paloalto TECHDOCS

VM-Series 部署指南

Version 10.2



docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2021-2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

February 26, 2022

Table of Contents

關於 VM-Series 防火牆 13
VM-Series 部署 14
高可用性 VM-Series 15
升級 VM-Series 防火牆 17
升級 PAN-OS 軟體版本（獨立版本） 17
升級 PAN-OS 軟體版本（HA 配對） 19
使用 Panorama 升級 PAN-OS 軟體版本 23
升級 PAN-OS 軟體版本（NSX 專用 VM-Series） 26
升級 VM-Series 型號 31
升級 HA 配對中的 VM-Series 型號 32
將 VM-Series 防火牆降級為舊版 33
VM-Series 外掛程式 35
在防火牆上設定 VM-Series 外掛程式 35
升級 VM-Series 外掛程式 36
在 VM-Series 防火牆上啟用巨型框架 39
Hypervisor 指派的 MAC 位址 41
發佈自訂 PAN-OS 度量以作為監控使用 42
存取 VM-Series 防火牆外部服務所使用的介面 44
PacketMMAP 和 DPDK 驅動程式支援 45
在 VM-Series 上啟用 NUMA 效能最佳化 47
在 VM-Series 防火牆上啟用 ZRAM 49
授權 VM-Series 防火牆 51
VM-Series 防火牆授權 52
授權類型 52
彈性 vCPU 和固定型號授權 53
彈性 vCPU 和固定型號部署 54
建立支援帳戶 56
VM-Series 防火牆的序號和 CPU ID 格式 57
授權 API 58
管理授權 API 金鑰 58
使用授權 API 59
授權 API 錯誤代碼 62
安裝授權 API 金鑰 64
使用基於 Panorama 的軟體防火牆授權管理 65
軟體 NGFW 積分 70
基於層和記憶體的最大限制 72

©2023 Palo Alto Networks, Inc.

啟動積分 82
建立部署設定檔 83
管理部署設定檔 84
註冊 VM-Series 防火牆（軟體 NGFW 積分） 85
佈建 Panorama 88
將 Panorama 移轉至軟體 NGFW 授權 89
轉移積分 93
更新您的軟體 NGFW 積分授權 95
停用授權（軟體 NGFW 積分） 96
設定已授權的 vCPU 數量 98
自訂資料平面核心 98
將防火牆移轉到彈性 VM-Series 授權 99
VM-Series 型號 104
VM-Series 系統需求 105
CPU 過度訂閱 107
VM-50 Lite 模式 108
VM-Series 型號授權類型 108
啟動 VM-Series 型號授權 119
註冊 VM-Series 防火牆 125
在 VM-Series 防火牆上安裝裝置憑證 128
在 BYOL 和 PAYG 授權之間切換 130
切換 VM-Series 型號授權 131
停用授權 134
更新 VM 系列防火牆授權搭售包 139
當授權到期時會怎麼樣？ 141
Cloud Security Service Provider（雲端安全服務供應商 - CSSP）的授權 144
取得 CSSP 授權套件的驗證碼 144
使用 CSSP 驗證碼註冊 VM-Series 防火牆 145
針對已註冊的 VM-Series 防火牆新增一般客戶資訊 146
在 ESXi 伺服器上設定 VM-Series 防火牆 149
VMware vSphere Hypervisor (ESXi) 上支援的部署 150
ESXi 上的 VM-Series—系統需求及限制 151
ESXi 上的 VM-Series—系統需求 151
ESXi 上的 VM-Series—系統限制 152
在 VMware vSphere Hypervisor (ESXi) 上安裝 VM-Series 防火牆 153
規劃 ESXi 專用 VM-Series 的介面 153
在 ESXi 伺服器上佈建 VM-Series 防火牆 154
在 ESXi 的 VM-Series 上執行初始組態 157

©2023 Palo Alto Networks, Inc.

將額外磁碟空間新增至 VM-Series 防火牆 158
在 ESXi 及 vCloud Air 上的 VM-Series 防火牆上使用 VMware 工具 159
使用 vMotion 在主機之間移動 VM-Series 防火牆 161
使用 VM-Series CLI 在 ESXi 上交換管理介面 162
vCenter 上的 VM 監控 163
關於 VMware vCenter 上的 VM 監控 163
安裝 VMware vCenter 專用 Panorama 外掛程式 164
設定 VMware vCenter 專用 Panorama 外掛程式 165
ESXi 部署的疑難排解 168
基本疑難排解 168
安裝問題 168
授權問題 170
連線問題 170
ESXi 專用 VM-Series 的效能調整 172
在 ESXi 上安裝 NIC 驅動程式 172
在 ESXi 上啟用 DPDK 173
在 ESXi 上啟用 SR-IOV 173
透過 SR-IOV 啟用 ESXi VLAN 存取模式 174
在 ESXi 上啟用 NIC 的多佇列支援 176
VNF 效能調整 176
在 vCloud Air 上設定 VM-Series 防火牆 189
關於 vCloud Air 上的 VM-Series 防火牆 190
vCloud Air 上支援的部署 191
在 vCloud Air 上部署 VM-Series 防火牆 192
在 VMware NSX-T 上設定 VM-Series 防火牆 199
在 VMware NSX-T（南北向）上設定 VM-Series 防火牆 200
VMware NSX-T（南北向）上支援的 VM-Series 防火牆部署 200
NSX-T（南北向）上的 VM-Series 防火牆元件 200
在 NSX-T（南北向）上部署 VM-Series 防火牆 202
將安全性政策從 NSX-V 延伸至 NSX-T 214
在 NSX-T（東西向）上設定 VM-Series 防火牆 216
NSX-T（東西向）上的 VM-Series 防火牆元件 216
NSX-T（東西向）整合的 VM-Series 防火牆 217
VMware NSX-T（東西向）上支援的 VM-Series 防火牆部署 219
使用以操作為中心的工作流程部署 VM-Series 220
使用以安全性為中心的工作流程部署 VM-Series 237
從 Panorama 刪除服務定義 266

©2023 Palo Alto Networks, Inc.

從 NSX-T 上的 VM-Series 操作移轉至安全性中心部署 267
將安全性政策從 NSX-V 延伸至 NSX-T 274
使用就地移轉將 VM-Series 從 NSX-V 移至 NSX-T 276

在 AWS 上設定 VM-Series 防火牆 283

關於 AWS 上的 VM-Series 防火牆 284
AWS EC2 實例類型 284
AWS GovCloud 上的 VM-Series 防火牆 284
AWS China 上的 VM-Series 防火牆 285
AWS Outposts 上的 VM-Series 防火牆 285
AWS 術語 285
搭配 Amazon ELB 使用的管理介面對應 287
調整 AWS 上的 VM-Series 防火牆效能 289
AWS 上支援的部署 290
在 AWS 上部署 VM-Series 防火牆 293
取得 AMI 293
為 AWS VPC 中的 VM-Series 規劃工作表 297
在 AWS 上啟動 VM-Series 防火牆 299
在 AWS Outposts 上啟動 VM-Series 防火牆 306
建立自訂 Amazon 機器映像 (AMI) 314
在 AWS 上加密 VM-Series 防火牆的 EBS 磁碟區 317
使用 VM-Series 防火牆 CLI 來交換管理介面 319
在 VM-Series 防火牆上啟用 CloudWatch 監控 319
VM-Series 與 AWS 閘道負載平衡器整合 324
手動整合 VM-Series 與閘道負載平衡器 326
VM-Series 自動調整規模群組與 AWS 閘道負載平衡器 340
AWS 上 VM-Series 防火牆的高可用性 354
AWS 上的 HA 概觀 354
HA 的 IAM 角色 355
HA 連結 358
活動訊號輪詢與您好訊息 358
裝置優先順序及先佔 358
HA 計時器 358
使用次要 IP 在 AWS 上設定主動/被動 HA 359
使用介面移動在 AWS 上設定主動/被動 HA 365
在 AWS 上移轉主動/被動 HA 369
使用案例：保護 AWS 雲端中的 EC2 實例 374
使用案例：使用動態位址群組保護 VPC 中的新 EC2 實例 388
使用案例：將 VM-Series 防火牆作為 AWS 上的 GlobalProtect 閘道 393

©2023 Palo Alto Networks, Inc.

GlobalProtect 基礎結構的元件 393
在 AWS 上部署 GlobalProtect 閘道 394
AWS 上的資源監控 396
在 Panorama 上透過 AWS 外掛程式監控 AWS 資源 396
設定 Panorama 上透過 AWS 外掛程式進行的 VM 監控 396
使用 Amazon ELB 服務自動調整 VM-Series 防火牆規模 408
AWS 專用 VM-Series 自動調整規模範本 2.0 版 410
AWS 專用 VM-Series 自動調整規模範本 2.1 版 441
在 AWS VPC 上監控的屬性清單 468
監控 AWS VPC 所需的 IAM 權限 469
在 KVM 上設定 VM-Series 防火牆 471
KVM 上的 VM-Series—需求與先決條件 472
在網路上連接 VM-Series 的選項 473
KVM 上 VM-Series 的先決條件 474
KVM 上支援的部署 479
保護單一主機上的流量 479
保護 Linux 主機之間的流量 479
在 KVM 上安裝 VM-Series 防火牆 481
使用 Virt-Manager 安裝 VM-Series 防火牆 481
使用 ISO 安裝 VM-Series 防火牆 488
使用 VM-Series CLI 在 KVM 上交換管理介面 490
啟用 SCSI 控制器 490
驗證 VM-Series 防火牆上網路介面順序的 PCI-ID 491
KVM 專用 VM-Series 的效能調整 493
在 Ubuntu 16.04.1 LTS 上安裝 KVM 和 Open vSwitch 493
在 KVM 上啟用 Open vSwitch 493
整合 Open vSwitch 與 DPDK 494
在 KVM 上啟用 SR-IOV 498
透過 SR-IOV 啟用 VLAN 存取模式 499
在 KVM 上啟用 NIC 的多佇列支援 500
在 KVM 上的 NUMA 節點中隔離 CPU 資源 501
智慧流量卸載 502
智慧型流量卸載需求 503
智慧型流量卸載介面 503
high availability （高可用性） 504
安裝 BlueField-2 DPU 506
安裝 VM-Series 防火牆 506
啟用虛擬功能 507

©2023 Palo Alto Networks, Inc.

檢查 BlueField-2 DPU 系統 508
安裝或升級 BlueField Bootstream 軟體 509
安裝或升級 Debian 套件 510
執行智慧型流量卸載 511
BlueField-2 DPU 疑難排解 513
PAN-OS 疑難排解 514
參考 516
在 Hyper-V 上設定 VM-Series 防火牆 517
Hyper-V 上支援的部署 518
保護單一 Hyper-V 主機上的流量 518
保護多個 Hyper-V 主機之間的流量 518
Hyper-V 的系統需求 520
Linux 整合服務 521
在 Hyper-V 上安裝 VM-Series 防火牆 522
開始之前 522
Hyper-V 上的 VM-Series 防火牆的效能調整 523
在 Hyper-V 主機上使用 Hyper-V 管理員佈建 VM-Series 防火牆 523
在 Hyper-V 主機上使用 PowerShell 佈建 VM-Series 防火牆 525
在 VM-Series 防火牆上執行初始組態 526
在 Azure 上設定 VM-Series 防火牆 529
關於 Azure 上的 VM-Series 防火牆 530
Azure 網路和 VM-Series 防火牆 530
Azure 安全中心整合 531
Azure 上的 VM-Series 防火牆範本 532
Azure 上的 VM-Series 最低系統需求 533
關於 Azure 上的 VM-Series 的高可用性支援 534
Azure Service 上的 VM-Series 的服務主體權限 534
Azure 上支援的部署 538
從 Azure Marketplace 部署 VM-Series 防火牆（解決方案範本） 539
從 Azure China Marketplace 部署 VM-Series 防火牆（解決方案範本） 548
Azure 中的 Panorama 協調部署 553
為協調部署做好準備 555
在 Azure 中協調 VM-Series 防火牆部署 559
建立 Azure 的自訂 VM-Series 映像 567
使用 Azure 安全性中心建議來保護您的工作負載 569
根據 Azure 安全性中心的建議部署 VM-Series 防火牆 569
從 Azure 安全性中心連線現有的 VM-Series 防火牆 570

©2023 Palo Alto Networks, Inc.

使用 Panorama 將日誌轉送至 Azure 安全性中心 572
在 Azure Stack 上部署 VM 系列防火牆 575
啟用 VM-Series 防火牆上的 Azure Application Insights 579
在 Azure 上監控 581
關於在 Azure 上監控 581
設定 Azure 外掛程式在 Panorama 上監控 581
在 Azure 上使用 Panorama 外掛程式監控的屬性 589
在 Azure 上設定主動/被動 HA 592
在 Azure 上設定主動/被動 HA（南北向和東西向流量） 593
在 Azure 上設定主動/被動 HA（僅限東西向流量） 605
使用 ARM 範本部署 VM-Series 防火牆 618
部署 VM-Series 和 Azure 應用程式閘道範本 622
VM-Series 和 Azure 應用程式閘道範本 622
開始使用 VM-Series 和 Azure 應用程式閘道範本 623
保護 Azure 上的 Kubernetes 服務 632
Azure 專用 Panorama 外掛程式如何保護 Kubernetes 服務？ 632
保護 AKS 叢集 636

在 OpenStack 上設定 VM-Series 防火牆 647

OpenStack 中的 VM-Series 部署 648
基本閘道 648
服務鏈結和服務調整規模 648
OpenStack 專用 VM-Series 解決方案的元件 650
基本閘道部署的熱度範本 652
服務鏈結和服務調整規模的熱度範本 654
虛擬網路 655
虛擬電腦 655
服務範本 656
服務實例 656
IPAM 656
服務原則 657
警報 658
在基本閘道部署中安裝 VM-Series 防火牆 659
使用服務鏈結或調整規模安裝 VM-Series 防火牆 662

在 Google Cloud Platform 上設定 VM-Series 防火牆 665

有關在 Google Cloud Platform 上的 VM-Series 防火牆 666
Google Cloud Plaform 與 VM-Series 防火牆 666
防火牆上的 VM-Series 最低系統需求 666

©2023 Palo Alto Networks, Inc.

在 Google Cloud Platform 上受支援的部署 668
網際網路閘道 668
區隔閘道 668
混合型 IPSec VPN 669
預備在 Google Cloud Platform 上設定 VM-Series 防火牆 670
一般需求 670
在 Panorama 上安裝 VM-Series 外掛程式 671
安裝 GCP 專用 Panorama 外掛程式 671
準備從 GCP Marketplace 部署 672
在 Google Cloud Platform 上部署 VM-Series 防火牆 679
從 Google Cloud Platform Marketplace 部署 VM-Series 防火牆 679
管理 Google Cloud Platform 負載平衡的介面交換 683
使用 VM-Series 防火牆 CLI 來交換管理介面 684
啟用在 VM Series 防火牆上的 Google Stackdriver 監控 685
啟用 VM 監控以追蹤在 Google Cloud Platform (GCP) 上的 VM 變更 687
使用動態位址群組保護 VPC 中的實例 689
使用自訂範本或 gcloud CLI 部署 VM-Series 防火牆 691
使用 GCP 專用 Panorama 外掛程式進行 VM 監控 693
使用 GCP 專用 Panorama 外掛程式設定 VM 監控 693
在 Google Cloud Platform 上自動調整 VM-Series 防火牆規模 700
Google Cloud Platform 專用自動調整規模元件 700
部署 GCP 自動調整規模範本 711

在 Cisco ENCS Network 上設定 VM-Series 防火牆 739

規劃 Cisco ENCS 部署 740
準備 Cisco ENCS 的 VM-Series 防火牆映像 742
從圖形使用者介面轉換 qcow2 檔案 742
從命令行介面轉換 qcow2 檔案 744
在 Cisco ENCS 上部署 VM-Series 防火牆 747

在 Oracle Cloud Infrastructure 上設定 VM-Series 防火牆 751

OCI 形狀類型 752
OCI 上支援的部署 753
準備在 OCI 上設定 VM-Series 防火牆 754
從 Oracle Cloud Marketplace 部署 VM-Series 防火牆 757
在 OCI 上設定主動/被動 HA 762

在 Alibaba Cloud 上設定 VM-Series 防火牆 771

Alibaba Cloud 上的 VM-Series 防火牆 772
Alibaba Cloud 上的 VM-Series 防火牆最低系統需求 773

©2023 Palo Alto Networks, Inc.

VM-Series 防火牆軟體需求 773
VM-Series 防火牆的 Alibaba Cloud 實例類型建議 773
Alibaba Cloud CLI 773
準備在 Alibaba Cloud 上部署 VM-Series 防火牆 774
選擇授權與規劃網路 774
準備使用 Aliyun 命令行介面 774
在 Alibaba Cloud 上部署 VM-Series 防火牆 776
建立 VPC 並設定網路 776
建立並設定 VM-Series 防火牆 779
保護 Alibaba Cloud 上的南北向流量的安全 783
設定 Alibaba Cloud 上的負載平衡 786
在 Cisco ACI 中設定防火牆 789
Palo Alto Networks 防火牆與 Cisco ACI 整合 790
服務圖形範本 791
多重內容部署 791
準備 ACI 環境進行整合 792
以網路政策模式整合防火牆與 Cisco ACI 793
以網路政策模式部署防火牆來保護東西向流量 793
以網路政策模式部署防火牆來保護南北向流量 809
Cisco ACI 中的端點監控 826
安裝 Cisco ACI 專用 Panorama 外掛程式 827
設定 Cisco ACI 外掛程式 828
Cisco ACI 專用 Panorama 外掛程式儀表板 831
在 Cisco CSP 上設定 VM-Series 防火牆 835
Cisco CSP 上的 VM-Series 系統需求 836
在 Cisco CSP 上部署 VM-Series 防火牆 837
Cisco TrustSec 的端點監控 839
Cisco TrustSec 專用 Panorama 外掛程式 840
大量同步 840
發佈訂閱 841
安裝 Cisco TrustSec 專用 Panorama 外掛程式 842
設定 Cisco TrustSec 專用 Panorama 外掛程式 843
對 Cisco TrustSec 專用 Panorama 外掛程式進行疑難排解 851
外掛程式狀態命令 851
偵錯命令 851
偵錯日誌 852

©2023 Palo Alto Networks, Inc.

在 Nutanix AHV 上設定 VM-Series 防火牆 853
Nutanix 上的 VM 監控 854
關於 Azure 上的 VM 監控 854
安裝 Nutanix 專用 Panorama 外掛程式 855
設定 Nutanix 專用 Panorama 外掛程式 855
啟動 VM-Series 防火牆 861
選擇啟動方法 862
基本設定 863
完成設定。 866
VM-Series 防火牆啟動工作流程 867
啟動套件 869
啟動套件結構 869
啟動套件傳遞 869
啟動程序組態檔案 871
init-cfg.txt 871
bootstrap.xml 871
在 Panorama 上產生 VM 驗證金鑰 872
建立 init-cfg.txt 檔案 874
init-cfg.txt 檔案元件 875
範例 init-cfg.txt 檔案 878
建立 bootstrap.xml 檔案 880
準備啟動程序授權 881
準備啟動程序套件 882
在 AWS 上啟動 VM-Series 防火牆 884
在 Azure 上啟動 VM-Series 防火牆 888
在 ESXi 上啟動 VM-Series 防火牆 892
使用 ISO 在 ESXi 上啟動 VM-Series 防火牆 892
使用區塊儲存裝置在 ESXi 上啟動 VM-Series 防火牆 892
在 Google Cloud Platform 上啟動 VM-Series 防火牆 894
在 Hyper-V 上啟動 VM-Series 防火牆 896
使用 ISO 在 Hyper-V 上啟動 VM-Series 防火牆 896
使用區塊儲存裝置在 Hyper-V 上啟動 VM-Series 防火牆 896
在 KVM 上啟動 VM-Series 防火牆 898
使用 ISO 在 KVM 上啟動 VM-Series 防火牆 898
使用區塊儲存裝置在 KVM 上啟動 VM-Series 防火牆 898
驗證啟動程序完成 900
啟動程序錯誤 901

 ©2023 Palo Alto Networks, Inc.

關於 VM-Series 防火牆

Palo Alto Networks VM-Series 防火牆是 Palo Alto Networks 下一代防火牆的虛擬形式。其適用於虛擬或雲端環境中，從而保護東西向與南北向流量的安全。

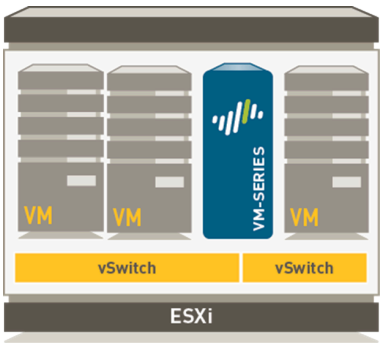
- VM-Series 部署
- 高可用性 VM-Series
- 升級 VM-Series 防火牆
- VM-Series 外掛程式
- 在 VM-Series 防火牆上啟用巨型框架
- Hypervisor 指派的 MAC 位址
- 發佈自訂 PAN-OS 度量以作為監控使用
- 存取 VM-Series 防火牆外部服務所使用的介面
- PacketMMAP 和 DPDK 驅動程式支援
- 在 VM-Series 上啟用 NUMA 效能最佳化
- 在 VM-Series 防火牆上啟用 ZRAM

VM-Series 部署

可在下列平台上部署 VM-Series 防火牆：

- 適用於 **VMware vSphere Hypervisor (ESXi)** 及 **vCloud Air** 的 **VM-Series**

  您可以在 VMware ESXi 上將任何 VM-Series 型號部署為來賓虛擬機器；適用於需要虛擬形式的雲端或網路。

  如需詳細資訊，請參閱在 ESXi 伺服器上設定 VM-Series 防火牆和在 vCloud Air 上設定 VM-Series 防火牆。

- **VMware NSX-T** 上的 **VM-Series**

  您可以在 NSX-T 環境中部署 VM-100、VM-300、VM-500 或 VM-700。

  如需詳細資料，請參閱在 VMware NSX-T（南北向）上設定 VM-Series 防火牆。

- 適用於 **Amazon Web Services (AWS)** 的 **VM-Series**

  您可以將任何 VM-Series 型號（VM-50 除外）部署在 AWS 雲端的 EC2 實例上。

  如需詳細資訊，請參閱在 AWS 上設定 VM-Series 防火牆。

- **Google Cloud Platform** 專用 **VM-Series**

  您可以在 Google Compute Engine 實例上部署除 VM-50 和 VM-50 Lite 外的任何 VM-Series 型號。如需詳細資料，請參閱在 Google Cloud Platform 上設定 VM-Series 防火牆。

- **Kernel Virtualization Module (KVM)** 適用的 **VM-Series**

  您可以將任何 VM-Series 型號部署在執行 KVM Hypervisor 的 Linux 伺服器上。如需詳細資訊，請參閱在 KVM 上設定 VM-Series 防火牆。

- **Microsoft Hyper-V** 專用 **VM-Series**

  您可以將任何 VM-Series 型號部署在已啟用 Hyper-V 角色附加元件的 Windows Server 2012 R2 伺服器上，或獨立式 Hyper-V 2012 R2 伺服器上。如需詳細資訊，請參閱在 Hyper-V 上設定 VM-Series 防火牆。

- **Microsoft Azure** 專用 **VM-Series**

  您可以將任何 VM-Series 型號（VM-50 除外）部署在 Azure VNet。

  如需詳細資訊，請參閱在 Azure 上設定 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

高可用性 VM-Series

高可用性 (HA) 是一種單一群組中配置兩個防火牆的組態，且這兩個防火牆的組態會同步處理，防止單點在網路上失效。兩個防火牆對等間的活動訊號連線可確保當其中一個對等損壞時能夠無縫容錯移轉。在兩個裝置叢集中設定防火牆可提供備援能力，並能讓您確保業務連續性。在 VM-Series 防火牆上的高可用性 (HA) 組態中，在相同類型的 Hypervisor 上必須部署兩個端點，向其指派相同的硬體資源（例如 CPU 核心/網路介面），並設定相同的授權/使用授權。如需關於 Palo Alto Networks 防火牆 HA 的一般資訊，請參閱高可用性。

VM-Series 防火牆支援與工作階段間的狀態主動/被動或主動/主動可用性，並支援組態同步處理。某些私人雲端 Hypervisor 的虛擬介接和第 3 層部署中才支援主動/主動部署，因此只有當每個防火牆都需要自己的路由實例，而且您一律需要在兩個防火牆之外進行完整且即時的備援時，才建議使用這種部署。如需將 VM-Series 防火牆設定為 HA 配對的指示，請參閱設定主動/被動 HA 及設定主動/主動 HA。

如果您在 Amazon Web Services (AWS) 或 Azure 這類公共雲端中部署 VM-Series 防火牆，則可以使用傳統主動/被動 HA 設定；請參閱 AWS 上 VM-Series 防火牆的高可用性以及在 Azure 上設定主動/被動 HA。或者，因為相較於私人資料中心，雲端基礎結構內建資源或區域備援的方式天生就不一樣，所以若要利用原生雲端服務，並建立具回復力的架構來維持最長執行時間，請參閱

- AWS—使用 Amazon ELB 自動調整 VM-Series 防火牆規模，在 VPC 內跨越兩個或三個「可用性設定組」來部署多個防火牆。
- Azure—VM-Series 和 Azure 應用程式閘道範本參數。

支援的功能/連結	ESX	KVM	AWS	NSX V	NSX T (N/S)	Hyper-V	Azure	GCP	OCI
主動/被動 HA	是	是	是	否。	是	是	是	否。	是
主動/主動 HA	是	是	否。	否。	否。	是	否。	否。	否。
HA 1	是	是	是	否。	是	是	是	是	是
HA2—（工作階段同步及保持活動）	是	是	是	否。	是	是	是	是	是
HA3	是	是	否。	否。	否。	是	否。	否。	否。

對於 *GCP* 上的 *VM-Series*，*HA1* 和 *HA2* 支援需要 *PAN-OS 10.0x* 或更新版本，以及 *VM-Series* 外掛程式 *2.0.5* 或更新版本。

針對 NSX-T (E/W) 上的 VM-Series 防火牆，可透過名為服務健康情況檢查的 NSX-T 功能達到高可用性。此 NSX-T 功能可讓您模擬服務實例失敗案例中的高可用性。設定了 VM-Series 防火牆後，如果 VM-Series 服務實例失敗，任何導向至該防火牆的流量將會重新導向至叢集中的其他防火牆

©2023 Palo Alto Networks, Inc.

（服務叢集部署），或是其他主機上的防火牆實例（主機型部署）。如需針對 NSX-T (E/W) 上的 VM-Series 防火牆詳細資訊，請參閱在 Panorama 上設定服務定義。

©2023 Palo Alto Networks, Inc.

升級 VM-Series 防火牆

升級 PAN-OS 版本或 VM-Series 型號，可讓您新增最新功能和修正，以利提升防火牆的安全功能和效能。

標準 PAN-OS 版本就是如此；這是可安裝在所有 Palo Alto Networks 防火牆上的正規版 PAN-OS。PAN-OS XFR 版本僅供 VM-Series 防火牆使用，其中可能包含 VM-Series 防火牆的新功能和錯誤修正。如果您在 VM-Series 防火牆上安裝 PAN-OS XFR 映像，早於您所安裝之軟體版本的 PAN-OS 版本，將不會提供新功能和修正。

由於 XFR 映像包含 VM-Series 防火牆專用的功能和修正，如果您升級至 XFR 版本，在下一個主要 PAN-OS 版本推出之前，您將必須持續使用 XFR 版本才能保有 XFR 特特定功能；XFR 中提供的所有修正和功能，都將累積彙總至下一個主要 PAN-OS 版本中。

- 升級 PAN-OS 軟體版本（獨立版本）
- 升級 PAN-OS 軟體版本（HA 配對）
- 使用 Panorama 升級 PAN-OS 軟體版本
- 升級 PAN-OS 軟體版本（NSX 專用 VM-Series）
- 升級 VM-Series 型號
- 升級 HA 配對中的 VM-Series 型號
- 將 VM-Series 防火牆降級為舊版

如需安裝 VM-Series 防火牆的指示，請參閱 VM-Series 部署。

先確認您防火牆型號的 VM-Series 系統需求，再進行升級。如果防火牆的記憶體小於 *5.5GB*，則防火牆上的系統容量（工作階段數目、規則、安全性區域、位址物件等等）將限制為 ***VM-50 Lite*** 的系統容量。

升級 PAN-OS 軟體版本（獨立版本）

檢視新功能，並解決問題和已知問題，然後使用下列程序升級不在 HA 設定中的防火牆。

為了避免影響流量，請將升級規劃在離峰時間進行。確定防火牆連線至可靠的電源。升級過程中的電力損耗會使防火牆無法使用。

STEP 1 | 確認有足夠的硬體資源供 VM-Series 防火牆使用。

若要查看每個 VM-Series 型號的資源需求，請參閱 VM-Series 系統需求。請先配置額外的硬體資源，再繼續進行升級程序；在每個 Hypervisor 上指派額外硬體資源的程序都不同。

如果 VM-Series 防火牆沒有型號所需的資源，則會預設為與 VM-50 相關聯的容量。

STEP 2 | 從網頁介面中，導覽至 **Device**（裝置） > **Licenses**（授權），並確定您擁有正確的 VM-Series 防火牆授權，而且授權已啟動。

在 VM-Series 防火牆獨立版上，導覽至 **Device**（裝置） > **Support**（支援），並確定您已啟動支援授權。

©2023 Palo Alto Networks, Inc.

STEP 3 | 儲存目前組態檔案的備份。



雖然防火牆會自動建立設定備份，但最好在升級前建立備份並儲存在外部。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後按一下 **Export named configuration snapshot**（匯出具名設定快照）。
2. 選取包含執行中組態的 XML 檔案（例如 **running-config.xml**），然後按一下 **OK**（確定）匯出組態檔案。
3. 將匯出的檔案儲存至防火牆外部的位置。如果您在升級時發生問題，便可使用此備份還原組態。

STEP 4 | 如果您已啟用 User-ID，在您升級後，防火牆將會清除 IP 位址與使用者名稱之間的對應以及群組對應，使其能夠重新填入 User-ID 來源中的屬性。若要測量您的環境重新填入對應所需的時間，請對防火牆執行下列 CLI 命令。

- 針對 IP 位址與使用者名稱的對應：
  - **show user user-id-agent state all**
  - **show user server-monitor state all**
- 針對群組對應：**show user group-mapping statistics**

STEP 5 | 確定防火牆執行最新的內容版本。

1. 選取 **Device**（裝置） > **Dynamic Updates**（動態更新），並查看哪個 **Applications**（應用程式）或 **Applications and Threats**（應用程式與威脅）內容版本是 [Currently Installed（目前安裝的）]。
2. 如果防火牆未執行 PAN-OS 所需的最低必要內容版本或更新版本，請 **Check Now**（立即檢查）以擷取可用更新清單。
3. 找出並 **Download**（下載）所需的內容發行版本。

   在您成功下載內容更新檔案後，該內容發行版本的 [Action（動作）] 欄中的連結會從 **Download**（下載）變更為 **Install**（安裝）。
4. **Install**（安裝）更新。

STEP 6 | 升級 VM-Series 外掛程式。

1. 升級之前，請檢查最新版本資訊，以取得新的 VM-Series 外掛程式是否會影響環境的詳細資料。

   例如，假設新的 VM-Series 外掛程式版本僅包括 AWS 功能。若要利用新功能，您必須更新 AWS 的 VM-Series 防火牆實例上的外掛程式。

   請不要安裝未套用至環境的升級。
2. 登入 VM-Series 防火牆，並檢查儀表板以檢視外掛程式版本。
3. 選取 **Device**（裝置） > **Plugins**（外掛程式），以檢視外掛程式版本。使用 **Check Now**（立即檢查），以檢查更新。
4. 選取外掛程式版本，在 Action（動作）欄中按一下 **Install**（安裝）來安裝外掛程式。

©2023 Palo Alto Networks, Inc.

STEP 7 | 升級 PAN-OS。

如果防火牆無法從管理連接埠存取網際網路，您可以從 Palo Alto Networks 客戶支援入口網站下載軟體映像，然後再將其手動 ***Upload***（上傳）至防火牆。

1. 選取 **Device**（裝置） > **Software**（軟體），然後按一下 **Check Now**（立即檢查）以顯示最新的 PAN-OS 更新。
2. 找出並 **Download**（下載）目標 PAN-OS 版本。
3. 在您下載映像後（手動升級則是在上傳映像後），請 **Install**（安裝）該映像。
4. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes** （是）。
   - 如果未提示您重新啟動，請選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後按一下 **Reboot Device**（重新啟動裝置）。

   此時，防火牆會清除 *User-ID* 對應，然後連線至 *User-ID* 來源以重新填入對應。
5. 如果您已啟用 User-ID，請先使用下列 CLI 命令確認防火牆已重新填入 IP 位址與使用者名稱的對應和群組對應，再允許流量。
   - **`show user ip-user-mapping all`**
   - **`show user group list`**
6. 如果您是首次升級至 XFR 版本，請重複此步驟，以升級至對應的 XFR 版本。

STEP 8 | 確認防火牆正在傳遞流量。

選取 **Monitor**（監控） > **Session Browser**（工作階段瀏覽器），然後確認您看到新的工作階段。

升級 PAN-OS 軟體版本（HA 配對）

使用下列程序，升級高可用性 (HA) 設定中的一對防火牆。此程序適用於主動/被動和主動/主動設定。

若要避免在高可用性 (HA) 設定中升級防火牆時的停機時間，每次更新一個 HA 對等：對於主動/主動防火牆，先升級哪個對等並沒有差別（但為了方便說明，此程序將說明如何先升級主動/次要對等）。對於主動/被動防火牆，您必須先升級被動端點，暫停主動端點（容錯移轉），更新主動端點，然後將該端點回復為運作狀態（容錯回復）。若要防止在升級 HA 對等期間發生容錯移轉，您必須先確定已停用先佔，再繼續進行升級。您只需停用配對中一個對等的先佔即可。

為了避免影響流量，請將升級規劃在離峰時間進行。確保防火牆連線至可靠的電源。升級過程中的電力損耗會使防火牆無法使用。

STEP 1 | 確認有足夠的硬體資源供 VM-Series 防火牆使用。

若要查看每個 VM-Series 型號的資源需求，請參閱 VM-Series 系統需求。請先配置額外的硬體資源，再繼續進行升級程序；在每個 Hypervisor 上指派額外硬體資源的程序都不同。

如果 VM-Series 防火牆沒有型號所需的資源，則會預設為與 VM-50 相關聯的容量。

©2023 Palo Alto Networks, Inc.

STEP 2 | 從網頁介面中，導覽至 **Device**（裝置） > **Licenses**（授權），並確定您擁有正確的 VM-Series 防火牆授權，而且授權已啟動。

在 VM-Series 防火牆獨立版上，導覽至 **Device**（裝置） > **Support**（支援），並確定您已啟動支援授權。

STEP 3 | 儲存目前組態檔案的備份。



雖然防火牆會自動建立設定備份，但最好是在升級前先建立備份並儲存於外部。

對配對中的每個防火牆執行下列步驟：

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後按一下 **Export named configuration snapshot**（匯出具名設定快照）。
2. 選取包含執行中組態的 XML 檔案（例如 **running-config.xml**），然後按一下 **OK**（確定）匯出組態檔案。
3. 將匯出的檔案儲存至防火牆外部的位置。如果您在升級時發生問題，便可使用此備份還原組態。

STEP 4 | 如果您已啟用 User-ID，在您升級後，防火牆將會清除 IP 位址與使用者名稱之間的對應以及群組對應，使其能夠重新填入 User-ID 來源中的屬性。若要測量您的環境重新填入對應所需的時間，請對防火牆執行下列 CLI 命令。

- 針對 IP 位址與使用者名稱的對應：
  - **show user user-id-agent state all**
  - **show user server-monitor state all**
- 針對群組對應：**show user group-mapping statistics**

STEP 5 | 確定 HA 配對中的每個防火牆都執行最新的內容版本。

請參閱版本資訊，瞭解您必須為 PAN-OS 10.2 版本安裝的最低內容版本。請確實遵循應用程式和威脅更新的最佳做法。

1. 選取 **Device**（裝置） > **Dynamic Updates**（動態更新），並查看 **Applications**（應用程式）或 **Applications and Threats**（應用程式與威脅），以確認哪個更新是 [Currently Installed（目前安裝的）]。
2. 如果防火牆未執行您安裝的軟體版本所需的最低必要內容版本或更新版本，請 **Check Now**（立即檢查）以擷取可用更新清單。
3. 找出並 **Download**（下載）所需的內容發行版本。

   在您成功下載內容更新檔案後，該內容發行版本的 [Action（動作）] 欄中的連結會從 **Download**（下載）變更為 **Install**（安裝）。
4. **Install**（安裝）更新。您必須在兩個對等上都安裝更新。

©2023 Palo Alto Networks, Inc.

STEP 6 | 升級 VM-Series 外掛程式。

1. 升級之前，請檢查最新版本資訊，以取得新的 VM-Series 外掛程式是否會影響環境的詳細資料。

   例如，假設新的 VM-Series 外掛程式版本僅包括 AWS 功能。若要利用新功能，您必須更新 AWS 的 VM-Series 防火牆實例上的外掛程式。

   請不要安裝未套用至環境的升級。

2. 登入 VM-Series 防火牆，並檢查儀表板以檢視外掛程式版本。
3. 選取 **Device**（裝置） > **Plugins**（外掛程式），以檢視外掛程式版本。使用 **Check Now**（立即檢查），以檢查更新。
4. 選取外掛程式版本，在 Action（動作）欄中按一下 **Install**（安裝）來安裝外掛程式。

   在 HA 對等中的 VM-Series 防火牆上安裝外掛程式時，請先將外掛程式安裝於被動對等，再安裝於主動對等。安裝外掛程式安裝於被動對等之後會轉換為非運作狀態。將外掛程式安裝於主動對等會將被動對等恢復為運作狀態。

STEP 7 | 停用每個配對中第一個對等的先佔。您只需要在 HA 配對中的一個防火牆上停用此設定，但務必要在認可成功後再繼續進行升級。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） 並編輯 **Election Settings**（選取設定）。
2. 若啟用，停用（清除）**Preemptive**（先佔）設定，然後按一下 **OK**（確認）。
3. **Commit**（提交）變更。

©2023 Palo Alto Networks, Inc.

STEP 8 | 在第一個對等上安裝 PAN-OS 版本。

若要盡可能縮短主動/被動設定的停機時間，請先升級被動對等。對於主動/主動設定，請先升級次要對等。最佳做法是，如果您使用主動/主動設定，則建議您在相同的維護期間內升級兩個對等。



如果您想要先測試 *HA* 是否正常運作再升級，您可以考慮先在主動/被動設定中升級主動對等，以確保在容錯移轉發生時不會有事件。

1. 在第一個對等上，選取 **Device**（裝置） > **Software**（軟體），然後按一下 **Check Now**（立即檢查）以瞭解最新的更新。
2. 找出並 **Download**（下載）目標 PAN-OS 版本。

   如果防火牆無法從管理連接埠存取網際網路，您可以從 Palo Alto Networks 支援入口網站下載軟體映像，然後再將其手動 ***Upload***（上傳）至防火牆。
3. 在您下載映像後（手動升級則是在上傳映像後），請 **Install**（安裝）該映像。
4. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes** （是）。
   - 如果未提示您重新啟動，請選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作） 和 **Reboot Device**（重新啟動裝置）。
5. 裝置完成重新開機後，請在 **Dashboard**（儀表板）上檢視 [High Availability（高可用性）] Widget，並確認您剛升級的裝置仍是 HA 設定中的被動或主動/次要對等。

STEP 9 | 在第二個對等上安裝 PAN-OS 版本。

1. （僅限主動/被動設定）暫停主動對等，使 HA 容錯移轉至您剛升級的對等。
   1. 在主要對等上，選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令），然後按一下 **Suspend local device**（暫停本機裝置）。
   2. 在 **Dashboard**（儀表板）上檢視 [High Availability（高可用性）] Widget，並確認狀態已變更為 **Passive**（被動）。
   3. 在另一個對等上，確認該對等處於主動狀態且正在傳遞流量（**Monitor**（監控） > **Session Browser**（工作階段瀏覽器））。
2. 在第二個對等上，選取 **Device**（裝置） > **Software**（軟體），然後按一下 **Check Now**（立即檢查）以瞭解最新的更新。
3. 找出並 **Download**（下載）目標 PAN-OS 版本。
4. 下載映像後，請加以 **Install**（安裝）。
5. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes** （是）。
   - 如果未提示您重新啟動，請選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作） 和 **Reboot Device**（重新啟動裝置）。
6. （僅限主動#被動設定）從您剛升級之對等的 CLI 執行以下命令，以讓防火牆再次運作：

   ```
   request high-availability state functional
   ```


©2023 Palo Alto Networks, Inc.

STEP 10 | 確認兩個對等都如預期傳遞流量。

在主動/被動設定中，只有主動對等應傳遞流量；在主動/主動設定，兩個對等都應傳遞流量。

執行下列 CLI 命令以確認升級成功：

- （僅限主動對等）若要確認主動對等正在傳遞流量，請執行 **show session all** 命令。
- 若要驗證工作階段同步，請執行 **show high-availability interface ha2** 命令，並確定 CPU 表格上的 Hardware Interface（硬體介面）計數器增加如下：
  - 在主動/被動組態中，只有主動對等會顯示傳輸的封包；被動對等將只會顯示接收的封包。

    如果您已啟用 *HA2* 保持活動，被動對等上的硬體介面計數器會同時顯示傳輸與接收封包。這是因為 *HA2* 保持活動是雙向，亦即兩個對等都會傳輸 *HA2* 保持活動封包。
  - 在主動/主動組態中，您會看到兩個對等上接收的封包與傳輸的封包。

STEP 11 | 如果您在升級前已停用先佔，請於此時重新加以啟用。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） 並編輯 **Election Settings**（選取設定）。
2. 選取 **Preemptive**（先佔），然後按一下 **OK**（確定）。
3. **Commit**（提交）變更。

使用 Panorama 升級 PAN-OS 軟體版本

使用以下程序升級您使用 Panorama 管理的防火牆。此程序應用在獨立的防火牆，以及部署在高可用性（HA）設定中的防火牆。

若 *Panorama* 無法直接連線至升級的伺服器，請遵循在 Panorama 未連線至網際網路時部署防火牆的更新的程序，以便手動下載映像至 *Panorama*，然後將映像散佈至防火牆。

在從 Panorama 升級防火牆之前，您必須：

- 確定 Panorama 正執行您要升級版本相同或更新的 PAN-OS 版本。您必須先升級 Panorama 及其日誌收集器（升級至 9.1），再將受管理的防火牆升級至此版本。此外，將日誌收集器升級至 9.1 時，由於記錄基礎結構有所變更，您必須將所有日誌收集器同時升級。
- 將 Panorama 升級至 9.1 時，請安排較寬鬆的維護期間（最多六小時）。此版本包含重大基礎結構變更，這表示 Panorama 升級會比過去的版本更耗時。
- 確保防火牆連接可靠的電源。升級過程中的電力損耗會使防火牆無法使用。

STEP 1 | 升級 Panorama 後，請將設定認可並推送至您預計要升級的防火牆。

©2023 Palo Alto Networks, Inc.

STEP 2 | 確認有足夠的硬體資源供 VM-Series 防火牆使用。

若要查看每個 VM-Series 型號的資源需求，請參閱 VM-Series 系統需求。請先配置額外的硬體資源，再繼續進行升級程序；在每個 Hypervisor 上指派額外硬體資源的程序都不同。

如果 VM-Series 防火牆沒有型號所需的資源，則會預設為與 VM-50 相關聯的容量。

STEP 3 | 從網頁介面中，導覽至 **Device**（裝置） > **Licenses**（授權），並確定您擁有正確的 VM-Series 防火牆授權，而且授權已啟動。

在 VM-Series 防火牆獨立版上，導覽至 **Device**（裝置） > **Support**（支援），並確定您已啟動支援授權。

STEP 4 | 在您打算升級的每個受管理的防火牆上，儲存目前組態檔案的備份。



雖然防火牆會自動建立設定備份，但最好在升級前建立備份並儲存在外部。

1. 從 Panorama 網路介面，選取 **Panorama** > **Setup**（設定） > **Operations**（操作） 然後按一下 **Export Panorama and devices config bundle**（匯出 **Panorama** 和裝置設定組合） 以產生並匯出 Panorama 和 每個受管理設備的最新設定備份。
2. 將匯出的檔案儲存至防火牆外部的位置。如果您在升級時發生問題，便可使用此備份還原組態。

STEP 5 | 在您計劃要升級的防火牆上更新內容發行版本。

請參閱版本資訊，瞭解 PAN-OS 10.2 所需的最低內容發行版本。請確認在部署內容更新至 Panorama 和受管理的防火牆時，遵循 應用程式和威脅內容更新的最佳實踐方法 。

1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Dynamic Updates**（動態更新） 和 **Check Now**（立即檢查） 以獲得最新更新。如果有可用的更新，Action（動作）欄會顯示 **Download**（下載）連結。
2. 如果尚未安裝，請 **Download**（下載）最新內容發佈版本。
3. 按一下 **Install**（安裝），選取您想要更新和更新的防火牆，然後按一下 **OK**（確認）。如果您正在升級 HA 防火牆，則您必須在兩個端點都升級內容。

STEP 6 | （僅限 HA 防火牆升級）如果您將升級為 HA 配對一部分的防火牆，請停用先佔。您僅需要在每個 HA 配對中的一個防火牆上停用此設定。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） 並編輯 **Election Settings**（選取設定）。
2. 若啟用，停用（清除）**Preemptive**（先佔）設定，然後按一下 **OK**（確認）。
3. **Commit**（提交）您的變更。在您繼續進行更新前，請確認提交成功。

STEP 7 | 下載目標 PAN-OS 版本映像。

1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體） 和 **Check Now**（立即檢查） 以獲得最新發行版本。
2. 根據您要升級到的發行版本，尋找並 **Download**（下載）防火牆指定檔案。您必須為每個您想要升級的防火牆型號（或防火牆系列）下載單獨的更新。

©2023 Palo Alto Networks, Inc.

STEP 8 | 在防火牆上安裝 PAN-OS 軟體更新。

1. 在對應您想要升級的防火牆型號的動作欄位中按一下 **Install**（安裝）。
2. 在部署軟體檔案對話框中，選取所有您想要升級的防火牆。若要減少停機時間，請僅選取每一個 HA 配對中的一個端點。對於主動/被動配對，請選取主動端點；對立主動/主動配對，請選取主動-次要端點。
3. （僅限 HA 防火牆升級）確定未選取 **Group HA Peers**（群組 **HA** 對等）。
4. 選取 **Reboot device after install**（安裝後重新啟動裝置）。
5. 若要開始升級，請按一下 **OK**（確認）。
6. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes**（是）。
   - 如果未提示您重新啟動，請選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作） 和 **Reboot Device**（重新啟動裝置）。
7. 在防火牆結束重新啟動後，請選取 **Panorama** > **Managed Devices**（受管理的裝置） 並驗證您升級的防火牆軟體版為 9.1.0。還要認證任何您在升級後仍舊為被動的防火牆的 HA 狀態。

STEP 9 | （僅限 HA 防火牆升級）升級每個 HA 配對中的次要 HA 對等。

1. （僅限主動/被動升級）暫停在每個正在升級的主動/被動配對主動裝置。
   1. 切換內容至主動防火牆。
   2. 在 **Dashboard**（儀表板）上的高可用性 Widget 中，驗證 **Local**（本機）防火牆狀態為 **Active**（主動）且 **Peer**（端點）為 **Passive**（被動）。
   3. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令） > **Suspend local device**（暫停本機裝置）。
   4. 返回至 **Dashboard**（儀表板）上的高可用性 Widget，並驗證 **Local**（本機）變更為 **Passive**（被動）且 **Peer**（端點）變更為 **Active**（主動）。
2. 返回 Panorama 內容，然後選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體）。
3. 在對應您正升級 HA 配對的防火牆型號的動作欄位中按一下 **Install**（安裝）。
4. 在部署軟體檔案對話框中，選取所有您想要升級的防火牆。這一次，僅選取您剛升級的 HA 防火牆的端點。
5. 確定未選取 **Group HA Peers**（群組 **HA** 配對）。
6. 選取 **Reboot device after install**（安裝後重新啟動裝置）。
7. 若要開始升級，請按一下 **OK**（確認）。
8. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes**（是）。
   - 如果未提示您重新啟動，請選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作） 和 **Reboot Device**（重新啟動裝置）。
9. （僅限主動#被動升級）從您剛升級之對等的 CLI 執行以下命令，以讓防火牆再次運作：

   ```
   request high-availability state functional
   ```


©2023 Palo Alto Networks, Inc.

STEP 10 | （僅限 PAN-OS XFR 升級）重複步驟 8 和步驟 9，將第一個對等和第二個對等升級至 PAN-OS XFR。

STEP 11 | 確認在每個受管理防火牆上執行的軟體與內容發佈版本。

1. 在 Panorama 上，選取 **Panorama** > **Managed Devices**（受管理的裝置）。
2. 在表格內找到防火牆，並檢閱內容和軟體版本。

   對於 HA 防火牆，您也可以驗證每個端點的 HA 狀態是否如預期。

STEP 12 | （僅限 HA 防火牆升級）如果您在升級之前在其中一個 HA 防火牆上停用先佔，請編輯 **Election Settings**（選取設定）（**Device**（裝置） > **High Availability**（高可用性）），針對該防火牆重新啟用 **Preemptive**（先佔）設定，然後 **Commit**（提交）。

升級 PAN-OS 軟體版本（NSX 專用 VM-Series）

選取最適合您部署的升級方法。

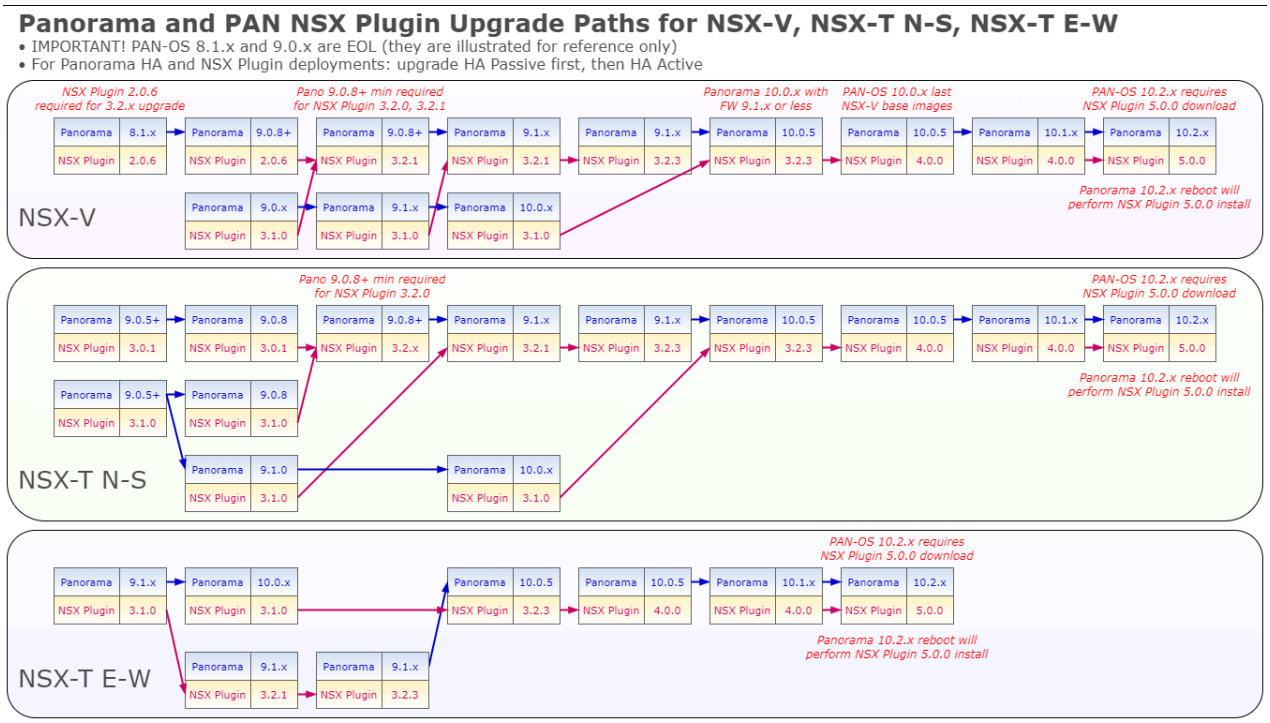
- 在維護時段升級 NSX 專用 VM-Series — 在維護時段使用此選項升級 VM-Series 防火牆，而不變更服務定義中的 OVF URL。
- 升級 NSX 專用 VM-Series 而不中斷流量 — 使用此選項升級 VM-Series 防火牆，而不中斷對來賓 VM 的服務或變更服務定義中的 OVF URL。

下圖顯示目前支援的 Panorama 與 VMware NSX 專用 Panorama 外掛程式組合，以及成功升級所需遵循的升級路徑。

- 以下每個方塊代表一種支援的組合。
- 升級 HA 配對中的 NSX 專用 Panorama 外掛程式或 Panorama 時，請先升級被動 Panorama 對等，之後再升級主動 HA 對等。

升級 VMware NSX 專用 VM-Series 部署之前，請檢閱如下所示的升級路徑，以瞭解哪些升級步驟所達到的外掛程式和 PAN-OS 組合，最適合您的環境。

©2023 Palo Alto Networks, Inc.



在維護時段升級 NSX 專用 VM-Series

對於 VM-Series 防火牆 NSX 版本，請使用 Panorama 升級防火牆上的軟體版本。

STEP 1 | 檢閱 VMware NSX 專用 VM-Series 升級路徑。

STEP 2 | 配置額外硬體資源給 VM-Series 防火牆。

確認有足夠的硬體資源供 VM-Series 防火牆使用。若要查看每個 VM-Series 型號的新資源需求，請參閱 VM-Series 系統需求。繼續升級程序之前，配置額外硬體資源。在每個 Hypervisor 上指派額外硬體資源的程序都不同。

©2023 Palo Alto Networks, Inc.

STEP 3 | 為每個您計劃升級的受管理防火牆儲存其組態檔案備份。



雖然防火牆會自動建立組態的備份，但最佳作法是在升級前先建立備份，並將它儲存在外部。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後按一下 **Export Panorama and devices config bundle**（匯出 **Panorama** 和裝置設定搭售包）。此選項用於手動產生和匯出 Panorama 和每個受管理設備的最新組態備份版本。
2. 將匯出的檔案儲存至防火牆外部的位置。如果您在升級時發生問題，便可使用此備份還原組態。

STEP 4 | 檢閱版本資訊，確認 PAN-OS 版本所需的 Content Release 版本。

您計劃升級的防火牆必須執行 PAN-OS 版本所需的 Content Release 版本。

1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Dynamic Updates**（動態更新）。
2. 檢查是否有最新的更新。按一下「立即檢查」（位於視窗的左下角）以檢查最新更新。動作欄中的連結表示是否有更新可用。如果有可用的版本，會顯示 **Download**（下載）連結。
3. 按一下 **Download**（下載）以下載選取的版本。成功下載後，**Action**（動作）欄中的連結會從 **Download**（下載）變更為 **Install**（安裝）。
4. 按一下 **Install**（安裝），並選取要安裝更新的裝置。完成安裝後，**Currently Installed**（目前已安裝）欄會顯示核取標記。

STEP 5 | 將軟體更新部署至所選的防火牆。



如果您的防火牆是設定在 *HA* 中，請確定清除 ***Group HA Peers***（群組 ***HA*** 端點）核取方塊，然後一次升級一個 *HA* 端點。

1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體）。
2. 檢查是否有最新的更新。按一下 **Check Now**（立即檢查）（位於視窗的左下角）以檢查最新更新。**Action**（動作）欄中的連結表示是否有更新可用。
3. 檢閱 **File Name**（檔案名稱）並按 **Download**（下載）。驗證下載的軟體版本符合網路上部署的防火牆型號。成功下載後，**Action**（動作）欄中的連結會從 **Download**（下載）變更為 **Install**（安裝）。
4. 按一下 **Install**（安裝），並選取要安裝軟體版本的設備。
5. 選取 **Reboot device after install**（安裝後重新啟動設備），然後按一下 **OK**（確定）。
6. 如果您的設備是設定在 HA 中，請清除 **Group HA Peers**（群組 **HA** 端點）核取方塊，然後一次升級一個 HA 端點。

STEP 6 | 確認在每個受管理設備上執行的軟體與 Content Release 版本。

1. 選取 **Panorama** > **Managed Devices**（受管理的裝置）。
2. 在表格上找到設備，並檢閱內容和軟體版本。

©2023 Palo Alto Networks, Inc.

在不影響流量的情況下升級 NSX 專用 VM-Series

使用下列程序在您的 VMware NSX 環境下升級 VM-Series 防火牆的 PAN-OS 版本。此程序可讓您透過將 VM 移轉至不同的 ESXi 主機來執行 PAN-OS 升級，不會中斷流量。

STEP 1 | 檢閱 VMware NSX 專用 VM-Series 升級路徑。

STEP 2 | 為每個您計劃升級的受管理防火牆儲存其組態檔案備份。



雖然防火牆會自動建立組態的備份，但最佳作法是在升級前先建立備份，並將它儲存在外部。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後按一下 **Export Panorama and devices config bundle**（匯出 **Panorama** 和裝置設定搭售包）。此選項用於手動產生和匯出 Panorama 和每個受管理設備的最新組態備份版本。
2. 將匯出的檔案儲存至防火牆外部的位置。如果您在升級時發生問題，便可使用此備份還原組態。

STEP 3 | 檢閱版本資訊，確認 PAN-OS 版本所需的 Content Release 版本。

您計劃升級的防火牆必須執行 PAN-OS 版本所需的 Content Release 版本。

1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Dynamic Updates**（動態更新）。
2. 檢查是否有最新的更新。按一下「立即檢查」（位於視窗的左下角）以檢查最新更新。動作欄中的連結表示是否有更新可用。如果有可用的版本，會顯示 **Download**（下載）連結。
3. 按一下 **Download**（下載）以下載選取的版本。成功下載後，**Action**（動作）欄中的連結會從 **Download**（下載）變更為 **Install**（安裝）。
4. 按一下 **Install**（安裝），並選取要安裝更新的裝置。完成安裝後，**Currently Installed**（目前已安裝）欄會顯示核取標記。

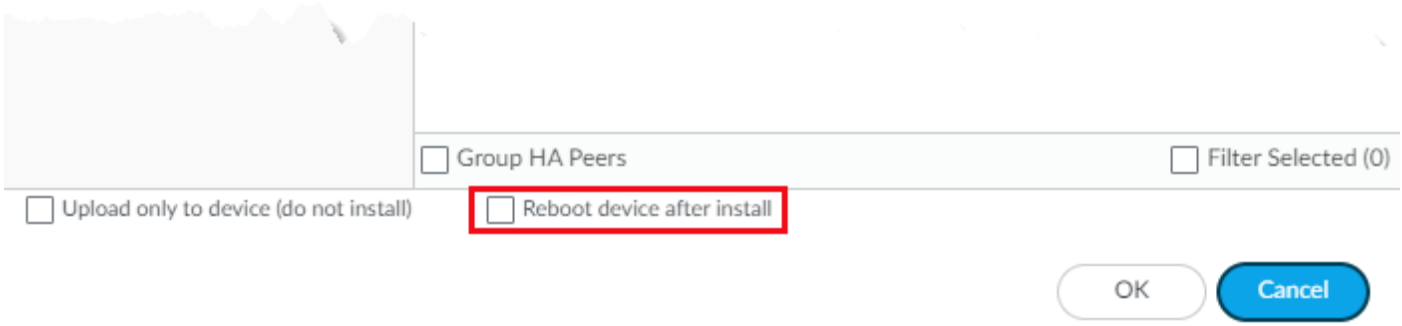
©2023 Palo Alto Networks, Inc.

STEP 4 | 下載 PAN-OS 映像至彙集中的所有 VM-Series 防火牆。

1. 登入 Panorama。
2. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體）。
3. 按一下 **Refresh**（重新整理）可檢視最新的軟體版本，同時檢閱 **Release Notes**（版本資訊）以檢視版本變更的說明，並檢視安裝軟體的移轉路徑。
4. 按一下 **Download**（下載）擷取軟體，然後按一下 **Install**（安裝）。

   安裝新的軟體映像後不重新啟動 *VM-Series* 防火牆。

5. 選取要升級的受管理裝置。
6. 清除 **Reboot device after install**（安裝後重新啟動裝置）核取方塊。



7. 按一下 **OK**（確定）。

STEP 5 | 在叢集中的第一個 ESXi 主機上升級 VM-Series 防火牆。

1. 登入 vCenter。
2. 選取 **Hosts and Clusters**（主機及叢集）。
3. 在主機上按一下滑鼠右鍵並選取 **Maintenance Mode**（維護模式） > **Enter Maintenance Mode**（進入維護模式）。
4. 從主機移轉（自動或手動）除 VM-Series 防火牆之外的所有 VM。
5. 關閉 VM-Series 防火牆電源。這應該會在主機上進入維護模式時自動進行。
6. （選用）將額外 CPU 或記憶體指派給 VM-Series 防火牆然後再繼續升級程序。

   確認有足夠的硬體資源供 VM-Series 防火牆使用。若要查看每個 VM-Series 型號的新資源需求，請參閱 VM-Series 型號。
7. 在主機上按一下滑鼠右鍵並選取 **Maintenance Mode**（維護模式） > **Exit Maintenance Mode**（退出維護模式）。退出維護模式將導致 NSX ESX Agent Manager (EAM) 開啟 VM-Series 防火牆。執行新的 PAN-OS 版本的防火牆將重新啟動。
8. 將所有 VM 移轉（自動或手動）回原始主機。

STEP 6 | 針對每個 ESXi 主機上的每個 VM-Series 防火牆，重複此程序。

©2023 Palo Alto Networks, Inc.

STEP 7 | 確認在每個受管理設備上執行的軟體與 Content Release 版本。

1. 選取 **Panorama** > **Managed Devices**（受管理的裝置）。
2. 在表格上找到設備，並檢閱內容和軟體版本。

升級 VM-Series 型號

VM-Series 防火牆的授權程序會使用 UUID 和 CPU ID，為每個 VM-Series 防火牆產生唯一的序號。因此，當您產生授權時，會將授權對應至 VM-Series 防火牆的特定實例且無法修改。

若是下列情況，請依照本節的指示：

- 將評估授權移轉至生產授權。
- 升級型號以增加容量。例如，您想要從 VM-100 升級至 VM-300-型號。

- 升級容量，這將在防火牆上重新啟動一些重要程序。建議使用 *HA* 組態以避免服務中斷；若要在 *HA* 配對升級容量，請參閱升級 HA 配對中的 VM-Series 型號。
- 在私人或公共雲部署中，如果是以 *BYOL* 選項授權您的防火牆，則在變更實例類型或 *VM* 類型之前，必須停用 VM。升級型號或實例會變更 *UUID* 和 *CPU ID*，因此在…時，您必須套用授權。

STEP 1 | 配置額外硬體資源給 VM-Series 防火牆。

在起始容量升級之前，您必須確認有足夠硬體資源可供 VM-Series 防火牆支援新的容量。在每個 Hypervisor 上指派額外硬體資源的程序都不同。

若要查看您的新 VM-Series 型號的硬體需求，請參閱 VM-Series 型號。

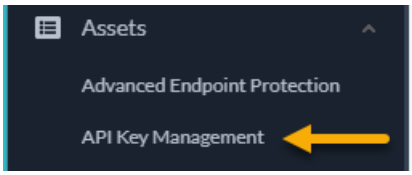
雖然容量升級不需要重新啟動 VM-Series 防火牆，但您需要關閉虛擬機器才能變更硬體配置。

STEP 2 | 從客戶支援入口網站擷取授權 API 金鑰。

1. 登入客戶支援入口網站。

   確保您使用的帳戶是您用來註冊初始授權的同一個帳戶。

2. 從左側功能表中，選取 **Assets**（資產） > **API Key Management**（**API** 金鑰管理）。
3. 複製 API 金鑰。



STEP 3 | 在防火牆上，使用 CLI 安裝上一步所複製的 API 金鑰。

```
request license api-key set key <key>
```


©2023 Palo Alto Networks, Inc.

STEP 4 | （如果您可存取網際網路）在 **Device**（裝置） > **Setup**（設定） > **Service**（服務）上，允許防火牆 **Verify Update Server identity**（驗證更新伺服器識別）。

STEP 5 | **Commit**（提交）您的變更。確定您在防火牆上有本機設定的使用者。如果設定超出未授權的 PA-VM 物件限制，在停用之後，Panorama 推送的使用者可能會無法使用。

STEP 6 | 升級容量。

選取 **Device**（裝置） > **Licenses**（授權） > **Upgrade VM Capacity**（升級 **VM** 容量），然後採用下列其中一種方式啟動授權與訂閱：

- （網際網路）**Retrieve license keys from license server**（從授權伺服器擷取授權金鑰）—如果您已在客戶支援入口網站上啟動您的授權，請使用此選項。
- （網際網路）**Use an authorization code**（使用授權碼） — 使用此選項可利用授權碼暫代先前尚未在支援入口網站上啟動的授權，升級 VM-Series 容量。出現提示時，請輸入 **Authorization Code**（授權碼），然後按一下 **OK**（確定）。
- （無網際網路）手動上傳授權金鑰—如果您的防火牆未經由網際網路連線至客戶支援入口網站，請使用此選項。從可存取網際網路的電腦登入 CSP，下載授權金鑰檔，將金鑰檔傳輸到防火牆所在相同網路中的電腦，然後上傳到防火牆。

STEP 7 | 確認已成功授權防火牆。

在 **Device**（裝置） > **Licenses**（授權）頁面上，確認已成功啟動授權。

升級 HA 配對中的 VM-Series 型號

升級 VM-Series 防火牆可讓您增加防火牆的容量。會根據 VM-Series 防火牆針對工作階段、規則、安全性區域、位址物件、IPSec VPN 通道和 SSL VPN 通道的處理進行最佳化的數量來定義容量。當您在 VM-Series 防火牆上套用新的容量授權時，防火牆上會實作型號和相關聯的容量。

升級前，驗證防火牆型號的 VM-Series 系統需求。如果防火牆的記憶體小於 *5.5GB*，則防火牆上的容量（工作階段數目、規則、安全性區域、位址物件等等）將限制為 *VM-50 Lite* 的容量。

此程序類似於升級 HA 設定中一對硬體型防火牆的程序。在容量升級過程中，工作階段同步會繼續（如果已啟用）。若要避免在高可用性 (HA) 組態中升級防火牆時的停機時間，每次更新一個 HA 端點。

在升級過程中，請勿變更防火牆的組態。在升級過程中，偵測到容量不符時會自動停用組態同步，等到兩個 *HA* 對等有相符的容量授權時，又會重新啟用。

如果 *HA* 配對中的防火牆有不同的主要軟體版本（例如 *9.1* 和 *9.0*）和不同容量，則兩個裝置都會進入「暫停」*HA* 狀態。因此，在升級容量之前，建議您確定兩個防火牆都執行相同版本的 *PAN-OS*。

©2023 Palo Alto Networks, Inc.

STEP 1 | 在被動防火牆上升級容量授權。

按照程序 升級 VM-Series 型號。

在此被動對等點上重新啟動某些程序後，新的 VM-Series 型號將顯示在儀表板上。由於與其活動對等方的容量不匹配，此升級後的對等方現在處於非運作狀態。

如果您已啟用工作階段同步，請確認 HA 對等之間的工作階段段已同步，再繼續下一步。若要驗證工作階段同步，請執行 **show high-availability interface ha2** 命令，並確定 CPU 表格上的 Hardware Interface（硬體介面）計數器增加如下：

- 在主動/被動組態中，只有主動對等會顯示傳輸的封包；被動對等將只會顯示接收的封包。

  如果您已啟用 HA2 保持活動，被動對等上的硬體介面計數器會同時顯示傳輸與接收封包。這是因為 HA2 保持活動是雙向，亦即兩個對等都會傳輸 HA2 保持活動封包。
- 在主動/主動組態中，您會看到兩個對等上接收的封包與傳輸的封包。

STEP 2 | 在主動防火牆上升級容量授權。

依照程序升級 VM-Series 型號。

在重要程序重新啟動之後，新的 VM-Series 型號會顯示在儀表板上。被動防火牆會變成主動，而此對等（先前為主動防火牆）會離開初始狀態而變成 HA 配對中的被動對等。

將 VM-Series 防火牆降級為舊版

使用下列工作流程可還原在您升級至不同功能版本之前所執行的設定。升級後所做的任何變更都會遺失。因此，請務必備份您目前的設定，以便在回復為較新的版本時還原這些變更。

使用下列程序可降級至舊版。

STEP 1 | 儲存目前組態檔案的備份。

雖然防火牆會自動建立設定的備份，但最佳做法是在升級前先建立備份，並將它儲存在外部。

1. **Export named configuration snapshot**（匯出具名設定快照）（**Device**（裝置） > **Setup**（設定） > **Operation**（操作））。
2. 選取包含執行中組態的 XML 檔案（例如 **running-config.xml**），然後按一下 **OK**（確定）匯出組態檔案。
3. 將匯出的檔案儲存至防火牆外部的位置。如果您在降級時發生問題，便可使用此備份還原設定。

©2023 Palo Alto Networks, Inc.

STEP 2 | 安裝先前的功能版本映像。

升級至新版本時，將會建立自動儲存版本。

1. **Check Now**（立即檢查）（**Device**（裝置） > **Software**（軟體））是否有可用的映像。
2. 找出您要降級的目標映像。如果尚未下載映像，請 **Download**（下載）。
3. 下載完成之後，請 **Install**（安裝）映像。
4. **Select a Config File for Downgrading**（選取用於降級的組態檔案），防火牆將在您重新啟動裝置後載入該檔案。多數情況下，您應選取在您從目前要降級的版本進行升級時自動儲存的設定。例如，如果您執行的是 PAN-OS 9.1，在降級至 PAN-OS 9.0.3 時，請選取 `autosave-9.0.3`。
5. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes**（是）。
   - 如果系統未提示您重新啟動，請移至 [Device Operations（裝置操作）]（**Device**（裝置） > **Setup**（設定） > **Operations**（操作）），並選取 **Reboot Device**（重新啟動裝置）。

©2023 Palo Alto Networks, Inc.

VM-Series 外掛程式

VM-Series 防火牆包括 VM-Series 外掛程式，這是與公共雲端提供者或私人雲端 Hypervisor 整合的內建外掛程式架構。可以手動升級與 PAN-OS 無關的 VM-Series 外掛程式，讓 Palo Alto Networks® 加速發行新的功能、修正程式或與新雲端提供者或 Hypervisor 的整合。

VM-Series 外掛程式可讓您管理 VM-Series 防火牆與受支援公共雲端平台（AWS、GCP 和 Azure）之間的雲端特定互動。外掛程式會啟用將自訂度量發佈至雲端監控服務（例如 AWS CloudWatch）、啟動、設定來自公共雲端環境的使用者認證佈建資訊，以及無縫更新 PAN-OS 上的雲端庫或代理程式。

VM-Series 外掛程式不會管理 ***VM-Series*** 防火牆和硬體型防火牆兩者通用的功能。例如，***VM*** 監控不屬於 ***VM-Series*** 外掛程式的一部分，因為它是核心 ***PAN-OS*** 功能，可協助您對來自 ***VM-Series*** 防火牆和硬體型防火牆的虛擬機器工作負載一致地強制執行政策。

VM-Series 外掛程式不會管理 Panorama 外掛程式。如需 ***VM-Series*** 外掛程式與 ***Panorama*** 外掛程式之間的差異，請參閱 VM-Series 外掛程式和 Panorama 外掛程式。

VM-Series 外掛程式是可以升級或降級但不能移除的內建元件。每個 PAN-OS 版本都包括對應至 PAN-OS 軟體版本的特定 VM-Series 外掛程式版本。當您降級至較舊 PAN-OS 軟體版本時，會將外掛程式版本降級至與 PAN-OS 版本相容的版本。您可以在虛擬防火牆本機升級或降級 VM-Series 外掛程式，或從 Panorama 集中管理外掛程式版本。

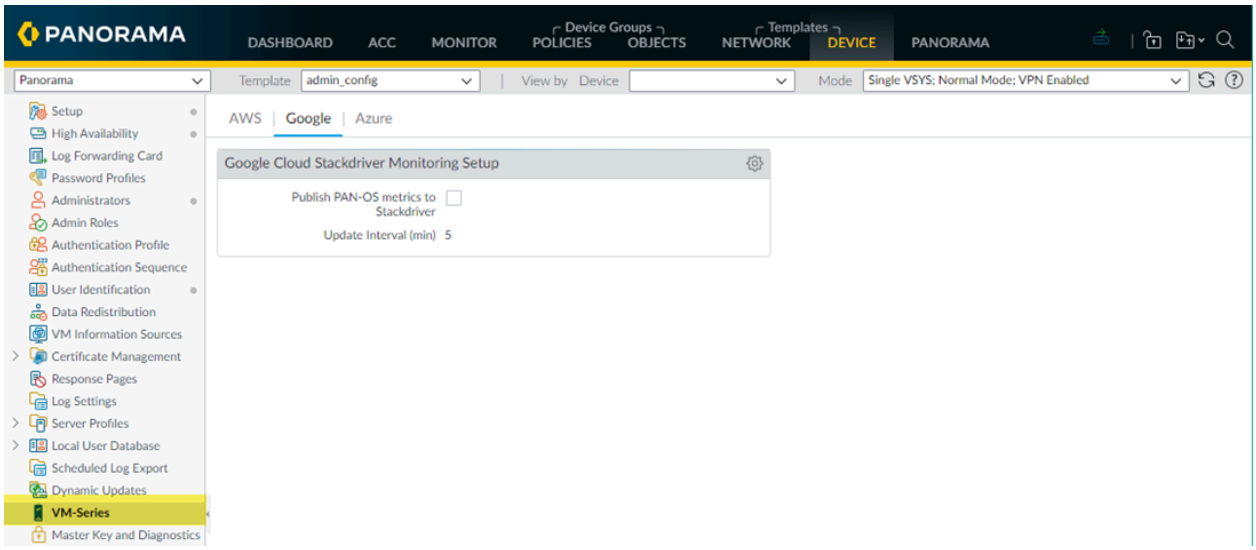
若要啟用 Panorama 來管理 VM-Series 外掛程式版本本身或發佈受管理防火牆的雲端特定度量，您必須在 Panorama 上手動安裝 VM-Series 外掛程式，如 Panorama 外掛程式所述。

- 在防火牆上設定 VM-Series 外掛程式
- 升級 VM-Series 外掛程式

在防火牆上設定 VM-Series 外掛程式

選取 **Device**（裝置） > **VM-Series**，為部署此 VM-Series 防火牆實例的雲端供應商設定外掛程式整合。

©2023 Palo Alto Networks, Inc.



如果在未使用公共介面（例如，VMware ESXi）的情況下於 Hypervisor 或雲端上部署防火牆，則此頁籤的名稱為 VM-Series，並顯示一般訊息。

升級 VM-Series 外掛程式

發行與 PAN-OS 無關的外掛程式更新時，您可以從 VM-Series 防火牆（如軟體或內容更新）或啟動檔案獨立升級外掛程式版本。

每個外掛程式版本都會提供 PAN-OS 相容性資訊，並包括一個或多個雲端環境的新功能或錯誤修正程式。

STEP 1 | 升級之前，請檢查最新版本資訊，以取得新的 VM-Series 外掛程式是否會影響環境的詳細資料。

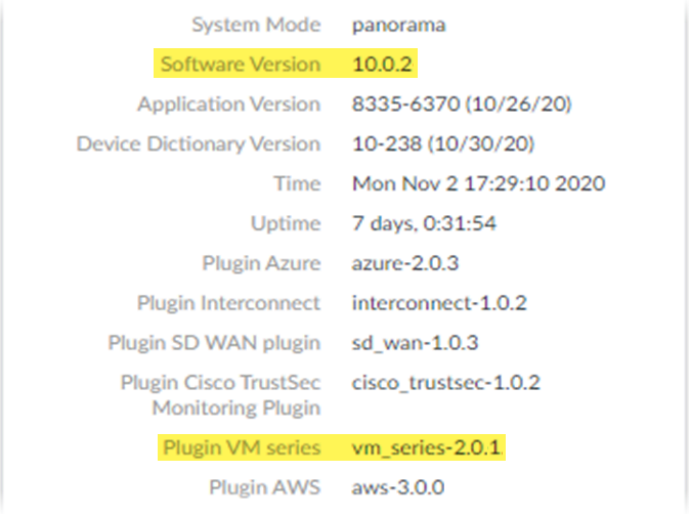
例如，假設新的 VM-Series 外掛程式版本僅包括 AWS 功能。若要利用新功能，您必須更新 AWS 的 VM-Series 防火牆實例上的外掛程式。

請不要安裝未套用至環境的升級。

僅在 *PAN-OS 10.2.0* 中支援 *VM-Series 3.0.0* 插件。

©2023 Palo Alto Networks, Inc.

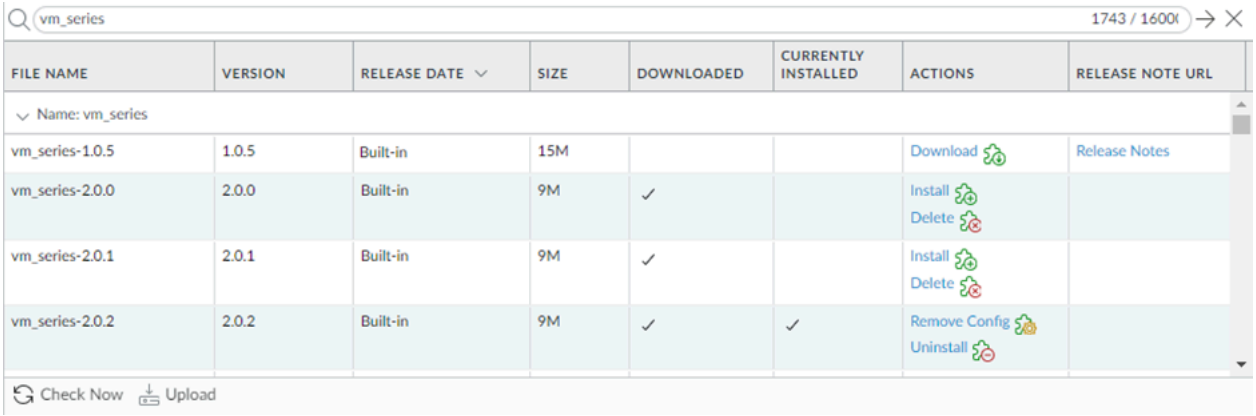
STEP 2 | 登入 VM-Series 防火牆，並檢查儀表板以檢視外掛程式版本。



STEP 3 | 選取 **Panorama** > **Plugins**（外掛程式），然後在搜尋欄位中輸入 **`vm_series`**。

選取 **Check Now**（立即檢查）以檢視可用的版本。

STEP 4 | 選擇 VM-Series 外掛程式版本，然後按一下 **Download**（下載）。

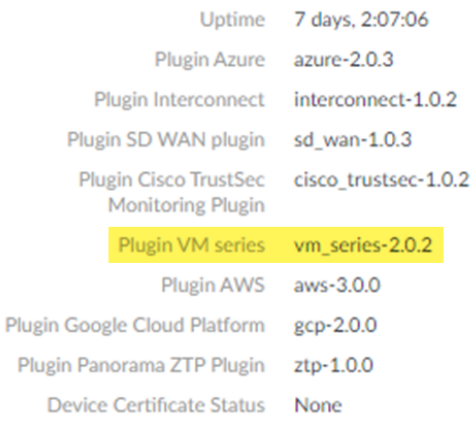


STEP 5 | 下載完成後，按一下 **Actions**（動作）欄中的 **Install**（安裝）。

防火牆會自動解除安裝先前安裝的外掛程式版本。

©2023 Palo Alto Networks, Inc.

STEP 6 | 檢視 **Dashboard**（儀表板），確認外掛程式已成功升級。



Uptime	7 days, 2:07:06
Plugin Azure	azure-2.0.3
Plugin Interconnect	interconnect-1.0.2
Plugin SD WAN plugin	sd_wan-1.0.3
Plugin Cisco TrustSec Monitoring Plugin	cisco_trustsec-1.0.2
Plugin VM series	vm_series-2.0.2
Plugin AWS	aws-3.0.0
Plugin Google Cloud Platform	gcp-2.0.0
Plugin Panorama ZTP Plugin	ztp-1.0.0
Device Certificate Status	None

©2023 Palo Alto Networks, Inc.

在 VM-Series 防火牆上啟用巨型框架

依預設，在 Layer 3 介面上所傳送封包的最大傳輸單位 (MTU) 大小為 1500 位元組。可以在每個介面上手動設定範圍為 512 至 1500 位元組的任意大小。某些組態需要具有一個 MTU 值大於 1500 位元組的乙太網路框架。這些框架稱為 Jumbo Frame。

若要在防火牆上使用 Jumbo Frame，您必須特別啟用全域級 Jumbo Frame。啟用後，所有 Layer 3 介面的預設 MTU 大小值將設定為 9192 位元組。此預設值可設定為範圍為 512 至 9216 位元組的任意值。

設定全域 Jumbo Frame 大小後，其將變為所有 Layer 3 介面的預設值，此介面沒有明確設定組態級 MTU 值。如果您僅僅想要在某些介面上交換 Jumbo Frame，這可能會存在問題。在這些情境中，您必須在每一個您不想使用預設值的 Layer 3 介面上設定 MTU 值。

下列步驟說明了如何在防火牆上啟用 Jumbo Frame，為所有 Layer 3 介面設定預設 MTU 值，以及隨後為指定介面設定不同的值。

啟用 *Jumbo Frame* 支援時，部署於多個 *NUMA* 節點的 *VM-Series* 防火牆實例會以封包 *MMAP* 模式出現。您必須停用 *Jumbo Frame* 支援，才能在部署於多個 *NUMA* 節點的 *VM-Series* 防火牆實例上使用 *DPDK*。

STEP 1 | 啟用 Jumbo Frame 並設定預設全域 MTU 值。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段），然後編輯 [Session Settings（工作階段設定）] 區段。
2. 選取 **Enable Jumbo Frame**（啟用 **Jumbo Frame**）。
3. 為 **Global MTU**（全域 **MTU**）輸入值。

   預設值是 9192。可接受的值範圍為：512 - 9216。
4. 按一下 **OK**（確定）。

   將會顯示訊息指出啟用或停用「巨型框架」模式需要重新啟動，而且第 3 層介面會繼承 **Global MTU**（全域 **MTU**）值。
5. 按一下 **Yes**（是）。

   顯示一則訊息提示您，Jumbo Frame 支援已啟用，並提醒您需要重新啟動設備，才能啟動此變更。
6. 按一下 **OK**（確定）。
7. 按一下 **Commit**（交付）。

©2023 Palo Alto Networks, Inc.

STEP 2 | 為 Layer 3 介面設定 MTU 值並重新啟動防火牆。

為介面設定的值將覆寫全域 *MTU* 值。

1. 選取 **Network**（網路） > **Interfaces**（介面）。
2. 選取 **Interface type**（介面類型）為 Layer3 的介面。
3. 選取 **Advanced**（進階） > **Other Info**（其他資訊）。
4. 輸入 **MTU** 值。

   預設值是 9192。可接受的值範圍為：512 - 9216。
5. 按一下 **OK**（確定）。
6. 按一下 **Commit**（交付）。
7. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後選取 **Reboot Device**（重新啟動裝置）。

©2023 Palo Alto Networks, Inc.

Hypervisor 指派的 MAC 位址

根據預設，VM-Series 防火牆會使用主機/超管理器指派給實體介面的 MAC 位址，以部署具有第 3 層介面的 VM-Series 防火牆。防火牆隨後可在其 ARP 回應中使用 Hypervisor 指派的 MAC 位址。此功能允許非學習交換器，例如 VMware vSwitch，將流量轉送至防火牆上的資料背板介面，而無需在 vSwitch 上啟用混合型模式。如果既未啟用混合型模式，也未使用 Hypervisor 指派的 MAC 位址，則當偵測到介面的目的地 MAC 位址與主機指派的 MAC 位址之間不符時，主機會丟棄框架。

在 *AWS* 和 *Azure* 上，沒有選項可啟用或停用 ***Hypervisor*** 指派的 ***MAC*** 位址。在兩個平台上都預設為啟用，無法停用。

如果您正在使用 Layer 2、Virtual Wire 或旁接介面模式部署 VM-Series 防火牆，則您必須在連接防火牆的虛擬交換器上，啟用混合式模式。使用 Hypervisor 指派的 MAC 位址只與第 3 層部署有關，其中防火牆通常為來賓虛擬機器的預設閘道。

在 VM-Series 防火牆上啟用 Hypervisor 指派的 MAC 位址功能時，請注意下列需求：

- 介面上的 **IPv6** 位址—在主動/被動 HA 組態中（請參閱高可用性 VM-Series），使用 IPv6 位址的第 3 層介面不得將 EUI-64 產生的位址用作介面識別碼（介面 ID）。由於 EUI-64 使用介面的 48 位元 MAC 位址來衍生介面的 IPv6 位址，因此 IP 位址不是靜態的。因此，當託管 VM-Series 防火牆的硬體隨故障復原變更時，HA 端點的 IP 位址也會變化，從而導致 HA 失敗。
- **IP** 位址租用—MAC 位址變更時，DHCP 用戶端、DHCP 轉送及 PPPoE 介面可能會釋放 IP 位址，因為原 IP 位址租用可能已終止。
- **MAC** 位址及 **Gratuitous ARP**—在高可用性組態中具有 Hypervisor 指派的 MAC 位址的 VM-Series 防火牆，其行為有別於與 MAC 尋址有關的硬體設備。硬體防火牆在高可用性配對中的設備間使用自產生浮動 MAC 位址，且用於個資料背板（即 eth 1/1）的唯一 MAC 位址被取代為虛擬 MAC 位址，這在兩個 HA 端點上的資料背板介面上很常見。您在高可用性 VM-Series 防火牆上啟用 Hypervisor 指派的 MAC 位址後，不會使用虛擬 MAC 位址。高可用性端點上的資料背板是獨一無二的，且由 Hypervisor 指定。

  由於每個資料背板介面均具有唯一的 MAC 位址，當發生故障復原時，現在的主動 VM-Series 防火牆必須傳送一個 Gratuitous ARP，以便相臨的設定可以知曉更新的 MAC/IP 位址配對。因此，若要啟用狀態容錯移轉，網路裝置不得封鎖或略過 Gratuitous ARP；如有需要，請務必在網際網路裝置上停用 ARP 毒害防禦功能。

執行下列步驟來設定 VM-Series 防火牆使用主機/Hypervisor 提供的介面 MAC 位址。

STEP 1 | 選取 **Device**（裝置） > **Management**（管理） > **Setup**（設定） > **General Settings**（一般設定）。

STEP 2 | 按一下 **Edit**（編輯）圖示。

STEP 3 | 勾選 **Use Hypervisor Assigned MAC Address**（使用超管理器指派的 **MAC** 位址）選項。

當 MAC 位址發生變更時，防火牆將產生系統日誌，記錄此轉換，且介面產生 Gratuitous ARP。

STEP 4 | 按一下 **OK**（確定）。

STEP 5 | **Commit**（提交）防火牆上的變更。您不需要重新啟動防火牆。

©2023 Palo Alto Networks, Inc.

發佈自訂 PAN-OS 度量以作為監控使用

防火牆原本就會發佈下列度量以監控在如 AWS® CloudWatch、Azure® Application Insights 與 Google® Stackdriver 這類公共雲端中的系統。這些度量可讓您評估防火牆效能和使用模式，使您可設定警報並採取動作以將事件自動化，如啟動或終止 VM-Series 防火牆的實例。因為這些度量乃是透過在防火牆上的內容更新來發佈，所以請確定您有需要啟用在您 VM-Series 防火牆上這個功能的最少內容發行版本。

指標	說明
資料平面 **CPU** 使用率 **(%)**	監控資料平面 CPU 使用量並測量防火牆上的流量負載。
資料平面封包緩衝區使用率 **(%)**	監控資料平面緩衝區使用量並測量緩衝區使用率。如果流量突然暴增，您可以監控緩衝區使用率，以確保防火牆不會用盡資料平面緩衝區，以導致丟棄封包。
GlobalProtect™ 閘道作用中通道數	監控部署為 GlobalProtect 閘道的防火牆上的作用中 GlobalProtect 工作階段數目。如果您使用此 VM-Series 防火牆作為 VPN 閘道來保護遠端使用者安全，請使用此度量。查看數據表以獲取防火牆模型可支援的最大作用中通道數。
GlobalProtect 閘道通道使用率 **(%)**	監控閘道上的作用中 GlobalProtect 通道並測量通道使用率。如果您使用此 VM-Series 防火牆作為 VPN 閘道來保護遠端使用者安全，請使用此度量。
panSessionConnectionsPerSecond	監控每秒的新連線建立速率。
panSessionThroughputKbps	監控輸送量，以 Kbps 為單位。
panSessionThroughputPps	監控每秒傳送的封包數目。
作用中的工作階段	監控防火牆上作用中的工作階段總數。作用中工作階段是出現在流程查閱表中的工作階段，將會依原則所需來檢查和轉送其中的封包。
工作階段使用率 **(%)**	監控目前作用中的 TCP、UDP、ICMP 與 SSL 工作階段以及封包速率、新連線建立速率和決定工作階段使用率的防火牆吞吐量。
SSLProxyUtilization (%)	在 SSL/TLS 解密方面監控用戶端執行 SSL 轉送 Proxy 工作階段的百分比。

若要發佈這些度量，請參閱：

©2023 Palo Alto Networks, Inc.

- 在 VM-Series 防火牆上啟用 CloudWatch 監控
- 在 VM-Series 防火牆上啟用 Azure Application Insights
- 在 VM Series 防火牆上啟用 Google Stackdriver 監控

©2023 Palo Alto Networks, Inc.

存取 VM-Series 防火牆外部服務所使用的介面

若要存取 Palo Alto Networks 伺服器以擷取授權以及軟體和內容更新，並發佈自訂 PAN-OS 度量，或擷取 IP 位址以及用於監控部署的虛擬電腦標記對應，VM-Series 防火牆會使用除下述之外的管理介面。若要使用平面介面而非所支援的管理介面，則您必須設定一個服務路由，以便指定防火牆可以使用的平面介面，來存取該伺服器或服務。

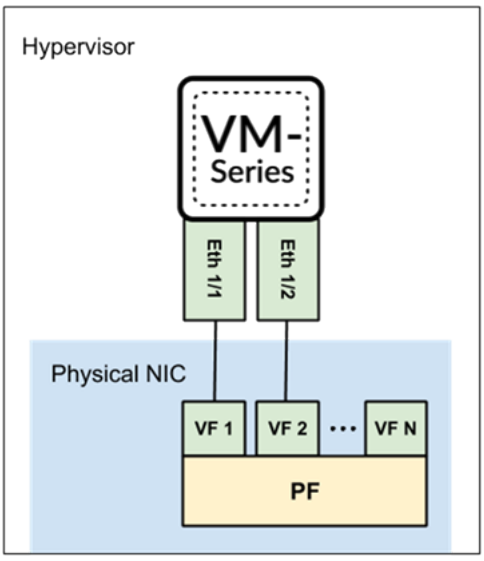
存取伺服器或服務	在 **VM-Series** 防火牆上使用的介面
授權	僅限管理介面
軟體更新	管理介面或服務路由
從 AWS S3 貯體、Azure 儲存檔案服務或 Google 儲存貯體這類雲端儲存位置啟動	僅限管理界面，包括交換介面時 如果您的 ***bootstrap.xml*** 檔案包含授權驗證碼，則無法使用服務路由。若要授權此防火牆，則必須使用管理界面。
發佈 PAN-OS 度量至雲端監控服務，如：AWS CloudWatch、Azure Application Insights 或 Google Stackdriver	僅限管理界面，包括交換介面時
VM 監控	管理介面或服務路由

©2023 Palo Alto Networks, Inc.

PacketMMAP 和 DPDK 驅動程式支援

單一根目錄輸入/輸出虛擬化 (SR-IOV) 依賴 VM-Series 防火牆上虛擬功能 (VF) 驅動程式與主機（超管理器）上實體功能 (PF) 驅動程式之間的通訊。主機使用 PF 驅動程式來與實體 NIC 通訊，VM-Series 防火牆使用 VF 驅動程式來與 PF 驅動程式通訊。

下圖簡單表示此概念。



SR-IOV

為何使用 SR-IOV？SR-IOV 是一種封包加速技術，可讓 virtual machine（虛擬機器 - VM）直接從 NIC 存取封包。相反地，使用 virtual switch（虛擬交換器 - vSwitch）時，由主機處理封包，透過虛擬交換器傳送封包，然後由 virtual machine（虛擬機器 - VM）接收封包。

在相容性矩陣中，PacketMMAP 驅動程式版本列出主機版本和 VM-Series 防火牆上的原生驅動程式版本。例如，主機上的 i40e 和防火牆上的 i40e（用於 PCI 通道）i40evf（用於 SR-IOV）。

若為 SR-IOV，假設 NIC 使用 i40e PF 驅動程式。主機透過 i40e 驅動程式來與 NIC 通訊。VM-Series 防火牆可以使用 VF 驅動程式 (i40evf)，直接與主機的 PF 驅動程式通訊。這可讓 VM-Series 防火牆直接存取，改善封包處理速度。為了確保相容性，請安裝比原生 PF 驅動程式版本更新的主機 PF 驅動程式版本。

PCI 通道

VM-Series 防火牆為何有原生 PF 驅動程式？如在網路上連接 VM-Series 的選項所述，使用 PCI 通道時，NIC 會保留給 VM-Series 防火牆，所以主機（或主機上的其他來賓）無法存取 NIC。在 PCI 通道設定中，VM-Series 防火牆使用原生 PF 驅動程式，直接與主機 NIC 通訊。

請參閱 PacketMMAP 驅動程式版本清單，以決定要安裝在主機上的 PF 驅動程式版本。請安裝高於 VM-Series 防火牆原生 PF 驅動程式的 PF 版本。

關於 PCI 通道，請參閱在 ESXi 上啟用 SR-IOV和在 KVM 上啟用 SR-IOV。

©2023 Palo Alto Networks, Inc.

DPDK

PAN-OS 有兩個封包處理模式—DPDK（預設值）和 MMAP—每個模式在 VM-Series 防火牆上都有對應的原生驅動程式。例如，如果防火牆在 DPDK 模式中，則防火牆會使用 DPDK i40evf 驅動程式版本來與主機的 i40e 驅動程式通訊（使用 SR-IOV 時）。或者，當防火牆是封包 MMAP 時，則會使用不同的 i40evf 驅動程式來與主機的 i40e 驅動程式通訊。

您可以在主機（超管理器）或來賓（VM-Series VM-Series）上啟用 DPDK。兩者都啟用可達到最佳效果。

- 在主機上啟用 DPDK 會以 DPDK 編譯 OVS。

  請參閱在主機上設定 OVS 和 DPDK。
- VM-Series DPDK 會在 VM-Series 防火牆上啟用原生 DPDK 驅動程式，因此在主機上不需要啟用 DPDK，但建議啟用以獲得最佳效能。

©2023 Palo Alto Networks, Inc.

在 VM-Series 上啟用 NUMA 效能最佳化

若要改善 VM-Series 防火牆的效能，您可以啟用 non-uniform memory access（非統一記憶體存取；NUMA）效能最佳化。啟用 NUMA 效能最佳化時，VM-Series 防火牆資料平面會使用連接至 NUMA 節點 0 的 vCPU。VM-Series 防火牆資料平面僅使用屬於 NUMA 節點 0 的 vCPU。VM-Series 管理平面使用核心 0，而 VM-Series 資料平面可以使用 NUMA 節點 0 上剩餘的 vCPU。此功能需要 PAN-OS 10.1.1 或更新版本，以及 VM-Series 外掛程式 2.1.1 或更新版本。

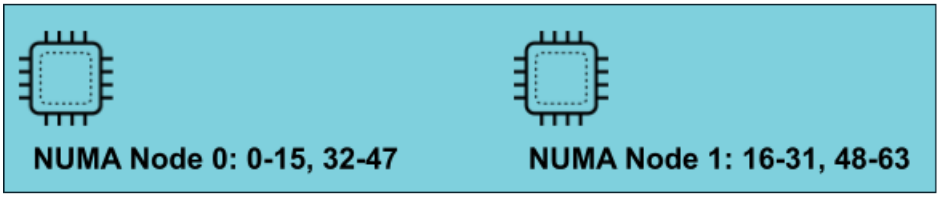
NUMA 效能最佳化在 PAN-OS 10.1 中預設為停用。

如果您的裝置有 64 個核心分散於兩個 NUMA 節點上，則未啟用 NUMA 效能最佳化時，VM-Series 防火牆使用的資料平面 vCPU 可能位於不同的節點，這會影響效能。例如，如果系統的組織如下列範例所示，且您部署的 VM-Series 防火牆總共有 32 個核心和 24 個資料平面核心。

如果沒有 NUMA 效能最佳化，VM-Series 防火牆會在節點 0 上使用核心 1 到 15，在節點 1 上使用核心 16 到 24，因為是按數值順序指派核心，而不論節點位置為何。如果啟用 NUMA 最佳化，VM-Series 只會使用節點 0 上的核心，在此例子中為 1 到 15 和 33 到 39，而不論數值順序為何。資料平面未使用的任何核心都指派給管理平面。

搭配自訂資料平面核心設定的 NUMA 性能最佳化，會優先使用 NUMA 設定。例如，對於啟用了 NUMA 性能最佳化和 47 個資料平面核心設定的 64 CPU VM，會優先使用 NUMA 設定。

如果指派給 *VM-Series* 防火牆的核心數目超過節點 *0* 上的 *vCPU* 數目，*VM-Series* 會使用節點 *0* 上的所有核心，而不會使用其他節點的任何核心。例如，如果您將 *30* 個核心指派給 *VM-Series* 防火牆，但節點 *0* 只有 *24* 個核心，則 *VM-Series* 防火牆的資料平面只會使用節點 *0* 上的 *24* 個核心。



STEP 1 | 登入 VM-Series CLI。

STEP 2 | 執行下列命令。

```
request plugins vm_series numa-perf-optimize enable on
```

```
先前的 NUMA 效能最佳化：無
要求的 NUMA 效能最佳化：已啟用
Please reboot the PA-VM.
```

STEP 3 | 重新啟動完成後，登入 VM-Series CLI，確認 NUMA 最佳化已啟用。

```
show plugins vm_series numa-perf-optimize
```

```
NUMA 效能最佳化：已啟用
```


©2023 Palo Alto Networks, Inc.

STEP 4 | 驗證資料平面核心的數目。

```
show plugins vm_series dp-cores
```

目前 DP 核心數：31 已設定的自訂 DP 核心數：47（目前核心總數：64）

STEP 5 | 若要停用 NUMA 效能最佳化，請使用下列命令。此命令需要您重新啟動 VM-Series 防火牆。

```
request plugins vm_series numa-perf-optimize enable off
```


©2023 Palo Alto Networks, Inc.

在 VM-Series 防火牆上啟用 ZRAM

如果 VM-Series 防火牆發生記憶體不足或用盡的情況，您可以啟用 ZRAM 以改善記憶體使用情形。ZRAM 是一個 Linux 核心模組，又稱為 compcache（壓縮快取），用於在 RAM 中建立壓縮區塊裝置。ZRAM 啟用時作為交換磁碟，由於位於 RAM 中，可讓交換的 I/O 更快。

完成以下步驟以啟用 ZRAM。

STEP 1 | 登入 VM-Series CLI。

STEP 2 | 使用下列 CLI 命令查明 VM 的記憶體總數。

```
grep pattern “KiB Mem :” mp-log mp-monitor.log
```

```
KiB Mem: 總計 9202656, 566504 可用, 3475840 已使用, 5160312 buff/cache
 KiB Mem: 總計 9202656, 497112 可用, 3481944 已使用, 5223600 buff/cache
 KiB Mem: 總計 9202656, 511744 可用, 3466768 已使用, 5224144 buff/cache
 KiB Mem: 總計 9202656, 511668 可用, 3466340 已使用, 5224648 buff/cache
 KiB Mem: 總計 9202656, 512124 可用, 3465700 已使用, 5224832 buff/cache
 KiB Mem: 總計 9202656, 511436 可用, 3465976 已使用, 5225244 buff/cache
 KiB Mem: 總計 9202656、510984 可用、3465944 已使用、5225728 buff/cache
```

STEP 3 | 將以上記憶體總數從 KB 轉換成 MB。例如：

9202656 / 1024 = 8987 MB

以 MB 為單位記下記憶體總數。您在下一個步驟中需要此值。

STEP 4 | 使用以下兩個 CLI 命令啟用 ZRAM。

```
debug software kernelcfg zram-swap enable
```

```
debug software kernelcfg zram-swap modify host-mem-threshold <total-memory-in-MB>
```

STEP 5 | 重新啟動 VM-Series 防火牆。

STEP 6 | 確認已啟用 ZRAM。

```
debug software kernelcfg zram-swap show config
```


©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

授權 VM-Series 防火牆

VM-Series 防火牆支援兩種授權類型（BYOL 和 PayGo），以及兩種不同的授權模式 — Software Next Generation Firewall Credits（軟體新世代防火牆積分；Software NGFW），適用於您以部署設定檔指定的彈性設定，以及固定 VM-Series 型號設定。這兩種模式也授權安全性服務和其他功能。

如果您是授權 CSSP 夥伴，請參閱 Cloud Security Service Provider（雲端安全服務供應商 - CSSP）的授權，以取得與您有關的資訊。

如需有關建立支援帳戶和管理授權的詳細資訊，請參閱下列主題：

- VM-Series 防火牆授權
- 建立支援帳戶
- VM-Series 防火牆的序號和 CPU ID 格式
- 授權 API
- 安裝授權 API 金鑰
- 使用基於 Panorama 的軟體防火牆授權管理
- 軟體 NGFW 積分
- VM-Series 型號
- Cloud Security Service Provider（雲端安全服務供應商 - CSSP）的授權

VM-Series 防火牆授權

本章比較下列授權資訊：

- 授權類型：BYOL 與 PayGo
- 彈性 vCPU 和固定型號授權：彈性 vCPU 與固定型號
- 彈性 vCPU 和固定型號部署：彈性和固定型號的部署步驟摘要。

授權類型

Palo Alto Networks 目前支援兩種授權類型：Bring Your Own License（自帶授權；BYOL）和 PAYG（Pay-As-You-Go，也稱為 PayGo；即用即付）。

類型	說明
BYOL	軟體 NGFW 積分—適用於執行所有 PAN-OS 版本的 VM-Series 防火牆。執行 PAN-OS 版本 10.0.4 和更新版本的 VM-Series 防火牆提供進階功能和更大彈性。彈性授權成本取決於 vCPU 數目、您已啟用的安全性服務，以及您選擇佈建 Panorama 來管理防火牆還是作為日誌收集器。 如需詳細解釋，請參閱軟體 NGFW 積分。
BYOL	VM-Series 型號授權—適用於所有 PAN-OS 版本。根據您選擇的 VM-Series 型號，vCPU 的數目固定不變。 彈性 ***vCPU*** 適用於 ***PAN-OS 10.0.4*** 和更新版本，支援進階功能和更多 ***vCPU***。 容量授權成本取決於 VM-Series 型號、裝置記憶體、儲存成本和支援權利。用於管理防火牆的安全性服務和 Panorama 部署需要額外成本。容量授權類型包括： · **VM-Series 企業授權合約（多重型號 ELA）**—VM-Series 防火牆的一年或三年全面授權合約。個人授權可以包括型號、安全服務、支援權利和 Panorama 選用裝置管理授權。 多重型號 ELA 提供權杖池，供您從中分配權杖來授權 VM-Series 防火牆。（這是 ELA 特有，不同於軟體 NGFW 積分池。） · 永久 VM-Series 型號容量授權，含支援權利和/或安全服務搭售包 1 或搭售包 2。 · 期限防火牆容量授權，含支援權利和您選擇的安全服務。
PayGo	從公共雲端市集（例如 AWS、Azure 或 GCP）或 Cloud Security Service Provider（雲端安全服務供應商；CSSP）購買。適用於供應商支援的 PAN-OS 版本。 在 9.1.1 之前 PAN-OS 版本中，PayGo 僅支援 VM-Series VM-300 型號。對於 PAN-OS 9.1.1 和更新版本，PayGo 可支援固定型號。支援傳統的 VM 型號，例如 VM-100、VM-300、VM-500 和 VM-700。

©2023 Palo Alto Networks, Inc.

彈性 vCPU 和固定型號授權

彈性 vCPU 軟體 NGFW 授權與固定 vCPU VM-Series 型號授權之間有何差異？對不同項目收費，並以不同方式提供資金。下表快速比較，並連結到更多詳細資訊。

	彈性 **vCPU**	**VM-Series** 型號（固定 **vCPU**）
說明	成本根據 vCPU 數目和您選擇的安全性服務而定。 除了 Panorama 耗用的 vCPU，沒有成本。 您購買可重複使用的軟體 NGFW 積分，在預定期限結束時會到期。啟動積分後，您可以將它們分配到積分池中。 若要使用積分，請選擇積分設定檔，並建立一個或多個部署設定檔。選擇您自己的防火牆即平台元件組合：VM-Series vCPU、安全性服務、作為管理或專用日誌收集的虛擬 Panorama，以及支援權利。以設定檔部署的所有防火牆都以相同的驗證碼授權，您可以從部署設定檔來管理防火牆。	成本取決於 VM-Series 型號容量授權、裝置記憶體和儲存體。Panorama 和安全性服務是另外購買。 · VM-Series 企業授權合約（多重型號 ELA）—VM-Series 防火牆的一年或三年全面授權合約。 多重型號 ELA 提供權杖池，供您從中分配權杖來授權 VM-Series 防火牆。 · 永久 VM-Series 型號容量授權，含支援權利和/或安全服務搭售包 1 或搭售包 2。 · 期限防火牆容量授權，含支援權利和您選擇的安全服務。
啟動	需要啟動電子郵件。啟動和註冊會自動進行。	需要啟動電子郵件，啟動後還需要另外的註冊步驟。
安全性服務	Threat Prevention、DNS Security、GlobalProtect、WildFire、URL Filtering、SD-WAN、DLP 及其他剛推出的服務。 當您建立部署設定檔時，您可以選擇安全性服務的任何組合。您可以隨時在設定檔中新增或移除安全性服務。	搭售包 **1**：Threat Prevention 和進階支援權利。 搭售包 **2**：Threat Prevention、DNS Security、GlobalProtect、WildFire、URL Filtering、SD-WAN、DLP 及進階支援權利。
PAN-OS 版本	多達 64 個彈性 vCPU 和進階服務選項，適用於執行 10.0.4 和更新版本的防火牆。	您可以在任何 PAN-OS 版本上部署 VM-Series 型號（固定 vCPU）。
資金	可重複使用的積分，可讓您取用防火牆即平台元件。 購買積分之後，您必須啟動積分，將積分與組織的特定帳戶建立關聯。啟動的積分將資金注入積分池，供您從中建立部署設定檔。	· 多重型號 ELA：權杖。 · 永久 VM-Series 型號容量授權，含支援權利和/或安全服務搭售包 1 或搭售包 2。您在購買時決定設定。除非您購買新的授權，否則無法變更設定。

©2023 Palo Alto Networks, Inc.

	彈性 vCPU	VM-Series 型號（固定 vCPU）
	部署防火牆時會消耗積分。當防火牆停用時，積分會釋出並歸還積分池供進一步使用。	• 期限防火牆容量授權，含支援權利和您選擇的安全服務。
部署設定	彈性。您可以隨時變更部署設定檔。設定檔的變更會傳播到共用部署設定檔驗證碼的所有防火牆。	VM-Series 型號容量不會變更，但如果您有 ELA，則可以新增安全性服務。 永永久授權和期限授權是事先設定並付費，不會變更。
部署	積分啟動後，請為特定環境或使用案例（例如「保護我的 NSX 環境」）建立部署設定檔，並設定防火牆 vCPU、安全性服務和選用的虛擬 Panorama。您可以建立任意數量的部署設定檔，並隨時自訂設定檔。 您必須具備客戶支援入口網站角色「積分管理員」（僅適用於帳戶管理），才能啟動和管理軟體 NGFW 積分。	接受 VM-Series ELA。部署和設定 VM-Series 防火牆。啟動型號授權並註冊防火牆。
Panorama	建立部署設定檔時，您可以選擇新增 Panorama 作為管理，或供使用部署設定檔的防火牆當作專用日誌收集器。此 Panorama 可以管理以部署設定檔的共用驗證碼所部署的防火牆。	Panorama 是另外的費用。實體或虛擬 Panorama 可用於防火牆管理或日誌收集。
升級或降級	如果 VM-Series 防火牆或 Panorama 有網際網路連線，則部署設定檔的變更會自動套用至防火牆。 如果防火牆沒有網際網路連線，請手動停止防火牆。在 [Assets（資產）] > [Software NGFW Credits（軟體 NGFW 積分）] 中，變更部署設定檔，然後在 CSP 中，下載授權金鑰並傳輸至 VM、從 CSP 取得設定檔並傳輸至 VM、重新啟動 VM，然後套用授權。 在任一情況下，您都不需要重新啟動防火牆。	變更為不同型號需要變更授權並重新啟動。

彈性 vCPU 和固定型號部署

下列檢查清單比較軟體 NGFW 積分和 VM-Series 型號授權方法的部署程序。

©2023 Palo Alto Networks, Inc.

彈性 vCPU	固定 vCPU（VM-Series 型號）
1. 建立支援帳戶. 2. 啟動積分. 您的組織可以有許多帳戶來代表不同的成本中心。在註冊期間，您需要將購買的積分與帳戶建立關聯。 3. 建立部署設定檔. 4. 在 Alibaba、AWS、Azure、Cisco ACI、Cisco CSP、Cisco ENCS、ESXi、Google Cloud Platform、Hyper-V、KVM、OpenStack 部署 VM-Series 防火牆。Oracle Cloud Infrastructure、vCloud Air、NSX-T 或 NSX-V 5. 在 VM-Series 防火牆上安裝裝置憑證（適用於網站授權，例如 Cortex Data Lake 和 Auto Focus）。	1. 建立支援帳戶. 2. 啟動 VM-Series 型號授權. 3. 註冊 VM-Series 防火牆. 4. 在 Alibaba、AWS、Azure、Cisco ACI、Cisco CSP、Cisco ENCS、ESXi、Google Cloud Platform、Hyper-V、KVM、OpenStack 部署 VM-Series 防火牆。Oracle Cloud Infrastructure、vCloud Air、NSX-T 或 NSX-V。 5. 在 VM-Series 防火牆上安裝裝置憑證（適用於網站授權，例如 Cortex Data Lake 和 Auto Focus）。

©2023 Palo Alto Networks, Inc.

