paloalto TECHDOCS

CN 系列 HSF 部署

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

December 13, 2021

Table of Contents

CN-Series HSF

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

Palo Alto Networks **CN-Series Hyperscale Security Fabric** (HSF) 1.0 是容器化下一代防火牆叢集，可為部署 5G 網路的行動服務提供者提供具高度可調整且可復原的下一代防火牆解決方案。

CN-Series HSF 解決方案提供：

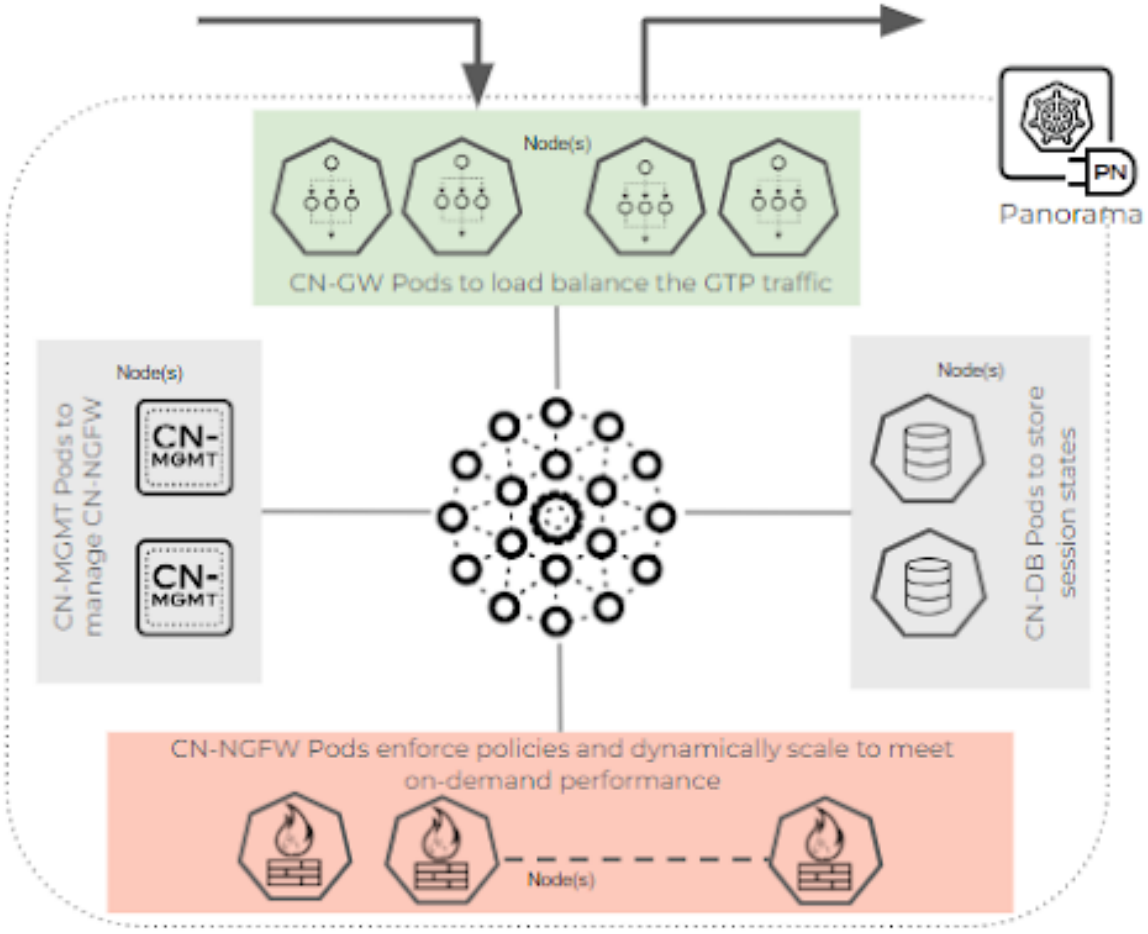
- 容器化 **NGFW** 的超可調整：隨選水平相應放大 AppID 和 GTP 效能。
- 高可用性和復原：提供彈性叢集，而這會根據預期的吞吐量和工作階段動態運作，並保證跨工作負載的業務連續性和工作階段復原能力。
- 消除外部負載平衡器相依性：提供易於部署和 DevOps 友好的環境，可以透過 Panorama 外掛程式完整協調。

CN-Series HSF 解決方案可部署在 RedHat Openshift（內部）或 AWS EKS 公共雲端管理的 Kubernetes 環境中。

CN-Series HSF 架構

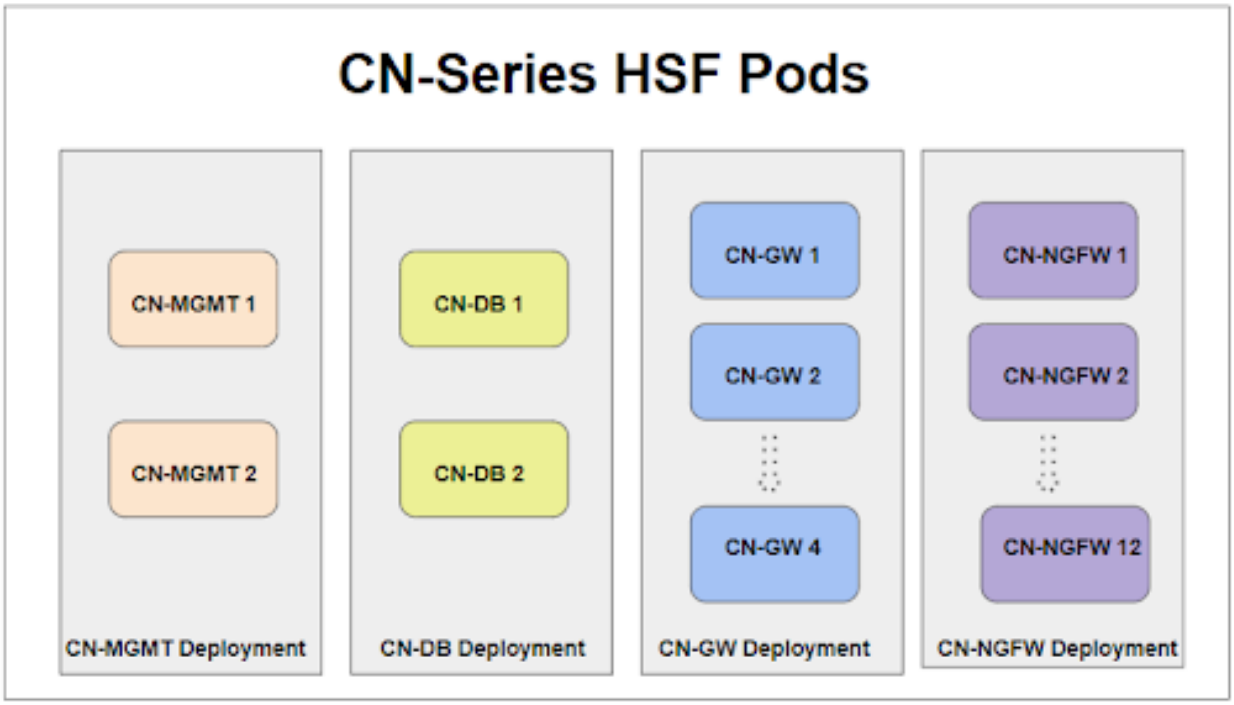
我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

CN-Series HSF 叢集是由內部網路所連線的 CN-MGMT（管理）、CN-NGFW（資料平面）、CN-GW（閘道）和 CN-DB（資料庫）Pod 集區所組成。CN-MGMT Pod 提供叢集管理平面功能。CN-NGFW Pod 提供叢集資料平面安全性功能。CN-GW Pod 是叢集的進入點，並且在 CN-NGFW Pod 之間分發流量。CN-DB Pod 提供 CN-NGFW Pod 所使用的中央叢集工作階段快取。



CN-Series HSF 支援兩個提供備援和可用性的 CN-MGMT 容器。不過，兩個 CN-MGMT 容器中只有一個可以接受來自 CN-NGFW DP 的連線。已連線的 CN-MGMT 將作為 StatefulSet 服務執行，以

允許 CN-NGFW 只連線至主動 CN-MGMT。除非目前 CN-MGMT 失敗，否則另一個 CN-MGMT 容器將不會連線至 CN-NGFW 容器。



Pod 的類型

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

CN-Series HSF 中有 3 種類型的資料平面 Pod，而且全部都使用相同的資料平面 Pod 映像，但將會有不同的 configmap 選項。CN-Series HSF 託管兩個管理 Pod。

CN-GW Pod - CN-GW Pod 是一種資料平面 Pod，可存取外部網路流量，以及管理進入和輸出流量的負載平衡。外部節點將只會知道 CN-GW Pod、其 IP 以及流量的所有資料子網路都會透過 Multus 介面連接至這些 Pod。CN-Series HSF 1.0 中最少支援 2 個和最多 4 個 CN-GW Pod。在 HSF 叢集部署的生命週期之前，CN-GW Pod 是靜態規模。例如，如果您一開始有 2 個 GW Pod，並且您想要相應放大，而 CN-NGFW Pod 可以動態相應放大，則必須重新部署具有額外 CN-GW Pod 數目的 HSF 叢集。

CN-DB Pod - CN-DB Pod 是一種資料平面 Pod，可以跨 CN-NGFW Pod 查詢工作階段/流程擁有權。CN-DB 支援根據不同的演算法（例如 ingress-slot、round-robin 和 session-load）來將工作階段

分發到不同的 CN-NGFW。CN-Series HSF 支援兩個 CN-DB Pod，並且在兩個 CN-DB Pod 之間複製工作階段資訊，而這兩個 CN-DB Pod 中的任何一個都會在流程的查閱/繫結時運作。

CN-NGFW Pod - CN-NGFW Pod 會處理 C 和 U 工作階段的實際流量、套用安全性政策，並允許單獨調整 CN-NGFW Pod。CN-Series HSF 1.0 中最少支援 2 個和最多 12 個 CN-NGFW Pod。

CN-MGMT Pod - 所有 NGFW Pod（CN-GW、CN-DB 和 CN-NGFW）都會透過 eth0 上的 IPsec 連線至單一 CN-MGMT Pod。

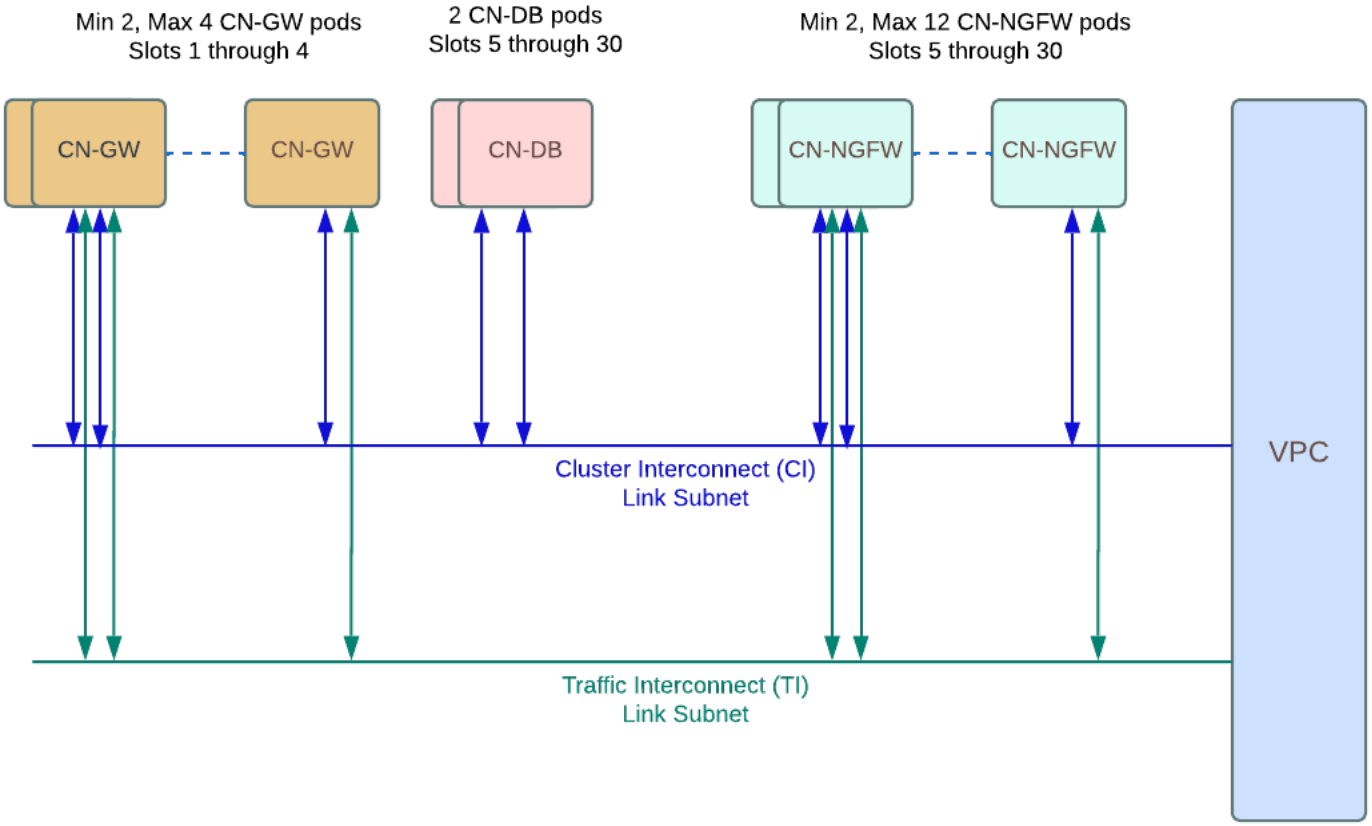
互連連結

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

所有 CN-GW、CN-DB 和 CN-NGFW Pod 都將會透過叢集互連 (CI) 連結（這是 Multus 介面）彼此連線。CI 連結是針對叢集通訊以及叢集成員之間轉寄封包所保留的資料連接埠。Ethernet x/1 用於所有相關 Pod 上的 CI 連結。CI 連結也可以用來將流量從某個 CN-NGFW 轉送至另一個 CN-NGFW。

CN-GW 和 CN-NGFW Pod 透過流量互連 (TI) 連結（這是 Multus 介面）彼此連線。TI 連結是針對叢集內的內部流量所保留的資料連接埠。Ethernet x/2 用於所有相關 Pod 上的 TI 連結。

在 CN-GW Pod 上，Ethernet x/3 以後將用作連線至客戶網路的外部介面。



CN-Series HSF 僅支援 *IPv4* 通訊協定。

針對內部部署環境，需要 *DHCP* 伺服器或 *IPAM*，才能將 *IP* 位址指派給 *CI* 和 *TI* 介面。針對 *AWS EKS*，*DHCP* 伺服器是基礎架構的一部分。因此，*IP* 位址會自動指派給雲端環境中的 *CI* 和 *TI* 介面。

授權 CN-Series HSF

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

CN-Series 防火牆授權是由 Panorama 上的 Kubernetes 外掛程式進行管理。CN-Series 防火牆是根據 Kubernetes 環境中所部署 CN-NGFW、CN-GW 和 CN-DB Pod 所使用的 vCPU（核心）總數進行授權。這些 Pod 所使用的每個 vCPU 都會耗用一個權杖。

- 啟動積分
- 建立 CN-Series HSF 部署設定檔
- 管理部署設定檔

啟動積分

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

您可以在組織內建立多個帳戶，各有不同用途。在啟動期間，每個預設積分池只能選擇一個帳戶。積分池一旦啟用，授與積分管理員角色的使用者就能將積分撥給部署，甚至將積分轉移到其他積分池。

如果您已有 CSP 帳戶，而且是超級使用者或管理員，系統會自動將積分管理員角色新增至設定檔。如果您沒有帳戶，CSP 會自動為您建立帳戶，並將積分管理員角色新增至設定檔。

您（購買者）會收到電子郵件，信中詳述訂閱、積分池 ID、訂閱開始和結束日期、購買的積分數量，以及預設積分池的描述（當您啟動積分時所建立的積分池）。

妥善保管此電子郵件供日後參考。

STEP 1 | 在電子郵件中，按一下 **Start Activation**（開始啟動）以檢視可用的積分池。

STEP 2 | 選取您要啟動的積分池。您可以使用搜尋欄位，依號碼或名稱來篩選帳戶清單。

如果您已購買多個積分池，則會自動選取這些積分池。核取記號代表上線積分的啟動連結。

系統會提示您驗證或登入。

如果您取消選取積分池，則會提醒您，如果想啟動這些積分，則必須返回電子郵件按一下 ***Start Activation***（開始啟動）連結。

STEP 3 | 選取 **Start Activation**（開始啟動）。

STEP 4 | 選取支援帳戶（您可以依帳戶號碼或名稱來搜尋）。

STEP 5 | 選取預設積分池。

STEP 6 | 選取 **Deposit Credits**（存入積分）。

您會看到存入成功的訊息。

STEP 7 | （選用）如果這是第一次啟動積分，您會看到 Create Deployment Profile（建立部署設定檔）對話方塊。

建立 CN-Series HSF 部署設定檔

這可在何處使用？	我需要哪些內容？
• CN 系列HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

使用以下程序建立 CN 系列部署設定檔。

STEP 1 | 如果您已有積分池，則請登入帳戶，然後從儀表板中選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分） > **Prisma NGFW Credits**（**Prisma NGFW** 積分） > **Create New Profile**（建立新設定檔）。

如果您剛啟動積分池，則會看到 **Create Deployment Profile**（建立部署設定檔）表單。

1. 選取 **CN-Series** 防火牆類型。
2. 選取 **PAN-OS 11.0**。
3. 按一下 **Next**（下一步）。

STEP 2 | CN-Series 設定檔。

1. **Profile Name**（設定檔名稱）。

   命名設定檔。

2. **Total vCPUs**（**vCPU** 總計）。

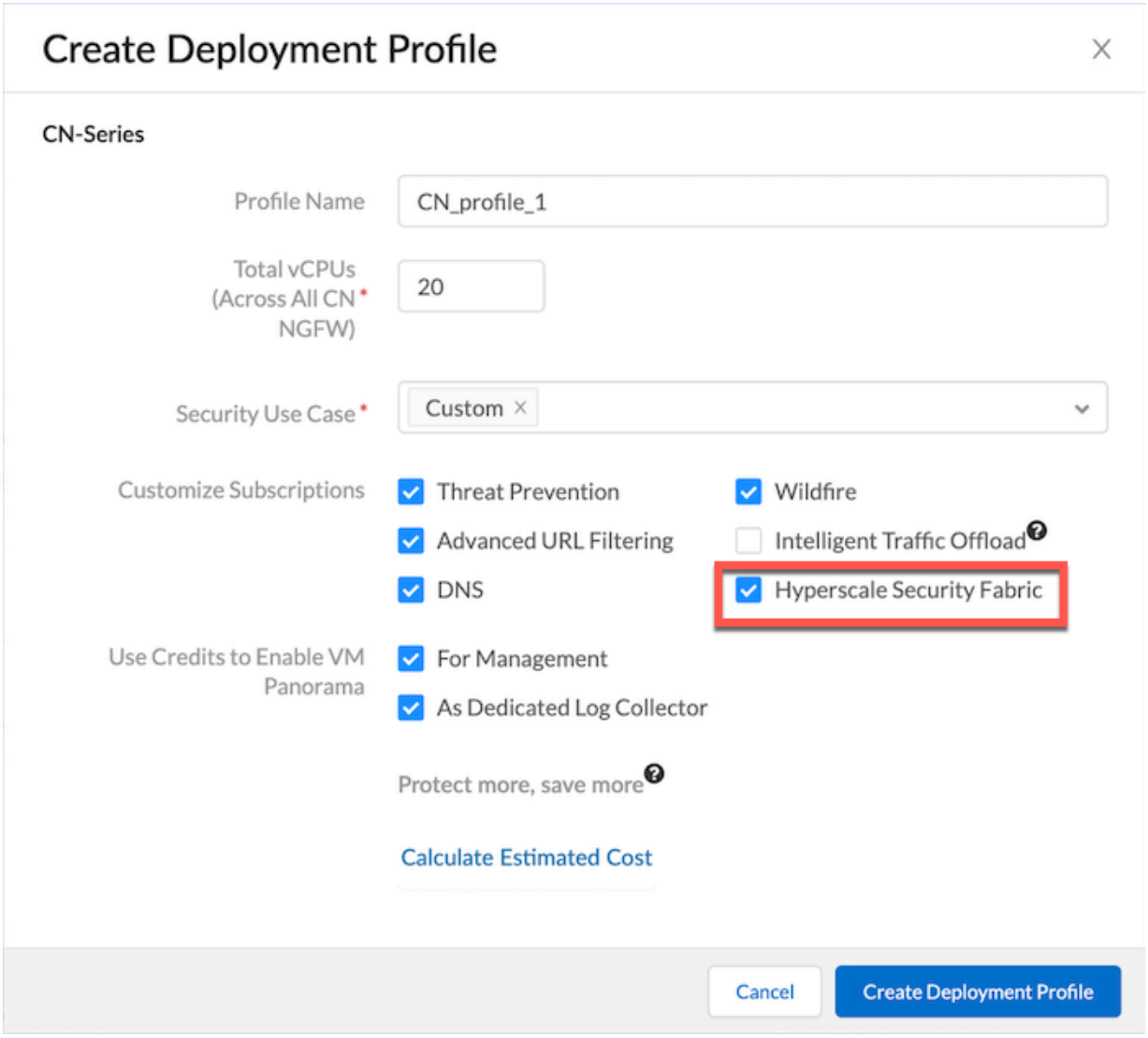
   輸入跨所有 Pod（CN-NGFW、CN-GW 和 CN-DB）所需的 vCPU 總數。

3. 從下拉式清單中，選取 [Security Use Case（安全性使用案例）]。下拉式清單中的每個安全性使用案例都會自動選取為所選擇使用案例建議的多個說明。如果您選取 [Custom（自訂）]，則可以指定您要在部署中使用的訂閱。

4. 在 **Customize Subscriptions**（自訂訂閱）下方選取 **Hyperscale Security Fabric**，以在您的訂閱上啟用 HSF。

5. （選用）**Use Credits to Enable VM Panorama**（使用積分來啟用 **VM Panorama**）—**For Management**（對於管理）或 **Dedicated Log Collector**（專用日誌收集器）。

STEP 3 | 按一下 **Calculate Estimated Cost**（計算預估成本），以檢視總積分和部署前可用的積分數量。



管理部署設定檔

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

您可以根據 CN-Series 部署的需求來編輯、複製或刪除 CN-Series 部署設定檔。此外，您還可以在建立部署設定檔之後於其中新增或移除訂閱。如需詳細資訊，請參閱管理部署設定檔。

CN-Series HSF 系統需求

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

- 建議的 CN-Series HSF 系統和容量矩陣
- 建議 CN-Series HSF 類別
- CN-Series HSF Jumbo 模式支援

建議的 CN-Series HSF 系統和容量矩陣

以下是我們針對 CN-Series HSF 所建議的系統需求。

下表依 CN-Series 大小來區隔資料：小型、中型和大型。CN-Series HSF 可執行的輸送量檢查會根據叢集的大小而不同。

- **HSF** 專用 **CN-Series** 小型
- **HSF** 專用 **CN-Series** 中型
- **HSF** 專用 **CN-Series** 大型

CN-Series HSF 需要兩個節點群組：各有兩個節點的 CN-MGMT 和 CN-DB。CN-GW 和 CN-NGFW 節點群組所需的節點數目取決於吞吐量。

叢集類別		小型	中	大
CN-GW	核心	24	24	24
	記憶體	16 GB	20 GB	24 GB
	頻寬	50 Gbps	100 Gbps	100 Gbps
	實例類型	c5n.9xlarge (36vCPU, 96Gi)	c5n.18xlarge	c5n.18xlarge
CN-DB	核心	8	8	12
	記憶體	0.64 x 12 x MaxSession (以百萬計) GB	0.64 x 12 x MaxSession (以百萬計) GB	0.64 x 10 x 10 GB
	頻寬	10 GbE	25 GbE	25 GbE

叢集類別		小型	中	大
	實例類型	c5n.4xlarge (16vCPU, 42Gi)	c5n.4xlarge	c5n.9xlarge
CN-MGMT	核心	4	12	12
	記憶體	16 GB	16 GB - 24 GB	16 GB - 24 GB
	頻寬	10 GbE	10 GbE	10 GbE
	磁碟	56 Gi	80 Gi	80 Gi
	實例類型	c5n.4xlarge (8vCPU, 21Gi)	c5n.4xlarge 或 c5d.9xlarge	c5n.4xlarge 或 c5d.9xlarge
CN-NGFW	核心	15	24	24 - 36
	記憶體	20 GB	16 GB - 47 GB	48 GB（超過 32 個核心需要 56 GB）
	頻寬	25 GbE	50 GbE	50 GbE
	實例類型	c5n.4xlarge (16vCPU, 42Gi)	c5n.9xlarge	c5n.9xlarge

建議 CN-Series HSF 類別

叢集類別	節點數目			介面總數	介面數目下限
	小型	中	大		
CN-GW	2	3	4	4-15	4
CN-DB	2	2	2	2	2
CN-MGMT	2	2	2	1	1
CN-NGFW	6	8	10	3	3
額外的 CN-NGFW 以涵蓋 DP 失敗	2	2	2	-	-

CN-Series HSF Jumbo 模式支援

啟用巨型支援時，Panorama 會將非 CN-MGMT 上所有介面的最大傳輸單位 (MTU) 設定為 8744 個位元組。

在巨型模式下，系統 *MTU* 是 *9000* 個位元組，而且如果未指定 *MTU*，則介面將會繼承系統 *MTU*。

在 *EKS* 主機中，*AWS EC2* 實例的預設 *MTU* 值為 *9000*。因此，主機端不需要任何設定。

停用巨型支援時，Panorama 會將非 CN-MGMT 上所有介面的最大傳輸單位 (MTU) 設定為 1756 個位元組。

您必須將 EKS 環境中的巨型和非巨型 MTU 值與 Panorama MTU 值相符。

模式	**MTU**（位元組）
Jumbo	EKS—9000 個位元組
非 Jumbo	適用於所有介面的 1756 個位元組

部署 CN-Series HSF 的先決條件

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

下列是部署 CN-Series HSF 的先決條件：

- 叢集需求
- 準備叢集
- 準備 Panorama 以進行 CN-Series HSF 部署

叢集需求

您將需要具有建立和管理 node-group 所需權限的 Kubernetes 叢集。您也需要 Kubernetes 外掛程式所需的資源，才能啟動 CN-Series 叢集。

