

在雲端和本地部署 CN-Series 防火牆

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-cluster-mode-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-plugin-cluster-mode-secret*。

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

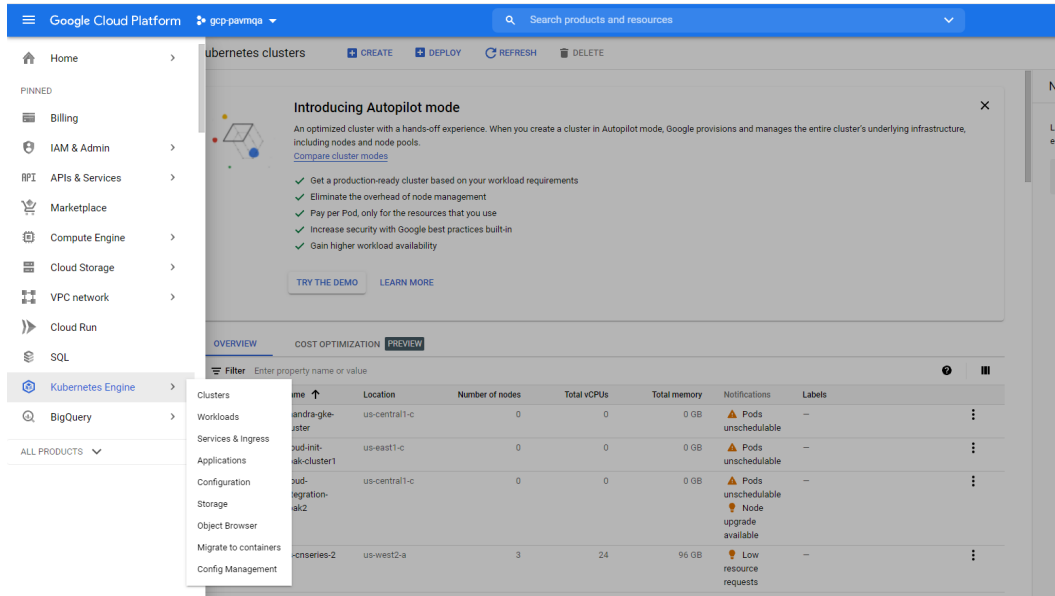
我可以在哪裡使用這個？	我需要哪些內容？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • Panorama 執行 PAN-OS 10.1.x 或更高版本 • Helm 3.6 or above version client 用於使用 Helm 進行 CN-Series 部署

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

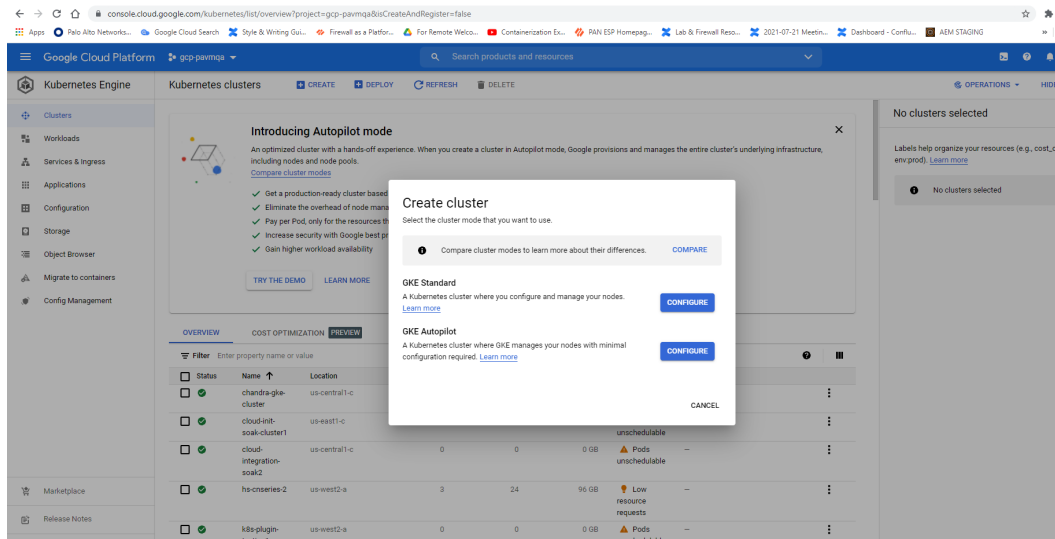
STEP 1 | 設定 Kubernetes 叢集。

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）。



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）。



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）。



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。

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 Definition

Name: on_prem-clstr

Description:

API server address: 10.2...

Type: Native-Kubernetes

Credentials:

Label Selector | Label Filter | Custom Certificate

0 items

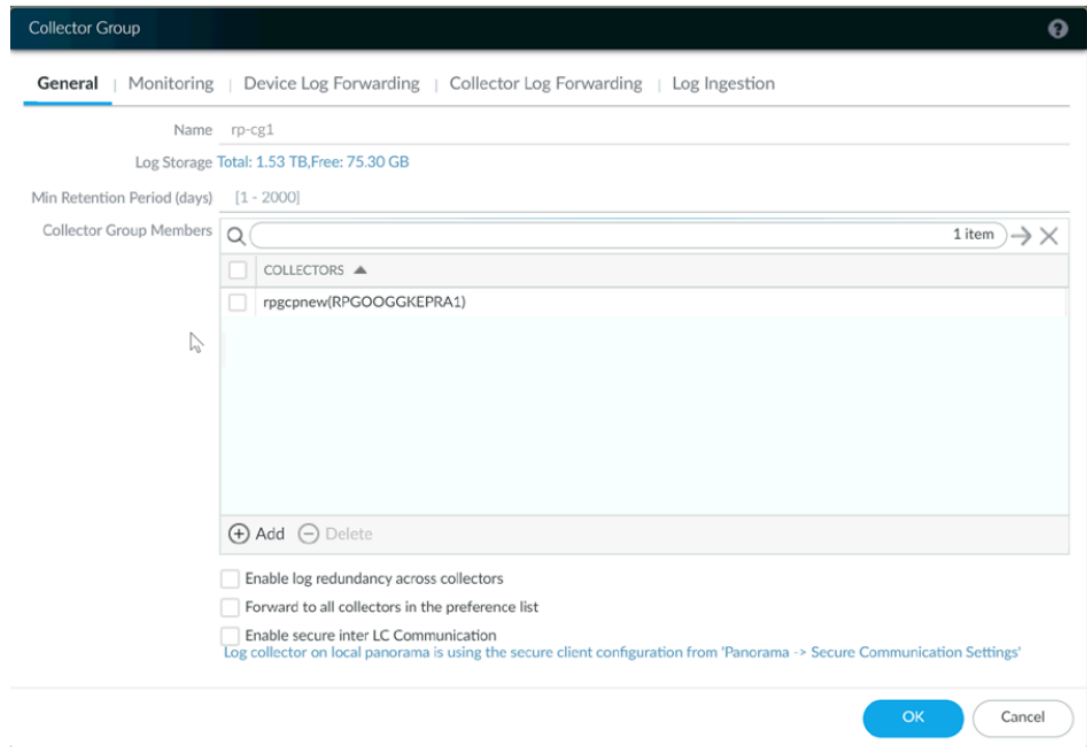
TAG PREFIX	NAMESPACE	LABEL SELECTOR FILTER	APPLY ON
------------	-----------	-----------------------	----------

+ Add - Delete

Validate OK Cancel

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）。



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。

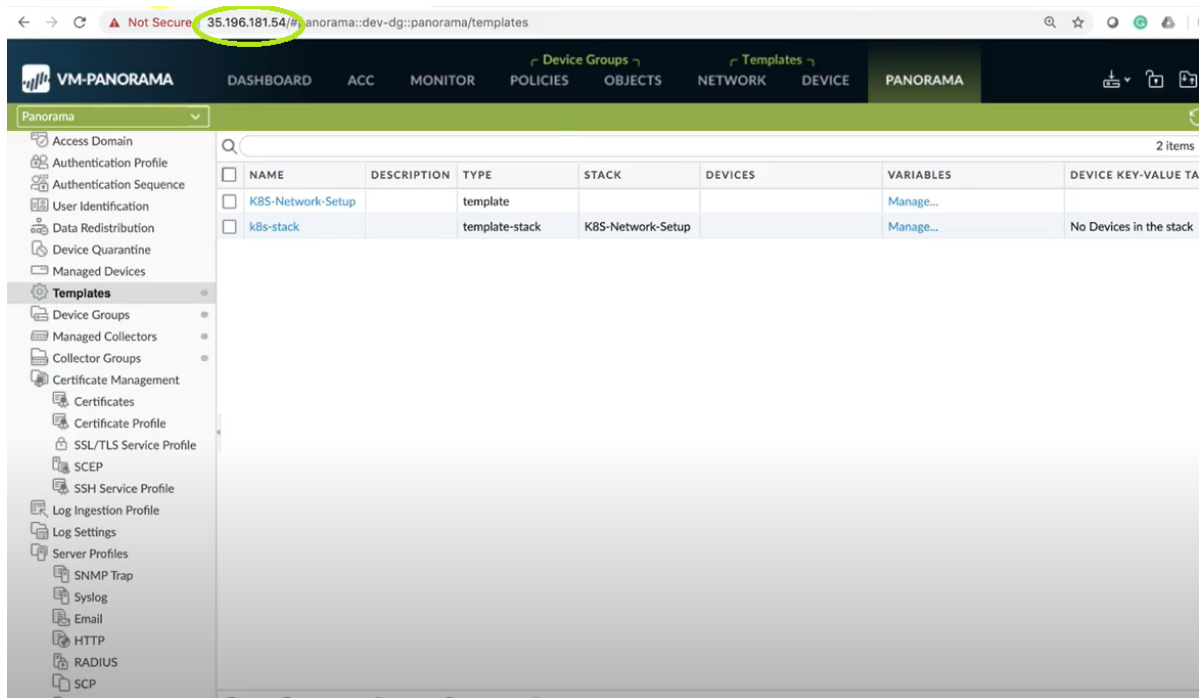
STEP 2 | （選用）如果您已在 Panorama 的 Kubernetes 外掛程式中設定自訂憑證，則必須執行下列命令來建立憑證密碼。請不要從 `ca.crt` 變更檔案名稱。`pan-cn-mgmt.yaml` 和 `pan-cn-ngfw.yaml` 中的自定憑證數量是選用項目。

```
kubectl -n kube-system create secret generic custom-ca --from-file=ca.crt
```

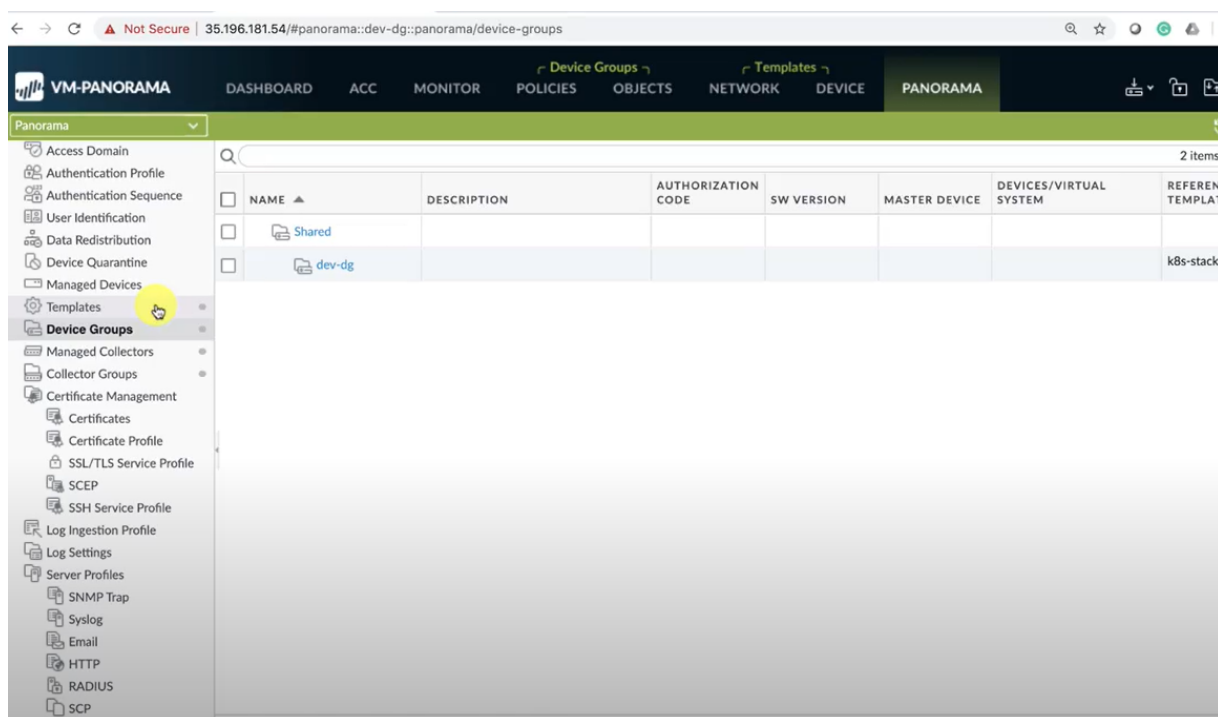
STEP 3 | 編輯 YAML 檔案，以提供部署 CN-Series 防火牆所需的詳細資料。

```
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: ""
```

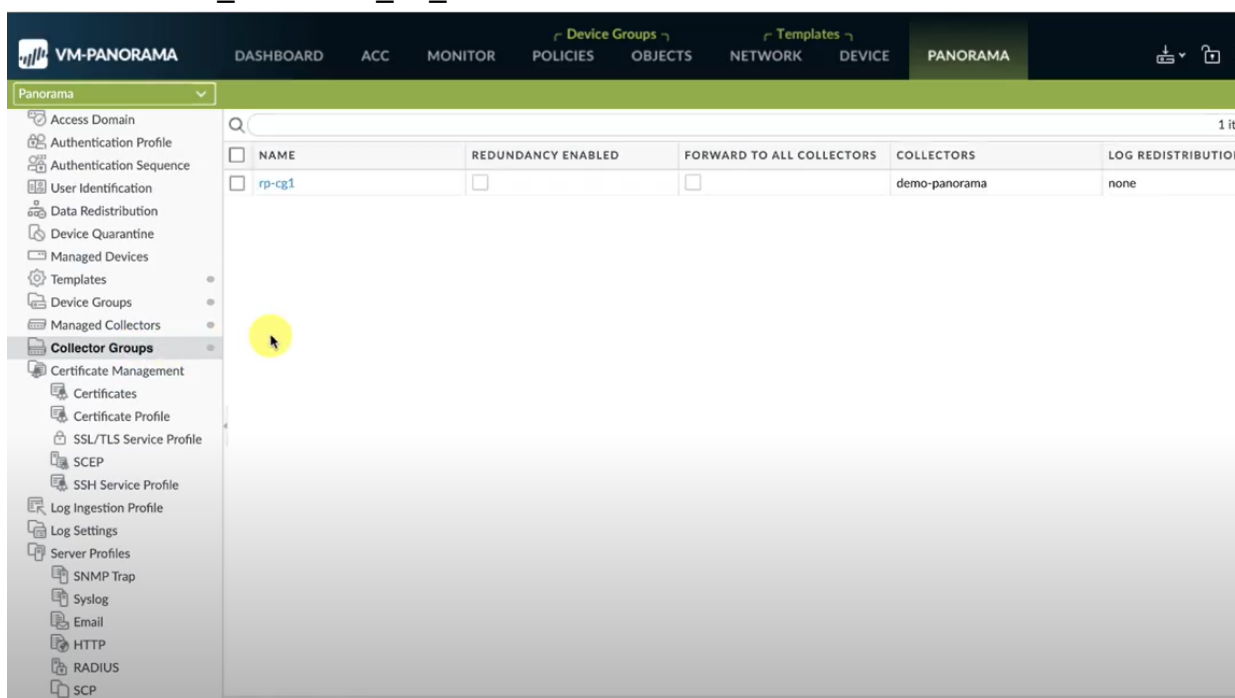
您必須確定 YAML 檔案上的 PAN_PANORAMA_IP 參數值符合您的實際 Panorama IP 位址，如下圖所示：