建立支援帳戶

您需要支援帳戶才能登入客戶支援入口網站 (CSP)。您必須登入才能啟動和管理軟體 NGFW 積分、存取軟體更新，或向 Palo Alto Networks 技術支援提交案例。支援帳戶可讓您檢視和管理您向 Palo Alto Networks 註冊的所有資產，包括設備、授權及訂閱。

對於所有授權選項（目前只在 AWS 中可用的依使用授權除外），您需要支援帳戶，才能下載安裝 VM-Series 防火牆所需的軟體套件。

如果您已有支援帳戶，則可以下載並安裝 VM-Series 防火牆軟體，然後繼續註冊 VM-Series 防火牆。

STEP 1 | 前往 https://support.paloaltonetworks.com/UserAccount/PreRegister。

STEP 2 | 輸入要與支援帳戶建立關聯的公司電子郵件地址。

STEP 3 | 選取下列選項之一，並在使用者註冊表單中填寫詳細資訊：

適用於 AWS 中的依使用授權

1. 按一下 **Register your Amazon Web Services VM-Series Instance**（註冊您的 **Amazon Web Services VM-Series** 實例）。
2. 在 AWS 管理主控台上，找到 AWS 實例 ID、AWS 產品代碼、您部署防火牆所在的 AWS 區域。
3. 填寫其他詳細資訊。

適用於所有其他授權

1. 按一下 **Register device using Serial Number or Authorization Code**（使用序號或驗證碼註冊裝置）。
2. 輸入容量驗證碼及銷售訂單號碼或客戶 ID。
3. 填寫其他詳細資訊。

STEP 4 | **Submit**（提交）表單。您將收到電子郵件，其中有連結可啟動使用者帳戶。

完成步驟來啟動帳戶。您的帳戶經驗證後，註冊即告完成，您可登入支援入口網站。

©2023 Palo Alto Networks, Inc.

VM-Series 防火牆的序號和 CPU ID 格式

啟動 VM-Series 防火牆時，防火牆的每個實例都是以防火牆的 CPU ID 和序號來唯一識別。CPU ID 格式和序號包含每個 VM-Series 防火牆實例的超管理器和授權類型的相關資訊。

- 對於 VM-Series 防火牆的基於使用量授權模式，防火牆啟動時會產生序號和 CPU ID，您可以使用這些詳細資訊來註冊依使用授權版公共雲端專用 VM-Series 防火牆（無驗證碼）。
- 透過 BYOL 模式，您可以在 Customer Support portal（客戶支援入口網站；CSP）上註冊 VM-Series 防火牆彈性授權或具有彈性授權的 VM-Series 防火牆。
  - 如果防火牆可直接存取網際網路，您可以在防火牆上套用驗證碼，以產生包含序號的授權檔案。
  - 如果防火牆離線，您必須使用 CSP 來輸入 CPU ID、UUID 和驗證碼，以產生包含序號的授權檔案。然後，您可以在防火牆上安裝授權。

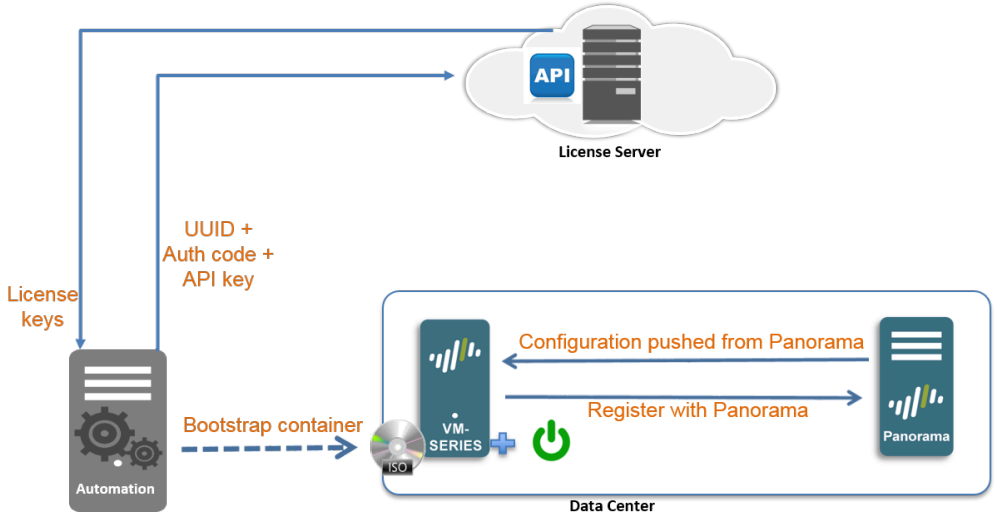
授權類型	序號	CPU ID
BYOL	15 位數，全部數值 範例：0071 **51** 345678909	<Hypervisor>:<ActualCPUID> 範例：**ESX**:12345678
PAYG	15 位數，英數字元 範例：**4** DE0YTAYOGMYYTN	<Hypervisor>:<Instance-ID>:<CloudProductCode>:<CloudRegion> 範例： **AWSMP**:1234567890abcdef0:6kxdw3bbmdeda 3o6i1ggqt4km:us-west1

©2023 Palo Alto Networks, Inc.

授權 API

您可以使用授權 API 來註冊驗證碼、擷取附加至驗證碼的授權、更新授權，以及停用 VM-Series 防火牆上的所有授權。此外，對於無法直接存取網際網路而無法到達 Palo Alto Networks 授權伺服器的防火牆，授權 API 可讓您授權防火牆。您可以手動管理授權，或使用自訂指令碼或協調運作服務來自動授權。

您還可以使用 Panorama 軟體防火牆授權外掛程式執行授權工作，包括離線授權。此外掛程式需要 *Panorama 10.0.0* 或更新版本，以及 *VM-Series* 外掛程式 *2.0.4* 或更新版本，您的受管 *VM-Series* 防火牆必須執行 *PAN-OS 9.1.0* 或更新版本，以及 *VM-Series* 外掛程式 *2.0.4* 或更新版本；*Azure* 專用 *VM-Series* 防火牆需要 *VM-Series* 外掛程式 *2.0.8*。



對於基於型號的授權，API 可讓您檢視驗證碼的詳細資訊，以追蹤附加至驗證碼或驗證碼搭售包的未使用授權數目，讓您能夠授權防火牆的多個實例。驗證碼搭售包包含 VM-Series 型號、訂閱及支援，採用單一、易於訂購的格式；您可以多次使用此搭售包，在部署 VM-Series 防火牆時進行授權。

為了使用 API，將會對各支援帳戶指派一個唯一的金鑰。各 API 呼叫是一個 POST 請求，請求必須包含 API 金鑰，以驗證授權伺服器的請求。驗證後，授權伺服器會以 JSON 格式 (content-type application/json) 傳送回應。

- 管理授權 API 金鑰
- 使用授權 API
- 授權 API 錯誤代碼
- 安裝授權 API 金鑰

管理授權 API 金鑰

若要取得使用授權 API 所需的 API 金鑰，您的帳戶在支援入口網站上必須具有進階使用者權限。相同的金鑰用來啟動和停用授權。

©2023 Palo Alto Networks, Inc.

API 金鑰到期日與支援帳戶中最新訂閱到期日的日期相同。如果您更新目前訂閱，而且需要重設 API 金鑰到期日，則可以重新產生金鑰（並將任何使用的現有金鑰都取代為這個新金鑰）或聯絡 Palo Alto Networks 支援，以取得擴展現有 API 金鑰條款的協助。

STEP 1 | 取得授權 API 金鑰。

1. 使用具有進階使用者權限的帳戶，登入 Palo Alto Networks 支援入口網站。
2. 選取 **Assets**（資產） > **API Key Management**（**API** 金鑰管理）。
3. 按一下 **Enable**（啟用）以檢視金鑰，並 複製來使用。產生金鑰後，金鑰就會一直啟用到您重新產生或停用它為止。

STEP 2 | 重新產生或撤銷 API 金鑰。

1. 您可以產生一個新的 API 金鑰，或撤銷使用金鑰。
   - 按一下 **Regenerate**（重新產生）以產生新的金鑰。如果您懷疑 API 金鑰可能已洩漏，您可以產生新的金鑰。重新產生會自動使舊的金鑰失效。
   - 如果您不打算再使用金鑰，請選取 **Disable**（停用）。停用 API 金鑰將撤銷該金鑰。

使用授權 API

用來存取授權 API 的基底 URI 是 https://api.paloaltonetworks.com/api/license；根據您要執行的工作而定（例如啟動授權，停用授權，或追蹤授權使用），URL 也不同。

API 要求必須使用 HTTP POST 方法，您必須將 API 金鑰加入 apikey HTTP 要求標頭中，並使用 `content-type application/x-www-form-urlencoded`，以 URL 編碼的表單資料來傳遞要求參數。

API 版本是選用，可包含下列值—0 或 1。如果有指定，則必須放在 `version` HTTP 要求標頭中。目前的 API 版本是 1；如果不指定版本，或指定版本 0，則要求會使用目前的 API 版本。

所有 API 以 JSON 格式呈現。

開始之前，取得授權 API 金鑰，並複製到本機磁碟機。這需要在執行下列任何工作之前完成：

- 啟動授權
- 停用授權
- 追蹤授權使用情況

啟動授權

標頭：apikey

參數：`uuid`、`cpuid`、`authCode`、`memory`、`serialNumber` 和 `vCPU`

URL：**`https://api.paloaltonetworks.com/api/license/activate`**

參數 uuid、cpuid、authCode 和 serialNumber 適用於所有 VM-Series 授權，不限 PAN-OS 版本。

選用參數 記憶體 和 `vCPU` 僅適用於彈性 vCPU（PAN-OS 10.0.4 和更新版本）。

©2023 Palo Alto Networks, Inc.

- 若是初次啟動授權，請在 API 要求中提供參數。例如：

```
curl -i -H
 "apikey:a103e3065360acc5e01666fb9335964fcfe668100666db6f3ff43d4544de0###"
 --data-urlencode cpuid=AWS:57060500FFFBE### --data-urlencode
 uuid=EC2278FF-F0CB-45E2-343B-E97984BAC### --data-urlencode
 authCode=D3521### --data-urlencode vcpu=4 --data-urlencode
 memory=8388608 https://api.paloaltonetworks.com/api/license/
activate
```

- 如果您在初次啟動授權期間未儲存授權金鑰，或發生網路連線問題，您可以從先前啟動的防火牆擷取授權。

  在 API 要求中，提供該防火牆的 `cpuid` 和 `uuid` ，或提供 `serialNumber`。

使用 **Curl** 啟動初始授權的請求：

```
curl -i -H "apikey:$APIKEY" --data-urlencode cpuid=51060400FFFBAB1F
 --data-urlencode uuid=564D0E5F-3F22-5FAD-DA58-47352C6229FF --data-
urlencode authCode=I7115398 https://api.paloaltonetworks.com/api/
license/activate
```

範例 **API** 回應：

```
[{"lfidField":"13365773","partidField":"PAN-SVC-PREM-
VM-300","featureFi--eld":"進階","功能說明欄位":"全天
候電話支援、進階更換硬體服務","keyField":"m4iZEL1t3n6Oa
+6ll1L7itDZTphYw48N1AMOZXutDgExC5f5pOA52+Qg1jmAxanB
\nKOyat4FJI4k2hWiBYz9cONuKoiaNOtAGhJvAuZmYgqAZejKueWrTzCuLrwxI/iEw
\nkRGR3cYG+j6o84RitR937m2iOk2v9o8RSfLVilgX28nqmcO8LcAnTqbrRWdFtwVk
\nluz47AUMXauuqwpMipouQYjk0ZL7fTHHslhyL7yFjCyxBoYXOt3JiqQ0OCDdBdDI
\n91RkVPylEwTKgSXm3xpzbmC2ciUR5b235gyqdyW8eQXKvaThuR8YyHr1Pdw/
lAjs\npyyIVFa6FufPacfB2RHApQ==\n","auth_codeField":"","錯
誤訊息欄位":null, "類型欄位":"SUP","註冊日期欄
位":"2016-06-03T08:18:41","開始日期欄位":"5/29/2016",
 "vm_capacityField":null,"uuidField":null,"cpuidField":null,"mac_baseField":nul
 "mac_countField":null,"drrField":null,"到期
欄位":"8/29/2016 12:00:00 AM","變更屬性":null},
{"lfidField":"13365774","partidField":"PAN-VM-300-TP", "功
能欄位":"威脅防護","功能說明欄位":"威脅防護","keyField":"NqaXoaFG
+9qj0t9Vu7FBMizDArj+pmFaQEd6I2OqfBfAibXrvuoFKeXX/K2yXtrl
\n2qJhNq3kwXBDxn181z3nrUOsQd/eW68dyp4jb1MfAwEM8mlnCyLhDRM3EE+umS4b
\ndZBRH5AQjPoaON7xZ46VMFovOR+asOUJXTptS/Eu1bLAI7PBp3+nm04dYTF9O50O
\ndey1jmGoiBZ9wBkesvukg3dVZ7gxppDvz14+wekYEJqPfM0NZyxsC5dnoxg9pciF
\ncFelhnTYlma1lXrCqjJcFdniHRwO0RE9CIKWe0g2HGo1uo2eq1XMxL9mE5t025im
\nblMnhL06smrCdtXmb4jjtg==\n","auth_codeField":"", "錯誤訊息欄
位":null,"類型欄位":"SUB","註冊日期欄位":"2016-06-03T08:18:41", "開
始日期欄位":"5/29/2016","vm_capacityField":null,"uuidField":null,
 "cpuidField":null,"mac_baseField":null,"mac_countField":null,"drrField":null,
 "到期欄位":"8/29/2016 12:00:00 AM","變更屬性":null} ...<truncated>
```


©2023 Palo Alto Networks, Inc.

回應中的 *feature_Field* 是指後面 *keyField* 中的金鑰類型。複製各金鑰至文字檔案，並使用 *.key* 副檔名儲存檔案。因為金鑰是 *json* 格式，所以不換行。如果解析器需要換行，請務必轉換為換行。確保相應地對各金鑰命名，並將其儲存至啟動套件的 */license* 資料夾。例如，包含具有金鑰類型的驗證碼，將其命名為 *I3306691_1pa-vm.key (for the capacity license key)*、*I3306691_1threat.key*（用於威脅防護授權金鑰）、*I3306691_1wildfire.key*（用於 *WildFire* 訂閱授權金鑰）。

使用 **Curl** 擷取先前啟動之授權的範本 **API** 要求：

```
curl -i -H "apikey:$APIKEY" --data-urlencode
 serialNumber=007200006142 https://api.paloaltonetworks.com/api/
license/activate
```

範例 **API** 回應：

```
[{"lfidField":"13365773","partidField":"PAN-SVC-
PREM-VM-300","featureField":"進階","功能說明欄位":"全天
候電話支援、進階更換硬體服務","keyField":"m4iZEL1t3n6Oa
+6ll1L7itDZTphYw48N1AMOZXutDgExC5f5pOA52+Qg1jmAxanB
\nKOyat4FJI4k2hWiBYz9cONuKoiaNOtAGhJvAuZmYgqAZejKueWrTzCuLrwxI/iEw
\nkRGR3cYG+j6o84RitR937m2iOk2v9o8RSfLVilgX28nqmcO8LcAnTqbrRWdFtwVk
\nluz47AUMXauuqwpMipouQYjk0ZL7fTHHslhyL7yFjCyxBoYXOt3JiqQ0OCDdBdDI
\n91RkVPylEwTKgSXm3xpzbmC2ciUR5b235gyqdyW8eQXKvaThuR8YyHr1Pdw/
lAjs\npyyIVFa6FufPacfB2RHApQ==\n","auth_codeField":"","錯
誤訊息欄位":null, "類型欄位":"SUP","註冊日期欄
位":"2016-06-03T08:18:41","開始日期欄位":"5/29/2016",
 "vm_capacityField":null,"uuidField":null,"cpuidField":null,"mac_baseField":nul
 "mac_countField":null,"drrField":null, "到期
欄位":"8/29/2016 12:00:00 AM","變更屬性":null},
{"lfidField":"13365774","partidField":"PAN-VM-300-TP", "功
能欄位":"威脅防護","功能說明欄位":"威脅防護","keyField":"NqaXoaFG
+9qj0t9Vu7FBMizDArj+pmFaQEd6I2OqfBfAibXrvuoFKeXX/K2yXtrl
\n2qJhNq3kwXBDxn181z3nrUOsQd/eW68dyp4jb1MfAwEM8mlnCyLhDRM3EE+umS4b
\ndZBRH5AQjPoaON7xZ46VMFovOR+asOUJXTptS/Eu1bLAI7PBp3+nm04dYTF9O50O
\ndey1jmGoiBZ9wBkesvukg3dVZ7gxppDvz14+wekYEJqPfM0NZyxsC5dnoxg9pciF
\ncFelhnTYlma1lXrCqjJcFdniHRwO0RE9CIKWe0g2HGo1uo2eq1XMxL9mE5t025im
\nblMnhL06smrCdtXmb4jjtg==\n","auth_codeField":"","錯誤訊息欄
位":null,"類型欄位":"SUB", "註冊日期欄位":"2016-06-03T08:18:41","開始日期欄
位":"5/29/2016","vm_capacityField" :null,"uuidField":null,"cpuidField":null,"mac
 "mac_countField":null,"drrField":null,"到期欄位":"8/29/2016 12:00:00
 AM","變更屬性":null} ...<truncated>
```

停用授權

URL: **https://api.paloaltonetworks.com/api/license/deactivate**

參數：encryptedToken

若要在無法直接存取網際網路的防火牆上停用授權，您必須在防火牆本機產生授權權杖檔案，然後在 API 要求中使用此授權權杖檔案。如需有關產生授權權杖檔案的詳細資訊，請參閱停用 VM 或停用授權（軟體 NGFW 積分）和使用 CLI 停用功能授權或訂閱。

標頭：apikey

©2023 Palo Alto Networks, Inc.

要求：https://api.paloaltonetworks.com/api/license/deactivate?encryptedtoken@<token>

使用 **Curl** 停用授權的範例 **API** 請求：

```
curl -i -H "apikey:$APIKEY" --data-urlencode
 encryptedtoken@dact_lic.05022016.100036.tok https://
api.paloaltonetworks.com/api/license/deactivate
```

範例 **API** 回應：

```
[{"序號欄位":"007200006150","功能名稱欄位":"","問題日期欄位":"", "成
功欄位":"Y","錯誤欄位":null,"為搭售包欄位":null,"變更屬性":null}, {"序
號欄位":"007200006150","功能名稱欄位":"","問題日期欄位":"", "成功欄
位":"Y","錯誤欄位":null,"為搭售包欄位":null,"變更屬性":null}, {"序
號欄位":"007200006150","功能名稱欄位":"","問題日期欄位":"", "成功欄
位":"Y","錯誤欄位":null,"為搭售包欄位":null,"變更屬性":null}, {"序
號欄位":"007200006150","功能名稱欄位":"","問題日期欄位":"", "成功欄
位":"Y","錯誤欄位":null,"為搭售包欄位":null,"變更屬性":null}, {"序
號欄位":"007200006150","功能名稱欄位":"","問題日期欄位":"", "成功欄
位":"Y","錯誤欄位":null,"為搭售包欄位":null,"變更屬性":null}, {"序號欄
位":"007200006150","功能名稱欄位":"","問題日期欄位":"", "成功欄位":"Y","錯誤
欄位":null,"為搭售包欄位":null, "變更屬性":null}]$
```

追蹤授權使用情況

URL: **https://api.paloaltonetworks.com/api/license/get**

參數：authCode

標頭：apikey

要求：https://api.paloaltonetworks.com/api/license/get?authCode=<authcode>

使用 **Curl** 追蹤授權使用情況的範例 **API** 要求：

```
curl -i -H "apikey:$APIKEY" --data-urlencode authcode=I9875031
 https://api.paloaltonetworks.com/api/license/get
```

範例 **API** 回應：

```
HTTP/1.1 200 OK 日期: 2016 年 5 月 5 日星期四 20:07:16 GMT 內容長度: 182
 {"AuthCode":"I9875031","UsedCount":4,"TotalVMCount":10,"UsedDeviceDetails":
[{"UUID":"420006BD-113D-081B-F500-2E7811BE80C
 9","CPUID":"D7060200FFFBAB1F","SerialNumber":"007200006142"}]}.....
```

授權 API 錯誤代碼

授權伺服器返回的 HTTP 錯誤代碼如下所示：

- 200 成功
- 400 錯誤
- 401 無效 API 金鑰API Key

©2023 Palo Alto Networks, Inc.

- 500 伺服器錯誤

©2023 Palo Alto Networks, Inc.

安裝授權 API 金鑰

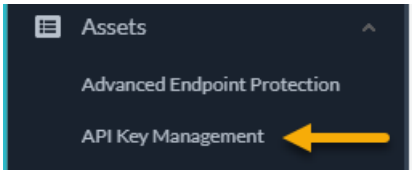
授權 API 金鑰可用來啟動、變更或停用授權。此程序適用於 VM-Series 防火牆或 Panorama 部署。

您必須具有超級使用者權限，才能從客戶支援入口網站擷取授權 API 金鑰，以及使用 CLI 在防火牆或 Panorama 上安裝金鑰。

在 Panorama 上，當您安裝授權 API 金鑰時，Panorama 會將 API 金鑰推送至受管理的裝置。如果受管理的裝置已安裝 API 金鑰，Panorama 會以新的 API 金鑰覆寫舊的金鑰。

STEP 1 | 從客戶支援入口網站擷取授權 API 金鑰。

1. 登入客戶支援入口網站。
2. 選取 **Assets**（資產） > **Licensing API**（授權 **API**）。
3. 複製 API 金鑰。



STEP 2 | 使用 CLI 安裝上一步所複製的 API 金鑰。將金鑰貼到要求中：

```
request license api-key set key <key>
```

STEP 3 | （選用）若要取代授權停用 API 金鑰，請使用下列 CLI 命令來刪除已安裝的 API 金鑰。

```
request license api-key delete
```

如果您刪除 API 密鑰，則必須先安裝另一個授權停用金鑰，才能停用授權。

©2023 Palo Alto Networks, Inc.

使用基於 Panorama 的軟體防火牆授權管理

Panorama 軟體防火牆授權外掛程式可讓您在 VM-Series 防火牆連線至 Panorama 時，自動授權防火牆。如果 VM-Series 防火牆位於部署的周邊，但未連線至 Palo Alto Networks 授權伺服器，則軟體防火牆授權外掛程式會利用 Panorama 來授權 VM-Series 防火牆，以簡化授權啟動程序。

此外，環境中有些 VM-Series 防火牆會使用自動調整規模和自動化來部署和刪除防火牆，以因應雲端的變動，軟體防火牆授權外掛程式會簡化這些 VM-Series 防火牆的授權啟動和停用。

不支援此外掛程式使用 *Pay-as-you-go*（即付即用；*PAYG*）。

請勿使用軟體防火牆授權外掛程式來授權 *VMware NSX* 專用 *VM-Series* 防火牆。*VMware NSX* 專用 *Panorama* 外掛程式會自動授權 *NSX* 和 *NSX-T* 中部署的 *VM-Series* 防火牆

。

此外，請勿使用此外掛程式授權部署在裝置群組中的防火牆，包括部署在 *NSX-T* 中的 *VM-Series* 防火牆實例。

若要安裝 Panorama 軟體防火牆授權外掛程式，您必須使用 Panorama 10.0.0 或更新版本，以及 VM-Series 外掛程式 2.0.4 或更新版本。VM-Series 防火牆必須執行 PAN-OS 9.1.0 或更新版本。

Azure 專用 *VM-Series* 防火牆需要 *VM-Series* 外掛程式 *2.0.8* 或更新版本。

如果您在安裝了多個外掛程式的 HA 配對中安裝了一個獨立的 Panorama 或兩個 Panorama 設備，則在未設定一或多個外掛程式的情況下，外掛程式可能不會收到更新的 IP-Tag 資訊。發生這種情況是因為 Panorama 不會將 IP-Tag 資訊轉送到未設定的外掛程式。此外，如果一或多個 Panorama 外掛程式未處於「已註冊」或「成功」狀態（每個外掛程式的正狀態不同），則可能會出現此問題。在繼續或執行下述命令之前，請確保您的外掛程式處於正狀態。

如果遇到此問題，有兩種權宜方案：

- 解除安裝未設定的外掛程式。建議您不要安裝未打算立即設定的外掛程式
- 您可以使用以下命令來變通處理此問題。對每個 Panorama 實例上的每個未設定外掛程式執行以下命令，以防止 Panorama 等待傳送更新。否則，防火牆可能會遺失一些 IP-Tag 資訊。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以透過執行以下命令來取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

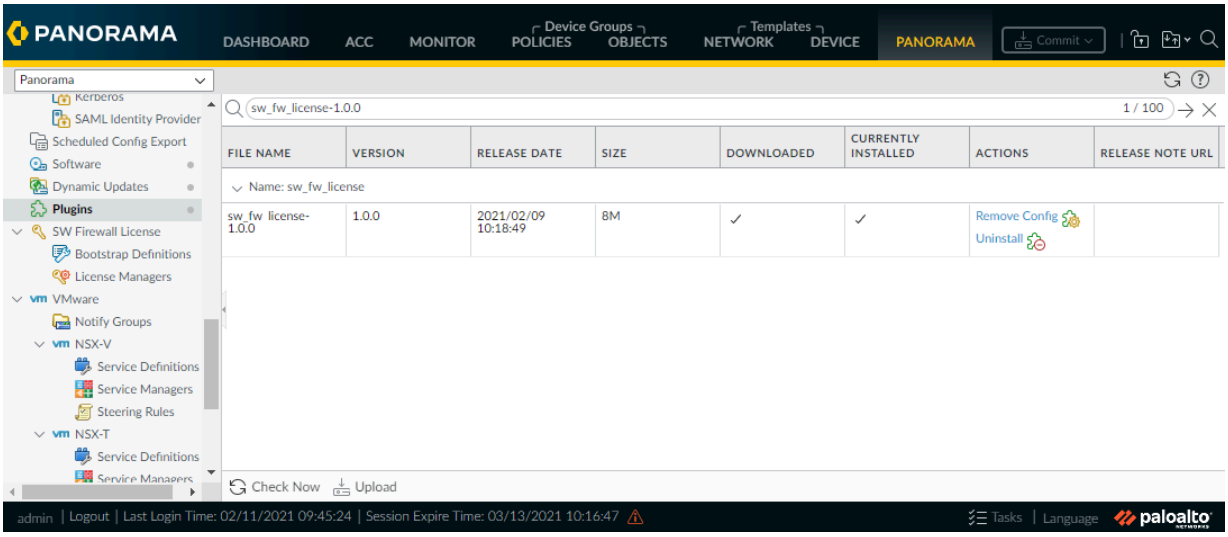
上述的命令在重新啟動後不會持續存在，並且必須在任何後續重新啟動時再次使用。對於 HA 配對中的 Panorama，必須在每個 Panorama 上執行命令。

©2023 Palo Alto Networks, Inc.

STEP 1 | 安裝 Panorama 專用軟體防火牆授權外掛程式。

1. 登入 Panorama 網頁介面。
2. 選取**Panorama** > 外掛程式 。
3. 按一下 **Check Now**（立即檢查），以取得可用的外掛程式清單。
4. 搜尋 sw_fw_license 來找出外掛程式。
5. 選取 **Download**（下載）並 **Install**（安裝）軟體授權外掛程式。

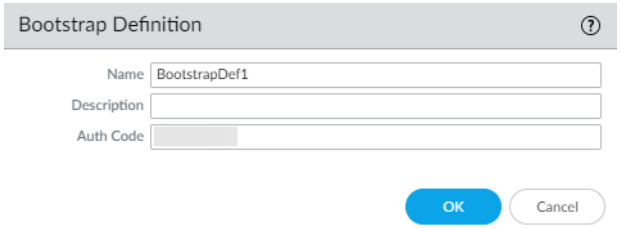
成功安裝之後，Panorama 會重新整理，**Panorama** 頁籤上會顯示軟體授權外掛程式。



©2023 Palo Alto Networks, Inc.

STEP 2 | 設定引導定義。

1. 選取 **Panorama** > **SW Firewall License**（軟體防火牆授權） > **Bootstrap Definitions**（引導定義）。
2. 按一下 **Add**（新增）。
3. 輸入描述性 **Name**（名稱）以識別引導定義。
4. （選用）輸入引導定義的 **Description**（說明）。
5. 輸入 **Auth Code**（驗證碼），供 Panorama 在 VM-Series 防火牆連線至 Panorama 時，用來授權防火牆。
6. 按一下 **OK**（確定）。



STEP 3 | 設定授權管理員。

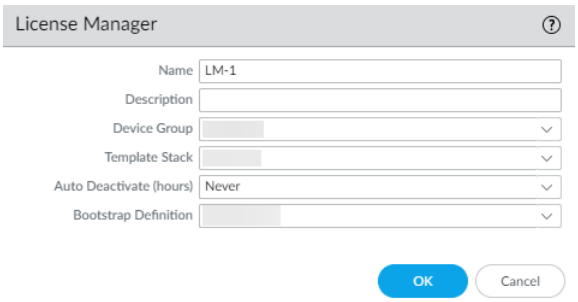
1. 選取 **Panorama** > **SW Firewall License**（軟體防火牆授權） > **License Managers**（授權管理員）。
2. 按一下 **Add**（新增）。
3. 輸入描述性 **Name**（名稱）以識別授權管理員。
4. （選用）輸入授權管理員的 **Description**（說明）。
5. 從下拉式清單中，選取 **Device Group**（裝置群組）。當使用授權管理員啟動的 VM-Series 防火牆連線至 Panorama 時，該防火牆會放在指定的裝置群組中。
6. 從下拉式清單中，選取 **Template Stack**（範本堆疊）。當使用授權管理員啟動的 VM-Series 防火牆連線至 Panorama 時，該防火牆會放在指定的範本堆疊中。
7. 在 **Auto Deactivate**（自動停用）欄位中，指定 Panorama 對已中斷連線的 VM-Series 防火牆停用授權之前，等待的時間量（以小時為單位）。當您選取 **Never**（永

©2023 Palo Alto Networks, Inc.

不）時，Panorama 不會停用已中斷連線的 VM-Series 防火牆。[Auto Deactivate（自動停用）] 預設為 Never（永不）。您可以將停用時間設定為 1 到 24（以小時為單位）。

在自動停用間隔內，外掛程式可能對已停止的 *VM-Series* 防火牆（由如預期停用的防火牆的相同授權管理員所管理）停用授權。

8. 從下拉式清單中，選取 **Bootstrap Definition**（引導定義）。針對與授權管理員相關聯的 VM-Series 防火牆，選取的引導定義會指定驗證碼，供 Panorama 用於授權這些防火牆。
9. 按一下 **OK**（確定）。
10. **Commit**（提交）您的變更。

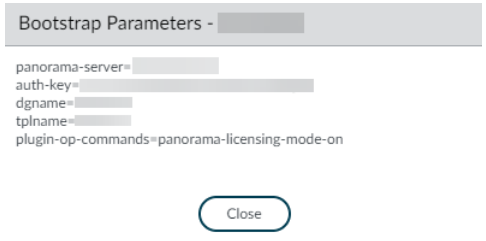


STEP 4 | （選用）建立 `init-cfg.txt` 檔案，以引導 VM-Series 防火牆。設定授權管理員後，當您部署 VM-Series 防火牆時，您可以複製並貼上 Panorama 產生的引導參數。根據您的部署，顯示的參數可能是下圖所示的參數子集。例如，如果 Panorama 設備部署在公共雲端，則引導參數不包含 Panorama 的公共 IP 位址。在此情況下，您必須在 `init-cfg.txt` 檔案中手動輸入公共 IP 位址。Panorama 一律產生 auth-key 和 **`plugin-op-commands=panorama-licensing-mode-on`**，以用於 `init-cfg.txt` 中。

此處顯示的驗證金鑰由 Panorama 產生，用於驗證 VM-Series 防火牆到 Panorama 的連線。此外，這個驗證金鑰會代替您可能在 Panorama 上產生並新增至 init-cfg.txt 檔案的 VM 驗證金鑰。

如果您在 *init-cfg.txt* 檔案中使用此處顯示的驗證金鑰，請不要使用手動產生的 *VM* 驗證金鑰。

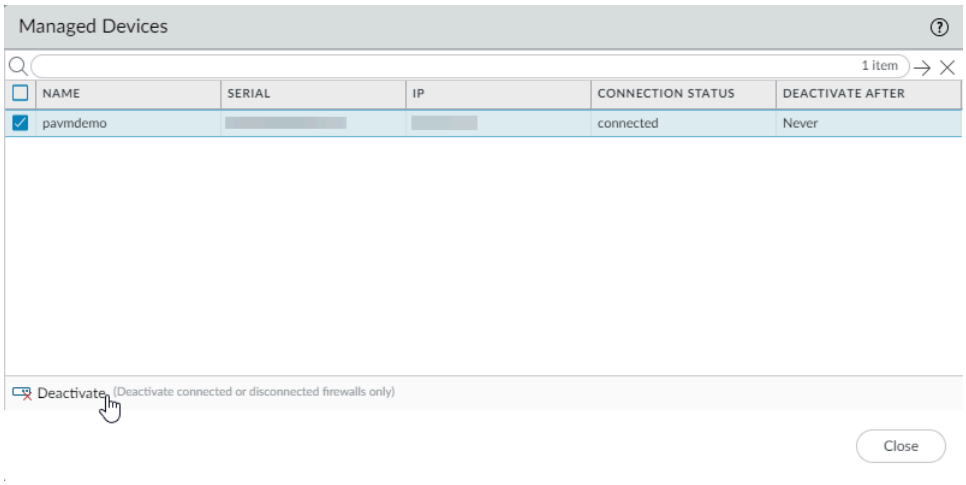
1. 選取 **Panorama** > **SW Firewall License**（軟體防火牆授權） > **License Managers**（授權管理員）。
2. 在給定授權管理員的 [Action（動作）] 欄，按一下 **Show Bootstrap Parameters**（顯示引導參數）。
3. 複製顯示的資訊並貼到文字編輯器中，以建立用於引導的 `init-cfg.txt` 檔案。
4. 完成後按一下 **Close**（關閉）。



 ©2023 Palo Alto Networks, Inc.

STEP 5 | （選用）檢視並停用受管理的 VM-Series 防火牆。從 **Show Devices**（顯示裝置）對話方塊中，您可以檢視給定授權管理員相關聯的裝置。您可以檢視名稱、序號、管理 IP 位址、連線狀態，以及 Panorama 為了停用已中斷連線的防火牆而等待的時間量。此外，您可以對受管理的 VM-Series 防火牆，手動停用授權。

1. 選取 **Panorama** > **SW Firewall License**（軟體防火牆授權） > **License Managers**（授權管理員）。
2. 在給定授權管理員的 [Action（動作）] 欄，按一下 **Show Devices**（顯示裝置）。
3. 若要手動停用已連線或中斷連線（但尚未停用）的受管理 VM-Series 防火牆，請選取一個或多個列出的 VM-Series 防火牆，然後按一下 **Deactivate**（停用）。



STEP 6 | （選用）驗證 Panorama 是否完成必要的 API 呼叫來授權已連線的防火牆。

1. 登入 Panorama 命令列介面。
2. 執行下列命令。

```
show plugins sw_fw_license panorama-api-requests
```


©2023 Palo Alto Networks, Inc.

軟體 NGFW 積分

軟體 NGFW 積分可用於支付軟體 NGFW（VM-Series 和 CN-Series）、Cloud-Delivered Security Services（雲端交付的安全性服務；CDSS），或是能夠或無法存取網際網路的網路（例如氣隙網路）中的 Panorama 設備。

您需要建立部署設定檔，以根據 PAN-OS 版本、每個防火牆的 vCPU 數量、部署設定檔支援的防火牆總數、Panorama 管理或日誌收集，以及安全性服務，設定一個或多個防火牆。以部署設定檔建立的所有 VM 都共用相同的驗證碼。

- 固定 vCPU—與所有 PAN-OS 版本相容。根據 VM-Series 型號 和安全性服務搭售包。變更型號或服務選項需要新的授權。
- 彈性 vCPU—選取彈性的 vCPU 數目和一組彈性的安全性服務。您可以修改部署設定檔以增加或減少 vCPU 數目、新增剛推出的新服務，或移除服務。部署設定檔的 vCP 數目上限為 64 個。

軟體 NGFW 積分是基於期限。期限可定義為 1 至 5 年的任何時間長度。分配的和未分配的積分在同意的期限結束時到期。您可以為積分池購買額外積分，但到期日必須與目標池相同。使用軟體 NGFW 積分估算器來計算並取得部署設定檔的積分。

如果您可經由網際網路連線至授權伺服器，但停止使用防火牆、安全性服務或 Panorama 部署，則分配給該資源的積分會退還給積分池，並重新分配給新資源。

如果您沒有網際網路連線，而無法連線至 Palo Alto Networks 更新伺服器（例如，在氣隙網路中），則可以從使用者介面或從 Panorama，在本機管理 VM-Series 防火牆。然後，管理員必須登入客戶支援入口網站來歸還授權權杖，才能重複使用資金。

使用以下支援的超管理器表格和隨後的資料平面上的 **vCPU** 總數表格，以確保為您選擇的 vCPU 數目分配必要的硬體資源。

層	記憶體
第 1 層	4.5 GB、5 GB、5 GB、5.5 GB、6 GB、6.5 GB、7 GB、8 GB
第 2 層	9 GB、10 GB、12 GB、14 GB、16 GB、18 GB
第 3 層	20 GB、24、GB、28 GB、32 GB、36 GB、40 GB、44 GB、48 GB、52 GB、56 GB、60 GB、64 GB
第 4 層	128 GB

記憶體設定檔	支援的 **Hypervisor**	最小硬碟
第 1 層 （4.5 GB、5 GB、5.5 GB、6 GB 記憶體）	ESXi、Hyper-V、KVM	• 使用 4.5 GB 記憶體：32GB（開機時 60GB） • 60GB

©2023 Palo Alto Networks, Inc.

記憶體設定檔	支援的 **Hypervisor**	最小硬碟
第 1 層	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、Cisco ENCS、NSX-T	60GB
第 2 層	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、Cisco ENCS、NSX-T	60GB
第 3 層	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、NSX-T	60GB
第 4 層	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、NSX-T	60GB

對於上面列出的所有記憶體設定檔，vCPU 最少 2 個。

第 *1* 層至少需要 *32GB* 的硬碟空間。但是，由於 *VM-Series* 基本映像通用於所有 *vCPU* 組合，因此在您授權具有 *4.5GB* 記憶體的 *VM-Series* 防火牆之前，必須分配 *60GB* 的硬碟空間。

為了達到最佳效能，單一 *CPU* 插槽上應該有所有必要的核心。

根據預設，除非您指派四個或更少的 vCPU，否則管理平面和資料平面 vCPU 會以一比三的比例指派。此外，最大資料平面 vCPU 會繫結至已配置的記憶體，如下表所述。例如，如果您將 16 個 vCPU 指派給 VM-Series 防火牆，則會將 4 個 vCPU 配置給管理平面，12 個 vCPU 配置給資料平面。如果將 20 個 vCPU 和 20GB 記憶體連接到 VM-Series 防火牆，則會將 12 個 vCPU 配置給資料平面，其餘的指派給管理平面。

或者，您也可以使用 VM-Series 防火牆 CLI 來自訂資料平面核心。這可讓您指定要指派給 VM-Series 防火牆上資料平面的 vCPU 數量。

第 **1** 層	**4.5 GB**	**5 GB**	**5.5 GB**	**6 GB**	**6.5 GB**	**7 GB**	**8 GB**
預設資料平面 vCPU	1	1	1	1	2	2	2

第 **2** 層	**9 GB**	**10 GB**	**12 GB**	**14 GB**	**16 GB**	**18 GB**	**20 GB**
預設資料平面 vCPU	4	4	4	4	12	12	12

©2023 Palo Alto Networks, Inc.

第 3 層	20 GB	24 GB	28 GB	32 GB	36 GB	40 GB	44 GB	48 GB	52 GB	56 GB	64 GB
預設資料平面 vCPU	12	12	12	12	12	12	12	12	12	24	47

第 4 層	121 - 128 GB
預設資料平面 vCPU	47

繼續執行軟體 NGFW 任務：

- 基於層和記憶體的最大限制
- 啟動積分
- 建立部署設定檔
- 管理部署設定檔
- 註冊 VM-Series 防火牆（軟體 NGFW 積分）
- 佈建 Panorama
- 將 Panorama 移轉至軟體 NGFW 授權
- 轉移積分
- 更新您的軟體 NGFW 積分授權
- 停用授權（軟體 NGFW 積分）
- 設定已授權的 vCPU 數量
- 自訂資料平面核心
- 將防火牆移轉到彈性 VM-Series 授權

基於層和記憶體的最大限制

下表指出在根據所配置的記憶體或層設定的防火牆上，單一 VM-Series 防火牆部署可建立、儲存、管理或互動的特定物件或資源的數目上限。這些限制適用於使用由軟體 NGFW 積分提供資金的授權 VM-Series 防火牆。

對於記憶體調整，記憶體增量分為四個層，表示 VM-Series 防火牆的設定容量。無論分配給 VM-Series 防火牆實例的記憶體量如何，該記憶體量所在的層都會確定非工作階段值的限制，例如安全性規則、位址物件、安全性設定檔等。

記憶體設定檔和 vCPU 總數決定自動指派給管理平面和資料平面的核心數目。此外，您還可以選擇自訂資料平面核心的分佈。

如果您使用軟體 NGFW 積分授權，則可以選擇記憶體設定檔來支援您對下列一個或多個資源的需求：

· 位址指派	· 介面	· 政策	· SSL 解密

©2023 Palo Alto Networks, Inc.

- App-ID
- EDL
- GlobalProtect 用戶端 VPN
- GlobalProtect 無用戶端 VPN
- high availability （高可用性）
- IPSec VPN
- L2 轉送
- 多點傳送
- NAT
- 物件（位址和服務）
- QoS
- 路由
- 安全性設定檔
- 安全性區域
- 工作階段
- URL 篩選
- 使用者-ID
- 虛擬路由器
- 虛擬系統
- Virtual Wire

工作階段

第 1 層	4.5 GB	5 GB	5.5 GB	6 GB	6.5 GB	7 GB	8 GB
工作階段數目上限 (IPv4 或 IPv6)	25,000	40,000	50,000	100,000	200,000	300,000	500,000
最大預設資料平面 vCPU 數	1	1	1	1	2	2	2

第 2 層	9 GB	10 GB	12 GB	14 GB	16 GB	18 GB	20 GB
工作階段數目上限 (IPv4 或 IPv6)	600,000	800,000	1,000,000	1,200,000	1,800,000	2,000,000	2,800,000
最大預設資料平面 vCPU 數	4	4	4	4	12	12	12

第 3 層	24 GB	28 GB	32 GB	36 GB	40 GB	44 GB
工作階段數目上限 (IPv4 或 IPv6)	3,600,000	4,400,000	5,200,000	6,000,000	6,800,000	6,800,000
最大預設資料平面 vCPU 數	12	12	12	12	12	12

第 3 層（續）	48 GB	52 GB	56 GB	64 GB
工作階段數目上限 (IPv4 或 IPv6)	7,600,000	8,400,000	9,200,000	10,000,000

©2023 Palo Alto Networks, Inc.

第 3 層（續）	48 GB	52 GB	56 GB	64 GB
最大預設資料平面 vCPU 數	12	12	24	47

第 4 層	121 - 128 GB
工作階段數目上限 (IPv4 或 IPv6)	14,000,000
最大預設資料平面 vCPU 數	47

政策

功能	第 1 層	第 2 層	第 3 層	第 4 層
安全性規則	1,500	10,000	20,000	65,000
安全性規則排程	256	256	256	256
NAT 規則	3,000	8,000	15,000	16,000
解密規則	1,000	1,000	2,000	5,000
應用程式取代規則	1,000	1,000	2,000	4,000
通道內容檢查規則	100	500	2,000	8,500
SD-WAN 規則	100	300	300	1,000
基於政策的轉送規則	100	500	2,000	2,000
被控制的入口網站規則	1,000	1,000	2,000	8,000
DoS 防護規則	1,000	1,000	1,000	2,000

安全性區域

功能	第 1 層	第 2 層	第 3 層	第 4 層
安全性地區數目上限	40	200	200	17,000

©2023 Palo Alto Networks, Inc.

物件（位址和服務）

功能	第 1 層	第 2 層	第 3 層	第 4 層
位址物件	10,000	20,000	40,000	160,000
位址群組	1,000	2,500	4,000	80,000
每個位址群組的成員	2,500	2,500	2,500	2,500
服務物件	2,000	2,000	5,000	12,000
服務群組	500	250	500	6,000
每個服務群組的成員	500	500	500	2,500
FQDN 位址物件	2,000	2,000	2,000	6,144
DAG IP 位址數目上限*（整個系統的容量）	2,500	300,000	300,500	500,000
每個 IP 位址的標籤	32	32	32	64

* 利用 AppMix 交易啟用 App-ID 和 User-ID 功能來測量的防火牆輸送量。

安全性設定檔

功能	第 1 層	第 2 層	第 3 層	第 4 層
安全性設定檔	375	750	750	750

App-ID

功能	第 1 層	第 2 層	第 3 層	第 4 層
自訂 App-ID 簽名	6,000	6,000	6,000	6,000
共用的自訂 App-ID	512	512	512	512
自訂 App-ID（虛擬系統專用）	6,416	6,416	6,416	6,416

©2023 Palo Alto Networks, Inc.

使用者-ID

功能	第 1 層	第 2 層	第 3 層	第 4 層
IP-使用者對應（管理平面）	524,288	524,288	524,288	524,288
IP-使用者對應（資料平面）	64,000	512,000	512,000	512,000
政策中使用的作用中唯一群組（LDAP 群組、XML API 群組和動態使用者群組的彙總）。*	1,000	10,000	10,000	10,000
User-ID 代理程式數目	100	100	100	100
User-ID 的受監控伺服器	100	100	100	100
終端機伺服器代理程式	400	2,000	2,500	2,500
每個使用者的標籤*（PAN-OS 9.1 和更新版本）	32	32	32	32

*利用 AppMix 交易啟用 App-ID 和 User-ID 功能來測量的防火牆輸送量。

SSL 解密

功能	第 1 層	第 2 層	第 3 層	第 4 層
SSL 輸入憑證數目上限	1,000	1,000	1,000	4,000
SSL 憑證快取（正向 Proxy）	128	4,000	8,000	32,000
並行解密工作階段數目上限	6,400	50,000	100,000	2,000,000
SSL 連接埠鏡像	是	是	是	是
SSL 解密代理	否。	否。	是	是
支援 HSM	是	是	是	是

©2023 Palo Alto Networks, Inc.

URL 篩選

功能	第 1 層	第 2 層	第 3 層	第 4 層
允許清單、封鎖清單和自訂類別的項目總數	25,000	25,000	100,000	100,000
自訂類別數目上限	2,849	2,849	2,849	2,849
自訂類別數目上限（虛擬系統專用）	500	500	500	500
用於 URL 篩選的資料平面快取大小	90,000	90,000	250,000	250,000
管理平面動態快取大小	100,000	100,000	600,000	900,000

EDL

功能	第 1 層	第 2 層	第 3 層	第 4 層
自訂清單數目上限	30	30	30	30
每個系統的 IP 數目上限	50,000	50,000	50,000	150,000
每個系統的 DNS 網域數目上限	50,000	2,000,000	2,000,00	4,000,000
每個系統的 URL 數目上限	50,000	100,000	100,000	250,000
最短檢查間隔（分鐘）	5	5	5	5

介面

功能	第 1 層	第 2 層	第 3 層	第 4 層
管理 - 頻外	NA	NA	NA	NA
管理 - 10/100/1000 高可用性	NA	NA	NA	NA
管理 - 40Gbps 高可用性	NA	NA	NA	NA
管理 - 10Gbps 高可用性	NA	NA	NA	NA
流量 - 10/100/1000	NA	NA	NA	NA
流量 - 100/1000/10000	NA	NA	NA	NA

©2023 Palo Alto Networks, Inc.

功能	第 1 層	第 2 層	第 3 層	第 4 層
流量 - 1Gbps SFP	NA	NA	NA	NA
流量 - 10Gbps SFP+	NA	NA	NA	NA
流量 - 40/100Gbps QSFP+/QSFP28	NA	NA	NA	NA
每個裝置的 802.1q 標籤	4,094	4,094	4,094	4,094
每個實體介面的 802.1q 標籤	4,094	4,094	4,094	4,094
介面數目上限（邏輯和實體）	2,048	4,096	4,096	4,096
彙總介面數目上限	NA	NA	NA	NA
SD-WAN 虛擬介面數目上限	300	1,000	1,000	1,000

虛擬路由器

功能	第 1 層	第 2 層	第 3 層	第 4 層
虛擬路由器	3	20	125	225

Virtual Wire

功能	第 1 層	第 2 層	第 3 層	第 4 層
虛擬介接	12	12	12	12

虛擬系統

功能	第 1 層	第 2 層	第 3 層	第 4 層
基本虛擬系統	1	1	1	1
虛擬系統數目上限 虛擬系統容量超過基本虛擬系統容量時需要額外的授權	NA	NA	NA	NA

©2023 Palo Alto Networks, Inc.

路由

功能	第 1 層	第 2 層	第 3 層	第 4 層
IPv4 轉送表大小*（跨虛擬路由器共用的項目）	5,000	32,000	100,000	待新增
IPv6 轉送表大小*（跨虛擬路由器共用的項目）	5,000	32,000	100,000	待新增
系統總計轉送表大小	5,000	32,000	100,000	待新增
32,000	50	50	50	待新增
路由對等數目上限（取決於通訊協定）	500	1,000	1,000	待新增
靜態項目 - DNS Proxy	1,024	1,024	1,024	待新增
Bidirectional Forwarding Detection（雙向轉送偵測；BFD）工作階段	128	1,024	1,024	待新增

*利用 AppMix 交易啟用 App-ID 和 User-ID 功能來測量的防火牆輸送量。

L2 轉送

功能	第 1 層	第 2 層	第 3 層	第 4 層
每個裝置的 ARP 表格大小	2,500	32,000	128,000	132,000
IPv6 芳鄰表格大小	2,500	32,000	128,000	132,000
每個裝置的 MAC 表格大小	2,500	32,000	128,000	132,000
每個廣播網域的 ARP 項目數上限	2,500	32,000	128,000	132,000
每個廣播網域的 MAC 項目數上限	2,500	32,000	128,000	132,000

NAT

功能	第 1 層	第 2 層	第 3 層	第 4 層
NAT 規則容量總計	3,000	8,000	8,000	待新增
NAT 規則數目上限（靜態）*	3,000	8,000	8,000	待新增

©2023 Palo Alto Networks, Inc.

功能	第 1 層	第 2 層	第 3 層	第 4 層
（將靜態 NAT 規則設定為滿載容量就不可使用其他 NAT 規則類型。）				
NAT 規則數目上限 (DIP)* （將 DIP NAT 規則設定為滿載容量就不可使用其他 NAT 規則類型。）	2,000	8,000	8,000	待新增
NAT 規則數目上限 (DIPP)	400	2,000	2,000	待新增
轉譯的 IP 數目上限 (DIP)	128,000	160,000	160,000	待新增
轉譯的 IP 數目上限 (DIPP)* （DIPP 轉譯的 IP 容量與 DIPP 集區過度訂閱值成正比。此處顯示的容量是根據 1x 的過度訂閱值。）	400	2,000	2,000	待新增
預設 DIPP 集區過度訂閱* （來源 IP 和來源連接埠跨並行工作階段重複使用）	2	8	8	待新增

*利用 AppMix 交易啟用 App-ID 和 User-ID 功能來測量的防火牆輸送量。

位址指派

功能	第 1 層	第 2 層	第 3 層	第 4 層
DHCP 伺服器	3	20	125	待新增
DHCP 轉送* （容量上限代表 DHCP 伺服器和 DHCP 轉送總計）	500	500	500	待新增
指派的位址數目上限	64,000	64,000	64,000	待新增

*利用 AppMix 交易啟用 App-ID 和 User-ID 功能來測量的防火牆輸送量。

high availability （高可用性）

功能	第 1 層	第 2 層	第 3 層	第 4 層
支援的裝置	2	2	2	2

©2023 Palo Alto Networks, Inc.

功能	第 1 層	第 2 層	第 3 層	第 4 層
虛擬位址數目上限	128	32	128	待新增

QoS

功能	第 1 層	第 2 層	第 3 層	第 4 層
QoS 政策數目	500	2,000	4,000	待新增
支援 QoS 的實體介面	6	12	12	12
每個實體介面的純文字節點	31	63	63	63
依政策進行 DSCP 標記	是	是	是	是
支援的子介面	NA	NA	NA	NA

IPSec VPN

功能	第 1 層	第 2 層	第 3 層	第 4 層
IKE 對等數目上限	1,000	1,000	2,000	待新增
站台對站台（含 Proxy ID）	1,000	4,000	8,000	待新增
SD-WAN IPSec 通道	1,000	1,000	2,000	待新增

GlobalProtect 用戶端 VPN

功能	第 1 層	第 2 層	第 3 層	第 4 層
通道數目上限（含 XAUTH 的 SSL、IPSec 和 IKE）	500	6,000	12,000	待新增

GlobalProtect 無用戶端 VPN

功能	第 1 層	第 2 層	第 3 層	第 4 層
SSL 通道數目上限	100	1,200	2,500	25,000

©2023 Palo Alto Networks, Inc.

多點傳送

功能	第 1 層	第 2 層	第 3 層	第 4 層
複寫（輸出介面）	100	100	100	待新增
路由	2,000	4,000	4,000	待新增

啟動積分

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（請參閱VM-Series 防火牆授權中的「預設積分池」）。

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，依號碼或名稱篩選帳戶清單。

如果您購買多個積分池（請參閱軟體 NGFW 積分），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）。

您會看到存款成功的訊息。

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。

繼續建立部署設定檔。

©2023 Palo Alto Networks, Inc.

建立部署設定檔

若要建立部署設定檔，您必須有客戶支援入口網站帳戶 (CSP)，而且可存取已啟動的積分池。

開始之前，請預估有多少防火牆將使用部署設定檔中的設定。您不必一次部署所有防火牆。

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） > **Create Deployment Profile**（建立部署設定檔）。

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 VM-Series 防火牆類型。
2. 選取 PAN-OS 版本。
   - **Fixed Models**（固定型號） (VM-Series 型號)
   - 彈性 **vCPU**（**PAN-OS 10.0.4** 和更新版本）
3. 按一下 **Next**（下一步）。

STEP 2 | VM-Series 設定檔。

1. **Profile Name**（設定檔名稱）。

   命名設定檔。
2. **Number of Firewalls**（防火牆數目）。

   輸入此設定檔部署的防火牆數目（假設您有足夠的積分）。您不必一次部署所有防火牆。
3. 防火牆型號：

   選擇 VM-Series 型號。

   Planned vCPU/Firewall（規劃的 **vCPU/** 防火牆） （PAN-OS 10.0.4 或更新版本）。

   輸入每個防火牆的 vCPU 數目。

   安全使用案例：選擇一個使用案例。
4. **Customize Subscriptions**（自訂訂閱）。

   選擇使用案例後，您可以新增或移除安全服務。
5. （選用）**Use Credits to Enable VM Panorama**（使用積分來啟用 **VM Panorama**）。

   選擇 Panorama 使用案例 — 管理和/或日誌收集器。

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 | 建立部署設定檔。

您可能需要等待數秒鐘，設定檔才會出現在**Current Deployment Profiles**（目前的部署設定檔）頁籤清單中。在分配完成之前，**Credits Consumed/Allocated**（已耗用/分配的積分）欄會

©2023 Palo Alto Networks, Inc.

顯示 0 和 **Update Pending**（更新擱置中）。請捲動至底端，然後移至最後一頁，以尋找您的設定檔。

稍後若要檢視您的部署設定檔，請按一下父積分池的 **Details**（詳細資訊）按鈕，然後選取 **Current Deployment Profiles**（目前的部署設定檔）。

- 請注意最右邊的設定檔驗證碼；軟體 NGFW 積分驗證碼以 D 開頭。
- 在分配完成之前，**Credits Consumed/Allocated**（已耗用/分配的積分）欄會顯示 0 和 **Update Pending**（更新擱置中）。
- **Audit Trail**（稽核線索）頁籤會顯示 **Credit Transactions**（積分交易）和您管理的 **Deployment Profiles**（部署設定檔）。您也可以在此頁籤中依時間搜尋設定檔。

  使用搜尋來尋找您的設定檔，並展開橫列以檢視您在建立設定檔時指定的設定。

管理部署設定檔

建立部署設定檔後，您可以編輯、複製或刪除設定檔。

- 編輯部署設定檔
- 複製部署設定檔
- 刪除部署設定檔

編輯部署設定檔

STEP 1 | 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分），然後在您用來建立設定檔的積分池上按一下 **Details**（詳細資訊）按鈕。

STEP 2 | 選取 **Current Deployment Profiles**（目前的部署設定檔）頁籤。

STEP 3 | 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 4 | 進行變更，然後選取 **Update Deployment Profile**（更新部署設定檔）。

STEP 5 | 選取 **Audit Trail**（稽核線索）頁籤，然後使用搜尋來尋找您的設定檔。

使用搜尋來尋找您的設定檔，並展開橫列以檢視您在建立設定檔時指定的設定。

複製部署設定檔

STEP 1 | 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分），然後在您用來建立設定檔的積分池上按一下 **Details**（詳細資訊）按鈕。

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）。

©2023 Palo Alto Networks, Inc.

STEP 4 | 選取 **Audit Trail**（稽核線索）頁籤，然後使用搜尋來尋找您的設定檔。

展開橫列以檢視您複製的設定。這是新的設定，具有不同的設定檔名稱和驗證碼。

刪除部署設定檔

刪除部署設定檔之前，您必須在任何使用部署設定檔的防火牆上停用授權（軟體 NGFW 積分），然後停用 VM。

STEP 1 | 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分），然後在您用來建立設定檔的積分池上按一下 **Details**（詳細資訊）按鈕。

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）。

註冊 VM-Series 防火牆（軟體 NGFW 積分）

註冊需要存取 Palo Alto Networks 客戶支援入口網站 (CSP)，並擁有支援帳戶。如有必要，請建立一個帳戶。

在啟動期間，管理員會啟動積分池並存入積分。當任何人建立部署設定檔時，都會建立一個身份驗證代碼。完成以下程序之一以啟動註冊。

- 裝置可以存取 CSP
- 設備無法存取 CSP

©2023 Palo Alto Networks, Inc.

如果防火牆能夠連接到 **CSP**，請使用以下步驟：

1. 使用您的帳戶認證登入 CSP。
2. 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分）。

   找到您的積分池並檢視詳細資訊。
3. 檢視目前部署設定檔 並選擇（或建立）設定檔。

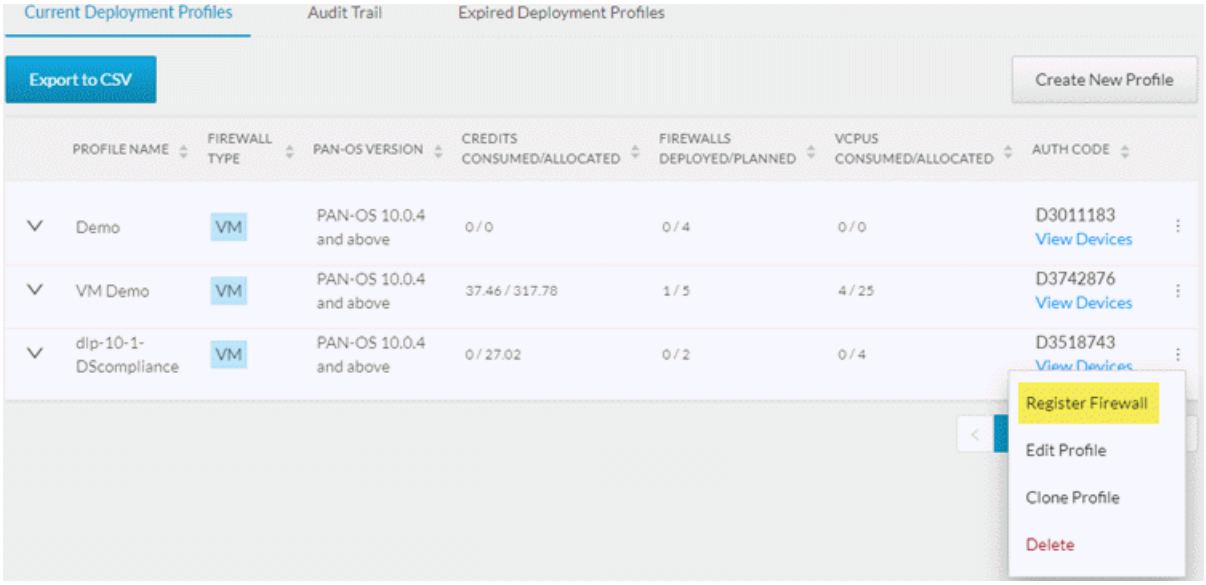
   您將使用此設定檔中的身份驗證代碼來授權您使用它建立的任何防火牆。防火牆彈性授權的驗證碼以字母 D 開頭。
4. 登入 VM-Series 防火牆網頁介面。
5. 驗證 Palo Alto Networks 更新伺服器設定。
   1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務）。
   2. 確認 **Update Server**（更新伺服器）設定為 `updates.paloaltonetworks.com`。
   3. 確認已選取 **Verify Update Server Identity**（驗證更新伺服器識別）。
6. 選取 **Device**（裝置） > **Licenses**（授權）。
   1. 選取 **Activate feature using authorization code**（使用授權碼啟動功能）連結。
   2. 輸入部署設定檔中的 VM-Series 授權碼。
   3. 按一下 **OK**（確定），以確認授權升級。防火牆會聯絡 Palo Alto Networks 更新伺服器，並根據 VM-Series 型號取用防火牆所需的權杖。
7. 確認 **Dashboard**（儀表板）顯示有效的序號，且 **PA-VM** 授權顯示在 **Device**（裝置） > **Licenses**（授權）頁籤中。
8. 驗證您的防火牆已在 CSP 上註冊：
   - 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分）
   - 驗證碼欄，**View Devices**（檢視裝置）並找到您部署的序號。
   - 在積分池中，耗用的積分、部署的防火牆和耗用的 vCPU 應該會增加，以反映您的部署。

©2023 Palo Alto Networks, Inc.

如果防火牆無法連接到 **CSP**，請使用以下步驟：

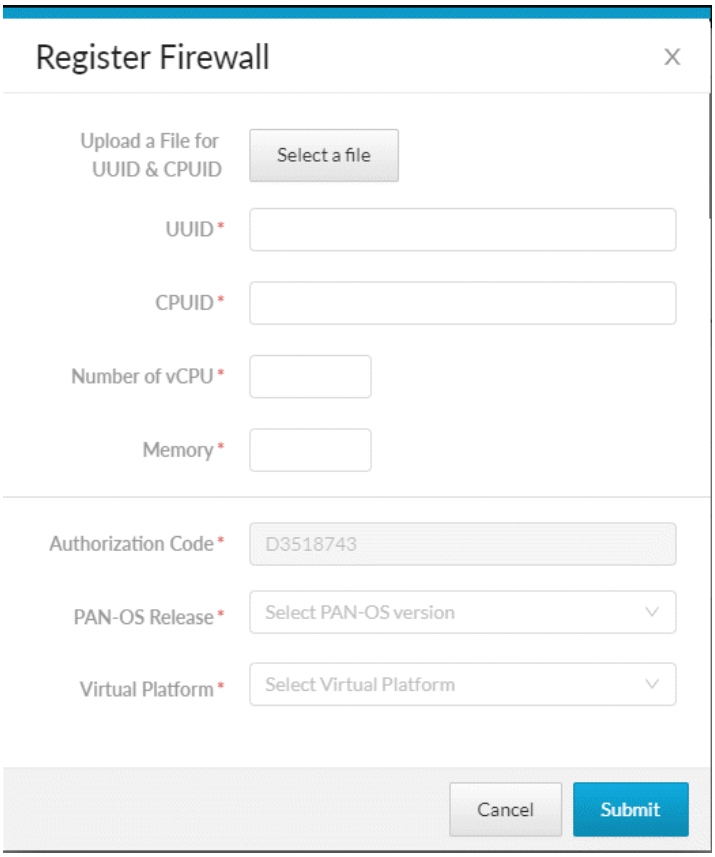
此工作流程會將您的防火牆新增到支援資料庫。由於防火牆無法連線至授權伺服器，因此您必須手動將授權從 CSP 傳給防火牆。

1. 使用您的帳戶認證登入 CSP。
2. 選取新的設定檔，選取垂直省略符號（[More Options（更多選項）]），然後選取 **Register Firewall**（註冊防火牆）。



這會開啟裝置註冊表單。輸入防火牆的資訊，然後按一下 **Submit**（提交）：

©2023 Palo Alto Networks, Inc.



這會將防火牆與設定檔及其驗證碼建立關聯，並指派序號。

3. 按一下 **View Devices**（檢視裝置），在 **Software NGFW Devices**（軟體 **NGFW** 裝置）中查看相關聯的防火牆。

   在 **License**（授權）欄中，將每個授權金鑰下載到某個位置，以安全將檔案傳輸到防火牆。

4. 登入防火牆，選取 **Device**（裝置） > **Licenses**（授權）。

   必須透過網頁介面安裝授權金鑰。防火牆不支援透過 *SCP* 或 *FTP* 安裝授權金鑰。

   - 按一下 **Manually Upload License**（手動上傳授權）。
   - 確認 [Dashboard（儀表板）] 顯示有效的序號，且 **Device**（裝置） > **Licenses**（授權）頁籤中顯示 **PA-VM** 授權。

佈建 Panorama

只有當您建立部署設定檔時選取 Panorama，才能看到此選項。如有必要，您可以編輯設定檔。

STEP 1 | 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分），然後在您用來建立設定檔的積分池上按一下 **Details**（詳細資訊）按鈕。

©2023 Palo Alto Networks, Inc.

STEP 2 | 在最右邊選取垂直省略符號（[More Options（更多選項）]），然後選取 **Provision Panorama**（佈建 **Panorama**）和 **Provision**（佈建）。您會看到目前部署設定檔已佈建的防火牆清單。

這會建立 Panorama，指派序號和型號 PAN-PRA-1000-CP，並將 Panorama 註冊為資產。您剛佈建的 Panorama 是最後一個列出的 Panorama。請注意，驗證碼以 F 開頭（與部署設定檔不同），但到期日與設定檔的積分池相同。

複製序號。

STEP 3 | 從部署設定檔，**View Devices**（檢視裝置），然後在 [Software NGFW Devices（軟體 NGFW 裝置）] 頁面上選取 **Panorama**。這會顯示所有 SW NGFW Panorama。

使用您複製的序號，作為搜尋序號的 **Search By**（搜尋依據）。

您也可以選取 **Assets**（資產） > **Software NGFW Devices**（軟體 **NGFW** 裝置），並使用您複製的序號，作為搜尋序號的 **Search By**（搜尋依據）。

將 Panorama 移轉至軟體 NGFW 授權

您可以將 VM-ELA 或永久虛擬 Panorama 授權移轉到軟體新世代防火牆（軟體 NGFW）授權。

- 移轉具有 CSP 存取權的 Panorama
- 移轉可存取 CSP 的 Panorama HA 配對
- 將無法存取 CSP 的獨立 Panorama 移轉到彈性授權
- 將無法存取 CSP 的 HA 配對移轉到彈性授權

移轉具有 CSP 存取權的 Panorama

完成以下程序，以將您的 VM-ELA 或永久虛擬 Panorama 授權移轉到軟體 NGFW 授權。此移轉可讓您將現有的 Panorama 裝置移轉到軟體 NGFW 授權，而不會發生中斷，同時還能保留現有的序號。由於您的序號不會變更，因此您的日誌和現有原則將保留。

STEP 1 | 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分），然後在您用來建立設定檔的積分池上按一下 **Details**（詳細資訊）連結。

STEP 2 | 在最右邊選取垂直省略符號（[More Options（更多選項）]），選取 **Provision Panorama**（佈建 **Panorama**）然後按一下 **Migrate Existing**（移轉現有內容）。

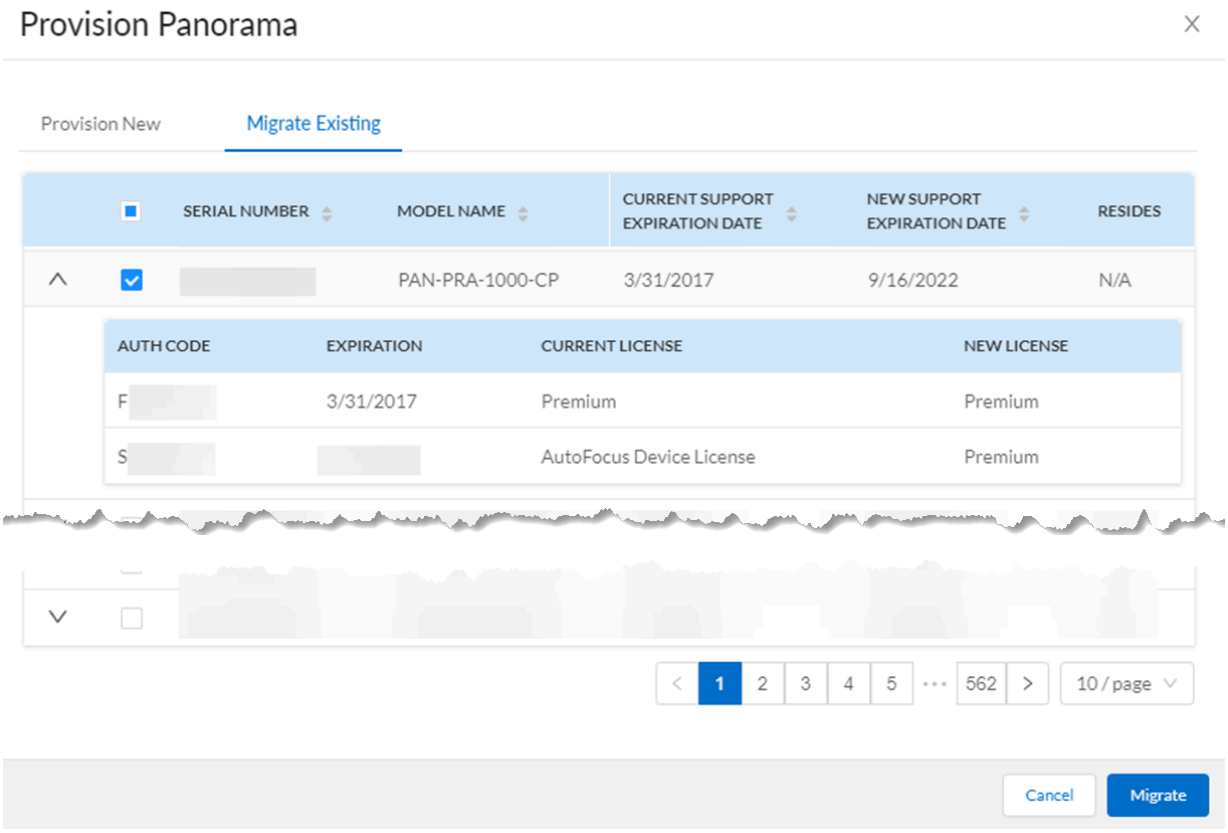
CSP 顯示與您帳戶關聯的所有虛擬 Panorama 裝置。

STEP 3 | 對要移轉的每個虛擬 Panorama 勾選核取方塊。

©2023 Palo Alto Networks, Inc.

STEP 4 | 按一下 **Migrate**（移轉）。

驗證 **Current Support Expiration Date**（目前支援到期日期）已更新。此外，您可以展開每一列，以查看套用至所選 Panorama 的各個授權。



移轉可存取 CSP 的 Panorama HA 配對

完成以下程序，以將具有 VM-ELA 或永久授權的 HA 配對移轉到軟體 NGFW 授權。此移轉可讓您將現有的 Panorama 裝置移轉到軟體 NGFW 授權，而不會發生中斷，同時還能保留現有的序號。由於您的序號不會變更，因此您的日誌和現有原則將保留。

STEP 1 | 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分），然後在您用來建立設定檔的積分池上按一下 **Details**（詳細資訊）連結。

STEP 2 | 在最右邊選取垂直省略符號（[More Options（更多選項）]），選取 **Provision Panorama**（佈建 **Panorama**）然後按一下 **Migrate Existing**（移轉現有內容）。

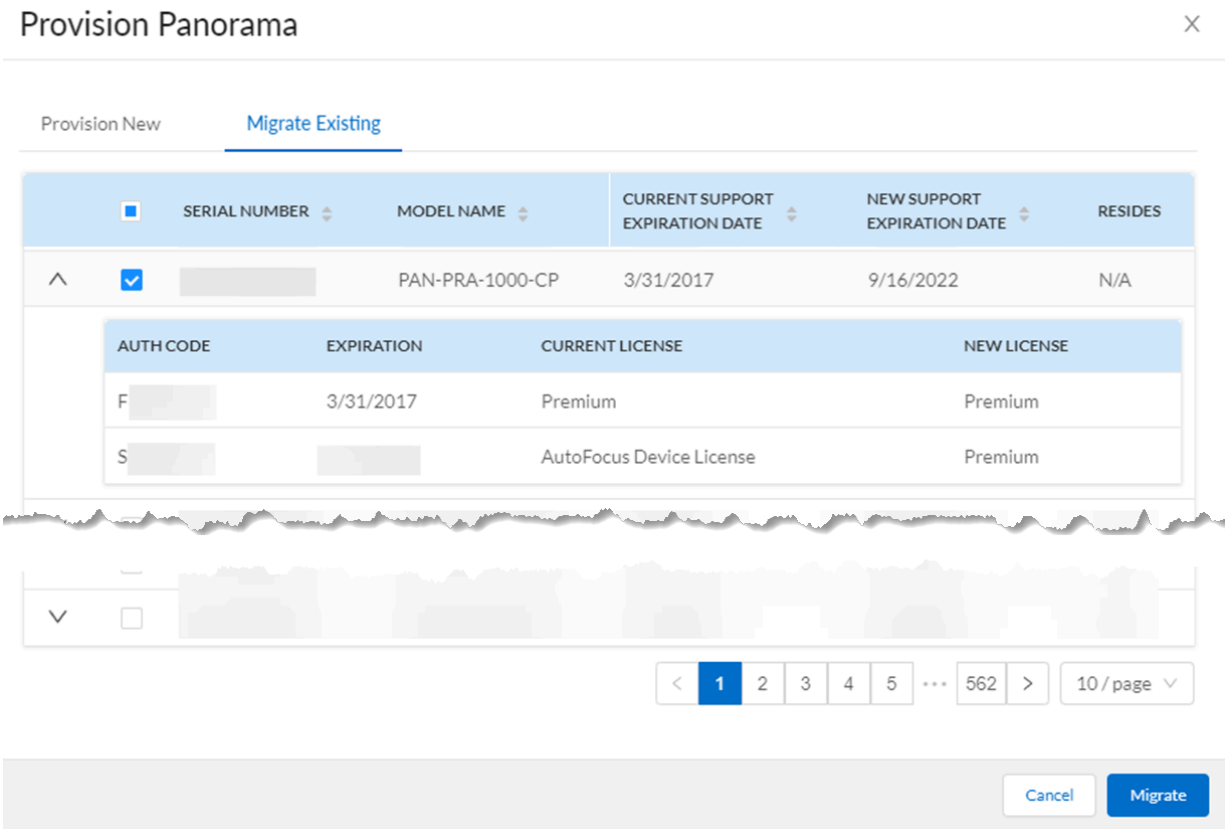
CSP 顯示與您帳戶關聯的所有虛擬 Panorama 裝置。

STEP 3 | 對要移轉的每個虛擬 Panorama 勾選方塊。

©2023 Palo Alto Networks, Inc.

STEP 4 | 選取 **Migrate**（移轉）。

驗證 **Current Support Expiration Date**（目前支援到期日期）已更新。此外，您可以展開每一列，以查看套用至所選 Panorama 的各個授權。



將無法存取 CSP 的獨立 Panorama 移轉到彈性授權

完成以下程序，以將您的 VM-ELA 或永久虛擬 Panorama 授權移轉到軟體 NGFW 授權，即使您的 Panorama 無法存取 CSP。沒有 CSP 的移轉需要變更序號，但它可讓您的 Panorama 裝置移轉到軟體 NGFW 授權並保留您現有的原則。

Panorama 支援的最低版本是 *8.1*。如果必須升級 *PAN-OS*，請在開始移轉程序之前進行。如果要管理使用彈性 *vCPU* 和進階服務的防火牆，*PAN-OS* 版本必須是 *10.0.4* 或更新版本。

STEP 1 | 在您的 Panorama 上，視需要進行升級，並記下序號和目前支援的到期日期。

STEP 2 | 在 CSP 中，選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分），然後在積分池上按一下 **Details**（詳細資訊）連結。選擇一個部署設定檔，或新建一個。

©2023 Palo Alto Networks, Inc.

STEP 3 | 在最右邊選取垂直省略符號（[More Options（更多選項）]），選取 **Provision Panorama**（佈建 **Panorama**）然後選取 **Migrate Existing**（移轉現有內容）。

CSP 顯示與您帳戶關聯的所有虛擬 Panorama 裝置。

STEP 4 | 勾選每個要移轉的虛擬 Panorama，然後選取 **Migrate**（移轉）。

STEP 5 | 在 Panorama 上，將序號替換為您在 CSP 中佈建的 Panorama 序號。等待一分鐘，然後重新整理頁面。

STEP 6 | 在 CSP 中，選取您佈建的 Panorama 並下載所有授權（支援授權、管理授權和作為日誌管理器的 Panorama，如果您的部署設定檔包含。

安全地將授權傳遞給您的 Panorama。

STEP 7 | 上傳所有軟體 NGFW 授權。

STEP 8 | 驗證 **Current Support Expiration Date**（目前支援到期日期）已更新。此外，您可以展開每一列，以查看套用至所選 Panorama 的支援授權和/或記錄授權。

將無法存取 CSP 的 HA 配對移轉到彈性授權

當您的 HA 配對無法與 CSP 通訊時，請使用此程序。此過程會起始容錯移轉。

STEP 1 | 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分），然後在積分池上按一下 **Details**（詳細資訊）按鈕。

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

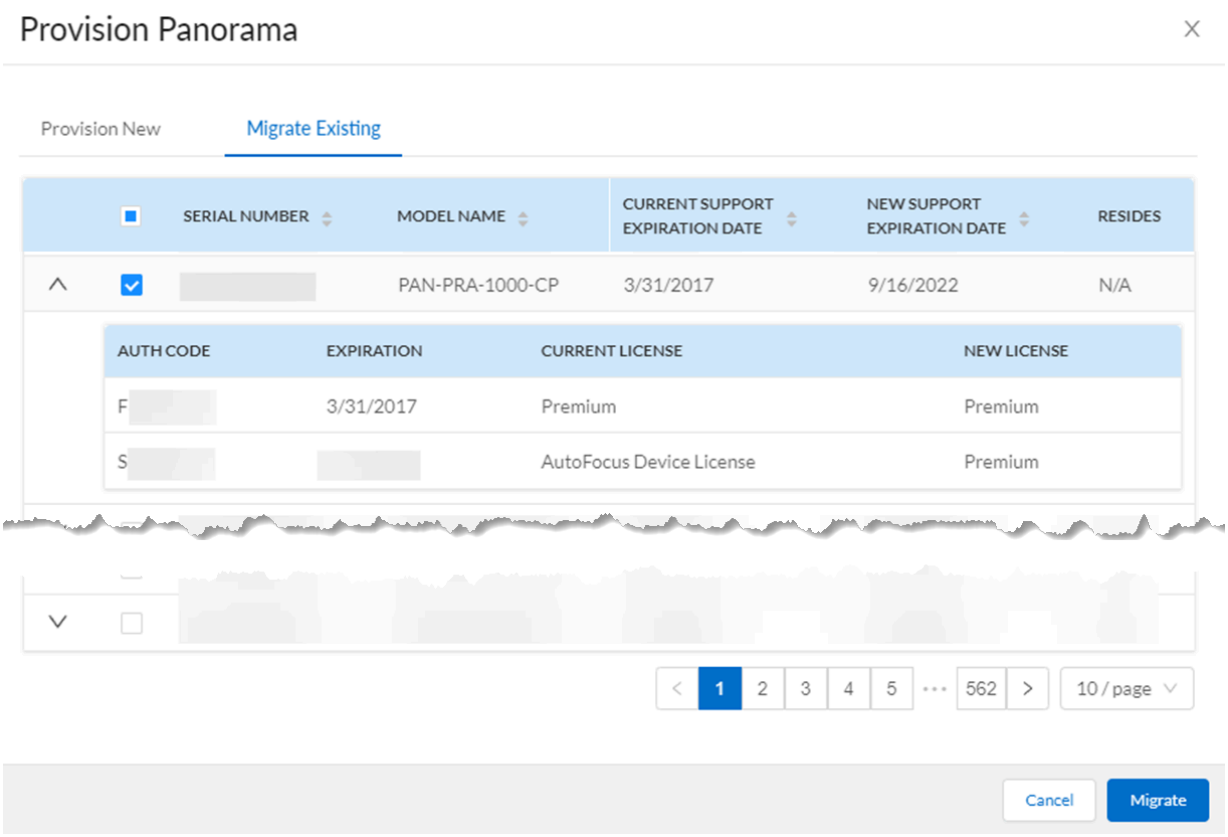
CSP 顯示與目前支援帳戶關聯的所有虛擬 Panorama 裝置。

STEP 3 | 選取 **Provision New**（佈建新內容），勾選要移轉的每個虛擬 Panorama 方塊，然後選取 **Migrate**（移轉）。

移轉的 Panoramas 顯示為軟體 NGFW 裝置。

©2023 Palo Alto Networks, Inc.

STEP 4 | 驗證 **Current Support Expiration Date**（目前支援到期日期）已更新。此外，您可以展開每一行，以查看套用至所選 Panorama 的各個授權。



轉移積分

從 Customer Support Portal（客戶支援入口網站；CSP），將積分轉移到同一帳戶中的積分池，或轉移到您可存取的另一個帳戶中的積分池。

- 不同的 CSP 帳戶
- 此帳戶中的不同積分池

不同的 **CSP** 帳戶

STEP 1 | 登入您的 CSP 帳戶。

©2023 Palo Alto Networks, Inc.

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. **Credit Pool ID#**（積分池 **ID** 號碼）—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）。

您可能需要稍待片刻或重新整理畫面，才能看到變更。

STEP 6 | 若要檢視積分池的積分交易，請選取 **Details**（詳細資訊），然後選取 **Audit Trail**（稽核線索）。

此帳戶中的不同積分池

STEP 1 | 登入 CSP 帳戶。

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

- 識別目的地積分池，並記下積分池 ID。
- 如果沒有您所指定類型的目的地積分池，系統會提示您建立新的積分池。

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 Pool in this Account**（此帳戶中的不同積分池）。

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. **Credit Pool ID#**（積分池 **ID** 號碼）—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）。

您可能需要稍待片刻或重新整理畫面，才能看到變更。

STEP 6 | 若要檢視積分池的積分交易，請選取 **Details**（詳細資訊），然後選取 **Audit Trail**（稽核線索）。

©2023 Palo Alto Networks, Inc.

更新您的軟體 NGFW 積分授權

當部署設定檔過期時，它會從 [Current Deployment Profiles（目前的部署設定檔）] 頁籤移動到 [Renew Profiles（更新設定檔）] 頁籤。在 [Renew Profiles（更新設定檔）] 頁籤中，您可以從 Palo Alto Networks 客戶支援入口網站快速更新部署設定檔，而不會中斷 VM-Series 防火牆的操作。在部署設定檔過期並移至 [Renew Profiles（更新設定檔）] 頁籤後，您有 30 天的時間來更新設定檔。任何未在 30 天內更新的部署設定檔都會過期並移至 [Expired Deployment Profiles（過期的部署設定檔）] 頁籤。如需詳細資訊，請參閱 當授權到期時會怎麼樣？。

更新後，您可能會注意到之前的部署設定檔之間發生了一些變化。*Prisma NGFW Credits* 和 *Virtual NGFW Credits* 積分池現在都稱為「軟體 *NGFW* 積分」積分池。此外，由於產品定價模型的變更，您積分池中的積分數量可能會在更新後發生變化。

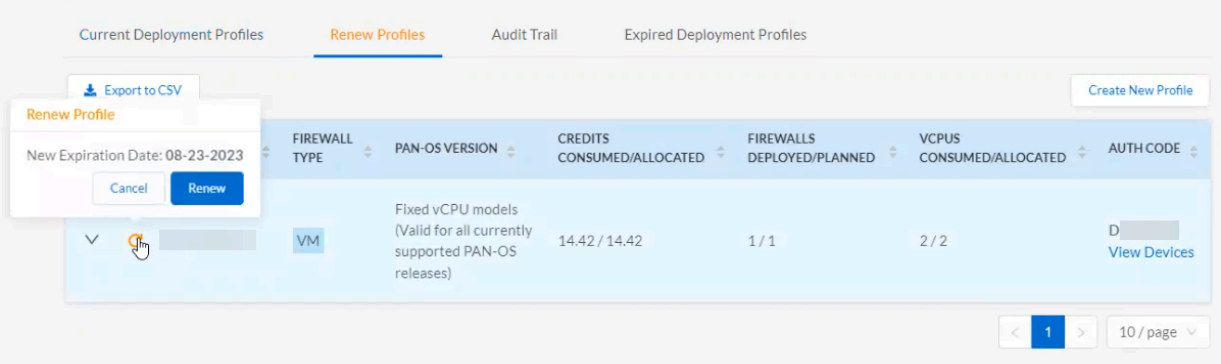
STEP 1 | 登入 Palo Alto Networks 客戶支援入口網站。

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

STEP 3 | 找到要更新的部署設定檔，然後按一下 **Details**（詳細資訊）。

STEP 4 | 選取 **Renew Profiles**（更新設定檔）。

STEP 5 | 按一下更新圖示，然後按一下 **Renew**（更新）進行確認。

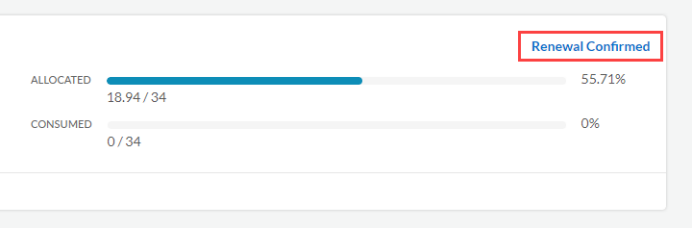


©2023 Palo Alto Networks, Inc.

STEP 6 | 驗證您的部署設定檔是否已成功更新。

1. 按一下 **Current Deployment Profiles**（目前的部署設定檔）。
2. 確認顯示已更新的部署設定檔。

   此外，您可以返回 Software NGFW 儀表板以檢視您的積分池。成功更新後，積分池顯示 **Renewal Confirmed**（更新已確認）。此訊息將一直保留到您更新的軟體 NGFW 積分到期日期結束。



停用授權（軟體 NGFW 積分）

刪除防火牆（或託管防火牆的 VM）之前，您必須先從 CSP 停用任何授權，否則授權積分無法歸還給積分池。

當您可經由網際網路存取授權伺服器時，在 CSP 上停用防火牆會自動移除授權，剩餘積分會歸還給部署設定檔。停用授權之後，您必須刪除防火牆，否則會繼續消耗積分。

如果您無法存取網際網路，則必須從防火牆匯出授權權杖。然後，在 CSP 中，開始停用並上傳權杖（或貼上權杖文字），以完成停用。

- 網際網路存取
- 無法存取網際網路
- 無法存取網際網路 - Panorama 管理

直接存取網際網路。

1. 選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分），然後在您用來建立部署設定檔的積分池上按一下 **Details**（詳細資訊）按鈕。
2. 找出您的部署設定檔，在最右邊選取垂直省略符號（[More Options（更多選項）]），然後選取 **Deactivate Firewall**（停用防火牆）。
3. 勾選您要停用的防火牆，然後選取停用防火牆。

©2023 Palo Alto Networks, Inc.

無法存取網際網路。

1. 登入防火牆網頁介面，然後選取 **Device**（裝置） > **Licenses**（授權）。
2. 在 [License Management（授權管理）] 區段中，選取 **Deactivate VM**（停用 **VM**）。

   驗證將在防火牆上停用的授權/權利清單。
3. 選取手動完成以開始停用。

   按一下匯出授權權杖連結，將權杖檔案儲存至用戶端。權杖檔名如下所示：`20150128_1307_dact_lic.01282015.130737.tok`

   此時，已在防火牆上停用授權，但積分尚未歸還給積分池。
4. 使用權杖檔案向授權伺服器註冊變更：

   1. 登入 Palo Alto Networks 客戶支援網站。
   2. 選取 **Assets**（資產） > **VM-Series Auth-Codes**（**VM-Series** 驗證碼） > **Deactivate License(s)**（停用授權）。

   在 [Deactivate Licenses（停用授權）] 表單中，貼上權杖文字，或將權杖複製到可存取網際網路的電腦，然後將權杖檔案上傳至 CSP，以完成授權移除。
5. 刪除 VM

無法存取網際網路 — Panorama 管理

1. 登入 Panorama 網頁介面，然後選取 **Panorama** > **Device Deployment**（裝置部署） > **Licenses**（授權）。
2. 選取 **Deactivate VMs**（停用 **VM**），然後選取您要停用的 VM-Series 防火牆。
3. 選取手動完成以匯出權杖檔案。
4. 按一下匯出授權權杖連結，以儲存權杖檔案。權杖檔名如下所示：20150128_1307_dact_lic.01282015.130737.tok

   如果匯出成功，則會顯示完成訊息，防火牆將自動重新啟動。
5. 使用權杖檔案向授權伺服器註冊變更。

   1. 登入 Palo Alto Networks 客戶支援網站。
   2. 選取 **Assets**（資產） > **VM-Series Auth-Codes**（**VM-Series** 驗證碼） > **Deactivate License(s)**（停用授權）。

   在 [Deactivate Licenses（停用授權）] 表單中，貼上權杖文字，或將權杖複製到可存取網際網路的電腦，然後將權杖檔案上傳至 CSP，以完成授權移除。
6. （選用）在 Panorama 上，將已停用的 VM-Series 防火牆視為受管理的裝置移除。

   您可以建立另一個裝置群組，在其中指派已停用的防火牆，而不刪除已停用的防火牆。

   1. 選取 **Panorama** > **Managed Devices**（受管理的設備）。
   2. 選取您停用的防火牆，然後按一下 **Delete**（刪除）。

©2023 Palo Alto Networks, Inc.

設定已授權的 vCPU 數量

您可以指定在使用軟體 NGFW 積分時獲得授權的 vCPU 數量，而不是授權所選運算執行個體上所有可用的 vCPU。如此一來，您就可以使用更大的運算執行個體，而不會耗用超過必要的軟體 NGFW 積分。

此功能需要 *VM-Series* 外掛程式 *2.1.4* 或更新版本。

您可以使用啟動程序外掛程式 op 命令或 VM-Series 防火牆 CLI，指定要授權的 vCPU 數目。

- 若要在啟動載入 VM-Series 防火牆時設定核心數，請將下列命令新增至 init-cfg.txt 檔案。

  plugin-op-commands=set-cores:<number-of-cores>

  例如：

  plugin-op-commands=set-cores:4
- 若要設定已部署的 VM-Series 防火牆上的核心數，請使用下列 CLI 命令。

  request plugins vm_series set-cores cores <number-of-cores>

  例如：

  request plugins vm_series set-cores cores 16

  您必須重新啟動 VM-Series 防火牆，此變更才會生效。

自訂資料平面核心

如軟體 NGFW 積分中所述，當使用軟體 NGFW 積分部署防火牆時，由記憶體設定檔和 vCPU 總數決定自動指派給管理平面和資料平面的核心數目。在大多數情況下，預設組態運作良好。

自訂資料平面核心是選用功能，可讓您以兩種方式自訂資料平面核心數目：

- 在初始部署期間，使用 **init-cfg.txt** 檔案啟動程序參數 **plugin-op-commands=set-dp-cores:<#-cores>**。請參閱 init-cfg.txt 檔案元件。
- 從部署的防火牆，使用 VM-Series CLI 命令 **request plugins vm_series dp-cores <#-cores>**。此程序概述如下。

您通常會增加資料平面核心數目（減少管理平面核心數目），以改善效能。資料平面核心自訂不需要變更部署設定檔或額外積分，因為 vCPU 總數維持不變。

- 在執行 PAN-OS 10.1 或更新版本，且由 10.0.4 和更新版本的軟體 NGFW 積分池授權的防火牆上，支援資料平面核心自訂。
- 以下幾項不支援資料平面核心自訂：
  - NSX-T
  - 智慧流量卸載

在 VM-Series 防火牆上，依照下列步驟自訂資料平面核心。

©2023 Palo Alto Networks, Inc.

STEP 1 | 登入 VM-Series 防火牆並檢視核心數目。

```
admin@PA-VM(active)>show plugins vm_series dp-cores
Device current DP cores:13 (Total cores:18)
```

STEP 2 | 變更資料平面核心的數目。

請注意，您至少必須有一個管理平面核心，核心太少會影響效能。

在這個例子中，我們將資料平面增加到 14 個。

```
admin@PA-VM(active)>request plugins vm_series dp-cores 14
Device current DP cores:14 (Total cores:18)
```

STEP 3 | 重新啟動 VM-Series 防火牆。

選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後按一下 **Reboot Device**（重新啟動裝置）。

STEP 4 | 使用 **show plugins vm_series dp-cores** 確認 DP 核心數目已變更。

將防火牆移轉到彈性 VM-Series 授權

您可以將 VM-Series 防火牆永久或 ELA 授權，移轉至彈性 VM-Series 防火牆授權（使用軟體 NGFW 積分提供資金）。您可以同時從 Panorama 切換個別防火牆或多個防火牆上的授權。

使用此程序可從評估授權移轉到非評估積分池授權驗證碼，而不會發生中斷。

完成下列其中一個程序來移轉授權。

- 可存取 CSP 的獨立防火牆
- 獨立防火牆，無法存取 CSP
- 移轉具有 CSP 存取權的 Panorama 管理防火牆
- Panorama 管理防火牆，無法存取 CSP
- Panorama 管理的防火牆和 Panorama 都無權存取 CSP
- 驗證移轉

可存取 CSP 的獨立防火牆

此過程不會中斷通過防火牆的流量。

STEP 1 | 登入 VM-Series 防火牆網頁介面。

STEP 2 | 驗證 Palo Alto Networks 更新伺服器設定。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務）。
2. 確認 **Update Server**（更新伺服器）設定為 `updates.paloaltonetworks.com`。
3. 確認已選取 **Verify Update Server Identity**（驗證更新伺服器識別）。

©2023 Palo Alto Networks, Inc.

STEP 3 | 登入 CSP 並建立部署設定檔。如果您要移轉的授權是用於具有 ELA 或永久授權的 VM-Series 防火牆，則當您為彈性授權建立 SW NGFW 部署設定檔時，您必須選擇 **Fixed Models**（固定型號），並使用相同的 VM-Series 型號和 vCPU 數量。

您將使用此設定檔中的驗證碼。防火牆彈性授權的驗證碼以字母 D 開頭，如下所示。

STEP 4 | 選取 **Device**（設備） > **Licenses**（授權）。

如果目前的 VM-Series 型號和您要移轉到的 VM-Series 型號不同，請選取 **Upgrade VM Capacity**（升級 **VM** 容量）連結。

如果移轉前後的 VM-Series 型號相同，請選取 **Activate feature using authorization code**（使用授權碼啟動功能）連結。

STEP 5 | 輸入新的部署設定檔中的 VM-Series 授權碼。

STEP 6 | 按一下 **OK**（確定），以確認授權升級。防火牆會聯絡 Palo Alto Networks 更新伺服器，並根據 VM-Series 型號取用防火牆所需的權杖。

STEP 7 | （選用）驗證移轉。

STEP 8 | 針對部署中的每個 VM-Series 防火牆，重複此程序。

獨立防火牆，無法存取 CSP

在無法存取 CSP 的情況下移轉防火牆上的授權。

STEP 1 | 如有必要，請在 VM-Series 防火牆上安裝授權 API 金鑰。

STEP 2 | 透過 CLI 使用手動模式停用固定型號授權。

STEP 3 | 使用手動程序從防火牆停用 VM，然後登入 CSP，並使用權杖檔案停用 VM。

STEP 4 | 在 CSP 中，建立部署設定檔使用與先前固定型號授權相同的 VM-Series 型號、vCPU 數量和安全性訂閱。您將使用此設定檔中的驗證碼。

STEP 5 | 選取新的設定檔，按一下垂直省略符號，然後選取 **Register Firewall**（註冊防火牆）。

1. 輸入 VM 和防火牆資訊，然後選取 **Submit**（提交）。這會將防火牆與設定檔及其驗證碼建立關聯，並指派序號。
2. 按一下 **View Devices**（檢視裝置），在 **Software NGFW Devices**（軟體 **NGFW** 裝置）中查看相關聯的裝置。
3. 在 **License**（授權）欄中，將授權金鑰下載到某個位置，以安全將檔案傳輸到主機電腦。

STEP 6 | 在防火牆上，選取 **Device**（裝置） > **Licenses**（授權）。

必須透過網頁介面安裝授權金鑰。防火牆不支援透過 *SCP* 或 *FTP* 安裝授權金鑰。

STEP 7 | 按一下 **Manually Upload License**（手動上傳授權），並輸入授權金鑰。

©2023 Palo Alto Networks, Inc.

STEP 8 | 確認 **Dashboard**（儀表板）顯示有效的序號，且 **PA-VM** 授權顯示在 **Device**（裝置） > **Licenses**（授權）頁籤中。

STEP 9 | （選用）驗證移轉。

移轉具有 CSP 存取權的 Panorama 管理防火牆

在 Panorama 管理的防火牆上從固定授權移轉到彈性授權。

STEP 1 | 開始之前，確保您在防火牆上安裝授權 API 金鑰。

STEP 2 | 登入 Panorama 網頁介面。

STEP 3 | 驗證防火牆的 Palo Alto Networks 更新伺服器設定。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務）。
2. 確認 **Update Server**（更新伺服器）設定為 `updates.paloaltonetworks.com`。
3. 確認已選取 **Verify Update Server Identity**（驗證更新伺服器識別）。

STEP 4 | 如果還沒有為新的授權建立部署設定檔，請這樣做。需要此設定檔才能為移轉的 Panorama 產生新的授權碼。

STEP 5 | 擷取 VM-Series 授權碼。彈性授權的防火牆授權碼以字母 F 開頭，如下所示。

STEP 6 | 套用新的授權碼。

1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Licenses**（授權），然後 **Activate**（啟動）。
2. 輸入 VM-Series 授權碼。
3. 使用篩選，以選取要授權的受管理防火牆。
4. 在每個防火牆的 **Auth Code**（授權碼）欄中，輸入授權碼。
5. **Activate**（啟動）以確認授證升級。Panorama 會聯絡 Palo Alto Networks 更新伺服器，並根據您選擇的 VM-Series 型號、vCPU 和服務，取用防火牆所需的權杖。

STEP 7 | （選用）o。

Panorama 管理防火牆，無法存取 CSP

移轉無法訪問 CSP 的 Panorama 管理 VM-Series 防火牆。

STEP 1 | 開始之前，確保您在防火牆上安裝授權 API 金鑰。

STEP 2 | **Panorama**，無法存取網際網路—在離線 Panorama 管理的防火牆上移轉授權

STEP 3 | 使用手動程序從 Panorama 停用 VM，然後登入 CSP，並使用權杖檔案停用 VM。

STEP 4 | 在 CSP 中，建立部署設定檔使用與固定型號授權相同的 VM-Series 型號、vCPU 數量、安全性訂閱和 Panorama。您將使用此設定檔中的驗證碼。

©2023 Palo Alto Networks, Inc.

STEP 5 | 選取新的設定檔，按一下垂直省略符號，然後選取 **Register Firewall**（註冊防火牆）。

1. 輸入 VM 和防火牆資訊，然後選取 **Submit**（提交）。這會將防火牆與設定檔及其驗證碼建立關聯，並指派序號。
2. 按一下 **View Devices**（檢視裝置），在 **Software NGFW Devices**（軟體 **NGFW** 裝置）中查看相關聯的裝置。
3. 在 **License**（授權）欄中，將授權金鑰下載到某個位置，以安全將檔案傳輸到主機電腦。

STEP 6 | 套用新的授權碼。

1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Licenses**（授權），然後按一下 **Activate**（啟動）。
2. 使用篩選，以選取要授權的受管理防火牆。
3. 在每個防火牆的 **Auth Code**（驗證碼）欄，輸入部署設定檔中的授權碼。
4. 按一下 **Activate**（啟動）以確認授證升級。Panorama 會聯絡 Palo Alto Networks 更新伺服器，並根據您選擇的 VM-Series 型號、vCPU 和服務，取用防火牆所需的權杖。

STEP 7 | （選用）驗證移轉。

Panorama 管理的防火牆和 Panorama 都無權存取 CSP

當 Panorama 和受管理防火牆都無權存取 CSP 時，請在受管理防火牆上移轉授權。

STEP 1 | 如有必要，請在 VM-Series 防火牆上安裝授權 API 金鑰。

STEP 2 | 透過 CLI 使用手動模式停用固定型號授權。

STEP 3 | 使用手動程序從防火牆停用 VM，然後登入 CSP，並使用權杖檔案停用 VM。

STEP 4 | 在 CSP 中，建立部署設定檔使用與先前固定型號授權相同的 VM-Series 型號、vCPU 數量和安全性訂閱。您將使用此設定檔中的驗證碼。

STEP 5 | 選取新的設定檔，按一下垂直省略符號，然後選取 **Register Firewall**（註冊防火牆）。

1. 輸入 VM 和防火牆資訊，然後選取 **Submit**（提交）。這會將防火牆與設定檔及其驗證碼建立關聯，並指派序號。
2. 按一下 **View Devices**（檢視裝置），在 **Software NGFW Devices**（軟體 **NGFW** 裝置）中查看相關聯的裝置。
3. 在 **License**（授權）欄中，將授權金鑰下載到某個位置，以安全將檔案傳輸到主機電腦。

STEP 6 | 在防火牆上，選取 **Device**（裝置） > **Licenses**（授權）。

必須透過網頁介面安裝授權金鑰。防火牆不支援透過 *SCP* 或 *FTP* 安裝授權金鑰。

STEP 7 | 按一下 **Manually Upload License**（手動上傳授權），並輸入授權金鑰。

STEP 8 | 確認 **Dashboard**（儀表板）顯示有效的序號，且 **PA-VM** 授權顯示在 **Device**（裝置） > **Licenses**（授權）頁籤中。

©2023 Palo Alto Networks, Inc.

STEP 9 | （選用）驗證移轉。

驗證移轉

驗證授權移轉是否成功。

STEP 1 | 在裝置上檢查授權到期日，驗證授權是否成功更新。

STEP 2 | 驗證部署設定檔中啟用的所有訂閱是否套用至您的裝置。

STEP 3 | 在 CSP 上，驗證預期分配的積分數量與積分池中取用的積分是否相符。

STEP 4 | 在 CSP 上，驗證相關聯的權杖或授權數量是否歸還給先前的驗證碼。

©2023 Palo Alto Networks, Inc.

VM-Series 型號

VM-Series 防火牆有下列固定 vCPU 型號 # VM-50、VM-100、VM-200、VM-300、VM-500、VM-700 和 VM-1000-HV。除非下面另有說明，否則這些型號適用於所有支援的 PAN-OS 版本。用於部署 VM-Series 防火牆的軟體套件（*.xva*、*.ova* 或 *.vhdx* 檔案）在所有型號上通用。

您可以將固定型號 ***ELA*** 或永久授權移轉到彈性授權，並保留固定型號，或者，您可以將授權換成彈性 ***vCPU*** 授權。請參閱VM-Series 防火牆授權以比較授權方法。

- 在 VMware ESXi 和 vCloud Air、KVM、Microsoft Hyper-V、Cisco ACI、Cisco ENCS 及 Cisco CSP 上，所有型號都可以部署為來賓 virtual machine（虛擬機器 - VM）。
- 在公共雲端環境中（Amazon Web Services、Azure、Google Cloud Platform、Oracle Cloud Infrastructure、Alibaba Cloud），VM-50 除外，支援所有型號。
- 對於 VMware NSX，僅支援 VM-100、VM-200、VM-300、VM-500 和 VM-1000-HV 防火牆。

當您在 VM-Series 防火牆上套用容量授權時，防火牆上會實作型號和相關的容量。會根據 VM-Series 防火牆針對工作階段、規則、安全性區域、位址物件、IPSec VPN 通道和 SSL VPN 通道的處理進行最佳化的數量來定義容量。為了確保您針對網路需求購買了正確的型號，請使用下表瞭解各型號的最大容量以及依型號而定的容量差異：

Model	工作階段	安全性規則	動態 IP 位址	安全性區域	IPSec VPN 通道	SSL VPN 通道
VM-50	50,000	· 250 · Lite 模式中 200	1,000	15	· 250 · Lite 模式中 25	· 250 · Lite 模式中 25
VM-100 VM-200	250,000	1,500	2,500	40	1,000	500
VM-300 VM-1000-HV	800,000	10,000	100,000	40	2,000	2,000
VM-500	2,000,000	10,000	100,000	200	4,000	6,000
VM-700	10,000,000	20,000	100,000	200	8,000	12,000

如需您可在哪些平台上部署 VM-Series 防火牆的相關資訊，請參閱 VM-Series 部署。如需 VM-Series 防火牆型號的詳細資訊，請參閱 Palo Alto Networks 防火牆比較工具。您也可以檢閱關於 VM-Series 防火牆的一般資訊。

©2023 Palo Alto Networks, Inc.

- VM-Series 系統需求
- CPU 過度訂閱
- VM-50 Lite 模式
- VM-Series 型號授權類型
- 啟動 VM-Series 型號授權
- 註冊 VM-Series 防火牆
- 在 VM-Series 防火牆上安裝裝置憑證
- 在 BYOL 和 PAYG 授權之間切換
- 切換 VM-Series 型號授權
- 停用授權
- 更新 VM 系列防火牆授權搭售包

VM-Series 系統需求

VM-Series 防火牆的每個實例都需要最低資源配置—主機伺服器上的 CPU 數目、記憶體和磁碟空間。請利用下表來確認您將必要的硬體資源分配給 VM-Series 型號或記憶體設定檔。

PAN-OS 10.2 增加了額外的特性和功能，因此需要稍多的記憶體。若要提供與 PAN-OS 10.2 之前版本相同的工作階段規模，您需要增加最小記憶體分配。若是不根據 PAN-OS 10.2 之前的設定增加最小記憶體，最大工作階段規模將縮小。

VM-Series 型號	支援的 **Hypervisor**	支援的 **vCPU**	最小記憶體	啟用 **GTP** 時的最小記憶體	最小硬碟	最大（舊版）工作階段數	**PAN-OS 10.2*** 中的擴展工作階段	用於舊版工作階段數的推薦記憶體
VM-50	ESXi、Hyper-V、KVM	2	• 5.5GB • Lite 模式中 4.5GB	• 6GB • Lite 模式中 5GB	32GB（開機時 60GB）	65,000 • Lite 模式中 50,000	• 50,000 • Lite 模式中 25,000	• 6GB • 5.5GB
VM-100	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、Cisco ENCS、NSX-T (VM-100)	2	6.5GB	7.5 GB	60GB	250,000	200,000	7 GB

©2023 Palo Alto Networks, Inc.

VM-Series 型號	支援的 Hypervisor	支援的 vCPU	最小記憶體	啟用 GTP 時的最小記憶體	最小硬碟	最大（舊版）工作階段數	PAN-OS 10.2* 中的擴展工作階段	用於舊版工作階段數的推薦記憶體
	Azure 上的 VM-100 需要 4 個 vCPU。							
VM-300	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、Cisco ENCS、NSX-T (VM-300)	2、4	9 GB（最小值） 11 GB（推薦）	10 GB	60GB	800,000	600,000	10 GB
VM-500	AWS、Azure、Cisco ACI、Cisco CSP、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、NSX-T	2、4、8	16GB	20GB	60GB	2,000,000	1,800,000	18 GB
VM-700	AWS、Azure、ESXi、Google Cloud Platform、Hyper-V、KVM、OCI、Alibaba Cloud、Cisco ACI、Cisco CSP、NSX-T	2、4、8、16	56GB	64GB	60GB	10,000,000	10,000,000	56GB

*固定型號的 VM-Series 防火牆，其授權由軟體 NGFW 積分資助。

**在 PAN-OS 10.2 中，9 GB 可能不夠，具體取決於防火牆上使用的功能集或功能集組合（如 GTP 或高性能功能）。如果您遇到記憶體資源相關的問題，請將記憶體增加至 11 GB，以滿足某些功能或功能組合的其他記憶體需求。

©2023 Palo Alto Networks, Inc.

你可以在 VM-50 上啟用 LIte 模式。Lite 模式是專為資源有限的環境準備的可替換操作模式。如需詳細資訊，請參閱 VM-50 Lite 模式。

為了達到最佳效能，單一 *CPU* 通訊端上應該有所有必要的核心。

在操作方面，*VM-50* 防火牆至少需要 *32GB* 硬碟空間。不過，因為 *VM-Series* 基本映像是所有型號通用，在授權 *VM-50* 之前，您必須配置 *60GB* 硬碟空間。

根據指派給 VM-Series 防火牆的 vCPU 數目而定，指派給管理平面和指派給資料平面的 vCPU 數目有所不同。如果您指派的 vCPU 數目超過授權正式支援的數量，多出來的任何 vCPU 會指派給管理平面。

vCPU 總計	管理平面 **vCPU**	資料平面 **vCPU**
2	1	1
4	2	2
8	2	6
16	4	12

CPU 過度訂閱

VM-Series 防火牆在所有型號上都支援 CPU 過度訂閱。CPU 過度訂閱可讓您在執行 x86 架構的 Hypervisor 上部署更高密集度的 VM-Series 防火牆。根據所需的 CPU 配置，您可以部署兩個 (2:1) 至五個 (5:1) VM-Series 防火牆。在規劃部署時，請利用下列公式來計算硬體所能支援的 VM-Series 防火牆數目。

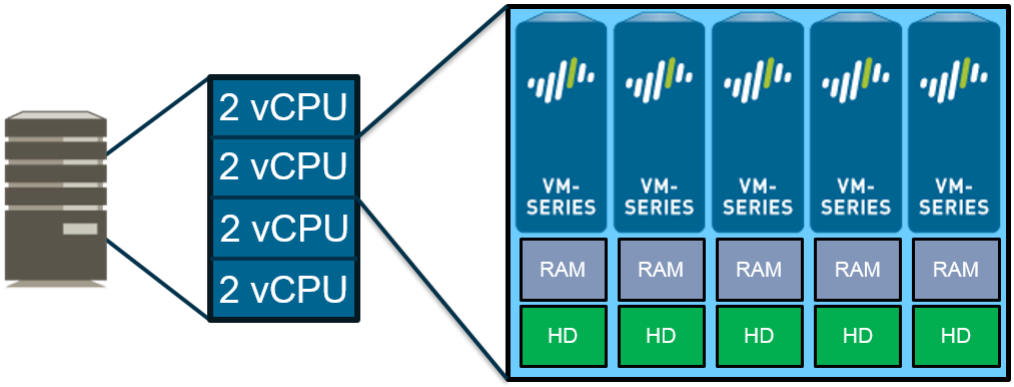
（CPU 總數 x 過度訂閱率）/每個防火牆的 CPU 數目 = VM-Series 防火牆總數

例如，假設比例是 5:1，則具備 16 個實體 CPU 和至少 180GB 記憶體 (40 × 4.5GB) 的主機電腦，最多可支援 40 個實例給 VM-50。每個 VM-50 需要兩個 vCPU，每一對 vCPU 可以有五個相關聯的 VM-50。

（16 個 CPU x 5）/2 = 40 個 VM-50 防火牆

除了符合最低的 VM-Series 系統需求，享受過度訂閱並不需要任何其他組態。正常部署 VM-Series 防火牆就會自動形成資源過度訂閱。在規劃部署時，請考量其他功能，例如虛擬交換器，以及主機上本身需要硬體資源的來賓電腦。

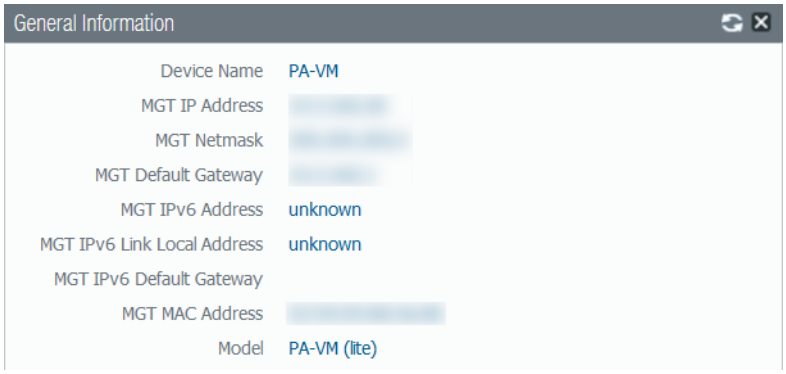
©2023 Palo Alto Networks, Inc.



