paloalto TECHDOCS

CN-Series 入門

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

August 25, 2023

Table of Contents

Kubernetes 的 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 對於使用 Helm 的 CN-Series 部署

Palo Alto Networks 容器原生防火牆 (CN-Series) 原本整合至 Kubernetes (k8s)，提供完整 L7 可見度、應用程式層級區隔、DNS 安全性，以及保護流過公用雲端或資料中心環境內信任區域之流量的進階威脅。它可讓您隔離與保護工作負載、應用程式堆疊和服務，即使個別容器擴大、縮小或跨主機也是一樣，並持續套用根據 Kubernetes 標籤的安全性原則。

Kubernetes 環境中的應用程式部署是動態的，而且容器生命週期通常會涉及下列團隊：

- **Platform (PAAS) Admin**（平台 **(PAAS)** 管理員）—管理公用雲端和資料中心內的 Kubernetes 叢集和其他基礎架構元件。
- **App Teams**（應用程式團隊）—在 PAAS 管理員所提供的 Kubernetes 命名空間/專案中部署其個別容器化和其他應用程式。
- **Security Admin**（安全性管理員）—佈建整個部署的安全性，包括 Kubernetes 叢集和個別容器化應用程式。

在此動態案例中，以及與多個團隊的相互作用下，安全性管理和監視深具挑戰。CN-Series 可讓安全性管理員佈建跨大範圍環境之容器化應用程式的安全性，包括「雲端提供者受管理 k8s」（例如 GKE、EKS、AKS、AliCloud ACK）和「客戶受管理 k8s」（例如 Openshift），以及公用雲端或內部部署資料中心上的「原生 k8s」。CN-Series 使用 Kubernetes 建構和中繼資料驅動原則，讓團隊可以將部署自動化，以及有效率地強制執行安全性原則來持續地防止已知和未知威脅。

使用 CN-Series 防火牆保護 Kubernetes 工作負載

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

CN-Series 防火牆會部署為兩組 Pod：一組用於管理平面 (CN-MGMT)，另一組用於防火牆資料平面 (CN-NGFW)。防火牆資料平面以 daemon 集執行，讓 Kubernetes 內的單一命令能一次在 Kubernetes 叢集中的所有節點上部署防火牆。管理平面以 Kubernetes 服務執行。

CN-Series 防火牆透過 Panorama 主控台進行管理。Panorama 中的 Kubernetes 外掛程式會提供環境中容器的相關資訊，進而順暢啟用基於內容的網路安全性政策。

例如，Kubernetes 命名空間可用於定義防火牆政策中的流量來源。您可以在內部部署或公共雲端託管的 Kubernetes 環境中部署 CN-Series 防火牆。

CN-Series 防火牆也可以部署到雲端管理的 Kubernetes 產品中，包括 Google Kubernetes Engine (GKE®)、Azure Kubernetes Service (AKS)、Alibaba Cloud (ACK) 和 Amazon Elastic Kubernetes Service (EKS)。您也可以透過 Kubernetes 套件管理員（例如 Helm）進行部署。

CN-Series 提供容器信任區域與其他工作負載類型之輸入、輸出和東西向流量的威脅防護，而不讓開發速度變慢。

部署 CN-Series 的容器流量第 7 層可見度，並使用威脅防護設定檔來強制執行安全性原則，以保護跨 Kubernetes 命名空間界限的允許流量，以及使用硬體和 VM-Series 防火牆來共用該內容，確保跨整個混合雲端環境的一致原則強制執行模型。

Prevent Data Exfiltration from Kubernetes Environments（防止資料從 **Kubernetes** 環境外洩）：

CN-Series 防火牆提供多種安全功能，可防止敏感資料從 Kubernetes 環境外洩。流量內容檢查（包括 TLS/SSL 加密流量檢查）可確實識別並修復包含惡意負載的封包。URL 篩選會阻止與潛在惡意網站（包括惡意程式碼儲存庫）的輸出連線。

Prevent Lateral Spread of Threats Across Kubernetes Namespace Boundaries（防止威脅跨 **Kubernetes** 命名空間橫向傳播）：

應用程式之間的信任界限是執行分割政策以防止威脅橫向移動的邏輯位置。在許多 Kubernetes 環境中，Kubernetes 命名空間即為信任界限。CN-Series 防火牆可以在 Kubernetes 命名空間之間以及 Kubernetes 命名空間與其他工作負載類型（例如 VM 和裸機伺服器）之間實施威脅防禦政策，以阻止威脅在雲端原生應用程式和舊架構之間移動。

CN-Series 重要概念

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

CN-Series 防火牆旨在提供保護容器化環境中應用程式安全所需的工具。若要瞭解 CN-Series 如何融入容器化網路，請務必瞭解一些重要概念。

- 叢集—您容器化環境的基礎；您所有的容器化應用程式都在叢集上執行。
- 節點—根據叢集，節點可能是虛擬機器或實體機器，其中包含 Pod 所需的必要服務。
- **Pod**—您可以在 Kubernetes 中部署和管理的最小可部署運算單元。在分散式 PAN-OS 架構中，將 CN-Series 防火牆部署為兩個 Pod：CN-MGMT 和 CN-NGFW。如需詳細資訊，請參閱「CN-Series 核心建置區塊」。
- 命名空間—命名空間是實體叢集所支援的虛擬叢集。在多個使用者分散到多個團隊和函數的環境中，可以使用命名空間在單一叢集中將它們分開。
- 容器網路介面 **(CNI)**—設定容器網路介面的外掛程式。此外，CNI 還會移除在刪除容器時用於網路連線的已配置資源。
- **DaemonSet**—在 Kubernetes 部署中，DaemonSet 確保部分或所有節點都執行特定 Pod 的複本。將節點新增至 Kubernetes 叢集時，會將 DaemonSet 所定義的 Pod 複本新增至每個新的節點。當您將 CN-Series 防火牆部署為 DaemonSet 時，叢集的每個節點上都會部署一個 CN-NGFW Pod 複本（每個 CN-MGMT 配對最多 30 個）。
- **Kubernetes** 服務—將一組 Pod 上執行之應用程式公開為網路服務的抽象概念。當您將 CN-Series 部署為服務時，部署的 CN-NGFW Pod 數目是由您在設定 yaml 檔案時所定義。
- **Kuberenetes CNF-** 部署「CN-series 作為 Kubernetes-CNF」可解決透過雲端提供者的原生路由、vRouters 和機架頂部 (TOR) 交換器這類外部實體來使用服務函數鏈結 (SFC) 的流量的相關挑戰。「CN-series 作為 Kubernetes-CNF」部署模式不會影響應用程式 Pod。
- **Horizontal Pod Autoscaler (HPA)**（水平 **Pod** 自動調整規模器 **(HPA)**）—根據 CPU 使用率或工作階段使用率這類各種度量，自動調整部署、複本集或具狀態集中的 Pod 數目。

  CN-Series 僅支援 *HPA* 僅作為 *Kubernetes* 服務。

- **HSF**—Palo Alto Networks CN-Series Hyperscale Security Fabric (HSF) 1.0 是容器化新世代防火牆叢集，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新世代防火牆解決方案。

CN-Series 核心建置區塊

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

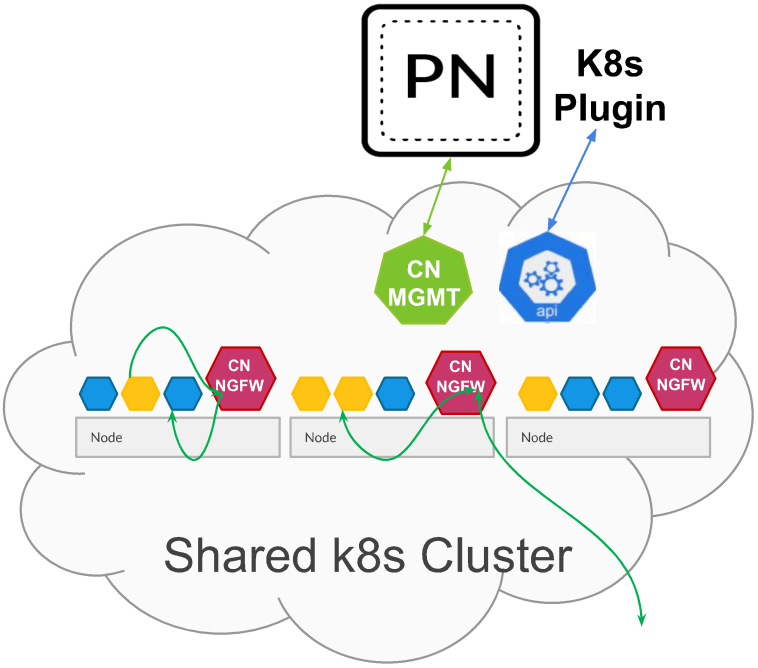
CN-Series 防火牆是容器化新一代防火牆，可提供 Kubernetes 叢集上容器化應用程式工作負載的可見度和安全性。CN-Series 防火牆使用原生 Kubernetes (K8s) 建構和 Palo Alto Networks 元件來執行這項作業。

部署 CN-Series 防火牆的核心建置組塊：

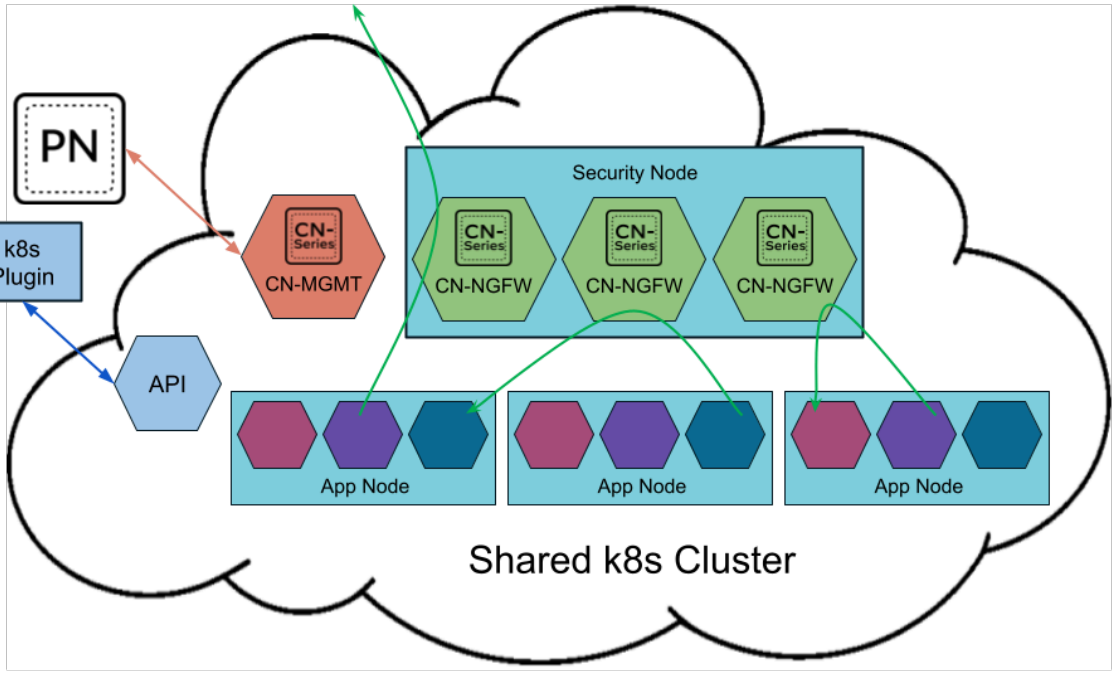
- **CN-Series** 部署檔案—若要在容器化環境中部署 CN-Series，您必須下載並部署各種 CN-Series 部署檔案。
  - PAN-CN-MGMT—init 容器會產生憑證，以用於保護 CN-MGMT Pod 執行個體之間以及 CN-MGMT Pod 與 CN-NGFW Pod 之間的通訊。
  - PAN-CN-MGMT-CONFIGMAP
  - PAN-CN-MGMT-SECRET—可讓 Panorama 驗證防火牆，以將每個防火牆新增為受管理的裝置。部署留存期需要 VM 驗證金鑰。如果連線要求缺少有效金鑰，則 CN-Series 防火牆將無法向 Panorama 註冊。
  - PAN-CN-NGFW
  - PAN-CN-NGFW-CONFIGMAP
  - PAN-CNI
  - PAN-CNI-CONFIGMAP
  - PAN-CNI-MULTUS
- 具有 **CN-MGMT** 和 **CN-NGFW Pod** 的分散式 **PAN-OS** 架構—容器化防火牆的管理平面 (CN-MGMT) 和資料平面 (CN-NGFW) 不同，可啟用應用程式的較佳執行時期保護，以及支援較小的涵蓋範圍。CN-MGMT 和 CN-NGFW 是搭配使用容器映像檔和 YAML 資訊清單檔案與 ConfigMap 物件所部署。
- **CN-MGMT** 執行為 StatefulSet，確保它具有永久性磁碟區，而且公開為 Kubernetes 環境中可使用 DNS 找到的 K8s 服務。CN-MGMT 提供容錯，而且單一 CN-MGMT Pod 可以管理 CN-MGMT Pod 重新啟動或失敗時的現有 CN-NGFW Pod。

- **CN-NGFW** 可以部署為 DaemonSet 或 Kubernetes 服務。DaemonSet 部署適用於節點、Pod 較大的 Kubernetes 環境，而且需要低延遲，以及/或需要高防火牆容量。「CN-Series 作為 Kubernetes 服務」適用於節點較小的 Kubernetes 環境，以及/或需要更動態的防火牆。
  - 部署 **as a DaemonSet**（為 **DaemonSet**）時，CN-NGFW Pod 的每個執行個體都可以保護在同一個節點上執行的 30 個應用程式 Pod。此架構可讓您在每個節點上放置您要保護叢集中工作

負載的 CN-NGFW DaemonSet Pod，而且一對 CN-MGMT Pod 可以在叢集內連線並管理最多 30 個 CN-NGFW Pod。如需限制的詳細資訊，請參閱 CN-Series 效能和調整規模。



- 部署 **as a Kubernetes Service**（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。



- 進行網路插入的 **PAN-CNI** 外掛程式—PAN-CNI 外掛程式負責在每個 Pod 上配置網路介面，而這會啟用與 CN-NGFW Pod 的網路連線。可讓您部署 CN-Series 的 YAML 檔案包括 PAN-CNI DaemonSet，而這會將 PAN-CNI 外掛程式插入至叢集內每個節點上的 CNI 外掛程式鏈。此外掛程式會在需要判斷是否啟用安全性時讀取每個應用程式 Pod 的註釋，並將流量在輸入和輸出 Pod 時重新導向至 CN-NGFW Pod 進行檢查。

- 進行集中管理的 **Panorama**—Panorama 作為中樞，以管理容器化防火牆的設定和授權。它也會管理 Kubernetes 外掛程式，以啟用 Kubernetes 叢集的監視以及集中「安全性」原則管理。您可以使用實體或虛擬 Panorama 設備，並將它部署至內部部署或公用雲端環境中。Panorama 必須具有防火牆管理平面 Pod (CN-MGMT) 的網路連線，確保它可以授權 (CN-NGFW) 防火牆並使用 Panorama 範本和裝置群組來推送設定和原則。Palo Alto Networks 建議在 HA 設定中部署 Panorama。

  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。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。您也可以使用社群支援的範本，以利用 Helm 和 Terraform 來部署 CN-Series。

- **Panorama** 上的 **Kubernetes** 外掛程式—Kubernetes 外掛程式管理 CN-Series 防火牆的授權。授權是根據您選擇配置給 CN-NGFW Pod 的核心數目。每個 CN-NGFW Pod 都會使用一個授權權杖，而且，在您啟用驗證碼之後，會在 Panorama 本機管理權杖，以及從 Palo Alto Networks 授權伺服器擷取指定數目的權杖。在 Kubernetes 節點上啟動每個 CN-NGFW 時，Panorama 會在本機散佈授權權杖。

  Panorama 上的 Kubernetes 外掛程式也可讓您監視叢集，以及利用您用來組織 Kubernetes 物件（例如 Pod、服務、部署以及相關聯的識別屬性）的 Kubernetes 標籤，讓您可以建立內容感知「安全性」原則規則。Kubernetes 外掛程式會與 API 伺服器通訊，並以接近即時的速度來擷取中繼資料以查看叢集內執行的應用程式。Kubernetes 外掛程式會收集 Kubernetes 叢集中的命名空間、服務和標籤來建立叢集內相關聯物件之 IP 位址與標記對應的標記，接著可以將它們用於安全性原則。如需更多詳細資訊，請參閱 Kubernetes 屬性的 IP 位址與標記對應。

  它也會收集應用程式 YAML 中所指定連接埠的相關資訊，以及建立「服務物件」。

  雖然會與每個叢集中的 CN-NGFW Pod 自動共用這些標記和服務物件，但是您也可以啟用與硬體型或 VM-Series 防火牆共用標記和服務物件。標記可作為「動態位址群組」中的比對準則，而您接著可以用來保護 Pod 或命名空間之間、流向網際網路公開服務或輸出連線的流量。

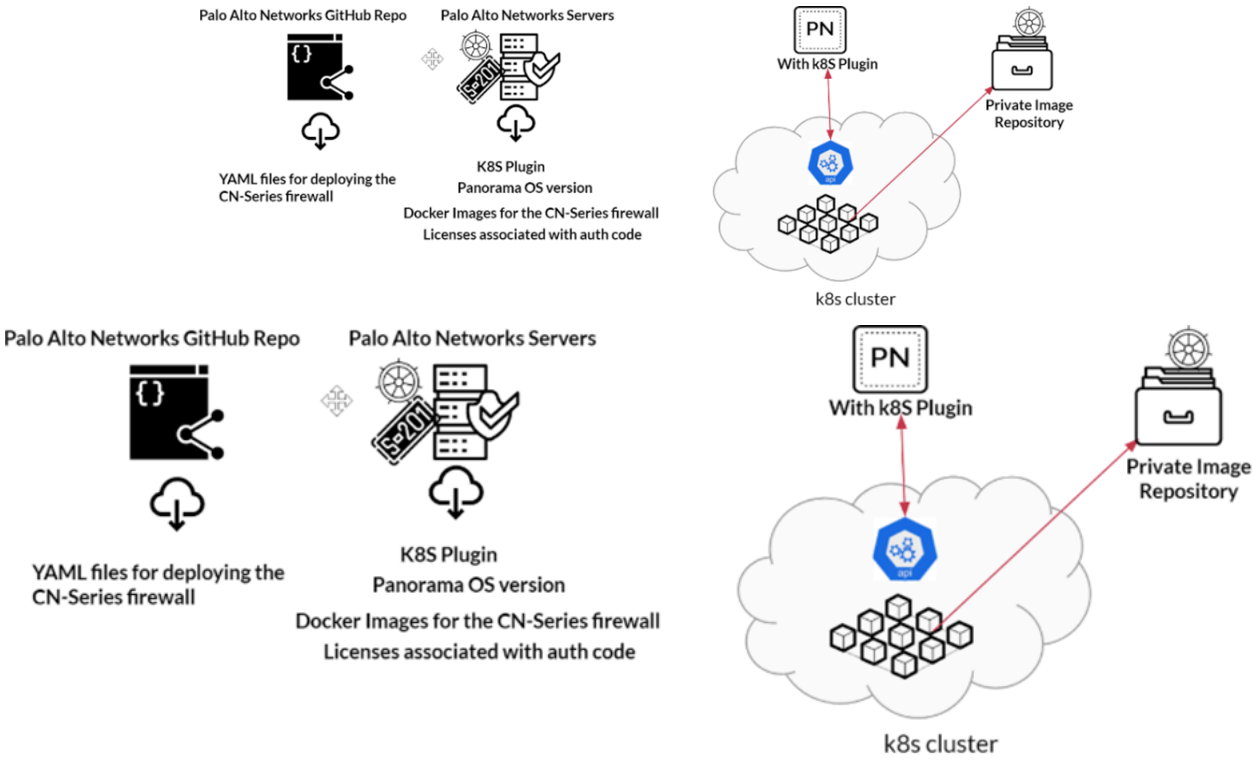
  Palo Alto Networks 建議在 HA 設定中部署 Panorama，以在失敗時，讓 Panorama 對等節點持續接收 IP 位址更新。如果您部署單一 Panorama 執行個體，則失敗時，來自任何現有應用程式 Pod 的流量不受影響，而且會在 CN-NGFW Pod 上強制執行目前原則。啟動新的 Pod 時，所有具有來源「ANY」的規則都會符合這個新 Pod，而且將會根據原則規則允許或封鎖來自這個新 Pod 的流量。例如，如果有「反間諜程式」原則規則可封鎖從任何 來源到外部世界的輸出存取權，則此規則將會套用至新 Pod，而且設定檔可以保護流量。如果具有預設拒絕 規則，將會拒絕來自此新 Pod 的流量。

