

在雲端和本地部署 CN-Series 防火牆

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters: Palo Alto Networks 3000 Tannery Way Santa Clara, CA 95054 www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc. www.paloaltonetworks.com

© 2021-2021 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

December 13, 2021

Table of Contents

在 GKE 上部署 CN-Series 防火牆	5
在 GKE 上部署 CN-Series 防火牆作為 Kubernetes 服務	6
在 GKE 上部署 CN-Series 防火牆作為 DaemonSet	19
在 OKE 上部署 CN-Series 防火牆	31
在 OKE 上部署 CN-Series 防火牆作為 Kubernetes 服務	32
在 OKE 上將 CN-Series 防火牆部署為 DaemonSet	44
在 EKS 上部署 CN-Series 防火牆	55
在 AWS EKS 上部署 CN-Series 防火牆作為 Kubernetes 服務	56
在 AWS EKS 上部署 CN-Series 防火牆作為 Daemonset	65
從 AWS Marketplace 部署 CN-Series	74
在 AliCloud (ACK) 上部署 CN-Series 防火牆作為 Kubernetes 服	
務	81
在 OpenShift 上部署 CN-Series	103
在 OpenShift Operator 中樞上部署 CN-Series	105



在 GKE 上部署 CN-Series 防火牆

我可以在哪裡使用這個?	我需要哪些內容?
• CN-Series 部署	• CN-Series 10.1.x or above Container Images
	• Panorama 執行 PAN-OS 10.1.x 或更高版本
	• Helm 3.6 or above version client 用於使用 Helm 進行 CN-Series 部署

在您檢閱 CN 系列建置區塊以及使用 CN 系列保護 Kubernetes 環境中的工作流程高階概觀之後,就可以在 GKE 平台上開始部署 CN-Series 防火牆來保護相同叢集內容器之間的流量,以及容器與其他工作負載類型之間的流量(例如虛擬機器和裸機伺服器)。



您需要 kubectl 或 Helm 這類標準 Kubernetes 工具來部署和管理 Kubernetes 叢集、應用 程式和防火牆服務。

如需詳細資訊,請參閱使用 Helm 圖表和範本部署 CN-Series 防火牆。Panorama 未設計成進行 Kubernetes 叢集部署和管理的協調器。進行叢集管理的範本是由「受管理 Kubernetes 提供者」所提供。Palo Alto Networks 提供社群支援的範本,以利用 Helm 和 Terraform 來部署 CN-Series。

- 在 GKE 上部署 CN-Series 防火牆作為 Kubernetes 服務
- 在 GKE 上部署 CN-Series 防火牆作為 DaemonSet



從部署「CN-Series 作為 DaemonSet」移到「CN-Series 作為服務」之前(反之亦 然),您必須刪除並重新套用 plugin-serviceaccount.yaml。如需詳細資訊, 請參閱建立用於叢集驗證的服務帳戶。

- 當您在 GKE 上部署 CN-Series 作為 DaemonSet 時, pan-plugin-clustermode-secret 不得存在。
- 當您在 GKE 上部署 CN-Series 作為 Kubernetes 服務時, 必須要有 pan-plugincluster-mode-secret。

在 GKE 上部署 CN-Series 防火牆作為 Kubernetes 服務

我可以在哪裡使用這個?	我需要哪些內容?
• CN-Series 部署	 CN-Series 10.1.x or above Container Images Denorma 執行 DANLOS 10.1.x 或更直版本
	 Panorama 執行 PAN-OS 10.1.X 或更高版本 Helm 3.6 or above version client 用於使用 Helm 進行 CN-Series 部署

完成下列程序,以在 GKE 平台上部署 CN-Series 防火牆作為 Kubernetes 服務:

STEP 1 | 設定 Kubernetes 叢集。

若要在 GKE 中建立叢集,請執行下列動作:

1. 按一下導覽功能表,並移至 **Kubernetes Engine**(**Kubernetes** 引擎),然後選取 **clusters**(叢 集)。

=	Google Cloud Platf	orm	🕈 gcp-pavmqa 👻			Q Se	arch products and r	resources		~				
A	Home	>	ubernetes clus	ters	CREATE 🖬 🖬	DEPLOY CREFRESH	DELETE							
PINN	ED													
-	Billing		•	Introduci	ng Autopilot n	node					×			
Θ	IAM & Admin	>	•	including node	es and node pools. ter modes	ni experience, when you cre	ate a cluster in Autopin	or mode, boogle pro	rsions and manages	ane entre cluster's underlying initiasouco	ure,			
API	APIs & Services	>	•	🗸 Get a proc	✓ Get a production-ready cluster based on your workload requirements									
È	Marketplace			 Eliminate Pay per P 	Eliminate the overhead of node management A Pay one Pod only for the resources that you use									
۲	Compute Engine	>		 Increase : Gain high 	security with Google b er workload availabilit	est practices built-in y								
	Cloud Storage	>												
11	VPC network	>		TRY THE DEM	LEARN MORE									
}≽	Cloud Run													
\$	SQL		OVERVIEW	COST OPTIMI	IZATION PREVIEW									
٦	Kubernetes Engine	>	= Filter Enter pr	operty name or	value					Ø				
~			Clusters	ime 个	Location	Number of nodes	Total vCPUs	Total memory	Notifications	Labels				
Q	BigQuery	>	Workloads	uster	us-central I-c	U	U	0 GB	unschedulable	-	:			
ALL F	RODUCTS 🗸		Services & Ingress Applications	oud-init- ak-cluster1	us-east1-c	0	0	0 GB	A Pods unschedulable	-	:			
			Configuration	oud-	us-central1-c	0	0	0 GB	A Pods	-	:			
			Storage	ak2					Node					
			Object Browser						upgrade available					
			Migrate to containers	-cnseries-2	us-west2-a	3	24	96 GB	E Low	-	:			
			g-management						requests					

- **2.** 按一下 Create (建立)。
- **3.** 選取 GKE Standard (GKE 標準) 作為您要使用的叢集模式, 然後按一下 Configure (設定)。

← → C ☆ console.cloud	d.google.com/kubernet Google Cloud Search	es/list/overview? Style & Writing Gi	project=gcp-pavmqa&isC ui 🛷 Firewall as a Platfo	reateAndRegister=fals	e co 💶 Containerizatio	1 Ex 🥠 PAN E	SP Homepag 🔀	Lab & Firewall Res	o 🔀 2021-07-21 Meetin	🔀 Dashi	ooard - Conflu	AEM STAGING	\$	*
	n 🔹 gcp-pavmqa 👻			Q Sea	rch products and res	purces			~			-	. 0	
Kubernetes Engine	Kubernetes clu	usters	CREATE E DEPLO	VY CREFRESH	DELETE							S OPERATION	is ≠	HIDE
⊕ Clusters		Introduci	ng Autonilat mad							×	No clu	usters selected		
Workloads A Services & Ingress	•	An optimized including nod Compare clus	cluster with a hands-off exp es and node pools. Iter modes	e serience. When you crea	te a cluster in Autopilot r	tode, Google prov	risions and manage	es the entire cluste	r's underlying infrastructure,	~	Labels F env:proc	nelp organize your resourd d). <u>Learn more</u>	ces (e.g., o	ost_ce
Applications Configuration	•	✓ Get a pror ✓ Eliminate	duction-ready cluster based	Create clus	ster						0	No clusters selected		
Storage		 Pay per P Increase r 	od, only for the resources t security with Google best p	Select the cluster m	node that you want to use									
0 Object Browser		🗸 Gain high	er workload availability	 Compar 	re cluster modes to learn	more about their	differences.	COMPARE						
Migrate to containers Config Management		TRY THE DEM	IEARN MORE	GKE Standard A Kubernetes cluste Learn more	er where you configure a	nd manage your n	odes.	CONFIGURE						
	OVERVIEW	COST OPTIM	ZATION PREVIEW	GKE Autopilot			televal -							
	Tilter Enter	property name or	value	configuration requir	red. Learn more	our nodes with m	Inimal	CONFIGURE	0					
	Status	Name Chandra-gke- cluster	Location us-central1-c					CANCEL		:				
	0 0	cloud-init- soak-cluster1	us-east1-c			_	unschedulable	GARGEE		:				
		cloud- integration- soak2	us-central1-c	0	0	0 GB	Pods unschedulable			:				
常 Marketplace		hs-cnseries-2	us-west2-a	3	24	96 GB	Low resource requests	-		:				
 Release notes 		k8s-plugin-	us-west2-a	0	0	0 GB	A Pods	-		:				

4. 輸入 [Name (名稱)]、[Version (版本)]、[Location (位置)]、[Node subnet (節點子網路)]這類叢集基本資訊,然後按一下 Create (建立)。

\equiv Google Cloud Platform	Search products	and
 Create a Kubernetes clust 	ADD NODE POOL 🖀 REMOVE NODE POOL	
 Create a Kubernetes clust Cluster basics NODE POOLS default-pool CLUSTER Automation Networking Some form fields are incorrect Security Metadata Features 	er ADD NODE POOL Image: REMOVE NODE POOL Cluster basics The new cluster will be created with the name, version, and in the location you specify here. After the cluster is created, name and location can't be changed. Image: Cluster Description of the cluster is created, name and location can't be changed. Image: Cluster Description of the cluster is created, name and location can't be changed. Image: Cluster Description of the cluster is created, name and location can't be changed. Image: Cluster Description of the cluster is created, name and location can't be changed. Image: Cluster Description of the cluster is created, name and location can't be changed. Image: Cluster Description of the cluster is created, name and location can't be changed. Image: Cluster Description of the cluster is created, name and location can't be cluster. Image: Cluster Description of the cluster is created, name and location can't be cluster. Image: Cluster Description of the cluster is created, name and location can't be cluster. Image: Cluster Description of the cluster is created. Image: Clusterescluster.	
	Release channel • Regular channel (default) • Version • 1.20.10-gke.301 (default) •	
	CREATE CAN	CEL

如果您的叢集位於 GKE 上,則請務必讓 Kubernetes Network Policy API 允許叢 集管理員指定允許彼此通訊的 Pod。需要此 API, CN-NGFW 與 CN-MGMT Pod 才能通訊。

CPU platform and GPU			
Auto-upgrade: On	~	Create a Kubernetes cluster	
More options			
			Networking
			VFC native
+ Add node pool			
			Network
Enable Cloud Run for Anthos			one i
			Node subnet ill
			default (10.128.0.0/20)
Availability, networking, security, and additional features			Z Automatically create secondary ranges
0	·		Pod address more (Cational)
			Exemple: 10.96.0.0/14
			Maximum pods per node (Optional) (()
			Mask for Pod address range per node: /24
			Service address range (Colling)
			Example: 10.94.0.0/18
			Enable Internade visibility Reveals your internade visibility Reveals your internade traffic to Goog vis networking tables. To get logs, to enable VPC flow logs in the selected submework.
			Loed balancing
			Enable HTTP load balancing. (i)
			Network accurity
			- Private causile: @

1. 請驗證叢集具有足夠的版本。預設 GKE 節點集區規格不適用於 CN-Series 防火牆。您必 須確保叢集具有 CN-Series 先決條件資源以支援防火牆:

kubectl get nodes

kubectl describe node <node-name>

檢視命令輸出之「容量」標題下的資訊,以查看所指定節點上可用的 CPU 和記憶體。 CPU、記憶體和磁碟儲存體配置將取決於您的需求。請參閱 CN-Series 效能和調整規模。 確保您具有下列資訊:

• 收集「端點 IP 位址」,以在 Panorama 上設定 API 伺服器。

cluster Dennit	ion			(
	Name	on_prem-clstr		
	Description			
API s	erver address	10.2.		
	Туре	Native-Kuberne	tes	
Cri	edentials			
Label Calastan	Label City	n I Curtury (Contra to	
Label Selector	Label Filte	er Custom (Certificate	
				Oitoms) > >
Q				$\circ \text{items} \rightarrow >$
C C TAG PREFIX	NAMES	PACE	LABEL SELECTOR FILTER	
C TAG PREFIX	NAMES	PACE	LABEL SELECTOR FILTER	
Q	NAMES	PACE	LABEL SELECTOR FILTER	
Q	NAMES	PACE	LABEL SELECTOR FILTER	
Q	NAMES	PACE	LABEL SELECTOR FILTER	
Q	NAMES	PACE	LABEL SELECTOR FILTER	
C TAG PREFIX	NAMES	PACE	LABEL SELECTOR FILTER	
C C C C C C C C C C C C C C C C C C C	NAMES	PACE	LABEL SELECTOR FILTER	

Panorama 使用此 IP 位址來連線至 Kubernetes 叢集。

• 從 Panorama 收集範本堆疊名稱、裝置群組名稱、Panorama IP 位址和日誌收集器群組 名稱(選用)。

Collector Group	Θ
General Monitoring	Device Log Forwarding Collector Log Forwarding Log Ingestion
Name	rp-cg1
Log Storage	Total: 1.53 TB,Free: 75:30 GB
Min Retention Period (days)	[1 - 2000]
Collector Group Members	Q(1item) → X
	rpgcpnew(RPGOOGGKEPRA1)
- 9	
	Add ⊖ Delete
	Enable log redundancy across collectors
	Forward to all collectors in the preference list
	Enable secure inter LC Communication Log collector on local panorama is using the secure client configuration from 'Panorama -> Secure Communication Settings'
	OK Cancel

如需詳細資訊,請參閱建立父系裝置群組和範本堆疊。

- 收集授權碼以及自動註冊 PIN ID 和值。
- 將映像檔下載至其中的容器映像檔儲存庫位置。
- STEP 2| (選用)如果您已在 Panorama 的 Kubernetes 外掛程式中設定自訂憑證,則必須執行下列命令 來建立憑證密碼。請不要從 ca.crt 變更檔案名稱。pan-cn-mgmt.yaml 和 pan-cn-ngfw.yaml 中的 自定憑證數量是選用項目。

kubectl -n kube-system create secret generic custom-ca --fromfile=ca.crt

STEP 3| 编輯 YAML 檔案,以提供部署 CN-Series 防火牆所需的詳細資料。

apiVersion: v1
kind: ConfigMap
metadata:
name: pan-mgmt-config
namespace: kube-system
data:
PAN_OPERATION_MODE: "daemonset"
PAN_SERVICE_NAME: "pan-mgmt"
Panorama settings
PAN_PANORAMA_IP: "35.196.181.54"
PAN_PANORAMA_AUTH_KEY:
PAN_DEVICE_GROUP: "dev-dg"
PAN_TEMPLATE: "k8s-stack"
#Non-mandatory parameters
PAN_PANORAMA_CGNAME: "rp-cg1"
#PAN_CERTIFICATE: ""
#PAN_CERTKEYFILE: ""
#PAN CERTPASSPHRASE: ""

您必須確定 YAML 檔案上的 PAN_PANORAMA_IP 參數值符合您的實際 Panorama IP 位址,如下 圖所示:

VM-PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE PANORAMA Panorama	6
Panorama V [©] Access Domain [©] Authentication Profile [©] Authentication Sequence [©] MAME [©] DSCRIPTION TYPE STACK DEVICES VARIABLES DEVICE KEY-1 Manage. [©] Data Redistribution [©] Data Redistribution [©] Data Redistribution [©] Manage. Manage. Manage. No Devices	• ₽ ₹
Image: Constraint of the sequence of the sequen	E
Mathemiciation Profile NAME DESCRIPTION TYPE STACK DEVICES VARIABLES DEVICE KEY-1 Manage Authemiciation Sequence K85-Network-Setup Implate Implate Manage Manage DEVICE KEY-1 Discription K85-Network-Setup Implate Implate K85-Network-Setup Manage No Devices Managed Devices Managed Devices Manage No Device State No Device State No Device State	2 items
Authentication Sequence K85-Network-Setup template Manage Duser Identification K85-Network-Setup template Manage Duser Identification K85-Network-Setup Manage No Devices in template Duser Quarantine Managed Devices Manage No Device in template	ALUE TA
Image: Construction Image: Construction Imag	
arg Data Redistribution k8s-stack template-stack K8S-Network-Setup Manage No Devices in Device Quarantine Managed Devices	
[⊘] Device Quarantine	e stack
Managed Devices	
Tamplatas	
Provide Contract of Contract o	
Construction of the second sec	
Concess Googles -	
Certificates	
Certificate Profile	
☆ SSL/TLS Service Profile	
La scep	
SSH Service Profile	
R Log Ingestion Profile	
Ca Log Settings	
P Server Profiles	
P SNMP Trap	
P Systog	
Re Email	
पाम छी	
là radius	
LD SCP	

您必須確定 YAML 檔案上 PAN_DEVICE_GROUP 和 PAN_TEMPLATE 的參數值符合您在 Panorama 上建立的裝置群組和範本堆疊名稱,如下圖所示:

← → C ▲ Not Secure 3	35.19	6.181.54/#panor	rama::dev-do	g::panorama/dev	ce-groups					© ☆	0 6	6
······································	D/	ASHBOARD	ACC	MONITOR	C Device	Groups – OBJECTS	r T NETWO	remplates n RK DEVICE	PANORAMA		≟ ∗ ໃ	∎ ₽₹
Panorama 🗸												E
Access Domain	Q											2 items
Authentication Frome		NAME 🛋		DESCRIPTIO	N	AUT	HORIZATION E	SW VERSION	MASTER DEVICE	DEVICES/VIRTUAL SYSTEM	RI	EFEREN
Data Redistribution		G Shared										
Device Quarantine		🕞 der	v-dg								k	3s-stack
Certificate Profile SELTLS Service Profile												
C Log Ingestion Profile C Log Settings C Syslog C Syslog E Email C HTTP C RADIUS C SCP												

您必須確定 PAN_PANORAMA_CG_NAME 的參數值與您建立的日誌收集器名稱相同。

	DASHBOAR		MONITOR			C Templat		PANORAMA	±, ∿
Panorama		Acc	MONITOR	r o ercito	0002013	MENIFORK	DEVICE	TARORAMA	
C Access Domain									
20 Authentication Profile	Q								1
Authentication Sequence	NAME		REDUI	NDANCY ENABLE	D FOR	WARD TO ALL COL	LECTORS	COLLECTORS	LOG REDISTRIBUTIO
User Identification	rp-cg1							demo-panorama	none
Data Redistribution									
B Device Quarantine									
Managed Devices									
Templates									
Device Groups									
Managed Collectors									
Collector Groups									
Certificate Management									
Certificates									
Certificate Profile									
C SSL/TLS Service Profile	-								
SCEP									
SSH Service Profile									
Log Ingestion Profile									
Log Settings									
Server Profiles									
SNMP Trap									
Syslog									
Email									
HTTP									
RADIUS									
Disce									

如需詳細資訊,請參閱 CN-Series 部署 yaml 檔案中的可編輯參數以取得詳細資料。

STEP 4| 如果您在 Kubernetes 環境中使用自動調整規模,請參閱啟用水平 Pod 調整規模。

STEP 5| 部署 CN-NGFW 服務。執行下列步驟:



部署為 Kubernetes 服務時,可以將 CN-NGFW 執行個體部署在安全性節點上,並將應用程式 Pod 流量重新導向至可用的 CN-NGFW 執行個體以進行檢查和強制執行。



- 請驗證您已使用 pan-cni-serviceaccount.yaml 來建立服務帳戶。
 請參閱建立叢集驗證的服務帳戶。
- 2. 使用 Kubectl 來執行 pan-cni-configmap.yaml。



STEP 6 | 部署 CN-MGMT StatefulSet。

-xrc2z

管理平面預設會部署為可提供容錯的 StatefulSet。最多可以將 30 個防火牆 CN-NGFW Pod 連線 至 CN-MGMT StatefulSet。

- 1. (僅為靜態佈建 PV 的必要項目) 部署 CN-MGMT StatefulSet 的「永久性磁碟區 (PV)」。
 - 1. 建立目錄,以符合 pan-cn-pv-local.yaml 中所定義的本機磁碟區名稱。

您需要至少2個背景工作節點上有六(6)個目錄。請登入將部署 CN-MGMT StatefulSet 以建立目錄的每個背景工作節點。例如,若要建立名為/mnt/pan-local1到/mnt/pan-local6 的目錄,請使用命令:

Running

2m12s

mkdir -p /mnt/pan-local1 /mnt/pan-local2 /mnt/pan-local3 /
mnt/pan-local4 /mnt/pan-local5 /mnt/pan-local6

2. 修改 pan-cn-pv-local.yaml。

符合 nodeaffinity 下方的主機名稱,並驗證您已修改上面您在 spec.local.path 中建立的目錄,然後部署檔案來建立新的 storageclass pan-local-storage 和本機 PV。

2. 驗證您已修改 pan-cn-mgmt-configmap 和 pan-cn-mgmt YAML 檔案

EKS 中的範例 pan-cn-mgmt-configmap。

apiVersion: v1 kind:ConfigMap metadata: name: pan-mgmtconfig namespace: kube-system data:PAN_SERVICE_NAME: pan-mgmt-svc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama settings PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP: "<panorama-device-group>" PAN_TEMPLATE_STACK: "<panoramatemplate-stack>" PAN_CGNAME: "<panorama-collectorgroup>" # ctnr mode: "k8s-service", "k8s-ilbservice"