VM-50 Lite 模式

標準 VM-50 雖然是 VM-Series 中最小的款式，但在某些環境下需要較可用資源更多的資源。VM-50 Lite 模式為硬體資源受限的環境提供了一套備選方案。VM-50 Lite 需要 4.5GB 的記憶體，而非標準 VM-50 所需要的 5.5GB。VM-50 Lite 使用的授權與標準 VM-50 相同，但是在配置為 4.5GB RAM 時，會以 Lite 模式出現。

- 在高可用性部置中，這兩種 ***VM-Series*** 防火牆的授權必須與 ***VM-50*** 相同，以避免容量不符的問題。若容量授權不符，則 ***VM-50***（非 ***Lite***）被視為容量更高；***VM-50*** 在 ***VM-50 Lite*** 仍在運作時會變成不運作。
- ***VM-50 Lite*** 不支援巨型框架；***VM-50*** 和 ***VM-50 Lite*** 不支援 ***WildFire*** 內嵌 ***ML***。



VM-Series 型號授權類型

下列授權及適用授權適用於 VM-Series 防火牆：

- 容量授權—VM-Series 防火牆需要基礎授權（又稱為容量授權），以啟用防火牆上的型號（VM-50、VM-100、VM-200、VM300、VM-500、VM-700 或 VM-1000-HV）及相關聯的容量。容量授權包含在搭售包中，可以是永久或基於期限：
  - 永久授權—授權無到期日期，允許您無限期使用 VM-Series 防火牆的授權容量。永久授權僅適用於 VM-Series 容量授權。

©2023 Palo Alto Networks, Inc.

- 期限授權—期限授權允許您在指定期限內使用 VM-Series 防火牆。此授權具有到期日期，到期前，系統會提示您更新授權。期限授權適用於容量授權，支援各項權利和使用授權。

- **VM-Series ELA**—對於高成長企業，VM-Series 企業授權合約 (VM-Series ELA) 提供固定價格的授權選項，允許最多使用 BYOL 無限制地部署 VM-Series 防火牆。ELA 是一份為期一年或三年的合約，合約期滿時不會進行授權校正。

  有兩種類型的 VM-Series ELA：

  - 如果您已在 2018 年 12 月 4 日之前購買 VM-Series ELA，則具有傳統 VM-Series ELA，其中包括任何所支援 Hypervisor 或公共雲端環境上您選擇的單一 VM-Series 型號。使用此 ELA，您會接收到每個 VM-Series 防火牆實例之容量、支援、GlobalProtect、PAN-DB URL 篩選、威脅防護和 WildFire 訂閱的單一授權碼。您也可以無限制地部署裝置管理授權所隨附的 Panorama 虛擬設備，且各有 1000 個防火牆。

    Palo Alto Networks 從 2019 年 4 月 16 日開始逐步淘汰傳統 VM-Series ELA。將現有企業授權客戶的帳戶移轉至多重型號 ELA 時，現有企業授權客戶會收到其支援代表的通知。授權權杖將根據 VM-Series 防火牆訂閱合約進行散佈；不需要執行其他動作，就能持續操作防火牆。如果您想要管理 VM-Series ELA 授權權杖，則必須指定 ELA 管理員。只有 Palo Alto Networks 客戶支援入口網站 (CSP) 上的超級使用者角色才能指派 ELA 管理員。

  - 包括大部分 VM-Series 防火牆公事包型號以及 GlobalProtect、PAN-DB URL 篩選、威脅防護、WildFire 訂閱和支援權利的多重型號 VM-Series ELA，會呼叫您在 2018 年 12 月 4 日之後購買的 VM-Series 企業授權合約（多重型號 ELA）（作為新的購買或作為傳統 VM-Series ELA 的重新購買）。您也可以無限制地部署具有裝置管理授權的 Panorama 虛擬設備，且各有 1000 個防火牆。

公共雲端專用 VM-Series 防火牆授權

VM-Series 授權策略與 AWS、Azure 和 Google Cloud Platform 相同。有不同的授權類型（請參閱授權類型—VM-Series 防火牆）以及自帶授權與即付即用方式：

- 自帶授權 **(BYOL)**—從合作夥伴、經銷商或直接從 Palo Alto Networks 購買的授權。BYOL 支援各別功能授權、支援授權以及訂閱搭售包。

  - 對於個別 BYOL 授權，您必須在部署 VM-Series 防火牆之後套用授權碼。
  - BYOL 搭售包有一個您可包含在啟動套件中的授權碼（請參閱啟動 VM-Series 防火牆）。所有包含在搭售包裡的訂閱都在防火牆啟動時予以授權。

  OCI GovCloud 上 *VM-Series* 防火牆的 *BYOL* 授權需要 *FIPS* 和非 *FIPS* 模式的 *PAN-OS 10.1.2* 或更高版本。

©2023 Palo Alto Networks, Inc.

- 即付即用 **(PAYG)**—也稱之為 依使用授權或使用時付費授權。PAYG 授權可從您的雲端供應商處購買：
  - AWS：從AWS Marketplace購買。支援以小時和以年計費的 PAYG 選項。
  - Azure：從Azure Marketplace購買。支援以小時計費的 PAYG 選項。
  - Google Cloud Platform：從 Google Cloud Platform Marketplace 購買。Google Cloud Platform 支援每分鐘的 PAYG 選項。
  - Oracle Cloud Infrastructure：（PAN-OS 10.0.3 或更新版本）從 Oracle Cloud Marketplace 購買。

    OCI 上的 *VM-Series PAYG* 授權不支援 *VM-100*。

  如使用 PAYG 授權搭售包，則防火牆將預先授權且在您部署後隨時可用；您不會收到驗證碼。當您從 Cloud 主控台停止或終止防火牆時，PAYG 授權會暫停或終止。

  PAYG 授權會根據配置給實例的硬體來套用 VM-Series 容量授權。PAYG 實例會檢查可供實例使用的硬體資源量，並套用可用資源允許的最大 VM-Series 防火牆容量授權。例如，如果實例具有 2 個 vCPU 和 16 GB 的記憶體，則會根據 vCPU 的數量套用 VM-100 的容量授權。不過，如果實例具有 16 個 vCPU 和 16 GB 的記憶體，則會根據記憶體數量套用 VM-500 的授權。如需 VM-Series 型號資源需求的詳細資訊，請參閱VM-Series 系統需求。

  最初部署為執行 *PAN-OS 9.1.2* 的 *PAYG* 防火牆實例，不支援 *PAN-OS* 的降級。在 *PAN-OS 9.1.2* 之前部署的防火牆實例，可降級至較舊的 *PAN-OS* 版本。

  PAYG 授權搭售如下：

授權功能	搭售包 **1**	搭售包 **2**	搭售包 **3**
VM-Series 防火牆功能授權	VM-100、VM-300、	VM-500、VM-700、	VM-500、VM-700、VM-500、V
進階支援	✓	✓	✓
威脅防禦（AV、IPS 與惡意軟體防禦）	✓	✓	
GlobalProtect		✓	✓
PAN-DB URL Filtering		✓	
WildFire		✓	✓
DNS 安全性		✓	✓
Advanced URL Filtering 進階 URL 篩選			✓
進階威脅防護			✓

©2023 Palo Alto Networks, Inc.

使用 *VM-Series* 防火牆 *CLI* 來檢視您套用的 *PAYG* 授權時，***show system info*** 命令顯示的值與 ***request license info*** 命令顯示的輸出不同。對於 *PAN-OS* 版本 *9.1.1* 和更早版本，不論已套用的 *VM-Series* 型號，***request license info*** 命令永遠將型號顯示為 *VM-300*。

您無法在 PAYG 和 BYOL 授權之間切換。若要從 PAYG 改為 BYOL，請聯絡 Palo Alto Networks 通路夥伴或業務代表來購買 BYOL 授權，並取得可用來授權防火牆的 BYOL 驗證碼。如果您已部署防火牆且想要切換授權，請參閱在 BYOL 和 PAYG 授權之間切換。

如果您有 *VM-Series* 防火牆的評估複本，且想要轉換成相同授權類型（*BYOL* 至 *BYOL*）的完整授權（購買的）複本，您可以停用評估授權，然後就地啟動購買的授權。相關指示請參閱升級 VM-Series 防火牆。

VM-Series 企業授權合約（多重型號 ELA）

VM-Series 企業授權合約 (VM-Series ELA) 是一年或三年的全方位授權合約，可讓您購買 VM-Series 防火牆，以及 GlobalProtect、PAN-DB URL 篩選、威脅防護、WildFire 和 DNS 安全性訂閱。它也包括 Panorama 的支援權利和裝置管理授權。多重型號 VM-Series ELA 提供使用單一合約的簡化授權管理，可讓您部署符合您企業安全性需求的任何 VM-Series 防火牆型號。

當您購買多重型號 VM-Series ELA 時，請預測您訂閱期間所需的防火牆數目。根據您的預測和可容納未來成長的其他配置，您在客戶支援入口網站 (CSP) 上的帳戶具有授權權杖集區，可讓您部署任何型號的 VM-Series 防火牆。根據您部署的防火牆型號和防火牆數目，會從您可用的授權權杖集區中扣除指定數目的權杖。會根據每種防火牆型號的值，計算從您的帳戶產生的權杖：

- VM-50—10 個權杖
- VM-100—25 個權杖
- VM-300—50 個權杖
- VM-500—140 個權杖
- VM-700—300 個權杖

使用 VM-Series ELA，合約期滿時不會進行授權校正，這表示即使您部署的防火牆多於原始預測，還是不會向您追溯費用。因此，為了平衡彈性與責任，VM-Series ELA 使用條款包括有限和無限期間，以說明如何在需要時取用權杖和部署防火牆。如需詳細資料，請參閱 ELA 條款。您使用 VM-Series ELA 所部署的 VM-Series 防火牆沒有永久授權，而在條款到期時，您必須更新合約來延長支援權利，以及持續存取防火牆上的軟體和內容版本更新。

使用 CSP 上的 ELA 管理員角色，您可以在屬於不同部門的其他管理員之間，使用他們自己的 CSP 帳戶來傳輸或分割授權權杖。此共用可讓您企業中的其他管理員依需求部署 VM-Series 防火牆，只要他們在其個別 CSP 帳戶中有可用的權杖。請參閱管理 VM-Series ELA 授權權杖來邀請其他管理員共用 ELA 權杖，以及部署符合您企業安全性需求的任何 VM-Series 防火牆型號。如果想要隨著組織性需求不斷變化而重新散佈權杖，您也可以收回權杖，從 VM-Series ELA 中移除 CSP 帳戶。

觀賞 VM-Series 多重型號 ELA 影片

- 管理 VM-Series ELA 授權權杖
- 接受 VM-Series ELA

©2023 Palo Alto Networks, Inc.

管理 **VM-Series ELA** 授權權杖

VM-Series 企業授權合約（多重型號 ELA） (VM-Series ELA) 可讓您彈性具有可與企業中其他管理員共用的單一合約。您必須具有 Palo Alto Networks 客戶支援入口網站 (CSP) 的超級使用者角色才能啟動 ELA，而且啟動 ELA 授權碼時，您會繼承 CSP 的 ELA 管理員角色。

使用 ELA 管理員角色，您可以管理可用來部署合約所含的 VM-Series 防火牆和訂閱的授權權杖集區。您可以邀請其他管理員共用 VM-Series ELA 權杖、授與每個管理員可用的 VM-Series 防火牆實例的型號和數目，以及從 VM-Series ELA 移除 CSP 帳戶。根據您為每個授與者配置的項目，他們會接收到接著可以用來部署 VM-Series 防火牆的特定數目的權杖。

額外的購買和授與不會直接新增至 ***CSP*** 帳戶中的可用 ***VM-Series*** 防火牆數目；而是將 ***ELA*** 授權權杖新增至 ***VM-Series ELA*** 權杖集區。***ELA*** 管理員之後可以將 ***ELA*** 授權權杖配置至給定的 ***CSP*** 帳戶，以增加可用的 ***VM-Series*** 防火牆數目。

STEP 1 | （僅限傳統 VM-Series ELA 客戶）指定 ELA 管理員來管理權杖。

已移轉至多重型號 ELA 的現有企業授權客戶必須指定 ELA 管理員來管理 VM-Series ELA 授權權杖。轉換時，不需要其他動作，就能繼續操作防火牆，不過，除非已指派 ELA 管理員，否則您將無法（重新）配置權杖來部署防火牆。只有具有 CSP 超級使用者角色的管理員才能指定 ELA 管理員，而 ELA 管理員接著可以管理權杖或將權杖授與其他管理員。

1. 登入 Palo Alto Networks CSP。
2. 選取 **Members**（成員） > **Manage Users**（管理使用者）。
3. 按一下 **Actions**（動作）下方的鉛筆圖示，以編輯您想要指派 ELA 管理員角色的使用者。
4. 選取 **ELA Administrator**（**ELA** 管理員），然後按一下核取記號，將新的角色新增至選取的使用者。
5. 繼續步驟 3。

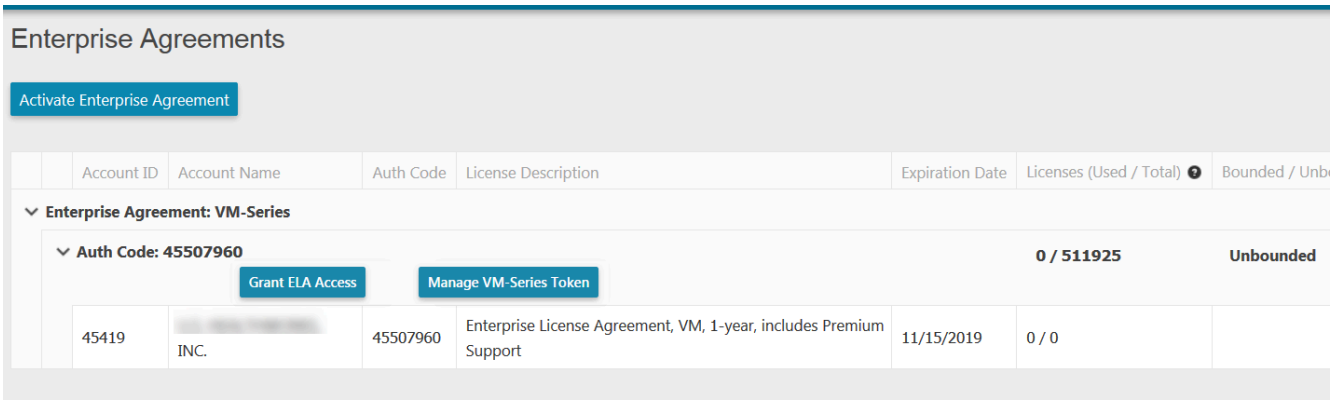
©2023 Palo Alto Networks, Inc.

STEP 2 | 啟動 ELA 授權碼。

啟動 ELA 的管理使用者會繼承 CSP 的 ELA 管理員和超級使用者角色，而且可以管理權杖或將權杖授與其他管理員。

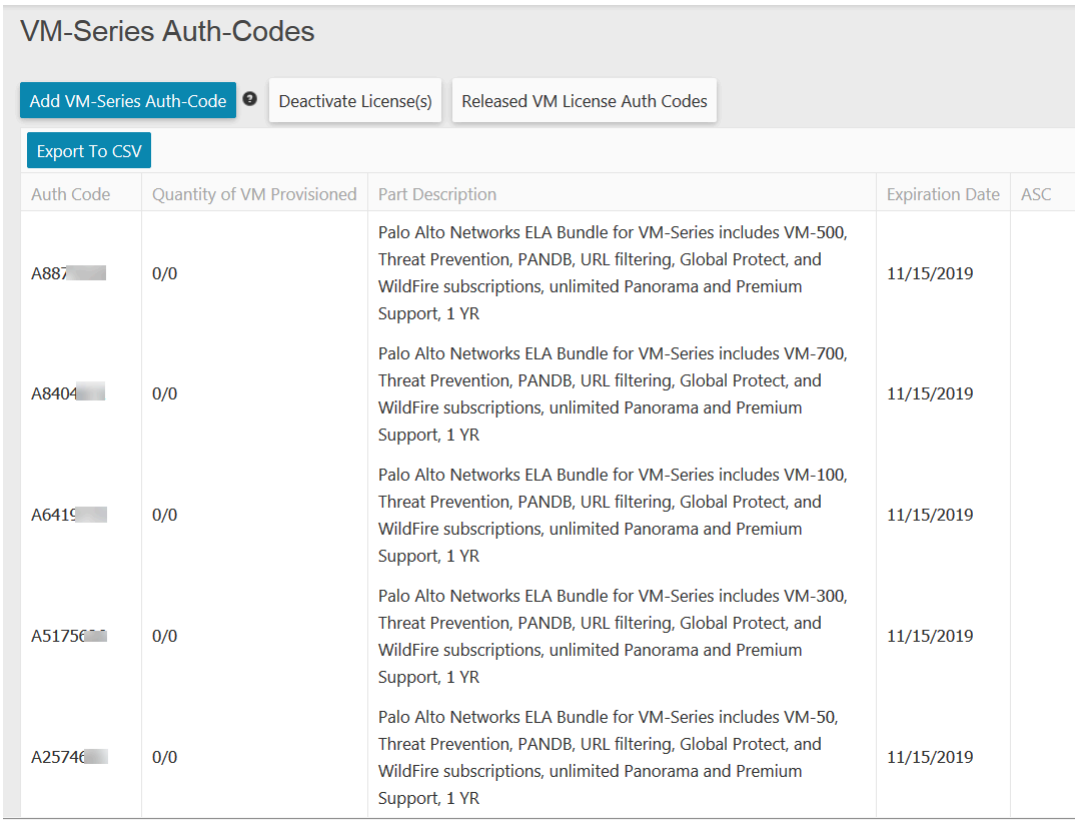
1. 登入 Palo Alto Networks CSP。
2. 選取 **Assets**（資產） > **Enterprise Agreements**（企業合約） > **Activate Enterprise Agreement**（啟動企業合約）。
3. 輸入 **Authorization Code**（授權碼），然後 **Agree and Submit**（同意並提交）EULA。

   在 [Enterprise Agreements（企業合約）] 之下，確認已將授權碼註冊到您的帳戶：VM-Series。此頁面顯示授權碼、帳戶 ID、帳戶名稱、授權說明、到期日、您有的授權數目（已使用/總計），以及合約的有限和無限期間內有多少可用於部署。



4. 選取 **Assets**（資產） > **VM-Series Auth-Codes**，以檢視用於部署 VM-Series 防火牆的每個型號以及 ELA 所隨附的相關聯訂閱的授權碼。

©2023 Palo Alto Networks, Inc.



VM-Series Auth-Codes

Add VM-Series Auth-Code | Deactivate License(s) | Released VM License Auth Codes

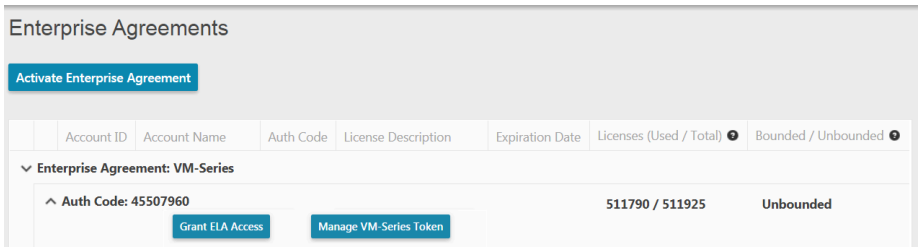
Export To CSV

Auth Code	Quantity of VM Provisioned	Part Description	Expiration Date	ASC
A887	0/0	Palo Alto Networks ELA Bundle for VM-Series includes VM-500, Threat Prevention, PANDB, URL filtering, Global Protect, and WildFire subscriptions, unlimited Panorama and Premium Support, 1 YR	11/15/2019	
A8404	0/0	Palo Alto Networks ELA Bundle for VM-Series includes VM-700, Threat Prevention, PANDB, URL filtering, Global Protect, and WildFire subscriptions, unlimited Panorama and Premium Support, 1 YR	11/15/2019	
A6419	0/0	Palo Alto Networks ELA Bundle for VM-Series includes VM-100, Threat Prevention, PANDB, URL filtering, Global Protect, and WildFire subscriptions, unlimited Panorama and Premium Support, 1 YR	11/15/2019	
A51756	0/0	Palo Alto Networks ELA Bundle for VM-Series includes VM-300, Threat Prevention, PANDB, URL filtering, Global Protect, and WildFire subscriptions, unlimited Panorama and Premium Support, 1 YR	11/15/2019	
A25746	0/0	Palo Alto Networks ELA Bundle for VM-Series includes VM-50, Threat Prevention, PANDB, URL filtering, Global Protect, and WildFire subscriptions, unlimited Panorama and Premium Support, 1 YR	11/15/2019	

©2023 Palo Alto Networks, Inc.

STEP 3 | 授與 ELA 存取企業中的其他管理員。

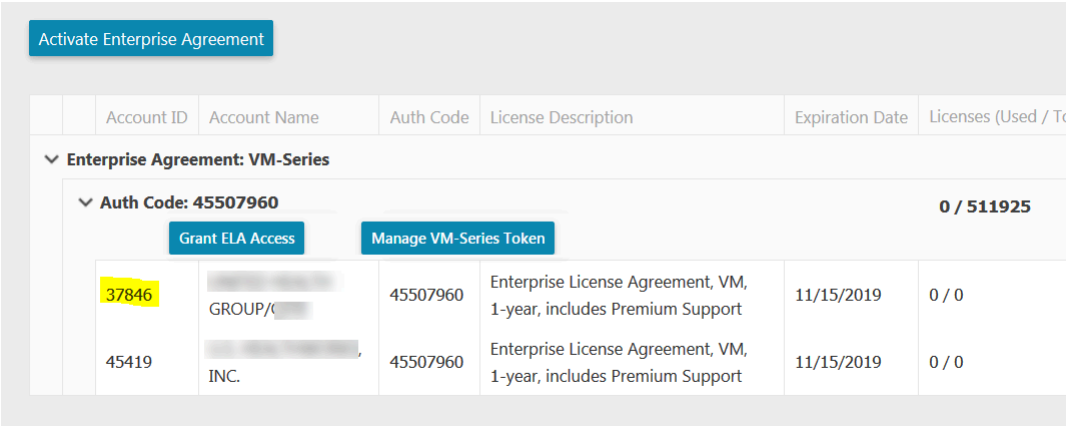
此功能可讓您與企業或部門內的其他管理員共用 VM-Series ELA，讓他們可以依需求部署 VM-Series 防火牆。身為 ELA 管理員，您可以將存取權授與已向 CSP 上的電子郵件位址註冊的其他使用者。



1. 在 **Assets**（資產） > **Enterprise Agreements**（企業合約）上，選取 **Grant ELA Access**（授與 **ELA** 存取）。
2. 輸入您想要邀請的管理員的 **Destination Email**（目的地電子郵件）位址。

   您在上面輸入的目的地電子郵件位址必須是具有超級使用者角色的 CSP 上的註冊使用者，他們才能登入並接受授與。如果未在 CSP 上註冊電子郵件位址，則您必須先在 **Members**（成員） > **Create New User**（建立新使用者）上建立使用者的新帳戶。
3. 選取 **Notify User**（通知使用者），以觸發您所輸入電子郵件位址的通知電子郵件。

   收件者必須登入 CSP 以接受 VM-Series ELA。收件者接受授與之後，**Assets**（資產） > **Enterprise Agreements**（企業合約）上會提供帳戶 ID，如下列螢幕擷取畫面所示。

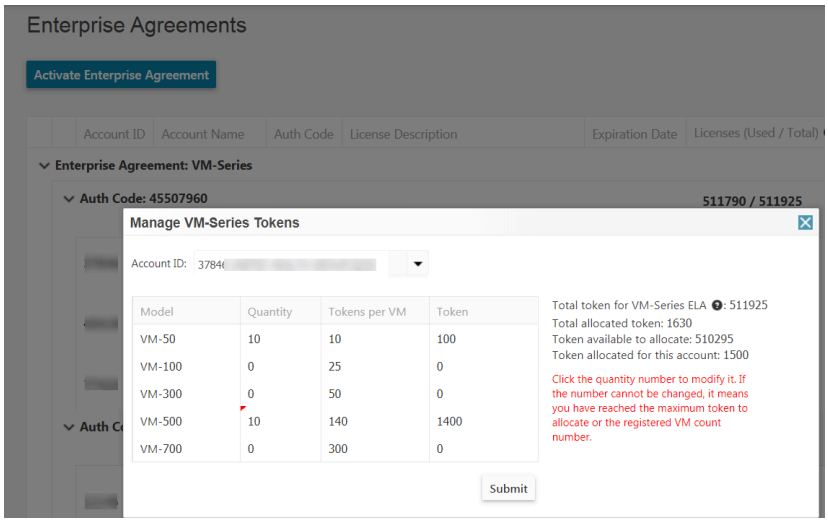


©2023 Palo Alto Networks, Inc.

STEP 4 | 配置用於部署防火牆的權杖。

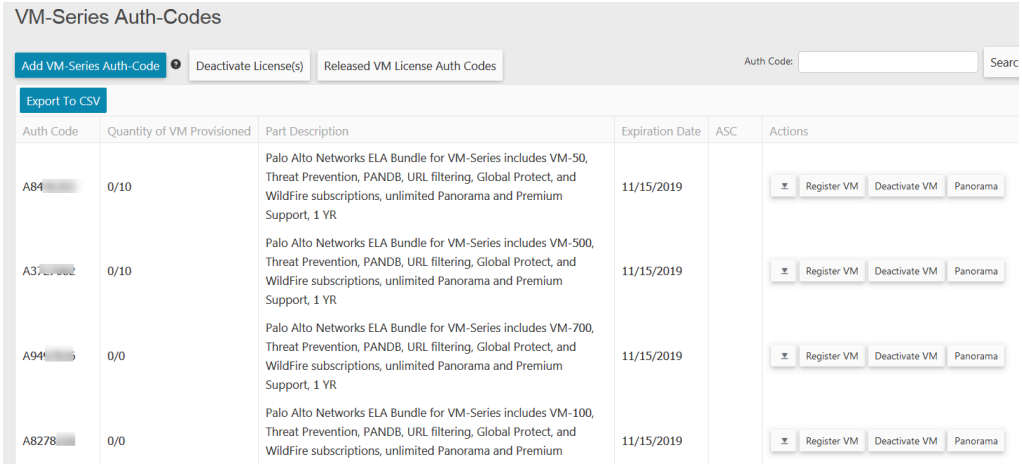
1. 選取 **Assets**（資產） > **Enterprise Agreements**（企業合約） > **Manage VM-Series Tokens**（管理 **VM-Series** 權杖）。

   針對每個帳戶 ID，您可以指定想要配置的型號的防火牆數目。根據防火牆型號和數量，會自動計算權杖數目，並可供使用。在此範例中，您允許 VM-50 和 VM-500 各有 10 個實例。



2. 確認帳戶中所處置的精確防火牆實例數目。

   選取 **Assets**（資產） > **VM-Series Auth-Code**，以確認您配置的授權碼。在此範例中，帳戶可以佈建 VM-50 和 VM-500 各 10 個實例。收件者部署防火牆時，會從總可用集區中扣除權杖數目，而且您可以檢視他們已佈建的防火牆實例數目與您為他們配置的總數量的比率。隨著安全性需求演變，您可以彈性地配置更多數量，而且只要您有可用的權杖，就允許存取不同的 VM-Series 防火牆型號。



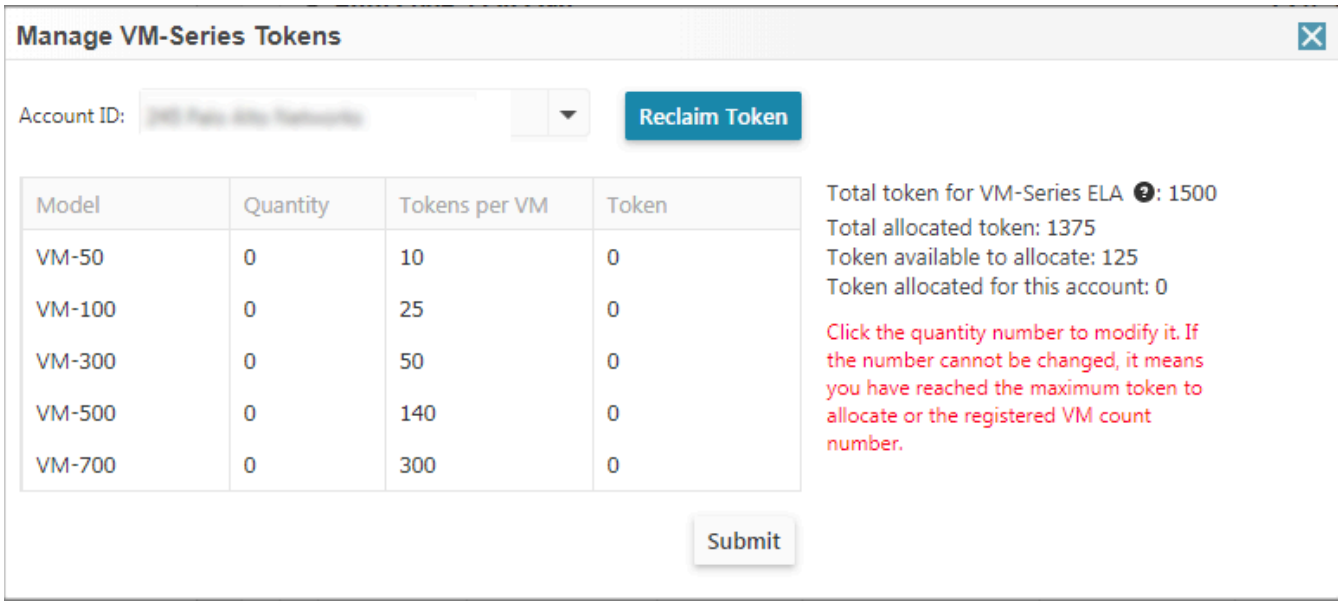
 ©2023 Palo Alto Networks, Inc.

STEP 5 | 從 VM-Series ELA 移除 CSP 帳戶，以收回權杖。

您無法收回配置給 *CSP* 帳戶的權杖的某個部分。藉由收回權杖，您將從 *VM-Series ELA* 移除整個 *CSP* 帳戶，並將所有相關聯的權杖重新配置給權杖集區。

1. 確認 VM-Series 防火牆未使用與您要移除之 CSP 帳戶相關聯的所有權杖。視需要停用 VM-Series 防火牆，以佈建權杖來進行移除。
2. 選取 **Assets**（資產） > **Enterprise Agreements**（企業合約） **> Manage VM-Series Token**（管理 **VM-Series** 權杖）。

   選取您想要收回權杖的帳戶 ID，然後按一下 **Reclaim Token**（收回權杖）。如果權杖可供收回，則您會接收到已成功移除的確認。



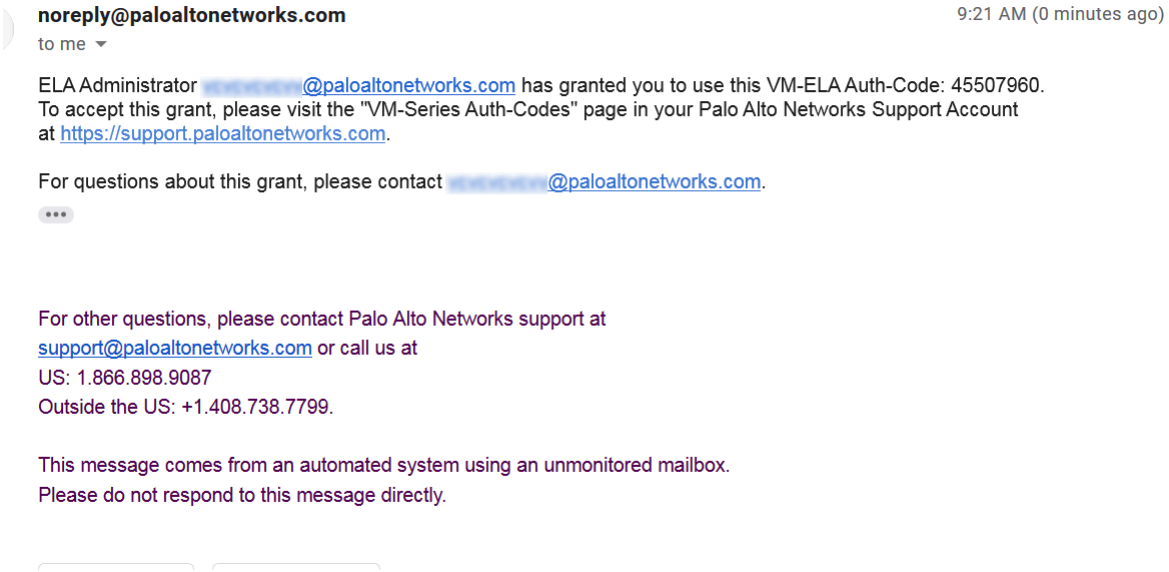
接受 VM-Series ELA

如果您的企業已購買 VM-Series ELA，則 ELA 管理員可以邀請您共用合約以及共用授權權杖集區，讓您可以存取可讓您依需求部署 VM-Series 防火牆的 VM-Series 防火牆授權碼。當您接收用於存取 VM-Series ELA 的授與時，會收到內含可登入 Palo Alto Networks 客戶支援入口網站 (CSP) 的連結的電子郵件通知，而且必須同意並接受使用條款。在您接受 ELA 使用條款之後，ELA 管理員可以配置授權您使用的 VM-Series 防火牆型號和數目；會在您的帳戶中處理相應數目的 VM-Series ELA 權杖。

©2023 Palo Alto Networks, Inc.

STEP 1 | 檢查您的電子郵件收件匣中是否有授與通知。

通知包括已邀請您共用 VM-Series ELA 的 ELA 管理員的電子郵件位址。

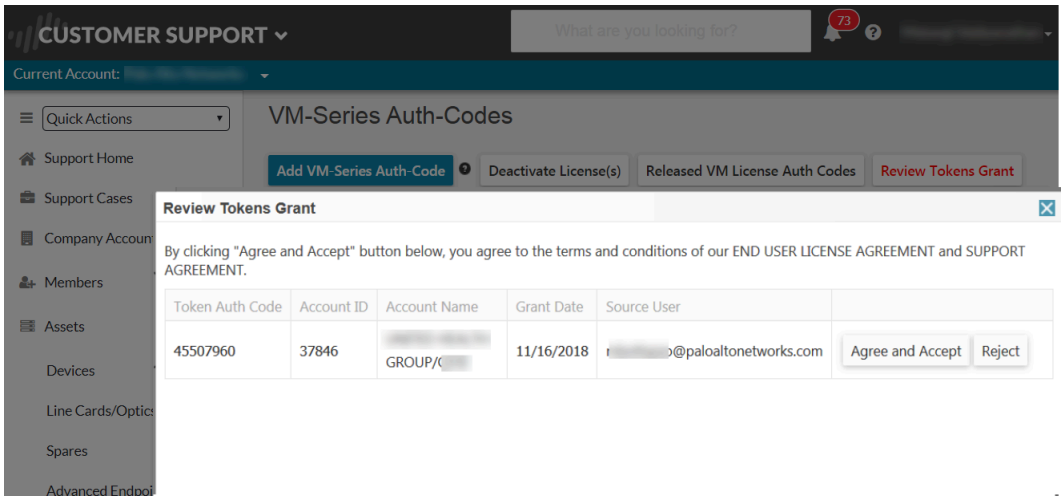


STEP 2 | 接受授與。

您必須先檢閱條款並接受 EULA 和支援合約，ELA 管理員才能配置可讓您部署 VM-Series 防火牆的權杖。

1. 登入 Palo Alto CSP。
2. 選取 **VM-Series Auth Codes**（**VM-Series** 授權碼）以 **Review Tokens Grant**（檢閱權杖授與）。

   您必須同意並接受 EULA 和支援合約，才能接受授與。如果您拒絕它，則給予您授與的 ELA 管理員會收到您拒絕授與的電子郵件通知。請務必讓 ELA 管理員知道您已接受授與，讓他/她可以配置您可以部署的 VM-Series 防火牆型號和數量。

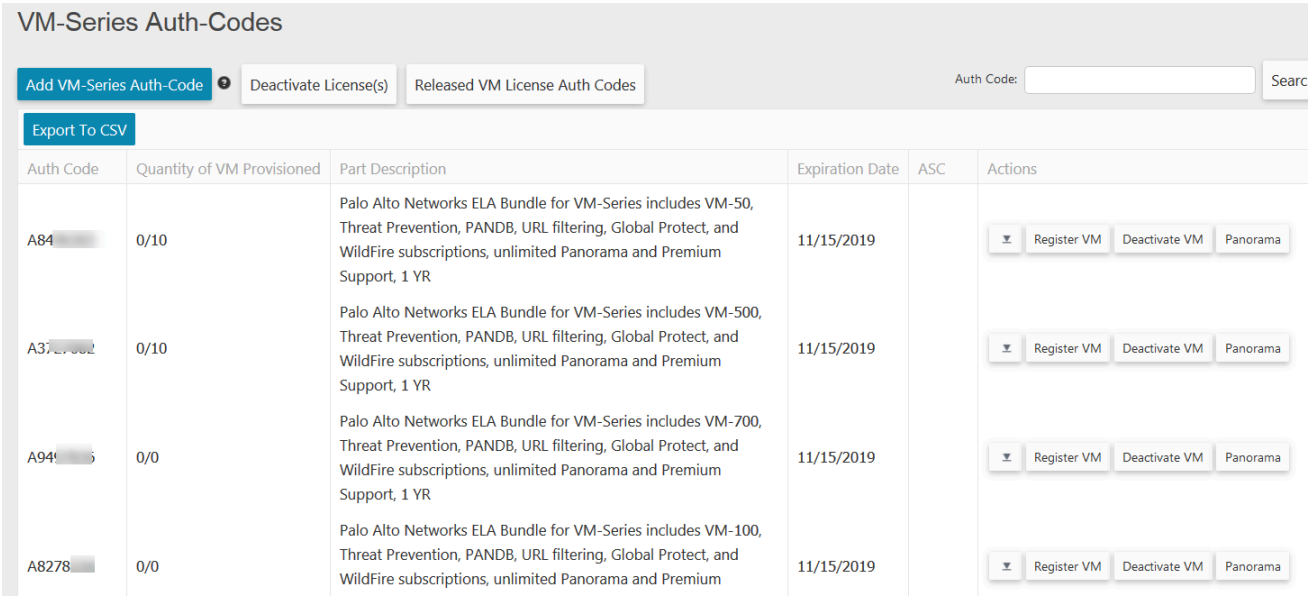


如果您屬於 *CSP* 上的多個帳戶，並意外接受錯誤帳戶中的授與，則必須要求 *ELA* 管理員將授與重新傳送給您。除非您接受正確帳戶中的授與，否則請不要開始使用授權碼來佈建防火牆。

©2023 Palo Alto Networks, Inc.

STEP 3 | 確認為您配置的 VM-Series 型號和數目。

ELA 管理員配置您可以佈建的 VM-Series 防火牆型號和實例數目之後，您可以選取 **Assets**（資產） > **VM-Series Auth Codes**（**VM-Series** 授權碼），以檢視為您配置的型號和數目。例如，下列螢幕擷取畫面中的授與會顯示可讓您部署 VM-50 和 VM-500 各 10 個實例的授權碼。



在您部署防火牆並將它們註冊到 CSP 時，佈建的防火牆數目會遞增。**Quantity of VM Provisioned**（佈建的 **VM** 數量）會顯示每個型號的已佈建數目與可用數目比率。

啟動 VM-Series 型號授權

若要在 VM-Series 防火牆上啟動授權，您必須先完成 VM-Series 防火牆的部署以及初始組態。若要部署防火牆，請參閱 VM-Series 部署。

對於所有 BYOL 型號，包含 AWS、Azure、Google Public Cloud，請使用本章節中的指示。對於公共雲端內依使用授權部分，您無需啟動該授權。您必須註冊公共雲端專用依使用授權模式的 VM-Series 防火牆（無授權碼），以啟動進階支援權利。

對於 *AWS Marketplace* 中依使用授權模式的 *VM-Series* 防火牆，支援具有完整和簡短 *AWS* 實例 *ID* 的實例。

在啟動 VM-Series 防火牆上授權之前，防火牆將缺乏序號、資料背板介面的 MAC 位址也並非唯一位址，且只能支援最少數量的工作階段。由於在授權防火牆之前，MAC 位址並非唯一位址，因此為了防止 MAC 位址重疊而導致問題，請確定您沒有多個未授權的 VM-Series 防火牆。

啟動授權時，授權伺服器會使用虛擬機器的 UUID 和 CPU ID，為 VM-Series 防火牆產生唯一的序號。將容量驗證碼與序號結合使用，即可驗證您的資格。

VM-Series 防火牆的 ***License***（授權）頁籤會顯示所有授權模式的標準 *VM-300* 授權檔案。若要尋找您特定授權模式的資訊，請柬是 *UI* 中的統資訊，或使用 *CLI* 檢視系統資訊。

©2023 Palo Alto Networks, Inc.

對 *VM-Series* 防火牆授權後，如果您需要刪除及重新部署 *VM-Series* 防火牆，請確定在防火牆上停用授權。停用授權可讓您將有效授權轉移至 *VM-Series* 防火牆的新實例，無需求助技術支援。

- 啟動 VM-Series 防火牆的授權（獨立版本）
- 啟動 VMware NSX 專用 VM-Series 防火牆的授權
- 授權啟動問題的疑難排解

啟動 VM-Series 防火牆的授權（獨立版本）

如果未選取利用訂閱搭售包來使用啟動工作流程，您必須部署 VM-Series 防火牆並完成初始組態，才能在 VM-Series 防火牆上啟動授權。

- 直接存取網際網路
- 無法存取網際網路

直接存取網際網路

若要啟動授權，防火牆必須設有 IP 位址、網路遮罩、預設閘道及 DNS 伺服器 IP 位址。

防火牆必須具備有效的 DNS 組態，而且能夠連線網路，才能存取 Palo Alto Networks 授權伺服器。

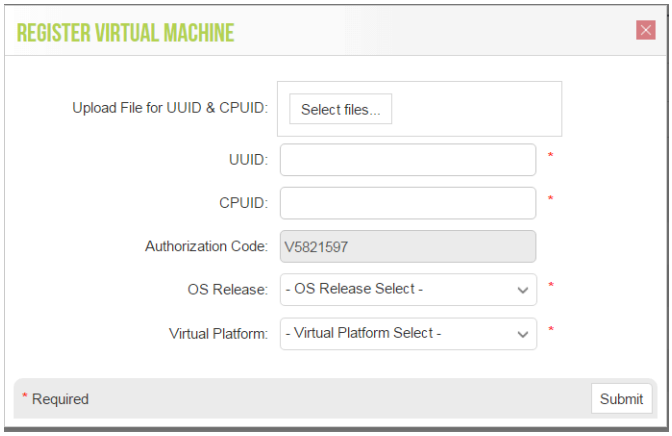
1. 選取 **Device**（裝置） > **Licenses**（授權），然後選取 **Retrieve license keys from license server**（從授權伺服器擷取授權金鑰）連結。
2. 防火牆將連線至更新伺服器 (updates.paloaltonetworks.com)，並自動下載授權及重新啟動。
3. 重新登入 Web 介面並確認 **Dashboard**（儀表板）顯示有效的序號。如果顯示 **Unknown** 一詞，則意味設備未經授權。
4. 在 **Device**（裝置） > **Licenses**（授權）上，驗證 **PA-VM** 授權是否已新增至裝置。

   如果您看到錯誤訊息，請參閱授權啟動問題的疑難排解。

©2023 Palo Alto Networks, Inc.

無法存取網際網路

1. 選取 **Device**（裝置） > **Licenses**（授權），然後按一下 **Activate Feature using Auth Code**（使用驗證碼啟動功能）連結。
2. 按一下 **Download Authorization File**（下載授權檔案），然後在用戶端電腦上下載 **authorizationfile.txt**。
3. 將 **authorizationfile.txt** 複製到可存取網際網路的電腦，並登入支援入口網站。按一下 **My VM-Series Auth-Codes**（我的 **VM-Series** 驗證碼）連結，從清單中選取適用的驗證碼，然後按一下 **Register VM**（註冊 **VM**）連結。
4. 在 **Register Virtual Machine**（註冊虛擬機器）頁籤上傳授權檔案。選取您已部署防火牆的 PAN-OS 版本和 Hypervisor，以完成註冊程序。VM-Series 防火牆的序號會附加至您的帳戶記錄。



5. 導覽至 **Assets**（資產） > **My Devices**（我的裝置），並搜尋剛才註冊的 VM-Series 裝置，然後按一下 **PA-VM** 連結。這會將 VM-Series 授權金鑰下載到用戶端電腦。
6. 將授權金鑰複製到可存取 VM-Series 防火牆網頁介面的電腦，再導覽至 **Device**（裝置） > **Licenses**（授權）。

   必須透過網頁介面安裝授權金鑰。防火牆不支援透過 *SCP* 或 *FTP* 安裝授權金鑰。
7. 按一下 **Manually Upload License**（手動上傳授權）連結並輸入授權金鑰。在防火牆上啟動容量授權時，系統會重新啟動。
8. 登入裝置並確認 **Dashboard**（儀表板）顯示有效的序號，且 **PA-VM** 授權顯示在 **Device**（裝置） > **Licenses**（授權）頁籤中。

啟動 VMware NSX 專用 VM-Series 防火牆的授權

Panorama 作為 VMware NSX 專用 VM-Series 防火牆的中央管理點，當 Panorama 可直接存取網際網路時，授權啟動程序會自動進行。Panorama 連線至 Palo Alto Networks 更新伺服器以擷取授權，在部署新的 NSX 專用 VM-Series 防火牆後，它會與 Panorama 通訊以取得授權。如果 Panorama 未連線網際網路，您需要授權對 VM-Series 防火牆的各實例授權，以便防火牆可連線至 Panorama。

此整合式解決方案的驗證碼（例如 PAN-VM-1000-HV-SUB-BND-NSX2）包含資安威脅、URL 篩選及 WildFire 使用授權的授權，以及要求期間的進階支援。

©2023 Palo Alto Networks, Inc.

若要啟動授權，您必須完成下列工作：

- 已向支援帳戶註冊驗證碼。如果您沒有註冊驗證碼，授權伺服器將無法建立授權。
- 在 Panorama 的 Service Definition（服務定義）中輸入驗證碼。在 Panorama 上，選取 **VMWare Service Manager**（**VMWare** 服務管理員），將 **Authorization Code**（驗證碼）新增至 **VMware Service Definition**（**VMware** 服務定義）。

> 如果您已經購買試用驗證碼，您可以使用 *VM-1000-HV* 容量授權最多授權 *5* 個 *VM-Series* 防火牆，期間達 *30* 或 *60* 天。由於此解決方案可讓您在每個 *ESXi* 主機上部署一個 *VM-Series* 防火牆，因此使用試用授權時，*ESXi* 叢集最多可包含 *5* 個 *ESXi* 主機。

下列啟動授權的程序是手動的。如果您有自動指令碼或協調運作服務，您可以使用授權 API 對擷取 VM-Series 防火牆授權的程序進行自動化設定。

- 當 Panorama 可存取網際網路時在 NSX 上的 VM-Series 防火牆上啟動授權
- 當 Panorama 無法存取網際網路時在 NSX 上的 VM-Series 防火牆上啟動授權
- 授權啟動問題的疑難排解

當 **Panorama** 可存取網際網路時在 **NSX** 上的 **VM-Series** 防火牆上啟動授權

當 Panorama 可存取網際網路時，請完成下列程序來啟動 NSX 專用 VM-Series 防火牆。

STEP 1 | 確認 VM-Series 防火牆已連線至 Panorama。

1. 登入 Panorama。
2. 選取 **Panorama** > **Managed Devices**（受管理的裝置），並確定防火牆顯示為 Connected（已連線）。

STEP 2 | 確認各防火牆已授權。

選取 **Panorama** > **Device Deployment**（裝置部署） > **Licenses**（授權），並確認 Panorama 已比對驗證碼且將授權套用至各防火牆。

如果您沒有看到授權，按一下 **Refresh**（重新整理）。選取您要擷取使用授權的 VM-Series 防火牆，然後按一下 **OK**（確定）。

當 **Panorama** 無法存取網際網路時在 **NSX** 上的 **VM-Series** 防火牆上啟動授權

當 Panorama 無法存取網際網路時，請完成下列程序來啟動 NSX 專用 VM-Series 防火牆。

STEP 1 | 尋找 VM-Series 防火牆的 CPU ID 及 UUID。

1. 從 vCenter 伺服器取得防火牆的 IP 位址。
2. 登入 Web 介面，然後選取 **Dashboard**（儀表盤）。
3. 從 General Information（一般資訊）Widget 取得防火牆的 **CPU ID** 及 **UUID**。

©2023 Palo Alto Networks, Inc.

STEP 2 | 啟動驗證碼並產生授權金鑰。

1. 使用帳戶認證登入 Palo Alto Networks 客戶支援網站。若您需要新帳戶，請參閱建立支援帳戶。
2. 選取 **Assets**（資產） > **VM-Series Auth Codes**（**VM-Series** 授權碼），並按一下 **Add VM-Series Auth Codes**（新增 **VM-Series** 授權碼）以輸入授權碼。
3. 在您剛才註冊的驗證碼相對應的列中選取 **Register VM**（註冊 **VM**），輸入防火牆的 CPU ID 及 UUID，然後按一下 **Submit**（提交）。入口網站將產生防火牆的序號。
4. 選取 **Assets**（資產） > **Devices**（裝置），然後搜尋序號。
5. 按一下 Actions column（動作欄）連結，將各金鑰下載至本機筆記型電腦。除了訂閱授權金鑰，您還必須取得容量授權及支援授權金鑰。

STEP 3 | 上載金鑰至防火牆。

1. 登入防火牆 Web 介面。
2. 選取 **Device**（裝置） > **Licenses**（授權），然後選取 **Manually upload license key**（手動上傳授權金鑰）。
3. **Browse**（瀏覽）以選取金鑰，然後按一下 **OK**（確定），在防火牆上安裝授權。

   首先安裝容量授權金鑰檔案（*pa-vm.*金鑰）。套用容量授權金鑰後，*VM-Series* 防火牆將會重新啟動。啟動時，防火牆有一個序號，您可用於註冊在 *Panorama* 上作為受管理設備的防火牆。
4. 重複該程序在防火牆上安裝各金鑰。
5. 選取 **Dashboard**（儀表盤），並確認您可以看到 General Information（一般資訊）Widget 中的 **Serial #**（序號）。

STEP 4 | 在 Panorama 上新增防火牆的序號。

選取 **Panorama** > **Managed Devices**（受管理的裝置），然後按一下 **Add**（新增）以輸入 NSX 專用 VM-Series 防火牆的序號。防火牆現在應能夠連線 Panorama，以便防火牆取得其組態及原則規則。

授權啟動問題的疑難排解

本節討論啟動授權時最常見的一些問題。

授權沒有足夠記憶體的 PA-VM 會導致類似下列的錯誤：

```
伺服器錯誤：金鑰檢查失敗：資源檢查失敗。所需記憶體：6.5GB，配置記憶體：4.8GB
```

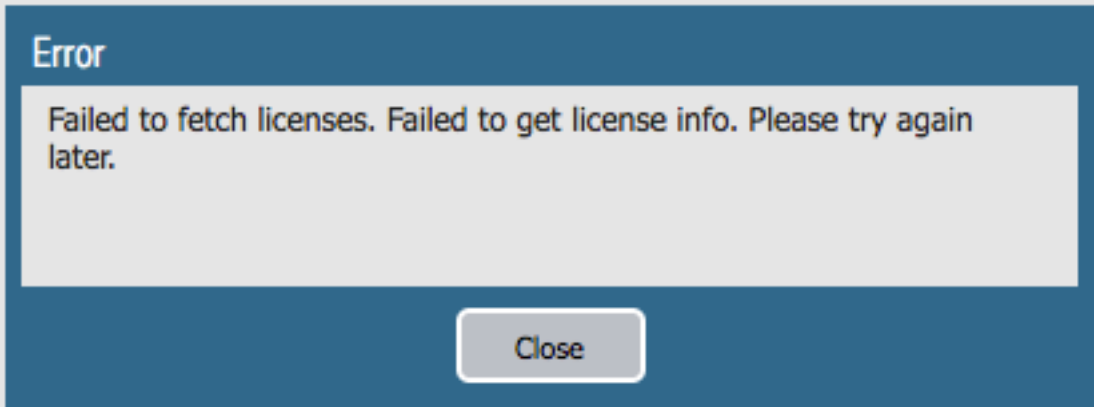
若要修正此問題，請佈建授權所需的額外記憶體，並使用命令 **`request license fetch`** 來擷取授權。

如果您使用任何其他命令，則會失敗並顯示以下錯誤：

```
伺服器錯誤：無法擷取授權：無法將佈建授權功能應用於已佈建的裝置。
```

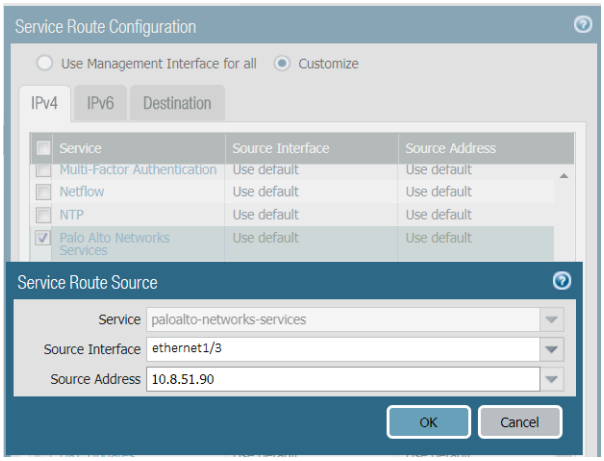

©2023 Palo Alto Networks, Inc.

如果您看到的錯誤指出無法擷取授權。無法取得授權資訊。請稍後再試，或出現一般通訊錯誤訊息。



驗證下列事項：

- 防火牆能夠使用服務路由將流量路由至 Palo Alto Networks 伺服器嗎？依預設，防火牆使用管理介面來存取伺服器。如果您打算使用資料平面介面，請確保您已設定服務路由。



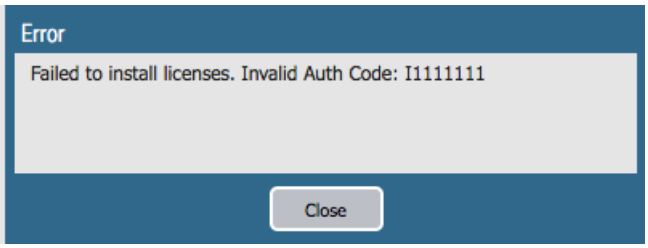
- 在網際網路上路由正常運作嗎？以 SSH 進入防火牆，ping 可公開存取的 IP 位址，例如 4.2.2.2。如果您使用資料平面介面，務必使用 source 選項。例如：ping count 3 source 10.0.1.1 host 4.2.2.2。
- DNS 設定正確嗎？以 SSH 進入防火牆，ping DNS 名稱，例如 google.com。例如：

```
warby@warbylan> ping count 3 source 10.0.1.1 host google.com
PING google.com (216.58.195.78) from 10.0.1.1 : 56(84) bytes of data.
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=1 ttl=55 time=11.6 ms
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=2 ttl=55 time=11.9 ms
64 bytes from sfo07s16-in-f78.1e100.net (216.58.195.78): icmp_seq=3 ttl=55 time=11.5 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 11.586/11.721/11.975/0.200 ms
```


©2023 Palo Alto Networks, Inc.

如果您看到的錯誤指出「無效驗證碼」：



驗證下列事項：

- 您已正確輸入驗證碼。
- 您已在支援入口網站上將驗證碼註冊到您的帳戶。
- 驗證碼尚未達到 VM-Series 防火牆的最大佈建容量。
  - 對於舊版授權，請登入 CSP，然後選取 **Assets**（資產） > **VM-Series Auth-Codes**（**VM-Series** 驗證碼）。
  - 對於軟體 NGFW 積分，如果您知道部署設定檔，請登入 CSP，選取 **Assets**（資產） > **Software NGFW Credits**（軟體 **NGFW** 積分），找出您的設定檔，然後按一下 **Details**（詳細資訊）。

    您也可以選取 **Assets**（資產） > **Software NGFW Devices**（軟體 **NGFW** 裝置），並依驗證碼搜尋。

註冊 VM-Series 防火牆

在您購買 VM-Series 防火牆時，您會收到電子郵件，信中附上 VM-Series 型號的容量授權驗證碼、支援權利驗證碼，以及訂閱授權的一個或多個驗證碼。若要使用驗證碼，您必須向 Palo Alto Network 客戶支援網站上的支援帳戶註冊該驗證碼。使用 VMware 整合式 NSX 解決方案時，電子郵件中會包含一個驗證碼、支援權利及一或多個訂閱授權，該驗證碼搭售 VM-Series 型號一或多個實例的容量授權。

在公共雲端（AWS、Azure、Google Cloud Platform）內依使用授權，則您不會收到驗證碼。然而，若要啟動 Palo Alto Networks 的升級支援權利，您必須建立一個支援帳戶，並在 Palo Alto Networks 客戶支援網站上註冊 VM-Series 防火牆。

依照本節的指示，使用您的支援帳戶來註冊容量驗證碼或防火牆。

- 註冊 VM-Series 防火牆（軟體 NGFW 積分）
- 註冊 VM-Series 防火牆（使用驗證碼）
- 註冊依使用授權版公共雲端專用 VM-Series 防火牆（無驗證碼）

註冊 VM-Series 防火牆（使用驗證碼）

請完成下列程序，使用驗證碼來註冊 VM-Series 防火牆。

STEP 1 | 使用帳戶認證登入 Palo Alto Networks 客戶支援網站。視需要建立支援帳戶。

STEP 2 | 選取 **Assests**（資產） > **VM-Series Auth-Codes**（**VM-Series** 驗證碼） > **Add VM-Series Auth-Code**（新增 **VM-Series** 驗證碼）。

©2023 Palo Alto Networks, Inc.

STEP 3 | 在 **Add VM-Series Auth-Code**（新增 **VM-Series** 驗證碼）欄位中，輸入您以電子郵件接收的容量驗證碼，再按一下最右側的核取記號以儲存輸入。頁面隨即顯示註冊至您支援帳戶的驗證碼清單。

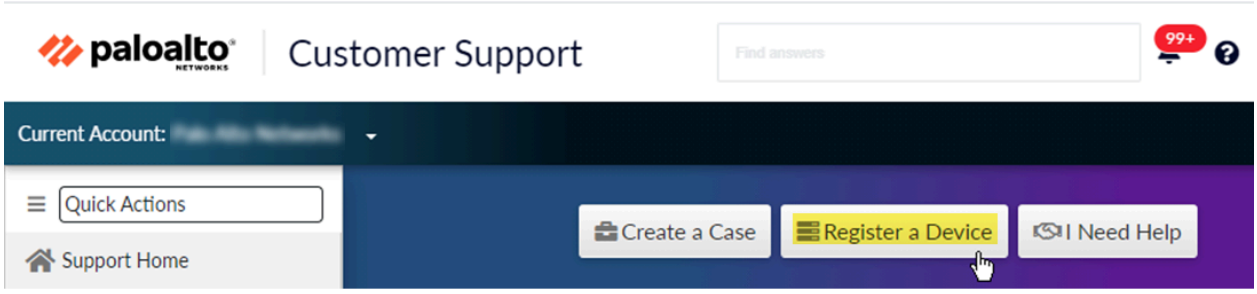
您可以追蹤已部署的 VM-Series 防火牆數目，及仍可針對每個驗證碼使用的授權數目。使用所有可用的授權時，不會在 VM-Series Auth-Codes（VM-Series 驗證碼）頁面上顯示驗證碼。若要檢視所有部署的資產，請選取 **Assets**（資產） > **Devices**（裝置）。

註冊依使用授權版公共雲端專用 VM-Series 防火牆（無驗證碼）

若要在 Palo Alto Networks Customer Support Portal（客戶支援入口網站；CSP）上註冊基於使用量的防火牆，您可以使用自動註冊或手動註冊。自動註冊基於使用量的防火牆可讓您在啟動防火牆時立刻無縫註冊防火牆，並存取與 CSP 帳戶相關聯的網站授權權利。如需詳細資料，請參閱在 VM-Series 防火牆上安裝裝置憑證。

使用下列工作流程來手動註冊 VM-Series 防火牆。開始手動註冊程序之前，請先登入 VM-Series 防火牆，並記下儀表板上的序號和 CPU ID（UUID 是選用）。

STEP 1 | 登入 Palo Alto Networks 客戶支援網站，按一下 **Assets**（資產） > **Devices**（裝置） > **Register New Devices**（註冊新的裝置）。

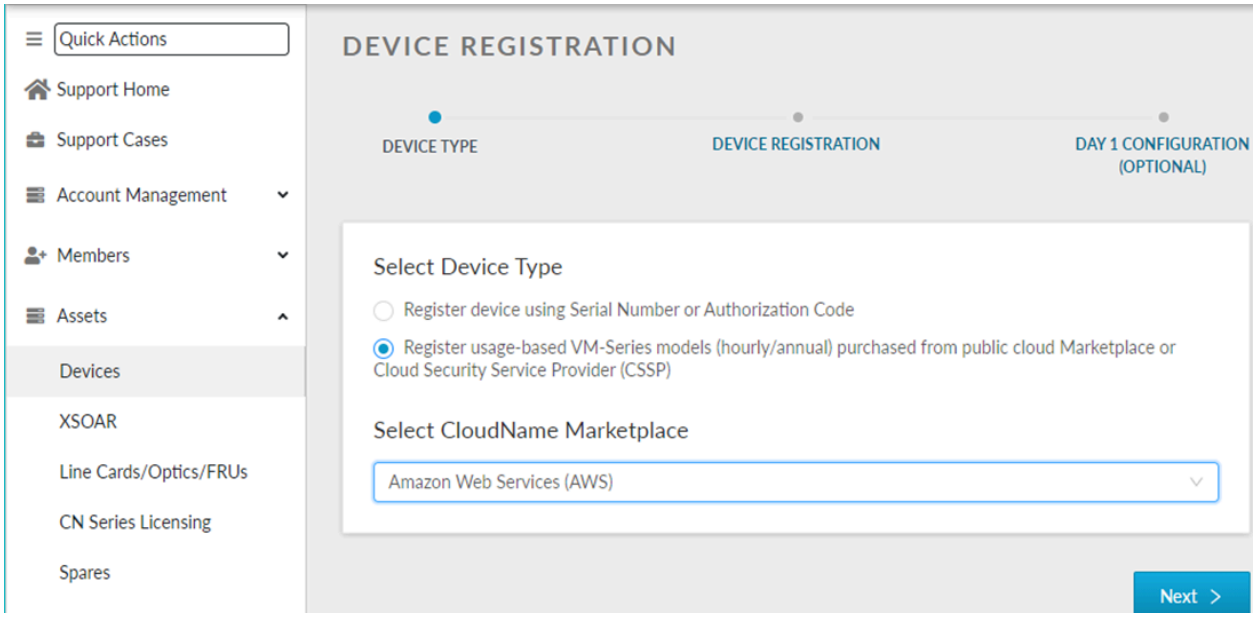


1. 選取 **Register usage-based VM-Series models (hourly/annual) purchased from public cloud Marketplace**（註冊從公共雲端 **Marketplace** 購買的基於使用量 **VM-**

©2023 Palo Alto Networks, Inc.

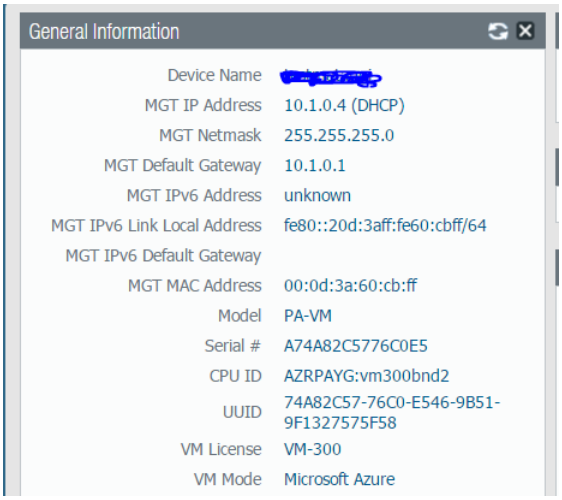
Series 型號（每小時/每年）或 **Cloud Security Service Provider**（雲端安全服務供應商；**CSSP**））。

2. 選取 **Cloud Marketplace**（雲端 **Marketplace**）廠商，然後按一下 **Next**（下一步）。



STEP 2 | 輸入 VM-Series 防火牆的 **Serial #**（序號）、**CPU ID** 和 **UUID**。

例如，從 VM 上的 VM-Series 防火牆儀表板，您會看到下列資訊。



如果您打算離線使用防火牆，請選取 ***Offline***（離線）核取方塊，並輸入您打算使用的 *PAN-OS* 版本。

STEP 3 | **Agree and Submit**（同意和提交），以接受 EULA 並註冊防火牆。

STEP 4 | 確認您購買的授權詳細資訊出現在 CSP 的 **Assets**（資產）頁面。

©2023 Palo Alto Networks, Inc.

在 VM-Series 防火牆上安裝裝置憑證

防火牆需要裝置憑證，才能擷取網站授權權益及安全地存取雲端服務，例如 WildFire、AutoFocus 和 Cortex Data Lake。有兩種方法可將網站授權套用至 VM-Series 防火牆：一次性密碼 - OTP 和自動註冊 PIN。每個密碼或 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。您使用的方法取決於用來部署防火牆的授權類型，以及防火牆是否由 Panorama 管理。

- 一次性密碼—對於已向 Palo Alto Networks 授權伺服器註冊的 VM-Series 防火牆，您必須在客戶支援入口網站上產生一次性密碼 - OTP，並套用至 VM-Series 防火牆。此方法適用於小規模未受管理部署中採用 BYOL 或 ELA 授權的 VM-Series 防火牆，以及由 Panorama 管理的手動部署 VM-Series 防火牆。
- 註冊 PIN—此方法可讓您在 VM-Series 防火牆初次啟動時套用網站授權。此方法適用於採取用量型授權 (PAYG)、在啟動時啟動載入或採用任何一種自動化部署的 VM-Series 防火牆，而不論授權類型。自動註冊 PIN 可讓您在啟動時自動向 CSP 註冊用量型防火牆，並擷取網站授權。

對於 NSX-T 上的 VM-Series 防火牆，您可以將自動註冊 PIN 新增至服務定義設定，以便防火牆在初次啟動時擷取裝置憑證。如需詳細資訊，請參閱 NSX-T（南北向）和 NSX-T（東西向）的服務定義設定。如果您將先前部署的防火牆升級到支援裝置憑證的 PAN-OS 版本，您可以使用 一次性密碼 - OTP，將裝置憑證個別地套用至這些防火牆。

一次性密碼和自動註冊 PIN 必須於到期之前使用。否則，您必須返回 CSP 來產生新的密碼和 PIN。

讓防火牆在啟動時自動擷取網站授權。

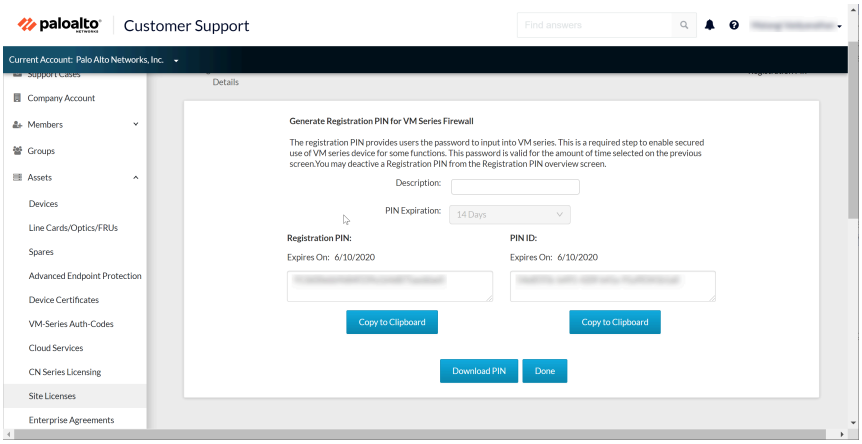
防火牆需要裝置憑證，才能取得網站授權權益及安全地存取雲端服務。若要在啟動防火牆時擷取網站授權，您必須在啟動套件的 /license 資料夾中包含驗證碼，並在 init-cfg.txt 檔案中新增

©2023 Palo Alto Networks, Inc.

自動註冊 PIN ID 和值，然後放入 /config 資料夾中。新增自動註冊 PIN ID 和值也會自動註冊 VM-Series 防火牆上的 PAYG 或用量型實例。

1. 登入客戶支援入口網站 (CSP)。
2. 產生 VM-Series 註冊 PIN。

   選取 **Assets**（資產） > **Device Certificates**（裝置憑證） > **Generate Registration PIN**（產生註冊 **PIN**）。儲存 PIN ID 和值。務必在 PIN 過期之前啟動防火牆。

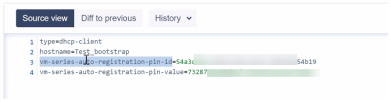


3. 在 init-cfg.txt 檔案中新增註冊 PIN ID 和值。

   除了必要參數，還必須包含：

```
vm-series-auto-registration-pin-id=
```

```
vm-series-auto-registration-pin-value=
```



4. 登入防火牆，確認您在防火牆上可以看到網站授權。

©2023 Palo Alto Networks, Inc.

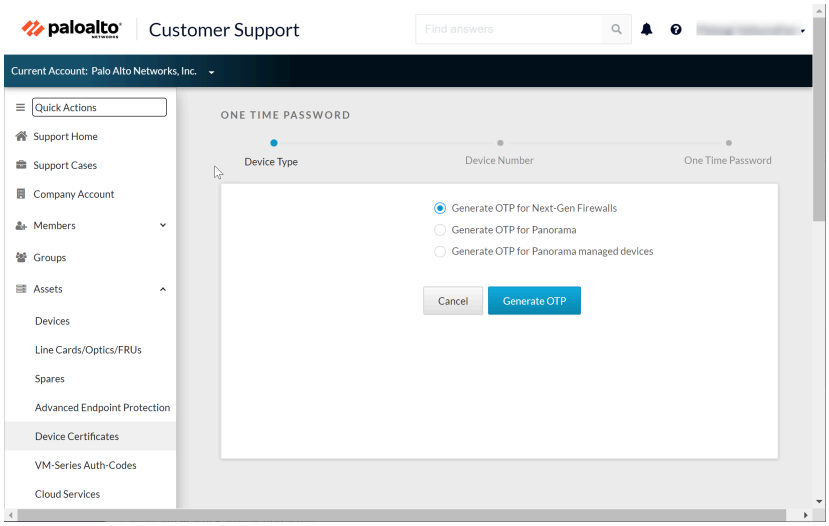
產生一次性密碼 - OTP，並在防火牆上手動擷取裝置憑證。

防火牆需要此裝置憑證，才能取得網站授權權益及安全地存取雲端服務。

1. 登入客戶支援入口網站。

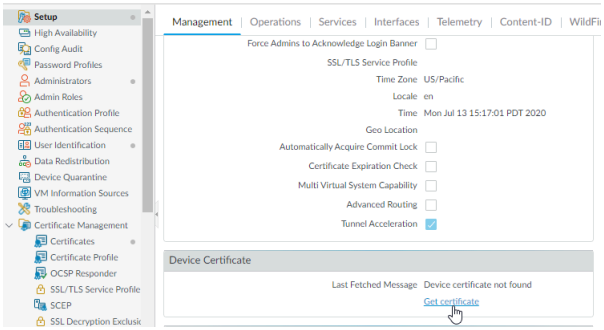
   如果尚未註冊 VM-Series 防火牆，請這麼做。

2. 選取 **Assets**（資產） > **Device Certificates**（裝置憑證） > **Generate OTP**（產生 **OTP**）。



3. 從清單中選取防火牆來 **Generate OTP**（產生 **OTP**）。
4. 登入防火牆並擷取裝置憑證。

   選取 **Setup**（設定） > **Management**（管理） > **Device Certificate**（裝置憑證）和 **Get Certificate**（取得憑證）



5. 確認已擷取裝置憑證，而且在防火牆上可以看到網站授權。

如果使用 Panorama 來管理 VM-Series 防火牆，請參閱在受管理的防火牆上安裝裝置憑證。

在 BYOL 和 PAYG 授權之間切換

VM-Series 防火牆無法在 BYOL 和 PAYG 授權選項之間轉換。如果您已在 AWS、Azure 或 Google Cloud Platform 中以 PAYG 或 BYOL 選項部署 VM-Series 防火牆，而現在想要切換至另一個選項，請依照下列指示儲存並匯出現有防火牆的組態、部署新的防火牆，然後將設定還原到新的防火牆。

©2023 Palo Alto Networks, Inc.

STEP 1 | 將目前組態的備份儲存到外部伺服器。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後 **Export named configuration snapshot**（匯出具名設定快照）。
2. 選取包含執行中組態的 XML 檔案（例如 running-config.xml），然後按一下 **OK**（確定）匯出組態檔案。
3. 將匯出的檔案儲存至防火牆外部的位置。

STEP 2 | 部署新的防火牆，並依情況註冊或啟動授權。

若為新的 PAYG 實例：

1. 在 AWS、Azure 或 Google Cloud Platform Marketplace 中，針對您要部署的 PAYG 授權搭售包選取軟體映像。
2. 在 AWS、Azure 或 Google 公共雲端部署新的 VM-Series 防火牆。請參閱設定 AWS 上的 VM-Series 防火牆、設定 Azure 上的 VM-Series 防火牆或設定 Google Cloud Platform 上的 VM-Series 防火牆。
3. 註冊依使用授權版公共雲端專用 VM-Series 防火牆（無驗證碼）。

若為新的 BYOL 實例：

1. 聯絡業務代表或經銷商來購買 BYOL 授權，並取得 BYOL 驗證碼以用來授權您的防火牆。
2. 註冊 VM-Series 防火牆（使用驗證碼）。
3. 在 AWS 或 Azure 公共雲端部署新的 VM-Series 防火牆。請參閱設定 AWS 上的 VM-Series 防火牆、設定 Azure 上的 VM-Series 防火牆或設定 Google Cloud Platform 上的 VM-Series 防火牆。
4. 啟動 VM-Series 防火牆的授權（獨立版本）。

STEP 3 | 在新部署的防火牆上，還原您匯出的組態。

1. 存取新部署之防火牆的網頁介面。
2. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），並按一下 **Import named configuration snapshot**（匯入具名設定快照）、[Browse（瀏覽）] 至外部主機上的設定檔案，然後按一下 **OK**（確定）。
3. 按一下 **Load named configuration snapshot**（上載具名組態快照），選取您剛才匯入的組態 **Name**（名稱），然後按一下 **OK**（確定）。
4. 按一下 **Commit**（提交），使用您剛才匯入的快照覆寫執行中組態。
5. 在刪除防火牆或停用被取代防火牆上的授權之前，確認新防火牆上的組態符合您要取代的防火牆。

切換 VM-Series 型號授權

您可以使用 BYOL 選項切換目前部署的 VM-Series 防火牆的授權。例如，您可以從訂閱搭售包移至企業授權合約 (ELA)，反之亦然，而不會中斷通過防火牆的流量。您也可以從 Panorama 在個別防火牆上切換授權，或同時在多個防火牆上切換授權。

請勿使用此程序在 *PAYG* 與 *BYOL* 之間切換 *ELA* 或永久授權。如需詳細資訊，請參閱在 BYOL 和 PAYG 授權之間切換。

©2023 Palo Alto Networks, Inc.

完成下列其中一個程序，以執行下列其中一個授權變更：

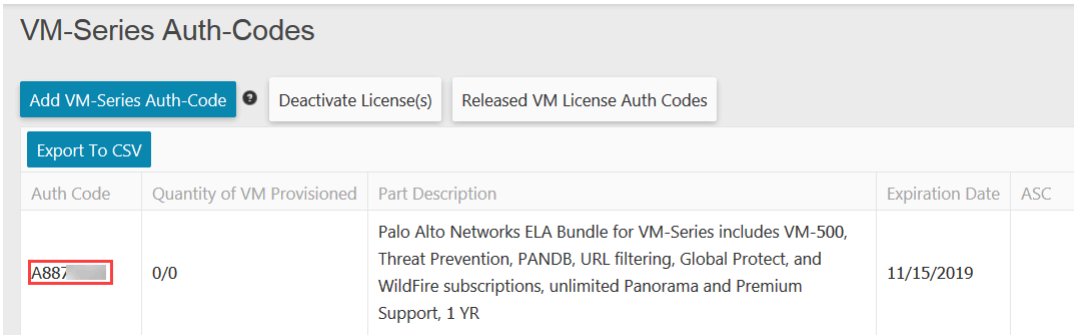
- 訂閱搭售包 1 到訂閱搭售包 2
- 訂閱搭售包 1 或 2 到 ELA
- 容量授權到訂閱搭售包或 ELA

切換至 ELA 授權之前，您必須配置足夠權杖來支援目前部署的 VM-Series 防火牆數目。如需每個 VM-Series 型號所需權杖的詳細資訊，請參閱VM-Series 企業授權合約（多重型號 ELA）。

切換獨立防火牆上的授權。

1. 註冊授權碼。
   - 針對訂閱搭售包，註冊新授權碼。
   - 針對 ELA，請啟動 ELA 授權碼。

   不要使用 *ELA* 授權碼來啟動單一 *VM-Series* 防火牆。註冊 *ELA* 之後，請使用 *VM-Series* 型號授權碼來啟動個別防火牆。您可以在客戶支援入口網站的 ***Assets***（資產） **> *VM-Series Auth-Codes***（***VM-Series*** 授權碼） 下找到這些授權碼。
2. 登入 VM-Series 防火牆網頁介面。
3. 驗證 Palo Alto Networks 更新伺服器設定。
   1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務）。
   2. 確認 **Update Server**（更新伺服器）設定為 updates.paloaltonetworks.com。
   3. 確認已選取 **Update Server Identity**（更新伺服器識別）。
4. 套用 VM-Series 授權碼。ELA 的防火牆授權碼開頭為字母 A，如下所示。

   1. 選取 **Device**（裝置） > **Licenses**（授權），並選取 **Activate feature using authentication code**（使用授權碼啟動功能）連結。
   2. 輸入 VM-Series 授權碼。
   3. 按一下 **OK**（確定），以確認授權升級。防火牆會聯絡 Palo Alto Networks 更新伺服器，並根據 VM-Series 型號使用防火牆所需的權杖。
   4. 檢查授權到期日，驗證已成功更新授權。
5. 針對部署中的每個 VM-Series 防火牆，重複此程序。

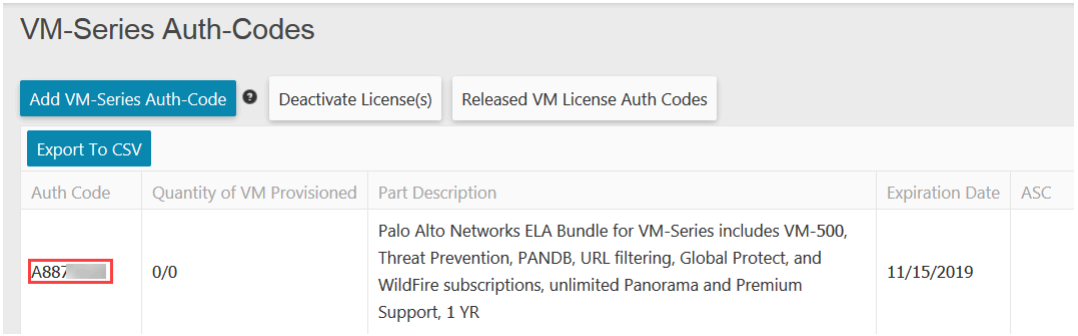
©2023 Palo Alto Networks, Inc.

使用 Panorama，切換受管理防火牆上的授權。

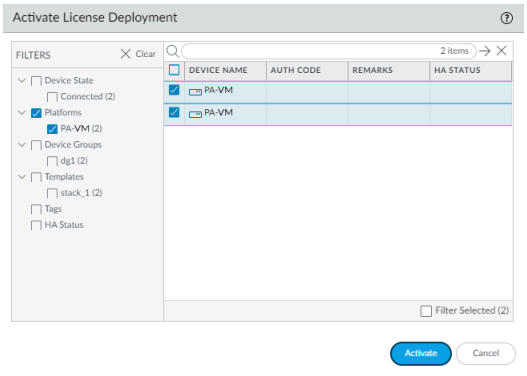
1. 註冊授權碼。
   - 針對訂閱搭售包，註冊新授權碼。
   - 針對 ELA，請啟動 ELA 授權碼。

   > 不要使用 *ELA* 授權碼來啟動單一 *VM-Series* 防火牆。註冊 *ELA* 之後，請使用 *VM-Series* 型號授權碼來啟動個別防火牆。您可以在客戶支援入口網站的 ***Assets***（資產） **> *VM-Series Auth-Codes***（***VM-Series*** 授權碼） 下找到這些授權碼。

2. 登入 Panorama 網頁介面。
3. 驗證防火牆的 Palo Alto Networks 更新伺服器設定。
   1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務）。
   2. 確認 **Update Server**（更新伺服器）設定為 updates.paloaltonetworks.com。
   3. 確認已選取 **Update Server Identity**（更新伺服器識別）。
4. 套用 VM-Series 授權碼。ELA 的防火牆授權碼開頭為字母 A，如下所示。



   1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Licenses**（授權），然後按一下 **Activate**（啟動）。
   2. 輸入 VM-Series 授權碼。
   3. 使用篩選，以選取要授權的受管理防火牆。
   4. 在每個防火牆的 **Auth Code**（授權碼）欄中，輸入授權碼。
   5. 按一下 **Activate**（啟動），以確認授權升級。Panorama 會聯絡 Palo Alto Networks 更新伺服器，並根據 VM-Series 型號使用防火牆所需的權杖。



©2023 Palo Alto Networks, Inc.

6. 檢查授權到期日，驗證已成功更新授權。

停用授權

授權停用程序可讓您自行管理授權。無論您要移除一個或多個有效授權或指定給防火牆的使用授權（基於硬體的防火牆或 VM-Series 防火牆），還是要停用 VM-Series 防火牆及取消指派所有有效授權及使用授權，請在防火牆或 Panorama（並非在 Palo Alto Networks 客戶支援網站上）開始停用程序。

為了成功停用授權，您必須安裝停用 API 金鑰，並啟用更新伺服器識別的驗證（預設為啟用）。PAN-OS 會使用此停用 API 金鑰向所有更新授權服務進行驗證。如果防火牆和授權伺服器之間沒有連線，則手動停用授權不需要此停用 API 金鑰。

如果防火牆/Panorama 可存取網際網路，並且可與 Palo Alto Networks 授權伺服器通訊，則按一下按鈕即可自動完成授權移除程序。如果防火牆/Panorama 無法存取網際網路，您必須使用兩步程序，手動完成程序。在第一步中，從防火牆或 Panorama 產生及匯出一個包含停用金鑰資訊的語彙基元檔案。在第二步中，登入 Palo Alto Networks 客戶支援網站後，上傳權杖檔案，將授權金鑰與防火牆解除關聯。

- 使用 CLI 停用功能授權或使用授權
- 停用 VM

使用 CLI 停用功能授權或使用授權

如果在防火牆上安裝授權/訂閱，但需要重新指派給另一個防火牆，您可以停用個人授權，然後在另一防火牆上重新使用同一授權碼，而無須求助技術支援。僅 CLI 中支援此功能，執行 PAN-OS 的實體和虛擬裝置都支援此功能。此程序通常用於固定型號永久授權或 ELA 授權。

- 網際網路存取（自動模式）
- 無法存取網際網路（手動模式）

網際網路存取（自動模式）

STEP 1 | 登入防火牆的 CLI。

STEP 2 | 針對您要停用的功能，檢視授權金鑰的名稱。

```
request license deactivate key features
```

STEP 3 | 停用授權或訂閱。

使用自動模式移除授權金鑰。

```
request license deactivate key features <name> mode auto
```

name 是授權金鑰檔案的全名。例如：

```
admin@vmPAN2> request license deactivate key features <name>
```

```
WildFire_License_2015_01_28_I5820573.key mode auto007200002599
 WildFire 授權成功 已成功刪除授權金鑰
```


©2023 Palo Alto Networks, Inc.

無法存取網際網路（手動模式）

使用手動模式移除授權金鑰，並為基於型號的授權產生授權權杖。此程序假設您已在防火牆上安裝授權 API 金鑰。

STEP 1 | 登入防火牆的 CLI。

STEP 2 | 針對您要停用的功能，檢視授權金鑰的名稱。

```
request license deactivate key features
```

STEP 3 | 從命令列手動停用授權。

```
request license deactivate key features <name> mode manual
```

例如：

```
admin@PA-VM> request license deactivate key features
```

```
PAN_DB_URL_Filtering_2015_01_28_I6134084.key mode manual
 Successfully removed license keys dact_lic.01282015.100502.tok
```

權杖檔案採用 `dact_lic.timestamp.tok`，格式，其中 timestamp 採用 `dmmyyyy.hrminsec` 格式。

STEP 4 | 確認語彙基元檔案產生。

```
show -token-files
```

STEP 5 | 匯出權杖檔案。

將此命令輸入成一行：

```
scp export license-token-file to <username@serverIP>
from <token_filename>
```

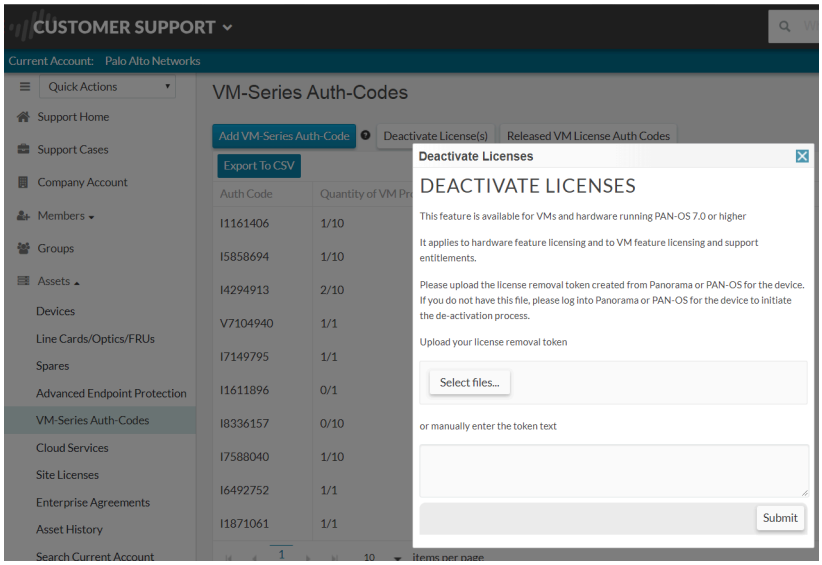
例如：

```
scp export license-token-file to admin@10.1.10.55:/tmp/ from
dact_lic.01282015.100502.tok
```


©2023 Palo Alto Networks, Inc.

STEP 6 | 登入 Palo Alto Networks 客戶支援入口網站。

1. 在 **Assets**（資產）頁籤上，按一下 **Deactivate License(s)**（停用授權）連結。
2. 選取 **Assets**（資產） > **VM-Series Auth-Codes**（**VM-Series** 驗證碼），然後選取 **Deactivate License(s)**（停用授權）。
3. 上傳權杖檔案以完成停用。



停用 VM

不再需要 VM-Series 防火牆的 BYOL 實例時，您可以在防火牆或 Panorama 上，從網頁介面、CLI 或 XML API，釋放所有現用授權（訂閱授權、基於型號的容量授權及支援權利）。授權會記入您的帳戶，以便您在 VM-Series 防火牆的不同實例上使用同一驗證碼。

停用 VM 將移除所有授權/權利，並將 VM-Series 防火牆置於未授權狀態；防火牆沒有序號並且僅支援最低數量的工作階段。由於防火牆上的組態完好無缺，您可以重新套用一組授權，並視需在防火牆上復原完整功能。



刪除 ***VM-Series*** 防火牆之前，務必停用授權。如果您在停用授權之前刪除防火牆，則有兩個選項：

受 ***Panorama*** 管理—從 *Panorama* 停用授權。

不受 ***Panorama*** 管理—聯絡 Palo Alto Networks 客戶支援來協助您停用。

- 從防火牆停用 VM
- 從 Panorama 停用 VM

從防火牆停用 VM

完成下列程序，以透過防火牆停用 VM 授權。

STEP 1 | 登入網頁介面，然後選取 **Device**（裝置） > **Licenses**（授權）。

STEP 2 | 在 [License Management（授權管理）] 區段中，選取 **Deactivate VM**（停用 **VM**）。

©2023 Palo Alto Networks, Inc.

您只能在 VM 上看到此選項。實體防火牆上沒有此選項。

STEP 3 | 驗證將在防火牆上停用的授權/權利清單。

STEP 4 | 選取下列選項之一開始停用 VM：

- （經由網際網路存取 Palo Alto Networks 授權伺服器）選取 **Continue**（繼續）。

  系統將提示您重新啟動防火牆；重新啟動時，授權就會停用。

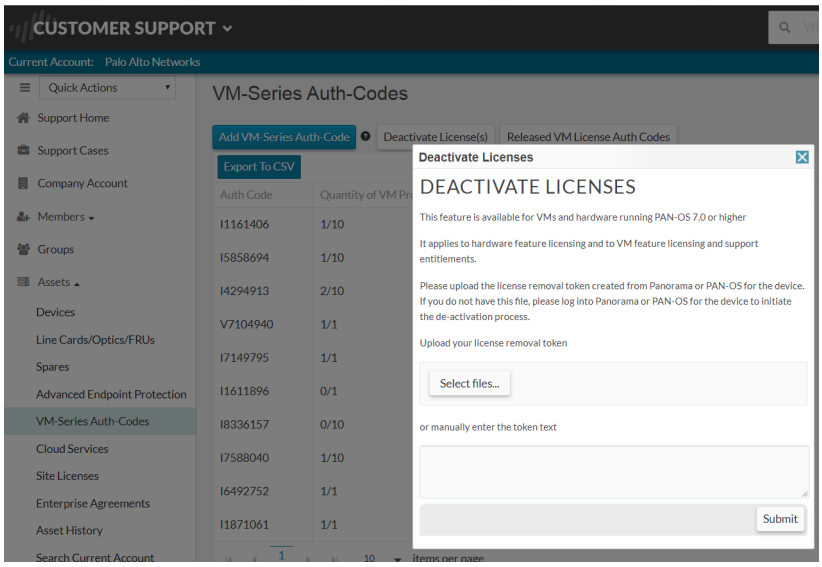
- （無網際網路）—選取 **Complete Manually**（手動完成）。

  按一下 **Export license token**（匯出授權語彙基元）連結，將語彙基元檔案儲存至本機電腦。以下是權杖檔名範例：20150128_1307_dact_lic.01282015.130737.tok

  系統將提示您重新啟動防火牆；重新啟動時，授權就會停用。

STEP 5 | （手動程序 —無網際網路）使用權杖檔案向授權伺服器註冊變更：

1. 登入 Palo Alto Networks 客戶支援網站。
2. 選取 **Assets**（資產） > **VM-Series Auth-Codes**（**VM-Series** 驗證碼） > **Deactivate License(s)**（停用授權）。
3. 登入 Palo Alto Networks 客戶支援網站後，上傳權杖檔案以完成停用程序。



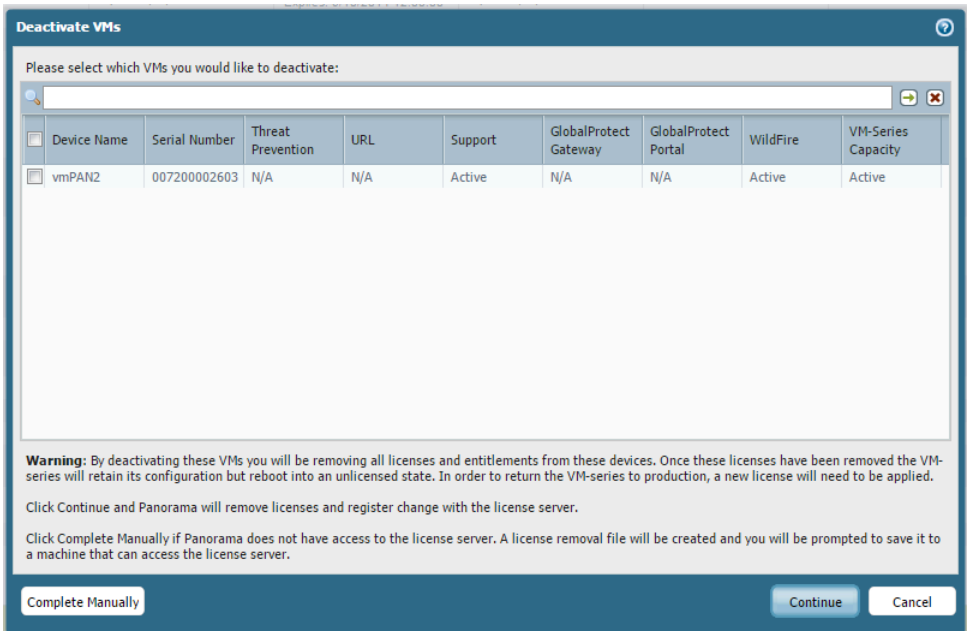
從 **Panorama** 停用 **VM**

完成下列程序，以透過 Panorama 停用 VM 授權。

STEP 1 | 登入 Panorama Web 介面，然後選取 **Panorama** > **Device Deployment**（裝置部署） > **Licenses**（授權）。

©2023 Palo Alto Networks, Inc.

STEP 2 | **Deactivate VMs**（停用 **VM**），並選取您要停用的 VM-Series 防火牆。

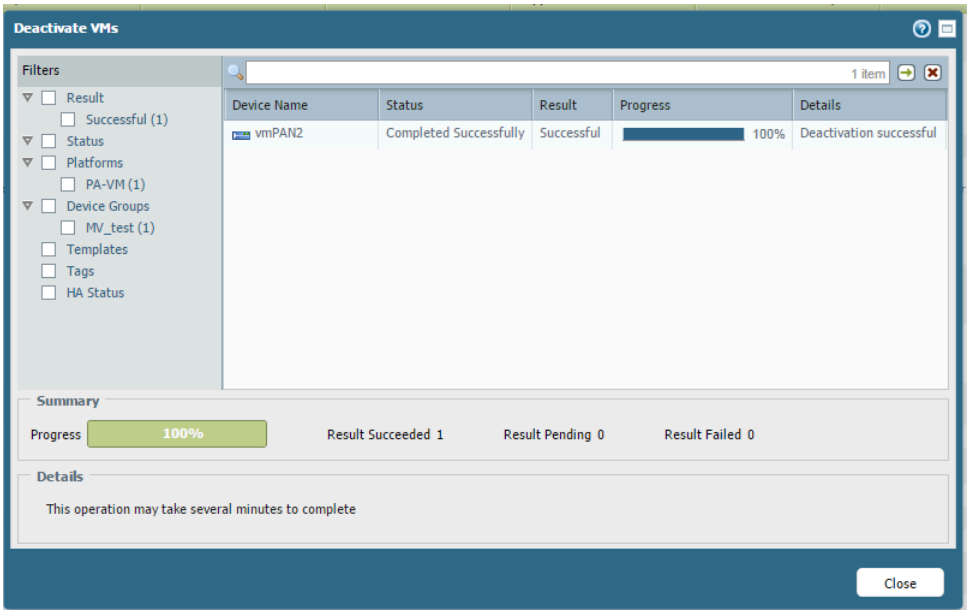


STEP 3 | 選取下列選項之一以停用 VM：

- **Continue**（繼續）#如果 Panorama 可直接與 Palo Alto Networks 授權伺服器通訊，且可註冊變更。若要確認防火牆上已停用授權，請選取 **Refresh on Panorama**（在 **Panorama** 上重新整理） > **Device Deployment**（裝置部署） > **Licenses**（授權）。防火牆將自動重新啟動。
- **Complete Manually**（手動完成）# 如果 Panorama 無法存取網際網路，Panorama 會產生權杖檔案。

  按一下 **Export license token**（匯出授權語彙基元）連結，將語彙基元檔案儲存至本機電腦。以下是權杖檔名範例：20150128_1307_dact_lic.01282015.130737.tok

  螢幕上會顯示成功完成訊息，防火牆將自動重新啟動。



 ©2023 Palo Alto Networks, Inc.

STEP 4 | （僅手動程序 — 無網際網路）使用權杖檔案向授權伺服器註冊變更。

1. 登入 Palo Alto Networks 客戶支援網站。
2. 選取 **Assets**（資產） > **VM-Series Auth-Codes**（**VM-Series** 驗證碼） > **Deactivate License(s)**（停用授權）。
3. 上傳權杖檔案以完成停用。

STEP 5 | 移除作為 Panorama 上受管理設備的已停用 VM-Series 防火牆。

1. 選取 **Panorama** > **Managed Devices**（受管理的裝置）。
2. 從受管理的設定清單中，選取您要移除的防火牆，然後按一下 **Delete**（刪除）。

請不要刪除防火牆，如果您願意，您可以建立單獨的設備群組，並將停用的 *VM-Series* 防火牆指派給此設定群組。

更新 VM 系列防火牆授權搭售包

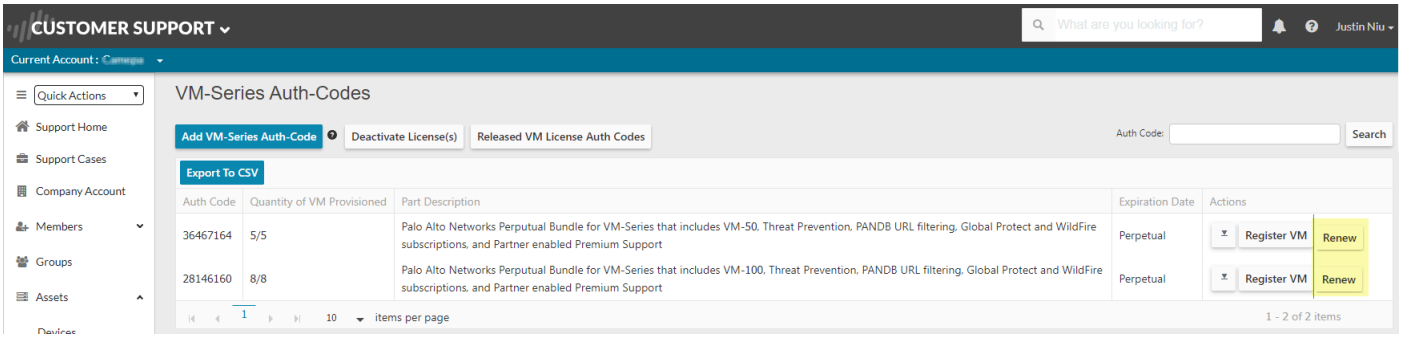
當您的 VM 系列防火牆搭售包授權到期時，您可登入 Palo Alto Networks 客戶支援入口網站並調整授權數量以滿足您的部署需求。更新時，您可檢閱您的使用趨勢並根據您的未來需求，從下列選項中進行選擇：

- **Renew**（更新）—您可選擇按現狀更新所有授權，或者增加或減少授權數量。如果您減少所需的授權數量，則必須獲取未更新的防火牆的基本搭售包，否則您將失去未更新的部分。如果您增加授權數量，新增的授權將新增至您現有的授權碼。
- **Change to Basic Bundle**（變更為基本搭售包）—如果您擁有包含訂閱的 VM 系列搭售包 1 或搭售包 2 授權，可變更為包含永久容量授權和支援權利的基本搭售包。當您切換至基本搭售包時，將保留之前購買的 VM 系列防火牆型號。目前已部署並與現有驗證碼相關聯的所有防火牆將繼續運作，且支援權利將具有新的到期日期。對於任何未佈建的防火牆，您將收到一個新的驗證碼以用來部署新實例。
- **Forfeit**（放棄）—放棄您不再需要的授權。如果您部署了不想更新的防火牆，則您需要選取您想要停止更新之實例的序號。您可透過目前安裝的軟體與內容版本繼續使用這些防火牆實例，但您的訂閱及支援權利將不再有效。因此，若要放棄您尚未佈建的 VM-Series 防火牆的授權，只需要選取您要放棄的數量。

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

STEP 2 | 選取 **Assets**（資產） > **VM-Series Auth-Codes**（**VM-Series** 驗證碼）並找到您想要更新的驗證碼。

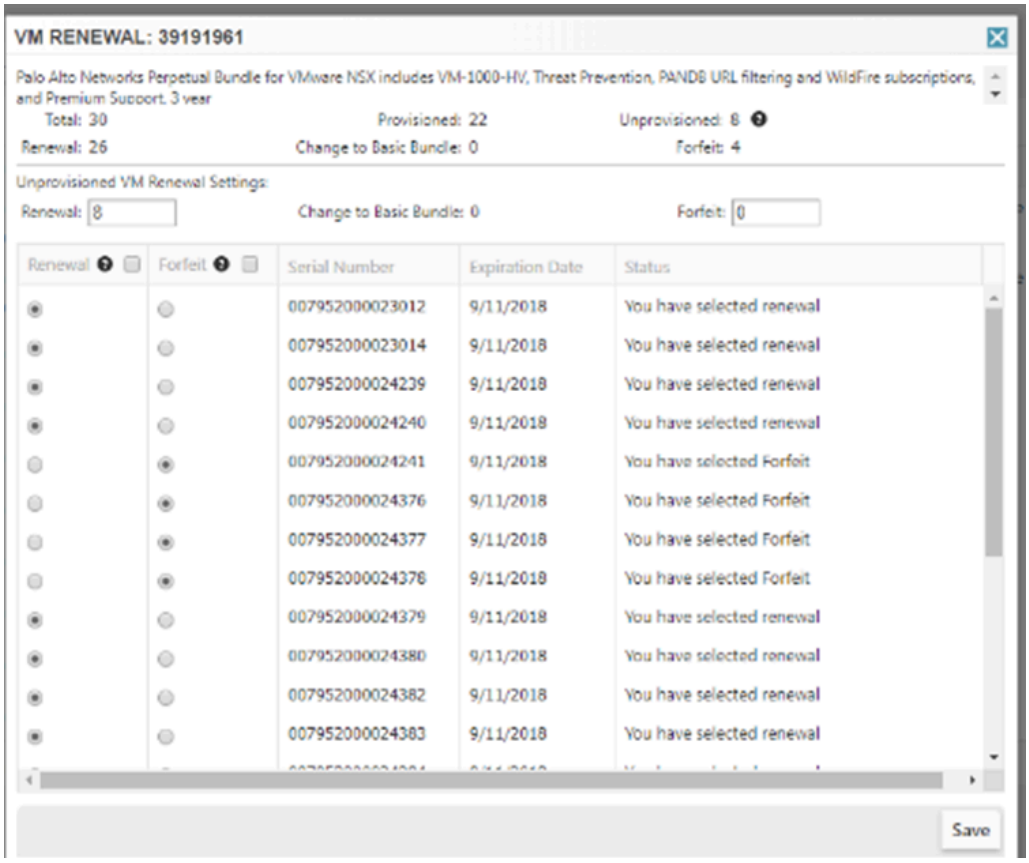
Renew（更新）選項顯示符合更新資格的驗證碼。



 ©2023 Palo Alto Networks, Inc.

STEP 3 | 按一下 **Renew**（更新）連結以選取 **Renew**（更新）、**Change to Basic Bundle**（變更為基本搭售包）或 **Forfeit**（放棄）的序號。

如果您已佈建防火牆，則請選取列中對應至序號的適當選項。如果您有未佈建的防火牆實例，則請在 **Unprovisioned VM Renewal Settings**（未佈建的 **VM** 更新設定）下方選取每個所選擇更新選項的數量。



STEP 4 | **Save**（儲存）變更。

您將收到變更已提交進行處理的螢幕確認資訊。提交變更之後，如果您再次選取 [Renew（更新）]，則可以檢視每個序號的要求狀態。如果更新處理已開始，而您需要進行其他修訂，則會無法儲存變更。如需協助，您可以使用 renewals@paloaltonetworks.com 聯絡更新團隊。

©2023 Palo Alto Networks, Inc.

當授權到期時會怎麼樣？

Palo Alto Networks VM-Series 防火牆和訂閱為防火牆提供新增功能和/或存取 Palo Alto Networks 雲端提供的服務。如果授權在 30 天內到期，系統日誌中會每天顯示一條警告訊息，直到訂閱更新或到期為止。授權到期後，某些訂閱將繼續以有限的容量運行，而另一些訂閱將完全停止運行。您可在此處瞭解每個訂閱到期後會怎麼樣。

授權到期的確切時間是到期日第二天凌晨 *12:00* 點 *(GMT)*。例如，如果您的授權排程於 *1* 月 *20* 日結束服務，則您在當天剩餘時間內可以使用功能。在新的一天起始之際，即 *1* 月 *21* 日凌晨 *12:00* 點 *(GMT)*，授權將到期。無論防火牆上設定的時區為何，所有授權相關功能都按照格林威治標準時間 *(GMT)* 運作。

授權	到期行為
VM-Series	您仍可以： 您可以繼續配置和使用在授權到期之前部署的防火牆，而工作階段容量不會發生變化。防火牆不會自動重新啟動並導致流量中斷。 但是，如果防火牆因任何原因重新啟動，防火牆將進入未授權狀態。在未授權狀態下，支援的工作階段數限制為 1200。沒有其他管理平面功能或設定選項受到限制。
威脅防禦	系統日誌中顯示警示，表明授權已過期。 您仍可以： · 使用授權到期時安裝的特徵碼，除非您使用手動方式或作為自動排程的一部分安裝新的僅針對應用程式的內容更新。如果是後者，此更新將刪除您現有的威脅特徵碼，且您將不再獲得針對它們的保護。 · 使用和修改自訂 App-ID™ 和威脅威脅。 您不可再： · 安裝新的特徵碼。 · 將特徵碼降至以前的版本。
DNS 安全性	您仍可以： · 如果您具有有效的威脅防護授權，請使用本機的 DNS 特徵碼。 您不可再： · 取得新的 DNS 特徵碼。
進階 URL 篩選/URL 篩選	您仍可以：

©2023 Palo Alto Networks, Inc.

授權	到期行為
	· 使用自訂 URL 類別強制執行原則。 · 當授權過期時，使用本機快取中的 PAN-DB 類別強制執行原則。 您不可再： · 獲取有關快取的 PAN-DB 類別的更新。 · 連線至 PAN-DB URL 篩選資料庫。 · 獲取未快取 URL的 PAN-DB 類別。 · 使用進階 URL 篩選即時分析 URL 要求。
WildFire	您仍可以： · 轉送 PE 進行分析。 · 如果您具有有效的威脅防護訂閱，則每 24-48 小時獲取一次特徵碼更新。 您不可再： · 透過 WildFire 公開和私人雲端獲取五分鐘更新。 · 轉送高級檔案類別，如 APK、Flash 檔案、PDF、Microsoft Office 檔案、Java Applet、Java 檔案（.jar 和 .class），以及 SMTP 和 POP3 電子郵件訊息中包含的 HTTP/HTTPS 電子郵件連結。 · 使用 WildFire API。 · 使用 WildFire 裝置來裝載 WildFire 私人雲端或 WildFire 混合雲端。
AutoFocus	您仍可以： · 將外部動態清單與 AutoFocus 資料一起使用，寬限期為三個月。 您不可再： · 存取 AutoFocus 入口網站。 · 檢視 AutoFocus Intelligence Summary（AutoFocus 情報摘要）以獲取監控日誌或 ACC 構件。
Cortex 資料湖	您仍可以： · 存儲日誌資料，寬限期為 30 天，之後將其刪除。 · 將日誌轉送到 Cortex 資料湖，直到 30 天寬限期結束。
GlobalProtect	您仍可以： · 將應用程式用於執行 Windows 和 macOS 的端點。

©2023 Palo Alto Networks, Inc.

授權	到期行為
	· 設定一個或多個內部/外部閘道。 您不可再： · 存取 Linux OS 應用程式和 iOS、Android、Chrome OS 及 Windows 10 UWP 的行動應用程式。 · 使用外部閘道 IPv6。 · 執行 HIP 檢查。 · 使用無用戶端 VPN。 · 根據目的地網域、用戶端處理序和視訊串流應用程式強制執行分割通道。
支援	您不可再： · 接收軟體更新。 · 下載 VM 映像。 · 受益於技術支援。

©2023 Palo Alto Networks, Inc.