  您可以使用 *Kubernetes* 外掛程式，將 *Kubernetes* 叢集內部署的 *Pod*、節點、命名空間和服務的 *IP* 位址與標記對應散佈至實體或 *VM-Series* 防火牆，即使您尚未在該叢集中部署 *CN-Series* 防火牆也是一樣。

使用 CN-Series 防火牆保護 Kubernetes 叢集所需的元件

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



下列是您部署 CN-Series 防火牆和保護 Kubernetes 叢集內部署之應用程式的所需項目。

- **Panorama**—一個硬體型或虛擬設備，可連線至已部署應用程式和 CN-Series 防火牆的 Kubernetes 叢集。CN-Series 防火牆授權管理和設定管理需要 Panorama。如需詳細資訊，請參閱 CN-Series 核心建置區塊。
- **Panorama** 上的 **Kubernetes** 外掛程式—因為容器化應用程式的變更率，所以需要此外掛程式才能查看叢集內的容器活動，以及管理叢集內每個節點上部署之防火牆的授權權杖配置。

  Kubernetes 外掛程式會使用服務帳戶認證來連線至 Kubernetes 叢集。在這裡，它會擷取資源屬性和標籤，以及建立標記和服務物件。這些標記可以用來建立「動態位址群組」，並在「安全性」原則中參照它們以進行 IP 流量強制執行。您也可以在「安全性」原則中使用服務物件，以根據連接埠和 IP 位址來允許或拒絕流量。標記和服務物件可讓您查看和細微地控制 Kubernetes 叢集內的流量強制執行。

- **Docker** 映像檔—為了支援分散式架構，CN-Series 防火牆具有 Palo Alto Networks 入口網站上可用的四個 Docker 映像。這些映像檔會發佈為三個壓縮 tar 封存檔（tar.gz 格式），而且您必須將這些映像檔解壓縮，以及對映像檔登錄執行 Docker 推送。

  註：請確定映像檔與 YAML 檔案版本相容。壓縮檔案為：

  - **PanOS_cn-10.1.0.tgz**—此封存檔包括防火牆管理平面 (CN-MGMT) 和防火牆資料平面 (CN-NGFW) 映像檔。

    例如，解壓縮的映像檔名稱為：`panos_cn_ngfw:10.1.0-b7` 和 `panos_cn_mgmt:10.1.0-b7`

    - **Pan_cn_mgmt_init-2.0.0.tgz**—此封存檔包括 init 容器 (CN-INIT)，其中包含在防火牆上部署管理平面所需的公用程式。init 容器會啟用 CN-MGMT 與 CN-NFGW Pod 之間的安全 IPSec 通訊。例如，解壓縮的映像檔名稱為：`pan_cn_mgmt_init:1.0.0-b1-c1`。
    - **Pan_cni-2.0.0.tgz**—此封存檔包括可啟用 CN-MGMT 與 CN-NFGW 之間連線的 CNI 外掛程式，以及在應用程式 Pod 上重新設定網路介面，以將流量重新導向至每個節點上的 CN-NGFW Pod。例如，解壓縮的映像檔名稱為：`pan_cni:2.0.0`。

上面列出的映像檔名稱是範例，將會變更以反映最新版本。您可以在 Palo Alto Networks 入口網站上找到最新映像。

- **YAML Files**（**YAML** 檔案）—YAML 檔案包含用於在 Kubernetes 叢集中部署資源的必要欄位和物件規格，並且在 GitHub 上進行發佈。

  您需要的所有 YAML 欄位（適用於原生 Kubernetes 或 GKE 這類支援的環境）都會結合並壓縮為一個資料夾，以方便您使用。

  YAML 檔案是透過 *HELM* 圖表自動予以部署，這是部署 *CN-Series* 防火牆的建議方法。

  - CN-MGMT 有三個 YAML 檔案：`pan-cn-mgmt.yaml`、`pan-cn-mgmt-configmap.yaml`、`pan-cn-mgmt-secret.yaml`、`pan-cn-mgmt-slot-cr.yaml` 和 `pan-cn-mgmt-slot-crd.yaml`。
  - 「CN-NGFW 作為 DaemonSet」有兩個 YAML 檔案：`pan-cn-ngfw.yaml` 和 `pan-cn-ngfw-configmap.yaml`。除了先前提到的檔案之外，「CN-NGFW 作為 Kubernetes 服務」還具有 `pan-cn-ngfw-svc.yaml`。
  - CNI 外掛程式具有三個 YAML 檔案：`pan-cni-configmap.yaml` 和 `pan-cni.yaml` 或 `pan-cni-multus.yaml`。

    如果您要在 Multus CNI 作為 *meta-plugin* 且呼叫其他 CNI 外掛程式的環境上部署 CN-Series，則必須選擇 `pan-cni.yaml` 或 `pan-cni-multus.yaml`。

    在 OpenShift 上部署 CN-Series 時，預設會啟用 Multus，而 pan-cni.yaml 就已足夠。然而，如果您要在支援 Multus CNI 但為選用的環境（例如具有自我管理（原生）環境）上部署 CN-Series，則請使用 pan-cni-multus.yaml，而非 pan-cni.yaml。

    - 也會有下面的服務帳戶建立小節中所參照的 *`pan-cni-serviceaccount.yaml`*。
    - 針對 *OpenShift* 部署，會有額外的 *`pan-cni-net-attach-def.yaml`*。
  - 服務帳戶建立—三個 YAML 檔案：`pan-mgmt-serviceaccount.yaml`、`pan-cni-serviceaccount.yaml` 和 `plugin-serviceaccount.yaml`。

    `pan-mgmt-serviceaccount.yaml` 和 `pan-cni-serviceaccount.yaml` 是供 CN-MGMT 和 CN-NGFW Pod 向叢集進行驗證。

    `plugin-serviceaccount.yaml` 是供 Panorama 上的 Kubernetes 外掛程式向叢集進行驗證。
  - **Persistent volume YAML for Native Kubernetes deployments**（原生 **Kubernetes** 部署的永久性磁碟區）—`pan-cn-pv-manual.yaml` 和 `pan-cn-pv-local.yaml`。

    `pan-cn-pv-manual.yaml` 是僅針對具有單一節點叢集的 PoC 所提供。Palo Alto Networks 強烈建議使用動態佈建的永久性磁碟區，來儲存 `pan-cn-mgmt.yaml` 中所參照 CN-MGMT Pod 的設定和日誌。針對這兩個 CN-MGMT Pod，請務必在叢集內設定永久性磁碟區。
- 授權驗證碼—驗證碼可讓您授權叢集內每個節點上部署的每個 CN-NGFW Pod 執行個體。

  授權驗證碼繫結至您在 Palo Alto Networks CSP 上建立的 CN-Series 部署設定檔。此外，它還會啟用您在建立部署設定檔時選取的任何安全性訂閱。

額外 CN-Series 資源

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

您可以使用下列資源進一步瞭解 CN-Series 防火牆，以及它如何協助您保護容器化網路的安全。

- CN-Series 防火牆—觀看這些影片，以了解 CN-Series 防火牆。
- CN-Series 的原因、內容和作法—Palo Alto Networks 即時社群上由三部分組成的部落格系列（含內嵌影片），描述 CN-Series 防火牆的原因、內容和作法。
- Palo Alto Network Qwiklab—使用 Palo Alto Networks Qwiklab 進行實驗室練習，並在 AWS 或 GCP 中嘗試 CN-Series 防火牆。
- Kubernetes 版本資訊的 Panorama 外掛程式—請閱讀版本資訊，瞭解 Kubernetes 的 Panorama 外掛程式最新版本所引進的功能和增強功能。
- PAN-OS 版本資訊—檢視 PAN-OS 版本資訊，以進一步瞭解最新版 PAN-OS 中引進的 CN-Series 功能和增強功能。
- Panorama 管理員指南—Panorama 這個介面用來與 Kubernetes 環境連線、管理所部署 CN-Series 防火牆，以及定義安全性政策。

CN-Series 系統需求

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

本章節介紹在 Kubernetes 叢集和內部部署環境中部署 CN-Series 防火牆的建議系統需求。

本節涵蓋下列項目：

- Kubernetes 叢集的 CN-Series 系統需求
- 內部部署 Kubernetes 部署的 CN-Series 系統需求
- CN-Series 效能和調整規模
- CN-Series 部署—支援的環境

Kubernetes 叢集的 CN-Series 系統需求

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

以下是使用多種支援模式部署 CN-Series 防火牆的建議系統需求。

- PAN-OS 10.1
- PAN-OS 10.2 和更新版本

PAN-OS 10.1

下表顯示在其上部署 CN-Series 之叢集的系統需求。這些值是 CPU、記憶體和磁碟儲存空間的一般指導方針；您部署的資源量可能會根據您的需求而不同。

「*CN-Series* 中型」不適用於「*CN-Series* 作為 *Daemonset*」。

資源	CN-MGMT-Small	CN-NGFW-Small	CN-MGMT-Medium	CN-NGFW-Medium	CN-MGMT-Large	CN-NGFW-Large
記憶體（最小值）	3GB	• 2 GB (Daemonset) • 2.5 GB（K8s 服務）	3GB	6GB	4GB	48GB
CPU（最小值）	2（建議）	2（建議）	2（建議）	4（建議）	4（建議）	12（建議）
CPU 最大值	不適用	31	不適用	31	不適用	31
磁碟	50GB	不適用	50GB	不適用	50GB	不適用

PAN-OS 10.2 和更新版本

只有 Daemonset 和 Kubernetes CNF 模式才支援 5G-Native 安全性。

CN-MGMT 和 *CN-NGFW* 的記憶體與核心組合分別適用於「小型」、「中型」和「大型」。與 *CN-MGMT* 相關的「小型」、「中型」與「大型」組合會直接對應至各自的 *CN-NGFW*。

表 **1:** 建議的 **CN-Series** 系統和容量矩陣

CN 模式	資源	小型	中	中	中	大	大
Daemonset	最小 CN-MGMT 記憶體	3G	3G	4G	4G	16G	16G
	最小 CN-NGFW 記憶體	2G	6.5G	16G	32G	48G	56G
	建議的 CN-MGMT 核心	2	2	2	4	8	12
	最大 CN-NGFW 核心	2	4	8	16	31	47
	磁碟	52Gi	52Gi	52Gi	52Gi	52Gi	52Gi
	DPDK 巨型分頁大小	不適用	不適用	不適用	不適用	不適用	不適用
Kubernetes 服務	最小 CN-MGMT 記憶體	3G	3G	4G	4G	16G	16G
	最小 CN-NGFW 記憶體	4G	6.5G	16G	32G	48G	56G
	建議的 CN-MGMT 核心	2	2	2	4	8	12

CN 模式	資源	小型	中	中	中	大	大
	最大 CN-NGFW 核心	2	4	8	16	31	47
	磁碟	52Gi	52Gi	52Gi	52Gi	52Gi	52Gi
	DPDK 巨型分頁大小	不適用	不適用	不適用	不適用	不適用	不適用
Kubernetes CNF	最小 CN-MGMT 記憶體	3G	3G	4G	4G	16G	16G
	最小 CN-NGFW 記憶體	2G	6.5G	16G	32G	48G	56G
	建議的 CN-MGMT 核心	2	2	2	4	8	12
	最大 CN-NGFW 核心	2	4	8	16	31	47
	磁碟	52Gi	52Gi	52Gi	52Gi	52Gi	52Gi
	DPDK 巨型分頁大小	1G	1G	2G	2G	4G	4G

內部部署 Kubernetes 部署的 CN-Series 系統需求

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

請檢閱下列內部部署之部署的先決條件：

- 確定 Kubernetes 叢集中的所有節點都可以存取容器映像檔。
- 針對兩個 CN-MGMT Pod，設定叢集內的永久性磁碟區。因為主動管理 CN-NGFW Pod 的 CN-MGMT Pod 部署為 StatefulSet，所以這兩個執行個體都必須可以存取永久性磁碟區。

若要取得 *Rancher* 叢集的 *SSH* 存取權，您必須確保將 *kubeconfig* 檔案的內容複製至 `/.kube/config` 位置下，然後只有您才能為您的叢集執行 *kubectl* 命令。

此外，您還應該確定系統上已安裝 *Kubernetes* 命令列工具 *kubectl*。如需詳細資訊，請參閱安裝工具。

對於具有 *Rancher* 支援的 *CN-Series*，在下列主節點上安裝 *Docker*：*Ubuntu 18.0.4 LTS VM*、含 *8* 個 *vCPU* 和 *32G* 記憶體，且最少有 *200G* 磁碟。如需詳細資訊，請參閱在 Ubuntu 18.04 上安裝 Docker。

對於 *Ubuntu 18.0.4*，應該使用下列命令將機器上的核心更新為最新核心：

```
sudo apt install linux-generic-hwe-18.04 -y
```

CN-Series 效能和調整規模

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

下列各節列出使用 CN-Series 防火牆保護 Kubernetes 工作負載所需之不同元件的規模數字：

- CN-Series 元件上支援的規模
- Panorama 上 Kubernetes 外掛程式所支援的規模
- CN-Series 關鍵效能度量

CN-Series 元件上支援的規模

如需 CN-Series CPU、記憶體和磁碟儲存空間定義的相關資訊，請參閱 Kubernetes 叢集的 CN-Series 系統需求。

下表依 CN-Series 大小來區隔一些資料：小型、中型和大型。這些 CN-Series 大小具有下列記憶體值：

- **CN-Series** 小型—最低 2.5G CN-NGFW 和 3G 的 CN-MGMT
- **CN-Series Medium**（**CN-Series** 中型）—最低 6G 的 CN-NGFW 和 3G 的 CN-MGMT
- **CN-Series** 大型—最低 42G 的 CN-NGFW 和 4G 的 CN-MGMT

屬性	**CN-Series** 規模 **(DaemonSet)**	**CN-Series** 規模 **(K8s** 服務**)**	**CN-Series** 規模 **(K8s-CNF)**
每個 K8s 叢集的最大 CN-MGMT 配對	主動/被動 HA 模式中的 4 個 CN-MGMT 配對	主動/被動 HA 模式中的 4 個 CN-MGMT 配對	主動/被動 HA 模式中的 4 個 CN-MGMT 配對
每個 CN-MGMT 配對的最大 CN-NGFW Pod	30	30	30
CN-NGFW 所保護的 Kubernetes Pod（每個 K8s 節點）	30（PAN-OS 10.1.8 或更早版本）	無	不適用

屬性	CN-Series 規模 (DaemonSet)	CN-Series 規模 (K8s 服務)	CN-Series 規模 (K8s-CNF)
	125（已安裝 k8s 2.0.2 的 PAN-OS 10.1.9 和以上版本）	此部署模式與 *K8s* 節點上的應用程式 *Pod* 數目無關。	此部署模式與 *K8s* 節點上的應用程式 *Pod* 數目無關。
每個 CN-NGFW 的最大 TCP/IP 工作階段數目	CN-Series 小型：20,000 CN-Series 中型：819,200 CN-Series 大型：10,000,000	CN-Series 小型：250,000 CN-Series 中型：819,200 CN-Series 大型：10,000,000	CN-Series 小型：250,000 CN-Series 中型：819,200 CN-Series 大型：10,000,000
最大動態位址群組 IP 位址* 每個 CN-MGMT 配對	CN-Series 小型：2500（PAN-OS 10.0.6 和更早版本） 10,000（PAN-OS 10.0.7 和更新版本）	CN-Series 小型：2500（PAN-OS 10.0.6 和更早版本） 10,000（PAN-OS 10.0.7 和更新版本） CN-Series 中型：200,000 CN-Series 大型：300,000	CN-Series 小型：2500（PAN-OS 10.0.6 和更早版本） 10,000（PAN-OS 10.0.7 和更新版本） CN-Series 中型：200,000 CN-Series 大型：300,000
每個 IP 位址的標記* 每個 CN-MGMT 配對	32	32	32
最大安全性地區	CN-Series 小型：2 CN-Series 中型：40 CN-Series 大型：200	CN-Series 小型：2 CN-Series 中型：40 CN-Series 大型：200	CN-Series 小型：2 CN-Series 中型：40 CN-Series 大型：200
安全性設定檔	CN-Series 小型：38 CN-Series 中型：375 CN-Series 大型：750	CN-Series 小型：375 CN-Series 中型：375 CN-Series 大型：750	CN-Series 小型：375 CN-Series 中型：375 CN-Series 大型：750

屬性	CN-Series 規模 (DaemonSet)	CN-Series 規模 (K8s 服務)	CN-Series 規模 (K8s-CNF)
最大介面數	針對 **PAN OS 10.1.8** 或更早版本： CN-Series 小型：30 CN-Series 中型：30 CN-Series 大型：30 針對已安裝 **k8s 2.0.2** 的 **PAN-OS 10.1.9** 和以上版本： CN-Series 小型：250 CN-Series 中型：250 CN-Series 大型：250	CN-Series 小型：2 CN-Series 中型：2 CN-Series 大型：2	CN-Series 小型：60 CN-Series 中型：60 CN-Series 大型：60

*請參閱防火牆比較工具。

政策	CN-Series 小型 （最低 2.5G 的 CN-NGFW 和最低 3G 的 CN-MGMT）	CN-Series 中型 （最低 6G 的 CN-NGFW 和最低 2G 的 CN-MGMT）	CN-Series 大型 （最低 42G 的 CN-NGFW 和低 4G 的 CN-MGMT）
安全性規則	1500	10,000	20,000
安全性規則排程	256	256	256
NAT 規則 *CNF* 模式上支援 *NAT* 規則。	無	不適用	不適用
解密規則	1000	1000	2000
應用程式取代規則	1000	1000	2000
通道內容檢查規則	100	500	2000

政策	**CN-Series** 小型 （最低 **2.5G** 的 **CN-NGFW** 和最低 **3G** 的 **CN-MGMT**）	**CN-Series** 中型 （最低 **6G** 的 **CN-NGFW** 和最低 **2G** 的 **CN-MGMT**）	**CN-Series** 大型 （最低 **42G** 的 **CN-NGFW** 和低 **4G** 的 **CN-MGMT**）
SD-WAN 規則	不適用	不適用	不適用
基於政策的轉送規則 *CNF* 模式上支援政策型轉送規則。	無	不適用	不適用
被控制的入口網站規則	不適用	不適用	不適用
DoS 防護規則	• 100 (DaemonSet) • 1000（K8s 服務）	1000	1000

物件（位址和服務）	**CN-Series** 小型 （最低 **2.5G** 的 **CN-NGFW** 和最低 **3G** 的 **CN-MGMT**）	**CN-Series** 中型 （最低 **6G** 的 **CN-NGFW** 和最低 **2G** 的 **CN-MGMT**）	**CN-Series** 大型 （最低 **42G** 的 **CN-NGFW** 和低 **4G** 的 **CN-MGMT**）
位址物件	10,000	10,000	40,000
位址群組	1000	1000	4000
每個位址群組的成員	2500	2500	2500
服務物件	2000	2000	5000
服務群組	500	500	500
每個服務群組的成員	500	500	500
FQDN 位址物件	2000	2000	2000
最大動態位址群組 IP 位址	2500	200,000	300,000

物件（位址和服務）	**CN-Series** 小型 （最低 **2.5G** 的 **CN-NGFW** 和最低 **3G** 的 **CN-MGMT**）	**CN-Series** 中型 （最低 **6G** 的 **CN-NGFW** 和最低 **2G** 的 **CN-MGMT**）	**CN-Series** 大型 （最低 **42G** 的 **CN-NGFW** 和低 **4G** 的 **CN-MGMT**）
每個 IP 位址的標籤	32	32	32

App-ID	**CN-Series** 小型 （最低 **2.5G** 的 **CN-NGFW** 和最低 **3G** 的 **CN-MGMT**）	**CN-Series** 中型 （最低 **6G** 的 **CN-NGFW** 和最低 **2G** 的 **CN-MGMT**）	**CN-Series** 大型 （最低 **42G** 的 **CN-NGFW** 和低 **4G** 的 **CN-MGMT**）
自訂 App-ID 簽名	6000	6000	6000
共用的自訂 App-ID	512	512	512
自訂 App-ID（虛擬系統專用）	6416	6416	6416

