable Image cannot be deleted	i
Image	R
VM-Series-9.0.1-Base-KVM-Image	×Ŧ
Device Type 🔏 Device Bus	ズ
DISK × 🔻 SCSI	×v
Bootable	
Image Device (2)	٢
Image	ズ
Select	
Select Device Type 🧳 Device Bus	×

21. Modify the drop-down select for *Image Device (2)* to point to the *Bootstrap ISO* you imported earlier – **do not check** the checkbox next to *Bootable* – the ISO image is only used to provide configuration settings during the provisioning process – the VM never boots from the ISO image

The default values for VCPUs (4), Cores (1), and Memory (9 GB) are valid for a Palo Alto Networks VM-Series VM-100, VM-200, or VM-300 license.

(-/
VM-Series-9	.0.1-Base	-KVM-Image	×Ŧ
Device Type	Ř	Device Bus	X
DISK	×Ŧ	SCSI	×v
Bootable			
Image Devi	ce (2)		
Image			X
VM-Series B	ootstrap	.iso	×Ŧ
Device Type	Ř	Device Bus	Ř
CD-ROM	×	IDE	×Ŧ
Bootable			
PUs	Ň	Cores per vCPU	
PUs	×	Cores per vCPU	
PUs mory (GiB)	×	Cores per vCPU	•

- **NOTE**: If you intend to deploy another VM-Series license, please review the Palo Alto Networks VM-Series System Requirements documentation for the required resources:
- <u>https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/about-the-vm-series-firewall/vm-series</u>
 - 22. Leave the value for *network_function_provider: PaloAlto* blank

VGPUS	Ð
No vGPU is available on this cluster	
Categories	ţ
Ensure that SSH port (22) is open in the security policies of the selected categories.	
network_function_provider: PaloAlto	×
Key: Value	-

- 23. In the *Network Adapters* section, choose the *Network* as defined in the *Project* created earlier for *NIC1* (VM-Series management interface)
- **NOTE**: Do not configure a Static IP address the Nutanix Calm automation framework operates optimally when IP addresses are assigned via DHCP

	iron					
Ne an	twork d Run	Configurat	tion is nee ork.	ded for Ad	ctions	
Su se Ni	bnet o lected Cs.	only from fi . To change	rst NICs cli e the clust	uster can l er, remove	be e all the	
Clust	er: Ntr	nx-Cluster				
NIC	1				0	x
mg	ymt-ne	etwork			X	-
Stati						_
		ave	Sta	tic I	P	
NIC	2	eave Field	Sta d Bla	tic I ank	P	
NIC NIC	2 2 3	eave Field	Sta d Bla	tic I ank	P	
NIC NIC Egre	2 2 3 55	eave Field	Sta d Bla	tic l ank	P	
NIC Ingre NIC Egre	2 ess 3 ss	eave Field	Sta d Bla	tic I ank	P	
NIC NIC Egre NIC TAP	2 2 3 55 4	eave Field	Sta d Bla	tic l ank	P	

24. Do not uncheck the checkbox in the *Serial Ports* section – this will cause significant delays in the amount of time it takes for the VM-Series instances to boot

SE	RIAL PORTS (1)	e
0.	Connected	<u> </u>

25. It is not necessary to configure any additional settings as the default values are optimized for deployment in the majority of Nutanix customer's environments ***

SEF	RIAL PORTS (1))		Đ
0.	Connect	ed		1 ×
	nnection heck log-in up	oon cre	eate	
Cred	ential			
adı	min			×Ŧ
adı Addr	min ess			×▼
Addr NIC	min ess C 1			× •
Addr NIC Conr	min ess 21 nection Type	Ř	Connection Port	× • × •
Addr NIC Conr SSI	min ess C 1 H	<i>₹</i> × •	Connection Port	× • × •
Addr NIC Conr SSI	min ess C 1 ection Type H y (in seconds)	* × *	Connection Port 22 Retries	×* ×* *

*** in some rare cases where the Nutanix AHV cluster nodes operate at high utilization rates, it may be necessary to increase the default timeout value from 700 (seconds) to 800 or 900. Increasing the timeout value does not negatively affect the deployment of VM-Series in any way. It provides additional time for PAN-OS XML API programmatic functions to finish processing.