您需要將下列內容設定為叢集先決條件：

- EKS 或 Openshift (4.10) 叢集，根據您所擁有的環境，您需要建立 VPC 和子網路，並設定啟動 EKS 叢集所需的 IAM 角色。

  如需建立 EKS 叢集的相關資訊，請參閱建立 Amazon EKS 叢集。

  如需建立 Openshift 叢集的相關資訊，請參閱安裝 Openshift 叢集。
- Kubernetes 1.22 版或更新版本。

  如需相關資訊，請參閱使用部署工具安裝 Kubernetes。
- Multus CNI，以啟用將多個網路介面附加至 Kubernetes 中的 Pod。

  如需詳細資訊，請參閱安裝 Multus CNI。
- 四個節點群組，具有 CN 系列需求中所述的最低要求。

準備叢集

您將需要設定下列項目：

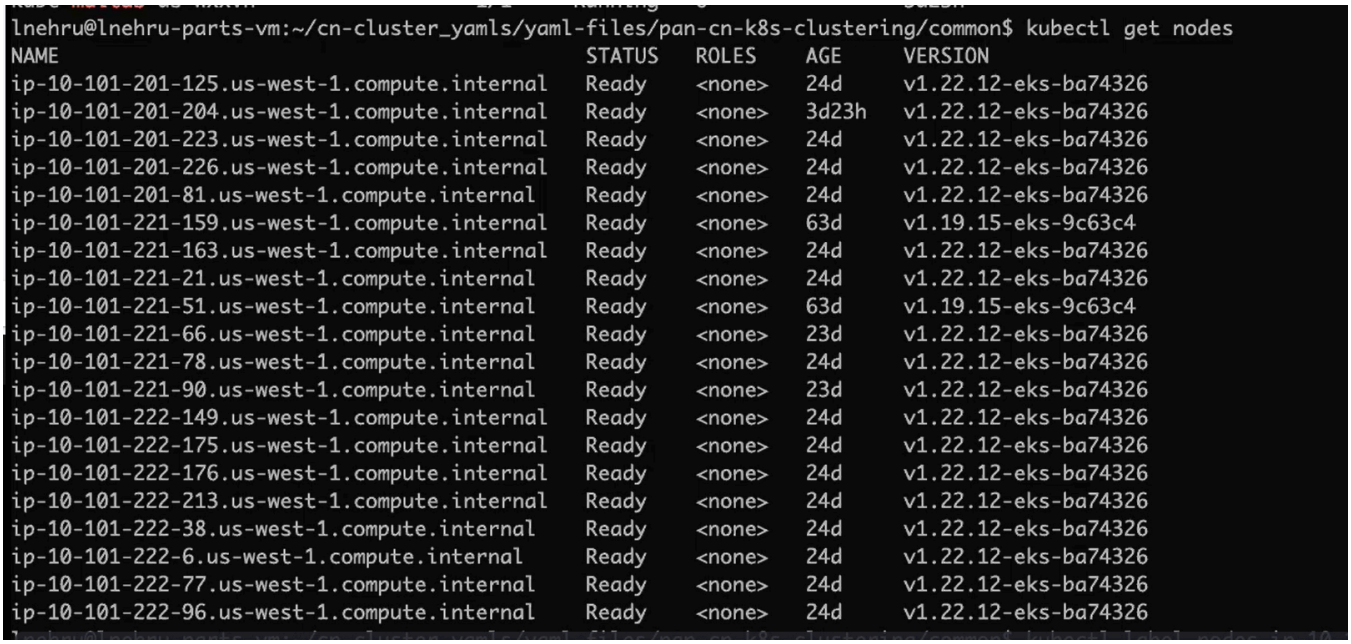
- Nodegroup 和節點
- 節點標籤
- 服務帳戶
- 介面

Nodegroup 和節點

您至少需要 8 個節點才能處理拓撲，以及容納解決方案中的所有 Pod。Palo Alto Networks 建議使用 4 組 nodegroup，且各至少有兩個節點。確定您不允許 MP nodegroup 與其餘 3 個 nodegroup 重疊。

如果您想要使用 DPDK，則需要具有已在其上設定 DPDK 驅動程式的 AMI。如需詳細資訊，請參閱在 AWS EKS 上設定 DPDK。

在您執行 EKS 叢集之後，請搭配使用 CloudFormation 範本與 Multus，以啟動具有 nodetypes 的 nodegroup 和 EC2 實例。



```
lnehru@lnehru-parts-vm:~/cn-cluster_yamls/yaml-files/pan-cn-k8s-clustering/common$ kubectl get nodes
NAME                                          STATUS   ROLES    AGE     VERSION
ip-10-101-201-125.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-201-204.us-west-1.compute.internal   Ready    <none>   3d23h   v1.22.12-eks-ba74326
ip-10-101-201-223.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-201-226.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-201-81.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-221-159.us-west-1.compute.internal   Ready    <none>   63d     v1.19.15-eks-9c63c4
ip-10-101-221-163.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-221-21.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-221-51.us-west-1.compute.internal    Ready    <none>   63d     v1.19.15-eks-9c63c4
ip-10-101-221-66.us-west-1.compute.internal    Ready    <none>   23d     v1.22.12-eks-ba74326
ip-10-101-221-78.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-221-90.us-west-1.compute.internal    Ready    <none>   23d     v1.22.12-eks-ba74326
ip-10-101-222-149.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-175.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-176.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-213.us-west-1.compute.internal   Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-38.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-6.us-west-1.compute.internal     Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-77.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
ip-10-101-222-96.us-west-1.compute.internal    Ready    <none>   24d     v1.22.12-eks-ba74326
```

節點標籤

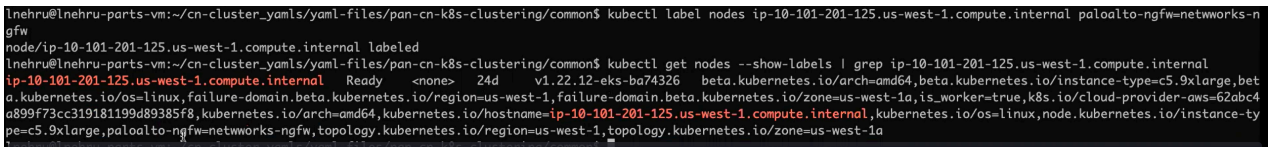
使用下列命令，以標示所有節點：

```
kubectl label node (MP_node_name) Panw-mp=Panw-mp
kubectl label node (DB_node_name) Panw-db=Panw-db
kubectl label node (GW_node_nam) Panw-gw=Panw-gw
kubectl label node (NGFW_node_name) Panw-ngfw=Panw-ngfw
```

以下是節點標籤範例：

```
CN-NGFW - paloalto-ngfw: networks-ngfw
CN-MGMT - paloalto-mgmt: networks-mgmt
CN-GW - paloalto-gw: networks-gw
CN-DB - paloalto-db: networks-db
```

預期會針對每種節點類型提供鍵值配對。此外，建議使用預設值 key paloalto 和值 networks。不過，如果您選擇變更節點標籤，則需要在設定中進行相應的變更。



標示節點之後，請下載啟動叢集所需的 YAML。

服務帳戶

部署的已擴充權限是使用服務帳戶 yaml 所提供。若要建立服務帳戶，Kubernetes 叢集應該就緒。

1. 執行 `plugin-deploy-serviceaccount.yaml` 的服務帳戶 YAML。

   服務帳戶會啟用 Panorama 向叢集進行驗證所需的權限來擷取 Kubernetes 標籤和資源資訊。此服務帳戶的名稱預設為 pan-plugin-user。

2. 導覽至 yaml-files/clustering 資料夾/common，然後部署下列項目：

   ```
   kubectl apply -f plugin-deploy-serviceaccount.yaml
   ```

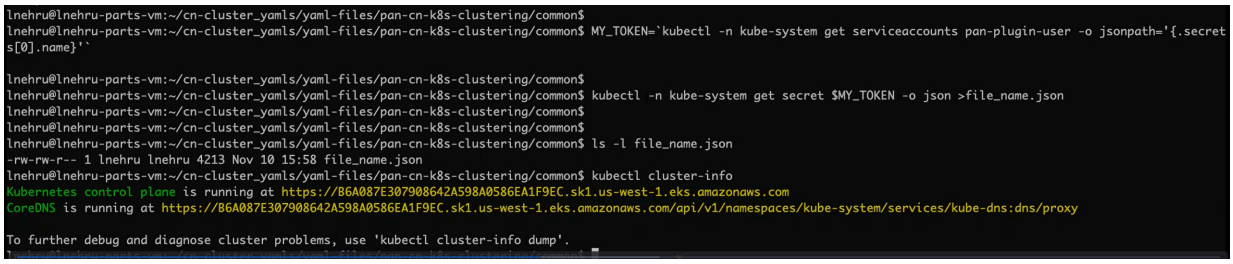
   ```
   kubectl apply -f pan-mgmt-serviceaccount.yaml
   ```

   ```
   kubectl -n kube-system get secrets | grep pan-plugin-user-token
   ```

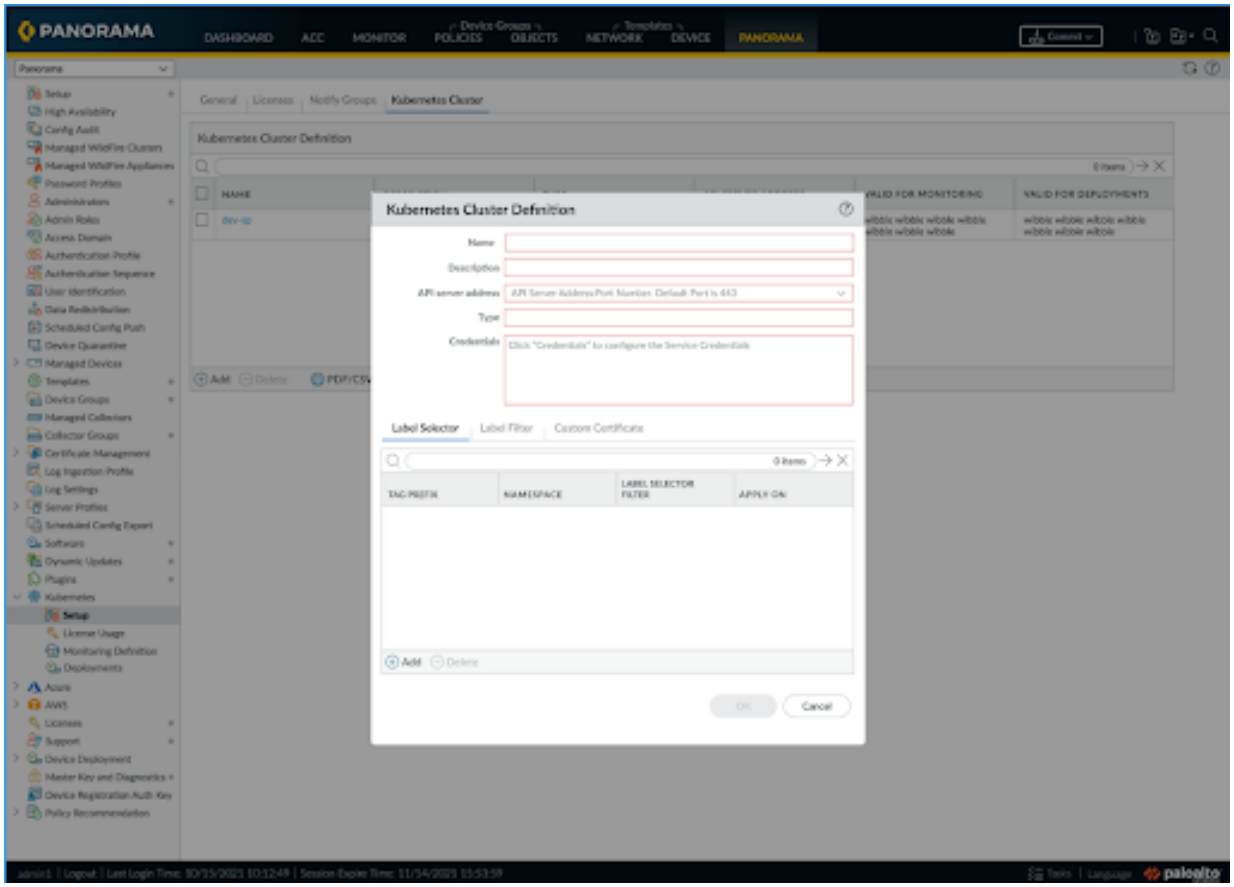
   建立包含密碼的認證檔案（例如 cred.json），並儲存此檔案。您需要將此檔案上傳至 Panorama，以設定用於監控叢集的 Kubernetes 外掛程式。

3. 檢視與此服務帳戶相關聯的祕密。

```
kubectl -n kube-system get secrets (secrets-from-above-command) -o
json >> cred.json
```



4. 將 cred.json 上傳至 kubernetes 外掛程式，並驗證驗證狀態。



在 Panorama 上進行第一個驗證後置提交之後，外掛程式將會繼續定期呼叫驗證邏輯，並更新 UI 上的驗證狀態。

介面

您將需要建立 CN-DB、CN-NGFW 和 CN-GW 所需的 ENI。識別這些介面的 PCI 匯流排 ID，之後會使用這些 ID 來建立用於將 Pod 互連的網路附件定義。

1. 使用您在建立叢集時所建立的金鑰/使用者，以透過 SSH 連線至節點。

   ```
   ssh ec2-user@(node_ip) -i private_(key)
   ```

2. 安裝 ethtool 套件。

   ```
   Sudo yum install ethtool
   ```

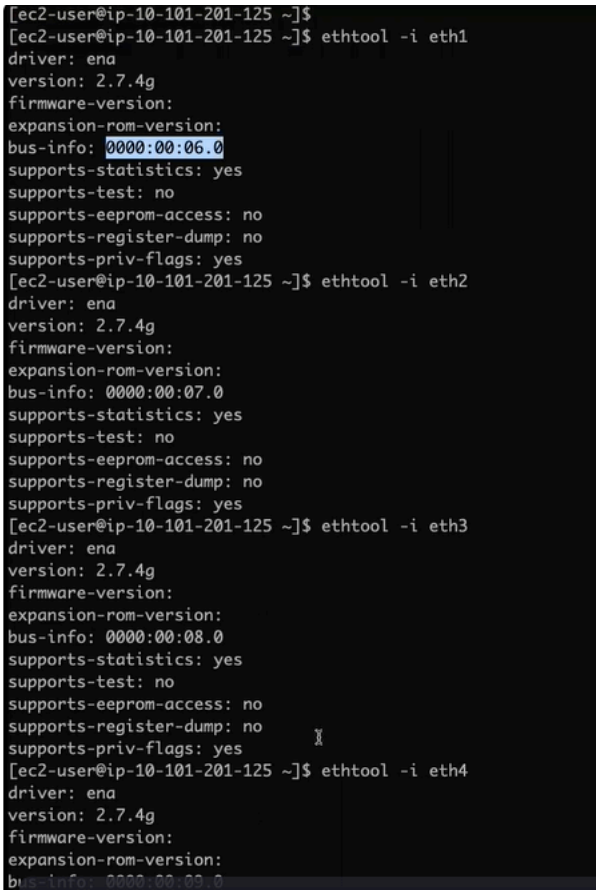
   ```
   sudo yum update -y && sudo yum install ethtool -y
   ```

3. 識別介面名稱。

   ```
   ifconfig
   ```

4. 識別介面的 PCI 匯流排 ID，以在 Pod 上部署網路連線。

```
ethtool -i (i/f)
```



此處，eth0 是節點管理介面、eth1 是 CI 介面、eth2 是TI、eth3 是外部介面 1、eth4 是外部介面 2。在針對 CN-MGMT 所標記的節點中，您只會找到用於管理的 eth0 介面。針對 CN-DB，您將會有 eth1；針對 CN-NGFW，您將會有 eth1、eth2；針對 CN-GW，您將會有 eth1、eth2 以及您在環境中所建立的數個外部介面。

```
   net-attach-1 - 0000:00:08.0 net-attach-2 - 0000:00:09.0 net-
attach-def-ci-db - 0000:00:06.0 net-attach-def-ci-gw - 0000:00:06.0
 net-attach-def-ci-ngfw - 0000:00:06.0 net-attach-def-ti-gw -
 0000:00:07.0 net-attach-def-ti-ngfw - 0000:00:07.0
```

部署的所有 Pod 都需要位於不同的節點，因為它們將使用相同的網路附件定義，因此每個 Pod 都需要存取相同的 PCI 匯流排 ID。例如，如果 net-attach 要將 PCI ID 6 用於 C/U Pod CI 連結，則每個 C/U Pod 都需要放置在具有來自相同子網路的 PCI ID 6 介面的節點上。

5. 修改網路附件定義 YAML 上的 PCI 匯流排 ID。

```
   { "cniVersion":"0.3.1", "type": "host-device",
"pciBusID":"0000:00:07.0" }
```


在這裡，第一個連結 eth1 用作 CI、eth2 用作 TI，而 eth3 之後項目用於外部連結。

6. 套用先決條件 YAML 檔案。

```
kubectl apply -f pan-mgmt-serviceaccount.yaml
kubectl apply -f net-attach-def-1.yaml
kubectl apply -f net-attach-def-2.yaml
kubectl apply -f net-attach-def-ci-db.yaml
kubectl apply -f net-attach-def-ci-gw.yaml
kubectl apply -f net-attach-def-ci-ngfw.yaml
kubectl apply -f net-attach-def-ti-gw.yaml
kubectl apply -f net-attach-def-ti-ngfw.yaml
```

在 Openshift 中，套用 `Kubectl apply -f ctrcfg-pidslimit.yaml`。如需 pidlimit 的詳細資訊，請參閱設定工作。

如果使用靜態 PV，則請在標記為 CN-MGMT Pod 的節點上建立靜態 PV 裝載磁碟區。

```
/mnt/pan-local1, /mnt/pan-local2, /mnt/pan-local3, /mnt/pan-local4, /
mnt/pan-local5, /mnt/pan-local6
```


準備 Panorama 以進行 CN-Series HSF 部署

CN-Series HSF 設定和部署是透過 Panorama 所完成。部署 CN-Series HSF 之前，請確保您已完成下列先決條件。

STEP 1 | 部署軟體版本為 11.0 的 Panorama，並安裝最小內容版本。

1. 移至 **Panorama** > **Dynamic Updates**（動態更新），以取得 PAN-OS 11.0 上的最小內容發行版本。

   請參閱 PAN-OS 版本資訊。

2. 移至 **Panorama** > **Software**（軟體），以取得軟體版本。

   根據您要升級的目標發行版本，找到並下載型號特定檔案。例如，若要將 M-Series 設備升級至 Panorama 11.0.0，請下載 Panorama_m-11.0.0 映像；若要將 Panorama 虛擬設備升級至 Panorama 11.0.0，請下載 Panorama_pc-11.0.0 映像。

   成功下載之後，所下載映像檔的 **Action**（動作）欄會從 [Download（下載）] 變更為 [Install（安裝）]。

STEP 2 | 如果您想要 Panorama 收集防火牆日誌，則請驗證 Panorama 處於 Panorama 模式。

STEP 3 | 在 Panorama 上，安裝 Kubernetes 外掛程式 4.0 版本。如果您將 Panorama 設備部署為 HA 配對，則必須先在主要（主動）對等上安裝 Kubernetes 外掛程式。

1. 登入 Panorama 網頁介面，並選取 **Panorama** > **Plugins**（外掛程式），然後按一下 **Check Now**（立即檢查）以取得可用外掛程式清單。
2. 選取 **Download**（下載），並 **Install**（安裝） Kubernetes 外掛程式 4.0 版。

   在您成功安裝外掛程式之後，會重新整理 Panorama，而且 Kubernetes 外掛程式會出現在 **Panorama** 頁籤上。

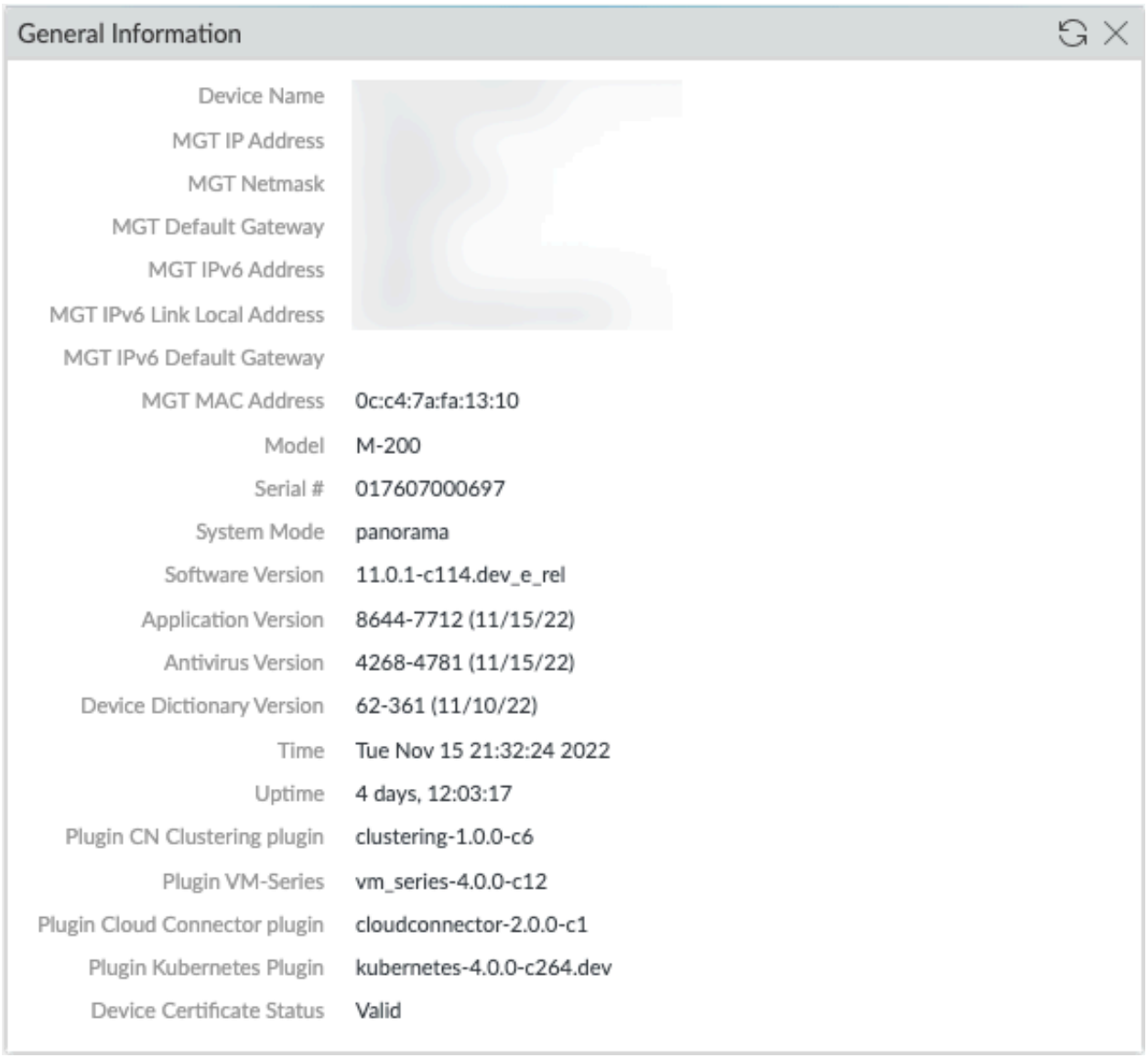
   如果 Panorama 部署在 HA 配對中，則請使用步驟 3 中所述的步驟以在次要（被動）Panorama 上安裝 Kubernetes 外掛程式。
3. 按一下 **Commit to Panorama**（提交至 **Panorama**）。

   此提交會建立 **K8S-CNF-Clustering-Readonly** 範本，以與 CN-Series HSF 搭配使用。最多需要一分鐘的時間，以在 Panorama 上顯示介面。此範本具有下列連結的網路設定：針對 CN-GW、CN-DB 和 CNNGFW Pod 的預先設定叢集互連 (CI) 連結，以及針對 CN-GW 和 CN-NGFW Pod 的流量互連 (TI) 連結。**K8S-CNF-Clustering-Readonly** 會建立 30

個邏輯路由器，而且每個邏輯路由器都有兩個介面。Ethernet x/1 是叢集互連 (CI) 連結，而 Ethernet x/2 是叢集互連 (TI) 連結。

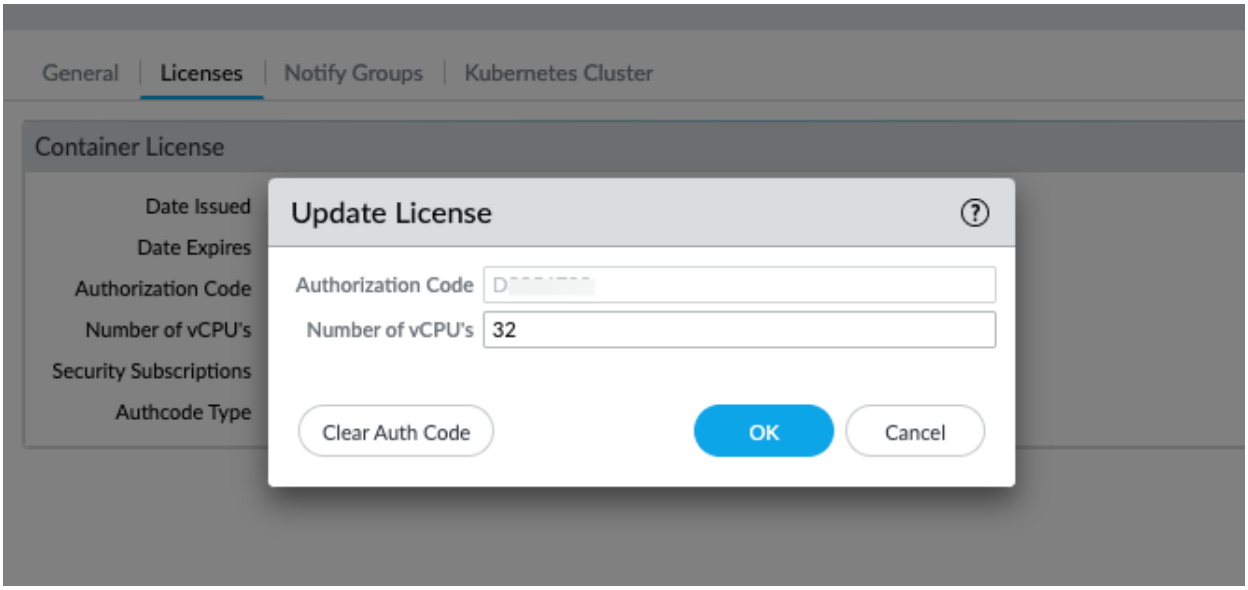
請確定您未重新命名 ***K8S-CNG-Clustering-Readonly*** 範本。

您可以在 Panorama **Dashboard**（儀表板） > **General Information**（一般資訊）**]** 上驗證 **[General Information**（一般資訊）**] Widget**。



STEP 4 | 取得 Panorama 上的 CN-Series HSF 授權積分。

1. 選取 **Panorama** > **Plugins**（外掛程式） > **Kubernetes** > **Setup**（設定） > **Licenses**（授權）。
2. 選取 **Activate/update using authorization code**（使用授權碼啟動/更新），以及輸入授權碼和所需的資料平面 vCPU 總數。您必須建立部署設定檔以取得您的 CN 系列授權碼。



使用 *HSF* 部署 *CN-Series* 時，如果部署的 *Pod*（*CN-NGFW*、*CN-GW* 和 *CN-DB*）數目超過配置的 *vCPU* 數目，則您有四個小時的寬限期可將更多的 *vCPU* 新增至您的部署設定檔，或刪除足夠的 *Pod*。如果您未在四小時的寬限期內配置額外的 *vCPU*，或刪除未授權的 *Pod*，則未授權的 *Pod* 將會重新啟動，並建立流量中斷。已授權的 *Pod* 會保留已授權狀態。