Cloud Security Service Provider（雲端安全服務供應商 - CSSP）的授權

Palo Alto Networks CSSP 夥伴計畫可讓服務供應商提供安全即服務或安全即託管應用程式給一般客戶。Palo Alto Networks 為授權的 Cloud Security Service Provider（雲端安全服務供應商 - CSSP）夥伴提供的授權供應項目，不同於為企業使用者提供的供應項目。

針對 CSSP 夥伴，對於與訂閱和支援一起搭售的 VM-Series 防火牆，Palo Alto Networks 支援依使用授權模式。CSSP 夥伴可以結合 VM-Series 型號的期限型容量授權和可選取的訂閱授權（包括 Threat Prevention、URL 篩選、AutoFocus、GlobalProtect 和 WildFire），還有可存取技術支援和軟體更新的支援權利。如果您打算在 HA 組態中部署防火牆，您可以購買符合成本效益的高可用性選項。

- 取得 CSSP 授權套件的驗證碼
- 使用 CSSP 驗證碼註冊 VM-Series 防火牆
- 針對已註冊的 VM-Series 防火牆新增一般客戶資訊

取得 CSSP 授權套件的驗證碼

若要成為 CSSP 夥伴，您必須參加 Palo Alto Networks CSSP 夥伴計畫。如需有關參加 CSSP 計畫的資訊，請聯絡 Palo Alto Networks 通路業務經理。如果已參加，Palo Alto Network 支援入口網站會提供工具讓您選取授權套件、追蹤授權使用情形和運用授權權利。

授權套件是下列選項的組合：

- 使用期限—即用即付選項包括每小時、每月、1 年和 3 年。
- VM-Series 防火牆型號—VM-100、VM-200、VM-300 和 VM-1000-HV，提供型號及每個機型相關聯的容量。
- 訂閱搭售包—三個選項為基本、搭售包 1 和搭售包 2。基本選項不包括任何訂閱；搭售包 1 具有威脅防護授權（包括 IPS、AV、惡意軟體防護）；搭售包 2 具有威脅防護（包括 IPS、AV、惡意軟體防護）、DNS 安全性、GlobalProtect、WildFire 和 PAN-DB URL 篩選授權。
- 支援層級—進階支援或後備支援。
- 備援防火牆—選項為高可用性 (HA) 或沒有 HA。如果您打算部署一對備援防火牆，則這是符合成本效益的選項。

例如，供應項目 PAN-VM-300-SP-PREM-BND1-YU 是一年期套件，包含 VM-300 及進階支援和訂閱搭售包 1。每個套件最多支援 10,000 個 VM-Series 防火牆實例。

選取授權套件之後，您會收到附有驗證碼的電子郵件；履行程序可能長達 48 小時。

STEP 1 | 使用帳戶認證登入 Palo Alto Networks 客戶支援網站。若您需要新帳戶，請參閱建立支援帳戶。

STEP 2 | 選取 **CSSP** > **Order History**（訂購歷程記錄），以檢視您的支援帳戶中註冊的驗證碼清單。

部署防火牆時，您必須根據驗證碼來註冊防火牆的每一個實例。

©2023 Palo Alto Networks, Inc.

使用 CSSP 驗證碼註冊 VM-Series 防火牆

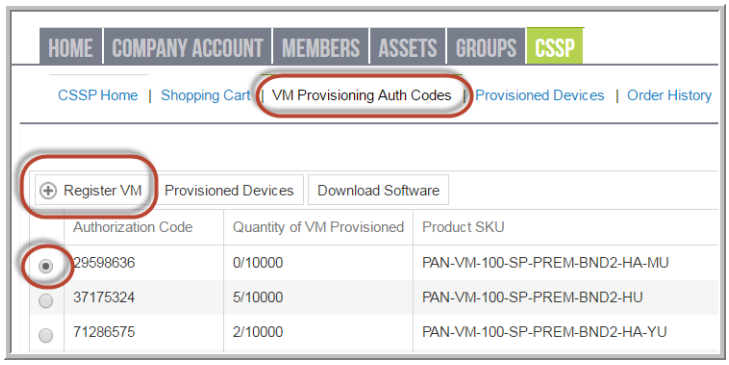
若要在 VM-Series 防火牆上啟動授權，您必須先完成 VM-Series 防火牆的部署以及初始組態。如果您是 CSSP 夥伴，您可以選取下列選項來註冊防火牆：

- API—如果您在協調運作服務上有自訂指令碼，請使用授權 API。使用此選項時，Panorama 不需要直接存取網際網路。
- 啟動程序—使用此選項可自動設定防火牆，並於第一次啟動時授權。請參閱啟動 VM-Series 防火牆。
- 防火牆網頁介面—您可以使用防火牆網頁介面啟動 VM-Series 防火牆的授權（獨立版本）。不論防火牆是否可存取網際網路，此工作流程都適用。
- 客戶支援入口網站—使用此選項在 Palo Alto Networks 客戶支援入口網站上註冊防火牆，如下所示。

STEP 1 | 使用帳戶認證登入 Palo Alto Networks 客戶支援網站。若您需要新帳戶，請參閱建立支援帳戶。

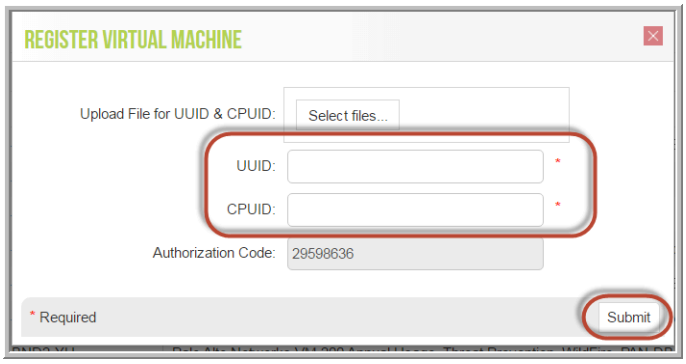
STEP 2 | 選取 **CSSP** > **Order History**（訂購歷程記錄），以檢視您的支援帳戶中註冊的驗證碼清單。

STEP 3 | 選取 **CSSP** > **VM Provisioning Auth Codes**（**VM** 佈建驗證碼），再選取 **Authorization Code**（授權碼），然後按一下 **Register VM**（註冊 **VM**）。



 ©2023 Palo Alto Networks, Inc.

STEP 4 | 輸入 VM 實例的 **UUID** 和 **CPUID**，然後按一下 **Submit**（提交）。入口網站將產生防火牆的序號。



您可以追蹤已部署的 ***VM-Series*** 防火牆數目，及仍可針對每個驗證碼使用的授權數目。若要檢視以特定授權碼所註冊的防火牆總數，請選取 ***CSSP > VM Provisioning Auth Codes***（***VM*** 佈建授權碼），並選取 ***Authorization Code***（授權碼），然後按一下 ***Provisioned Devices***（佈建的裝置）。

針對已註冊的 VM-Series 防火牆新增一般客戶資訊

對於 CSSP 獲授權者，在您註冊防火牆之後，您可以使用 Palo Alto Networks 支援入口網站或「授權 API」，將 VM-Series 防火牆的序號連結至您佈建防火牆所針對的客戶。

- 針對已註冊的 VM-Series 防火牆新增一般客戶資訊（客戶支援入口網站）。支援入口網站以使用者名稱和密碼進行驗證。
- 針對已註冊的 VM-Series 防火牆新增一般客戶資訊 (API)。API 使用「授權 API」金鑰進行驗證。

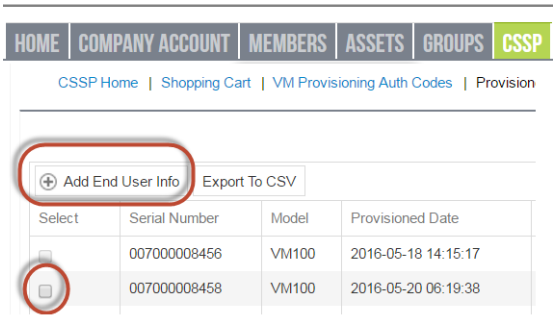
針對已註冊的 **VM-Series** 防火牆新增一般客戶資訊（客戶支援入口網站）

請完成下列程序，透過客戶支援入口網站，針對已註冊的防火牆新增使用者資訊。

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

STEP 2 | 選取 **CSSP** > **Provisioned Devices**（佈建的裝置）。

STEP 3 | 選取 **Serial Number**（序號），然後按一下 **Add End User Info**（新增使用者資訊）。

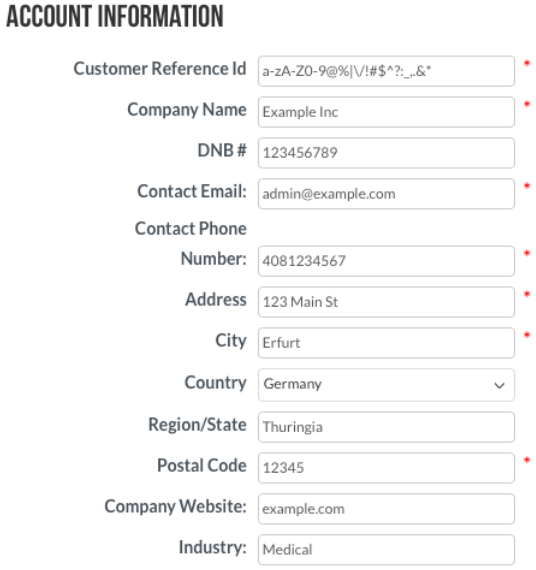


©2023 Palo Alto Networks, Inc.

STEP 4 | 輸入客戶的 **Account Information**（帳戶資訊），如下所示。

- Customer Reference Id（客戶參照 ID）：必要
- Company Name（公司名稱）:必要
- DNB #:Data Universal Numbering System（資料環球編碼系統 - D-U-N-S）號碼
- Contact Email（聯絡人電子郵件）：必要，使用者電子郵件地址
- Contact Phone Number（聯絡人電話號碼）：使用者電話號碼
- Address:必要，使用者地址
- 國家/地區：必要，ISO 雙字母國碼
- City（城市）：必要，使用者城市名稱
- Region/State（地區/州）：必要；若為美國和加拿大，您必須輸入 ISO 雙字母分區碼；對於其他所有國家/地區，任何文字字串都有效。
- Postal Code（郵遞區號）：必要，使用者郵遞區號
- Company Website（公司網站）：使用者網站 URL
- Industry（行業）：使用者行業別，例如網路或諮詢顧問

按一下 **Submit**（提交）來儲存詳細資訊。



新增帳戶資訊之後，您可以尋找所有已註冊給客戶的防火牆。在 ***Search Existing End User***（搜尋現有使用者）中，輸入客戶 ***ID*** 或客戶名稱，然後按一下 ***Search***（搜尋），尋找所有已佈建給客戶的防火牆。

針對已註冊的 VM-Series 防火牆新增一般客戶資訊 (API)

存取 API 的 URL 是 https://api.paloaltonetworks.com/api/license/ReportEndUserInfo。

API 要求必須使用 HTTP POST 方法，而且您必須加入含有 API 金鑰的 HTTP 要求標頭，並將內容類型指定為 JSON。API 回應是 JSON 格式。

STEP 1 | 取得授權 API 金鑰。

©2023 Palo Alto Networks, Inc.

STEP 2 | 針對向 CSSP 註冊的 VM-Series 防火牆，使用 ReportEndUserInfo API 新增使用者資訊。

URL：**`https://api.paloaltonetworks.com/api/license/ReportEndUserInfo`**

標頭：

- Content-Type: application/json
- apiKey:*API* 金鑰

參數：

- `SerialNumbers`:必要，至少提供一個有效的防火牆序號
- `CustomerReferenceId`：必要
- `CompanyName`:必要，使用者公司名稱
- `DnBNumber`:Data Universal Numbering System（資料環球編碼系統 - D-U-N-S）號碼
- `PhoneNumber`:使用者電話號碼
- `EndUserContactEmail`:必要，使用者電子郵件地址
- `Address`：必要，使用者地址
- `Country`：必要，ISO 雙字母國碼
- `City`：必要，使用者城市名稱
- `Region/State`：必要；若為美國和加拿大，您必須輸入 ISO 雙字母分區碼；對於其他所有國家/地區，任何字母字串都有效。
- `PostalCode`:必要，使用者郵遞區號
- `Industry`：使用者行業別，例如網路或諮詢顧問
- `WebSite`:使用者網站 URL
- `CreatedBy`:提交此資訊的系統或個人

針對已註冊的 **VM-Series** 防火牆，使用 **Curl** 新增使用者資訊的範例要求：

```
curl -X POST "http://api.paloaltonetworks.com/api/license/
ReportEndUserInfo" \-H "內容類型: application/json" \-H "apikey:
 your_key_here" \--data-raw '{ "序號": ["0001A101234"], "客戶帳
戶 ID":12345, "公司名稱":"範例公司", "DnB 號碼":"123456789", "地
址":"123 大道", "城市":"森尼韋爾", "地區":"CA", "州":"CA", "國家/地
區":"US", "郵遞區號":"12345", "行業":"醫療", "電話號碼":"4081234567",
 "網站": "example.com", "使用者聯絡電子郵件": "admin@example.com", "建
立者":"Jane Doe"}'
```

範例 **API** 回應：

```
"{"訊息":"使用者資訊已成功更新"}"
```

如果您收到錯誤，請參閱授權 API 錯誤代碼。

©2023 Palo Alto Networks, Inc.

在 ESXi 伺服器上設定 VM-Series 防火牆

VM-Series 防火牆是以開放式虛擬化聯盟 (OVA) 格式散佈，這是封裝和部署虛擬機器的標準方式。您可以在能執行 VMware ESXi 的任何 x86 設備上安裝此解決方案。

為了部署 VM-Series 防火牆，您必須熟悉包含 vSphere 網路的 VMware 和 vSphere、ESXi 主機設定和組態，以及虛擬機器來賓部署。

若想要自動化 VM-Series 防火牆的部署程序，您可以使用最佳化的組態和原則建立金質標準的範本，然後在您的網路中，使用 vSphere API 和 PAN-OS XML API 來快速部署新的 VM-Series 防火牆。

請參閱下列主題中的相關資訊：

- VMware vSphere Hypervisor (ESXi) 上支援的部署
- ESXi 上的 VM-Series—系統需求及限制
- 在 VMware vSphere Hypervisor (ESXi) 上安裝 VM-Series 防火牆
- vCenter 上的 VM 監控
- ESXi 部署的疑難排解
- ESXi 專用 VM-Series 的效能調整

VMware vSphere Hypervisor (ESXi) 上支援的部署

您可以在 ESXi 伺服器上部署 VM-Series 防火牆的一或多個實例。您在網路上放置 VM-Series 防火牆的位置，係根據拓撲而定。從下列選項中選取（適用於未使用 VMware NSX 的環境）：

- 每台 **ESXi** 主機一個 **VM-Series** 防火牆—ESXi 主機上的每台 VM 伺服器會先經過防火牆，再結束實體網路的主機。VM 伺服器會透過虛擬標準交換器連接至防火牆。來賓伺服器沒有其他網路連線，因此防火牆可看見及控制所有離開 ESXi 主機的流量。此使用案例另有一種使用方式，但此方式亦需要所有流量流經防火牆，包含相同 ESXi 主機上的伺服器至伺服器的流量（東西向流量）。
- 每個虛擬網路一個 **VM-Series** 防火牆—針對每個虛擬網路部署一個 VM-Series 防火牆。如果您已設計網路，使得一或多台 ESXi 主機都有屬於內部網路的一個虛擬機器群組、一個屬於外部網路的群組，及屬於 DMZ 的群組，您可以部署一個 VM-Series 防火牆來防護每個群組中的伺服器。如果群組或虛擬網路未與任何其他虛擬網路共用虛擬交換器或連接埠群組，則可將它與主機內或跨主機的所有其他虛擬網路加以隔離。由於沒有通往任何其他網路的實體或虛擬路徑，因此每個虛擬網路上的伺服器都必須使用防火牆，以便與任何其他網路進行通訊。防火牆針對所有已連接至每個虛擬網路的虛擬（標準或散佈）交換器，能看見並控制從中離開的所有流量。
- **Hybrid environment**（混合型環境）—使用實體與虛擬主機兩者。VM-Series 防火牆可以取代在傳統彙總位置中的防火牆設備。混合環境為所有裝置實現了通用服務器平台的優勢，並取消了硬體和軟體升級依賴關係。

使用 ESXi 上的 VM-Series 系統需求及限制與在 VMware vSphere Hypervisor (ESXi) 上安裝 VM-Series 防火牆繼續。

©2023 Palo Alto Networks, Inc.

ESXi 上的 VM-Series—系統需求及限制

本節針對 VMware vSphere Hypervisor (ESXi) 上的 VM-Series 防火牆列出其需求及限制。若要部署 VM-Series 防火牆，請參閱在 VMware vSphere Hypervisor (ESXi) 上安裝 VM-Series 防火牆。

- ESXi 上的 VM-Series—系統需求
- ESXi 上的 VM-Series—系統限制

ESXi 上的 VM-Series—系統需求

您可以在 ESXi 伺服器上建立和部署 VM-Series 防火牆的多個實例。由於防火牆的每個實例在 ESXi 伺服器上都需要具備最低的資源配置（CPU 數量、記憶體和磁碟空間），因此請務必符合以下規格來確保最佳效能。

VM-Series 防火牆具有下列要求：

- 主機 CPU 必須為具有虛擬化延伸的 x86 型 Intel 或 AMD CPU。
- 請參閱相容性矩陣，以瞭解支援的 ESXi 版本。vmx 版本支援是以您用來部署 VM-Series 防火牆的 OVA 為基礎，而且您無法修改此版本。升級或降級 VM-Series 軟體版本，並不會變更已在啟動時啟用的 vmx 版本。
- 有關您的 VM-Series 型號的最低硬體需求，請參閱 VM-Series 系統需求。
- 至少兩個網路介面 (vNIC)。一個是管理介面專用的 vNIC，一個用於資料介面。對於資料流量，您最多可新增八個額外的 vNIC。對於其他的介面，請使用 ESXi 伺服器上的 VLAN Guest Tagging (VGT)，或設定防火牆上的子介面。

  依預設會啟用 Hypervisor 指派的 MAC 位址。vSphere 會指派唯一的 vNIC MAC 位址給 VM-Series 防火牆的每個資料平面介面。如果您停用 Hypervisor 指派的 MAC 位址，VM-Series 防火牆會從自己的集區中指派給每個介面一個 MAC 位址。因為這會造成每個介面的 MAC 位址不同，所以您必須啟用防火牆數據平面介面附加的虛擬交換器連接群組上的混合式模式；這會讓防火牆收到框架（請參閱在 ESXi 伺服器上佈建 VM-Series 防火牆）。如果混合式模式與 Hypervisor 指派的 MAC 位址皆未啟用，防火牆不會接收任何流量。這是因為當框架的目的地 MAC 位址與 vNIC MAC 位址不相符時，vSphere 不會轉送框架到虛擬電腦上。
- 依預設，ESXi 上的 VM-Series 防火牆會啟用 Data Plane Development Kit（資料平面開發套件 - DPDK）。如需 DPDK 的詳細資訊，請參閱在 ESXi 上啟用 DPDK。

©2023 Palo Alto Networks, Inc.

- 為了讓 VM-Series 防火牆達到最佳效能，在部署 VM-Series 防火牆之前，您可以對主機進行下列調整。如需詳細資訊，請參閱ESXi 專用 VM-Series 的效能調整。
  - **Enable DPDK**（啟用 **DPDK**）。DPDK 可讓主機避開 Linux 核心來加速處理封包。反之，與 NIC 互動是透過驅動程式和 DPDK 程式庫。
  - **Enable SR-IOV**（啟用 **SR-IOV**）。Single root I/O virtualization（單一根 I/O 虛擬化 - SR-IOV）可讓單一根埠下的單一 PCIe 實體裝置，以多個單獨實體裝置呈現給 Hypervisor 或來賓。

    不要在您啟用 SR-IOV 的實體連接埠上設定 vSwitch。若要與主機或其他在此網路上的虛擬電腦通訊，則 VM-Series 防火牆必須有實體連接埠的獨佔存取權，且與在該介面上的虛擬功能 (VF) 相關聯。
  - **Enable multi-queue support for NICs**（啟用 **NIC** 的多佇列支援）。多重佇列可讓網路效能隨著 vCPU 數目而調整，還能建立多個 TX 和 RX 佇列來平行處理封包。

ESXi 上的 VM-Series—系統限制

VM-Series 防火牆功能相當類似 Palo Alto Networks 硬體防火牆，但是有下列限制：

- 請勿在使用 ESXi 上 VM-Series NSX 版防火牆的 VMware 快照功能。快照可影響效能及導致不定期和不一致的封包遺失。請參閱 VMWare 使用快照的最佳作法建議。

  如果您需要組態備份，請使用 Panorama 或從防火牆使用 **Export named configuration snapshot**（匯出具名組態快照）（Device（裝置）> Set up（設定）> Operations（操作））。使用 **Export named configuration snapshot**（匯出具名組態快照）匯出防火牆上的啟用組態 (`running-config.xml`)，您可以將其儲存至任意網路位置。
- 建議使用專用的 CPU 核心。
- ESXi 上的 VM-Series 防火牆不支援高可用性 (HA) 連結監控。使用路徑監控功能以確認對目標 IP 位址或下一躍點 IP 位址的連線。
- 總共可設定高達 10 個連接埠；這是 VMware 限制。一個連接埠用於管理流量，最多 9 個可用於資料流量。
- 僅支援 vmxnet3 驅動程式。
- 不支援虛擬系統。
- 如果 ESXi 主機有同質 CPU 設定，則 vSphere 6.5、6.7 和 7.0 支援 VM-Series 防火牆的 vMotion。主機安裝在 vSphere 6.5 或 6.7 時，使用 vMotion 在主機之間移動 VM-Series 防火牆需要 PAN-OS 9.1.6 和更新版本。
- 在連線至第 2 層的 ESXi vSwitch 連接埠群組以及 VM-Series 防火牆的 vwire 介面上，必須啟用偽造的傳輸和混合式模式。
- 若要搭配 ESXi 上的 VM-Series 防火牆一起使用 PCI 裝置，memory mapped I/O（記憶體對應 I/O - MMIO）必須低於 4GB。您可以在伺服器的 BIOS 中停用超出 4GB 的 MMIO。此為 ESXi 限制。
- 使用 ESXi 7.0 時，如果以 PCI 裝置通道將 VF 連接至 virtual machine（虛擬機器 - VM），介面不會出現。

©2023 Palo Alto Networks, Inc.

在 VMware vSphere Hypervisor (ESXi) 上安裝 VM-Series 防火牆

若要安裝 VM-Series 防火牆，您必須擁有開放式虛擬化格式 (OVA) 範本的存取權。使用您在訂購完成電子郵件收到的驗證碼，以註冊您的 VM-Series 防火牆及下載 OVA 範本。OVA 範本為包含三種檔案類型的壓縮檔：

- .mf:OVF 資訊清單檔，包含封裝中個別檔案的 SHA-1 摘要
- .ovf:OVF 描述元檔案，包含封裝及其中內容的所有中繼資料
- .vmdk:虛擬磁碟影像檔案，包含防火牆的虛擬版本

完成下列工作以安裝並設定 ESXi 上的 VM-Series。

- 規劃 ESXi 專用 VM-Series 的介面
- 在 ESXi 伺服器上佈建 VM-Series 防火牆
- 在 ESXi 的 VM-Series 上執行初始組態
- （選用）將額外磁碟空間新增至 VM-Series 防火牆
- 在 ESXi 及 vCloud Air 上的 VM-Series 防火牆上使用 VMware 工具
- 使用 vMotion 在主機之間移動 VM-Series 防火牆
- 使用 VM-Series CLI 在 ESXi 上交換管理介面

規劃 ESXi 專用 VM-Series 的介面

您可以規劃 VM-Series 防火牆 vNIC 和介面的對應，以避免重新啟動和組態問題。下表說明當 ESXi 上的 10 個 vNIC 全都啟用時，VMware vNIC 與 VM-Series 介面之間的預設對應。

VMware vNIC	VM-Series 介面
1	乙太網路 1/0 (mgmt)
2	乙太網路 1/1 (eth1)
3	乙太網路 1/2 (eth2)
4	乙太網路 1/3 (eth3)
5	乙太網路 1/4 (eth4)
6	乙太網路 1/5 (eth5)
7	乙太網路 1/6 (eth6)
8	乙太網路 1/7 (eth7)

©2023 Palo Alto Networks, Inc.

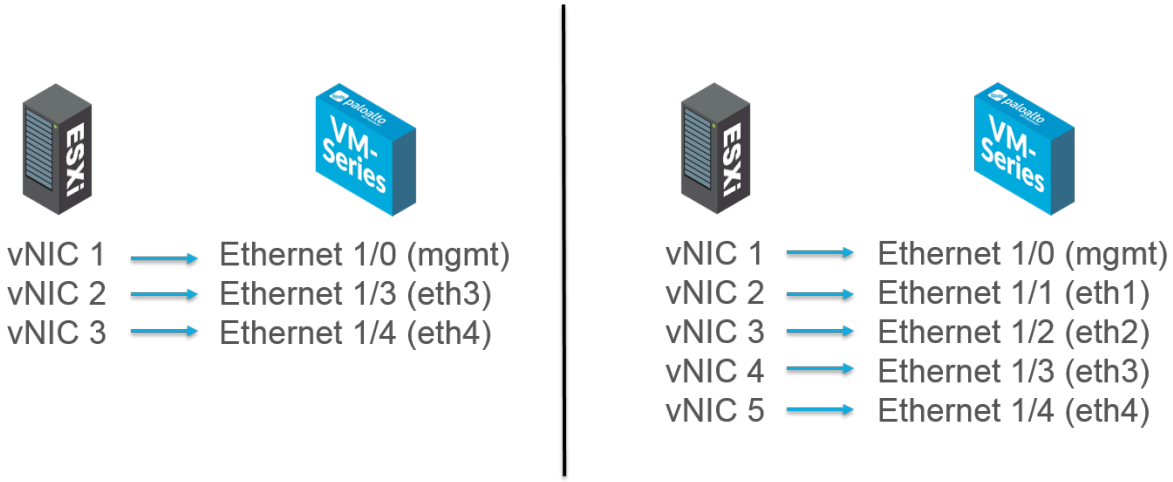
VMware vNIC	VM-Series 介面
9	乙太網路 1/8 (eth8)
10	乙太網路 1/9 (eth9)

不論您在 ESXi 上新增哪些 vNIC，VM-Series 防火牆上的對應都維持相同。您在防火牆上啟動的介面，一律會在 ESXi 上取得下一個可用的 vNIC。

在下圖中，在 VM-Series 防火牆上的 eth3 和 eth4 與 ESXi 上的 vNIC 2 和 3 配對，而 eth1 和 eth2 則並不對應，如左側所示。

如果您想要在維護現有對應的同時新增兩個其他介面，則請啟動 vNIC 4 和 5 並重新啟動防火牆。保留現有 vNIC 對應，因為您最後對應的介面之後又新增了介面。

如果您啟動在 VM-Series 防火牆上的 eth1 和 eth2，介面將自行重新排列（如右側所示），造成對應不符而影響流量。



為了避免先前範例所述的問題，您可以採取下列動作：

- 在第一次佈建 ESXi 主機時，啟動第一個外的所有九個 vNIC。在啟動 VM-Series 防火牆之前新增全部九個 vNIC 作為預留位置，可讓您不按順序使用任何 VM-Series 介面。
- 若所有 vNIC 已啟動，則新增其他介面不需重新開機。因為 ESXi 上的每個 vNIC 都需要您選取網路，您可以建立空的連接埠群組作為網路預留位置。
- 請勿移除 VM-Series 防火牆 vNIC，以避免對應不符。

在 ESXi 伺服器上佈建 VM-Series 防火牆

使用這些指示在（獨立式） ESXi 伺服器上部署 VM-Series 防火牆。有關部署 VM-Series NSX 版防火牆，請參閱在 VMware NSX-T 上設定 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

STEP 1 | 下載 OVA 檔案。

註冊 VM-Series 防火牆並從 Palo Alto Networks 客戶支援網站取得 OVA 檔案。

OVA 檔案包含基礎安裝。基礎安裝完成後，您必須從支援的入口網站下載並安裝最新的 *PAN-OS* 版本。這可確保您擁有建立基礎映像後最新採用的修正程式。如需指示，請參閱升級 PAN-OS 軟體版本（獨立版本）。

STEP 2 | 部署 OVA 檔案前，請設定 VM-Series 防火牆所需的虛擬標準交換器或虛擬分散式交換器。

如果是部署具有第 *3* 層介面的 *VM-Series* 防火牆，依預設，防火牆會使用 Hypervisor 指派的 MAC 位址。如果您選取停用 *Hypervisor* 指派的 *MAC* 位址，或部署具有 *Layer 2*、*Virtual Wire* 或旁接介面的防火牆，您必須設定（設定為 ***Accept***（接受））附加至 *VM-Series* 防火牆的任何虛擬交換器以允許下列模式：混合式模式、*MAC* 位址變更及偽造的傳輸。

設定虛擬標準交換器或虛擬分散式交換器接收 VM-Series 防火牆的框架。

虛擬標準交換器

1. 導覽至 **Home**（首頁） > **Hosts and Clusters**（主機及叢集）並選取主機。
2. 按一下 **Configure**（設定）頁籤並檢視 **Virtual Switches**（虛擬交換器）。對於各個 VM-Series 防火牆連接的虛擬交換器，按一下 **Properties**（屬性）。
3. 反白顯示與虛擬交換器對應的連接埠群組並按一下 **Edit Settings**（編輯設定）。在 vSwitch 屬性中，按一下 **Security**（安全性）頁籤，然後將 **Promiscuous Mode**（混合式模式）、**MAC Address Changes**（**MAC** 位址變更）及 **Forged Transmits**（偽造的傳輸）設為 **Accept**（接受），然後按一下 **OK**（確定）。這個變更會傳播到虛擬交換器中所有的連接埠群組。

虛擬分散式交換器

1. 選取 **Home**（首頁） > **Networking**（網路）。選取您的虛擬分散式交換器並反白顯示您要編輯的 **Distributed Port Group**（分散式連接埠群組）。
2. 按一下 **Edit Settings**（編輯設定），選取 **Policies**（政策） > **Security**（安全性），將 **Promiscuous Mode**（混合式模式）、**MAC Address Changes**（**MAC** 位址變更）及 **Forged Transmits**（偽造的傳輸）設為 **Accept**（接受），然後按一下 **OK**（確定）。

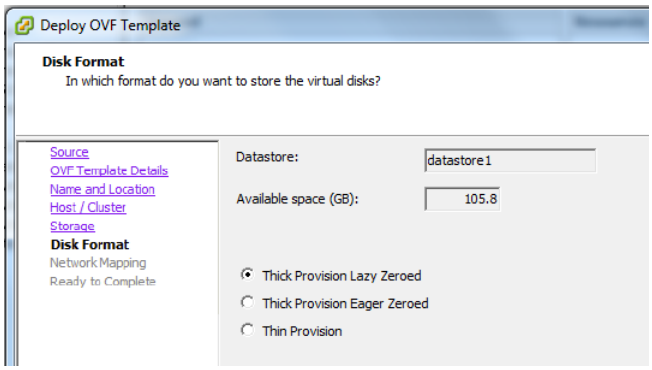
©2023 Palo Alto Networks, Inc.

STEP 3 | 部署 OVA。

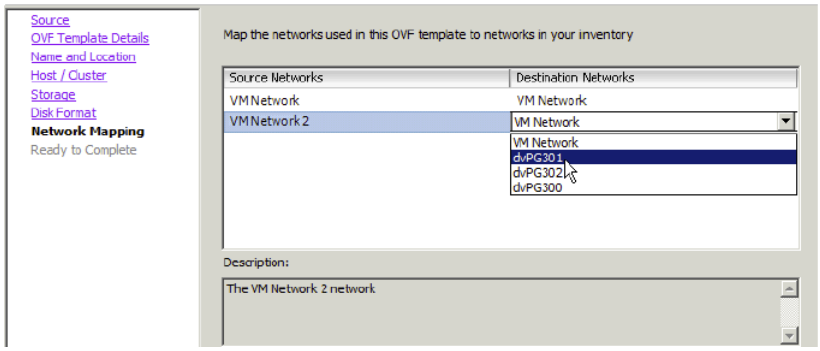
如果您將額外的介面 *(vNIC)* 新增至 *VM-Series* 防火牆，則必須重新開機（因為在開機循環期間會偵測新的介面）。若要將重新開機防火牆的需要最小化，則在初始部署或在維修視窗中啟動介面。

若要檢視安裝的進度，請監控 ***Recent Tasks***（最近的工作）清單。

1. 使用 vSphere 用戶端登入 vCenter。必要時，您也可以直接移至目標 ESXi 主機。
2. 從 vSphere Web 用戶端，前往 **Hosts and Clusters**（主機及叢集），並以滑鼠右鍵按一下主機，然後選取 **Deploy OVF Template**（部署 **OVF** 範本）。
3. 瀏覽至您先前下載的 OVA 檔案。選取檔案，然後按一下 **Next**（下一步）。檢閱範本詳細資料，然後按一下 **Next**（下一步）。
4. 命名 VM-Series 防火牆實例，在 **Inventory Location**（詳細目錄位置）視窗中，選取資料中心和資料夾，然後按 **Next**（下一步）
5. 選取 VM-Series 防火牆的 ESXi 主機，並按一下 **Next**（下一步）。
6. 選取用於 VM-Series 防火牆的資料存放，並按一下 **Next**（下一步）。
7. 保留資料存放佈建的預設設定，並按一下 **Next**（下一步）。預設為 **Thick Provision Lazy Zeroed**（重量型佈建延遲歸零）。

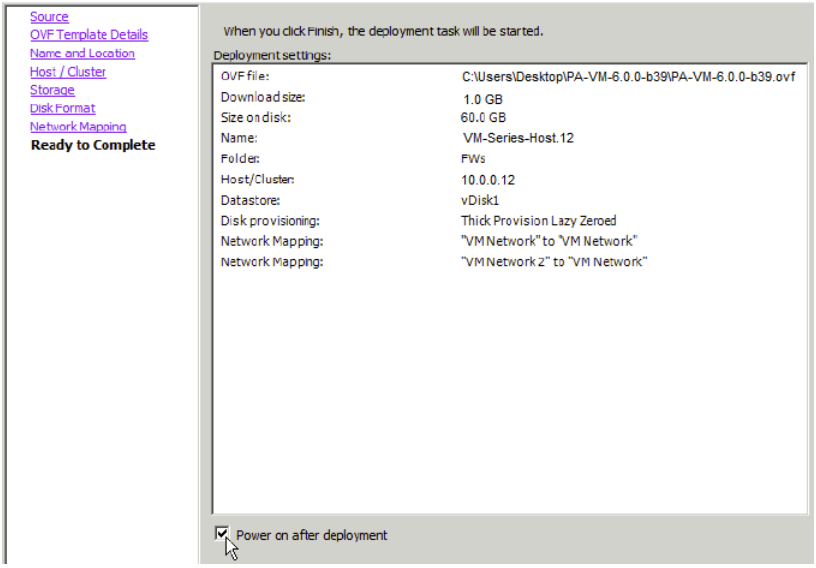


8. 選取用於兩個初始 vNIC 的網路。第一個 vNIC 會用於管理介面，第二個 vNIC 會用於第一個資料連接埠。確定 **Source Networks**（來源網路）對應至正確的 **Destination Networks**（目的地網路）。



9. 檢閱詳細資料，選取 **Power on after deployment**（部署後啟動），然後按一下 **Next**（下一步）。

 ©2023 Palo Alto Networks, Inc.



10. 部署完成時，按一下 **Summary**（摘要）頁籤，檢閱目前的狀態。

在 ESXi 的 VM-Series 上執行初始組態

在 ESXi 伺服器上使用虛擬設備主控台，設定 VM-Series 防火牆的網路存取。依預設，VM-Series 防火牆使用 DHCP 取得管理介面的 IP 位址，但您也可以指派一個靜態 IP 位址。完成初始組態之後，請存取網頁介面來完成進一步的組態設定工作。如果您使用 Panorama 執行中央管理，請參閱《Panorama 管理員指南》以取得使用 Panorama 管理裝置的詳細資訊。

如果您使用啟動程序在 ESXi 上執行 VM-Series 防火牆的組態，請參閱在 ESXi 上啟動 VM-Series 防火牆。

如需啟動程序的一般資訊，請參閱啟動 VM-Series 防火牆。

STEP 1 | 從網路管理員收集必要資訊。

- MGT 連接埠的 IP 位址
- 網路遮罩
- 預設閘道
- DNS 伺服器 IP 位址

STEP 2 | 存取 VM-Series 防火牆的主控台。

1. 在 ESXi 伺服器上針對 VM-Series 防火牆選取 **Console**（主控台）頁籤，或在 VM-Series 防火牆上按一下滑鼠右鍵並選取 **Open Console**（開啟主控台）。
2. 按下 Enter 以存取登入畫面。
3. 輸入預設的使用者名稱/密碼 (admin/admin) 進行登入。
4. 輸入 **`configure`** 切換至組態模式。

©2023 Palo Alto Networks, Inc.

STEP 3 | 設定管理介面的網路存取設定。

輸入下列命令：

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> 網路遮罩 <netmask>
default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

STEP 4 | 提交您的變更並結束組態模式。

輸入 **commit** 。

輸入 **exit**。

STEP 5 | 驗證執行防火牆管理所需要的外部服務之網路存取權，例如 Palo Alto Networks 更新伺服器。

1. 使用 Ping 公用程式來確認與 Palo Alto Networks 更新伺服器的網路連線，如下列範例所示。確認是否進行了 DNS 解析並且回應中包含更新伺服器的 IP 位址（更新伺服器不會對偵測要求做出回應）。 驗證 DNS 解析後，按下 Ctrl+C 停止偵測要求。

   ```
   admin@PA-220 > ping host updates.paloaltonetworks.com
   ```

   ```
   PING 更新.paloaltonetworks.com (10.101.16.13) 56(84) 位元組
   資料。從 192.168.1.1 icmp_seq=1 無法存取目標主機 從 192.168.1.1
    icmp_seq=2 無法存取目標主機 從 192.168.1.1 icmp_seq=3 無法存取目標
   主機 從 192.168.1.1 icmp_seq=4 無法存取目標主機
   ```

2. 使用下列 CLI 命令以擷取來自 Palo Alto Networks 更新伺服器的防火牆支援權利相關資料：如果您可以連線，則請求支援檢查，此更新伺服器將回應您防火牆的支援狀態。

STEP 6 | 在您開始測試 VM-Series 防火牆前，請先套用容量驗證碼並擷取授權。

未授權的 VM-Series 防火牆最多可同時處理大約 1230 個工作階段。視乎環境可能很快會達到工作階段限制，導致不可預測的結果。

將額外磁碟空間新增至 VM-Series 防火牆

VM-Series 防火牆需要安裝 60 GB 大小的虛擬磁碟，其中的 21 GB 用於日誌記錄（依預設）。

- 對於大型部署，使用 Panorama 彙總所有下一代防火牆的資料，並提供網路上所有流量的可視性。Panorama 提供集中化的日誌與報告。
- 對於您未使用 Phanorama 的小型部署，可新增新的虛擬磁碟以增加日誌儲存容量。新虛擬磁碟可支援 60 GB 到 2TB 的日誌儲存容量。工作說明如下。

當虛擬設備設定為使用虛擬磁碟時，*VM-Series* 防火牆就不再儲存日誌。如果設備失去與新虛擬磁碟的連線，可能會在失敗間隔期間遺失日誌。若必要，將新建立的虛擬磁碟置於提供 *RAID* 備援的資料存放上。對於具有日誌記錄特性的應用程式而言，*RAID10* 所提供的寫入效能最佳。

©2023 Palo Alto Networks, Inc.

STEP 1 | 關閉 VM-Series 防火牆電源。

STEP 2 | 在 ESXi 伺服器上，將虛擬磁碟新增至防火牆。

1. 在 ESXi 伺服器上，選取 VM-Series 伺服器。
2. 按一下 **Edit Settings**（編輯設定）。
3. 按一下 **Add**（新增）以啟動新增硬體精靈，出現提示時選取下列選項：
   1. 選取 **Hard Disk**（硬碟）做為硬體類型。
   2. 選取 **Create a new virtual disk**（建立新虛擬磁碟）。
   3. 選取 **SCSI** 做為虛擬磁碟類型。
   4. 選取 **Thick provisioning**（重量型佈建）磁碟格式。
   5. 在位置欄位中，選取 **Store with the virtual machine option**（使用虛擬機器選項儲存）。資料存放不需要常駐於 ESXi 伺服器中。
   6. 驗證設定正確，再按一下 **Finish**（完成）結束精靈。隨即會將新磁碟新增至虛擬設備的設備清單中。

STEP 3 | 開啟防火牆電源。

啟動防火牆會使虛擬磁碟在第一次使用時初始化。初始化程序的完成時間將隨新虛擬磁碟的大小而異。

當新虛擬磁碟初始化並備妥後，PAN-OS 會將所有日誌從現有磁碟移到新虛擬磁碟。新日誌項目現在會寫入此新虛擬磁碟。

PAN-OS 也會產生記錄新磁的系統日誌項目。

若您重複使用之前用來儲存 *PAN-OS* 日誌的虛擬磁碟，則所有來自已有磁碟的日誌將被覆寫。

STEP 4 | 確認新虛擬磁碟的大小。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理）。
2. 在 Logging and Reporting Settings（登入與報告設定）部分中，驗證 **Log Storage**（日誌儲存）容量正確顯示新磁碟容量。

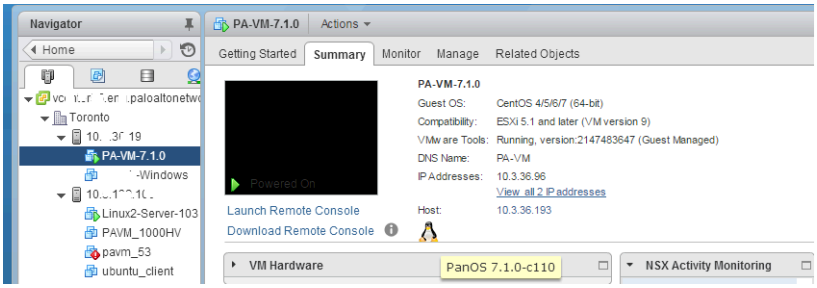
在 ESXi 及 vCloud Air 上的 VM-Series 防火牆上使用 VMware 工具

VMware 工具公用程式改善了來自 vCenter 伺服器與 vCloud Director 的 VM-Series 防火牆管理。VMware 工具與 VM-Series 防火牆專用軟體映像一起搭售，且所有更新都與新 OVF 映像一起提供。您無法使用 vCenter 伺服器或 vCloud Director 手動安裝或更新 VMware 工具。

©2023 Palo Alto Networks, Inc.

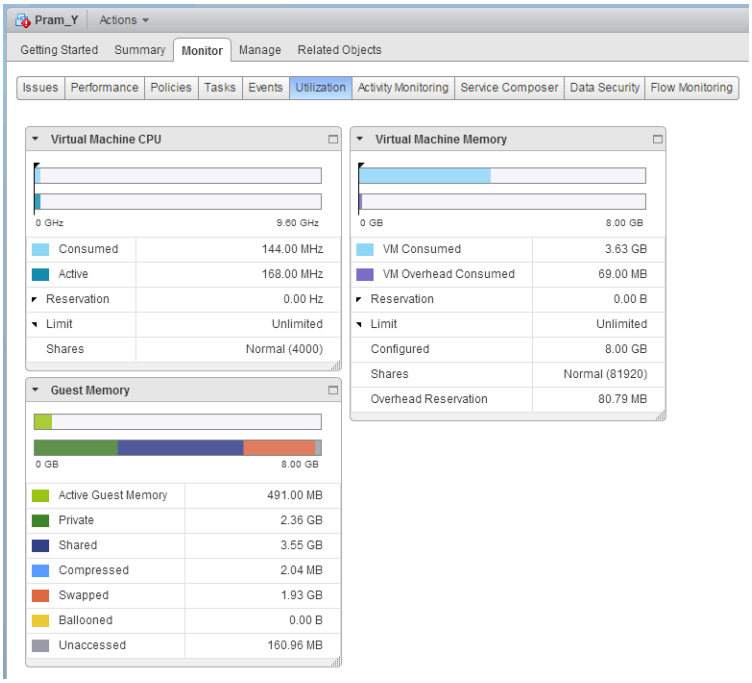
檢視管理介面上的 IP 位址以及防火牆和 Panorama 上的軟體版本。

在 vCenter 伺服器上的 Hosts and Cluster（主機及彙集）部分，選取防火牆或 Panorama 並檢視 **Summary**（摘要）頁籤，瞭解指派給管理介面的 IP 位址資訊及目前安裝的軟體版本資訊。



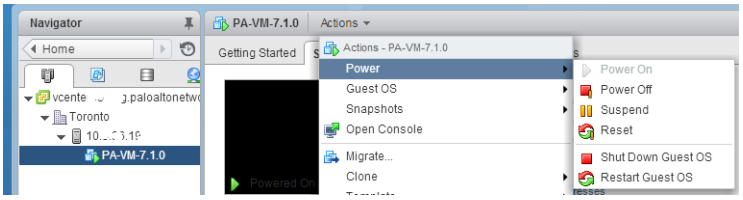
檢視硬碟、記憶體及 CPU 的資源使用率標準。使用這些標準在 vCenter 伺服器上啟用警報。

在 vCenter 伺服器的 [Hosts and Cluster（主機及叢集）] 區段中，選取防火牆或 Panorama，並檢視 **Monitor**（監控） > **Utilization**（使用率）頁籤，以瞭解硬碟、記憶體及 CPU 使用率的相關資訊。



從 vCenter 伺服器進行非失誤性關閉或重新啟動防火牆及 Panorama。

在 vCenter 伺服器的 [Hosts and Cluster（主機及叢集）] 區段中，選取防火牆或 Panorama，並選取 **Actions**（動作） > **Power**（電源）下拉式清單。

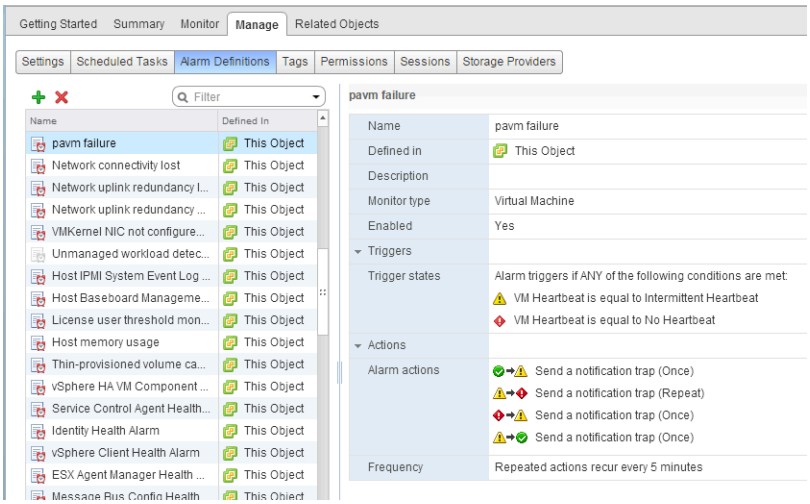


 ©2023 Palo Alto Networks, Inc.

建立您希望收到通知事件的警報定義，或您希望指定自動執行動作的事件。

如需建立警報定義的詳細資訊，請參閱 VMware 文件。

在 vCenter 伺服器上的 Hosts and Cluster（主機及叢集）部分，選取防火牆或 Panorama，並選取 **Manage**（管理） > **Alarm Definitions**（警報定義），以新增觸發條件並指定達到閾值時的動作。例如，在指定期間缺少活動訊號，或記憶體資源的使用超過臨界值。下列擷取畫面顯示如何使用監控防火牆或 Panorama 的活動訊號通知。



使用 vMotion 在主機之間移動 VM-Series 防火牆

在 VMware ESXi 上具有同質 CPU 設定的 ESXi 主機之間，使用 vMotion 移動 VM-Series 防火牆時，為了維護流量，您必須使用 PAN-OS CLI，在 vMotion 期間暫停 VM-Series 防火牆的內部活動訊號監控。您可以指定活動訊號監控暫停的時間量（以分鐘為單位）。活動訊號監控最多可以暫停 60 分鐘。當暫停間隔到期或您刻意結束暫停間隔時，活動訊號監控就會繼續。

如果 ESXi 主機有同質 CPU 設定，則 vSphere 6.5、6.7 和 7.0 支援 VM-Series 防火牆的 vMotion。

如果您執行 ***vSphere 7.0*** 或更新版本，則使用 ***vMotion*** 時不需要這些命令。

STEP 1 | 登入 VM-Series 防火牆 CLI。

STEP 2 | 使用下列命令設定活動訊號監控暫停間隔。一執行命令就會開始暫停。如果 vMotion 所花時間比預期更長，您可以重新執行此命令來設定更長的新間隔，於命令再次執行時開始計時。

```
request system heartbeat-pause set interval <pause-time-in-minutes>
```

您可以使用下列命令檢視暫停間隔的剩餘時間。

```
request system heartbeat-pause show interval
```

STEP 3 | （選用）如果您在暫停間隔經過之前完成 vMotion，則可以將間隔設為零 (0) 來結束暫停。

```
request system heartbeat-pause set interval 0
```


©2023 Palo Alto Networks, Inc.

使用 VM-Series CLI 在 ESXi 上交換管理介面

根據預設，VM-Series 防火牆會將第一個介面 (eth0) 指派為管理介面。不過，在某些部署中，第一個介面必須預先對應至公共 IP 位址。因此，管理介面必須指派給不同的介面。將公共 IP 位址指派給管理介面會有安全性風險。

此程序需要 VM-Series 外掛程式 2.0.7 或更新版本。

或者，您可以在啟動載入時，在 init-cfg.txt 檔案元件 中啟用管理介面交換。

STEP 1 | 登入 VM-Series 防火牆 CLI 並輸入下列命令：

```
set system setting mgmt-interface-swap enable yes
```

STEP 2 | 確認您要交換介面並將 eth1 資料平面介面用作管理介面。

STEP 3 | 重新啟動防火牆以使交換生效。使用下列命令：

```
request restart system
```

STEP 4 | 確認介面已交換。使用下列命令：

```
debug show vm-series interfaces all Phoenix_interface   Base-
OS_port   Base-OS_MAC        PCI-ID         Driver mgt(interface-
swap) eth0   0e:53:96:91:ef:29   0000:00:04.0   ixgbevf Ethernet1/1
           eth1    0e:4d:84:5f:7f:4d       0000:00:03.0   ixgbevf
```


©2023 Palo Alto Networks, Inc.

vCenter 上的 VM 監控

安裝和設定 VMware vCenter 專用 Panorama 外掛程式來擷取 vCenter 環境中來賓的 IP 位址，以及使用該資訊利用動態位址群組來建立政策。

VMware vCenter 專用 *Panorama* 外掛程式不支援 *Proxy* 伺服器。

- 關於 VMware vCenter 上的 VM 監控
- 安裝 VMware vCenter 專用 Panorama 外掛程式
- 設定 VMware vCenter 專用 Panorama 外掛程式

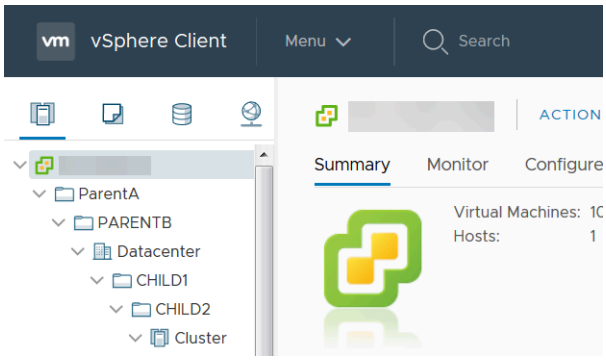
關於 VMware vCenter 上的 VM 監控

VMware vCenter 專用 Panorama 外掛程式會提供工具，以使用動態位址群組建立 vCenter 環境的原則。動態位址群組可讓您建立因應環境中的變更（例如新增或刪除來賓）而自動調整的原則。VMware vCenter 外掛程式會監控 vCenter 環境中的變更，並與 Panorama 共用該資訊。

外掛程式會處理接收自 vCenter 的資訊，並將其轉換為 Panorama 上的一組標籤，而您可以使用這組標籤作為將 IP 位址指派給動態位址群組的比對準則。每個標籤都有一個首碼，說明 VM 上方的階層。

在此範例中，Panorama 中的每個標籤都會以如下的首碼開頭。每個標籤都包含 vCenter 名稱、資料中心名稱和叢集名稱；如果您的 vCenter 階層中有資料夾，標籤也將包含資料夾名稱。標籤中的物件順序會與 vCenter 階層中的順序相符。

vcenter.<vcenter-name>_ParentA_ParentB_Datacenter_CHILD1_CHILD2_Cluster_<tag>



VMware vCenter 專用 *Panorama* 外掛程式不支援與 *vApps* 和資源集區相關聯的標籤。

標籤會以下列格式顯示在 Panorama 中：

- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_vmname.<vm-name>**—此標籤會根據虛擬機器名稱來對應虛擬機器 IP 位址。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_guestos.<guest-os>**—此標籤會根據來賓作業系統來對應虛擬機器 IP 位址。

©2023 Palo Alto Networks, Inc.

- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_annotation.<annotation>**—此標籤會根據註釋來對應虛擬機器 IP 位址。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_vlanId.<vlan-ID>**—此標籤會根據 VLAN ID 來對應虛擬機器 IP 位址。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_host-ip.<host-ip>**—此標籤會根據主機 IP 位址來對應虛擬機器 IP 位址。
- **vcenter.<vcenter-name>_<datacenter-name>_<cluster-name>_<tag-category>.<user-defined-tag>**—此標籤會根據在 vCenter 中創建的使用者定義標記來對應虛擬機器 IP 位址。

外掛程式最多支援每個 *VM* 有 *16* 個使用者定義標籤。不會處理任何超過 *16* 個的使用者定義標籤。

vCenter 專用 Panorama 外掛程式無法處理長度超過 128 個字元的標籤；這包括字母、數字和特殊字元。vCenter 物件名稱中的空格會取代為正斜線。此外，Panorama 也不支援 vCenter VM 名稱和註釋中的非 ASCII 特殊字元或下列特殊字元：’ **<>&**”。標籤若包含不受支援的字元，Panorama 即會捨棄該標籤。

若要擷取端點 IP 位址到標籤的對應資訊，您必須設定虛擬環境中每個 vCenter 的監控定義。監控定義會指定允許 Panorama 連線至 vCenter 的使用者名稱和密碼。它也指定裝置群組，以及包含 Panorama 將標籤推送至其中的防火牆的相應通知群組。在您設定監控定義而且 VMware vCenter 專用 Panorama 外掛程式擷取標籤之後，您可以建立 DAG，以及新增標籤作為比對準則。

安裝 VMware vCenter 專用 Panorama 外掛程式

若要開始在 vCenter 上監控端點，請下載並安裝 VMware vCenter 專用 Panorama 外掛程式。

如果您有 Panorama HA 組態，請在每個 Panorama 端點上重複此安裝程序。在 Panoramas 上以 HA 對等安裝外掛程式時，請先將外掛程式安裝於被動對等，再安裝於主動對等。安裝外掛程式安裝於被動對等之後會轉換為非運作狀態。將外掛程式安裝於主動對等會將被動對等恢復為運作狀態。

如果您在安裝了多個外掛程式的 HA 配對中安裝了一個獨立的 Panorama 或兩個 Panorama 設備，則在未設定一或多個外掛程式的情況下，外掛程式可能不會收到更新的 IP-Tag 資訊。發生這種情況是因為 Panorama 不會將 IP-Tag 資訊轉送到未設定的外掛程式。此外，如果一或多個 Panorama 外掛程式未處於「已註冊」或「成功」狀態（每個外掛程式的正狀態不同），則可能會出現此問題。在繼續或執行下述命令之前，請確保您的外掛程式處於正狀態。

如果遇到此問題，有兩種權宜方案：

- 解除安裝未設定的外掛程式。建議您不要安裝未打算立即設定的外掛程式
- 您可以使用以下命令來變通處理此問題。對每個 Panorama 實例上的每個未設定外掛程式執行以下命令，以防止 Panorama 等待傳送更新。否則，防火牆可能會遺失一些 IP-Tag 資訊。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以透過執行以下命令來取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

上述的命令在重新啟動後不會持續存在，並且必須在任何後續重新啟動時再次使用。對於 HA 配對中的 Panorama，必須在每個 Panorama 上執行命令。

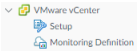
©2023 Palo Alto Networks, Inc.

STEP 1 | 選取**Panorama** > 外掛程式 。

STEP 2 | 選取 **Upload**（上傳），然後按一下 **Browse**（瀏覽）以找到外掛程式檔案。

STEP 3 | 按一下 **OK**（確定）以完成上傳。

STEP 4 | 選取外掛程式版本，在 Action（動作）欄中按一下 **Install**（安裝）來安裝外掛程式。安裝完成時，Panorama 會通知您。



設定 VMware vCenter 專用 Panorama 外掛程式

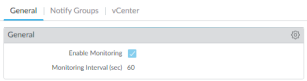
安裝外掛程式之後，請完成下列程序，以建立 Panorama 與 vCenter 之間的連線。

若要讓外掛程式監控 vCenter 環境中的虛擬機器，您必須安裝 VMware 工具。在 vCenter 中，無法在外部擷取 VM 的 IP 位址；只有透過 VMware 工具才能看到它們。此外，外掛程式需要原生唯讀權限，才能從 vCenter 擷取 IP 位址資訊。

STEP 1 | 登入 Panorama 網頁介面。

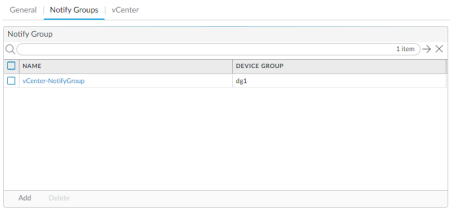
STEP 2 | 啟用監控，並設定監控間隔。

1. 選取 **Panorama** > **VMware vCenter** > **Setup**（設定） > **General**（一般）。
2. 選取 **Enable Monitoring**（啟用監控）。這會監控部署中的所有 vCenter。
3. 設定 **Monitoring Interval**（監控間隔），單位為秒。監控間隔是 Panorama 從 vCenter 擷取已更新網路資訊的頻率。預設值為 60 秒，範圍介於 60 到 84600 秒之間。



STEP 3 | 建立通知群組。

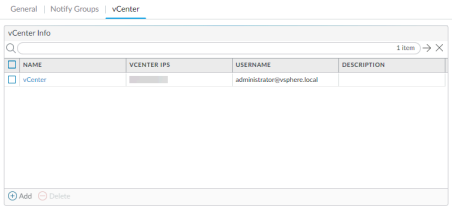
1. 選取 **Panorama** > **VMware vCenter** > **Setup**（設定） > **Notify Groups**（通知群組）。
2. 按一下 **Add**（新增）。
3. 輸入通知群組的描述性 **Name**（名稱）。
4. 選取 vCenter 部署中的裝置群組。



 ©2023 Palo Alto Networks, Inc.

STEP 4 | 新增 vCenter 資訊。VMware vCenter 專用 Panorama 外掛程式最多支援 16 個 vCenter 實例。

1. 選取 **Panorama** > **VMware vCenter** > **Setup**（設定） > **vCenter**。
2. 輸入 vCenter 的描述性 **Name**（名稱）。
3. 輸入 vCenter 和連接埠（如果適用）的 IP 位址或 FQDN。
4. 輸入 vCenter 使用者名稱。
5. 輸入並確認 vCenter 密碼。
6. 按一下 **Validate**（驗證），以確認 Panorama 可使用您輸入的登入認證連線至 vCenter。
7. 按一下 **OK**（確定）。



STEP 5 | 最多設定 16 個監控定義。

一個 *vCenter* 實例只能指派給一個監控定義。

1. 選取 **Panorama** > **VMware vCenter** > **Monitoring Definition**（監控定義），然後按一下 **Add**（新增）。
2. 輸入描述性 **Name**（名稱），並選擇性地輸入說明以識別您要使用此定義的 vCenter。
3. 選取 **vCenter** 和 **Notify Group**（通知群組）。
4. 按一下 **OK**（確定）。



STEP 6 | **Commit**（提交）您的變更。

STEP 7 | 確認您可在 Panorama 上檢視 VM 資訊，並定義動態位址群組的比對準則。

在比對準則中使用多個標籤時，必須使用 *OR* 運算子；使用 *AND* 運算子將無法運作。

部分瀏覽器延伸可能會封鎖 *Panorama* 與 *vCenter* 之間的 *API* 呼叫，進而防止 *Panorama* 接收比對準則。如果 *Panorama* 未顯示比對準則，而且您使用瀏覽器延伸，則請停用延伸，並 *[Synchronize Dynamic Objects*（同步處理動態物件）*]* 以填入 *Panorama* 可用的標籤。

©2023 Palo Alto Networks, Inc.

STEP 8 | 確認將 VM 中的位址新增至 DAG。

1. 選取 **Panorama** > **Objects**（物件） > **Address Groups**（位址群組）。
2. 在 DAG 的 [Addresses（位址）] 欄中，按一下 **More**（更多）。

   Panorama 會根據您指定的比對準則來顯示已新增至該 DAG 的 IP 位址清單。

STEP 9 | 在原則中使用動態位址群組。

1. 選取 **Policies**（政策） > **Security**（安全性）。
2. 按一下 **Add**（新增），然後輸入原則的 **Name**（名稱）和 **Description**（說明）。
3. 新增 **Source Zone**（來源區域）以指定流量來源於哪個區域。
4. 新增流量將終止於哪個 **Destination Zone**（目的地區域）。
5. 對於 **Destination Address**（目的地位址），請選取您剛才建立的動態位址群組。
6. 針對流量指定動作—**Allow**（允許）或 **Deny**（拒絕），並選擇性地將預設安全性設定檔附加至規則。
7. 重複步驟 1 到 6，建立另一個原則規則。
8. 按一下 **Commit**（交付）。

STEP 10 | 同步處理動態物件，即可隨時更新 vCenter 中的動態物件。同步處理動態物件可讓您在虛擬環境中維護變更內容，並可讓您自動更新政策規則中使用的動態位址群組，以啟用應用程式。

1. 選取 **Panorama** > **VMware vCenter** > **Monitoring Definition**（監控定義）。
2. 按一下 **Synchronize Dynamic Objects**（同步處理動態物件）。

STEP 11 | 如果重新啟動 vCenter 部署中的防火牆，或中斷與 Panorama 的連線，則該防火牆會與 vCenter 專用 Panorama 外掛程式不同步，而且不再接收更新。防火牆與 Panorama 重新連線之後，您必須手動同步處理 Panorama 與防火牆。

1. 登入 Panorama CLI。
2. 執行下列命令。

   ```
   admin@Panorama> request plugins vmware_vcenter sync
   ```


©2023 Palo Alto Networks, Inc.

ESXi 部署的疑難排解

VM-Series 防火牆的許多疑難排解步驟與 PAN-OS 的硬體版本類似。發生問題時，您應該檢查介面計數器及系統日誌檔案，必要時使用偵錯來建立擷取。

下節說明如何為某些常見的問題進行疑難排解：

- 基本疑難排解
- 安裝問題
- 授權問題
- 連線問題

基本疑難排解



網路疑難排解工具的建議事項

讓不同的疑難排解站台在虛擬化環境中擷取流量或加入測試封包很有用。安裝一般的疑難排解工具（例如 *tcpdump*、*nmap*、*hping*、*traceroute*、*iperf*、*tcpedit*、*netcat* 等），從頭開始建立全新的作業系統可能有幫助。接著可關閉這台電腦的電源並轉換至範本。每次需要工具時，很快就能夠將疑難排解用戶端（虛擬機器）部署到有問題的虛擬交換器，用以分析網路問題。完成測試時可捨棄實例，並在下次需要時再次使用範本。

關於防火牆的效能相關問題，請先檢查防火牆 Web 介面的 **Dashboard**（儀表板）。若要檢視警示，或建立技術支援或統計資料傾印檔案，請導覽至 **Device**（裝置） > **Support**（支援）。

如需 vSphere 用戶端的相關資訊，請移至 **Home**（首頁） > **Inventory**（詳細目錄） > **VMs and Templates**（**VM** 及範本），並選取 VM-Series 防火牆實例，然後按一下 **Summary**（摘要）頁籤。在 **Resources**（資源）下，檢查使用的記憶體、CPU 及儲存相關的統計資料。如需資源歷程，請按一下 **Performance**（效能）頁籤，並監控隨時間變化的資源使用情況。

安裝問題

- OVA 部署問題
- 防火牆為什麼會啟動到維護模式？
- 我如何修改 VM-1000-HV 授權的基礎映像檔？

OVA 部署問題

- VM-Series 是作為開放式虛擬化聯盟 (OVA) 格式檔案中的 zip 封存傳遞，可解壓縮為三個檔案。

  若您在部署 OVA 映像時發生問題，請確定這三個檔案已解壓縮並可存取。如有必要，請再次下載並解壓縮此 OVA 映像。

©2023 Palo Alto Networks, Inc.

- OVA 映像中的虛擬磁碟大小約 1GB。它必須存在於執行 vSphere 客戶端的電腦中，或必須可作為 OVA 映像 URL 存取。
  - 請確定 vSphere 用戶端電腦與目標 ESXi 主機之間的網路連線具備低延遲與足夠的頻寬。若連線狀況不良，則 OVA 部署可能花費數小時，或逾時後失敗。

    若您將映像託管至一個與 ESXi 主機相同網路的裝置上，則可以將問題降至最低。
  - 任何在此路徑中的防火牆必須允許來自 vSphere 客戶端至 ESXi 主機的 TCP 連接埠 902 與 443。
- ESX 6.5.0a 所建立的 4887370 限制每個通訊端為 2 個 CPU 核心。若您在部署 VM-300、VM-500 或 VM-700 時，想要在每個通訊端配置 2 個以上 vCPU，請參閱 VMware KB：https://kb.vmware.com/s/article/53354 以瞭解權宜方案。

防火牆為什麼會啟動到維護模式？

如果您已購買 VM-1000-HV 授權，並正在 VMware ESXi 伺服器上，以獨立模式部署 VM-Series 防火牆，則您必須配置 VM-Series 防火牆所需的最少記憶體。

若要避免啟動維護模式，則必須修改基礎影像檔（請參閱我如何修改 VM-1000-HV 授權的基礎映像檔？），或先在 ESXi 主機或 vCenter 伺服器上編輯設定，然後開啟 VM 系列防火牆電源。

另外，也請確認介面是否為 VMXnet3。將此介面類型設定為任何其他格式，則此防火牆將啟動維護模式。

我如何修改 VM-1000-HV 授權的基礎映像檔？

如果您已購買 VM-1000-HV 授權，並正在 VMware ESXi 伺服器上以獨立模式部署 VM-Series 防火牆，請依照這些指示，修改 VM-Series 防火牆的基礎映像檔（.ova 或 .xva）中定義的下列屬性。

重要：修改下列值以外的值將導致基礎映像檔失效。

STEP 1 | 使用 notepad 之類的文字編輯工具來開啟基礎映像檔，例如 7.0.0。

STEP 2 | 搜尋 4096 並變更配置為 5012（即 5 GB）的記憶體如下：

```
<Item> <rasd:AllocationUnits>位元組 * 2^20</
rasd:AllocationUnits><rasd:Description>記憶體
大小</rasd:Description><rasd:ElementName>4096
 MB 記憶體</rasd:ElementName><rasd:InstanceID>2</
rasd:InstanceID><rasd:ResourceType>4</
rasd:ResourceType><rasd:VirtualQuantity>4096</
rasd:VirtualQuantity><Item><rasd:AllocationUnits>位元
組 * 2^20</rasd:AllocationUnits><rasd:Description>記
憶體大小</rasd:Description><rasd:ElementName>5120MB 記
憶體</rasd:ElementName><rasd:InstanceID>2</
rasd:InstanceID><rasd:ResourceType>5</
rasd:ResourceType><rasd:VirtualQuantity>5120</rasd:VirtualQuantity>
```


©2023 Palo Alto Networks, Inc.

STEP 3 | 針對您的部署，視需要將虛擬 CPU 核心數從 2 變更為 4 或 8：

```
<Item> <rasd:AllocationUnits>赫茲 * 10^6</
rasd:AllocationUnits><rasd:Description>虛擬 CPU 數
量</rasd:Description><rasd:ElementName>2 個虛
擬 CPU</rasd:ElementName><rasd:InstanceID>1</
rasd:InstanceID><rasd:ResourceType>3</
rasd:ResourceType><rasd:VirtualQuantity>2</
rasd:VirtualQuantity><vmw:CoresPerSocket ova:required="false">2</
vmw:CoresPerSocket></Item><Item><rasd:AllocationUnits>赫
茲 * 10^6</rasd:AllocationUnits><rasd:Description>虛
擬 CPU 數量</rasd:Description><rasd:ElementName>4 個
虛擬 CPU</rasd:ElementName><rasd:InstanceID>1</
rasd:InstanceID><rasd:ResourceType>3</
rasd:ResourceType><rasd:VirtualQuantity>4</
rasd:VirtualQuantity><vmw:CoresPerSocket ova:required="false">2</
vmw:CoresPerSocket> </Item>
```

此外，您也可以部署防火牆，並在開啟 VM-Series 防火牆電源前，在 ESXi 主機或 vCenter 伺服器上直接編輯記憶體和虛擬 CPU 配置。

授權問題

- 為什麼我無法套用支援或功能授權？
- 為什麼我的複製 VM-Series 防火牆沒有有效的授權？
- 移動 VM-Series 防火牆是否會造成授權失效？

為什麼我無法套用支援或功能授權？

您是否已經在 VM-Series 防火牆上套用容量驗證碼？在可以啟動支援或功能授權前，必須先套用容量驗證碼，讓設備可以取得序號。需要此序號才能在 VM-Series 防火牆上啟動其他授權。

為什麼我的複製 **VM-Series** 防火牆沒有有效的授權？

VMware 可將唯一的 UUID 指定給每一個虛擬機器（包括 VM-Series 防火牆）。因此在複製 VM-Series 防火牆時，會將新 UUID 指定給它。由於 VM-Series 防火牆之每個實例的序號和授權皆繫結至 UUID，因此複製授權的 VM-Series 防火牆將產生內含無效授權的新防火牆。您需要新的驗證碼，才能在最近部署的防火牆上啟動授權。您必須套用容量驗證碼和新的支援授權，才能在 VM-Series 防火牆上取得完整的功能、支援和軟體升級。

移動 **VM-Series** 防火牆是否會造成授權失效？

如果您手動將 VM-Series 防火牆從一部主機移至另一部主機，請確定選取 **This guest was moved**（已移動此來賓）選項以防止授權失敗。

連線問題

- 為什麼 VM-Series 防火牆不會接收任何網路流量？

©2023 Palo Alto Networks, Inc.

為什麼 VM-Series 防火牆不會接收任何網路流量？

在 VM-Series 防火牆上檢查流量日誌（**Monitor**（監控） > **Logs**（日誌））。如果日誌空白，請使用下列 CLI 命令來檢視 VM-Series 防火牆介面上的封包：

```
show counter global filter delta yes 全域計數器：自上次採樣以來的經過時間：594.544 秒
  ---------------------------------------------------------------------------
示的總計數器：0
  ---------------------------------------------------------------------------
```

在 vSphere 環境中檢查下列問題：

- 檢查連接埠群組，並確認防火牆和虛擬機器位於正確的連接埠群組

  確定已正確對應介面。

  網路介面卡 1 = 管理

  網路介面卡 2= Ethernet1/1

  網路介面卡 3= Ethernet1/2

  對於每一個虛擬機器，檢查設定來驗證介面對應至正確的連接埠群組。
- 確認已為每一個連接埠群組或整個交換器啟用混合式模式，或已將防火牆設定為 Hypervisor 指派的 MAC 位址。

  由於資料平面 PAN-OS MAC 位址不同於 vSphere 指定的 vNIC MAC 位址，因此如果未啟用 Hypervisor 指派的 MAC 位址，連接埠群組（或整個 vSwitch）必須採用混合式模式：

  - 在 vSphere 上檢查 VLAN 設定。

    vSphere 連接埠群組的 VLAN 設定有兩個用途：它能決定哪些連接埠群組共用 Layer 2 網域，及決定是否標記上行連接埠 (802.1Q)。
  - 檢查實體交換器連接埠設定

    若在包含上行連接埠的連接埠群組上指定 VLAN ID，vSphere 會使用 802.1Q 來標記輸出框架。標籤必須符合實體交換器上的組態，否則無法傳遞流量。

    如果使用虛擬散佈交換器 (vDS)，請檢查連接埠統計資料；標準交換器不會提供任何連接埠統計資料

©2023 Palo Alto Networks, Inc.

ESXi 專用 VM-Series 的效能調整

ESXi 專用 VM-Series 防火牆是高效能裝備，但可能需要調整 Hypervisor，才能達到最佳結果。本節說明一些最佳作法和建議，有助於發揮 VM-Series 防火牆的最佳效能。為了發揮最佳效能，建議使用 ESXi 6.0.0.0 或更新版本。

- 在 ESXi 上安裝 NIC 驅動程式
- 在 ESXi 上啟用 DPDK
- 在 ESXi 上啟用 SR-IOV
- 透過 SR-IOV 啟用 ESXi VLAN 存取模式
- 在 ESXi 上啟用 NIC 的多佇列支援
- VNF 效能調整

在 ESXi 上安裝 NIC 驅動程式

為了發揮最佳效能，請搭配 Intel 10GB 網路介面使用 SR-IOV，這需要 ixgbe 4.4.1 驅動程式才能支援每個介面使用多重介面。

STEP 1 | 取得 ESXi 主機上的網路介面清單。

1. 登入 ESXi 主機 CLI。
2. 使用下列命令傳回網路介面清單：

```
$ esxcli network nic list
```

STEP 2 | 決定特定介面的驅動程式版本。

您可以使用 **ethtool** 或 **esxcli**，以決定目前安裝的驅動程式版本。下列範例使用 vNIC4 並傳回驅動程式版本 3.21.6。

- ethtool—**ethtool -l *<nic-name>***

```
$ ethtool -I vNIC4 driver: ixgbe version:3.21.6iov 韌體版
本: 0x80000389 匯流排資訊: 0000:04:00.0
```

- esxcli—**esxcli network nic get -n *<nic-name>***

```
$ esxcli network nic get -n vNIC4 公告自動交涉: true 公告連結
模式: 自動交涉: true 纜線類型: 目前訊息層級: 7 驅動程式資訊: 匯流排資
訊:0000:04:00.0 驅動程式: ixgbe固件版本: 0x80000389 版本: 3.21.6iov 偵
測到連結: false 連結狀態: 關閉 名稱: vNIC4 PHYAddress:0 暫停自動
交涉: true 暫停 RX: true 暫停 TX: true 支援連接埠: 光纖 支援自動交
涉: true 支援暫停: true 支援喚醒: false 收發器: 外部 喚醒: 無
```


©2023 Palo Alto Networks, Inc.

STEP 3 | 安裝新的驅動程式。

1. 從 VMware 網站下載 ixgbe 4.4.1 驅動程式。解壓縮內容至本機目錄，並找到驅動程式的 .zip 或 .vib 檔案。
2. 在 ESXi 主機資料存放區建立新的資料夾。
3. 複製您已解壓縮至 ESXi 主機資料存放區新建資料夾的本機 .zip 或 .vib 檔案。
4. 在 ESXi 主機上啟用維護模式。
5. 使用下列命令之一安裝新的驅動程式，使用 -d 表示 .zip 檔案， -v 表示 .vib 檔案。

   - ```
     $ esxcli software vib install -d <path to driver .zip file>
     ```
   - ```
     $ esxcli software vib install -v <path to driver .vib file>
     ```

   您必須指定 .zip 或 .vib 檔案的絕對路徑。例如：

   ```
   $ esxcli software vib install -d "/vmfs/volumes/
   Datastore/DirectoryName/DriverName.zip"
   ```
6. 驗證 VIB 安裝。

   ```
   $ esxcli software vib list
   ```
7. 重新啟動 ESXi 主機。

在 ESXi 上啟用 DPDK

Data Plane Development Kit（資料平面開發套件；DPDK）可加快網路介面卡 (NIC) 封包處理速度，以提升 VM-Series 效能。在 VM-Series 防火牆上，ESXi 上依預設會啟用 DPDK。

若要利用 DPDK，您使用的 NIC 必須搭配 DPDK 驅動程式版本所述其中一個支援的 DPDK 驅動程式：

如果您停用 DPDK，則 NIC 會使用 PacketMMap 而非 DPDK。您可使用命令 **set system setting dpdk-pkt-io off** 停用 DPDK。

請參閱 ESXi 超管理器支援及 PacketMMAP 和 DPDK 驅動程式支援的相容性矩陣（依 PAN-OS 版本分組）。

在 ESXi 上啟用 SR-IOV

Single root I/O virtualization（單一根 I/O 虛擬化 - SR-IOV）可讓單一根埠下的單一 PCIe 實體裝置，以多個單獨實體裝置呈現給 Hypervisor 或來賓。在 SR-IOV NIC 上啟用虛擬功能裝置來啟用 SR-IOV，並在 vCenter 中修改來賓設定。

ESXi 專用 VM-Series 上的 SR-IOV 需要 PacketMMAP 驅動程式版本所述的其中一個 Intel NIC 驅動程式。請參閱「相容性矩陣」，以瞭解 PAN-OS 版本支援的 SR-IOV 和 DPDK 驅動程式。

有兩種方法可在 ESXi 上啟用 SR-IOV。

©2023 Palo Alto Networks, Inc.

- **SR-IOV** 傳遞—使用此方法時，您在 SR-IOV NIC 上啟用虛擬功能裝置，然後在 vCenter 中修改來賓設定，將 SR-IOV VF 介面新增為介面卡類型「SR-IOV 傳遞」。請參閱將虛擬功能當作 SR-IOV 傳遞介面卡指派給虛擬電腦。

  此方法（適用於 PAN-OS 8.1.2 和更新版本）可讓您將 SR-IOV PF 新增至 vSwitch 或 DvSwitch。

- **PCI Adaptor**（**PCI** 介面卡）—PAN-OS 8.0 至 8.1.1 需要此方法。您可以在 8.1 部署指南的在 ESXi 上啟用 SR-IOV 中，檢視 PCI 介面卡工作流程。

  在您啟用 SR-IOV 的實體連接埠上，您無法設定 vSwitch，這是 PCI 介面卡方法的限制。VM-Series 防火牆對於實體連接埠及該介面上相關聯的虛擬功能 (VF)，必須具有獨佔存取權，才能與主機或網路上的其他虛擬電腦通訊。請參閱在 vSphere Web 用戶端新增 PCI 裝置。

透過 SR-IOV 啟用 ESXi VLAN 存取模式

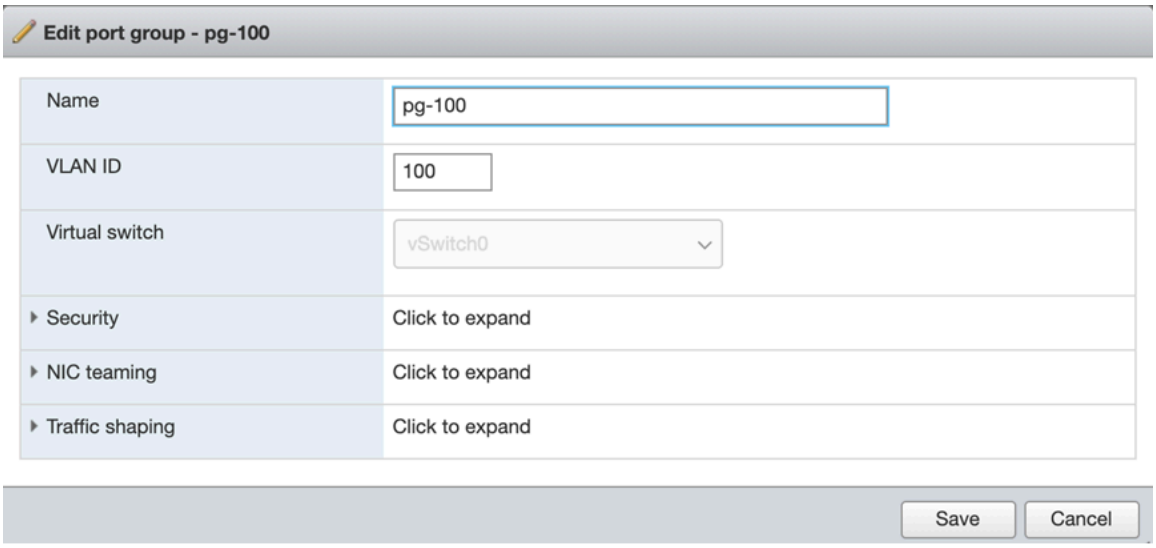
ESXi 上的 VM-Series 防火牆可在 VLAN 存取模式中運作，以支援某些使用案例，其中，防火牆部署為 virtual network function（虛擬網路功能；VNF），在多租用戶雲端/資料中心環境中提供安全性即服務。在 VLAN 存取模式中，每個 VNF 在每個網路都有專用的虛擬網路介面 (VNI)，且無需 VLAN 標籤即可傳送和接收送往/來自 SR-IOV 虛擬功能 (VF) 的封包；您可以在主機 Hypervisor 的實體和虛擬功能上啟用此功能。當您隨後在 VM-Series 防火牆上啟用 VLAN 存取模式時，防火牆無需 VLAN 標籤即可在其所有資料平面介面間傳送和接收流量。此外，如果您設定 QoS 原則，防火牆即會在存取介面上強制執行 QoS，並且以不同的方式處理多租用戶部署中的流量。

根據預設，*ESXi* 上的 *VM-Series* 防火牆在 *VLAN* 主幹模式中運作。

©2023 Palo Alto Networks, Inc.

STEP 1 | 在主機系統上，設定要在 VLAN 存取模式中運作的實體和虛擬功能。

1. 在 VMware Host Client 詳細目錄中，按一下 **Networking**（網路），然後按一下 **Port groups**（連接埠群組）。
2. 在您要編輯的清單中，以滑鼠右鍵按一下連接埠群組，然後選取 **Edit settings**（編輯設定）。輸入新連接埠群組的 **Name**（名稱）。針對 **VLAN ID** 輸入新的值。



若要讓 *VM-Series* 防火牆發揮最佳效能，請務必：

- 啟用 *CPU* 釘選。
- 停用重播防護（如果您已設定 *IPSec* 通道）。

  在防火牆網頁介面上，選取 ***Network***（網路） **> *IPSec Tunnels***（***IPSec*** 通道），然後選取 *IPSec* 通道，按一下 ***General***（一般），選取 ***Show Advanced Options***（顯示進階選項），然後清除 ***Enable Replay Protection***（啟用重播防護）。

STEP 2 | 在 VM-Series 防火牆上存取 CLI。

STEP 3 | 啟用 VLAN 存取模式。

```
request plugins vm-series vlan-mode access-mode on
```

on 會啟用 VLAN 存取模式；若要使用 VLAN 主幹模式，請輸入 **request plugins vm-series vlan-mode access-mode off**。

STEP 4 | 重新啟動防火牆。

```
request restart system
```

STEP 5 | 確認 VLAN 模式設定。

```
show plugins vm-series vlan-mode
```


©2023 Palo Alto Networks, Inc.

在 ESXi 上啟用 NIC 的多佇列支援

多重佇列可讓網路效能隨著 vCPU 數目而調整，還能建立多個 TX 和 RX 佇列來平行處理封包。修改 .vmx 檔案或存取 Advanced Settings（進階設定）來啟用多重佇列。

STEP 1 | 啟用多重佇列。

1. 開啟 .vmx 檔案。
2. 新增下列參數：

```
ethernetX.pnicFeatures = “4”
```

STEP 2 | 啟用 receive-side scaling（接收端調整規模 - RSS）。

1. 登入 ESXi 主機上的 CLI。
2. 執行下列命令：

```
$ vmkload_mod -u ixgbe $ vmkload_mod ixgbe RSS=”4,4,4,4,4,4”
```

STEP 3 | 為了發揮最佳效能，請為每個乙太網路/vSwitch 裝置配置更多執行緒。這受限於 ESXi 主機上可用的備用 CPU 資源數量。

1. 開啟 .vmx 檔案。
2. 新增下列參數：

```
ethernetX.ctxPerDev = “1”
```

VNF 效能調整

本主題提供 VM-Series 部署的 VNF 調整指導。可供參考協助您為 VM-Series 部署選擇一些參數設定。嘗試調整之前，請熟悉在 VMware vSphere Hypervisor (ESXi) 上安裝 VM-Series 防火牆的步驟，包括如何設定調整參數和屬性。

本指導可能不適用於以 *SD-WAN*、*MSSP* 或 *CSSP* 使用案例為對象的白箱或灰箱環境上的 *VM-Series* 部署。

VM-Series 是高效能設備，有各種規格，取決於尺寸、超管理器佔地面積，以及私人或公共雲端中的部署位置。

變更全域和主機層級設定會影響相同主機上執行的其他 VM。請考慮任何利弊得失，慎選您的部署最適合的參數。

- ESXi 調整參數
- 使用案例
- 參考

©2023 Palo Alto Networks, Inc.

ESXi 調整參數

為了在 VM-series 上獲得最佳效能，您可以調整硬體、超管理器和網路 I/O 參數。

此處提及的參數不見得適用於每一種部署模型。

- BIOS 設定
- 實體設定
- 虛擬 NIC 設定
- NUMA 和資源考量

BIOS 設定

本節推薦可增強 VM-Series 防火牆效能的 BIOS 電源管理、超執行緒和 Intel VT-D 設定，最後以範例 BIOS 設定來舉例說明。

- 電源管理
- 超執行緒
- Intel Virtualization Technology for Directed I/O
- 範例 BIOS 設定

電源管理

對於延遲敏感性應用程式，任何形式的電源管理會拖延閒置系統（處於多種省電模式的其中一種）回應外部事件的歷程。VMware 建議將 BIOS 電源管理設定設為「靜態高效能」（無作業系統控制的電源管理），實際停用任何形式的主動電源管理。配備 Intel Nehalem 等級和更高等級 CPU（Intel Xeon 55xx 和更高等級）的伺服器提供其他兩個電源管理選項：C-states 和 Intel Turbo Boost。

放任 C-states 啟用會增加記憶體延遲，因此，對於低延遲的工作負載，不建議如此。即使是增強型 C-state（稱為 C1E），也會延遲更久才喚醒 CPU 從暫停（閒置）狀態變成全功率。VMware 建議在 BIOS 中停用 C1E，以進一步縮短延遲。

- 對於 HP，請將 [Power Regulator Mode（電源調節器模式）] 設為 [Static High Mode（靜態高模式）]，並停用 [QPI Processor（QPI 處理器）]、[C-state support（C-state 支援）] 和 [C1E Support（C1E 支援）]。
- 對於 Dell，請將 [Power Management Mode（電源管理模式）]、[CPU power（CPU 電源）] 和 [Performance Management（效能管理）] 設為 [Maximum Performance（最高效能）]。

另一個需要考慮的參數是 P-states。為了徹底發揮效能，請在 BIOS 上停用 P-state 設定。

Intel Turbo Boost 經過一段時間可能導致效能變化。為了保持一致又穩定的效能，請停用 Turbo Boost。

超執行緒

如果硬體和 BIOS 支援超執行緒，ESXi 會自動在主機上啟用超執行緒。為了讓 VM-series 防火牆發揮最佳效能，請在 ESXi 主機上停用超執行緒。

©2023 Palo Alto Networks, Inc.

如果部署環境需要啟用超執行緒，請務必從存取 PCI 裝置的相同 NUMA/Socket 節點，預留所有 CPU 資源給 VM-Series 防火牆。

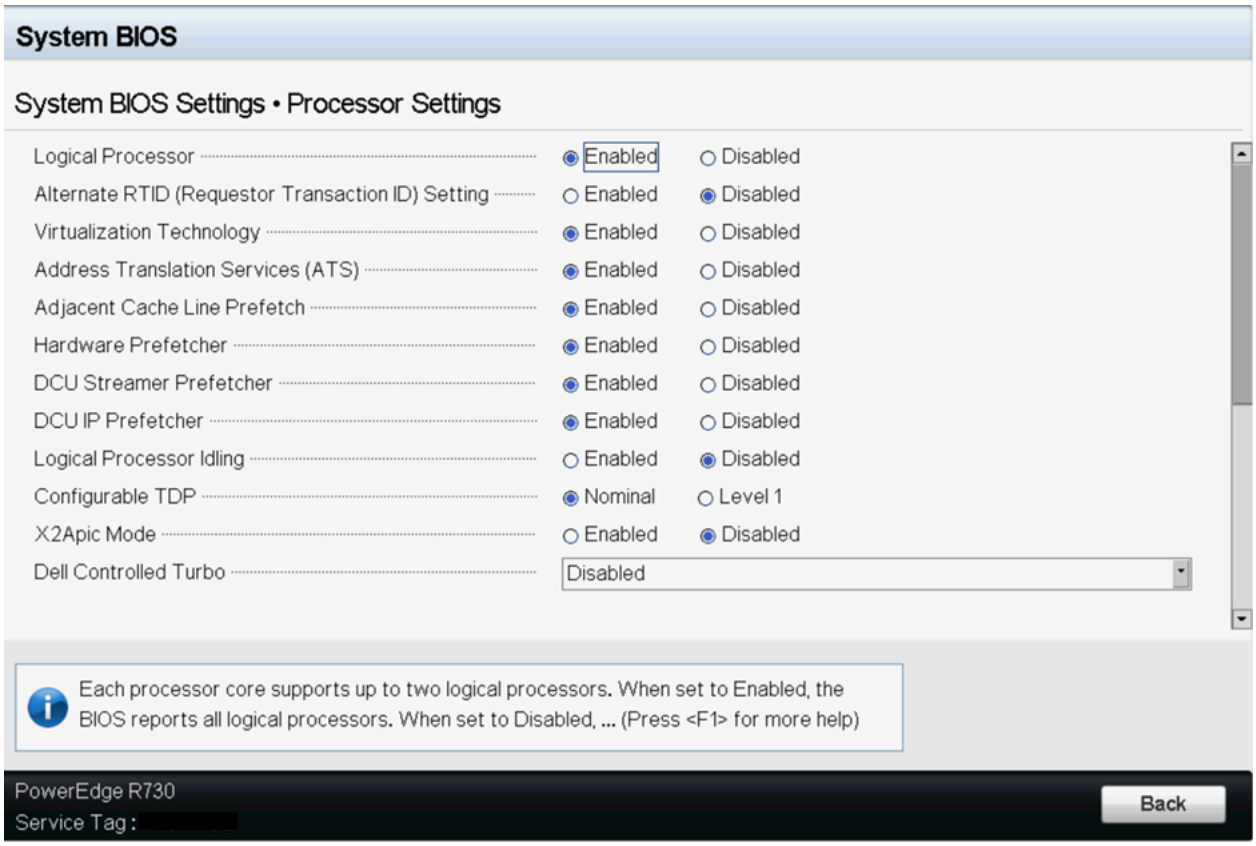
總之，請將 PA-VM 設定成單一 NUMA VM。如需詳細資訊，請參閱NUMA 和資源考量。

Intel Virtualization Technology for Directed I/O

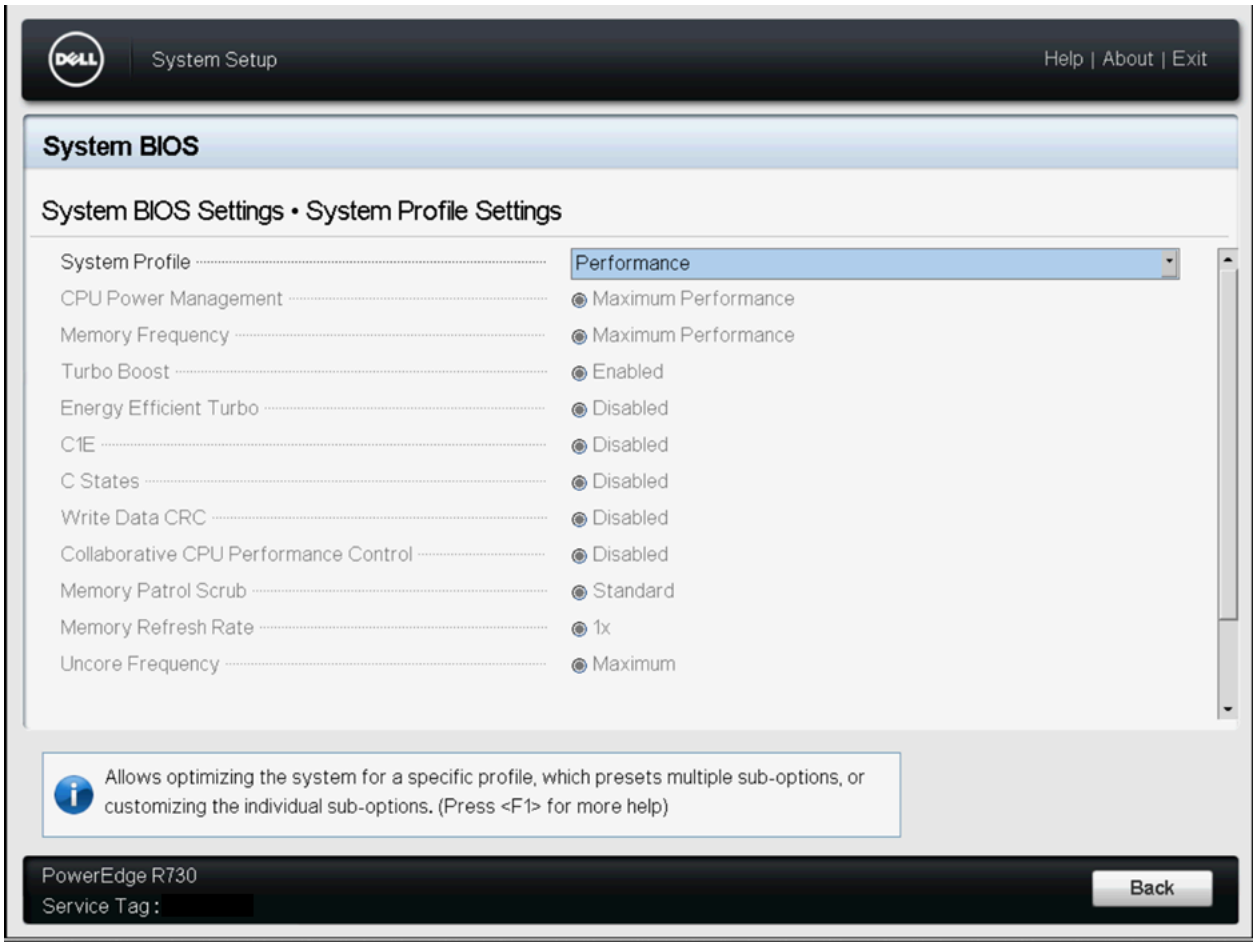
Intel Virtualization Technology for Directed I/O (Intel VT-D) 可將 LAN 卡專用於來賓系統，以展現高於模擬 LAN 卡的網路效能。請在 BIOS 上啟用此功能。如果您打算利用 SR-IOV 提高效能（建議），請啟用 SRI-OV BIOS 設定。

範例 **BIOS** 設定

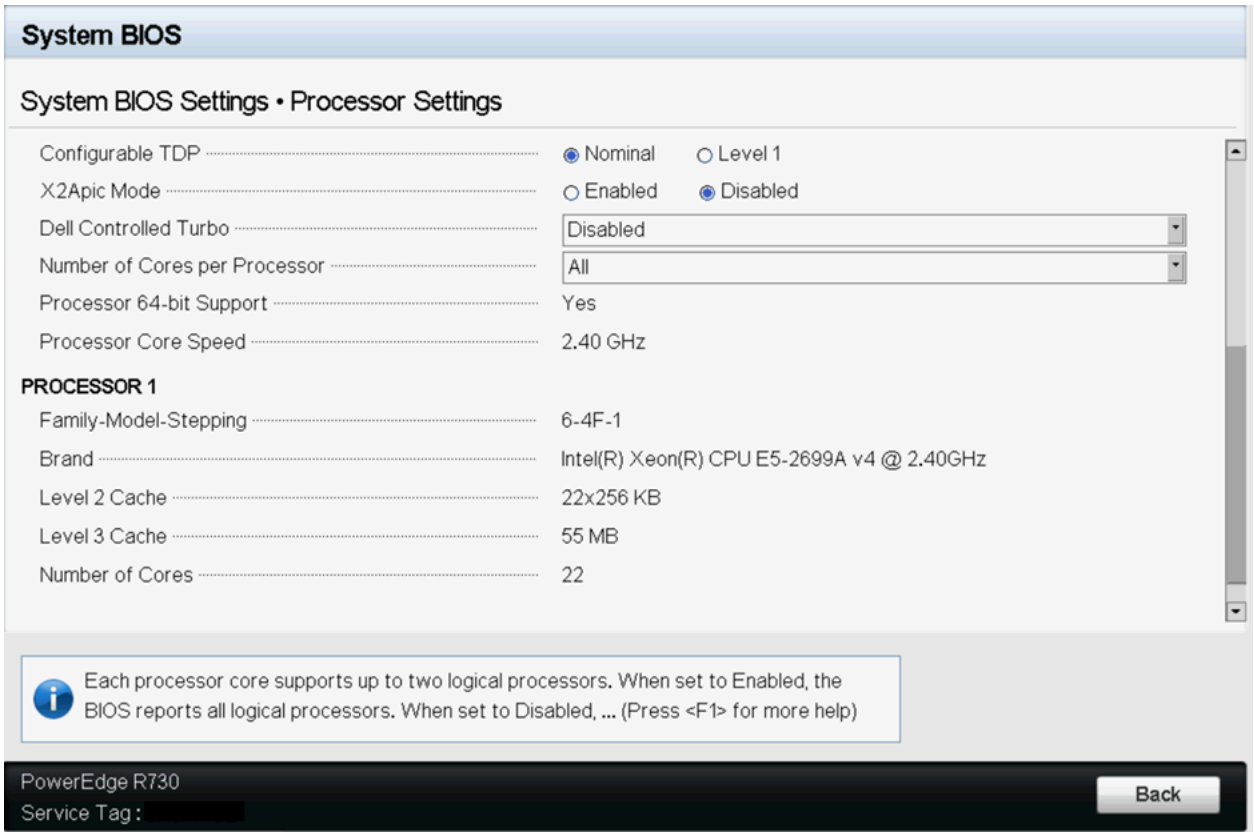
下列螢幕擷取畫面顯示 Dell BIOS 中的系統設定檔設定和處理器設定。



 ©2023 Palo Alto Networks, Inc.



©2023 Palo Alto Networks, Inc.



實體設定

大多數 1 GbE 或 10 GbE 網路介面卡 (NIC) 都支援一個稱為插斷仲裁或插斷節流的功能，可聯合從 NIC 到主機的插斷，以免主機不堪負荷而耗盡所有 CPU 週期來處理插斷。不過，對於延遲敏感性工作負載，收到封包或成功在網路上傳送封包時，NIC 延遲傳遞插斷的時間，就是工作負載延遲更久的時間。為了讓 PA-VM 發揮最佳效能，請停用插斷仲裁。例如，在 ESXi 主機上停用實體 NIC 插斷仲裁，如下所示：

```
# esxcli system module parameters set -m ixgbe -p
 "InterruptThrottleRate=0"
```

- 傳輸佇列
- 佇列配對

傳輸佇列

對於排入佇列中等待傳輸的封包，ESXi 上行 pNIC 層也維護一個軟體 Tx 佇列，依預設保留 500 個封包。如果工作負載是 I/O 密集型，且傳輸封包大量爆增，則此佇列可能溢滿，導致上行層丟棄封包。使用下列 ESXi 命令可以將 Tx 佇列擴大到最多 10,000 個封包：

```
# esxcli system settings advanced set -i 10000 -o /Net/
MaxNetifTxQueueLen
```


©2023 Palo Alto Networks, Inc.

視 ESXi 主機上使用的實體 NIC 和特定版本的 ESXi 驅動程式而定，有時因為 pNIC 上的傳輸環太小又填滿，pNIC 驅動程式中可能丟棄封包，。大多數 pNIC 驅動程式允許讓您使用下列命令來擴大傳輸環：

```
# ethtool -G vmnic0 tx 4096
```

此命令將 Tx 環擴大為 4096 個項目。使用下列命令可以查明特定 pNIC 驅動程式可設定的大小上限，以及目前實際上的 Tx 環大小：

```
# ethtool -g vmnic0
```

```
vmnic0 的環參數：預設最大值：RX：4096 RX Mini：0 RX Jumbo：0 TX：4096 目前硬體設定：RX：512 RX Mini：0 RX Jumbo：0 TX：4096
```

佇列配對

有些 pNIC 驅動程式（例如 Intel 的 ixgbe 和 Broadcom 的 bnx2x）也支援「佇列配對」，對於 ESXi 上行層而言，這表示接收執行緒 (NetPoll) 還會將配對傳輸佇列上傳輸的封包處理完畢。對於某些頻繁傳輸的工作負載，這會造成延遲將傳輸處理完畢，導致 vNIC 的傳輸環已無空間再傳輸更多封包，迫使來賓作業系統中的 vNIC 驅動程式丟棄封包。

對 ESXi 主機上的所有 pNIC 停用佇列配對，即可建立單獨的執行緒將 pNIC 傳輸處理完畢。因此會及時處理完畢，在 vNIC 的傳輸環中釋出空間來傳輸更多封包。

停用佇列配對的 ESXi 命令如下：

```
# esxcli system settings advanced set -o /Net/
NetNetqRxQueueFeatPairEnable -i 0
```

您必須重新啟動 ESXi 主機，這才會生效。

如果在專用主機上使用 *VM-700* 的 *PCI* 通道，則 *NIC/NIC* 驅動程式不需要調整效能。但這種部署模式不常見。

虛擬 **NIC** 設定

如有可能，請使用 SR-IOV 以提高效能，如下列主題所述：

- SR-IOV
- VMXNET3/vSwitch 和虛擬插斷聯合
- 在 Intel x710/x520 上啟用多佇列支援

SR-IOV

- 變更 SR-IOV 驅動程式的模組參數之後需要重新啟動 ESXi 主機。

©2023 Palo Alto Networks, Inc.

- 在 ESXi 主機上停用實體 NIC 插斷仲裁，如下所示：

```
# esxcli system module parameters set -m ixgbe -p
 "InterruptThrottleRate=0 “
```

- 如果您啟用多佇列支援，則還必須對驅動程式啟用 Receive-Side Scaling（接收端調整規模 - RSS）。
  - 若要啟用 RSS，請將連接埠值設為 4。
  - 以逗號分隔字串指定連接埠。

  範例—設定 3 個 NIC，各有 2 個連接埠。

```
$ vmkload_mod -u ixgbe esxcli system module parameters set -m ixgbe
 -p RSS=” 4,4,4,4,4,4”
```

```
$ vmkload_mod ixgbe RSS=” 4,4,4,4,4,4”
```

  範例—對單一連接埠設定 RSS：

```
$ vmkload_mod -u ixgbe esxcli system module parameters set -m ixgbe
 -p RSS=” 0,4,0,0,0,0”
```

VMXNET3/vSwitch 和虛擬插斷聯合

根據預設，VMXNET3 支援插斷聯合演算法（基於相同理由，實體 NIC 實作插斷仲裁）。為了避免太多插斷湧入主機系統，收集封包時會為多個封包產生單一插斷。這稱為插斷聯合。

插斷聯合是指在您發出強制插斷之前，網路介面接收的流量，或收到流量之後經過的時間量。太快或太頻繁插斷會導致系統效能不佳，因為核心會停止（或「插斷」）執行中的工作，以處理來自硬體的插斷要求。如果流量來不及從 NIC 離開，則太遲插斷可能導致流量遺失—更多流量抵達，覆蓋先前仍等著核心接收的流量。若要透過 vSphere Web 用戶端停用此功能，請前往 **VM Settings**（**VM** 設定） > **Options**（選項） > **Advanced General**（進階一般） > **Configuration Parameters**（設定參數），為 **ethernetX.coalescingScheme** 新增一筆項目，值為 **disabled**。

若要對主機上的所有虛擬 NIC 停用虛擬插斷聯合（影響所有 VM，而不只是延遲敏感性的 VM 而已），請設定進階網路效能選項。前往 **Configuration**（設定） > **Advanced Settings**（進階設定） > **Net**（網路），將 **CoalesceDefaultOn** 設為 **0**（停用）。

在 **Intel x710/x520** 上啟用多佇列支援

使用 ESXi 6.0.0 或更新版本，搭配支援多佇列的 ixgbe 驅動程式版本。請參閱相容性矩陣中的 SR-IOV 驅動程式版本。修改 **.vmx** 檔案或存取 **Advanced Settings**（進階設定）以啟用多佇列支援：

```
ethernetX.pnicFeatures = “4”
```

若要設定多核關聯性以便 vSwitch 可以超過 300K PPS，請設定：

©2023 Palo Alto Networks, Inc.

```
ethernetX.pnicFeatures = “4” ethernetX.ctxPerDev = “1 "
```

設定 **ethernetX.ctxPerDev = “1”** 就像一個二進制旗標（設置為 1 以啟用）。此二進位旗標會新增 CPU 執行緒，只處理來自連接埠 **ethernetX** 的流量。這樣可提升流量排程效能。

NUMA 和資源考量

NUMA 的全名是 Non-Uniform Memory Access（非統一記憶體存取）。多核心處理器的設計很複雜。為了解決這種系統的效能問題，您需要知道 NUMA 與 CPU 釘選的所有細微差別。必須查明的事項：

- 執行緒在哪些核心上執行？（如果已啟用超執行緒，請查看超執行緒）
- vCPU 在哪些核心上執行？（親和性）
- 實體 NIC 安裝在哪個 NUMA 插槽？
- 記憶體配置在何處？（NUMA 效應）

  任何插槽上執行的執行緒會看到一個統一記憶體空間 – 因此，可讀取/寫入其他插槽的區域記憶體。
- 節點上的不同插槽之間共用記憶體嗎？
- 存取不同插槽上的記憶體比存取區域記憶體花更多時間。

  NUMA 效應是指執行緒過度存取不同 NUMA 範圍內的記憶體。為了防止跨 NUMA 的問題，請避免 Socket 0 和 Socket 1 之間的通訊使用 Quick Path Interconnect（快速路徑互連 - QPi）。

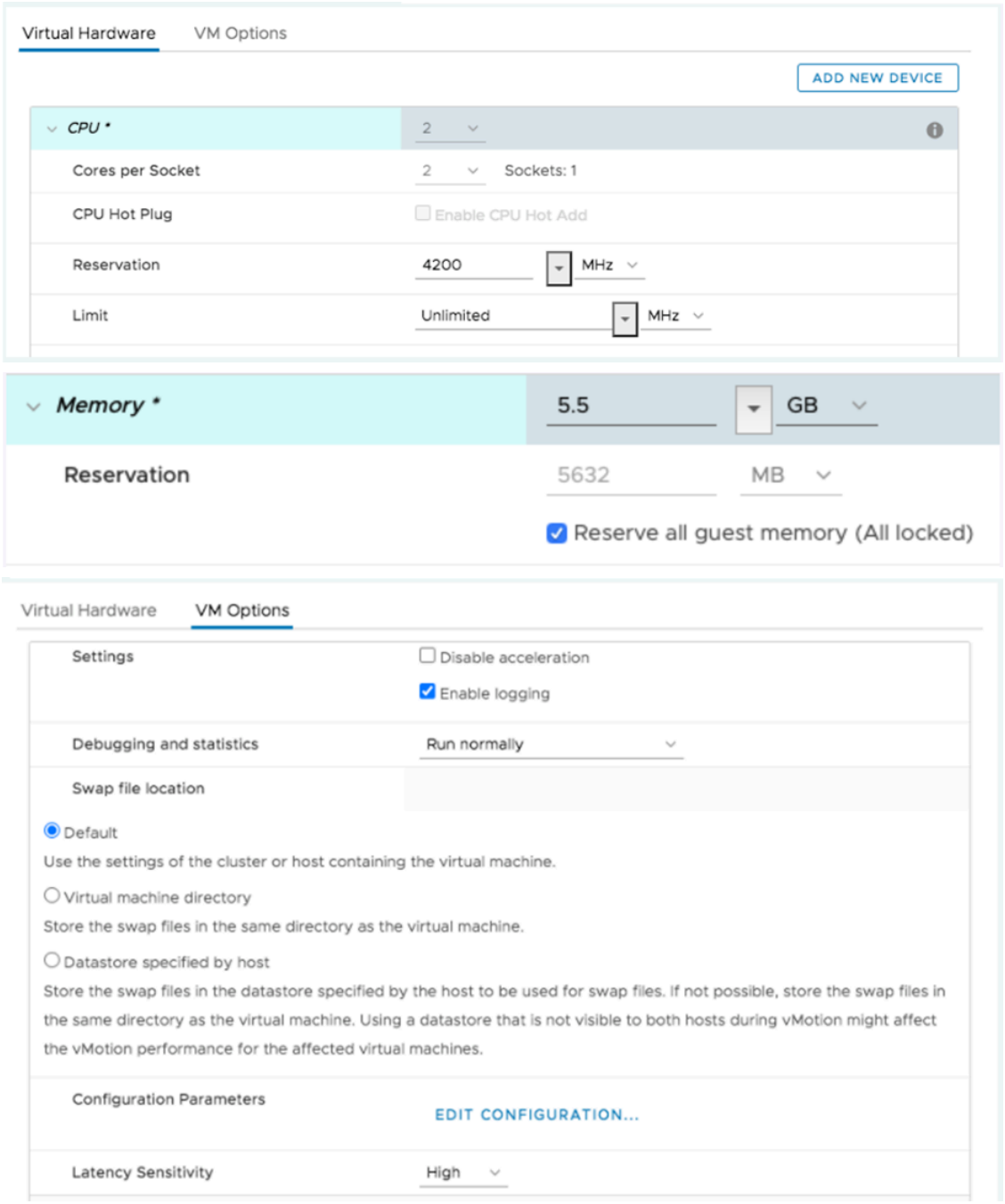
對於延遲敏感性 VM（例如 PA-VM），VMware 建議您不要投入太多 vCPU，而超過 ESXi 主機上的實體 CPU（處理器）數量。例如，如果主機有 8 個 CPU 核心，請將 VM 的 vCPU 數量限制為 7。這可確保 ESXi VMkernel 排程器更有可能將 vCPU 放在不與其他排程脈絡競爭的 pCPU 上，例如來自其他 VM 或 ESXi 協助程式領域的 vCPU。最好確保您配置給 VM 的 vCPU 數量不超過 VM 中目前耗用 CPU 的處理序或執行緒數量。

為了獲得最佳效能，所有 vCPU 都應該排定在相同 NUMA 節點上，且應該從連接至該 NUMA 節點的區域實體記憶體供給並配置所有 VM 記憶體。這可以透過 VM 設定 **numa.nodeAffinity=0, 1,** … 來變更，其中 0、1 等等是插槽號碼。

若要確保 VM 獨佔存取 CPU 資源，請將 [Latency Sensitivity（延遲敏感度）] 設為 [High（高）]。為了讓新的設定生效，VM CPU 保留必須設為最大，記憶體應該保留，而 CPU 限制必須設為無限制。

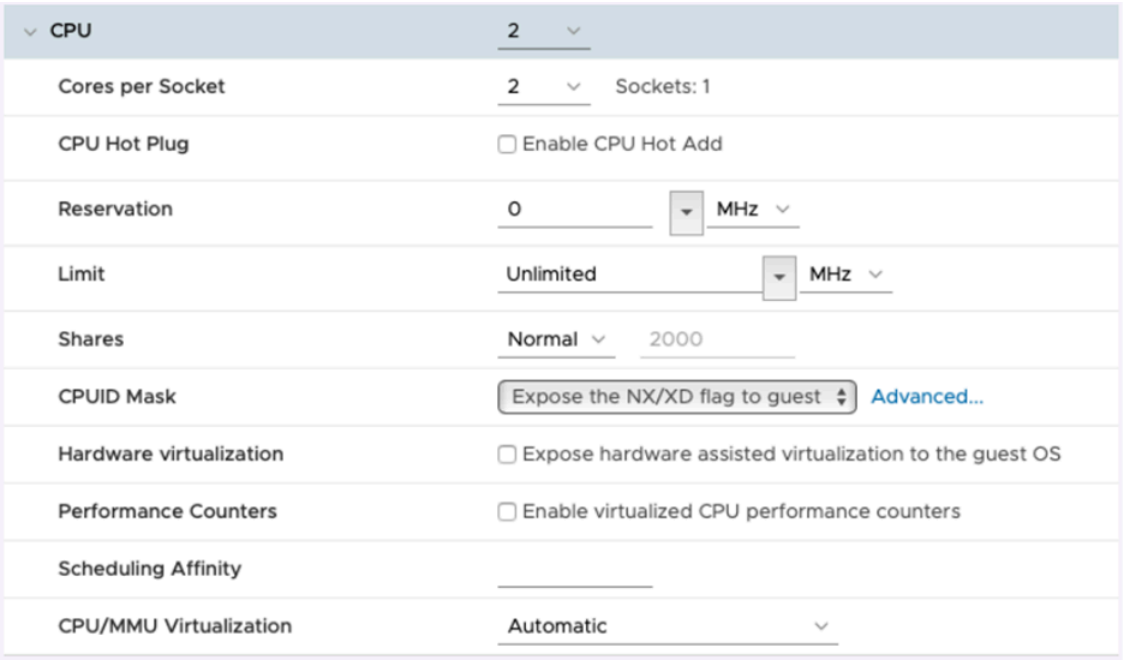
- 在較新版本中，請使用 vSphere Web 用戶端將 [VM Latency Sensitivity（VM 延遲敏感度）] 選項設為 [High（高）]（預設值為 [Normal（正常）]）。
- 在較舊版本中，請將 **sched.cpu.latencySensitivity** 設為 [High（高）]。

©2023 Palo Alto Networks, Inc.