PAN CTNR MODE TYPE: "k8s-service" #Non-mandatory parameters # Recommended to have same name as the cluster name provided in Panorama Kubernetes plugin - helps with easier identification of pods if managing multiple clusters with same Panorama #CLUSTER NAME: "<Cluster name>" #PAN PANORAMA IP2: "" # Comment out to use CERTs otherwise PSK for IPSec between pan-mgmt and pan-ngfw #IPSEC_CERT_BYPASS: "" # No values needed # Override auto-detect of jumbo-frame mode and force enable system-wide #PAN JUMBO FRAME ENABLED: "true" # Start MGMT pod with GTP enabled.For complete functionality, need GTP # enable at Panorama as well. #PAN GTP ENABLED: "true" # Enable high feature capacities. These need high memory for MGMT pod and # higher/matching memory than specified below for NGFW pod. #PAN NGFW MEMORY="6Gi" #PAN NGFW MEMORY="40Gi" # For enabling faster datapath -AF XDP, default is AF PACKETV2. This requires kernel support. #PAN DATA MODE: "next-gen" #HPA params #PAN CLOUD: "EKS #PAN NAMESPACE EKS: "EKSNamespace" #PUSH INTERVAL: "15" #time interval to publish metrics to AWS cloudwatch

範例 pan-cn-mgmt.yaml

initContainers: - name: pan-mgmt-init image: <your-privateregistry-image-path>

containers: - name: pan-mgmt image: <your-private-registryimage-path> terminationMessagePolicy:FallbackToLogsOnError

3. 使用 Kubectl 來執行 yaml 檔案。

kubectl apply -f pan-cn-mgmt-configmap.yaml kubectl apply -f pan-cn-mgmt-slot-crd.yaml kubectl apply -f pan-cn-mgmt-slot-cr.yaml kubectl apply -f pan-cn-mgmt-secret.yaml kubectl apply -f pan-cn-mgmt.yaml

只有在您先前尚未完成建立叢集驗證的服務帳戶時,才必須執行 pan-mgmt-serviceaccount.yaml。

4. 執行下列命令,驗證已啟動 CN-MGMT Pod:

kubectl get pods -l app=pan-mgmt -n kube-system

這需要大約 5-6 分鐘。

STEP 7| 部署 CN-NGFW Pod。

1. 驗證您已修改 PAN-CN-NGFW-CONFIGMAP 和 PAN-CN-NGFW 中詳述的 YAML 檔案。

containers: - name: pan-ngfw-container image: <your-privateregistry-image-path>

2. 使用 Kubectl apply 來執行 pan-cn-ngfw-configmap.yaml。

kubectl apply -f pan-cn-ngfw-configmap.yaml

3. 使用 Kubectl apply 來執行 pan-cn-ngfw.yaml。

kubectl apply -f pan-cn-ngfw.yaml

4. 驗證 CN-NGFW Pod 正在執行。

kubectl get pods -n kube-system -l app=pan-ngfw -o wide

- STEP 8| 執行下列步驟,以啟用水平 Pod 自動調整規模:
 - 1. 在 CN-Series 叢集中部署自訂度量堆疊驅動程式介面卡。叢集名稱必須透過 K8s 密碼提供。
 - 2. 從 Palo Alto Networks GitHub 儲存庫,下載 GKE 特有 HPA yaml 檔案。
 - 3. 如果您的 CN-MGMT 部署在自訂命名空間中,則請使用自訂命名空間來更新 pan-cn-adapater.yaml。預設命名空間是 kube-system。
 - 4. 更新 GKE 特定 pan-cn-mgmt-configmap.yaml 中的 HPA 參數。

#PAN CLOUD: "GKE"

#HPA_NAME: 「<name>」**#**用於識別每個命名空間或每個租用戶的 HPA 資源的唯一 名稱

#PUSH INTERVAL: [15] **#**將度量發佈到 Starckdriver 的時間間隔

- 使用 HPA_NAME(取代為名稱)來修改 pan-cn-hpa-dp.yaml 和 pan-cn-hpamp.yaml(如上述 pan-cn-mgmt-configmap.yaml 檔案中所更新),並根據應該觸發的 HPA 來更新度量。
 - 1. 輸入最小和最大複本數目。
 - **2.** (選用)變更縮減和擴充頻率值,以符合您的部署。如果您未變更這些值,則會使用 預設值。
 - **3.** (選用)變更您要用於調整規模之每個度量的臨界值。如果您未變更這些值,則會使用預設值。
 - 4. 儲存變更。
- 6. 部署 HPA yaml 檔案。檔案必須依下面所述的順序進行部署。
 - 1. 使用 Kubectl 來執行 pan-cn-adapter.yaml

kubectl apply -f pan-cn-adapter.yaml

2. 使用 Kubectl 來執行 pan-cn-crole.yaml

kubectl apply -f pan-cn-crole.yaml

3. 使用 Kubectl 來執行 pan-cn-hpa-dp.yaml

kubectl apply -f pan-cn-hpa-dp.yaml

4. 使用 Kubectl 來執行 pan-cn-hpa-mp.yaml

kubectl apply -f pan-cn-hpa-mp.yaml

- 7. 驗證您的部署。
 - 使用 kubectl 來確認自訂度量命名空間中的自訂度量介面卡 Pod。

kubectl get pods -n custom-metrics

• 使用 kubectl 檢查 HPA 資源。

kubectl get hpa -n kube-system

kubectl describe hpa <hpa-name> -n kube-system

如需詳細資訊,請參閱在 CN-Series 上啟用水準 Pod 自動縮放。

STEP 9| 驗證您可以在 Kubernetes 叢集上看到 CN-MGMT、CN-NGFW 和 PAN-CNI。

kubectl -n kube-system get pods

STEP 10 | 標註應用程式 yaml 或命名空間, 讓來自其新 Pod 的流量重新導向至防火牆。

您需要新增下列註釋,以將流量重新導向至 CN-NGFW 來進行檢查:

annotations: paloaltonetworks.com/firewall: pan-fw

例如,對於「default」命名空間中的所有新 Pod:

kubectl annotate namespace default paloaltonetworks.com/ firewall=pan-fw



在部分平台上, pan-cni 在 CNI 外掛程式鏈中未作用時,可以啟動應用程式 Pod。 若要避免這類情況,您必須在應用程式 Pod YAML 中指定這裡顯示的磁碟區。

volumes: - name: pan-cni-ready hostPath: path: /var/log/ pan-appinfo/pan-cni-ready type:Directory

STEP 11 | 在叢集中部署應用程式。

在 GKE 上部署 CN-Series 防火牆作為 DaemonSet

我可以在哪裡使用這個?	我需要哪些內容?
• CN-Series 部署	• CN-Series 10.1.x or above Container Images
	• Panorama 執行 PAN-OS 10.1.x 或更高版本
	• Helm 3.6 or above version client 用於使用 Helm 進行 CN-Series 部署

完成下列程序,以在 GKE 平台上部署 CN-Series 防火牆作為 Daemonset:

STEP1| 設定 Kubernetes 叢集。

若要在 GKE 中建立叢集,請執行下列動作:

1. 按一下導覽功能表,並移至 **Kubernetes Engine**(**Kubernetes** 引擎),然後選取 **clusters**(叢 集)。

=	Google Cloud Plat	form	🗣 gcp-pavmqa 👻			Q Se	arch products and r	esources			~	
ŵ	Home	>	ubernetes clus	ters	CREATE 🖬 🖬	DEPLOY CREFRESH	DELETE					
PINN	ED											
	Billing		•	Introduci	ng Autopilot n	node						×
Θ	IAM & Admin	>	• 🚓	including node	cluster with a hands-c is and node pools. ter modes	nt experience, when you cre	ate a cluster in Autopie	ot mode, Google prov	isions and manages	the entire cluster's under	iying intrastructure	
API	APIs & Services	>	•	🗸 Get a proc	duction-ready cluster I	based on your workload requ	irements					
Ŷ	Marketplace			 Eliminate Pay per P 	the overhead of node od, only for the resour	management ces that you use						
۲	Compute Engine	>		 Increase : Gain high 	security with Google b er workload availabilit	est practices built-in y						
	Cloud Storage	>										
11	VPC network	>		TRY THE DEM	LEARN MORE							
)≽	Cloud Run											
\$	SQL		OVERVIEW	COST OPTIMI	ZATION PREVIEW							
٢	Kubernetes Engine	>	E Filter Enter pr	operty name or v	Location	Number of podec	Total vCPI is	Total memory	Notifications	Labele	v	
Q,	BigQuery	>	Workloads	andra-gke- uster	us-central1-c	0	0	0 GB	A Pods unschedulable	-		:
ALL F	RODUCTS 🗸		Services & Ingress Applications	oud-init- ak-cluster1	us-east1-c	0	0	0 GB	A Pods unschedulable	-		:
			Configuration	oud- legration-	us-central1-c	0	0	0 GB	A Pods unschedulable	-		:
			Object Browser	ak2					Node upgrade available			
			Migrate to containers Config Management	-cnseries-2	us-west2-a	3	24	96 GB	Low resource resource	-		:

- **2.** 按一下 Create (建立)。
- **3.** 選取 GKE Standard (GKE 標準) 作為您要使用的叢集模式, 然後按一下 Configure (設定)。

← → C ☆ console.clour	d.google.com/kubernet Google Cloud Search	es/list/overview? Style & Writing G	project=gcp-pavmqa&is0 ui 🛷 Firewall as a Platfo	reateAndRegister=false	a 💶 Containerization	Ex 🥠 PAN E	SP Homepag 🔀	Lab & Firewall Re	so 🞽 2021-07-21 Meetin.	🞽 Dashb	ioard - Conflu 🚦	AEM STAGING	\$	*
	n 🔹 gcp-pavmqa 👻			Q Sear	ch products and reso	ources			~			-	. 0	٠
Kubernetes Engine	Kubernetes clu	usters	CREATE 🖬 DEPLI	DY CREFRESH	T DELETE							😵 OPERATIO	INS 👻	HIDE
⊕ Clusters		Introduc	ng Autonilot mod	•						×	No clust	ters selected		
Services & Ingress	•	An optimized including nod Compare clus	cluster with a hands-off ex es and node pools. Iter modes	e perience. When you creat	e a cluster in Autopilot n	ode, Google pro	isions and manages	s the entire cluste	er's underlying infrastructure,		Labels help env:prod). (organize your resou Learn more	rces (e.g., c	cost_ce
Applications Configuration	•	✓ Get a pro	duction-ready cluster base	Create clus	ter						0	No clusters selected	1	
Storage		 Pay per F Increase 	od, only for the resources t security with Google best p	h Select the cluster m	ode that you want to use									
Collect Browser		🗸 Gain high	er workload availability	Compare	cluster modes to learn	more about their	differences.	COMPARE						
Migrate to containers Onfig Management		TRY THE DE	IEARN MORE	GKE Standard A Kubernetes cluste Learn more	where you configure ar	d manage your n	odes.	ONFIGURE						
	OVERVIEW	COST OPTIM	ZATION PREVIEW	GKE Autopilot										
	Tilter Enter	property name or	value	configuration require	d. Learn more	our nodes with m	o	ONFIGURE	0					
	Status	Name 🕇	Location											
	00	chandra-gke- cluster	us-central1-c					CANCEL		•				
		cloud-init- soak-cluster1	us-east1-c				unschedulable			:				
		cloud- integration- soak2	us-central1-c	0	0	0 GB	A Pods unschedulable			:				
W Marketplace		hs-cnseries-2	us-west2-a	3	24	96 GB	Eow resource requests	-		:				
 Reference nuclés 		k8s-plugin-	us-west2-a	0	0	0 GB	A Pods	-		:				

4. 輸入 [Name (名稱)]、[Version (版本)]、[Location (位置)]、[Node subnet (節點子網路)]這類叢集基本資訊,然後按一下 Create (建立)。

≡	Google Cloud Platform	se gop	p-pavmqa 🔻		
÷	Create a Kubernetes clust	er	ADD NODE POOL		
•	Cluster basics		Cluster basics		
NODE	real	~	The new cluster will be created with the name, version, and in the here. After the cluster is created, name and location can't be cha	e locatio nged.	n you specify
CLUS	TER	Ť	To experiment with an affordable cluster, try My first set-up guides	cluster	in the Cluster
0	Networking Some form fields are incorrect		Name cluster-1		9
•	Security		Location type		
٠	Metadata		Regional		
٠	Features		Zoneus-central1-c		• 0
			Specify default node locations O Current default. us-central1-c Control plane version		
			Choose a release channel for automatic management of your cluster's cadence. Choose a static version for more direct management of your more.	s version r cluster	and upgrade s version. <u>Learn</u>
			O Static version		
			Release channel		
			Release channel Regular channel (default)		•
			Version 1.20.10-gke.301 (default)		•
					CREATE CANCEL

 如果您的叢集位於 GKE 上,則請務必讓 Kubernetes Network Policy API 允許叢集管 理員指定允許彼此通訊的 Pod。需要此 API, CN-NGFW 與 CN-MGMT Pod 才能通 訊。

CPU platform and GPU	
Auto-upgrade: On	 Create a Kubernetes cluster
More options	
	Networking
	VPC native
+ Add node pool	Enable VPC native (using alias IP) (i)
	Network ()
	default
Enable Cloud Run for Anthos ②	Noda subert
	default (10.128.0.0/20)
Availability networking security and additional feature	195
	Automatically create secondary ranges
	Pod address range (Optional) 💮
	Exemple: 10.96.0.0/14
	Maximum pods per node (2010011)
	110
	Mask for Pod address range per node: /24
	Service oddress range (Opticma)
	Example: 10.94.0.0/18
	Enable Internede visibility
	Reveals your intranode traffic to Googie's networking fabric to evaluate the first sector of the sec
	to endee vincing in the exercise scone work.
	Even balancing
	(e) share the constraint of
	Network accurity

請驗證叢集具有足夠的版本。確保叢集具有 CN-Series 系統需求以支援防火牆。

kubectl get nodes

kubectl describe node <node-name>

檢視命令輸出之「容量」標題下的資訊,以查看所指定節點上可用的 CPU 和記憶體。 CPU、記憶體和磁碟儲存體配置將取決於您的需求。請參閱 CN-Series 效能和可擴充性。 確保您具有下列資訊:

• 收集「端點 IP 位址」,以在 Panorama 上設定 API 伺服器。

Cluster Definition					0
	Name	on_prem-clstr			
Des	cription				
API server	address	10.2.			
	Туре	Native-Kubernet	es		\sim
Credentials					
Label Selector La	bel Filte	er Custom C	ertificate		
Q					0 items \rightarrow \times
TAG PREFIX	NAMES	PACE	LABEL SELECTOR FILTER		APPLY ON
🕀 Add 🕞 Delete					
Validate					OK Cancel

Panorama 使用此 IP 位址來連線至 Kubernetes 叢集。

如需詳細資訊,請參閱設定用於監視叢集的 Kubernetes 外掛程式。

• 從 Panorama 收集範本堆疊名稱、裝置群組名稱、Panorama IP 位址和日誌收集器群組名稱 (選用)。

Collector Group	0
General Monitoring	Device Log Forwarding Collector Log Forwarding Log Ingestion
Name	rp-cg1
Log Storage	Total: 1.53 TB,Free: 75.30 GB
Min Retention Period (days)	[1 - 2000]
Collector Group Members	Q(1item)→X
	COLLECTORS
	rpgcpnew(RPGOOGGKEPRA1)
	Enable log redundancy across collectors
	Forward to all collectors in the preference list
	Enable secure inter LC Communication Log collector on local panorama is using the secure client configuration from 'Panorama -> Secure Communication Settings'
	OK Cancel

如需詳細資訊,請參閱建立父系裝置群組和範本堆疊。

- 收集授權碼以及自動註冊 PIN ID 和值。
- 將映像檔下載至其中的容器映像檔儲存庫位置。
- STEP 2| (選用)如果您已在 Panorama 的 Kubernetes 外掛程式中設定自訂憑證,則必須執行下列命令 來建立憑證密碼。請不要從 ca.crt 變更檔案名稱。pan-cn-mgmt.yaml 和 pan-cn-ngfw.yaml 中的 自定憑證數量是選用項目。

kubectl -n kube-system create secret generic custom-ca --fromfile=ca.crt

STEP 3| 编輯 YAML 檔案,以提供部署 CN-Series 防火牆所需的詳細資料。

您需要取代 YAML 檔案中的映像路徑以包括私人 Google Container 登錄的路徑,以及提供必要 參數。請參閱 CN-Series 部署 yaml 檔案中的可編輯參數以取得詳細資料。

STEP 4| 部署 CNI DaemonSet。

CNI 容器部署為 DaemonSet(一個節點一個 Pod),而且它會在節點上所部署之每個應用程式的 CN-NGFW Pod 上建立兩個執行個體。當您使用 kubectl 命令來執行 pan-cni YAML 檔案時,它會變成每個節點上服務鏈的一部分。

- 1. CN-Series 防火牆需要三個「服務」帳戶,而這些帳戶具有授權它與 Kubernetes 叢集資源 通訊的最小權限。您應該建立為 CN-Series 叢集身分驗證建立建立服務帳戶,並驗證是否 已使用 pan-cni-serviceaccount.yaml 建立服務帳戶。
- 2. 使用 Kubectl 來執行 pan-cni-configmap.yaml。

kubectl apply -f pan-cni-configmap.yaml

3. 使用 Kubectl 來執行 pan-cni.yaml。

kubectl apply -f pan-cni.yaml

- 4. 請驗證您已修改 pan-cni-configmap 和 pan-cni YAML 檔案。
- 5. 執行下列命令, 並確認您的輸出與下列範例相似。

@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke	(vi	eries-mktplace) \$	kubectl get pods	-n kube-system	grep pan-cni
pan-cni-nmqkf		Running 0	2m11s		
pan-cni-wjrkq		Running 0	2m11s		
pan-cni-xrc2z		Running 0	2m12s		
<pre>@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke</pre>	(v	eries-mktplace)\$			

STEP 5| 部署 CN-MGMT StatefulSet。

管理平面預設會部署為可提供容錯的 StatefulSet。最多可以將 30 個防火牆 CN-NGFW Pod 連線 至 CN-MGMT StatefulSet。

1. 驗證您已修改 pan-cn-mgmt-configmap 和 pan-cn-mgmt YAML 檔案。

範例 pan-cn-mgmt-configmap

name: pan-mgmt-config

metadata:

namespace: kube-system

data:

PAN_SERVICE_NAME: pan-mgmt-svc

PAN_MGMT_SECRET: pan-mgmt-secret

Panorama settings

PAN_PANORAMA_IP: [x.y.z.a]

PAN_DEVICE_GROUP: [dg-1]

PAN_TEMPLATE_STACK: [temp-stack-1]

PAN_CGNAME: [CG-GKE]

非強制性參數

#建議與 Panorama Kubernetes 外掛程式中提供的叢集名稱具有相同的名稱 - 如果管理具有相同 Panorama 的多個叢集,則有助於更輕鬆地識別 Pod

#CLUSTER_NAME: [<Cluster name>]

#PAN PANORAMA IP2: ""

#註解使用 CERT, 除此以外 PSK 用於 pan-mgmt 和 pan-ngfw 之間的 IPSec

#IPSEC_CERT_BYPASS: ""

#不需要值

#取代 Jumbo 框架模式的自動偵測並強制啟用 systemwide#PAN_JUMBO_FRAME_ENABLED: "true"

#啟動啟用 GTP 的 MGMT Pod。若要獲得完整的功能,需要在 Panorama 上啟用 GTP。

在雲端和本地部署 CN共PAN GTP_ENABLED: "true" 26

©2024 Palo Alto Networks, Inc.