3. 驗證是否已更新可用授權積分數目。

STEP 5 | 建立父系裝置群組。

您必須使用 CN-Series HSF 所需的必要政策和物件來建立裝置群組。當您部署 CN-Series HSF 時，必須參考此裝置群組。

1. 移至 **Panorama** > **Device Groups**（裝置群組），然後按一下 **Add**（新增）。
2. 輸入唯一的 **Name**（名稱）及 **Description**（描述）以識別裝置群組。
3. 在裝置群組階層中選取位於您建立裝置上方的 **Parent Device Group**（父系裝置群組）（預設為 **Shared**（共用））。
4. 按一下 **OK**（確定）。

   裝置群組名稱會啟動至叢集中的 CN-MGMT Pod。CN-MGMT Pod 使用這些啟動參數連線至 Panorama 時，裝置群組會與叢集設定中的叢集名稱相關聯。針對 Panorama 高可用

性 (HA)，CN-MGMT Pod 會將更新傳送至主動和被動 Panorama。會自動填入作用中 CN-NGFW、CN-DB 和 CN-GW Pod 的叢集資訊。

5. 選取 **Commit**（提交） > **Commit and Push**（提交並推送），以將裝置群組設定提交並推送至 Panorama。

STEP 6 | 建立變數範本，以啟用流量。

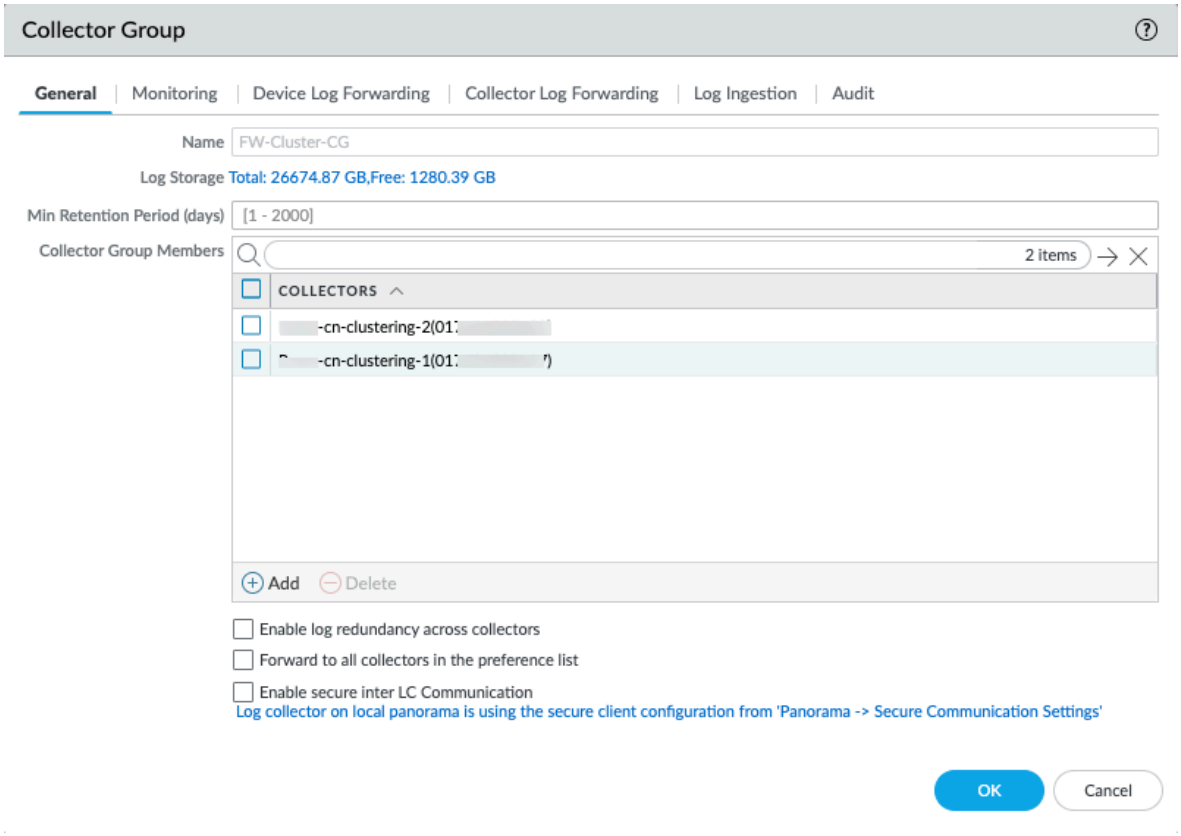
1. 移至 **Panorama** > **Templates**（範本），然後按一下 **Add**（新增）。
2. 輸入範本的唯一 **Name**（名稱）。
3. 輸入選用 **Description**（說明）。
4. 設定變數範本以啟用流量。

   您可以在部署 *CN-Series HSF* 之前或之後設定此範本。

STEP 7 | 建立日誌收集器，並將其新增至日誌收集器群組。

1. 移至 **Panorama** > **Collector Groups**（收集器群組），然後 **Add**（新增）收集器群組。
2. 輸入「收集器群組」的 **Name**（名稱）。
3. 輸入收集器群組保留防火牆日誌的 **Minimum Retention Period**（最短保留週期）天數（1 至 2,000）。

   依預設，欄位是空白，表示收集器群組無限期保留日誌。
4. 將日誌收集器（1 至 16 個）**Add**（新增）至 Collector Group Members（收集器群組成員）清單。



5. 選取 **Commit**（提交） > **Commit and Push**（提交並推送），以將您的變更提交並推送至 Panorama 和您設定的收集器群組。

Kubernetes 外掛程式將會建立和管理 *Panorama authkey*。

部署 HSF 叢集

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

確保滿足將 CN-Series 防火牆部署為 HSF 的先決條件之後，請導覽至 **Kubernetes** > **Deployments**（部署），然後按一下 **Add**（新增）。

您將需要設定下列頁籤來部署 HSF 叢集。

- 總言
- 節點資料
- 映像和儲存體
- CN 設定
- 自動調整

總言

在 **Deployments**（部署）快顯視窗的 **General**（一般）頁籤區段上，輸入下列詳細資料。

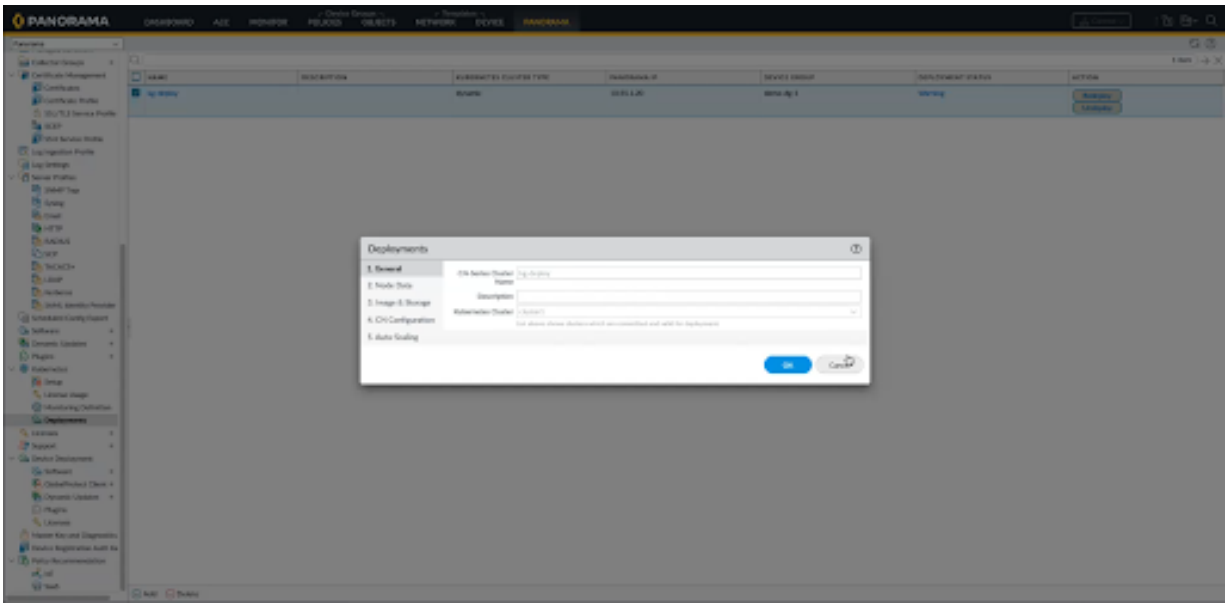
STEP 1 | **CN-Series Cluster Name**（**CN-Series** 叢集名稱）—CN-Series HSF 的名稱。

STEP 2 | （選用）**Description**（說明）—說明 HSF 叢集的文字字串。

STEP 3 | **Kubernetes Cluster**（**Kubernetes** 叢集）—會在外掛程式的 **Setup**（設定）區段下方建立叢集項目清單。從下拉式清單中，選擇您所建立的相關叢集。

只有在詳細資料已提交且對部署有效時，才會顯示 *Kubernetes* 叢集。

STEP 4 | **CN-Series Cluster Name**（**CN-Series** 叢集名稱）—CN-Series HSF 的名稱。

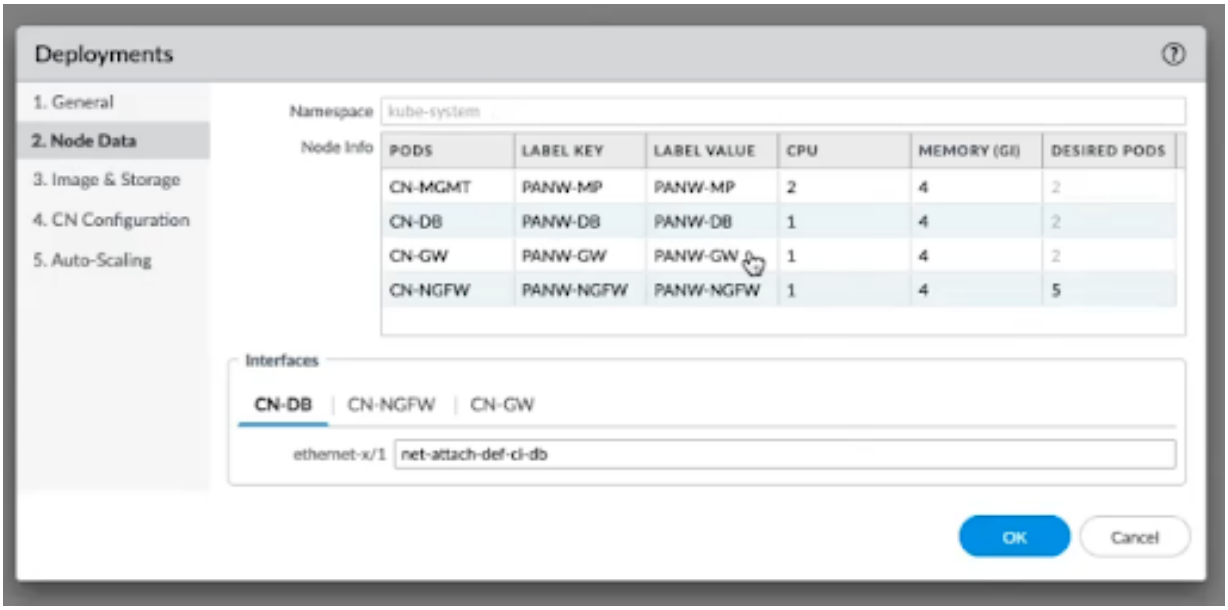


節點資料

在 **Deployments**（部署）快顯視窗的 **Node Data**（節點資料）頁籤區段上，輸入下列詳細資料。

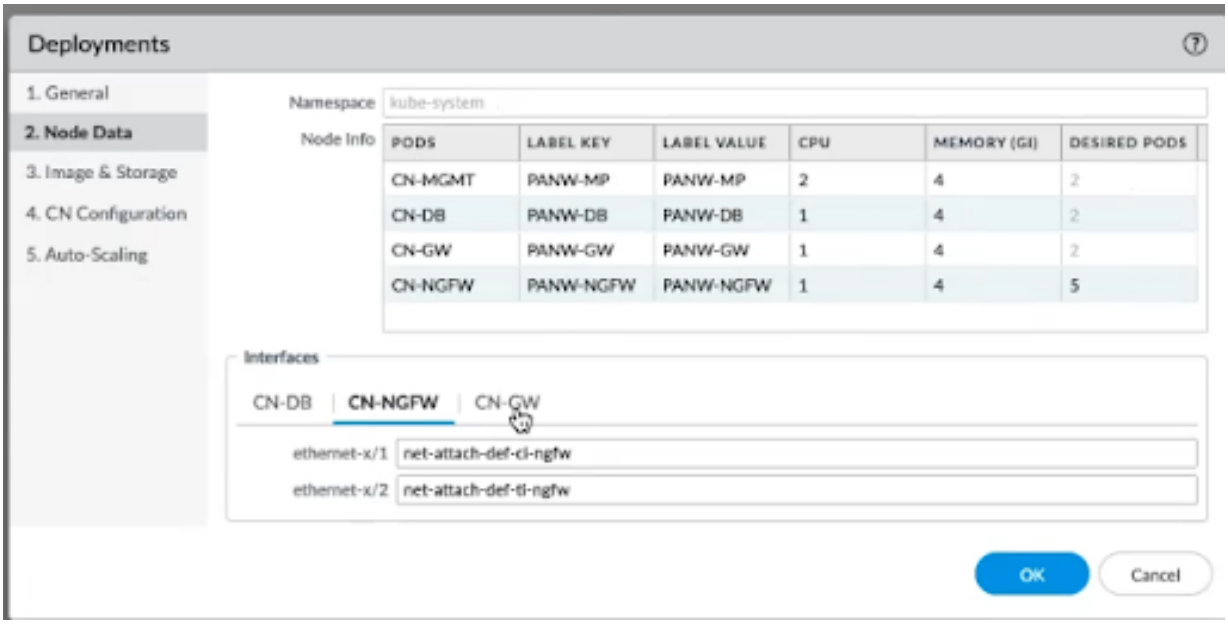
STEP 1 | **Namespace**（命名空間）—現有 Kubernetes 叢集中將部署 CN-Series HSF 的命名空間。

STEP 2 | **Node Info**（節點資訊）—節點集區標籤用來部署每種類型的 CN Pod。您需要根據節點上的可用性，以針對每種 Pod 類型指定 CPU、記憶體和所需 Pod。標籤和標籤值配對是存在於節點上的先決條件值，而且您必須新增用來標示節點的相同鍵值配對。



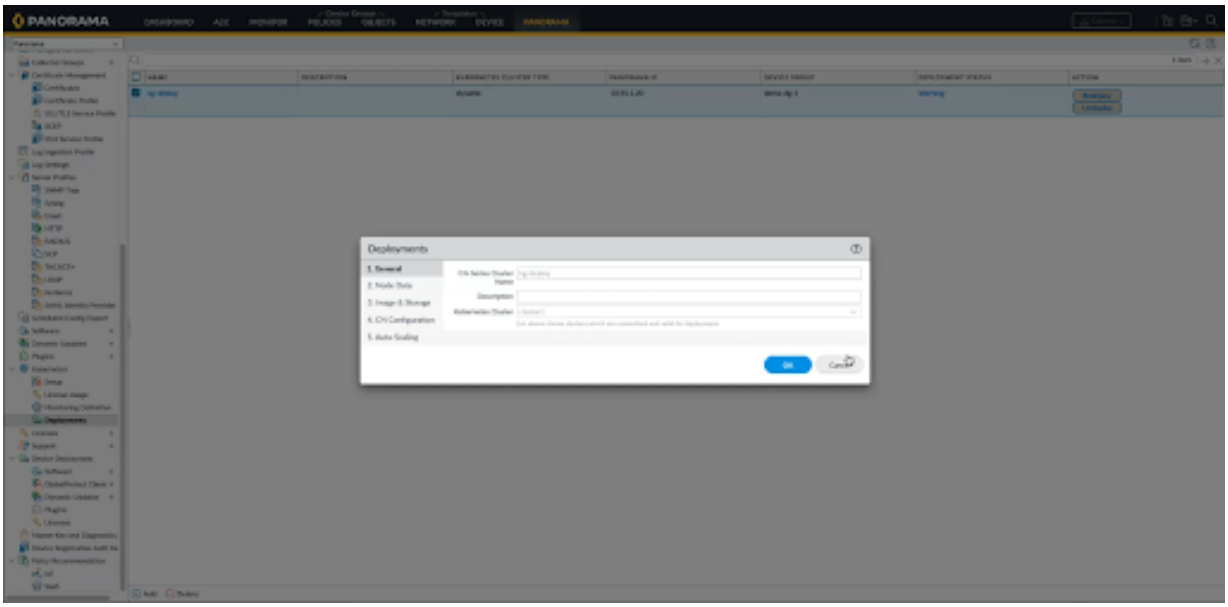
STEP 3 | **Interfaces**（介面）—需要新增 CN-DB、NGFW、CN-GW Pod 的介面名稱。每個介面都需要在 Kubernetes 叢集上套用特定 net-attach-def。根據預設，外掛程式將會命名為 Ethernet x/1 和

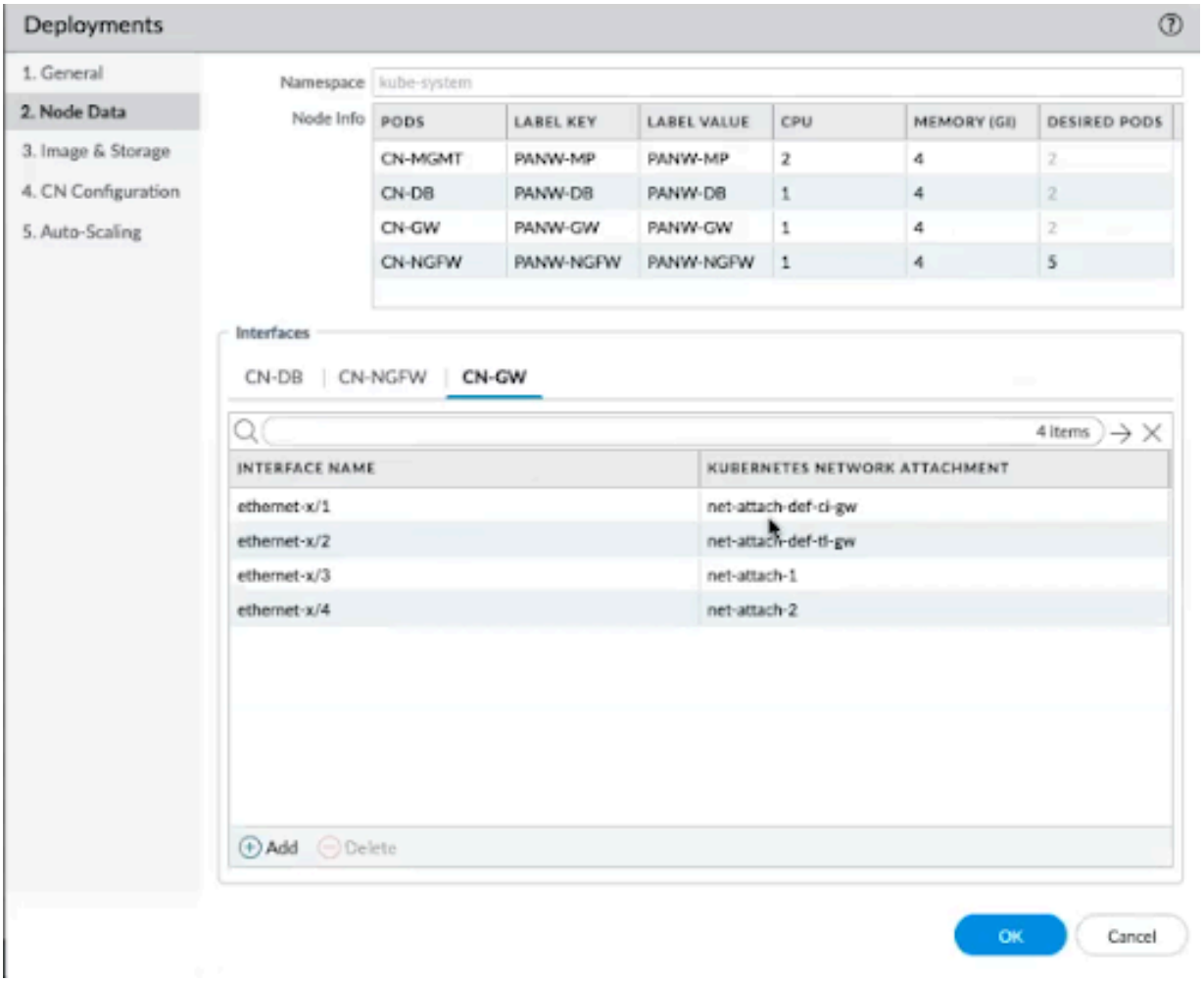
Ethernet x/2。如果您變更 Ethernet x/1 和 Ethernet x/2 的介面名稱，則也需要在網路附件區段中進行變更。針對 CN-GW Pod，您最多可以新增 12 個介面，但不包括 CI 和 TI 介面。



只有在詳細資料已提交且對部署有效時，才會顯示 *Kubernetes* 叢集。

STEP 4 | **CN-Series Cluster Name**（**CN-Series** 叢集名稱）—CN-Series HSF 的名稱。





映像和儲存體

在 **Deployments**（部署）快顯視窗的 **Image & Storage**（映像和儲存體）頁籤區段上，輸入下列詳細資料。

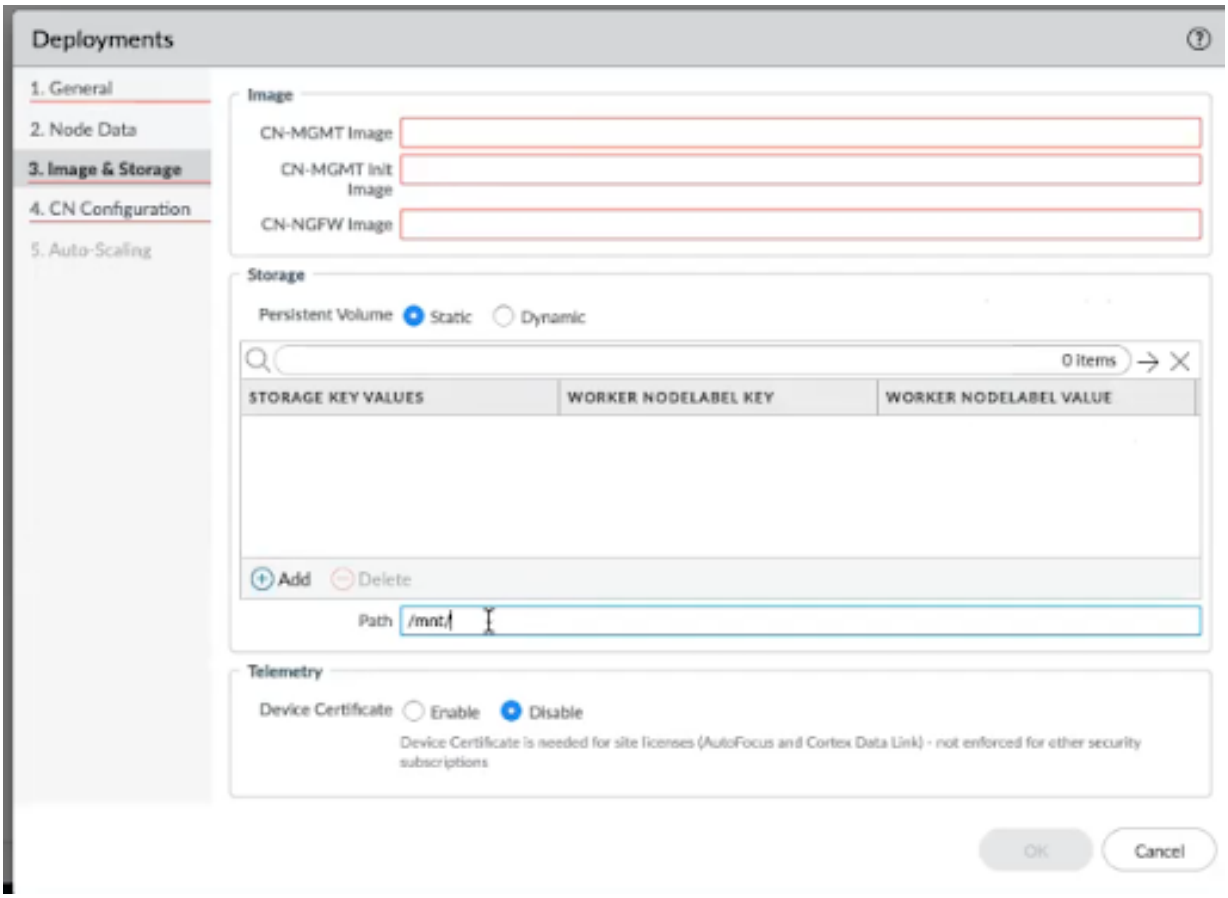
STEP 1 | **Image**（映像）—您需要將映像儲存至本機或 AWS 儲存庫，而這無法透過 Panorama 進行驗證。不過，Kubernetes 叢集可以連線至儲存映像的儲存庫。

1. **CN-MGMT** 映像：來自儲存庫的完整 URI，其中是由 Kubernetes 環境存取映像來部署 CN-MGMT Pod。
2. **CN-MGMT INIT** 映像：CN-MGMT Pod 所需的 init 映像。
3. **CN-NGFW** 映像：來自儲存庫的完整 URI，其中是由 Kubernetes 環境存取映像來部署 CN-NGFW Pod。

STEP 2 | **Storage**（儲存體）—如果您想要設定獨占儲存體，則請在 EKS 環境的 [Storage（儲存體）] 區段中按一下 **Dynamic**（動態），並針對 Openshift 環境，按一下 [Static（靜態）] 或

[Dynamic（動態）]，而外掛程式將會設定雲端儲存。如果您已選擇 **Static**（靜態），則需要輸入 Storage Key Values、Worker Nodelabel Key 和 Worker Nodelabel Value。您也需要輸入裝載儲存體的 **Path**（路徑）。

您必須在 *kubernetes* 環境的命名空間中新增有效的非預設儲存體類別。否則，如果已選取動態儲存體選項，但未提供儲存體類別名稱，則將會選取命名空間中存在的預設儲存體類別。



STEP 3 | **Certificates**（憑證）—這是可啟用或停用授權這類資訊的裝置憑證資訊，如果已啟用，則您將需要提供 PIN ID 和 PIN 值。

CN 設定

在 **Deployments**（部署）快顯視窗的 **CN Configuration**（**CN** 設定）頁籤區段上，輸入下列詳細資料。

STEP 1 | **Primary Panorama IP**（主要 **Panorama IP**）—顯示安裝外掛程式的 Panorama 的公共和私人 IP 位址值。

STEP 2 | **Secondary Panorama IP**（次要 **Panorama IP**）—顯示安裝外掛程式的次要 Panorama（進行 HA 時）的公共和私人 IP 位址值。