SSL 解密	**CN-Series** 小型 （最低 **2.5G** 的 **CN-NGFW** 和最低 **3G** 的 **CN-MGMT**）	**CN-Series** 中型 （最低 **6G** 的 **CN-NGFW** 和最低 **2G** 的 **CN-MGMT**）	**CN-Series** 大型 （最低 **42G** 的 **CN-NGFW** 和低 **4G** 的 **CN-MGMT**）
SSL 輸入憑證數目上限	1000	1000	1000
SSL 憑證快取（轉寄 Proxy）	128	2000	8000
並行解密工作階段數目上限	• 1024 (DaemonSet) • 6400（K8s 服務）	15,000	100,000
SSL 連接埠鏡像	否。	否。	否。
SSL 解密代理	否。	否。	否。
支援 HSM	否。	否。	否。

URL 篩選	CN-Series 小型 （最低 2.5G 的 CN-NGFW 和最低 3G 的 CN-MGMT）	CN-Series 中型 （最低 6G 的 CN-NGFW 和最低 2G 的 CN-MGMT）	CN-Series 大型 （最低 42G 的 CN-NGFW 和低 4G 的 CN-MGMT）
允許清單、封鎖清單和自訂類別的項目總數	25,000	25,000	100,000
自訂類別數目上限	• 500 (DaemonSet) • 2849（K8s 服務）	2849	2849
用於 URL 篩選的資料平面快取大小	• 5000 (DaemonSet) • 90,000（K8s 服務）	90,000	250,000
管理平面動態快取大小	100,000	100,000	600,000

EDL	CN-Series 小型 （最低 2.5G 的 CN-NGFW 和最低 3G 的 CN-MGMT）	CN-Series 中型 （最低 6G 的 CN-NGFW 和最低 2G 的 CN-MGMT）	CN-Series 大型 （最低 42G 的 CN-NGFW 和低 4G 的 CN-MGMT）
自訂清單數目上限	30	30	30
每個系統的 IP 數目上限	50,000	50,000	50,000
每個系統的 DNS 網域數目上限	50,000	500,000	2,000,000
每個系統的 URL 數目上限	50,000	100,000	100,000
最短檢查間隔（分鐘）	5	5	5

位址指派	**CN-Series** 小型 （最低 **2.5G** 的 **CN-NGFW** 和最低 **3G** 的 **CN-MGMT**）	**CN-Series** 中型 （最低 **6G** 的 **CN-NGFW** 和最低 **2G** 的 **CN-MGMT**）	**CN-Series** 大型 （最低 **42G** 的 **CN-NGFW** 和低 **4G** 的 **CN-MGMT**）
DHCP 伺服器	3	10	125
DHCP 轉送	否。	否。	否。
所指派位址數目上限	64,000	64,000	64,000

介面	**CN-Series** 小型 （最低 **2.5G** 的 **CN-NGFW** 和最低 **3G** 的 **CN-MGMT**）	**CN-Series** 中型 （最低 **6G** 的 **CN-NGFW** 和最低 **2G** 的 **CN-MGMT**）	**CN-Series** 大型 （最低 **42G** 的 **CN-NGFW** 和低 **4G** 的 **CN-MGMT**）
介面數目上限（邏輯和實體）	• 60 (DaemonSet) • 2（K8s 服務） • 2 (K8s-CNF)	• 60 (DaemonSet) • 2（K8s 服務） • 2 (K8s-CNF)	• 60 (DaemonSet) • 2（K8s 服務） • 2 (K8s-CNF)
管理 - 超出界限	不適用	不適用	不適用
管理 - 10/100/1000 高可用性	不適用	不適用	不適用
管理 - 40G 高可用性	不適用	不適用	不適用
管理 - 10G 高可用性	不適用	不適用	不適用
流量 - 10/100/1000	不適用	不適用	不適用
流量 - 100/1000/10000	不適用	不適用	不適用
流量 - 1G SFP	不適用	不適用	不適用
流量 - 10G SFP+	不適用	不適用	不適用
流量 - 40/100G QSFP+/QSFP28	不適用	不適用	不適用

介面	**CN-Series** 小型 （最低 **2.5G** 的 **CN-NGFW** 和最低 **3G** 的 **CN-MGMT**）	**CN-Series** 中型 （最低 **6G** 的 **CN-NGFW** 和最低 **2G** 的 **CN-MGMT**）	**CN-Series** 大型 （最低 **42G** 的 **CN-NGFW** 和低 **4G** 的 **CN-MGMT**）
每個裝置的 802.1q 標籤	不適用	不適用	不適用
每個實體介面的 802.1q 標籤	不適用	不適用	不適用
彙總介面數目上限	不適用	不適用	不適用
SD-WAN 虛擬介面數目上限	不適用	不適用	不適用

NAT	**CN-Series** 小型 （最低 **2.5G** 的 **CN-NGFW** 和最低 **3G** 的 **CN-MGMT**）	**CN-Series** 中型 （最低 **6G** 的 **CN-NGFW** 和最低 **2G** 的 **CN-MGMT**）	**CN-Series** 大型 （最低 **42G** 的 **CN-NGFW** 和低 **4G** 的 **CN-MGMT**）
NAT 規則容量總計	不適用	不適用	不適用
NAT 規則數目上限（靜態）	不適用	不適用	不適用
NAT 規則數目上限 (DIP)	不適用	不適用	不適用
NAT 規則數目上限 (DIPP)	不適用	不適用	不適用
已轉換 IP 數目上限 (DIP)	不適用	不適用	不適用
已轉換 IP 數目上限 (DIPP)	不適用	不適用	不適用
預設 DIPP 集區過度訂閱	不適用	不適用	不適用

使用者-ID	CN-Series 小型 （最低 2.5G 的 CN-NGFW 和最低 3G 的 CN-MGMT）	CN-Series 中型 （最低 6G 的 CN-NGFW 和最低 2G 的 CN-MGMT）	CN-Series 大型 （最低 42G 的 CN-NGFW 和低 4G 的 CN-MGMT）
IP-使用者對應（管理平面）	不適用	不適用	不適用
IP-使用者對應（資料平面）	不適用	不適用	不適用
政策中使用的作用中和唯一群組	不適用	不適用	不適用
User-ID 代理程式數目	不適用	不適用	不適用
User-ID 的受監控伺服器	不適用	不適用	不適用
終端機伺服器代理程式	不適用	不適用	不適用
每個使用者的標籤	不適用	不適用	不適用

路由	CN-Series 小型 （最低 2.5G 的 CN-NGFW 和最低 3G 的 CN-MGMT）	CN-Series 中型 （最低 6G 的 CN-NGFW 和最低 2G 的 CN-MGMT）	CN-Series 大型 （最低 42G 的 CN-NGFW 和低 4G 的 CN-MGMT）
IPv4 轉送表大小	不適用	不適用	不適用
IPv6 轉送表大小	不適用	不適用	不適用
系統總計轉送表大小	不適用	不適用	不適用
路由對等數目上限（取決於通訊協定）	不適用	不適用	不適用
靜態項目 - DNS Proxy	不適用	不適用	不適用
雙向轉送偵測 (BFD) 工作階段	不適用	不適用	不適用

L2 轉送	CN-Series 小型 （最低 2.5G 的 CN-NGFW 和最低 3G 的 CN-MGMT）	CN-Series 中型 （最低 6G 的 CN-NGFW 和最低 2G 的 CN-MGMT）	CN-Series 大型 （最低 42G 的 CN-NGFW 和低 4G 的 CN-MGMT）
每個裝置的 ARP 表格大小	不適用	不適用	不適用
IPv6 芳鄰表格大小	不適用	不適用	不適用
每個裝置的 MAC 表格大小	不適用	不適用	不適用
每個廣播網域的 ARP 項目數上限	不適用	不適用	不適用
每個廣播網域的 MAC 項目數上限	不適用	不適用	不適用

QoS	CN-Series 小型 （最低 2.5G 的 CN-NGFW 和最低 3G 的 CN-MGMT）	CN-Series 中型 （最低 6G 的 CN-NGFW 和最低 2G 的 CN-MGMT）	CN-Series 大型 （最低 42G 的 CN-NGFW 和低 4G 的 CN-MGMT）
QoS 政策數目	不適用	不適用	不適用
支援 QoS 的實體介面	不適用	不適用	不適用
每個實體介面的純文字節點	不適用	不適用	不適用
依政策的 DSCP 標記	不適用	不適用	不適用
支援的子介面	不適用	不適用	不適用

IPSec VPN	**CN-Series** 小型 （最低 **2.5G** 的 **CN-NGFW** 和最低 **3G** 的 **CN-MGMT**）	**CN-Series** 中型 （最低 **6G** 的 **CN-NGFW** 和最低 **2G** 的 **CN-MGMT**）	**CN-Series** 大型 （最低 **42G** 的 **CN-NGFW** 和低 **4G** 的 **CN-MGMT**）
IKE 對等數目上限	不適用	不適用	不適用
站台對站台（含 Proxy ID）	不適用	不適用	不適用
SD-WAN IPSec 通道	不適用	不適用	不適用

GlobalProtect	**CN-Series** 小型 （最低 **2.5G** 的 **CN-NGFW** 和最低 **3G** 的 **CN-MGMT**）	**CN-Series** 中型 （最低 **6G** 的 **CN-NGFW** 和最低 **2G** 的 **CN-MGMT**）	**CN-Series** 大型 （最低 **42G** 的 **CN-NGFW** 和低 **4G** 的 **CN-MGMT**）
GlobalProtect 用戶端 **VPN** 通道數目上限（含 XAUTH 的 SSL、IPSec、IKE）	不適用	不適用	不適用
GlobalProtect 無用戶端 **VPN** SSL 通道數目上限	不適用	不適用	不適用

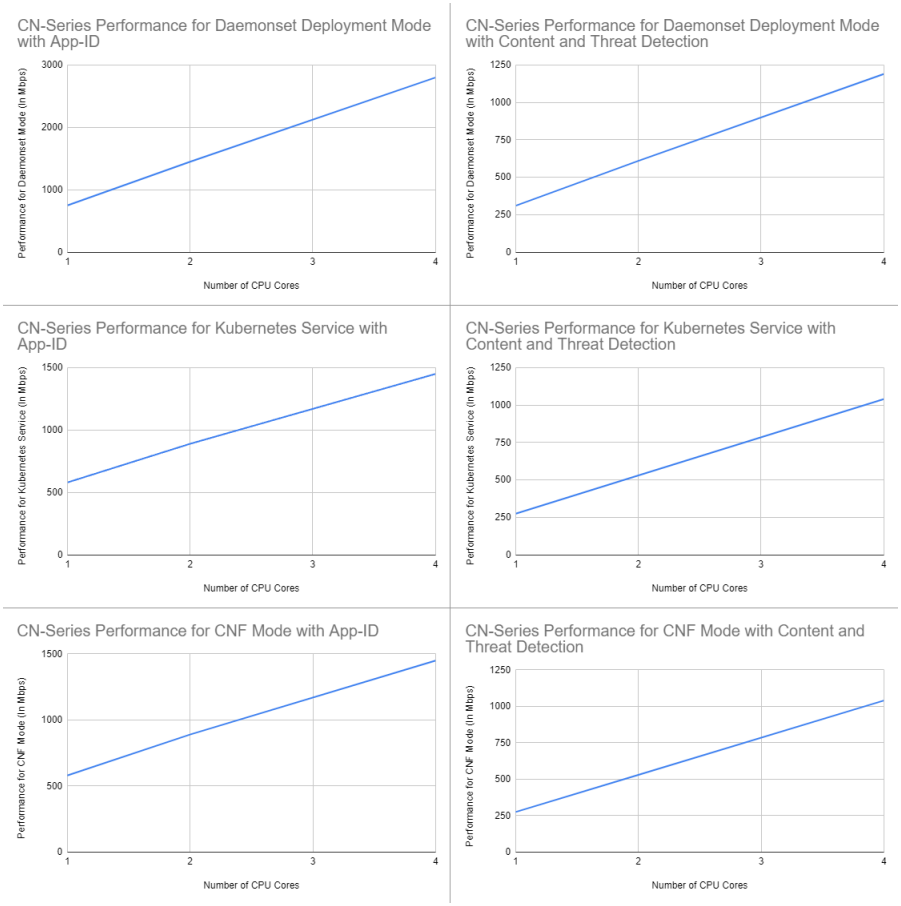
多點傳送	**CN-Series** 小型 （最低 **2.5G** 的 **CN-NGFW** 和最低 **3G** 的 **CN-MGMT**）	**CN-Series** 中型 （最低 **6G** 的 **CN-NGFW** 和最低 **2G** 的 **CN-MGMT**）	**CN-Series** 大型 （最低 **42G** 的 **CN-NGFW** 和低 **4G** 的 **CN-MGMT**）
複寫（輸出介面）	不適用	不適用	不適用
路由	不適用	不適用	不適用

Panorama 上 Kubernetes 外掛程式所支援的規模

屬性	**Kubernetes** 外掛程式規模
K8s Panorama 外掛程式上的最大叢集	32（跨所有支援的環境，例如原生 K8s、AKS、EKS、GKE）

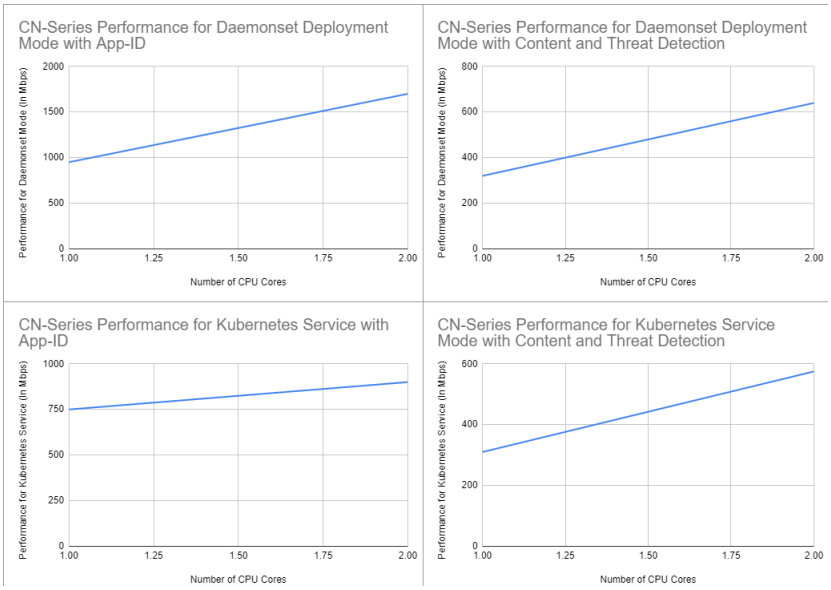
CN-Series 關鍵效能度量

AWS EKS 上的 **CN-Series**				
	CPU 核心	**CN-Series** 作為 **DaemonSet (MMAP)**	**CN-Series** 作為 **Kubernetes** 服務 **(MMAP)**	**CN-Series** 作為 **Kubernetes CNF (MMAP)**
App-ID	1	750 Mbps	580 Mbps	580 Mbps
內容和威脅偵測	1	310 Mbps	275 Mbps	275 Mbps
App-ID	2	1.45 Gbps	890 Mbps	890 Mbps
內容和威脅偵測	2	610 Mbps	530 Mbps	530 Mbps
App-ID	4	2.8 Gbps	1.45 Gbps	1.45 Gbps
內容和威脅偵測	4	1.19 Gbps	1.04 Gbps	1.04 Gbps



Google Cloud GKE 上的 CN-Series（已啟用 XDP）			
	CPU 核心	**CN-Series 作為 DaemonSet**	**CN-Series 作為 Kubernetes 服務**
App-ID	1	950 Mbps	750 Mbps
內容和威脅偵測	1	320 Mbps	310 Mbps
App-ID	2	1.7 Gbps	900 Mbps
內容和威脅偵測	2	640 Mbps	575 Mbps

在 *Google Kubernetes Engine (GKE)* 上，使用節點間以及相同叢集之相同節點上的 *Pod* 間導向的流量來處理下表中資訊的測試



功能/屬性	**CN-Series** 小型	**CN-Series** 中型	**CN-Series** 大型
每個 CN-NGFW 之 vCPU 的防火牆輸送量 (已啟用 App-ID)	500 Mbps	500 Mbps	500 Mbps
每個 CN-NGFW 之 vCPU 的威脅防護輸送量	250 Mbps	250 Mbps	250 Mbps
工作階段數目上限	• 20,000 (DaemonSet) • 250,000（K8s 服務） • 250,000 (K8s-CNF)	819,200	10,000,000
每個 CN-NGFW 之 vCPU 的 IPSec VPN 輸送量	不適用	不適用	不適用
每秒連線數	不適用	不適用	無

CN-Series 部署—支援的環境

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 圖表的 CN-Series 部署

本章節說明 CN-Series 防火牆的相容性和版本需求。

- PAN-OS 10.1
- PAN-OS 10.2
- PAN-OS 11.0
- PAN-OS 11.1
- PAN-OS 11.2

PAN-OS 10.1

您可以在下列環境中部署 CN-Series 防火牆：

產品	版本
容器執行時期	Docker CRI-O Containerd
Kubernetes 版本	1.17 到 1.27
雲端提供者受管理 Kubernetes	• AWS EKS（CN-Series 的 1.17 到 1.27 作為精靈集和服務部署模式。） • AWS Outpost 上的 EKS（1.17 到 1.25） *AWS Outpost 上 EKS 的 CN-Series 不支援 SR-IOV 或 Multus。* • Azure AKS（1.17 到 1.27） 在 *Azure AKS* 中，*PAN-OS 10.1.10h1* 是支援 *kubernetes 1.25* 及更新版本的所需最低版本。

產品	版本
	• AliCloud ACK (1.26) • GCP GKE（1.17 到 1.27）  包括 *GKE* 資料平面 *V2*。
客戶受管理 Kubernetes	在公用雲端或內部部署資料中心上。 請確定此表格列出 Kubernetes 版本、「CNI 類型」和「主機 VM OS」版本。 VMware TKG + 1.1.2 版 • 基礎架構平台—vSphere 7.0 • Kubernetes 主機 VM OS—Photon OS
Kubernetes 主機 VM	作業系統： • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 和更新版本 • CoreOS 21XX、22XX • 容器最佳化 OS
	Linux 核心版本： • 4.18 或更新版本（僅限 K8s 服務模式） • 啟用 AF_XDP 模式所需的 5.4 或更新版本。如需詳細資訊，請參閱 CN-Series 部署 YAML 檔案中的可編輯參數。
	Linux 核心 Netfilter：Iptables
CNI 外掛程式	CNI Spec 0.3 和更新版本： • AWS-VPC • Azure • Calico • Flannel • Weave • 針對 AliCloud，Terway

產品	版本

	• 針對 Openshift、OpenshiftSDN
	• 在作為 DaemonSet 的 CN-Series 防火牆上，支援下列項目。
	  • Multus
	  • 橋接器
	  • SR-IOV
	  • Macvlan

OpenShift	**CN-Series** 作為 **DaemonSet**： 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12 和 4.13 **CN-Series** 作為 **K8s** 服務： （PAN-OS 10.1.2 和更新版本） 4.7、4.8、4.9、4.10、4.11、4.12 和 4.13 *PAN-OS 10.1.10h1* 是支援 *4.12* 及更新版本的所需最低版本。

另請在部署 CN-Series 防火牆之前參考 Kubernetes 叢集的 CN-Series 系統需求。

PAN-OS 10.2

您可以在下列環境中部署 CN-Series 防火牆：

產品	版本
容器執行時期	Docker CRI-O Containerd
Kubernetes 版本	1.17 到 1.27
雲端提供者受管理 Kubernetes	• AWS EKS（CN-Series 的 1.17 到 1.27 作為精靈集和服務部署模式。） • AWS EKS（CN-Series 的 1.17 到 1.22 作為 CNF 部署模式。）

產品	版本
	• AWS Outpost 上的 EKS（1.17 到 1.22）  *AWS Outpost* 上 *EKS* 的 *CN-Series* 不支援 *SR-IOV* 或 *Multus*。 • Azure AKS（1.17 到 1.28）  在 *Azure AKS* 中，*PAN-OS 10.2.4h3* 是支援 *kubernetes 1.25* 及更新版本的所需最低版本。 • GCP GKE（1.17 到 1.27）  在 *GCP GKE* 中，*PAN-OS 10.2.4h3* 是支援 *kubernetes 1.25* 及更新版本的所需最低版本。  包括 *GKE* 資料平面 *V2*。 • Google Anthos 1.12.3 • OCI OKE (1.23)
客戶受管理 Kubernetes	在公用雲端或內部部署資料中心上。 請確定此表格列出 Kubernetes 版本、「CNI 類型」和「主機 VM OS」版本。 VMware TKG + 1.1.2 版 • 基礎架構平台—vSphere 7.0 • Kubernetes 主機 VM OS—Photon OS
Kubernetes 主機 VM	作業系統： • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 和更新版本 • CoreOS 21XX、22XX • 容器最佳化 OS
	Linux 核心版本： • 4.18 或更新版本（僅限 K8s 服務模式）