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：



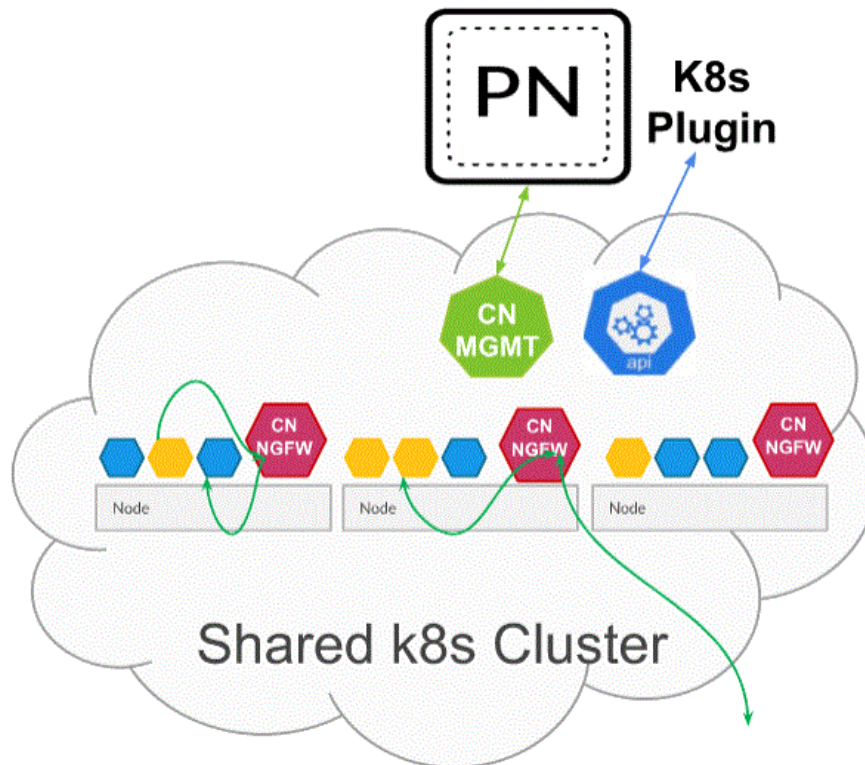
您必須確定 `PAN_PANORAMA_CG_NAME` 的參數值與您建立的日誌收集器名稱相同。



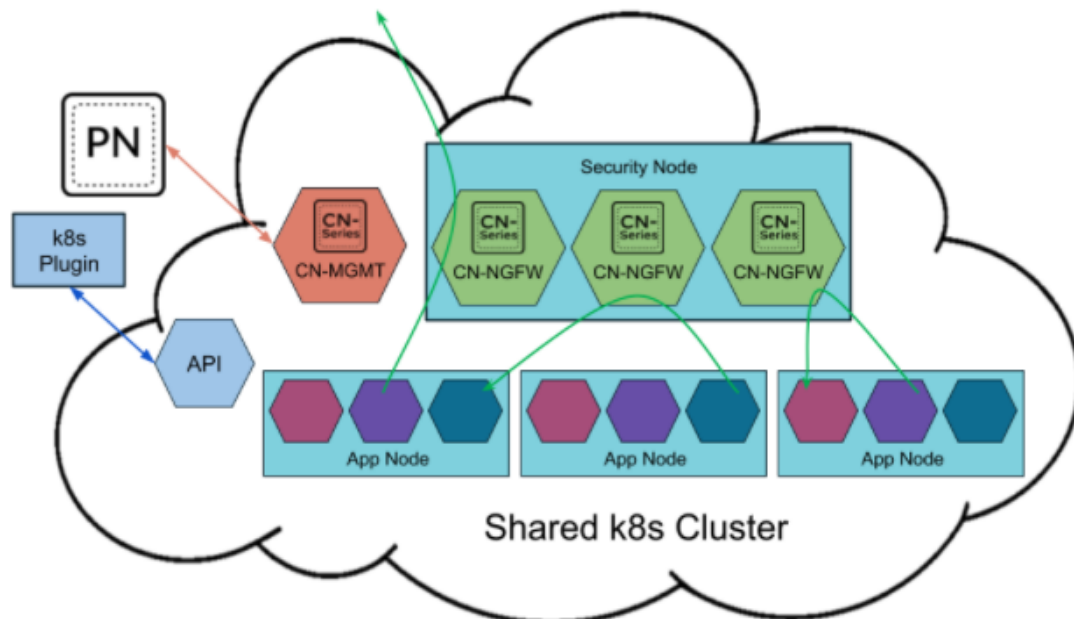
如需詳細資訊，請參閱 [CN-Series 部署 yaml 檔案](#) 中的可編輯參數以取得詳細資料。

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。



1. 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 `KubectI` 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 series-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
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v series-mktplace) $
```

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。

```
apiVersion: v1 kind:ConfigMap metadata: name: pan-mgmt-
config 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-
template-stack>" PAN_CGNAME: "<panorama-collector-
group>" # ctr mode: "k8s-service", "k8s-ilb-service"
```

```
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-registry-
image-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-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 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
```

5. 使用 HPA_NAME（取代為名稱）來修改 **pan-cn-hpa-dp.yaml** 和 **pan-cn-hpa-mp.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-adapater.yaml


```
kubectl apply -f pan-cn-adapater.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

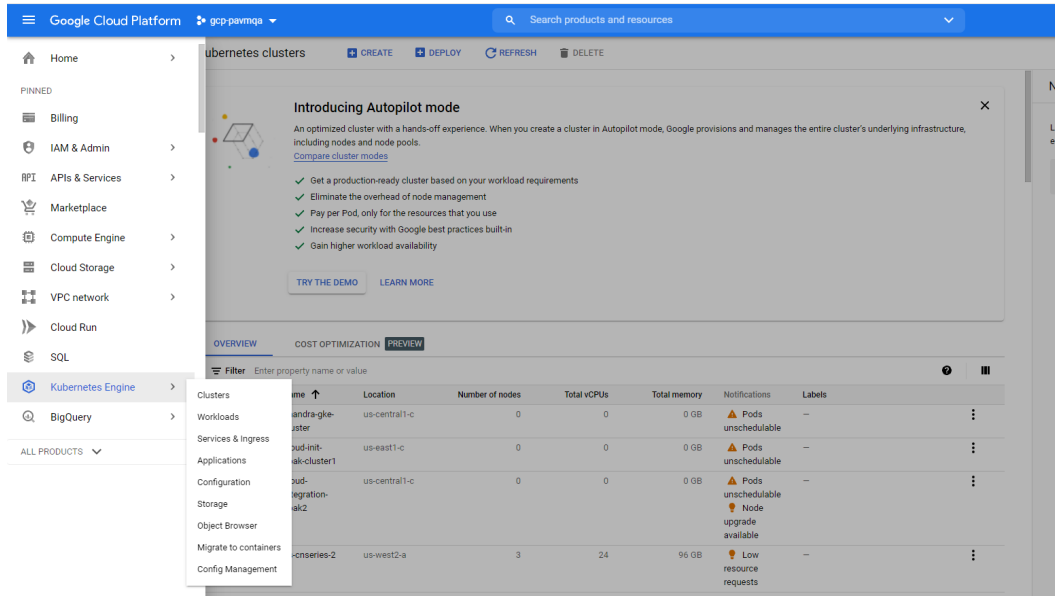
我可以在哪裡使用這個？	我需要哪些內容？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • Panorama 執行 PAN-OS 10.1.x 或更高版本 • Helm 3.6 or above version client 用於使用 Helm 進行 CN-Series 部署

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

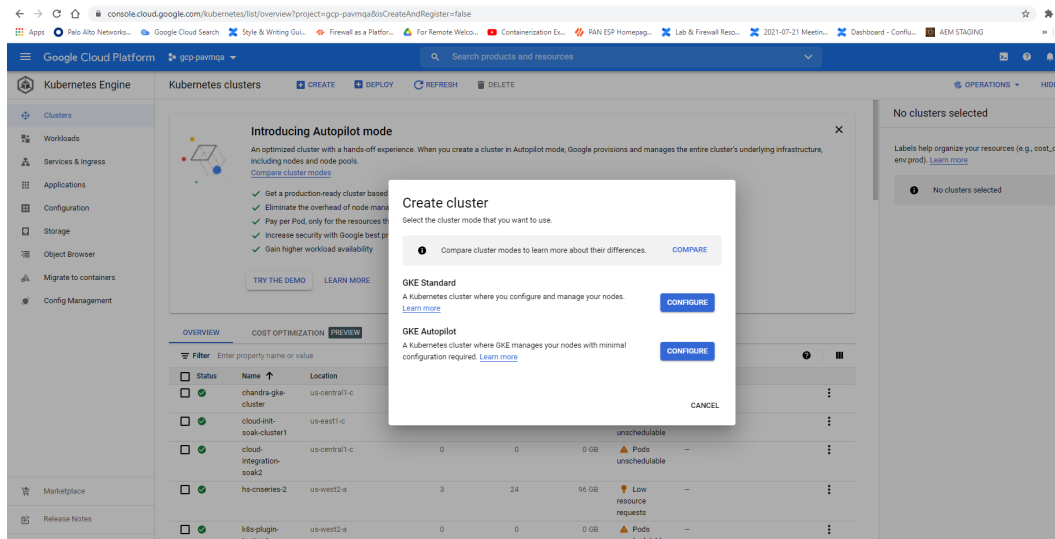
STEP 1 | 設定 Kubernetes 叢集。

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）。



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）。



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）。



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。

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

Name: on_prem-clstr

Description:

API server address: 10.2...

Type: Native-Kubernetes

Credentials:

Label Selector | Label Filter | Custom Certificate

0 items

TAG PREFIX	NAMESPACE	LABEL SELECTOR FILTER	APPLY ON
------------	-----------	-----------------------	----------

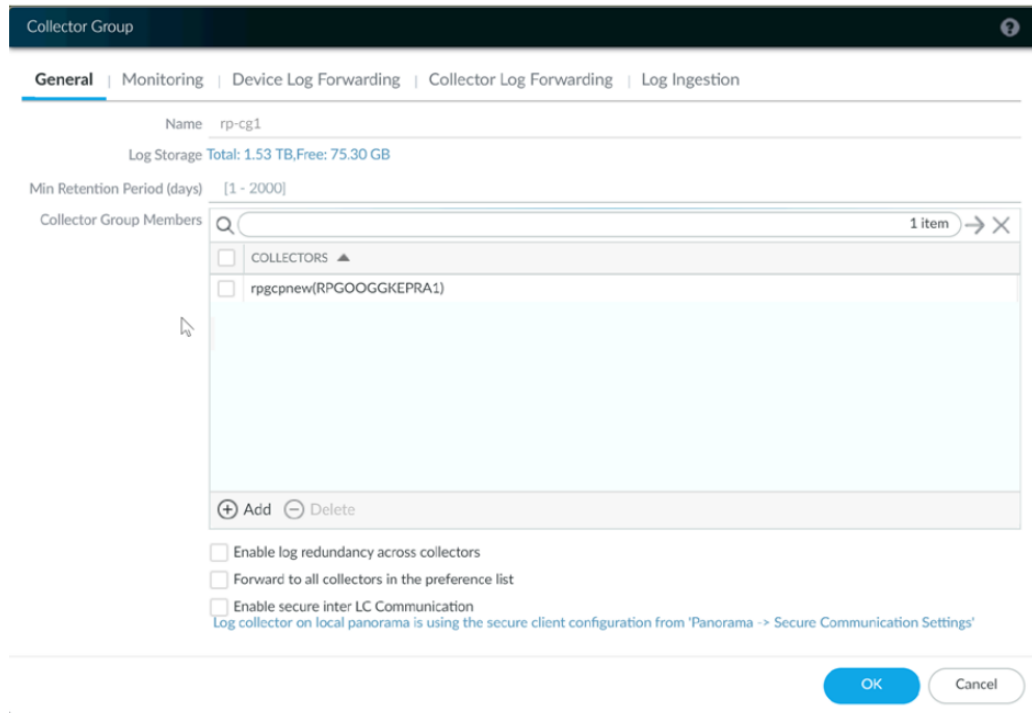
+ Add - Delete

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）。



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 --from-file=ca.crt
```

STEP 3 | 編輯 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 (v series-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
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v series-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 system-  
wide#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。
```

```
#PAN_GTP_ENABLED: "true"
```

```
#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-NGFW 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-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> <none>
```

```
pan-ngfw-ds-qsr6 1/1 Running 0 27h 10.233.115.189 rk-k8-vm-
worker-1 <none> <none>
```