#啟用高功能容量。這些需要 MGMT Pod 的高記憶體和比以下為 NGFW Pod 指定更高/相符的記憶體。

範例 pan-cn-mgmt.yaml

initContainers:

- name: pan-mgmt-init

image: <your-private-registry-image-path>

containers: - name: pan-mgmt

image: <your-private-registry-image-path>

terminationMessagePolicy: FallbackToLogsOnError

2. 使用 Kubectl 來執行 yaml 檔案。

kubectl apply -f pan-cn-mgmt-configmap.yaml

kubectl apply -f pan-cn-mgmt-secret.yaml

kubectl apply -f pan-cn-mgmt.yaml

只有在您先前尚未完成建立叢集驗證的服務帳戶時,才必須執行 pan-mgmt-serviceaccount.yaml。

3. 驗證 CN-MGMT Pod 已啟動。

這需要大約 5-6 分鐘。

使用 kubectl get pods -l app=pan-mgmt -n kube-system NAME READY STATUS RESTARTS AGEpan-mgmt-sts-0 1/1 Running 0 27hpan-mgmt-sts-1 1/1 Running 0 27h

STEP 6| 部署 CN-NGFW Pod。

防火牆資料平面 CN-NGFW Pod 預設會部署為 DaemonSet。CN-NFGW Pod 執行個體可以保護節 點上最多 30 個應用程式 Pod 的流量。

1. 驗證您已修改 PAN-CN-NGFW-CONFIGMAP 和 PAN-CN-NGFW 中詳述的 YAML 檔案。

containers: - name: pan-ngfw-container image: <your-privateregistry-image-path>

2. 使用 Kubectl apply 來執行 pan-cn-ngfw-configmap.yaml。

kubectl apply -f pan-cn-ngfw-configmap.yaml

3. 使用 Kubectl apply 來執行 pan-cn-ngfw.yaml。

kubectl apply -f pan-cn-ngfw.yaml

4. 驗證所有 CN-NGFW Pod 都正在執行(叢集中一個節點會有一個 Pod)。

這是4節點內部部署叢集的範例輸出。

kubectl get pods -n kube-system -l app=pan-ngfw -o wide

NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES

pan-ngfw-ds-8g5xb 1/1 Running 0 27h 10.233.71.113 rk-k8-node-1
<none>

pan-ngfw-ds-qsrm6 1/1 Running 0 27h 10.233.115.189 rk-k8-vmworker-1 <none>

pan-ngfw-ds-vqk7z 1/1 Running 0 27h 10.233.118.208 rk-k8-vmworker-3 <none>

pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vmworker-2 <none> STEP 7 | 驗證您可以在 Kubernetes 叢集上看到 CN-MGMT、CN-NGFW 和 PAN-CNI。

kubectl -n kube-system get pods

- 0 27hpan-cni-5fhbg 1/1 Running
- 0 27hpan-cni-9j4rs 1/1 Running
- 0 27hpan-cni-ddwb4 1/1 Running
- 0 27hpan-cni-fwfrk 1/1 Running
- 0 27hpan-cni-h57lm 1/1 Running
- 0 27hpan-cni-h57lm 1/1 Running
- 0 27hpan-cni-j62rk 1/1 Running
- 0 27hpan-cni-lmxdz 1/1 Running
- 0 27hpan-mgmt-sts-0 1/1 Running
- 0 27hpan-mgmt-sts-1 1/1 Running
- 0 27hpan-ngfw-ds-8g5xb 1/1 Running
- 27hpan-ngfw-ds-qsrm6 1/1 Running
- 0 27hpan-ngfw-ds-vqk7z 1/1 Running
- 0 27hpan-ngfw-ds-zncqg 1/1 Running
- STEP 8 標註應用程式 yaml 或命名空間, 讓來自其新 Pod 的流量重新導向至防火牆。

您需要新增下列註釋,以將流量重新導向至 CN-NGFW 來進行檢查:

annotations: paloaltonetworks.com/firewall: pan-fw

例如,對於「default」命名空間中的所有新 Pod:

kubectl annotate namespace default paloaltonetworks.com/ firewall=pan-fw

在部分平台上, pan-cni 在 CNI 外掛程式鏈中未作用時,可以啟動應用程式 Pod。
 若要避免這類情況,您必須在應用程式 Pod YAML 中指定這裡顯示的磁碟區。

volumes: - name: pan-cni-ready hostPath: path: /var/log/ pan-appinfo/pan-cni-ready type:Directory

STEP 9 在叢集中部署應用程式。

在 OKE 上部署 CN-Series 防火牆

我可以在哪裡使用這個?	我需要哪些內容?
• CN-Series 部署	• CN-Series 10.1.x or above Container Images
	• Panorama 執行 PAN-OS 10.1.x 或更高版本
	• Helm 3.6 or above version client 用於使用 Helm 進行 CN-Series 部署

Oracle Kubernetes Engine (OKE) 是一種 OCI 服務,可讓您部署 kubernetes 叢集。您現在可以在 OKE 叢集上部署 CN-Series 防火牆以作為 Daemonset,並將 Kubernetes 作為服務。

在您檢閱 CN 系列建置區塊以及使用 CN 系列保護 Kubernetes 環境中的工作流程高階概觀之後,就可以在 OKE 平台上開始部署 CN-Series 防火牆來保護相同叢集內容器之間的流量,以及容器與其他工作負載類型之間的流量(例如虛擬機器和裸機伺服器)。



您需要 kubectl 或 Helm 這類標準 Kubernetes 工具來部署和管理 Kubernetes 叢集、應用 程式和防火牆服務。

如需詳細資訊,請參閱使用 Helm 圖表和範本部署 CN-Series 防火牆。Panorama 未設計成進行 Kubernetes 叢集部署和管理的協調器。進行叢集管理的範本是由「受管理 Kubernetes 提供者」所提供。Palo Alto Networks 提供社群支援的範本,以利用 Helm 和 Terraform 來部署 CN-Series。

- 在 OKE 上部署 CN-Series 防火牆作為 Kubernetes 服務
- 在 OKE 上將 CN-Series 防火牆部署為 DaemonSet

從部署「CN-Series 作為 DaemonSet」移到「CN-Series 作為服務」之前(反之亦 然),您必須刪除並重新套用 plugin-serviceaccount.yaml。如需詳細資訊, 請參閱建立用於叢集驗證的服務帳戶。

- 當您在 OKE 上部署 CN-Series 作為 DaemonSet 時, pan-plugin-clustermode-secret 不得存在。
- 當您在 OKE 上部署 CN-Series 作為 Kubernetes 服務時,必須要有 pan-plugincluster-mode-secret。

在 OKE 上部署 CN-Series 防火牆作為 Kubernetes 服務

我可以在哪裡使用這個?	我需要哪些內容?
• CN-Series 部署	• CN-Series 10.1.x or above Container Images
	• Panorama 執行 PAN-OS 10.1.x 或更高版本
	• Helm 3.6 or above version client 用於使用 Helm 進行 CN-Series 部署

完成下列程序,以在 OKE 平台上部署 CN-Series 防火牆作為 Kubernetes 服務:



Oracle Linux 8.5 OS 是在 OKE 上部署 CN-Series 防火牆的唯一合格環境。

STEP 1| 設定 Kubernetes 叢集。

若要在 OKE 中建立叢集, 請執行下列動作:

1. 登入 Oracle Cloud Infrastructure。

CLE Cloud Infrastructure

SIGN IN
Signing in to cloud tenant:
Change tenant
Sign in with your Oracle Cloud Infrastructure credentials
USER NAME
PASSWORD
Sign In Forgot password?

- 2. 按一下導覽功能表,並移至 Under Solutions and Platform (在解決方案和平台下),然後按 一下 Developer Services (開發人員服務)。
- 3. 按一下 Kubernetes Clusters (Kubernetes 叢集)。
- 4. 選取區間,然後按一下 Create Cluster (建立叢集)。

RACLE Cloud

ſS	Cluster	rs <i>in</i> Tute	orial2 Compa	artmer	nt	
' S	() Cluste	rs Requirements	: Preparing for Container En	gine for Kuber	<u>netes</u>	
ре	Create Cluste	er		1		
ENT	Name	Status	Node Pools	VCN	Version	Cre
2 2			No clusters exist. Crea	ate one to get s	started.	
oot)/Tutorial2						



- **5.** 在 [Create Cluster (建立叢集)] 對話方塊中,按一下 Custom Create (自訂建立),然後 一下 Launch Workflow (啟動工作流程)。
- 6. 在 Create Cluster (建立叢集)頁面上, 輸入叢集 Name (名稱)和其他詳細資訊。
- 7. 按 Next (下一步),以檢閱您為新叢集輸入的詳細資訊。
- 8. 在 [Review (檢閱)] 頁面上, 按一下 Create Cluster (建立叢集)。

RACLE Cloud

er Creation

١V

Resourc	ces to be created				
Basic I	Information				
Cluster	Cluster Name: cluster1				
Compart	Compartment: Tutorial2				
Version:	Version: v1.18.10				
Netwo	rk				
Compart	ment: Tutorial2	Network Security Groups:	Not Enabled		
VCN Name:	oke-vcn-quick- cluster1-4baf5729a	Kubernetes API Private Endpoint:	Auto Assigned		
		Kubernetes API Public Endpoint:	Auto Assigned		
		Kubernetes CIDR Block: 1	0.96.0.0/16		

and Privacy Cookie Preferences

Copyright © 2019, Oracle and/or its

Q US West (Phoenix) ✓

1. 您必須確保叢集具有 CN-Series 先決條件資源以支援防火牆:

kubectl get nodes kubectl describe node <node-name> 檢視命令輸出之「容量」標題下的資訊,以查看所指定節點上可用的 CPU 和記憶體。 CPU、記憶體和磁碟儲存體配置將取決於您的需求。請參閱 CN-Series 效能和調整規模。 確保您具有下列資訊:

• 收集「端點 IP 位址」,以在 Panorama 上設定 API 伺服器。

Cluster Definition	ı				0	
	Name on_prem-clstr					
D	escription					
API serve	er address	10.2.				
	Туре	Native-Kubernetes ~				
Crede	ntials				Î.	
Label Selector	abel Filte	er Custom C	ertificate			
Q					$_{0 \text{ items}} \rightarrow \times$	
TAG PREFIX	NAMES	PACE	LABEL SELECTOR FILTER		APPLY ON	
+ Add - Delete						

Panorama 使用此 IP 位址來連線至 Kubernetes 叢集。

• 從 Panorama 收集範本堆疊名稱、裝置群組名稱、Panorama IP 位址和日誌收集器群組 名稱(選用)。

Collector Group	θ
General Monitoring	Device Log Forwarding Collector Log Forwarding Log Ingestion
Name	rp-cg1
Log Storage	Total: 1.53 TB,Free: 75.30 GB
Min Retention Period (days)	[1 - 2000]
Collector Group Members	Q(1item) → X
	COLLECTORS
	rpgcpnew(RPGOOGGKEPRA1)
6	
	(+) Add (-) Delete
	Forward to all collectors in the preference list
	Enable secure inter LC Communication Log collector on local panorama is using the secure client configuration from 'Panorama -> Secure Communication Settings'
	OK Cancel
如需詳細資訊,請參閱建立父系裝置群組和範本堆疊。

- 收集授權碼以及自動註冊 PIN ID 和值。
- 備妥可將映像下載至其中的容器映像儲存庫位置。
- STEP 2 (選用)如果您已在 Panorama 的 Kubernetes 外掛程式中設定自訂憑證,則必須執行下列命 令來建立憑證密碼。請不要從 ca.crt 變更檔案名稱。pan-cn-mgmt-dynamic-pv.yaml 和 pan-cnngfw.yaml 中的自訂憑證數量是選用項目。

kubectl -n kube-system create secret generic custom-ca --fromfile=ca.crt

STEP 3| 编輯 YAML 檔案,以提供部署 CN-Series 防火牆所需的詳細資料。

apiVersion: v1
kind: ConfigMap
metadata:
name: pan-mgmt-config
namespace: kube-system
data:
PAN_OPERATION_MODE: "daemonset"
PAN_SERVICE_NAME: "pan-mgmt"
Panorama settings
PAN_PANORAMA_IP: "35.196.181.54"
PAN_PANORAMA_AUTH_KEY:
PAN_DEVICE_GROUP: "dev-dg"
PAN_TEMPLATE: "k8s-stack"
#Non-mandatory parameters
PAN_PANORAMA_CGNAME: "rp-cg1"
#PAN_CERTIFICATE: ""
#PAN_CERTKEYFILE: ""
#PAN CERTPASSPHRASE: ""

您必須確定 YAML 檔案上的 PAN_PANORAMA_IP 參數值符合您的實際 Panorama IP 位址,如下 圖所示:

VM-PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE PANORAMA Panorama	6
Panorama V [©] Access Domain [©] Authentication Profile [©] Authentication Sequence [©] MAME [©] DSCRIPTION TYPE STACK DEVICES VARIABLES DEVICE KEY-1 Manage. [©] Data Redistribution [©] Data Redistribution [©] Data Redistribution [©] Manage. Manage. Manage. No Devices [©] Managed Devices Managed Devices Manage No Devices	⊡ ₽ ₽
Image: Constraint of the sequence of the sequen	E
Mathemiciation Profile NAME DESCRIPTION TYPE STACK DEVICES VARIABLES DEVICE KEY-1 Manage Authemiciation Sequence K85-Network-Setup Implate Implate Manage Manage DEVICE KEY-1 Discription K85-Network-Setup Implate Implate K85-Network-Setup Manage No Devices Managed Devices Managed Devices Manage No Device State No Device State No Device State	2 items
Authentication Sequence K85-Network-Setup template Manage Duser Identification K85-Network-Setup template Manage Duser Identification K85-Network-Setup Manage No Devices in template Duser Quarantine Managed Devices Manage No Device in template	ALUE TA
Image: Construction Image: Construction Imag	
arg Data Redistribution k8s-stack template-stack K8S-Network-Setup Manage No Devices in Device Quarantine Managed Devices	
[⊘] Device Quarantine	e stack
Managed Devices	
Tamplatas	
Provide Contract of Contract o	
Construction of the second sec	
Concess Googles -	
Certificates	
Certificate Profile	
☆ SSL/TLS Service Profile	
La scep	
SSH Service Profile	
R Log Ingestion Profile	
Ca Log Settings	
P Server Profiles	
P SNMP Trap	
P Systog	
Re Email	
पाम छी	
là radius	
LD SCP	

您必須確定 YAML 檔案上 PAN_DEVICE_GROUP 和 PAN_TEMPLATE 的參數值符合您在 Panorama 上建立的裝置群組和範本堆疊名稱,如下圖所示:

← → C ▲ Not Secure 3	85.196	6.181.54/#panor	rama::dev-dg:	:panorama/devi	ce-groups					Q \$	0 0	0 0
UM-PANORAMA	DA	ASHBOARD	ACC	MONITOR	C Device	Groups – OBJECTS	r T NETWO	emplates – RK DEVICE	PANORAMA		÷	œ 🗄
Panorama 🗸 🗸												E
C Access Domain	Q											2 items
Authentication Frome		NAME 🛋		DESCRIPTION	N	AU	THORIZATION	SW VERSION	MASTER DEVICE	DEVICES/VIRTUAL SYSTEM		REFEREN
Data Redistribution		G Shared										
B Device Quarantine		Ga de	v-dg									k8s-stack
Managed Devices Managed Devices Device Groups Managed Collectors Collector Groups Certificate Management Certificates Certificates Certificates Certificates SSL/TLS Service Profile SSL/TLS Service Profile SSLS Service Profile SSLS Service Profile Composition Profile Composition Profile SSLS Service Profile Composition Profi	-											
ER, Log Ingestion Profile Image: Log Settings Image: Server Profiles Image: System												
C) SCP												

您必須確定 PAN_PANORAMA_CG_NAME 的參數值與您建立的日誌收集器名稱相同。

				C Device	Groups n	r Templat	tes n		1 0
W PANORAMA	DASHBOARD	ACC	MONITOR	POLICIES	OBJECTS	NETWORK	DEVICE	PANORAMA	÷ .
Panorama 🗸 🗸									
C Access Domain	Q								1
Real Authentication Profile				DANCY FRANK			FOTOS	COLLECTORS	
Authentication Sequence	NAME		REDUN	DANCY ENABLES	FOR	WARD TO ALL COLL	LECTORS	COLLECTORS	LOG REDISTRIBUTIC
B User Identification	rp-cg1							demo-panorama	none
Data Redistribution									
lo Device Quarantine									
Managed Devices									
Templates									
E Device Groups									
Managed Collectors									
Collector Groups									
Certificate Management									
Certificates									
Certificate Profile									
SSL/TLS Service Profile	1								
SCEP									
SSH Service Profile									
Log Ingestion Profile									
Log Settings									
Server Profiles									
SNMP Trap									
Syslog									
Email									
The HTTP									
RADIUS									
Disce									

如需詳細資訊,請參閱 CN-Series 部署 yaml 檔案中的可編輯參數以取得詳細資料。

STEP 4| 部署 CN-NGFW 服務。執行下列步驟:



部署為 Kubernetes 服務時,可以將 CN-NGFW 執行個體部署在安全性節點上,並將應用程式 Pod 流量重新導向至可用的 CN-NGFW 執行個體以進行檢查和強制執行。

在 OKE 上將 CN-Series 防火牆部署為 Kubernetes 服務時,您可以使用 pan-cn-k8s-service 原生資料夾中的 yaml 檔案。



- 請驗證您已使用 pan-cni-serviceaccount.yaml 來建立服務帳戶。
 請參閱建立叢集驗證的服務帳戶。
- 2. 使用 Kubectl 來執行 pan-cni-configmap.yaml。

kubectl apply -f pan-cni-configmap.yaml

3. 使用 kubectl 來執行 pan-cn-ngfw-svc.yaml。

```
kubectl apply -f pan-cn-ngfw-svc.yaml
```



必須在 pan-cni.yaml 之前部署此 yaml。

4. 使用 Kubectl 來執行 pan-cni.yaml。

kubectl apply -f pan-cni.yaml

- 5. 請驗證您已修改 pan-cni-configmap 和 pan-cni YAML 檔案。
- 6. 執行下列命令, 並確認您的輸出與下列範例相似。

@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v	eries-mktplace)\$ k	kubectl get pods -r	n kube-system	grep pan-cni
<pre>pan-cni-nmqkf</pre>	Running 0	2m11s		
pan-cni-wjrkq	Running 0	2m11s		
pan-cni-xrc2z	Running 0	2m12s		
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v	eries-mktplace) \$			

STEP 5| 部署 CN-MGMT StatefulSet。

管理平面預設會部署為可提供容錯的 StatefulSet。最多可以將 30 個防火牆 CN-NGFW Pod 連線 至 CN-MGMT StatefulSet。

1. 驗證您已修改 pan-cn-mgmt-configmap 和 pan-cn-mgmt YAML 檔案。

OKE 中的範例 pan-cn-mgmt-configmap。

apiVersion: v1 kind:ConfigMap metadata: name: pan-mgmtconfig namespace: kube-system data:PAN_SERVICE_NAME: pan-mgmt-svc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama settings PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP: "<panorama-device-group>" PAN_TEMPLATE_STACK: "<panoramatemplate-stack>" PAN_CGNAME: "<panorama-collector-group>" PAN_CTNR_MODE_TYPE: "k8s-service" #Non-mandatory parameters # Recommended to have same name as the cluster name provided in Panorama Kubernetes plugin - helps with easier identification of pods if managing multiple clusters with same Panorama #CLUSTER_NAME: "<Cluster name>" #PAN_PANORAMA_IP2: "" # Comment out to use CERTs otherwise PSK for IPSec between panmgmt and pan-ngfw #IPSEC_CERT_BYPASS: "" # No values needed # Override auto-detect of jumbo-frame mode and force enable system-wide #PAN_JUMB0_FRAME_ENABLED: "true" # Start MGMT pod with GTP enabled.For complete functionality, need GTP # enable at Panorama as well. #PAN_GTP_ENABLED: "true" # Enable high feature capacities.這些需要 MGMT Pod 具有高記憶體,以及 # 下面 針對 NGFW Pod 所指定的較高/相符記憶體。# 請參照系統需求文件,以查看每個記 憶體設定檔所支援的最大支援 NGFW CPU 大小 #。#PAN_NGFW_MEMORY:"6.5Gi" #PAN_NGFW_MEMORY:"48Gi" #PAN_NGFW_MEMORY:"56Gi"

範例 pan-cn-mgmt-dynamic-pv.yaml

```
initContainers: - name: pan-mgmt-init image: <your-private-
registry-image-path> command: ["/usr/bin/pan_start.sh"]
imagePullPolicy:始終
```

containers: - name: pan-mgmt image: <your-private-registryimage-path> terminationMessagePolicy:FallbackToLogsOnError

2. 使用 Kubectl 來執行 yaml 檔案。

```
kubectl apply -f pan-cn-mgmt-configmap.yaml
kubectl apply -f pan-cn-mgmt-slot-crd.yaml
kubectl apply -f pan-cn-mgmt-slot-cr.yaml
kubectl apply -f pan-cn-mgmt-secret.yaml
kubectl apply -f pan-cn-mgmt-dynamic-pv.yaml
```

只有在您先前尚未完成建立叢集驗證的服務帳戶時,才必須執行 pan-mgmt-serviceaccount.yaml。

3. 執行下列命令,驗證已啟動 CN-MGMT Pod:

```
kubectl get pods -l app=pan-mgmt -n kube-system
```

這需要大約 5-6 分鐘。

STEP 6| 部署 CN-NGFW Pod。

1. 驗證您已修改 PAN-CN-NGFW-CONFIGMAP 和 PAN-CN-NGFW 中詳述的 YAML 檔案。

containers: - name: pan-ngfw-container image: <your-privateregistry-image-path>

2. 使用 Kubectl apply 來執行 pan-cn-ngfw-configmap.yaml。

kubectl apply -f pan-cn-ngfw-configmap.yaml

3. 使用 Kubectl apply 來執行 pan-cn-ngfw.yaml。

kubectl apply -f pan-cn-ngfw.yaml

4. 驗證 CN-NGFW Pod 正在執行。

kubectl get pods -n kube-system -l app=pan-ngfw -o wide

STEP 7 | 驗證您可以在 Kubernetes 叢集上看到 CN-MGMT、CN-NGFW 和 PAN-CNI。

kubectl -n kube-system get pods

STEP 8 標註應用程式 yaml 或命名空間, 讓來自其新 Pod 的流量重新導向至防火牆。

您需要新增下列註釋,以將流量重新導向至 CN-NGFW 來進行檢查:

annotations: paloaltonetworks.com/firewall: pan-fw

例如,對於「default」命名空間中的所有新 Pod:

kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw



在部分平台上, pan-cni 在 CNI 外掛程式鏈中未作用時,可以啟動應用程式 Pod。 若要避免這類情況,您必須在應用程式 Pod YAML 中指定這裡顯示的磁碟區。

volumes: - name: pan-cni-ready hostPath: path: /var/log/ pan-appinfo/pan-cni-ready type:Directory

STEP 9 在叢集中部署應用程式。

在 OKE 上將 CN-Series 防火牆部署為 DaemonSet

我可以在哪裡使用這個?	我需要哪些內容?
• CN-Series 部署	• CN-Series 10.2.x or above Container Images
	• Panorama 執行 PAN-OS 10.2.x 或更高版本
	• Helm 3.6 or above version client 用於使用 Helm 進行 CN-Series 部署

完成下列程序,以在 OKE 平台上將 CN-Series 防火牆部署為 Daemonset:



Oracle Linux 8.5 OS 是在 OKE 上部署 CN-Series 防火牆的唯一合格環境。

STEP 1| 設定 Kubernetes 叢集。

若要在 OKE 中建立叢集, 請執行下列動作:

1. 登入 Oracle Cloud Infrastructure。

CLE Cloud Infrastructure

SIGN IN
Signing in to cloud tenant:
Change tenant
Sign in with your Oracle Cloud Infrastructure credentials
USER NAME
PASSWORD
Sign In Forgot password?