26. Scroll to back to the top and click Save



Deploy Palo Alto Networks VM-Series Application from Calm Blueprint

1. Once the settings for the Nutanix Calm Blueprint for Palo Alto Networks VM-Series save completely, click the *Launch* button



2. On the next screen, review the settings to ensure accuracy

≡	Q Calm *
X	Palo Alto Networks - VM-Series - Calm Blueprint
•6	Name of the Application
	Palo Alto Networks VM-Series Application
١١	Application Profile
¢ ⁰	I AHV
ô	Profile Configuration
•	Palo Alto Networks VM-Series Count No of palo alto VMs to be provisioned in AHV cluster. 2
	IP Address of Panorama Provide IP of Panorama
	10.3.6.97
	Username for Panorama API Administrator Credential used to make api operations for panorama configuration nutanixadmin
	Password for Panorama API Administrator Credential used to make api operations for panorama configuration
	11311 O
	Device Group for Palo Alto VMs Device group created on panorama for palo alto VMs
	Nutanix_Device_Group
	Template for Palo Alto VMs
?	Cancel

3. Confirm the password for the delegated Administrator account



4. Click the Create button to deploy VM-Series

Microsegment_Zone		
Virtual wir e for Palo Alto VMs		
Virtual wire created on panorama for palo alto VMs		
Nutanix_vWire		
	Cancol	Cront

5. You can switch to the Manage tab to follow along with the process



	Q. Calm						🐥 💿 🗿 ? 🌣 admin 🗸
Â	Palo Alto Networks VM-Series Application						Delete ?
e(8	Overview • Manage • Services • /	Audit • ?					
	Status		Summary			Configuration	
IIA	PROVISIONING			On	0	Application UUID	eaa24e06-262b- 4593-80b5-47ade1dc1097
0 ⁰			0	O Busy	0	Blueprint	Palo Alto Networks - VM-Series -
A	Project Paio Alto N	letworks VM-Series Deployment	→	Error	0	Application Profile	AHV
	Owner	admin		Off Off	0	Cloud	×
	Variables						
	Palo Alto Networks VM-Series Count ①						Сору
	IP Address of Panorama () 10.3.6.97						Сору
	Username for Panorama API Administra nutanixadmin	tor 🕕					Сору
							•



I Pri	sm Central X	🕡 techbd-panorama	× +			- 0	×
$\langle \boldsymbol{\leftarrow} \rangle$	\rightarrow C' $rac{1}{2}$	🛈 🔏 https://10	0.3.6.251:9440/console/#page/	/explore/calm/applications/eaa24e06-262b-4593-80b5-4	7 ☑ ☆	\$ ∥\ 🗊 இ	> ≡
	AC 🗎 JeffH Lab 🗎 Nutanix	🏓 AWS					
≡	Q. Calm				A 💿 O (🧿 ? 🌣 adm	
Â	Palo Alto Networks VM-Se	ries Application				Delete	?
•6	Overview • Manage	 Services Aud 	it • ?		STATED	IDDAVAL ITDA PW	
33	ScaleUp				Status	SUCCESS	^
IA	ScaleDown				CreateNFChain Finished - today a	at 11:08 PM	
ê	* Create	0			C CreateNFChain Finished - today	at 11:08 PM	
•	Start				ConfigurePanar Finished - today a	'oma at 11:08 PM	
	C Restart			PaloAltoVM	ConfigurePanar	oma ± at 11:10 PM ±	
	X Delete			Create	PaloAlto Create Finished - today at 11:12	2.PM	
	>_ Soft Delete			Package Install	Started	today at 11:10 PM SUCCESS	
				PaloAlto Create PaloAlto Start	ConfigureFirew Finished - today a	all ± at 11:12 PM ±	
				Create	ConfigureFirew	all ± at 11:12 PM	
?				reate Deployment	PS PaloAlto Start Finished - today at 11:12	≥PM ¥	~
	오 🛱 📜 🛓	£ 😢 🌖			0 🖞 🛟 🖩	⑧ 記 dッ) 11:25 PM 9/5/2019	Q