STEP 3 | **Device Group**（裝置群組）—您需要在設定部署之前建立 DG，如先決條件小節所提及。[Device Group（裝置群組）] 下拉式清單會列出目前 Panorama 上的所有 DG，而且您需要選擇有效的 DG。CN-MGMT Pod 將會在此 DG 下方進行註冊。如需建立裝置群組的步驟，請參閱準備 Panorama 以進行 CN-Series HSF 部署 的步驟 5。

STEP 4 | **Template**（範本）—設定部署之前，您需要針對 CN-GW 特定詳細資料建立範本 (variable_template)，如先決條件小節所提及。[Template（範本）] 下拉式清單列出目前 Panorama 上的所有範本。您需要選擇適合您目前部署的範本。在 HSF 部署之後，外掛程式會將此範本與 K8S-CNF-Clustering-Readonly 範本一起新增至範本堆疊，而後者處理 CN-DB 和 CN-NGFW Pod 的基本設定。其也會在 CN-GW Pod 上設定 CI 和 TI 連結。CN-MGMT Pod 會從範本堆疊中取得設定。如需建立變數範本的步驟，請參閱準備 Panorama 以進行 CN-Series HSF 部署 的步驟 6。

STEP 5 | **Log Collector Group (LCG)**（日誌收集器群組 **(LCG)**）—此下拉式清單會列出目前 Panorama 上的所有日誌收集器群組，而且需要選擇適合的 LCG。其也會設定 CN-GW Pod 的 CI 和 TI 連結。如需建立 LCG 的步驟，請參閱準備 Panorama 以進行 CN-Series HSF 部署 的步驟 7。

STEP 6 | **Jumbo Frame**（巨型框架）—[Jumbo Frame（巨型框架）] 下拉式清單會列出值：**Enable**（啟用）、**Disable**（停用）和 **AutoDetect**（自動偵測）。此設定適用於 CN-Series HSF 中的所有 Pod。

STEP 7 | **5G Enabled**（已啟用 **5G**）—這是具有 **Enable**（啟用）和 **Disable**（停用）選項的按鈕選項，並且參照 CN-Series HSF 上所需的 GTP 設定。

您需要在 ***variable_template*** 檔案中處理範本上所需的進一步設定。

STEP 8 | **DPDK**—這是具有 **Enable**（啟用）和 **Disable**（停用）選項的選項按鈕。如果基礎資源不支援 DPDK，則根據預設，CN-Series HSF 將會預設為 packetmmap。

在 *EKS* 上，如果您想要使用 *DPDK*，則需要具有已在其上設定 *DPDK* 驅動程式的 *AMI*。如需詳細資訊，請參閱在 AWS EKS 上設定 DPDK。

若要在 Openshift 上啟用 DPDK，您需要在工作節點上啟用巨型分頁。如需詳細資訊，請參閱設定巨型分頁。

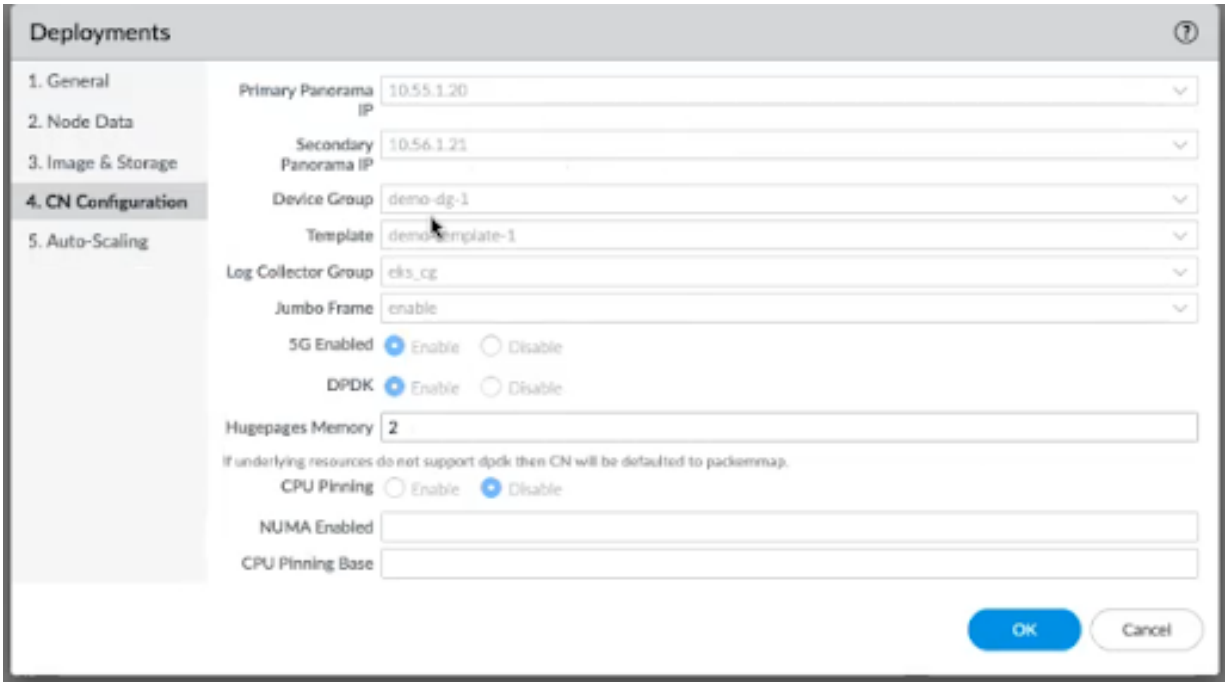
您也需要在工作節點上啟用 VFIO PCI 驅動程序。

```
modprobe vfio-pci echo 1 > /sys/module/vfio/parameters/
enable_unsafe_noiommu_mode
```

STEP 9 | **CPU Pinning**（**CPU** 釘選）—選擇啟用或停用 CPU 釘選。

STEP 10 | **Numa Enabled**（已啟用 **Numa**）—提供 NUMA 的節點編號。

STEP 11 | **CPU Pinning Base**（**CPU** 釘選庫）—提供您想要從中開始轉送程序的 CPU 釘選，並跳過編號較低的 CPU。



自動調整

在 **Deployments**（部署）快顯視窗的 **Auto-Scaling**（自動調整）頁籤區段上，輸入下列詳細資料。

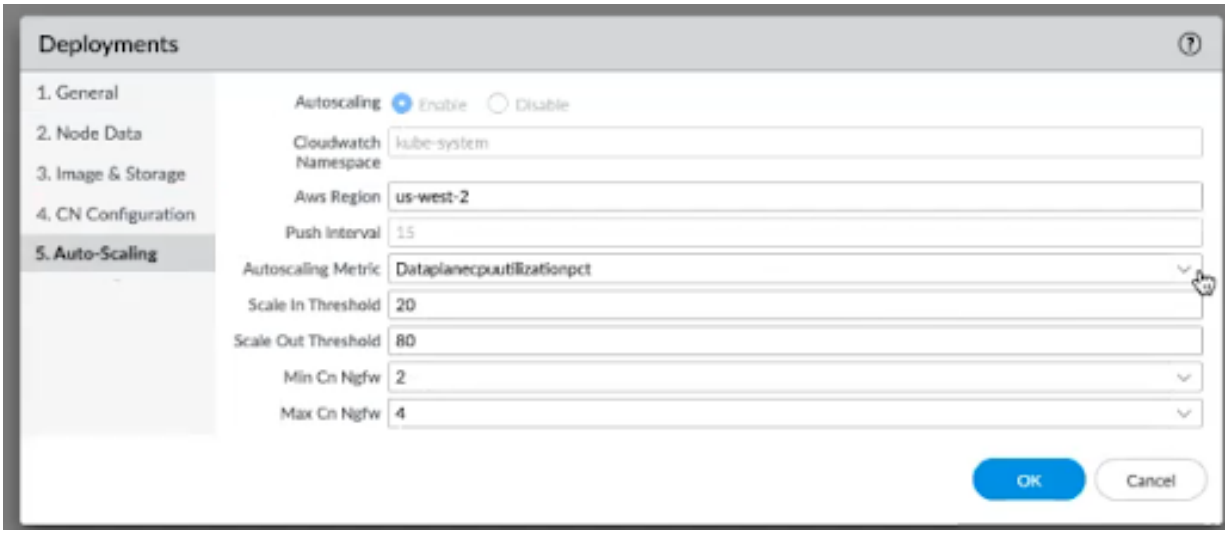
- 只有具有 *EKS Kubernetes 1.22* 版的 *EKS* 環境上才支援自動調整。其他 *Kubernetes* 系統的 *[Auto-Scaling*（自動調整）*]* 頁籤會變成灰色。
- 您將需要部署 在 EKS 環境中使用 KEDA 的自訂指標型 HPA，自動調整才能運作。

STEP 1 | 在 **Autoscaling**（自動調整）區段中，輸入 **Autoscaling Metric**（自動調整指標）、**Scale In Threshold**（相應縮小閾值）和 **Scale Out Threshold**（相應放大閾值）。

STEP 2 | 按一下 **OK**（確定），以提交部署。

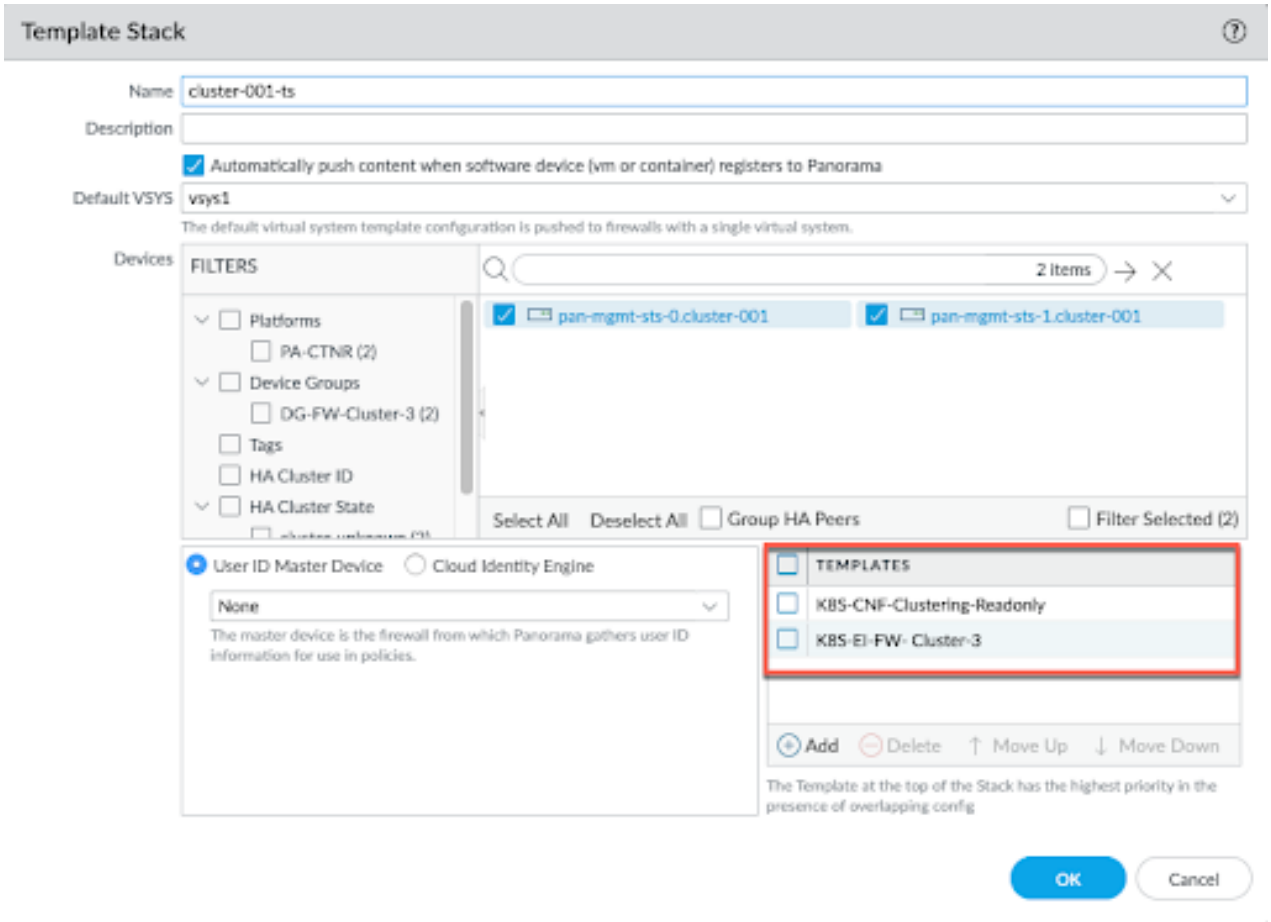
以下是自動調整所支援的指標。

- `dataplanecpuutilizationpct`
- `dataplanepacketbufferutilization`
- `pansessionactive`
- `pansessionutilization`
- `pansessionsslproxyutilization`
- `panthroughput`
- `panpacketrate`
- `panconnectionspersecond`



在您輸入所有設定詳細資料之後，[Deployments（部署）] 頁籤會顯示所儲存的單一部署的詳細資料。按一下 **Commit**（提交），以繼續部署。提交完成之後，外掛程式會顯示 [Deploy（部署）] 按鈕。按一下 **Deploy**（部署）按鈕，以部署 CN-Series HSF。

在 CN-Series HSF 部署之後，叢集會使用 K8S-CNF-Clustering-Readonly 範本以及您在準備 Panorama 以進行 CN-Series HSF 部署 步驟 6 中所建立的變數範本來建立範本堆疊 `<cluster-name>-ts`。



您在 HSF 部署設定期間所參考的裝置群組（在準備 Panorama 以進行 CN-Series HSF 部署 的步驟 5 中所建立) 以及在 HSF 部署之後所自動建立的範本堆疊會啟動至 CN-MGMT Pod。CN-MGMT Pod 連線至 Panorama 時，裝置群組和範本堆疊會自動與 HSF 名稱相關聯。

CN-DB、CN-GW 和 CN-NGFW Pod 的 HSF 資訊會在它們作用時自動予以填入。這些 Pod 都啟動並執行時，CN-MGMT Pod 會將 CI IP 位址、Pod 詳細資料、裝置 ID 和軟體版本這類詳細資料傳送至 Panorama。

針對 Panorama 高可用性 (HA)，CN-MGMT Pod 會將更新傳送至主動和被動 Panorama。

不同的部署狀態

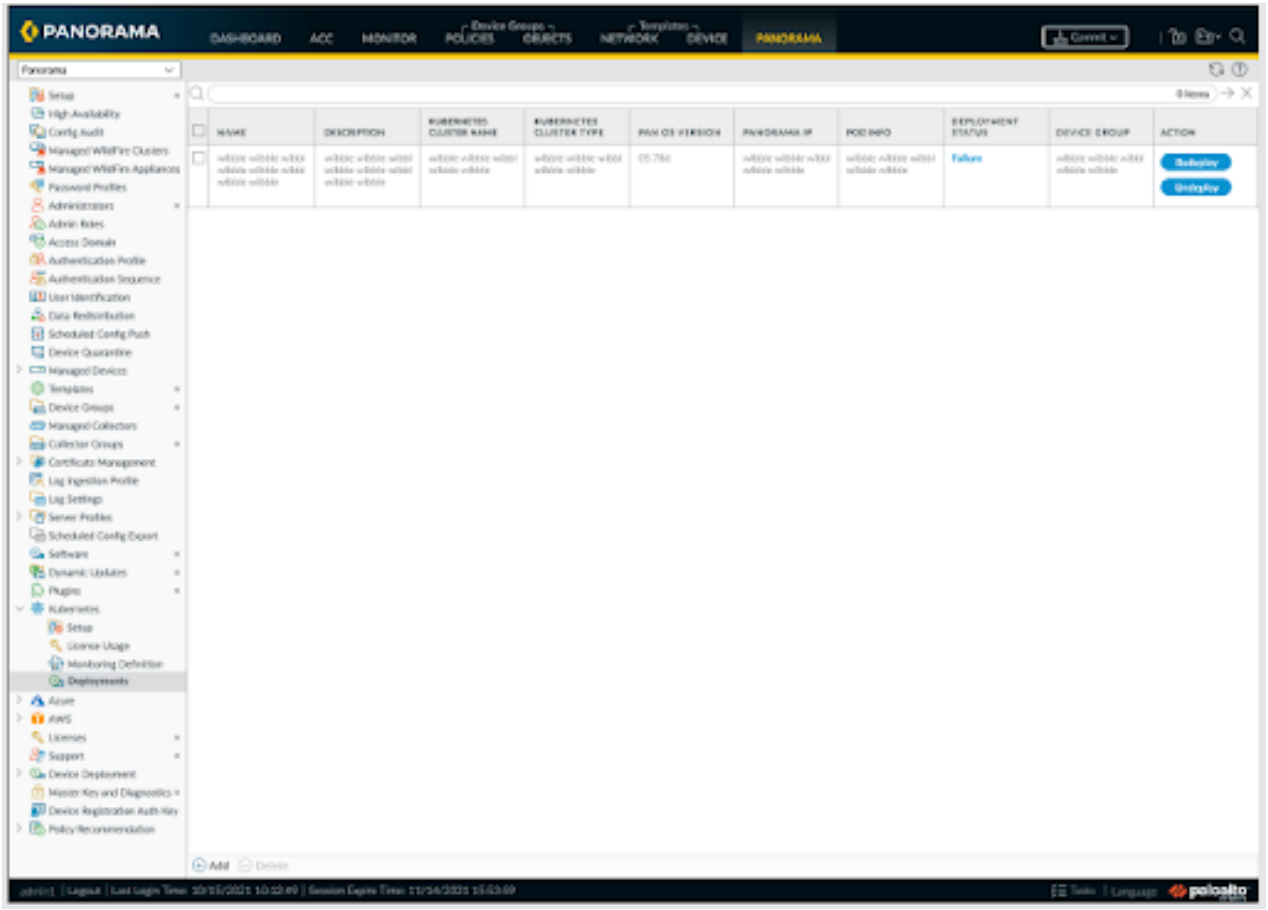
我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

在您輸入所有設定詳細資料之後，[Deployments（部署）] 頁籤會顯示所儲存的單一部署的詳細資料。部署有 5 個階段：

1. 需要提交
2. 未部署
3. 正在部署
4. 警告
5. 成功/失敗

1. 按一下 **Commit**（提交），以繼續部署。您可能會注意到已停用 [Deploy（部署）] 按鈕，而且部署狀態在您按一下 [Commit（提交）] 之後變更為 **Not Deployed**（未部署）。在提交完成之後，啟用 [Deploy（部署）] 按鈕。
2. 按一下 [Deploy（部署）]，以繼續部署 CN-Series CNF。部署狀態變更為 [Deploying（正在部署）]。在此階段期間，會建立 Panorama 設定，並產生 CN-GW，而且外掛程式會開始進行 api 呼叫以部署 CN-Series HSF。
3. [Deploying（正在設定）] 狀態接著會根據資源可用性和設定詳細資料而變更為 **Warning**（警告）、**Success**（成功）或 **Failure**（失敗）。然後啟用 [Redeploy（重新部署）] 和 [Undeploy（取消部署）] 按鈕。
4. 按一下 [Redeploy（重新部署）] 以變更已啟用的參數，並在按一下 [Redeploy（重新部署）] 之前提交變更。
5. 按一下 **Undeploy**（取消部署），以刪除建立為此部署一部分的所有 CN-Series HSF Pod。

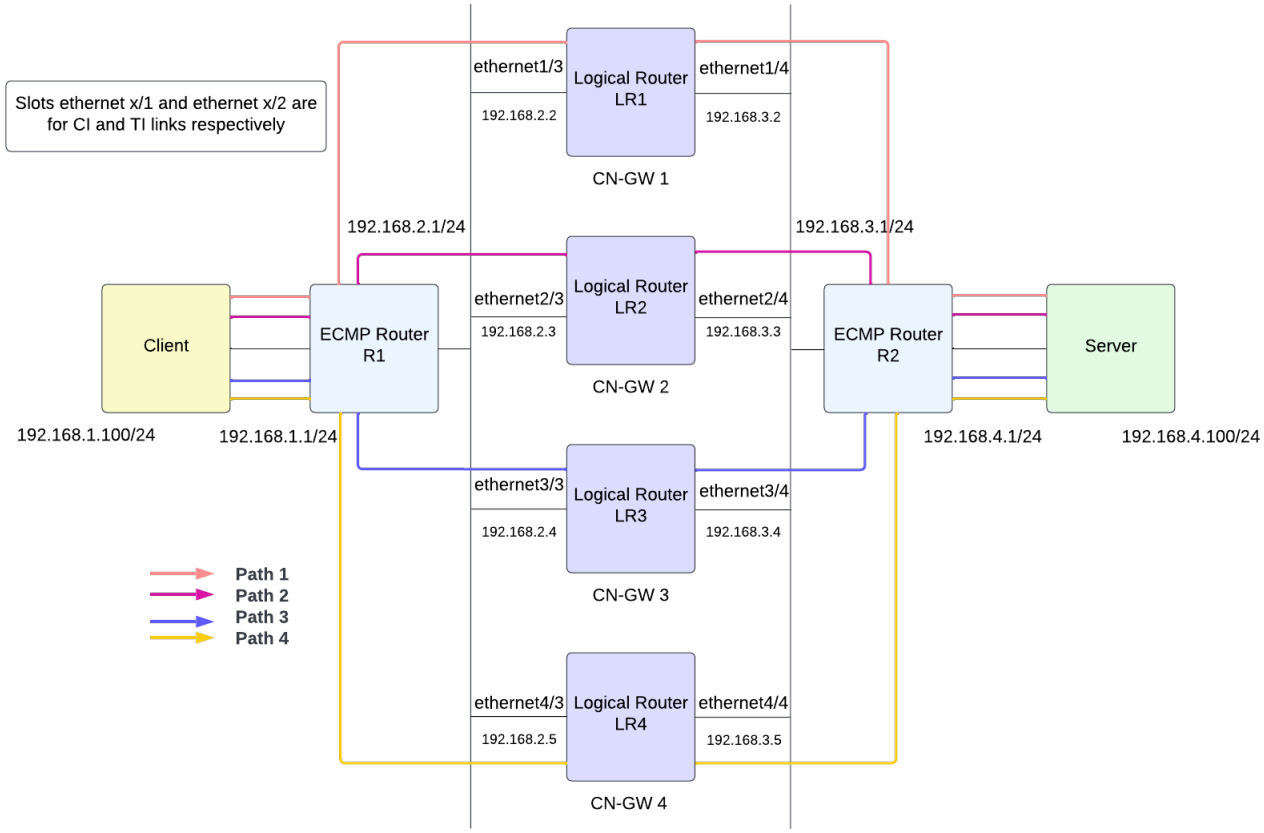
刪除所有 *CN-Series HSF Pod* 之後，仍然會保留所有 *Panorama* 設定。



設定流向 CN-Series HSF 的流量

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

上流/下游路由器使用流量型 ECMP 演算法。流量到達 CN-GW 時，會使用對稱雜湊演算法，以透過流量互連 (TI) 連結，將流量分發到其中一個可用的 CN-NGFW。雙向（用戶端到伺服器和伺服器到用戶端）符合工作階段的流量一律會經過相同的 CN-NGFW。CN-NGFW 處理流量之後，而且如果您將政策設定為 **Allow**（允許）流量，則會將流量封包送回 CN-GW 以到達伺服器。



STEP 1 | 在防火牆上建立邏輯路由器，以參與第三層路由。

1. 移至 **Network**（網路） > **Routing**（路由） > **Logical Router**（邏輯路由器），然後從 **Template**（範本）下拉式清單中選取變數範本。
2. 選取預設虛擬路由器，或針對新邏輯路由器新增 **Name**（名稱）。
3. 選取 **General**（一般），然後新增已定義的 **Interface**（介面）。

   重複此步驟，以新增所有您想要新增至邏輯路由器的介面。

   ethernetX/1 和 *ethernetX/#* 介面分別保留給 *CI* 和 *TI* 連結。選取 ***ethernet1/3*** 與 ***ethernet1/14*** 之間的介面。
4. 按一下 **OK**（確定）。
5. 設定靜態路由的管理距離。範圍為 10 至 240；預設值為 10。

   為網路所需的路由類型設定管理距離。虛擬路由器有兩個以上的不同路由通向相同目的地時，將會利用管理距離從不同路由通訊協定和靜態路由中選取最佳路徑，優先選擇距離更短的路由。
6. 啟用 ECMP 以利用多個等價路徑進行轉送。
7. 按一下 **OK**（確定）。

STEP 2 | 設定第三層介面以啟用流量。

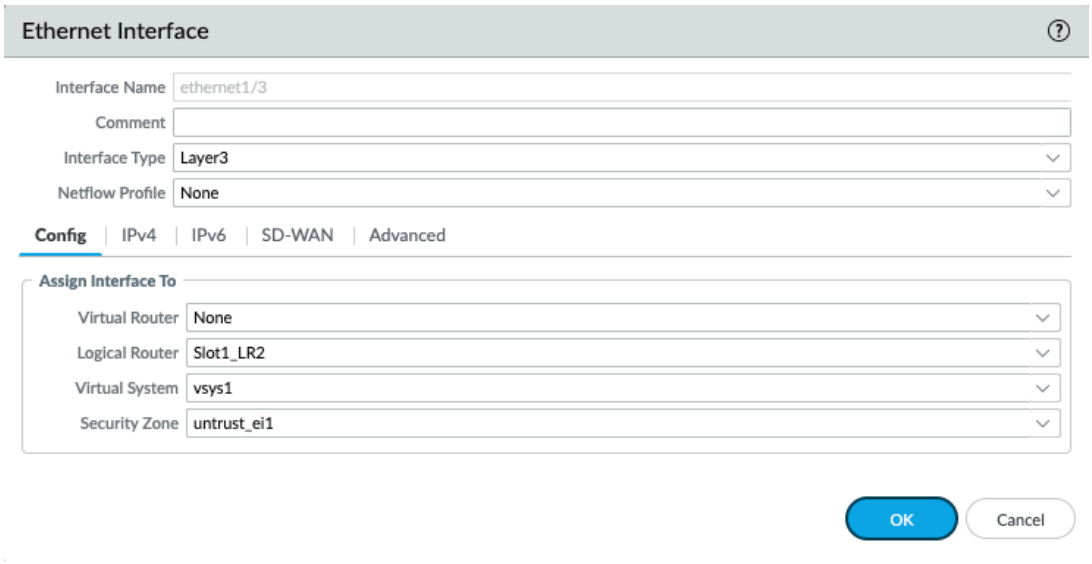
當您準備 Panorama 以進行 CN-Series HSF 部署時，可能已建立變數範本。若要啟用透過叢集網路的流量，您必須使用 CN-Series HSF 負載平衡所需的必要網路和流量設定來設定變數範本。

您必須使用 IPv4 位址來設定第三層乙太網路介面，以讓防火牆可以在這些介面上執行路由。您一般要使用下列程序設定用於連線網際網路的外部介面和用於連線內部網路的介面。