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

```
pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vm-
worker-2 <none> <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-5fhhg 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-qsr6 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 *DemonSet*」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 *DemonSet* 時，*pan-plugin-cluster-mode-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-plugin-cluster-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。

ORACLE Cloud Infrastructure



SIGN IN

Signing in to cloud tenant:

[Change tenant](#)

Sign in with your Oracle Cloud Infrastructure credentials

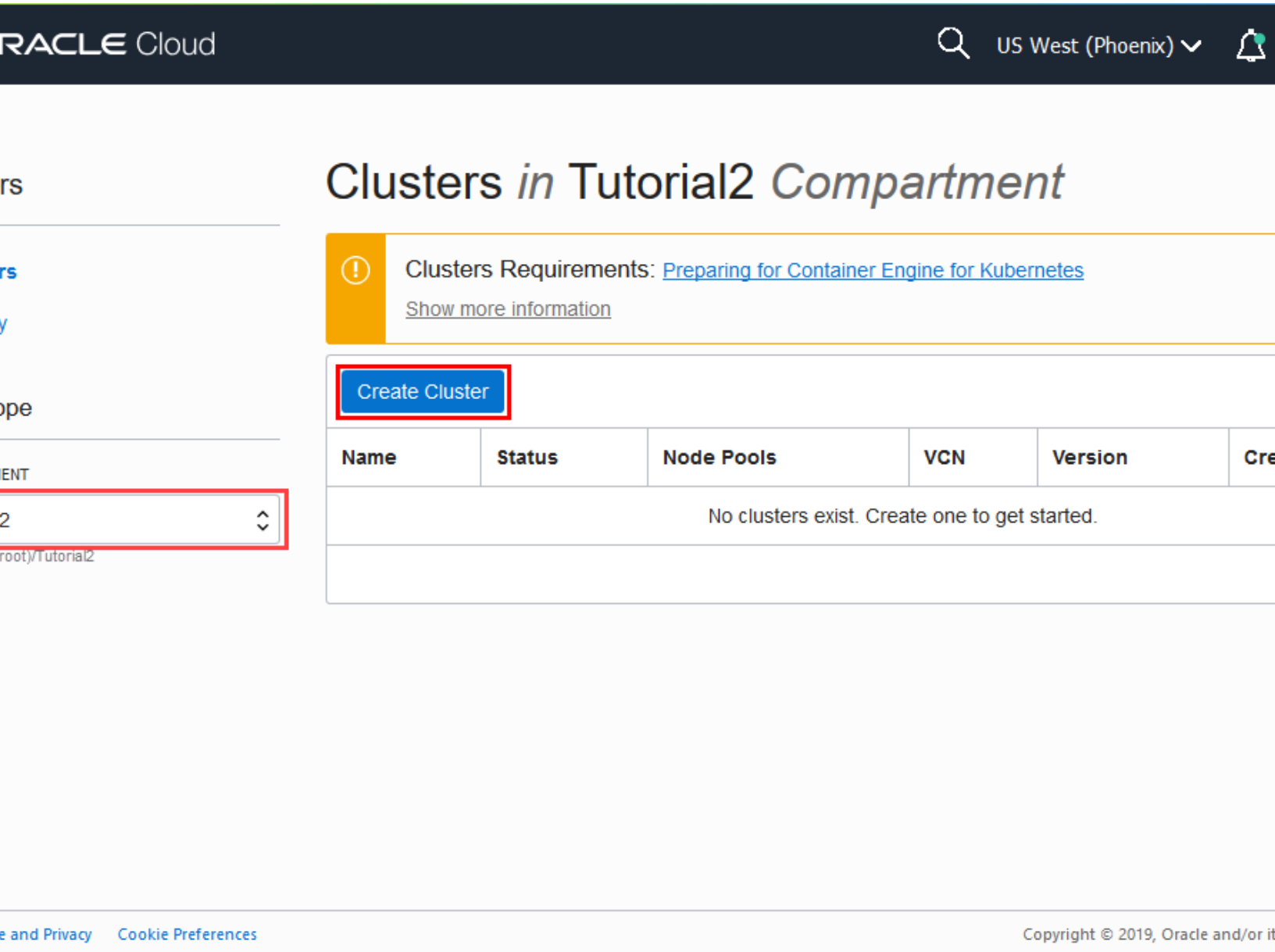
USER NAME

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）。



5. 在 [Create Cluster（建立叢集）] 對話方塊中，按一下 **Custom Create**（自訂建立），然後按一下 **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）。



Cluster Creation

Cluster

NEW

Resources to be created

Basic Information

Cluster Name: cluster1**Compartment:** Tutorial2**Version:** v1.18.10

Network

Compartment: Tutorial2**VCN Name:** oke-vcn-quick-
cluster1-4baf5729a**Network Security Groups:** Not Enabled**Kubernetes API Private Endpoint:** Auto
Assigned**Kubernetes API Public Endpoint:** Auto
Assigned**Kubernetes CIDR Block:** 10.96.0.0/16

Create Cluster

[Cancel](#)

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

Name

on_prem-clstr

Description

API server address

10.2

Type

Native-Kubernetes

Credentials

Label Selector

Label Filter

Custom Certificate

0 items

→

×

TAG PREFIX	NAMESPACE	LABEL SELECTOR FILTER	APPLY ON

+

Add

-

Delete

Validate

OK

Cancel

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

1 item

→

×

☐	COLLECTORS ▲
☐	rpgcpnew(RPGOOGGKEPRA1)

+

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。
- 備妥可將映像下載至其中的容器映像儲存庫位置。

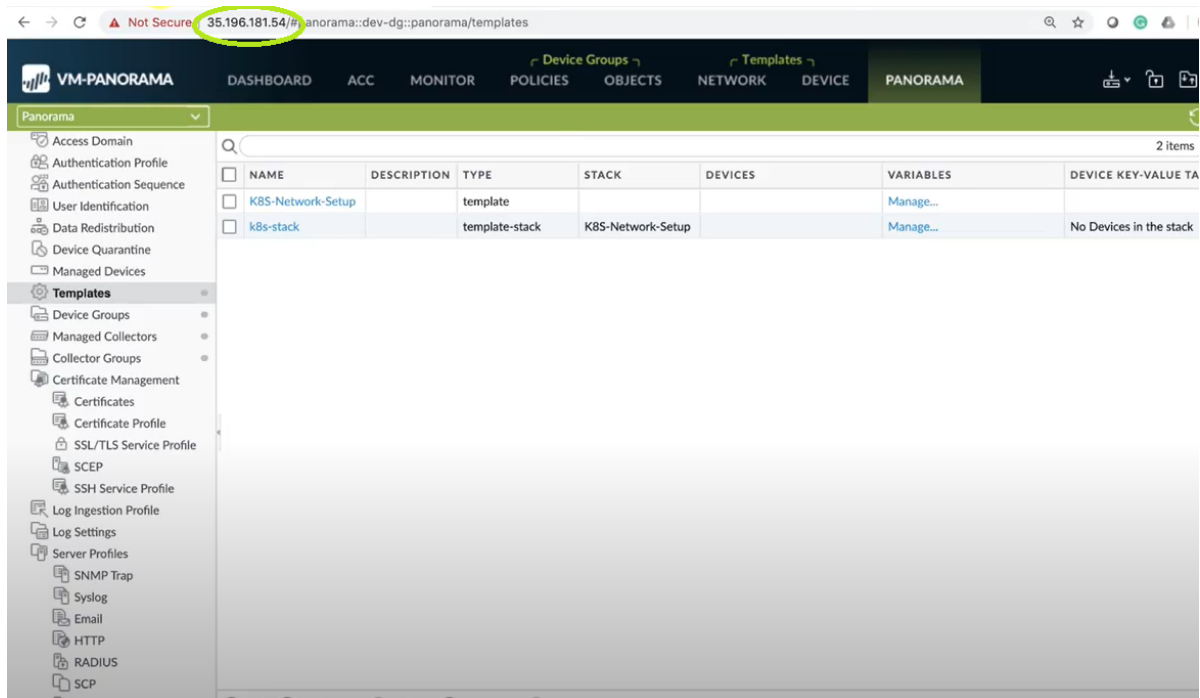
STEP 2 | （選用）如果您已在 Panorama 的 Kubernetes 外掛程式中設定自訂憑證，則必須執行下列命令來建立憑證密碼。請不要從 `ca.crt` 變更檔案名稱。`pan-cn-mgmt-dynamic-pv.yaml` 和 `pan-cn-ngfw.yaml` 中的自訂憑證數量是選用項目。

```
kubectrl -n kube-system create secret generic custom-ca --from-file=ca.crt
```

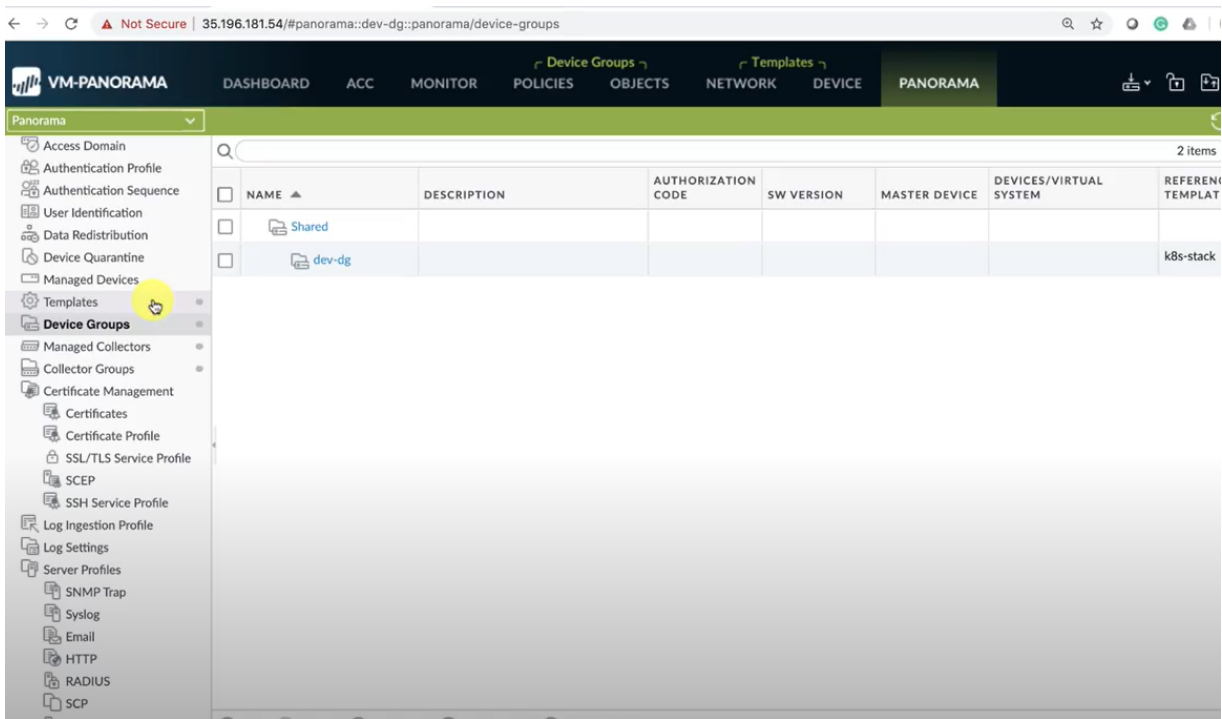
STEP 3 | 編輯 YAML 檔案，以提供部署 CN-Series 防火牆所需的詳細資料。