產品	版本
	• 啟用 AF_XDP 模式所需的 5.4 或更新版本。如需詳細資訊，請參閱 CN-Series 部署 YAML 檔案中的可編輯參數。
	Linux 核心 Netfilter：Iptables

CNI 外掛程式	CNI Spec 0.3 和更新版本：
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• 針對 Openshift、OpenshiftSDN、OVN Kubernetes
	• 在作為 DaemonSet 的 CN-Series 防火牆上，支援下列項目。
	  • Multus
	  • 橋接器
	  • SR-IOV
	  • Macvlan

OpenShift	• 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12 和 4.13 版 *OpenShift 4.7* 僅適用於「*CN-Series 作為 DaemonSet*」。 • OpenShift on AWS *PAN-OS 10.2.4h3* 是支援 *4.12* 及更新版本的所需最低版本。

另請在部署 CN-Series 防火牆之前參考 Kubernetes 叢集的 CN-Series 系統需求。

PAN-OS 11.0

您可以在下列環境中部署 CN-Series 防火牆：

產品	版本
容器執行時期	Docker CRI-O Containerd
Kubernetes 版本	1.17 到 1.27
雲端提供者受管理 Kubernetes	• AWS EKS（CN-Series 的 1.17 到 1.27 作為精靈集和服務部署模式。） • AWS EKS（CN-Series 的 1.17 到 1.22 作為 CNF 部署模式。） • AWS Outpost 上的 EKS（1.17 到 1.25） *AWS Outpost 上 EKS 的 CN-Series 不支援 SR-IOV 或 Multus。* • Azure AKS（1.17 到 1.27） 在 *Azure AKS* 中，*PAN-OS 11.0.2* 是支援 *kubernetes 1.25* 及更新版本的所需最低版本。 • GCP GKE（1.17 到 1.27） 包括 *GKE* 資料平面 *V2*。 • OCI OKE (1.23)
客戶受管理 Kubernetes	在公用雲端或內部部署資料中心上。 請確定此表格列出 Kubernetes 版本、「CNI 類型」和「主機 VM OS」版本。 VMware TKG + 1.1.2 版 • 基礎架構平台—vSphere 7.0 • Kubernetes 主機 VM OS—Photon OS
Kubernetes 主機 VM	作業系統： • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 和更新版本

產品	版本
	• CoreOS 21XX、22XX • 容器最佳化 OS
	Linux 核心版本： • 4.18 或更新版本（僅限 K8s 服務模式） • 啟用 AF_XDP 模式所需的 5.4 或更新版本。如需詳細資訊，請參閱 CN-Series 部署 YAML 檔案中的可編輯參數。
	Linux 核心 Netfilter：Iptables

CNI 外掛程式	CNI Spec 0.3 和更新版本：
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• 針對 Openshift、OpenshiftSDN、OVN Kubernetes
	• 在作為 DaemonSet 的 CN-Series 防火牆上，支援下列項目。
	  • Multus
	  • 橋接器
	  • SR-IOV
	  • Macvlan

OpenShift	• 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12 和 4.13 版。 *OpenShift 4.7* 僅適用於「*CN-Series* 作為 *DaemonSet*」。 *PAN-OS 11.0.2* 是支援 *4.12* 及更新版本的所需最低版本。 • AWS 上的 OpenShift

另請在部署 CN-Series 防火牆之前參考 Kubernetes 叢集的 CN-Series 系統需求。

PAN-OS 11.1

您可以在下列環境中部署 CN-Series 防火牆：

產品	版本
容器執行時期	Docker CRI-O Containerd
Kubernetes 版本	1.17 到 1.27
雲端提供者受管理 Kubernetes	• AWS EKS（CN-Series 的 1.17 到 1.27 作為精靈集和服務部署模式。） • AWS EKS（CN-Series 的 1.17 到 1.22 作為 CNF 部署模式。） • AWS Outpost 上的 EKS（1.17 到 1.25） *AWS Outpost* 上 *EKS* 的 *CN-Series* 不支援 *SR-IOV* 或 *Multus*。 • Azure AKS（1.17 到 1.27） 在 *Azure AKS* 中，*PAN-OS 11.0.2* 是支援 *kubernetes 1.25* 及更新版本的所需最低版本。 • GCP GKE（1.17 到 1.27） 包括 *GKE* 資料平面 *V2*。 • OCI OKE (1.23)
客戶受管理 Kubernetes	在公用雲端或內部部署資料中心上。 請確定此表格列出 Kubernetes 版本、「CNI 類型」和「主機 VM OS」版本。 VMware TKG + 1.1.2 版 • 基礎架構平台—vSphere 7.0 • Kubernetes 主機 VM OS—Photon OS
Kubernetes 主機 VM	作業系統： • Ubuntu 16.04

產品	版本
	• Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 和更新版本 • CoreOS 21XX、22XX • 容器最佳化 OS
	Linux 核心版本： • 4.18 或更新版本（僅限 K8s 服務模式） • 啟用 AF_XDP 模式所需的 5.4 或更新版本。如需詳細資訊，請參閱 CN-Series 部署 YAML 檔案中的可編輯參數。
	Linux 核心 Netfilter：Iptables

CNI 外掛程式	CNI Spec 0.3 和更新版本：
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• 針對 Openshift、OpenshiftSDN、OVN Kubernetes
	• 在作為 DaemonSet 的 CN-Series 防火牆上，支援下列項目。
	  • Multus
	  • 橋接器
	  • SR-IOV
	  • Macvlan

OpenShift	• 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12 和 4.13 版。 *OpenShift 4.7* 僅適用於「*CN-Series* 作為 *DaemonSet*」。 *PAN-OS 11.0.2* 是支援 *4.12* 及更新版本的所需最低版本。

產品	版本
	• AWS 上的 OpenShift

另請在部署 CN-Series 防火牆之前參考 Kubernetes 叢集的 CN-Series 系統需求。

PAN-OS 11.2

您可以在下列環境中部署 CN-Series 防火牆：

產品	版本
容器執行時期	Docker CRI-O Containerd
Kubernetes 版本	1.17 到 1.27
雲端提供者受管理 Kubernetes	• AWS EKS（CN-Series 的 1.17 到 1.27 作為精靈集和服務部署模式。） • AWS EKS（CN-Series 的 1.17 到 1.22 作為 CNF 部署模式。） • AWS Outpost 上的 EKS（1.17 到 1.25） *AWS Outpost 上 EKS 的 CN-Series 不支援 SR-IOV 或 Multus。* • Azure AKS（1.17 到 1.27） 在 *Azure AKS* 中，*PAN-OS 11.0.2* 是支援 *kubernetes 1.25* 及更新版本的所需最低版本。 • GCP GKE（1.17 到 1.27） 包括 *GKE* 資料平面 *V2*。 • OCI OKE (1.23)
客戶受管理 Kubernetes	在公用雲端或內部部署資料中心上。 請確定此表格列出 Kubernetes 版本、「CNI 類型」和「主機 VM OS」版本。 VMware TKG + 1.1.2 版

產品	版本
	• 基礎架構平台—vSphere 7.0 • Kubernetes 主機 VM OS—Photon OS
Kubernetes 主機 VM	作業系統： • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 22.04 • RHEL/Centos 7.3 和更新版本 • CoreOS 21XX、22XX • 容器最佳化 OS
	Linux 核心版本： • 4.18 或更新版本（僅限 K8s 服務模式） • 啟用 AF_XDP 模式所需的 5.4 或更新版本。如需詳細資訊，請參閱 CN-Series 部署 YAML 檔案中的可編輯參數。
	Linux 核心 Netfilter：Iptables

CNI 外掛程式	CNI Spec 0.3 和更新版本：
	• AWS-VPC
	• Azure
	• Calico
	• Flannel
	• Weave
	• 針對 Openshift、OpenshiftSDN、OVN Kubernetes
	• 在作為 DaemonSet 的 CN-Series 防火牆上，支援下列項目。
	  • Multus
	  • 橋接器
	  • SR-IOV
	  • Macvlan

產品	版本
OpenShift	• 4.2、4.4、4.5、4.6、4.7、4.8、4.9、4.10、4.11、4.12 和 4.13 版。 *OpenShift 4.7* 僅適用於「*CN-Series* 作為 *DaemonSet*」。 *PAN-OS 11.0.2* 是支援 *4.12* 及更新版本的所需最低版本。 • AWS 上的 OpenShift

另請在部署 CN-Series 防火牆之前參考 Kubernetes 叢集的 CN-Series 系統需求。

CN-Series 部署先決條件

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

若要部署 CN-Series 防火牆，您必須先符合下列先決條件：

- 授權 CN-Series 防火牆
- 在 CN-Series 防火牆上安裝裝置憑證
- 建立叢集驗證的服務帳戶
- 安裝 Kubernetes 外掛程式並設定 CN-Series 的 Panorama
- 取得 CN-Series 部署的映像檔和檔案

授權 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 對於使用 Helm 的 CN-Series 部署

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 環境中部署之 CN-NGFW Pod 所使用的 vCPU（核心）總數進行授權。CN-NGFW 所使用的每個 vCPU 都會耗用一個權杖。

- 啟動積分—從啟動積分開始。啟動後，您可以將積分池中的積分套用至 CN-Series 部署設定檔。
- 建立 CN-Series 部署設定檔—在部署設定檔中，您將指定配置給所產生驗證碼的 vCPU 數目。然後，您將使用與您的 CN-Series 部署設定檔相關聯的驗證碼來授權 Kubernetes 叢集中的 CN-Series 防火牆。您可以根據配置的 vCPU 數目，使用部署設定檔來授權 CN-NGFW Pod。部署設定檔中的單一驗證碼可以用來在不同的 Kubernetes 環境、不同叢集或不同的 Panorama 執行個體上授權 CN-Series。

  在 CN-Series-as-a-Kubernetes-Service 部署中，如果環境中部署的 CN-NGFW Pod 數目超過配置的 vCPU 數目，則您有 30 天的寬限期可將更多的 vCPU 新增部署設定檔，或刪除足夠的 CN-NGFW Pod。如果您未在 30 天寬限期內配置額外的 vCPU 或刪除未授權的 Pod，則將會取消叢集中所有 CN-Series 防火牆的授權。

  將 CN-Series 部署為 DaemonSet 時，如果部署的 CN-NGFW Pod 數目超過配置的 vCPU 數目，則您有四小時的寬限期，將更多的 vCPU 新增至部署設定檔，或刪除足夠的 CN-NGFW 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 將會停止處理流量。已授權的 Pod 仍然會有授權。

  您也可以選擇在建立 CN-Series 部署設定檔時佈建虛擬 Panorama 設備。
- 管理部署設定檔—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。

授權會套用至叢集層級的 *CN-Series*。個別 *CN-NGFW* 可能會顯示為未授權，不過，除非取消整個叢集的授權，否則會授權叢集中的所有 *Pod*。

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

我可以在哪裡使用這個？	我需要哪些內容？
	• 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。

繼續建立 CN-Series 部署設定檔。

建立 CN-Series 部署設定檔

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 或更新版本 • Helm 3.6 or above version client使用 Helm 的 CN-Series 部署

使用下列程序建立 CN-Series 部署設定檔。

STEP 1 | 如果您已有積分池，請登入帳戶，然後從儀表板選取 **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 10.2 and above**（**PAN-OS 10.2** 和更新版本）。
3. 按一下 **Next**（下一步）。

STEP 2 | CN-Series 設定檔。

1. **Profile Name**（設定檔名稱）。

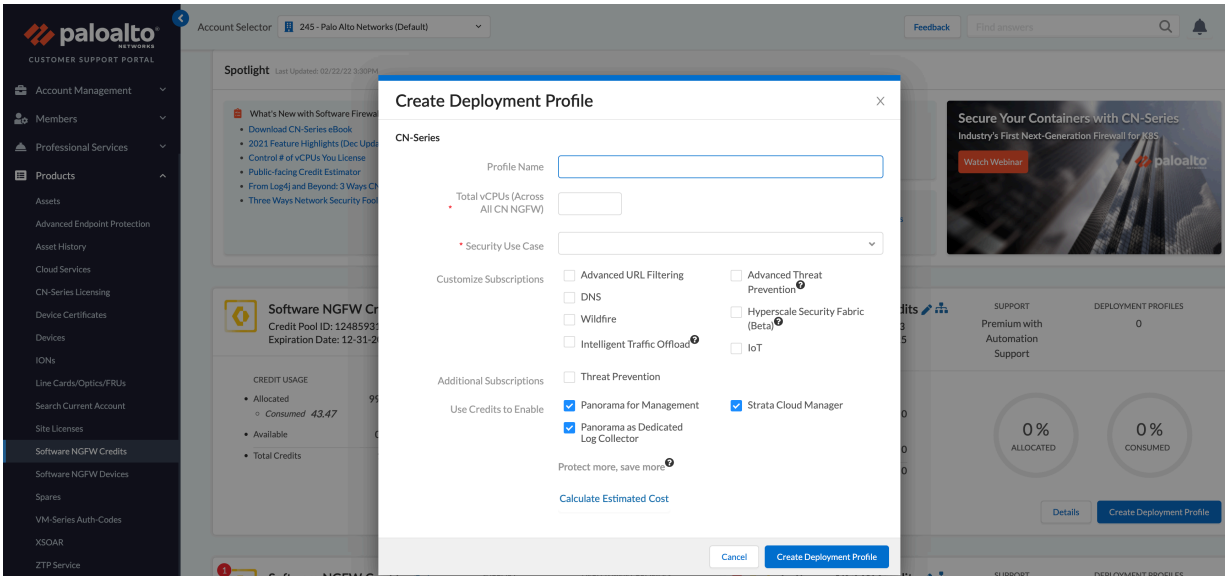
   命名設定檔。
2. **Total vCPUs**（**vCPU** 總計）。

   輸入跨所有 CN-NGFW 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. （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 | （選用）將滑鼠游標停留在 **Protect more, save more**（保護更多，節省更多）後面的問號上，以瞭解分配積分對節省效果有何影響。

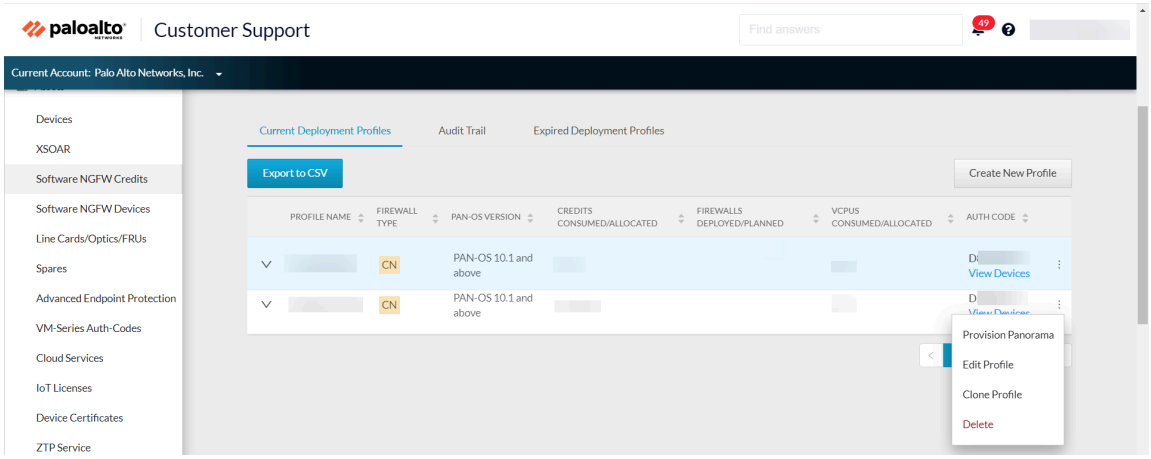
STEP 4 | 按一下 **Calculate Estimated Cost**（計算預估成本），以檢視總積分和部署前可用的積分數量。

（選用）將滑鼠游標停留在預估值後面的問號上，以檢視每個元件的積分明細。

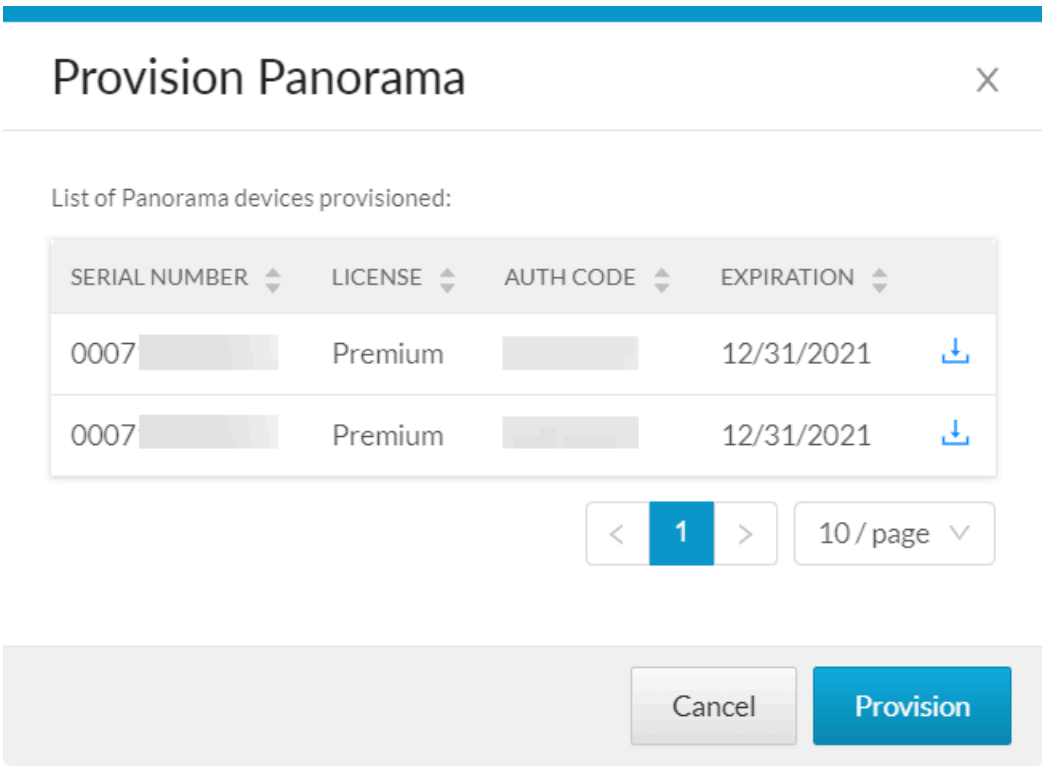


STEP 5 | （選用）佈建 Panorama。如果您已使用積分啟用 VM Panorama，則請完成下列步驟以佈建 Panorama 並產生序號。管理 CN-Series 部署需要 Panorama。將序號套用至 Panorama 之後，Panorama 將會聯絡授權更新伺服器，並擷取授權。

1. 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分） > **Prisma NGFW Credits**（**Prisma NGFW** 積分），並找到部署設定檔。
2. 在最右邊選取垂直省略符號，然後選取 **Provision Panorama**（佈建 **Panorama**）。



3. 按一下 [Provision Panoram（佈建 Panorama）] 產生序號。
4. 記錄或複製要套用至 Panorama 執行個體的序號。



5. 註冊 Panorama。

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-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

您可以使用下列程序來管理現有部署設定檔。

- 編輯部署設定檔
- 複製部署設定檔
- 刪除部署設定檔
- 將積分轉移至相同帳戶中的池
- 將積分轉移至不同的 CSP 帳戶

編輯部署設定檔

您可以修改現有部署設定檔來新增更多積分，將額外的 vCPU 指派給部署。與要修改之部署設定檔相關聯的驗證碼不得在 Panorama 上使用。

STEP 1 | 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分），然後選擇設定檔（選取一列）。

STEP 2 | 在最右邊選取垂直省略符號（[More Options（更多選項）]），然後選取 **Edit Profile**（編輯設定檔）。

STEP 3 | 進行變更，並選取 **Update Deployment Profile**（更新部署設定檔）。

複製部署設定檔

完成下列程序來複製現有部署設定檔。

STEP 1 | 前往 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分），然後選取設定檔（選取一列）。