Verify PAN-OS XML API Configuration Settings

Switch to the Panorama Web UI to verify Nutanix Calm provisioned the following settings:

• VM-Series are Registered (Managed Devices -> Summary)

malaalta			DE DE	VICE GROUPS	TEM					
	Dashboard	ACC Mo	nitor Policie	s Objects	Network	Device P	anorama	📥 Comm	it 👻 💣 😡 Config	- Search
Context Panorama									Manual 🦷	🖌 🖸 🕜 Help
😡 Setup 🔹 🔺	۹.								3	2 items 🔿 🙁
High Availability			IP A	ldress						
Managed WildFire Clusters	Tags	Serial Number	IPV4	IPV6	Variables	Template	Device State	HA Status	Shared Policy	Template
Reserved Profiles	Shared > Nutanix_De	evice_Group								
Admin Roles		007054000072	10.3.6.94 (DHCP)		Create	Nutanix_Templa	Connected		In Sync	In sync
Authentication Profile		007054000072	10.3.6.91 (DHCP)		Create	Nutanix_Templa	Connected		O In Sync	O In sync

• Device Group is provisioned

😺 Setup 🔹	~ 🔍						
High Availability							
Na Config Audit		Name 📥	Description	Authorization Code	SW Version	Master Device	Devices/Virtual System
Managed WildFire Clusters							
📲 Managed WildFire Appliances		▼					
Password Profiles			Device group added from calm				PA-VM, PA-VM
Admin Roles		Nucanix_Device_di					
Access Domain							
🔞 Authentication Profile							
Authentication Sequence							
User Identification							
V 📼 Managed Devices							
Summary •							
🔤 Health							
🄀 Troubleshooting							
Templates							
Device Groups 🔹	4						
-Managad Collectors							

• Template and Template Stack are provisioned



Verify VM-Series Virtual Machines Provisioning

Switch to the VM-Series Web UI for each instance deployed to verify the following:

• Licenses activated

PA-VM		AutoFocus Device Licen	se
Date Issued Se Date Expires N Description St	eptember 05, 2019 ever tandard VM-100	Date Issued Date Expires Description	September 05, 2019 February 11, 2026 AutoFocus Device License
DNS Security			
Date Issued Se Date Expires Ju Description Pa	eptember 05, 2019 uly 30, 2020 alo Alto Networks DNS Security License	GlobalProtect Gateway Date Issued	September 05, 2019
PAN-DB URL Filtering Date Issued Se Date Expires Ju Description Pa	eptember 05, 2019 Jly 30, 2020 alo Alto Networks URL Filtering License	Description	GlobalProtect Gateway License
ACTIVE Y	es	Premium Date Issued	September 05, 2019
Threat Prevention Date Issued Se Date Expires Ju Description Th	eptember 05, 2019 uly 30, 2020 hreat Prevention	Date Expires Description	July 30, 2020 24 x 7 phone support; advanced replacement hardware service
License Management Retrieve license keys from I Activate feature using auth Manually upload license key Deactivate VM Upgrade VM capacity	license server norization code r	WildFire License Date Issued Date Expires Description	September 05, 2019 July 30, 2020 WildFire signature feed, integrated WildFire logs, WildFire API

• Virtual Wire

paloalto		Dashboard	ACC	Monitor	Policies Obje	ots Network	Device
Interfaces M Zones	• •	Name		Interface1	Interface2	Tag /	Allowed
Par Virtual Wires Virtual Routers PSec Tunnels GRE Tunnels DHCP DNS Proxy ColobalProtect	•	Nutanix_vWire	٩	ethernet1/1	ethernet1/2	2 0-409	94

• Security Zone

NETWORKS®	Dashboard	ACC	Monitor	Policies	Objects	Network	Device	
🚥 Interfaces								
M Zones								
😼 VLANs 🔁 Virtual Wires 🍄 Virtual Routers	Name	Туре	Interfac System	es / Virtual	Zone Protection Profile	Packet Buffer Protection	Log Setting	Er
@ IPSec Tunnels ⋘ GRE Tunnels] Microsegment_Zo	virtual-wire	etherne	t1/1				
			etherne	t1/2				