您可以在部署 *CN-Series HSF* 之前或之後設定此範本。

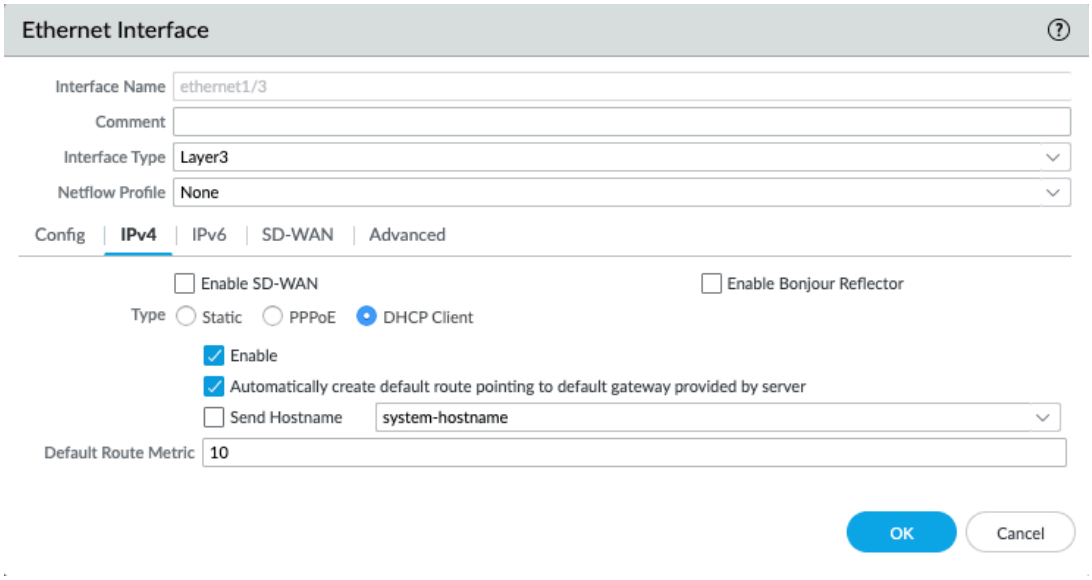
請不要將此範本的設定與 *Kubernetes* 外掛程式安裝期間自動建立的 ***K8S-CNF-Clustering-Readonly*** 範本重疊。

1. 移至 **Network**（網路） > **Interfaces**（介面），然後從 **Template**（範本）下拉式清單中選取變數範本。
2. 選取 **Ethernet**（乙太網路）介面，以 **Add Interface**（新增介面）。
3. 選取介於 1 與 30 之間的 **Slot**（插槽）。
4. 輸入 **`ethernet1/3`** 與 **`ethernet1/14`** 之間的 **Interface Name**（介面名稱）。
5. 針對 **Interface Type**（介面類型），選取 **Layer 3**（第三層）。
6. 在 **Config**（設定）頁籤上：
   - 針對 **Logical Router**（邏輯路由器），選取您在步驟 1 中設定的邏輯路由器。
   - 對於 **Virtual System**（虛擬系統），選取您要設定的虛擬系統（如果是多虛擬系統防火牆）。
   - 對於 **Security Zone**（安全性區域），選取介面所屬的區域或建立 **New Zone**（新區域）。



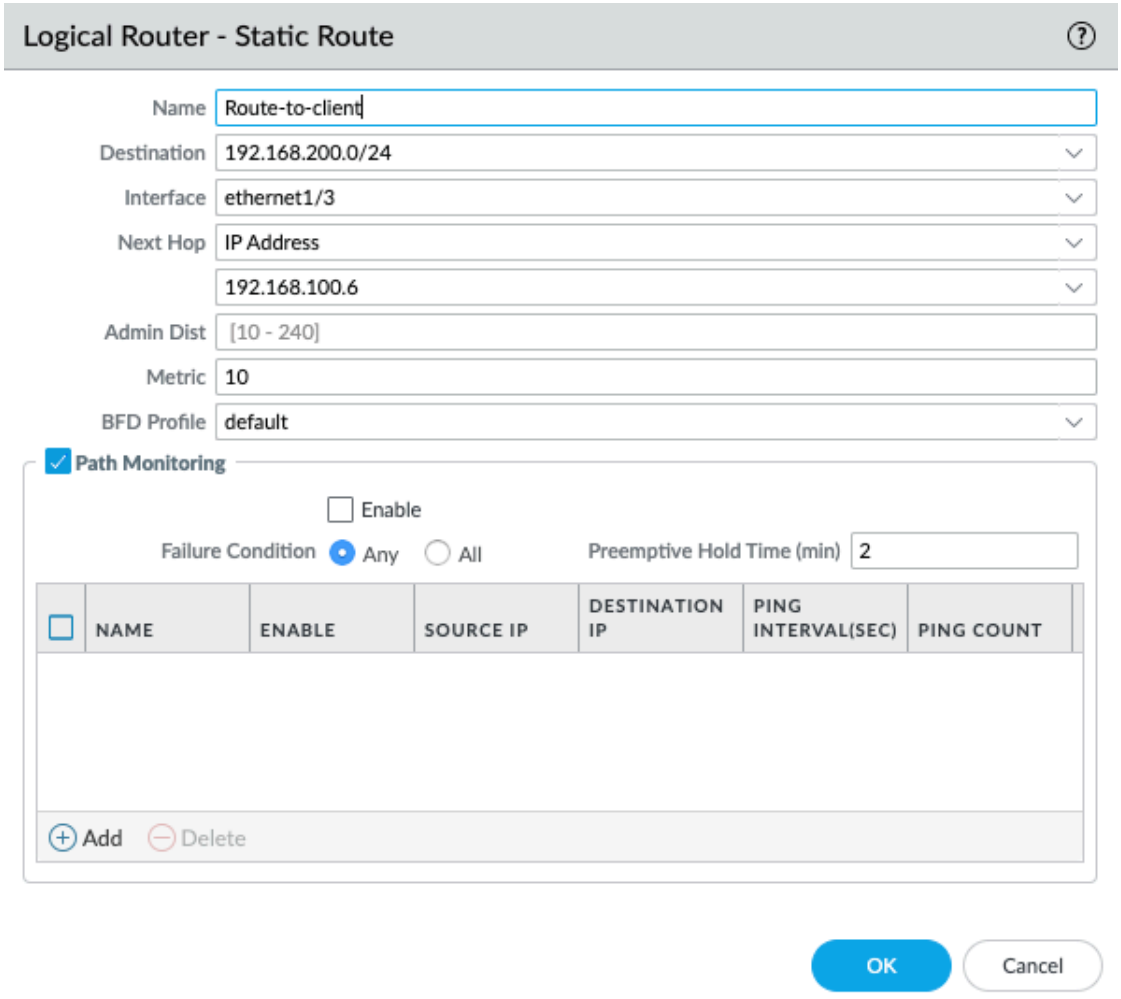
7. 在 **IPv4** 頁籤上，選取 **DHCP Client**（**DHCP** 用戶端）。

   防火牆介面用作 DHCP 用戶端，接收動態指定的 IP 位址。防火牆也能夠將 DHCP 用戶端介面所接收的設定傳播到防火牆上運作的 DHCP 伺服器。如需詳細資訊，請參閱將介面設定為 DHCP 用戶端。
8. 按一下 **OK**（確定）。



STEP 3 | 設定邏輯路由器的靜態路由。

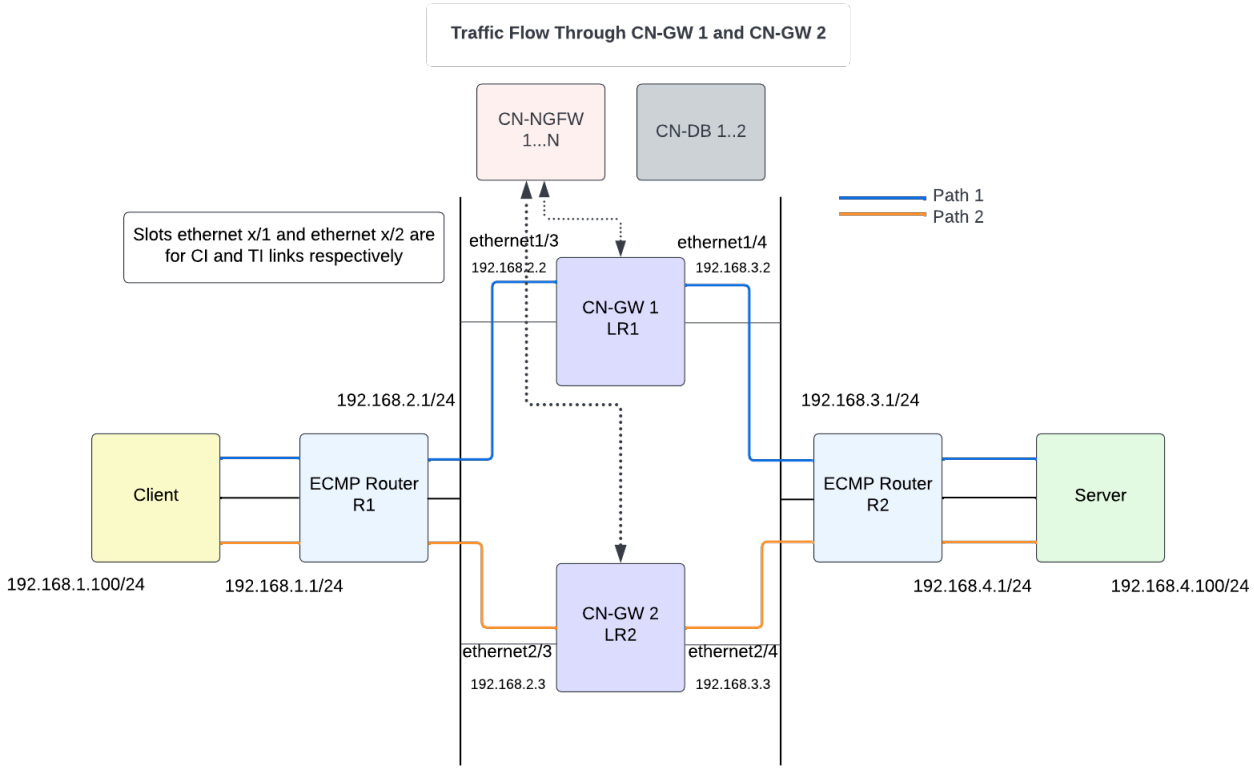
1. 移至 **Network**（網路） > **Routing**（路由） > **Logical Router**（邏輯路由器），然後從 **Template**（範本）下拉式清單中選取變數範本。
2. 選取 **Static**（靜態） > **IPv4** 頁籤，然後按一下 **Add**（新增）。
3. 輸入靜態路由的 **Name**（名稱）。
4. 輸入 **Destination**（目的地）路由和網路遮罩。例如，192.168.200.0/24。
5. 選取封包用於進入下一個躍點的傳出介面。
6. 針對 **Next Hop**（下一個躍點），選取 **ip-address**，然後輸入內部閘道的 IP 位址。例如，192.168.100.2。
7. 輸入路由的 **Admin Distance**（管理距離），以覆寫為此虛擬路由器的靜態路由所設定的預設管理距離（範圍為 10 到 240；預設值為 10）。
8. 輸入路由的 **Metric**（公制）（範圍為 1 至 65535）。
9. 將 **BFD Profile**（**BFD** 設定檔）套用至靜態路由，因此，在靜態路由失敗時，防火牆會移除路由，並使用替代路由。預設值為 **None**（無）。
10. 按一下 **OK**（確定）。



測試案例：第三層 BFD 型 CN-GW 失敗處理

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

此測試會評估處理 CN-GW 失敗所需的 BFD 設定。BFD 設定檔可處理上游/下游路由器上的 CN-GW 失敗。



對稱流量

- 如果進入流量介面是 CN-GW 1，則尋找輸出介面的路由查閱位於 LR1 上。
  - 路由 1：目的地：用戶端子網路；下一個躍點：R1
  - 路由 2：目的地：伺服器子網路；下一個躍點：LR2
- 如果進入流量介面是 CN-GW 2，則尋找輸出介面的路由查閱位於 LR2 上。
  - 路由 1：目的地：用戶端子網路；下一個躍點：R1
  - 路由 2：目的地：伺服器子網路；下一個躍點：R2

非對稱流量

CN-Series HSF 也支援非對稱流量。例如，流經 CN-GW 1 的用戶端到伺服器流量比對工作階段 1，以及流經 CN-GW 2 的伺服器到用戶端流量比對工作階段 1。針對非對稱流量，所有面向 R1 的介面都必須位於相同的區域。同樣地，所有面對 R2 的介面都必須位於相同的區域。

LR 間路由

例如，如果進入流量介面是 CN-GW 1，則尋找輸出介面的路由查閱位於 LR1 上。如果具有路由可到達下一個躍點作為 LR2 的伺服器，則 CN-NGFW 會將流量傳送至 LR2。根據 CN-GW 2 LR2 路由查閱，會將封包傳送至伺服器。

STEP 1 | 移至 **Network**（網路） > **Routing**（路由） > **Routing Profiles**（路由設定檔） > **BFD**，然後從 **Template**（範本）下拉式清單中選取變數範本。

您必須在外部路由器和邏輯路由器上啟用 BFD。

STEP 2 | 按一下 **Add**（新增），以針對 BFD 設定檔新增。

STEP 3 | 輸入 **Name**（名稱）。

STEP 4 | 選擇 BFD 的運作 **Mode**（模式）：

- 主動—BFD 啟動向對等體傳送控制封包（預設）。至少其中一個 BFD 對等體必須為主動；可都為主動。
- 被動—BFD 等候對等體傳送控制封包並視需回應。

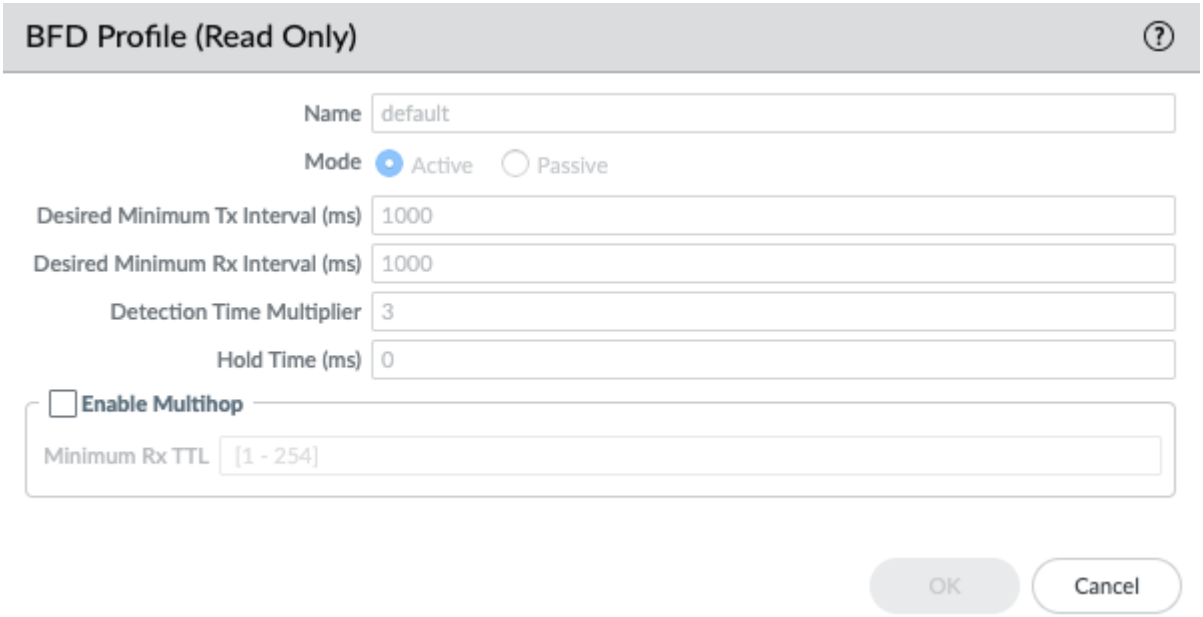
STEP 5 | 輸入 **Desired Minimum Tx Interval (ms)**（所需最小 **Tx** 間隔（毫秒））。這是您希望 BFD 通訊協定（稱為 BFD）傳送 BFD 控制封包的最小間隔（以毫秒計）；您因此會與對等體交涉傳輸間隔。

STEP 6 | 輸入 **Detection Time Multiplier**（偵測時間乘數）。本機系統將從遠端系統接收到的 **Detection Time Multiplier**（偵測時間乘數）乘以遠端系統允許的傳輸間隔（**Required Minimum Rx Interval**（要求最小傳送間）以及最後接收到的**Desired Minimum Tx Interval**（所需最小傳送間隔）取其大）來計算偵測時間。如果偵測時間到期之前 BFD 未從其對等體收到 BFD 控制封包，則會發生故障。範圍是 2 到 50；預設值為 3。

STEP 7 | 輸入 **Hold Time (ms)**（保留時間（毫秒））。此為 BFD 傳輸 BFD 控制封包之前連結啟動後的延遲時間（毫秒）。**Hold Time**（保留時間）僅適用於 BFD 主動模式。如果 BFD 在 **Hold Time**（保留時間）期間接收 BFD 控制封包，則會略過它們。範圍為 0-120000；預設值為 0。

STEP 8 | 選取 **Multihop**（多重躍點）以透過 BGP 多重躍點啟用 BFD。輸入 **Minimum Rx TTL**（最小 **Rx TTL**）。此為 BGP 支援多重躍點 BFD 時 BFD 將在 BFD 控制封包中接受（接收）的最小存留值（躍點數）。（範圍為 1-254；無預設）。

STEP 9 | 按一下 **OK**（確定）以儲存 BFD 設定檔。



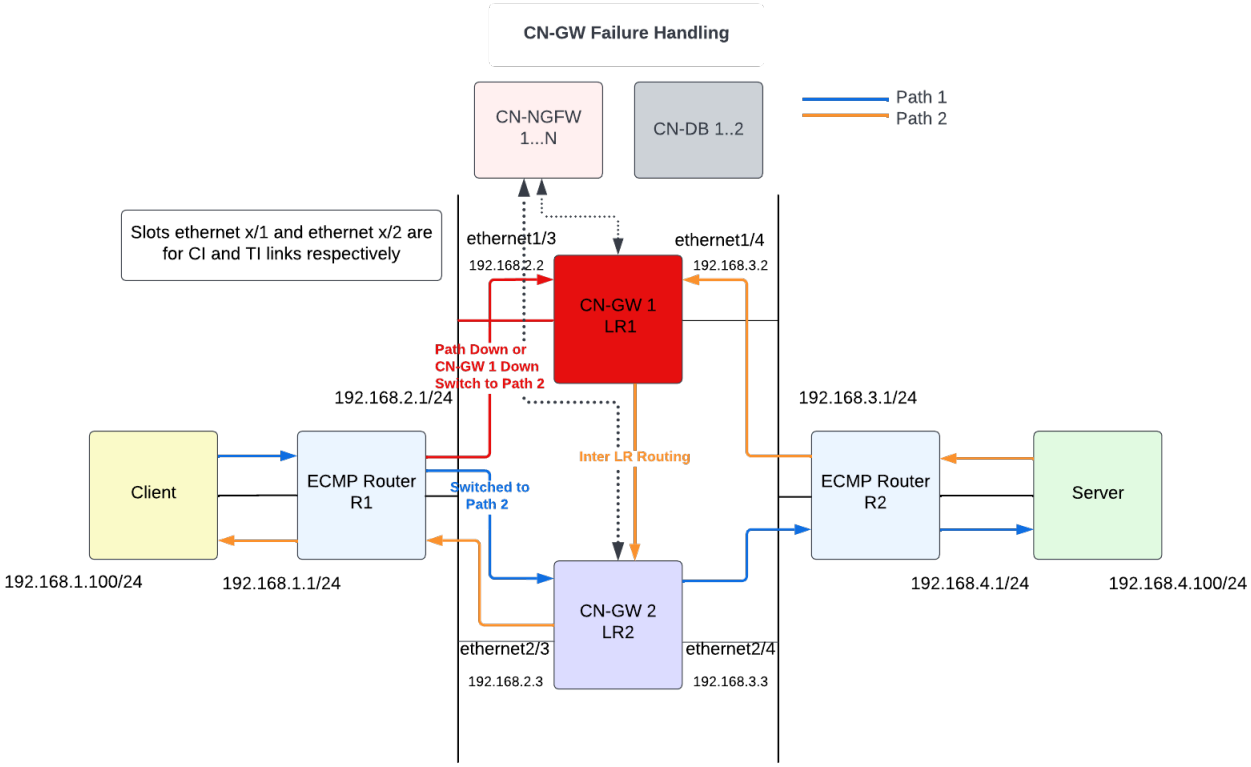
STEP 10 | 設定邏輯路由器的靜態路由。

1. 移至 **Network**（網路） > **Routing**（路由） > **Logical Router**（邏輯路由器），然後從 **Template**（範本）下拉式清單中選取變數範本。
2. 選取 **Static**（靜態） > **IPv4** 頁籤，然後按一下 **Add**（新增）。
3. 輸入靜態路由的 **Name**（名稱）。
4. 輸入 **Destination**（目的地）路由和網路遮罩。例如，192.168.200.0/24。
5. 選取封包用於進入下一個躍點的傳出介面。
6. 針對 **Next Hop**（下一個躍點），選取 **ip-address**，然後輸入內部閘道的 IP 位址。例如，192.168.100.2。
7. 輸入路由的 **Admin Distance**（管理距離），以覆寫為此虛擬路由器的靜態路由所設定的預設管理距離（範圍為 10 到 240；預設值為 10）。
8. 輸入路由的 **Metric**（公制）（範圍為 1 至 65535）。
9. 將先前步驟中所建立的 **BFD Profile**（**BFD** 設定檔）套用至靜態路由，因此，在靜態路由失敗時，防火牆會移除路由，並使用替代路由。
10. 按一下 **OK**（確定）。

BFD 設定可處理 CN-GW 和路徑失敗。在下列流量圖中，請考慮用戶端與伺服器之間的兩個 SSH 工作階段。工作階段 1 流經路徑 1，而工作階段 2 流經路徑 2。如果關閉 CN-GW 1 或路徑 1，則 R1 與 CN-GW 1、R2 與 CN-GW 1 之間的 BFD 設定可協助 R1 識別路徑失敗，並透過路徑 2 傳送流量。所有面對 R1 的介面都必須位於相同的區域。同樣地，面對 R2 的介面必須位於相同的區域。

路由 1：目的地：用戶端子網路；下一個躍點為 R1，指標 10

路由 2：目的地：伺服器子網路；下一個躍點為 LR2，指標 11

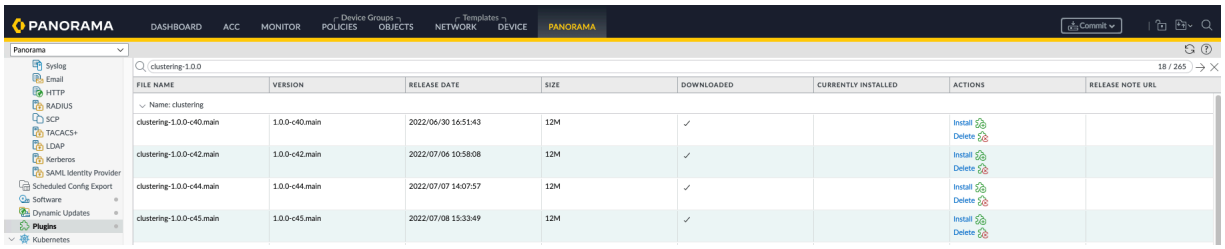


檢視 CN-Series HSF 摘要和監控

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

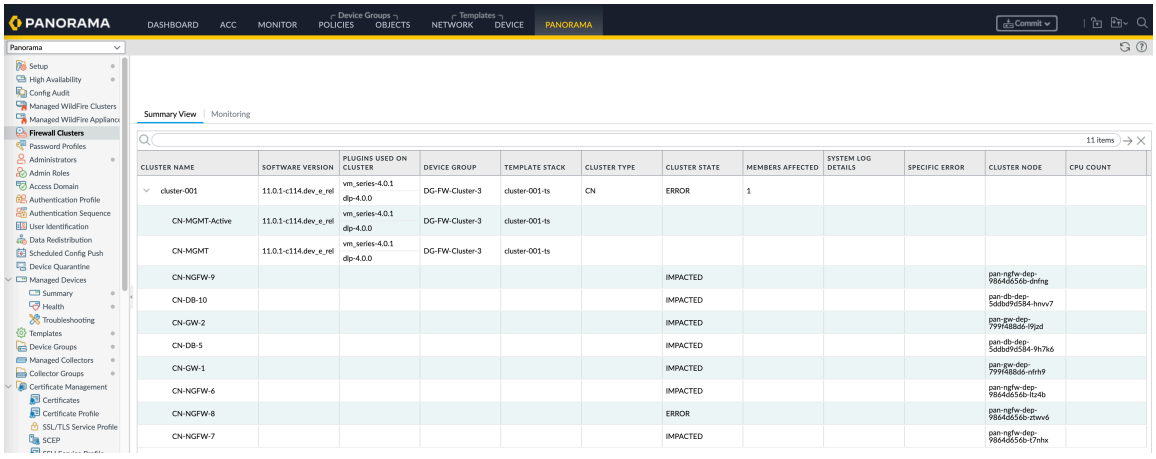
您可以在 Panorama 網頁介面的 **Firewall Clusters**（防火牆叢集）頁籤下方檢視 CN-Series HSF 的摘要和監控資訊。若要檢視和存取防火牆叢集，您必須從 **Panorama** > **Admin Roles**（管理員角色）> **Web UI** 清單中 **Enable**（啟用） > **Firewall Clusters**（防火牆叢集）。如需詳細資訊，請參閱設定管理員角色設定檔。

您必須從 **Panorama** > **Plugins**（外掛程式）中安裝 Clustering 1.0.0 外掛程式，才能在 **Firewall Clusters**（防火牆叢集）下方檢視叢集詳細資料。



摘要檢視

檢視防火牆在最後五分鐘所擷取 CN-Series 叢集的相關資訊。按一下重新整理按鈕，以載入最新的詳細資料。

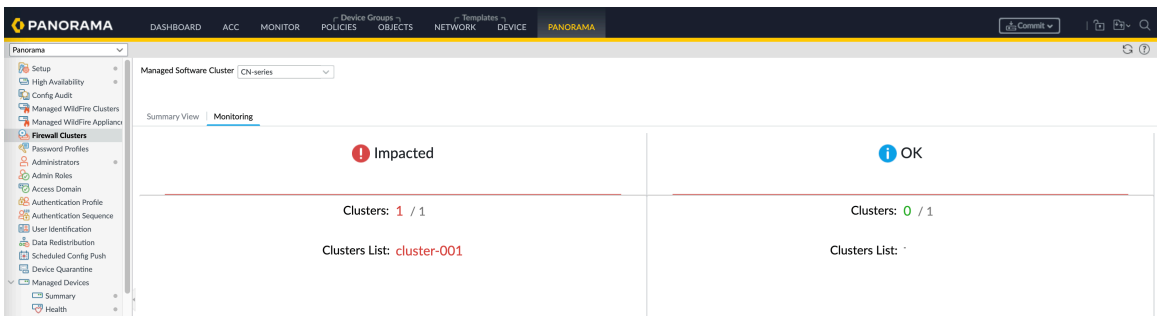


欄位	說明
叢集名稱	防火牆叢集的名稱。

欄位	說明
軟體版本	PAN-OS 版本。
叢集上所使用的外掛程式	叢集上所使用的外掛程式清單。 僅支援 *CN-Series* 防火牆外掛程式。
範本堆疊	與叢集相關聯的範本堆疊名稱。
裝置群組	與叢集相關聯的裝置群組名稱。
Cluster State 叢集狀態	顯示叢集是否受到影響。
叢集類型	叢集的類型。 僅支援 *CN-Series* 防火牆叢集類型。
受影響的成員	受影響的叢集成員數目和其名稱。
系統日誌詳細資料	顯示系統事件的詳細資料。
特定錯誤	叢集中的特定錯誤清單。按一下連結，以在 **Monitor**（監控） > **Logs**（日誌） > **System**（系統）下方檢視錯誤的更多詳細資料，而您可以在其中檢視日誌。
叢集節點	Pod 的名稱。
CPU 計數	使用的 CPU 數目。