STEP 2 | 在最右邊選取垂直省略符號（[More Options（更多選項）]），然後選取 **Clone Profile**（複製設定檔）。

STEP 3 | 變更設定檔名稱、進行任何其他變更，然後選取 **Create Deployment Profile**（建立部署設定檔）。

刪除部署設定檔

刪除部署設定檔之前，您必須刪除任何使用該設定檔的防火牆。與要刪除之部署設定檔相關聯的驗證碼不得在 Panorama 上使用。

STEP 1 | 在 CSP 中，選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分），然後選取設定檔（選取一列）。

STEP 2 | 在最右邊選取垂直省略符號（[More Options（更多選項）]），然後選取 **Delete**（刪除）。

將積分轉移至相同帳戶中的池

您可以將積分轉移至您可存取之不同帳戶中的積分池。

STEP 1 | 登入 CSP 帳戶。

STEP 2 | 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分）。

- 識別來源積分池，並記下積分池 ID。
- 識別目的地積分池，並記下積分池 ID。

STEP 3 | 前往來源積分池，並選取左下方的 **Transfer Credits**（轉移積分）。

STEP 4 | 選取 **Different CSP account**（不同的 **CSP** 帳戶）。

1. **New credit type**（新積分類型）—選擇積分類型。此時，來源與目的地類型必須相同。
2. 積分池 **ID#**—選擇積分池 ID 號碼。如果目的地帳戶沒有任何所選擇類型的積分池，則 CSP 會提示您建立積分池。
3. **Amount to transfer**（要轉帳的金額）—輸入要轉帳的金額。

STEP 5 | 選取 **Update Credits**（更新積分）。

將積分轉移至不同的 CSP 帳戶

您可以將積分轉移至相同帳戶中的積分池。

STEP 1 | 登入您的 CSP 帳戶。

STEP 2 | 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分）。

- 識別來源積分池，並記下積分池 ID。
- 識別目的地積分池，並記下積分池 ID。

  如果目的地位於不同的帳戶中，則請從左上方的 **Current Account**（目前帳戶）下拉式清單中選取它，然後選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分）。找到目的地，並記下積分類型和積分池 ID。

STEP 3 | 前往來源積分池，並按一下左下方的 **Transfer Credits**（轉移積分）。

STEP 4 | 選擇不同的 CSP 帳戶。

1. **Transfer to**（轉移至）—選擇帳戶名稱。
2. **As credit type**（作為積分類型）—選擇積分類型。此時，來源與目的地類型必須相同。
3. 積分池 **ID#**—選擇積分池 ID 號碼。如果目的地帳戶沒有任何所選擇類型的積分池，則 CSP 會提示您建立積分池。
4. **Amount to transfer**（要轉帳的金額）—輸入要轉帳的金額。

STEP 5 | 選取 **Update Credits**（更新積分）。

在 CN-Series 防火牆上安裝裝置憑證

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

防火牆需要裝置憑證來授權安全存取 Palo Alto 雲端傳遞的安全性服務 (CDSS)，例如 WildFire、AutoFocus 和 Strata 記錄日誌服務。您必須套用自動註冊 PIN 才能將 CDSS 授權套用至 CN-Series 防火牆部署。每個 PIN 都在客戶支援入口網站 (CSP) 上產生，且為 Palo Alto Networks 支援帳戶所獨有。若要成功安裝裝置憑證，CN-Series 管理平面 Pod (CN-MGMT) 必須具有輸出網際網路連線，且必須在網路上允許使用以下完全合格網域名稱 (FQDN) 和連接埠。

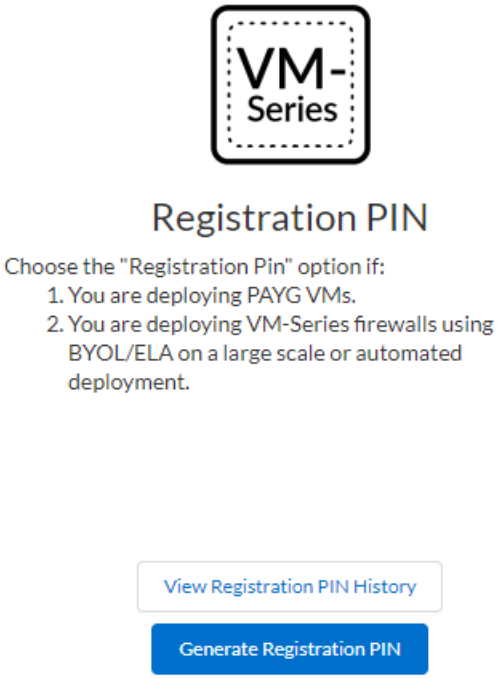
FQDN	連接埠
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com • http://ocsp.godaddy.com	TCP 80
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • https://certificatetrusted.paloaltonetworks.com • https://certificate.paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 和 TCP 443

若要將裝置憑證新增至沒有現有裝置憑證的現有部署中，您必須在將有效的 *PIN ID* 和值新增至 `pan-cn-mgmt-secret.yaml` 後重新部署 *CN-Series* 防火牆。針對公共雲端 *CN-Series* 部署，您必須在重新部署之前刪除永久性磁碟區宣告。針對靜態/原生 *Kubernetes* 部署，您必須在重新部署之前刪除永久性磁碟區宣告和永久性磁碟區。

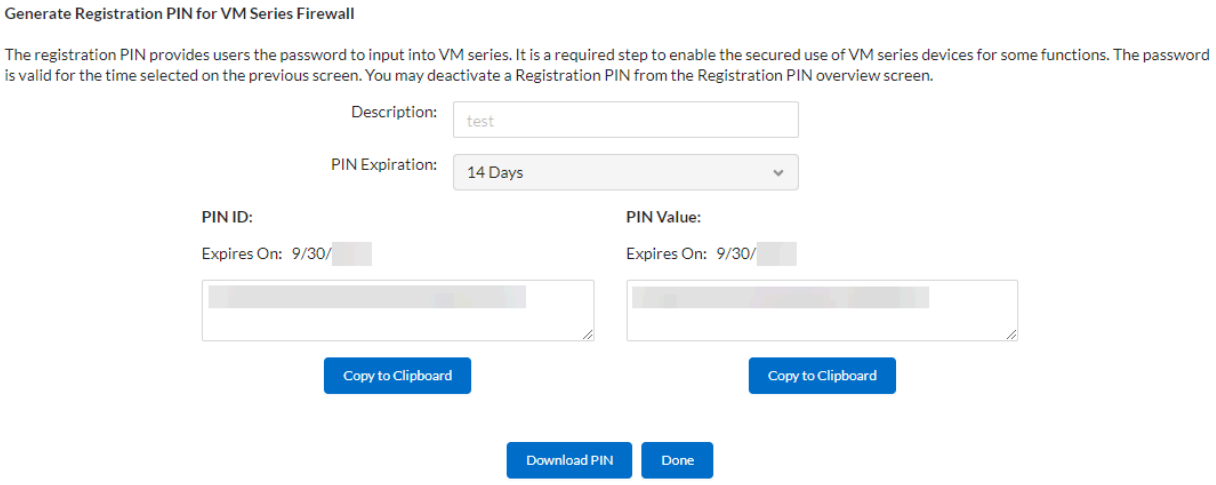
STEP 1 | 使用帳戶認證登入 Palo Alto Networks 客戶支援入口網站。

如果您需要新的帳戶，則請參閱如何建立新的 Customer Support Portal 使用者帳戶。

STEP 2 | 選取 **Assets**（資產） > **Device Certificates**（裝置憑證） > **Generate Registration PIN**（產生註冊 **PIN**）。



STEP 3 | 輸入 **Description**（說明），然後從下拉式清單中選取 **PIN Expiration**（**PIN** 到期）。



STEP 4 | 儲存 PIN ID 和值。

儲存 PIN ID 和值。此 PIN ID 和值是 `pan-cn-mgmt-secret.yaml` 檔案中用來部署 CN-Series 防火牆的。務必在 PIN 過期之前啟動防火牆。

```
# Thermite Certificate retrieval CN-SERIES-AUTO-REGISTRATION-PIN-
ID: "<your-pin-id>" CN-SERIES-AUTO-REGISTRATION-PIN-VALUE: "<your-
pin-value>"
```

建立叢集驗證的服務帳戶

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 圖表的 CN-Series 部署

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。使用 `plugin-serviceaccount.yaml` 所建立的服務帳戶 (pan-plugin-user) 可讓 Panorama 上的 Kubernetes 外掛程式向 Kubernetes 叢集進行驗證以擷取 Pod 上的中繼資料。其他兩個 yaml 檔案（`pan-mgmt-serviceaccount.yaml` 和 `pan-cni-serviceaccount.yaml`）會建立 pan-mgmt-sa 和 pan-cni-sa 服務帳戶，來啟用容錯 CN-Mgmt Pod 之間以及 CN-MGMT Pod 與 CN-NGFW Pod 之間的驗證。

YAML 檔案預設會在 *kube-system* 命名空間中建立服務帳戶和祕密；*Kubernetes* 外掛程式只會尋找 *kube-system* 命名空間中的祕密。

若要建立服務帳戶，Kubernetes 叢集應該就緒。

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

此服務帳戶會啟用 Panorama 向 GKE 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。

1. **`kubectl apply -f plugin-serviceaccount.yaml`**
2. **`kubectl -n kube-system get secrets | grep pan-plugin-user`**

   檢視與此服務帳戶相關聯的祕密。

   如果您使用的是 *kubernetes* 版本 *1.24* 或更新版本，請執行以下命令以檢視與此服務帳戶關聯的密碼：

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

3. **`kubectl -n kube-system get secrets <secrets-from-above-command> -o json >> cred.json`**

   在此範例中，建立名稱為 cred.json 且包含祕密的認證檔案，並儲存此檔案。您需要將此檔案上傳至 Panorama，以設定用於監控安裝 Kubernetes 外掛程式並設定 CN-Series 的 Panorama中叢集的 Kubernetes 外掛程式。

STEP 2 | 執行 `pan-mgmt-serviceaccount.yaml` 和 `pan-cni-serviceaccount.yaml`。

`pan-mgmt-serviceaccount.yaml` 會建立名稱為 pan-sa 的服務帳戶，而且是啟用 CN-MGMT 與 CN-NGFW Pod 彼此通訊、PAN-CNI 和 Kubernetes API 伺服器的必要項目。如果您修改此服務帳戶，則也必須更新您用來部署 CN-MGMT 和 CN-NFGW Pod 的 YAML 檔案。`pan-cni-serviceaccount.yaml` 會建立名稱為 pan-cni-sa 的服務帳戶。

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

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

STEP 3 | 驗證服務帳戶。

```
kubectl get serviceaccounts -n kube-system
```

如果您要使用 *HELM* 圖表，則步驟 *2* 和 *3* 會由 *HELM* 圖表自動執行，而且不需要手動執行。

安裝 Kubernetes 外掛程式並設定 CN-Series 的 Panorama

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

您可以在內部部署或雲端中部署 Panorama 設備，只要 Panorama 設備可以與您要部署 CN-Series 防火牆的 Kubernetes 叢集連線即可。此工作流程會帶您完成安裝 Kubernetes 外掛程式、啟用驗證碼以及設定 Kubernetes 外掛程式來監視叢集的程序。

您必須小心規劃要配置給 *Panorama* 的積分數。變更積分數後，您不需要在 *Panorama OS 11.0* 上重新部署 *CN-Series* 防火牆。

如需詳細資訊，請參閱授權 CN-Series 防火牆和軟體 NGFW 積分估算器。

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，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）]。

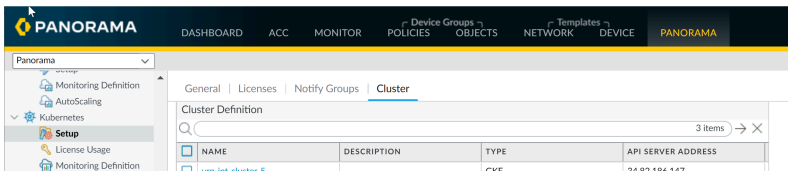
STEP 2 | 如果您想要 Panorama 收集防火牆日誌，則請驗證 Panorama 處於 Panorama 模式。

STEP 3 | 在 Panorama 上，安裝 Kubernetes 外掛程式。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。

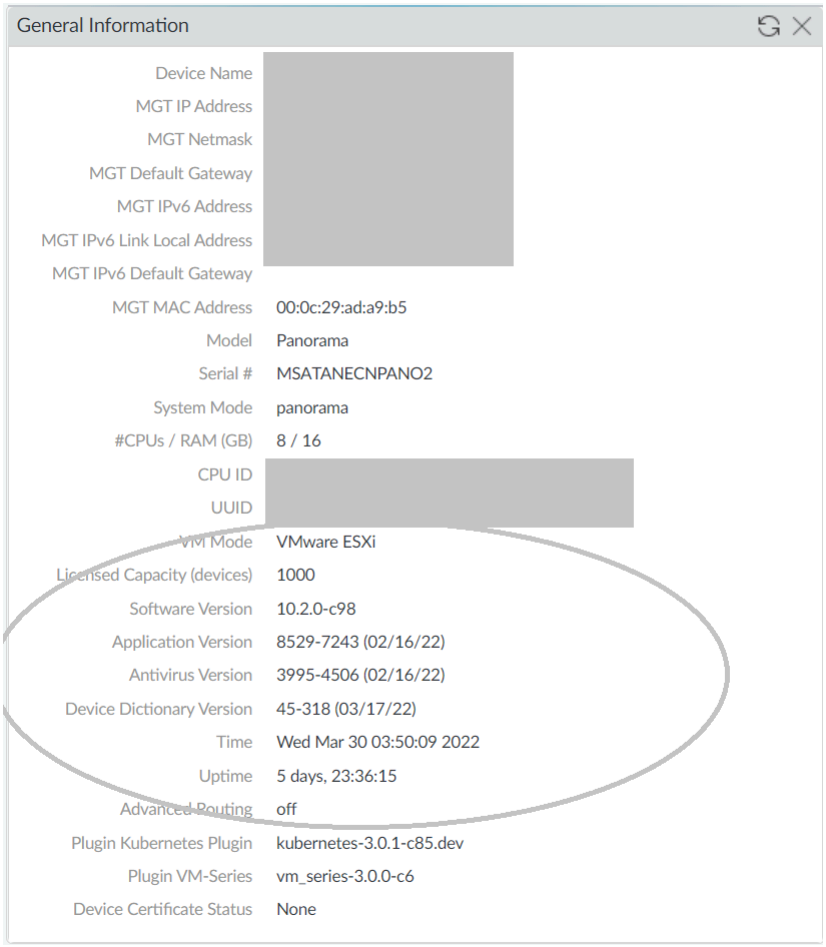
1. 登入 Panorama 網頁介面，選取 **Panorama** > **Plugins**（外掛程式）並按一下 **Check Now**（立即檢查）以取得可用外掛程式清單。
2. 選取 **Download**（下載）並 **Install**（安裝） Kubernetes 外掛程式

   在您成功安裝之後，會重新整理 Panorama，而且 Kubernetes 外掛程式會顯示在 **Panorama** 頁籤上。

如果 Panorama 部署在 HA 配對中，則請遵循步驟 3 中所述的上述步驟在次要（被動）Panorama 上安裝 Kubernetes 外掛程式。



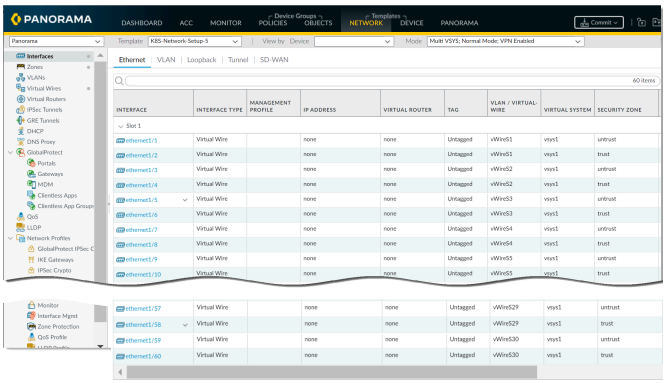
您也可以驗證 Panorama **Dashboard**（儀表板）上的 [General Information（一般資訊）] Widget。



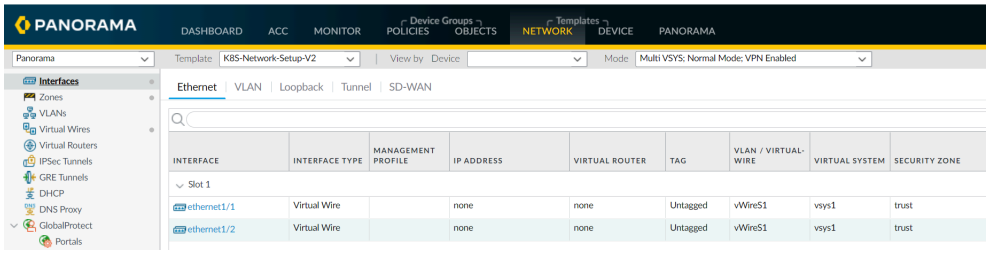
STEP 4 | 提交您在 Panorama 上的變更。

按一下 **Commit to Panorama**（提交至 **Panorama**）。提交會建立四個範本：**K8S-Network-Setup**、**K8S-Network-Setup-V2**、**K8S-Network-Setup-V3** 和 **K8S-Network-Setup-V3-HA**。最多需要一分鐘的時間，以在 Panorama 上顯示介面。

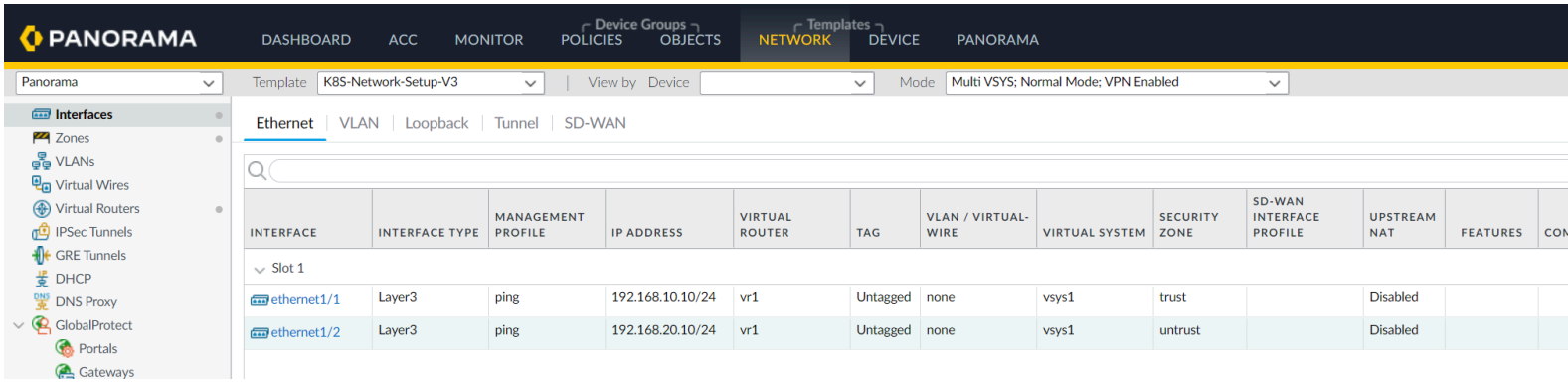
- **K8S-Network-Setup** 與「CN-Series 作為 DaemonSet」搭配使用，並且具有 30 個虛擬連線；作為虛擬連線一部分以保護應用程式的介面配對。因此，在一個節點上，「CN-NGFW 作為 DaemonSet」最多可以保護 30 個應用程式 Pod。



- **K8S-Network-Setup-V2** 與「CN-Series 作為 Kubernetes 服務」搭配使用，並且具有一個虛擬介接；作為虛擬介接一部分以保護 Pod 應用程式的介面配對。