• Network Interfaces

paloalto	Dashboard	ACC Mon	tor Policies	Objec	ts Network	Device		📥 Commit 🧉	🕼 Config 👻 🔍 Search
									😒 🔞 Help
Interfaces M Zones	Ethernet VLAN	Loopback Tun	nel						
VLANs									24 items 🔿 🗶
Virtual Routers	Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual- Wire	Security Zone
GRE Tunnels	🚥 ethemet1/1 👒	Virtual Wire			none	none	Untagged	Nutanix_vWire	Microsegment_Zone ^
DHCP	🗰 ethernet1/2 🛛 🥹	Virtual Wire			none	none	Untagged	Nutanix_vWire	Microsegment_Zone
V S GlobalProtect	ethernet1/3			6	none	none	Untagged	none	none
Portale	mm othernot1/4			(ill)	none	none	Untanged	none	none

Apply Microsegmentation Policy via Nutanix Flow and VM-Series

Nutanix provides a framework whereby traffic between virtual machines can be redirected through Nutanix Flow for traditional traffic enforcement via an integrated firewall that processes traffic at layer-4 based on source/destination port and protocol.

For customers that want to reap the benefits of Palo Alto Networks Next-Generation Firewall, deploying VM-Series on Nutanix AHV with the Calm Blueprint automatically creates a Service Chain. The Service Chain allows customers to transparently redirect traffic at the Virtual NIC driver layer to VM-Series for low latency packet redirection to Palo Alto Networks' industry-leading application layer firewall.

Applying Application and Category objects to your applications allows the administrator to quickly and easily control traffic flows between workloads. In the following example, we secure a two-tier deployment of WordPress. The tiers are separated into a web tier and a database tier. The WordPress front-end web and application server are deployed on one Virtual Machine while the MySQL database is deployed on another Virtual Machine.

An Application object is defined to represent WordPress as an application (*AppType: WordPress*) and is further divided into two categories – the web tier (*AppTier: web*) and the database tier (*AppTier: db*). The Application object and Category objects are applied to the two Virtual Machines.

	d • Category 🔄	X		
< Back to VMs	VM	1	Categories	2
VM	WordPress Web Frontend	VM	AppType: WordPress	
WordPress	1 m			
Web Frontend			AppTier: web	
Cluster: Ntnx-Cluster				
Summary				
Console				
Recovery Points				
Snapshots				
Alerts				
Events				
Metrics ~				
NICs				
Disks				
Categories				

	ckend ► Category 👘	Х		4
< Back to VMs	VM	1	Categories	2
WordPross	WordPress Database Backend	VM	AppType: WordPress	
Database			AppTier: db	
Backend				
Cluster: Ntnx-Cluster	Ļ			
Summary				
Console				
Recovery Points				
Snapshots				
Alerts			ß	
Events				
Metrics ~				
NICs				
Disks				
Categories				

We create a Security Policy in Nutanix Flow to quickly and easily apply a Microsegmentation policy to control the east/west traffic flows between the WordPress web application server and the WordPress database server.

- 1. Navigate to *Policies -> Security Policies*
- 2. Click Create a Security Policy and choose Secure an Application

	*	×	A 3 0 3
Security Policies	Create Security Policy Type name Secure an Application Total Secure Isolate Environments		
	Name Purpose Quarantine Inspect VMs in C	Policy Quarantined No VMs	Status

3. Provide a *Name* and *Description* for the new security policy, then choose *App Type: WordPress* in the drop-down select, then click *Next*

1	Define Policy	2 Secure Applicatio	n 3 Review
An	app security pol	icy segments an app type	category and only
and		becine devices on the net	WOIK.
Word	dPress-Microseg	mentation	
Purpose	e		
Man	age traffic flows	between web tier and dat	abase tier
Secure	e this app 🕜		
App	Type: WordPress	5	

4. Since we already have a Palo Alto Networks Next-Generation Firewall securing the north/south traffic at the perimeter, select the *Whitelist Only* drop-down select and choose *Allow All*

	Create App Security Policy						
< Back	(1	Define Policy 2 Secure Application 3	Review	View Policy Model Next	>		
Inbound Deny all Incon No inbound rules hav	Whitelist Only ^ Allow All Whitelist Only	AppType WordPress AppType WordPress 2VA Set rules on App Tiers, instead	Outbound	Allow All			
All inbound traffic s + Add S	will be blocked.						