此外，還可使用 VM 設定 **Host Affinity**（主機親和性），將 VM 的 vCPU 釘選到主機 CPU 核心，如此就絕不會排定到不同的核心。使用主機親和性時，請謹記 NUMA 和超執行緒。如果系統負荷過度，請避免設定主機親和性。如需詳細資訊，請參閱 CPU 相似性的潛在問題。

©2023 Palo Alto Networks, Inc.



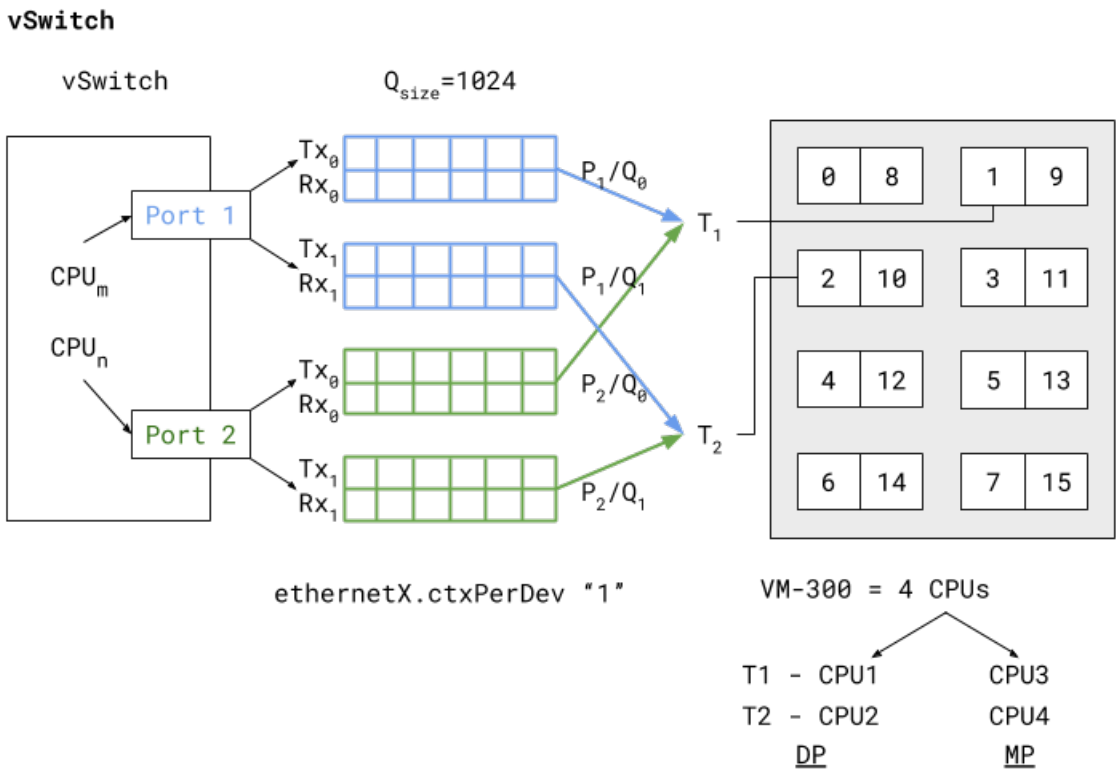
實作調整參數後，請使用 esxtop 或 CPU 圖表來檢查 VM 的 CPU 就緒 (%RDY) 和共同停止 (%CSTP)。這兩個值都應該接近 0%，以確保獨佔存取 CPU 資源。您也可以使用 esxtop 來檢查 NUMA 使用情況，並確保 VM 的記憶體資源未分散於 NUMA 節點。如需詳細資訊，請參閱判讀 esxtop 統計資料。

使用案例

使用案例 **1**：**vSwitch** 部署

下圖顯示 ESXi 主機上部署的 PA-VM，其中資料連接埠「連接埠 1」和「連接埠 2」連結至 PA-VM 的 eth1 和 eth2。每個連接埠裝載兩個佇列配對（例如，Tx0/Rx0 和 Tx1/Rx1）或已啟用多佇列。

©2023 Palo Alto Networks, Inc.



對於往返多個佇列收送的封包，啟用多佇列和 RSS 來負載平衡可增強處理效能。根據 vCPU 至連接埠/佇列對應的內部邏輯（在此案例中），抵達和離開 P1/Q0 和 P2/Q0 的封包由執行於（即釘選至）vCPU1 的資料平面工作 T1 來處理。資料平面工作 T2 遵循類似的關聯，如以上 vSwitch 部署圖所示。

兩個資料平面工作分別在 vCPU1 和 vCPU2 上執行，這些為非同層級 CPU（表示在超執行緒情況下不共用相同核心）。這表示即使啟用超執行緒，工作指派也可以釘選至不同核心，以提高效能。另外，這些資料平面工作 vCPU 全部屬於相同的 NUMA 節點（或插槽），可避免 NUMA 相關的效能問題。

擴大佇列，並將 vCPU 或執行緒專用於連接埠以排定往返於這些連接埠的流量，即可解決另外兩個效能瓶頸。擴大佇列大小 (Qsize) 可因應流量突然大量暴增，以免在突發性流量下丟棄封包。將專用 CPU 執行緒 (**ethernetX.ctxPerDev = 1**) 新增給連接埠層級封包處理，能夠以更高速率處理流量，從而提高流量吞吐量來達到線路速率。

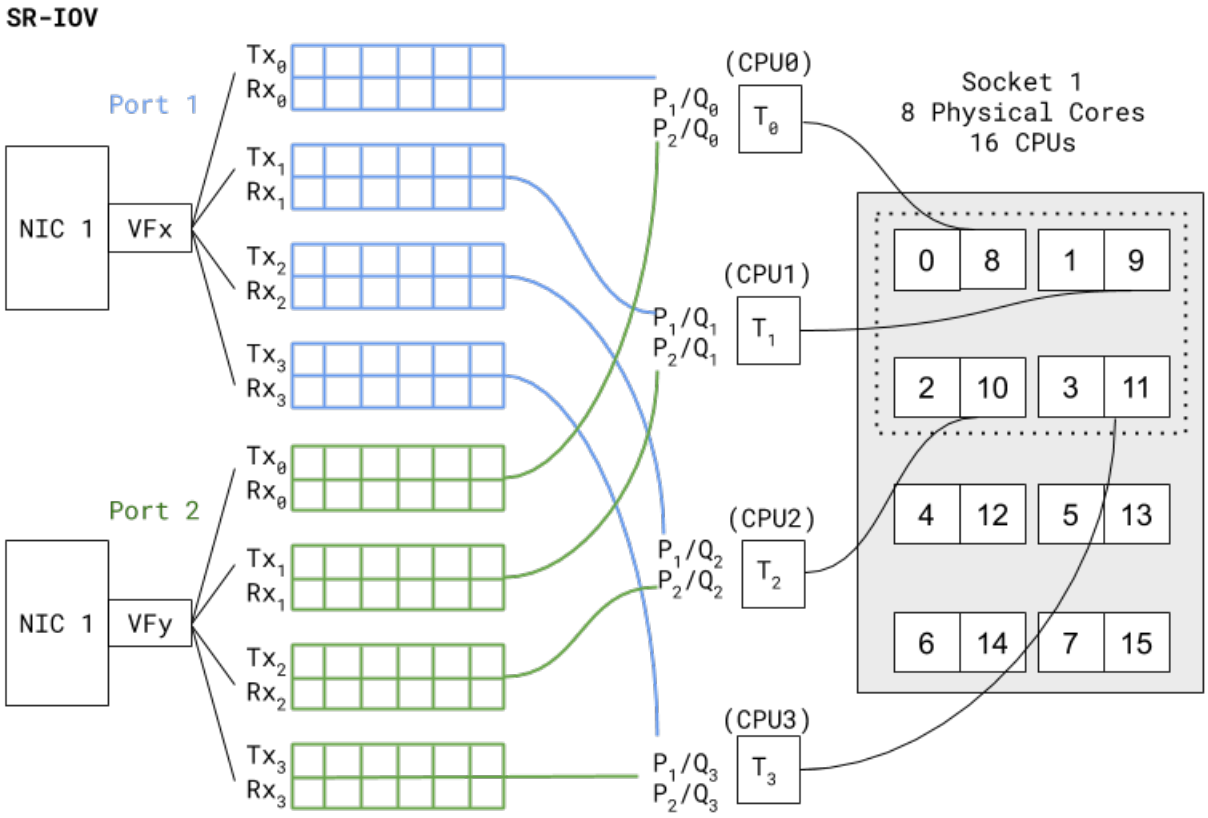
效能也取決於 PA-VM 封包處理技術。這可以設為 DPDK 或 PacketMMAP。DPDK 使用輪詢模式驅動程式（取決於驅動程式類型），以持續輪詢佇列中接收的封包。這帶來更高的吞吐量效能。封包發現的延遲取決於輪詢期間。如果是連續輪詢（亦即 PANOS cli 中的 busy-poll 設定），則資料平面工作的 vCPU 使用率會達到 100%，但可發揮最佳效能。在內部，軟體採用毫秒層級的輪詢時間，以防止濫用 CPU 資源。

反之，PacketMMAP 的效能低於 DPDK，但適用於網路層級的任何驅動程式。就 DPDK 而言，vSwitch 驅動程式必須支援 DPDK。PacketMMAP 可處理當連接埠收到封包並放入接收佇列時所引起的插斷。對於每個封包或一組封包，這表示會引起插斷，並從接收佇列取出封包來處理。這會縮短封包處理的延遲，但會降低吞吐量，因為每次都必須處理插斷，導致 CPU 負荷加重。一般而言，PacketMMAP 的封包處理延遲低於 DPDK（不修改忙碌輪詢）。

©2023 Palo Alto Networks, Inc.

使用案例 **2**：**SR-IOV** 部署

以下 SR-IOV 圖顯示的 PAVM 部署類似於 vSwitch 使用案例，但採用 SR-IOV 模式。



在 SR-IOV 中，相容的實體 NIC 連接埠（以實體功能呈現）實質上分割為多個介面（以虛擬功能呈現）。上圖顯示 NIC1 Port1 有一個名為 VFX 的 VF，與其中一個 PAVM 資料平面介面相關聯 — 例如 eth1。Port2 VF 至 PAVM eth2 也建立類似的關聯。封包處理鏈類似於 vSwitch 環境中的部署封包處理鏈。唯一的差別在於 SR-IOV VF 驅動程式應該相容於 PAN-OS 中使用的驅動程式。另外，因為沒有內部 vSwitch（在主機）來切換流量，所以不需要為連接埠排定的流量設定專用執行緒（亦即，此設定中不需要 **`ethernetX.ctxPerDev = 1`**）。銜接 SR-IOV 和 DPDK 的介面可發揮比 vSwitch 使用案例更高的封包處理效能。

參考

- 針對資料密集型工作負載來調整 VMware vCloud NFV
- 對 vSphere 中 Telco 和 NFV 工作負載進行效能調整的最佳做法
- CPU 相似性的潛在問題
- 判讀 esxtop 統計資料

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

在 vCloud Air 上設定 VM-Series 防火牆

您可以使用 vCloud Air 入口網站，透過 vCloud Director 入口網站或使用 vCloud Air API，在 vCloud Air 上的虛擬資料中心 (vDC) 部署 VM-Series 防火牆。

- 關於 vCloud Air 上的 VM-Series 防火牆
- vCloud Air 上支援的部署
- 在 vCloud Air 上部署 VM-Series 防火牆

關於 vCloud Air 上的 VM-Series 防火牆

您可以使用 vCloud Air 入口網站或透過 vCloud Director 入口網站，在 VMware vCloud Air 的虛擬資料中心 (vDC) 部署 VM-Series 防火牆。若要集中管理所有實體及 VM-Series 防火牆，您可使用現有 Panorama 或在內部或 vCloud Air 部署新 Panorama。

vCloud Air 上的 VM-Series 防火牆需要下列各項：

- 來自 Palo Alto Networks 客戶支援網站的 ESXi 版軟體映像，這是一個 Open Virtualization Alliance（開放式虛擬化聯盟 - OVA）檔案。目前，vCloud Air Marketplace 不託管軟體映像。

  為了有效部署 VM-Series 防火牆，需要在 vApp 中包含防火牆軟體映像。vApp 是預先設定的虛擬設備容器（虛擬電腦與作業系統映像），作為單一物件管理。例如，如果 vApp 包含一組多層應用程式及 VM-Series 防火牆，每次您部署 vApp 時，VM-Series 防火牆將自動保障使用 vApp 部署的 Web 伺服器與資料庫伺服器的安全。
- 在自帶授權 (BYOL) 機型中，從合作夥伴、經銷商或直接從 Palo Alto Networks 購買的授權與使用授權；vCloud Air 上 VM-Series 的依使用授權不可用。
- 由於 vCloud Air 上實施的安全性限制，vCloud Air 上的 VM-Series 防火牆最好部署第 3 層介面，且必須啟用介面才能使用 Hypervisor 指派的 MAC 位址。如果不啟用 Hypervisor 指派的 MAC 位址，由於 vCloud Air 上的 vSwitch 不支援混合式模式或 MAC 偽造的傳輸，VMware vSwitch 無法將流量轉送至 VM-Series 防火牆上的資料平面介面。使用旁接介面、Layer 2 介面或 Virtual Wire 介面無法部署 VM-Series 防火牆。

在主動/被動高可用性組態中，可以部署 vCloud Air 上的 VM-Series 防火牆。然而，vCloud Air 上的 VM-Series 防火牆不支援託管於 vCloud Air 的 virtual machine（虛擬機器 - VM）的 VM 監控功能。

如需關於 vCloud Air 的完整資訊，請參閱 VMware 的 vCloud Air 文件。

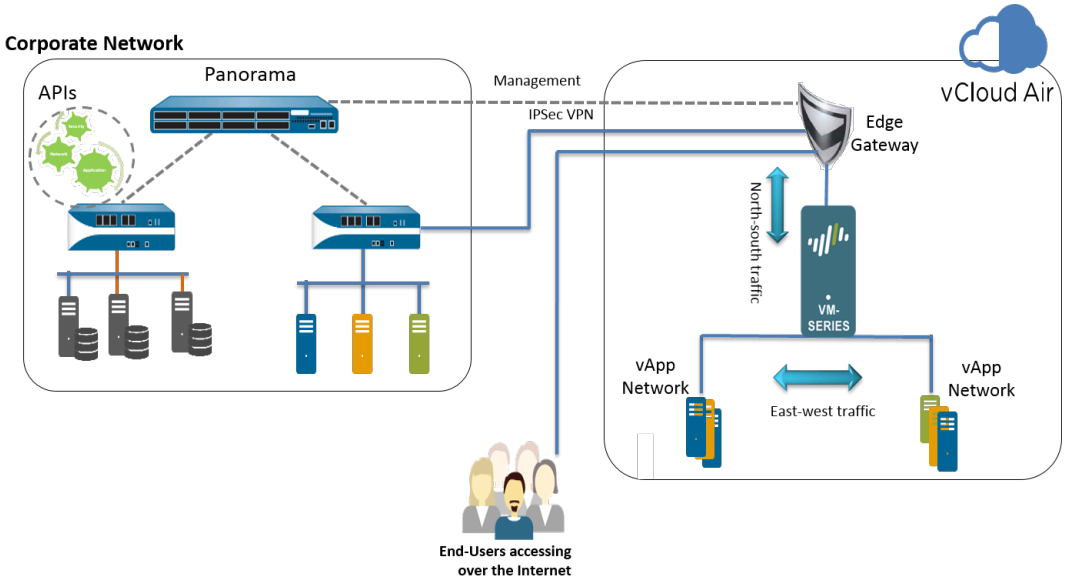
©2023 Palo Alto Networks, Inc.

vCloud Air 上支援的部署

若要安全啟用應用程式，封鎖未知威脅，以及與環境中的變更保持移至，您可以採用下列方式在擁有第 3 層介面的 vCloud Air 上部署 VM-Series 防火牆：

- 保障虛擬資料中心周邊—將 VM-Series 防火牆部署成為連接 vCloud Air 上的隔離與路由網路的虛擬機器。在此部署中，防火牆保障周遊 vCloud Air 基礎結構的所有南北向流量。
- 設定混合型雲端—將資料中心及私人雲端擴充為 vCloud Air 並使用 VPN 連接來啟用企業網路與資料中心之間的通訊。在此部署中，VM-Series 防火牆使用 IPSec 來加密流量及保障存取雲端的使用者。
- 保障 **vDC** 中應用程式子網路之間的流量—改善安全性，透過建立應用程式層對網路分段及隔離流量，然後部署 VM-Series 防火牆來防禦子網路與應用程式層之間的橫向威脅。

下圖結合了全部三種部署情境且包含 Panorama。Panorama 簡化原則更新，集中原則管理並提供集中的日誌記錄與報告。



©2023 Palo Alto Networks, Inc.

在 vCloud Air 上部署 VM-Series 防火牆

使用本節中的相關指示，在 vCloud Air 上的隨選或專用 vDC 中部署 VM-Series 防火牆。此步驟假設您已設定 vDC，包括允許流量出入 vDC 所需的閘道，以及將管理流量與資料流量路由至 vDC 所需的網路。

STEP 1 | 從 Palo Alto Networks 客戶支援網站取得 VM-Series OVA 映像；vCloud Air Marketplace 目前不託管軟體映像。

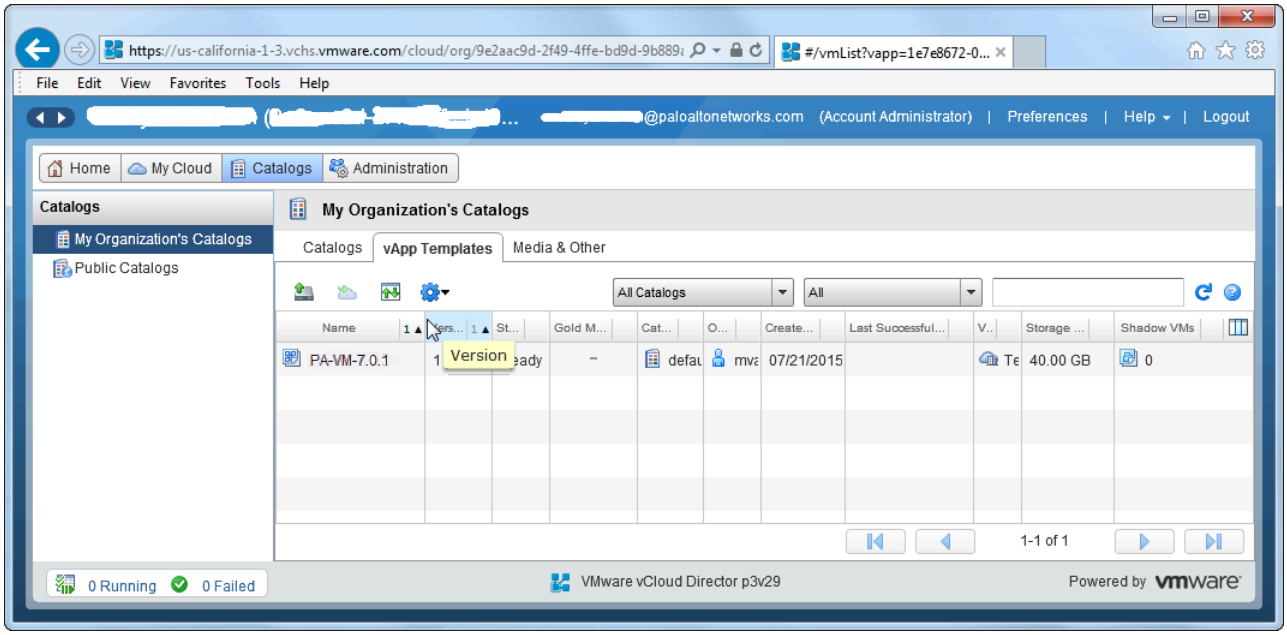
1. 移至：www.paloaltonetworks.com/services/support.html。
2. 依 **PAN-OS for VM-Series Base Images**（**VM-Series** 基礎映像的 **PAN-OS**） 篩選並下載 OVA 映像。例如，PA-VM-ESX-9.1.0.ova。

STEP 2 | 從 OVA 映像中擷取開放式虛擬化格式 (OVF)，並將 OVF 檔案匯入 vCloud Air 目錄。

從 OVA 映像中擷取檔案時，確定在相同的目錄內放置所有檔案—.mf、.ovf 及 .vmdk。

如需從 OVA 映像中擷取 OVF 檔案的相關指示，請參閱 VMware 文件：https://www.vmware.com/support/developer/ovf/#sthash.WUp55ZyE.dpuf

匯入 OVF 檔案後，VM-Series 防火牆的軟體映像會列在 **My Organization’s Catalogs**（我的組織目錄）中。



STEP 3 | 選取工作流程。

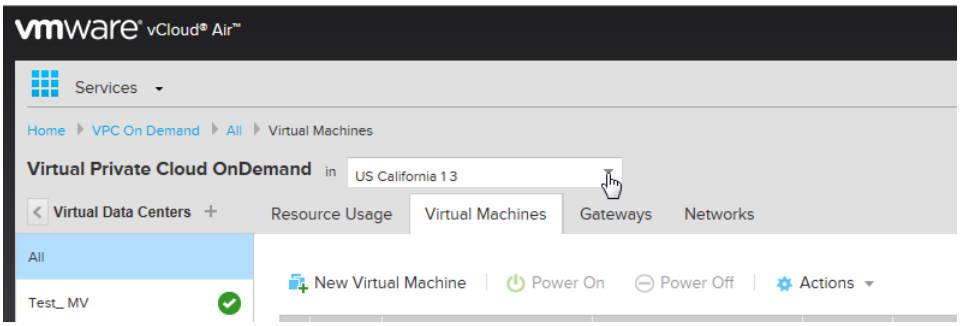
vApp 是一系列用於預先設定的虛擬設備的範本，包含虛擬電腦及作業系統映像。

- 如果您要建立新的 vDC 及新的 vApp 來包含 VM-Series 防火牆，請移至步驟 4。
- 如果您已部署 vDC 且擁有一個 vApp，現在想要將 VM-Series 防火牆新增至 vApp 來保護流量安全，則請移至步驟 5

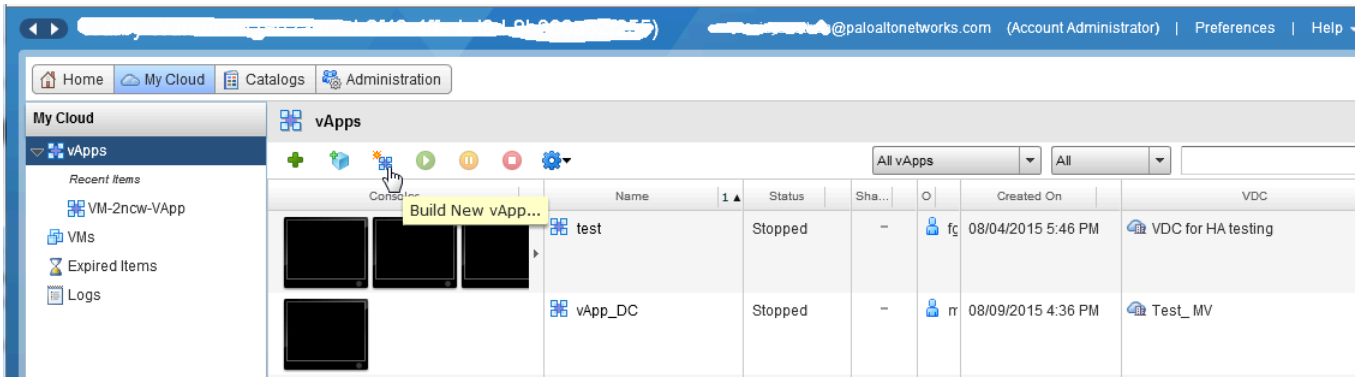
©2023 Palo Alto Networks, Inc.

STEP 4 | 建立包含 VM-Series 防火牆的 vDC 及 vApp。

1. 登入 vCloud Air。
2. 選取 **VPC OnDemand**（隨選 **VPC**）並選取您想要部署 VM-Series 防火牆的位置。



3. 選取 **Virtual Data Centers**（虛擬資料中心），然後按一下 **+** 以新增虛擬資料中心。
4. 選取 vDC，按一下滑鼠右鍵，然後選取 **Manage Catalogs in vCloud Director**（在 **vCloud Director** 中管理目錄）。將會重新導向至 vCloud Director web 介面。
5. 建立包含一個或多個虛擬電腦的新 vApp，包括 VM-Series 防火牆：
   1. 選取 **My Cloud**（我的雲端） > **vApps**，然後按一下 **Build New vApp**（建置新的 **vApp**）。



   2. 選取 **Name and Location**（名稱與位置），然後選取此 vApp 將在此執行的 **Virtual Datacenter**（虛擬資料中心）。依預設，執行階段及儲存區的 **Leases**（租用）從不會過期，且 vApp 不會自動停止。
   3. **Add Virtual Machines**（新增虛擬電腦）。若要從 **Look in:**（查詢：）下拉式清單中新增 VM-Series 防火牆映像，請依序選取 **My Organization's Catalog**（我的組織目錄）和映像，然後按一下 **Add**（新增）。按一下 **Next**（下一步）。
   4. 部署時，設定 **Resources**（資源）以指定虛擬電腦的儲存原則。VM-Series 防火牆使用 **Standard**（標準）選項。
   5. 設定 **Virtual Machines**（虛擬電腦）。對各虛擬電腦命名並選取您要連接的網路。您必須將 NIC 0（用於管理存取）連接至預設路由網路；NIC 1 用於資料流量。您可以稍後新增額外 NIC。
   6. 確認設定並按一下 **Finish**（完成）。
   7. 繼續步驟 6。

©2023 Palo Alto Networks, Inc.

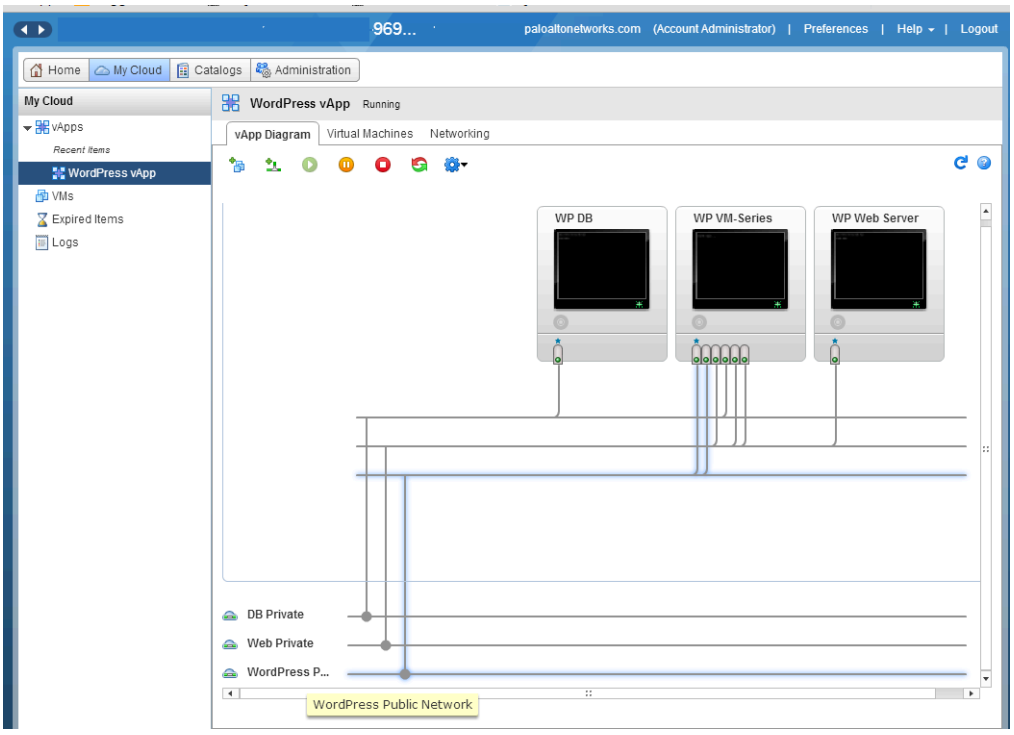
STEP 5 | 將 VM-Series 防火牆新增至 vApp。

1. 登入 vCloud Air。
2. 從左側面板選取現有 **Virtual Data Center**（虛擬資料中心），按一下滑鼠右鍵，然後選取 **Manage Catalogs in vCloud Director**（在 **vCloud Director** 管理目錄）。將會重新導向至 vCloud Director web 介面。
3. 選取 **My Cloud**（我的雲端） > **vApps**，然後按一下要包含 VM-Series 防火牆的 vApp 的 **Name**（名稱）。
4. 開啟 vApp（按兩下名稱），選取 **Virtual Machines**（虛擬電腦），然後按一下 ✚ 以新增虛擬電腦。
   1. 在 **Look in:**（查詢：）下拉式清單中，選取 **My Organization's Catalog**（我的組織目錄），選取 VM-Series 防火牆映像，然後按一下 **Add**（新增）。按一下 **Next**（下一步）。
   2. 按一下 **Next**（下一步）略過**Configure Resources**（設定資源）。VM-Series 防火牆使用 **Standard**（標準）選項，且不修改儲存原則。
   3. 輸入防火牆的 **Name**（名稱），針對管理存取 **(NIC 0)**，選取預設路由網路與 **IP Mode**（**IP** 模式）—Static（靜態）或 DHCP。您可以設定 NIC 1，並在步驟 6 中新增額外的 NIC。按一下 **Next**（下一步）。
   4. 確認此 vApp 如何連接至 vDC—此 vApp 中的虛擬電腦的閘道位址與網路遮罩。
   5. 確認您已新增 VM-Series 防火牆，然後按一下 **Finish**（完成）。
   6. 繼續步驟 6。

©2023 Palo Alto Networks, Inc.

STEP 6 | 根據部署所需，將 VM-Series 防火牆的資料介面連接至隔離或路由網路。

1. 在 vCloud Director 中，選取 **My Cloud**（我的雲端） > **vApps**，然後選取您剛才建立或編輯的 vApp。
2. 選取 **Virtual Machines**（虛擬電腦），然後選取 VM-Series 防火牆。然後按一下滑鼠右鍵，然後選取 **Properties**（屬性）。
3. 選取 **Hardware**（硬體），捲動至 NIC 區段，然後選取 **NIC 1**。
4. 根據 VM-Series 防火牆資料流量的連線需求，將資料平面網路介面連接至 vApp 網路或組織 VDC 網路。若要建立新網路：
   1. 在網路下拉式清單中，按一下 **Add Network**（新增網路）。
   2. 選取 **Network Type**（網路類型），輸入名稱，然後按一下 **OK**（確定）。
   3. 確認新網路已連接至介面。
5. 若要將額外 NIC 新增至防火牆，按一下 **Add**（新增）並重複上述步驟 4。您最多可以將七個資料背板介面連接至 VM-Series 防火牆。
6. 確認 VM-Series 防火牆的管理介面連接至 vDC 上的預設路由子網路，且至少一個資料背板介面連接至路由或隔離網路。
   1. 選取 **My Cloud**（我的雲端） > **vApps**，然後按兩下您剛才編輯的 vApp 的 **Name**（名稱）。
   2. 確認 **vApp Diagram**（**vApp** 圖）中的網路連接性。

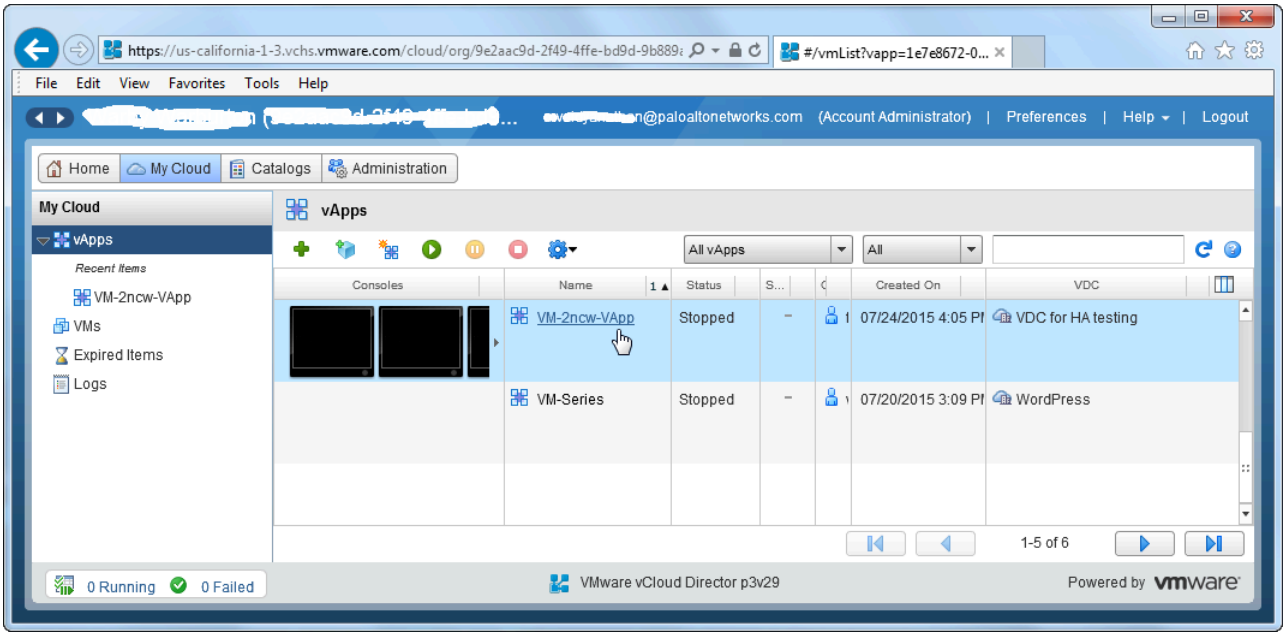


 ©2023 Palo Alto Networks, Inc.

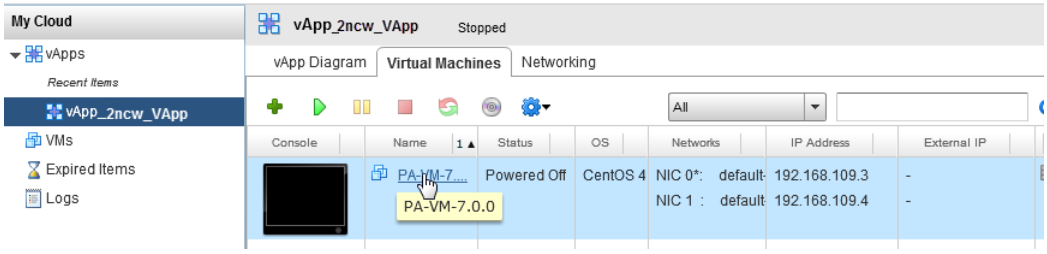
STEP 7 | （選用）編輯為 VM-Series 防火牆配置的硬體資源。

只有在您需要將額外 CPU、記憶體或硬碟配置到防火牆時才需要。

1. 選取 **My Cloud**（我的雲端） > **vApps**，然後按兩下您剛才部署的 vApp 的 **Name**（名稱）。



2. 選取 **Virtual Machine**（虛擬電腦），然後按一下 VM-Series 防火牆的 **Name**（名稱），即可存取虛擬電腦屬性。



3. 為 VM-Series 防火牆新增額外的 **Hardware**（硬體）資源：
   - 有關您的 VM-Series 型號的 vCPU、記憶體和磁碟最低需求，請參閱 VM-Series 系統需求。
   - NIC：一個管理介面及多達七個資料背板介面。

STEP 8 | 開啟 VM-Series 防火牆電源。

STEP 9 | 為 VM-Series 防火牆管理介面設定 IP 位址。

在 ESXi 的 VM-Series 上執行初始組態。

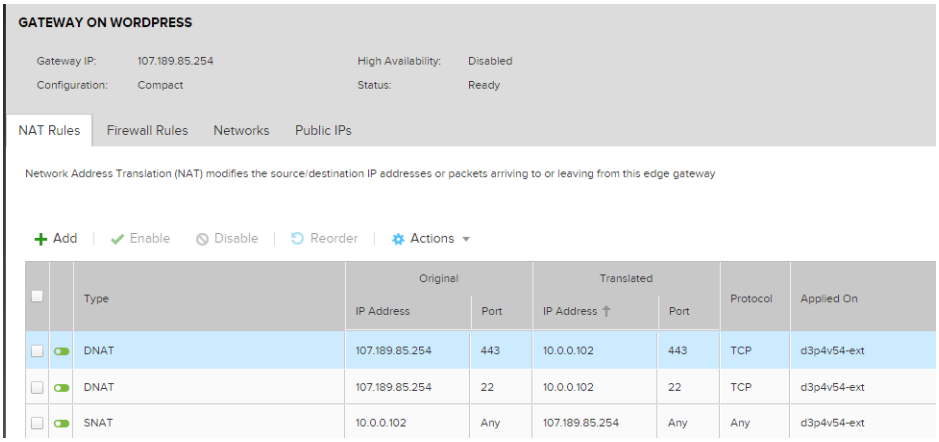
vCloud Air 上的 VM-Series 防火牆支援 VMware 工具，您可以在 ESXi 及 vCloud Air 上的 VM-Series 防火牆上使用 VMware 工具，以檢視 VM-Series 防火牆的管理 IP 位址。

©2023 Palo Alto Networks, Inc.

STEP 10 | 在 vCloud Air Edge Gateway 上定義 NAT 規則，為 VM-Series 防火牆啟用網際網路存取。

1. 選取 **Virtual Data Centers**（虛擬資料中心） > **Gateways**（閘道），然後選取閘道並按兩下以新增 **NAT Rules**（**NAT** 規則）。
2. 建立兩項 DNAT 規則。一個用於允許 SSH 存取，另一個用於允許 HTTPS 存取，目標是存取 VM-Series 防火牆上管理連接埠的 IP 位址。
3. 建立 SNAT 規則，以便針對從 VM-Series 防火牆上的管理連接埠到外部 IP 位址啟動的所有流量，轉譯內部來源 IP 位址。

若要傳送及接收防火牆資料背板介面的流量，您必須在 *vCloud Air Edge Gateway* 上建立額外 *DNAT* 及 *SNAT* 規則。



STEP 11 | 登入防火牆的網頁介面。

在本範例中，web 介面的 URL 為 https://107.189.85.254

使用 Edge Gateway 上的 NAT 規則，將外部 IP 位址及連接埠 107.189.85.254:443 轉譯為私人 IP 位址及連接埠 10.0.0.102:443。

STEP 12 | 新增驗證碼在防火牆上啟動授權。

啟動授權。

STEP 13 | 設定 VM-Series 防火牆以使用 Hypervisor 指派的 MAC 位址。

Hypervisor 指派的 MAC 位址

©2023 Palo Alto Networks, Inc.

STEP 14 | 將資料背板介面設為 Layer 3 介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）。
2. 按一下 **Ethernet 1/1** 的連結，然後依照以下所述設定：
   - 介面類型：**Layer3**
   - 選取 **Config**（設定）頁籤，然後將介面指派給預設路由器。
   - 在 **Config**（介面類型）頁籤上，從 **Security Zone**（安全性區域）下拉式清單中選取 **New Zone**（新區域）。定義新地區，例如 untrust，然後按一下 **OK**（確定）。
   - 選取 **IPv4**，指派靜態 IP 位址。
   - 在 **Advanced**（進階） > **Other Info**（其他資訊）上，展開 **Management Profile**（管理設定檔）下拉式清單，然後選取 **New Management Profile**（新增管理設定檔）。
   - 輸入設定檔的 **Name**（名稱），例如 allow_ping，然後選取 Permitted Services（許可的服務）清單中的 Ping，然後按一下 **OK**（確定）。
   - 若要儲存介面設定，請按一下 **OK**（確定）。
3. 對每個額外介面重複此程序。
4. 按一下 **Commit**（提交）來儲存變更。

©2023 Palo Alto Networks, Inc.

在 VMware NSX-T 上設定 VM-Series 防火牆

VM-Series 防火牆可部署在 VMware NSX-T 上，以保護南北向和東西流量的安全。

- 在 VMware NSX-T（南北向）上設定 VM-Series 防火牆
- 在 NSX-T（東西向）上設定 VM-Series 防火牆

在 VMware NSX-T（南北向）上設定 VM-Series 防火牆

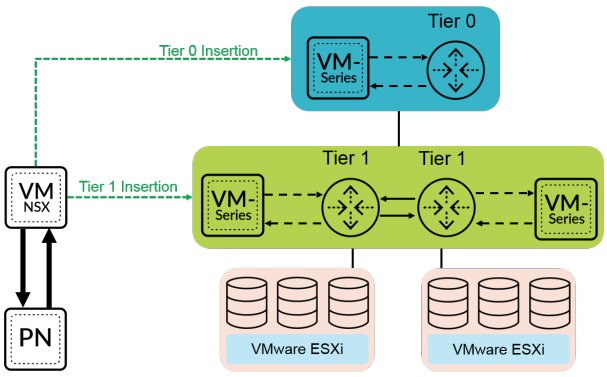
VMware NSX-T 上的 VM-Series 防火牆會整合 Palo Alto 新世代防火牆和 Panorama 與 ESXi 主機伺服器，為 NSX-T 軟體定義資料中心內的所有南北向流量提供廣泛的可見度和安全應用程式啟用。

下列各主題提供 VMware NSX-T 上 VM-Series 防火牆的相關資訊：

- VMware NSX-T（南北向）上支援的 VM-Series 防火牆部署
- NSX-T（南北向）上的 VM-Series 防火牆元件
- 在 NSX-T（南北向）上部署 VM-Series 防火牆
- 將安全性政策從 NSX-V 延伸至 NSX-T

VMware NSX-T（南北向）上支援的 VM-Series 防火牆部署

您可以將一個或多個 VM-Series 防火牆實例部署為 VMware NSX-T Data Center 中的合作夥伴服務。將 VM-Series 防火牆連接至任何層 0 或層 1 邏輯路由器，以保護南北向流量。您可以將 VM-Series 防火牆部署為獨立服務實例或是高可用性 (HA) 配對中的兩個防火牆。Panorama 會管理與 NSX-T 管理員的連線以及 NSX-T 軟體定義資料中心內部署的 VM-Series 防火牆。



- 層 0 插入—層 0 插入會將 VM-Series 防火牆部署至層 0 邏輯路由器，以處理邏輯與實體網路之間的流量。當您使用層 0 插入來部署 VM-Series 防火牆時，NSX-T 管理員會使用您在 Panorama 上設定的部署資訊，利用虛擬介接模式以將防火牆連接至層 0 邏輯路由器。
- 層 1 插入—層 1 插入會將 VM-Series 防火牆部署至層 1 邏輯路由器，以提供與區段的下行連線以及與層 0 邏輯路由器的上行連線。NSX-T 管理員會使用虛擬介接模式，以將已部署層 1 插入的 VM-Series 防火牆連接至層 1 邏輯路由器。

部署防火牆之後，您可以設定流量重新導向規則，以在跨層 0 或層 1 路由器時將流量傳送至 VM-Series 防火牆。您在 Panorama 上設定的安全性政策規則會推送至受管理的 VM-Series 防火牆，然後套用至通過防火牆的流量。

NSX-T（南北向）上的 VM-Series 防火牆元件

下列各表格顯示此 Palo Alto Networks 與 VMware NSX-T 整合解決方案的元件。

©2023 Palo Alto Networks, Inc.

VMware 元件	
vCenter/ESXi	vCenter 伺服器是 vSphere 套件的集中管理工具。ESXi 是一個可啟用計算虛擬化的 Hypervisor。 請參閱 VMware 的「相容性矩陣」，以瞭解您的 NSX-T 的版本與 vCenter 之間的相容性。
NSX-T 管理員	必須安裝 VMware NSX-T Data Center 2.4.0 和更新版本，並向 vCenter 伺服器進行註冊。需要有 NSX-T 管理員，才能在 ESXi 叢集的 ESXi 主機上部署 VM-Series 防火牆。

Palo Alto Networks 元件	
PAN-OS	需要有 VM-Series 基本映像 (PA-VM-NST-9.1.zip)，才能在 NSX-T 上部署 VM-Series 防火牆。 在 ESXi 伺服器上部署 NSX 專用 VM-Series 防火牆的最低系統需求取決於 VM-Series 型號。如需 VM-Series 型號的最低硬體需求，請參閱VM-Series 型號。
Panorama Panorama 必須執行與其將管理的防火牆相同或更新的版本。	NSX-T 上的 VM-Series 防火牆需要 Panorama 9.1 或更新版本。 Panorama 是 Palo Alto Networks 新世代防火牆的集中管理工具。在此解決方案中，Panorama 與 NSX-T 管理員搭配運作，以部署、授權和集中管理（設定和政策）NSX-T 專用 VM-Series 防火牆。 Panorama 必須能夠連線到 NSX-T 管理員、VM-Series 防火牆和 Palo Alto Networks 更新伺服器。 如需部署 Panorama 設備的相關資訊，請參閱 Panorama 管理員指南。
VMware NSX 專用 Panorama 外掛程式	3.0.0 或更新版本
VM-Series 外掛程式	1.0.6 或更新版本
VM-Series 防火牆型號	VM-100、VM-300、VM-500 和 VM-700 支援 NSX-T。

©2023 Palo Alto Networks, Inc.

在 NSX-T（南北向）上部署 VM-Series 防火牆

完成下列工作，以使用 VM-Series 防火牆保護 NSX-T 環境中的南北向流量。

下列程序涉及 ***NSX-T Manager 3.0***

。

- 安裝 VMware NSX 專用 Panorama 外掛程式
- 啟用 NSX-T 管理員與 Panorama 之間的通訊
- 在 Panorama 上建立範本堆疊和裝置群組
- 在 Panorama 上設定服務定義
- 部署 VM-Series 防火牆
- 將流量導向至 VM-Series 防火牆
- 在 NSX-T 上將安全性政策套用至 VM-Series 防火牆
- 使用 vMotion 在主機之間移動 VM-Series 防火牆

安裝 **VMware NSX** 專用 **Panorama** 外掛程式

下載並安裝 VMware NSX 專用 Panorama 外掛程式。在安裝或升級外掛程式之前，請先參閱相容性矩陣。

如果您有 Panorama HA 組態，請在每個 Panorama 端點上重複此安裝程序。在 Panorama HA 對等上安裝外掛程式時，請先將外掛程式安裝於被動對等，再安裝於主動對等。安裝外掛程式安裝於被動對等之後會轉換為非運作狀態。將外掛程式安裝於主動對等會將被動對等恢復為運作狀態。

如果您在安裝了多個外掛程式的 HA 配對中安裝了一個獨立的 Panorama 或兩個 Panorama 設備，則在未設定一或多個外掛程式的情況下，外掛程式可能不會收到更新的 IP-Tag 資訊。發生這種情況是因為 Panorama 不會將 IP-Tag 資訊轉送到未設定的外掛程式。此外，如果一或多個 Panorama 外掛程式未處於「已註冊」或「成功」狀態（每個外掛程式的正狀態不同），則可能會出現此問題。在繼續或執行下述命令之前，請確保您的外掛程式處於正狀態。

如果遇到此問題，有兩種權宜方案：

- 解除安裝未設定的外掛程式。建議您不要安裝未打算立即設定的外掛程式
- 您可以使用以下命令來變通處理此問題。對每個 Panorama 實例上的每個未設定外掛程式執行以下命令，以防止 Panorama 等待傳送更新。否則，防火牆可能會遺失一些 IP-Tag 資訊。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以透過執行以下命令來取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

上述的命令在重新啟動後不會持續存在，並且必須在任何後續重新啟動時再次使用。對於 HA 配對中的 Panorama，必須在每個 Panorama 上執行命令。

STEP 1 | 選取**Panorama** > 外掛程式 。在安裝或升級外掛程式之前，請先參閱相容性矩陣。

STEP 2 | 選取 **Check Now**（立即檢查） 以擷取可用更新清單。

©2023 Palo Alto Networks, Inc.

STEP 3 | 選取 Action（動作）欄中的 **Download**（下載）以下載外掛程式。

STEP 4 | 選取外掛程式版本，在 Action（動作）欄中按一下 **Install**（安裝）來安裝外掛程式。安裝完成時，Panorama 會通知您。

啟用 NSX-T 管理員與 Panorama 之間的通訊

完成下列程序，以啟用 Panorama 與 NSX-T 管理員之間的通訊。您最多可將 Panorama 連線至 16 個 NSX-T 管理員。如果您要將 Panorama 連線至多個 NSX-T 管理員，則必須謹慎規劃裝置群組階層和範本堆疊，並考量它們與部署所需的其他元件如何互動。服務定義會參照裝置群組和範本堆疊，並將該資訊推送至相關 ESXi 叢集中的防火牆。

STEP 1 | （選用）繞過用於 Panorama 與 NSX-T 管理員之間通訊的 Proxy 伺服器設定，在 Panorama 上設定於 **Panorama** > **Setup**（設定） > **Services**（服務） > **Proxy Server**（**Proxy** 伺服器）下方。此命令可讓 Panorama 直接與 NSX-T 管理員通訊，同時維護其他服務的 Proxy 通訊。

1. 登入 Panorama CLI。
2. 執行下列命令，以啟用或停用 Proxy 繞過。

   ```
   admin@Panorama> request plugins vmware_nsx proxy bypass {yes | no}
   ```

   選取 **yes**（是）以啟用 Proxy 繞過，而選取 **no**（否）以停用 Proxy 繞過。依預設會將其設定為 **no**（否）。

STEP 2 | 登入 Panorama 網頁介面。

使用 Web 瀏覽器中的安全連線 (https)，利用您在初始設定期間指派的 IP 位址和密碼登入 (https://<*IP address*>)。

STEP 3 | 設定 NSX-T 管理員存取權。對每個要與 Panorama 連線的 NSX-T 管理員重複此程序。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服務管理員），然後按一下 **Add**（新增）。
2. 輸入 NSX-T 管理員的描述性 **Name**（名稱）。
3. （選用）新增 NSX-T 管理員的 **Description**（說明）。
4. 輸入用來存取 NSX-T 管理員的 **NSX Manager URL**（**NSX** 管理員 **URL**）（NSX-T 管理員叢集虛擬 IP 位址或 FQDN）。
5. 輸入 **NSX Manager Login**（**NSX** 管理員登入）認證—使用者名稱和密碼，供 Panorama 驗證 NSX-T 管理員。
6. 按一下 **OK**（確定）。

如果您變更 *NSX-T* 管理員登入密碼，請確保立即在 *Panorama* 上更新密碼。不正確的密碼會使 *Panorama* 與 *NSX-T* 管理員之間的連線中斷。

STEP 4 | 將您的變更提交至 Panorama。

按一下 **Commit**（提交） 和 **Commit to Panorama**（提交至 **Panorama**）。

©2023 Palo Alto Networks, Inc.

STEP 5 | 在 Panorama 上驗證連線狀態。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服務管理員）。
2. 確認 **Status**（狀態）欄中的訊息。

   成功連線時，狀態會顯示成 **Registered**（已註冊）。這指出 Panorama 和 NSX-T 管理員同步。

   失敗的狀態訊息為：

   - **No connection**（無連線）：無法連線/建立與 NSX-T 管理員的網路連線。
   - **Invalid Credentials**（無效的認證）：存取認證（使用者名稱和/或密碼）不正確。
   - **Out of sync**（未同步）：在 Panorama 上定義的組態設定與 NSX-T 管理員上定義的組態設定不同。如需失敗原因的詳細資料，請按一下連結。例如，NSX-T 管理員的服務定義可能與 Panorama 上所定義的服務定義同名。若要修正錯誤，請使用錯誤訊息中所列的服務定義名稱來驗證 NSX-T 管理員上的服務定義。除非 Panorama 與 NSX-T 管理員上的設定同步，否則您無法在 Panorama 上新增新的服務定義。
   - **Connection Disabled**（連線已停用）：已手動停用 Panorama 與 NSX-T 管理員之間的連線。

在 Panorama 上建立範本堆疊和裝置群組

若要使用 Panorama 管理 NSX-T 上的 VM-Series 防火牆，防火牆必須屬於裝置群組及範本堆疊。設備群組可讓您將需要類似原則和物件的防火牆組合成邏輯單元；您可在 Panorama 上，使用 **Objects**（物件）和 **Policies**（原則）頁籤來定義組態。使用範本堆疊來設定 VM-Series 防火牆在網路上操作時所需要的設定；在 Panorama 上，請使用 **Device**（裝置） 和 **Network**（網路）頁籤來定義設定。NSX-T 設定中使用的每個範本堆疊都必須與一個服務定義相關聯。

在 NSX-T 中部署的防火牆有兩個預設區域，和兩個設定於虛擬介接模式的介面。Ethernet1/1 是 **south**（南向）區域的一部分，ethernet1/2 是 **north**（北向）區域的一部分。若要將原則規則從 Panorama 推送至受管理的防火牆，您必須設定與 Panorama 上的對應範本堆疊中的防火牆相符的區域和介面。

STEP 1 | 新增設備群組或設備群組階層。

1. 選取 **Panorama** > **Device Groups**（裝置群組），然後按一下 **Add**（新增）。您還可以建立裝置群組階層。
2. 輸入唯一的 **Name**（名稱）及 **Description**（描述）以識別裝置群組。
3. 按一下 **OK**（確定）。
4. 按一下 **Commit**（提交），並選取 **Panorama** 作為 **Commit Type**（提交類型），以將變更儲存到 Panorama 上正在執行的組態。

STEP 2 | 新增範本。

1. 選取 **Panorama** > **Templates**（範本），然後按一下 **Add**（新增）。
2. 輸入唯一的 **Name**（名稱）和 **Description**（描述）以識別範本。
3. 按一下 **OK**（確定）。
4. 按一下 **Commit**（提交），再選取 **Panorama** 做為 **Commit Type**（提交類型），以便將變更儲存到 Panorama 上正在執行的組態。

©2023 Palo Alto Networks, Inc.

STEP 3 | 建立範本堆疊。

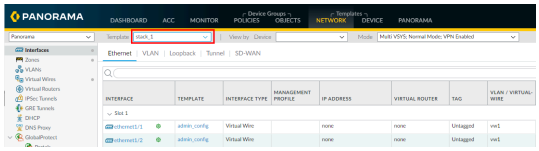
1. 選取 **Panorama** > **Templates**（範本），然後按一下 **Add Stack**（新增堆疊）。
2. 輸入唯一的 **Name**（名稱）和 **Description**（描述）以識別範本。
3. 按一下 **Add**（新增），以新增您先前建立的範本。
4. 按一下 **OK**（確定）。
5. 按一下 **Commit**（提交），然後選取 **Commit to Panorama**（提交至 **Panorama**），將變更儲存到 Panorama 上正在執行的設定。

STEP 4 | 設定虛擬介接、介面和區域。請確實從下拉式清單中選取正確的範本，如下所示。您建立的物件必須符合下列準則：

如果您變更預設的虛擬介接或區域名稱，*Panorama* 上的虛擬介接和區域必須與防火牆上使用的名稱相符。

- 使用 **ethernet1/1** 和 **ethernet1/2**。
- 名為 **vw1** 的虛擬介接物件。
- 第一個區域名為 **south**，請輸入 **virtual-wire**，並包含 **ethernet1/1**。
- 第二個區域名為 **north**，請輸入 **virtual-wire**，並包含 **ethernet1/2**。

對部署中的每個範本重複此程序。



STEP 5 | 按一下 **Commit**（提交），再選取 **Panorama** 做為 **Commit Type**（提交類型），以便將變更儲存到 Panorama 上正在執行的組態。

STEP 6 | 更新範本堆疊的 DNS 和 NTP 伺服器資訊。如果您在部署中使用裝置憑證，則必須完成此步驟。這是為了確保部署在 NSX-T 環境中的防火牆，具有到達裝置憑證伺服器所需的正確 DNS 資訊。

1. 確認您從 **Template**（範本）下拉式清單中指定正確的範本堆疊。
2. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務），然後按一下 **Edit**（編輯）圖示。
3. 在 [Services（服務）] 頁籤上，輸入 **Primary DNS Server**（主要 **DNS** 伺服器）和 **Secondary DNS Server**（次要 **DNS** 伺服器）的 IP 位址。
4. 在 NTP 頁籤上，輸入 **NTP Server**（**NTP** 伺服器）的 IP 位址。
5. 按一下 **OK**（確定）。
6. 將您的變更 **Commit**（提交）至 Panorama。

©2023 Palo Alto Networks, Inc.

在 Panorama 上設定服務定義

服務定義會指定安裝於 NSX-T 資料中心環境中的 VM-Series 防火牆的設定。服務定義必須包含裝置群組、範本堆疊和 OVF URL。

STEP 1 | 新增服務定義

您可以在 *Panorama* 上建立多達 *32* 個服務定義。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Service Definitions**（服務定義）。
2. 按一下 **Add**（新增）來建立新的服務定義。
3. 輸入服務定義的描述性 **Name**（名稱）。
4. （選用）新增 **Description**（說明）以識別將使用此服務定義部署的 VM-Series 防火牆的功能或用途。

STEP 2 | 指定設備群組及範本堆疊至服務定義。

務必在 Panorama 上建立範本堆疊和裝置群組。

由於將從 Panorama 集中管理此解決方案中部署的防火牆，因此必須指定防火牆所屬的 **Device Group**（裝置群組）及 **Template Stack**（範本堆疊）。所有使用此服務定義部署的防火牆均屬於該指定的範本堆疊及設備群組。

1. 在 **Device Group**（設備群組）下拉式清單中選取設備群組或設備群組階層。
2. 在 **Template**（範本）下拉式清單中選取範本堆疊。

   您無法將指派給一個服務定義的範本堆疊或設備群組重新用於另一個服務定義。

STEP 3 | 指定 OVF 檔案的位置。

下載 zip 檔案，解壓縮以擷取 .ovf、mf 和 .vmdk 檔案，並儲存至相同的目錄。ovf 和 vmdk 檔案會用來部署防火牆的每個實例。

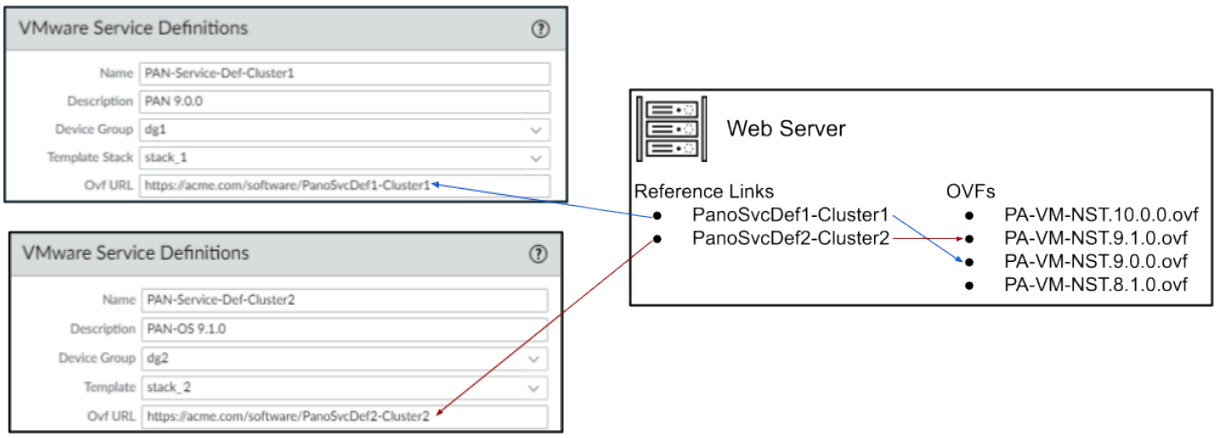
視需要修改伺服器上的安全性設定，讓您可以下載這類型的檔案。例如，在 IIS 伺服器上修改 MiME 類型組態；在 Apache 伺服器上編輯 .htaccess 檔案。

在 *VM-Series* 防火牆成功部署 *NSX* 服務之後，請勿變更 *Panorama* 服務定義 *OVF* 路徑。成功部署 *VM-Series* 防火牆之後，變更 *OVF* 路徑可能會導致 *NSX* 服務部署失敗狀態。您可以在 *NSX-T* 管理員中解決此失敗，但這可能會導致所有 *VM-Series* 防火牆重新部署。

建議使用可擴展的 OVF 路徑名稱，還可讓您變更基礎映像，而不影響已部署的防火牆。使用的路徑應該像 **https://acme.com/software/PanoSvcDef1-Cluster1.ovf** 這樣，而不是 **https://acme.com/software/PA-VM-NST.9.1.0.ovf**。使用靜態路徑參考，未來就不需要變更 OVF 路

©2023 Palo Alto Networks, Inc.

徑。建議您為部署中的每個 Panama 服務定義 (vSphere 叢集) 建立路徑，並視需要變更 Web 伺服器上的 PAN-OS 基礎映像參考。



在 **OVF URL** 中，新增託管 ovf 檔案的 Web 伺服器位置。http 和 https 都是支援的通訊協定。

Panorama 與 *Web* 伺服器之間必須有網路連線，才能擷取 *OVF* 檔案。

您可以在服務定義中使用相同的 OVF 版本或不同的版本。如果在服務定義中使用不同的 OVF 版本，則您可在不同 ESXi 彙集中的 VM-Series 防火牆上變更 PAN-OS 版本。

STEP 4 | 選取 **North South**（南北向）作為防火牆的 **Insertion Type**（插入類型）。

STEP 5 | 若要在 NSX Manager 部署 VM-Series 防火牆時自動擷取裝置憑證，請設定裝置憑證。

啟用此選項可將裝置憑證套用至新部署的 VM-Series 防火牆。只有在使用支援裝置憑證的基本映像 OVF 來部署防火牆時，才使用此選項。Panorama 會隨著服務定義，將裝置憑證資訊推送至 NSX Manager。在 NSX 中部署新的防火牆後，裝置憑證會在防火牆啟動時安裝於防火牆。

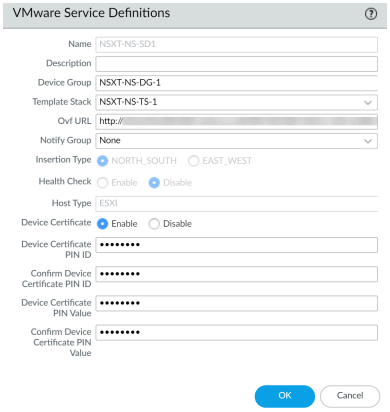
針對 VMware NSX 上的 VM-Series 防火牆，關於支援裝置憑證的 OVF 清單，請參閱 Palo Alto Networks 相容性矩陣。

如果您的 OVF 支援裝置憑證，則無論是否使用裝置憑證，您都必須啟用裝置憑證。如果 OVF 不支援裝置憑證，請停用此選項。

1. 如果尚未登入客戶支援入口網站並產生註冊 PIN 和 PIN ID，請這麼做。
2. 在 **Device Certificate**（裝置憑證）下方，按一下 **Enable**（啟用）。
3. 複製 PIN ID，輸入到 **Device Certificate PIN ID**（裝置憑證 **PIN ID**）欄位中。
4. 在 **Confirm Device Certificate PIN ID**（確認裝置憑證 **PIN ID**）欄位中，重新輸入 PIN ID。
5. 複製 PIN 值，輸入到 **Device Certificate PIN Value**（裝置憑證 **PIN** 值）欄位中。
6. 在 **Confirm Device Certificate PIN Value**（確認裝置憑證 **PIN** 值）欄位中，重新輸入 PIN 值。

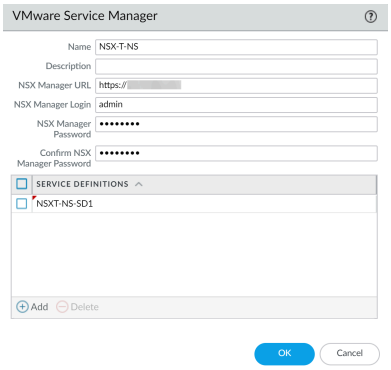
©2023 Palo Alto Networks, Inc.

STEP 6 | 按一下 **OK**（確定）以儲存服務定義。



STEP 7 | 將服務定義連接至服務管理員。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Service Manager**（服務管理員），然後按一下服務管理員名稱的連結。
2. 在 Service Definitions（服務定義）下，按一下 **Add**（新增），從下拉式清單中選取您的服務定義。
3. 按一下 **OK**（確定）。



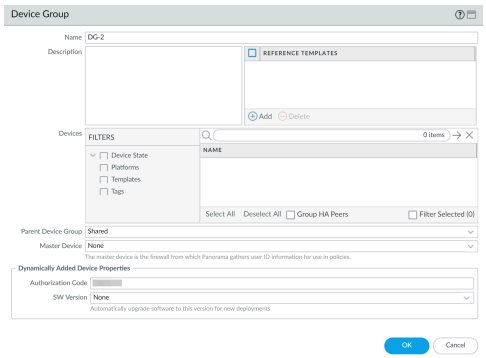
©2023 Palo Alto Networks, Inc.

STEP 8 | 新增驗證碼以授權防火牆。

1. 選取 **Panorama** > **Device Groups**（裝置群組），然後選擇與您剛才建立的服務定義相關聯的裝置群組。
2. 在 **Dynamically Added Device Properties**（動態新增的裝置屬性） 下方，新增您在訂購完成電子郵件中收到的授權碼，並選擇性地從 **SW Version**（SW 版本）下拉式清單中選取 [None（無）]。

   防火牆部署至 NSX-T 後，會自動新增至裝置群組、使用您提供的授權碼進行授權，並升級至您所指定的 PAN-OS 版本。

   在支援入口網站上，您可以檢視授權您部署的防火牆總數，以及已使用的授權數目與您授權碼所啟用的授權總目的比例。



STEP 9 | **Commit to Panorama**（提交至 **Panorama**）。

STEP 10 | 在 NSX-T 管理員上，確認服務定義是否可用。

選取 **System**（系統） > **Service Deployments**（服務部署） > **Catalog**（目錄）。服務定義會列為 NSX-T 管理員上的服務實例。

部署 VM-Series 防火牆

完成 Panorama 上的設定之後，請執行下列程序以在 NSX-T Data Center 中啟動 VM-Series 防火牆。

在 high availability（高可用性 - HA）之下於 NSX-T 上部署 VM-Series 防火牆時，兩個防火牆都部署至相同的裝置群組和範本堆疊。

STEP 1 | 登入 NSX-T 管理員。

STEP 2 | 選取 **System**（系統） > **Service Deployments**（服務部署） > **Deployment**（部署）。

STEP 3 | 從 **Partner Service**（合作夥伴服務）下拉式清單中，選取您的服務定義。

STEP 4 | 按一下 **Deploy Service**（部署服務）。

STEP 5 | 輸入 VM-Series 防火牆的描述性 **Service Deployment Name**（服務部署名稱）。

STEP 6 | 在 **Attachment Points**（連接點）下方，選取第 0 層或第 1 層路由器。NSX-T 管理員會將 VM-Series 防火牆連接至選取的路由器，並將通過該路由器的流量重新導向至 VM-Series 防火牆，以進行檢驗。您必須選取未連接服務插入的路由器。

©2023 Palo Alto Networks, Inc.

STEP 7 | 選取 **Compute Manager**（計算管理員）。計算管理員是管理您資料中心的 vCenter 伺服器。

STEP 8 | 選取 **Cluster**（叢集）。您可以任何不含 Edge 傳輸節點的叢集上部署 VM-Series 防火牆。

STEP 9 | 選取 **Datastore**（資料存放區）。

STEP 10 | 進行網路設定。

1. 按一下 **Networks**（網路）欄中的 **Edit Details**（編輯詳細資訊）。
2. 選取 **Primary Interface Network**（主要介面網路）。
3. 輸入 **Primary Interface IP**（主要介面 **IP**）。
4. 輸入 **Primary Gateway Address**（主要閘道位址）。
5. 輸入 **Primary Subnet Mask**（主要子網路遮罩）。
6. 按一下 **Save**（儲存）。

STEP 11 | NSX-T Manager 會根據您選取的合作夥伴服務，預先填入 **Deployment Specification**（部署規格）和 **Deployment Template**（部署範本）。

STEP 12 | 將 **Failure Policy**（失敗政策）設定為 [Allow（允許）] 或 [Block（封鎖）]。失敗政策定義在防火牆變成無法使用時，NSX-T 管理員如何處理導向至 VM-Series 防火牆的流量。

STEP 13 | 選取 VM-Series 防火牆的 **Deployment Mode**（部署模式）：[Standalone（獨立）] 或 [High Availability（高可用性）]。如果您有邊緣節點叢集，且選取高可用性，則除了部署在作用中邊緣節點的防火牆，NSX-T Manager 還會在待命邊緣節點部署額外的 VM-Series 防火牆。

STEP 14 | 按一下 **Save**（儲存）以部署 VM-Series 防火牆。

STEP 15 | 確認您的防火牆已連線至 Panorama。

1. 登入 Panorama。
2. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）。
3. 確認您的防火牆列在正確的裝置群組底下，且 **Device State**（裝置狀態）顯示為 **Connected**（已連線）。

   VM-Series 防火牆的裝置名稱在 Panorama 上對 NSX-T (NS) 部署顯示為 **PA-VM:<nsx.clusterid>**，對 NSX-T (EW) 部署顯示為 **PA-VM:<nsx.servicevmid>**。

將流量導向至 VM-Series 防火牆

完成下列程序，以將流量導向至 VM-Series 防火牆。對於南北向流量，重新導向規則預設為無狀態，且不可變更。此外，NSX-T 會自動為傳回流量建立對應的自反規則。

當您以 HA 模式部署 NSX-T 南北向的 VM-Series 防火牆時，您必須為 HA 對等雙方都建立流量重新導向規則。此外，您必須先為主動對等建立重新導向規則，其次再為被動對等建立。

自反規則不會出現在 *NSX-T Web* 介面中。

STEP 1 | 登入 NSX-T 管理員。

©2023 Palo Alto Networks, Inc.

STEP 2 | 確認您處於 **Policy**（政策）模式。

STEP 3 | 選取 **Security**（安全性） > **North South Security**（南北向安全性） > **Network Introspection (N-S)**（網路自我檢查 **(N-S)**）。

STEP 4 | 按一下 **Add Policy**（新增政策）。

STEP 5 | 輸入原則的描述性 **Name**（名稱）。

STEP 6 | 從 **Redirect To**（重新導向至）下拉式清單中，選取 VM-Series 防火牆服務實例。NSX-T Manager 會根據您選取的服務實例，自動填入 **Applied To**（套用至）欄位。

STEP 7 | 選取新建立的政策。

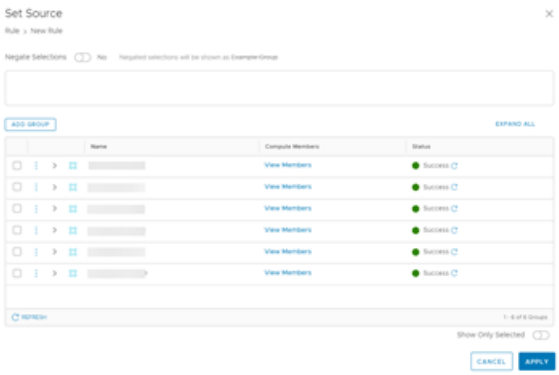
STEP 8 | 按一下 **Add Rule**（新增規則）。

如果您的 *NSX-T* 環境具有主動/待命 *HA* 中的 *Edge* 節點，您就必須為每個 *Edge* 節點建立一個重新導向規則。在進行容錯移轉時，*NSX-T* 並不會自動將重新導向規則套用至待命節點。

STEP 9 | 按一下 **Name**（名稱）欄位，然後輸入規則的描述性名稱。

STEP 10 | 依預設，來源設定為 [Any（任何）]。完成下列步驟，以指定不同的來源。

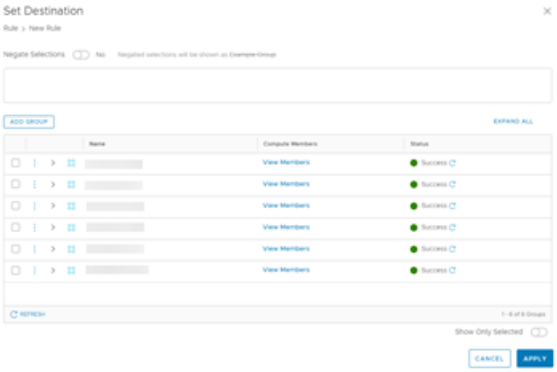
1. 按一下 **Source**（來源）欄中的編輯按鈕。
2. 選取一或多個群組以設為來源，或按一下 [Add Group（新增群組）] 建立新群組。
3. 按一下 **Apply**（套用）。



©2023 Palo Alto Networks, Inc.

STEP 11 | 依預設，目的地設定為 [Any（任何）]。完成下列步驟，以指定不同的目的地。

1. 按一下 **Destination**（目的地）欄中的編輯按鈕。
2. 選取一或多個群組以設為目的地，或按一下 [Add Group（新增群組）] 建立新群組。
3. 按一下 **Apply**（套用）。



STEP 12 | 依預設，[Any（任何）] 服務會重新導向至防火牆。完成下列步驟，以指定特定服務和通訊協定。

1. 按一下 **Services**（服務）欄中的編輯按鈕。
2. 選取一或多個群組以設為服務，或按一下 [Add Service（新增服務）] 建立新服務。
3. 按一下 **Apply**（套用）。

STEP 13 | 從 **Action**（動作）下拉式清單中，選取 **Redirect**（重新導向）以將流量傳送至 VM-Series 防火牆。

STEP 14 | **Enable**（啟用）規則NSX-T 管理員會發佈您剛建立的重新導向規則，並自動建立傳回流量的自反規則。自反規則不會出現在 NSX-T 管理員 Web 介面中。



STEP 15 | 如果在 HA 中部署 VM-Series 防火牆，請為被動 HA 對等建立另一個規則。

若傳回流量未導向至 *VM-Series* 防火牆，請手動設定傳回流量的流量重新導向規則。

在 NSX-T 上將安全性政策套用至 VM-Series 防火牆

既然，您已部署 VM-Series 防火牆，並建立流量重新導向規則以將流量傳送至防火牆，就可以使用 Panorama 集中管理 VM-Series 防火牆上的安全性政策規則。

STEP 1 | 登入 Panorama。

©2023 Palo Alto Networks, Inc.

STEP 2 | 建立安全性原則規則。

根據預設，防火牆會建立允許雙向轉送偵測 *(BFD)* 的規則。請不要建立封鎖 *BFD* 的規則。如果封鎖 *BFD*，則 *NSX-T* 會認為防火牆無法使用。

1. 選取 **Policies**（政策） > **Security**（安全性） > **Prerules**（預先規則）。
2. 選取在 Panorama 上建立範本堆疊和裝置群組中您為了管理 NSX-T 上的 VM-Series 防火牆而建立的 **Device Group**（裝置群組）。
3. 按一下 **Add**（新增），並輸入規則的 **Name**（名稱）和 **Description**（說明）。在此範例中，安全性規則允許 WebFrontEnd 伺服器與應用程式伺服器之間的所有流量。
4. 選取 **Source Zone**（來源區域）及 **Destination Zone**（目的地區域）。
5. 針對 **Source Address**（來源位址）和 **Destination Address**（目的地位址），選取或鍵入位址、靜態位址群組或區域。

   NSX-T 上的 *VM-Series* 防火牆不支援用於南北向流量的動態位址群組。

6. 選取要允許的 **Application**（應用程式）。在此範例中，我們會建立 **Application Group**（應用程式群組），包含群組在一起之特定應用程式的靜態群組。
   1. 按一下 **Add**（新增），選取 **New Application Group**（新應用程式群組）。
   2. 按一下 **Add**（新增），選取要在群組中包含的應用程式。
   3. 按一下 **OK**（確定）以建立應用程式群組。
7. 針對流量指定動作—**Allow**（允許）或 **Deny**（拒絕），選擇性地在 Profiles（設定檔）下為防毒、反間諜軟體和漏洞保護附加預設的安全性設定檔。
8. 按一下 **Commit**（認可），選取 **Commit to Panorama**（認可至 **Panorama**）。按一下 **OK**（確定）。

STEP 3 | 將政策套用至 NSX-T 上的 VM-Series 防火牆。

1. 按一下 **Commit**（認可） > **Push to Devices**（推送至裝置） > **Edit Selections**（編輯選取）。
2. 選取裝置群組，然後按一下 **OK**（確定）。
3. 選取 **Force Template Values**（強制範本值）。根據預設，Panorama 不會將防火牆上的物件取代為 Panorama 上共用名稱的物件。您必須選取 [Force Template Values（強制範本值）]，將原則推送至受管理的防火牆。
4. 按一下 **Yes**（是）以確認強制範本值。
5. 按一下 **OK**（確定）。
6. 驗證提交成功。

STEP 4 | （選用）使用範本來推送網路和裝置組態的基本組態，例如 DNS 伺服器、NTP 伺服器、syslog 伺服器和登入橫幅。

如需使用範本的詳細資訊，請參閱《Panorama 管理員指南》。

©2023 Palo Alto Networks, Inc.

使用 vMotion 在主機之間移動 VM-Series 防火牆

在 VMware NSX-T 中具有同質 CPU 設定的 ESXi 主機之間，使用 vMotion 移動 VM-Series 防火牆時，為了維護流量，您必須使用 PAN-OS CLI，在 vMotion 期間暫停 VM-Series 防火牆的內部活動訊號監控。您可以指定活動訊號監控暫停的時間量（以分鐘為單位）。活動訊號監控最多可以暫停 60 分鐘。當暫停間隔到期或您刻意結束暫停間隔時，活動訊號監控就會繼續。

如果 ESXi 主機有同質 CPU 設定，則 vSphere 6.5、6.7 和 7.0 支援 VM-Series 防火牆的 vMotion。

如果您執行 *vSphere 7.0* 或更新版本，則使用 *vMotion* 移動 *VM-Series* 防火牆時不需要此程序。

STEP 1 | 登入 VM-Series 防火牆 CLI。

STEP 2 | 使用下列命令設定活動訊號監控暫停間隔。一執行命令就會開始暫停。如果 vMotion 所花時間比預期更長，您可以重新執行此命令來設定更長的新間隔，於命令再次執行時開始計時。

```
request system heartbeat-pause set interval <pause-time-in-minutes>
```

您可以使用下列命令檢視暫停間隔的剩餘時間。

```
request system heartbeat-pause show interval
```

STEP 3 | （選用）如果您在暫停間隔經過之前完成 vMotion，則可以將間隔設為零 (0) 來結束暫停。

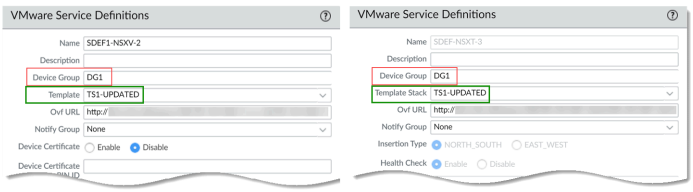
```
request system heartbeat-pause set interval 0
```

將安全性政策從 NSX-V 延伸至 NSX-T

如果您從 NSX-V 部署轉向 NSX-T 部署，或合併 NSX-T 部署與 NSX-V 部署，則不必重新建立政策規則，就能將現有安全性政策從 NSX-V 延伸至 NSX-T。作法是利用現有的裝置群組，並在 NSX-V 與 NSX-T 服務定義之間共用裝置群組。將政策移轉至 NSX-T 之後，您可以繼續使用 NSX-V 專用 VM-Series，或移除您的 NSX-V 部署。

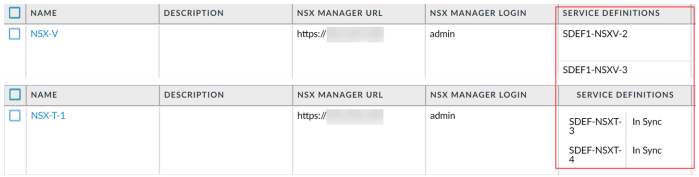
STEP 1 | 安裝 VMware NSX 專用 Panorama 外掛程式 3.2.0 或更新版本。升級之前，請參閱 VMware NSX 專用 Panorama 外掛程式 3.2.0 版本資訊。

STEP 2 | 針對部署中的每個 NSX-V 服務定義，設定 NSX-T 服務定義。請勿建立新的裝置群組，改為使用現有的 NSX-V 裝置群組。使用現有裝置群組可讓您將 NSX-V 上使用的相同安全性政策規則，套用至 NSX-T 上部署的 VM-Series 防火牆。如果您的政策參考特定區域，請將 NSX-V 服務定義中相同的範本堆疊，新增至 NSX-T 服務定義。此外，如果裝置群組參考特定範本，請確定您選取的範本堆疊包含裝置群組中參考的範本。



©2023 Palo Alto Networks, Inc.

STEP 3 | 設定 NSX-T 服務管理員，並將 NSX-T 服務定義與服務管理員建立關聯。

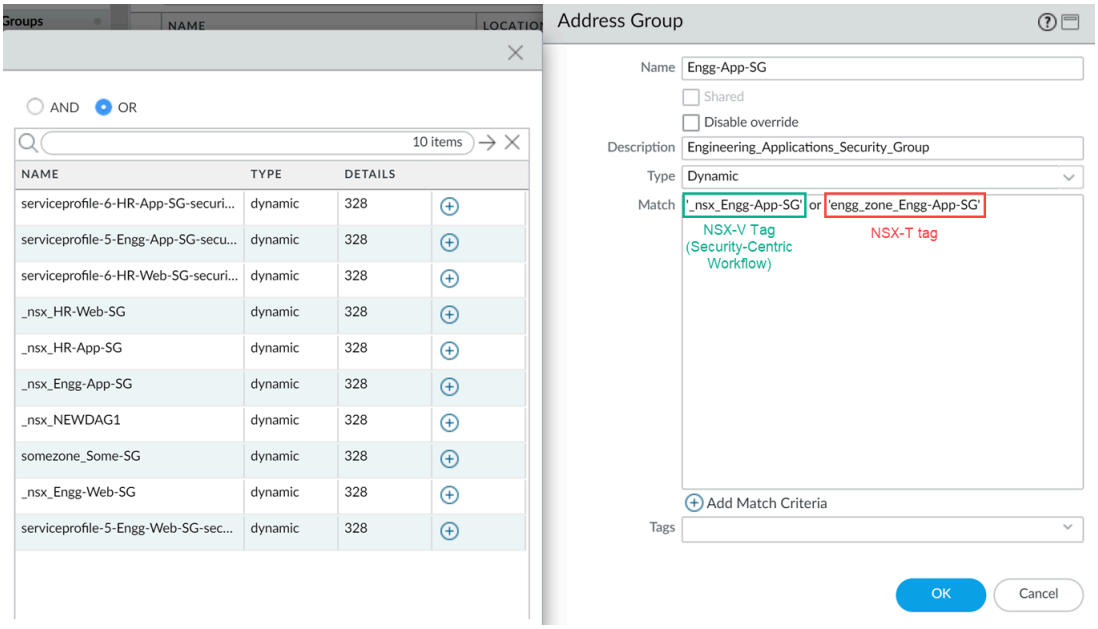


STEP 4 | 準備 NSX-T 環境和部署 VM-Series 防火牆。在啟動 VM-Series 防火牆之前，您必須先建立安全性群組、服務鏈和流量重新導向政策。

- 在 NSX-T（南北向）上部署 VM-Series 防火牆
- 使用以操作為中心的工作流程部署 VM-Series

STEP 5 | 將 NSX-T 標籤新增至現有的動態位址群組。

1. 選取 **Panorama** > **Objects**（物件） > **Address Groups**（位址群組）。
2. 按一下現有 NSX-V 動態位址群組的名稱。
3. 按一下 **Add Match Criteria**（新增比對規則），以顯示來自 NSX-V 和 NSX-T 的標籤。
4. 將 NSX-T 標籤新增至動態位址群組。標籤之間務必使用 **OR** 運算子。
5. 新增所有必要的標籤之後，按一下 **OK**（確定）。
6. **Commit**（提交）您的變更。



STEP 6 | 當您的 VM 工作負載成功從 NSX-V 移轉至 NSX-T 之後，如果您打算中止使用 NSX-V，請從動態位址群組中移除 NSX-V 標籤。當所有 NSX-V 相關設定從 NSX 專用 Panorama 外掛程式移除，且 VM-Series 防火牆設定也從 NSX-V 管理員移除之後，所有 NSX-V 標籤及對應的 IP 位址就會取消註冊。

©2023 Palo Alto Networks, Inc.

在 NSX-T（東西向）上設定 VM-Series 防火牆

VMware NSX-T 上的 VM-Series 防火牆會整合 Palo Alto 新世代防火牆和 Panorama 與 ESXi 主機伺服器，為 NSX-T 軟體定義資料中心內的所有東西向流量提供廣泛的可見度和安全應用程式啟用。

- NSX-T（東西向）上的 VM-Series 防火牆元件
- NSX-T（東西向）整合的 VM-Series 防火牆
- VMware NSX-T（東西向）上支援的 VM-Series 防火牆部署
- 使用以操作為中心的工作流程部署 VM-Series
- 使用以安全性為中心的工作流程部署 VM-Series
- 從 Panorama 刪除服務定義
- 從 NSX-T 上的 VM-Series 操作移轉至安全性中心部署
- 將安全性政策從 NSX-V 延伸至 NSX-T
- 使用就地移轉將 VM-Series 從 NSX-V 移至 NSX-T

NSX-T（東西向）上的 VM-Series 防火牆元件

下列表格顯示此 Palo Alto Networks 與 VMware NSX-T（東西向）整合解決方案的元件。

VMware 元件	
vCenter/ESXi	vCenter 伺服器是 vSphere 套件的集中管理工具。ESXi 是一個可啟用計算虛擬化的 Hypervisor。 請參閱 VMware 的「相容性矩陣」，以瞭解您的 NSX-T 的版本與 vCenter 之間的相容性。
NSX-T 管理員	必須安裝 VMware NSX-T Data Center 2.5.0，並向 vCenter 伺服器進行註冊。需要有 NSX-T 管理員，才能在 ESXi 叢集的 ESXi 主機上部署 VM-Series 防火牆。

Palo Alto Networks 元件	
PAN-OS	PAN-OS 10.1.x 和更新版本。 需要有 VM-Series 基本映像（例如 PA-VM-NST-10.1.0zip），才能在 NSX-T 上部署 VM-Series 防火牆。 在 ESXi 伺服器上部署 NSX 專用 VM-Series 防火牆的最低系統需求取決於 VM-Series 型號。如

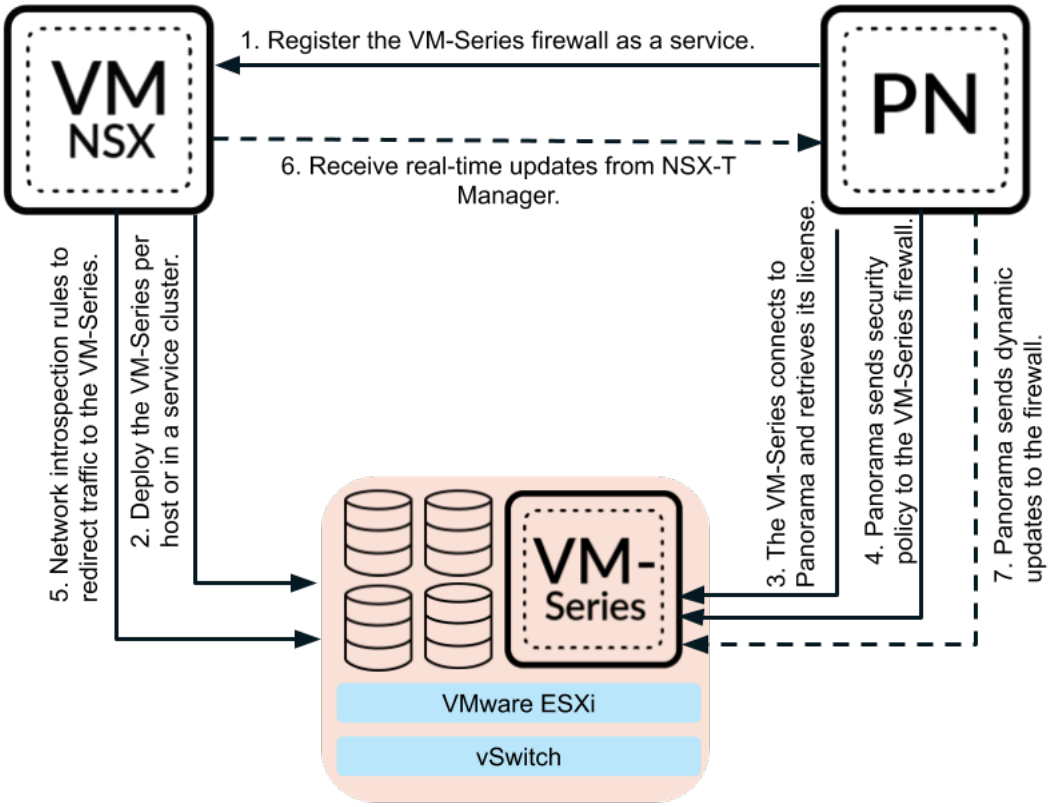
©2023 Palo Alto Networks, Inc.

Palo Alto Networks 元件	
	需 VM-Series 型號的最低硬體需求，請參閱VM-Series 型號。
Panorama Panorama 必須執行與其將管理的防火牆相同或更新的版本。	對於執行 10.1.0 的防火牆，NSX-T 上的 VM-Series 防火牆需要 Panorama 10.1.0 和更新版本 Panorama 是 Palo Alto Networks 新世代防火牆的集中管理工具。在此解決方案中，Panorama 與 NSX-T 管理員搭配運作，以部署、授權和集中管理（設定和政策）NSX-T 專用 VM-Series 防火牆。 Panorama 必須能夠連線到 NSX-T 管理員、VM-Series 防火牆和 Palo Alto Networks 更新伺服器。 如需部署 Panorama 設備的相關資訊，請參閱 10.2 Panorama 管理員指南。
VMware NSX 專用 Panorama 外掛程式	3.1.0 或更新版本 4.0.0 或更新版本，適用於以安全性為中心的工作流程
VM-Series 外掛程式	1.0.8 或更新版本
VM-Series 防火牆型號	VM-100、VM-300、VM-500 和 VM-700 支援 NSX-T。 在 ***NSX-T*** 上部署 ***VM-Series*** 防火牆之前，請確定您有足夠的硬體資源可支援您所選擇的部署模型（服務叢集或個別主機）中的 ***VM-Series*** 防火牆數目。這在部署大型防火牆（例如 ***VM-700***）時十分重要。

NSX-T（東西向）整合的 VM-Series 防火牆

NSX-T 管理員、vCenter、Panorama 和 VM-Series 防火牆可搭配運作，克服您的 NSX-T Data Center 在資訊安全方面遭遇到的挑戰。

©2023 Palo Alto Networks, Inc.



1. 將 **VM-Series** 防火牆註冊為服務 — 使用 Panorama 連線至您的 VMware NSX-T 管理員。Panorama 可使用 NSX-T API 與 NSX-T 管理員通訊，並可建立雙向通訊。在 Panorama 上，您可以藉由輸入 NSX-T 管理員的 IP 位址、使用者名稱和密碼來設定服務管理員，進而起始通訊。

   建立與 NSX-T 管理員的通訊之後，請設定服務定義。服務定義包括 VM-Series 防火牆基礎映像的位置、為 VM-Series 防火牆授權所需的授權碼，以及防火牆即將屬於的裝置群組和範本堆疊。

   此外，NSX-T 管理員可使用此連線，將 NSX-T 環境中的最新變更傳送至 Panorama。
2. 在個別主機或服務叢集中部署 **VM-Series** 防火牆 — NSX-T 管理員可使用 Panorama 在服務定義中推送的資訊，來部署 VM-Series 防火牆。您可以選擇要部署 VM-Series 防火牆的位置（服務叢集或個別 ESXi 主機），以及 NSX-T 將管理 IP 位址提供給 VM-Series 防火牆的方式（DHCP 或靜態 IP）。當防火牆啟動時，NSX-T 管理員的 API 會將 VM-Series 防火牆連線至 Hypervisor，使其能夠從 vSwitch 接收流量。

©2023 Palo Alto Networks, Inc.

3. **VM-Series** 連線至 **Panorama** — 然後，VM-Series 防火牆會連線至 Panorama 以取得其授權。Panorama 會從 Palo Alto Networks 更新伺服器取得授權，並將其傳送至防火牆。防火牆取得其授權後，就會重新啟動並使用序號再次開始運作。

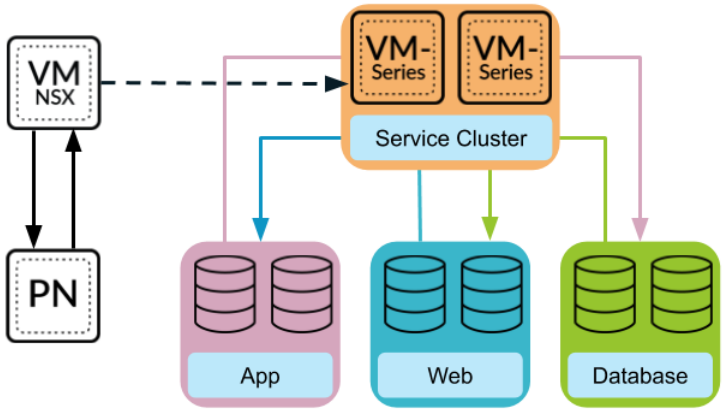
   如果 *Panorama* 無法存取網際網路，即無法擷取授權並將其推送至防火牆，這時您就必須手動為個別防火牆授權。如果 *VM-Series* 防火牆無法存取網際網路，您就必須將序號新增至 *Panorama* 以註冊為受管理的裝置，讓 *Panorama* 能夠推送範本堆疊、裝置群組，以及其他設定資訊。如需詳細資訊，請參閱 啟動 VMware NSX 專用 VM-Series 防火牆的授權。

4. **Panorama** 將安全性原則傳送至 **VM-Series** 防火牆 — 防火牆在重新連線至 Panorama 時，將會新增至服務定義所定義的裝置群組和範本堆疊，且 Panorama 會將適當的安全性原則推送至該防火牆。防火牆此時已準備就緒，可為您保護 NSX-T Data Center 中的流量。
5. 建立網路自我檢查規則，將流量重新導向至 **VM-Series** 防火牆 — 在 NSX-T 管理員上建立服務鏈結和網路自我檢查規則，以重新導向您 NSX-T Data Center 中的流量。
6. 從 **NSX-T** 管理員傳送即時更新 — NSX-T 管理員會將與虛擬環境中的變更有關的即時更新傳送至 Panorama。這些更新包括將流量傳送至 VM-Series 防火牆的群組在群組成員資格和虛擬機器 IP 位址方面的變更。
7. **Panorama** 傳送動態更新 — Panorama 在接收到來自 NSX-T 管理員的更新時，將會從其受管理的 VM-Series 防火牆傳送這些更新。Panorama 會根據您所決定的準則將虛擬機器放入動態位址群組，並將這些動態位址群組成員資格資訊推送至防火牆。如此，防火牆即可將正確的安全性原則套用至 NSX-T Data Center 中的虛擬機器輸入和輸出的流量。

VMware NSX-T（東西向）上支援的 VM-Series 防火牆部署

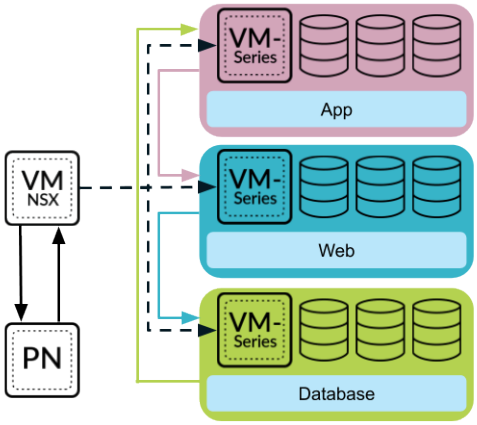
您可以將一或多個 VM-Series 防火牆實例部署為 VMware NSX-T Data Center 中的合作夥伴服務，以保護東西向流量並執行微分割。若要設定 VM-Series 防火牆以執行微分割，您可以在服務叢集中或個別主機上部署防火牆。

- 服務叢集 — 在叢集化部署中，所有 VM-Series 防火牆都會安裝在單一叢集上。VM 與群組之間的流量會先重新導向至 VM-Series 叢集以進行原則檢查和強制執行，然後再送往目的地。在設定叢集化部署時，您可以指定叢集內的特定主機，或選取 **Any**（任何）讓 NSX-T 選擇主機。



©2023 Palo Alto Networks, Inc.

- 主機型 — 在個別主機部署中，VM-Series 防火牆的實例會部署在 ESXi 叢集中的各主機上。相同主機上，來賓之間的流量會受到本機防火牆的檢查，因此無須離開主機進行檢查。離開主機的流量會先受到防火牆的檢查，才會到達 vSwitch。



部署防火牆之後，您可以設定流量重新導向規則，以將流量傳送至 VM-Series 防火牆。您在 Panorama 上設定的安全性政策規則會推送至受管理的 VM-Series 防火牆，然後套用至通過防火牆的流量。

若要在 VMware NSX-T 上部署 VM-Series 防火牆，您有兩個工作流程選項：以操作為中心和以安全性為中心的部署。

- 以操作為中心 — 在以操作為中心的工作流程中，部署程序的某些部分是在 Panorama 上執行，而其餘部分是在 NSX-T 管理員上執行。在 Panorama 上，您必須先啟用 Panorama 與 NSX-T 管理員之間的通訊，設定服務定義，然後啟動 VM-Series 防火牆。然後，您必須登入 NSX-T 管理員，並繼續設定來建立服務鏈和導向規則。若要完成 VM-Series 部署，您必須返回 Panorama 建立安全性政策。
- 以安全性為中心 — 在以安全性為中心的工作流程中，您可以將 Panorama 當作單一窗口來控制和管理安全性操作。您可以從 Panorama 完成整個部署工作流程。VMware NSX 專用 Panorama 外掛程式會將設定推送至 NSX-T 管理員，以建立服務鏈和導向規則。

建議您在 NSX-T 上為 VM-Series 部署選取一個部署工作流程，以方便使用。不過，VMware NSX-T 專用 VM-Series 防火牆支援在同一個外掛程式上同時使用這兩個工作流程。

使用以操作為中心的工作流程部署 VM-Series

完成下列工作以部署 VM-Series 防火牆，為您 NSX-T 資料中心內的東西向流量提供保護。

- 安裝 VMware NSX 專用 Panorama 外掛程式
- 啟用 NSX-T 管理員與 Panorama 之間的通訊
- 在 Panorama 上建立範本堆疊和裝置群組
- 在 Panorama 上設定服務定義
- 在 NSX-T（東西向）上啟動 VM-Series 防火牆
- 新增服務鏈結
- 將流量導向至 VM-Series 防火牆

©2023 Palo Alto Networks, Inc.

- 將安全性原則套用至 NSX-T（東西向）上的 VM-Series 防火牆
- 使用 vMotion 在主機之間移動 VM-Series 防火牆

安裝 VMware NSX 專用 Panorama 外掛程式

下載並安裝 VMware NSX 專用 Panorama 外掛程式。在安裝或升級外掛程式之前，請先參閱相容性矩陣。

如果您有 Panorama HA 組態，請在每個 Panorama 端點上重複此安裝程序。在 Panorama HA 對等上安裝外掛程式時，請先將外掛程式安裝於被動對等，再安裝於主動對等。安裝外掛程式安裝於被動對等之後會轉換為非運作狀態。將外掛程式安裝於主動對等會將被動對等恢復為運作狀態。

如果您在安裝了多個外掛程式的 HA 配對中安裝了一個獨立的 Panorama 或兩個 Panorama 設備，則在未設定一或多個外掛程式的情況下，外掛程式可能不會收到更新的 IP-Tag 資訊。發生這種情況是因為 Panorama 不會將 IP-Tag 資訊轉送到未設定的外掛程式。此外，如果一或多個 Panorama 外掛程式未處於「已註冊」或「成功」狀態（每個外掛程式的正狀態不同），則可能會出現此問題。在繼續或執行下述命令之前，請確保您的外掛程式處於正狀態。

如果遇到此問題，有兩種權宜方案：

- 解除安裝未設定的外掛程式。建議您不要安裝未打算立即設定的外掛程式
- 您可以使用以下命令來變通處理此問題。對每個 Panorama 實例上的每個未設定外掛程式執行以下命令，以防止 Panorama 等待傳送更新。否則，防火牆可能會遺失一些 IP-Tag 資訊。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以透過執行以下命令來取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

上述的命令在重新啟動後不會持續存在，並且必須在任何後續重新啟動時再次使用。對於 HA 配對中的 Panorama，必須在每個 Panorama 上執行命令。

STEP 1 | 選取 **Panorama** > **Plugins**（外掛程式）。

STEP 2 | 選取 **Check Now**（立即檢查） 以擷取可用更新清單。

STEP 3 | 選取 Action（動作）欄中的 **Download**（下載）以下載外掛程式。

STEP 4 | 選取外掛程式版本，在 Action（動作）欄中按一下 **Install**（安裝）來安裝外掛程式。安裝完成時，Panorama 會通知您。

啟用 NSX-T 管理員與 Panorama 之間的通訊

完成下列程序，以啟用 Panorama 與 NSX-T 管理員之間的通訊。您最多可將 Panorama 連線至 16 個 NSX-T 管理員。如果您要將 Panorama 連線至多個 NSX-T 管理員，則必須謹慎規劃裝置群組階層和範本堆疊，並考量它們與部署所需的其他元件如何互動。服務定義會參照裝置群組和範本堆疊，並將該資訊推送至相關 ESXi 叢集中的防火牆。

©2023 Palo Alto Networks, Inc.

STEP 1 | （選用）繞過用於 Panorama 與 NSX-T 管理員之間通訊的 Proxy 伺服器設定，在 Panorama 上設定於 **Panorama** > **Setup**（設定） > **Services**（服務） > **Proxy Server**（**Proxy** 伺服器）下方。此命令可讓 Panorama 直接與 NSX-T 管理員通訊，同時維護其他服務的 Proxy 通訊。

1. 登入 Panorama CLI。
2. 執行下列命令，以啟用或停用 Proxy 繞過。

   admin@Panorama> request plugins vmware_nsx proxy bypass {yes | no}

   選取 **yes**（是）以啟用 Proxy 繞過，而選取 **no**（否）以停用 Proxy 繞過。依預設會將其設定為 **no**（否）。

STEP 2 | 登入 Panorama 網頁介面。

使用 Web 瀏覽器中的安全連線 (https)，利用您在初始設定期間指派的 IP 位址和密碼登入 (https://<*IP address*>)。

STEP 3 | 設定 NSX-T 管理員存取權。對每個要與 Panorama 連線的 NSX-T 管理員重複此程序。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服務管理員），然後按一下 **Add**（新增）。
2. 輸入 NSX-T 管理員的描述性 **Name**（名稱）。
3. （選用）新增 NSX-T 管理員的 **Description**（說明）。
4. 輸入用來存取 NSX-T 管理員的 **NSX Manager URL**（**NSX** 管理員 **URL**）（NSX-T 管理員叢集虛擬 IP 位址或 FQDN）。
5. 輸入 **NSX Manager Login**（**NSX** 管理員登入）認證—使用者名稱和密碼，供 Panorama 驗證 NSX-T 管理員。
6. 按一下 **OK**（確定）。



如果您變更 *NSX-T* 管理員登入密碼，請確保立即在 *Panorama* 上更新密碼。不正確的密碼會使 *Panorama* 與 *NSX-T* 管理員之間的連線中斷。

STEP 4 | 將您的變更提交至 Panorama。

按一下 **Commit**（提交） 和 **Commit to Panorama**（提交至 **Panorama**）。

STEP 5 | 在 Panorama 上驗證連線狀態。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服務管理員）。
2. 確認 **Status**（狀態）欄中的訊息。

   成功連線時，狀態會顯示成 **Registered**（已註冊）。這指出 Panorama 和 NSX-T 管理員同步。

   失敗的狀態訊息為：

   - **No connection**（無連線）：無法連線/建立與 NSX-T 管理員的網路連線。
   - **Invalid Credentials**（無效的認證）：存取認證（使用者名稱和/或密碼）不正確。
   - **Out of sync**（未同步）：在 Panorama 上定義的組態設定與 NSX-T 管理員上定義的組態設定不同。如需失敗原因的詳細資料，請按一下連結。例如，NSX-T 管理員的服務

©2023 Palo Alto Networks, Inc.

定義可能與 Panorama 上所定義的服務定義同名。若要修正錯誤，請使用錯誤訊息中所列的服務定義名稱來驗證 NSX-T 管理員上的服務定義。除非 Panorama 與 NSX-T 管理員上的設定同步，否則您無法在 Panorama 上新增新的服務定義。

- **Connection Disabled**（連線已停用）：已手動停用 Panorama 與 NSX-T 管理員之間的連線。

在 Panorama 上建立範本堆疊和裝置群組

若要使用 Panorama 管理 NSX-T 專用 VM-Series 防火牆，防火牆必須屬於裝置群組以及為範本堆疊成員的範本。設備群組可讓您將需要類似原則和物件的防火牆組合成邏輯單元；您可在 Panorama 上，使用 **Objects**（物件）和 **Policies**（原則）頁籤來定義組態。使用範本堆疊來設定 VM-Series 防火牆在網路上操作時所需要的設定，並建立關聯；在 Panorama 上，請使用 **Device**（裝置）和 **Network**（網路）頁籤來定義組態。Panorama 上具有您 NSX-T 設定所使用之區域的每個範本堆疊，都必須與服務定義相關聯；您在範本堆疊內至少必須建立一個區域，NSX-T 管理員才能將流量重新導向至 VM-Series 防火牆。

Panorama 可同時支援 NSX-T 南北向和 NSX-T 東西向的部署。建議您為 NSX-T 南北向和 NSX-T 東西向設定個別的裝置群組、範本堆疊和服務定義。

STEP 1 | 新增設備群組或設備群組階層。

1. 選取 **Panorama** > **Device Groups**（裝置群組），然後按一下 **Add**（新增）。您還可以建立裝置群組階層。
2. 輸入唯一的 **Name**（名稱）及 **Description**（描述）以識別裝置群組。
3. 按一下 **OK**（確定）。
4. 按一下 **Commit**（提交），並選取 **Panorama** 作為 **Commit Type**（提交類型），以將變更儲存到 Panorama 上正在執行的組態。

STEP 2 | 新增範本。

1. 選取 **Panorama** > **Templates**（範本），然後按一下 **Add**（新增）。
2. 輸入唯一的 **Name**（名稱）和 **Description**（描述）以識別範本。
3. 按一下 **OK**（確定）。
4. 按一下 **Commit**（提交），再選取 **Panorama** 做為 **Commit Type**（提交類型），以便將變更儲存到 Panorama 上正在執行的組態。

STEP 3 | 建立範本堆疊。

1. 選取 **Panorama** > **Templates**（範本），然後按一下 **Add Stack**（新增堆疊）。
2. 輸入唯一的 **Name**（名稱）和 **Description**（描述）以識別範本。
3. 按一下 **OK**（確定）。
4. 按一下 **Commit**（提交），然後選取 **Commit to Panorama**（提交至 **Panorama**），將變更儲存到 Panorama 上正在執行的設定。

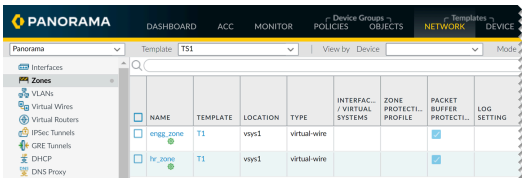
©2023 Palo Alto Networks, Inc.

STEP 4 | 建立每個範本的區域。

每個區域都會對應至 NSX-T 管理員上的一個服務設定檔。區域必須是虛擬介接類型且與服務定義相關聯的範本才算合格。

在每個範本中，您最多可以新增 32 個區域。

1. 選取 **Network**（網路） > **Zones**（區域）。
2. 在 **Template**（範本）下拉式清單中，選取正確的範本。
3. 選取 **Add**（新增），然後輸入區域 **Name**（名稱）。
4. 將介面 **Type**（類型）設為 **Virtual Wire**（虛擬介接）。
5. 按一下 **OK**（確定）。
6. 確認區域已連接至正確的範本。



7. 按一下 **Commit**（提交），再選取 **Panorama** 做為 **Commit Type**（提交類型），以便將變更儲存到 Panorama 上正在執行的組態。

   認可時，Panorama 會在 NSX-T 管理員上建立每個合格區域的對應服務設定檔。

STEP 5 | 更新範本堆疊的 DNS 和 NTP 伺服器資訊。如果您在部署中使用裝置憑證，則必須完成此步驟。這是為了確保部署在 NSX-T 環境中的防火牆，具有到達裝置憑證伺服器所需的正確 DNS 資訊。

1. 確認您從 **Template**（範本）下拉式清單中指定正確的範本堆疊。
2. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務），然後按一下 **Edit**（編輯）圖示。
3. 在 [Services（服務）] 頁籤上，輸入 **Primary DNS Server**（主要 **DNS** 伺服器）和 **Secondary DNS Server**（次要 **DNS** 伺服器）的 IP 位址。
4. 在 NTP 頁籤上，輸入 **NTP Server**（**NTP** 伺服器）的 IP 位址。
5. 按一下 **OK**（確定）。
6. 將您的變更 **Commit**（提交）至 Panorama。

在 Panorama 上設定服務定義

服務定義會指定安裝於 NSX-T 資料中心環境中的 VM-Series 防火牆的設定。服務定義必須包含裝置群組、範本堆疊和 OVF URL。

©2023 Palo Alto Networks, Inc.