```
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: ""
```

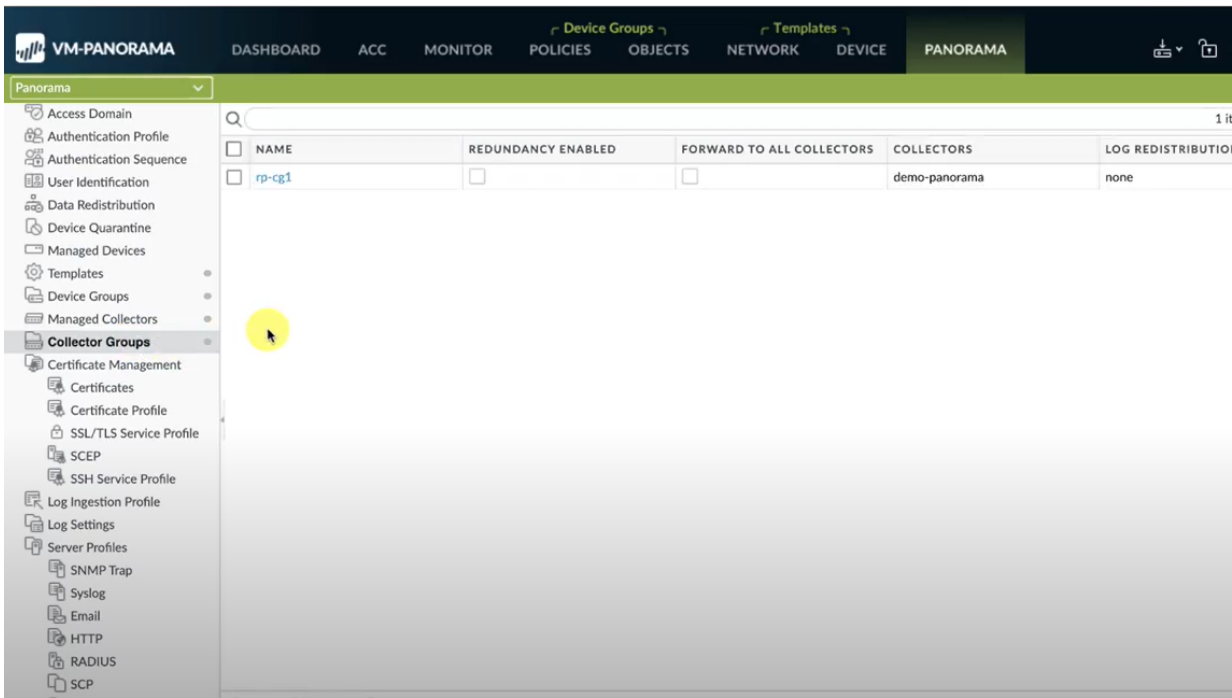
您必須確定 YAML 檔案上的 PAN_PANORAMA_IP 參數值符合您的實際 Panorama IP 位址，如下圖所示：



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：

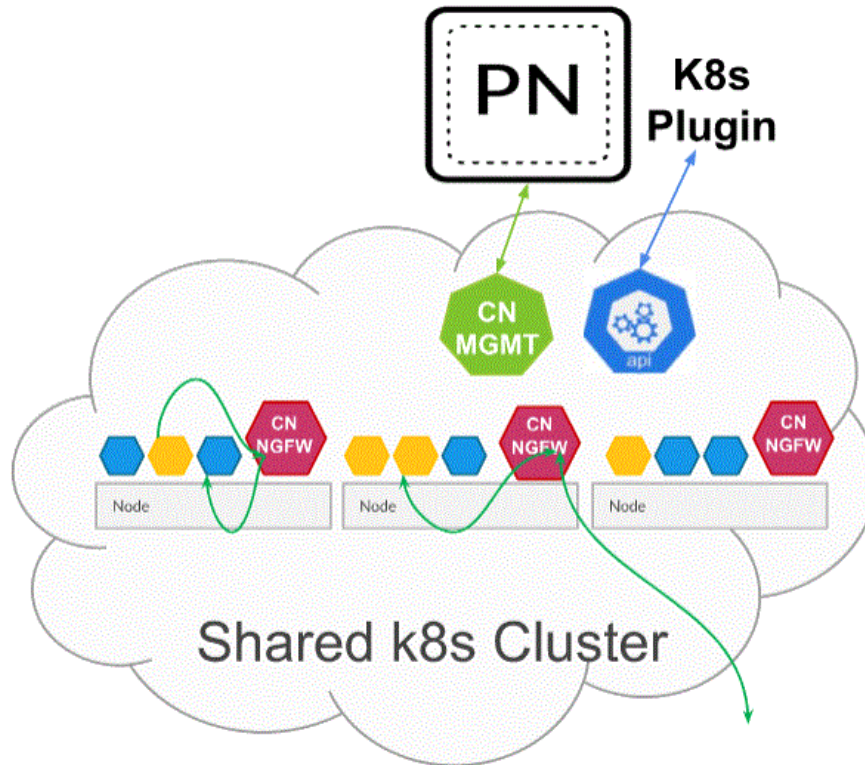


您必須確定 `PAN_PANORAMA_CG_NAME` 的參數值與您建立的日誌收集器名稱相同。



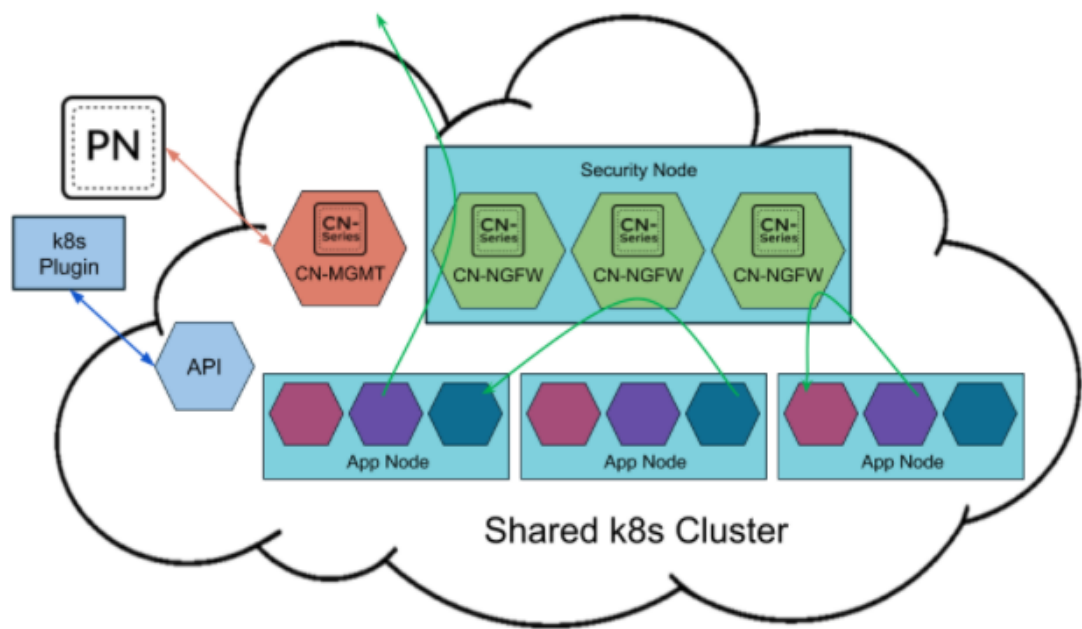
如需詳細資訊，請參閱 [CN-Series 部署 yaml 檔案](#) 中的可編輯參數以取得詳細資料。

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。



1. 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-series-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
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v-series-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-mgmt-
config 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-
  template-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 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. 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-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-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-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 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。

ORACLE Cloud Infrastructure



SIGN IN

Signing in to cloud tenant:

[Change tenant](#)

Sign in with your Oracle Cloud Infrastructure credentials

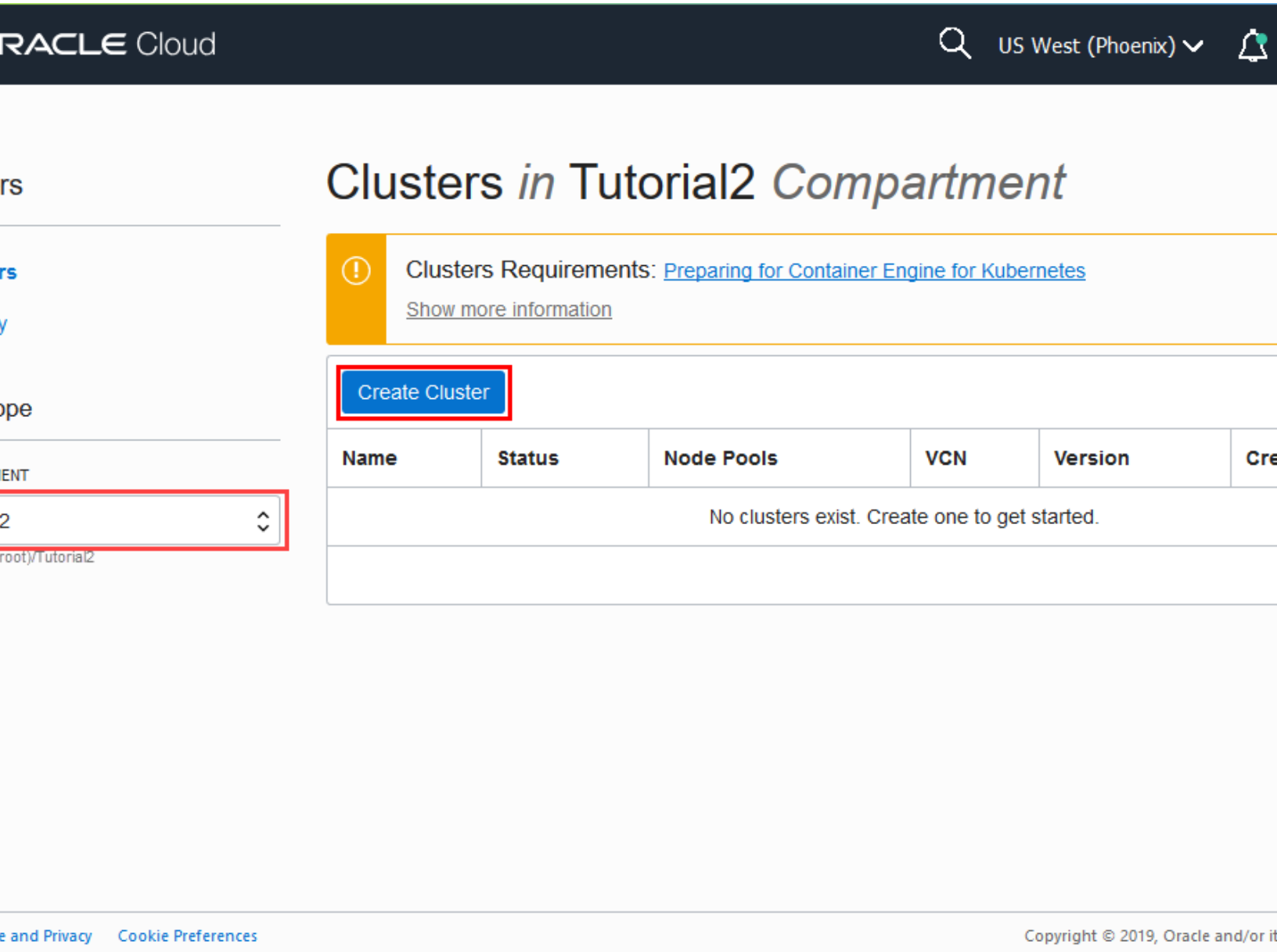
USER NAME

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）。



5. 在 [Create Cluster（建立叢集）] 對話方塊中，按一下 **Custom Create**（自訂建立），然後按一下 **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）。

ORACLE Cloud

🔍

US West (Phoenix) ▼

Cluster Creation

Create Cluster

Preview

Resources to be created

Basic Information

Cluster Name:

cluster1

Compartment:

Tutorial2

Version:

v1.18.10

Network

Compartment:

Tutorial2

VCN Name:

oke-vcn-quick-cluster1-4baf5729a

Network Security Groups:

Not Enabled

Kubernetes API Private Endpoint:

Auto Assigned

Kubernetes API Public Endpoint:

Auto Assigned

Kubernetes CIDR Block:

10.96.0.0/16

Create Cluster

Cancel

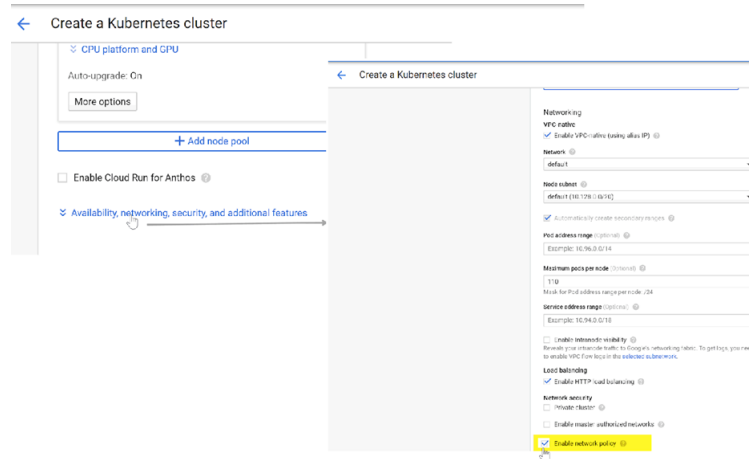
Terms and Privacy

Cookie Preferences

Copyright © 2019, Oracle and/or its



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。



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

Description

API server address

10.2.

Type

Native-Kubernetes

Credentials

Label Selector

Label Filter

Custom Certificate

Q

0 items

→

×

TAG PREFIX	NAMESPACE	LABEL SELECTOR FILTER	APPLY ON
------------	-----------	-----------------------	----------

+

 Add

-

 Delete

Validate

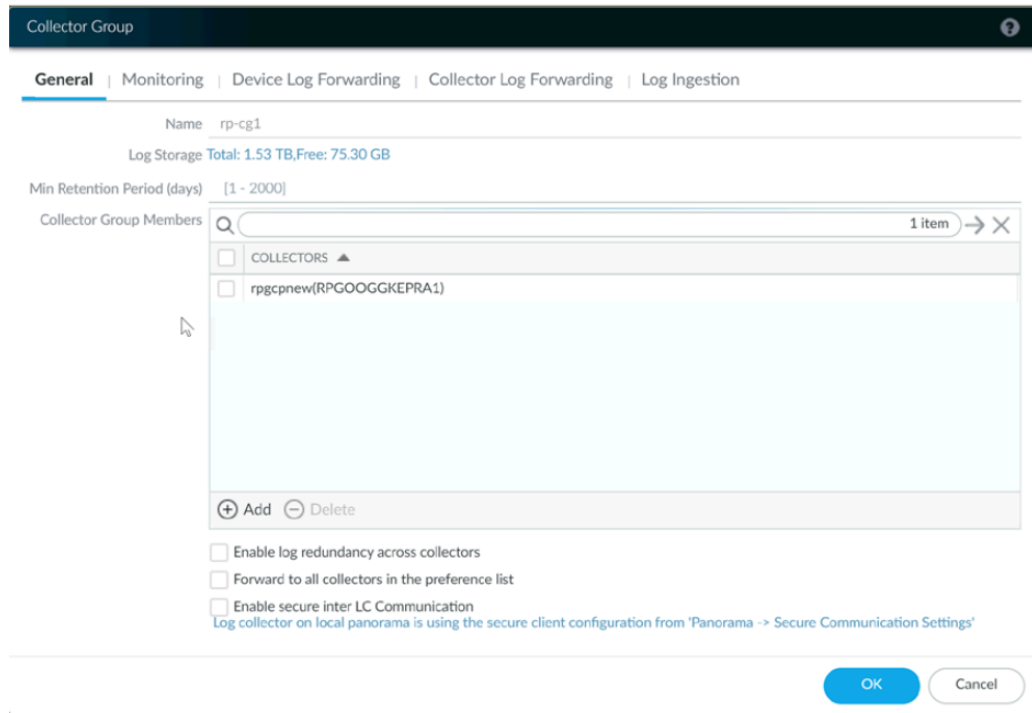
OK

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）。



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 --from-file=ca.crt
```

STEP 3 | 編輯 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。



在 OKE 上部署 CN-Series 防火牆作為 *Daemonset* 時，您可以使用 `pan-cn-k8s-daemonset` 原生資料夾中的 `yml` 檔案。

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.yml` 建立服務帳戶。

2. 使用 `Kubectl` 來執行 `pan-cni-configmap.yml`。

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

3. 使用 `Kubectl` 來執行 `pan-cni.yml`。

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

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-series-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
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v-series-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`

```
apiVersion: v1 kind:ConfigMap metadata: name: pan-mgmt-
config 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-
  template-stack>" PAN_CGNAME: "<panorama-collector-group>" #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.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 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-NGFW 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-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> <none>
```

```
pan-ngfw-ds-qsr6 1/1 Running 0 27h 10.233.115.189 rk-k8-vm-
worker-1 <none> <none>
```

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

```
pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vm-
worker-2 <none> <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-qsr6 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-cluster-mode-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-plugin-cluster-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。

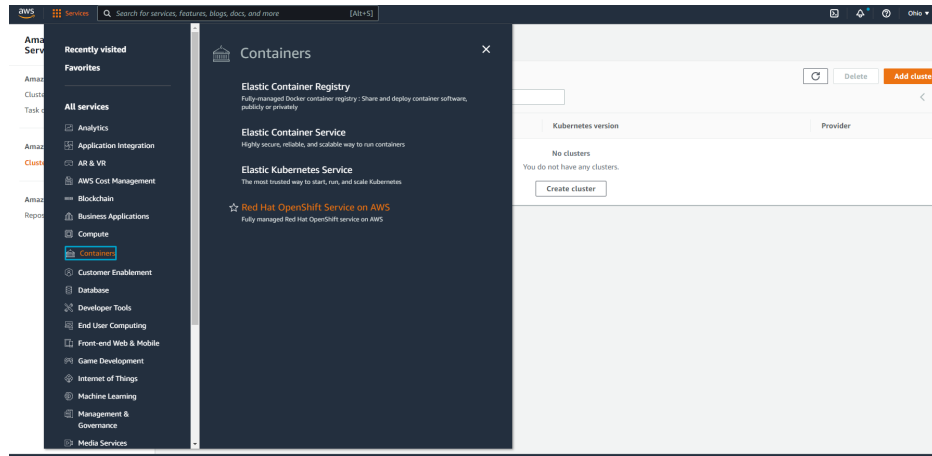
開始之前，請確保 CN-Series YAML 檔案版本與 PAN-OS 版本相容。

- 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

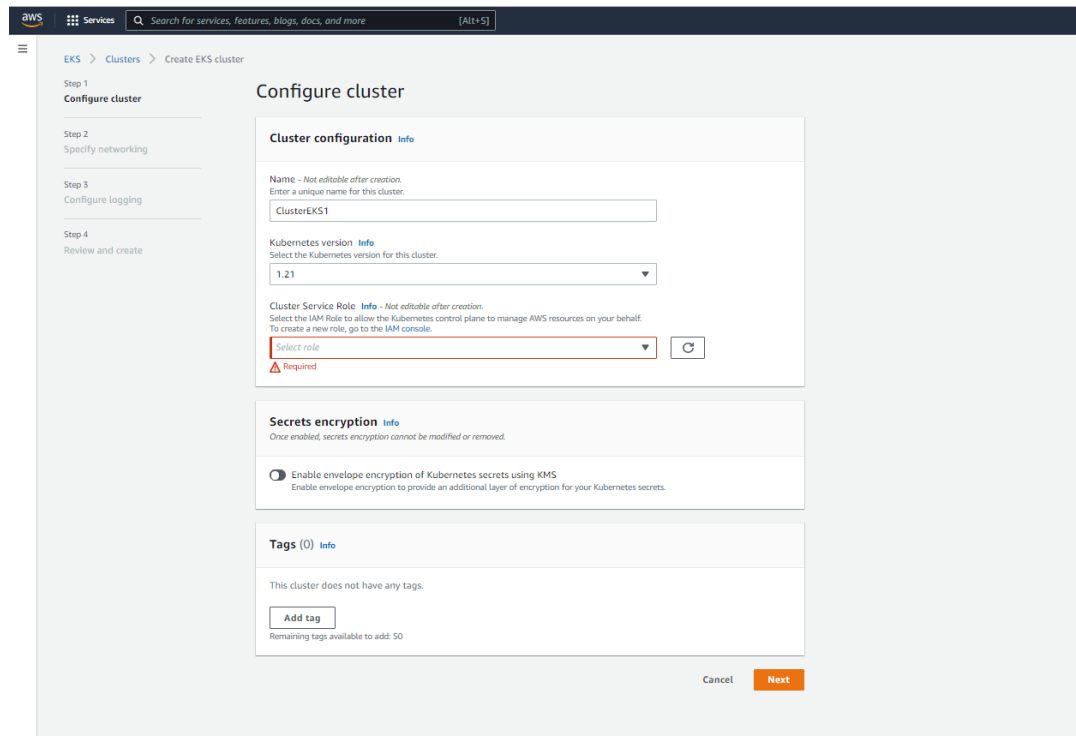
STEP 1 | 設定 Kubernetes 叢集。

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）。



1. 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 --from-file=ca.crt
```