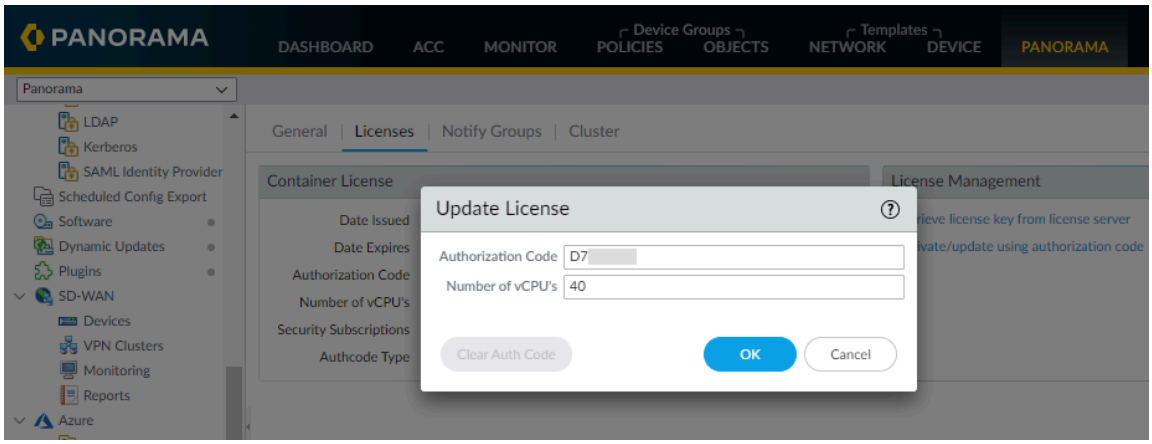


- **K8S-Network-Setup-V3** 範本有一個範例設定，您可以對其進行複製，也可以對其進行修改以符合您想要的設定。Kubernetes CNF 模式可以保護容器和非容器工作負載。您可以將其作為獨立的第三層進行部署。



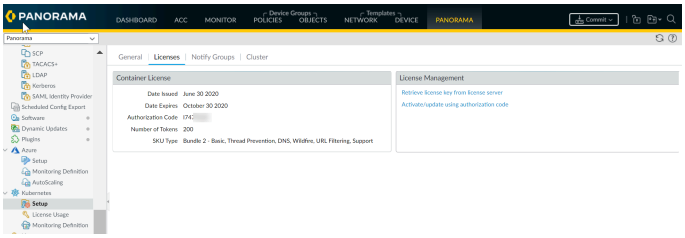
STEP 5 | 取得 Panorama 上的 CN-Series 授權積分。

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 CN-Series 部署設定檔，才能取得 CN-Series 驗證碼。



如果您部署 CN-Series 防火牆，而未啟動授權，則會有 4 小時寬限期，在此期間之後，防火牆就會停止處理流量。在寬限期之後，CN-NGFW 執行個體將會根據 `pan-cn-ngfw-configmap.yaml` 中定義的 (FAILOVER_MODE) 進行 failopen（預設值）或 failclose。在 fail-open 模式中，防火牆將會接收並送出封包，而不會套用任何安全性原則。轉換為 fail-open 時將需要重新啟動，並且會導致該期間發生流量短暫中斷（預期大約是 10-30 秒）。在 fail-close 模式中，防火牆將會捨棄所有收到的封包。fail-close 將會關閉 CN-NGFW Pod，並將積分釋出到可用積分集區以授權新的 CN-NGFW Pod。

3. 驗證已更新可用的授權積分數目。



STEP 6 | 產生 VM 驗證金鑰。

1. 請確保符合下列先決條件：
   - 擁有一台具有 Panorama 網路存取權的電腦。
   - 知道 Panorama IP 位址。
   - 管理介面支援 SSH（為預設設定）。如果管理員已停用 SSH，而您想要將它重新啟用：選取 **Panorama** > **Setup**（設定） > **Interfaces**（介面）、按一下 **Management**（管理）、選取 **SSH**、按一下 **OK**（確定）、選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後將您的變更 **Commit**（提交）至 Panorama 設定。
2. 若要使用 SSH 存取 CLI：
   1. 在 SSH 用戶端中輸入 Panorama IP 位址，並使用連接埠 22。
   2. 出現提示時輸入您的管理存取認證。登入後，將顯示當日訊息，然後在操作模式中顯示 CLI 提示。例如：

      ```
      admin@ABC_Sydney>
      ```
3. 使用下列操作命令：

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

   例如，若要產生一個 24 小時有效的金鑰，請輸入下列命令：

   request bootstrap vm-auth-key generate lifetime 24

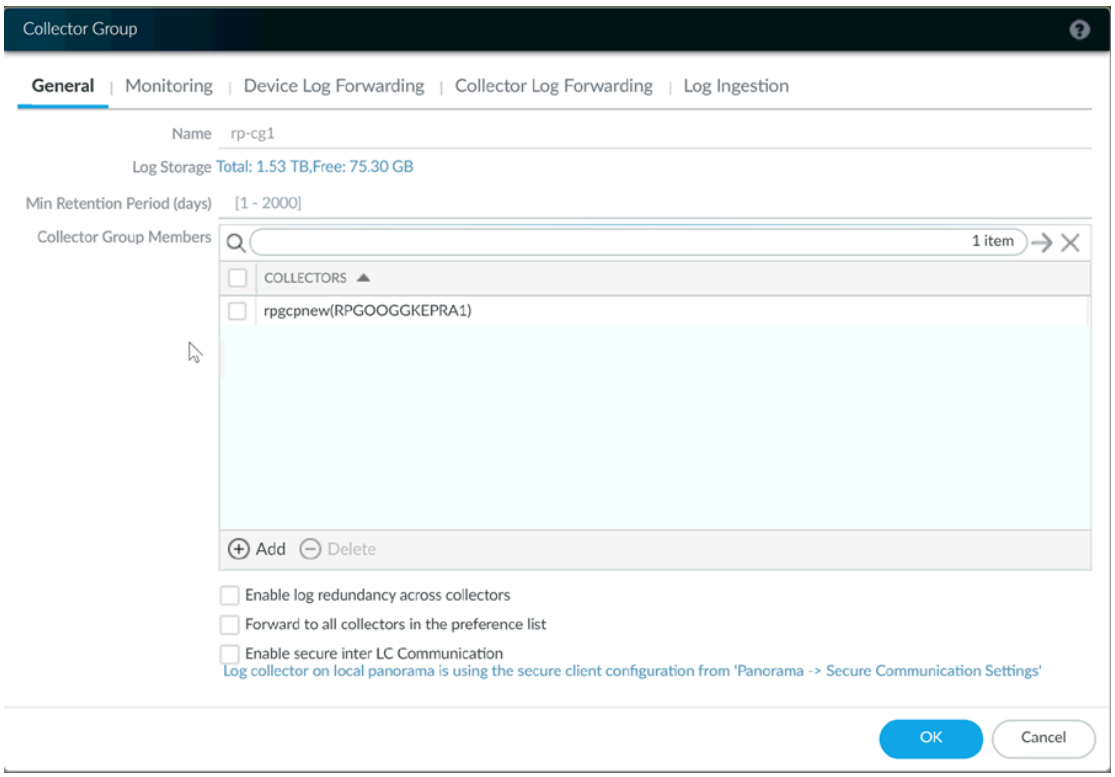
   ```
   已產生 VM 驗證金鑰 755036225328715。  過期於：2020/01/29 12:03:52
   ```
4. 您應該確保將 VM 驗證金鑰儲存至某處，因為稍後的步驟需要該金鑰。

STEP 7 | 建立父「裝置群組」和「範本堆疊」。

您必須建立範本堆疊和裝置群組，而且稍後在您編輯 YAML 檔案以部署 CN-MGMT Pod 時將參照此範本堆疊和裝置群組。Panorama 上的 Kubernetes 外掛程式會建立稱為 K8S-Network-Setup 的範本，而且此範本將會是您在這裡定義的範本堆疊一部分。

1. 建立範本堆疊，並將 K8S-Network-Setup 範本新增至範本堆疊。
    1. 選取 **Panorama** > **Templates**（範本）和 **Add Stack**（新增堆疊）。
    2. 輸入用來識別網域的唯一 **Name**（名稱）。
    3. 新增並選取 **K8S-Network-Setup** 範本以用於 daemonset、**K8S-Network-Setup-V2** 以用於 kubernetes 即服務部署、**K8S-Network-Setup-V3** 以用於獨立 CNF 部署，或 **K8S-Network-Setup-V3-HA** 以用於 CNF HA 部署。
    4. 按一下 **OK**（確定）。
2. 建立裝置群組。
    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）。
3. 如果您使用 Panorama 虛擬設備，則可以建立日誌收集器，並將其新增至日誌收集器群組。
    1. 移至 **Panorama** > **Collector Groups**（收集器群組），然後選取 **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），然後將您的變更 **Commit and Push**（提交並推送）至 Panorama 和您設定的收集器群組。

4. 如果您要使用進階路由，則請予以啟用。

   1. 移至 **Panorama** > **Templates**（範本）> **Device**（裝置）。
   2. 在 **Management**（管理）頁籤中選取 **Advanced Routing**（進階路由）（僅適用於 kubernetes CNF 部署模式）。

STEP 8 | 設定用於監視叢集的 Kubernetes 外掛程式。

該程序中的下一步是將 Kubernetes 叢集資訊新增至 Panorama，以確保兩者可以彼此通訊。

Panorama 最多支援 *32* 個 *Kubernetes* 叢集。

若要確保外掛程式與 Kubernetes 叢集同步，外掛程式會依設定的間隔來輪詢 Kubernetes API 伺服器，並依預先定義的間隔接聽來自 Kubernetes Watch API 的通知。

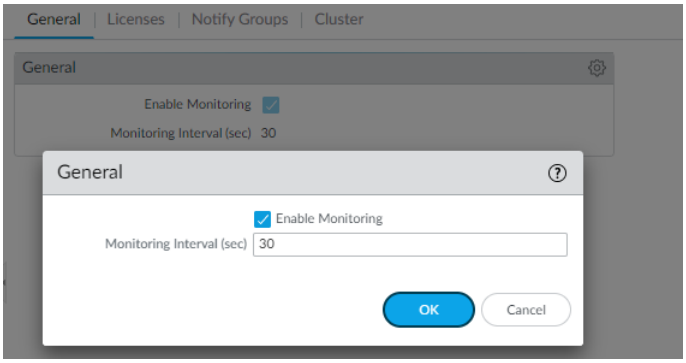
在您新增叢集資訊之後，Panorama 一律會擷取服務、節點、複本集，然後建立其標記，讓您可以查看和控制進出這些叢集的流量。您可以選擇性地指定是否要 Panorama 擷取 Kubernetes 標籤

的相關資訊，同時建立這些標籤的標記。請參閱 Kubernetes 屬性的 IP 位址與標記對應，查看受支援的屬性。

1. 檢查監視間隔。

   Panorama 用來輪詢 Kubernetes API 伺服器端點的預設間隔是 30 秒。

   1. 選取 **Panorama** > **Plugins**（外掛程式） > **Kubernetes** > **Setup**（設定） > **General**（一般）。
   2. 驗證已選取 **Enable Monitoring**（啟用監視）。
   3. 按一下齒輪圖示來編輯 **Monitoring Interval**（監視間隔），並變更為 30-300 秒的範圍。



2. 選取 **Panorama** > **Plugins**（外掛程式） > **Kubernetes** > **Setup** （設定） > **Cluster**（叢集）和 **Add Cluster**（新增叢集）。

   請確定您未將相同的 Kubernetes 叢集新增至多個 Panorama (單一執行個體或 HA 配對) 設備，因為您可能會看到如何在裝置群組中註冊 IP 位址對應的不一致。

3. 輸入 **Name**（名稱）和 **API Server Address**（**API** 伺服器位址）。

   這是您必須從 Kubernetes 部署取得之叢集的「端點 IP 位址」。請輸入最多 20 個字元的名稱，以唯一識別叢集的名稱。您無法修改此名稱，因為 Panorama 會為在叢集內找到的 Pod、節點、服務建立標記時使用叢集名稱。

   API 伺服器位址格式可以是主機名稱或「IP 位址:連接埠號碼」，而且，如果您要使用連接埠 443（預設連接埠），則不需要指定連接埠。

4. 選取叢集部署所在的環境 **Type**（類型）。

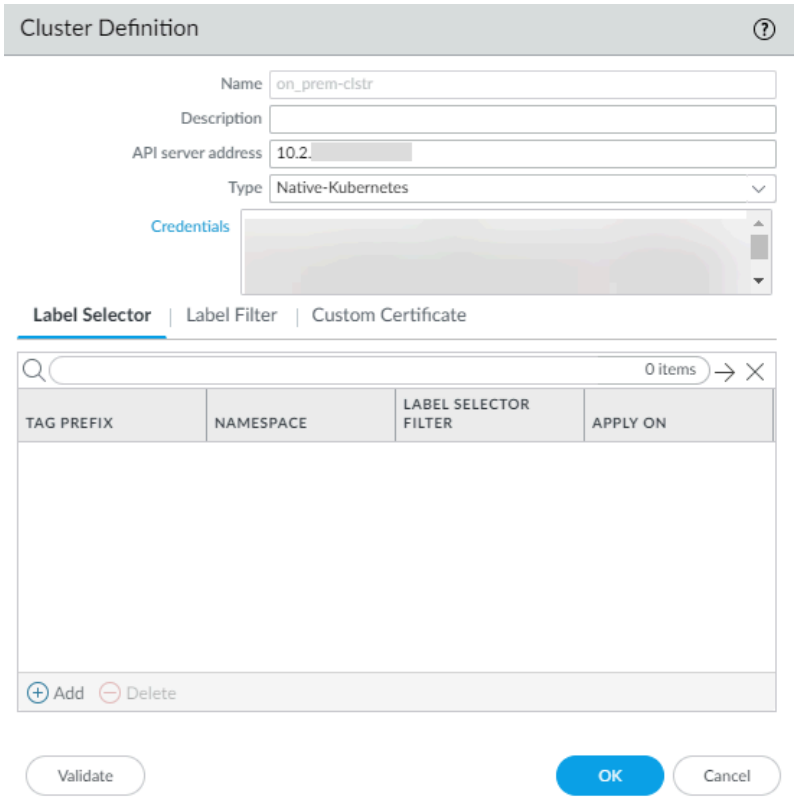
   可用選項為 [AKS]、[EKS]、[GKE]、[Native Kubernetes（原生 Kubernetes）]、[OpenShift] 和 [Other（其他）]。

5. 上傳 Panorama 與叢集通訊所需的服務帳戶 **Credential**（認證）。如 建立叢集驗證的服務帳戶 工作流程中所述，此服務帳戶的檔案名稱是 `plugin-svc-acct.json`。

   如果您透過 *CLI/API* 上傳服務認證，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*。如果您於 *GUI* 上傳服務認證檔案，則不需要這些步驟。

6. 按一下 **OK**（確定）。

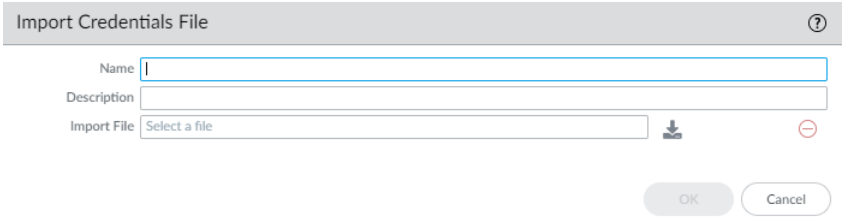
您可以保留「標籤篩選」和「標籤選取器」設定以供稍後使用。此選用任務可讓您擷取您要 Panorama 為其建立標記的任何自訂或使用者定義的標籤。



STEP 9 | （選用）如果您的 Kubernetes 叢集 API 伺服器憑證是由憑證鏈進行簽置，則 Panorama 之 Kubernetes 外掛程式的認證需要鏈中的每個憑證。如果您的 API 伺服器使用憑證鏈，則您必須將鏈中的所有憑證都合併到單一 .crt 檔案，並將其新增至外掛程式。

Kubernetes 外掛程式最多支援四個憑證。

1. 選取 **Panorama** > **Kubernetes** > **Setup**（設定） > **Cluster**（叢集） > **Add**（新增） > **Custom Certificate**（自訂憑證） > **Add**（新增），以匯入憑證檔案。
2. 輸入描述性的 **Name**（名稱）。
3. （選用）輸入 **Description**（說明）。
4. 按一下匯入圖示，並導覽至憑證檔案。
5. 按一下 **OK**（確定）。



STEP 10 | （選用）設定每個叢集的 Proxy。

與其他外掛程式不同，Kubernetes 外掛程式不會使用 **Panorma** > **Setup**（設定） > **Services**（服務）下設定的 Proxy。相反地，如果您想要啟用或略過 Proxy，則必須輸入每個叢集的 Proxy。設定時，Kubernetes 外掛程式使用此 Proxy 伺服器 IP 位址對此叢集的 API 伺服器進行所有 API 呼叫。

1. 登入 Panorama 上的 CLI。
2. 輸入下列 CLI 命令來設定此 Kubernetes 叢集的 Proxy 伺服器。

   ```
   > configure> set plugins kubernetes setup cluster-credentials <cluster-name>  cluster-proxy enable-proxy <yes/no> proxy-port <port>  proxy-server <IP> proxy-user <username>  secure-proxy-password <password>
   *** username and password are optional ***
   ```

STEP 11 | 接下來的步驟：

1. 取得 CN-Series 部署的映像檔和檔案
2. 部署 CN-Series 防火牆
3. 設定 Panorama 保護 Kubernetes 部署

取得 CN-Series 部署的映像檔和檔案

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

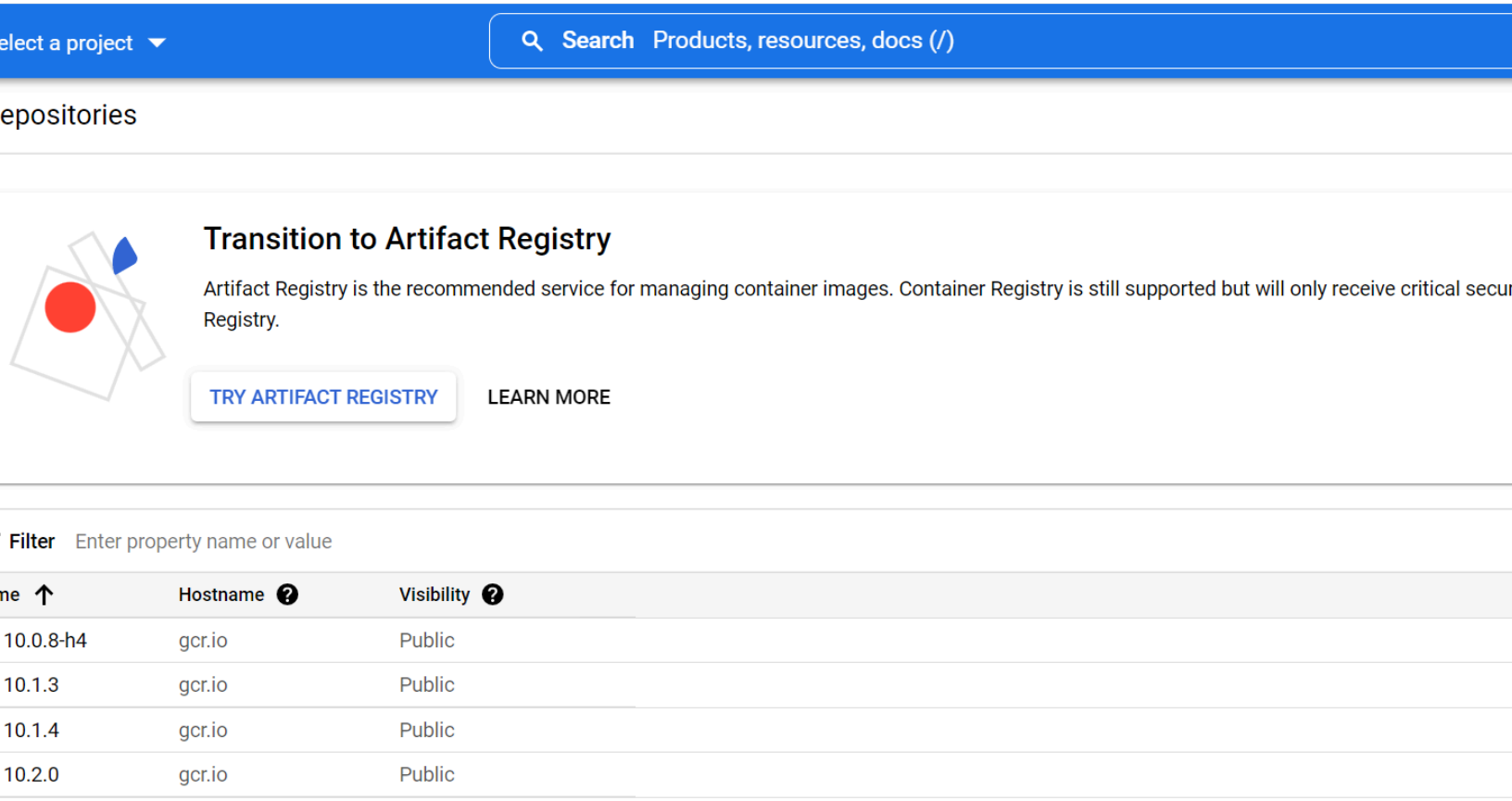
在開始部署之前，請參閱下表，確保您已下載相容的檔案。

PAN-OS 版本	**YAML** 版本	**CNI** 版本	**MGMT-INIT** 版本
PAN-OS 11.1.x	3.0.x	3.0.x	3.0.x
PAN-OS 11.0.x	3.0.x	3.0.x	3.0.x
PAN-OS 10.2.x	3.0.x	3.0.x	3.0.x
PAN-OS 10.1.x	3.0.x	3.0.x	3.0.x
PAN-OS 10.0.x	1.0.x	1.0.x	3.0.x