STEP 1 | （選用）設定通知群組

指定當虛擬環境變更時應該通知的裝置群組，以建立通知群組。指定的裝置群組所包含的防火牆，將會收到安全性群組和其中來賓 VM 的 IP 位址的即時更新。防火牆會使用此更新，決定構成原則中參照之動態位址群組的最新成員清單。

1. 選取 **Panorama** > **VMware** > **Notify Group**（通知群組），然後按一下 **Add**（新增）。
2. 為通知群組指定具描述性的 **Name**（名稱）。
3. 勾選當虛擬環境變更時應該通知的所有裝置群組的核取方塊。如果裝置群組沒有可用的核取方塊，這表示裝置群組將自動包含於裝置群組階層。
4. 按一下 **OK**（確定）。

STEP 2 | 新增服務定義

您可以在 *Panorama* 上建立多達 *32* 個服務定義。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Service Definitions**（服務定義）。
2. 按一下 **Add**（新增）來建立新的服務定義。
3. 輸入服務定義的描述性 **Name**（名稱）。
4. （選用）新增可識別 VM-Series 防火牆功能或用途的 **Description**（說明），將會使用此服務定義部署該防火牆。

STEP 3 | 指定設備群組及範本堆疊至服務定義。

務必在 Panorama 上建立範本堆疊和裝置群組。

由於將從 Panorama 集中管理此解決方案中部署的防火牆，因此必須指定防火牆所屬的 **Device Group**（裝置群組）及 **Template Stack**（範本堆疊）。所有使用此服務定義部署的防火牆均屬於該指定的範本堆疊及設備群組。

1. 在 **Device Group**（設備群組）下拉式清單中選取設備群組或設備群組階層。
2. 在 **Template**（範本）下拉式清單中選取範本堆疊。

   您無法將指派給一個服務定義的範本堆疊或設備群組重新用於另一個服務定義。

STEP 4 | 指定 OVF 檔案的位置。

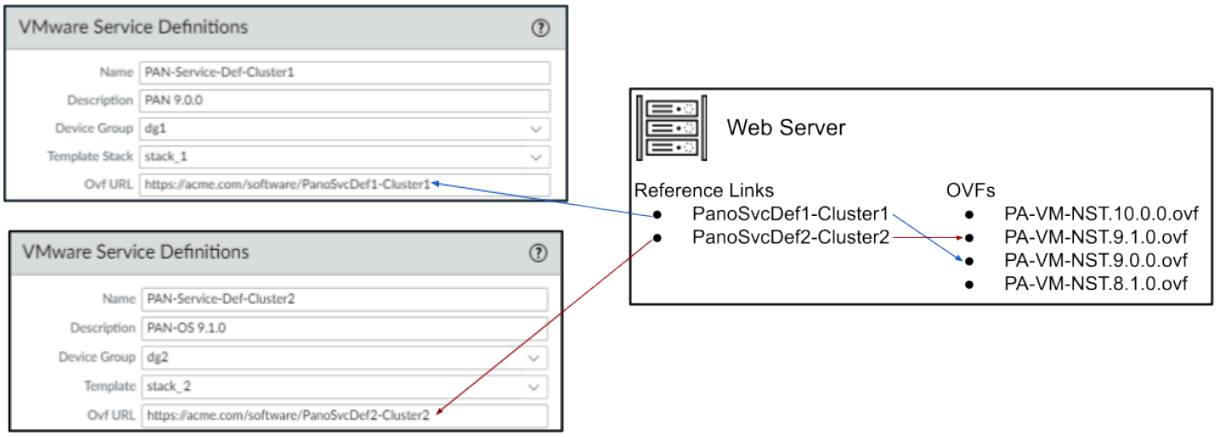
下載 zip 檔案，解壓縮以擷取 .ovf、mf 和 .vmdk 檔案，並儲存至相同的目錄。ovf 和 vmdk 檔案會用來部署防火牆的每個實例。

在 *VM-Series* 防火牆成功部署 *NSX* 服務之後，請勿變更 *Panorama* 服務定義 *OVF* 路徑。成功部署 *VM-Series* 防火牆之後，變更 *OVF* 路徑可能會導致 *NSX* 服務部署失敗狀態。您可以在 *NSX-T* 管理員中解決此失敗，但這可能會導致所有 *VM-Series* 防火牆重新部署。

建議使用可擴展的 OVF 路徑名稱，還可讓您變更基礎映像，而不影響已部署的防火牆。使用的路徑應該像 **https://acme.com/software/PanoSvcDef1-Cluster1.ovf** 這樣，而不是 **https://**

©2023 Palo Alto Networks, Inc.

acme.com/software/PA-VM-NST.9.1.0.ovf。使用靜態路徑參考，未來就不需要變更 OVF 路徑。建議您為部署中的每個 Panama 服務定義 (vSphere 叢集) 建立路徑，並視需要變更 Web 伺服器上的 PAN-OS 基礎映像參考。



在 **OVF URL** 中，新增託管 ovf 檔案的 Web 伺服器位置。http 和 https 都是支援的通訊協定。

您可以在服務定義中使用相同的 OVF 版本或不同的版本。如果在服務定義中使用不同的 OVF 版本，則您可在不同 ESXi 彙集中的 VM-Series 防火牆上變更 PAN-OS 版本。

STEP 5 | （選用）選取 **Notify Group**（通知群組）。

STEP 6 | 選取 **East West**（東西向）作為防火牆的 **Insertion Type**（插入類型）。

STEP 7 | （選用）啟用 **Health Check**（健康情況檢查）。在 VMware NSX 3.2.0 和更新版本專用的 Panorama 外掛程式中，預設會啟用健康情況檢查。在舊版外掛程式中，預設會停用健康情況檢查。此 NSX-T 功能也稱為服務健康情況檢查，可讓您模擬服務實例失敗案例中的高可用性。設定了 VM-Series 防火牆後，如果 VM-Series 服務實例失敗，任何導向至該防火牆的流量將會重新導向至叢集中的其他防火牆（服務叢集部署），或是其他主機上的防火牆實例（主機型部署）。

在 *NSX-T* 中認可並部署 *VM-Series* 防火牆之後，即無法在服務定義中停用或啟用健康情況檢查。若嘗試在健康情況檢查設定中認可變更，將會傳回認可失敗。若要變更此一狀況，您必須刪除並重建服務定義，然後重新部署 *VM-Series* 防火牆。

©2023 Palo Alto Networks, Inc.

STEP 8 | 若要在 NSX Manager 部署 VM-Series 防火牆時自動擷取裝置憑證，請設定裝置憑證。

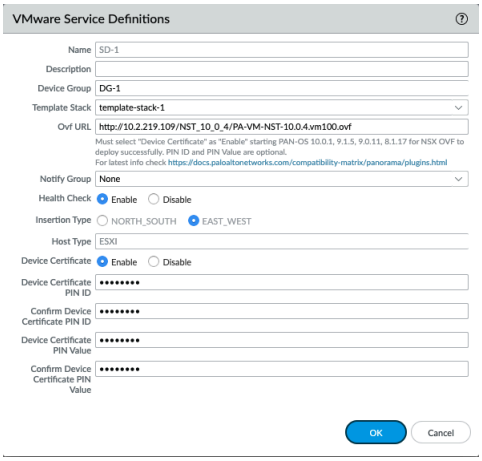
啟用此選項可將裝置憑證套用至新部署的 VM-Series 防火牆。只有在使用支援裝置憑證的基本映像 OVF 來部署防火牆時，才使用此選項。Panorama 會隨著服務定義，將裝置憑證資訊推送至 NSX Manager。在 NSX 中部署新的防火牆後，裝置憑證會在防火牆啟動時安裝於防火牆。

針對 VMware NSX 上的 VM-Series 防火牆，關於支援裝置憑證的 OVF 清單，請參閱 Palo Alto Networks 相容性矩陣。

如果您的 OVF 支援裝置憑證，則無論是否使用裝置憑證，您都必須 **Enable**（啟用）裝置憑證。如果 OVF 不支援裝置憑證，請停用此選項。

1. 如果尚未登入客戶支援入口網站並產生註冊 PIN 和 PIN ID，請這麼做。
2. 在 **Device Certificate**（裝置憑證）下方，按一下 **Enable**（啟用）。
3. 複製 PIN ID，輸入到 **Device Certificate PIN ID**（裝置憑證 **PIN ID**）欄位中。
4. 在 **Confirm Device Certificate PIN ID**（確認裝置憑證 **PIN ID**）欄位中，重新輸入 PIN ID。
5. 複製 PIN 值，輸入到 **Device Certificate PIN Value**（裝置憑證 **PIN** 值）欄位中。
6. 在 **Confirm Device Certificate PIN Value**（確認裝置憑證 **PIN** 值）欄位中，重新輸入 PIN 值。

STEP 9 | 按一下 **OK**（確定）以儲存服務定義。

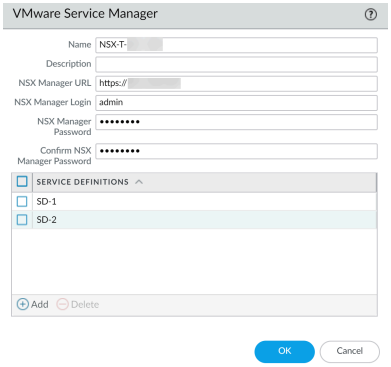


 ©2023 Palo Alto Networks, Inc.

STEP 10 | 將服務定義連接至服務管理員。

您無法在多個服務管理員中使用一個服務定義。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Service Manager**（服務管理員），然後按一下服務管理員名稱的連結。
2. 在 Service Definitions（服務定義）下，按一下 **Add**（新增），從下拉式清單中選取您的服務定義。
3. 按一下 **OK**（確定）。

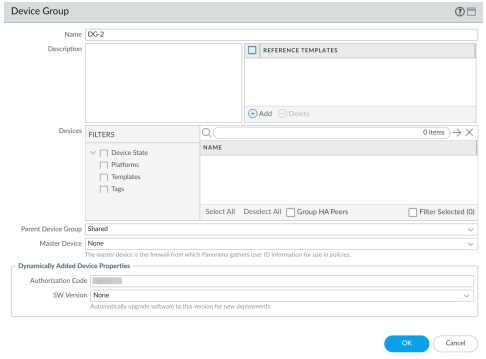


STEP 11 | 新增驗證碼以授權防火牆。

1. 選取 **Panorama** > **Device Groups**（裝置群組），然後選擇與您剛才建立的服務定義相關聯的裝置群組。
2. 在 **Dynamically Added Device Properties**（動態新增的裝置屬性） 下方，新增您在訂購完成電子郵件中收到的授權碼，並選擇性地從 **SW Version**（**SW** 版本）下拉式清單中選取 [None（無）]。

   防火牆部署至 NSX-T 後，會自動新增至裝置群組、使用您提供的授權碼進行授權，並升級至您所指定的 PAN-OS 版本。

   在支援入口網站上，您可以檢視授權您部署的防火牆總數，以及已使用的授權數目與您授權碼所啟用的授權總目的比例。



STEP 12 | **Commit to Panorama**（提交至 **Panorama**）。

©2023 Palo Alto Networks, Inc.

STEP 13 | 在 NSX-T 管理員上，確認服務定義是否可用。

選取 **System**（系統） > **Service Deployments**（服務部署） > **Catalog**（目錄）。服務定義會列為 NSX-T 管理員上的服務實例。

在 NSX-T（東西向）上啟動 VM-Series 防火牆

完成下列程序，將 VM-Series 防火牆以服務的形式部署在您的 NSX-T 環境中。**Deployment Specification**（部署設定）和 **Deployment Template**（部署範本）欄位會自動填入隨著服務定義從 Panorama 推送的資訊。

請勿編輯 *[Deployment Attributes*（部署屬性）*]* 底下的任何設定。這些值會從 *Panorama* 匯入，加以變更會導致部署失敗。

STEP 1 | 登入 NSX-T 管理員。

STEP 2 | 選取 **System**（系統） > **Service Deployments**（服務部署） > **Deployment**（部署）。

STEP 3 | 從 **Partner Service**（合作夥伴服務）下拉式清單中，選取您的服務定義。

STEP 4 | 按一下 **Deploy Service**（部署服務）。

STEP 5 | 輸入服務部署的描述性 **Name**（名稱）。

STEP 6 | 選取 **Compute Manager**（計算管理員）(vCenter)。

STEP 7 | 選取 **Deployment Type**（部署類型）— **Clustered**（叢集化）或 **Host Based**（主機型）。

STEP 8 | 如果您選取 **Clustered**（叢集化）作為 **Deployment Type**（部署類型），請輸入 **Clustered Deployment Count**（叢集化部署計數），以指定要在叢集上部署的 VM-Series 防火牆數目。

STEP 9 | 如果您要在叢集化部署中啟動 VM-Series，請選取 **Host**（主機）。從 **Host**（主機）下拉式清單中選取特定主機，或選取 **Any**（任何）以允許 NSX-T 管理員選擇主機。在 **Per Host**（個別主機）部署中，此選項會呈現為灰色。

STEP 10 | 選取 **Data Store**（資料存放區）作為 VM-Series 防火牆的儲存庫。在叢集化部署中，如果您針對主機選擇了 **Any**（任何），請選取共用資料存放區；如果您指定了特定主機，請選取本機資料存放區。

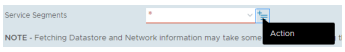
STEP 11 | 設定 **Networks**（網路）設定。

1. 在 [Networks（網路）] 欄中，按一下 **Set**（設定）。
2. 針對 **eth0 - Management Nic**（**eth0 - 管理 Nic**），選取 **Network**（網路）。
3. 選取 **Network Type**（網路類型）— DHCP 或靜態 IP 集區。如果您選擇靜態 IP 集區，請選取 **IP Pool**（**IP** 集區）。
4. 勾選 **eth1 - Data-1 Nic**。
5. 按一下 **Save**（儲存）。

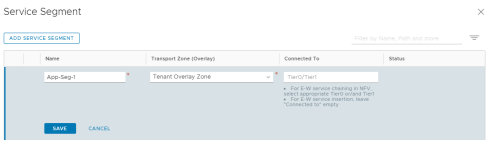
©2023 Palo Alto Networks, Inc.

STEP 12 | 選取或設定 **Service Segment**（服務區段）。若要設定服務區段，請完成下列程序。

1. 按一下 **Service Segments**（服務區段）欄中的 **Action**（動作）。



2. 按一下 **Add Service Segment**（新增服務區段）。
3. 輸入描述性的 **Name**（名稱）。
4. 選取 **Transport Zone (Overlay)**（傳輸區域 **(Overlay)**）。
5. 按一下 **Save**（儲存）和 **Close**（關閉）。



STEP 13 | 選取將要部署服務的 **Cluster**（叢集）。您必須選取具有 **NSX Configuration**（**NSX** 設定）的叢集。

STEP 14 | 按一下 **Save**（儲存）。

STEP 15 | 確認您的防火牆已成功部署。

1. 選取 **System**（系統） > **Service Deployments**（服務部署） > **Service Instances**（服務實例）。
2. 確認您的防火牆已列出，且 **Deployment Status**（部署狀態）顯示為 **Up**（啟動）。

STEP 16 | 確認您的防火牆已連線至 Panorama。

1. 登入 Panorama。
2. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）。
3. 確認您的防火牆列在正確的裝置群組底下，且 **Device State**（裝置狀態）顯示為 **Connected**（已連線）。

   VM-Series 防火牆的裝置名稱在 Panorama 上對 NSX-T (NS) 部署顯示為 **PA-VM:<nsx.clusterid>**，對 NSX-T (EW) 部署顯示為 **PA-VM:<nsx.servicevmid>**。

新增服務鏈結

服務鏈結是邏輯序列中一組服務的群組。流量重新導向至服務鏈結後，將會依據您所設定的順序通過每個服務。

STEP 1 | 選取 **Security**（安全性） > **Network Introspection**（網路自我檢查） > **Service Chains**（服務鏈結） > **Add Chain**（新增鏈結）。

STEP 2 | 輸入服務鏈結的描述性 **Name**（名稱）和 **Description**（說明）（選用）。

STEP 3 | 選取您部署 VM-Series 防火牆時所套用的 **Service Segment**（服務區段）。

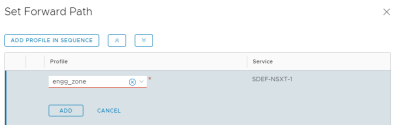
©2023 Palo Alto Networks, Inc.

STEP 4 | 設定轉送路徑。服務鏈結是服務設定檔的邏輯序列，讓流量可依據您指定為轉送路徑的順序通過各服務。

1. 選取 **Set Forward Path**（設定轉送路徑） > **Add Profile in Sequence**（在序列中新增設定檔）。
2. 選取服務設定檔。服務欄會根據您所選取的服務設定檔自動填入。
3. 按一下 **Add**（新增）。
4. （選用）如果您的 NSX-T 環境中有其他合作夥伴服務設定檔，請按一下 **Add Profile in Sequence**（在序列中新增設定檔）將其新增至此服務鏈結。

   每個服務定義只能選取一個服務設定檔。

5. 新增服務設定檔後，請按一下 **Save**（儲存）。



STEP 5 | 在 [Reverse Path（反向路徑）] 欄中，勾選 **Inverse Forward**（反向轉送）**Path**（路徑），讓傳回的流量以相反的順序通過服務鏈結。

STEP 6 | （選用）如果選取了其他合作夥伴服務設定檔，請設定反向路徑。

您必須選取設定於轉送路徑中的相同 *VM-Series* 服務設定檔。

1. 選取 **Set Reverse Path**（設定反向路徑） > **Add Profile in Sequence**（在序列中新增設定檔）。
2. 選取服務設定檔。服務欄會根據您所選取的服務設定檔自動填入。
3. 按一下 **Add**（新增）。
4. （選用）如果您的 NSX-T 環境中有其他服務設定檔，請按一下 **Add Profile in Sequence**（在序列中新增設定檔）將其新增至此服務鏈結。
5. 新增服務設定檔後，請按一下 **Save**（儲存）。

STEP 7 | 設定 **Failure Policy**（失敗原則）— **Allow**（允許）或 **Block**（封鎖）。這會定義 NSX-T 在服務設定檔失敗時所將採取的動作。

STEP 8 | 按一下 **Save**（儲存）。

將流量導向至 VM-Series 防火牆

設定將虛擬機器或虛擬機器群組的流量導向至 VM-Series 防火牆的原則規則。

STEP 1 | 選取 **Security**（安全性） > **Network Introspection (E-W)**（網路自我檢查 **(E-W)**） > **Rules**（規則） > **Add Policy**（新增原則）。

STEP 2 | 按一下 **New Policy**（新增原則），為您的原則提供描述性名稱。

©2023 Palo Alto Networks, Inc.

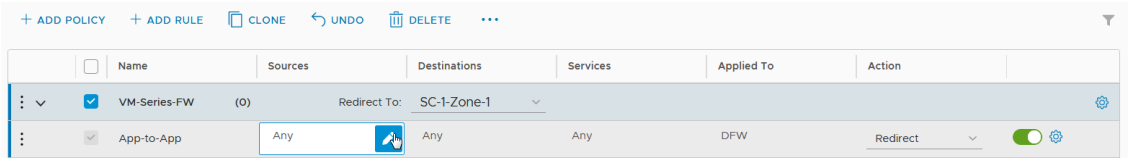
STEP 3 | 從 **Redirect To**（重新導向至）下拉式清單中選取您的服務鏈結。

STEP 4 | 選取原則，然後按一下 **Add Rule**（新增規則）。

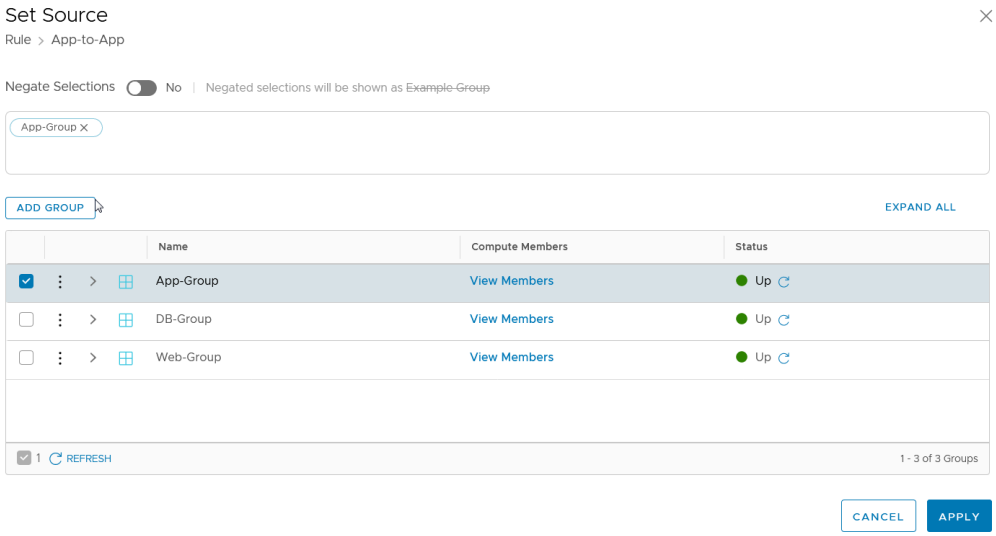
STEP 5 | 按一下 **New Rule**（新增規則），為您的規則提供描述性名稱。

STEP 6 | 選取來源。

1. 按一下來源欄中的鉛筆圖示，以選擇虛擬機器的來源群組。



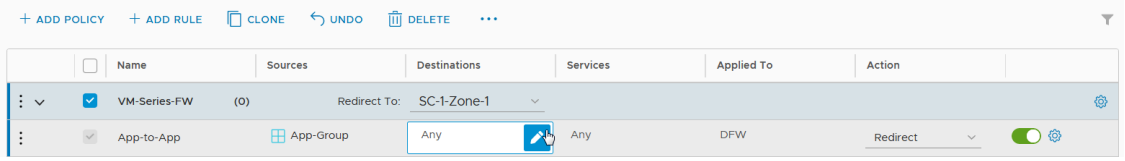
2. 勾選一或多個來源群組。
3. 按一下 **Apply**（套用）。



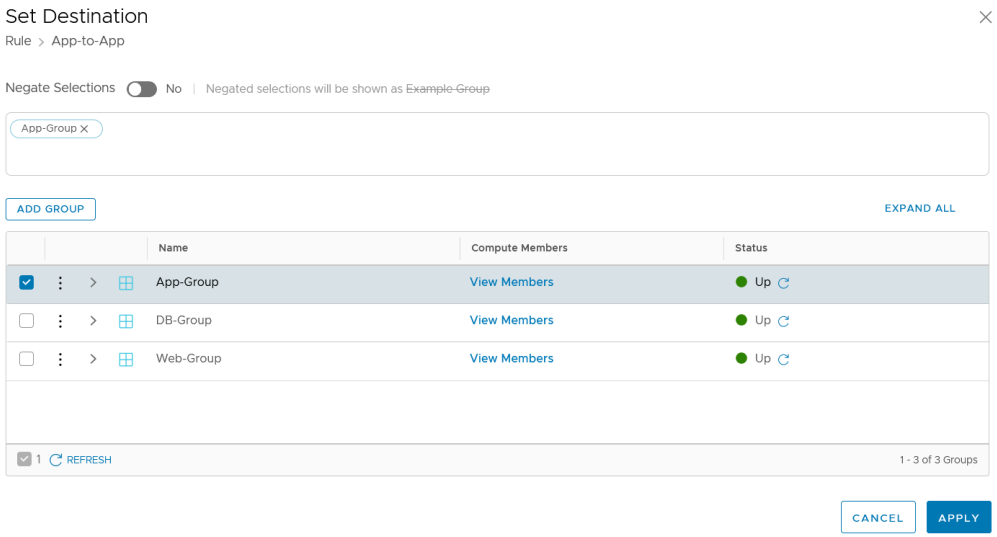
 ©2023 Palo Alto Networks, Inc.

STEP 7 | 選取 **Destination**（目的地）。

1. 按一下目的地欄中的鉛筆圖示，以選擇虛擬機器的來源群組。



2. 勾選一或多個目的地群組。
3. 按一下 **Apply**（套用）。



STEP 8 | （選用）選取要套用規則的 **Services**（服務）。

STEP 9 | 在 **Applied To**（套用至）欄位中選擇下列其中一項：

- 選取 **DFW**，將規則套用至所有連接至邏輯交換器的虛擬 NIC。
- 選取 **Groups**（群組），將規則套用至一或多個指定群組中的成員虛擬機器的虛擬 NIC。

STEP 10 | 選取 **Action**（動作）— **Redirect**（重新導向）或 **Do Not Redirect**（不重新導向）。

STEP 11 | 按一下 **Publish**（發佈）。

STEP 12 | 重複此程序以建立其他原則或規則。

將安全性原則套用至 NSX-T（東西向）上的 VM-Series 防火牆

現在，您已在 NSX-T 管理員上建立重新導向規則，接下來您可以使用 Panorama 集中管理 VM-Series 防火牆上的原則。

若要集中管理原則，請在安全性原則中附加動態位址群組作為來源或目的地位址，並推送至防火牆；防火牆可動態擷取每個安全性群組包含之虛擬機器的 IP 位址，以強制指定群組中之虛擬機器所傳送與接收的流量符合規範。

STEP 1 | 登入 Panorama。

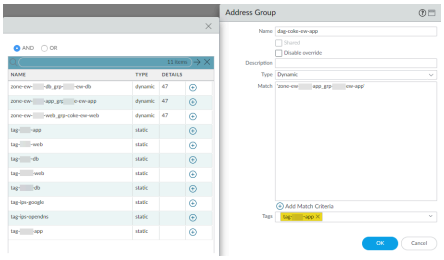
©2023 Palo Alto Networks, Inc.

STEP 2 | 建立動態位址群組。

1. 選取 **Object**（物件） > **Address Groups**（位址群組）。
2. 從 **Device Group**（裝置群組）下拉式清單中，選取您為管理 NSX-T 上的 VM-Series 防火牆而建立的裝置群組。
3. 按一下 **Add**（新增），然後輸入動態位址群組的 **Name**（名稱）和 **Description**（說明）。
4. 在 **Type**（類型）中選取 **Dynamic**（動態）。
5. 將比對準則新增至動態位址群組。

   部分瀏覽器延伸可能會封鎖 *Panorama* 與 *NSX-T* 之間的 *API* 呼叫，進而防止 *Panorama* 接收比對準則。如果 *Panorama* 未顯示比對準則，而且您使用瀏覽器延伸，則請停用延伸，並 *[Synchronize Dynamic Objects*（同步處理動態物件）*]* 以填入 *Panorama* 可用的標籤。
6. 按一下 **Add Match Criteria**（新增比對準則）。
7. 選取 **And** 或 **Or** 運算子，然後按一下安全性群組名稱旁的加號 (+) 圖示，以將它新增至動態位址群組。

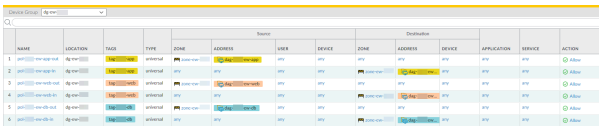
   比對準則對話方塊中顯示的安全性群組衍生自您在 *NSX-T* 管理員上定義的群組。這裡只提供安全性原則中所參考的群組，以及從中將流量重新導向至 *VM-Series* 防火牆的群組。



8. 按一下 **OK**（確定）。
9. 重複這些步驟，以建立部署所需的適當數目的動態位址群組。
10. **Commit**（提交）您的變更。

©2023 Palo Alto Networks, Inc.

STEP 3 | 建立安全性原則規則。



1. 選取 **Policies**（政策） > **Security**（安全性） > **Prerules**（預先規則）。
2. 選取在 Panorama 上建立範本堆疊和裝置群組中您為了管理 NSX-T 上的 VM-Series 防火牆而建立的 **Device Group**（裝置群組）。
3. 按一下 **Add**（新增），並輸入規則的 **Name**（名稱）和 **Description**（說明）。在此範例中，安全性規則允許 WebFrontEnd 伺服器與應用程式伺服器之間的所有流量。
4. 選取 **Source Zone**（來源區域）及 **Destination Zone**（目的地區域）。兩欄中的區域名稱必須相同。
5. 針對 **Source Address**（來源位址）和 **Destination Address**（目的地位址），選取或鍵入位址、位址群組或地區。在此範例中，我們會選取位址群組，即您先前建立的動態位址群組。
6. 選取要允許的 **Application**（應用程式）。在此範例中，我們會建立 **Application Group**（應用程式群組），包含群組在一起之特定應用程式的靜態群組。
   1. 按一下 **Add**（新增），選取 **New Application Group**（新應用程式群組）。
   2. 按一下 **Add**（新增），選取要在群組中包含的應用程式。
   3. 按一下 **OK**（確定）以建立應用程式群組。
7. 針對流量指定動作—**Allow**（允許）或 **Deny**（拒絕），選擇性地在 Profiles（設定檔）下為防毒、反間諜軟體和漏洞保護附加預設的安全性設定檔。
8. 重複以上的步驟以建立適當的政策規則。
9. 按一下 **Commit**（提交），選取 Commit Type（提交類型）作為 **Panorama**。按一下 **OK**（確定）。

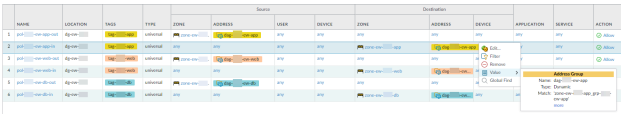
STEP 4 | 將原則套用至 NSX-T 專用 VM-Series 防火牆。

1. 按一下 **Commit**（提交），並選取 **Device Groups**（裝置群組）作為 Commit Type（提交類型）。
2. 選取裝置群組（在此範例中為「NSX-T 裝置群組」），然後按一下 **OK**（確定）。
3. 驗證提交成功。

©2023 Palo Alto Networks, Inc.

STEP 5 | 驗證在 VM-Series 防火牆上填入動態位址群組的成員。

1. 從 Panorama 中交換設備內容，啟動接收您套用原則之防火牆的 Web 介面。
2. 在 VM-Series 防火牆上，選取 **Policies**（原則） > **Security**（安全性），再選取規則。
3. 選取位址群組連結旁的下拉箭頭，再選取 **Inspect**（檢驗）。您也可以驗證比對準則是否正確。



4. 按一下 **more**（更多）連結，並確認出現已註冊的 IP 位址清單。

   將為此位址群組的所有 IP 位址強制執行原則，並在此處顯示。

STEP 6 | （選用）使用範本來推送網路和裝置組態的基本組態，例如 DNS 伺服器、NTP 伺服器、syslog 伺服器和登入橫幅。

如需使用範本的詳細資訊，請參閱《Panorama 管理員指南》。

STEP 7 | 建立地區保護設定檔並將其附加至地區。

地區保護設定檔提供流量保護，並且能夠防禦連接埠掃描、連接埠整理及封包式攻擊。可讓您保護資料中心虛擬電腦間的層級內及層級間流量，以及目的地為資料中心虛擬電腦（工作負載）的網際網路流量。

1. 選取 **Template**（範本）。
2. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Zone Protection**（區域保護），以新增和設定新的設定檔。
3. 選取 **Network**（網路） > **Zones**（區域），並按一下列出的 default-zone，然後在 **Zone Protection Profile**（區域保護設定檔）下拉式清單中選取設定檔。

STEP 8 | 建立 DoS 保護設定檔並將其附加至 DoS 保護原則規則。

1. 選取 **Device Group**（設備群組）。
2. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **DoS Protection**（**DoS** 保護），以新增和設定新的設定檔。
   - 分類設定檔可讓您建立適用於單一來源 IP 的臨界值。例如，您可以為符合原則的 IP 位址設定最大工作階段速率，然後在觸發臨界值後，封鎖該單一 IP 位址。
   - 彙總設定檔可讓您建立適用於符合原則的所有封包的最大工作階段速率。臨界值適用於結合的所有 IP 位址的新工作階段速率。觸發臨界值後，會影響符合原則的所有流量。
3. 在 **Policy**（原則） > **DoS Protection**（**DoS** 保護）中建立新 DoS 保護原則規則，並向其附加新設定檔。

使用 vMotion 在主機之間移動 VM-Series 防火牆

在 VMware NSX-T 中具有同質 CPU 設定的 ESXi 主機之間，使用 vMotion 移動 VM-Series 防火牆時，為了維護流量，您必須使用 PAN-OS CLI，在 vMotion 期間暫停 VM-Series 防火牆的內部活動

 ©2023 Palo Alto Networks, Inc.

訊號監控。您可以指定活動訊號監控暫停的時間量（以分鐘為單位）。活動訊號監控最多可以暫停 60 分鐘。當暫停間隔到期或您刻意結束暫停間隔時，活動訊號監控就會繼續。

如果 ESXi 主機有同質 CPU 設定，則 vSphere 6.5、6.7 和 7.0 支援 VM-Series 防火牆的 vMotion。

如果您執行 *vSphere 7.0* 或更新版本，則使用 *vMotion* 移動 *VM-Series* 防火牆時不需要此程序。

STEP 1 | 登入 VM-Series 防火牆 CLI。

STEP 2 | 使用下列命令設定活動訊號監控暫停間隔。一執行命令就會開始暫停。如果 vMotion 所花時間比預期更長，您可以重新執行此命令來設定更長的新間隔，於命令再次執行時開始計時。

```
request system heartbeat-pause set interval <pause-time-in-minutes>
```

您可以使用下列命令檢視暫停間隔的剩餘時間。

```
request system heartbeat-pause show interval
```

STEP 3 | （選用）如果您在暫停間隔經過之前完成 vMotion，則可以將間隔設為零 (0) 來結束暫停。

```
request system heartbeat-pause set interval 0
```

使用以安全性為中心的工作流程部署 VM-Series

您可以使用以安全性為中心的工作流程，從 Panorama 控制和管理 NSX-T 專用 VM-Series 防火牆。您不需要存取 NSX-T 管理員，也能建立服務鏈和導向規則；但仍然必須在 NSX-T 管理員上建立服務部署。

- 安裝 VMware NSX 專用 Panorama 外掛程式
- 啟用 NSX-T 管理員與 Panorama 之間的通訊
- 在 Panorama 上建立範本堆疊和裝置群組
- 在 Panorama 上設定服務定義
- 在 NSX-T（東西向）上啟動 VM-Series 防火牆
- 建立動態位址群組
- 建立安全性政策
- 建立動態位址群組成員資格準則
- 產生導向政策
- 產生導向規則

安裝 VMware NSX 專用 Panorama 外掛程式

下載並安裝 VMware NSX 專用 Panorama 外掛程式。在安裝或升級外掛程式之前，請先參閱相容性矩陣。

以安全性為中心的部署工作流程需要 *VMware NSX 4.0.0* 專用 *Panorama* 外掛程式。此外，您必須從 *VMware NSX 3.2.x* 專用 *Panorama* 外掛程式升級至外掛程式 *4.0.0*

©2023 Palo Alto Networks, Inc.

如果您有 Panorama HA 組態，請在每個 Panorama 端點上重複此安裝程序。在 Panorama HA 對等上安裝外掛程式時，請先將外掛程式安裝於被動對等，再安裝於主動對等。安裝外掛程式安裝於被動對等之後會轉換為非運作狀態。將外掛程式安裝於主動對等會將被動對等恢復為運作狀態。

如果您在安裝了多個外掛程式的 HA 配對中安裝了一個獨立的 Panorama 或兩個 Panorama 設備，則在未設定一或多個外掛程式的情況下，外掛程式可能不會收到更新的 IP-Tag 資訊。發生這種情況是因為 Panorama 不會將 IP-Tag 資訊轉送到未設定的外掛程式。此外，如果一或多個 Panorama 外掛程式未處於「已註冊」或「成功」狀態（每個外掛程式的正狀態不同），則可能會出現此問題。在繼續或執行下述命令之前，請確保您的外掛程式處於正狀態。

如果遇到此問題，有兩種權宜方案：

- 解除安裝未設定的外掛程式。建議您不要安裝未打算立即設定的外掛程式
- 您可以使用以下命令來變通處理此問題。對每個 Panorama 實例上的每個未設定外掛程式執行以下命令，以防止 Panorama 等待傳送更新。否則，防火牆可能會遺失一些 IP-Tag 資訊。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以透過執行以下命令來取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

上述的命令在重新啟動後不會持續存在，並且必須在任何後續重新啟動時再次使用。對於 HA 配對中的 Panorama，必須在每個 Panorama 上執行命令。

STEP 1 | 選取 **Panorama** > **Plugins**（外掛程式）。

STEP 2 | 選取 **Check Now**（立即檢查） 以擷取可用更新清單。

STEP 3 | 選取 Action（動作）欄中的 **Download**（下載）以下載外掛程式。

STEP 4 | 選取外掛程式版本，在 Action（動作）欄中按一下 **Install**（安裝）來安裝外掛程式。安裝完成時，Panorama 會通知您。

啟用 NSX-T 管理員與 Panorama 之間的通訊

完成下列程序，以啟用 Panorama 與 NSX-T 管理員之間的通訊。您最多可將 Panorama 連線至 16 個 NSX-T 管理員。如果您要將 Panorama 連線至多個 NSX-T 管理員，則必須謹慎規劃裝置群組階層和範本堆疊，並考量它們與部署所需的其他元件如何互動。服務定義會參照裝置群組和範本堆疊，並將該資訊推送至相關 ESXi 叢集中的防火牆。

©2023 Palo Alto Networks, Inc.

STEP 1 | （選用）繞過用於 Panorama 與 NSX-T 管理員之間通訊的 Proxy 伺服器設定，在 Panorama 上設定於 **Panorama** > **Setup**（設定） > **Services**（服務） > **Proxy Server**（**Proxy** 伺服器）下方。

此命令可讓 Panorama 直接與 NSX-T 管理員通訊，同時維護其他服務的 Proxy 通訊。

1. 登入 Panorama CLI。
2. 執行下列命令，以啟用或停用 Proxy 繞過。

   admin@Panorama> request plugins vmware_nsx proxy bypass {yes | no}

   選取 **yes**（是）以啟用 Proxy 繞過，而選取 **no**（否）以停用 Proxy 繞過。依預設會將其設定為 **no**（否）。

STEP 2 | 登入 Panorama 網頁介面。

使用 Web 瀏覽器中的安全連線 (https)，利用您在初始設定期間指派的 IP 位址和密碼登入 (https://<*IP address*>)。

STEP 3 | 設定 NSX-T 管理員存取權。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服務管理員），然後按一下 **Add**（新增）。
2. 輸入 NSX-T 管理員的描述性 **Name**（名稱）。
3. （選用）新增 NSX-T 管理員的 **Description**（說明）。
4. 輸入用來存取 NSX-T 管理員的 **NSX Manager URL**（**NSX** 管理員 **URL**）（NSX-T 管理員叢集虛擬 IP 位址或 FQDN）。
5. 輸入 **NSX Manager Login**（**NSX** 管理員登入）認證—使用者名稱和密碼，供 Panorama 驗證 NSX-T 管理員。
6. 按一下 **OK**（確定）。
7. 對每個要與 Panorama 連線的 NSX-T 管理員重複此程序。



如果您變更 *NSX-T* 管理員登入密碼，請確保立即在 *Panorama* 上更新密碼。不正確的密碼會使 *Panorama* 與 *NSX-T* 管理員之間的連線中斷。

STEP 4 | 將您的變更提交至 Panorama。

按一下 **Commit**（提交） 和 **Commit to Panorama**（提交至 **Panorama**）。

 ©2023 Palo Alto Networks, Inc.

STEP 5 | 在 Panorama 上驗證連線狀態。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服務管理員）。
2. 確認 **Status**（狀態）欄中的訊息。

   成功連線時，狀態會顯示成 **Registered**（已註冊）。這指出 Panorama 和 NSX-T 管理員同步。

   失敗的狀態訊息為：

   - **No connection**（無連線）：無法連線/建立與 NSX-T 管理員的網路連線。
   - **Invalid Credentials**（無效的認證）：存取認證（使用者名稱和/或密碼）不正確。
   - **Out of sync**（未同步）：在 Panorama 上定義的組態設定與 NSX-T 管理員上定義的組態設定不同。如需失敗原因的詳細資料，請按一下連結。例如，NSX-T 管理員的服務定義可能與 Panorama 上所定義的服務定義同名。若要修正錯誤，請使用錯誤訊息中所列的服務定義名稱來驗證 NSX-T 管理員上的服務定義。除非 Panorama 與 NSX-T 管理員上的設定同步，否則您無法在 Panorama 上新增新的服務定義。
   - **Connection Disabled**（連線已停用）：已手動停用 Panorama 與 NSX-T 管理員之間的連線。

在 Panorama 上建立範本堆疊和裝置群組

若要使用 Panorama 管理 NSX-T 專用 VM-Series 防火牆，防火牆必須屬於裝置群組以及為範本堆疊成員的範本。設備群組可讓您將需要類似原則和物件的防火牆組合成邏輯單元；您可在 Panorama 上，使用 **Objects**（物件）和 **Policies**（原則）頁籤來定義組態。使用範本堆疊來設定 VM-Series 防火牆在網路上操作時所需要的設定，並建立關聯；在 Panorama 上，請使用 **Device**（裝置）和 **Network**（網路）頁籤來定義組態。在 Panorama 上，任何範本堆疊若有 NSX-T 設定中使用的區域，則必須與您稍後將建立的服務定義相關聯；您在範本堆疊內至少必須建立一個區域，NSX-T 管理員才能將流量重新導向至 VM-Series 防火牆。稍後，您會將裝置群組和範本結合到 NSX-T 部署，並建立服務定義。

Panorama 可同時支援 NSX-T 南北向和 NSX-T 東西向的部署。您必須為 NSX-T 南北向和 NSX-T 東西向設定個別的裝置群組、範本堆疊和服務定義。

STEP 1 | 新增設備群組或設備群組階層。

1. 選取 **Panorama** > **Device Groups**（裝置群組），然後按一下 **Add**（新增）。您還可以建立裝置群組階層。
2. 輸入唯一的 **Name**（名稱）及 **Description**（描述）以識別裝置群組。
3. 按一下 **OK**（確定）。
4. 按一下 **Commit**（提交），並選取 **Panorama** 作為 **Commit Type**（提交類型），以將變更儲存到 Panorama 上正在執行的組態。

©2023 Palo Alto Networks, Inc.

STEP 2 | 新增範本。

1. 選取 **Panorama** > **Templates**（範本），然後按一下 **Add**（新增）。
2. 輸入唯一的 **Name**（名稱）和 **Description**（描述）以識別範本。
3. 按一下 **OK**（確定）。
4. 按一下 **Commit**（提交），再選取 **Panorama** 做為 **Commit Type**（提交類型），以便將變更儲存到 Panorama 上正在執行的組態。

STEP 3 | 建立範本堆疊並新增您剛建立的範本。

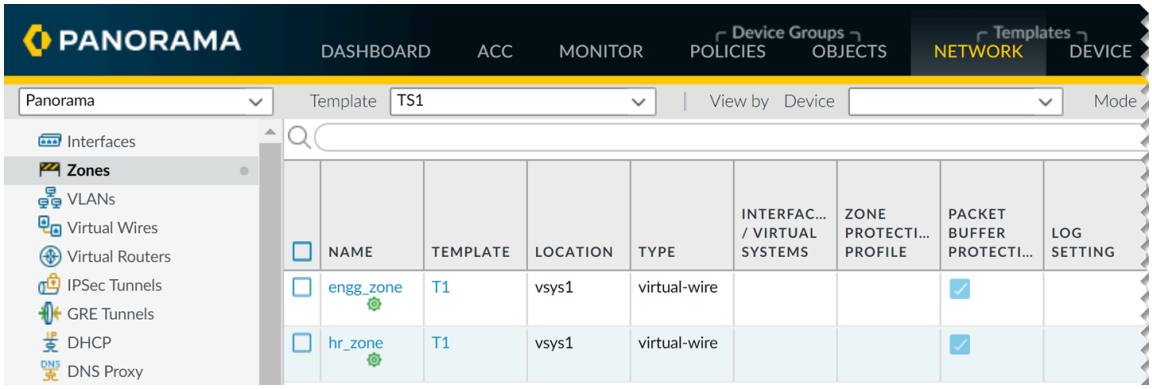
1. 選取 **Panorama** > **Templates**（範本），然後按一下 **Add Stack**（新增堆疊）。
2. 輸入唯一的 **Name**（名稱）及 **Description**（描述）以識別範本堆疊。
3. 在 **Templates**（範本）下，按一下 **Add**（新增），然後從下拉式清單中選取您在步驟 2 建立的範本。
4. 按一下 **OK**（確定）。
5. 按一下 **Commit**（提交），然後選取 **Commit to Panorama**（提交至 **Panorama**），將變更儲存到 Panorama 上正在執行的設定。

STEP 4 | 建立每個範本的區域。

VMware NSX 專用 Panorama 外掛程式會將每個區域對應至 NSX-T 管理員上的服務設定檔。區域必須是虛擬介接類型，而且屬於將與服務定義相關聯的範本，才算合格；如需詳細資訊，請參閱在 Panorama 上設定服務定義。在大多數使用案例中，單一區域就足夠。但是，您必須為多租用戶建立多個區域

在每個範本中，您最多可以新增 32 個區域。

1. 選取 **Network**（網路） > **Zones**（區域）。
2. 在 **Template**（範本）下拉式清單中，選取正確的範本。
3. 選取 **Add**（新增），然後輸入區域 **Name**（名稱）。
4. 將介面 **Type**（類型）設為 **Virtual Wire**（虛擬介接）。
5. 按一下 **OK**（確定）。
6. 確認區域已連接至正確的範本。



7. 按一下 **Commit**（提交），再選取 **Panorama** 做為 **Commit Type**（提交類型），以便將變更儲存到 Panorama 上正在執行的組態。

©2023 Palo Alto Networks, Inc.

STEP 5 | 更新範本堆疊的 DNS 和 NTP 伺服器資訊。如果您在部署中使用裝置憑證，則必須完成此步驟。這是為了確保部署在 NSX-T 環境中的防火牆，具有到達裝置憑證伺服器所需的正確 DNS 資訊。

1. 確認您從 **Template**（範本）下拉式清單中指定正確的範本堆疊。
2. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務），然後按一下 **Edit**（編輯）圖示。
3. 在 [Services（服務）] 頁籤上，輸入 **Primary DNS Server**（主要 **DNS** 伺服器）和 **Secondary DNS Server**（次要 **DNS** 伺服器）的 IP 位址。
4. 在 NTP 頁籤上，輸入 **NTP Server**（**NTP** 伺服器）的 IP 位址。
5. 按一下 **OK**（確定）。
6. 將您的變更 **Commit**（提交）至 Panorama。

在 Panorama 上設定服務定義

服務定義可讓您在 NSX-T 管理員上將 VM-Series 防火牆註冊為合作夥伴安全性服務。服務定義必須包含裝置群組、範本堆疊和 OVF URL。

STEP 1 | （選用）設定通知群組

指定當虛擬環境變更時應該通知的裝置群組，以建立通知群組。指定的裝置群組所包含的防火牆，將會收到安全性群組和其中來賓 VM 的 IP 位址的即時更新。防火牆會使用此更新，決定構成原則中參照之動態位址群組的最新成員清單。

1. 選取 **Panorama** > **VMware** > **Notify Group**（通知群組），然後按一下 **Add**（新增）。
2. 為通知群組指定具描述性的 **Name**（名稱）。
3. 勾選當虛擬環境變更時應該通知的所有裝置群組的核取方塊。如果裝置群組沒有可用的核取方塊，這表示裝置群組將自動包含於裝置群組階層。
4. 按一下 **OK**（確定）。

STEP 2 | 新增服務定義

您可以在 *Panorama* 上建立多達 *32* 個服務定義。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Service Definitions**（服務定義）。
2. 按一下 **Add**（新增）來建立新的服務定義。
3. 輸入服務定義的描述性 **Name**（名稱）。
4. （選用）新增可識別 VM-Series 防火牆功能或用途的 **Description**（說明），將會使用此服務定義部署該防火牆。

©2023 Palo Alto Networks, Inc.

STEP 3 | 指定設備群組及範本堆疊至服務定義。

務必在 Panorama 上建立範本堆疊和裝置群組。

由於將從 Panorama 集中管理此解決方案中部署的防火牆，因此必須指定防火牆所屬的 **Device Group**（裝置群組）及 **Template Stack**（範本堆疊）。所有使用此服務定義部署的防火牆均屬於該指定的範本堆疊及設備群組。

1. 在 **Device Group**（設備群組）下拉式清單中選取設備群組或設備群組階層。
2. 在 **Template**（範本）下拉式清單中選取範本堆疊。

您無法將指派給一個服務定義的範本堆疊或設備群組重新用於另一個服務定義。

STEP 4 | 指定 OVF 檔案的位置。

下載 zip 檔案，解壓縮以擷取 .ovf、mf 和 .vmdk 檔案，並儲存至相同的目錄。ovf 和 vmdk 檔案會用來部署防火牆的每個實例。

在 *VM-Series* 防火牆成功部署 *NSX* 服務之後，請勿變更 *Panorama* 服務定義 *OVF* 路徑。成功部署 *VM-Series* 防火牆之後，變更 *OVF* 路徑可能會導致 *NSX* 服務部署失敗狀態。您可以在 *NSX-T* 管理員中解決此失敗，但這可能會導致所有 *VM-Series* 防火牆重新部署。

在 **OVF URL** 中，新增託管 ovf 檔案的 Web 伺服器位置。http 和 https 都是支援的通訊協定。

您可以在服務定義中使用相同的 OVF 版本或不同的版本。如果在服務定義中使用不同的 OVF 版本，則您可在不同 ESXi 彙集中的 VM-Series 防火牆上變更 PAN-OS 版本。

STEP 5 | （選用）選取 **Notify Group**（通知群組）。

STEP 6 | 選取 **East West**（東西向）作為防火牆的 **Insertion Type**（插入類型）。

STEP 7 | （選用）啟用 **Health Check**（健康情況檢查）。

預設會啟用健康情況檢查。此 NSX-T 功能也稱為服務健康情況檢查，可讓您模擬服務實例失敗案例中的高可用性。設定了 VM-Series 防火牆後，如果 VM-Series 服務實例失敗，任何導向至該防火牆的流量將會重新導向至叢集中的其他防火牆（服務叢集部署），或是其他主機上的防火牆實例（主機型部署）。

在 *NSX-T* 中認可並部署 *VM-Series* 防火牆之後，即無法在服務定義中停用或啟用健康情況檢查。若嘗試在健康情況檢查設定中認可變更，將會傳回認可失敗。若要變更此一狀況，您必須刪除並重建服務定義，然後重新部署 *VM-Series* 防火牆。

©2023 Palo Alto Networks, Inc.

STEP 8 | 若要在 NSX Manager 部署 VM-Series 防火牆時自動擷取裝置憑證，請設定裝置憑證。

啟用此選項可將裝置憑證套用至新部署的 VM-Series 防火牆。只有在使用支援裝置憑證的基本映像 OVF 來部署防火牆時，才使用此選項。Panorama 會隨著服務定義，將裝置憑證資訊推送至 NSX Manager。在 NSX 中部署新的防火牆後，裝置憑證會在防火牆啟動時安裝於防火牆。

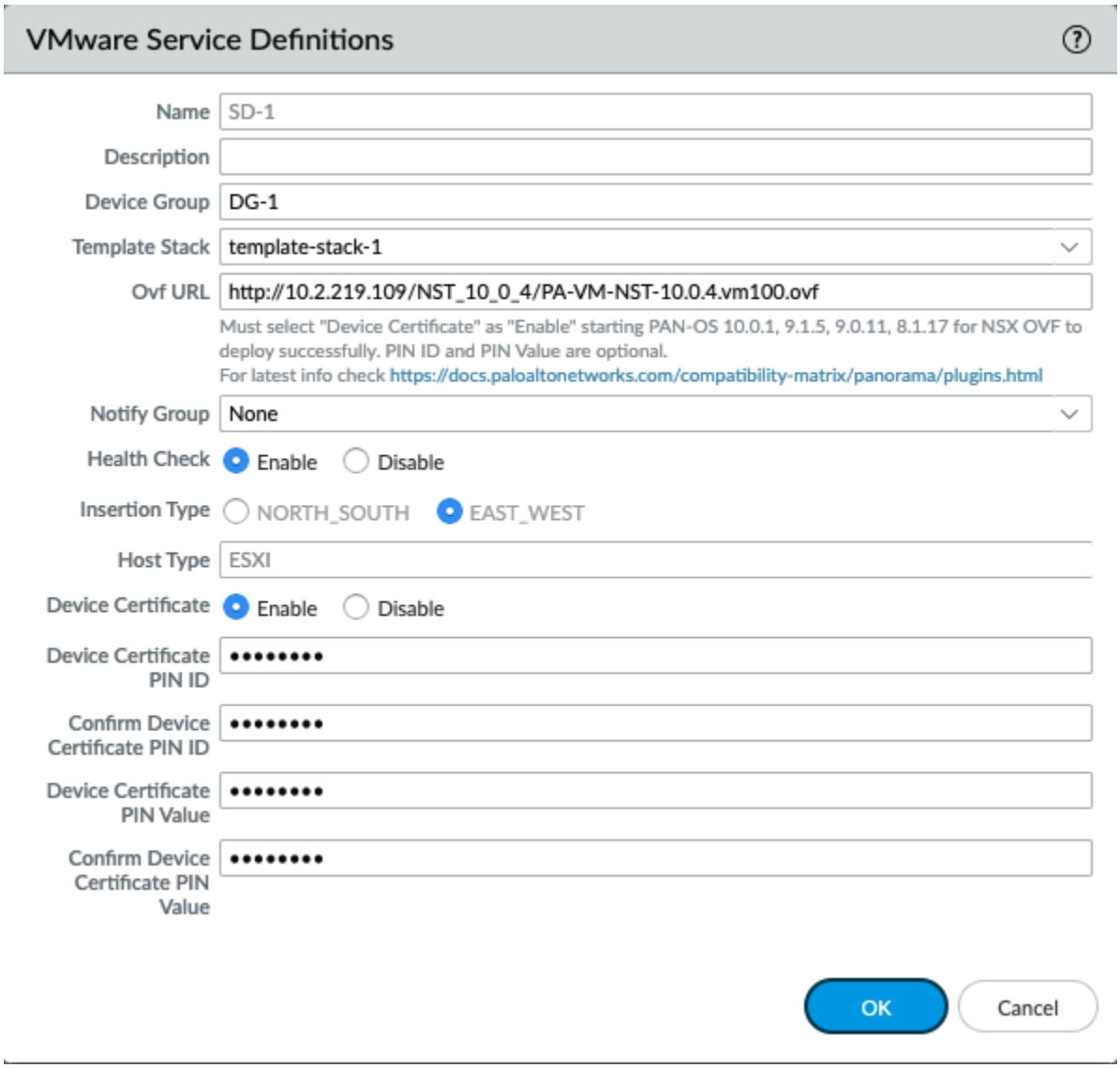
針對 VMware NSX 上的 VM-Series 防火牆，關於支援裝置憑證的 OVF 清單，請參閱 Palo Alto Networks 相容性矩陣。

如果您的 OVF 支援裝置憑證，則無論是否使用裝置憑證，您都必須啟用裝置憑證。如果 OVF 不支援裝置憑證，請停用此選項。

1. 如果尚未登入客戶支援入口網站並產生註冊 PIN 和 PIN ID，請這麼做。
2. 在 **Device Certificate**（裝置憑證）下方，按一下 **Enable**（啟用）。
3. 複製 PIN ID，輸入到 **Device Certificate PIN ID**（裝置憑證 **PIN ID**）欄位中。
4. 在 **Confirm Device Certificate PIN ID**（確認裝置憑證 **PIN ID**）欄位中，重新輸入 PIN ID。
5. 複製 PIN 值，輸入到 **Device Certificate PIN Value**（裝置憑證 **PIN** 值）欄位中。
6. 在 **Confirm Device Certificate PIN Value**（確認裝置憑證 **PIN** 值）欄位中，重新輸入 PIN 值。

©2023 Palo Alto Networks, Inc.

STEP 9 | 按一下 **OK**（確定）以儲存服務定義。

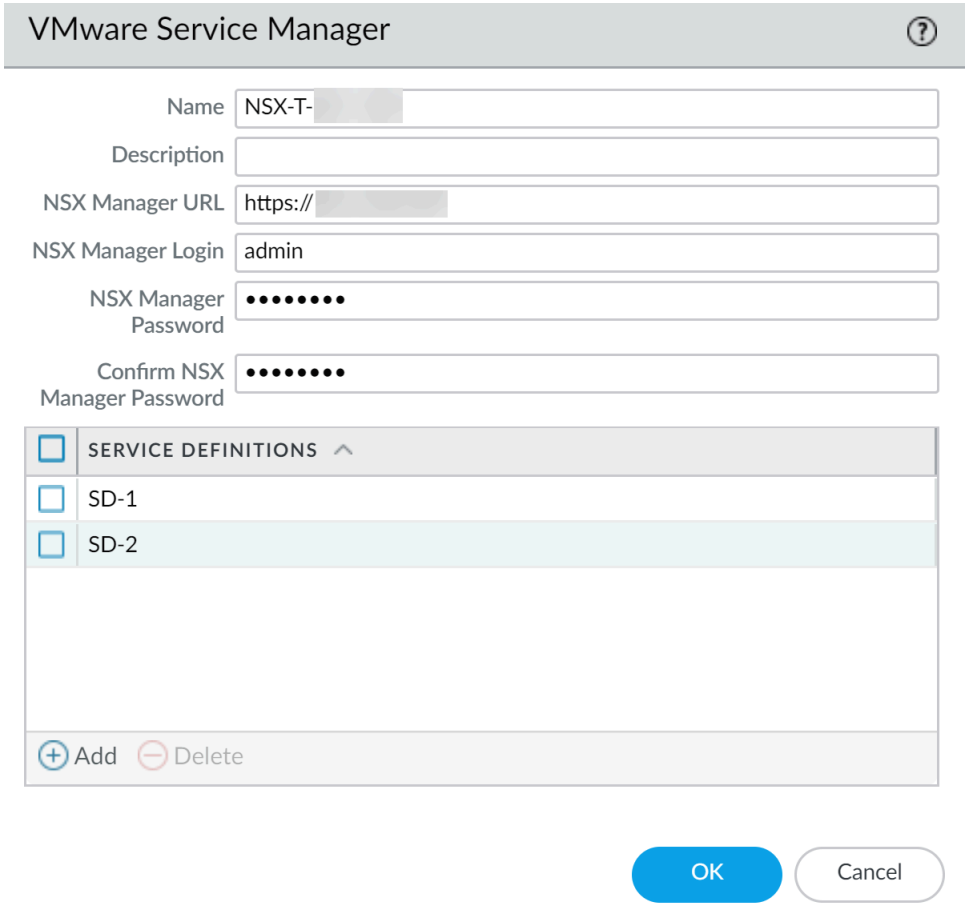


©2023 Palo Alto Networks, Inc.

STEP 10 | 將服務定義連接至服務管理員。

您無法在多個服務管理員中使用一個服務定義。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Service Manager**（服務管理員），然後按一下服務管理員名稱的連結。
2. 在 Service Definitions（服務定義）下，按一下 **Add**（新增），從下拉式清單中選取您的服務定義。
3. 按一下 **OK**（確定）。



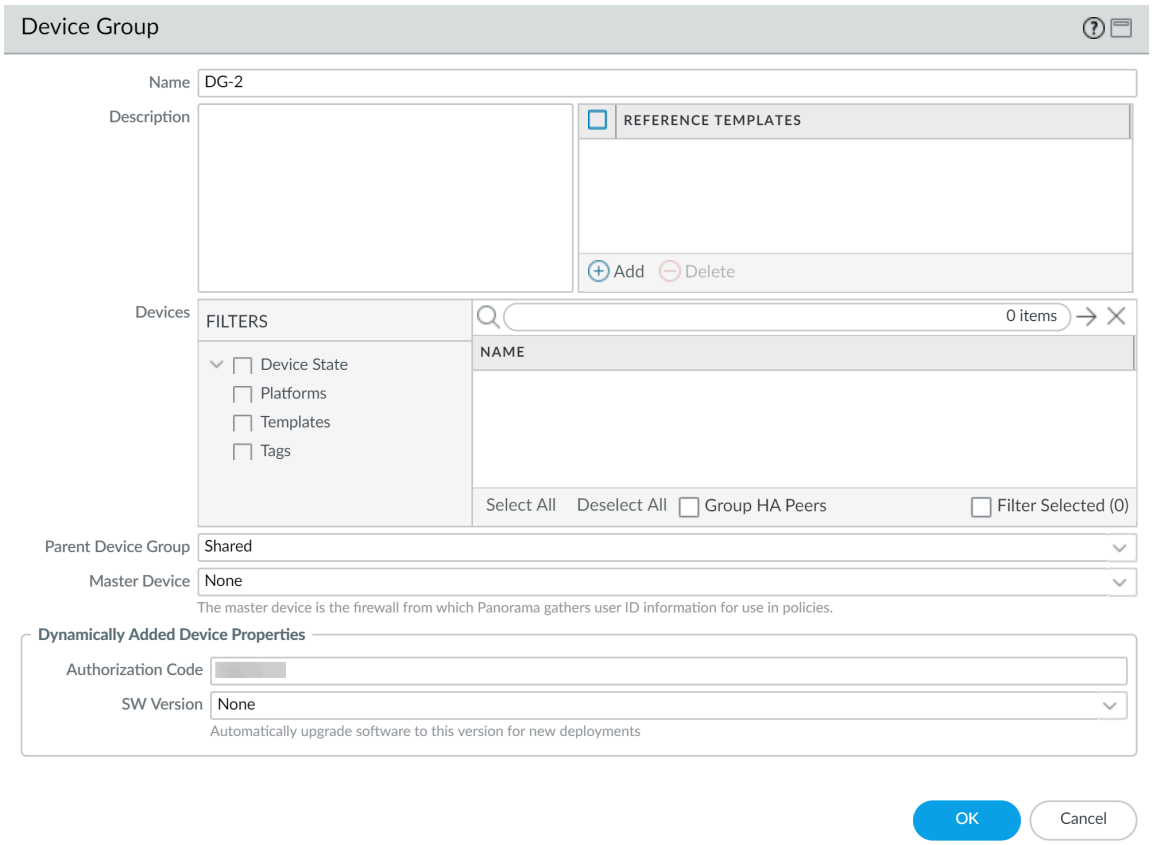
©2023 Palo Alto Networks, Inc.

STEP 11 | 新增驗證碼以授權防火牆。

1. 選取 **Panorama** > **Device Groups**（裝置群組），然後選擇與您剛才建立的服務定義相關聯的裝置群組。
2. 在 **Dynamically Added Device Properties**（動態新增的裝置屬性） 下方，新增您在訂購完成電子郵件中收到的授權碼，並選擇性地從 **SW Version**（**SW** 版本）下拉式清單中選取 [None（無）]。

   防火牆部署至 NSX-T 後，會自動新增至裝置群組、使用您提供的授權碼進行授權，並升級至您所指定的 PAN-OS 版本。

   在支援入口網站上，您可以檢視授權您部署的防火牆總數，以及已使用的授權數目與您授權碼所啟用的授權總目的比例。



STEP 12 | **Commit to Panorama**（提交至 **Panorama**）。

©2023 Palo Alto Networks, Inc.

STEP 13 | 在 NSX-T 管理員上，確認服務定義是否可用。

選取 **System**（系統） > **Service Deployments**（服務部署） > **Catalog**（目錄）。服務定義會列為 NSX-T 管理員上的服務實例。

在 NSX-T（東西向）上啟動 VM-Series 防火牆

完成下列程序，將 VM-Series 防火牆以服務的形式部署在您的 NSX-T 環境中。**Deployment Specification**（部署設定）和 **Deployment Template**（部署範本）欄位會自動填入隨著服務定義從 Panorama 推送的資訊。

請勿編輯 *[Deployment Attributes*（部署屬性）*]* 底下的任何設定。這些值會從 *Panorama* 匯入，加以變更會導致部署失敗。

STEP 1 | 登入 NSX-T 管理員。

STEP 2 | 選取 **System**（系統） > **Service Deployments**（服務部署） > **Deployment**（部署）。

STEP 3 | 從 **Partner Service**（合作夥伴服務）下拉式清單中，選取您的服務定義。

STEP 4 | 按一下 **Deploy Service**（部署服務）。

STEP 5 | 輸入服務部署的描述性 **Name**（名稱）。

STEP 6 | 選取 **Compute Manager**（計算管理員）(vCenter)。

STEP 7 | 選取 **Deployment Type**（部署類型）— **Clustered**（叢集化）或 **Host Based**（主機型）。

STEP 8 | 如果您選取 **Clustered**（叢集化）作為 **Deployment Type**（部署類型），請輸入 **Clustered Deployment Count**（叢集化部署計數），以指定要在叢集上部署的 VM-Series 防火牆數目。

STEP 9 | 如果您要在叢集化部署中啟動 VM-Series，請選取 **Host**（主機）。從 **Host**（主機）下拉式清單中選取特定主機，或選取 **Any**（任何）以允許 NSX-T 管理員選擇主機。在 **Host Based**（主機型）部署中，此選項會停用。

STEP 10 | 選取 **Data Store**（資料存放區）作為 VM-Series 防火牆的儲存庫。在叢集化部署中，如果您針對主機選擇了 **Any**（任何），請選取共用資料存放區；如果您指定了特定主機，請選取本機資料存放區。

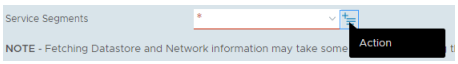
STEP 11 | 設定 **Networks**（網路）設定。

1. 在 [Networks（網路）] 欄中，按一下 **Set**（設定）。
2. 針對 **eth0 - Management Nic**（**eth0 - 管理 Nic**），選取 **Network**（網路）。
3. 選取 **Network Type**（網路類型）— DHCP 或靜態 IP 集區。如果您選擇靜態 IP 集區，請選取 **IP Pool**（**IP** 集區）。
4. 勾選 **eth1 - Data-1 Nic**。
5. 確認兩個介面都勾選。
6. 按一下 **Save**（儲存）。

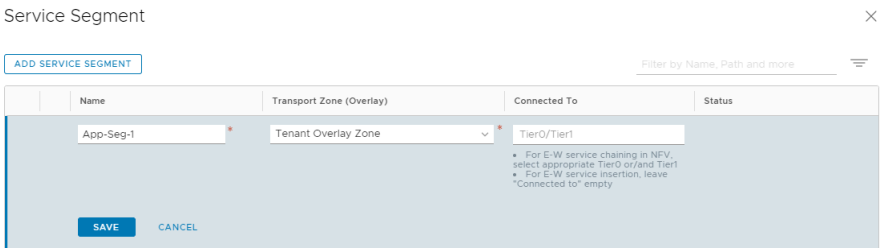
 ©2023 Palo Alto Networks, Inc.

STEP 12 | 選取或設定 **Service Segment**（服務區段）。若要設定服務區段，請完成下列程序。

1. 按一下 **Service Segments**（服務區段）欄中的 **Action**（動作）。



2. 按一下 **Add Service Segment**（新增服務區段）。
3. 輸入描述性的 **Name**（名稱）。
4. 選取 **Transport Zone (Overlay)**（傳輸區域 **(Overlay)**）。
5. 按一下 **Save**（儲存）和 **Close**（關閉）。



STEP 13 | 選取將要部署服務的 **Cluster**（叢集）。您必須選取具有 **NSX Configuration**（**NSX** 設定）的叢集。

STEP 14 | 按一下 **Save**（儲存）。

STEP 15 | 確認您的防火牆已成功部署。

1. 選取 **System**（系統） > **Service Deployments**（服務部署） > **Service Instances**（服務實例）。
2. 確認您的防火牆已列出，且 **Deployment Status**（部署狀態）顯示為 **Up**（啟動）。

STEP 16 | 確認您的防火牆已連線至 Panorama。

1. 登入 Panorama。
2. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）。
3. 確認您的防火牆列在正確的裝置群組底下，且 **Device State**（裝置狀態）顯示為 **Connected**（已連線）。

   VM-Series 防火牆的裝置名稱在 Panorama 上對 NSX-T (NS) 部署顯示為 **PA-VM:<nsx.clusterid>**，對 NSX-T (EW) 部署顯示為 **PA-VM:<nsx.servicevmid>**。

建立動態位址群組

一個安全性群組為一個組合來賓的邏輯容器，這些來賓來自叢集中的多台 ESXi 主機。當您建立符合正確準則的動態位址群組並提交變更時，NSX-T 管理員上會建立相應的安全性群組。必須建立安全性群組以管理並保護來賓。

若要讓動態位址群組成為 NSX-T 上的安全性群組，您必須依下列格式在動態位址群組中新增比對準則：‘**_nsxt_<dynamic-address-group-name>**’。在比對準則中新增的動態位址名稱必須完全符合動態位址群組名稱。例如，稱為 **applications** 的動態位址群組必須包含比對準則「**_nsxt_applications**」。此外，您必須將裝置群組中的動態位址群組加入服務定義中（服務管理員的一部分），然後提交。

©2023 Palo Alto Networks, Inc.

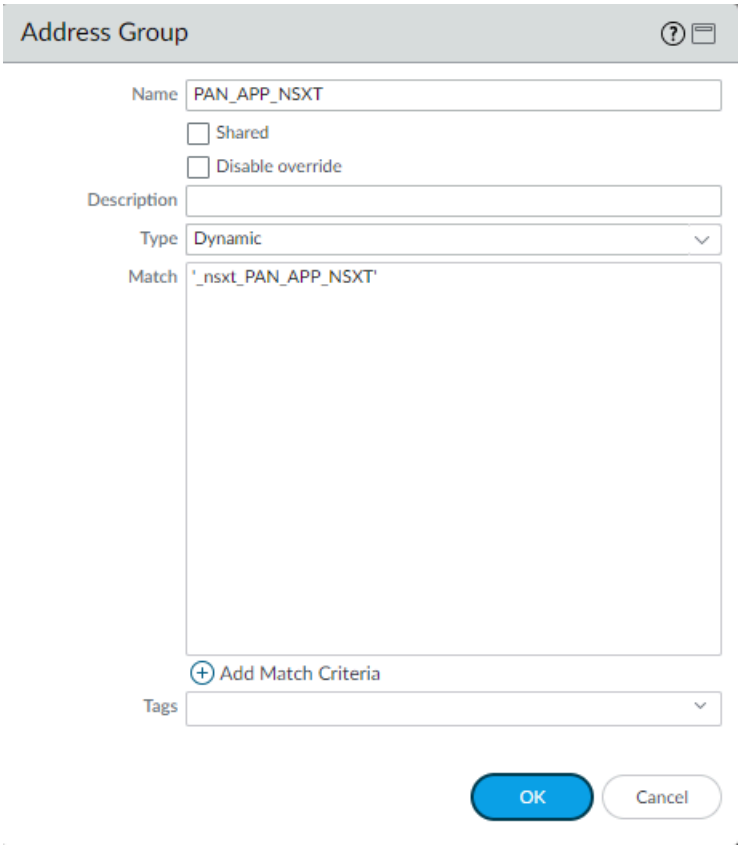
從動態位址組創建的每個安全組都採用以下格式：**<service-def-name>_<dynamic-address-group-name>**。例如，**ServiceDef1_applications**。

在 *Panorama* 上設定的每個裝置群組中，您建立的每個動態位址群組必須有唯一名稱。

STEP 1 | 針對您的部署所需的每個安全性群組，建立動態位址群組。

1. 選取 **Object**（物件） > **Address Groups**（位址群組）。
2. 確認您是在 NSX-T 服務定義相關聯的裝置群組中設定動態位址群組。
3. 按一下 **Add**（新增），再輸入位址群組的 **Name**（名稱）和 **Description**（說明）。
4. 在 **Type**（類型）中選取 **Dynamic**（動態）。
5. 定義比對準則。

   若要讓動態位址群組成為 *NSX-T* 管理員中的安全性群組，必須以單引號括住比對準則字串，且字首為 *_nsxt_*，後面接著位址群組的確切名稱。例如，「***_nsxt_PAN_APP_NSX***」。
6. 針對您需要的每個安全性群組，重複此程序。



STEP 2 | **Commit**（提交）您的變更。

建立安全性政策

建立安全性政策規則，以自動產生在導向政策中使用的導向規則。

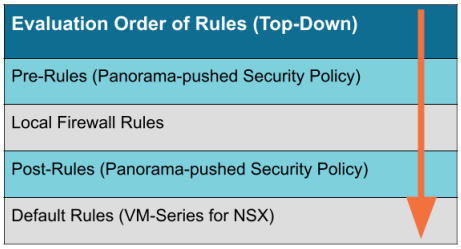
©2023 Palo Alto Networks, Inc.

當您產生導向規則時，您可以選擇根據預先規則、後續規則或全部來產生導向規則。如果您選取 [All（全部）]，NSX 專用 VMware 外掛程式會為預先和後續規則中的每個適用安全性建立導向規則。這可能導致建立不必要的導向規則，更難以管理規則。為了輕鬆區隔導向規則和安全性規則，您可以將導向規則建立為後續規則，將安全性規則建立為預先規則。

若要根據 Panorama 上建立的安全性規則自動產生導向規則，安全性規則必須符合下列準則：

- 屬於向 NSX-T 服務管理員註冊的父或子裝置群組。
- 是內部網路區政策，而且只包含一個區域。
- 不包括針對規則設定的靜態位址群組、IP 範圍或網路遮罩。

在 Panorama 中決定在何處定義 NSX-T 導向規則時（預先或後續規則庫），請考慮您將在 Panorama 上建立的安全性政策規則和 NSX-T 導向規則數目，以及規則套用至流量的順序。預先規則比後續規則更早套用至流量。



- 預先規則 — 您可以使用 Panorama 預先規則庫來定義 NSX-T 導向規則和 VM-Series 防火牆安全性政策規則。如果您在相同規則庫中定義安全性規則和導向規則，則必須考慮安全性規則和導向規則的相對順序。如果規則庫龐大，同時包含導向規則和安全性政策規則，則擴展時，可能會變得難以管理這兩種規則。
- 後續規則 — 將用於檢查和實施的安全性政策規則，與用於產生 NSX-T 導向規則的安全性規則分開，有助於您在有大量規則的部署中擴展。當您自動產生導向規則時，外掛程式會為指定規則庫中每個符合必要準則的規則產生導向規則。因此，將兩種規則隔開，就能避免無意中產生多餘的導向規則。建議使用後續規則庫來管理導向規則，尤其是在有大量安全性政策規則的部署中。

您在安全性規則中指定的來源和目的地動態位址群組。當您自動產生導向規則時，套用規則的地方（NSX-T 分散式防火牆或安全性群組），取決於您在設定安全性規則時指定的來源和目的地。如果您選取任何來源或目的地，NSX-T 管理員會將導向規則套用至分散式防火牆。如果您選取動態位址群組作為來源和目的地，則導向會套用至這些安全性群組中的來賓 VM。如果您手動建立導向規則，則可以指定要套用導向規則的安全性群組。

請確保用來定義導向規則的安全性政策，不含以操作為中心的部署工作流程中設定的動態位址群組。如此一來，導向規則來源和目的地將以 source-any 和 destination-any 推送至 NSX-T 管理員。這可能會影響 NSX-T 環境中的流量。

如果您停用將用來自動產生導向規則的安全性規則，導向規則也會停用。

- 使用預先規則庫定義 NSX-T 導向規則
- 使用後續規則庫定義 NSX-T 導向規則
- 將安全性原則套用至 NSX-T（東西向）上的 VM-Series 防火牆

©2023 Palo Alto Networks, Inc.

使用預先規則庫定義 **NSX-T** 導向規則

下列程序說明如何建立安全性政策規則，以用來產生 NSX-T 導向規則，以及如何建立安全性政策，由 Pananama 推送至 VM-Series 防火牆來檢查和管制流量。

除非您瞭解規則在 NSX-V 管理員及 VM-Series 防火牆和 Panorama 上的運作方式，否則請不要套用流量重新導向政策。VM-Series 防火牆上的預設原則是設定為拒絕所有流量，意味將捨棄重新導向至 VM-Series 防火牆的所有流量。

在相關聯的裝置群組中，建立安全性原則規則。對於每個安全性規則，將 Rule Type（規則類型）設為 Intrazone（內部網路區），在相關聯的範本堆疊中選取一個區域，然後選取動態位址群組作為來源和目的地。如果在 Panorama 中建立合格的安全性政策，當 Panorama 中產生並提交導向規則時，將有助於在 NSX-T 管理員上建立相應的導向規則。

STEP 1 | 在 Panorama 中，選取 **Policies**（政策） > **Security**（安全性） > **Pre Rules**（預先規則）。

STEP 2 | 按一下 **Add**（新增），並輸入安全性原則規則的 **Name**（名稱）和 **Description**（說明）。

STEP 3 | 確認您是在 NSX-T 服務定義相關聯的裝置群組中設定安全性規則。

STEP 4 | 將 Rule Type（規則類型）設為 **intrazone (Devices with PAN-OS 6.1 or later)**（內部網路區（具有 **PAN-OS 6.1** 或更新版本的裝置））。

STEP 5 | 在 Source（來源）頁籤中，將來源區域設為與服務定義相關聯的範本堆疊中的區域。然後，選取您先前建立的動態位址群組（NSX-T 安全性群組），作為 [Source Address（來源位址）]。請勿新增任何靜態位址群組、IP 範圍或網路遮罩作為 Source Address（來源位址）。

STEP 6 | 在 Destination（目的地）頁籤中，Panorama 不允許您設定目的地區域，因為您將規則類型設為內部網路區。然後，選取您先前建立的動態位址群組（NSX-T 安全性群組），作為 [Destination Address（目的地位址）]。請勿新增任何靜態位址群組、IP 範圍或網路遮罩作為 Destination Address（目的地位址）。

STEP 7 | 按一下 **OK**（確定）。

STEP 8 | 針對您需要的每個導向規則，重複步驟 1 到 7。

STEP 9 | **Commit**（提交）您的變更。

STEP 10 | 將安全性原則套用至 NSX-T（東西向）上的 VM-Series 防火牆.

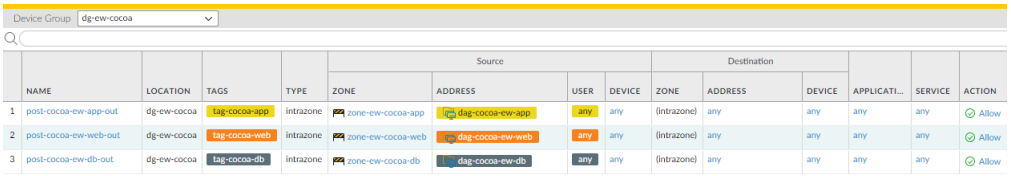
使用後續規則庫定義 **NSX-T** 導向規則

在發布規則庫中建立安全性政策規則以定義 NSX-T 導向規則。

©2023 Palo Alto Networks, Inc.

STEP 1 | 建立安全性原則規則。

1. 在 Panorama 中，選取 **Policies**（政策） > **Security**（安全性） > **Post Rules**（後續規則）。
2. 確認您是在 NSX-T 服務定義相關聯的裝置群組中設定安全性政策規則。
3. 按一下安全性政策規則的名稱以編輯規則。
4. 將 Rule Type（規則類型）設為 **intrazone (Devices with PAN-OS 6.1 or later)**（內部網路區（具有 **PAN-OS 6.1** 或更新版本的裝置））。
5. 在 Source（來源）頁籤中，將來源區域設為與服務定義相關聯的範本堆疊中的區域。然後，選取您先前建立的動態位址群組作為 [Source Address（來源位址）]。請勿新增任何靜態位址群組、IP 範圍或網路遮罩作為 Source Address（來源位址）。
6. 在 Destination（目的地）頁籤中，Panorama 不允許您設定目的地區域，因為您將規則類型設為內部網路區。然後，選取您先前建立的動態位址群組作為 [Destination Address（目的地位址）]。請勿新增任何靜態位址群組、IP 範圍或網路遮罩作為 Destination Address（目的地位址）。
7. 按一下 **OK**（確定）。
8. 針對您需要的每個導向規則，重複步驟 1 到 7。



STEP 2 | 將您的變更 **Commit**（提交）至 Panorama。

STEP 3 | 將安全性政策規則套用到 VM-Series NSX-T EW SEC 中心防火牆。

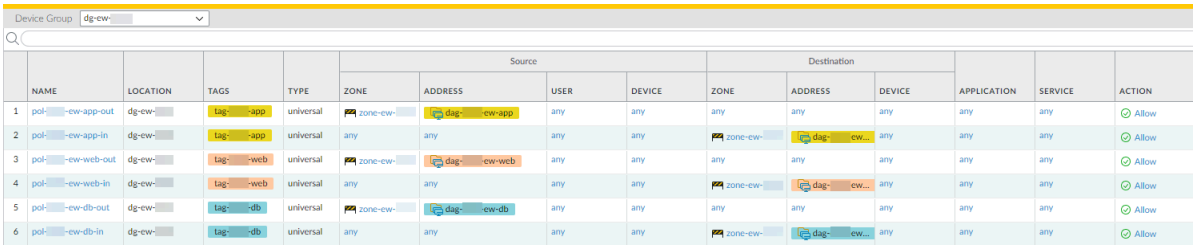
將安全性原則套用至 **NSX-T**（東西向）上的 **VM-Series** 防火牆

既然已定義導向規則，您現在可以使用 Panama 來集中管理 VM-Series 防火牆上的政策。

若要集中管理原則，請在安全性原則中附加動態位址群組作為來源或目的地位址，並推送至防火牆；防火牆可動態擷取每個安全性群組包含之虛擬機器的 IP 位址，以強制指定群組中之虛擬機器所傳送與接收的流量符合規範。

©2023 Palo Alto Networks, Inc.

STEP 1 | 建立安全性原則規則。



1. 選取 **Policies**（政策） > **Security**（安全性） > **Prerules**（預先規則）。
2. 選取在 Panorama 上建立範本堆疊和裝置群組中您為了管理 NSX-T 上的 VM-Series 防火牆而建立的 **Device Group**（裝置群組）。
3. 按一下 **Add**（新增），並輸入規則的 **Name**（名稱）和 **Description**（說明）。在此範例中，安全性規則允許 WebFrontEnd 伺服器與應用程式伺服器之間的所有流量。
4. 選取 **Source Zone**（來源區域）及 **Destination Zone**（目的地區域）。兩欄中的區域名稱必須相同。
5. 針對 **Source Address**（來源位址）和 **Destination Address**（目的地位址），選取或鍵入位址、位址群組或地區。在此範例中，我們會選取位址群組，即您先前建立的動態位址群組。
6. 選取要允許的 **Application**（應用程式）。在此範例中，我們會建立 **Application Group**（應用程式群組），包含群組在一起之特定應用程式的靜態群組。
   1. 按一下 **Add**（新增），選取 **New Application Group**（新應用程式群組）。
   2. 按一下 **Add**（新增），選取要在群組中包含的應用程式。
   3. 按一下 **OK**（確定）以建立應用程式群組。
7. 針對流量指定動作—**Allow**（允許）或 **Deny**（拒絕），選擇性地在 Profiles（設定檔）下為防毒、反間諜軟體和漏洞保護附加預設的安全性設定檔。
8. 重複以上的步驟以建立適當的政策規則。
9. 按一下 **Commit**（提交），選取 Commit Type（提交類型）作為 **Panorama**。按一下 **OK**（確定）。

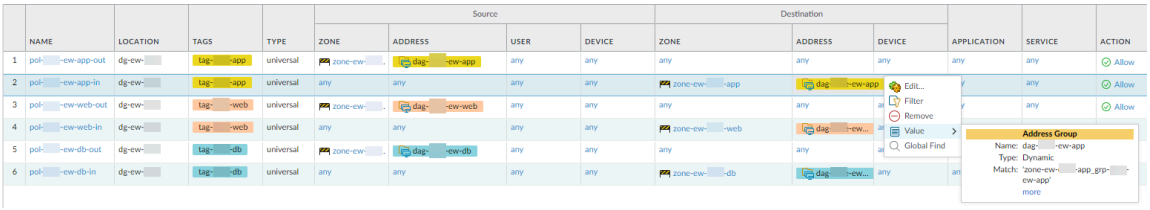
STEP 2 | 將原則套用至 NSX-T 專用 VM-Series 防火牆。

1. 按一下 **Commit**（提交），並選取 **Device Groups**（裝置群組）作為 Commit Type（提交類型）。
2. 選取裝置群組（在此範例中為「NSX-T 裝置群組」），然後按一下 **OK**（確定）。
3. 驗證提交成功。

©2023 Palo Alto Networks, Inc.

STEP 3 | 驗證在 VM-Series 防火牆上填入動態位址群組的成員。

1. 從 Panorama 中交換設備內容，啟動接收您套用原則之防火牆的 Web 介面。
2. 在 VM-Series 防火牆上，選取 **Policies**（原則） > **Security**（安全性），再選取規則。
3. 選取位址群組連結旁的下拉箭頭，再選取 **Inspect**（檢驗）。您也可以驗證比對準則是否正確。



4. 按一下 **more**（更多）連結，並確認出現已註冊的 IP 位址清單。

   將為此位址群組的所有 IP 位址強制執行原則，並在此處顯示。

STEP 4 | （選用）使用範本來推送網路和裝置組態的基本組態，例如 DNS 伺服器、NTP 伺服器、syslog 伺服器和登入橫幅。

如需使用範本的詳細資訊，請參閱《Panorama 管理員指南》。

STEP 5 | 建立地區保護設定檔並將其附加至地區。

地區保護設定檔提供流量保護，並且能夠防禦連接埠掃描、連接埠整理及封包式攻擊。可讓您保護資料中心虛擬電腦間的層級內及層級間流量，以及目的地為資料中心虛擬電腦（工作負載）的網際網路流量。

1. 選取 **Template**（範本）。
2. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Zone Protection**（區域保護），以新增和設定新的設定檔。
3. 選取 **Network**（網路） > **Zones**（區域），並按一下列出的 default-zone，然後在 **Zone Protection Profile**（區域保護設定檔）下拉式清單中選取設定檔。

STEP 6 | 建立 DoS 保護設定檔並將其附加至 DoS 保護原則規則。

1. 選取 **Device Group**（設備群組）。
2. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **DoS Protection**（**DoS** 保護），以新增和設定新的設定檔。
   - 分類設定檔可讓您建立適用於單一來源 IP 的臨界值。例如，您可以為符合原則的 IP 位址設定最大工作階段速率，然後在觸發臨界值後，封鎖該單一 IP 位址。
   - 彙總設定檔可讓您建立適用於符合原則的所有封包的最大工作階段速率。臨界值適用於結合的所有 IP 位址的新工作階段速率。觸發臨界值後，會影響符合原則的所有流量。
3. 在 **Policy**（原則） > **DoS Protection**（**DoS** 保護）中建立新 DoS 保護原則規則，並向其附加新設定檔。

©2023 Palo Alto Networks, Inc.

建立動態位址群組成員資格準則

在 NSX-T 中，您可以在 NSX 專用 Panorama 外掛程式中為屬於 NSX-T 安全性群組（動態位址群組）的虛擬機器和 IP 集，設定成員資格準則。對於每個動態位址群組，您必須指定服務定義，並定義最多五個比對準則，每個準則最多包含五個比對規則。

您在外掛程式上建立此成員資格準則，然後推送至 *NSX-T* 管理員。但是，這並不會將成員資格準則套用至部署中的來賓虛擬機器。您必須在 *NSX-T* 管理員中定義成員資格資料，例如標籤，然後套用至來賓 *VM*。

依規定，NSX-T 專用 Panorama 外掛程式識別和分類虛擬機器是根據兩種成員資格類型 — 虛擬機器或 IP 集。下表列出每個成員類型可用的鍵和運算子。

成員類型	金鑰	運算子
IP 集	頁籤	等於
虛擬電腦	· 頁籤 · 名稱 · 作業系統名稱 · 電腦名稱	· 等於 · 包含 · 開頭為 · 結尾為 · 不等於（不適用於標籤鍵）

只能在 *Panorama* 上變更成員資格準則，請勿在 *NSX-T* 管理員上變更。如果您在 *NSX-T* 管理員上變更，*VMware NSX* 專用 *Panorama* 外掛程式會顯示服務定義不同步。您應該按一下 ***Out-of-Sync***（不同步）連結，以查明不同步狀態的具體原因。如果原因是成員資格準則變更，請按一下 ***NSX-T Config-Sync***（***NSX-T*** 設定同步），以執行設定同步。

STEP 1 | 選取 **Panorama** > **VMware** > **NSX-T** > **Membership Criteria**（成員資格準則） > **Add**（新增）。

對於至少有一個動態位址群組的服務定義，若要新增或修改成員資格準則，您可以按一下服務定義名稱，而不是按一下 **Add**（新增）。

STEP 2 | 從 **Name**（名稱）中，選取成員資格準則的服務定義。選取的服務定義必須具有 East_West 插入類型，而且屬於以安全性為中心的部署。

STEP 3 | 按一下 **Add**（新增）以指定動態位址群組。

STEP 4 | 從下拉式清單中選取 **Dynamic Address Group**（動態位址群組）。下拉式清單列出特定服務定義相關聯的動態位址群組。

外掛程式 *UI* 會顯示 *Panorama* 上設定的動態和靜態位址群組。設定成員資格準則時，請小心不要誤選靜態位址群組。

STEP 5 | 按一下 **Add**（新增），以定義與所選動態位址群組相關聯的準則。

©2023 Palo Alto Networks, Inc.

STEP 6 | 輸入 **Criteria**（準則）的描述性名稱。

STEP 7 | 按一下 **Add**（新增）以定義規則。

STEP 8 | 定義規則。您最多可以建立五個規則。

1. 輸入規則的描述性名稱。
2. 選取 **Member Type**（成員類型）—[Virtual Machine（虛擬機器）] 或 [IP Set（IP 集）]。
3. 選取 **Key**（鍵）—[Tag（標籤）]、[Name（名稱）]、[OS Name（作業系統名稱）]、[Computer Name（電腦名稱）]。
4. 選取 **Operator**（運算子）—[Equals（等於）]、[Contains（包含）]、[Starts With（開頭為）]、[Ends With（結尾為）]、[Not Equals（不等於）]。
5. 輸入 **Value**（值）。

   如果 [Key（鍵）] 設定為 [Tag（標籤）]，則 [Value（值）] 為 [Tag（標籤）]。外掛程式使用者介面不會列出標籤，因此您必須使用 Panorama CLI（搭配 NSX-T 管理員 3.0.0 和更新版本）。

   request plugins vmware_nsx nsx_t nsxt-tags service-definition <SD_name>
6. （選用）輸入 **Scope**（範圍）。範圍僅適用於 **Tag**（標籤）鍵。在 NSX-T 中，範圍是套用至物件標籤的選用值。範圍是在 NSX-T 管理員上定義。例如，如果您根據作業系統來

©2023 Palo Alto Networks, Inc.

標記虛擬機器，則可以為 Windows、Linux 和 MacOS 建立標籤，然後將每個標籤的範圍設定為作業系統。

若要檢視標籤和範圍，請使用 Panorama CLI（搭配 NSX-T 管理員 3.0.0 和更新版本）。

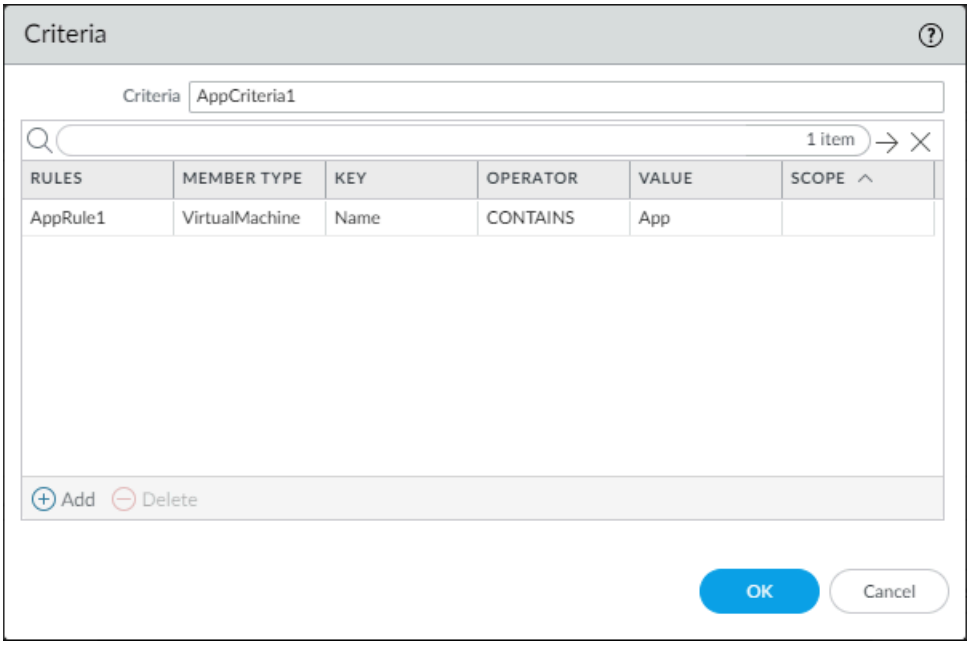
執行以下命令來檢視標籤清單。

```
request plugins vmware_nsx nsx_t nsxt-tags service-definition <SD_name>
```

執行以下命令來檢視特定標籤相關聯的範圍。

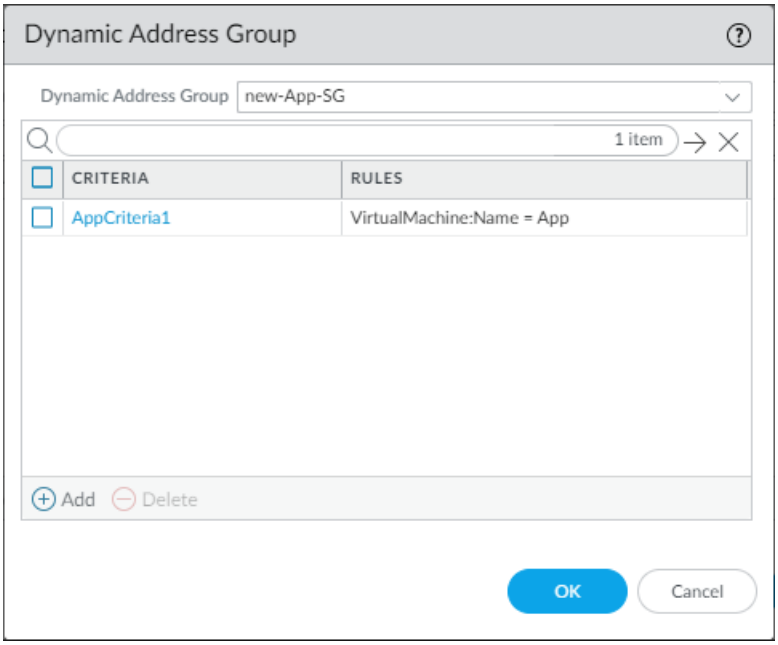
```
request plugins vmware_nsx nsx_t nsxt-scope tag <tag_value> service-definition <SD-name>
```

7. 按一下 **OK**（確定）。
8. （選用）按一下 **Add**（新增）以建立更多（總計最多五個）規則。

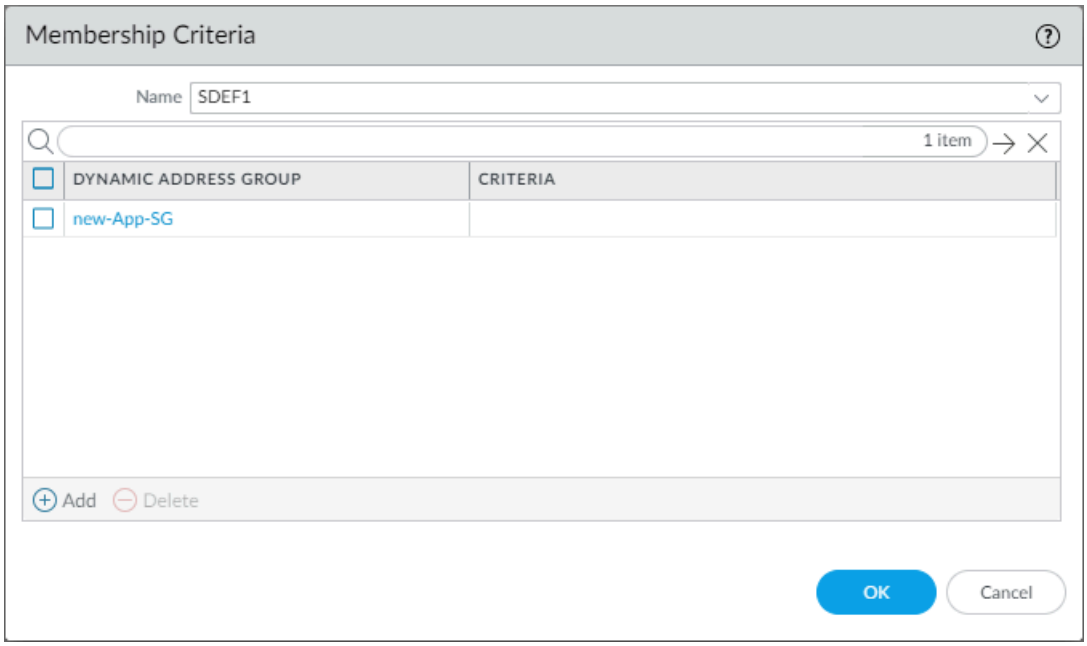


©2023 Palo Alto Networks, Inc.

STEP 9 | 在 [Dynamic Address Group（動態位址群組）] 視窗上，按一下 **OK**（確定）完成，或按一下 **Add**（新增）以建立更多準則（總計最多五個）和規則。



STEP 10 | 在 [Membership Criteria（成員資格準則）] 視窗上，按一下 **OK**（確定）完成，或按一下 **Add**（新增）以指定更多動態位址群組。



產生導向政策

NSX-T 使用導向政策來定義流量將導向的服務鏈。您可以手動建立導向政策，也可以自動產生導向政策。

當您自動產生導向政策時，VMware NSX 專用 Panorama 外掛程式會為每個指定的服務管理員和相關聯的服務定義，建立導向政策。根據預設，TCP 嚴格會停用，且 [Failure Policy（失敗政

©2023 Palo Alto Networks, Inc.

策）] 設定為 Allow（允許）。自動產生的政策採用 **auto_<service-def-name>_<zone-name>_steering_policy** 命名格式。

啟用 TCP 嚴格時，防火牆會強制要求三向交握。如果防火牆在工作階段中途接收流量（例如，由於流量不對稱），但未偵測到三向交握，則會丟棄工作階段。如需詳細資訊，請參閱 VMware NSX-T 文件。

失敗政策定義防火牆故障時如何處理流量。如果您選取 [Allow（允許）]，流量會繼續前往目的地。如果您選取 [Block（封鎖）]，則會丟棄流量。

此外，您可以選取所有服務管理員，而不是選取特定的服務管理員。如果您的任何服務管理員包含以操作為中心的服務定義，則不建議選擇 **All**（全部）。對於以操作為中心的服務定義，此外掛程式會為相關聯的每個區域建立導向政策，然後推送至 NSX-T 管理員。如果您選擇 **All**（全部），請確認您在自動產生導向政策時選取的服務管理員，只包含以安全性為中心的服務定義。

如果您自動產生導向政策，也必須自動產生導向規則。如果您手動建立導向政策，也必須手動建立導向規則。

- 自動產生導向政策
- 手動建立導向政策

只能在 *Panorama* 上變更導向政策，請勿在 *NSX-T* 管理員上變更。如果您在 *NSX-T* 管理員上變更，*VMware NSX* 專用 *Panorama* 外掛程式會顯示服務定義不同步。您應該按一下 ***Out-of-Sync***（不同步）連結，以查明不同步狀態的具體原因。如果原因是導向政策變更，請按一下 ***NSX-T Config-Sync***（***NSX-T*** 設定同步），以執行設定同步。

自動產生導向政策

使用下列程序自動產生導向政策。

下列步驟適用於指定服務管理員，而不是選取 ***All***（全部）。

STEP 1 | 選取 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（網路自我檢查） > **Policy**（政策）。

STEP 2 | 按一下 **Auto Generate**（自動產生）。

STEP 3 | 在 **Service Managers**（服務管理員）中，選擇 **Select**（選取）。

如果您選取 ***All***（全部），而非選取特定的服務管理員，此外掛程式會為設定中每個服務管理員相關聯的每個服務定義，產生導向政策。此外，請確定您選取的服務管理員包含以安全性為中心的服務定義。

STEP 4 | 按一下 **Add**（新增）以選取服務管理員。

STEP 5 | 從下拉式清單中，選取 **Service Manager**（服務管理員）。

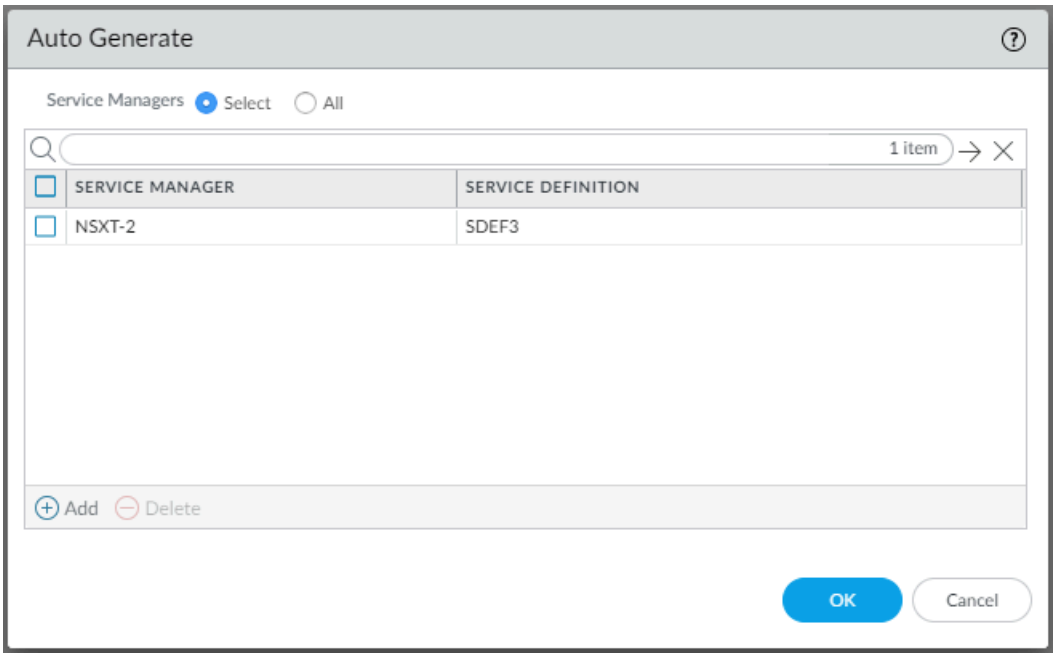
STEP 6 | 按一下 **Add**（新增）以選取服務定義。

 ©2023 Palo Alto Networks, Inc.

STEP 7 | 從下拉式清單中選取服務定義。

STEP 8 | 按一下 **OK**（確定），再按一次 **OK**（確定）。

STEP 9 | 將您的變更 **Commit**（提交）至 Panorama。



手動建立導向政策

使用下列程序手動建立導向政策。

STEP 1 | 選取 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（網路自我檢查） > **Policy**（政策）。

STEP 2 | 按一下 **Add**（新增）。

STEP 3 | 輸入導向政策的描述性 **Name**（名稱）。

導向政策名稱不能包含任何空格。

STEP 4 | 從下拉式清單中，選取 **Service Definition**（服務定義）。

STEP 5 | 從下拉式清單中，選取 **Service Chain**（服務鏈）。

STEP 6 | （選用）啟用 **TCP Strict**（TCP 嚴格）。此選項預設為停用。

STEP 7 | 選擇 **Failure Policy**（失敗政策）— **Allow**（允許）或 **Block**（封鎖）。預設為 Allow（允許）。

STEP 8 | 按一下 **OK**（確定）。

©2023 Palo Alto Networks, Inc.

STEP 9 | 將您的變更 **Commit**（提交）至 Panorama。



產生導向規則

導向政策中定義導向規則。規則定義流量的來源和目的地、自我檢查服務、套用規則的 NSX-T 物件，以及流量重新導向政策。您可以手動建立導向規則，也可以自動產生導向規則。

您必須先產生或建立導向政策，再產生或建立導向規則。

若要根據 Panorama 上建立的安全性規則自動產生導向規則，安全性規則必須符合下列準則：

- 屬於向 NSX-T 服務管理員註冊的父或子裝置群組。
- 是內部網路區政策，而且只包含一個區域。
- 不包括針對規則設定的靜態位址群組、IP 範圍或網路遮罩。

自動產生的導向規則採用 **auto_<device-group-name>_<device-group-rule-name>** 命名格式。

根據預設，設定自動產生的導向規則時不指定 NSX 服務。此外，[NSX Traffic Direction（NSX 流量方向）] 設定為 in-out、[Logging（記錄）] 為 disabled（已停用）、[IP protocol（IP 通訊協定）] 為 ipv4-ipv6、[Action（動作）] 設定為 redirect（重新導向）。自動產生規則後，您可以更新導向以變更預設值。

此外，您可以選取所有服務管理員，而不是選取特定的服務管理員。不建議選擇 **All**（全部）。

如果您自動產生導向政策，也必須自動產生導向規則。如果您手動建立導向政策，也必須手動建立導向規則。

- 自動產生導向規則
- 手動建立導向規則

只能在 *Panorama* 上變更導向規則，請勿在 *NSX-T* 管理員上變更。如果您在 *NSX-T* 管理員上變更，*VMware NSX* 專用 *Panorama* 外掛程式會顯示服務定義不同步。您應該按一下 ***Out-of-Sync***（不同步）連結，以查明不同步狀態的具體原因。如果原因是導向規則變更，請按一下 ***NSX-T Config-Sync***（***NSX-T*** 設定同步），以執行設定同步。

自動產生導向規則

使用下列程序自動產生導向規則。

©2023 Palo Alto Networks, Inc.

當您自動產生導向規則時，套用規則的地方（NSX-T 分散式防火牆或安全性群組），取決於您在設定安全性規則時指定的來源和目的地。如果您選取 **Any**（任何）來源或目的地，NSX-T 管理員會將導向規則套用至分散式防火牆。如果您選取動態位址群組作為來源和目的地，則導向會套用至這些安全性群組中的來賓 VM。

如果您對同屬於導向規則設定的裝置群組設定進行任何變更，例如，轉向規則中對應至 [Applied To（套用至）] 設定的來源和目的地位址群組，則必須再次自動產生導向規則，變更才會生效。

下列步驟適用於指定服務管理員，而不是選取 ***All***（全部）。

STEP 1 | 選取 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（網路自我檢查） > **Rule**（規則）。

STEP 2 | 按一下 **Auto Generate**（自動產生）。

STEP 3 | 從下拉式清單中選取 [Security Rules（安全規則）] 類型—**All**（全部）、僅 **Pre Rulebase**（預先規則庫）或僅 **Post Rulebase**（後續規則庫）。從服務定義中提取安全性規則時是依下列步驟規定。

如果您重新產生導向規則，則會刪除所有目前的規則，並根據選取的規則庫建立新規則。如果您最初使用預先規則庫建立導向規則，然後使用後續規則庫重新產生導向規則，則只會保留後續規則庫導向規則。

STEP 4 | 對於 **Type**（類型），選擇 **Select**（選取）。

STEP 5 | 按一下 **Add**（新增），以指定 **Service Manager**（服務管理員）和 **Service Definition**（服務定義）。

STEP 6 | 從下拉式清單中，選取 **Service Manager**（服務管理員）。

STEP 7 | 按一下 **Add**（新增）以選取服務定義。

STEP 8 | 按一下 **OK**（確定）。

STEP 9 | 按一下 **OK**（確定）以完成，或按一下 **Add**（新增）以指定其他服務管理員和服務定義。

©2023 Palo Alto Networks, Inc.

STEP 10 | （選用）按一下自動產生的規則，以修改下列預設選項。

如果您重新產生導向規則，則會覆寫您對先前產生的導向規則所做的任何變更。

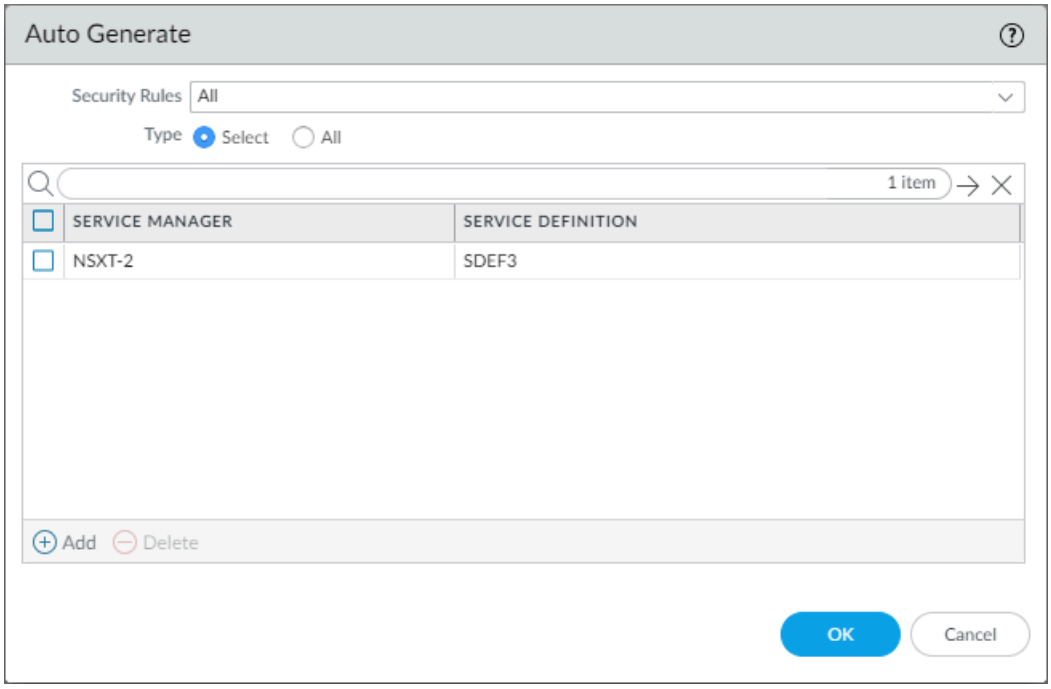
- 啟用 NSX-T **Logging**（記錄）。
- 按一下 **Add**（新增）以指定 **NSX Services**（**NSX** 服務），例如 Active Directory 伺服器、HTTPS、DNS 等。
- **Disable**（停用）規則。如果您停用導向規則，但對應的安全性規則已啟用（**Device Group**（裝置群組） > **Policies**（政策） > **Security**（安全性）），則還是會啟用該導向規則。
- **Applied to**（套用至）可讓您變更要套用導向規則的地方 — **DFW** 或 **Security Group**（安全性群組）。

STEP 11 | 清除不需要或不正確的導向規則。

例如，如果裝置群組包含的安全性規則就位在 NSX-T 導向規則的同一個規則庫，該外掛程式會根據這些非 NSX-T 安全性規則來產生安全性規則。因為這些規則不會參考 NSX-T 動態位址群組，所以在 NSX-T 管理員，這些規則的來源和目的地會設定為 Any（任何）。這種情況可能會影響 NSX-T 管理員如何引導流量。若要避免這種情況，您必須手動刪除不正確的導向規則。

1. 選取不正確的導向規則。
2. 按一下 **Delete**（刪除）。
3. 按一下 **Yes**（是）以確認刪除。

STEP 12 | **Commit**（提交）您的設定，以推送至 NSX-T 管理員。



 ©2023 Palo Alto Networks, Inc.