STEP 3 | 編輯 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 aws-ebs-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：

1. 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。
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. 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`
2. 使用 Kubectl 來執行 `pan-cn-externalmetrics.yaml`
`kubectl apply -f pan-cn-externalmetrics.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`

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。

1. 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 (v...series-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
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v...series-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-mgmt-
config 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-
template-stack>" PAN_CGNAME: "<panorama-collector-
group>" # ctr mode: "k8s-service", "k8s-ilb-service"
PAN_CTR_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-registry-
image-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

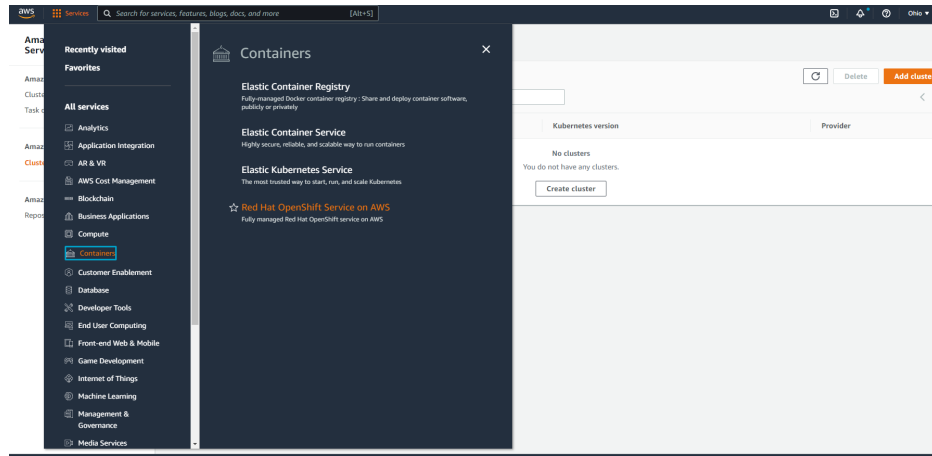
這可在何處使用？	我需要什麼？
• CN-Series 部署	• CN-Series 10.1.x or above Container Images • Panorama 執行 PAN-OS 10.1.x 或更高版本 • Helm 3.6 or above version client 使用 Helm 進行 CN-Series 部署

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

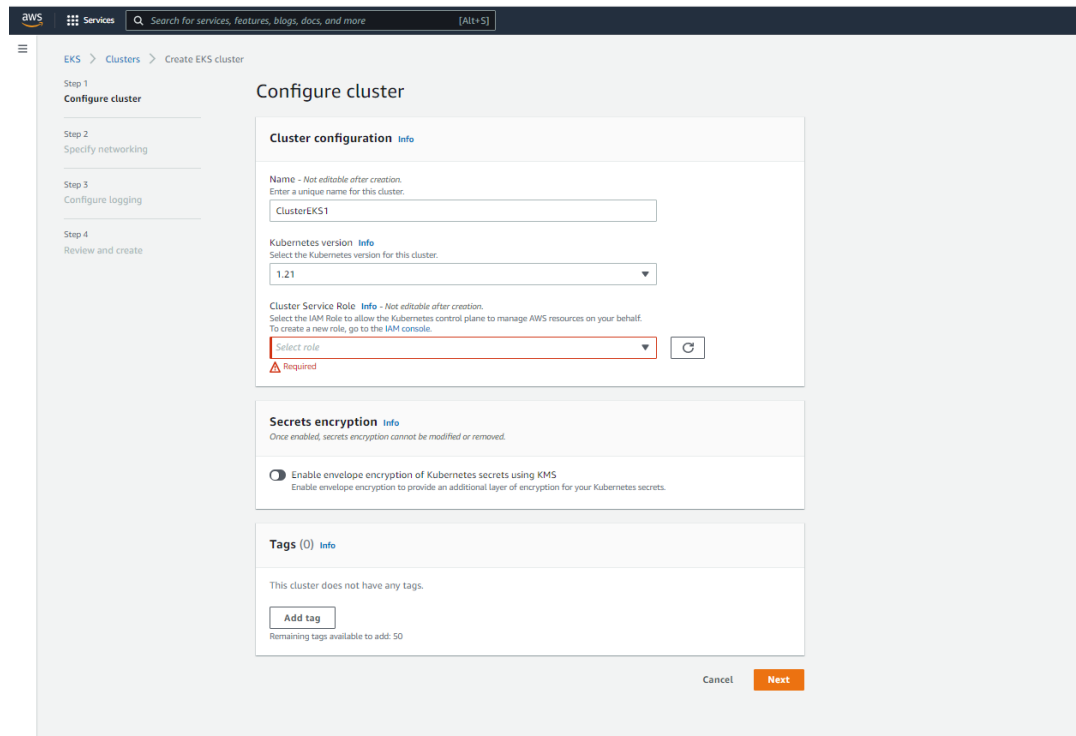
STEP 1 | 設定 Kubernetes 叢集。

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）。



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。

Cluster Definition

Name: on_prem-clstr

Description:

API server address: 10.2...

Type: Native-Kubernetes

Credentials:

Label Selector | Label Filter | Custom Certificate

0 items

TAG PREFIX	NAMESPACE	LABEL SELECTOR FILTER	APPLY ON
------------	-----------	-----------------------	----------

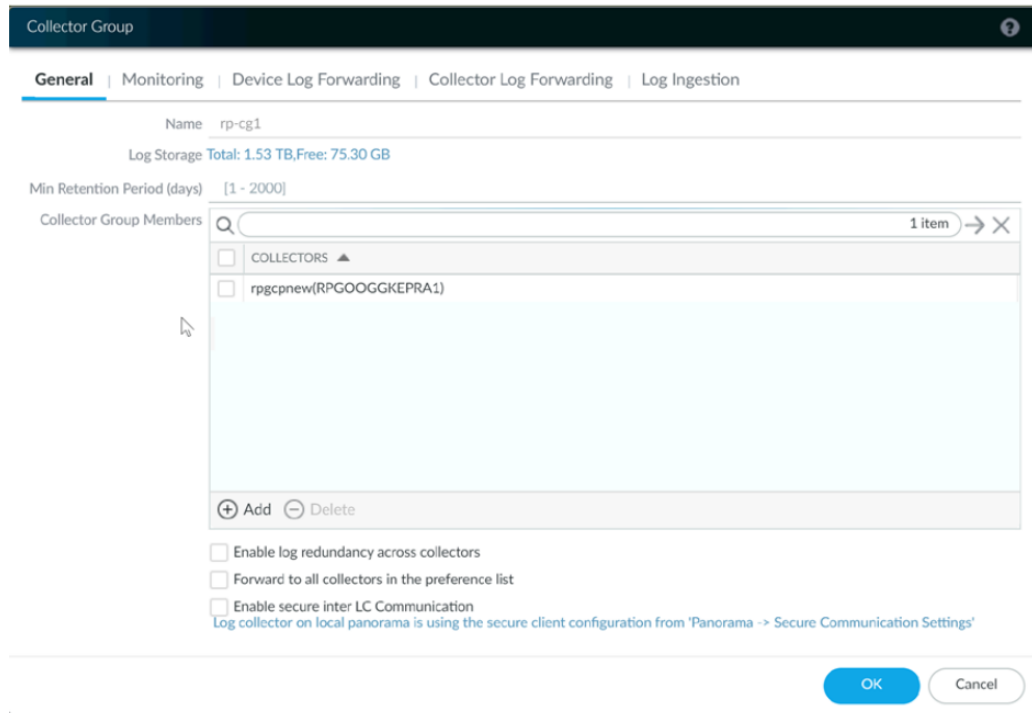
+ Add - Delete

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）。



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。

```
kubectrl -n kube-system create secret generic custom-ca --from-file=ca.crt
```

STEP 3 | 編輯 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-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 (v-series-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
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v-series-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 `aws-ebs-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: 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-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: "Cluster-
name" #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-registry-  
image-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-NGFW 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-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> <none>
```

```
pan-ngfw-ds-qsr6 1/1 Running 0 27h 10.233.115.189 rk-k8-vm-
worker-1 <none> <none>
```

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

```
pan-ngfw-ds-zncqg 1/1 Running 0 27h 10.233.91.210 rk-k8-vm-
worker-2 <none> <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-qsr6 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。



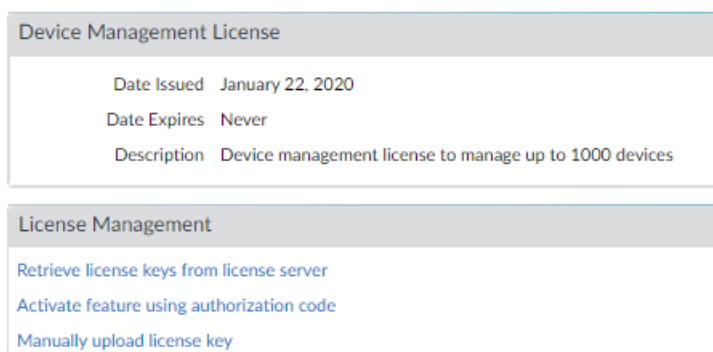
如果您已經在 AWS 上部署授權的 *Panorama* 執行個體，則請略過這些步驟。

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。
3. 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。



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.

Fulfillment option Helm Chart ▼	Supported services • Amazon EKS • Amazon EKS Anywhere • Self-managed Kubernetes
Software version Version1.2.2 (Nov 22, 2021) ▼	Fulfillment option description Deploy CN-Series on EKS and RedHat Openshift using Helm Chart

STEP 9 | 按一下 **Continue to Launch**（繼續啟動）。

1. 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  
  
eksctl create iamserviceaccount \  
  --name my-service-account \  
  --namespace kube-system \  
  --cluster <ENTER_YOUR_CLUSTER_NAME_HERE>
```

Copy

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=000xxxxxxx \  
  \ --set panorama.deviceGroup=Panorama-DG \  
  \ --set panorama.template=Panorama-TS \  
  \
```

```
--set panorama.cgName=Panorama-CG \ --set
imagePullSecrets=awsmc-image-pull-secret
```

Step 2: Launch the software

Use the following commands to launch this software by installing a Helm chart on your Amazon EKS cluster.

```
export HELM_EXPERIMENTAL_OCI=1

aws ecr get-login-password \
  --region us-east-1 | helm registry login \
  --username AWS \
```

[Copy](#)

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.

```
kubectl create namespace kube-system
kubectl create serviceaccount my-service-account --namespace kube-system

AWSMP_TOKEN=<CREATE_TOKEN_ABOVE>
AWSMP_ROLE_ARN=arn:aws:iam::018147215560:role/service-role/AWSMarketplaceLicenseT
```

[Copy](#)

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 ./
awsmc-chart/* \ --set serviceAccount.create=false
\ --set serviceAccount.name=my-service-account
\ --set cluster.deployTo=eks|openshift \ --set
```

```
panorama.ip=Panorama-IP \ --set panorama.ip2=Panorama-IP2 \ --set panorama.authKey=000xxxxxxx \ --set panorama.deviceGroup=Panorama-DG \ --set panorama.template=Panorama-TS \ --set panorama.cgName=Panorama-CG \ --set imagePullSecrets=awsmp-image-pull-secret
```

Step 3: Launch the software

Use the following commands to launch the software by installing a Helm chart from Amazon Elastic Container Registry (ECR).