請透過下列步驟從 Google Cloud Platform 的公用容器登錄中擷取 Docker 映像，然後繼續部署 CN-Series 防火牆：

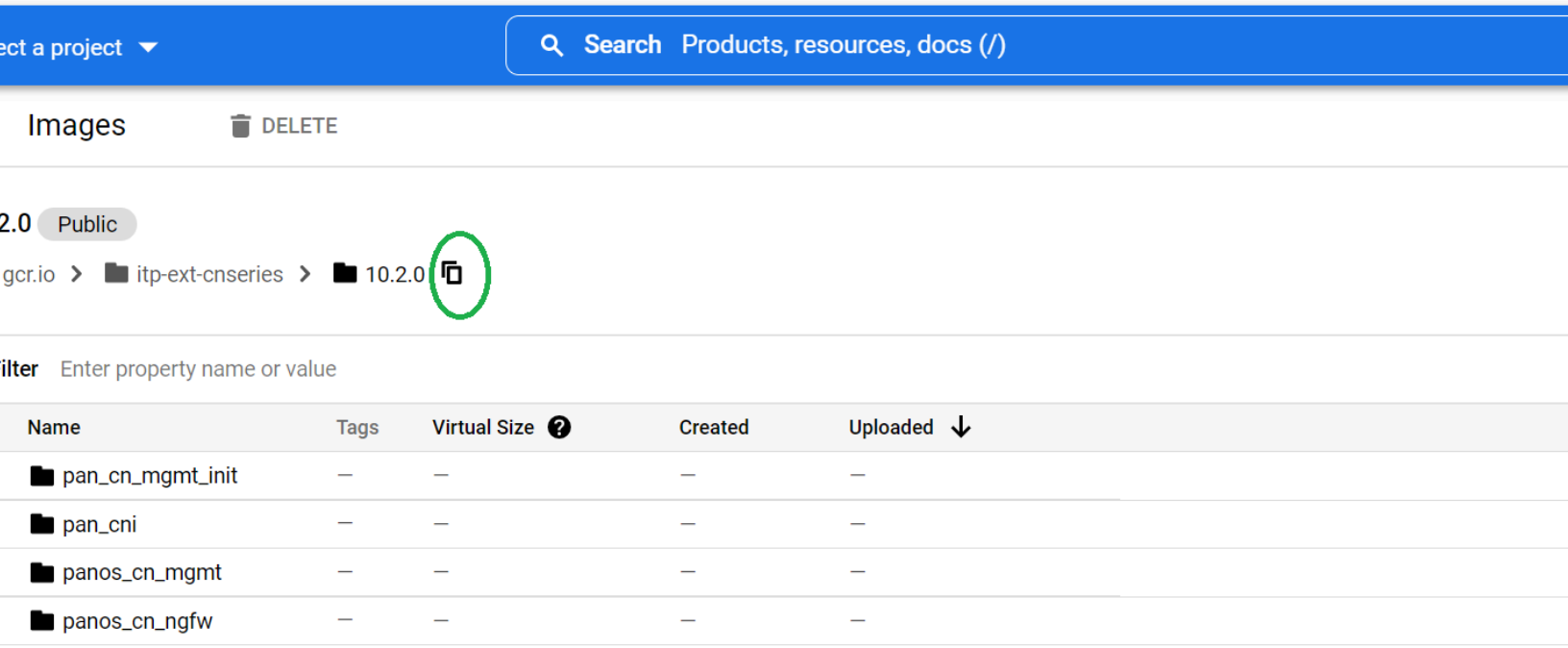
來自公用容器登錄的 **Docker** 映像：

1. 根據您的 PAN-OS 版本，從公用雲端儲存庫中提取所需的 Docker 映像。



2. 選取所需的 PAN OS 版本。

3. 將每個映像路徑的連結複製至部署 YAML 檔案中的適當位置。



請執行下列動作，以從 GitHub 取得 YAML 檔案：

1. 開啟您計劃使用之部署方法的資料夾：DaemonSet、Kubernetes 服務或 Kubernetes CNF。
2. 從對應於您環境的資料夾下載 yaml 檔案。

   從 Native-k8s 資料夾中取得檔案，以與內部部署或雲端部署中的原生 Kubernetes 搭配使用。

   從 GKE 的個別受管理 Kubernetes 資料夾中取得檔案。

來自 **Palo Alto Networks CSP** 的 **Docker** 映像：

使用下列步驟以從 GitHub 取得 YAML 檔案，以及從 Palo Alto Networks CSP 下載 Docker 映像，並將其推送至私人登錄，再繼續部署 CN-Series 防火牆。

STEP 1 | 下載 Docker 映像檔和 YAML 檔案。

1. 從 Palo Alto Networks Customer Support Portal (CSP) 取得壓縮 tar 封存檔。
   1. 使用您的支援帳戶登入 CSP。
   2. 選取 **Updates**（更新） > **Software Updates**（軟體更新）。
   3. 從 **Please Select**（請選取）下拉式清單中，選取 **PAN-OS Container Images**（**PAN-OS** 容器映像檔）。
   4. 為您要部署的 PAN-OS 版本下載下列檔案。

      PanOS_cn-X.X.X.tgz - 適用於 CN-MGMT 和 CN-NGFW Pod。

      Pan_cn_mgmt_init-X.X.X.tgz - 適用於執行為 CN-MGMT Pod 一部分的 init 容器。

      Pan_cni-2.0.0.tgz - 適用於 PAN-CNI Pod。
2. 從 GitHub 中取得 YAML 檔案。
   1. 開啟您計劃使用之部署方法的資料夾：DaemonSet、Kubernetes 服務或 Kubernetes CNF。
   2. 從對應於您環境的資料夾下載 yaml 檔案。

      從 Native-k8s 資料夾中取得檔案，以與內部部署或雲端部署中的原生 Kubernetes 搭配使用。

      從 AKS、EKS 或 GKE 的個別受管理 Kubernetes 資料夾中取得檔案。

STEP 2 | 擷取 Docker 映像檔，並將它推送至容器登錄。

例如，在 GKE 部署上，您將映像檔上傳至 GKE 上的「容器登錄」，並取得在 YAML 檔案中進行參照的映像檔路徑。請在執行 Docker 引擎的用戶端系統上使用下列命令。

將下列步驟中的 *x* 變數取代為符合您所使用映像檔版本的值。例如，*Pan_cn_mgmt-init-2.0.0.tgz* 或 *pan_cni:2.0.0*。

1. 載入映像檔。

   ```
   docker load -i PanOS_cn-x.x.x.tgz
   ```

   ```
   docker load -i Pan_cn_mgmt-init-x.x.x.tgz
   ```

   ```
   docker load -i Pan_cni-x.x.x.tgz
   ```

   在這些步驟之後，「Docker 映像檔」將會顯示映像檔，例如，「paloaltonetworks/panos_cn_mgmt:x.x.x」。

2. 標記這些映像檔，以包括私人登錄詳細資料。

   ```
   docker tag paloaltonetworks/panos_cn_mgmt:x.x.x <your_registry>/paloaltonetworks/panos_cn_mgmt:x.x.x
   ```

   ```
   docker tag paloaltonetworks/panos_cn_ngfw:x.x.x <your_registry>/paloaltonetworks/panos_cn_ngfw:x.x.x
   ```

   ```
   docker tag paloaltonetworks/pan_cn_mgmt_init:x.x.x <your_registry>/paloaltonetworks/pan_cn_mgmt_init:x.x.x
   ```

   ```
   docker tag paloaltonetworks/pan_cni:x.x.x <your_registry>/paloaltonetworks/pan_cni:x.x.x
   ```

3. 將這些映像檔推送至私人登錄。

   ```
   docker push <your_registry>/paloaltonetworks/panos_cn_mgmt:x.x.x
   ```

   ```
   docker push <your_registry>/paloaltonetworks/panos_cn_ngfw:x.x.x
   ```

   ```
   docker push <your_registry>/paloaltonetworks/pan_cn_mgmt_init:x.x.x
   ```

   ```
   docker push <your_registry>/paloaltonetworks/pan_cni:x.x.x
   ```

具 CN-Series 防火牆的 Strata 記錄日誌服務

我可以在哪裡使用這個？	我需要哪些內容？
• 具 CN-Series 防火牆的 Strata 記錄日誌服務	• Panorama 執行至少 PAN-OS 11.1 版本 • Strata 記錄日誌服務授權

Strata 記錄日誌服務透過業界唯一標準來標準化和聯結企業資料，達成以 AI 為基礎的網路安全創新。如需更多詳細資訊，請參閱 Strata 日誌記錄服務簡介和 Panorama 受管理防火牆的 Strata 日誌記錄服務。Strata 記錄日誌服務現在可以從 CN-Series 新世代防火牆收集日誌資料。當您購買 Strata 記錄日誌服務授權時，註冊到您支援帳戶的所有防火牆都會收到 Strata 記錄日誌服務授權。您也會收到一個連結，您需要透過這個連結來啟動 Strata 記錄日誌服務執行個體。

若要開始使用 CN-Series 防火牆 Strata 日誌記錄服務日誌，您必須先確認已為 CN-Series 防火牆安裝 Kubernetes 外掛程式並設定 Panorama。請向 CN-MGMT Pod 提供裝置憑證才能進行 Strata 記錄日誌服務連線。請務必使用 CSP 帳戶註冊 CN-MGMT Pod，以確保 CN-MGMT Pod 確實反映在您的 Strata 記錄日誌服務執行個體。將有效 PIN-ID 和 PIN-value 新增至 `pan-cn-mgmt-secret.yaml` 檔案，以成功安裝裝置憑證。CN-Series 防火牆需要能授權安全存取 Strata 記錄日誌服務的裝置憑證。如需更多詳細資訊，請參閱在 CN-Series 防火牆上安裝裝置憑證。

部署 CN-Series 防火牆後，請確認您的 CN-MGMT Pod 是否出現在您客戶支援入口網站帳戶的 **Registered Devices**（已註冊裝置）下。如需更多詳細資訊，請參閱註冊防火牆。請使用 Panorama 設定 CN-Series 防火牆，在 CSP 帳戶上建立 CN-Series 部署設定檔，並使用授權碼將授權從 Panorama 推送到 CN-Series 防火牆。

設定具 **CN-Series** 防火牆的 **Strata** 記錄日誌服務

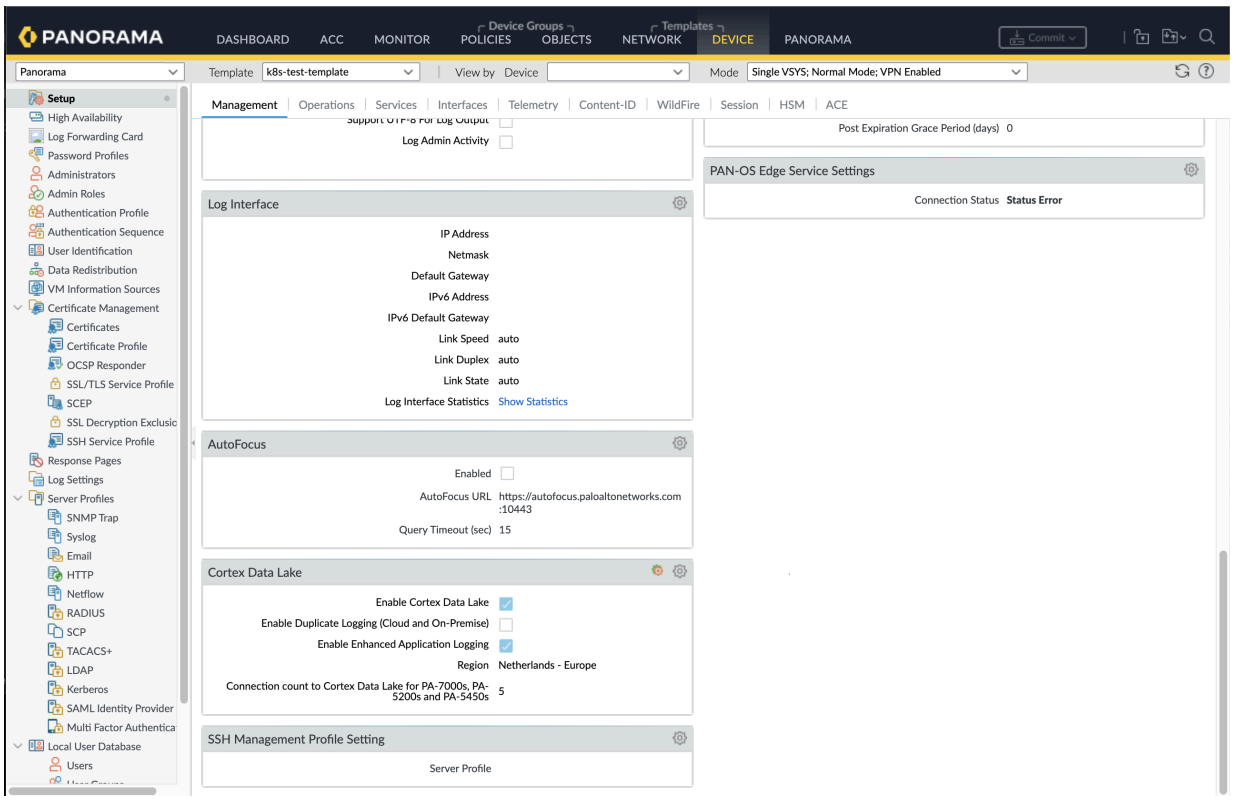
Strata 記錄日誌服務為雲端交付的服務和應用程式提供基於雲端的集中式日誌儲存和整合。

請務必擁有日誌記錄授權且在您的 *CSP* 帳戶中建立 *Strata* 記錄日誌服務執行個體。如需更多詳細資訊，請參閱 Strata 記錄日誌服務。

請完成以下步驟，在 Panorama 上設定 Strata 記錄日誌服務並將其推送到防火牆：

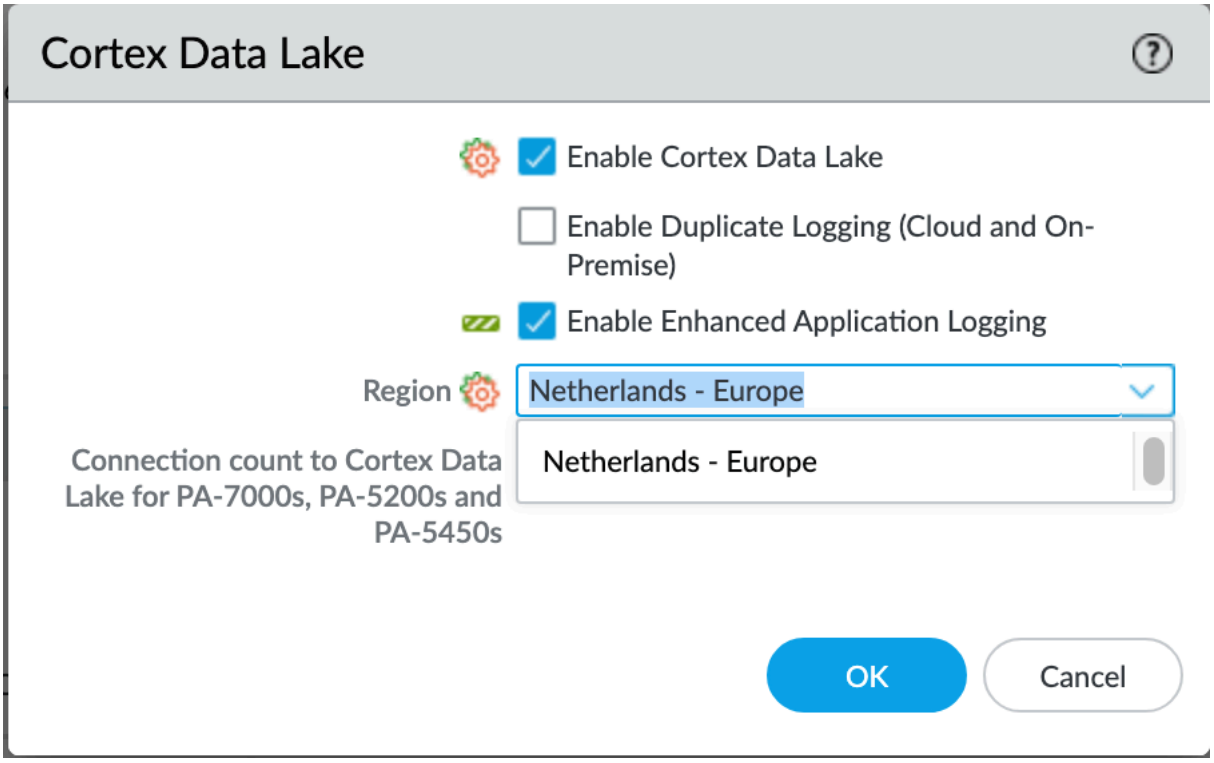
1. 掛載您的 Panorama 到 Strata 記錄日誌服務，以在裝置上啟用 Strata 記錄日誌服務的設定。
2. 掛載 CN-Series 防火牆到 Strata 記錄日誌服務執行個體。

3. 在 panorama 中，前往 **Device**（裝置）頁籤，按 **Strata Logging Service**（**Strata** 記錄日誌服務）窗格的 **Settings**（設定）。



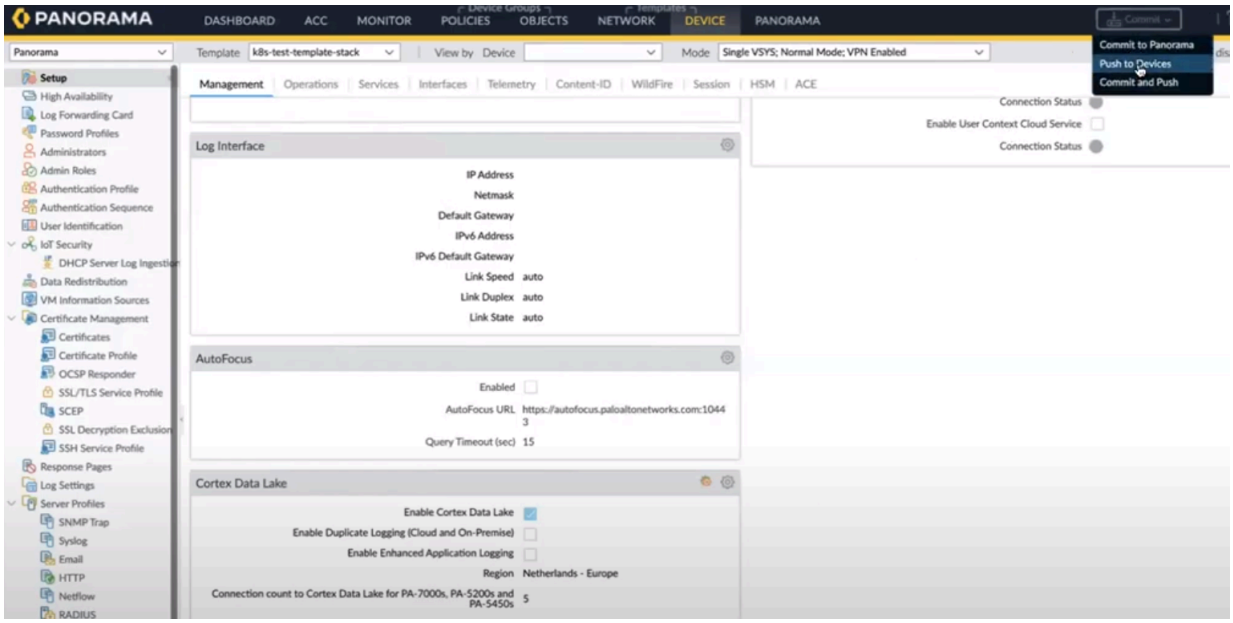
現在您可以看到該 **Region**（區域）已填滿。

4. 按一下 **Enable Strata Logging Service**（啟用 **Strata** 記錄日誌服務）。



5. 按一下 **OK**（確定）。

6. 前往 **Commit**（提交）> **Push to Devices**（推送至裝置）。



7. 選擇您的 **CN-MGMT** Pod。

8. 按一下 **OK**（確定）。已推送

   CN-MGMT Pod 的 Strata 記錄日誌服務設定。CN-MGMT Pod 現在將啟動與 Strata 記錄日誌服務執行個體的連線。

一旦您的掛載防火牆處於 **connected**（已連線）狀態，您就可以開始向 Strata 記錄日誌服務執行個體傳送日誌。如需更多詳細資訊，請參閱開始向 Strata 記錄日誌服務傳送日誌（Panorama 管理）。