手動建立導向規則

使用下列程序手動建立導向規則。

STEP 1 | 選取 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（網路自我檢查） > **Rule**（規則）。

STEP 2 | 按一下 **Add**（新增）。

STEP 3 | 輸入導向規則的描述性 **Name**（名稱）。

導向規則名稱不能包括任何空格。

STEP 4 | 從下拉式清單中，選取 **Steering Policy**（導向政策）。

STEP 5 | 從下拉式清單中，選取 **Device Group**（裝置群組）。

STEP 6 | 從下拉式清單中，選取 **Security Rule**（安全性規則）。

[Security Rule（安全性規則）*]* 下拉式清單顯示的規則來自服務定義所有裝置群組的所有安全性規則。請確定您選取適當的安全性規則。

STEP 7 | 指定 **Action**（動作）— **Redirect**（重新導向）或 **Do Not Redirect**（不重新導向）。

STEP 8 | （選用）啟用 NSX-T **Logging**（記錄）。

STEP 9 | 指定 **IP Protocol**（**IP** 通訊協定）— **ipv4-ipv6**、**ipv4** 或 **ipv6**。

STEP 10 | 指定 **NSX Traffic Direction**（**NSX** 流量方向）— **in-out**、**in** 或 **out**。

STEP 11 | （選用）按一下 [Add（新增）] 以指定 **NSX Services**（**NSX** 服務），例如 Active Directory 伺服器、HTTPS、DNS 等。

不支援下列 *ALG* 服務：*FTP*、*TFTP*、*ORACLE_TNS*、*SUN_RPC_TCP*、*SUN_RPC_UDP*、*MS_RPC_TCP*、*MS_RPC_UDP*、*NI*

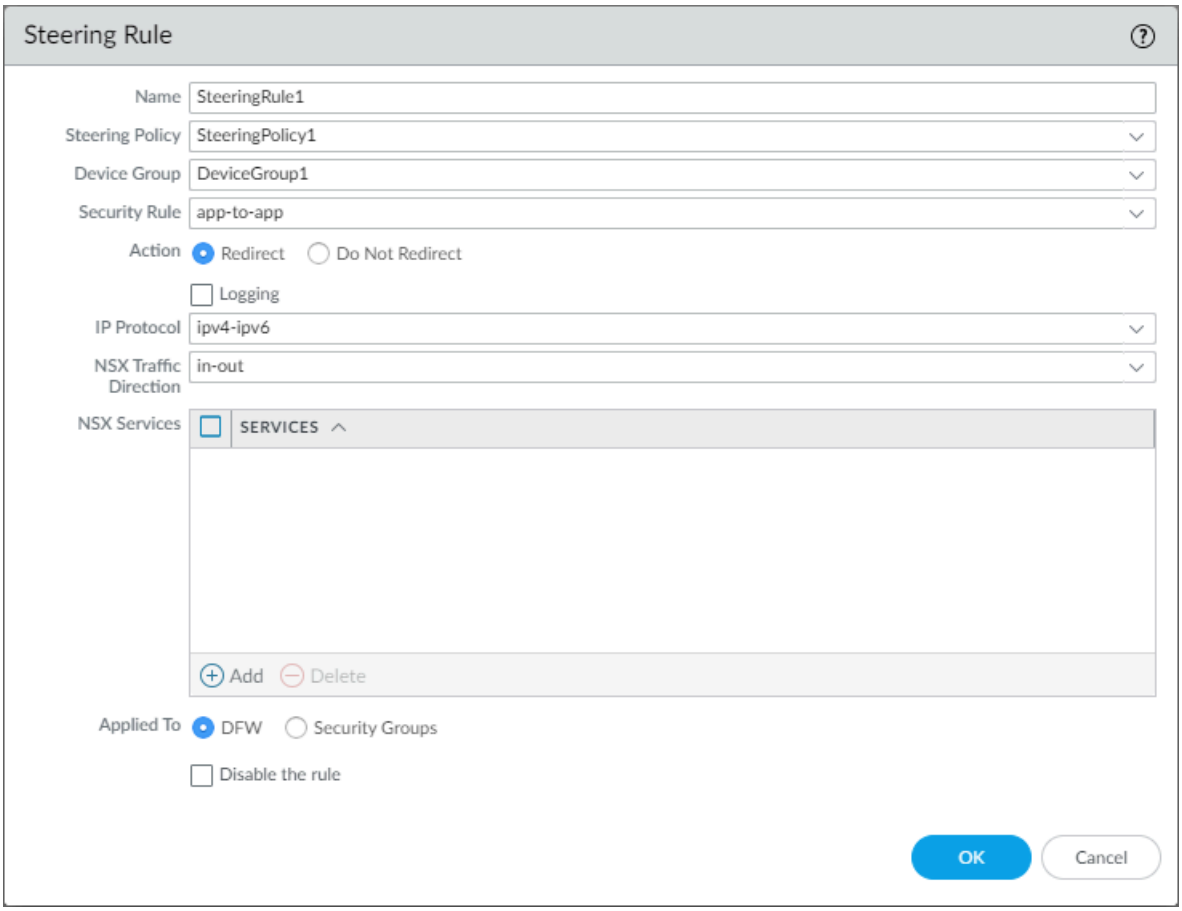
STEP 12 | **Applied To**（套用至）— **DFW** 或 **Security Groups**（安全性群組）。您可以選取一或多個安全性群組。安全性群組是從 Panorama 上設定的動態位址群組建立。安全性群組名稱的格式如下：**<servicedefinition>_<dynamic-address-group>**。如果您選取 DFW，則所有來賓 VM 不論安全性成員資格，都套用導向規則。

STEP 13 | （選用）停用規則。

STEP 14 | 按一下 **OK**（確定）。

 ©2023 Palo Alto Networks, Inc.

STEP 15 | **Commit**（提交）您的設定，以推送至 NSX-T 管理員。



從 Panorama 刪除服務定義

在 Panorama 上，完成以下程序，從 NSX-T 設定中刪除服務定義。

STEP 1 | 登入 Panorama。

STEP 2 | 如果是以安全性為中心的部署，請針對要刪除的服務定義，刪除相關聯的導向規則和導向策略。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（網路自我檢查） > **Rules**（規則）。
2. 選取要刪除的導向規則。
3. 按一下 **Delete**（刪除）。
4. 選取 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（網路自我檢查） > **Policy**（政策）。
5. 選取要刪除的導向政策。
6. 按一下 **Delete**（刪除）。

STEP 3 | **Commit**（提交）您的變更。

STEP 4 | 刪除部署在 NSX-T 中而且與要刪除的服務定義相關聯的 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

STEP 5 | 刪除與服務定義相關聯的成員資格準則。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Membership Criteria**（成員資格準則）。
2. 選取要刪除的準則。
3. 按一下 **Delete**（刪除）。

STEP 6 | 將服務定義與相關聯的服務管理員解除連結。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Service Managers**（服務管理員）。
2. 按一下服務管理員名稱。
3. 選取服務定義。
4. 按一下 **Delete**（刪除）。
5. 按一下 **OK**（確定）。

STEP 7 | 將您的變更 **Commit**（提交）至 Panorama。

從 NSX-T 上的 VM-Series 操作移轉至安全性中心部署

使用下列程序，將以操作為中心的 NSX-T 部署移轉至以安全性為中心的 NSX-T 部署。

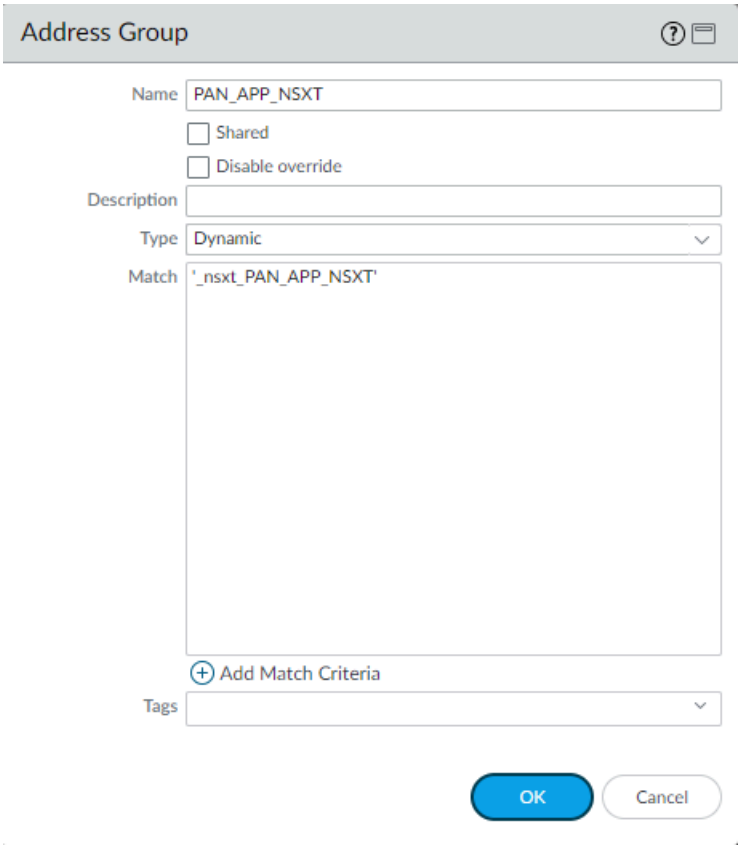
STEP 1 | 登入 Panorama。

©2023 Palo Alto Networks, Inc.

STEP 2 | 修改動態位址群組的比對準則，以遵循以安全性為中心的部署所需的格式。

1. 選取 **Object**（物件） > **Address Groups**（位址群組）。
2. 確認您是在 NSX-T 服務定義相關聯的裝置群組中設定動態位址群組。
3. 按一下先前建立的 NSX-T 動態位址群組的名稱。
4. 編輯比對準則。

   若要讓動態位址群組成為 *NSX-T* 管理員中的安全性群組，必須以單引號括住比對準則字串，且字首為 *_nsxt_*，後面接著位址群組的確切名稱。例如，「***_nsxt_PAN_APP_NSX***」。
5. 針對您需要的每個安全性群組，重複此程序。



 ©2023 Palo Alto Networks, Inc.

STEP 3 | 將作為 NSX-V 導向規則的安全性規則設定為內部網路區。

1. 在 Panorama 中，選取 **Policies**（政策） > **Security**（安全性） > **Pre Rules**（預先規則）。
2. 確認您是在 NSX-T 服務定義相關聯的裝置群組中設定安全性規則。
3. 按一下 **Add**（新增），並輸入安全性原則規則的 **Name**（名稱）和 **Description**（說明）。
4. 將 Rule Type（規則類型）設為 **intrazone (Devices with PAN-OS 6.1 or later)**（內部網路區（具有 **PAN-OS 6.1** 或更新版本的裝置））。
5. 在 Source（來源）頁籤中，將來源區域設為與服務定義相關聯的範本堆疊中的區域。然後，選取您先前建立的動態位址群組作為 [Source Address（來源位址）]。請勿新增任何靜態位址群組、IP 範圍或網路遮罩作為 Source Address（來源位址）。
6. 在 Destination（目的地）頁籤中，Panorama 不允許您設定目的地區域，因為您將規則類型設為內部網路區。然後，選取您先前建立的動態位址群組作為 [Destination Address（目的地位址）]。請勿新增任何靜態位址群組、IP 範圍或網路遮罩作為 Destination Address（目的地位址）。
7. 按一下 **OK**（確定）。
8. 針對您需要的每個導向規則，重複步驟 1 到 7。
9. **Commit**（提交）您的變更。

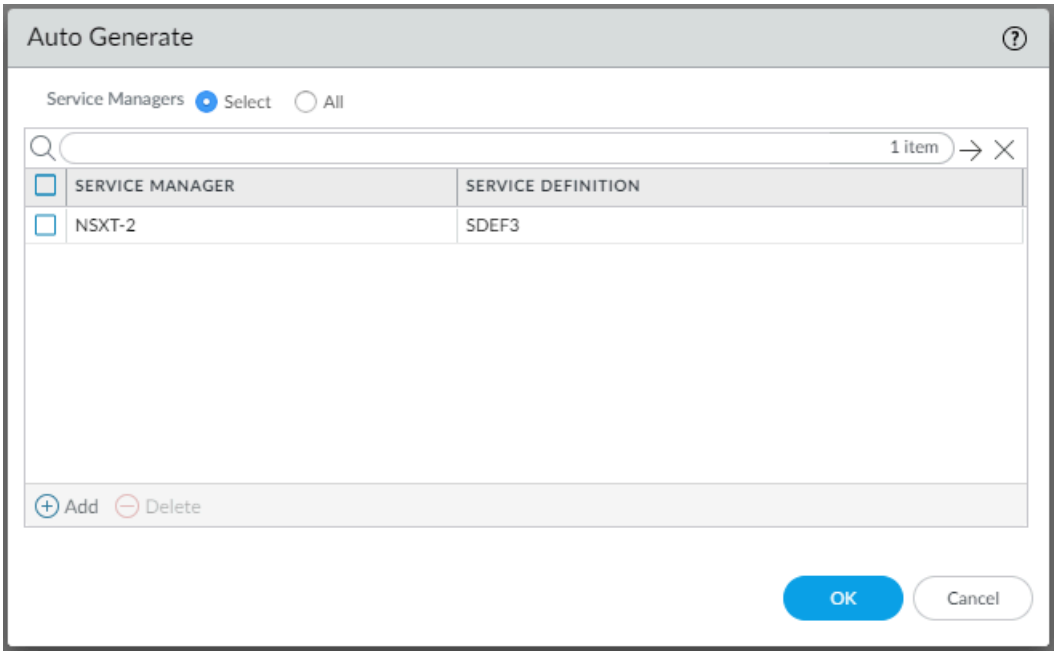
©2023 Palo Alto Networks, Inc.

STEP 4 | 自動產生新的導向政策。

下列步驟適用於指定服務管理員，而不是選取 **All**（全部）。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（網路自我檢查） > **Policy**（政策）。
2. 按一下 **Auto Generate**（自動產生）。
3. 在 **Service Managers**（服務管理員）中，選擇 **Select**（選取）。

   如果您選取 ***All***（全部），而非選取特定的服務管理員，此外掛程式會為設定中每個服務管理員相關聯的每個服務定義，產生導向政策。
4. 按一下 **Add**（新增）以選取服務管理員。
5. 從下拉式清單中，選取 **Service Manager**（服務管理員）。
6. 按一下 **Add**（新增）以選取服務定義。
7. 從下拉式清單中選取服務定義。
8. 按一下 **OK**（確定），再按一次 **OK**（確定）。



9. **Commit**（提交）您的變更。

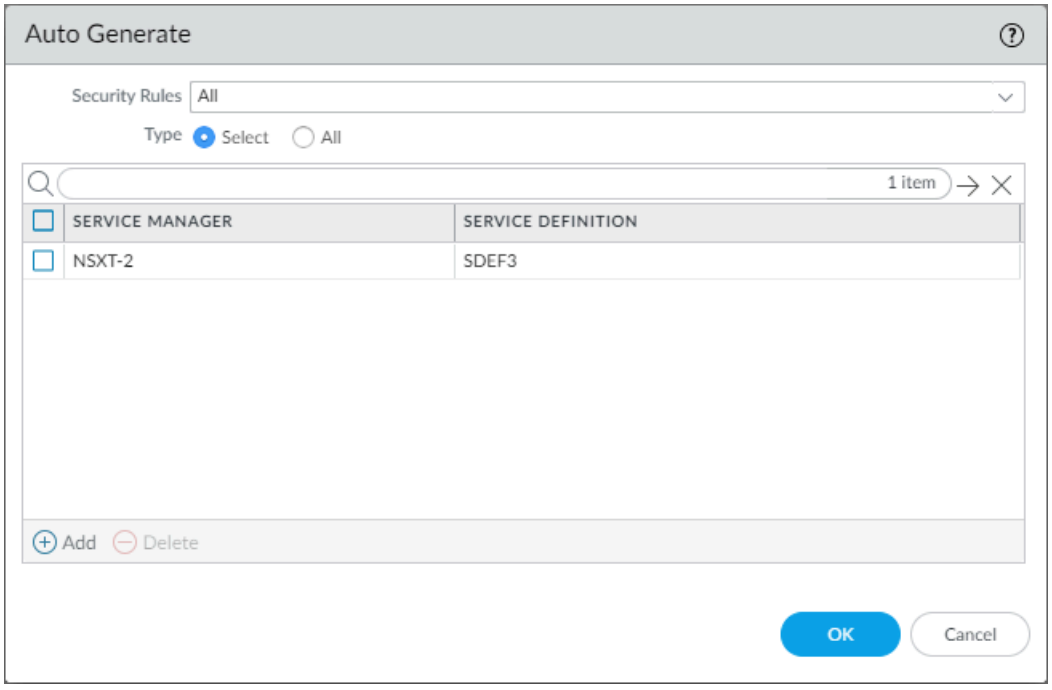
©2023 Palo Alto Networks, Inc.

STEP 5 | 自動產生新的導向規則。

如果您自動產生導向政策，也必須自動產生導向規則。如果您手動建立導向政策，也必須手動建立導向規則。

下列步驟適用於指定服務管理員，而不是選取 ***All***（全部）。

1. 選取 **Panorama** > **VMware** > **NSX-T** > **Network Introspection**（網路自我檢查） > **Rule**（規則）。
2. 按一下 **Auto Generate**（自動產生）。
3. 從下拉式清單中選取 [Security Rules（安全規則）] 類型—**All**（全部）、僅 **Pre Rulebase**（預先規則庫）或僅 **Post Rulebase**（後續規則庫）。從服務定義中提取安全性規則時是依下列步驟規定。
4. 對於 **Type**（類型），選擇 **Select**（選取）。
5. 按一下 Add（新增），以指定 **Service Manager**（服務管理員）和 **Service Definition**（服務定義）。
6. 從下拉式清單中，選取 **Service Manager**（服務管理員）。
7. 按一下 **Add**（新增）以選取服務定義。
8. 按一下 **OK**（確定）。
9. 按一下 **OK**（確定）以完成，或按一下 **Add**（新增）以指定其他服務管理員和服務定義。
10. （選用）按一下自動產生的規則，以修改預設選項。



STEP 6 | 建立動態位址群組成員資格準則.

STEP 7 | 將您的變更 **Commit**（提交）至 Panorama。

©2023 Palo Alto Networks, Inc.

STEP 8 | 從 NSX-T 管理員刪除以操作為中心的導向規則。

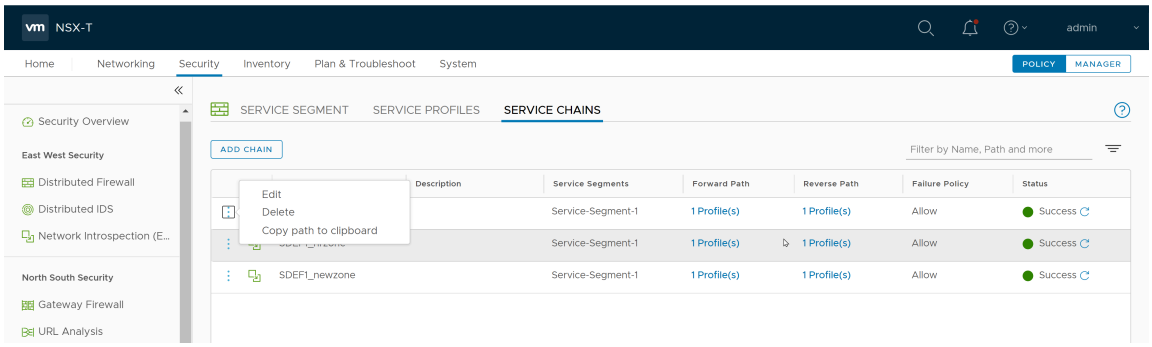
1. 登入 NSX-T 管理員。
2. 選取 **Security**（安全性） > **Network Introspection (E-W)**（網路自我檢查 **(E-W)**） > **Rules**（規則）。
3. 選取每個以操作為中心的導向規則。
4. 按一下 **Delete**（刪除）。

©2023 Palo Alto Networks, Inc.

STEP 9 | 從 NSX-T 管理員刪除以操作為中心的服務鏈。

1. 登入 NSX-T 管理員。
2. 選取 **Security**（安全性） > **Network Introspection**（網路自我檢查） > **Service Chains**（服務鏈）。
3. 按一下垂直省略符號。
4. 按一下 **Delete**（刪除）。

©2023 Palo Alto Networks, Inc.



將安全性政策從 NSX-V 延伸至 NSX-T

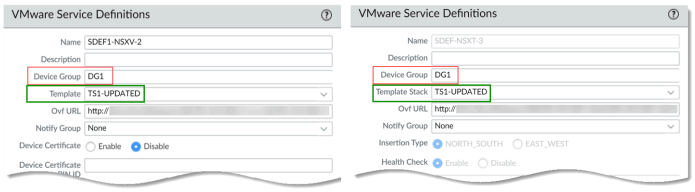
如果您從 NSX-V 部署轉向 NSX-T 部署，或合併 NSX-T 部署與 NSX-V 部署，則不必重新建立政策規則，就能將現有安全性政策從 NSX-V 延伸至 NSX-T。作法是利用現有的裝置群組，並在 NSX-V

©2023 Palo Alto Networks, Inc.

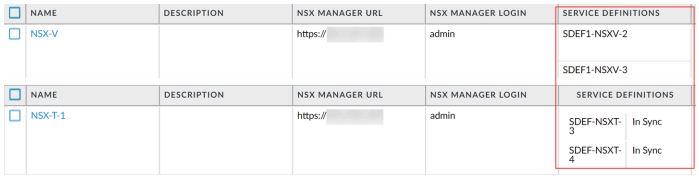
與 NSX-T 服務定義之間共用裝置群組。將政策移轉至 NSX-T 之後，您可以繼續使用 NSX-V 專用 VM-Series，或移除您的 NSX-V 部署。

STEP 1 | 安裝 VMware NSX 專用 Panorama 外掛程式 3.2.0 或更新版本。升級之前，請參閱 VMware NSX 專用 Panorama 外掛程式 3.2.0 版本資訊。

STEP 2 | 針對部署中的每個 NSX-V 服務定義，設定 NSX-T 服務定義。請勿建立新的裝置群組，改為使用現有的 NSX-V 裝置群組。使用現有裝置群組可讓您將 NSX-V 上使用的相同安全性政策規則，套用至 NSX-T 上部署的 VM-Series 防火牆。如果您的政策參考特定區域，請將 NSX-V 服務定義中相同的範本堆疊，新增至 NSX-T 服務定義。此外，如果裝置群組參考特定範本，請確定您選取的範本堆疊包含裝置群組中參考的範本。



STEP 3 | 設定 NSX-T 服務管理員，並將 NSX-T 服務定義與服務管理員建立關聯。



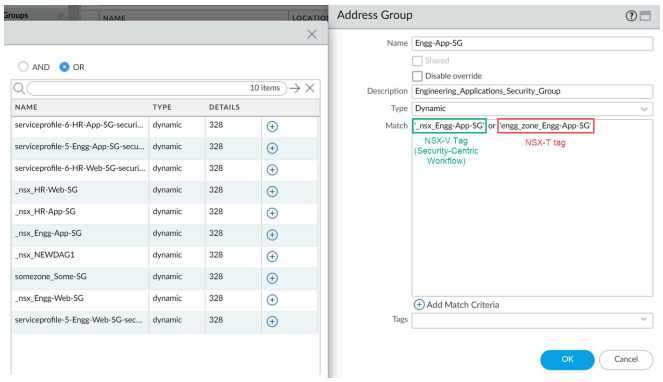
STEP 4 | 準備 NSX-T 環境和部署 VM-Series 防火牆。在啟動 VM-Series 防火牆之前，您必須先建立安全性群組、服務鏈和流量重新導向政策。

- 在 NSX-T（南北向）上部署 VM-Series 防火牆
- 使用以操作為中心的工作流程部署 VM-Series

©2023 Palo Alto Networks, Inc.

STEP 5 | 將 NSX-T 標籤新增至現有的動態位址群組。

1. 選取 **Panorama** > **Objects**（物件） > **Address Groups**（位址群組）。
2. 按一下現有 NSX-V 動態位址群組的名稱。
3. 按一下 **Add Match Criteria**（新增比對規則），以顯示來自 NSX-V 和 NSX-T 的標籤。
4. 將 NSX-T 標籤新增至動態位址群組。標籤之間務必使用 **OR** 運算子。
5. 新增所有必要的標籤之後，按一下 **OK**（確定）。
6. **Commit**（提交）您的變更。



STEP 6 | 當您的 VM 工作負載成功從 NSX-V 移轉至 NSX-T 之後，如果您打算中止使用 NSX-V，請從動態位址群組中移除 NSX-V 標籤。當所有 NSX-V 相關設定從 NSX 專用 Panorama 外掛程式移除，且 VM-Series 防火牆設定也從 NSX-V 管理員移除之後，所有 NSX-V 標籤及對應的 IP 位址就會取消註冊。

使用就地移轉將 VM-Series 從 NSX-V 移至 NSX-T

請完成下列程序，將 VM-Series 防火牆設定從 NSX-V 移轉至 NSX-T。您可以移轉設定，以重複使用 Panorama 上已設定的政策和動態位址群組。此程序參考 VMware 文件中發佈的資訊和程序，以及 PAN 專用的步驟。

此程序僅支援以操作為中心的 NSX-V 部署。部署表示將流量重新導向至 VM-Series 防火牆的政策規則是在 NSX-V 管理員中建立，而不是在 Panorama 中建立。

此程序需要 *NSX-T* 管理員 *3.1.0* 或更新版本。

執行此移轉時，建議規劃安全性停機。

STEP 1 | 根據 VMware 所述的步驟，為移轉而準備 NSX-V 和 NSX-T 環境。

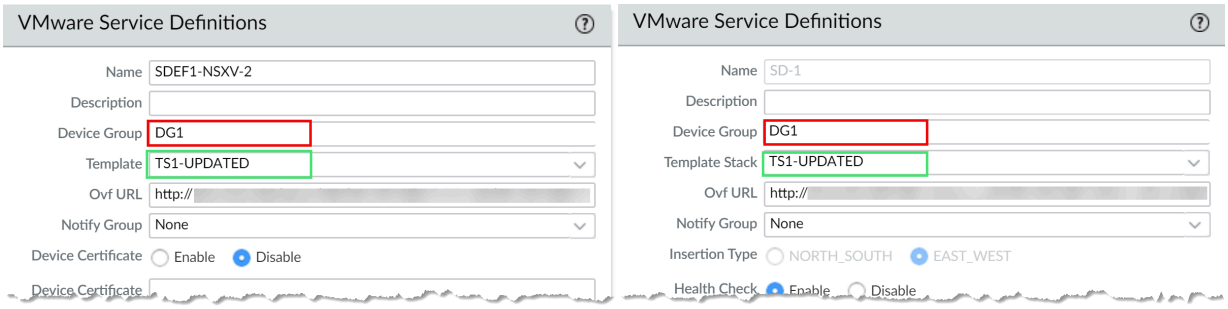
STEP 2 | 安裝 VMware NSX 專用 Panorama 外掛程式 3.2.0 或更新版本。升級之前，請參閱 VMware NSX 專用 Panorama 外掛程式 3.2.0 版本資訊。

STEP 3 | 啟用 NSX-T 管理員與 Panorama 之間的通訊.

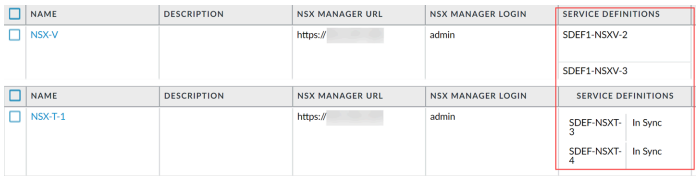
STEP 4 | 針對部署中的每個 NSX-V 服務定義，設定 NSX-T 服務定義。請勿建立新的裝置群組，改為使用現有的 NSX-V 裝置群組。使用現有裝置群組可讓您將 NSX-V 上使用的相同安全性政策規

©2023 Palo Alto Networks, Inc.

則，套用至 NSX-T 上部署的 VM-Series 防火牆。如果您的政策參考特定區域，請將 NSX-V 服務定義中相同的範本堆疊，新增至 NSX-T 服務定義。此外，如果裝置群組參考特定範本，請確定您選取的範本堆疊包含裝置群組中參考的範本。



STEP 5 | 設定 NSX-T 服務管理員，並將 NSX-T 服務定義與服務管理員建立關聯。



STEP 6 | 確認您的 NSX-T 設定出現在 NSX-T 管理員上。

1. 登入 NSX-T 管理員。
2. 選取 **System**（系統） > **Service Deployments**（服務部署） > **Catalog**（目錄）。
3. 確認列出您的 NSX-T 服務定義。
4. 選取 **Security**（安全性） > **Network Introspection**（網路自我檢查） > **Service Profiles**（服務設定檔）。
5. 確認列出與 NSX-T 範本相關聯的區域。

STEP 7 | 如果尚未在 NSX-T 管理員中新增計算管理員，請這麼做。確認註冊狀態和連線狀態為啟動之後，繼續如下。

STEP 8 | 將 NSX-V 設定匯入至 NSX-T。

©2023 Palo Alto Networks, Inc.

STEP 9 | 從 NSX-V 解除安裝服務實例。



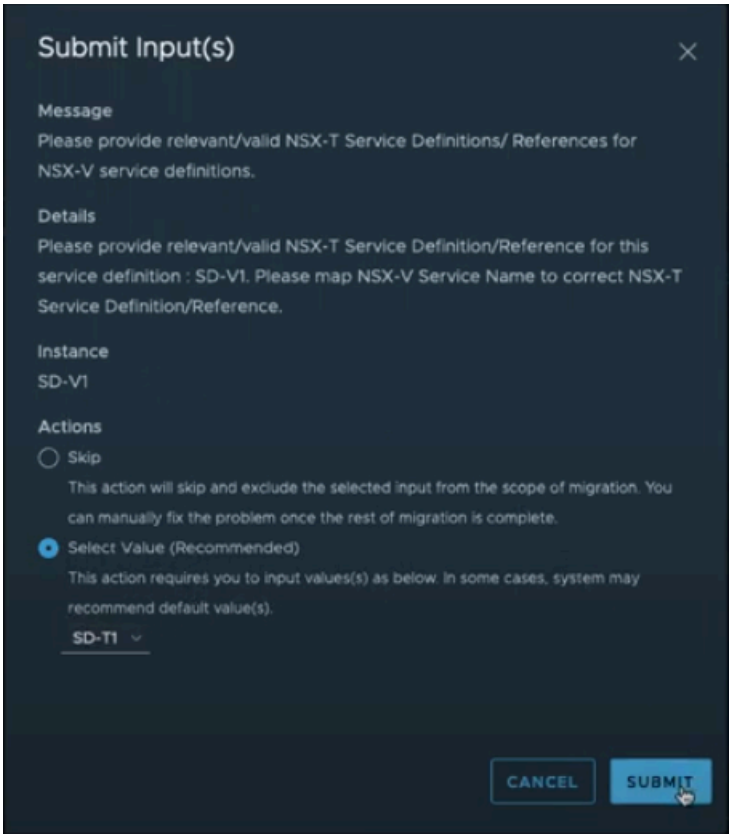
此步驟會導致流量中斷。

1. 登入 vSphere 用戶端。
2. 選取 **Installation and Upgrade**（安裝與升級） > **Service Deployment**（服務部署）。
3. 選取您的服務部署。
4. 按一下 **Delete**（刪除）。
5. 按一下 **Delete**（刪除）以確認。

©2023 Palo Alto Networks, Inc.

STEP 10 | 在 NSX-T 管理員上解決設定問題。解決設定問題時，您必須採取具體行動來移轉 VM-Series 防火牆設定。在大部分情況下，您可以接受 NSX-T 管理員提出的建議。

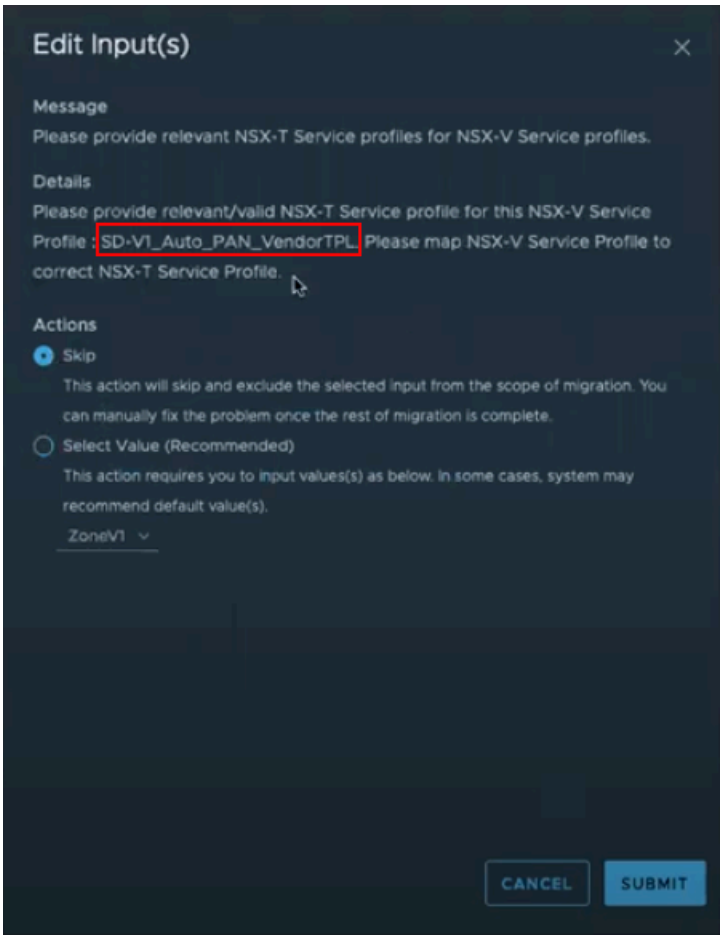
1. 解析服務插入設定時，請確認您選取先前在 NSX-T 的 VM-Series 專用 Panorama 上設定的正確服務定義。



2. 繼續解析剩餘設定。
3. 在移至 **Migrate Configuration**（移轉設定）之前，系統會要求您提供用於服務插入的傳輸區域。
4. 將 NSX-V 上的服務設定檔對應至 NSX-T 上相應的服務設定檔。

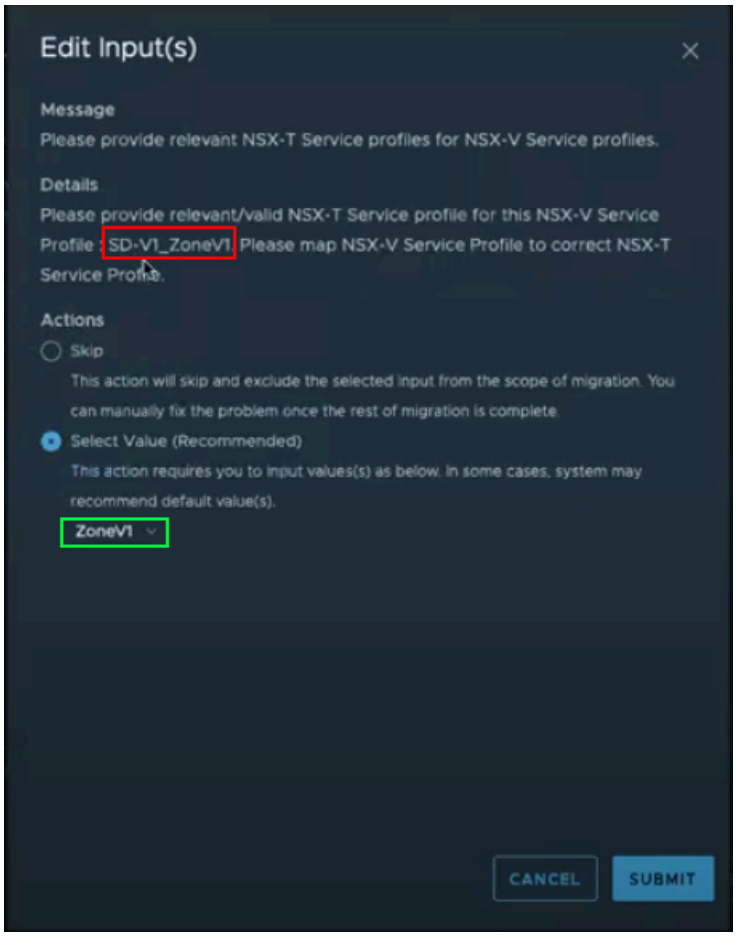
   1. 可以略過 Auto_PAN_VendorTPL。

©2023 Palo Alto Networks, Inc.



2. 將 NSX-T 服務設定檔對應至相應的 NSX-V 服務設定檔。

©2023 Palo Alto Networks, Inc.



STEP 11 | 移轉設定。

STEP 12 | 確認已成功移轉設定。

1. 選取 **Inventory**（詳細目錄） > **Groups**（群組），確認您的 IP 組和安全性群組存在。您可以按一下安全性群組名稱，檢查安全性群組中有正確的 IP 位址。
2. 選取 **Security**（安全性） > **Network Introspection Settings**（網路自我檢查設定） > **Service Segment**（服務區段），確認已建立服務區段。
3. 選取 **Security**（安全性） > **Network Introspection Settings**（網路自我檢查設定） > **Service Chains**（服務鏈），確認已建立服務鏈。按一下 [Forward Path（正向路徑）] 和 [Reverse Path（反向路徑）] 欄中的 [Profiles（設定檔）] 連結，以檢視您的服務設定檔。
4. 選取 **Security**（安全性） > **Network Introspection (E-W)**（網路自我檢查 **(E-W)**），確認已建立流量重新導向規則，可將流量導向至 VM-Series 防火牆的服務設定檔。

STEP 13 | 如適用，修改和移轉邊緣。

STEP 14 | 設定和移轉主機。

©2023 Palo Alto Networks, Inc.

STEP 15 | 將 NSX-T 標籤新增至現有的動態位址群組。

1. 選取 **Panorama** > **Objects**（物件） > **Address Groups**（位址群組）。
2. 按一下現有 NSX-V 動態位址群組的名稱。
3. 按一下 **Add Match Criteria**（新增比對規則），以顯示來自 NSX-V 和 NSX-T 的標籤。
4. 將 NSX-T 標籤新增至動態位址群組。如果您選擇不移除 NSX-V 標籤，請確保在標籤之間使用 **OR** 運算子。
5. 新增所有必要的標籤之後，按一下 **OK**（確定）。
6. **Commit**（提交）您的變更。

STEP 16 | 在 NSX-T（東西向）上啟動 VM-Series 防火牆.您不需要建立新的服務區段，而是選取移轉期間建立的服務區段。

©2023 Palo Alto Networks, Inc.

在 AWS 上設定 VM-Series 防火牆

可將 VM-Series 防火牆部署於公共 Amazon Web Services (AWS) 雲端及 AWS GovCloud。只要再經過妥善設定，就能為 EC2 實例上所部署的應用程式保護其存取作業，也能放置在 AWS 的 Virtual Private Cloud（虛擬私人雲端 - VPC）之中。

- 關於 AWS 上的 VM-Series 防火牆
- AWS 上支援的部署
- 在 AWS 上部署 VM-Series 防火牆
- VM-Series 與 AWS 閘道負載平衡器整合
- AWS 上 VM-Series 防火牆的高可用性
- 使用案例：保護 AWS 雲端中的 EC2 實例
- 使用案例：使用動態位址群組保護 VPC 中的新 EC2 實例
- 使用案例：將 VM-Series 防火牆作為 AWS 上的 GlobalProtect 閘道
- AWS 上的 VM 監控
- 使用 Amazon ELB 服務自動調整 VM-Series 防火牆規模
- 在 AWS VPC 上監控的屬性清單

關於 AWS 上的 VM-Series 防火牆

Amazon Web Service (AWS) 是公共雲端服務，可讓您在 Amazon 所管理的共用基礎結構上執行應用程式。這些應用程式可部署在可調式的運算容量上，或部署在不同 AWS 區域的 EC2 實例上，並由使用者透過網際網路存取。

為了達成網路一致性並能輕鬆管理 EC2 實例，Amazon 提供虛擬私人雲端服務 (VPC)。VPC 是 AWS 公共雲端的一部分，並獲指派私人網路空間中的 CIDR 區塊 (RFC 1918)。在 VPC 內，您可以視需要打造公共/私人子網路，並在這些子網路中將應用程式部署在 EC2 實例上。若要允許存取 VPC 內的應用程式，您可以在 EC2 實例上部署 VM-Series 防火牆。接著可設定 VM-Series 防火牆保護在 VPC 內的 EC2 實例進出的流量。

VM-Series 防火牆適用於公共 AWS 雲端及 AWS GovCloud。公共 AWS 和 AWS GovCloud 中的 VM-Series 防火牆支援自帶授權 (BYOL) 模式與即付即用 (PAYG) 小時付費模式（可從 AWS Marketplace 購買的依使用授權模式）。如需授權詳細資料，請參閱 公共雲端專用 VM-Series 防火牆授權。

- AWS EC2 實例類型
- AWS GovCloud 上的 VM-Series 防火牆
- AWS China 上的 VM-Series 防火牆
- AWS Outposts 上的 VM-Series 防火牆
- AWS 術語
- 搭配 Amazon ELB 使用的管理介面對應
- 調整 AWS 上的 VM-Series 防火牆效能

AWS EC2 實例類型

關於支援的實例類型，請參閱 EC2 實例上的 VM-Series 型號。

您可以在資源比最低 VM-Series 系統需求更多的 AWS 實例大小上部署 VM-Series 防火牆。如果您為 VM-Series 防火牆型號選取較大的實例大小，雖然防火牆只使用表格所示的最大 vCPU 核心數和記憶體，但卻可享受 AWS 提供的更快網路效能。如果您想要變更以 If BYOL 選項授權的 VM-Series 防火牆的實例類型，您必須先停用 VM 在切換實例類型，以確保授權的有效性。請參閱升級 VM-Series 型號以瞭解其原因。

如需在 AWS 上調整 VM-Series 防火牆規模的指導，請參閱本文章。

AWS GovCloud 上的 VM-Series 防火牆

AWS GovCloud 是一個隔離的 AWS 區域，符合美國政府機構及客戶的監管與合規要求。

為了保護工作負載（包含所有類別的受控未分類資訊 (CUI) 資料及 AWS GovCloud (US) 區域中政府導向的公開資料）的安全，VM-Series 防火牆在標準 AWS 公共雲端及 AWS GovCloud 上提供同樣穩健的安全性。AWS GovCloud 與標準 AWS 公共雲端上的 VM-Series 防火牆支援相同功能。

請參閱 AWS GovCloud 上的 AMI，在 AWS 上部署 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

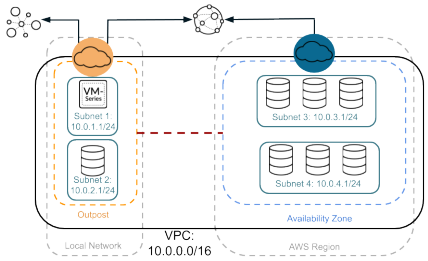
AWS China 上的 VM-Series 防火牆

AWS China Marketplace 提供具有 BYOL 選項的 VM-Series 防火牆，適用區域包括 AWS China（北京）和 AWS China（寧夏回族自治區）。您必須有不同於全球 AWS 帳戶的 AWS China 帳戶，才能在 AWS China 上存取此映像和使用 AWS 資源。

在 AWS 上啟動 VM-Series 防火牆之前，請務必檢閱 VM-Series 系統需求。

AWS Outposts 上的 VM-Series 防火牆

若要為內部部署的工作負載提供與 AWS 雲端的工作負載相同的安全性層級，您可以在內部部署位置的 AWS Outposts 機架上，安裝 AWS 上的 VM-Series 防火牆。使用您所在 AWS 地區的 AWS 市集 BYOL AMI，在 AWS Outposts 子網路中部署 VM-Series 防火牆實例。



請參閱註冊 VM-Series 防火牆（使用驗證碼），在 Palo Alto Networks 客戶支援網站建立支援帳戶並註冊 VM-Series 防火牆，以啟用 Palo Alto Networks 授與您的支援權利。

AWS 術語

本文件假設您熟悉 AWS VPC 上的網路和組態。為了提供本節中所使用詞彙的內容，我們在這裡簡述本文件參照的 AWS 詞彙（部分定義直接取自 AWS 詞彙表）：

詞彙	說明
EC2	彈性雲端運算 一種 Web 服務，可讓您啟動與管理 Amazon 資料中心中的 Linux/UNIX 與 Windows 伺服器實例。
AMI	Amazon 機器映像 AMI 提供啟動實例（亦即雲端中的虛擬伺服器）所需的資訊。 VM-Series AMI 是加密的機器映像，其中包含執行個體化 EC2 實例上 VM-Series 防火牆所需的作業系統。
ELB	彈性負載平衡 ELB 是一項 Amazon Web 服務，透過在多個彈性雲端運算 (EC2) 實例中路由流量，可幫助改善應用程式的可用性與擴充性。ELB 偵錯不健康的 EC2 實例並將流量重新路由至健康的實例，直至不健康的實例被還原。ELB 只能將流量傳送至下一個躍點負載平衡 EC2 實例的主要介

©2023 Palo Alto Networks, Inc.

詞彙	說明
	面。因此，若要將 ELB 與 AWS 上的 VM-Series 防火牆搭配使用，防火牆必須能夠將主要介面用於資料平面流量。
ENI	彈性網路介面 可附加至 EC2 實例的額外網路介面。ENI 中包含主要私人 IP 位址、一或多個次要私人 IP 位址、公共 IP 位址、彈性 IP 位址（選用）、MAC 位址、所指定安全性群組中指定的成員資格、說明，以及來源/目的地檢查旗標。
EC2 實例的 IP 位址類型	EC2 實例可以有不同類型的 IP 位址。 · 公共 IP 位址：可在網際網路上路由的 IP 位址。 · 私人 IP 位址：私人 IP 位址範圍內依照 RFC 1918 中定義的 IP 位址。您可以為啟動 EC2 執行個體的子網路選擇手動指派 IP 位址，或在 CIDR 區塊範圍內自動指派 IP 位址。 如果您要手動指派 IP 位址，Amazon 會保留每個子網路中的前四 (4) 個 IP 位址和最後一 (1) 個 IP 位址，以供 IP 網路使用。 · 彈性 IP 位址 (EIP)：一種靜態 IP 位址，您已在 Amazon EC2 或 Amazon VPC 中配置然後連接至實例的位址。彈性 IP 位址與您的帳戶有關，與特定的實例無關。其之所以彈性，是因為您可以視需求的變更，輕鬆地配置、連接、卸除及釋放這些位址。 公用子網路中的執行個體可以擁有私人 IP 位址、公用 IP 位址和彈性 IP 位址 (EIP)；私人子網路中的執行個體將擁有私人 IP 位址，並選擇性地擁有 EIP。
實例類型	Amazon 定義的規格，其中明訂實例的記憶體、CPU、儲存容量及每小時成本。有一部分的實例類型是針對標準應用程式所設計的，其他的則是針對 CPU 密集型、記憶體密集型等應用程式所設計。
VPC	Virtual Private Cloud（虛擬私人雲端） 一種彈性的網路，其中植入的基礎結構、平台及應用程式服務共用共同的安全性與互相連線。
IGW	Amazon 提供的網際網路閘道。 將網路連線至網際網路。您可以將 VPC 之外 IP 位址的流量路由至網際網路閘道。
IAM 角色	身分及存取管理 對 AWS 上的 VM-Series 防火牆啟用高可用性時需要。在擔任角色後，IAM 角色定義應用程式可使用的 API 動作及資源。在故障復原時，IAM 角色可讓 VM-Series 防火牆安全發出 API 請求，將資料背板介面從主動端點切換至被動端點。

©2023 Palo Alto Networks, Inc.

詞彙	說明
	VM 監控也需要 IAM 角色。請參閱在 AWS VPC 上監控的屬性清單。
子網路	可附加 EC2 實例之 VPC 的 IP 位址範圍區段。EC2 實例可根據您的安全性與作業需求分組成數個子網路。 子網路有兩種類型： · 私人子網路：無法從網際網路存取此子網路中的 EC2 實例。 · 公共子網路：網際網路閘道會連接至公共子網路，且從網際網路可存取此子網路中的 EC2 實例。
安全性群組	安全性群組會連接至 ENI，並指定系統允許在網際網路上建立輸入/輸出連線的通訊協定、連接埠及 IP 位址範圍清單。 在 ***AWS VPC*** 中，安全性群組與網路 ***ACL*** 會控制輸入與輸出流量；安全性群組會規範 ***EC2*** 實例的存取，而網路 ***ACL*** 則範範子網路的存取。由於您正在部署的是 ***VM-Series*** 防火牆，因此請在安全性群組與網路 ***ACL*** 中設定更多的權限規則，並允許防火牆安全地啟用 ***VPC*** 中的應用程式。
路由表	一組路由規則，可控制離開任何與路由表關聯之子網路的流量。一個子網路只能與一個路由表相關聯。
金鑰配對	一組安全性認證，用來以電子方式證實您的身分。金鑰配對包含私人金鑰與公共金鑰。啟動 VM-Series 防火牆時，您必須為 VM-Series 防火牆產生金鑰配對或選取現有的金鑰配對。必須有私人金鑰才能存取維護模式中的防火牆。
CloudWatch	Amazon CloudWatch 是可讓您針對 AWS 上的 VM-Series 防火牆來收集和追蹤度量的監控服務。啟用時，防火牆會使用 AWS API 將原生 PAN-OS 度量發佈至 CloudWatch。

搭配 Amazon ELB 使用的管理介面對應

依預設，彈性網路介面 (ENI) eth0 對應至防火牆上的 MGT 介面，ENI eth1 則對應至防火牆上的乙太網路 1/1。由於 ELB 只能將流量傳送至下一個躍點負載平衡 EC2 實例的主要介面，VM-Series 防火牆必須能夠將主要介面用於資料平面流量。

在下列情境中，其中 VM-Series 防火牆位於 Amazon ELB 之後，防火牆可以在主要介面上接收資料平面流量（如需拓撲圖，請參閱使用 Amazon ELB 服務自動調整 VM-Series 防火牆規模）：

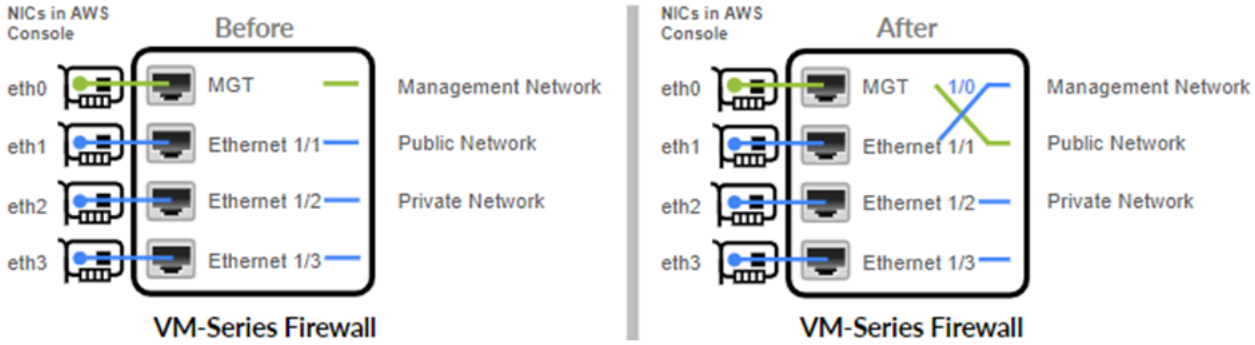
· VM-Series 防火牆對直接輸出至網際網路的流量提供保護，而無需使用 VPN 連結或 Direct Connect 連結返回公司網路。

©2023 Palo Alto Networks, Inc.

- 每個防火牆只有一個後端伺服器時，例如 Web 伺服器，VM-Series 防火牆會對網際網路型應用程式提供保護。VM-Series 防火牆及 Web 伺服器可線性擴充、成對，以及部署在 ELB 之後。

  目前，若要在需要 *ELB* 分層式部署的使用案例中擴充防火牆及應用程式層 *EC2* 實例，交換管理介面會阻止您無縫部署 *ELB* 解決方案。交換管理介面只能部分解決 *ELB* 的整合問題。

為使防火牆傳送及接收 eth0 而非 eth1 上的資料流量，您必須在防火牆內交換 ENI 的對應，如此一來，ENI eth0 將對應至乙太網路 1/1，ENI eth1 將對應至防火牆上的 MGT 介面，如下所示。



若可行，請交換管理介面，然後再設定防火牆或定義原則規則。

交換介面的對應方式可讓 ELB 將流量散佈及路由至 VM-Series 防火牆（位於 AWS 上的相同或不同可用性區域）上的健康實例，以增加容量及提升容錯能力。

只有 VM-Series 防火牆受 Amazon ELB 服務保護時，才需要介面交換。如果您的需求是在設定的傳統高可用性中部署 VM-Series 防火牆，則不需要設定本節所述的介面交換。繼續AWS 上 VM-Series 防火牆的高可用性。

若要交換介面，可執行下列選項：

- 啟動時 — 啟動防火牆時，您可輸入 **mgmt-interface-swap=enable** 命令（AWS 管理主控台上的 **User data**（使用者資料）欄位，請參閱在 AWS 上啟動 VM-Series 防火牆）或 CLI，或者您可以在啟動程序組態中包含新的 **mgmt-interface-swap** 操作命令。
- 啟動之後 — 啟動防火牆之後，在防火牆上使用 VM-Series 防火牆 CLI 來交換管理介面（**set system setting mgmt-interface-swap enable yes** 操作命令）。

  - 為了防止防火牆上發生非預期的行為，請選取一種方法一致地指定介面交換設定（在啟動載入設定中、在防火牆上從 *CLI*，或使用 *AWS* 主控台上的 *Amazon EC2 User data*（使用者資料）欄位）。
  - 確保您可以存取 *AWS* 主控台（管理主控台或 *CLI*）以檢視 *eth1* 介面的 *IP* 位址。此外，確認 *AWS* 安全性群組規則允許連線（*HTTPS* 及 *SSH*）至新的管理介面。
  - 如果您在介面交換前已設定防火牆或已定義的原則規則，請檢查 *eth0* 或 *eth1* 的任何 *IP* 位址變更是否會影響原則規則。

©2023 Palo Alto Networks, Inc.

調整 AWS 上的 VM-Series 防火牆效能

以下設定會影響效能：

- PAN-OS 版本 9.0.3 和更早版本支援 AWS C5 和 M5 實例類型，這些實例類型預設有彈性網路轉接器支援 SR-IOV 模式。如需詳細資訊，請參閱彈性網路轉接器 – Amazon EC2 的高效能網路介面。
- PAN-OS 版本 9.0.4 和更新版本預設為 C5 和 M5 實例類型提供 DPDK 支援。防火牆在 DPDK 模式中會使用 DPDK 驅動程式。有關支援的驅動程式清單，請參閱 VM-Series 防火牆上的 PacketMMAP 和 PDK 驅動程式，以及官方 DPDK 版本資訊。
- 若要享有 IETF RFC 8926 (Geneve) 封裝和改進的輸送量，請升級到 PAN-OS 10.0.2 或更新版本，並參考 VM-Series 與 AWS Gateway Load Balancer 整合。

使用 VM-Series CLI 來檢視 DPDK 設定或啟用包裝 I/O。

檢視防火牆上的 DPDK 設定

STEP 1 | 登入 VM-Series 防火牆 CLI。

STEP 2 | 檢視 DPDK 設定。如果 DPDK 已啟用，則輸出如下：

```
> show system setting dpdk-pkt-io on
```

```
裝置目前的資料包 IO 模式：DPDK 裝置 DPDK 封包 IO 功能：是 裝置預設封包 IO 模式：DPDK
```

啟用 DPDK 包裝 I/O

STEP 1 | 登入 VM-Series 防火牆 CLI

STEP 2 | 啟用 DPDK：

```
> set system setting dpdk-pkt-io on
```

STEP 3 | 重新啟動裝置。

在防火牆上，選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後選取 **Reboot Device**（重新啟動裝置）。

©2023 Palo Alto Networks, Inc.

AWS 上支援的部署

VM-Series 防火牆會保護進出 AWS 虛擬私人雲端 (VPC) 內 EC2 實例的輸入與輸出流量。由於 AWS VPC 僅支援 IP 網路（Layer 3 網路功能），所以只能使用 Layer 3 介面部署 VM-Series 防火牆。

- 部署 VM-Series 防火牆以保護在 AWS 虛擬私人雲端中代管的 EC2 實例。

  如果您在 AWS 雲端中代管您的應用程式，則部署 VM-Series 防火牆可為透過網際網路存取這些應用程式的使用者保護並安全地啟用這些應用程式。例如，下圖顯示的 VM-Series 防火牆部署在網際網路閘道所連接的邊緣子網路中。應用程式部署在無法直接存取網際網路的私人子網路中。

  當使用者必須存取私人子網路中的應用程式時，則在驗證安全性原則並執行目的地 NAT 後防火牆會收到要求，並將要求導向至適當的應用程式。在傳回路徑上，防火牆會收到流量、套用安全性原則，並使用來源 NAT 將內容傳遞給使用者。請參閱使用案例：保護 AWS 雲端中的 EC2 實例。

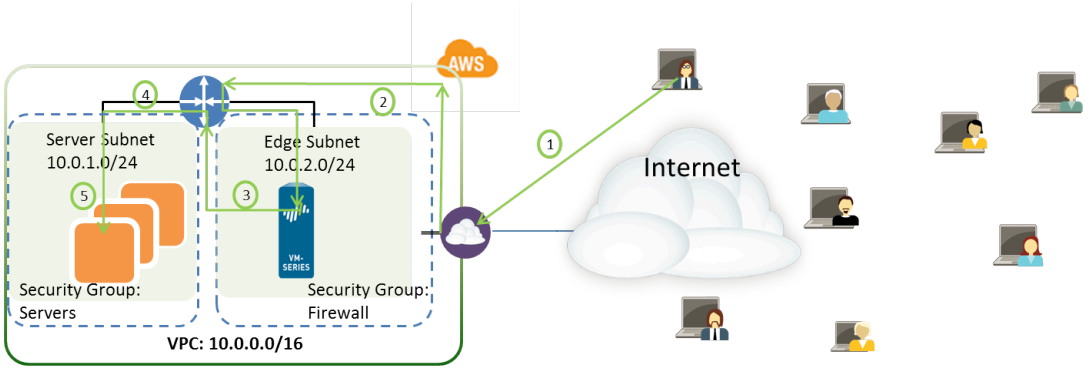


圖 **1:** 適用於 **EC2** 實例的 **VM-Series**

- 針對在 AWS 虛擬私人雲端內的公司網路與 EC2 實例之間的 VPN 存取部署 VM-Series 防火牆。

  若要將公司網路與 AWS 雲端中部署的應用程式連線，您可以將防火牆設為 IPSec VPN 通道的終止點。此 VPN 通道允許網路上的使用者安全地存取雲端中的應用程式。

  如需集中管理功能，請在整個網路之間一致地強制實行原則，如需集中日誌記錄與報告，您也可以在公司網路中部署 Panorama。如果您必須設定透過 VPN 存取多個 VPC，則使用 Panorama 可讓您輕鬆地按區域將防火牆分組並管理這些防火牆。

©2023 Palo Alto Networks, Inc.

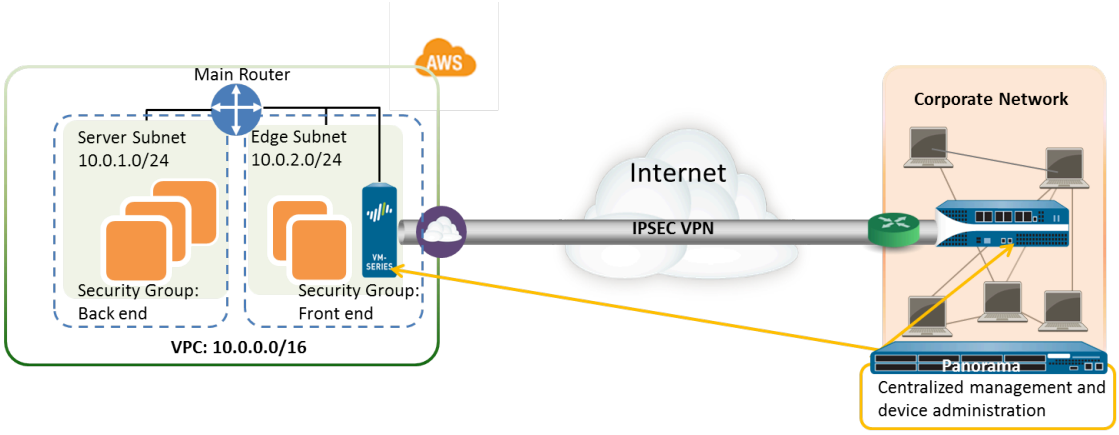


圖 **2:** 適用於 **VPN** 存取的 **VM-Series**

- 將 VM-Series 防火牆部署為 GlobalProtect 閘道，可使用筆記型電腦保護遠端使用者的存取。筆記型電腦上的 GlobalProtect 代理程式會連線至閘道，然後根據要求而定，閘道會設定 VPN 連線至公司網路，或將要求連線至網際網路。若要為行動設備上的使用者強制實行安全性相容性（使用 GlobalProtect 應用程式），則 GlobalProtect 閘道會結合 GlobalProtect Mobile Security Manager 一起使用。GlobalProtect Mobile Security Manager 可確保會使用搭配公司應用程式與網路使用的設備設定與帳戶資訊來管理與設定行動設備。

  在上述各使用案例中，您可以在主動/被動高可用性 *(HA)* 配對中部署 *VM-Series* 防火牆。如需在 *HA* 中設定 *VM-Series* 防火牆的資訊，請參閱使用案例：使用動態位址群組保護 VPC 中的新 EC2 實例。

- 使用 Amazon 彈性負載平衡 (ELB) 服務部署 VM-Series ，從而在下列情境中，VM-Series 防火牆部署在 Amazon ELB 之後，防火牆可以接收主要介面上的資料平面流量：
  - VM-Series 防火牆對直接輸出至網際網路的流量提供保護，而無需使用 VPN 連結或 Direct Connect 連結返回公司網路。
  - 每個防火牆只有一個後端伺服器時，例如 Web 伺服器，VM-Series 防火牆會對網際網路型應用程式提供保護。VM-Series 防火牆及 Web 伺服器可線性擴充、成對，以及部署在 ELB 之後。

  如果您要使用 Amazon ELB 服務自動調整 VM-Series 防火牆規模，則請使用 GitHub 儲存庫中提供的 CloudFormation 範本，以 ELB 分層式拓撲來部署 VM-Series，此拓撲具有網際網路連結傳統 ELB，還有內部傳統負載平衡器或內部應用程式負載平衡器（內部 ELB）。

©2023 Palo Alto Networks, Inc.

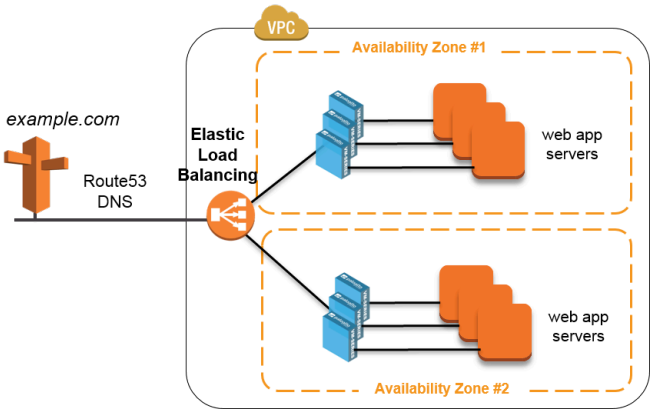


圖 **3:** 配備 **ELB** 的 **VM-Series**

防火牆部署在 *ELB* 之前時，您無法設定防火牆來傳送及接收 *eth0* 上的資料平面流量。*VM-Series* 防火牆必須部署在 *Amazon ELB* 之後。

您可以使用 VM-Series 防火牆 CLI 來交換管理介面，或在啟動時啟用它。如需詳細資訊，請參閱搭配 Amazon ELB 使用的管理介面對應。

如果您要部署負載平衡器分層式拓撲，請參閱使用 Amazon ELB 服務自動調整 VM-Series 防火牆規模。

除了 *Palo Alto Networks* 官方支援政策所涵蓋的上述連結之外，*Palo Alto Networks* 還會在 Palo Alto Networks GitHub 儲存庫中提供社群支援的範本，讓您能夠開始探索 *AWS* 上的雲端自動化和調整規模之旅中可用的解決方案。請參閱 AWS Transit VPC 以瞭解中樞和訂閱 *VPC* 部署，而此部署可讓您保護 *VPC* 之間以及 *VPC* 與內部部署/混合式雲端資源之間的流量，並保護流向網際網路的輸出流量。

©2023 Palo Alto Networks, Inc.

在 AWS 上部署 VM-Series 防火牆

- 取得 AMI
- 為 AWS VPC 中的 VM-Series 規劃工作表
- 在 AWS 上啟動 VM-Series 防火牆
- 在 AWS Outposts 上啟動 VM-Series 防火牆
- 建立自訂 Amazon 機器映像 (AMI)
- 在 AWS 上加密 VM-Series 防火牆的 EBS 磁碟區
- 使用 VM-Series 防火牆 CLI 來交換管理介面
- 在 VM-Series 防火牆上啟用 CloudWatch 監控

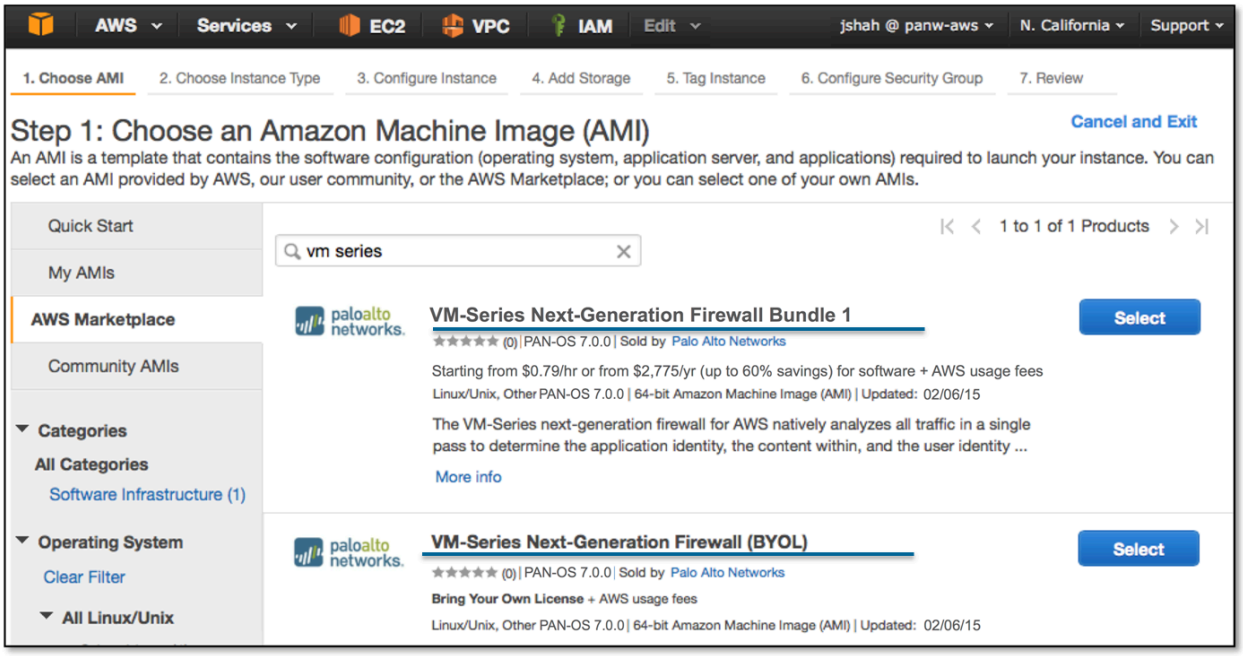
取得 AMI

從相應的 Marketplace 取得公共 AWS 雲端和 AWS GovCloud 的 Amazon 機器映像。

- 公共 AWS 雲端中的 AMI
- AWS GovCloud 上的 AMI
- 取得 VM-Series 防火牆 Amazon 機器映像 (AMI) ID

公共 AWS 雲端中的 AMI

在 AWS Marketplace 中，VM-Series 防火牆的 AMI 支援 Bring Your Own License（自帶授權 - BYOL）及依使用授權定價選項。



若要使用 BYOL 選項購買授權，請聯絡您的 Palo Alto Networks 銷售工程師或零售商。

©2023 Palo Alto Networks, Inc.

AWS GovCloud 上的 AMI

自帶授權 (BYOL) 模式與依使用授權版 VM-Series 防火牆可從 AWS GovCloud Marketplace 獲取。

使用 GovCloud 帳戶，您可在 Marketplace 搜尋 Palo Alto Networks 並尋找 VM-Series 防火牆的 AMI。確定先檢閱支援的 EC2 實例類型，再啟動防火牆。如需詳細資訊，請參閱在 AWS 上啟動 VM-Series 防火牆。

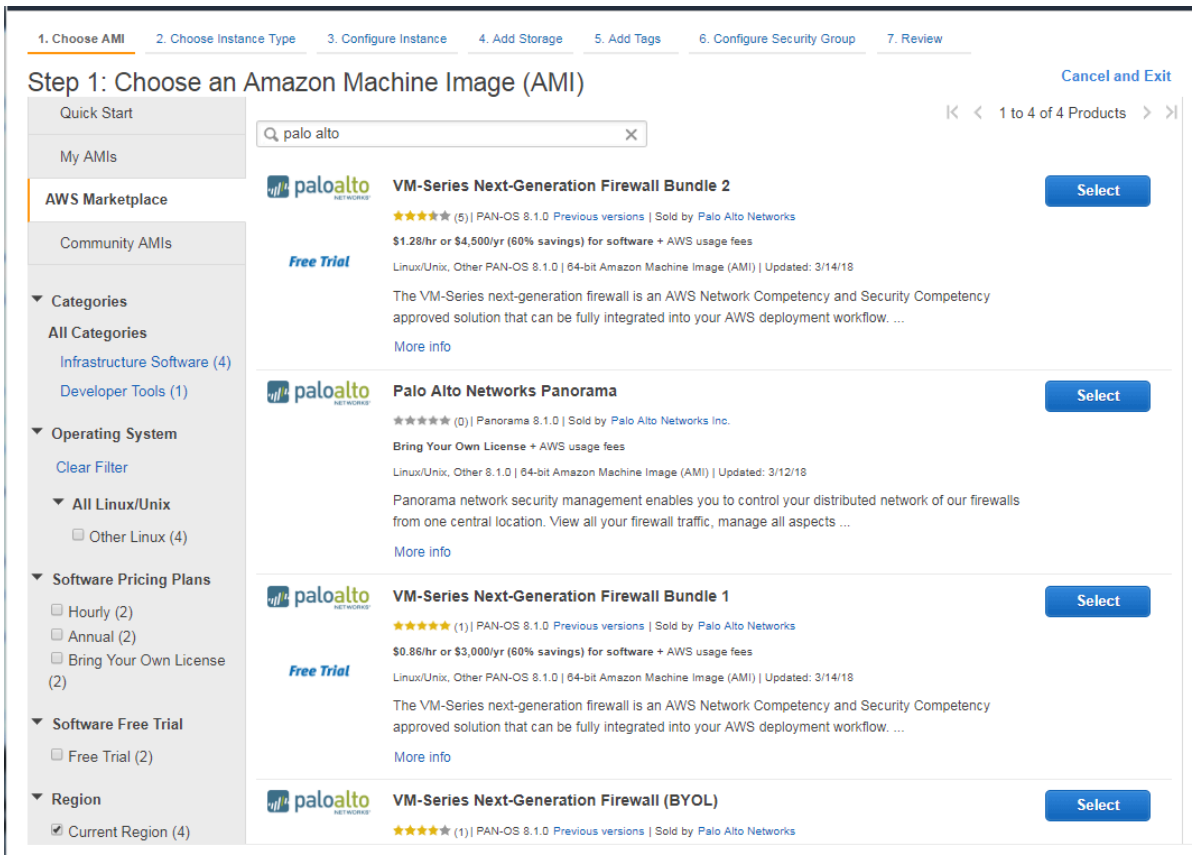


表 **1:** 檢閱 **AWS** 上 **VM-Series** 的系統需求與限制

需求	詳細資訊
EC2 實例類型	您選取的 EC2 實例類型，必須符合 VM-Series 防火牆型號的 VM-Series 系統需求。如果您在不符合這些需求的 EC2 實例類型上部署 VM-Series 防火牆，則防火牆會以維護模式啟動。 為了在 *AWS* 上支援 *VM* 監控及高可用性，*VM-Series* 防火牆必須能夠直接連線 *AWS API* 服務端點，而無需在防火牆管理介面與 *AWS API* 端點之間設置任何 *Proxy* 伺服器（例如 *ec2.us-west-2.amazonaws.com*）。

©2023 Palo Alto Networks, Inc.

需求	詳細資訊
Amazon 彈性區塊儲存區 (EBS)	VM-Series 防火牆必須使用 Amazon 彈性區塊儲存區 (EBS) 磁碟區進行儲存。EBS 最佳化提供最佳化的組態堆疊，及 Amazon EBS I/O 額外的專用功能。
網路	由於 AWS 僅支援 Layer 3 網路功能，所以只能使用 Layer 3 介面部署 VM-Series 防火牆。在 AWS VPC 中部署的 VM-Series 防火牆上不支援 Layer 2 介面、Virtual Wire、VLAN 及子介面。
介面	總共支援八個介面—一個管理介面，以及最多七個用於資料流量的彈性網路介面 (ENI)。VM-Series 防火牆不支援熱連接 ENI；若要偵測是否新增或移除 ENI，您必須重新啟動防火牆。 您選取的 ***EC2*** 實例類型可決定您可啟用的 ***ENI*** 總數。例如，*c3.8xlarge* 支援八 *(8)* 個 ***ENI***。
支援權利與授權	若為自帶授權模式，必須有支援帳戶與有效的 VM-Series 授權，才能取得 Amazon 機器映像 (AMI) 檔，需要有此映像檔才能在 AWS VPC 中安裝 VM-Series 防火牆。VM-Series 防火牆需要的授權—容量授權、支援授權，以及資安威脅、URL 過濾、WildFire 等的使用授權—必須向 Palo Alto Networks 購買。若要為您的授權購買部署，請與您的業務代表聯絡。請參閱公共雲端專用 VM-Series 防火牆授權。 對於依使用授權版機型，可購買每小時或每年度計價搭售包並在 AWS 上直接扣帳。然而，您必須在 Palo Alto Networks 註冊支援權利。如需詳細資訊，請參閱註冊依使用授權版公共雲端專用 VM-Series 防火牆（無驗證碼）。

取得 VM-Series 防火牆 Amazon 機器映像 (AMI) ID

使用下列指示來尋找 VM-Series 防火牆的 AMI ID，而 VM-Series 防火牆符合您要在其中啟動 VM-Series 防火牆的 PAN-OS 版本、授權類型和 AWS 區域。

STEP 1 | 在用來擷取 AMI ID 的用戶端上安裝 AWS CLI，並使用 AWS 認證登入。

如需安裝 CLI 的指示，請參閱 AWS 文件。

©2023 Palo Alto Networks, Inc.

STEP 2 | 使用下列 CLI 命令來尋找 AMI-ID。

```
aws ec2 describe-images --filters "Name=product-
code,Values=<license-type-value>" Name=name,Values=PA-VM-AWS*<PAN-
OS-version>*  --region <region> --output json
```

您需要以相關資訊取代角括號 <> 中的值，如下所示：

- 使用每種授權類型的 VM-Series 產品代碼。值為：
  - 搭售包 1—

    ```
    e9yfvyj3uag5uo5j2hjikv74n
    ```

  - Bundle 2—

    ```
    hd44w1chf26uv4p52cdynb2o
    ```

  - BYOL—

    ```
    6njl1pau431dv1qxipg63mvah
    ```

- 使用 PAN-OS 版本— 10.0。如果 PAN-OS 版本內有多個功能版本，則會列出所有 AMI-ID。例如，在 9.0.x 中，您將檢視 9.0、9.0.3.xfr、9.0.5.xfr 和 9.0.6 版的 AMI ID 清單，而且可以使用所需 PAN-OS 版本的 AMI-ID。
- 從下列位置取得 AWS 區域詳細資料：https://docs.aws.amazon.com/general/latest/gr/rande.html.

例如：若要找到美國加州地區的 PAN-OS 10.0.0 專用 VM-Series 搭售包 1 的 AMI-ID，CLI 命令為：

```
 aws ec2 describe-images --filters "Name=product-
code,Values=e9yfvyj3uag5uo5j2hjikv74n" "Name=name,Values=PA-VM-
AWS*10.0*"  --region us-west-1 --output json
```

輸出為：

```
 { "產品代碼": [ { "產品代碼 ID": "e9yfvyj3uag5uo5j2hjikv74n", "產
品代碼類型": "marketplace" } ], "虛擬化類型": "hvm", "Hypervisor":
 "xen", "映像擁有者別名": "aws-marketplace", "Ena 支援": true,
 "SriovNet 支援": "簡易", "映像 ID": "ami-06f7a63d7481d0ded", "狀
態": "可用", "區塊裝置對應": [ { "裝置名稱": "/dev/xvda", "Ebs": { "快
照 ID": "snap-0009036179b39824b", "終止時刪除": false, "磁碟區類型":
 "gp2", "磁碟區大小":60, "加密": false } } ], "架構": "x86_64", "映
像位置": "aws-marketplace/PA-VM-AWS-10.0.0-f1260463-68e1-4bfb-
bf2e-075c2664c1d7-ami-06f7a63d7481d0ded.1", "根裝置類型": "ebs",
 "擁有者 ID":"679593333241", "根裝置名稱": "/dev/xvda", "建立日
期":"2020-07-20T12:45:22.000Z", "公用": true, "映像類型": "機器",
```


©2023 Palo Alto Networks, Inc.

```
 "名稱":"PA-VM-AWS-10.0.0-f1260463-68e1-4bfb-bf2e-075c2664c1d7-
ami-06f7a63d7481d0ded.1" }
```

您也可以輸出為表格格式。例如，若要查看 PAN-OS 10.0.2 的 BYOL 映像的 AMI：

```
aws ec2 describe-images --filters "Name=product-
code,Values=6njl1pau431dv1qxipg63mvah" "Name=name,Values=PA-VM-
AWS*10.0.2*" --region us-west-1 --output table --query "Images[*].
{Name:Name,AMI:ImageId,State:State}"
```

```
----------------------------------------------------
 ----------------------------------------------------
 ----------------------|描述圖片 |+-----------------------
+-------------------------
 ------------------------------------------------------ --------
+-------------+| AMI | 名稱 |狀態 |+-----------------------
+------------ ------------------------------------------------------
 --------+-------------+| ami-037b90bd9b630f594| PA-
VM-AWS-10.0.2-7064e142-2859-40a4-ab62-8b0996b842e9-
ami-07a0e94019f2a2001.4 | 可用 |+-----------------------
+-------------------------
 ------------------------------------------------------ --------
+-------------+
```

為 AWS VPC 中的 VM-Series 規劃工作表

為了輕鬆部署，請在您要在每個子網路內部署的 VPC 與 EC2 實例內規劃子網路。開始之前，請使用下表來對照在 VPC 中將 VM-Series 防火牆部署與插入到流量流向中時所需的網路資訊：

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

設定項目	值
VPC CIDR	
安全性群組	
子網路（公共）CIDR	
子網路（私人）CIDR	
子網路（公共）路由表	
子網路（私人）路由表	
安全性群組 · 防火牆的管理存取規則 (eth0/0)	

©2023 Palo Alto Networks, Inc.

設定項目	值
· 防火牆資料面板介面的存取規則 · 指派給應用程式伺服器的介面存取規則。	
ELB 之後的 VM-Series 防火牆	
EC2 實例 1（VM-Series 防火牆） 只有連接至公開子網路的資料面板介面需要 ***EIP***。	子網路： 實例類型： 管理介面 IP： 管理介面 EIP： 資料背板介面 eth1/1 · 私人 IP： · EIP（視需要）： · 安全性群組： 資料背板介面 eth1/2 · 私人 IP： · EIP（視需要）： · 安全性群組：
EC2 實例 2（要保護的應用程式） 為正要部署的額外應用程式重複這幾組的值。	子網路： 實例類型： 管理介面 IP： 預設閘道： 資料背板介面 1 · 私人 IP：
高可用性 **(HA)** 需求	如果您在高可用性（主動/被動）組態中部署 VM-Series 防火牆，必須確保執行下列步驟： · 部署實例時，建立 IAM 角色並將角色指派給 VM-Series 防火牆。請參閱HA 的 IAM 角色。 · 在同一 AWS 可用性區域部署 HA 端點。 · HA 配對中的主動防火牆必須最少擁有三個 ENI：兩個資料背板介面與一個管理介面。 HA 配對中的主動防火牆必須擁有一個 ENI 用於管理，以及一個 ENI 用作資料背板介面；您將資料背板設定為 HA2 介面。

©2023 Palo Alto Networks, Inc.

設定項目	值
	請勿將額外的資料背板附加至 *HA* 配對中的被動防火牆。在故障復原時，先前主動防火牆的資料平面介面將移至（卸除，然後連接）現在的主動防火牆（之前的被動防火牆）。

在 AWS 上啟動 VM-Series 防火牆

如果尚未在您的支援帳戶中註冊您在訂購完成電子郵件中收到的容量授權碼，請參閱註冊 VM-Series 防火牆。註冊之後，請使用 Marketplace 中所發佈的 AMI 或如下在 AWS VPC 中建立自訂 Amazon 機器映像 (AMI)，以部署 VM-Series 防火牆：

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 存取 AWS 主控台。

登入 AWS 主控台，並選取 [EC2 Dashboard（EC2 儀表板）]。

STEP 2 | 針對您的網路需求設定 VPC。

無論您是在現有的 VPC 中啟動 VM-Series 防火牆，還是建立新的 VPC，VM-Series 防火牆都必須能夠從 EC2 實例接收流量，也必須能在 VPC 與網際網路之間執行輸入與輸出通訊。

如需建立 VPC 並設定以進行存取的指示，請參閱 AWS VPC 文件。

如需完整工作流程的範例，請參閱使用案例：保護 AWS 雲端中的 EC2 實例。

1. 建立新的 VPC 或使用現有的 VPC。請參閱 AWS 入門指南文件。
2. 確認網路與安全性元件已適當定義。
   - 啟用網際網路通訊。預設的 VPC 包含網際網路閘道，如果您在預設的子網路中安裝 VM-Series 防火牆，則該防火牆可存取網際網路。
   - 建立子網路。子網路是指派給 VPC 的 IP 位址範圍區段，您可以在該 VPC 中啟動 EC2 實例。VM-Series 防火牆必須屬於公共子網路，才能設定該防火牆存取網際網路。
   - 視需要建立安全性群組，以管理 EC2 實例/子網路的輸入與輸出流量。
   - 為私人子網路的路由表新增路由，以確定流量可在 VPC 中整個子網路與安全性群組之間路由（若適當的話）。
3. 如果您要在 HA 中部署一對 VM-Series 防火牆，您必須先定義 HA 的 IAM 角色才能在 AWS 上設定主動/被動 HA。
4. （選用）如果您使用啟動程序來執行 VM-Series 防火牆的組態，請參閱在 AWS 中啟動 VM-Series 防火牆。如需有關啟動載入的詳細資訊，請參閱啟動 VM-Series 防火牆和選擇啟動方法。

©2023 Palo Alto Networks, Inc.

STEP 3 | 啟動 VM-Series 防火牆。

雖然啟動時可將額外網路介面 *(ENI)* 新增至 *VM-Series* 防火牆，重新啟動防火牆時，*AWS* 將對管理介面釋放自動指派的公共 *IP* 位址。因此，為了確保管理介面的連接性，您必須先對管理介面指派彈性 *IP* 位址，在將額外介面連接至防火牆。

如果您想要保留 EIP 位址，可將一個 EIP 位址指派給 eth 1/1 介面，並將此介面用於管理流量與資料流量。若要限制介面上允許的服務或限制可登入 eth 1/1 介面的 IP 位址，請將管理設定檔附加至介面。

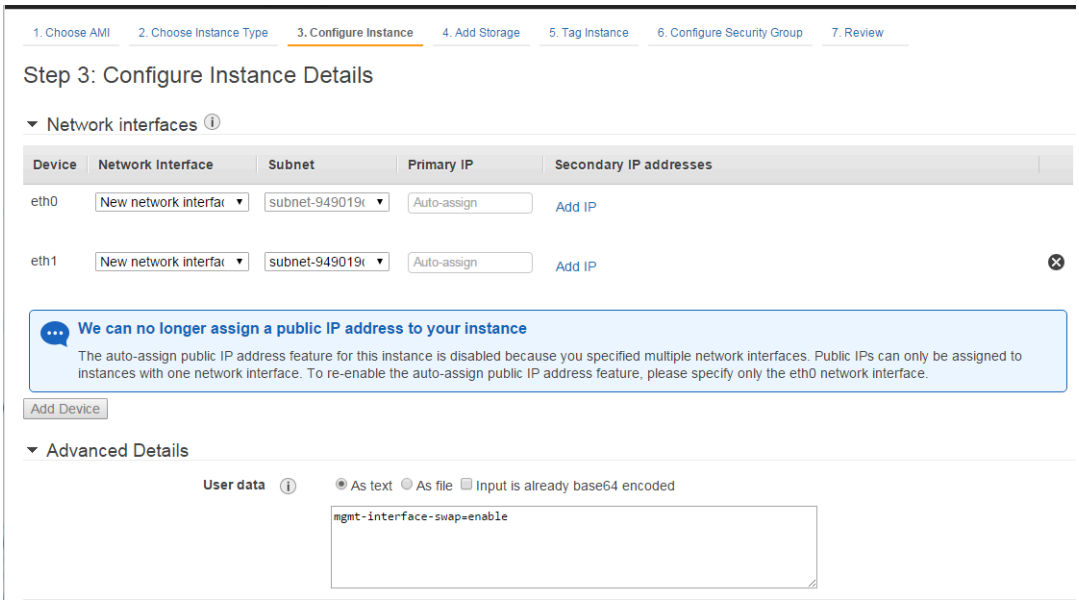
1. 在 EC2 儀表板中，按一下 **Launch Instance**（啟動實例）。
2. 選取 VM-Series AMI。若要取得 AMI，請參閱取得 AMI。
3. 在 EC2 實例上啟動 VM-Series 防火牆。
   1. 選取 **EC2 instance type**（**EC2** 實例類型），以配置防火牆所需的資源，然後按 **Next**（下一步）。有關資源需求，請參閱 VM-Series 系統需求。
   2. 選取 VPC。
   3. 選取 VM-Series 管理介面將連接到哪一個公共子網路。
   4. 選取 **Automatically assign a public IP address**（自動指派公共 **IP** 位址）。這可讓您為 VM-Series 防火牆的管理介面取得可公開存取的 IP 位址。

      您稍後可將彈性 IP 位址連接到管理介面；不同於公共 IP 位址在實例終止時會與防火牆中斷關聯，彈性 IP 位址提供持續性，並會重新連接至 VM-Series 防火牆的新（或替代）實例，且無論您在何處參照該位址皆無須重新設定 IP 位址。
   5. 選取 **Launch as an EBS-optimized instance**（作為 **EBS** 最佳化的實例啟動）。
   6. 對於使用 ELB 的部署，新增另一個網路介面，讓您能夠將防火牆上的管理介面和資料介面互換。交換介面需要最少兩個 ENI（eth0 及 eth1）。
      - 展開 Network Interfaces（網路介面）區段，然後按一下 **Add Device**（新增設備），以新增其他網路介面。

        確定 VPC 設置多個子網路，以便在啟動時可新增其他 ENI。

        如果您啟動的防火牆只有一個 *ENI*：
        - 介面交換命令會導致防火牆以維護模式啟動。
        - 新增第二個 *ENI* 時必須重新啟動防火牆。
      - 展開 [Advanced Details（進階詳細資料）] 區段，然後在 **User Data**（使用者資料）欄位中以文字輸入 **`mgmt-interface-swap=enable`**，以在啟動期間執行介面交換。

©2023 Palo Alto Networks, Inc.



Bootstrap Package（啟動套件）—如果您以啟動套件來啟動防火牆，則也可以在 **`mgmt-interface-swap=enable`** 後面輸入分號分隔符號，然後輸入 **`vmseries-bootstrap-aws-s3bucket=<bucketname>`**。

User Data（使用者資料）—如果您以使用者資料來啟動載入，請在 **`mgmt-interface-swap=enable`** 後面輸入分號分隔符號，然後根據以使用者資料輸入基本設定（公共雲端）輸入額外的鍵值組。

AWS Secret（**AWS** 機密）—如果您以 AWS 機密來啟動載入，請在 **`mgmt-interface-swap=enable`** 後面輸入分號分隔符號，然後以鍵值組輸入機密名稱，如在 AWS 上啟動 VM-Series 防火牆的步驟 3 所述。例如：

7. 接受預設的 **Storage**（儲存區）設定。防火牆會使用磁碟區類型 SSD (gp2)。

   首次存取防火牆時，需要金鑰配對。此外在維護模式中存取防火牆時，也需要金鑰配對。

8. （選用）**Tagging**（加標籤）。新增一個或多個標籤，建立您自己用於識別中繼資料，並對 VM-Series 防火牆分組。例如，新增一個 **Name**（名稱）標籤，附帶可幫助您記住在此 VM-Series 防火牆上交換的 ENI 介面的 **Value**（值）。
9. 選取現有的 **Security Group**（安全性群組）或建立新的群組。此安全性群組適用於限制存取防火牆的管理介面。最少考慮對管理介面啟用 https 及 ssh 存取。
10. 若出現提示，請為您的設定選取適當的 **SSD** 選項。
11. 選取 **Review and Launch**（複查並啟動）。複查以確定您的選取是正確的，然後按一下 **Launch**（啟動）。
12. 選取現有的金鑰配對或建立新的金鑰配對，並同意金鑰免責聲明。
13. 下載私人金鑰並儲存至安全的位置；副檔名為 **`.pem`**。此金鑰如果遺失，您無法重新產生此金鑰。

    需要 5-7 分鐘才能啟動 VM-Series 防火牆。您可以在 EC2 儀表板上檢視進度。程序完成時，VM-Series 防火牆會出現在 EC2 儀表板上的 **Instances**（實例）頁面。

©2023 Palo Alto Networks, Inc.

STEP 4 | 設定防火牆的新管理密碼。

在 *VM-Series* 防火牆 *CLI* 上，您必須先設定唯一的管理密碼，才能存取防火牆的 *Web* 介面。若要登入 *CLI*，您需要用於啟動防火牆的私密金鑰。

1. 在 VM-Series 防火牆的命令行介面 (CLI) 中使用公共 IP 位址執行 SSH。您需要在上面的 3 中使用或建立的私人金鑰，來存取 CLI。

   如果您新增額外 *ENI* 來支援搭配 *ELB* 的部署，則必須先建立彈性 *IP* 位址並將其指派給 *ENI*，才能存取 *CLI*，請參閱6。

   如果使用 PuTTY 進行 SSH 存取，您必須將 .pem 格式轉換為 .ppk 格式。請參閱 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html

2. 輸入下列命令登入防火牆：

   ssh-i *<private_key.pem>* admin@*<public-ip_address>*

3. 使用下列命令設定新密碼，並依照畫面上的提示進行：

   configure

   set mgt-config users admin password

4. 如果有需要啟動的 BYOL，請設定 DNS 伺服器 IP 位址，以便防火牆可存取 Palo Alto Networks 授權伺服器。輸入下列命令設定 DNS 伺服器 IP 位址：

   set deviceconfig system dns-setting servers primary *<ip_address>*

5. 使用下列命令提交變更：

   commit

6. 終止 SSH 工作階段。

STEP 5 | 關閉 VM-Series 防火牆。

1. 在 EC2 儀表板中，選取 **Instances**（實例）。
2. 在清單中選取 VM-Series 防火牆，然後按一下 **Actions**（動作） > **Stop**（停止）。

STEP 6 | 建立彈性 IP 位址 (EIP) 並指派給用於防火牆管理存取與重新啟動 VM-Series 防火牆的 ENI。

1. 選取 **Elastic IPs**（彈性 **IP**），然後按一下 **Allocate New Address**（配置新位址）。
2. 選取 **EC2-VPC**，然後按一下 **Yes, Allocate**（是，配置）。
3. 選取新配置的 EIP，然後按一下 **Associate Address**（建立位址關聯）。
4. 選取 **Network Interface**（網路介面）和與管理介面關聯的 **Private IP address**（私人 **IP** 位址），然後按一下 **Yes, Associate**（是，建立關聯）。

©2023 Palo Alto Networks, Inc.

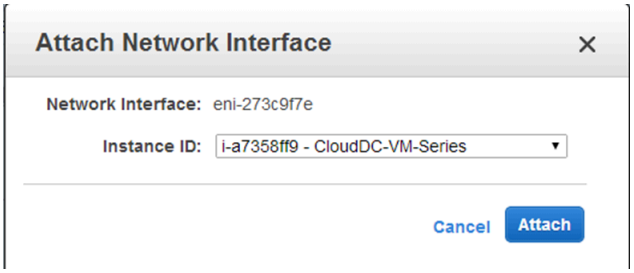
STEP 7 | 建立虛擬網路介面並將介面連接至 VM-Series 防火牆。虛擬網路介面在 AWS 上稱為 Elastic Network Interfaces（彈性網路介面 - ENI），可作為防火牆上的資料平面網路介面。這些介面用於處理出入防火牆的資料流量。

您需要至少兩個 EMI 允許入埠與出埠流量出入防火牆。您在 VM-Series 防火牆上可新增最多七個 ENI 來處理資料流量；請檢查 EC2 實例類型確認防火牆上支援的數目上限。

1. 在 EC2 儀表板上，選取 **Network Interfaces**（網路介面），然後按一下 **Create Network Interface**（建立網路介面）。
2. 為介面輸入描述性名稱。
3. 選取子網路。使用子網路 ID 確定您已選取正確的子網路。您只能將 ENI 連接至同一個子網路中的實例。
4. 輸入要指派給介面的 **Private IP**（私人 **IP**）位址，或選取 **Auto-assign**（自動指派）以自動指派所選子網路中可用 IP 位址內的 IP 位址。
5. 選取 **Security group**（安全性群組）以控制對資料平面網路介面的存取。
6. 按一下 **Yes, Create**（是，建立）。



7. 若要將 ENI 連接至 VM-Series 防火牆，請選取您剛剛建立的介面，然後按一下 **Attach**（附加）。



8. 選取 VM-Series 防火牆的 **Instance ID**（實例 **ID**），然後按一下 **Attach**（連接）。
9. 重複上述步驟至少再建立一個 ENI 並連接至防火牆。

STEP 8 | （依使用授權模式不需要）在 VM-Series 防火牆上啟動授權。

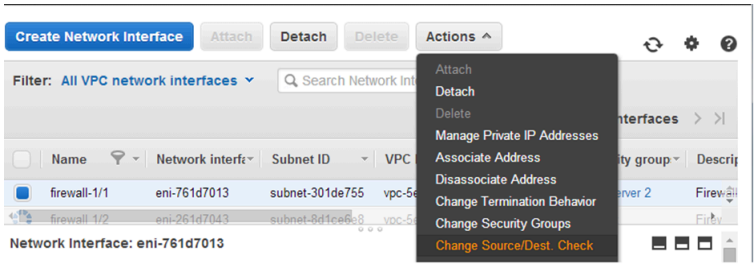
此工作不會在 *AWS* 管理主控台上執行。必須存取 *Palo Alto Networks* 支援入口網站與 *VM-Series* 防火牆的 *Web* 介面，才能啟動授權。

請參閱啟動授權。

©2023 Palo Alto Networks, Inc.

STEP 9 | 停用每個防火牆資料背板網路介面上的來源/目的地檢查。停用此選項可讓介面處理其目的地不是指派給網路介面之 IP 位址的網路流量。

1. 在 EC2 儀表板上，選取 **Network Interfaces**（網路介面）頁籤中的網路介面，例如 eth1/1。
2. 在 **Action**（動作）下拉式清單中選取 **Change Source/Dest. Check**（變更來源/目的地檢查）。



3. 按一下 **Disabled**（已停用），然後 **Save**（儲存）變更。
4. 為每個防火牆資料背板介面重複步驟 1-3。

©2023 Palo Alto Networks, Inc.

STEP 10 | 將資料背板網路介面設為防火牆上的 Layer 3 介面。

相關範例設定，請參閱步驟 14 至 17 # 使用案例：保護 AWS 雲端中的 EC2 實例。

在 *VPC* 內的應用程式伺服器上，將防火牆的資料背板網路介面定義為預設的閘道。

1. 使用 Web 瀏覽器中的安全連線 (https)，在初始設定期間使用您指派的 EIP 位址和密碼登入 (https://<Elastic_IP address>)。您將看見憑證警告；此為正常現象。繼續開啟網頁。
2. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）。
3. 按一下 **Ethernet 1/1** 的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：**Layer3**
   - 在 **Config**（設定）頁籤上，將介面指派給預設路由器。
   - 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。定義新區域，例如 VM_Series_untrust，然後按一下 **OK**（確定）。
   - 按一下 **IPv4** 頁籤，然後選取 **Static**（靜態）或 **DHCP Client**（**DHCP** 用戶端）。

     如果使用 **Static**（靜態）選項，請按一下 IP 部分中的 **Add**（新增），然後輸入介面的 IP 位址與網路遮罩，例如 10.0.0.10/24。

     確定 IP 位址符合您早先指派的 ENI IP 位址。

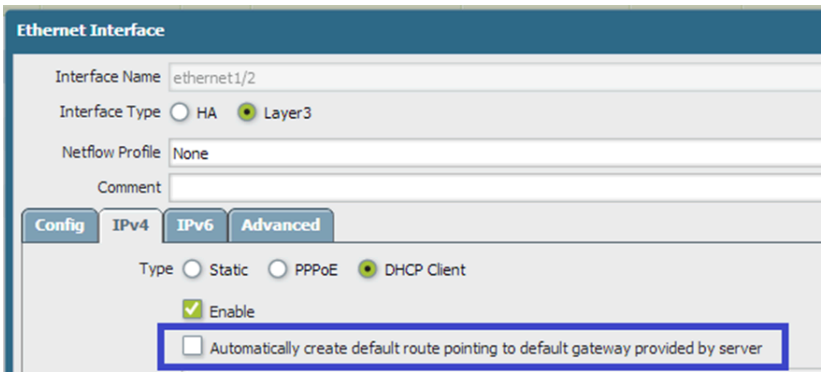
     如果使用 DHCP，請選取 **DHCP Client**（**DHCP** 用戶端）；將會自動取得您指派給 AWS 管理主控台中 ENI 的私人 IP 位址。
4. 按一下 **ethernet 1/2**（乙太網路 **1/2**）的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：**Layer3**
   - 安全性地區：VM_Series_trust
   - **IP Address**（**IP** 位址）：選取 **Static**（靜態）或 **DHCP Client**（**DHCP** 用戶端）選項按鈕。

     若為靜態，請按一下 IP 部分中的 **Add**（新增），然後輸入介面的 IP 位址與網路遮罩。確定 IP 位址符合您早先指派的連接 ENI IP 位址。
5. 按一下 **Commit**（交付）。確認介面的連結狀態為啟動。



若為 *DHCP*，請清除 ***Automatically create default route to default gateway provided by server***（自動建立伺服器所提供之預設閘道的預設路由）核取方塊。對於連接至 *VPC* 中私人子網路的介面，請停用此選項確定此介面處理的流量不會直接流至 *VPC* 上的網際網路閘道。

©2023 Palo Alto Networks, Inc.



STEP 11 | 建立 NAT 規則，以允許來自 VPC 內部署之伺服器的輸入和輸出流量。

1. 在防火牆的網頁介面上，選取 **Policies**（政策） > **NAT**。
2. 建立 NAT 規則以允許流量從防火牆上的資料背板網路介面流到 VPC 中的 Web 伺服器介面。
3. 建立 NAT 規則，以針對從 Web 伺服器至網際網路的流量，允許輸出存取。

STEP 12 | 建立安全性原則以允許/拒絕流量進/出 VPC 內部署的伺服器。

1. 在防火牆的網頁介面上，選取 **Policies**（政策） > **Security**（安全性）。
2. 按一下 **Add**（新增），然後指定您想要執行的地區、應用程式及日誌記錄選項，以限制與稽核透過網路周遊的流量。

STEP 13 | 在防火牆 Commit（提交）變更。

按一下 **Commit**（交付）。

STEP 14 | 確認 VM-Series 防火牆正在保護流量，以及 NAT 規則已生效。

1. 在防火牆的網頁介面上，選取 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量）。
2. 檢視日誌以確定在網路中周遊的應用程式符合您實作的安全性原則。

在 AWS Outposts 上啟動 VM-Series 防火牆

依照下列程序，將 VM-Series 防火牆部署在 AWS Ouptost 機架上。如果尚未使用您的支援帳戶來註冊您在訂購完成電子郵件中收到的容量授權碼，請參閱註冊 VM-Series 防火牆。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 存取 AWS Outposts 主控台。

©2023 Palo Alto Networks, Inc.

STEP 2 | 延伸您的 VPC 以納入 AWS Outpost 機架。

VM-Series 防火牆必須能夠從 EC2 實例接收流量，也必須能在 VPC 與網際網路之間執行輸入與輸出通訊。

請參閱 AWS Outpost 文件，以取得將您的連線至 VPC 的指示。

1. 確認網路與安全性元件已適當定義。
   - 啟用網際網路通訊。Outpost 需仰賴本機閘道連線至您的本機 LAN 和網際網路。
   - 建立 Outpost 子網路。
   - 視需要建立安全性群組，以管理 EC2 實例/子網路的輸入與輸出流量。
   - 為私人子網路的路由表新增路由，以確定流量可在 VPC 中整個子網路與安全性群組之間路由（若適當的話）。
2. 如果您要在 HA 中部署一對 VM-Series 防火牆，您必須先定義 HA 的 IAM 角色，才能AWS 上 VM-Series 防火牆的高可用性。
3. （選用）如果您使用啟動載入來執行 VM-Series 防火牆的設定，請參閱在 AWS 上啟動 VM-Series 防火牆。如需啟動程序的詳細資訊，請參閱啟動 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

STEP 3 | 啟動 VM-Series 防火牆。

> 雖然啟動時可將額外網路介面 *(ENI)* 新增至 *VM-Series* 防火牆，重新啟動防火牆時，*AWS* 將對管理介面釋放自動指派的公共 *IP* 位址。因此，為了確保管理介面的連接性，您必須先對管理介面指派彈性 *IP* 位址，在將額外介面連接至防火牆。

如果您想要保留 EIP 位址，可將一個 EIP 位址指派給 eth 1/1 介面，並將此介面用於管理流量與資料流量。若要限制介面上允許的服務或限制可登入 eth 1/1 介面的 IP 位址，請將管理設定檔附加至介面。

1. 在 EC2 儀表板中，按一下 **Launch Instance**（啟動實例）。
2. 選取 VM-Series AMI。若要取得 AMI，請參閱取得 AMI。
3. 在 EC2 實例上啟動 VM-Series 防火牆。
   1. 選取 **EC2 instance type**（**EC2** 實例類型），以配置防火牆所需的資源，然後按 **Next**（下一步）。有關資源需求，請參閱 VM-Series 系統需求。
   2. 選取 VPC。
   3. 選取 VM-Series 管理介面將連接到 Outpost 上的哪一個公用子網路。
   4. 選取 **Automatically assign a public IP address**（自動指派公共 **IP** 位址）。這可讓您為 VM-Series 防火牆的管理介面取得可公開存取的 IP 位址。

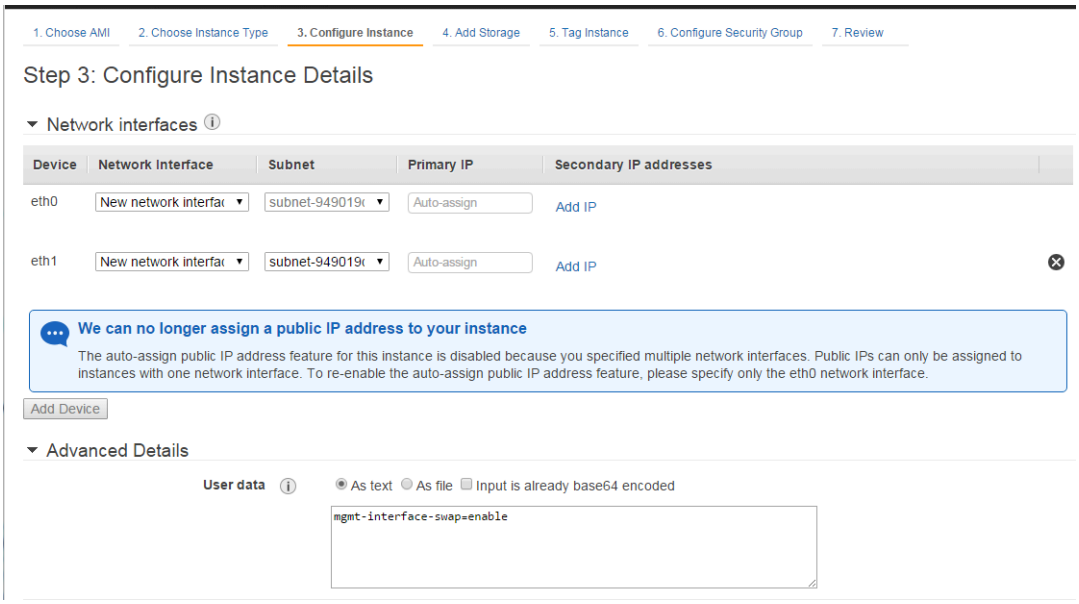
      您稍後可將彈性 IP 位址連接到管理介面；不同於公共 IP 位址在實例終止時會與防火牆中斷關聯，彈性 IP 位址提供持續性，並會重新連接至 VM-Series 防火牆的新（或替代）實例，且無論您在何處參照該位址皆無須重新設定 IP 位址。
   5. 選取 **Launch as an EBS-optimized instance**（作為 **EBS** 最佳化的實例啟動）。
   6. 對於使用 ELB 的部署，新增另一個網路介面，讓您能夠將防火牆上的管理介面和資料介面互換。交換介面需要最少兩個 ENI（eth0 及 eth1）。
      - 展開 Network Interfaces（網路介面）區段，然後按一下 **Add Device**（新增設備），以新增其他網路介面。

        確定 VPC 設置多個子網路，以便在啟動時可新增其他 ENI。

        > 如果您啟動的防火牆只有一個 *ENI*：
        > - 介面交換命令會導致防火牆以維護模式啟動。
        > - 新增第二個 *ENI* 時必須重新啟動防火牆。
      - 展開 [Advanced Details（進階詳細資料）] 區段，然後在 [User Data（使用者資料）] 欄位中以文字輸入 **`mgmt-interface-swap=enable`** ，以在啟動期間執行介面交換。

        > 如果您要啟動防火牆，則也可以在 ***`vmseries-bootstrap-aws-s3bucket=<bucketname>`*** 後面使用逗號分隔符號來輸入 ***`mgmt-interface-swap=enable`***。

©2023 Palo Alto Networks, Inc.



7. 接受預設的 **Storage**（儲存區）設定。防火牆會使用磁碟區類型 SSD (gp2)

   首次存取防火牆時，需要金鑰配對。此外在維護模式中存取防火牆時，也需要金鑰配對。

8. （選用）**Tagging**（加標籤）。新增一個或多個標籤，建立您自己用於識別中繼資料，並對 VM-Series 防火牆分組。例如，新增一個 **Name**（名稱）標籤，附帶可幫助您記住在此 VM-Series 防火牆上交換的 ENI 介面的 **Value**（值）。
9. 選取現有的 **Security Group**（安全性群組）或建立新的群組。此安全性群組適用於限制存取防火牆的管理介面。最少考慮對管理介面啟用 https 及 ssh 存取。
10. 若出現提示，請為您的設定選取適當的 **SSD** 選項。
11. 選取 **Review and Launch**（複查並啟動）。複查以確定您的選取是正確的，然後按一下 **Launch**（啟動）。
12. 選取現有的金鑰配對或建立新的金鑰配對，並同意金鑰免責聲明。
13. 下載私人金鑰並儲存至安全的位置；副檔名為 `.pem`。此金鑰如果遺失，您無法重新產生此金鑰。

    需要 5-7 分鐘才能啟動 VM-Series 防火牆。您可以在 EC2 儀表板上檢視進度。程序完成時，VM-Series 防火牆會出現在 EC2 儀表板上的 **Instances**（實例）頁面。

©2023 Palo Alto Networks, Inc.

STEP 4 | 設定防火牆的新管理密碼。

在 *VM-Series* 防火牆 *CLI* 上，您必須先設定唯一的管理密碼，才能存取防火牆的 *Web* 介面。若要登入 *CLI*，您需要用於啟動防火牆的私密金鑰。

1. 在 VM-Series 防火牆的命令行介面 (CLI) 中使用公共 IP 位址執行 SSH。您需要在上面的 3 中使用或建立的私人金鑰，來存取 CLI。

   如果您新增額外 *ENI* 來支援搭配 *ELB* 的部署，則必須先建立彈性 *IP* 位址並將其指派給 *ENI*，才能存取 *CLI*，請參閱6。

   如果使用 PuTTY 進行 SSH 存取，您必須將 .pem 格式轉換為 .ppk 格式。請參閱 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html

2. 輸入下列命令登入防火牆：

   ssh-i *<private_key.pem>* admin@*<public-ip_address>*

3. 使用下列命令設定新密碼，並依照畫面上的提示進行：

   configure

   set mgt-config users admin password

4. 如果有需要啟動的 BYOL，請設定 DNS 伺服器 IP 位址，以便防火牆可存取 Palo Alto Networks 授權伺服器。輸入下列命令設定 DNS 伺服器 IP 位址：

   set deviceconfig system dns-setting servers primary *<ip_address>*

5. 使用下列命令提交變更：

   commit

6. 終止 SSH 工作階段。

STEP 5 | 關閉 VM-Series 防火牆。

1. 在 EC2 儀表板中，選取 **Instances**（實例）。
2. 在清單中選取 VM-Series 防火牆，然後按一下 **Actions**（動作） > **Stop**（停止）。

STEP 6 | 建立彈性 IP 位址 (EIP) 並指派給用於防火牆管理存取與重新啟動 VM-Series 防火牆的 ENI。

1. 選取 **Elastic IPs**（彈性 **IP**），然後按一下 **Allocate New Address**（配置新位址）。
2. 選取 **EC2-VPC**，然後按一下 **Yes, Allocate**（是，配置）。
3. 選取新配置的 EIP，然後按一下 **Associate Address**（建立位址關聯）。
4. 選取 **Network Interface**（網路介面）和與管理介面關聯的 **Private IP address**（私人 **IP** 位址），然後按一下 **Yes, Associate**（是，建立關聯）。

©2023 Palo Alto Networks, Inc.