監控

檢視 CN-Series 防火牆叢集健康資訊。



欄位	說明
受管理的軟體叢集	選取防火牆叢集。 僅支援 *CN-Series* 防火牆叢集類型。
受影響	受影響的防火牆叢集清單。 • **CN-Clusters** — 受影響的 CN-Series 防火牆叢集數目。 • **Clusters Impacted**（受影響的叢集）— 顯示受影響的叢集清單。 按一下以在 **Interconnect Status**（互連狀態）和 **Cluster Utilization**（叢集使用率）儀表板中檢視叢集的詳細資訊。
OK	未受影響的防火牆叢集清單。 • **Clusters**（叢集）—未受影響的 CN-Series 防火牆叢集數目。 • **Clusters List**（叢集清單）—顯示未受影響的叢集清單。 按一下以在 **Interconnect Status**（互連狀態）和 **Cluster Utilization**（叢集使用率）儀表板中檢視叢集的詳細資訊。

互連狀態	檢視所選取時間範圍的叢集互連詳細資料。
	選取 **Last 5 Mins**（最後 **5** 分鐘），以檢視下列詳細資料。
	• **Cluster Name**（叢集名稱）— 防火牆叢集的名稱。
	• **Cluster Type**（叢集類型）— 叢集的類型。
	僅支援 *CN-Series* 防火牆叢集類型。
	• **Cluster Creation Time**（叢集建立時間）— 叢集建立時間。
	• **Current Cluster State**（目前叢集狀態）—顯示叢集是否受到影響。
	  • **Current Cluster Detail**（目前叢集詳細資料）—按一下目前叢集狀態連結，以檢視受影響叢集的更多詳細資料。
	• **Cluster Interconnect Status**（叢集互連狀態）—顯示叢集互連。
	  • **Current Cluster Detail**（目前叢集詳細資料）—按一下目前互連狀態連結，以檢視受影響叢集的更多詳細資料。
	• **Traffic Interconnect**（流量互連）—流量互連的狀態。
	• **External Connection**（外部連線）— 外部連線的狀態。
	• **Impacted Links**（受影響的連結）— 受影響連結的數目。
	• **Management Connectivity**（管理連線）— 管理連線的數目。

欄位	說明
	• **Impacted Cluster Member**（受影響的叢集成員）— 受影響的叢集成員清單。 • **Time Stamp Hi-Res Uptime**（時間戳記高解析度執行時間）— 執行時間時間戳記。 • **Time Stamp Hi-Res Downtime**（時間戳記高解析度停機）— 停機時間時間戳記。 選取任何其他時間範圍只會顯示下列資訊。 • 叢集名稱 • 叢集類型 • 叢集建立時間 • 目前叢集狀態 • 叢集互連狀態 • 流量互連 • 外部連線

叢集使用率	檢視整個防火牆叢集、記憶體和資料使用率。
	• **Cluster Name**（叢集名稱）—防火牆叢集的名稱。展開 [Cluster Name（叢集名稱）] 會顯示該叢集中所有 Pod 的詳細資料。
	  • **Cluster Details**（叢集詳細資料）—按一下叢集名稱連結，以檢視所選取叢集的吞吐量、記憶體和資料使用率詳細資料。
	• **Cluster Type**（叢集類型）—叢集的類型。
	  僅支援 *CN-Series* 防火牆叢集類型。
	• **Cluster State**（叢集狀態）— 顯示叢集的健康情況。
	• **Cluster Throughput (gbps)**（叢集輸送量 **(gbps)**）— 防火牆叢集輸送量 (Gbps)。
	• **CPS**— 每秒連線數。
	• **Session Count (Sessions)**（工作階段計數（工作階段數））— 工作階段數目。
	• **Average Data Plane (%) Within Health Threshold**（健康閾值內的平均資料平面 **(%)**）— 以百分比表示的平均資料平面閾值。
	• **Management Plane CPU (%)**（管理平面 **CPU (%)**）— 管理平面 CPU 使用率（百分比）。

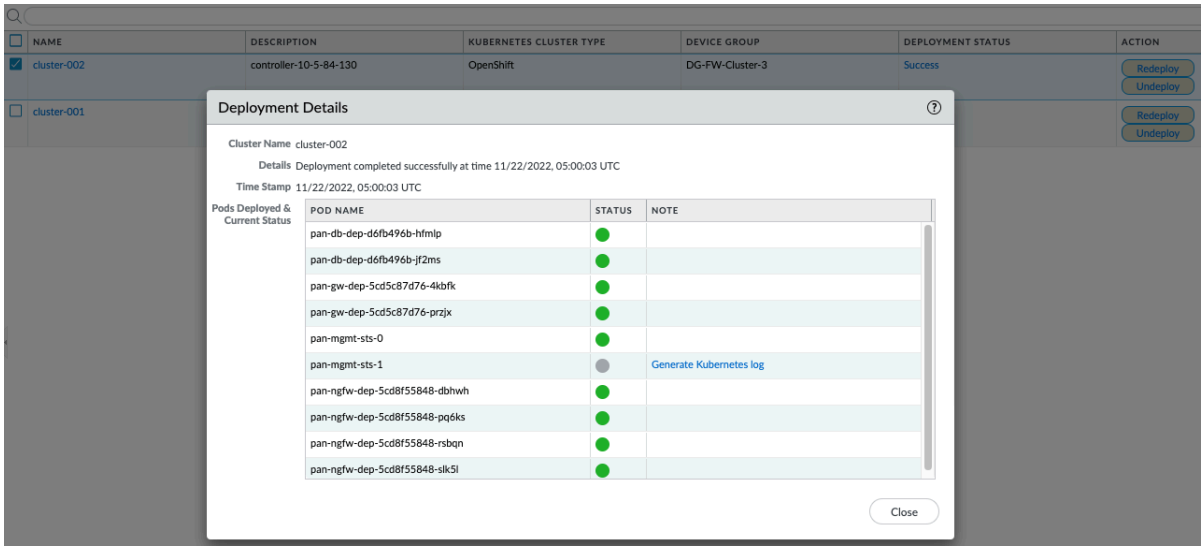
欄位	說明
	• **Management Plane Mem (%)**（管理平面記憶體 **(%)**）— 管理平面記憶體使用（百分比）。 • **Logging Rate (Log/Sec)**（記錄速率（日誌/秒））— 在叢集上產生日誌的速率。 • **DP Auto-Scale Status**（**DP** 自動調整狀態）— 資料平面自動調整詳細資料。

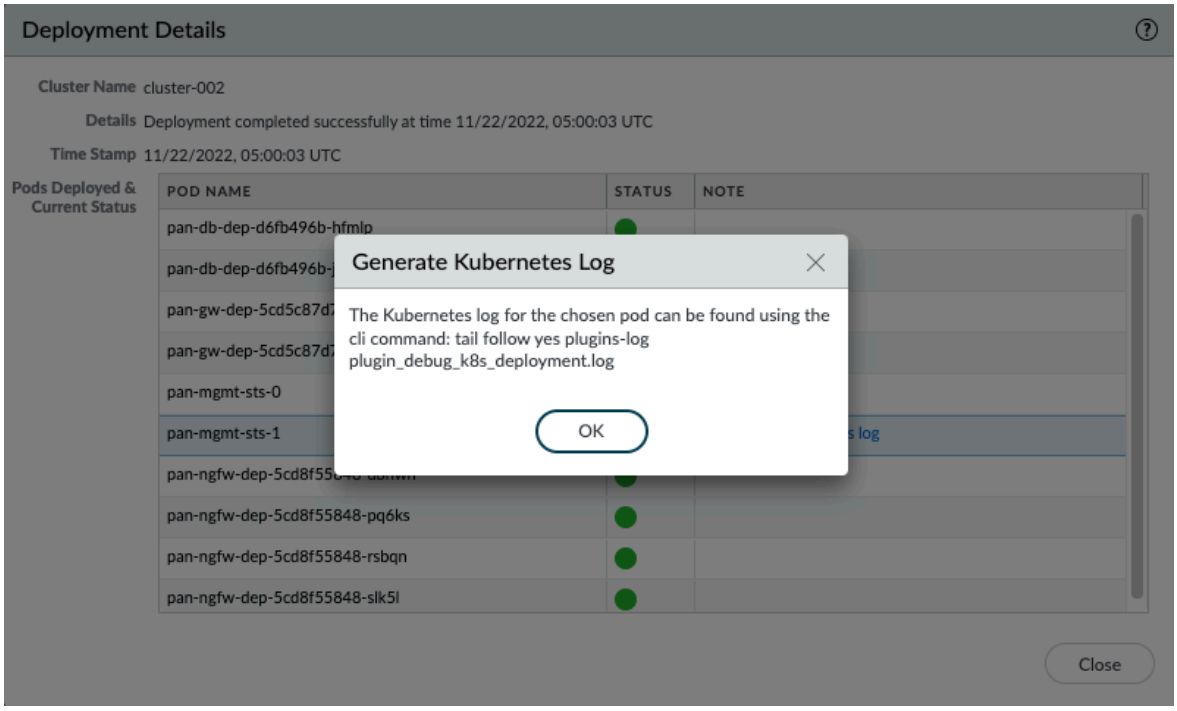
驗證 CN-Series HSF 部署

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

您可以在 **Panorama** > **Kubernetes** 下方的 **Deployment**（部署） 區段中驗證 CN-Series HSF 部署。按一下 **Deployment Status**（部署狀態）下方的連結，以檢視部署的詳細資料。

已部署的 Pod 和其目前狀態會透過顏色編碼，並顯示在 **Deployment Status**（部署狀態）區段中。您可以按一下失敗 Pod 部署的 **Note**（注意）下方的連結，以檢視更多詳細資料。





在 Panorama CLI 中使用下列命令，以產生日誌。

```
debug plugins kubernetes generate-pod-log deployment_name pod_name
 <value> Name of the pod
```

```
show plugins kubernetes deployment-status
```

```
show plugins kubernetes deployment-details name
```

偵錯 **Kubernetes** 外掛程式與 **CN-Series HSF** 之間的同步問題

Kubernetes 外掛程式會使用 Watch API 以從 Pod、服務和節點收集 CN-Series HSF 的相關資訊。Watch API 是一種通知型 API，可在叢集狀態變更時傳送更新。為了確保外掛程式與已部署的 CN-Series HSF 同步，外掛程式會接聽通知，並顯示 HPA 和升級/降級事件通知。

外掛程式會使用下列偵錯命令，以根據外掛程式狀態來偵錯特定節點。

```
debug plugin kubernetes kubectl-logs pod <pod-name>
```

此偵錯命令會產生日誌檔，而這個日誌檔會包含命令中所傳遞節點的 `kubectl` 說明日誌，並儲存至外掛程式日誌檔。

在 EKS 環境中使用 KEDA 的自訂指標型 HPA

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

EKS 環境中的 HPA 實作需要您使用 KEDA（Kubernetes 型事件驅動自動調整規模器）。下列是自訂指標型 HPA 實作的先決條件：

- 針對來自 YAML 的叢集，啟用 HPA。
  - 確定 HPA 參數已填入 pan-cn-mgmt-configmap.yaml 檔案中。
  - 確定 `PAN_NAMESPACE_EKS` 欄位在您區域的 AWS 帳戶中具有唯一名稱。這避免覆寫來自具有相同 EKS 命名空間的不同 CN 叢集的指標。
- CN-MGMT 將指標發佈至 Cloudwatch。

  CN-MGMT Pod 需要必要的權限才能存取 Cloudwatch 資源、收集 CN-NGFW 指標，以及將自訂指標發佈至 Cloudwatch。作法是將 `CloudWatchFullAccess` 政策新增至您在建立 nodegroup 時所指定的節點 IAM 角色。
- 從 AWS 中，部署叢集自動調整規模器。如需詳細資訊，請參閱叢集自動調整規模器。

使用 AWS 來驗證 KEDA

若要驗證 KEDA，您可以將 keda 服務帳戶中的 role-arn 加上註釋，以將 IAM 角色與 keda 操作員服務帳戶相關聯。建議執行此步驟，因為這會避免新增節點 IAM 角色的 Cloudwatch 存取，而且只會讓 keda 服務帳戶存取 Cloudwatch，而不是執行 keda 的整個節點。

將 IAM 角色與 keda 操作員服務帳戶相關聯：

1. 建立叢集的 IAM OIDC 提供者 - 您只需要建立叢集的 IAM OIDC 提供者一次。
2. 使用您服務帳戶所需的權限，以建立 IAM 角色並連接其 IAM 政策。確定您在執行此步驟時提供 Cloudwatch 存取政策。
3. 將 IAM 角色與服務帳戶相關聯 – 針對需要存取 AWS 資源的每個 Kubernetes 服務帳戶，完成此工作。
4. 從 AWS 中，部署叢集自動調整規模器。如需詳細資訊，請參閱叢集自動調整規模器。

部署 KEDA Pod

若要部署 Keda #od，請下載最新的 keda 檔案。

```
kubectl apply -f keda-2.7.1.yaml
```

外掛程式會根據您依據調整需求所提供的輸入來修改和套用 yaml。

觀察 Cloudwatch 主控台中的值，然後檢查目標 Pod 如何相應縮小和相應放大。

在 CN 系列 HSF 中設定動態路由

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• Panorama 使用最低 PAN-OS 11.1 版本執行

CN 系列超大規模安全架構 **(HSF)** 現在引入了透過 BGP 和透過 BFD 的 BGP 通訊協定的動態路由。使用動態路由，您可以透過可跨邏輯路由器所使用的設定檔型篩選清單和條件路由對應來獲得穩定、高效能和高可用的第 3 層路由。這些設定檔能夠更細微地篩選每個動態路由通訊協定的路由，並改進跨多個通訊協定的路由重新散佈。

BGP 尋找資料可能傳輸的可用路徑，並根據自治系統中可用的 IP 首碼挑選最佳路由。雙向轉送偵測 (BFD) 設定管理 CN-GW Pod 和路徑故障。

若要啟用動態路由，您需要設定 Panorama 和 CN 系列 HSF 叢集。叢集中至少需要 2 個 CN-MGMT、2 個 CN-NGFW、2 個 CN-DB 和 1 個 CN-GW。BGP 對等在 CN 叢集和外部路由器之間設定。

在 *CN* 系列 *HSF* 上，*PANOS 11.x.x* 將支援動態路由。如需取得 *PAN-OS 11.0* 的相關資訊，請參閱 *PAN-OS* 文件中的取得 CN 系列部署的映像和檔案。

在 Panorama 中，您需要設定裝置群組，並透過裝置群組管理 HSF 叢集。若要設定 HSF 叢集，請參閱 部署 HSF 叢集。

在 HSF 叢集上設定 BGP，您需要執行以下步驟：

1. 啟用進階路由
2. 設定邏輯路由器
3. 建立靜態路由 用於 CN-GW 回送介面。
4. 在進階路由引擎上設定 BGP。

   1. 目前，*BGP* 路由僅支援 *IPv4*。
   2. 在建立對等時，請確保您建立一個回送，並為 ***Addressing***（定址）頁籤中的每個 *CN-GW* 提供回送 *IP* 位址。

5. （選用）建立 BGP 路由設定檔用於驗證、計時器、位址系列、抑制、路由重新散佈到 BGP 和 BGP 篩選。
6. （選用）為進階路由引擎建立篩選器，例如存取清單、首碼清單、AS 路徑存取清單、社群清單和路由對應。
7. 按一下 **Commit to Panorama**（提交至 **Panorama**）。設定提交到 Panorama 之後，BGP 將設定到每個 CN-GW。

若要檢查 BGP 狀態，請登入 CN-MGMT 並執行以下命令：

- 顯示進階路由 BGP 摘要

```
admin@pan-mgmt-sts-1.cluster-001> show advanced-routing bgp route logical-router slot1-LR-1

Status codes:  R removed, d damped, * valid, r ribFailure, S stale, = multipath,
               s suppressed, i internal, > best, h history
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  e egp, i igp, ? incomplete

Logical router: slot1-LR-1
BGP table version is 10, local router ID is 88.0.0.1, vrf ID 0
Default local pref 100, local AS 88
------------------------------------------------------------------------------
   Network              Next Hop            Metric LocPrf Weight Path
*> 3.3.3.0/24           0.0.0.0                  0    100  32768  i
*> 192.168.85.0/24      200.0.0.1                0    100      0 22 i
------------------------------------------------------------------------------
Displayed 2 route(s) 2 path(s)

Logical router: slot1-LR-1
BGP table version is 0, local router ID is 88.0.0.1, vrf ID 0
Default local pref 100, local AS 88
------------------------------------------------------------------------------
   Network              Next Hop            Metric LocPrf Weight Path
------------------------------------------------------------------------------
Displayed 0 route(s) 0 path(s)

admin@pan-mgmt-sts-1.cluster-001> show advanced-routing route type bgp logical-router slot1-LR-1



Logical Router: slot1-LR-1
==========================
flags: A:active, E:ecmp, Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext 1, O2:ospf ext 2

destination                             protocol        nexthop                                 distance  metric    flag      tag       age          inte
ace
192.168.85.0/24                         bgp             200.0.0.1                               20        0         A E               00:04:07

192.168.85.0/24                         bgp             2.2.2.222                               20        0         A E               00:04:07     ethe
et1/3
total route shown: 2
```

- 顯示進階路由 BGP 對等狀態

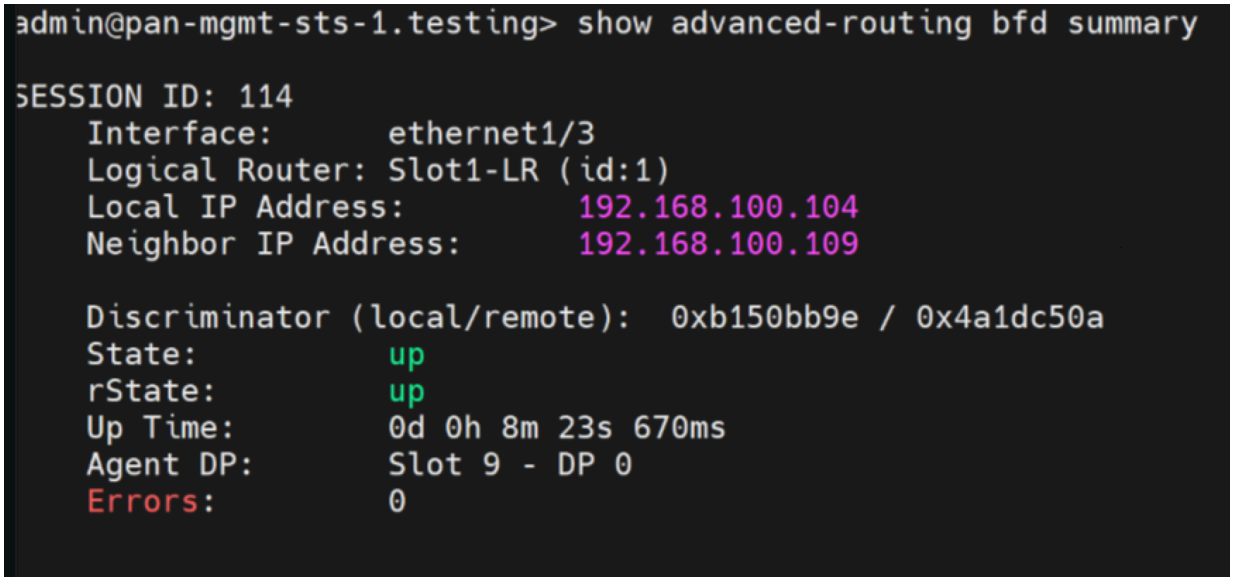
```
admin@pan-mgmt-sts-1.testing> show advanced-routing bgp peer status peer-name DHCP-PEER

Logical Router: Slot1-LR
==============
Peer Name:                DHCP-PEER
BGP State:                Established, up for 00:01:15
```

- 顯示進階路由 BGP 對等詳細資料

```
admin@pan-mgmt-sts-1.testing> show advanced-routing bgp peer details

Peer: DHCP-PEER
==============
Peer name                   DHCP-PEER
Logical router:             Slot1-LR
Remote router ID:           11.11.11.1
Remote AS:                  65008
Remote address:             192.168.100.109:34986
Local address:              192.168.100.102:179
Peer group:                 DHCP-BGP
Peer status:                Established
Up time:                    188 s
Hold time:                  90 s (configured 90)
Keepalive interval:         30 s (configured 30)
Connection retry timer:     15 s
Estimated RTT:              3 ms
Last reset time:            222 s ago
Last reset reason:          No AFI/SAFI activated for peer
BGP connection:             sharedNetwork
Connection established:     2
Connection dropped:         1

Address family:             ipv4Unicast
  Packet queue length:      0
  Update group id:          2
  Sub group id:             2
  Prefix allowed Max:       1000 (warning-only)
  Prefix accepted:          2810
  Prefix Sent:              2920
  Prefix allowed Max warnning: True
  Prefix allowed warnning threshold: 100
  Inbound soft reconfiguration allowed: True

Neighbor capabilities:
  4byteAs                       advertisedAndReceived
  extendedMessage               advertisedAndReceived
  addPath                       {'ipv4Unicast': {'rxAdvertisedAndReceived': True}}
  routeRefresh                  advertisedAndReceivedOldNew
  enhancedRouteRefresh          advertisedAndReceived
  multiprotocolExtensions       {'ipv4Unicast': {'advertisedAndReceived': True}}
  hostName                      {'advHostName': 'pan-mgmt-sts-1.testing', 'advDomainName': 'n/a', 'rcvHostName': 'vyos', 'rcvDomainName': 'n/
  gracefulRestart               advertisedAndReceived
admin@pan-mgmt-sts-1.testing>
```

若要從 CN-MGMT 檢查 BFD 狀態，請執行以下命令

- 顯示進階路由 `BFD` 摘要



- 顯示進階路由 BFD 詳細資料

```
admin@pan-mgmt-sts-1.testing> show advanced-routing bfd details

BFD Session ID: 114
    Version:         1
    Interface:       ethernet1/3
    Protocol:        BGP
    Local IP Address:          192.168.100.104
    Neighbor IP Address:       192.168.100.109

    BFD profile:               default

    State (local/remote):           up / up
    Up Time:         0d 0h 8m 46s 650ms
    Discriminator (local/remote):  0xb150bb9e / 0x4a1dc50a
    Mode:            Active
    Demand Mode:     Disabled
    Poll Bit:        Disabled
    Multihop:        Disabled
    Multihop TTL:    255
    Local Diag Code:                  0 (No Diagnostic)
    Last Received Remote Diag Code:   0 (No Diagnostic)

    Transmit Hold Time:             0ms
    Desired Min Tx Interval:        1000ms
    Required Min Rx Interval:       1000ms
    Received Min Rx Interval:       1000ms
    Negotiated Transmit Interval:   1000ms
    Detect Multiplier:              3
    Received Multiplier:            3
    Detect time (exceeded):         3000ms (1)
    Tx Control Packets (last):      649 (861ms ago)
    Rx Control Packets (last):      604 (669ms ago)
    Agent DP:        Slot 9 - DP 0
    Errors:          0

    Last Recieved Packet:
        Version:         1
        My Discriminator:          0x4a1dc50a
        Your Discriminator:        0xb150bb9e
        Diag Code:       0 (No Diagnostic)
        Length:          24
        Demand bit:      0        Poll bit:        0
        Final bit:       0        Multipoint:      0
        Control Plane Independent:      0
        Authentication Present:         0
        Desired Min Tx Interval:        1000ms
        Required Min Rx Interval:       1000ms
        Detect Multiplier:              3
        Required Min Echo Rx Interval: 50ms
```

CN-Series HSF：使用案例

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

下列是 CN-Series HSF 的使用案例：

- 5G 流量測試
  - 具有 N3+N4 可見性和關聯政策的 5G 安全性
  - 使用應用程式識別和威脅檢查進行輸入/輸出保護
- 根據所支援自訂指標來相應放大防火牆
- 測試案例：CN-MGMT 失敗處理
- 測試案例：CN-NGFW 失敗處理
- 測試案例：CN-DB 失敗處理

5G 流量測試

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

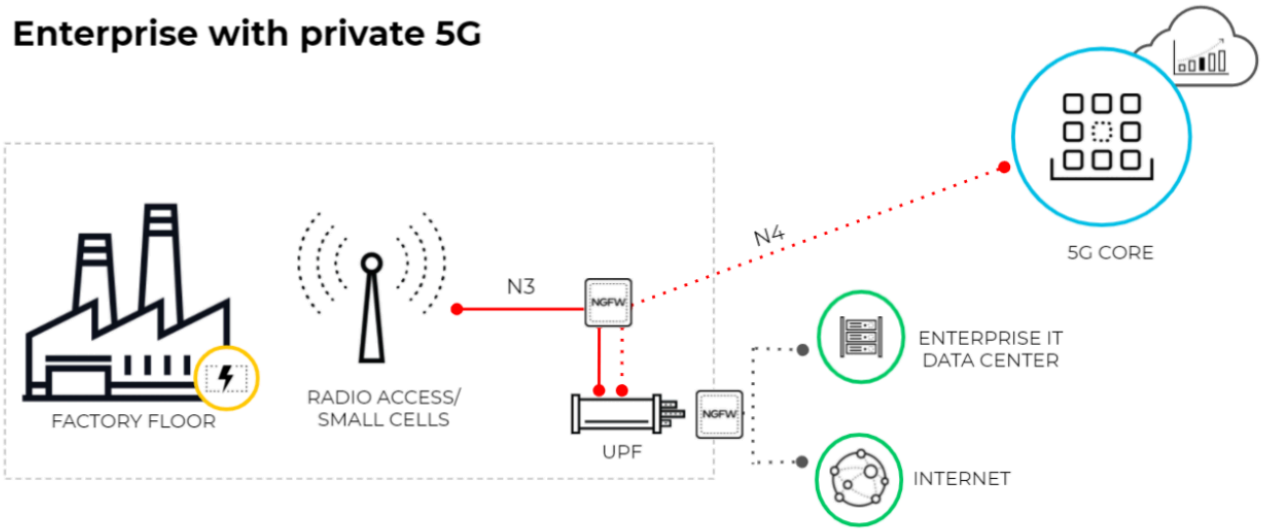
保護網路邊緣需要平衡具有高頻寬、低延遲和即時存取（使用者體驗）的流量檢查和控制（安全性需求）。如果流量是由許多防火牆所處理、應用程式託管於邊緣網站，或者網路邊緣是 IoT 資料的彙總點，則這些問題將會變得更加困難。此外，區隔 5G 網路中的使用者和控制平面，會難以在用戶或裝置層級套用安全性政策，並且缺乏環境型威脅可見性。使用 N3 和 N4 介面所放置的防火牆會提供：