5. In the center column, select Set Rules on App Tiers instead



6. Click + Add Tier

Create App Security Policy							
< Back	1 Defin	Policy 2 Secure Application 3	Review	View Policy Model	Next >		
Inbound All Sources	Allow All	AppType WordPress	Outbound All Destinations	Allow All •			

7. Select App Tier: web

	Create App Security Policy	? ×
4 Back	Define Policy Secure Application 3 Review	View Policy Model Next >
Inbound Allow All -	AppType WordPress	Outbound Allow All -

8. Click + Add Tier and select App Tier: db

				Create App Security Policy				? X
< Back			1 Defir	ne Policy 2 Secure Application	3 Review		View Policy Model	Next >
	Inbound All Sources	Allow All	•	AppType WordPress AppTier web VMs in this tier can talk to each other Select a Tier Select a Tier AppTier : Default AppTier : ob AppTier : db	TVMs 	Outbound All Destinations	Allow All ~	

9. Select Set Rules within App

Create App Security Policy							
< Back		1	Define Policy 2 Secure	Application 3 Review		View Policy Model	Next >
			Set Rules to & from App	Set Rules within App			
	Inbound	Allow All	AppType W	ordPress	Outbound	Allow All	
	All Sources		AppTier web VMs in this tier can talk	1VMs to each other	All Destinations		
			AppTier db	1VMs			
			VMs in this tier can talk	to each other			

10. Click on the rectangle representing *AppTier: web* to select it – a blue outline will appear

			Create App Security F	Policy			? ×
< Back		(1)	Define Policy 2 Secure Applica	ation 3 Review		View Policy Model	Next >
			Set Rules to & from App Set	Rules within App			
	Inbound All Sources	Allow All	AppType WordPre	ss tvMs h other ?	Outbound All Destinations	Allow All	
			AppTier db VMs in this tier can talk to each	1VMs • other			

11. Click the + sign on the right side of AppTier: db

Create App Security Policy							
< Back		1 Define Policy 2 Secure Application 3 Review	View Policy Model Next >				
		Set Rules to & from App Set Rules within App					
	Inbound Allow All	AppType WordPress Outbound	Allow All				
	All Sources	AppTier web TVMs All Destinations Can VMs in this tier talk to each other ? •					
		AppTier db TVMs					
		VMs in this tier can talk to each other					

12. In the Create Tier to Tier Rule that appears, enter the TCP/UDP/ICMP traffic flows to redirect to VM-Series via the *Service Chain*, check the box next to *Redirect through a service chain*, and then select *PANOS_CHAIN* in the drop-down select

AppTie	r web		Aj	opTier db	
Specify the	protoco	l details for	this rule	+ Add	Port/Protoc
PROTOCOL		PORTS	TYPE	CODE	ACTION
TCP	•	3306			×
ICMP	~		Any	Any	×
Redirect	through	a service c	hain		
PANO	S CHAI	N			,

In this rule, both MySQL (3306/tcp) and all ICMP traffic is redirected to VM-Series

13. Click *Save* to add the rule

		Create App Security Policy	?
< Back		Define Policy Secure Application ③ Review View Policy Model	Next
		Set Rules to & from App Set Rules within App	
Inbound	Allow All	AppType WordPress Outbound Allow A	All
All Source	25	AppTier web 1VMs Can VMs in this tier talk to each other ? Yes No	
		AppTer db TVMs VMs in this tier can talk to each other	

14. Click Next

15. Choose either *Save and Monitor*, or if you are ready to enforce the new *Tier to Tier* rule with VM-Series, simply click *Apply Now*