- **2.** 按一下導覽功能表,並移至 Under Solutions and Platform (在解決方案和平台下),然後按 一下 Developer Services (開發人員服務)。
- 3. 按一下 Kubernetes Clusters (Kubernetes 叢集)。
- 4. 選取區間,然後按一下 Create Cluster (建立叢集)。

RACLE Cloud

ſS	Cluster	rs <i>in</i> Tute	orial2 Compa	artmer	nt	
' S	① Cluste	rs Requirements	: Preparing for Container En	gine for Kuber	<u>netes</u>	
ре	Create Cluste	er	1			
ENT	Name	Status	Node Pools	VCN	Version	Cre
2 2			No clusters exist. Crea	ate one to get s	started.	
oot)/Tutorial2						



- **5.** 在 [Create Cluster (建立叢集)] 對話方塊中,按一下 Custom Create (自訂建立),然後 一下 Launch Workflow (啟動工作流程)。
- 6. 在 Create Cluster (建立叢集)頁面上, 輸入叢集 Name (名稱)和其他詳細資訊。
- 7. 按 Next (下一步),以檢閱您為新叢集輸入的詳細資訊。
- 8. 在 [Review (檢閱)] 頁面上, 按一下 Create Cluster (建立叢集)。

RACLE Cloud

er Creation

Basic I	Information						
Cluster I	Name: cluster1						
Compart	Compartment: Tutorial2						
Version:	v1.18.10						
Netwo	rk						
Compart	ment: Tutorial2	Network Security Groups:	Not Enabled				
VCN Name:	oke-vcn-quick- cluster1-4baf5729a	Kubernetes API Private Endpoint:	Auto Assigned				
		Kubernetes API Public	Auto				
		Endpoint:	Assigned				
		Kubernetes CIDR Block: 1	0.96.0.0/16				

and Privacy Cookie Preferences

Copyright © 2019, Oracle and/or its

 \bigcirc US West (Phoenix) \checkmark

Ĵ



如果您的叢集位於 OKE 上,則請務必讓 Kubernetes Network Policy API 允許叢集管 理員指定允許彼此通訊的 Pod。需要此 API, CN-NGFW 與 CN-MGMT Pod 才能通訊。

CPU platform and GPU			
Auto-upgrade: On	÷	Create a Kubernetes cluster	
More options			Matamakian
			MC onthe
			Enable VPC native (using alias IP) (i)
+ Add node pool			Natural (I)
			default
Enable Cloud Run for Anthos			
			Noda subnet (i)
			default (10.128 0 0/20)
Availability, networking, security, and additional features			☑ Automatically create secondary ranges. ◎
			Pod address range (Optional)
			Exemple: 10.96.0.0/14
			Mazimum poda per node (Optional)
			110
			Mask for Pod address range per node: /24
			Service address range (Opticnal)
			Example: 10.94.0.0/18
			Enable Intransde visibility Reveals your intransde traffic to Goog Vis networking fabric. To get logs yo to enable VPC flow logs in the selected subnetwork.
			Load balanding
			Enable HTTP load balancing (ii)
			Network security
			Private cluster
			Frable master authorized networks

請驗證叢集具有足夠的版本。確定叢集具有 CN-Series 先決條件資源以支援防火牆。

kubectl get nodes

kubectl describe node <node-name>

檢視命令輸出之「容量」標題下的資訊,以查看所指定節點上可用的 CPU 和記憶體。 CPU、記憶體和磁碟儲存體配置將取決於您的需求。請參閱 CN-Series 的效能和可擴展性。 確保您具有下列資訊:

• 收集「端點 IP 位址」,以在 Panorama 上設定 API 伺服器。

Cluster Definition					?
	Name	on_prem-clstr			
Des	cription				
API server	address	10.2.			
	Туре	Native-Kubernet	es		\sim
Credent	tials				^
Label Selector La	bel Filte	er Custom C	ertificate		
Q.(0 items	$\rightarrow \times$
TAG PREFIX	NAMES	PACE	LABEL SELECTOR FILTER	APPLY ON	
🕂 Add 🕞 Delete					
Validate				ОК	Cancel

Panorama 使用此 IP 位址來連線至 Kubernetes 叢集。

如需詳細資訊,請參閱設定用於監視叢集的 Kubernetes 外掛程式。

• 從 Panorama 收集範本堆疊名稱、裝置群組名稱、Panorama IP 位址和日誌收集器群組名稱 (選用)。

Collector Group	0
General Monitoring	Device Log Forwarding Collector Log Forwarding Log Ingestion
Name	rp-cg1
Log Storage	Total: 1.53 TB,Free: 75.30 GB
Min Retention Period (days)	[1 - 2000]
Collector Group Members	Q(1item)→X
	COLLECTORS
	rpgcpnew(RPGOOGGKEPRA1)
5	
	Enable log redundancy across collectors
	Forward to all collectors in the preference list
	Enable secure inter LC Communication Log collector on local panorama is using the secure client configuration from 'Panorama -> Secure Communication Settings'
	OK Cancel

如需詳細資訊,請參閱建立父系裝置群組和範本堆疊。

- 收集授權碼以及自動註冊 PIN ID 和值。
- 將映像檔下載至其中的容器映像檔儲存庫位置。
- STEP 2| (選用)如果您已在 Panorama 的 Kubernetes 外掛程式中設定自訂憑證,則必須執行下列命 令來建立憑證密碼。請不要從 ca.crt 變更檔案名稱。pan-cn-mgmt-dynamic-pv.yaml 和 pan-cn-ngfw.yaml 中的自訂憑證數量是選用項目。

kubectl -n kube-system create secret generic custom-ca --fromfile=ca.crt

STEP 3| 编輯 YAML 檔案,以提供部署 CN-Series 防火牆所需的詳細資料。

您需要取代 YAML 檔案中的映像路徑以包括私人 Google Container 登錄的路徑,以及提供必要 參數。請參閱 CN-Series 部署 yaml 檔案中的可編輯參數以取得詳細資料。

STEP 4| 部署 CNI DaemonSet。

CNI 容器部署為 DaemonSet(一個節點一個 Pod),而且它會在節點上所部署之每個應用程式的 CN-NGFW Pod 上建立兩個執行個體。當您使用 kubectl 命令來執行 pan-cni YAML 檔案時,它會變成每個節點上服務鏈的一部分。



- 1. CN-Series 防火牆需要三個「服務」帳戶,而這些帳戶具有授權它與 Kubernetes 叢集資源 通訊的最小權限。您應該建立使用 CN-Series 為叢集驗證建立服務帳戶,並驗證是否已使 用 pan-cni-serviceaccount.yaml 建立服務帳戶。
- 2. 使用 Kubectl 來執行 pan-cni-configmap.yaml。

kubectl apply -f pan-cni-configmap.yaml

3. 使用 Kubectl 來執行 pan-cni.yaml。

kubectl apply -f pan-cni.yaml

- 4. 請驗證您已修改 pan-cni-configmap 和 pan-cni YAML 檔案。
- 5. 執行下列命令, 並確認您的輸出與下列範例相似。



STEP 5| 部署 CN-MGMT StatefulSet。

管理平面預設會部署為可提供容錯的 StatefulSet。最多可以將 30 個防火牆 CN-NGFW Pod 連線 至 CN-MGMT StatefulSet。

1. 驗證您已修改 pan-cn-mgmt-configmap 和 pan-cn-mgmt YAML 檔案。

範例 pan-cn-mgmt-configmap

apiVersion: v1 kind:ConfigMap metadata: name: pan-mgmtconfig namespace: kube-system data:PAN_SERVICE_NAME: pan-mgmt-svc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama settings PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP: "<panorama-device-group>" PAN_TEMPLATE_STACK: "<panoramatemplate-stack>" PAN_CGNAME: "<panorama-collector-group>"#Nonmandatory parameters # Recommended to have same name as the cluster name provided in Panorama Kubernetes plugin - helps with easier identification of pods if managing multiple clusters with same Panorama #CLUSTER_NAME: "<Cluster name>" #PAN_PANORAMA_IP2: "" # Comment out to use CERTs otherwise PSK for IPSec between pan-mgmt and pan-ngfw #IPSEC_CERT_BYPASS: "" # No values needed # Override autodetect of jumbo-frame mode and force enable system-wide #PAN_JUMBO_FRAME_ENABLED: "true" # Start MGMT pod with GTP enabled.For complete functionality, need GTP # enable at Panorama as well. #PAN_GTP_ENABLED: "true" # Enable high feature capacities.這些需要 MGMT Pod 具有高記憶體,以及 # 下面針對 NGFW Pod 所指定的較高/相符記憶體。# 請參照系統需求文件,以查看每個記憶 體設定檔所支援的最大支援 NGFW CPU 大小 #。#PAN_NGFW_MEMORY:"6.5Gi" #PAN_NGFW_MEMORY:"48Gi" #PAN_NGFW_MEMORY:"56Gi"

範例 pan-cn-mgmt-dynamic-pv.yaml

```
initContainers: - name: pan-mgmt-init image: <your-private-
registry-image-path>
```

```
containers: - name: pan-mgmt image: <your-private-registry-
image-path> terminationMessagePolicy:FallbackToLogsOnError
```

2. 使用 Kubectl 來執行 yaml 檔案。

```
kubectl apply -f pan-cn-mgmt-configmap.yaml
kubectl apply -f pan-cn-mgmt-secret.yaml
kubectl apply -f pan-cn-mgmt-dynamic-pv.yaml
```

只有在您先前尚未完成使用 CN-Series 建立叢集驗證的服務帳戶時,才必須執行 panmgmt-serviceaccount.yaml。

3. 驗證 CN-MGMT Pod 已啟動。

這需要大約 5-6 分鐘。

```
使用 kubectl get pods -l app=pan-mgmt -n kube-system
NAME READY STATUS RESTARTS AGEpan-mgmt-sts-0 1/1
Running 0 27hpan-mgmt-sts-1 1/1 Running 0 27h
```

STEP 6| 部署 CN-NGFW Pod。

防火牆資料平面 CN-NGFW Pod 預設會部署為 DaemonSet。CN-NFGW Pod 執行個體可以保護節 點上最多 30 個應用程式 Pod 的流量。

1. 驗證您已修改 PAN-CN-NGFW-CONFIGMAP 和 PAN-CN-NGFW 中詳述的 YAML 檔案。

containers: - name: pan-ngfw-container image: <your-privateregistry-image-path>

2. 使用 Kubectl apply 來執行 pan-cn-ngfw-configmap.yaml。

kubectl apply -f pan-cn-ngfw-configmap.yaml

3. 使用 Kubectl apply 來執行 pan-cn-ngfw.yaml。

kubectl apply -f pan-cn-ngfw.yaml

4. 驗證所有 CN-NGFW Pod 都正在執行(叢集中一個節點會有一個 Pod)。

這是4節點內部部署叢集的範例輸出。

kubectl get pods -n kube-system -l app=pan-ngfw -o wide

NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES

pan-ngfw-ds-8g5xb 1/1 Running 0 27h 10.233.71.113 rk-k8-node-1
<none>

pan-ngfw-ds-qsrm6 1/1 Running 0 27h 10.233.115.189 rk-k8-vmworker-1 <none>

pan-ngfw-ds-vqk7z 1/1 Running 0 27h 10.233.118.208 rk-k8-vmworker-3 <none>

pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vmworker-2 <none> STEP 7 | 驗證您可以在 Kubernetes 叢集上看到 CN-MGMT、CN-NGFW 和 PAN-CNI。

kubectl -n kube-system get pods

- 0 27hpan-cni-5fhbg 1/1 Running
- 0 27hpan-cni-9j4rs 1/1 Running
- 0 27hpan-cni-ddwb4 1/1 Running
- 0 27hpan-cni-fwfrk 1/1 Running
- 0 27hpan-cni-h57lm 1/1 Running
- 0 27hpan-cni-h57lm 1/1 Running
- 0 27hpan-cni-j62rk 1/1 Running
- 0 27hpan-cni-lmxdz 1/1 Running
- 0 27hpan-mgmt-sts-0 1/1 Running
- 0 27hpan-mgmt-sts-1 1/1 Running
- 0 27hpan-ngfw-ds-8g5xb 1/1 Running
- 27hpan-ngfw-ds-qsrm6 1/1 Running
- 0 27hpan-ngfw-ds-vqk7z 1/1 Running
- 0 27hpan-ngfw-ds-zncqg 1/1 Running
- STEP 8 標註應用程式 yaml 或命名空間, 讓來自其新 Pod 的流量重新導向至防火牆。

您需要新增下列註釋,以將流量重新導向至 CN-NGFW 來進行檢查:

annotations: paloaltonetworks.com/firewall: pan-fw

例如,對於「default」命名空間中的所有新 Pod:

kubectl annotate namespace default paloaltonetworks.com/ firewall=pan-fw

在部分平台上, pan-cni 在 CNI 外掛程式鏈中未作用時,可以啟動應用程式 Pod。
 若要避免這類情況,您必須在應用程式 Pod YAML 中指定這裡顯示的磁碟區。

volumes: - name: pan-cni-ready hostPath: path: /var/log/ pan-appinfo/pan-cni-ready type:Directory

STEP 9 在叢集中部署應用程式。

在 EKS 上部署 CN-Series 防火牆

我可以在哪裡使用這個?	我需要哪些內容?
• CN-Series 部署	• CN-Series 10.1.x or above Container Images
	• Panorama 執行 PAN-OS 10.1.x 或更高版本
	• Helm 3.6 or above version client 用於使用 Helm 進行 CN-Series 部署

在您檢閱 CN-Series 建置區塊以及使用 CN-Series 保護 Kubernetes 環境中的工作流程高階概觀之後,就可以在 AWS EKS 平台上開始部署 CN-Series 防火牆來保護相同叢集內容器之間的流量,以及容器與其他工作負載類型之間的流量(例如虛擬機器和裸機伺服器)。



您需要 kubectl 或 Helm 這類標準 Kubernetes 工具來部署和管理 Kubernetes 叢集、應用 程式和防火牆服務。

如需詳細資訊,請參閱使用 Helm 圖表和範本部署 CN-Series 防火牆。Panorama 未設計成進行 Kubernetes 叢集部署和管理的協調器。進行叢集管理的範本是由「受管理 Kubernetes 提供者」所提供。Palo Alto Networks 提供社群支援的範本,以利用 Helm 和 Terraform 來部署 CN-Series。

- 在 AWS EKS 上部署 CN-Series 防火牆作為 Kubernetes 服務
- 在 AWS EKS 上部署 CN-Series 防火牆作為 Daemonset
- 從 AWS Marketplace 部署 CN-Series



從部署「CN-Series 作為 DaemonSet」移到「CN-Series 作為服務」之前(反之亦 然),您必須刪除並重新套用 plugin-serviceaccount.yaml。如需詳細資訊, 請參閱建立用於叢集驗證的服務帳戶。

- 當您在 EKS 上部署 CN-Series 作為 DaemonSet 時, pan-plugin-clustermode-secret 不得存在。
- 當您在 EKS 上部署 CN-Series 作為 Kubernetes 服務時, 必須要有 pan-plugincluster-mode-secret。

在 AWS EKS 上部署 CN-Series 防火牆作為 Kubernetes 服務

我可以在哪裡使用這個?	我需要哪些內容?
• CN-Series 部署	• CN-Series 10.1.x or above Container Images
	• Panorama 執行 PAN-OS 10.1.x 或更高版本
	• Helm 3.6 or above version client 對於使用 Helm 的 CN-Series 部署

完成下列程序,以將 CN-Series 防火牆部署為 Kubernetes 服務。

開始之前,請確保 CN-Series YAML 檔案版本與 PAN-OS 版本相容。

- PAN-OS 10.1.2 或更新版本需要 YAML 2.0.2
- PAN-OS 10.1.0 和 10.1.1 需要 YAML 2.0.0 或 2.0.1

STEP 1 設定 Kubernetes 叢集。

若要在 AWS EKS 中建立叢集, 請執行下列動作:

1. 按一下 Services (服務) 導覽功能表, 然後移至 Containers (容器) ->Elastic Kubernetes Service (彈性 Kubernetes 服務)。



- **2.** 按一下 Create Cluster (建立叢集)。
- 3. 填寫所需的詳細資訊,然後按一下 Create (建立)。

EVS > Custors > Custors	Services	Q Search for services, feat	ures, blogs, docs, and more	[Alt+S]				
Sep 1 Configure cluster Sep 2 Configure cluster inte Sep 3 Cluster configuration inte Sep 4 Non - Met definition for crustes: Sep 4 Cluster Service Mole for the duate: Cluster Service Mole for the duate: Cluster Service Mole for the duate: Cluster Service Mole for the duate: Cluster Service Mole for the duate: Cluster Service Mole for Clusters corted plane to manage AWS resources on your between Cluster Service Mole for menoet: Cluster Service Mole for Clusters corted plane to manage AWS resources on your between Cluster Service Mole for menoet: Cluster Service Mole for Clubernets corted plane to manage AWS resources on your between Cluster Service Mole for menoet: Cluster Service Mole for Clubernets corted plane to manage AWS resources on your between Cluster Service Mole for menoet: Cluster Mole mole service for On fuldernets servers using MMS Cluster menope encryption for Mole menoet servers Cluster Mole mole service for On fuldernets servers using MMS Cluster menope encryption for your Klubernets servers Tags (0) info Tis cluster does not that your; Tis cluster does not that your;	EKS > Cluster	rs > Create EKS cluster						
Sup 2 Specify networking Cluster configuration info Sup 3 Configure Logging Name - Not refielde efficie rotation: Sup 4 Review and create Name - Not refielde efficie rotation: Cluster Service Notify Sup 4 Sup 4 Review and create Name - Not refielde efficie rotation: Cluster Service Notify Sup 4 Sup 4 Review and create Name - Not refielde efficie rotation: Cluster Service Notify Sup 4 Sup 4 Name - Not refielde efficie rotation: Cluster Service Notify Sup 4 Sup 4 Name - Not refielde efficie rotation: Cluster Service Notify Sup 4 Sup 4 Name - Not refielde efficie rotation: Cluster Service Notify Sup 4 Set the Notify the Julian due Notifielde efficie rotation: Sup 4 Cluster Service Notify bland with the Nationation controls: Sup 4 Cluster Service Notify bland with the Nationation controls: Sup 4 Cluster Service Notify bland with the Nationation controls: Sup 4 Set the Nationation control bland with controls: Cluster Service Notify bland with the Nationation controls: Set the Nationation control bland with the Nationatin controt the modified or removed: Clu	Step 1 Configure cluste	er	Configure cluster					
Step 3 Configure togging Mee Act extended effer creation. Step 4 Review and create Cleaner for the cluate. Cluate Step 4 Review and create Cluate Step 4 Step 4 Step 4 Review and create Step 4 Review and create Cluate Step 4 Step 4 S	Step 2 Specify network	ing	Cluster configuration Info					
Supple Burgel A Review and create Latter KS11 Latter KS12 Cluster Ksvike Role Info - Net extende of the contexts. States the UMP field to allow the Kdentexts control plane to manage MVS resources on your behalt. Testers the UMP field to allow the Kdentexts control plane to manage MVS resources on your behalt. States the UMP field to allow the Kdentexts. States the UMP field to allow the Indified or removed. States envelope encryption field Tage (0) info This cluster does not have any tags.	Step 3		Name - Not editable after creation. Enter a unique name for this cluster.					
Step 4 Review and create Kubernetes version infe Step 4 Review and create Step 4 Review and create La Image: Comparison of the two status and the two creates Step 4 Review and create Step 4 Review and create Later 5 envice Role infe - Not schedule of nor creates Step 4 Review and create Step 5 Review and create Step 5 Review and create Step 5 Review and create Step 5 Review and create The create and review play go to the MM corrects Step 5 Review and create The create and review play go to the two for modeline or removed. Create and review play go to the provide an additional layer of encryption for your Kubernetes secrets. Tags (0) Infe This cluster does not have any tags.	configure toggi		ClusterEKS1					
121 ▼ Cluster Service Role Info-Acte editable after creation. Select the UM Role after creation. Select the UM Role and the Common. ▼ Propried ▼ Required ▼ Discrete enversion, go to be Mole Common. ▼ Propried ▼ Core mobiled, sorters encyption info © Core mobiled, sorters encyption after or menowed. ● Core mobiled, sorters encyption after or movied. ● Enable envelope encryption fund Core Core mobiled, sorters encryption after or movied. ● Tags (0) Info Tags (0) Info This cluster does not have any tags. ■	Step 4 Review and crea	te	Kubernetes version Info Select the Kubernetes version for this cluste	r.				
Cluster Service Role Infe - Nos exitable after oransian. Salect the UAN Role saleov the K&Dennetes control plane to manage AWS resources on your behalf. ■ Infect Cole ■ Repaired			1.21		•			
Secrets encryption info Once endeling secrets encryption annot be modified or removed. Image: Trade envelope encryption of Kubernetes secrets using KMS Enable envelope encryption to provide an additional layer of encryption for your Kubernetes secrets. Tags (0) Info This cluster does not have any tags.			Cluster Service Role Info - Not editable Select the IAM Role to allow the Kuberneter To create a new role, go to the IAM console.	after creation. control plane to manage AWS resources on your beh	alf.			
			Select role		•	C		
Secrets encryption Into Once enabled secrets encryption annot be modified or removed. Enable envelope encryption of Kubernetes secrets using KMS Enable envelope encryption to provide an additional layer of encryption for your Kubernetes secrets. Tags (0) Info This cluster does not have any tags.			Required					
Tags (0) Info This cluster does not have any tags.			Secrets encryption Info Once enabled, secrets encryption cannot be r Enable envelope encryption of K Enable envelope encryption to provid	notified or removed. ubernetes secrets using KMS an additional layer of encryption for your Kubernete	es secrets.			
This cluster does not have any tags.			Tags (0) Info					
			This cluster does not have any tags.					
Add tag Remaining tags available to add: 50			Add tag Remaining tags available to add: 50					
Cancel Next						Cancel	Next	