```
export HELM_EXPERIMENTAL_OCI=1

aws ecr get-login-password \
  --region us-east-1 | helm registry login \
  --username AWS \
```

Copy

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 consume an application or resource.

Search

< 1 > ⓘ

Name	Value	Max count	Usage	Units	Overages	Allow check in
vCPU	-	1000	5	Count	Not Allowed	Allowed
AWS::Marketplace::Usage	Enabled	-	-	None	-	Not Allowed

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

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

DASHBOARD

ACC

MONITOR

POLICIES

OBJECTS

NETWORK

DEVICE

panorama

Commit

Manual

11 ite

	DEVICE NAME	VIRTUAL SYSTEM	MODEL	TAGS	SERIAL NUMBER	IP Address		VARIABLES	TEMPLATE	DEVICE STATE
						IPv4	IPv6			
						vrp-gke5-dg (1/2 Devices Connected): Shared > vrp-gke5-dg				
☐	mp1 pan-mgmt-sts-0		PA-CTNR		8056	10.12.0.17		Create	vrp-gke5-ts	Connected
☐	mp2 pan-mgmt-sts-1				866	10.12.2.20		Create	vrp-gke5-ts	Connected

3. 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。

DASHBOARDACCMONITORPOLICIESOBJECTSNETWORKDEVICEPANORAMA

Q

Node ID	Firewall Pod Name	License Status	Node Status
rr-cluster-1 (3 Nodes, 3/3 Licensed)			
rr-cluster-1-default-pool-e2d3de37-1jtz	pan-ngfw-ds-4qfb		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

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 *pan-plugin-cluster-mode-secret*。

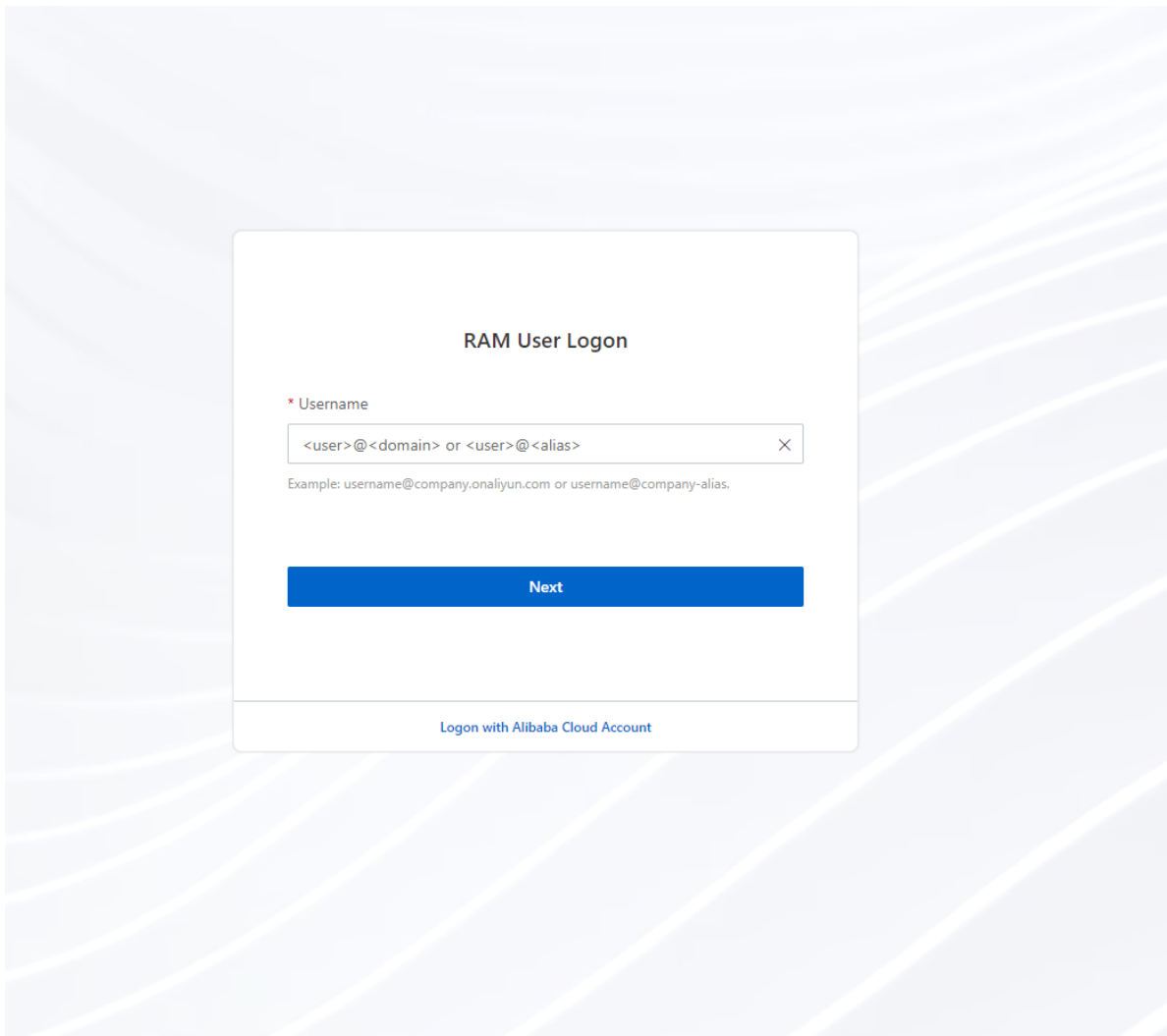
開始之前，請確保 CN-Series YAML 檔案版本與 PAN-OS 版本相容。如需詳細資訊，請參閱 [CN-Series YAML](#)。

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

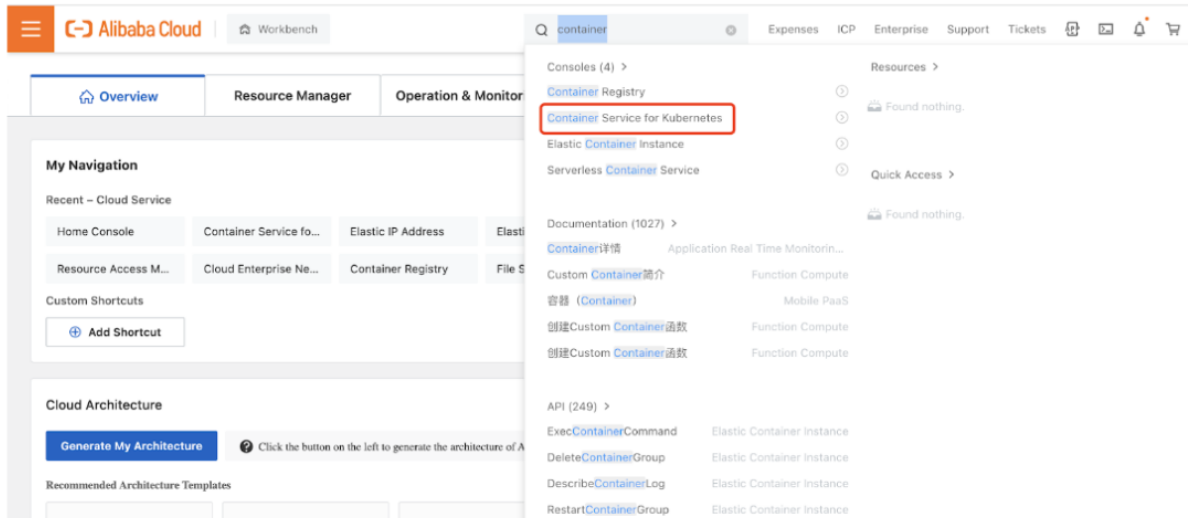
STEP 1 | 設定 Kubernetes 叢集。

若要在 ACK 中建立叢集，請執行以下操作：

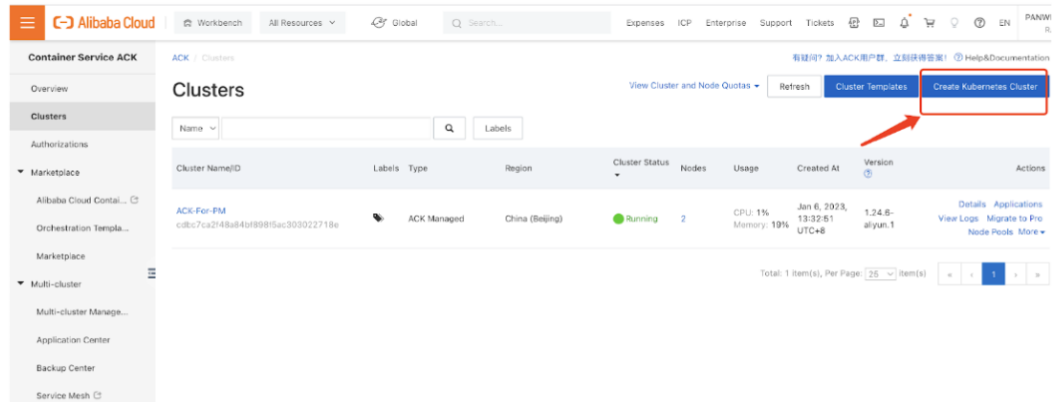
1. 使用您的 RAM 登入憑證登入 [RAM 使用者登入](#)。



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）。



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-2zewkdrmhjzfc2ibotn, 10.1...

Create VPC Plan Kubernetes CIDR blocks in VPC networks

Network Plug-in

FlannelTerway

You cannot change the network plug-in after the cluster is created. How to select a network plug-i

Kubernetes cluster

IPVLAN (The inclusive ENI mode uses a combination of IPVLAN and eBPF as the virtualization technology. Only Alibaba Cloud Linux is supported)

Support for NetworkPolicy Policy-based network traffic control is provided.

vSwitch

Select 1-5 vSwitches. We recommend that you select vSwitches in different zones to ensure high availability for the cluster.

☐	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-2zepoq1k3a7zx1pk2laf5	Beijing Zone C	10.101.0.0/24	252
☒	cn-pod2	vsw-2ze5v4zny1j58rzdd19t	Beijing Zone A	10.101.102.0/24	243

- 選取 **POD vSwitch**。

Pod vSwitch

AllZoneA (2 / 1)

	inside	vsw-2zej8ngtuy6r6qy1eoil	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	252
☒	cn-pod1	vsw-2zex1z33lu6ffu72ko5ry	Beijing Zone A	10.101.101.0/24	252
☐	cn-node-ip	vsw-2ze5nzjrkzio4sbf5d2n9	Beijing Zone A	10.101.10.0/24	252

Create vSwitch

The prefix length of the VSwitch address is recommended to be no greater than 19 bits.

Service CIDR

192.168.0.0/16

Recommended Value:192.168.0.0/16

Valid values: 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 access. If the VPC does not have a NAT gateway, ACK automatically creates a NAT gateway and configures SNAT rules. For more information, see [NAT Gateway bill of materials](#).

Access to API Server [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 instance, the API server cannot access the API server.

☒ **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 Internet.

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. (If the RDS instance is not in the running state, the node pool cannot be scaled out.)

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 must use an advanced security group. [Security group overview](#)

Deletion Protection ☐ **Enable**
Cluster Cannot Be Deleted in Console or by Calling API

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 sn2nec) Move Up Move Down

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 120 GiB

Mount Data Disk You have selected 0 disks and can select 10 more.
Disk Parameters and Performance + Add Data Disk Recommended

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

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

- 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

Cluster Configurations Node Pool Configurations 3 Component Configurations

Ingress Do Not Install Nginx Ingress ALB Ingress MSE Ingress

SLB Network Type Public Network Internal Network

SLB Specifications slb.s1.small

Service Discovery ☐ Install NodeLocal DNSCache

Volume Plug-in CSI

Monitoring Agents ☐ Install CloudMonitor Agent on ECS Instance ☒ Enable Prometheus Monitoring

ACK Billing SLB Price: ¥ 0.220 /Hours 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	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

Terms of Service

During the cluster creation process, the following operations may be performed depending on cluster configurations:

- Create ECS instances, configure a public key to enable SSH login from master nodes to other nodes, and configure the Kubernetes cluster through Cloudinit.
- Create a security group that allows access to the VPC network over ICMP.
- Create VPC routing rules.
- Create a NAT gateway and Elastic IP addresses.
- Create a RAM role and grant it the following permissions: query, create, and delete ECS instances, create and delete cloud disks, and all permissions on SLB instances, CloudMonitor, VPC, Log Service, and NAS. The Kubernetes cluster dynamically creates SLB instances, cloud disks, and VPC routing rules based on your settings.
- Create an internal SLB instance and open port 6443.
- When you use a dedicated or managed Kubernetes cluster, the system collects log and monitoring information about control components on master nodes to help ensure cluster stability.

☒ I have read and understand the preceding statement. I also have read and accept the [Terms of Service and Disclaimer](#).

ACK Billing SLB Price: ¥ 0.220 /Hours
EIP Price: ¥ 0.800 /GB
ECS Price: ¥ 4.91 /Hours

Prev: Component Configurations

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`。



Alibaba Cloud

Workbench All Resources Global Search...

Expenses ICP Enterprise Support Tickets

ACK-For-PM

Cluster Information

Nodes

Node Pools

Nodes

Namespaces and Quota...

Workloads

Deployments

StatefulSets

DaemonSets

Jobs

CronJobs

Pods

Custom Resources

Network

Configurations

ACK-For-PM

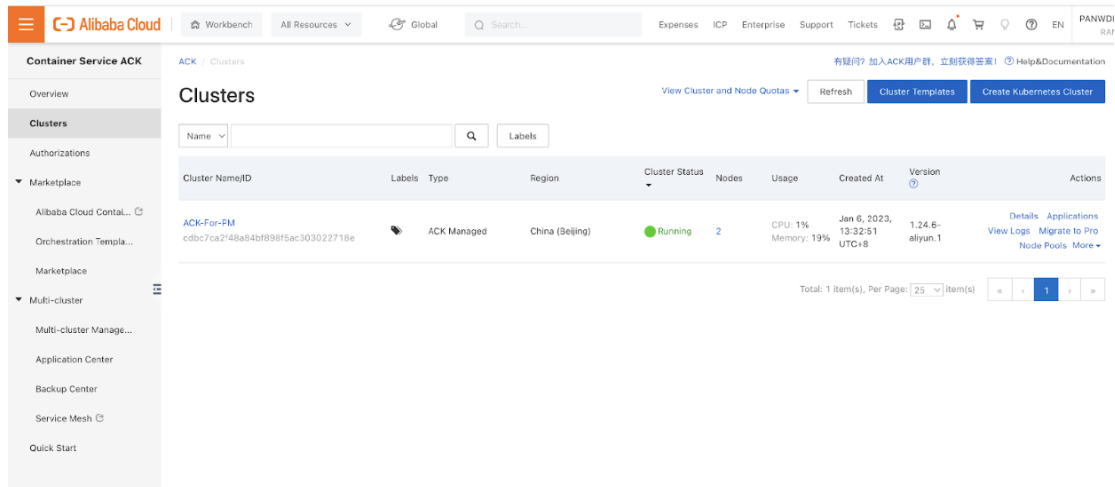
Overview Basic Information Connection Information Cluster Resources Cluster Logs Cluster Tasks

Basic Information

Cluster ID: cdbc7ca2f48a84bf898f5ac303022718e Running Region: China (Beijing) Time Zone: Asia/Shanghai

Cluster Information

API Server Public Endpoint	https://47.93.191.191:6443	Change EIP	Unbind EIP
API Server Internal Endpoint	https://10.101.10.169:6443	Set access control	Troubleshoot connection issues
Service CIDR	192.168.0.0/16		
RRSA OIDC	Enable RRSA	Configure RAM permissions for service accounts to isolate permissions among pods	
Kube-proxy Mode	ipvs		
Network Plug-in	terway-enlip		
Custom Certificate SANs	Update		
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

Description:

API server address: 10.2...

Type: Native-Kubernetes

Credentials:

Label Selector | Label Filter | Custom Certificate

0 items → ×

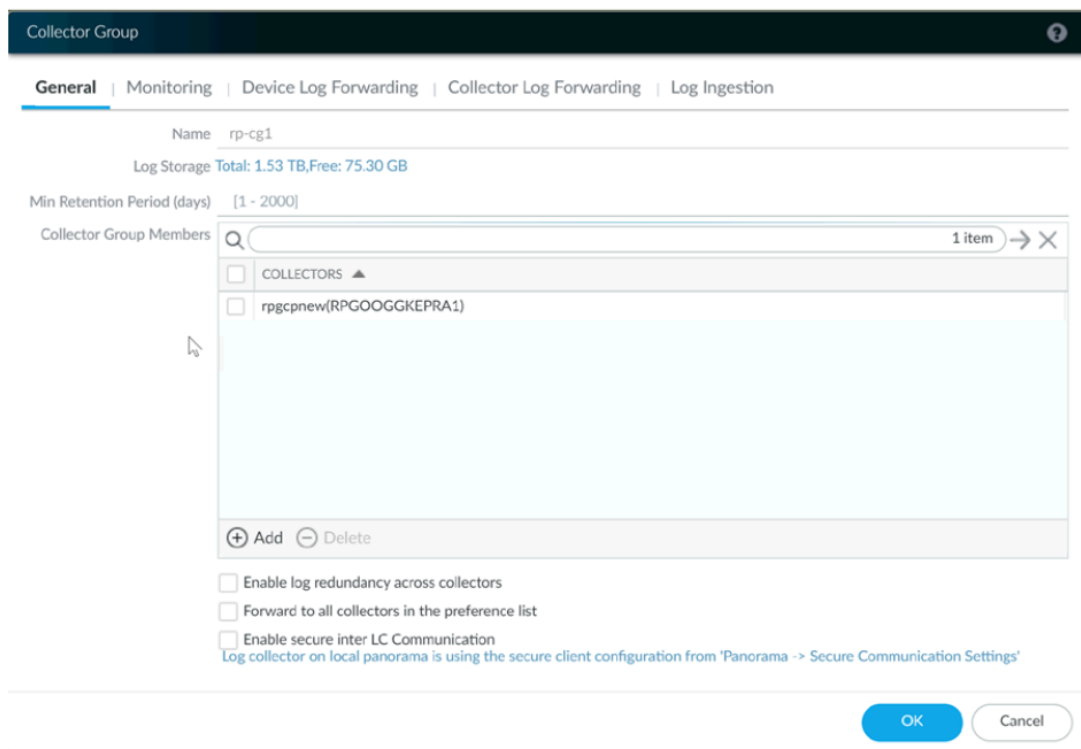
TAG PREFIX	NAMESPACE	LABEL SELECTOR FILTER	APPLY ON
------------	-----------	-----------------------	----------

+ Add - Delete

Validate OK Cancel

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）。



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 --from-file=ca.crt
```