- 已連線裝置之間的訊號層級可見性
- PFCP 和 GTP-U 的具狀態檢查
- 將用戶 ID/Equipment-ID/Slice-ID 與 GTP-U 流量弱點相關聯

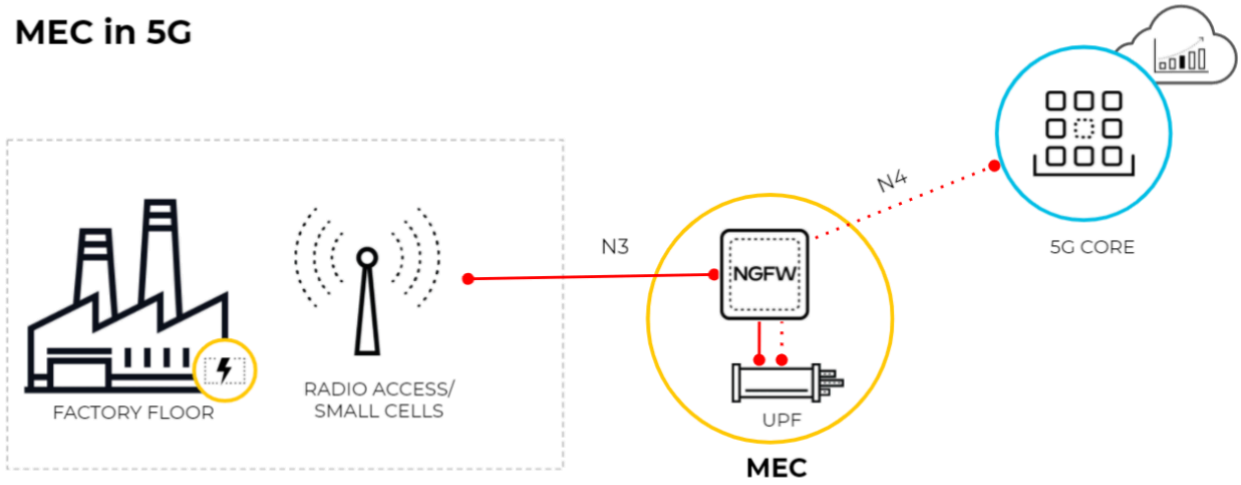
下列是 CN-Series HSF 的 5g 流量使用案例：

- 具有 N3+N4 可見性和關聯政策的 5G 安全性
- 使用應用程式識別和威脅檢查進行輸入/輸出保護

下圖說明可使用私人 5G 網路的企業。5G 核心功能為雲端型或在服務提供者的中央網站。5G 存取與 UPF 之間的連線使用 N3 介面。GTP-U 通道會攜帶 N3 介面上的使用者平面流量。UPF 與工作階段管理功能 (SMF) 之間的連線使用 N4 介面。PFCP 通訊協定會在 N4 介面上使用 UDP 交換來交換封包轉送規則。



此圖說明 5G 網路中的 MEC，其中使用者平面功能 (UPF) 位於邊緣或 MEC 位置，而 5G 核心功能是雲端型或位於服務提供者的中央網站。5G 存取與 UPF 之間的連線使用 N3 介面，而且 GTP-U 通道會透過 N3 介面來攜帶使用者平面流量。UPF 與 SMF 之間的連線使用 N4 介面，而且 PFCP 通訊協定會透過 N4 介面使用 UDP 來交換封包轉送規則。



具有 N3+N4 可見性和關聯政策的 5G 安全性

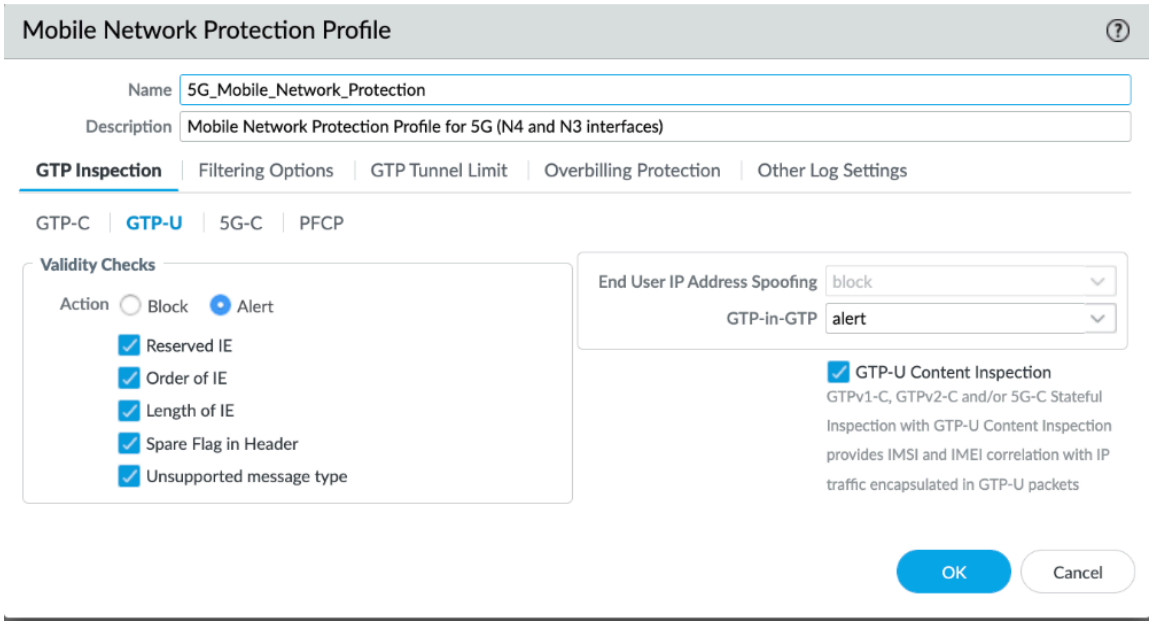
此測試案例會評估 CNF 叢集檢查和保護 N3+N4 介面流量的能力。

STEP 1 | 作為檢查和保護 N3+N4 介面流量的第一步，您將需要啟用 GTP 安全性。

1. 登入防火牆 Web 介面。
2. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理） > **General Settings**（一般設定），然後選取 **GTP-U Security**（**GTP-U** 安全性）。
3. 按一下 **OK**（確定）。
4. **Commit**（提交）變更。
5. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後選取 **Reboot Device**（重新啟動裝置）。

STEP 2 | 建立行動網路保護設定檔，並啟用 GTP-U 檢查。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Mobile Network Protection**（行動網路保護）。
2. **Add**（新增）設定檔，然後輸入 **Name**（名稱），例如 **`5G_Mobile_Network_Protection`**。
3. 在 **PFCP** 頁籤上，啟用 **Stateful Inspection**（具狀態檢查）。



STEP 3 | 選取您想要防火牆對 PFCP 流量執行的狀態檢查以及您想要防火牆在狀態檢查不成功時所採取的動作。

1. 判斷您想要使用的狀態檢查。
   - 檢查關聯訊息—檢查是否有任何失序或遭拒絕的 PFCP 關聯訊息。
   - **Check Session Messages**（檢查工作階段訊息）—檢查是否有任何失序或已拒絕的 PFCP 工作階段訊息；驗證所有 PFCP 工作階段訊息是否都符合現有 PFCP 關聯；警示或捨棄在設定 PFCP 關聯之前到達的 PFCP 工作階段訊息。
   - **Check Sequence Number**（檢查序號）—確認 PFCP 回應中的序號與先前 PFCP 要求訊息中的序號相符。
2. 如果狀態檢查不成功，則請選取您想要防火牆採取的動作。
   - **allow**—允許流量，而且不會在 GTP 日誌中產生日誌項目。
   - **block**—封鎖流量，並在 GTP 日誌中產生高嚴重性日誌項目。
   - **alert**—（預設值）允許流量，並在 GTP 日誌中產生高嚴重性日誌項目。

STEP 4 | （選用）為 PFCP 檢查設定記錄。

1. 選取您想要防火牆何時產生日誌項目。
   - **PFCP** 關聯開始時的日誌
   - **PFCP** 關聯結束時的日誌
   - **PFCP** 工作階段開始時的日誌
   - **PFCP** 工作階段結束時的日誌

STEP 5 | 啟用 PFCP 和 GTP-U 訊息的其他日誌設定

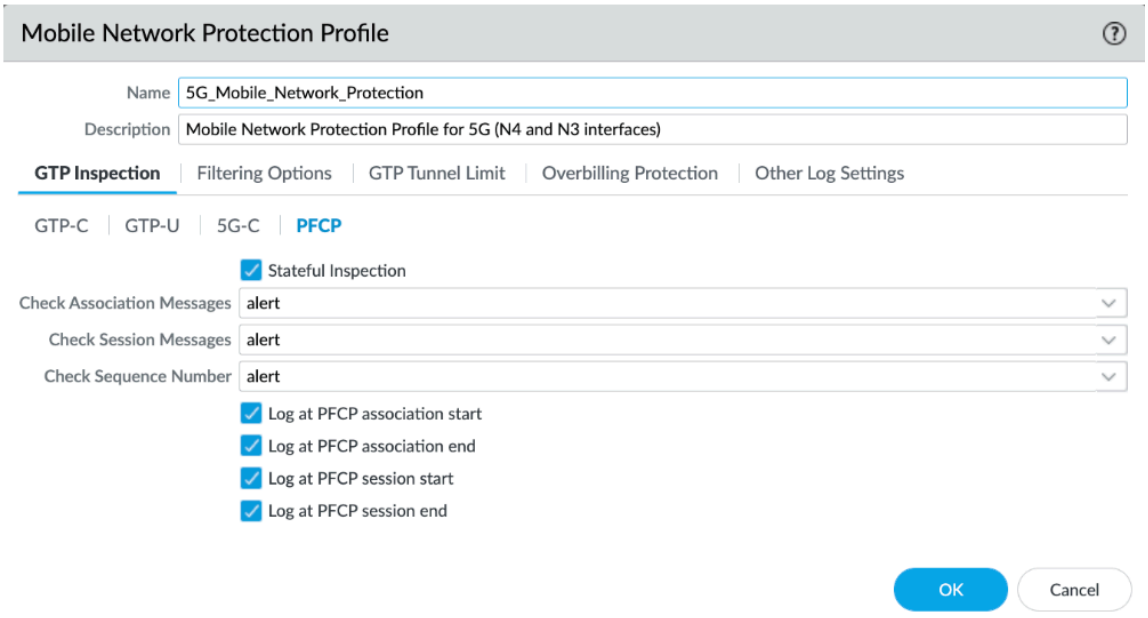
1. 在 **Other Log Settings**（其他日誌設定）頁籤上，選取您想要包括在日誌中的 **PFCP Allowed Message**（**PFCP** 允許的訊息）類型。

   只啟用這些選項以進行疑難排解。

   - 工作階段建立—這些 PFCP 訊息會設定工作階段，包括建立 GTP-U 通道。
   - 工作階段修改—如果工作階段 ID 或 PDR ID 發生變更（例如，由於從 4G 移至 5G 網路），就會傳送這些 PFCP 訊息。它包含 PFCP Session Modification Request（PFCP 工

作階段修改要求）和 PFCP Session Modification Response（PFCP 工作階段修改回應）之類的訊息。

- 工作階段刪除—這些 PFCP 訊息會終止 PFCP 工作階段，包括釋放相關資源。



STEP 6 | 建立來源和目的地分別為 N3 和 N4 介面且應用程式為 GTP-U 和 PFCP 的兩個安全性政策。

1. 選取 **Policies**（政策）> **Security**（安全性），並依 **Name**（名稱）**Add**（新增）安全性政策規則。
2. 選取 **Source**（來源），然後 **Add**（新增）**Source Zone**（來源區域），或選取 **Any**（任何）。
3. 針對 **Source Address**（來源位址），為 N3 介面上的 5G 元素端點 **Add**（新增）位址物件。
4. 針對 **Destination**（目的地），為 N3 介面上的 5G 元素端點 **Add**（新增）**Destination Address**（目的地位址）位址物件。
5. **Add**（新增）要允許的 **Applications**（應用程式），例如使用者平面，即 **GTP-U** 和 **PFCP**。
6. 在 **Actions**（動作）頁籤上，選取 **Action**（動作），例如，**Allow**（允許）。
7. 選取您所建立的 **Mobile Network Protection**（行動網路保護）設定檔。
8. 選取您想要套用的其他設定檔，例如 **Vulnerability Protection**（弱點保護）。
9. 選取日誌設定，例如 **Log at Session Start**（工作階段開始時的日誌）和 **Log at Session End**（工作階段結束時的日誌）。
10. 按一下 **OK**（確定）。
11. 同樣地，為 N4 介面建立另一個安全性政策。

STEP 7 | （選用）輸入來源中的 EDL 資訊，以根據設備 ID/用戶 ID/網路切片 ID 型保護來建立另一個安全性政策規則。

1. 選取 **Policies**（政策）> **Security**（安全性），然後依 **Name**（名稱）來**Add**（新增）安全性政策規則，例如設備 ID 安全性。
2. 選取 **Source**（來源），然後 **Add**（新增）**Source Zone**（來源區域），或選取 **Any**（任何）。
3. 使用下列任何格式，以 **Add**（新增）一個或多個 **Source Equipment**（來源設備）ID：
   - 5G 永久設備識別碼 (PEI)，包括 IMEI
   - IMSI（15 或 16 位數）
   - 類型指派代碼 (TAC) 的八位數 IMEI 前綴
   - 指定 IMEI 的 EDL
4. （選用）您可以將 **Source Subscriber**（來源用戶）和 **Network Slice**（網路切片）名稱新增至此安全性政策規則，以讓規則更具限制性。
5. 將 **Destination Zone**（目的地裝置）、**Destination Address**（目的地位址）和 **Destination Device**（目的地裝置）指定為 **Any**（任何）。
6. **Add**（新增）要允許的 **Applications**（應用程式），例如 **ssh**、**ssl**、**radmin**和 **telnet**。
7. 在 **Actions**（動作）頁籤上，選取 **Action**（動作），例如，**Allow**（允許）。
8. 選取您想要套用的設定檔，例如 **Antivirus**（防毒）、**Vulnerability Protection**（弱點保護）和 **Anti-Spyware**（反間諜軟體）。
9. 選取日誌設定，例如 **Log at Session Start**（工作階段開始時的日誌）和 **Log at Session End**（工作階段結束時的日誌）。
10. 按一下 **OK**（確定）。

    預期測試結果：
    - 驗證監控區段中的 GTP-U 日誌。
    - 驗證日誌的詳細資料區段，以了解用戶、設備、網路切片資訊。
    - 觀察規則命中計數是否增加。

使用應用程式識別和威脅檢查進行輸入/輸出保護

此測試案例會評估 CNF 叢集檢查和保護 N6 介面上上輸入和輸出流量的能力。

N6 介面透過 TCP/UDP 向網際網路攜帶純文字流量。現在，使用 N6 介面上所部署的 VM-Series 防火牆，您可以全面了解應用程式使用方式。防火牆可以使用 TP、Adv-URL 篩選、Wildfire、DNS 安全性這類 CDSS 訂閱對允許的流量來實作安全性。

下列步驟是執行此測試案例的大綱。如需執行個別步驟的詳細資料，請參閱具有 N3+N4 可見性和關聯政策的 5G 安全性。

STEP 1 | 使用適當的區域和介面，以為 N6 介面建立安全性政策。

STEP 2 | 使用預設安全性設定檔，或針對 URL 篩選、Wildfire、弱點保護等建立自訂類別。

STEP 3 | （選用）在 URL 類別下方，針對允許的 URL 建立自訂設定檔。

STEP 4 | （選用）建立多個符合不同準則的安全性政策。建立安全性政策時，請選取步驟 3 中所建立的設定檔。

STEP 5 | 傳送流量。

STEP 6 | 以輸入/輸出方向傳送惡意流量，並驗證是否已封鎖流量。

預期結果：

- 政策的命中數會增加。
- 檢查 URL 篩選、流量和威脅日誌的適當日誌。

根據所支援自訂指標來相應放大防火牆

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

此測試有助於驗證 CN-Series HSF 叢集根據自動調整中所指定的自訂指標值目標來進行自動調整的能力。

STEP 1 | 建立 CN-Series HSF 叢集時，啟用自動調整，以根據自動調整中所指定的自訂指標目標值來進行自動調整。如需詳細資訊，請參閱 部署 HSF 叢集

STEP 2 | 進入 CloudWatch 命名空間，以將指標推送至 AWS CloudWatch。

STEP 3 | 輸入 EKS 叢集的地區。

STEP 4 | 輸入推送間隔。

STEP 5 | 選擇 Autoscaling Meric（自動調整規模指標）。在此範例中，您可能想要選擇 PansessionActive。

STEP 6 | 指定相應縮小閾值和相應放大閾值。例如，如果您有 2 個 NGFW Pod 正在執行，而且防火牆上的工作階段總數目前為 1000，則雲端監看指標將會顯示 500（每個 NGFW Pod）。

STEP 7 | 您可以將相應放大閾值設定為 250，而且自動調整應該再增加 2 個 NGFW Pod。

STEP 8 | 在 MGMT Pod 上使用 show session info 命令，以取得工作階段資訊

STEP 9 | 您可以指定可自動調整規模的最大和最小 NGFW Pod。

預期結果：NGFW Pod 應該根據相應放大閾值來自動調整規模

測試案例：CN-MGMT 失敗處理

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

此測試會評估 CN-NGMT 失敗處理。

CN-Series HSF 部署所需的最小 CN-MGMT Pod 數目為兩個，以確保失敗處理。部署之後，作用中 CN-MGMT Pod 會先成為 Leader，而第二個 CN-MGMT 會成為 Follower。這兩個 CN-MGMT Pod 具有相同的設定。在任何情況下，一個 CN-MGMT Pod 會處於 READY 狀態。CN-DB、CN-GW 和 CN-NGFW Pod 會透過流量互連 (TI) 連結來連線至處於 READY 狀態的 CN-MGMT Pod。

兩個 *CN-MGMT Pod* 未處於 *HA* 主動-被動或 *HA* 主動-主動模式。這兩個 *Pod* 都具有相同的設定，並使用 *Panorama* 進行設定。

CN-MGMT Pod 失敗是下列其中一個情況所造成。

- 活性檢查失敗
  - 如果關閉 `slotd`
  - 如果關閉 `ipsec` 或 `strongswan`
- CN-MGMT Pod 當機並重新啟動

STEP 1 | 從 Panorama CLI 中，輸入 `show clusters name`<cluster-name>以檢視 Leader 和 Follower CN-MGMT Pod。

下列輸出顯示 **`pan-mgmt-sts-1`** Pod 作用中。

```
Cluster: cluster-001 Creation time:2022/11/30 03:23:50 CN-MGMT pods:88C00D31E1FC86B
 (pan-mgmt-sts-0.cluster-001, connected, In Sync) 84CC9A394B3E196 (active,
 pan-mgmt-sts-1.cluster-001, connected, In Sync) Slot-ID PodName Type Version
 ------------------------------------------------------------------------------------------ 5
 pan-db-dep-6774cd774d-k49cm CN-DB 11.0.1-c183.dev_e_rel 1 pan-gw-dep-d849c7df8-4sk54 CN-GW
 11.0.1-c183.dev_e_rel 6 pan-ngfw-dep-668965d598-pnthb CN-NGFW 11.0.1-c183.dev_e_rel 8 pan-
ngfw-dep-668965d598-s2zcc CN-NGFW 11.0.1-c183.dev_e_rel 7 pan-ngfw-dep-668965d598-vf9l4 CN-NGFW
 11.0.1-c183.dev_e_rel 9 pan-ngfw-dep-668965d598-pmmjd CN-NGFW 11.0.1-c183.dev_e_rel 10 pan-
db-dep-6774cd774d-gjpkr CN-DB 11.0.1-c183.dev_e_rel 2 pan-gw-dep-d849c7df8-ct6wk CN-GW 11.0.1-
c183.dev_e_rel
```

STEP 2 | 從 Kubernetes 控制器 CLI 中，檢視 **pan-mgmt-sts-1** Pod 的叢集成員資格以及 CN-DB、CN-GW 和 CN-NGFW Pod 的狀態。

1. 輸入 `kubectl get pods -n kube-system`，以檢視所有 Pod 的狀態。

   輸出：

   pan-mgmt-sts-1 作用中。所有 CN-DB、CN-GW 和 CN-NGFW Pod 都會連線至 **pan-mgmt-sts-1**。

   ```
   NAME READY STATUS RESTARTS AGE pan-db-dep-6774cd774d-gjpkr 1/1 Running 0 69m
    pan-db-dep-6774cd774d-k49cm 1/1 Running 0 69m pan-gw-dep-d849c7df8-4sk54 1/1
    Running 0 69m pan-gw-dep-d849c7df8-ct6wk 1/1 Running 0 69m pan-mgmt-sts-0
    0/1 Running 0 83m pan-mgmt-sts-1 1/1 Running 0 83m pan-ngfw-dep-668965d598-
   pmmjd 1/1 Running 0 69m pan-ngfw-dep-668965d598-pnthb 1/1 Running 0 69m pan-
   ngfw-dep-668965d598-s2zcc 1/1 Running 0 69m pan-ngfw-dep-668965d598-vf9l4 1/1
    Running 0 69m
   ```

2. 從 **pan-mgmt-sts-1** 中，檢查叢集成員資格。

   進入 **pan-mgmt-sts-1** Pod。

   ```
   kubectl -n kube-system exec -it pan-mgmt-sts-1 -- bash
   ```

   ```
   su - admin
   ```

   使用下列命令，檢查是否所有 CN-DB、CN-GW 和 CN-NGFW Pod 都已連線至 Leader CN-MGMT Pod命令。

   ```
   show cluster-membership show-slot-info slot all
   ```

   輸出：

   ```
   MP leader status:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
    ================================================================================ 1 CN-GW
    192.168.23.101 192.168.24.100 UP UP UP 10 CN-DB 192.168.23.104 ::UP UP NA 2 CN-GW 192.168.23.100
    192.168.24.98 UP UP UP 5 CN-DB 192.168.23.102 ::UP UP NA 6 CN-NGFW 192.168.23.89 192.168.24.83 UP UP UP
    7 CN-NGFW 192.168.23.105 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.103 192.168.24.84 UP UP UP 9 CN-
   NGFW 192.168.23.82 192.168.24.81 UP UP UP
   ```

3. 從 **pan-mgmt-sts-0** 中，檢查叢集成員資格。

   進入 **pan-mgmt-sts-0** Pod。

   ```
   kubectl -n kube-system exec -it pan-mgmt-sts-0 -- bash
   ```

   ```
   su - admin
   ```

   使用下列命令，以檢查是否有任何 CN-DB、CN-GW 和 CN-NGFW Pod 連線至 Follower CN-MGMT Pod。

   ```
   show cluster-membership show-slot-info slot all
   ```

   輸出：

   ```
   沒有成員資訊
   ```

STEP 3 | 測試 CN-MGMT Pod 失敗處理。

1. 從 Kubernetes 控制器 CLI 中，輸入下列命令以刪除 Leader **pan-mgmt-sts-1** Pod。

```
kubectl -n kube-system delete pod pan-mgmt-sts-1
```

2. 從 Panorama CLI 中，輸入 `show clusters name <cluster-name>` 以檢視新的 Leader 和 Follower CN-MGMT Pod。

   下列輸出顯示 **pan-mgmt-sts-0** pod 現在作用中。

```
Cluster: cluster-001 Creation time:2022/11/30 03:23:50 CN-MGMT pods:88C00D31E1FC86B
 (active, pan-mgmt-sts-0.cluster-001, connected, In Sync) 84CC9A394B3E196
 (pan-mgmt-sts-1.cluster-001, connected, In Sync) Slot-ID PodName Type Version
 ------------------------------------------------------------------------------------ 5 pan-
db-dep-6774cd774d-k49cm CN-DB 11.0.1-c183.dev_e_rel 1 pan-gw-dep-d849c7df8-4sk54 CN-GW 11.0.1-
c183.dev_e_rel 6 pan-ngfw-dep-668965d598-pnthb CN-NGFW 11.0.1-c183.dev_e_rel 8 pan-ngfw-dep-668965d598-
s2zcc CN-NGFW 11.0.1-c183.dev_e_rel 7 pan-ngfw-dep-668965d598-vf9l4 CN-NGFW 11.0.1-c183.dev_e_rel 9 pan-
ngfw-dep-668965d598-pmmjd CN-NGFW 11.0.1-c183.dev_e_rel 10 pan-db-dep-6774cd774d-gjpkr CN-DB 11.0.1-
c183.dev_e_rel 2 pan-gw-dep-d849c7df8-ct6wk CN-GW 11.0.1-c183.dev_e_rel
```

STEP 4 | 從 Kubernetes 控制器 CLI 中，檢視 **pan-mgmt-sts-0** Pod 的叢集成員資格以及 CN-DB、CN-GW 和 CN-NGFW Pod 的狀態。

1. 輸入 `kubectl get pods -n kube-system`，以檢視所有 Pod 的狀態。

   輸出：

   pan-mgmt-sts-0 作用中。所有 CN-DB、CN-GW 和 CN-NGFW Pod 都會連線至 **pan-mgmt-sts-1**。

```
NAME READY STATUS RESTARTS AGE pan-db-dep-6774cd774d-gjpkr 1/1 Running 0 76m
 pan-db-dep-6774cd774d-k49cm 1/1 Running 0 76m pan-gw-dep-d849c7df8-4sk54 1/1
 Running 0 76m pan-gw-dep-d849c7df8-ct6wk 1/1 Running 0 76m pan-mgmt-sts-0
 1/1 Running 0 90m pan-mgmt-sts-1 0/1 Running 0 90m pan-ngfw-dep-668965d598-
pmmjd 1/1 Running 0 76m pan-ngfw-dep-668965d598-pnthb 1/1 Running 0 76m pan-
ngfw-dep-668965d598-s2zcc 1/1 Running 0 76m pan-ngfw-dep-668965d598-vf9l4 1/1
 Running 0 76m
```

2. 從 **pan-mgmt-sts-0** 中，檢查叢集成員資格。

   進入 **pan-mgmt-sts-0** Pod。

```
kubectl -n kube-system exec -it pan-mgmt-sts-0 -- bash
```

```
su - admin
```

   使用下列命令，檢查是否所有 CN-DB、CN-GW 和 CN-NGFW Pod 都已連線至 Leader CN-MGMT Pod命令。

```
show cluster-membership show-slot-info slot all
```

   輸出：

```
MP leader status:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================ 1 CN-GW
 192.168.23.101 192.168.24.100 UP UP UP 10 CN-DB 192.168.23.104 ::UP UP NA 2 CN-GW 192.168.23.100
 192.168.24.98 UP UP UP 5 CN-DB 192.168.23.102 ::UP UP NA 6 CN-NGFW 192.168.23.89 192.168.24.83 UP UP UP
 7 CN-NGFW 192.168.23.105 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.103 192.168.24.84 UP UP UP 9 CN-
NGFW 192.168.23.82 192.168.24.81 UP UP UP
```