 請驗證叢集具有足夠的版本。確保該叢集具有 CN-Series 先決條件資源以支援防火牆: kubectl get nodes kubectl describe node <node-name>

檢視命令輸出之「容量」標題下的資訊,以查看所指定節點上可用的 CPU 和記憶體。

CPU、記憶體和磁碟儲存體配置將取決於您的需求。請參閱 CN-Series 效能和調整規模。 確保您具有下列資訊:

- 收集「端點 IP 位址」,以在 Panorama 上設定 API 伺服器。Panorama 使用此 IP 位址來 連線至 Kubernetes 叢集。
- 從 Panorama 收集範本堆疊名稱、裝置群組名稱、Panorama IP 位址和日誌收集器群組 名稱(選用)。
- 收集授權碼以及自動註冊 PIN ID 和值。
- 將映像檔下載至其中的容器映像檔儲存庫位置。
- STEP 2 (選用)如果您已在 Panorama 的 Kubernetes 外掛程式中設定自訂憑證,則必須執行下列命令 來建立憑證密碼。請不要從 ca.crt 變更檔案名稱。pan-cn-mgmt.yaml 和 pan-cn-ngfw.yaml 中的 自定憑證數量是選用項目。

kubectl -n kube-system create secret generic custom-ca --fromfile=ca.crt

STEP 3 编輯 YAML 檔案,以提供部署 CN-Series 防火牆所需的詳細資料。

您需要取代 YAML 檔案中的映像檔路徑以包括私人登錄的路徑,以及提供必要參數。請參閱 CN-Series 部署 yaml 檔案中的可編輯參數以取得詳細資料。

- STEP 4 更新儲存類別。若要支援在 AWS Outpost 上部署的 CN-Series,您必須使用儲存驅動程式 awsebs-csi-driver,確保 Outpost 在建立動態持續性磁碟區 (PV) 期間從 Outpost 拉出磁碟區。
 - 1. 套用下列 yaml。

kubectl apply -k "github.com/kubernetes-sigs/aws-ebs-csi-driver/ deploy/kubernetes/overlays/stable/?ref=release-0.10"

2. 驗證 ebs-sc 控制器是否正在執行。

kubectl -n kube-system get pods

3. 更新 pan-cn-storage-class.yaml 以符合下面的範例。

apiVersion: v1 kind:StorageClass apiVersion: storage.k8s.io/ v1 metadata: name: ebs-sc provisioner: ebs.csi.aws.com volumeBindingMode:WaitForFirstConsumer parameters: type: gp2

4. 將 storageClassName: ebs-sc 新增至下面所顯示位置中的 pan-cn-mgmt.yaml。

volumeClaimTemplates: - metadata: name: panlogs spec: #storageClassName: pan-cn-storage-class //For better disk iops performance for logging accessModes: ["ReadWriteOnce"] storageClassName: ebs-sc // resources: requests: storage:20Gi # change this to 200Gi while using storageClassName for better disk iops - metadata: name: varlogpan spec: #storageClassName: pan-cn-storage-class //For better disk iops performance for dp logs accessModes: ["ReadWriteOnce"] storageClassName: ebs-sc resources: requests: storage:20Gi # change this to 200Gi while using storageClassName for better disk iops - metadata: name: varcores spec: accessModes: ["ReadWriteOnce"] storageClassName: ebs-sc resources: requests: storage:2Gi - metadata: name: panplugincfg spec: accessModes: ["ReadWriteOnce"] storageClassName: ebs-sc resources: requests: storage:1Gi - metadata: name: panconfig spec: accessModes: ["ReadWriteOnce"] storageClassName: ebs-sc resources: requests: storage:8Gi - metadata: name: panplugins spec: accessModes: ["ReadWriteOnce"] storageClassName: ebs-sc resources: requests: storage:200Mi

- STEP 5 | 如果您在 Kubernetes 環境中使用自動縮放,請執行下列動作:
 - 在「CN-Series 作為服務」叢集中,部署 Kubernetes 的 Amazon CloudWatch Metrics Adapter。您必須允許 CloudWatch 完整存取與 Kubernetes Pod 和叢集相關聯的兩個 IAM 角色。若要將自訂度量發佈至 CloudWatch,工作節點的角色必須要有 AWS 受管理政策 CloudWatchAgentServerPolicy, HPA 才能對其進行擷取。
 - 2. 從 Palo Alto Networks GitHub 儲存庫,下載 EKS 特有 HPA yaml 檔案。
 - **3.** 如果您的 CN-MGMT 部署在自訂命名空間中,則請使用自訂命名空間來更新 pan-cn-adapater.yaml。預設命名空間是 **kube-system**。

- 4. 修改 pan-cn-hpa-dp.yaml 和 pan-cn-hpa-mp.yaml。
 - 1. 輸入最小和最大複本數目。
 - (選用)變更縮減和擴充頻率值,以符合您的部署。如果您未變更這些值,則會使用預設 值。
 - 3. 針對您要用於調整規模的每個度量,複製下列區段。

 type:Pods pods: metric: name: pansessionactive target: type:AverageValue averageValue:30

- 4. 變更您要使用之度量的名稱,並將 averageValue 設定為上表所述的臨界值。如果您未 變更這些值,則會使用預設值。
- 5. 儲存變更。

如需詳細資訊,請參閱〈水平 Pod 自動調整規模〉。

- 5. 部署 HPA yaml 檔案。檔案必須依下面所述的順序進行部署。
 - 1. 使用 Kubectl 來執行 pan-cn-adapter.yaml

kubectl apply -f pan-cn-adapter.yaml

- 使用 Kubectl 來執行 pan-cn-externalmetrics.yaml
 kubectl apply -f pan-cn-externalmetrics.yaml
- 使用 Kubectl 來執行 pan-cn-hpa-dp.yaml
 kubectl apply -f pan-cn-hpa-dp.yaml
- 4. 使用 Kubectl 來執行 pan-cn-hpa-mp.yaml

kubectl apply -f pan-cn-hpa-mp.yaml

6. 驗證您的部署。

使用 kubectl 來確認自訂度量命名空間中的自訂度量介面卡 Pod。

kubectl get pods -n custom-metrics

使用 kubectl 檢查 HPA 資源。

kubectl get hpa -n kube-system

kubectl describe hpa <hpa-name> -n kube-system

- STEP 6 | 部署 CN-NGFW 服務。
 - 請驗證您已使用 pan-cni-serviceaccount.yaml 來建立服務帳戶。
 請參閱建立叢集驗證的服務帳戶。
 - 2. 使用 Kubectl 來執行 pan-cni-configmap.yaml。

kubectl apply -f pan-cni-configmap.yaml

3. 使用 kubectl 來執行 pan-cn-ngfw-svc.yaml。

```
kubectl apply -f pan-cn-ngfw-svc.yaml
```



必須在 pan-cni.yaml 之前部署此 yaml。

4. 使用 Kubectl 來執行 pan-cni.yaml。

kubectl apply -f pan-cni.yaml

- 5. 請驗證您已修改 pan-cni-configmap 和 pan-cni YAML 檔案。
- 6. 執行下列命令, 並確認您的輸出與下列範例相似。

kubectl get pods -n kube-system | grep pan-cni

@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (vī	eries-mktplace)	\$ k	ubectl get pods	-n	kube-system	grep	pan-cni
pan-cni-nmqkf		Running	0	2m11s				
pan-cni-wjrkq		Running	0	2m11s				
pan-cni-xrc2z		Running	0	2m12s				
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v	v	eries-mktplace)						

STEP 7 | 部署 CN-MGMT StatefulSet。

管理平面預設會部署為可提供容錯的 StatefulSet。最多可以將 30 個防火牆 CN-NGFW Pod 連線 至 CN-MGMT StatefulSet。

- 1. (僅為靜態佈建 PV 的必要項目) 部署 CN-MGMT StatefulSet 的「永久性磁碟區 (PV)」。
 - 1. 建立目錄,以符合 pan-cn-pv-local.yaml 中所定義的本機磁碟區名稱。

您需要至少2個背景工作節點上有六(6)個目錄。請登入將部署 CN-MGMT StatefulSet 以建立目錄的每個背景工作節點。例如,若要建立名為/mnt/pan-local1 到/mnt/pan-local6 的目錄,請使用命令:

mkdir -p /mnt/pan-local1 /mnt/pan-local2 /mnt/pan-local3 /
mnt/pan-local4 /mnt/pan-local5 /mnt/pan-local6

2. 修改 pan-cn-pv-local.yaml。

符合 nodeaffinity 下方的主機名稱,並驗證您已修改上面您在 spec.local.path 中建立的目錄,然後部署檔案來建立新的 storageclass pan-local-storage 和本機 PV。

2. 驗證您已修改 pan-cn-mgmt-configmap 和 pan-cn-mgmt YAML 檔案。

EKS 中的範例 pan-cn-mgmt-configmap。

apiVersion: v1 kind:ConfigMap metadata: name: pan-mgmtconfig namespace: kube-system data:PAN_SERVICE_NAME:
 pan-mgmt-svc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama settings PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP: "<panorama-device-group>" PAN_TEMPLATE_STACK: "<panorama-</pre> template-stack>" PAN_CGNAME: "<panorama-collector-group>" # ctnr mode: "k8s-service", "k8s-ilbservice" PAN_CTNR_MODE_TYPE: "k8s-service" #Non-mandatory parameters # Recommended to have same name as the cluster name provided in Panorama Kubernetes plugin - helps with easier identification of pods if managing multiple clusters with same Panorama #CLUSTER NAME: "<Cluster name>" #PAN PANORAMA IP2: "" # Comment out to use CERTs otherwise PSK for IPSec between pan-mgmt and pan-ngfw #IPSEC_CERT_BYPASS: "" # No values needed # Override auto-detect of jumbo-frame mode and force enable system-wide #PAN JUMBO FRAME ENABLED: "true" # Start MGMT pod with GTP enabled.For complete functionality, need GTP # enable at Panorama as well. #PAN_GTP_ENABLED: "true" # Enable high feature capacities. These need high memory for MGMT pod and # higher/matching memory than specified below for NGFW pod. #PAN_NGFW_MEMORY="6Gi" #PAN_NGFW_MEMORY="40Gi" # For enabling faster datapath -AF XDP, default is AF PACKETV2.This requires kernel support. #PAN DATA MODE: "next-gen" #HPA params #PAN CLOUD:"EKS'

#PAN_NAMESPACE_EKS:"EKSNamespace" #PUSH_INTERVAL:"15" #time
interval to publish metrics to AWS cloudwatch

```
範例 pan-cn-mgmt.yaml
```

```
initContainers: - name: pan-mgmt-init image: <your-private-
registry-image-path>
```

containers: - name: pan-mgmt image: <your-private-registryimage-path> terminationMessagePolicy:FallbackToLogsOnError

3. 使用 Kubectl 來執行 yaml 檔案。

kubectl apply -f pan-cn-mgmt-configmap.yaml kubectl apply -f pan-cn-mgmt-slot-crd.yaml kubectl apply -f pan-cn-mgmt-slot-cr.yaml kubectl apply -f pan-cn-mgmt-secret.yaml kubectl apply -f pan-cn-mgmt.yaml

只有在您先前尚未完成建立叢集驗證的服務帳戶時,才必須執行 pan-mgmt-serviceaccount.yaml。

4. 驗證 CN-MGMT Pod 已啟動。

這需要大約 5-6 分鐘。

使用 kubectl get pods -l app=pan-mgmt -n kube-system

STEP 8| 部署 CN-NGFW Pod。

1. 驗證您已修改 PAN-CN-NGFW-CONFIGMAP 和 PAN-CN-NGFW 中詳述的 YAML 檔案。

```
containers: - name: pan-ngfw-container image: <your-private-
registry-image-path>
```

2. 使用 Kubectl apply 來執行 pan-cn-ngfw-configmap.yaml。

kubectl apply -f pan-cn-ngfw-configmap.yaml

3. 使用 Kubectl apply 來執行 pan-cn-ngfw.yaml。

kubectl apply -f pan-cn-ngfw.yaml

4. 驗證 CN-NGFW Pod 正在執行。

kubectl get pods -n kube-system -l app=pan-ngfw -o wide

STEP 9| 在 CN-Series 上啟用水平 Pod 自動調整規模。

STEP 10 | 驗證您可以在 Kubernetes 叢集上看到 CN-MGMT、CN-NGFW 和 PAN-CNI。

kubectl -n kube-system get pods

STEP 11 | 標註應用程式 yaml 或命名空間, 讓來自其新 Pod 的流量重新導向至防火牆。

您需要新增下列註釋,以將流量重新導向至 CN-NGFW 來進行檢查:

annotations: paloaltonetworks.com/firewall: pan-fw

例如,對於「default」命名空間中的所有新 Pod:

kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw



在部分平台上, pan-cni 在 CNI 外掛程式鏈中未作用時,可以啟動應用程式 Pod。 若要避免這類情況,您必須在應用程式 Pod YAML 中指定這裡顯示的磁碟區。

volumes: - name: pan-cni-ready hostPath: path: /var/log/ pan-appinfo/pan-cni-ready type:Directory

STEP 12 | 在叢集中部署應用程式。

在AWS EKS 上部署 CN-Series 防火牆作為 Daemonset

這可在何處使用?	我需要什麼?
• CN-Series 部署	• CN-Series 10.1.x or above Container Images
	• Panorama 執行 PAN-OS 10.1.x 或更高版本
	• Helm 3.6 or above version client 使用 Helm 進行 CN-Series 部署

完成下列步驟以將 CN-Series 防火牆部署為 AWS EKS 上的 Dameonset:

STEP 1 設定 Kubernetes 叢集。

若要在 AWS EKS 中建立叢集, 請執行下列動作:

1. 按一下 Services (服務) 導覽功能表, 然後移至 Containers (容器) ->Elastic Kubernetes Service (彈性 Kubernetes 服務)。



- **2.** 按一下 Create Cluster (建立叢集)。
- 3. 填寫所需的詳細資訊,然後按一下 Create (建立)。

Configure cluster	Configure cluster	
Step 2 Specify networking	Cluster configuration Info	
Step 3	Name - Not editable after creation. Entre a unique name for this cluster.	
Configure logging	ClusterEKS1	
Step 4 Review and create	Kubernetes version Info Select the Kubernetes version for this cluster.	
	1.21	
	Cluster Service Role Info - Not estituble offer creation. Select the IAM Role to allow the Kubernets control plane to manage AWS resources on your behalf. To create a new role, ook the IAM Compose.	
	Select role C	
	Required	
	Secrets encryption Info Once enabled, secrets encoyption cannot be modified or removed.	
	Enable envelope encryption of Kubernetes secrets using KMS Enable envelope encryption to provide an additional layer of encryption for your Kubernetes secrets.	
	Tags (0) Info	
	This cluster does not have any tags.	
	Add tag	

請驗證叢集具有足夠的版本。確保叢集具有 CN-Series 先決條件資源來支援防火牆。

kubectl get nodes

kubectl describe node <node-name>

檢視命令輸出之「容量」標題下的資訊,以查看所指定節點上可用的 CPU 和記憶體。

CPU、記憶體和磁碟儲存體配置將取決於您的需求。請參閱 CN-Series 效能和調整規模。 確保您具有下列資訊:

• 收集「端點 IP 位址」,以在 Panorama 上設定 API 伺服器。

Des API server Credent Label Selector La C TAG PREFIX	Name scription r address Type titials	on_prem-clstr 10.2. Native-Kubernet er Custom C	ies iertificate	0 items)→ X
Des API server Credent Label Selector La C	r address Type titials	10.2. Native-Kubernet er Custom C	ies iertificate	0 items)→ ×
API server Credent Label Selector La C TAG PREFIX	r address Type atials abel Filte	10.2. Native-Kubernet er Custom C	ies iertificate	0 items)→ ×
Credent Label Selector La Q TAG PREFIX	Type	Native-Kubernet	ertificate	0 items)→ X
Credent Label Selector La	abel Filte	er Custom C	ertificate	0 items)→ X
Label Selector La	abel Filte	er Custom C	ertificate	0 items) \rightarrow X
Q				0 items \rightarrow \times
TAG PREFIX				
	NAMES	PACE	LABEL SELECTOR FILTER	APPLY ON
🕀 Add () Delete				
Unite Uperete				

Panorama 使用此 IP 位址來連線至 Kubernetes 叢集。

如需詳細資訊,請參閱設定用於監視叢集的 Kubernetes 外掛程式。

• 從 Panorama 收集範本堆疊名稱、裝置群組名稱、Panorama IP 位址和日誌收集器群組名稱 (選用)。

Collector Group	Θ
General Monitoring	Device Log Forwarding Collector Log Forwarding Log Ingestion
Name	rp-cg1
Log Storage	Total: 1.53 TB,Free: 75.30 GB
Min Retention Period (days)	[1 - 2000]
Collector Group Members	Q(1item)→X
	rpgcpnew(RPGOOGGKEPRA1)
	0.000
	(+) Add (-) Delete
	Enable log redundancy across collectors
	Forward to all collectors in the preference list
	Enable secure inter LC Communication Log collector on local panorama is using the secure client configuration from 'Panorama -> Secure Communication Settings'
	OK Cancel

如需詳細資訊,請參閱建立父系裝置群組和範本堆疊。

- 收集授權碼以及自動註冊 PIN ID 和值。
- 將映像檔下載至其中的容器映像檔儲存庫位置。
- STEP 2| (選用)如果您已在 Panorama 的 Kubernetes 外掛程式中設定自訂憑證,則必須執行下列命令 來建立憑證密碼。請不要從 ca.crt 變更檔案名稱。pan-cn-mgmt.yaml 和 pan-cn-ngfw.yaml 中的 自定憑證數量是選用項目。

kubectl -n kube-system create secret generic custom-ca --fromfile=ca.crt

STEP 3| 编輯 YAML 檔案,以提供部署 CN-Series 防火牆所需的詳細資料。

您需要取代 YAML 檔案中的映像路徑以包括私人 Google Container 登錄的路徑,以及提供必要 參數。請參閱 CN-Series 部署 yaml 檔案中的可編輯參數以取得詳細資料。

STEP 4| 部署 CNI DaemonSet。

CNI 容器部署為 DaemonSet(一個節點一個 Pod),而且它會在節點上所部署之每個應用程式的 CN-NGFW Pod 上建立兩個執行個體。當您使用 kubectl 命令來執行 pan-cni YAML 檔案時,它會變成每個節點上服務鏈的一部分。

- 1. CN-Series 防火牆需要三個「服務」帳戶,而這些帳戶具有授權它與 Kubernetes 叢集資 源通訊的最小權限。您應該建立為叢集驗證建立服務帳戶,並驗證是否已使用 pan-cniserviceaccount.yaml 建立服務帳戶。
- 2. 使用 Kubectl 來執行 pan-cni-configmap.yaml。

kubectl apply -f pan-cni-configmap.yaml

3. 使用 Kubectl 來執行 pan-cni.yaml。

kubectl apply -f pan-cni.yaml

- 4. 請驗證您已修改 pan-cni-configmap 和 pan-cni YAML 檔案。
- 5. 執行下列命令, 並確認您的輸出與下列範例相似。

@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v	eries-mktplace)\$ kubectl get pods -n kube-system grep pan-cni
<pre>pan-cni-nmqkf</pre>	Running 0 2mlls
pan-cni-wjrkq	Running 0 2m11s
pan-cni-xrc2z	Running 0 2m12s
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v	eries-mktplace)\$

STEP 5 更新儲存類別。若要支援在 AWS Outpost 上部署的 CN-Series,您必須使用儲存驅動程式 awsebs-csi-driver,確保 Outpost 在建立動態持續性磁碟區 (PV) 期間從 Outpost 拉出磁碟區。

1. 套用下列 yaml。

kubectl apply -k "github.com/kubernetes-sigs/aws-ebs-csi-driver/ deploy/kubernetes/overlays/stable/?ref=release-0.10"

2. 驗證 ebs-sc 控制器是否正在執行。

kubectl -n kube-system get pods

3. 更新 pan-cn-storage-class.yaml 以符合下面的範例。

apiVersion: v1 kind:StorageClass apiVersion: storage.k8s.io/ v1 metadata: name: ebs-sc provisioner: ebs.csi.aws.com volumeBindingMode:WaitForFirstConsumer parameters: type: gp2