CN-Series 防火牆的 IOT 安全性支援

我可以在哪裡使用這個？	我需要哪些內容？
• CN-Series 防火牆的 IoT 安全性	• 資料儲存在 Strata 記錄日誌服務的 IoT 訂閱的 Strata 記錄日誌服務授權 • Panorama 執行至少 PAN-OS 11.1 版本

如果是 Palo Alto Networks 新世代 CN-Series 防火牆，IoT 安全性解決方案會使用機器學習 (ML)，根據從防火牆接收的日誌中的中繼資料來瞭解已發現的 IoT 裝置。IoT 安全性也可以根據裝置的網路流量行為和動態更新的威脅摘要，來識別裝置中的弱點並評估風險。

為 CN-Series 防火牆手動新增規則時，您可以參考 IoT 安全性產生的政策規則建議。無論 PAN-OS 版本為何，IoT 安全性一律會產生安全性政策規則建議。

使用 ***IoT Security Subscription***（***IoT*** 安全性訂閱）（將資料儲存在 *Strata* 記錄日誌服務中）時，每個帳戶需要一個 *Strata* 記錄日誌服務授權，且必須確保 CN-Series 防火牆的 Strata 記錄日誌服務設定已完成。

如需更多詳細資訊，請參閱 IoT 安全性先決條件。

設定 **CN-Series** 防火牆的 **IOT** 支援

您必須確保您的環境符合使用 CN-Series 防火牆部署 IoT 安全性的所有先決條件。如需更多詳細資訊，請參閱 IoT 安全性先決條件。

若要設定 CN-Series 防火牆的 **IoT - Requires Data Lake**（**IoT -** 需要 **Data Lake**）訂閱，您必須完成以下步驟：

您必須將 *Panorama* 掛載到 *Strata* 日誌記錄服務執行個體。如需更多詳細資訊，請參閱以 Panorama 掛載防火牆。

1. 建立租用戶服務群組 (TSG)。如需更多詳細資訊，請參閱透過常見服務啟動 IoT 安全性訂閱中的 **Step 3**（步驟 **3**）。
2. 將 Strata 日誌記錄服務租用戶掛載到 TSG。在 TSG 中使用之前，請確認您已購買 Strata 日誌記錄服務並使用連結啟動它。
3. 透過 **IoT - Requires Data Lake**（**IoT -** 需要 **Data Lake**）選項建立 CN-Series 部署設定檔。
4. 按一下 **Finish Setup**（完成設定）。將部署設定檔關聯到 TSG 並按一下 **Activate**（啟動）後，系統將建立 IoT 租用戶（如果尚不存在）。

   然後，您可以將收集到的中繼資料轉送至基於雲端的日誌記錄服務，其中 IoT 安全性會用以識別網路上的各種 IoT 裝置。
5. 佈建 Panorama 並產生序號。如需更多詳細資訊，請參閱註冊 Panorama 並安裝授權。

6. 透過授權碼以 Panorama 設定 CN-Series 防火牆，以使用 kubernetes 外掛程式將授權從 Panorama 推送到 CN-Series 防火牆。如需更多詳細資訊，請參閱設定 Panorama 以保護 Kubernetes 部署。

   將部署授權碼套用到 Panorama 中的 Kubernetes 外掛程式。

   您現在可以在 IoT 租用戶上看到 CN-series 防火牆。
7. 設定範本 vwire 以允許並啟用區域中的裝置 ID。

   您可以使用預設範本 **K8S-Network-Setup-V2** 並在該範本中進行以下變更：

   - 為預設 vwire 啟用連結狀態直通和多點傳送防火牆。
   - 啟用預設區域的裝置識別。

   如需更多詳細資訊，請參閱設定虛擬介接。
8. 設定 **Enable Cortex Data Lake**（啟用 **Cortex Data Lake**）和 **Enable Enhanced Application Logging**（啟用增強型應用程式記錄）選項 Panorama 到 CN-Series 防火牆。如需更多詳細資訊，請參閱 CN-Series 防火牆的 Strata 日誌記錄服務設定。

若要設定 CN-Series 防火牆的 **IoT Security, Doesn't Require Data Lake**（**IoT** 安全性，不需要 **Data Lake**）訂閱，您必須先完成以下步驟：

Note（註）：您必須將 Panorama 掛載到 Strata 日誌記錄服務執行個體。使用 IoT 安全性 - 不需要 Data Lake 訂閱時，您必須在新增 CN-series 防火牆後在 IoT 入口網站中註冊 Panorama。如需更多詳細資訊，請參閱為 IoT 安全性準備防火牆的 **Step 2**（步驟 **2**）。

1. 建立租用戶服務群組 (TSG)。如需更多詳細資訊，請參閱透過常見服務啟動 IoT 安全性訂閱中的 **Step 3**（步驟 **3**）。
2. 透過 **IoT - Doesn’t Require Data Lake**（**IoT** - 不需要 **Data Lake**）選項建立 CN-Series 部署設定檔。
3. 設定您的 IOT 執行個體並選取 **Finish Setup**（完成設定），將您的部署設定檔與租用戶服務群組 (TSG) 建立關聯，以在 CN-Series 防火牆上啟用日誌記錄服務並將其設為取得和記錄網路流量中繼資料。如需更多詳細資訊，請參閱為 IoT 安全性準備防火牆。

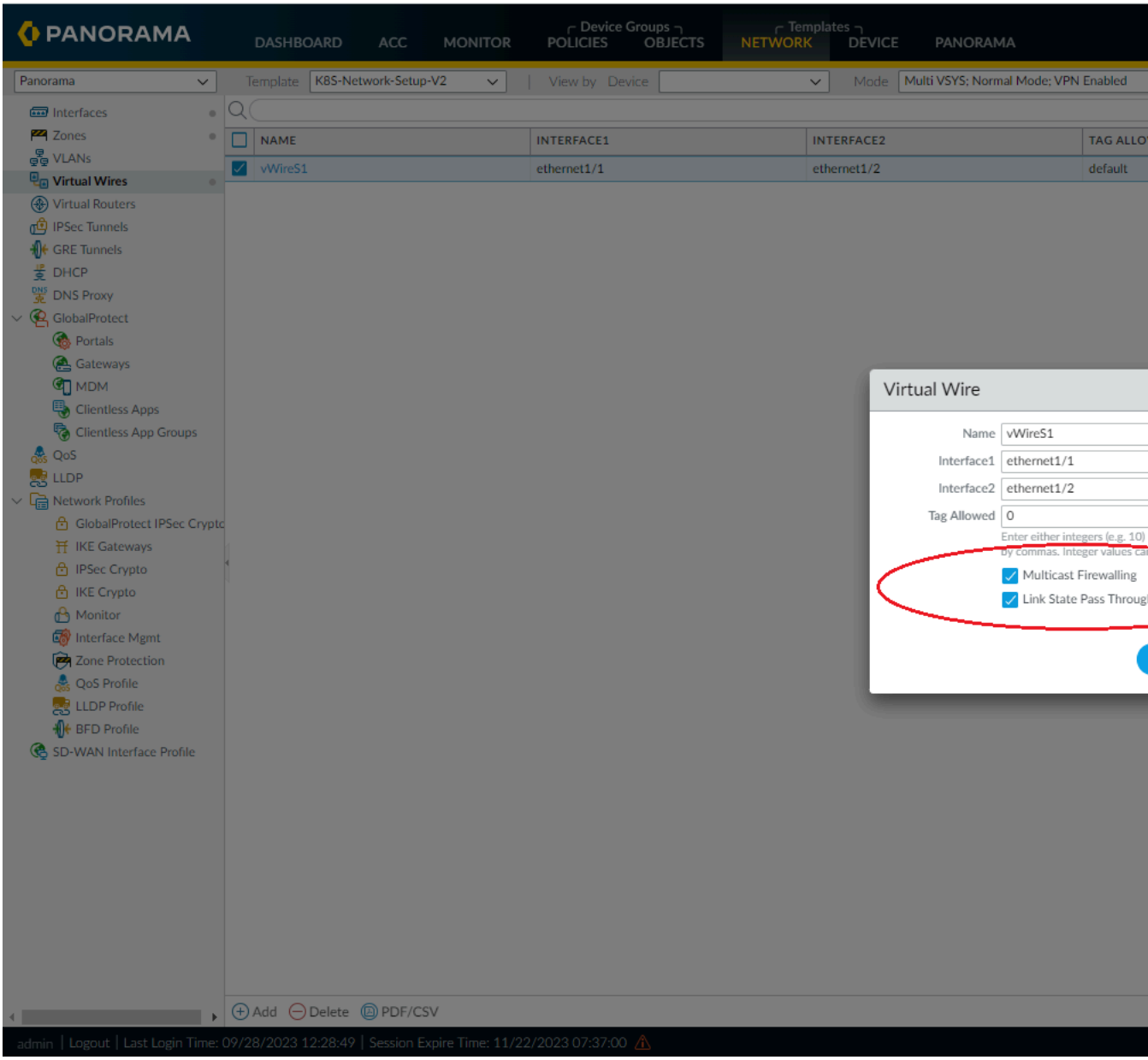
   然後，您可以將收集到的中繼資料轉送至基於雲端的日誌記錄服務，其中 IoT 安全性會用以識別網路上的各種 IoT 裝置。
4. 佈建 Panorama 並產生序號。如需更多詳細資訊，請參閱註冊 Panorama 並安裝授權。
5. 透過授權碼以 Panorama 設定 CN-Series 防火牆，以使用 kubernetes 外掛程式將授權從 Panorama 推送到 CN-Series 防火牆。如需更多詳細資訊，請參閱設定 Panorama 以保護 Kubernetes 部署。

   將部署授權碼套用到 Panorama 中的 Kubernetes 外掛程式。您現在可以在 IoT 租用戶上看到 CN-series 防火牆。

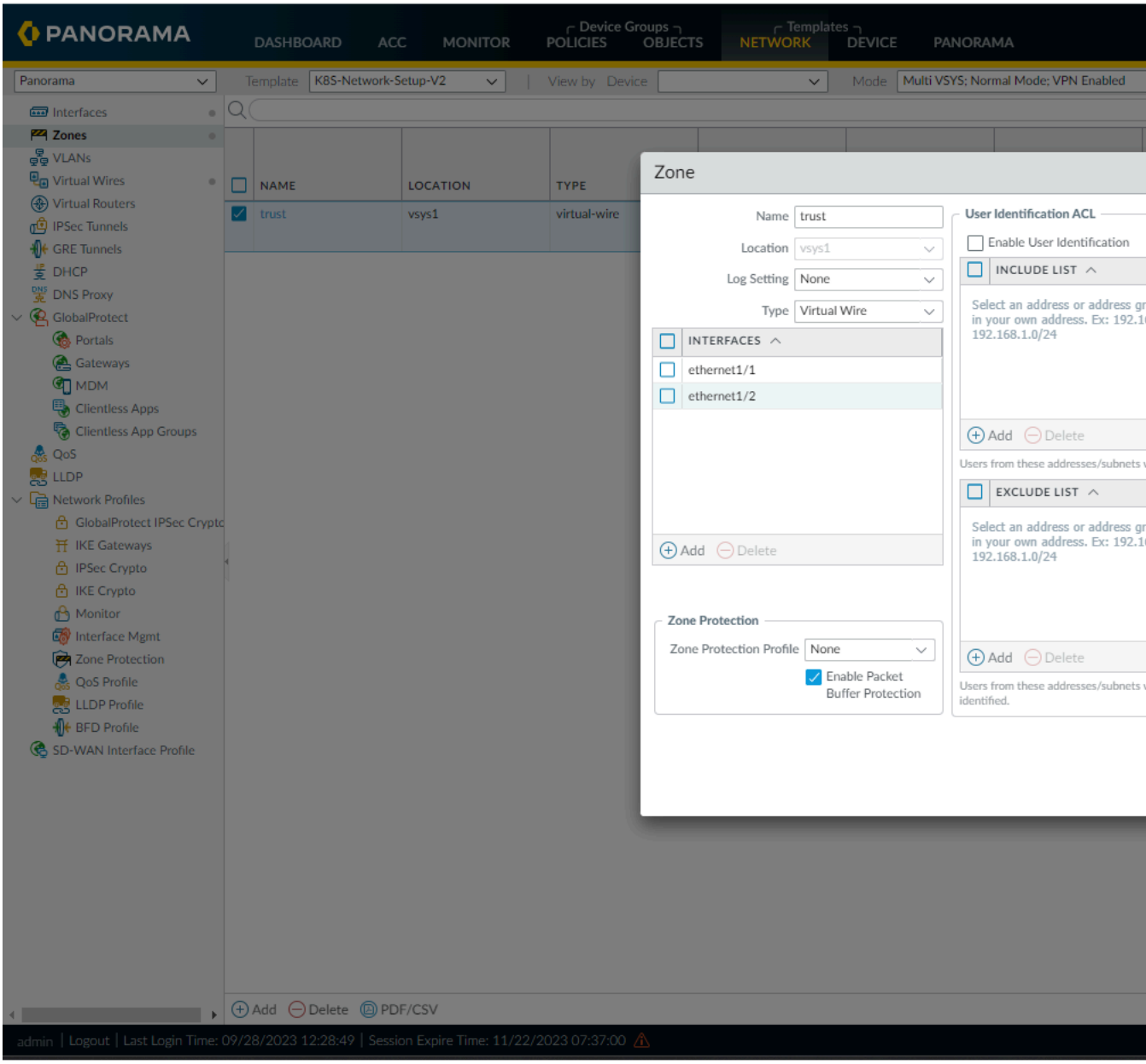
6. 設定範本 vwire 以允許並啟用區域中的裝置 ID。如需更多詳細資訊，請參閱設定虛擬介接。

   您可以使用預設範本 **K8S-Network-Setup-V** 並在該範本中進行以下變更：

   - 為預設 vwire 啟用連結狀態直通和多點傳送防火牆。



   - 啟用預設區域的裝置識別。



如需更多詳細資訊，請參閱設定虛擬介接。

k8s-template-v2 中設定的 Vwire 允許連結狀態通過和多點傳送防火牆。k8s-template-v2 的區域設定會啟用裝置識別

7. 設定 **Enable Cortex Data Lake**（啟用 **Cortex Data Lake**）和 **Enable Enhanced Application Logging**（啟用增強型應用程式記錄）選項 Panorama 到 CN-Series 防火牆。如需更多詳細資訊，請參閱 CN-Series 防火牆的 Strata 日誌記錄服務設定

成功將 Panorama 和 CN-Series 防火牆掛載到基於雲端的日誌記錄服務後，請前往您的 IoT 執行個體。

IoT 安全性擁有足夠資訊來從網路行為中識別裝置後，它會為 CN-Series 防火牆提供 IP 位址到裝置的對應，並為 Panorama 提供政策建議，Panorama 管理員可以匯入這些建議，然後推送到 CN-Series 防火牆以強制執行 IoT 裝置流量的政策。

按一下 IoT 安全性入口網站的 **Administration**（管理）> **Sites and Firewalls**（網站和防火牆）> **Firewalls**（防火牆），檢視日誌記錄服務串流到 IoT 安全性應用程式的日誌的狀態。如需更多詳細資訊，請參閱 IoT 安全性與防火牆的整合狀態。

CN-Series 防火牆上基於軟體直通的卸載

我可以在哪裡使用這個？	我需要哪些內容？
• CN-Series 作為 Kubernetes CNF 部署	• CN-Series 10.1.x or above Container Images • 針對 Panorama 管理的 CN-Series 防火牆，Panorama 執行 PAN-OS 11.0.4 或更新版本

概要

藉由基於軟體直通的智慧流量卸載 (ITO) 服務，CN-Series 防火牆能夠兼顧網路效能、安全性和成本。針對網路上的每個新流量，ITO 服務會判定該流量是否可以從安全檢查中受益。ITO 服務會將流量的前幾個封包路由到防火牆進行檢查，防火牆會決定是否檢查或卸載流量中的其餘封包。此判定結果是根據政策或由於流量無法供檢查。如果僅檢查可從安全檢查中受益的流量，則防火牆的整體負載會減少且效能會提高，同時兼顧安全狀況。

針對缺乏 DPU 的架構，基於軟體直通的 ITO 能夠利用可用的 NIC 來運作。請參閱超管理器支援矩陣以瞭解受支援的 NIC 和超管理器。

基於軟體直通的卸載支援 GTP-U 通道通訊協定。在 GTP-U 內，與 GTPU 內部工作階段軟體協調 Universal Time-through，在 GTPU 內部工作階段完成第七層檢查後，GTPU 封包會遵循現有軟體直通資料路徑、繞過不必要的操作、利用 FIB /MAC 快取，並執行完成。將 CN-Series 防火牆部署為 Kubernetes CNF 服務時，CN-Series 防火牆支援 GTP-U 特定流量卸載的 PAN-OS 軟體直通功能。

CN-Series 防火牆的 **GTP-U** 特定流量卸載

GTP 包括控制平面 (GTP-C)、使用者平面 (GTP-U) 和在 UDP/IP 上的計費（源自 GTP-C 的 GTP）傳輸流量。依支援 GTP 的型號檢視 PAN-OS 版本和 GTPv1-C、GTPv2-C 和 GTP-U 支援的 3GPP 技術標準。在 Palo Alto Networks® 防火牆上啟用 GTP 安全性，讓您保護行動核心網路架構免受格式錯誤的 GTP 封包、拒絕服務攻擊和狀態不良 GTP 訊息的影響，同時能保護行動訂閱者免受詐騙 IP 封包和過度收費攻擊。

GTP-U 定義於 3GPP TS 29.281。它跨多個訊號介面（例如 S1、S5 和 S8）封裝和路由使用者平面流量。GTP-U 訊息為使用者平面或訊號訊息。GTP-U 的註冊連接埠號碼是 2152。如需更多詳細資訊，請參閱 GTP 保護設定檔。

CN-Series 上基於軟體直通的卸載也支援 GTP-U 流量卸載。現在您可以將 CN-Series 上的智慧流量卸載訂閱作為 Kubernetes CNF 模式，以享有更高效能並利用 GTP 安全性保護行動網路。針對 CN-Series 作為 Kubernetes CNF 模式將檢查的每個 GTP-U 封包，系統將在內部工作階段上完成完整的

第七層檢查。如果防火牆確定此 GTP-U 封包的內部工作階段符合卸載條件，則屬於此工作階段的所有後續 GTP-U 封包都會被卸載。

以下是在 CN-Series 防火牆上設定基於軟體直通的卸載之前需考慮的重要事項：

- 根據預設，基於軟體直通的 ITO 設定為停用。
- 您只能使用 bootstrap/CLI 啟用此功能。
- 您可以在基於軟體直通的 ITO 中同時使用一般流量和 GTP-U 卸載的基於軟體直通的 ITO。
- 若要升級到啟用 ITO 的目前版本，請使用 CLI 升級後啟用工作階段卸載。

CN-Series 中，只有 *CN-Series* 作為 *Kubernetes CNF* 部署模式支援基於軟體直通的 *ITO*。

在 **CN-Series** 防火牆上啟用 **GTP-U** 內部工作階段卸載

若要在 CN-Series 防火牆上啟用 GTP-U 內部工作階段卸載，以下是啟用 GTP 安全性或 5G 安全性的先決條件。

您必須編輯 **`pan-cn-mgmt-configmap.yaml`** 檔案並進行以下變更：

在 `pan-cn-mgmt-configmap.yaml` 檔案中，`PAN_GTP_ENABLED`、`PAN_GTP_CUT_THRU` 和 `PAN_SW_CUT_THRU` 參數值必須為 `true` 才能啟用 GTP-U 內部工作階段卸載。

以下是更新後的 `pan-cn-mgmt-configmap.yaml` 檔案範例：

```
# 在啟用 GTP 的情況下啟動 MGMT Pod。為了獲得完整功能，您也需在 Panorama 上
啟用 GTP #。PAN_GTP_ENABLED: "true" # 在啟用 GTP SW 直通的情況下啟動
 MGMT Pod。PAN_GTP_CUT_THRU: "true" # 在啟用 SW 直通的情況下啟動 MGMT
 Pod。PAN_SW_CUT_THRU: "true"
```