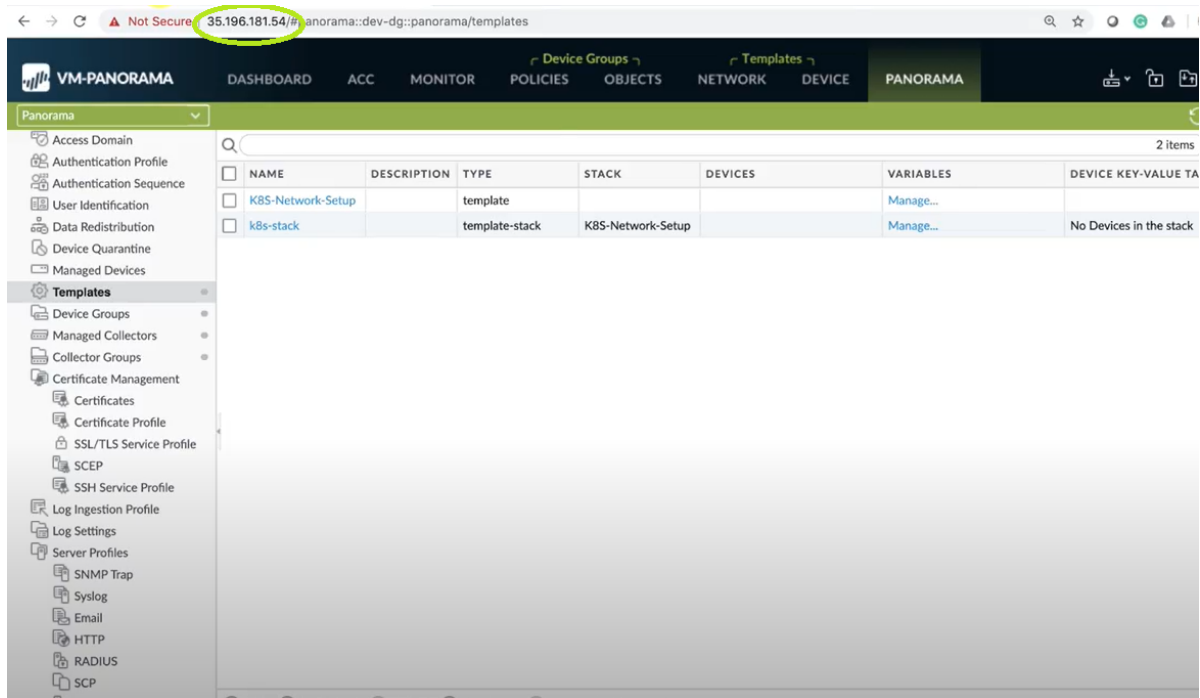
STEP 3 | 編輯 YAML 檔案，以提供部署 CN-Series 防火牆所需的詳細資料。

```
apiVersion: v1 kind:ConfigMap metadata: name: pan-mgmt-config
namespace: kube-system data: PAN_SERVICE_NAME: pan-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-template-stack>"
PAN_CGNAME: "<panorama-collector-group>" PAN_CTNR_MODE_TYPE: "k8s-
service"
```

```
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
```

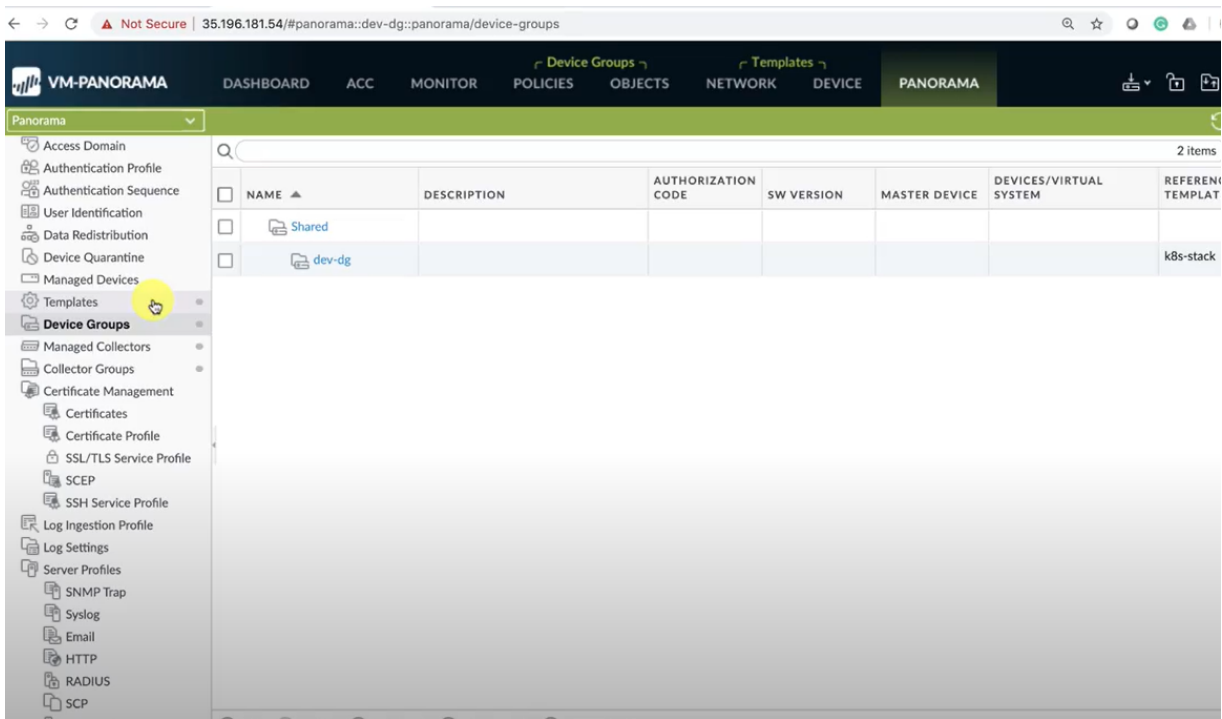
```
Certificate retrieval CN-SERIES-AUTO-REGISTRATION-PIN-ID: "<PIN
Id>" CN-SERIES-AUTO-REGISTRATION-PIN-VALUE: "<PIN-Value>"
```

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：

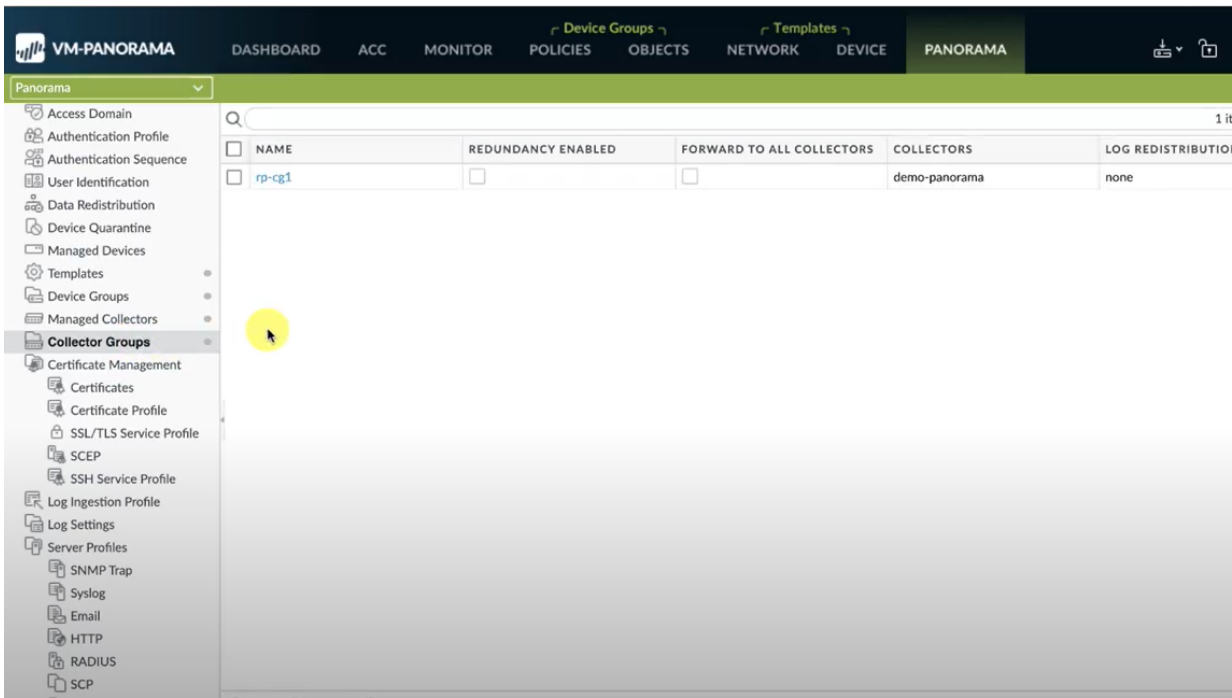


 **Palo Alto Networks Kubernetes Security - CN Series 的儲存庫** 中提供最新版本的 **YAML** 檔案。您可以從 **Switch**（切換）**branches/tags**（分支/標籤）下拉式功能表中選取最新的分支或標籤。

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：



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。



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。

1. 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 series-mktplace) $ kubectl get pods -n kube-system | grep pan-cni
pan-cni-nmqkf          Running    0          2m11s
pan-cni-wjrtkq         Running    0          2m11s
pan-cni-xrc2z          Running    0          2m12s
@cloudshell:~/Kubernetes-master/pan-cn-k8s-service/gke (v series-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-registry-
image-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。

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 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。

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 **eth0** 的安全。

STEP 1 | 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。

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—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。