					• • • •	? 🌣 admin ~
Security Policies 2 Total Security Policies	Create Security F					T Filters
	Type name to filter by					
	2 Total Secur	rity Policies				1-2 of 2 < >
	Name Purpose			Policy	Status	Last Modified
	0 Q	uarantine Inspect	VMs in Quarantin	Quarantined No VMs	Applied	4 month
	0 w	ordPres Manage	traffic flows betw	All Sources AppType WordPress All Destination	Monitoring	few seco

16. Switch to the VM-Series firewall *Monitor* tab for the appropriate firewall – or if you have centralized logging configured in Panorama, view the *Traffic* logs on the *Monitor* tab within the Panorama admin interface

Deploy Additional VM-Series via Calm Scale Out

As your workloads scale up, so does the number of Nutanix AHV cluster nodes in your environment. The Nutanix scale-out capability provides a method for administrators to add additional VM-Series instances to an existing deployment with only a few clicks.

The following example builds upon the two VM-Series instances we deployed to a Nutanix AHV cluster. To increase the scalability of the environment, we will leverage the Nutanix Calm Scale Up action to add an additional two instances of VM-Series across the AHV cluster.

- Q Calm x Applications

 Brownfield Applications . Im Type here to apply filters 111 2 Total Applications 00 NAME SOURCE BLUEPRINT STATE ô Palo Alto Networks - VM-Series - Calm Palo Alto Networks VM-Series Application Running Blueprint
- 1. Navigate to Calm -> Applications

2. Open the Palo Alto Networks VM-Series Application

≡	Q. Calm			
×	Applications			
0(<mark>0</mark>				
	Q Type here to apply filters			
II\				
00	2 Total Applications		DINT STATE	OWNER
Ô	Dalo Alto Networks VM Socies Application	Palo Alto Net	works - VM-Series - Calm	admin
-	Pato And Networks VM-Series Application	Blueprint	Kunning	aumin

3. Select the Manage tab



4. Click the > in the *ScaleUp* pane



5. Modify the SCALEOUT_COUNT to reflect the total number of additional VM-Series instances to deploy

≡	Q Calm						
â	Palo Alto Networks VM-Serie	es Application					
-6	Overview • Manage	 Services	it » ?				
88	ScaleUp		Run Action	: ScaleUp		:	× eate
IK	>_ ScaleDown		SCALEOU	T_COUNT			
00	Create	0					-
Ô	Start					Run Cancel	
	C Restart			8	PaloAltoVM		> (
	Stop				PaloAlto		> (s

6. Click Run

≡	Q Calm			🐥 💿 🔘 🌒 🕈 admi
â	Palo Aito Networks VM-Series A	pplication		Delete
(Overview • Manage •	Services • Audit • ?		· Run By admin
88	ScaleUp 1 Instances running			Status RUNNING
ih	>_ ScaleDown			s ScaleOut
¢ ⁰	* Create	\odot		PaloAlto - Substrate Pre Create
Ô	Start			Finished - today at 1:57 AM Started today at 1:56 AM
-	C Restart		🔀 PaloAltoVM	Stotus SUCCESS
	Stop		PaloAlto	G GenerateNumber Finished - today at 1:56 AM
	Delete		ScaleUp	G GenerateNumber Finished - today at 1:56 AM
	Soft Delete		ScaleUp	Sc PaloAlto - Substrate Create Last Updated At -today at 1:57 AM
			ScaleOut	Started today at 1:57 AM Status RUNNING
2				PN Last Updated At - today at 157 AM PN PaloAltoVM - Provision Nutanix PN Last Updated At - today at 157 AM
1				No new noti

That's it! Nutanix Calm will automatically:

- Provision the desired number of additional VM-Series instances
- Automate licensing of the additional VM-Series appliances
- Subscribe the newly created instances to the same Panorama server
- Add the new instances to the same Panorama Device Group, Template, and Template Stack as the existing instances
- Automatically commit the configuration
- Modify the *Service Chain* to allow traffic to be seamlessly redirected to the newly deployed VM-Series instances