3. 從 **pan-mgmt-sts-1** 中，檢查叢集成員資格。

   進入 **pan-mgmt-sts-1** pod。

   ```
   kubectl -n kube-system exec -it pan-mgmt-sts-1 -- bash
   ```

   ```
   su - admin
   ```

   使用下列命令，以檢查是否有任何 CN-DB、CN-GW 和 CN-NGFW Pod 連線至 Follower CN-MGMT Pod。

   ```
   show cluster-membership show-slot-info slot all
   ```

   輸出：

   ```
   沒有成員資訊
   ```

測試結果：Leader Pod `pan-mgmt-sts-1` 失敗時，Follower Pod `pan-mgmt-sts-0` 會成為新的 Leader。此 CN-MGMT 失敗處理機制可確保流量不中斷。不會影響現有或新工作階段。

測試案例：CN-NGFW 失敗處理

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

此測試會評估 CN-NGFW 失敗處理。

CN-NGFW 失敗可能是因下列情況所造成。

- 節點問題
- CN-NGFW Pod 當機並重新啟動
- 節點和 CN-NGFW Pod 沒有問題，但 **pan_task** 當機
- 在下列情況下，會從叢集成員資格中移除 CN-NGFW：
  - 透過 Eth0 介面的 IPsec 監控失敗
  - 叢集互連 (CI) 連結中斷
  - 流量互連 (TI) 連結中斷

在此情況下，用戶端與伺服器之間的 SSH 工作階段會安裝在 CN-NGFW 1 上。如果 CN-NGFW 1 關閉，則 SSH 工作階段必須透過容錯移轉至另一個 CN-NGFW 來保持使用中狀態。

STEP 1 | 從 Panorama CLI 中，輸入 `show clusters name`<cluster-name> 以檢視連線至 CN-MGMT Pod 的 CN-NGFW、CN-DB 和 CN-GW Pod。

```
Cluster: cluster-002 Creation time:2022/11/22 04:56:46 CN-MGMT pods:87F87FE94CBBB03
 (active, pan-mgmt-sts-0.cluster-002, connected, In Sync) Slot-ID PodName Type Version
 ------------------------------------------------------------------------------------- 1
 pan-gw-dep-5cd5c87d76-przjx CN-GW 11.0.1-c156.dev_e_rel 6 pan-db-dep-d6fb496b-jf2ms CN-DB
 11.0.1-c156.dev_e_rel 5 pan-ngfw-dep-5cd8f55848-dbhwh CN-NGFW 11.0.1-c156.dev_e_rel 8 pan-
ngfw-dep-5cd8f55848-slk5l CN-NGFW 11.0.1-c156.dev_e_rel 7 pan-db-dep-d6fb496b-hfmlp CN-DB
 11.0.1-c156.dev_e_rel 9 pan-ngfw-dep-5cd8f55848-pq6ks CN-NGFW 11.0.1-c156.dev_e_rel 2 pan-
gw-dep-5cd5c87d76-4kbfk CN-GW 11.0.1-c156.dev_e_rel 11 pan-ngfw-dep-5cd8f55848-rsbqn CN-NGFW
 11.0.1-c156.dev_e_rel
```

STEP 2 | 使用命令 `show cluster-membership show-slot-info slot all`，以檢視 CN-MGMT Pod `an-mgmt-sts-0` 的叢集成員資格詳細資料。

```
MP leader status:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================
 1 CN-GW 192.168.23.100 192.168.24.80 UP UP UP 11 CN-NGFW 192.168.23.87 192.168.24.93 UP
 UP UP 2 CN-GW 192.168.23.101 192.168.24.100 UP UP UP 7 CN-DB 192.168.23.102 ::UP UP NA 6
 CN-DB 192.168.23.104 ::UP UP NA 5 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW
 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP
```

ethernetx/3 子網路的所有介面都必須位於相同的區域。同樣地，ethernetx/4 子網路的所有介面都必須位於相同的區域。

STEP 3 | 使用 `show session all filter application ssh`，以檢視所有 SSH 工作階段。

針對每個工作階段，用戶端到伺服器和伺服器到用戶端會有兩個流程。

```
------------------------------------------------------------------------------ ID Application
 State Type Flag Src[Sport]/Zone/Proto (translated IP[Port]) Vsys Dst[Dport]/Zone (translated
 IP[Port]) ------------------------------------------------------------------------------
 1342177294 ssh ACTIVE FLOW 192.168.200.100[48702]/untrust_ei1/6 (192.168.200.100[48702])
 vsys1 192.168.250.100[22]/trust_ei2 (192.168.250.100[22]) admin@pan-mgmt-sts-1.cluster-001>
 show session id 1342177294 Session 1342177294 c2s flow: source:192.168.200.100 [untrust_ei1]
 dst:192.168.250.100 proto:6 sport:48702 dport:22 state:ACTIVE type:FLOW src user: unknown
 dst user: unknown s2c flow: source:192.168.250.100 [trust_ei2] dst:192.168.200.100 proto:6
 sport:22 dport:48702 state:ACTIVE type:FLOW src user: unknown dst user: unknown Slot :11 DP :0
 index(local): :14 start time :Mon Nov 21 21:30:02 2022 timeout :3600 sec time to live :3542 sec
 total byte count(c2s) :3887 total byte count(s2c) :4501 layer7 packet count(c2s) :23 layer7
 packet count(s2c) :20 vsys : vsys1 application : ssh rule : allow_inside-to-outside service
 timeout override(index) :False session to be logged at end :True session in session ager :True
 session updated by HA peer :False layer7 processing : completed URL filtering enabled :True
 URL category : search-engines session via syn-cookies :False session terminated on host :False
 session traverses tunnel :False session terminate tunnel :False captive portal session :False
 ingress interface : ethernet1/3 egress interface : ethernet1/4 session QoS rule :N/A (class 4)
 tracker stage l7proc : ctd decoder done end-reason : unknown
```

工作階段擁有者是插槽 11。

您可以使用下列範例命令來檢視篩選過的叢集流程詳細資料。

```
show cluster-flow all filter source-port 22
```

輸出：

```
--------------------------------------------------------------------------------
 Slot 5
 ------------------------------------------------------------------------------ Id
 State Type Src[Sport]/Proto Dst[Dport]
 --------------------------------------------------------------------------------
 536870940 ACTIVE FLOW 192.168.250.100[22]/6 192.168.200.100[48702]
 --------------------------------------------------------------------------------
 Slot 6
```

```
 ------------------------------------------------------------------------------- Id
 State Type Src[Sport]/Proto Dst[Dport]
 -------------------------------------------------------------------------------
 671088668 ACTIVE FLOW 192.168.250.100[22]/6 192.168.200.100[48702]
```

```
show cluster-flow all filter destination-port 22
```

輸出：

```
-------------------------------------------------------------------------------
 Slot 5
 ------------------------------------------------------------------------------- Id
 State Type Src[Sport]/Proto Dst[Dport]
 -------------------------------------------------------------------------------
 536870939 ACTIVE FLOW 192.168.200.100[48702]/6 192.168.250.100[22]
 -------------------------------------------------------------------------------
 Slot 6
 ------------------------------------------------------------------------------- Id
 State Type Src[Sport]/Proto Dst[Dport]
 -------------------------------------------------------------------------------
 671088667 ACTIVE FLOW 192.168.200.100[48702]/6 192.168.250.100[22]
```

STEP 4 | 使用命令 `kubectl -n kube-system delete pod pan-ngfw-dep-5cd8f55848-rsbqn`，以刪除插槽 11 上的 Pod。

輸出：

```
pod "pan-ngfw-dep-5cd8f55848-rsbqn" deleted
```

插槽 11 中 CN-NGFW Pod 所擁有的工作階段現在標記為孤立。

```
admin@pan-mgmt-sts-1.cluster-001> set system setting target-dp s5dp0 Session
 target dp changed to s6dp0 admin@pan-mgmt-sts-1.cluster-001> show cluster-flow
 id 536870939 Flow 536870939 start time :Mon Nov 21 21:30:02 2022 timeout :3600
 sec source :192.168.200.100 sport :48702 dest :192.168.250.100 dport :22 proto :6
 zone :1 type :FLOW state :ACTIVE ipver :4 fidx :28 cid :0 gft :0 gft' :1 predict :0
 orphan :1 flag_inager :0 ager_thread :3 flags :0 flow-data : type: l7 app-
id:25 startlog:1 endlog:1 denied:0 admin@pan-mgmt-sts-1.cluster-001> set system
 setting target-dp s6dp0 Session target dp changed to s6dp0 admin@pan-mgmt-
sts-1.cluster-001> show cluster-flow id 671088667 Flow 671088667 start time :Mon
 Nov 21 21:30:02 2022 timeout :3600 sec source :192.168.200.100 sport :48702
 dest :192.168.250.100 dport :22 proto :6 zone :1 type :FLOW state :ACTIVE ipver :4
 fidx :28 cid :0 gft :1 gft' :0 predict :0 orphan :1 flag_inager :0 ager_thread :4
 flags :0 flow-data : type: l7 app-id:25 startlog:1 endlog:1 denied:0
```

STEP 5 | 使用命令 `show session all filter application ssh`，以存取 SSH 工作階段。

防火牆將會容錯移轉至可用的 CN-NGFW Pod，以處理孤立流程。新的工作階段擁有者是插槽 7。

```
------------------------------------------------------------------------------ ID Application
 State Type Flag Src[Sport]/Zone/Proto (translated IP[Port]) Vsys Dst[Dport]/Zone (translated
 IP[Port]) ------------------------------------------------------------------------------
 805306374 ssh ACTIVE FLOW 192.168.200.100[48702]/untrust_ei1/6 (192.168.200.100[48702])
 vsys1 192.168.250.100[22]/trust_ei2 (192.168.250.100[22]) admin@pan-mgmt-sts-1.cluster-001>
 show session id 805306374 Session 805306374 c2s flow: source:192.168.200.100 [untrust_ei1]
 dst:192.168.250.100 proto:6 sport:48702 dport:22 state:ACTIVE type:FLOW src user: unknown
 dst user: unknown s2c flow: source:192.168.250.100 [trust_ei2] dst:192.168.200.100 proto:6
 sport:22 dport:48702 state:ACTIVE type:FLOW src user: unknown dst user: unknown Slot :7 DP :0
 index(local): :6 start time :Mon Nov 21 21:43:27 2022 timeout :3600 sec time to live :3581
 sec total byte count(c2s) :1350 total byte count(s2c) :1506 layer7 packet count(c2s) :17
 layer7 packet count(s2c) :11 vsys : vsys1 application : ssh rule :Promoted-session service
 timeout override(index) :False session to be logged at end :True session in session ager :True
```

```
 session updated by HA peer :False layer7 processing : completed URL filtering enabled :True
 URL category : search-engines session via syn-cookies :False session terminated on host :False
 session traverses tunnel :False session terminate tunnel :False captive portal session :False
 ingress interface : ethernet1/3 egress interface : ethernet1/4 session QoS rule :N/A (class 4)
 tracker stage l7proc : fastpath state none end-reason : unknown
```

叢集流程中未變更。

```
admin@pan-mgmt-sts-1.cluster-001> set system setting target-dp s5dp0 Session
 target dp changed to s5dp0 admin@pan-mgmt-sts-1.cluster-001> show cluster-flow
 id 536870939 Flow 536870939 start time :Mon Nov 21 21:30:02 2022 timeout :3600
 sec source :192.168.200.100 sport :48702 dest :192.168.250.100 dport :22 proto :6
 zone :1 type :FLOW state :ACTIVE ipver :4 fidx :12 cid :7 gft :0 gft' :1 predict :0
 orphan :0 flag_inager :0 ager_thread :3 flags :0 flow-data : type: l7 app-
id:25 startlog:1 endlog:1 denied:0 admin@pan-mgmt-sts-1.cluster-001> set system
 setting target-dp s6dp0 Session target dp changed to s6dp0 admin@pan-mgmt-
sts-1.cluster-001> show session id 805306374 Session 805306374 Bad Key: c2s:
 'c2s' Bad Key: s2c: 's2c' index(local): :6 admin@pan-mgmt-sts-1.cluster-001>
 show cluster-flow id 671088667 Flow 671088667 start time :Mon Nov 21 21:30:02
 2022 timeout :3600 sec source :192.168.200.100 sport :48702 dest :192.168.250.100
 dport :22 proto :6 zone :1 type :FLOW state :ACTIVE ipver :4 fidx :12 cid :7 gft :1
 gft' :0 predict :0 orphan :0 flag_inager :0 ager_thread :4 flags :0 flow-data :
 type: l7 app-id:25 startlog:1 endlog:1 denied:0
```

結果：

不會影響現有或新工作階段。Panorama 上已更新的叢集成員資格。

測試案例：CN-DB 失敗處理

我可以在哪裡使用這個？	我需要哪些內容？
• CN 系列 HSF 防火牆部署	• CN-Series 11.0.x or above Container Images • Panorama 執行 PAN-OS 11.0.x 或更高版本

此測試會評估 CN-DB 失敗處理。CN-Series HSF 部署的偏好 CN-DB Pod 數目為兩個。這兩個 CN-DB 的設定會相同。

CN-DB 1 長時間停機時，CN-DB 2 會處理現有工作階段，並設定新工作階段。CN-DB 1 再次啟動時，會檢查現有工作階段的工作階段同步、查閱和卸除，並設定新工作階段。

STEP 1 | 使用命令 `show cluster-membership show-slot-info slot all`，以檢視 CN-MGMT Pod 的叢集成員資格詳細資料。

```
MP leader status:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ================================================================================
 1 CN-GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP
 UP UP 2 CN-GW 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 ::UP UP NA 6
 CN-DB 192.168.23.104 ::UP UP NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW
 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP
```

STEP 2 | 刪除插槽 6 中的 CN-DB Pod。

1. 從 Panorama CLI，使用命令 `show clusters name cluster-001` 來取得插槽 6 上的 CN-DB Pod 名稱。

```
Cluster: cluster-001 Creation time:2022/11/22 05:11:09 CN-MGMT pods:8FF0233D36BD57D
 (active, pan-mgmt-sts-1.cluster-001, connected, In Sync) 8F846238B0740D2
 (pan-mgmt-sts-0.cluster-001, connected, In Sync) Slot-ID PodName Type Version
 ------------------------------------------------------------------------------------------ 5 pan-
db-dep-7b6f6c5458-5fgnr CN-DB 11.0.1-c156.dev_e_rel 1 pan-gw-dep-748cdb856d-4f66g CN-GW 11.0.1-
c156.dev_e_rel 2 pan-gw-dep-748cdb856d-p5qdd CN-GW 11.0.1-c156.dev_e_rel 7 pan-ngfw-dep-56cdfdd656-
srmdt CN-NGFW 11.0.1-c156.dev_e_rel 8 pan-ngfw-dep-56cdfdd656-hvcw2 CN-NGFW 11.0.1-c156.dev_e_rel 9 pan-
ngfw-dep-56cdfdd656-bjtmd CN-NGFW 11.0.1-c156.dev_e_rel 10 pan-ngfw-dep-56cdfdd656-6jq2f CN-NGFW 11.0.1-
c156.dev_e_rel 6 pan-db-dep-7b6f6c5458-4tvpq CN-DB 11.0.1-c156.dev_e_rel
```

2. 從控制器 CLI 中，輸入命令 `kubectl delete pod pan-db-dep-7b6f6c5458-4tvpq -n kube-system` 以刪除插槽 6 中的 CN-DB Pod。

   現在已刪除插槽 6 中的 CN-DB Pod。

```
admin@pan-mgmt-sts-1.cluster-001> show cluster-membership show-slot-info slot
 all MP leader status:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ============================================================================== 1 CN-
GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP UP UP 2 CN-GW
 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 ::UP UP NA 7 CN-NGFW 192.168.23.103
 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82
 192.168.24.81 UP UP UP
```

3. 使用命令 `show cluster-flow all`，以檢查叢集流量。

```
Slot 5 ------------------------------------------------------------------------------ Id
 State Type Src[Sport]/Proto Dst[Dport]
 ------------------------------------------------------------------------------
 536870953 ACTIVE FLOW 192.168.101.100[3784]/17 192.168.101.6[49156]
 536870958 ACTIVE FLOW 192.168.200.100[48706]/6 192.168.250.100[22] 536870954
 ACTIVE FLOW 192.168.100.6[49153]/17 192.168.100.100[3784] 536870955 ACTIVE
 FLOW 192.168.100.100[3784]/17 192.168.100.6[49153] 536870952 ACTIVE
 FLOW 192.168.101.6[49156]/17 192.168.101.100[3784] 536870951 ACTIVE FLOW
 192.168.100.101[3784]/17 192.168.100.6[49154] 536870960 OPENING FLOW
 fe80:0:0:0:20c:29ff:fe85:3442[133]/58 ff02:0:0:0:0:0:0:2[0] 536870957 ACTIVE FLOW
 192.168.101.101[3784]/17 192.168.101.6[49155] 536870959 ACTIVE FLOW 192.168.250.100[22]/6
 192.168.200.100[48706] 536870950 ACTIVE FLOW 192.168.100.6[49154]/17
 192.168.100.101[3784] 536870956 ACTIVE FLOW 192.168.101.6[49155]/17 192.168.101.101[3784]
 ------------------------------------------------------------------------------ Slot
 6 ------------------------------------------------------------------------------ No
 Active Flows
```

   具有 CN-DB Pod 的插槽 6 現在處於 PREPARE 狀態，並且關閉 CI 連結。

```
MP leader status:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ============================================================================== 1 CN-GW
 192.168.23.100 192.168.24.80 UP IMPACTED UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP IMPACTED UP
 2 CN-GW 192.168.23.101 192.168.24.100 UP IMPACTED UP 5 CN-DB 192.168.23.102 ::UP IMPACTED NA 6 CN-
DB 192.168.23.104 ::PREPARE DOWN NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP IMPACTED UP 8 CN-NGFW
 192.168.23.105 192.168.24.84 UP IMPACTED UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP IMPACTED UP
```

STEP 3 | 除非 CN-DB Pod 再次作用，否則請輸入 `show cluster-membership show-slot-info slot all`。

```
MP leader status:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ============================================================================================
 1 CN-GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP UP
 UP 2 CN-GW 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 ::UP UP NA 6 CN-
DB 192.168.23.104 ::PROBE UP NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW
 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP
```

STEP 4 | 使用命令 `show cluster-flow all`，以再次檢查叢集流量。

```
------------------------------------------------------------------------------ Slot 5
 ------------------------------------------------------------------------------ Id State Type
```

```
Src[Sport]/Proto Dst[Dport]
------------------------------------------------------------------------------
536870953 ACTIVE FLOW 192.168.101.100[3784]/17 192.168.101.6[49156] 536870958
ACTIVE FLOW 192.168.200.100[48706]/6 192.168.250.100[22] 536870954 ACTIVE FLOW
192.168.100.6[49153]/17 192.168.100.100[3784] 536870955 ACTIVE FLOW 192.168.100.100[3784]/17
192.168.100.6[49153] 536870952 ACTIVE FLOW 192.168.101.6[49156]/17 192.168.101.100[3784]
536870951 ACTIVE FLOW 192.168.100.101[3784]/17 192.168.100.6[49154] 536870960
OPENING FLOW fe80:0:0:0:20c:29ff:fe85:3442[133]/58 ff02:0:0:0:0:0:0:2[0] 536870957
ACTIVE FLOW 192.168.101.101[3784]/17 192.168.101.6[49155] 536870959 ACTIVE FLOW
192.168.250.100[22]/6 192.168.200.100[48706] 536870950 ACTIVE FLOW 192.168.100.6[49154]/17
192.168.100.101[3784] 536870956 ACTIVE FLOW 192.168.101.6[49155]/17 192.168.101.101[3784]
------------------------------------------------------------------------------ Slot 6
------------------------------------------------------------------------------ Id State Type
Src[Sport]/Proto Dst[Dport]
------------------------------------------------------------------------------
671088642 ACTIVE FLOW 192.168.101.100[3784]/17 192.168.101.6[49156] 671088641 ACTIVE FLOW
192.168.200.100[48706]/6 192.168.250.100[22] 671088643 ACTIVE FLOW 192.168.100.6[49153]/17
192.168.100.100[3784] 671088645 ACTIVE FLOW 192.168.100.100[3784]/17 192.168.100.6[49153]
671088644 ACTIVE FLOW 192.168.101.6[49156]/17 192.168.101.100[3784] 671088646
ACTIVE FLOW 192.168.100.101[3784]/17 192.168.100.6[49154] 671088647 ACTIVE FLOW
fe80:0:0:0:20c:29ff:fe85:3442[133]/58 ff02:0:0:0:0:0:0:2[0] 671088648 ACTIVE FLOW
192.168.101.101[3784]/17 192.168.101.6[49155] 671088649 ACTIVE FLOW 192.168.250.100[22]/6
192.168.200.100[48706] 671088650 ACTIVE FLOW 192.168.100.6[49154]/17 192.168.100.101[3784]
671088651 ACTIVE FLOW 192.168.101.6[49155]/17 192.168.101.101[3784]
```

- `show cluster-flow all filter count yes`

```
------------------------------------------------------------------------------ Slot 5
 ------------------------------------------------------------------------------ Number of
 sessions that match filter:11
 ------------------------------------------------------------------------------ Slot 6
 ------------------------------------------------------------------------------ Number of
 sessions that match filter:11
```

- `show cluster-membership show-slot-info slot all`

```
MP leader status:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State
 ============================================================================== 1 CN-
GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP UP UP 2 CN-GW
 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 ::UP UP NA 6 CN-DB 192.168.23.104 ::UP UP NA
 7 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW
 192.168.23.82 192.168.24.81 UP UP UP
```

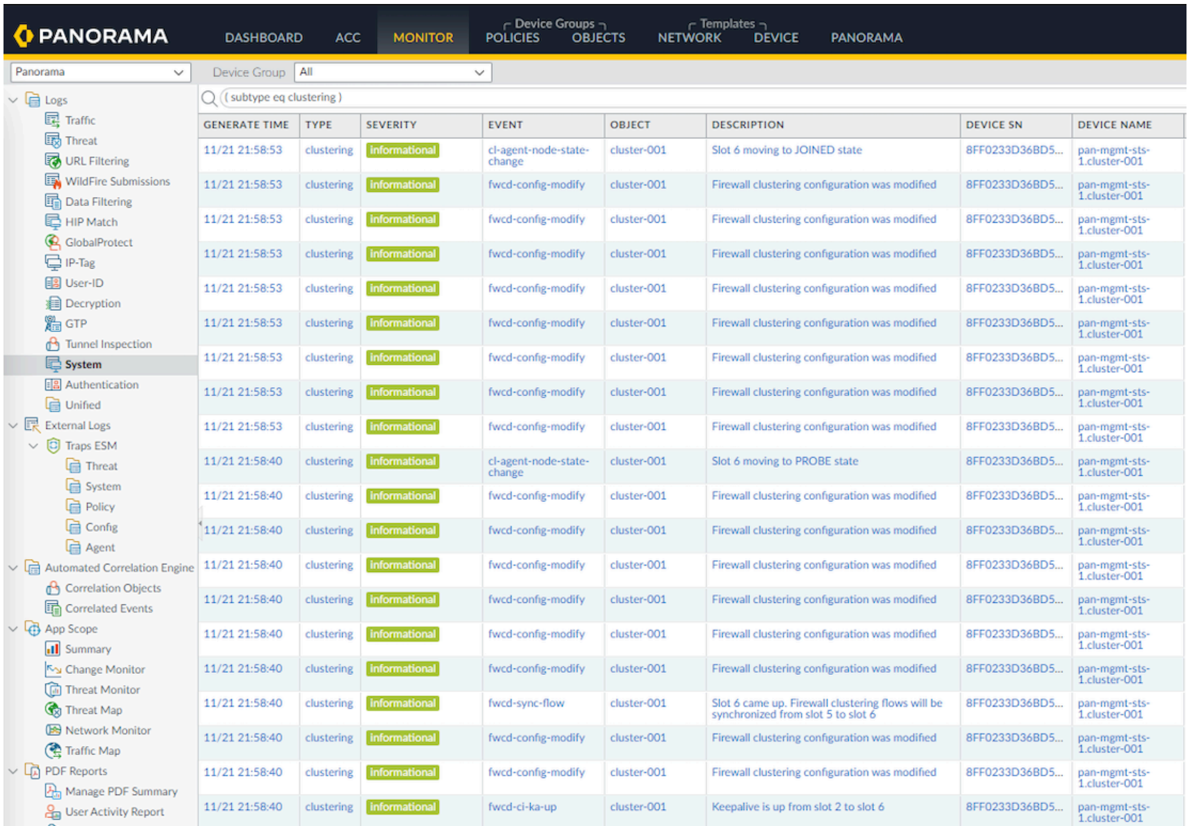
- 從 Panorama CLI

```
show clusters name cluster-001
```

```
Cluster: cluster-001 Creation time:2022/11/22 05:11:09 CN-MGMT pods:8FF0233D36BD57D
 (active, pan-mgmt-sts-1.cluster-001, connected, In Sync) 8F846238B0740D2
 (pan-mgmt-sts-0.cluster-001, connected, In Sync) Slot-ID PodName Type Version
 ------------------------------------------------------------------------------ 5 pan-db-
dep-7b6f6c5458-5fgnr CN-DB 11.0.1-c156.dev_e_rel 1 pan-gw-dep-748cdb856d-4f66g CN-GW 11.0.1-c156.dev_e_rel
 2 pan-gw-dep-748cdb856d-p5qdd CN-GW 11.0.1-c156.dev_e_rel 7 pan-ngfw-dep-56cdfdd656-srmdt CN-NGFW 11.0.1-
c156.dev_e_rel 8 pan-ngfw-dep-56cdfdd656-hvcw2 CN-NGFW 11.0.1-c156.dev_e_rel 9 pan-ngfw-dep-56cdfdd656-
```

```
bjtmd CN-NGFW 11.0.1-c156.dev_e_rel 10 pan-ngfw-dep-56cdfdd656-6jq2f CN-NGFW 11.0.1-c156.dev_e_rel 6 pan-db-
dep-7b6f6c5458-r449b CN-DB 11.0.1-c156.dev_e_rel
```

您可以在 **Monitor**（監控） > **Logs**（日誌） > **System**（系統）下方的 Panorama 網頁介面中檢視 CN-DB 變更



結果：

不會影響現有或新工作階段。Panorama 上已更新的叢集成員資格。

CN-Series 上不支援的功能

除非下面另有說明，否則 CN-Series 無法使用 PAN-OS 上支援的下列功能：

功能	DaemonSet	K8s 服務	CNF 模式	HSF 模式
驗證	否。	否。	否。	否。
日誌至 Cortex Data Lake	否。	否。	否。	否。
企業 DLP	否。	否。	否。	否。
非 vWire 介面	否。	否。	是	是
IoT Security	否。	否。	否。	否。
IPv6	是	否。	是	否。
NAT	否。	否。	是	否。
基於原則的轉送	否。	否。	是	否。
QoS	否。	否。	否。	否。
SD-WAN	否。	否。	否。	否。
使用者-ID	否。	否。	否。	否。
WildFire 內嵌 ML	否。	否。	否。	否。
SaaS 內嵌	否。	否。	否。	否。
IPSec	否。	否。	否。	否。
通道內容檢查	否。	否。	否。	否。