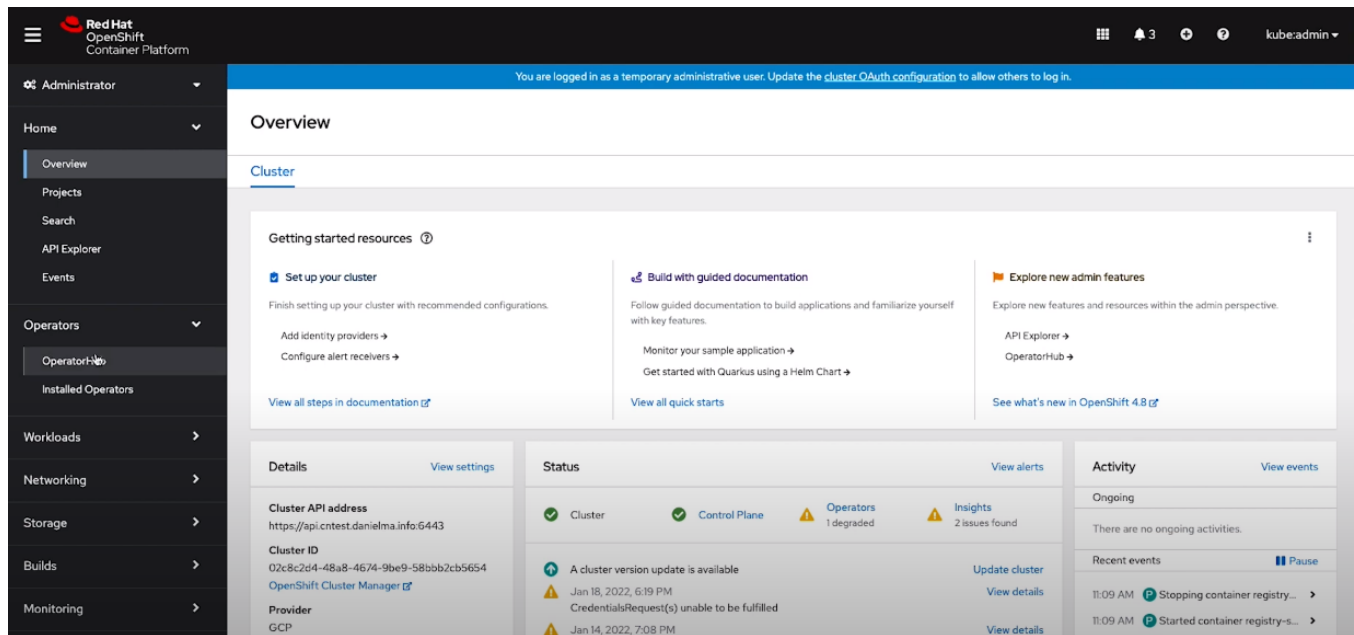


您需要 *PAN-OS 10.2* 或更高版本才能在 *OpenShift Operator* 中樞上部署 *CN-Series*。

以下是在 Redhat OpenShift Operator 中樞上部署 CN-Series 防火牆的步驟：

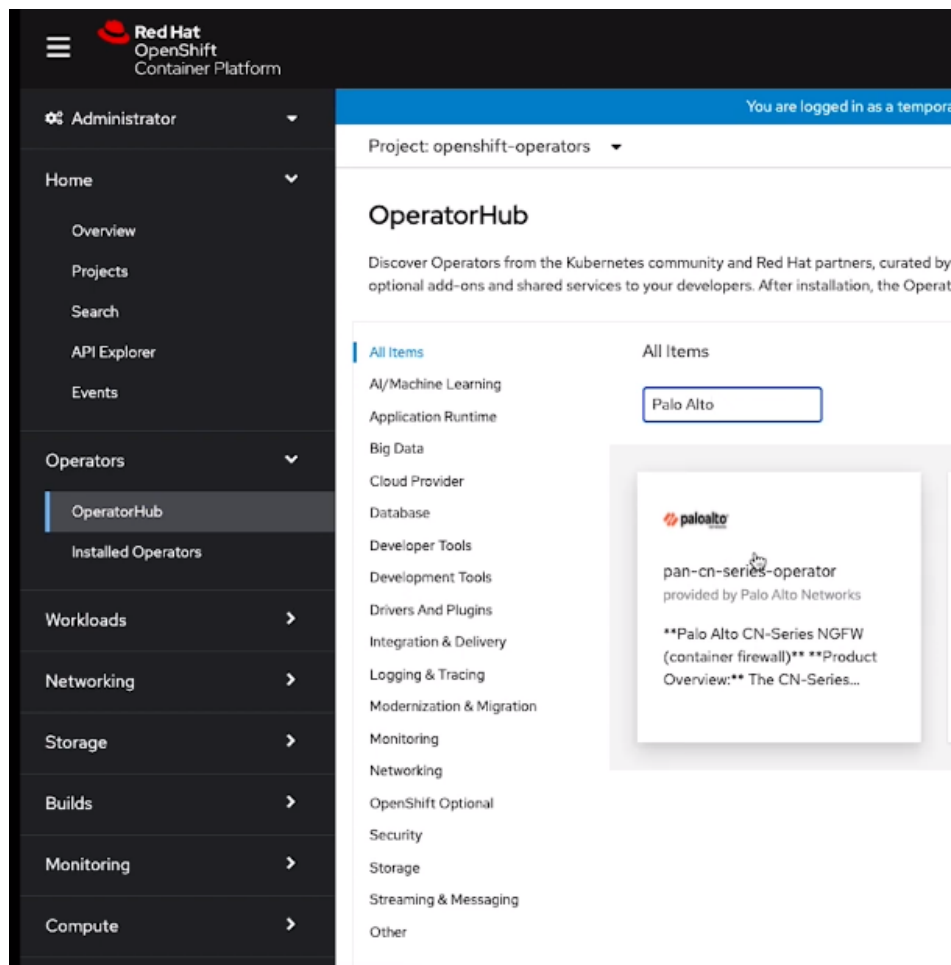
STEP 1 | 登入 Redhat OpenShift 容器主控台。

STEP 2 | 前往 **Operator**，然後按一下 **OperatorHub**。



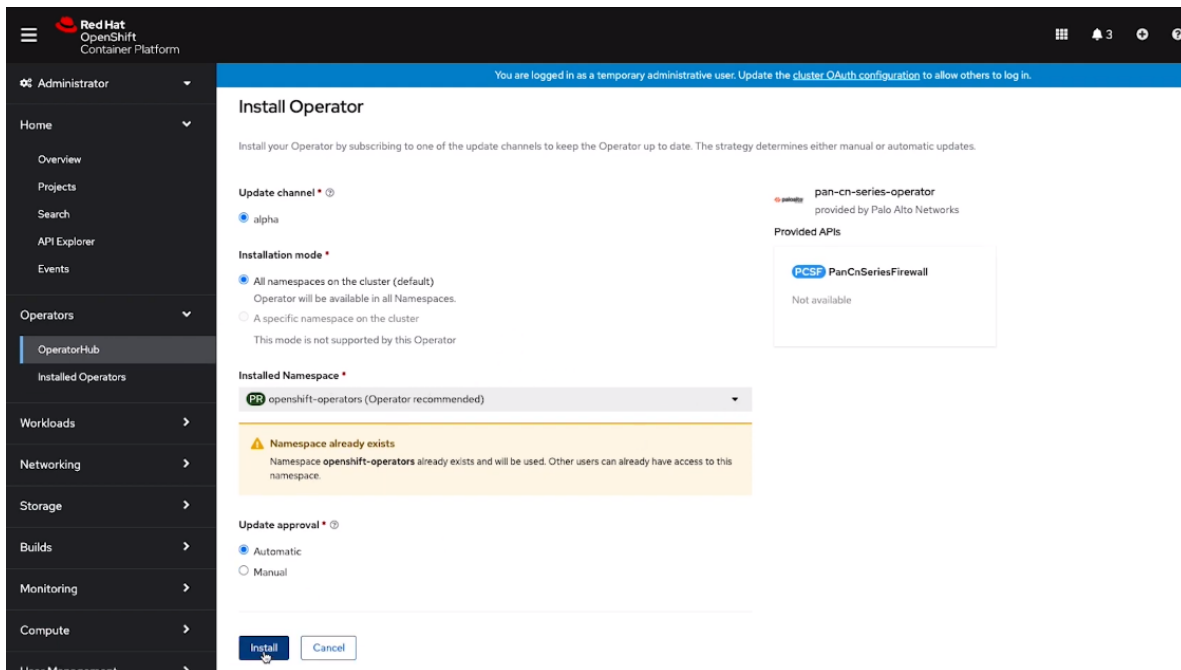
STEP 3 | 在 Operator 搜尋方塊中輸入 **Palo Alto**。

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。

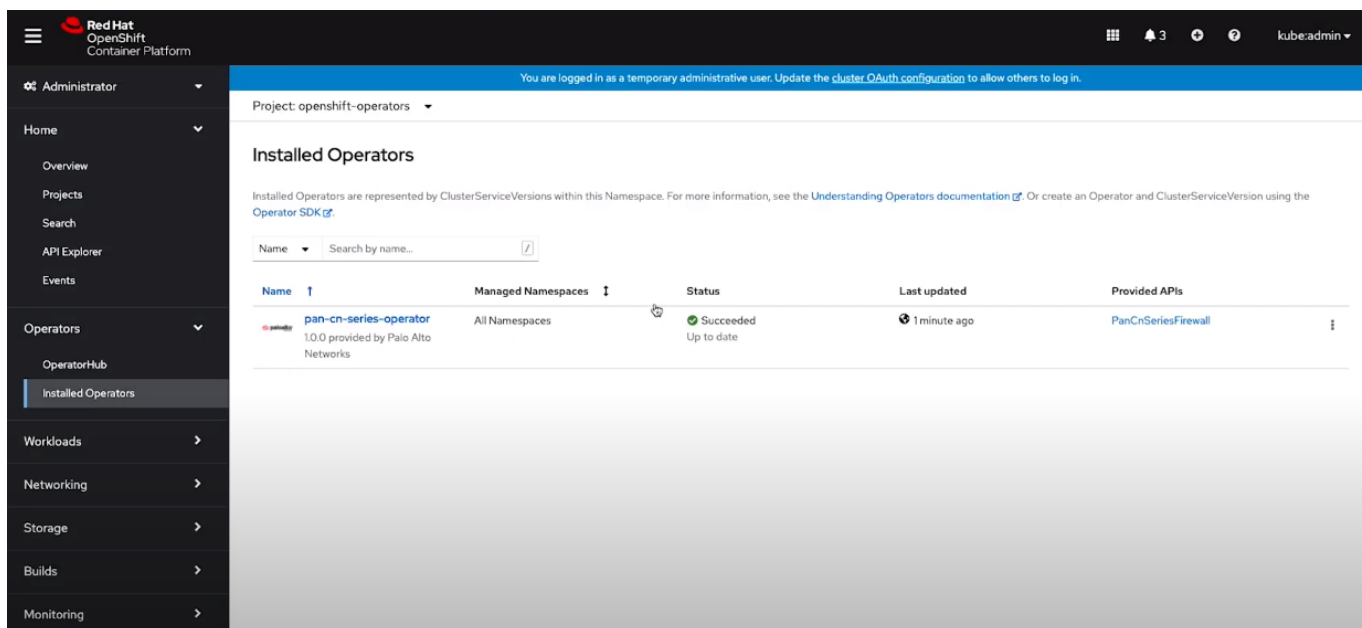
STEP 5 | 按一下 **Install**（安裝）在 OpenShift 叢集上安裝 pan-CN-Series Operator。



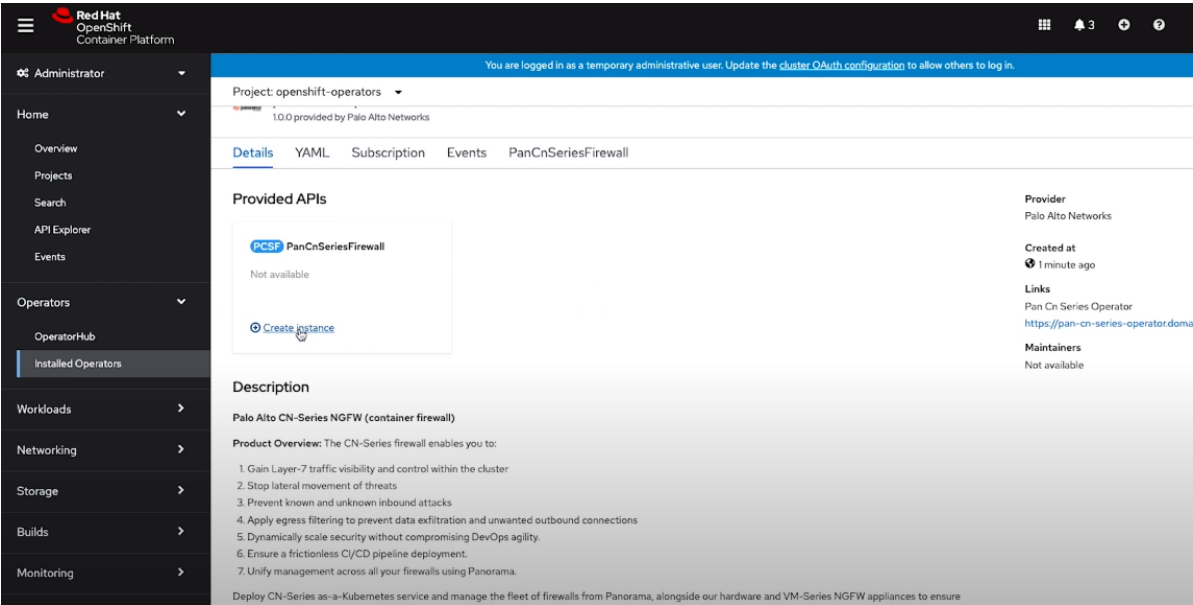
 在執行此處指定的後續部署步驟之前，請完成[預先安裝步驟](#)。

 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**。



STEP 7 | 按一下 **Create Instance**（建立實例）。



STEP 8 | 輸入唯一的運算數 **Name**（名稱）。

Project: openshift-operators

Name *

crs-sample

Labels

app=frontend

Minimum Replicas for DP

2

Minimum Replicas for DP

CPU Limit (DP)

1

Desired number of CPUs for DP

Memory Limit (DP)

4000

Desired memory for DP

CPU Limit (MP)

2

Desired number of CPUs for MP

Memory Limit (MP)

3000

Desired memory for MP

Panorama IP Address

<Panorama-IP>

Panorama IP Address

Secondary Panorama IP Address (Optional)

Secondary Panorama IP Address for HA deployment

vm-auth-key from Panorama

<Panorama-auth-key>

Authorization Key vm-auth-key from Panorama

Panorama Device Group

<Panorama-device-group>

Panorama Device Group

Panorama Template Stack

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）。



The screenshot shows a configuration form for a Panorama Template Stack. The form includes the following fields and labels:

- Panorama Log Collector Group Name**: A text input field with the value "<panorama-collector-group>".
- Panorama Log Collector Group Name**: A label for the next field.
- Customer Support Portal PIN ID (Optional)**: A text input field.
- Customer Support Portal PIN ID**: A label for the next field.
- Customer Support Portal PIN Value (Optional)**: A text input field.
- Customer Support Portal Value**: A label for the next field.
- Customer Support Portal Alternate URL (Optional)**: A text input field.
- Customer Support Portal Alternate URL**: A label for the next field.
- DP Image**: A text input field with the value "gcr.io/pan-cn-series/panos_cn_nfw".
- The docker image name and version of CN Series DP**: A label for the next field.
- DP Image Version**: A text input field with the value "preferred-10.2".
- DP Image Version**: A label for the next field.
- MP Image**: A text input field with the value "gcr.io/pan-cn-series/panos_cn_mgmt".
- The docker image name and version of CN Series MP**: A label for the next field.
- MP Image Version**: A text input field with the value "preferred-10.2".
- MP Image Version**: A label for the next field.
- PAN CNI Image**: A text input field with the value "gcr.io/pan-cn-series/pan_cni".
- The docker image name and version of CN Series pan-cni**: A label for the next field.
- PAN CNI Image Version**: A text input field with the value "preferred".
- PAN CNI Image Version**: A label for the next field.

At the bottom of the form, there are two buttons: **Create** and **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）。

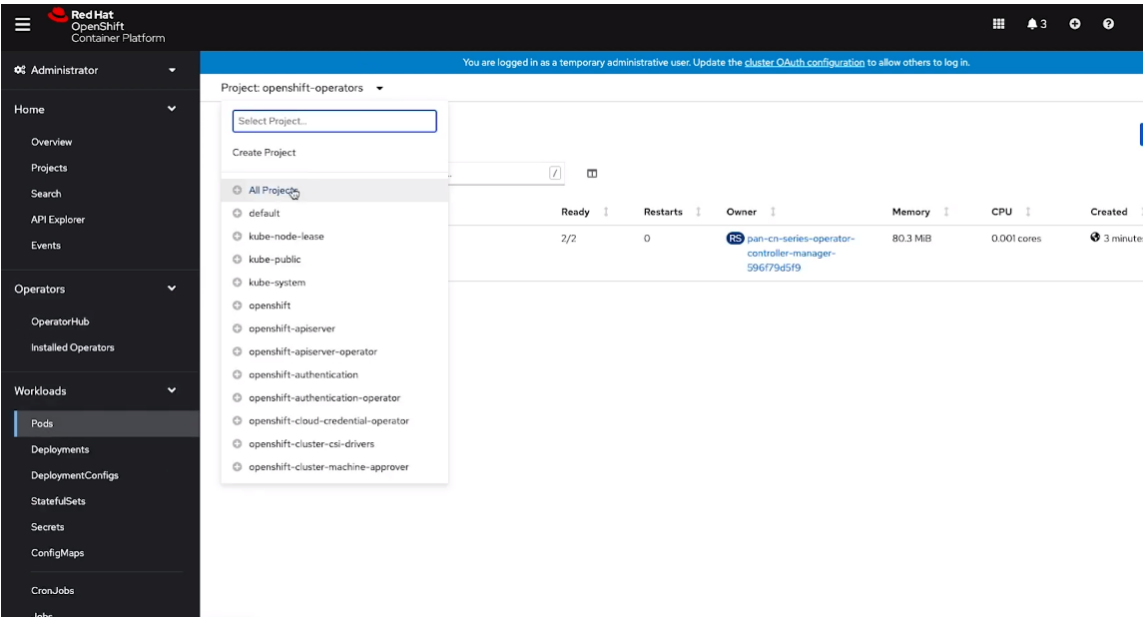
STEP 16 | 選用 輸入客戶支援入口網站 (CSP) **Pin ID**、**Pin value**（**Pin** 值）和 **Alternate URL**（替代 **URL**）。

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。

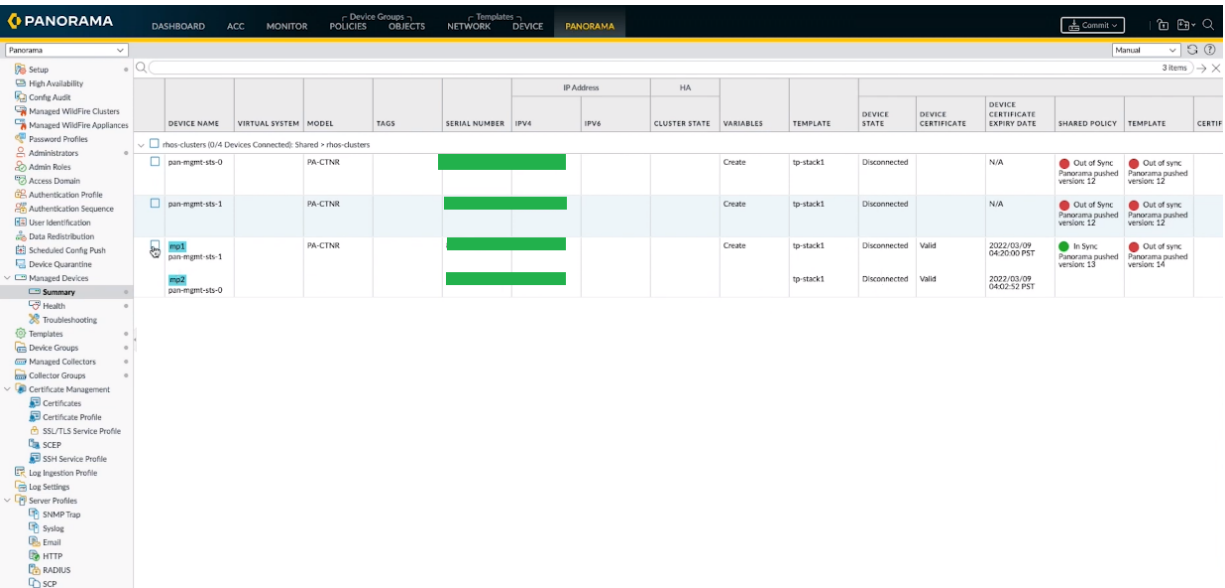
STEP 18 | 按一下 **Create**（建立）。

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。



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
```