4. 將 storageClassName: ebs-sc 新增至下面所顯示位置中的 pan-cn-mgmt.yaml。

volumeClaimTemplates: - metadata: name: panlogs spec: #storageClassName: pan-cn-storage-class //For better disk iops performance for logging accessModes: ["ReadWriteOnce"] storageClassName: ebs-sc // resources: requests: storage:20Gi # change this to 200Gi while using storageClassName for better disk iops - metadata: name: varlogpan spec: #storageClassName: pan-cn-storage-class //For better disk iops performance for dp logs accessModes: ["ReadWriteOnce"] storageClassName: ebs-sc resources: requests: storage:20Gi # change this to 200Gi while using storageClassName for better disk iops - metadata: name: varcores spec: accessModes: ["ReadWriteOnce"] storageClassName: ebs-sc resources: requests: storage:2Gi - metadata: name: panplugincfg spec: accessModes: ["ReadWriteOnce"] storageClassName: ebs-sc resources: requests: storage:1Gi - metadata: name: panconfig spec: accessModes: ["ReadWriteOnce"] storageClassName: ebs-sc resources: requests: storage:8Gi - metadata: name: panplugins spec: accessModes: ["ReadWriteOnce"] storageClassName: ebs-sc resources: requests: storage:200Mi

STEP 6| 部署 CN-MGMT StatefulSet。

管理平面預設會部署為可提供容錯的 StatefulSet。最多可以將 30 個防火牆 CN-NGFW Pod 連線 至 CN-MGMT StatefulSet。

- 1. (僅為靜態佈建 PV 的必要項目) 部署 CN-MGMT StatefulSet 的「永久性磁碟區 (PV)」。
 - 1. 建立目錄,以符合 pan-cn-pv-local.yaml 中所定義的本機磁碟區名稱。

您需要至少2個背景工作節點上有六(6)個目錄。請登入將部署 CN-MGMT StatefulSet 以建立目錄的每個背景工作節點。例如,若要建立名為/mnt/pan-local1 到/mnt/pan-local6 的目錄,請使用命令:

mkdir -p /mnt/pan-local1 /mnt/pan-local2 /mnt/pan-local3 /
mnt/pan-local4 /mnt/pan-local5 /mnt/pan-local6

2. 修改 pan-cn-pv-local.yaml。

符合 nodeaffinity 下方的主機名稱,並驗證您已修改上面您在 spec.local.path 中建立的目錄,然後部署檔案來建立新的 storageclass pan-local-storage 和本機 PV。

2. 驗證您已修改 pan-cn-mgmt-configmap 和 pan-cn-mgmt YAML 檔案。

EKS 中的範例 pan-cn-mgmt-configmap。

Session Contents Restored apiVersion: v1 kind:ConfigMap metadata: name: pan-mgmt-config namespace: kube-system data:PAN_SERVICE_NAME: pan-mgmt-svc PAN_MGMT_SECRET: panmgmt-secret # Panorama settings PAN_PANORAMA_IP: "x.y.z.a" PAN_DEVICE_GROUP: "dg-1" PAN_TEMPLATE_STACK: "temp-stack-1" PAN_CGNAME:"CG-EKS" # Intended License Bundle type - "CN-X-BASIC", "CN-X-BND1", "CN-X-BND2" # based on the authcode applied on the Panorama K8S plugin" PAN_BUNDLE_TYPE:"CN-X-BND2" #Non-mandatory parameters # Recommended to have same name as the cluster name provided in Panorama Kubernetes plugin - helps with easier identification of pods if managing multiple clusters with same Panorama #CLUSTER_NAME:"Clustername" #PAN_PANORAMA_IP2: "passive-secondary-ip" # Comment out to use CERTs otherwise bypass encrypted connection to etcd in pan-mgmt. # Not using CERTs for etcd due to EKS bug ETCD_CERT_BYPASS: "" # No value needed # Comment out to use CERTs otherwise PSK for IPSec between pan-mgmt and pan-ngfw # IPSEC_CERT_BYPASS: "" # No values needed

```
範例 pan-cn-mgmt.yaml
```

```
initContainers: - name: pan-mgmt-init image: <your-private-
registry-image-path>
```

containers: - name: pan-mgmt image: <your-private-registryimage-path> terminationMessagePolicy:FallbackToLogsOnError

3. 使用 Kubectl 來執行 yaml 檔案。

kubectl apply -f pan-cn-mgmt-configmap.yaml kubectl apply -f pan-cn-mgmt-slot-crd.yaml kubectl apply -f pan-cn-mgmt-slot-cr.yaml kubectl apply -f pan-cn-mgmt-secret.yaml kubectl apply -f pan-cn-mgmt.yaml

只有在您先前尚未完成使用 CN-Series 防火牆建立叢集驗證的服務帳戶時,才必須執行 pan-mgmt-serviceaccount.yaml。

4. 驗證 CN-MGMT Pod 已啟動。

這需要大約 5-6 分鐘。

使用 kubectl get pods -l app=pan-mgmt -n kube-system

NAME READY STATUS RESTARTS AGEpan-mgmt-sts-0 1/1 Running 0 27hpan-mgmt-sts-1 1/1 Running 0 27h

STEP 7| 部署 CN-NGFW Pod。

防火牆資料平面 CN-NGFW Pod 預設會部署為 DaemonSet。CN-NFGW Pod 執行個體可以保護節 點上最多 30 個應用程式 Pod 的流量。

1. 驗證您已修改 PAN-CN-NGFW-CONFIGMAP 和 PAN-CN-NGFW 中詳述的 YAML 檔案。

containers: - name: pan-ngfw-container image: <your-privateregistry-image-path>

2. 使用 Kubectl apply 來執行 pan-cn-ngfw-configmap.yaml。

kubectl apply -f pan-cn-ngfw-configmap.yaml

3. 使用 Kubectl apply 來執行 pan-cn-ngfw.yaml。

kubectl apply -f pan-cn-ngfw.yaml

4. 驗證所有 CN-NGFW Pod 都正在執行(叢集中一個節點會有一個 Pod)。

這是4節點內部部署叢集的範例輸出。

kubectl get pods -n kube-system -l app=pan-ngfw -o wide

NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES

pan-ngfw-ds-8g5xb 1/1 Running 0 27h 10.233.71.113 rk-k8-node-1
<none>

pan-ngfw-ds-qsrm6 1/1 Running 0 27h 10.233.115.189 rk-k8-vmworker-1 <none>

pan-ngfw-ds-vqk7z 1/1 Running 0 27h 10.233.118.208 rk-k8-vmworker-3 <none>

pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vmworker-2 <none>
STEP 8| 驗證您可以在 Kubernetes 叢集上看到 CN-MGMT、CN-NGFW 和 PAN-CNI。

kubectl -n kube-system get pods

- 0 27hpan-cni-5fhbg 1/1 Running
- 0 27hpan-cni-9j4rs 1/1 Running
- 0 27hpan-cni-ddwb4 1/1 Running
- 0 27hpan-cni-fwfrk 1/1 Running
- 0 27hpan-cni-h57lm 1/1 Running
- 0 27hpan-cni-h57lm 1/1 Running
- 0 27hpan-cni-j62rk 1/1 Running
- 0 27hpan-cni-lmxdz 1/1 Running
- 0 27hpan-mgmt-sts-0 1/1 Running
- 0 27hpan-mgmt-sts-1 1/1 Running
- 0 27hpan-ngfw-ds-8g5xb 1/1 Running
- 27hpan-ngfw-ds-qsrm6 1/1 Running
- 0 27hpan-ngfw-ds-vqk7z 1/1 Running
- 0 27hpan-ngfw-ds-zncqg 1/1 Running
- STEP 9 標註應用程式 yaml 或命名空間,讓來自其新 Pod 的流量重新導向至防火牆。

您需要新增下列註釋,以將流量重新導向至 CN-NGFW 來進行檢查:

annotations: paloaltonetworks.com/firewall: pan-fw

例如,對於「default」命名空間中的所有新 Pod:

kubectl annotate namespace default paloaltonetworks.com/
firewall=pan-fw

在部分平台上, pan-cni 在 CNI 外掛程式鏈中未作用時,可以啟動應用程式 Pod。
 若要避免這類情況,您必須在應用程式 Pod YAML 中指定這裡顯示的磁碟區。

volumes: - name: pan-cni-ready hostPath: path: /var/log/ pan-appinfo/pan-cni-ready type:Directory

STEP 10 | 在叢集中部署應用程式。

從 AWS Marketplace 部署 CN-Series

我可以在哪裡使用這個?	我需要哪些內容?
• CN-Series 部署	• CN-Series 10.1.x or above Container Images
	• Panorama 執行 PAN-OS 10.1.x 或更高版本
	• Helm 3.6 or above version client 對於使用 Helm 的 CN-Series 部署

您可以透過 AWS Marketplace 來授權 AWS EKS 上所部署的 CN-Series 防火牆作為 Kubernetes 服務。CN-Series 的授權可以是一個月、一年、兩年或三年,並且部署於 EKS 1.19 和更新版本或 Redhat Openshift 4.7 和更新版本。



此產品處於預覽階段。

使用此授權需要您更新附加至 Kubernetes 工作節點的 IAM 政策。



如果您使用透過 AWS Marketplace 購買的 PAYG 授權進行 CN-Series 部署,則請不要將 授權碼新增至 Kubernetes 的 Panorama 外掛程式。

STEP 1 完成下列先決條件。

1. 建立您的 EKS 或 Redhat OpenShift 叢集。

2. 部署 Panorama, 並安裝 Kubernetes 外掛程式。



如果您已經在AWS上部署授權的 Panorama 執行個體,則請略過這些步驟。

- 1. 在 Amazon EC2 執行個體上安裝 Panorama。
- 2. 安裝適用於 CN-Series 的 Kubernetes 外掛程式。
- 3. 安裝 Panorama 之後,請透過 cn-series-aws-marketplace@paloaltonetworks.com 向 CN-Series 團隊寄送電子郵件,以要求您 Panorama 的授權。請包括您的全名、公司電子郵 件、公司名稱、採購單號碼、AWS 帳戶名稱和 AWS 帳戶 ID。

- STEP 2| 將您的序號和授權套用至 Panorama。
 - 1. 登入 Panorama 網頁介面。
 - 2. 選擇 Panorama > Setup(設定) > Management(管理),然後按一下編輯 @ 圖示。
 - 輸入 Panorama Serial Number (序號) (包含在訂單完成電子郵件中),然後按一下 OK (確定)。
 - 4. 選取 Panorama > Licenses (授權)。
 - 5. 按一下 Activate feature using authorization code (使用授權碼啟動功能)。
 - 6. 輸入防火牆管理授權驗證碼,然後按一下 OK (確定) 以啟動授權。
 - 7. 驗證防火牆管理授權是否啟動。

裝置管理授權部分將顯示授權發佈的日期,授權到期時間,以及防火牆管理授權的說明。

Device Management License								
Date Issued January 22, 2020 Date Expires Never Description Device management license to manage up to 1000 device								
License Management								
Retrieve license keys from license server Activate feature using authorization code Manually upload license key								

STEP 3 | 更新您的 IAM 政策, 並將該政策附加至您的 Kubernetes 工作節點。

- 1. 登入 AWS 管理主控台, 並開啟 IAM 主控台。
- 1. 選取 Policies (原則)。
- 2. 從政策清單中, 選取 AWSLicenseManagerConsumptionPolicy 和 AWSMarketplaceMeteringRegisterUsage。
- 3. 選取 Actions (動作),然後選擇 Attach (附加)。
- 4. 選取要附加政策的工作節點身分識別。選取身分識別之後,請按一下 Attach policy (附加 政策)。

STEP 4| 下載 plugin-serviceaccount.yaml, 並在部署 Helm 圖表之前套用該 yaml。kubectl apply -f plugin-serviceaccount.yaml

- STEP 5| 存取 AWS Marketplace, 然後找到 CN-Series for AWS Marketplace 清單。
- **STEP 6** 按一下 Continue to Subscribe (繼續訂閱)。
- STEP 7 | 輸入要購買的授權數目。每個授權權利都相當於您的 CN-Series 部署所使用的一個 vCPU。 如需符合部署需求所需 vCPU 數目的指導,請參閱 CN-Series 系統需求和 CN-Series 效能和調整 規模。

STEP 8| 按一下 Continue to Configuration (繼續設定)。這會將授權新增至您的 AWS 帳戶。

- 1. 選取 Helm Chart (Helm 圖表) 作為 Fulfillment option (履行選項)。
- 2. 選取 Software version (軟體版本)的最新版本。

< Product Detail Subscribe Configure

Configure this software

Choose a fulfillment option and software version to launch this software.

Helm Chart	~	Supported services Amazon EKS 				
		Amazon EKS Anywhere				
		Setr-managed Kubernetes				
oftware version						

- **STEP 9**| 按一下 Continue to Launch (繼續啟動)。
 - 選取您的 Launch target(啟動目標)—Amazon-managed Kubernetes(Amazon 受管理的 Kubernetes)或 Self-managed Kubernetes(自我管理的 Kubernetes)。自我管理模式部署在 Redhat OpenShift 上。
 - **2.** 遵循 AWS Marketplace 清單中所顯示的 Launch Instruction (啟動指示)。指示會根據您的啟動目標而不同。
 - Amazon 受管理的 Kubernetes
 - 1. 複製 Launch Instruction (啟動指示)的 Step 1 (步驟 1)中的命令。
 - 2. 更新所複製的命令,以新增您的叢集名稱。

--cluster <ENTER_YOUR_CLUSTER_NAME_HERE>

3. 在您的 EKS 叢集上執行所複製的命令。

Step 1: Create an AWS IAM role and Kubernetes service account							
Use the following command to create an AWS IAM role and Kubernetes service account.							
kubectl create namespace kube-system	•	🗋 Сору					
eksctl create iamserviceaccount \							
name my-service-account (namespace kube-system \	-						

- 4. 複製 Launch Instruction (啟動指示)的 Step 2 (步驟 2)中的 Helm 圖表命令。
- 5. 更新 Helm 安裝資訊以包括您的 Panorama IP、Panorama 驗證金鑰、裝置群組名稱、 範本堆疊名稱和收集群組名稱。將 cluster.deployTo 設定為 eks。

```
helm install cn-series-helm \ --namespace kube-system ./
awsmp-chart/* \ --set serviceAccount.create=false
    \ --set serviceAccount.name=my-service-
account \ --set cluster.deployTo=eks \ --set
panorama.ip=Panorama-IP \ --set panorama.ip2=Panorama-
IP2 \ --set panorama.authKey=000xxxxxxxx
    \ --set panorama.deviceGroup=Panorama-DG
    \ --set panorama.template=Panorama-TS \
```

set panorama.cgName=Panorama-CG \set imagePullSecrets=awsmp-image-pull-secret		
Step 2: Launch the software		
Use the following commands to launch this software by installing a Helm chart on your Amaz	on EKS	cluster.
export HELM_EXPERIMENTAL_OCI=1		🗋 Сору
aws ecr get-login-password \		
region us-east-1 helm registry login \		
username AWS \	•	

- 6. 更新上面列出的值之後,請在您的 EKS 叢集上執行 helm install 命令。
- 自我管理的 Kubernetes
 - **1.** 完成 [Launch Instruction (啟動指示)]中的 [Step 1 (步驟 1)] 以建立授權權杖和 IAM 角色。

```
Step 1: Create a license token and IAM role
Choose Create token to generate a license token and AWS IAM role. These will be used to access the AWS License
Manager APIs for billing and metering. You can use an existing token if you have one.
```

Create token

- 2. 複製 Launch Instruction (啟動指示)的 Step 2 (步驟 2)中的命令。
- 3. 更新所複製的命令,以新增權杖值。

AWSMP_TOKEN=<CREATE_TOKEN_ABOVE>

4. 在 OpenShift 叢集上執行所複製的命令。

```
Step 2: Save the token and IAM role as a Kubernetes secret
```

Use the following commands to save the license token and IAM role as a secret in the cluster. The secret will be used in a following step when launching the software.



- 5. 複製 Launch Instruction (啟動指示)的 Step 3 (步驟 3)中的 Helm 圖表命令。
- 6. 更新 Helm 安裝資訊以包括您的 Panorama IP、Panorama 驗證金鑰、裝置群組名稱、 範本堆疊名稱和收集群組名稱。將 cluster.deployTo 設定為 openshift。

```
helm install cn-series-helm \ --namespace kube-system ./
awsmp-chart/* \ --set serviceAccount.create=false
    \ --set serviceAccount.name=my-service-account
    \ --set cluster.deployTo=eks|openshift \ --set
```

<pre>\set panorama.template=Panorama-TS \set panorama.cgName=Panorama-CG \set imagePullSecrets=awsmp-image-pull-secret</pre>	
Step 3: Launch the software	
Use the following commands to launch the software by installing a Helm chart from Amazon Elastic Container R (ECR).	egistry
export HELM_EXPERIMENTAL_OCI=1	ору
aws ecr get-login-password \region us-east-1 helm registry login \username AWS \	

7. 更新上面列出的值之後,請在您的 OpenShift 叢集上執行 helm install 命令。

STEP 10 | 驗證是否已將授權成功新增至您的帳戶。

- 1. 導覽至 AWS 授權管理員。
- 2. 選取 **Granted Licenses**(已授與的授權),然後找到 CN-Series for AWS Marketplace 清 單。
- 3. 在 Entitlements (權利)下,您可以查看授權總數和所使用授權數。

Entitlements An entitlement is a right to use, access, or												
Q Search										<	1 >	۲
Name	▼ Value	▼ Max count	⊽ Us	sage	∇	Units	⊽ 01	verages	∇	Allow check in		∇
vCPU	-		1000		5	Count	No	ot Allowed		Allowed		
AWS::Marketplace::Usage	Enabled		-		- 1	None	-			Not Allowed		

STEP 11 | 驗證 CN-Series 防火牆是否出現在 Panorama 中。

- 1. 登入 Panorama。
- 若要檢視 CN-MGMT Pod,請選取 Panorama > Managed Devices (受管理的裝置) > Summary (摘要)。

DAS	HBOARD AC	C MONITOR	C Device POLICIES	Groups – OBJECTS	← Templates NETWORK [DEVICE PANO	DRAMA	AMA		it v 🛛 🕞		
								Mar				
$Q \subset$	Q(11 ite											
					IP Address							
	DEVICE NAME	VIRTUAL SYSTEM	MODEL	TAGS	SERIAL NUMBER	IPV4	IPV6	VARIABLES	TEMPLATE	DEVICE STATE		
$\sim \square$	/rp-gke5-dg (1/2 De	vices Connected): Sha	ared > vrp-gke5-dg									
	mp1 pan-mgmt-sts-0		PA-CTNR		805(10.12.0.17		Create	vrp-gke5-ts	Connected		
	mp2 pan-mgmt-sts-1				866	10.12.2.20		Create	vrp-gke5-ts	Connected		

 若要驗證是否已授權 CN-NGFW Pod,請選取 Panorama > Plugins(外掛程式) > Kubernetes > License Usage(授權使用情況),並驗證是否已為每個 Pod 配置授權權 杖。

C Device Gro DASHBOARD ACC MONITOR POLICIES	ups Templates _ DBJECTS NETWORK DEVICE PANORAMA				
٩(
NODE ID	FIREWALL POD NAME	LICENSE STATUS	NODE STATUS		
rr-cluster-1 (3 Nodes, 3/3 Licensed)					
-rr-cluster-1-default-pool-e2d3de37-1jfz	pan-ngfw-ds-4qflb		Successfully licensed.		
			Created at: -06-11 22:30:37 UTC		
-rr-cluster-1-default-pool-e2d3de37-xhq5	pan-ngfw-ds-z5z8k		Successfully licensed.		
			Created at: -06-11 22:30:37 UTC		
-rr-cluster-1-default-pool-e2d3de37-jn8z	pan-ngfw-ds-vr8hx		Successfully licensed.		
			Created at: -06-11 22:30:36 UTC		

TECH**DOCS**

在 AliCloud (ACK) 上部署 CN-Series 防火牆作為 Kubernetes 服務

我可以在哪裡使用這個?	我需要哪些內容?
• CN-Series 部署	• CN-Series 10.1.x or above Container Images
	• Panorama 執行 PAN-OS 10.1.x 版或 PAN-OS 10.2.x 版本

在您檢閱 CN-Series 核心建置區塊以及使用 CN-Series 保護 Kubernetes 工作負載中的工作流程高階 概觀之後,就可以在 AliCloud ACK 平台上開始部署 CN-Series 防火牆來保護相同叢集內容器之間 的流量,以及容器與其他工作負載類型之間的流量(例如虛擬機器和裸機伺服器)。

您必須確保套用 plugin-serviceaccount.yaml 檔案。如需詳細資訊,請參閱建立叢集驗證的服務帳戶。



• 當您在 ACK 上部署 CN-Series 防火牆作為 Kubernetes 服務時,必須要有 panplugin-cluster-mode-secret。

開始之前,請確保 CN-Series YAML 檔案版本與 PAN-OS 版本相容。如需詳細資訊,請參閱 CN-Series YAML。

完成下列程序,以在 ACK 平台上部署 CN-Series 防火牆作為 Kubernetes 服務:

STEP 1| 設定 Kubernetes 叢集。

若要在 ACK 中建立叢集,請執行以下操作:

1. 使用您的 RAM 登入憑證登入 RAM 使用者登入。

RAM User Logon	
* Username	
<uset>@<comman> or <uset>@<campany.onaliyun.com or="" td="" username@company.alias.<=""></campany.onaliyun.com></uset></comman></uset>	
Next	
Logon with Alibaba Cloud Account	

- 2. 在頂部導覽列中, 選取您要建立叢集的區域, 並根據您的業務需求選取資源群組。
 - 建立叢集之後,無法變更叢集區域。
 - 依預設會顯示您帳戶中的所有資源群組。
- 3. 在搜尋列功能表上搜尋 Container Service for Kubernetes (Kubernetes 的容器服務)。

	C-) Alibaba Cloud 🛛 🗢 Workbench				Q container		0	Expenses	ICP	Enterprise	Support	Tickets	£	>_	¢.	Å	
_	-	_				Consoles (4) >					Resources >						
	分 Overview	Resource Manage	er	Operation & Mo	nitor	Container Registry	/	_									
						Container Service	for Kubernete	s			Found not						
						Elastic Container I	Instance										
	My Navigation					Serverless Contair	ner Service				Quick Acces	s >					
	Recent – Cloud Service																
	Home Console	Container Service fo	Elastic IF	P Address	Elasti	Documentation (10	027) >				Found not						
						Container详情	Applicatio	on Rea	al Time Monitori	n							
	Resource Access M	Cloud Enterprise Ne	Containe	er Registry	File S	Custom Container	简介		Function Com	bute							
(Custom Shortcuts					容器 (Container)			Mobile P								
	Add Shortcut					创建Custom Conta	ainer函数		Function Comp	oute							
						创建Custom Conta	ainer函数		Function Comp	oute							
(Cloud Architecture					API (249) >											
	Conorato Mu Architectur		n the left to	execute the exclute of		ExecContainerCon	mmand E	lastic	Container Insta	nce							
	Generate My Architectur	Click the button of	n the left to	generate the architect	ure of A	DeleteContainerG	roup E	lastic	Container Insta	nce							
1	Recommended Architecture Ter	nplates				DescribeContainer	rLog E	lastic	Container Insta	nce							
						RestartContainerG	Group E	lastic	Container Insta	nce							

4. 按一下Create Kubernetes Cluster (建立 Kubernetes 叢集)。



5. 若要建立叢集,您必須依照精靈的引導來設定軟體參數、硬體參數和基本參數。如需設定這 些必要參數的詳細資訊,請參閱在 ACK 上建立叢集。下列步驟代表在 ACK 平台上建立叢集 範例:



Alibaba 雲端 ACK 上的 CN-Series 僅支援 Terway 網路外掛程式。

• 選取 VPC, Network Plugin, (PC、網路外掛程式和 vSwitch)。

VPC	vpc-xiaofang (vpc-2zew	kdrmhjezfcm2ibotn, 10.1 🔻 💭			
	🔗 Create VPC 🔗 Plan Ku	bernetes CIDR blocks in VPC networks			
Network Plug-in	Flannel	Terway You carnot chan	ge the network plug-in after	the cluster is created.	S How to select a network plug
	Kubernetes cluster				
	IPVLAN (The inclusive	ENI mode uses a combination of IPVLAN and o	BPF as the virtualization teo	hnology. Only Alibaba Cl	loud Linux is supported)
	Support for NetworkPo	licy Policy-based network traffic control is pro			
vSwitch	Select 1~5 vSwitches. We	recommend that you select vSwitches in diffe	rent zones to ensure high av	ailability for the cluster.	
					No. 60 No.
	inside	vsw-2zej8ngtuyp6r6qy1eoil	Beijing Zone C	10.101.2.0/24	252
	outside	vsw-2zerc7sn6emhk9mq4lzy7	Beijing Zone C	10.101.1.0/24	252
	mgmt	vsw-2zepoq1k3a7zx1pk2iafs	Beijing Zone C	10.101.0.0/24	252
	cn-pod2	vsw-2ze5v4zny1j58rzzdd19t	Beijing Zone A	10.101.102.0/24	243

• 選取 POD vSwitch。

Pod vSwitch	All Z	oneA (2/1)				
		bour cross				
		inside	vsw-2zej8ngtuyp6r6qy1eoil	Beijing Zone C	10.101.2.0/24	252
		outside	vsw-2zerc7sn6emhk9mq4lzy7	Beijing Zone C	10.101.1.0/24	252
		mgmt	vsw-2zepoq1k3a7zx1pk2iafs	Beijing Zone C	10.101.0.0/24	
	✓	cn-pod2	vsw-2ze5v4zny1j58rzzdd19t	Beijing Zone A	10.101.102.0/24	252
	~	cn-pod1	vsw-2zex1z33iu6ffu72ko5ry	Beijing Zone A	10.101.101.0/24	252
		cn-node-ip	vsw-2ze5nzjrkzio4sbf5d2n9	Beijing Zone A	10.101.10.0/24	
	🔗 Crea	ate vSwitch				
	The pref	ix length of the VSwite	ch address is recommended to be no greater than	19 bits.		
Service CIDR	192.168	8.0.0/16	 Recommended Value:192.168.0.0/16 			
	Valid val	ues: 10.0.0.0/16-24.	172.16-31.0.0/16-24. and 192.168.0.0/16-24.			

• 選取 Configure SNAT, Access to API Server, Security Groups(設定 SNAT、API 伺服器 存取、安全性群組)和 Resource Group(資源群組)。

Configure SNAT	Configure SNAT for VPC
	Nodes and applications in the cluster have Internet access. If the VPC that you select has a NAT gateway, ACK uses this NAT gateway to enable Internet
	VPC does not have a NAT gateway, ACK automatically creates a NAT gateway and configures SNAT rules. For more information, see NAT Gateway bill
Access to API Server	slb.s1.small SLB Instance Specifications
	by default, an internal-facing SLB instance is created for the API server. You can modify the specification of the SLB instance. If you delete the SLB in
	access the API server.
	Z Expose API Server with EIP
	If you select this check box, the internal-facing SLB instance is associated with an EIP. This allows you to access the API server of the cluster over the
RDS Whitelist	Select RDS Instance
	We recommend that you go to the RDS console to add the CIDR blocks of the specified nodes and specified pods to a whitelist of the RDS instance. (
	RUS instance is not in the running state, the node pool cannot be scaled out.
Security Group	Create Basic Security Group Create Advanced Security Group
	To use a basic security group, the total number of pods in the cluster cannot exceed 2,000 if you select the Terway network plug-in. Otherwise, you r
	advanced security group. Security group overview
Deletion Protection	Enable
	Cluster Cannot Be Deleted in Console or by Calling API
Resource Group 💿	default resource group 🔍 🗸
	To create a resource group, click here.

• 選取節點集區設定的Quantity, Operating System (數量、作業系統和Logon Type (登入 類型)。

_	
	instance type is used. The actual instance types used to create nodes are subject to inventory availability.
	ecs.sn2nec.xlarge (4 vCPU 16 GiB, General purpose type family with enhanced network performance
Quantity	2 unit(s) 🗘
	Nodes will be evenly assigned to your selected vswitches.
	A standard managed cluster can contain up to 100 nodes. To use a larger cluster, create a professional managed cluster.
System Disk	SSD Disk T20 GIB
Mount Data Disk	You have selected 0 disks and can select 10 more.
C Dick Parameters and	_
O Disk Parameters and	+ Add Data Disk 1 th Recommended
Performance	
Operating System	Alibaba Cloud Linux 3.2104
Security	Disable Reinforcement based on classified protection CIS Reinforcement
Reinforcement	
Logon Type	Key Pair Password Later
Key Pair	key-par-Alibaba 🔹 🖸
	You can be an to the ECC expendence a key asin

SACK Billing SLB Price: ¥ 0.100 /Hours EIP Price: ¥ 0.800 /GB ECS Price: ¥ 4.91 /Hours Prev:Cluster Configurations Next:Configurations

• 移至Public Network tab (公用網路頁籤) 取消勾選Service Discovery, Volume Plugin (服務探索、磁碟區外掛程式)和Monitoring Agents (監控代理程式)核取方塊。

Create Cluster	Managed Kubernetes	Dedicated Kubernetes	Serverless Kubernetes	Managed Edge Kubernetes	Register Cluster
Cluste	r Configurations	· • •	Node Pool Configurations	3 Comp	oonent Configurations
Ingress	Do Not Install	Nginx Ingress	ALB Ingress	MSE Ingress	
	SLB Network Type	Public Network	nternal Network		
	SLB Specifications slb	s1.small	•		
Service Discovery	Install NodeLocal DNS	SCache			
	Runs a DNS caching age DNSConfig injection. View	nt on each node to improve D w Details	NS resolution performance and st	ability. After you install NodeLocal D	NSCache, you must enable automat
Volume Plug-in	CSI		unsel	ection all	
	How to select the volume	plug-in			
	Dynamically Provision	Volumes by Using the Defau	It NAS File Systems and CNFS Vie	w Details.	
	5 GiB of Capacity NAS sp Details	pace or 1 GB of Performance	NAS space is offered free of charg	ge to each ACK cluster for 12 month	s. For more information, see 🔗 Prici
Monitoring Agents	Install CloudMonitor A	gent on ECS Instance 🛛 🖒 Re	commended		
	Enable Prometheus M	onitoring 🖒 Recommended	S Pricing Details		
	Provides basic monitoring	g and alerts for Kubernetes o	lusters free of charge. Details		

O.220 June
 O.220 June
 O.200 June
 EIP Price: ¥ 0.800 /GB
 ECS Price: ¥ 4.91 /Hours
 Prev:Node Pool Configu

6. 選取 Terms of Service (服務條款) 核取方塊。

	RAM Role Authorization Check Dependent Service Activation Status	Passed			
	Dependent Service Activation Status				
		Passed			
	Auto Scaling Status Check	Passed			
	Service Quota Check	Passed			
	System Disk Size Check	Passed			
	Data Disk Size Check	Passed			
	Account Balance Check	Passed			
ennis of Service	Create ECS instances, configure a public key Create a security group that allows access t Create a NAT gataway and Elastic IP address Create a RAI role and grant it the following instances, CloudMontor, VPC, Log Service, I settings. Create an Internal SLB instance and open po When you use a dedicated or managed Kube ensure cluster stability. I rime cluster creation reads, rule created resort I have read and understand the preceding s	to enable SSH logon from m. othe VPC network over ICMP. ses. permissions: query, create, ar and NAS. The Kubernetes cluiv rt 6443. metes cluster, the system co arces will be charged. We rect tatement. I also have read and	ides to other nodes, and configure the Ku le ECS instances, create and delete cloud amically creates SLB instances, cloud di ag and monitoring information about cont of that you belete unused resources at the t the Terms of Service and Disclaimer.	ubernetes cluster through Cloudinit. I disks, and all permissions on SLB sks, and VPC routing rules based on you rol components on master nodes to help reamest opportunity.	ir)
			20 Mors 0 800		

- **7.** 按一下 Create Cluster (建立叢集)。
- 8. 檢查 API 伺服器金鑰以登入 ACK 叢集,並將以下內容複製到本機電腦上的 \$HOME/.kube/ config。

< ACK-For-PM +	All Clusters / ACK-For-PM
Cluster Information	ACK-For-PM
▼ Nodes	
Node Deals	Overview Basic Information Connection Information Cluster Resources Cluster Logs Cluster Tasks
Node Pools	
Nodes	Connect to a Kubernetes cluster using Kubecti
Namesnaces and Quota	Insue and compare kubers, nor more mormation, see instal and compare kubecu. Order and a second seco
	2. Ourright Countries.
 Workloads 	Public Access Internal Access Generate temporary subacoming Revoxe subacoming Revoxe subacoming
Dealerseete	
Deployments	Condensities Fundameters for the Second Se
StatefulSets	CHURINAL ANI DA LAN D. 2026. I S22 BI UICES
DaemonSets	apiVersion: v1 Copy
	clusters:
Jobs	- cluster:
CronJobs	server: https://47.93.191.191:6443
	cettiidate-autority-data: toori diguiditi apputning roomatison to ising a sole of ising a burger of the sole of th
Pods	TFVRINGTUILB6021#1Web212xVdGOVIEVIES80V3WM182xWW4KaEIHTD81H12:TVNNdvDFVVIEVIEREV3CH1KV0peV201bCRHVDN00FVEFR.deilBEXd0xkEx/Wond016b11EA13T
Custom Resources	RJeElgstvnrrv5ch9E0xdxakerTvnjd0r3murmuvFLrxdob11xnw51bwh2zFRBvUjnTlaC0W9URFdGc2FxSmhzbUvnwTJ4dmrxUxgKrxpBUkjnTl2C0U10210Mv1tvnl1bVYvW1hnd2c
h 11-1-1-1	nRWINGTBHQINXRINJY JHEUUVCQVFVQUE0SUJEd0F322dFSwpBb0lCqVFDGGxczVYVVQvTnIxdXBidkloutetRMmCoXBayjJ4VHB321FUTzY2dmFNU3U6OctNS2JmVDNnvEdICllyYUM
Network	akfhQVVVZGhPcTBNaklLb2xpUlRQOTBLRNQyZnVPZEU4RXE2U1p5WEI1UUIXUHp2czVMRlhYVm1xR0oKhjVBNjRvQzk0QXVycWI4SjJVbUJyVTBrSWxRZVQOLytjVU1VZ09aRU5KUjhXc
Configurations	Eniuenjinnenpraineuprakkjinaakkvenivsuapprissuarksensikinconkskunskmuvarbaidese Vhirge 4 afennijer 11 prisi pulis of podes 20 porksit 2 tiz prevense se s
	k100nFRFUGem2XBUhBaIIF12G10Se1VdidWIkF10UM0VzBVd0RTV2e0vYXT.255aUBDRkTvNIdavnz1F2V37dK50UV±V28FPkFnT1TB0IddINecOII1BNEdBBUVkPBdF0i93IIIUVBd01Dekt

9. 取得 ACK 叢集 API 伺服器公用端點位址。

E C-) Alibaba Cloud	🏠 Workbench 🛛 All Resources 👻 🦑 Global 🛛 Q. Search Expenses ICP Enterprise Support Tickets 🤂 🖾	1
< ACK-For-PM -	All Clusters / ACK-For-PM	
Cluster Information	ACK-For-PM	
▼ Nodes		
Node Pools	Overview Basic Information Connection Information Cluster Resources Cluster Logs Cluster Tasks	
Nodes	Basic Information	
Namespaces and Quota	Cluster.ID: cdbs7cs2/1489848789846ac303022718e Region: Cfilar (Beijing) Tirke Zone: Asia/Shanghai	De
▼ Workloads	Cluster Information	
Deployments	API Server Public Endpoint https://47.93.191.191:6443 Change EIP Unbind EIP	
StatefulSets	API Server Internal Endpoint https://10.101.10.169:6443 Set access control 🔗 Troubleshoot connection issues	
DaemonSets	Service CIDR 192.168.0.0/16	
CronJobs	RRSA OIDC Enable RRSA & Configure RAM permissions for service accounts to isolate permissions among pods	
Pods	Kube-proxy Mode ipvs	
Custom Resources	Network Plug-in terway-enlip	
Network	Custom Certificate SANs Update	
 Configurations 	Testing Domain *.cdbc7ca2f48a84bf898f5ac303022718e.cn-beijing.alicontainer.com Rebind Domain Name	



請驗證叢集具有足夠的版本。預設 GKE 節點集區規格不適用於 CN-Series 防火牆。您必須確保 叢集具有 CN-Series 先決條件資源以支援防火牆:

kubectl get nodes

kubectl describe node <node-name>

檢視命令輸出之「容量」標題下的資訊,以查看所指定節點上可用的 CPU 和記憶體。 CPU、記憶體和磁碟儲存體配置將取決於您的需求。請參閱 CN-Series 效能與擴充性。 您必須確保您擁有以下資訊: • 收集「端點 IP 位址」,以在 Panorama 上設定 API 伺服器。

Cluster Definition						?
	Name	on_prem-clstr				
Des	cription					
API server	address	10.2.				
	Туре	Native-Kubernet	es			\sim
Credent	tials					*
Label Selector La	bel Filte	er Custom C	ertificate			
Q					$0 \text{ items} \rightarrow$	\times
TAG PREFIX	NAMES	PACE	LABEL SELECTOR FILTER	,	APPLY ON	
↔ Add ⊖ Delete						

Panorama 使用此 IP 位址來連線至 Kubernetes 叢集。

• 從 Panorama 收集範本堆疊名稱、裝置群組名稱、Panorama IP 位址和日誌收集器群組名稱 (選用)。

Collector Group	
General Monitoring	Device Log Forwarding Collector Log Forwarding Log Ingestion
Name	rp-cg1
Log Storage	Total: 1.53 TB,Free: 75.30 GB
Min Retention Period (days)	[1 - 2000]
Collector Group Members	Q 1item >>>
	rpgcpnew(RPGOOGGKEPRA1)
<i>U</i> .	
	(+) Add (-) Delete
	Enable log redundancy across collectors
	Forward to all collectors in the preference list
	Enable secure inter LC Communication Log collector on local panorama is using the secure client configuration from 'Panorama -> Secure Communication Settings'
	OK Cancel

如需詳細資訊,請參閱建立父系裝置群組和範本堆疊。

- 收集 VM 驗證金鑰以及自動註冊 PIN ID 和值。
- 將映像檔下載至其中的容器映像檔儲存庫位置。
- STEP 2 (選用)如果您已在 Panorama 的 Kubernetes 外掛程式中設定自訂憑證,則必須執行下列命令 來建立憑證密碼。請不要從 ca.crt 變更檔案名稱。pan-cn-mgmt.yaml 和 pan-cn-ngfw.yaml 中的 自定憑證數量是選用項目。

kubectl -n kube-system create secret generic custom-ca --fromfile=ca.crt

STEP 3 | 编輯 YAML 檔案,以提供部署 CN-Series 防火牆所需的詳細資料。

apiVersion: v1 kind:ConfigMap metadata: name: pan-mgmt-config namespace: kube-system data:PAN_SERVICE_NAME: pan-mgmtsvc PAN_MGMT_SECRET: pan-mgmt-secret # Panorama settings PAN_PANORAMA_IP: "<panorama-IP>" PAN_DEVICE_GROUP: "<panoramadevice-group>" PAN_TEMPLATE_STACK: "<panorama-template-stack>" PAN_CGNAME: "<panorama-collector-group>" PAN_CTNR_MODE_TYPE: "k8sservice"

apiVersion: v1 kind:Secret metadata: name: pan-mgmt-secret namespace: kube-system type:Opaque stringData: # Panorama Auth Key PAN PANORAMA AUTH KEY: "<panorama-auth-key>" # Thermite Certificate retrieval CN-SERIES-AUTO-REGISTRATION-PIN-ID: "<PIN Id>" CN-SERIES-AUTO-REGISTRATION-PIN-VALUE: "<PIN-Value>"

您必須確定 YAML 檔案上的 PAN_PANORAMA_IP 參數值符合您的實際 Panorama IP 位址,如下 圖所示:

← → C A Not Secure (35.196.181.54/#) anorama::dev-dg::panorama/templates						@ ☆ Ø @ &		
uli vm-panorama	D	ASHBOARD A		r Dev OR POLICIE	vice Groups ¬ S OBJECTS	r Templates ר NETWORK DEVICE	PANORAMA	ti • • •
Panorama 🗸 🗸								ť
C Access Domain	Q	.(2 items
Authentication Profile		NAME	DESCRIPTION	TYPE	STACK	DEVICES	VARIABLES	DEVICE KEY-VALUE TA
Authentication Sequence		K9S-Network-Setup		template			Manage	
User Identification		k9s stack		template	KOC Natural Catur		Managem	No Douison in the stack
Data Redistribution		KOS-SLICK		template-stack	K65-Network-Setup		Manage	NO Devices in the stack
Managed Devices								
C Templates								
Device Groups								
Managed Collectors								
Collector Groups								
Certificate Management								
Certificates								
Certificate Profile	1							
SSL/TLS Service Profile								
C SCEP								
SSH Service Profile								
Log Ingestion Profile								
Log Settings								
Server Profiles								
SNMP Trap								
Syslog								
Email								
L HTTP								
RADIUS								
LD SCP			-					

Palo Alto Networks Kubernetes Security - CN Series 的儲存庫中提供最新版本的 *YAML* 檔案。您可以從 *Switch* (切換) *branches/tags* (分支/標籤) 下拉式功能表中 選取最新的分支或標籤。

您必須確定 YAML 檔案上 PAN_DEVICE_GROUP 和 PAN_TEMPLATE 的參數值符合您在 Panorama 上建立的裝置群組和範本堆疊名稱,如下圖所示:

	HBOARD ACC I	C Device C	roups T OBJECTS NETWO	emplates ¬ RK DEVICE	PANORAMA		‡⊸ िन ⊩न
Panorama							
Image: Construction Image: Construction Image: Constrediate Construction Image: Co							E
Authentication Prohle Authentication Sequence Sequence Just dentification Device Quarantine Managed Devices Device Groups Managed Collectors							2 items
Subser Identification	IAME 🔺	DESCRIPTION	AUTHORIZATION CODE	SW VERSION	MASTER DEVICE	DEVICES/VIRTUAL SYSTEM	REFERENC
C Device Quarantine Managed Devices C Templates Device Groups Managed Collectors	G Shared						
Managed Devices Control Templates Device Groups Managed Collectors	🕞 dev-dg						k8s-stack
Collector Groups Certificate Management Certificates Certificates Scrificate Profile SSL/TLS Service Profile SSL/TLS Service Profile Cog Settings Cog Settings SSH Server Profile Server Profiles SMMP Trap Syslog Email Cog HTTP							