Troubleshooting Resources & Documentation

Nutanix

- <u>Nutanix Flow Tech Note</u>
- <u>Nutanix Calm Reference Architecture</u>
- <u>Nutanix Support Portal</u>
- Blueprints Management Nutanix Support Portal
- Blueprints Usage Nutanix Support Portal
- <u>Nutanix: Network Microsegmentation Demo YouTube</u>
- Tech TopX: Datacenter Security with Flow

Palo Alto Networks

- Palo Alto Networks Support Site
- <u>Create a Support Account VM-Series Deployment Guide</u>
- License the VM-Series Firewall VM-Series Deployment Guide
- <u>Activate the License VM-Series Deployment Guide</u>
- Bootstrap the VM-Series Firewall VM-Series Deployment Guide
- <u>Generate the VM Auth Key on Panorama VM-Series Deployment Guide</u>
- Prepare the Licenses for Bootstrapping VM-Series Deployment Guide
- Create the init-cfg.txt File VM-Series Deployment Guide
- Prepare the Bootstrap Package VM-Series Deployment Guide
- Panorama Administrative Roles Panorama Administrator's Guide

Knowledge Base Articles

- How to Authorize and Install VM-Series Auth Codes Knowledge Base
 - * Valid support credentials required

Videos

- VM-Series Deployment: Bootstrapping Basics YouTube
 - * While this video refers to AWS/Azure/GCP, it is applicable to deploying on Nutanix as well

Technical Details

Nutanix

- Nutanix REST API Overview
- Nutanix Developer Portal
- How to create service chain using REST API

Nutanix API Calls

Get List of Existing Clusters

https://{{host}}:9440/api/nutanix/v3/clusters/list

Create a New Network Function Chain

https://{{host}}:9440/api/nutanix/v3/network_function_chains

Get a List of Existing Network Function Chains

https://{{host}}:9440/api/nutanix/v3/network_function_chains/list

Palo Alto Networks

● PAN-OS[®] and Panorama[™] API Guide

PAN-OS and Panorama API Calls

Generate API Key

https://{{host}}/api?type=keygen&user=admin&password=admin

Configure Devices

https://{{host}}/api/?type=config&action=get&xpath=/config/devices

Create Panorama Device Group

https://{{host}}/config/devices/entry[@name='localhost.localdomain']/device-group/entry[@name ='@@{Panorama_DeviceGroup}@@'

Create Panorama Template

https://{{host}}/config/devices/entry[@name='localhost.localdomain']/template/entry[@name='@@
{Panorama_Template}@@']

Create Template Stack

https://{{host}}/config/devices/entry[@name='localhost.localdomain']/template-stack/entry[@na me='@@{Panorama_TemplateStack}@@']

Configure Network Interfaces via Template

https://{{host}}/config/devices/entry[@name='localhost.localdomain']/template/entry[@name='@@
{Panorama_Template}@@']/config/devices/entry[@name='localhost.localdomain']/network/interface
/ethernet/entry

Create Virtual Wire

https://{{host}}/config/devices/entry[@name='localhost.localdomain']/network/virtual-wire/ent ry[@name='@@{Panorama_Vwire}@@']

Create Security Zone

https://{{host}}/config/devices/entry[@name='localhost.localdomain']/template/entry[@name='@@
{Panorama_Template}@@']/config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/zone/entry[@name='@@{Panorama_Zone}@@']

Add Template Variable

```
https://{{host}}/api?key={{key}}&type=config&action=set&xpath=/config/devices/entry[@name='lo
calhost.localdomain']/vsys/entry[@name='vsys1']
```

Commit Changes

https://{{host}}/api?key={{key}}&type=commit&cmd=<commit></commit>

Activate Licenses

https://api.paloaltonetworks.com/api/license/activate?uuid={{uuid}}&cpuid={{cpuid}}&authCode= {{authcode}}&serialNumber={{serialnumber}}

Show Device Licenses

https://{{host}}/api?key={{key}}&type=op&cmd=<request><batch><license><info></info></license></batch></request>