您必須確定 PAN_PANORAMA_CG_NAME 的參數值與您建立的日誌收集器名稱相同。

	DASUD	OAPD						+ ~ ~
	DASHB	OARD	ACC MONI	HOR POLICIES	OBJECTS	NETWORK DE	PANORAMA	
Panorama 🗸 🗸								
C Access Domain	Q							11
Re Authentication Profile								
Authentication Sequence		1E		REDUNDANCY ENABL	ED FOR	WARD TO ALL COLLECTO	ORS COLLECTORS	LOG REDISTRIBUTIO
Ser Identification	rp-ci	g1					demo-panorama	none
Data Redistribution								
Device Quarantine								
Managed Devices								
Templates								
Device Groups								
Managed Collectors								
Collector Groups								
Certificate Management								
Certificates								
Certificate Profile								
SSL/TLS Service Profile	1							
SCEP								
SSH Service Profile								
Log Ingestion Profile								
Log Settings								
Server Profiles								
SNMP Trap								
Syslog								
Email								
HTTP								
RADIUS								
ED SCP								

如需詳細資訊,請參閱 CN-Series yaml 檔案的可編輯參數,以取得詳細資料。

STEP 4| 部署 CN-NGFW 服務。執行下列步驟:

部署為 Kubernetes 服務時,可以將 CN-NGFW 執行個體部署在安全性節點上,並將應用程式 Pod 流量重新導向至可用的 CN-NGFW 執行個體以進行檢查和強制執行。

請驗證您已使用 pan-cni-serviceaccount.yaml 來建立服務帳戶。
 請參閱建立叢集驗證的服務帳戶。

使用 Kubectl 來執行 pan-cni-configmap.yaml。

```
kubectl apply -f pan-cni-configmap.yaml
```

3. 使用 kubectl 來執行 pan-cn-ngfw-svc.yaml。

```
kubectl apply -f pan-cn-ngfw-svc.yaml
```



必須在 pan-cni.yaml 之前部署此 yaml。

4. 使用 Kubectl 來執行 pan-cni.yaml。

```
kubectl apply -f pan-cni.yaml
```

- 5. 請驗證您已修改 pan-cni-configmap 和 pan-cni YAML 檔案。
- 6. 執行下列命令, 並確認您的輸出與下列範例相似。

	<pre>@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke</pre>	(vi	eries-mktplace)\$	kubectl	get pods	-n	kube-system	grep	pan-cni
pan-cni	-nmqkf		Running 0		2m11s				
pan-cni	-wjrkq		Running 0		2m11s				
- pan-cni	-xrc2z		Running 0		2m12s				
	<pre>@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke</pre>	(vi	eries-mktplace)\$						



Alicloud ACK 僅支持基於標準度量的自動縮放。

STEP 5| 部署 CN-MGMT StatefulSet。

管理平面預設會部署為可提供容錯的 StatefulSet。最多可以將 30 個防火牆 CN-NGFW Pod 連線 至 CN-MGMT StatefulSet。

- 1. (僅為靜態佈建 PV 的必要項目) 部署 CN-MGMT StatefulSet 的「永久性磁碟區 (PV)」。
 - 1. 建立目錄,以符合 pan-cn-pv-local.yaml 中所定義的本機磁碟區名稱。

您需要至少2個背景工作節點上有六(6)個目錄。請登入將部署 CN-MGMT StatefulSet 以建立目錄的每個背景工作節點。例如,若要建立名稱為/mnt/pan-local1到/ mnt/pan-local6 的目錄,請使用下列命令:

```
mkdir -p /mnt/pan-local1 /mnt/pan-local2 /mnt/pan-local3 /
mnt/pan-local4 /mnt/pan-local5 /mnt/pan-local6
```

2. 修改 pan-cn-pv-local.yaml。

符合 nodeaffinity 下方的主機名稱,並驗證您已修改上面您在 spec.local.path 中建立的目錄,然後部署檔案來建立新的 storageclass pan-local-storage 和本機 PV。



在 pan-cn-mgmt.yaml 檔案中, 您在建立 volumeClaimTemplates 時必 須新增儲存類別名稱 alicloud-disk-available。

例如:

storageClassName: alicloud-disk-available

所有 PV 的儲存大小應該至少為 20 G。

2. 驗證您已修改 pan-cn-mgmt-configmap 和 pan-cn-mgmt YAML 檔案。

範例 pan-cn-mgmt.yaml

```
initContainers: - name: pan-mgmt-init image: <your-private-
registry-image-path>
```

containers: - name: pan-mgmt image: <your-private-registryimage-path> terminationMessagePolicy:FallbackToLogsOnError

3. 使用 Kubectl 來執行 yaml 檔案。

kubectl apply -f pan-cn-mgmt-configmap.yaml kubectl apply -f pan-cn-mgmt-slot-crd.yaml kubectl apply -f pan-cn-mgmt-slot-cr.yaml kubectl apply -f pan-cn-mgmt-secret.yaml kubectl apply -f pan-cn-mgmt.yaml 只有在您先前尚未完成建立叢集驗證的服務帳戶時,才必須執行 pan-mgmt-serviceaccount.yaml。

4. 執行下列命令,驗證已啟動 CN-MGMT Pod:

```
kubectl get pods -l app=pan-mgmt -n kube-system
這需要大約 5-6 分鐘。
```

STEP 6 | 部署 CN-NGFW Pod。

- 驗證您已修改 PAN-CN-NGFW-CONFIGMAP 和 PAN-CN-NGFW 中詳述的 YAML 檔案。 containers: - name: pan-ngfw-container image: <your-privateregistry-image-path>
- 2. 使用 Kubectl apply 來執行 pan-cn-ngfw-configmap.yaml。

kubectl apply -f pan-cn-ngfw-configmap.yaml

3. 使用 Kubectl apply 來執行 pan-cn-ngfw.yaml。

kubectl apply -f pan-cn-ngfw.yaml

4. 驗證 CN-NGFW Pod 正在執行。

kubectl get pods -n kube-system -l app=pan-ngfw -o wide

STEP 7 | 驗證您可以在 Kubernetes 叢集上看到 CN-MGMT、CN-NGFW 和 PAN-CNI。

kubectl -n kube-system get pods

STEP 8 標註應用程式 yaml 或命名空間, 讓來自其新 Pod 的流量重新導向至防火牆。

您需要新增下列註釋,以將流量重新導向至 CN-NGFW 來進行檢查:

annotations: paloaltonetworks.com/firewall: pan-fw

例如,對於「default」命名空間中的所有新 Pod:

kubectl annotate namespace default paloaltonetworks.com/ firewall=pan-fw

STEP 9 在叢集中部署應用程式。

TECH**DOCS**

在 OpenShift 上部署 CN-Series

我可以在哪裡使用這個?	我需要哪些內容?						
• OpenShift 環境上的 CN-Series 部署	• CN-Series 10.1.x or above Container Images						
	• Panorama 執行 PAN-OS 10.1.x 或更高版本						

pan-cni 會保護應用程式 Pod 的預設「eth0」介面上的流量。如果您有多位置 Pod,則可以設定 CN-NGFW Pod 來保護其他介面,而這些介面已設定橋接器型連線來與其他 Pod 或主機通訊。根據應用程式 YAML 中的註釋,您可以設定 CN-Series 防火牆,檢查來自連接至每個 Pod 之所有介面或所選取數目之介面的流量。

pan-cni 不會建立任何網路,因此,不需要 IP 位址(如其他 CNI 外掛程式)。



需要 PAN-OS 10.1.3 或更新版本,以在 OpenShift 上部署「CN-Series 作為 Kubernetes 服務」。此外, OpenShift 上的「CN-Series 作為 Kubernetes 服務」只能保護介面 ethO 的安全。

STEP1| 部署叢集。

請參閱雲端平台廠商文件,並驗證 CN-Series 支援 OpenShift 版本和 CNI。檢閱 取得 CN-Series 防火牆的映像檔案 和 CN-Series yaml 檔案中的可編輯參數。

STEP 2 | 利用使用 CN-Series 保護 Kubernetes 工作負載中包含的工作流程。

您必須建立服務認證,以及部署防火牆 YAML。



註:如果您的服務認證檔案超過 10KB,則必須對檔案進行 gzip 處理,然後先對壓 縮檔案執行 base64 編碼,再上傳檔案內容或將其貼入 Panorama CLI 或 API。

STEP 3 | 設定 PAN-CNI 外掛程式來使用 Multus CNI 外掛程式。

OpenShift 上的 Multus CNI 是作為呼叫其他 CNI 外掛程式的「中繼外掛程式」。針對每個應用 程式,您必須:

1. 在每個 Pod 命名空間中部署 PAN-CNI NetworkAttachmentDefinition

```
kubectl apply -f pan-cni-net-attach-def.yaml -n <target-namespace>
```

2. 修改「應用程式 YAML」。

在您部署 pan-cni-net-attach-def.yaml 之後,請在應用程式 Pod yaml 中新增註釋:

```
paloaltonetworks.com/firewall: pan-fw
```

k8s.v1.cni.cncf.io/networks: pan-cni

如果您在上方註釋中具有其他網路,則請在需要檢查的網路後面新增 pan-cni。pan-cni 後面的網路則不會進行重新導向和檢查。



如果您的 Pod 具有多個網路介面,則必須在 pan-cni-configmap.yaml 的 「interfaces」下方指定您要 CN-NGFW Pod 檢查流量的介面名稱。

例如:

template: metadata: annotations: paloaltonetworks.com/ firewall: pan-fw k8s.v1.cni.cncf.io/networks: bridge-conf, macvlan-conf, sriov-conf, pan-cni



CN-Series 目前在 RedHat OpenShift 4.13 及更高版本上以 Kubernetes 服務部署模式 和 DaemonSet 模式支援 OVN-Kubernetes 容器網路介面 (CNI) 外掛程式。

TECH**DOCS**

在 OpenShift Operator 中樞上部署 CN-Series

我可以在哪裡使用這個?	我需要哪些內容?						
• CN-Series 部署	• CN-Series 10.1.x or above Container Images						
	• Panorama 執行 PAN-OS 10.2.x 及以上版本						

CN-Series 容器防火牆現已在 RedHat Openshift platform Operator 中樞上提供。您可以直接從 RedHat Operator 中樞部署、設定和操作 CN-Series 容器防火牆。

在 Openshift Operator 中樞上使用 CN-Series 的先決條件:

以下是在 Openshift Operator 中樞部署 CN-Series 防火牆的先決條件:

- 授權 CN-Series 防火牆。Panorama 上的 Kubernetes 外掛程式管理 CN-Series 防火牆授權。產生您的授權碼,並在您準備好部署 CN-Series 防火牆時將其放在手邊。如需詳細資訊,請參閱授權 CN-Series 防火牆。
- 在 Panorama 上產生 VM 驗證金鑰。
- 在 CN-Series 防火牆上安裝裝置憑證。
- 建立叢集驗證的服務帳戶。
- 部署 Panorama一您必須使用 Panorama 來設定、部署和管理 CN-Series 防火牆部署。如需部署和 設定 Panorama 設備的詳細資訊,請參閱設定 Panorama。
- 安裝 CN-Series 防火牆的 Kubernetes 外掛程式。
- OpenShift 叢集必須遵守 CN-Series 先決條件。
- 確保您有權存取 Palo Alto Networks 客戶服務入口網站 (CSP) 並且具有 Flex 積分。
- 確保您是 RedHat 客戶,擁有 OpenShift 授權以及有權在 OpenShift 中建立資源的帳戶。
- 確保 OpenShift 叢集遵循 CN-Series 先決條件。

如需詳細資訊,請參閱如何在 RedHat Openshift Operator 中樞上輕鬆地部署 CN-Series。

在 **OpenShift Operator** 中樞上部署 **CN-Series**:

pan-cni 會保護應用程式 Pod 的預設 eth0 介面上的流量。如果您有多位置 Pod,則可以設定 CN-NGFW Pod 來保護其他介面,而這些介面已設定橋接器型連線來與其他 Pod 或主機通訊。根據應用程式 YAML 中的註釋,您可以設定 CN-Series 防火牆,檢查來自連接至每個 Pod 之所有介面或所選取數目之介面的流量。

pan-cni 不會建立網路,因此不需要像其他 CNI 外掛程式那樣的 IP 位址。

您需要 PAN-OS 10.2 或更高版本才能在 OpenShift Operator 中樞上部署 CN-Series。

- 以下是在 Redhat OpenShift Operator 中樞上部署 CN-Series 防火牆的步驟:
- **STEP 1** 登入 Redhat OpenShift 容器主控台。
- **STEP 2**| 前往 Operator, 然後按一下 OperatorHub。



STEP 3| 在 Operator 搜尋方塊中輸入 Palo Alto。

STEP 4| 按一下 pan-cn-series-operator。



當您按下時,安裝視窗將會開啟 pan-CN-Series -operator 圖格。

STEP 5| 按一下 Install (安裝) 在 OpenShift 叢集上安裝 pan-CN-Series Operator。



在執行此處指定的後續部署步驟之前,請完成預先安裝步驟。

如果您的服務認證檔案超過 10KB,則必須對檔案進行 gzip 處理,然後先對壓縮檔案執行 base64 編碼,再上傳檔案內容或將其貼入 Panorama CLI 或 API。

STEP 6 | 在導覽功能表上,前往 **Installed Operators**(已安裝的 **Operator**),然後按一下您已安裝的 **pan-CN-Series -operator**。

Red Hat OpenShift Container Platfo	m			\$ 3	Ð	0	kube:admin -			
📽 Administrator		You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in								
		Project: openshift-operators 🔹								
Home	*									
Overview		Installed Operators								
Projects		Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators documentation g. Or create an Operator and ClusterServiceVersion using the								
Search		Operator SDK g.								
API Explorer		Name Variable Search by name								
Events		Name † Managed Namespaces ‡ Status Last updated	Pre	vided AP	ls					
Operators	*	pan-cn-series-operator All Namespaces Succeeded I minute ago	Pa	CnSeries	Firewall		I			
OperatorHub		Networks								
Installed Operators										
Workloads	>									
Networking										
Storage										
Builds	>									
Monitoring										
STEP 7| 按一下 Create Instance (建立實例)。

Red Hat OpenShift Container Platform			13 G	0
S Administrator	You are logged in as a temporary administrative user. Update the <u>cluster OAuth configuration</u> to allow others to log in			
	Project: openshift-operators 👻			
Home	1.0.0 provided by Palo Alto Networks			
Overview	Details YAML Subscription Events PanCnSeriesFirewall			
Projects				
Search	Provided APIs	Provider		
		Palo Alto Ne	tworks	
API Explorer	OCSD DancaSaries Eirawall	Constant at		
Events		I minute a	ao	
	Not available		.90	
Operators		Links Pag Co Soria	··· Operator	
		https://pan-e	cn-series-or	erator.doma
OperatorHub				
Installed Operators		Not available		
	Description	THE CHARGE		
	Description			
Workloads	Palo Alto CN-Series NGFW (container firewall)			
N. A	Product Overview: The CN-Series firewall enables you to:			
Networking				
	2. Stall Leger-7 trainic visibility and control within the cluster			
Storage	3. Prevent known and unknown inbound attacks			
	4. Apply egress filtering to prevent data exfiltration and unwanted outbound connections			
Builds	5. Dynamically scale security without compromising DevOps agility.			
	6. Ensure a frictionless CI/CD pipeline deployment.			
Monitoring	7. Unify management across all your firewalls using Panorama.			
	Deploy CN-Series as-a-Kubernetes service and manage the fleet of firewalls from Panorama, alongside our hardware and VM-Series NGFW appliances to ensure			

STEP 8| 輸入唯一的運算數 Name (名稱)。

Project openabilit-openators •	
Name*	
cseler-sample	
Labels	
apprilosterd	
Minimum Replices for DP	
- 2 *	
Minimum Replicas for DP	
CPU Linit (DP)	
- 1 +	
Desired number of CPUs for DP	
Memory Linit (DP)	
406i	
Desired memory for DP	
CPU Linit (MP)	
- 2 +	
Denired number of CPUs for MP	
Mensiry Linit (MP)	
306	
Desired memory for MP	
Penarana IP Address	
denorme IP	
Panorana IP Address	
Secondary Panarama IP Address (Optional)	
Secondary Panoaran IP Address for HA deployment	
vm-auth-key from Pancrama	
v eteknolika kuruut kuruu	
vanama bunko uroop	
or Wales every wyw	
· executive during output	

STEP 9 輸入 DP 和 MP Pod 的 Minimum Replicas for DP (DP 的最小複本數)、Memory Unit (記憶 體單元)和 vCPU Limit (vCPU 限制)。如需 vCPU 限制的資訊,請參閱 CN-Series 關鍵效 能度量。

STEP 10 | 輸入 Panorama IP Address (Panorama IP 位址)。

Panorama Template Stack
Panorama Log Collector Group Name
<pre><pre>cpanorama-collecto-group></pre></pre>
Panorama Log Collector Group Name
Customer Support Portal PIN ID (Optional)
Customer Support Portal PINID
Customer Support Portal PIN Value (Optional)
Customer Support Portal Value
Customer Support Portal Alternate URL (Optional)
Customer Support Portial Alternate URL
DPImage
gcziójpan-en-series/panos_en_ngfw
The docker image name and version of CN Series DP
DP Image Version
preferred-10.2
DP Image Version
MP image
gozio/pan-on-series/panos_cn_mgmt
The docker image name and version of CN Series MP
MP Image Version
preferred-10.2
MP Image Version
PAN CNI image
gczia/pan_cni
The docker image name and version of CN Series pan-cni
PAN CNI Image Version
preferred
PAN CNI Image Version
Create Cancel

STEP 11 | 選用 輸入 HA 部署的 Secondary Panorama IP Address (次要 Panorama IP 位址)

- STEP 12 | 輸入 CN-Series Panorama Auth Key (驗證金鑰)。
- **STEP 13** | 輸入 Panorama Device Group (Panorama 裝置群組)。
- **STEP 14** | 輸入 Panorama Template Stack (Panorama 範本堆疊)。
- STEP 15 | 輸入 Panorama Log Collector Group Name (Panorama 日誌收集器群組)。
- STEP 16 | 選用 輸入客戶支援入口網站 (CSP) Pin ID、Pin value (Pin 值) 和 Alternate URL (替代 URL)。
- STEP 17 | 根據您的 PAN-OS 版本,連結到 DP、MP 和 CNI 的適當映像。CN-Series 容器登錄主控台。
- **STEP 18** | 按一下 Create (建立)。
- STEP 19 | 在導覽功能表上,前往 Pod。

STEP 20 | 選擇專案 OpenShift-operators, 然後前往 kube-system 以檢視作為運算數一部分部署的 CNI、管理和資料平面 Pod 的名稱和狀態。

Red Hat OpenShift Container Platform							\$ 3	Ð	0
🕫 Administrator 🗸 👻		You are logged in as a temporary ad	ministrative user. Upd	date the <u>cluster OAuth configuration</u> to	allow others to log in.				
Home 🗸	Project: openshift-operators								
Overview Projects	Create Project								
Search API Explorer	All Projects default	Ready 1	Restarts 1	Owner 1	Memory I	CPU I		Created	
Events	kube-node-leasekube-public	2/2	0	controller-manager-	80.3 MiB	0.001	cores	•	3 minute
Operators ~	kube-systemopenshift			3901794319					
OperatorHub Installed Operators	openshift-apiserver openshift-apiserver-operator								
Workloads 🗸	 openshift-authentication openshift-authentication-operator 								
Pads Deployments	 openshift-cloud-credential-operator openshift-cluster-csi-drivers 								
DeploymentConfigs StatefulSets	openshift-cluster-machine-approver								
Secrets ConfigMaps									
CronJobs									

您可以在 Panorama 上檢查防火牆部署狀態。**Device State**(裝置狀態)將在部署之後不到 5 分鐘的時間內變改為 [Connected (已連線)]。



STEP 21 | 設定 PALO ALTO NETWORKS-CNI 外掛程式以與 Multus CNI 外掛程式一起使用。

OpenShift 上的 Multus CNI 是作為呼叫其他 CNI 外掛程式的 meta-plugin。針對每個應用程式, 您必須:

1. 執行以下命令,在每個 Pod 命名空間中部署 pan-cni-net-attach-def.yaml。

```
kubectl apply -f pan-cni-net-attach-def.yaml -n <target-namespace>
```

2. 修改「應用程式 YAML」。

在您部署 pan-cni-net-attach-def.yaml 之後,請在應用程式 Pod yaml 中新增以下註釋:

```
paloaltonetworks.com/firewall: pan-fw
```

k8s.v1.cni.cncf.io/networks: pan-cni

如果您在上方註釋中具有其他網路,則請在需要檢查的網路後面新增 pan-cni。pan-cni 後面的網路則不會進行重新導向和檢查。



如果您的 Pod 具有多個網路介面,則必須在 pan-cni-configmap.yaml 檔 案的interfaces (介面)區段下指定您希望 CN-NGFW Pod 檢查流量的介面名 稱。

例如:

範本: 中繼資料: 註釋: paloaltonetworks.com/firewall: pan-fw k8s.v1.cni.cncf.io/networks: pan-cni