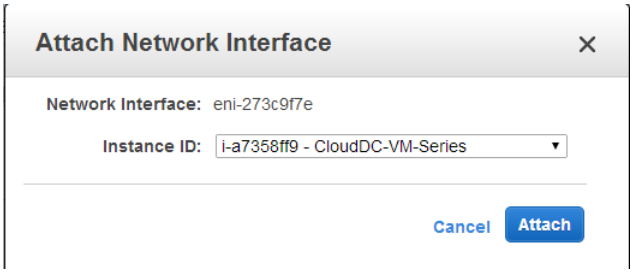
STEP 7 | 建立虛擬網路介面並將介面連接至 VM-Series 防火牆。虛擬網路介面在 AWS 上稱為 Elastic Network Interfaces（彈性網路介面 - ENI），可作為防火牆上的資料平面網路介面。這些介面用於處理出入防火牆的資料流量。

您需要至少兩個 EMI 允許入埠與出埠流量出入防火牆。您在 VM-Series 防火牆上可新增最多七個 ENI 來處理資料流量；請檢查 EC2 實例類型確認防火牆上支援的數目上限。

1. 在 EC2 儀表板上，選取 **Network Interfaces**（網路介面），然後按一下 **Create Network Interface**（建立網路介面）。
2. 為介面輸入描述性名稱。
3. 選取子網路。使用子網路 ID 確定您已選取正確的子網路。您只能將 ENI 連接至同一個子網路中的實例。
4. 輸入要指派給介面的 **Private IP**（私人 **IP**）位址，或選取 **Auto-assign**（自動指派）以自動指派所選子網路中可用 IP 位址內的 IP 位址。
5. 選取 **Security group**（安全性群組）以控制對資料平面網路介面的存取。
6. 按一下 **Yes, Create**（是，建立）。



7. 若要將 ENI 連接至 VM-Series 防火牆，請選取您剛剛建立的介面，然後按一下 **Attach**（附加）。



8. 選取 VM-Series 防火牆的 **Instance ID**（實例 **ID**），然後按一下 **Attach**（連接）。
9. 重複上述步驟至少再建立一個 ENI 並連接至防火牆。

STEP 8 | （依使用授權模式不需要）在 VM-Series 防火牆上啟動授權。

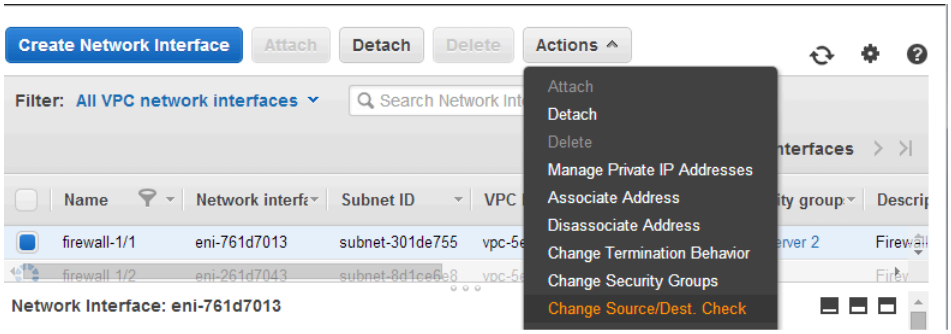
此工作不會在 *AWS* 管理主控台上執行。必須存取 *Palo Alto Networks* 支援入口網站與 *VM-Series* 防火牆的 *Web* 介面，才能啟動授權。

請參閱啟動授權。

©2023 Palo Alto Networks, Inc.

STEP 9 | 停用每個防火牆資料背板網路介面上的來源/目的地檢查。停用此選項可讓介面處理其目的地不是指派給網路介面之 IP 位址的網路流量。

1. 在 EC2 儀表板上，選取 **Network Interfaces**（網路介面）頁籤中的網路介面，例如 eth1/1。
2. 在 **Action**（動作）下拉式清單中選取 **Change Source/Dest. Check**（變更來源/目的地檢查）。



3. 按一下 **Disabled**（已停用），然後 **Save**（儲存）變更。
4. 為每個防火牆資料背板介面重複步驟 1-3。

©2023 Palo Alto Networks, Inc.

STEP 10 | 將資料背板網路介面設為防火牆上的 Layer 3 介面。

相關範例設定，請參閱步驟 14 至 17 # 使用案例：保護 AWS 雲端中的 EC2 實例。

在 *VPC* 內的應用程式伺服器上，將防火牆的資料背板網路介面定義為預設的閘道。

1. 使用 Web 瀏覽器中的安全連線 (https)，在初始設定期間使用您指派的 EIP 位址和密碼登入 (https://<Elastic_IP address>)。您將看見憑證警告；此為正常現象。繼續開啟網頁。
2. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）。
3. 按一下 **Ethernet 1/1** 的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：**Layer3**
   - 在 **Config**（設定）頁籤上，將介面指派給預設路由器。
   - 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。定義新區域，例如 VM_Series_untrust，然後按一下 **OK**（確定）。
   - 按一下 **IPv4** 頁籤，然後選取 **Static**（靜態）或 **DHCP Client**（**DHCP** 用戶端）。

     如果使用 **Static**（靜態）選項，請按一下 IP 部分中的 **Add**（新增），然後輸入介面的 IP 位址與網路遮罩，例如 10.0.0.10/24。

     確定 IP 位址符合您早先指派的 ENI IP 位址。

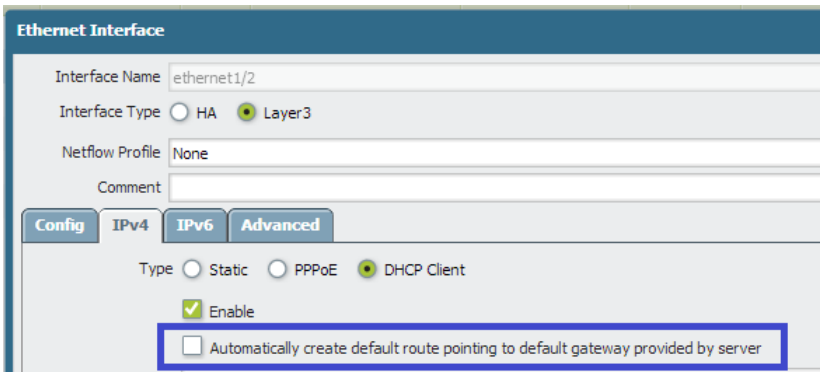
     如果使用 DHCP，請選取 **DHCP Client**（**DHCP** 用戶端）；將會自動取得您指派給 AWS 管理主控台中 ENI 的私人 IP 位址。
4. 按一下 **ethernet 1/2**（乙太網路 **1/2**）的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：**Layer3**
   - 安全性地區：VM_Series_trust
   - **IP Address**（**IP** 位址）：選取 **Static**（靜態）或 **DHCP Client**（**DHCP** 用戶端）選項按鈕。

     若為靜態，請按一下 IP 部分中的 **Add**（新增），然後輸入介面的 IP 位址與網路遮罩。確定 IP 位址符合您早先指派的連接 ENI IP 位址。
5. 按一下 **Commit**（交付）。確認介面的連結狀態為啟動。



若為 *DHCP*，請清除 ***Automatically create default route to default gateway provided by server***（自動建立伺服器所提供之預設閘道的預設路由）核取方塊。對於連接至 *VPC* 中私人子網路的介面，請停用此選項確定此介面處理的流量不會直接流至 *VPC* 上的網際網路閘道。

©2023 Palo Alto Networks, Inc.



STEP 11 | 建立 NAT 規則，以允許來自 VPC 內部署之伺服器的輸入和輸出流量。

1. 在防火牆的網頁介面上，選取 **Policies**（政策） > **NAT**。
2. 建立 NAT 規則以允許流量從防火牆上的資料背板網路介面流到 VPC 中的 Web 伺服器介面。
3. 建立 NAT 規則，以針對從 Web 伺服器至網際網路的流量，允許輸出存取。

STEP 12 | 建立安全性原則以允許/拒絕流量進/出 VPC 內部署的伺服器。

1. 在防火牆的網頁介面上，選取 **Policies**（政策） > **Security**（安全性）。
2. 按一下 **Add**（新增），然後指定您想要執行的地區、應用程式及日誌記錄選項，以限制與稽核透過網路周遊的流量。

STEP 13 | 在防火牆 Commit（提交）變更。

按一下 **Commit**（交付）。

STEP 14 | 確認 VM-Series 防火牆正在保護流量，以及 NAT 規則已生效。

1. 在防火牆的網頁介面上，選取 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量）。
2. 檢視日誌以確定在網路中周遊的應用程式符合您實作的安全性原則。

建立自訂 Amazon 機器映像 (AMI)

自訂 VM-Series AMI 可讓您使用您想要使用的 PAN-OS 版本，在網路上一致且彈性地部署 VM-Series 防火牆，而非限制為只能使用發佈至 AWS 公共 Marketplace 或 AWS GovCloud Marketplace 的 AMI。使用自訂 AMI 可加速使用所選擇的 PAN-OS 版本來部署防火牆的程序，因為它會減少下列操作的時間：使用 AWS 公共或 AWS GovCloud Marketplace 上所發佈的 AMI 來佈建防火牆，然後執行軟體升級來取得您有資格使用或想要在網路上使用的 PAN-OS 版本。此外，您還可以接著在自動調整規模 VM-Series 防火牆 CloudFormation 範本，或您已建立的任何其他範本中使用自訂 AMI。

您可以使用 BYOL、搭售包 1 或搭售包 2 授權來建立自訂 AMI。建立自訂 AMI 的程序需要您移除防火牆中的所有設定，並將它重設為原廠預設值，因此，在此工作流程中，您將從 AWS Marketplace 啟動新的防火牆實例，而非使用您已完全設定的現有防火牆。

©2023 Palo Alto Networks, Inc.

使用防火牆的 *BYOL* 版本來建立自訂 *AMI* 時，您必須先在防火牆上啟動授權，才能存取與下載 *PAN-OS* 軟體更新來升級防火牆，然後先停用防火牆上的授權，再將防火牆重設為原廠預設值，並建立自訂 *AMI*。如果您未停用授權，則會遺失您在此防火牆實例上套用的授權。

STEP 1 | 從 Marketplace 啟動 VM-Series 防火牆。

請參閱 3

STEP 2 | （僅適用於 BYOL）啟動授權。

STEP 3 | 安裝軟體更新，並將防火牆升級至您計劃使用的 PAN-OS 版本。

STEP 4 | （僅適用於 BYOL）停用授權。

STEP 5 | 執行私人資料重設。

私人資料重設會移除所有日誌，並還原預設設定。

系統磁碟不會予以消除，因此步驟 4 中的內容更新會保持不變。

1. 存取防火牆 CLI。
2. 移除所有日誌，並還原預設設定。

```
request system private-data-reset
```

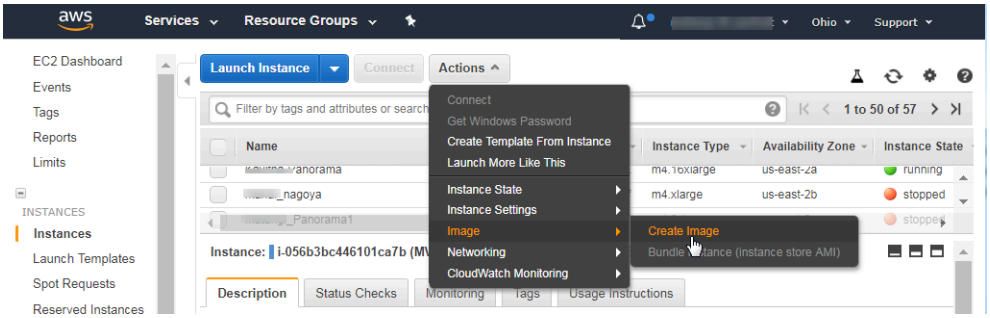
輸入 **y** 以確認。

防火牆會重新啟動以初始化預設設定。

©2023 Palo Alto Networks, Inc.

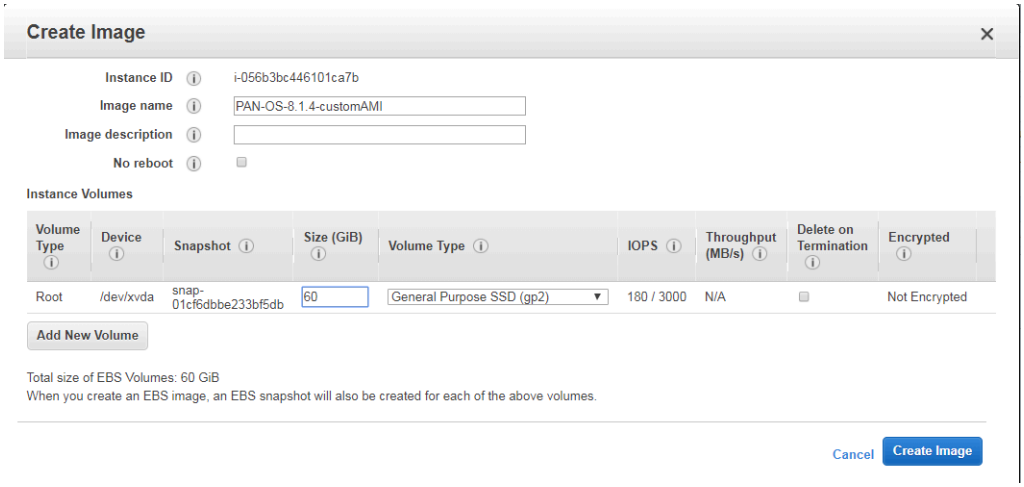
STEP 6 | 建立自訂 AMI。

1. 登入 AWS 主控台，並選取 [EC2 Dashboard（EC2 儀表板）]。
2. **Stop**（停止）VM-Series 防火牆。
3. 選取 VM-Series 防火牆實例，然後按一下 **Image**（映像） > **Create Image**（建立映像）。



4. 輸入自訂映像名稱，然後按一下 **Create Image**（建立映像）。

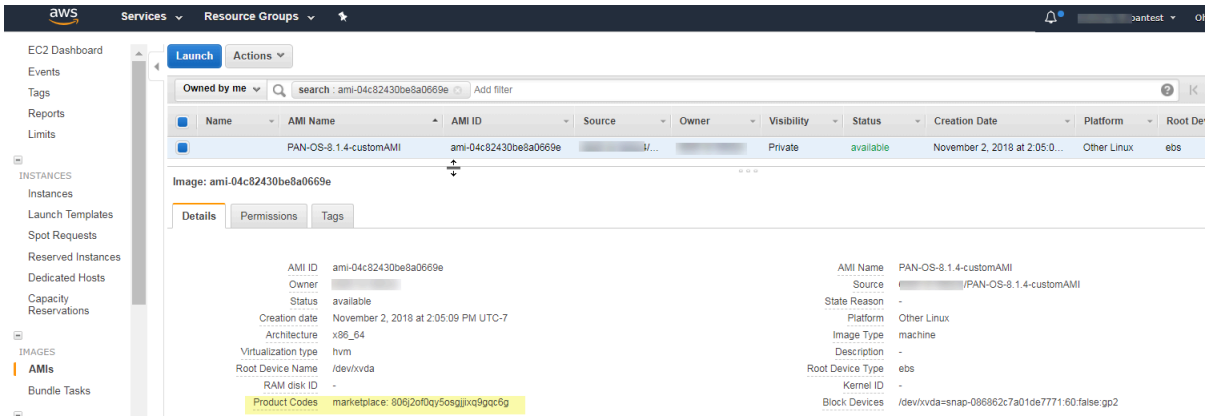
   60GB 的磁碟空間是最低需求。



5. 確認自訂 AMI 已建立並具有正確的產品代碼。

   1. 在 [EC2 Dashboard（EC2 儀表板）] 上，選取 **AMI**。
   2. 選取您剛剛建立的 AMI。根據您使用 BYOL、搭售包 1 還是搭售包 2 授權選項來選取 AMI，您應該會在詳細資料中看到下列其中一個 **Product Codes**（產品代碼）：
      - BYOL—6njl1pau431dv1qxipg63mvah
      - 搭售包 1—6kxdw3bbmdeda3o6i1ggqt4km
      - Bundle 2—806j2of0qy5osgjjixq9gqc6g

©2023 Palo Alto Networks, Inc.



STEP 7 | 在 AWS 上加密 VM-Series 防火牆的 EBS 磁碟區.

如果您計劃搭配使用自訂 AMI 與使用 Amazon ELB 服務自動調整 VM-Series 防火牆規模部署的 EBS 加密，則必須使用 AWS 帳戶的預設主要金鑰。

STEP 8 | 在防火牆上設定管理密碼。

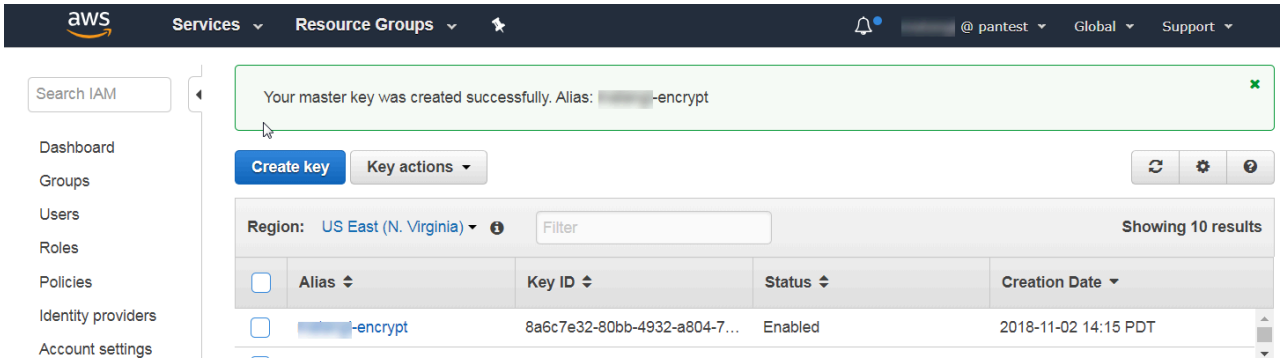
請參閱 4

在 AWS 上加密 VM-Series 防火牆的 EBS 磁碟區

EBS 加密適用於所有您可在其上部署 VM-Series 防火牆的 AWS EC2 實例類型。若要將資料安全地儲存至 AWS 上的 VM-Series 防火牆，您必須先建立 AWS 公共或 GovCloud Marketplace 上所發佈的 AMI 複本，或使用自訂 AMI，然後使用 AWS Key Management Service (KMS) 上的客戶主要金鑰 (CMK) 來加密 EBS 磁碟區。您可以使用 AWS 帳戶的預設主要金鑰或先前使用 AWS Key Management Service 所建立的任何 CMK，並讓 EBS 與 KMS 互動來確保資料安全性。

STEP 1 | 建立 AWS 上的加密金鑰，或者如果您要使用帳戶的預設主要金鑰，則請略過此步驟。

您將使用此金鑰來加密防火牆上的 EBS 磁碟區。請注意，金鑰是區域特有的。

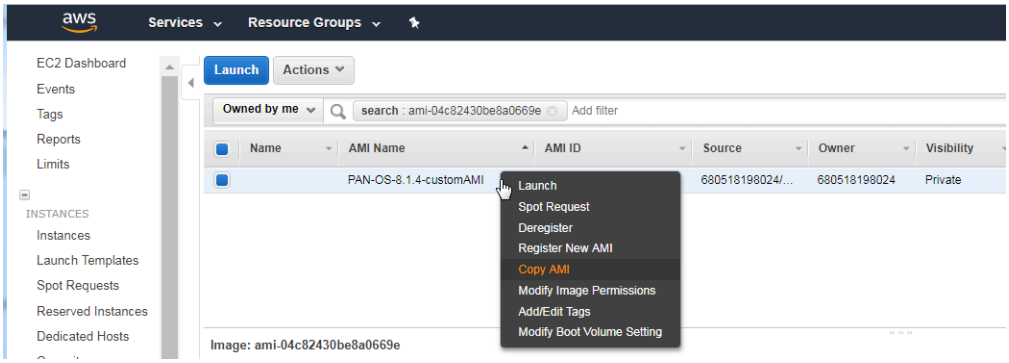


 ©2023 Palo Alto Networks, Inc.

STEP 2 | 使用金鑰來加密防火牆上的 EBS 磁碟區。

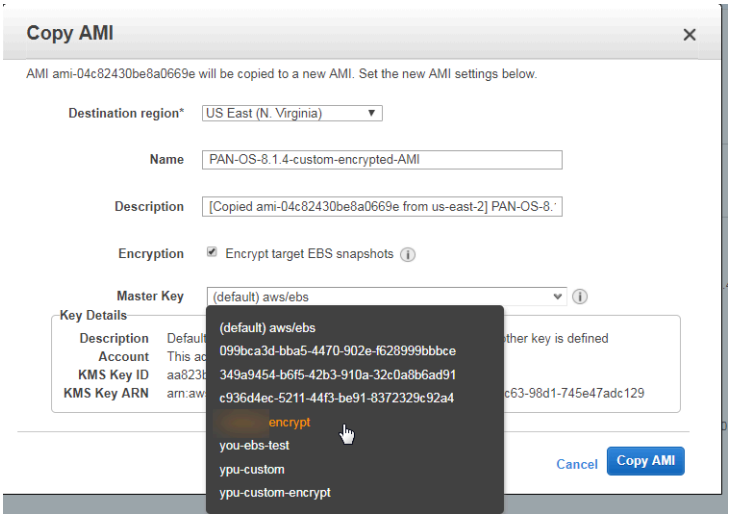
您必須建立您要加密之 AMI 的複本。您可以複製 AWS 公共或 GovCloud Marketplace 上所發佈的 AMI，或使用自訂 AMI (建立自訂 Amazon 機器映像 (AMI))。

1. 在 [EC2 Dashboard（EC2 儀表板）] 上，選取 AMI，並 **Copy AMI**（複製 **AMI**）。

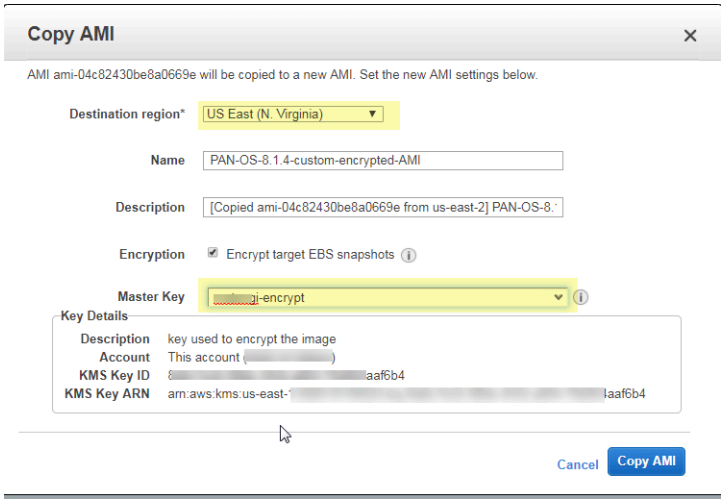


2. 設定 AMI 的詳細資料。

   務必選取 **Encrypt target EBS snapshots**（加密目標 **EBS** 快照）。

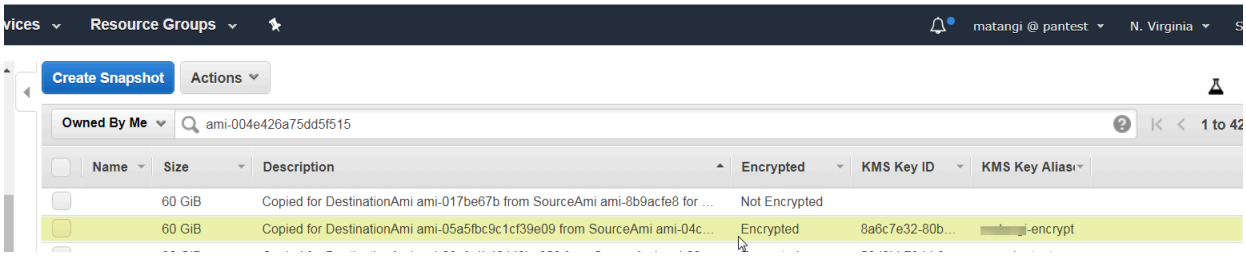


3. 選取加密金鑰，並 **Copy AMI**（複製 **AMI**）來建立已加密的 EBS 快照。



©2023 Palo Alto Networks, Inc.

4. 選取 **EC2 Dashboard**（**EC2** 儀表板） > **Snapshots**（快照），確認已使用您在上面選取的金鑰來加密 EBS 快照。



使用 VM-Series 防火牆 CLI 來交換管理介面

部署防火牆時，如果您沒有使用資料平面介面（乙太網路 1/1）來交換管理介面 (MGT)，則可使用 CLI 來啟用防火牆，以在啟動防火牆之後在主要介面上接收資料平面流量。

STEP 1 | 完成在 AWS 上啟動 VM-Series 防火牆的步驟 1 至 7。

繼續前，確認防火牆最少配備兩個 *ENI*（*eth0* 與 *eth1*）。如果啟動只配備一個 *ENI* 的防火牆，介面交換命令會導致防火牆啟動維護模式。

STEP 2 | 在 EC2 儀表盤上，檢視 eth1 介面的 IP 位址，並確認 AWS 安全性防火牆群組規則允許連線（HTTPS 與 SSH）至新的管理介面 (eth1)。

STEP 3 | 登入 VM-Series 防火牆 CLI 並輸入下列命令：

```
set system setting mgmt-interface-swap enable yes
```

STEP 4 | 確認您要交換介面並將 eth1 資料平面介面用作管理介面。

STEP 5 | 重新啟動防火牆以使交換生效。使用下列命令：

```
request restart system
```

STEP 6 | 確認介面已交換。使用下列命令：

```
debug show vm-series interfaces all Phoenix_interface   Base-
OS_port   Base-OS_MAC        PCI-ID         Driver mgt(interface-
swap) eth0   0e:53:96:91:ef:29   0000:00:04.0   ixgbevf Ethernet1/1
           eth1    0e:4d:84:5f:7f:4d       0000:00:03.0   ixgbevf
```

在 VM-Series 防火牆上啟用 CloudWatch 監控

AWS 上的 VM-Series 防火牆可以將原生 PAN-OS 度量發佈至 AWS CloudWatch，供您用來監控防火牆。這些度量可讓您評估效能和使用模式，據以採取動作來啟動或終止 VM-Series 防火牆的實例。

防火牆會依指定的時間間隔，使用 AWS API 將度量發佈至命名空間，這是 AWS 上用來收集度量的位置。當您將防火牆設定成將度量發佈至 AWS CloudWatch 時，您可以在兩個命名空間中檢視度量 — 主要命名空間會針對所有依設定使用命名空間的實例收集並彙總其選取的度量，次要命

©2023 Palo Alto Networks, Inc.

名空間則會以尾碼 `_dimensions` 自動建立，讓您使用主機名稱和 AWS 實例 ID 中繼資料（或維度）篩選度量，以及檢視個別 VM-Series 防火牆的使用情形和效能。

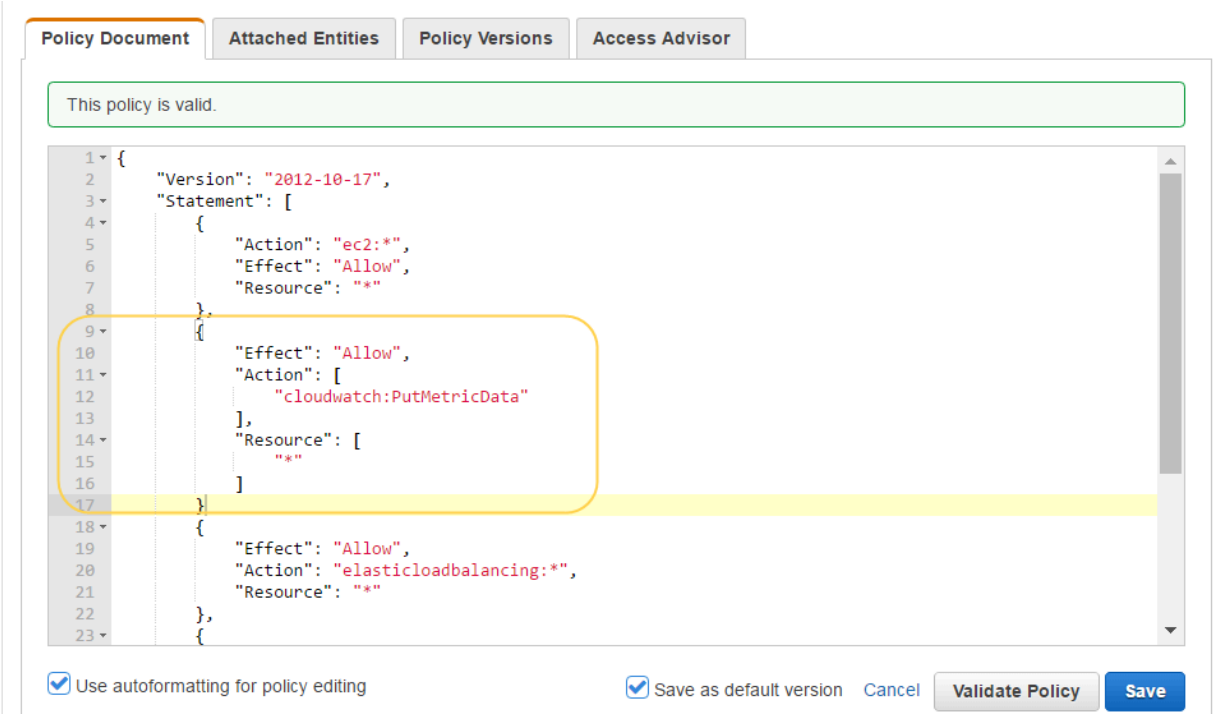
您可以在 CloudWatch 中監控度量，或建立自動縮放原則以觸發警報，並在受監控的度量達到閾值時，採取動作來手動部署防火牆的新實例。有關設定警告條件以採取相應放大或相應縮小動作的最佳作法，請參閱 AWS CloudWatch和自動調整規模群組 (ASG) 文件。

如需可發佈至 CloudWatch 的 PAN-OS 度量相關說明，請參閱發佈自訂 PAN-OS 度量以作為監控使用。

STEP 1 | 針對您用於在 AWS 上部署 VM-Series 防火牆的 AWS Identity and Access Management（識別和存取管理 - IAM）使用者角色，指派適當的權限。

不論您為 VM-Series 防火牆啟動新的實例，或將 AWS 上的現有 VM-Series 防火牆升級，與您的實例相關的 IAM 角色必須有權限將度量發佈至 CloudWatch。

1. 在 AWS 主控台上，選取 IAM。
2. 編輯 IAM 角色來授予下列權限：



您可以將權限複製並貼到此處：

```
{ "版本":"2012-10-17", "聲明": [ { "效果":"允許", "動作":
 [ "cloudwatch:輸入度量資料" ], "資源": [ "*" ] } ] }
```

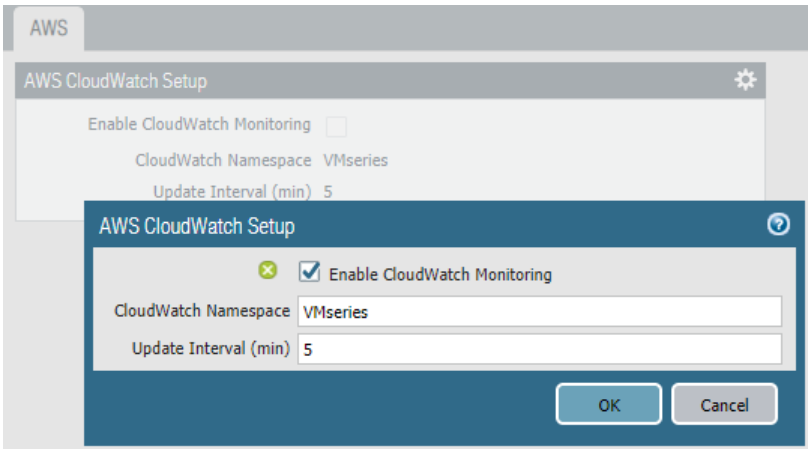

©2023 Palo Alto Networks, Inc.

STEP 2 | 在 AWS 上的 VM-Series 防火牆上啟用 CloudWatch。

1. 登入 VM-Series 防火牆的網頁介面
2. 選取 **Device**（裝置） > **VM-Series**。
3. 在 [AWS CloudWatch Setup（AWS CloudWatch 設定）] 中，按一下 **Edit**（編輯）（⚙），然後選取 **Enable CloudWatch Monitoring**（啟用 **CloudWatch** 監控）。

   1. 輸入防火牆可在其中發佈度量的 **CloudWatch Namespace**（**CloudWatch** 命名空間）。命名空間不能以 **AWS** 開頭。

      為 HA 配對或自動調整規模部署中的所有 VM-Series 防火牆彙總的度量，會發佈至您在上方輸入的命名空間。以 `_dimensions` 尾碼自動建立的命名空間，可讓您使用連接至防火牆的主機名稱或 AWS 實例 ID 中繼資料來篩選及檢視特定 VM-Series 防火牆的度量。
   2. 將 **Update interval**（更新間隔）設為 1-60 分鐘之間的值。這是防火牆將度量發佈至 CloudWatch 的頻率。預設值為 5 分鐘。



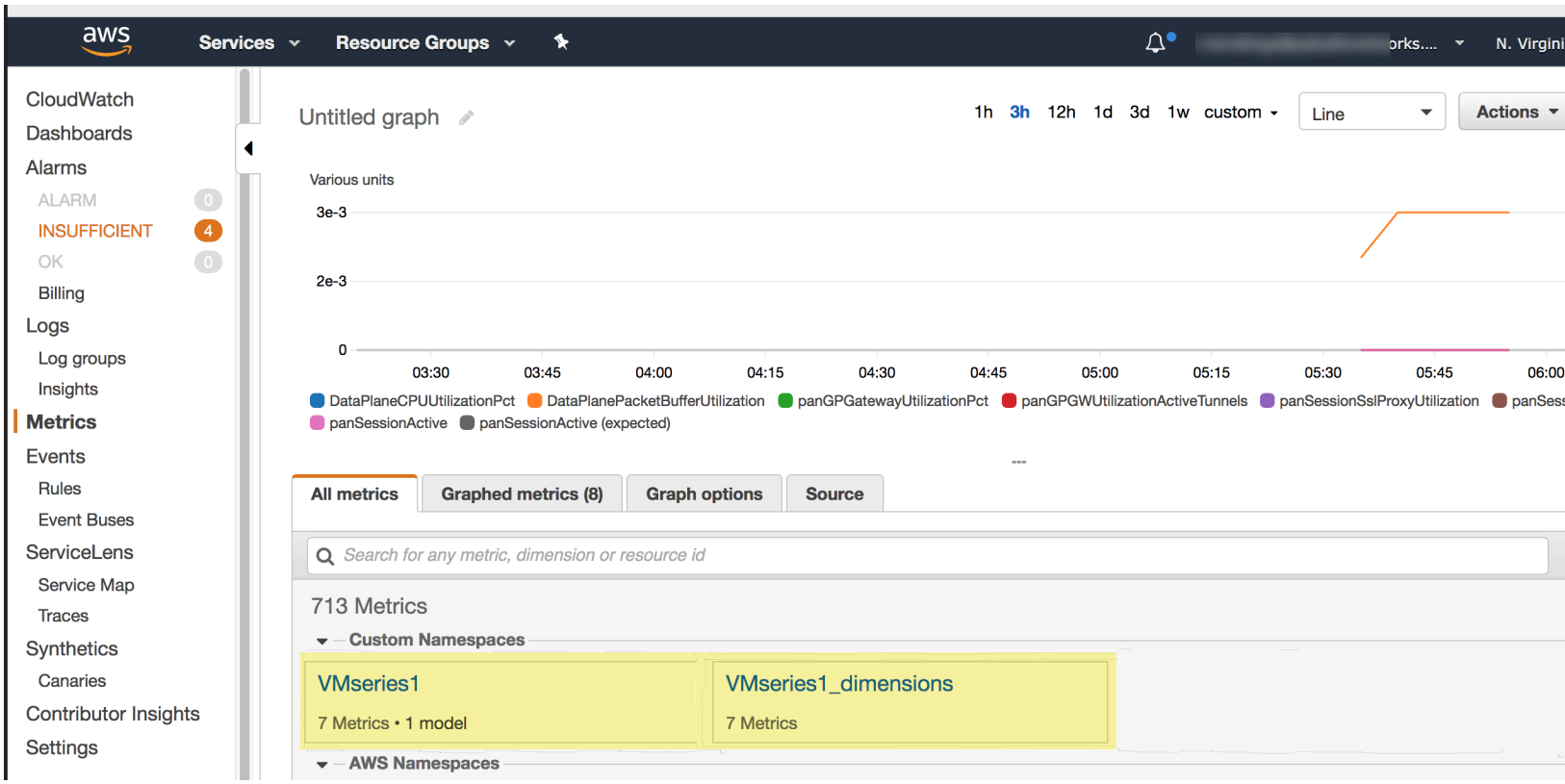
4. **Commit**（提交）變更。

   在防火牆開始將度量發佈至 CloudWatch 之前，您無法為 PAN-OS 度量設定警報。

©2023 Palo Alto Networks, Inc.

STEP 3 | 確認您在 CloudWatch 上可以看見度量。

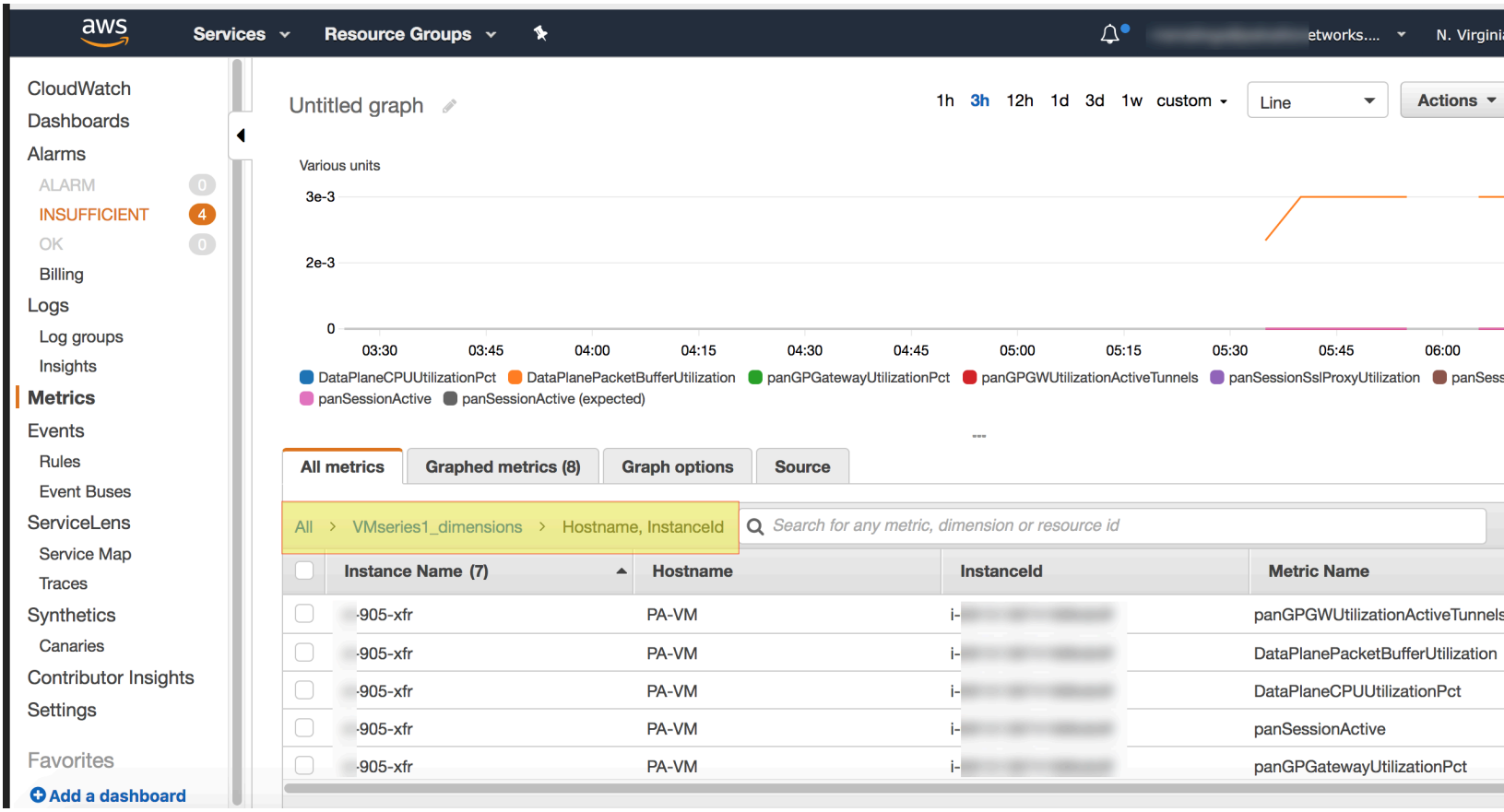
1. 在 AWS 主控台上，選取 **CloudWatch** > **Metrics**（度量），依類別來檢視 CloudWatch 度量。
2. 從 Custom Metrics（自訂度量）下拉式清單中，選取命名空間。



3. 確認您在檢視清單中可以看見 PAN-OS 度量。

   若要依特定防火牆的主機名稱或 AWS 實例 ID 進行篩選，請選取 `_dimensions`。

©2023 Palo Alto Networks, Inc.



STEP 4 | 在 CloudWatch 上為 PAN-OS 度量設定警報和動作。

請參閱 AWS 文件：http://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html

採用啟動程序組態的 VM-Series 防火牆大約需要 7-9 分鐘，才會開始提供服務。下列一些範例說明如何設定警報來觸發自動調整 VM-Series 防火牆的規模：

- 如果您將 VM-Series 防火牆的 2 個實例部署為 Global Protect Gateway 來保護遠端使用者安全，請使用「GlobalProtect 閘道作用中通道數」度量。您可以設定當作用中通道數持續 15 分鐘大於 300 時，就發出警報，然後您可以部署 VM-Series 防火牆的 2 個新實例，這些實例會啟動並設定成為 Global Protect Gateway。
- 如果您使用防火牆來保護 AWS 中的工作負載安全，請使用「工作階段使用率」度量，以根資源使用量來相應縮小或相應放大防火牆。您可以設定當工作階段使用率度量持續 15 分鐘大於 60% 時，就發出警報，以便部署 VM-Series 實例防火牆的一個實例。相反地，如果「工作階段使用率」持續 30 分鐘小於 50%，則終止 VM-Series 防火牆的實例。

©2023 Palo Alto Networks, Inc.

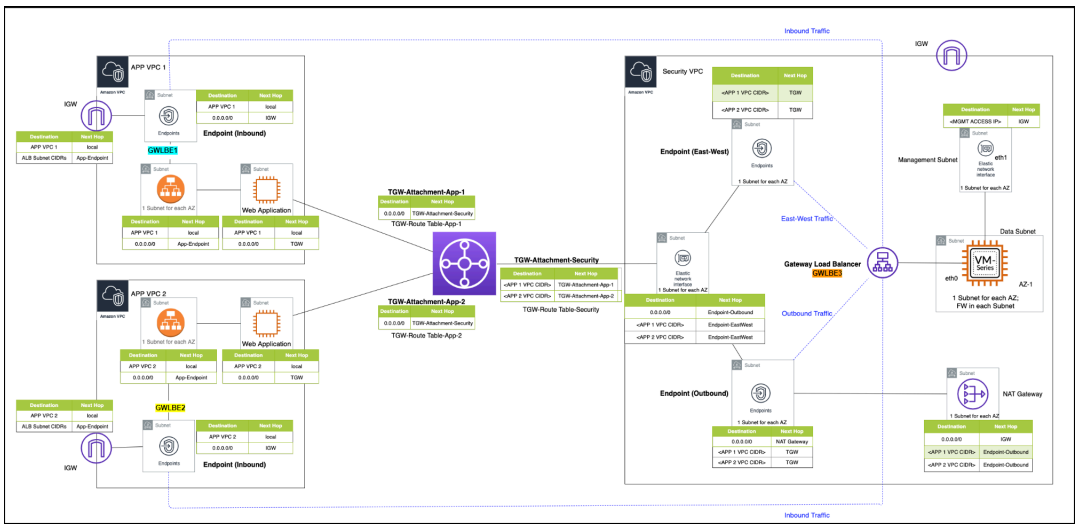
VM-Series 與 AWS 閘道負載平衡器整合

AWS 閘道負載平衡器 (GWLB) 是 AWS 管理的服務，可讓您部署 VM-Series 防火牆堆疊，並以水平擴展和容錯方式運作。然後，您可以將 AWS GWLB 搭配防火牆堆疊公開為 VPC 端點服務，以檢查流量和防禦威脅。您可以為 VPC 端點服務建立閘道負載平衡器端點 (GWLBE)，以輕鬆地在應用程式的輸出、東西向和輸入流量中，插入自動調整規模的 VM-Series 防火牆堆疊。VM-Series 防火牆和 GWLB 使用 GENEVE 封裝，讓流量封包標頭和承載保持不變，以便應用程式完整看到來源的識別。

在轉送和輸入使用案例中，*VM-Series* 防火牆部署在 *GWLB* 後方時支援解密，包括使用 *DHE/ECPHE* 密碼的 *TLS1.2* 和 *TLS1.3*。

在 *GWLB* 後方部署 *VM-Series* 防火牆需要您設定 AWS 傳輸閘道。

下圖說明 GWLB 與 VM-Series 整合如何簡化 AWS 傳輸閘道 (TGW) 環境。您將中央安全性 VPC 連接至傳輸閘道。中央安全性 VPC 包含 GWLB，可將 VM-Series 防火牆堆疊調整規模和平衡流量負載。



為了確保 VM-Series 防火牆可以檢查 VPC 連接之間路由的流量，您必須在 VM-Series 防火牆所在安全性 VPC 的傳輸閘道 VPC 連接上，啟用設備模式。您可以使用以下命令啟用設備模式：

```
modify-transit-gateway-vpc-attachment --transit-gateway-attachment-id
 <value> --options ApplianceModeSupport=enable
```

如需詳細說明，請參閱啟用設備模式。

這可確保對稱地路由雙向流量—要求與回應流量都導向至防火牆 VPC 中相同的閘道端點，GWLB 會維持固定導向至相同的 VM-Series 防火牆來檢查，之後再繼續到正確目的地。

搭配 GWLB 來部署時，您可以使用 VM-Series 防火牆來保護：

- 輸入流量—源自 VPC 外部並前往應用程式 VPC 之內資源（例如 Web 伺服器）的流量。在 AWS 安全性群組所允許流量中，VM-Series 防火牆會防止惡意軟體和弱點進入網路。

©2023 Palo Alto Networks, Inc.

- 輸出流量—源自應用程式 VPC 並前往網際網路上外部資源的流量。VM-Series 防火牆確保應用程式 VPC 中的工作負載連接至允許的服務（例如 Windows Update）和允許的 URL 類別，並防止敏感資訊的資料外洩，以保護輸出流量。此外，在傳回流量中，VM-Series 安全性設定檔會防止惡意軟體和弱點進入網路。
- 東西向流量—在傳輸閘道環境中，東西向流量是指 VPC 間的流量，例如兩個不同應用程式 VPC 中的來源和目的地工作負載之間的流量。VM-Series 防火牆會保護東西向流量免於惡意軟體傳播。

若要保護傳往您的應用程式 VPC 的輸入流量：

1. 建立 GWLBE 端點（上圖中的 GWLBE1 和 GWLBE2），在您的分支 VPC 中關聯單獨的子網路。確保您在應用程式 VPC 中對 GWLB 終端節點、ALB 以及應用程式和傳輸閘道附件具有單獨的子網路。
2. 在應用程序 VPC 中新增路由表（除了 VPC 本地路由之外），如下所示：
   1. 具有 IGW 邊緣關聯的路由表 - 新增以 ALB 為目的地的路由，目標為 GWLBE。
   2. 具有 ALB 子網路關聯的路由表 - 新增以 0.0.0.0/0 為目的地的路由，目標為 GWLBE。
   3. 具有 GWLBE 子網路關聯的路由表 - 新增以 0.0.0.0/0 為目的地的路由，目標為 IGW。

具備這些路由後，到達 VPC IGW 的輸入流量就會被路由到 GWLBE。GWLBE 將流量轉送到 GWLB，而 GWLB 又會將流量傳送到安全 VPC 中的 VM-Series 防火牆進行檢查。防火牆將請求流量傳送回應用程式 VPC GWLBE，而後者會透過 ALB 將流量轉送到應用程式。對此請求的回應流量由 ALB 傳送到應用程式 GWLBE，而後者會將流量傳送到 GWLB。而 GWLB 又會將流量傳送到 VM-Series 防火牆。檢查回應流量後，防火牆將回應流量傳送回應用程式 VPC GWLBE，而後者會將流量傳送到 IGW。

若要保護應用程式 VPC 的輸出流量：

1. 在集中式防火牆 VPC 中建立一個GWLBE（上圖中的GWLBE3）。確保您在應用程式 VPC 中對 GWLB 終端節點、傳輸閘道附件和安全性 VPC 內的 NAT 閘道具有單獨的子網路。
2. 在安全性 VPC 中建立 NAT 閘道。

©2023 Palo Alto Networks, Inc.

3. 新增路由表如下：
   1. 具有應用程式子網路關聯的路由表 - 新增以 0.0.0.0/0 為目的地的路由，目標為 TGW。這是對 VPC 本地路由的補充。
   2. 安全性 VPC 中的路由表：
      - 與 TGW 附件子網路關聯的路由表 - 除了 VPC 本地路由外，再新增以 0.0.0.0/0 為目的地的路由，目標為 GWLBE3。
      - 與 GWLBE 子網路關聯的路由表 - 除了 VPC 本地路由外，再新增以 0.0.0.0/0 為目的地的路由，目標為 NAT 閘道。新增以應用程式 VPC CIDR 為目的地，且以 TGW 為目標的路由。
      - 與 NAT 閘道子網路關聯的路由表 - 除了 VPC 本地路由外，再新增以 0.0.0.0/0 為目的地的路由，目標為 IGW。新增以應用程式 VPC CIDR 為目的地，且以 GWLBE3 為目標的路由。
   3. 新增傳輸閘道路由表，如下所示：
      - 具有 App1-1 VPC TGW-Attachment 關聯的路由表 - 新增以 0.0.0.0/0 為目的地，且附件 ID 為安全性 VPC TGW 附件的路由。
      - 具有 App2-2 VPC TGW-Attachment 關聯的路由表 - 新增以 0.0.0.0/0 為目的地，且附件 ID 為安全性 VPC TGW 附件的路由。
      - 具有安全性 VPC TGW-Attachment 關聯的路由表 - (a) 新增以 App-1 VPC CIDR 為目的地，且附件 ID 為 Application-1 VPC TGW 附件的路由。 (b) 新增以 App-2 VPC CIDR 為目的地，且附件 ID 為 Application-2 VPC TGW 附件的路由。

   具備此配置後，從 Application (App1) 發起的輸出流量被傳送到 TGW，而 TGW 會將其轉送到安全性 VPC 子網路。然後，流量被路由到安全性 GWLBE(GWLBE3)，後者將流量傳送到 VM-Series 防火牆，以透過 GWLB 進行檢查。VM-Series 防火牆在檢查後將流量傳送回 GWLBE3，而 GWLBE3 將流量轉送到透過 IGW 傳送流量的 NAT 閘道。同樣地，回應流量通過 NAT 閘道到達 GWLBE3、VM-Series 防火牆和 TGW，然後再路由回應用程式。

   東西向流量也是透過上述步驟中描述的路由和設定進行管理。當流量從 App1 傳送到 App2 時，流量通過 TGW，而 TGW 又將流量路由到 GWLBE3。GWLBE3 通過 GWLB 將流量轉送到 VM-Series 防火牆。VM-Series 防火牆在檢查後將封包傳送回 GWLBE3。GWLBE3 然後通過 TGW 將封包轉送給 App2。從 App-2 到 App-1 的回應流量將採用反轉路徑。

   建議將所有子網路都放置在同一個 AZ，避免跨區域流量費用。

手動整合 VM-Series 與閘道負載平衡器

請參閱下列主題，以手動整合 VM-Series 防火牆與 AWS 閘道負載平衡器。

- 啟用 VM-Series 與閘道負載平衡器整合
- 手動整合 VM-Series 與閘道負載平衡器
- （選用）將 VPC 端點與 VM-Series 介面建立關聯
- （選用）對 AWS 上的 VM-Series 啟用覆疊路由

©2023 Palo Alto Networks, Inc.

啟用 VM-Series 與閘道負載平衡器整合

整合 VM-Series 防火牆與 GWLB 時，首先必須讓 VM-Series 防火牆能夠處理 GWLB 端點重新導向至防火牆的流量。您可以使用 VM-Series 防火牆 CLI、透過 VM-Series 啟動載入套件或 AWS 主控台的使用者資料欄位來啟用此功能。

VM-Series 防火牆部署搭配 GWLB 需要：

- PAN-OS 10.0.2 或更新版本
- VM-Series 外掛程式 2.0.2 或更新版本
- Panorama 10.0.2 或更新版本（如果您使用 Panorama 來管理防火牆）

下表列出啟用和 VPC 端點的 GWLB 流量檢查所需的命令。操作命令可用於啟動載入 init-cfg.txt 檔案中，或 AWS 主控台的使用者資料欄位中。

啟動程序參數	CLI 命令	說明
op-command-modes=mgmt-interface-swap	op-command-modes=mgmt-interface-swap 此命令需要防火牆重新啟動之後才會生效。	交換 eth0 和 eth1。預設情況下，GWLB 僅會將流量傳送到其目標實例的 Eth0。兩者交換後，Eth0 會變成資料介面，而 eth1 會變成管理介面。
plugin-op-commands=aws-gwlb-inspect:enable	request plugins vm_series aws gwlb inspect enable <yes/no>	使 VM-Series 防火牆能夠處理通過 GWLB 的流量。

手動整合 VM-Series 與閘道負載平衡器

請完成下列程序，手動整合 AWS 上的 VM-Series 防火牆與 GWLB。

如果您在啟動載入時透過使用者資料將 *VPC* 端點與介面或子介面建立關聯，但 *bootstrap.xml* 檔案未包含介面設定，您可以在防火牆啟動之後設定介面。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

©2023 Palo Alto Networks, Inc.

STEP 1 | 設定安全性 VPC。如需有關建立安全性 VPC 的詳細資訊，請參閱 AWS 文件。

- 建立兩個子網路：一個用於管理，另一個用於資料。
- 建立兩個安全性群組：一個用於防火牆管理，另一個用於資料。
- 管理子網路安全性群組應該允許管理存取使用 https 和 ssh。
- 請確保資料 VPC 中的安全性群組允許 GENEVE 封裝的封包（UDP 連接埠 6081）。
- 如果部署包括傳輸閘道和 VPC 之間移動的流量，您必須在安全性 VPC 連接上啟用設備模式。



GWLB 的目標群組無法使用 *HTTP* 來檢查健康情況，因為 *VM-Series* 防火牆不允許以不安全的通訊協定來存取。請改用 *HTTPS* 或 *TCP* 之類的其他通訊協定。

©2023 Palo Alto Networks, Inc.

STEP 2 | 啟動 VM-Series 防火牆。

1. 在 EC2 儀表板中，按一下 **Launch Instance**（啟動實例）。
2. 選擇 Palo Alto VM-Series AMI。若要取得 AMI，請參閱取得 AMI。
3. 在 EC2 實例上啟動 VM-Series 防火牆。

   1. 選取 **EC2 instance type**（**EC2** 實例類型），以配置防火牆所需的資源，然後按 **Next**（下一步）。如需瞭解最低資源需求，請參閱VM-Series 系統需求。
   2. 選取安全性 VPC。
   3. 選取資料子網路以連接至 eth0。
   4. 為 eth1 新增另一個網路介面，作為介面交換之後的管理介面。交換介面需要最少兩個 ENI（eth0 及 eth1）。

      - 展開 [Network Interfaces（網路介面）] 區段，然後按一下 **Add Device**（新增裝置），以新增其他網路介面並設定該介面的管理子網路。

        確定 VPC 設置多個子網路，以便在啟動時可新增其他 ENI。

        如果您啟動的防火牆只有一個 *ENI*：

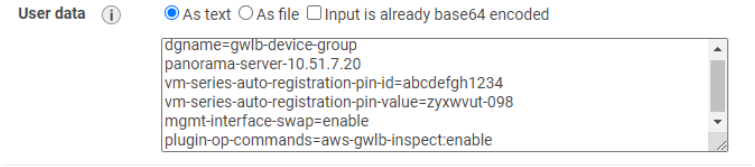
        - 介面交換命令會導致防火牆以維護模式啟動。
        - 新增第二個 *ENI* 時必須重新啟動防火牆。

      - 展開 [Advanced Details（進階詳細資料）] 區段，然後在 **User Data**（使用者資料）欄位中以文字輸入，以在啟動期間執行介面交換。

        `mgmt-interface-swap=enable`

        `plugin-op-commands=aws-gwlb-inspect:enable`

        如果您將目標類型設為 *VM-Series* 防火牆上特定介面的 *IP* 位址，則不需要啟用管理介面交換。

   5. 接受預設的 **Storage**（儲存區）設定。防火牆會使用磁碟區類型 SSD (gp2)。
   6. 若出現提示，請為您的設定選取適當的 **SSD** 選項。
   7. （選用）**Tagging**（加標籤）。新增一個或多個標籤，建立您自己用於識別中繼資料，並對 VM-Series 防火牆分組。例如，新增一個 **Name**（名稱）標籤，附帶可幫助您記住在此 VM-Series 防火牆上交換的 ENI 介面的 **Value**（值）。
   8. 為 eth0（資料介面）選取資料 **Security Group**（安全性群組）。在 UDP 連接埠 6081 上啟用流量。

      如果您對防火牆啟用健康情況檢查，則無法使用 HTTP。請改用 HTTPS 或 TCP 之類的其他通訊協定。

©2023 Palo Alto Networks, Inc.

9. 選取 **Review and Launch**（複查並啟動）。複查以確定您的選取是正確的，然後按一下 **Launch**（啟動）。
10. 選取現有的金鑰配對或建立新的金鑰配對，並同意金鑰免責聲明。

    首次存取防火牆時，需要金鑰配對。此外在維護模式中存取防火牆時，也需要金鑰配對。

11. 下載私人金鑰並儲存至安全的位置；副檔名為 `.pem`。此金鑰如果遺失，您無法重新產生此金鑰。

    需要 5-7 分鐘才能啟動 VM-Series 防火牆。您可以在 EC2 儀表板上檢視進度。程序完成時，VM-Series 防火牆會出現在 EC2 儀表板上的 **Instances**（實例）頁面。

STEP 3 | 將管理安全性群組連接至 eth1（管理介面）。允許 ssh 和 https。如需詳細資訊，請參閱 AWS 文件。

STEP 4 | 建立彈性 IP 位址 (EIP) 並指派給用於防火牆管理存取 (eth1) 的 ENI。

1. 選取 **Elastic IPs**（彈性 **IP**），然後按一下 **Allocate New Address**（配置新位址）。
2. 選取 **EC2-VPC**，然後按一下 **Yes, Allocate**（是，配置）。
3. 選取新配置的 EIP，然後按一下 **Associate Address**（建立位址關聯）。
4. 選取 **Network Interface**（網路介面）和與管理介面關聯的 **Private IP address**（私人 **IP** 位址），然後按一下 **Yes, Associate**（是，建立關聯）。

STEP 5 | 設定防火牆的新管理密碼。

在 *VM-Series* 防火牆 *CLI* 上，您必須先設定唯一的管理密碼，才能存取防火牆的 *Web* 介面。若要登入 *CLI*，您需要用於啟動防火牆的私密金鑰。

1. 使用 EIP 透過 SSH 進入 VM-Series 防火牆的 Command Line Interface（命令列介面 - CLI）。需要上述您使用或建立的私人金鑰，並以使用者名稱 **admin** 來存取 CLI。

   如果使用 PuTTY 進行 SSH 存取，您必須將 .pem 格式轉換為 .ppk 格式。請參閱 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html
2. 輸入下列命令登入防火牆：

   ssh -i <*private_key.pem*> admin@<*public-ip_address*>
3. 使用下列命令設定新密碼，並依照畫面上的提示進行：

   configure

   set mgt-config users admin password
4. 如果有需要啟動的 BYOL，請設定 DNS 伺服器 IP 位址，以便防火牆可存取 Palo Alto Networks 授權伺服器。輸入下列命令設定 DNS 伺服器 IP 位址：

   set deviceconfig system dns-setting servers primary <*ip_address*>
5. 使用下列命令提交變更：

   commit
6. 終止 SSH 工作階段。

©2023 Palo Alto Networks, Inc.

STEP 6 | 將資料平面網路介面設定為防火牆上的第三層介面。

在 *VPC* 內的應用程式伺服器上，將防火牆的資料背板網路介面定義為預設的閘道。

1. 使用 Web 瀏覽器中的安全連線 (https)，在初始設定期間使用您指派的 EIP 位址和密碼登入 (https://<Elastic_IP address>)。您將看見憑證警告；此為正常現象。繼續開啟網頁。
2. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）。
3. 按一下 **Ethernet 1/1** 的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：**Layer3**
   - 在 **Config**（設定）頁籤上，將介面指派給預設虛擬路由器。
   - 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。定義一個新區域並將其餘欄位保留為預設值，然後按一下 **OK**（確定）。
   - 在 **IPv4** 頁籤上，選取 **DHCP Client**（**DHCP** 用戶端）。

     如果使用 DHCP，請選取 **DHCP Client**（**DHCP** 用戶端）；將會自動取得您指派給 AWS 管理主控台中 ENI 的私人 IP 位址。
   - 在 [Advanced（進階）] 頁籤上，建立管理設定檔以啟用 HTTP 服務作為管理設定檔建立的一部分，並允許來自 GWLB 的健康情況檢查探查。
4. 按一下 **Commit**（交付）。確認介面的連結狀態為啟動。

STEP 7 | 建立安全性政策以允許/拒絕流量。

因為 *VM-Series* 與 *GWLB* 整合時會將流量視為內部網路區，所以預設內部網路區規則會允許所有流量。對於不符合其他任何安全性政策規則的流量，最佳做法以拒絕動作取代預設內部網路區規則。

1. 在防火牆的網頁介面上，選取 **Policies**（政策） > **Security**（安全性）。
2. 按一下 **Add**（新增），然後指定您想要執行的安全性地區、應用程式及日誌記錄選項，以限制和稽核周遊網路的流量。

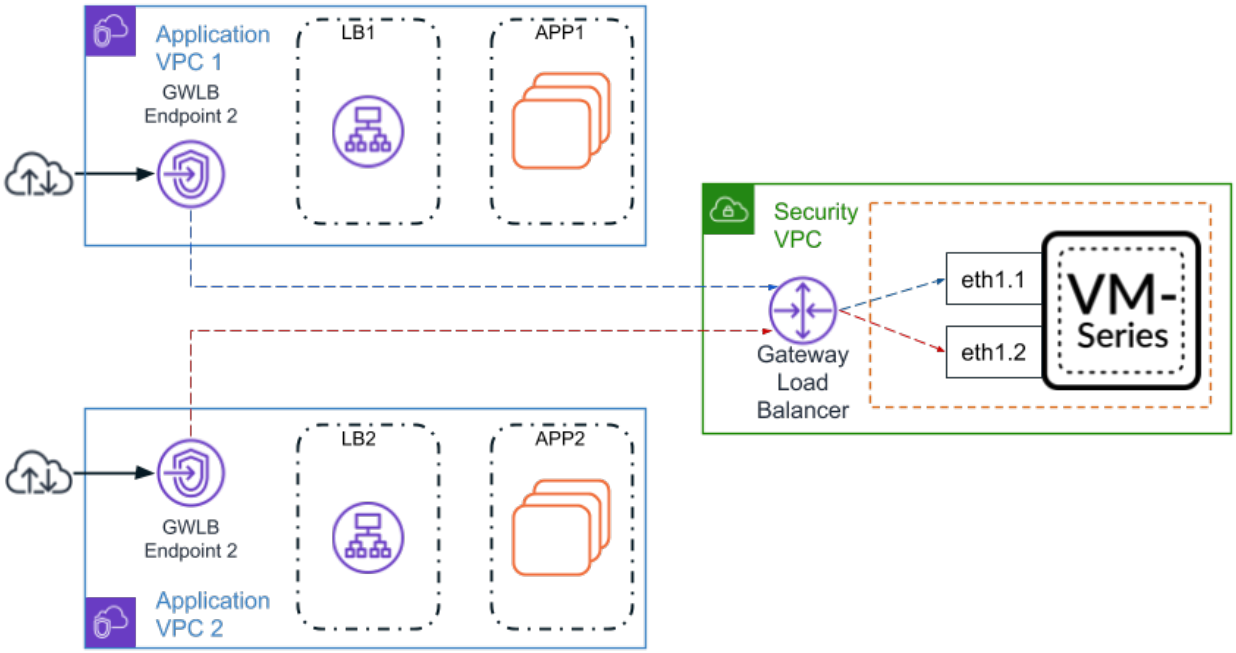
STEP 8 | 在防火牆 **Commit**（提交）變更。

將 VPC 端點與 VM-Series 介面建立關聯

您可以將一或多個 VPC 端點與 VM-Series 防火牆的介面或子介面建立關聯。您可以將單一 VPC 中的所有端點與防火牆上的相同子介面建立關聯，以一致地強制執行政策。或者，如果部署中的 VPC 有重疊的 IP 位址，您可以將不同 VPC 中的端點與不同子介面建立關聯，以差別地強制執行政策。

整合 *VM-Series* 防火牆與 *GWLB* 並不一定要將 *VPC* 與介面或子介面建立關聯。

©2023 Palo Alto Networks, Inc.



您可以使用下列方法設定介面並將 VPC 與防火牆介面建立關聯：

- 將介面設定加入 **bootstrap.xml** 檔案中，將關聯命令納入為 **init-cfg.txt** 檔案或 AWS 使用者資料的一部分。
- 部署防火牆之後，手動設定介面，並使用防火牆 CLI 將 VPC 與介面建立關聯。

您可以將多個 VPC 端點與 VM-Series 防火牆的單一介面建立關聯。不過，您必須將每個 VPC 端點個別地建立關聯。例如，若要將 VPC 端點 1 和 VPC 端點 2 與子介面 ethernet1/1.2 建立關聯，您必須針對每個 VPC 端點個別地執行關聯命令。

下表說明用來將 VPC 與介面建立關聯的命令。您可以將操作命令加入 **init-cfg.txt** 檔案或 AWS 使用者資料中。

啟動程序參數	CLI 命令	說明
plugin-op-commands= aws-gwlb-associate-vpce:<vpce-id>@ethernet<subinterface>	request plugins vm_series aws gwlb associate vpc-endpoint <vpce-id> interface <subinterface>	將 VPC 端點與防火牆上的介面或子介面建立關聯。指定的介面會指派給安全性地區。
—	request plugins vm_series aws gwlb disassociate vpc-endpoint <vpce-id> interface <subinterface>	將 VPC 端點與防火牆上的介面或子介面取消關聯。指定的介面會指派給安全性地區。
—	show plugins vm_series aws gwlb	顯示與 GWLB 部署有關的防火牆操作狀態。不會顯示防火牆設定。

©2023 Palo Alto Networks, Inc.

啟動程序參數	CLI 命令	說明
		例如，如果與不存在的介面設定關聯，雖然會設定關聯，但不會成為操作狀態的一部分。因此不會顯示。

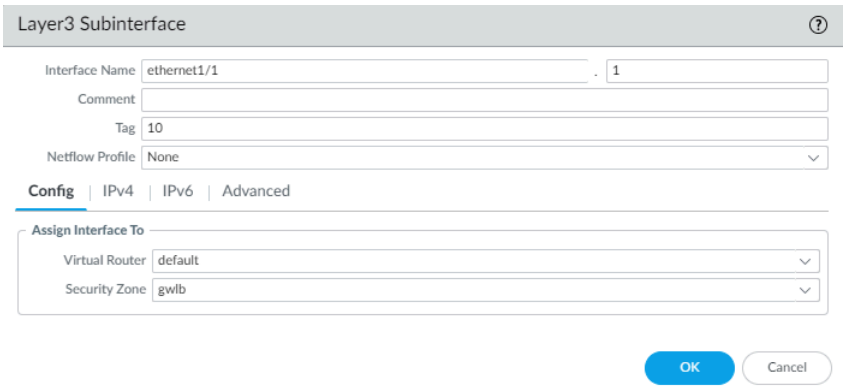
當使用啟動載入 init-cfg.txt 檔案或 AWS 使用者資料，與 VPC 建立關聯時，您可以同時列出多個介面或子介面。所有命令必須以逗號分隔清單形式自成一行，不能有空格，如下列範例所示。

```
plugin-op-commands=aws-gwlb-inspect:enable,aws-gwlb-associate-
vpce:vpce-0913731043b5c0ebc@ethernet1/1.1,aws-gwlb-associate-
vpce:vpce-08207ccb4cb23a1de@ethernet1/1.1,aws-gwlb-associate-
vpce:vpce-07b66cca88821d6e1@ethernet1/1.2,aws-gwlb-associate-
vpce:vpce-0a9a583fdb928492b@ethernet1/1.3
```

如果您使用子介面來分隔流量，請為每個 VPC 建立子介面，並將子介面與 VPC 建立關聯。

STEP 1 | 設定子介面。

1. 登入防火牆 Web 介面。
2. 選取 **Network**（網路） > **Interface**（介面）。
3. 反白顯示 **ethernet1/1**，然後按一下 **Add Subinterface**（新增子介面）。
4. 輸入用來識別子介面的數值尾碼（1 至 9,999）。
5. 輸入子介面的 **VLAN Tag**（**VLAN** 標籤）（1 至 4,094）。此欄位為必填，但不使用 VLAN。
6. 選取 **Virtual Router**（虛擬路由器）作為預設值。
7. 選取 **Security Zone**（安全性區域）。
8. 在 **IPv4** 頁籤上，將 **Type**（類型）設定為 **DHCP Client**（**DHCP** 用戶端）。
9. 按一下 **OK**（確定）。
10. 針對每個 VPC 端點重複此命令。



©2023 Palo Alto Networks, Inc.

STEP 2 | 將介面與 VPC 端點建立關聯。

1. 登入防火牆 CLI。
2. 執行下列命令：

   request plugins vm_series aws gwlb associate vpc-endpoint <vpce-id> interface <subinterface>

   例如：

   request plugins vm_series aws gwlb associate vpc-endpoint vpce-02c4e6g8ha97h7e39 interface ethernet1/1.4

   您可以在 *AWS* 主控台找到 *VPC* 端點 *ID*。

3. 針對每個介面和 VPC 端點關聯，重複此命令。

STEP 3 | 驗證介面與 VPC 端點關聯。

show plugins vm_series aws gwlb

```
啟用 GWLB: True 覆疊路由: False
 ------------------------------------------------------------------ VPC
 endpoint Interface
 ------------------------------------------------------------------
 vpce-0aeb1a919bd4ae609 ethernet1/1.1 vpce-0294375bfe413f04a
 ethernet1/1.2
```

STEP 4 | 如有必要，您可以使用下列命令，取消 VPC 端點與介面的關聯。

request plugins vm_series aws gwlb disassociate vpc-endpoint <vpce-id> interface <subinterface>

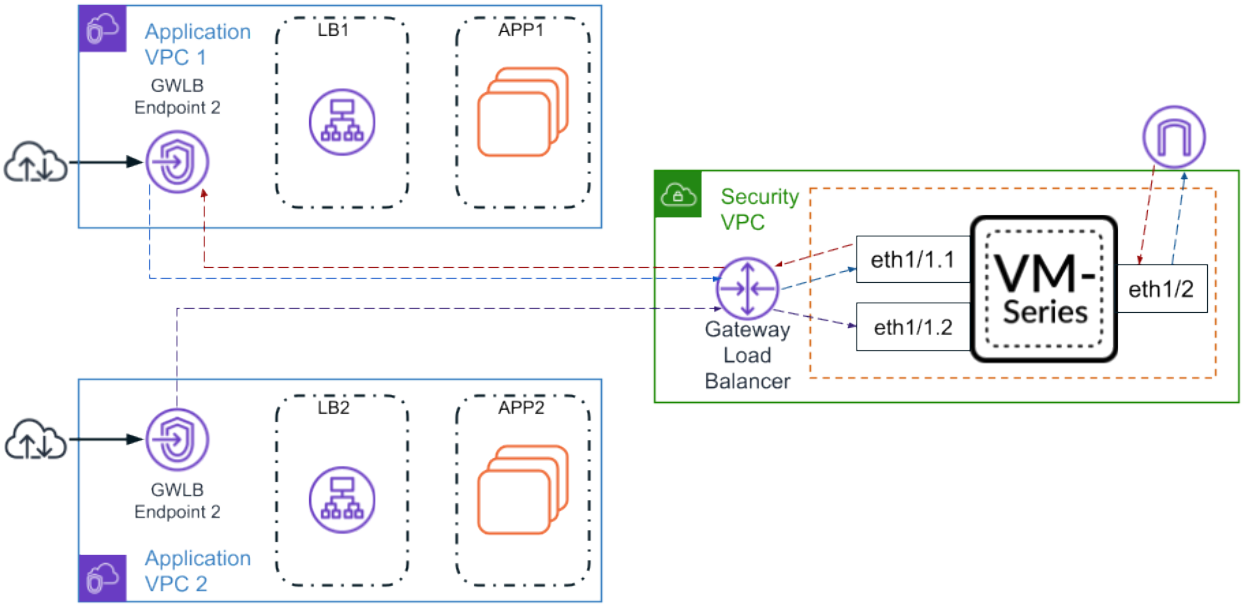
對 AWS 上的 VM-Series 啟用覆疊路由

覆疊路由需要 *PAN-OS 10.0.5* 或更新版本。

AWS GWLB 在 VM-Series 防火牆整合中使用覆疊路由，可讓您使用雙區域政策來檢查離開（輸出）AWS 環境的流量。這可讓封包從不同於進入時的介面離開 VM-Series 防火牆。

設定覆疊路由時，防火牆可以執行第 3 層路由查閱，查詢封包的內部標頭。如果目的地與進入介面相同，封包會正常導向。工作階段中的所有未來封包都視為 vwire，就好像未啟用覆疊路由一樣。如果封包要移至輸出目的地，防火牆會將封包解封，並將封包轉送至 IGW 或 NAT 閘道。封包傳回時，防火牆會重新套用封裝。

©2023 Palo Alto Networks, Inc.



使用下列程序來啟用覆疊路由。

STEP 1 | 開始之前，請確定您為信任和不受信任的介面建立不同的子網路。

STEP 2 | 手動整合 VM-Series 與閘道負載平衡器。

STEP 3 | （選用）將 VPC 端點與 VM-Series 介面建立關聯。

STEP 4 | 使用覆疊路由 CLI 命令。如果您在 AWS 使用者資料或 init-cfg.txt 啟動程序檔案中包含覆疊路由 op-command，則不需要此 CLI 命令。

1. 登入防火牆命令列介面。
2. 執行下列命令。

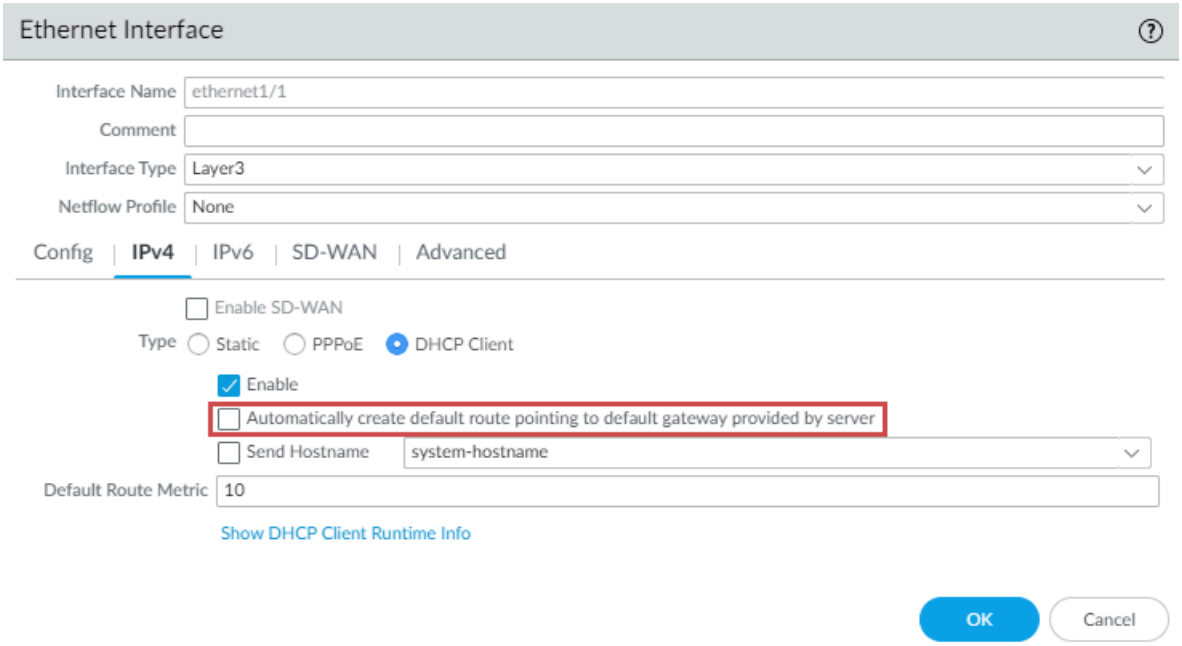
```
request plugins vm_series aws gwlb overlay-routing enable yes
```

STEP 5 | 登入防火牆 Web 介面。

©2023 Palo Alto Networks, Inc.

STEP 6 | 在信任（進入）介面上，停用 **Automatically create default route pointing to default gateway provided by server**（自動建立預設路由來指向伺服器所提供的預設閘道）。

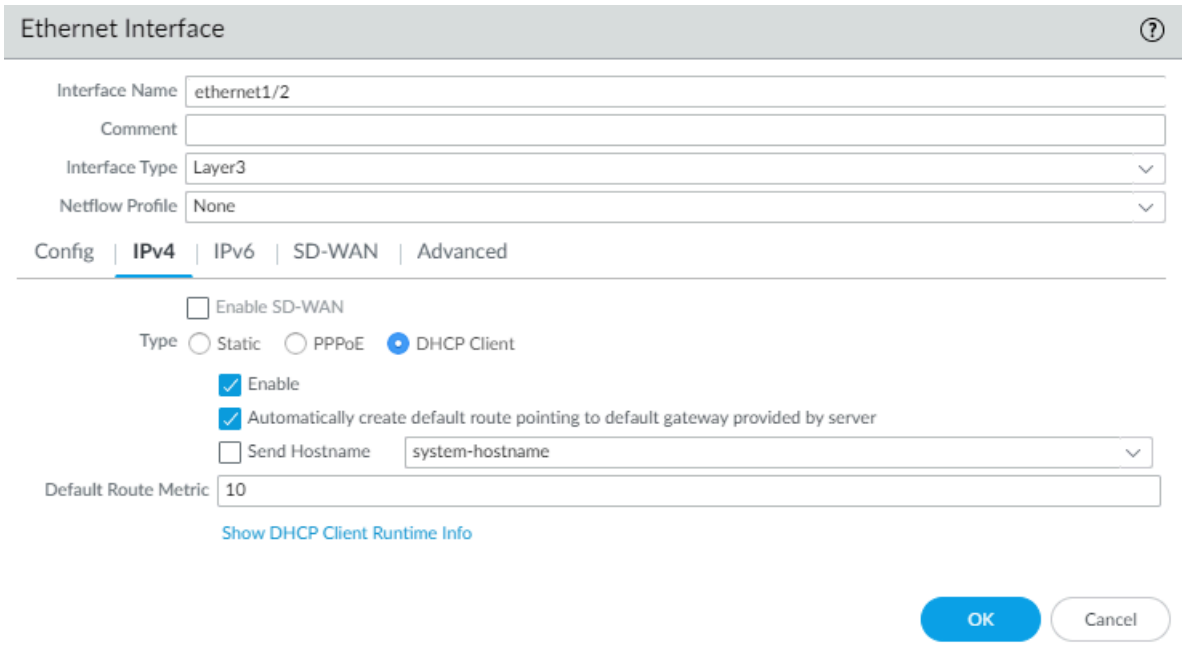
1. 選取 **Network**（網路） > **Interfaces**（界面） > **Ethernet**（乙太網路）。
2. 按一下您的信任介面，然後按一下 [IPv4] 頁籤。
3. 取消勾選 **Automatically create default route pointing to default gateway provided by server**（自動建立預設路由來指向伺服器所提供的預設閘道）。
4. 按一下 [OK（確定）]。



©2023 Palo Alto Networks, Inc.

STEP 7 | 設定介面乙太網路 1/2。

1. 選取 **Network**（網路） > **Interfaces**（界面） > **Ethernet**（乙太網路）。
2. 選取 **Interface Type**（介面通道）—**Layer 3**（第三層）。
3. 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。此區域將作為不受信任的區域，並從安全性 VPC 導出輸出流量。定義新區域，例如 VM-Series-untrust，然後按一下 **OK**（確定）。
4. 在 **IPv4** 頁籤上，選取 **DHCP Client**（**DHCP** 用戶端）。
5. 選取 **Automatically create default route pointing to default gateway provided by server**（自動建立預設路由來指向伺服器所提供的預設閘道）。
6. 按一下 **OK**（確定）。



©2023 Palo Alto Networks, Inc.

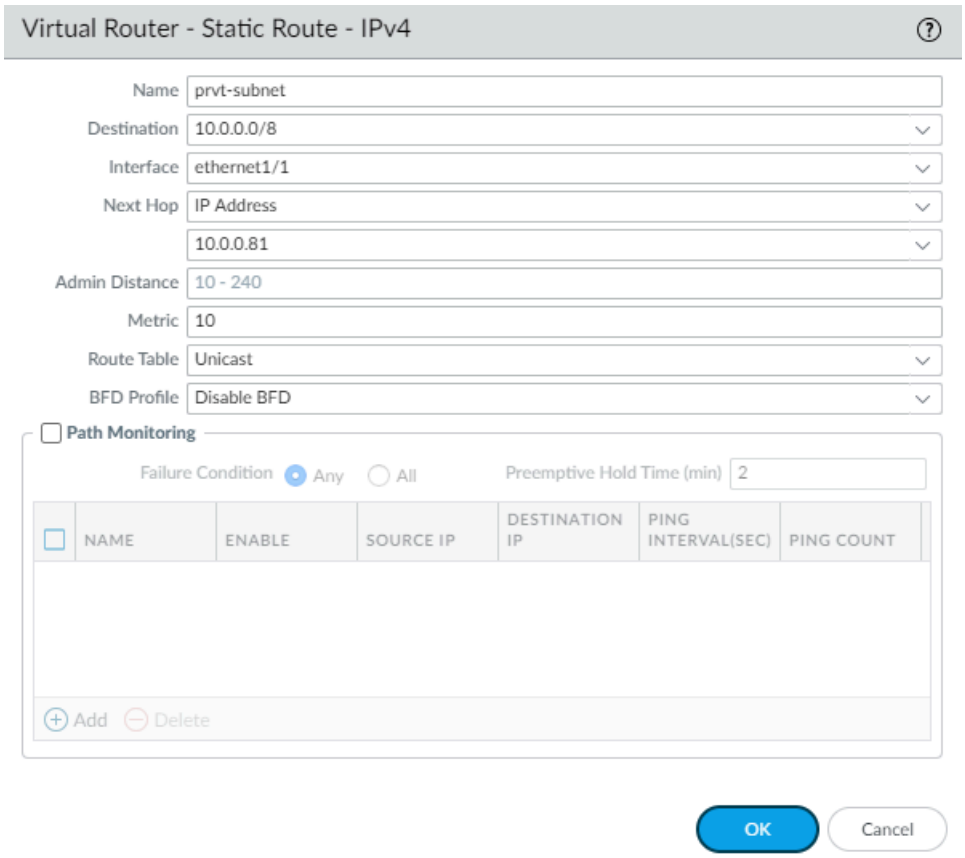
STEP 8 | 設定虛擬路由器。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器） > **Add**（新增）。
2. 輸入虛擬路由器的描述性 **Name**（名稱）。
3. 在 **Interfaces**（介面）下，**Add**（新增）Ethernet1/1、Ethernet1/1 下的任何子介面，以及 Ethernet1/2。
4. 按一下 **Static Routes**（靜態路由） > **Add**（新增）。
   1. 輸入靜態路由的描述性名稱。
   2. 對於 **Destination**（目的地），輸入應用程式 VPC 子網路的私有 IP 位址。
   3. 從 **Interface**（介面）下拉式清單中，選取信任（進入）介面。
   4. 對於 **Next Hop**（下一個躍點），選取 [IP Address（IP 位址）]，然後輸入信任介面的閘道 IP 位址。您可以在 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路） > **Dynamic-DHCP Client**（動態-DHCP 用戶端）上找到閘道 IP 位址。



   5. 按一下 **OK**（確定）。

©2023 Palo Alto Networks, Inc.



5. 確保靜態路由可以到達部署中的所有應用程式 VPC。您可以建立一些大型彙總路由（涵蓋所有 RFC1918）或應用程式 VPC 特定路由。如果您使用子介面，則不需要路由返回子介面。輸出檢查只會尋找相符的介面，而不是相符的子介面。
6. 按一下 **OK**（確定）。

STEP 9 | 為流量輸出 Ethernet1/2 建立 NAT 政策。

1. 選取 **Policies**（政策） > **NAT** > **Add**（新增）。
2. 輸入 NAT 政策規則的描述性 **Name**（名稱）。
3. 從 **NAT Type**（**NAT** 類型）下拉式清單中，選取 **ipv4**。
4. 在 **Original Packet**（原始封包）頁籤上，將 **Source Zone**（來源區域）設定為 any，將 **Destination Zone**（目的地區域）設定為不受信任的（輸出）區域。
5. 在 **Translated Packet**（轉譯的封包）頁籤上，設定下列參數。
   - Translation Type（轉譯類型）：Dynamic IP and Port （動態 IP 及連接埠）
   - 位址類型：介面位址
   - Interface（介面）：從下拉式清單中選取不受信任的（輸出）連接埠。
   - IP 位址：無
6. 按一下 **OK**（確定）。

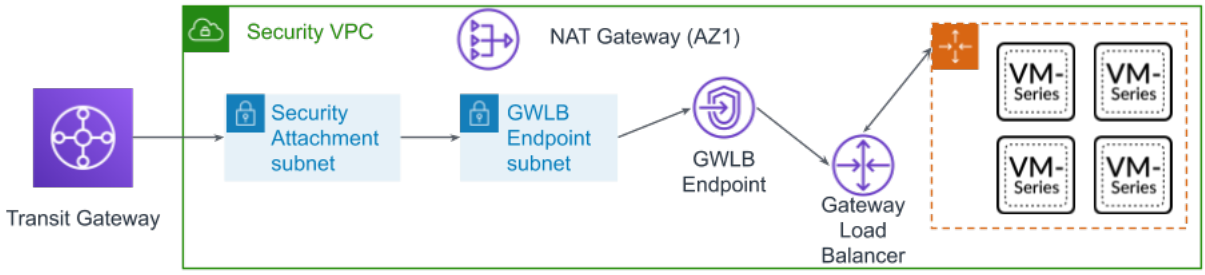
STEP 10 | **Commit**（提交）您的變更。

©2023 Palo Alto Networks, Inc.

VM-Series 自動調整規模群組與 AWS 閘道負載平衡器

Palo Alto Networks 的 AWS 專用自動調整規模範本協助您整合和設定 VM-Series 防火牆與 GWLB，以保護部署於 AWS 中的應用程式。此範本利用 AWS 可擴充性功能，獨立自動地調整 AWS 中所部署 VM-Series 防火牆的規模，以應付應用程式工作負載資源激增的需求。

這些是社群支援的範本。



此解決方案提供安全性 VPC 範本和應用程式範本。安全性 VPC 範本針對每個可用性區域，部署 VM-Series 防火牆自動調整規模群組、GWLB、GWLBE、GWLBE 子網路、安全性連接子網路，以及 NAT 閘道。請從 Palo Alto Networks GitHub 儲存庫下載 CloudFormation 範本。

與 AWS GWLB 整合的 VM-Series 自動調整規模範本包含下列建置區塊：

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

建置區塊	說明
PAN Components（PAN 元件）	· 執行 10.0.2 或更新版本的 Panorama · PAN-OS 10.0.2 或更新版本 · Panorama 上安裝的 VM-Series 外掛程式 2.0.2 或更新版本
防火牆範本 （社群支援的範本）	根據您選擇的可用性區域 (AZ) 數量，`firewall-new-vpc-v3.0.template` 會部署下列項目： 範本最多支援四個 AZ。 · 用於 Lambda 管理、傳輸閘道連接、GWLB 端點和 NAT 閘道的子網路，以及信任子網路。 · 每個子網路的路由表 · 傳輸閘道連接和路由表 · NAT 和網際網路閘道 · 每個 AZ 各一個自動調整規模群組（具有一個 VM-Series 防火牆）。 · 每個 AZ 各一個 GWLB 和一個 GWLB 端點。

©2023 Palo Alto Networks, Inc.

建置區塊	說明
	防火牆範本的 VPC CIDR 應該大於 /23。 由於生產環境中的諸多變化，包括（但不限於）子網路、可用性區域、路由表、安全性群組等若干元件。您必須在新的 VPC 中部署 `firewall-new-vpc-v3.0.template`。  *AWS 專用 VM-Series 自動調整規模範本不會部署傳輸閘道或 Panorama。啟動 firewall-new-vpc-v3.0.template 之前，您必須部署傳輸閘道和 Panorama。*
應用程式範本 （社群支援的範本）	根據您選擇的可用性區域 (AZ) 數量，`panw-aws-app-v3.0.template` 會部署下列項目：  範本最多支援四個 *AZ*。 · 用於 Lambda、傳輸閘道連接、GWLB 端點和應用程式負載平衡器的子網路。 · 每個子網路的路由表，以及與網際網路閘道相關聯的輸入路由表，用於將輸入流量導向至 GWLB 端點。 · 一個應用程式負載平衡器 · 一個網際網路閘道 · 每個 AZ 各一個自動調整規模群組（具有一個 Ubuntu 實例）。 應用程式範本的 VPC CIDR 應該大於 /23。  應用程式範本可當作範例來驗證安全性範本。
Lambda 功能	AWS Lambda 提供穩健的事件驅動自動化，不需要複雜的協調運作軟體。除了部署以上幾列所述的元件，`firewall-new-vpc-v3.0.template` 還會執行下列功能： · 在防火牆啟動或終止時新增或移除介面 (ENI)。 · 在您刪除堆疊或終止實例時刪除所有相關聯的資源。 · 在發生相應縮小事件時，將作為 Panorama 管理裝置的防火牆移除。 · 在相應縮小事件導致防火牆終止時停用授權。 · 定期監控傳輸閘道是否有新的連接或分離，並據以更新安全性 VPC 中的路由表。
啟動程序檔案 GitHub 儲存庫中提供的	此解決方案需要 init-cfg.txt 檔案和 bootstrap.xml 檔案，才能讓 VM-Series 防火牆有基本組態來處理流量。

©2023 Palo Alto Networks, Inc.

建置區塊	說明
bootstrap.xml 檔案僅供測試和評估。在生產部署中，您必須在啟動之前修改 bootstrap.xml 中的範例認證。	· **`init-cfg.txt`** 檔案包含 mgmt-interface-swap 操作命令，可讓防火牆在其主要介面 (eth0) 上接收資料平面流量。此自動調整規模解決方案需要交換資料平面介面和管理介面，以便應用程式 GWLB 將 Web 流量轉送至自動調整規模層的 VM-Series 防火牆。 · **`bootstrap.xml`** 檔案可啟用防火牆網路介面的基本連線，還可讓防火牆連接至 AWS CloudWatch 命名空間，而此命名空間符合您在啟動範本時所輸入的堆疊名稱。

如果您需要從 ***AWS*** 刪除這些範本，一定要先刪除應用程式範本。嘗試刪除防火牆範本會導致刪除失敗。

- 啟動範本之前
- 啟動防火牆範本
- 啟動應用程式範本

啟動範本之前

在啟動範本來整合 VM-Series 防火牆自動調整規模群組與 AWS GWLB 之前，您必須完成下列程序。

STEP 1 | 開始之前，請確定您已完成下列動作。

- 取得搭售包的驗證碼，該搭售包支援部署可能需要的防火牆數目。您必須將此授權碼儲存至名為 **`authcodes`** 的文字檔案（無副檔名），並將 **`authcodes`** 檔案放在啟動程序套件的 **`/license`** 資料夾中。
- 從 GitHub 儲存庫，下載啟動 VM-Series 閘道負載平衡器範本所需的檔案。
- 建立傳輸閘道。此傳輸閘道銜接安全性 VPC 與應用程式 VPC。
  - 請記下傳輸閘道 ID，稍後部署範本時需要用到。
  - 您必須將 0.0.0.0/0 路由新增至應用程式附件路由表，以指向安全性附件來保護東西向和輸出流量。
  - 確保 **Default route table association**（預設路由表關聯）和 **Default route table propagation**（預設路由表傳播）已停用。
- 對於防火牆範本和應用程式範本，建議的 VPC CIDR 應該大於 /23。

閘道 ***GWLB*** 的目標群組無法使用 ***HTTP*** 來檢查健康情況，因為 ***VM-Series*** 防火牆不允許以不安全的通訊協定來存取。請改用 ***HTTPS*** 或 ***TCP***。

STEP 2 | 部署執行 10.0.2 的 Panorama 並完成下列設定。

Panorama 必須允許 AWS 公共 IP 位址。VM-Series 防火牆會使用範本建立的 NAT 閘道外部 IP 位址來存取 Panorama。

©2023 Palo Alto Networks, Inc.

STEP 3 | 下載 VM-Series 外掛程式並安裝在 Panorama 上。

1. 選取 **Panorama** > **Plugins**（外掛程式），使用 **Check Now**（立即檢查）尋找新的外掛程式套件。VM-Series外掛程式名稱為 `vm_series`。
2. 查閱外掛程式版本資訊，以確定哪個版本會為您提供有用的升級。
3. 選取外掛程式版本，在 Action（動作）欄中選取 **Download**（下載）。
4. 按一下 Action（動作）欄中的 **Install**（安裝）。安裝完成時，Panorama 會通知您。
5. 要檢視外掛程式，選取 **Device**（裝置） > **VM-Series**（**VM-Series**）。

©2023 Palo Alto Networks, Inc.

STEP 4 | 設定範本。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Templates**（範本），然後按一下 **Add**（新增）。
   1. 輸入描述性的 **Name**（名稱）。
   2. 按一下 **OK**（確定）。
3. 設定 virtual router（虛擬路由器 - VR）。
   1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器）。
   2. 確定您已從 **Template**（範本）下拉式清單中選取您在上面建立的範本。
   3. 按一下 **Add**（新增）。
   4. 使用下列格式命名 virtual router（虛擬路由器 - VR）：VR-<tempstackname>。
   5. 在 virtual router（虛擬路由器 - VR）上啟用 ECMP。
   6. 按一下 **OK**（確定）。
4. 設定介面和建立區域。
   1. 選取 **Network**（網路） > **Interfaces**（介面），然後按一下 **Add Interface**（新增介面）。
   2. 選取 **Slot 1**（插槽 **1**），然後選取介面名稱（例如，乙太網路 1/1）。
   3. 將 **Interface Type**（介面類型）設為第三層。
   4. 在 **Config**（介面類型）頁籤上，從 **Security Zone**（安全性區域）下拉式清單中選取 **New Zone**（新區域）。在 Zone（區域）對話方塊中，定義新區域的 **Name**（名稱），例如網際網路，然後按一下 **OK**（確定）。
   5. 在 **Virtual Router**（虛擬路由器 **- VR**）下拉式清單中，選取您在上面建立的 virtual router（虛擬路由器 - VR）。
   6. 選取 **IPv4**，然後按一下 **DHCP Client**（**DHCP** 用戶端）。
   7. 按一下 **OK**（確定）。
5. 建立管理設定檔，以允許在上述建立的介面上以 HTTPS 支援健康情況檢查。
   1. 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **Interface Mgmt**（介面管理），然後按一下 **Add**（新增）。
   2. 選取可在該介面管理流量的通訊協定：**Ping**、**Telnet**、**SSH**、**HTTP**、**HTTP OCSP**、**HTTPS** 或 **SNMP**。

      不要啟用 ***HTTP*** 或 ***Telnet***，因為這些通訊協定以明文傳輸，因此不安全。
6. 將介面管理設定檔指派給介面。
   1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取介面類型：**Ethernet**（乙太網路）、**VLAN**、**Loopback**（回送） 或 **Tunnel**（通道），接著再選取該介面。
   2. 選取 **Advanced**（進階） > **Other info**（其他資訊），然後選取您剛新增的 **Management Profile**（管理設定檔）。
   3. 按一下 **OK**（確定）。
7. 設定 DNS 伺服器和 FQDN 重新整理時間。

©2023 Palo Alto Networks, Inc.

1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務），然後按一下編輯圖示。
2. 將 **Primary DNS Server**（主要 **DNS** 伺服器）設為 169.254.169.253。這是 AWS DNS 位址。
3. 將 **Minimum FQDN Refresh Time**（**FQDN** 最短重新整理時間）設為 60 秒。
4. 按一下 **OK**（確定）。

8. **Commit**（提交）您的變更。需要這樣做才能繼續下一步。
9. 建立管理員。
   1. 選取 **Device**（裝置） > **Administrators**（管理員）。
   2. 輸入 **pandemo** 作為 **Name**（名稱）。
   3. 將 **Password**（密碼）設為 **demopassword** 並 **Confirm**（確認）。
   4. 按一下 **OK**（確定）。
10. **Commit**（提交）您的變更。

STEP 5 | 設定範本堆疊，並將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. 按一下 **Add**（新增）並選取範本。
4. 按一下 **OK**（確定）來儲存範本堆疊。

STEP 6 | 建立 **Device Group**（裝置群組）。

1. 選取 **Panorama** > **Device Groups**（裝置群組）。
2. 按一下 **Add**（新增）。
3. 輸入描述性的 **Name**（名稱）。
4. 按一下 **OK**（確定）。
5. 新增一個允許所有安全性預先規則。
   1. 確定您已從 **Device Group**（裝置群組）下拉式清單中選取您在上面建立的裝置群組。
   2. 選取 **Policies**（政策） > **Security**（安全性） > **Pre Rules**（預先規則），然後按一下 **Add**（新增）。
   3. 輸入描述性的 **Name**（名稱）。
   4. 在 **Source**（來源）、**User**（使用者）、**Destination**（目的地）、**Application**（應用程式）和 **Service/URL Category**（服務/**URL** 類別）下方，選取 [any（任何）]。
   5. 在 **Actions**（動作）下方，選取 **Allow**（允許）。
   6. 按一下 **OK**（確定）。
6. **Commit**（提交）您的變更。

©2023 Palo Alto Networks, Inc.

STEP 7 | 將防火牆的授權停用 API 金鑰新增至 Panorama。

1. 登入客戶支援入口網站。
2. 選取 **Assets**（資產） > **API Key Management**（**API** 金鑰管理）。
3. 複製 API 金鑰。
4. 使用 CLI 安裝上一步所複製的 API 金鑰。

   request license api-key set key *<key>*

STEP 8 | 部署 Panorama 之後，您必須在 AWS 中如下所述在 Panorama 安全性群組上開啟下列連接埠。

- 連接埠 **443 (HTTPS)**—初始部署防火牆範本時，請保持 HTTPS 的開啟狀態，讓 Lambda 可以連線至 Panorama。

  當您保護連接埠 443 時，請指定從中允許連線的 IP 位址範圍，以及指派給 NAT 閘道的 EIP。部署中的 NAT 閘道數量取決於您設定的可用性區域數量。若要在 AWS 中找到 NAT 閘道 EIP，請移至 **VPC** > **NAT Gateways**（**NAT** 閘道）。請記下進行 HTTPS 之安全性群組的 EIP 資訊。

  此外，若要允許 Panorama 在堆疊刪除之後釋放防火牆授權，您必須允許流量來自您部署防火牆範本所在地區的 CIDR 範圍。您可以在此連結尋找您所在地區的 CIDR。
- 連接埠 **3978**—連接埠 3978 必須可以接收來自任何 IP 位址的流量。

啟動防火牆範本

此工作流程說明如何部署防火牆範本。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 修改 `init-cfg.txt` 檔案，並將它上傳至 `/config` 資料夾。

因為您使用 Panorama 啟動 VM-Series 防火牆，所以應該修改 `init-cfg.txt` 檔案，如下所示。不需要 `bootstrap.xml` 檔案。

確保使用上面在 init-cfg.txt 文件中建立的裝置群組和範本名稱。

```
type=dhcp-client ip-address= default-gateway= netmask= ipv6-
address= ipv6-default-gateway= hostname= vm-auth-key= panorama-
server= panorama-server-2= tplname= dgname= dhcp-send -
hostname=yes dhcp-send-client-id=yes dhcp-accept-server-
hostname=yesdhcp-accept-server-domain=yes plugin-op-commands=aws-
gwlb-inspect:enable
```

您的 init-cfg.txt 檔案必須包含 **`plugin-op-commands=aws-gwlb-inspect:enable`**。整合 VM-Series 防火牆與 GWLB 時需要如此。

您必須將裝置憑證自動註冊 PIN 新增至 init-cfg.txt 檔案，才能在部署 VM-Series 防火牆實例時自動安裝裝置憑證。

©2023 Palo Alto Networks, Inc.

STEP 2 | 在啟動套件的 `/license` 資料夾中新增授權驗證碼。

1. 使用文字編輯器建立名為 **`authcodes`** 的新文字檔案（無副檔名）。
2. 將 BYOL 授權的授權碼新增至此檔案，並儲存。授權碼必須代表搭售包，而且必須支援您部署可能需要的防火牆數目。如果您使用個別授權碼，而非搭售包，則防火牆只會擷取檔案中第一個授權碼的授權金鑰。

STEP 3 | 將防火牆範本 (**`panw-aws.zip`**) 和應用程式範本 (**`app.zip`**) 的 Lambda 程式碼上傳至 S3 貯體。您可以使用用於啟動的相同 S3 貯體。

如果由不同於防火牆的帳戶來管理應用程式堆疊，請使用應用程式帳戶在與防火牆範本相同的 AWS 地區建立另一個 s3 貯體，並將 **`app.zip`** 複製到該 s3 貯體。

STEP 4 | 選取防火牆範本。

1. 在 AWS 管理主控台，選取 **CloudFormation** > **Create Stack**（建立堆疊）。
2. 從 Git repository（Git 儲存庫）選取 **Upload**（上傳）最新的防火牆範本，選擇防火牆範本來部署範本啟動的資源。按一下 [Open（開啟）] 和 [Next（下一步）]。
3. 指定堆疊名稱。堆疊名稱可讓您唯一地識別所有使用此範本所部署的資源。

STEP 5 | 輸入堆疊的描述性 **Name**（名稱）。名稱必須是 28 個字元或更少。

STEP 6 | 設定 VPC 的參數。

1. 輸入可用性區域數量，並從可用性區域下拉式清單中選取區域。
2. 查閱並輸入 VM-Series 防火牆的 AMI ID。確保 AMI ID 符合您選取使用的 AWS 區域、PAN-OS 版本和 BYOL 或 PAYG 授權選項。如需詳細資訊，請參閱取得 Amazon Machine Image ID。
3. 選取 EC2 **Key pair**（金鑰配對）（從下拉式清單）以啟動防火牆。若要登入防火牆，您必須提供此金鑰配對及其相關聯私密金鑰的名稱。
4. 如果您想要 **Enable Debug Log**（啟用偵錯日誌），請選取 **Yes**（是）。啟用偵錯日誌會產生更詳細的日誌，這有助於部署問題的疑難排解。這些日誌是以堆疊名稱產生，並儲存在 AWS CloudWatch 中。

依預設，範本使用 CPU 使用率作為 VM-Series 防火牆的調整規模參數。 自訂 PAN-OS 度量會自動發佈至與您稍早指定的堆疊名稱相符的 CloudWatch 命名空間。

STEP 7 | 指定 Amazon S3 貯體的名稱。

1. 輸入含有啟動程序套件的 S3 貯體的名稱。

   如果啟動載入貯體未適當設定，或貯體名稱輸入不正確，啟動載入程序會失敗，您也無法登入防火牆。負載平衡器的健康情況檢查也會失敗。
2. 輸入含有 panw-aws.zip 檔案的 S3 貯體的名稱。如前所提及，您可以針對啟動程序和 Lambda 程式碼使用一個 S3 貯體。

©2023 Palo Alto Networks, Inc.

STEP 8 | 指定金鑰以允許 API 存取防火牆和 Panorama。

1. 輸入防火牆驗證 API 呼叫時必須使用的金鑰。預設金鑰是以範例檔案為基礎，僅適用於測試和評估。在生產環境中，您必須針對 API 呼叫建立個別的 PAN-OS 登入，並產生相關聯的金鑰。
2. 輸入 API 金鑰，以允許 AWS Lambda 對 Panorama 發出 API 呼叫。在生產環境中，您應該針對 API 呼叫建立個別的登入，並產生相關聯的金鑰。

STEP 9 | 新增 AWS 帳戶號碼。您必須提供帳戶號碼，以用來部署任何連接至 GWLB 的 VPC。請以逗號分隔清單輸入這些值。您可以在部署範本之後新增額外的帳戶號碼。

若要找出您的帳戶號碼，請在 AWS 主控台右上角按一下您的 AWS 使用者名稱，然後選取 **My Security Credentials**（我的安全登入資料）。

STEP 10 | 輸入傳輸閘道 ID。需要傳輸閘道 ID 才能保護東西向和輸出流量。如果您不輸入傳輸閘道 ID，範本會假設與 GWLB 整合的防火牆只檢查輸入流量。

STEP 11 | 輸入安全性 VPC 的 CIDR。

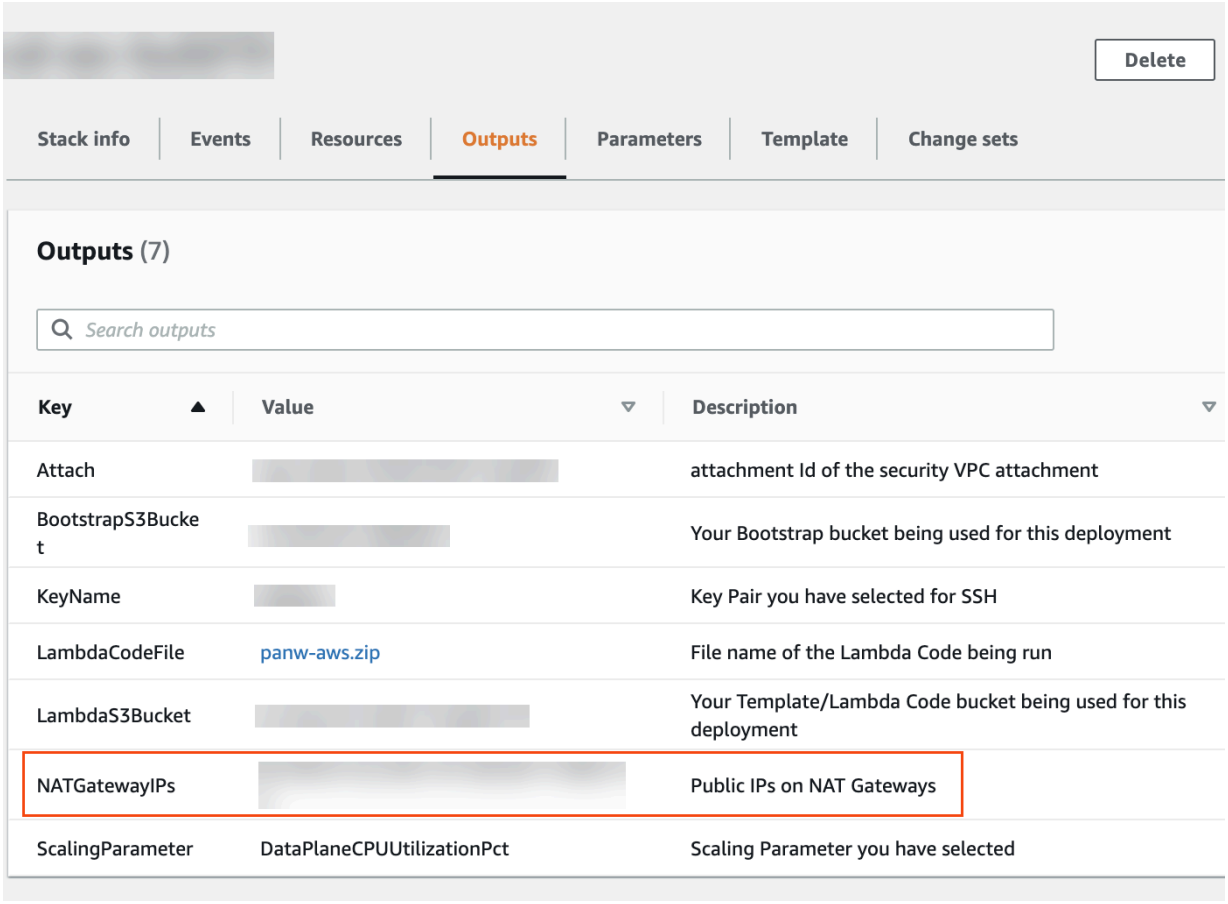
STEP 12 | 檢閱範本設定並啟動範本。

1. 選取 **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**（我瞭解此範本可能導致 **AWS CloudFormation** 建立 **IAM** 資源）。
2. 按一下 **Create**（建立）來啟動範本。將會顯示 CREATE_IN_PROGRESS 事件。
3. 成功部署時，狀態會更新為 CREATE_COMPLETE。

STEP 13 | 確認範本已啟動所有必要資源。

©2023 Palo Alto Networks, Inc.

STEP 14 | 建立規則，在部署 Panorama 設備的安全群組上允許 NAT 閘道 IP 位址。必須如此，才能讓防火牆連線至 Panorama。您可以在 CFT 安全性堆疊輸出中找到 NAT 閘道 IP 位址清單。



 ©2023 Palo Alto Networks, Inc.

1. 存取 AWS VPC 主控台。
2. 在導覽窗格上，選取 **Security Groups**（安全性群組）。
3. 在部署 Panorama 之處選取安全性。
4. 選取 **Actions**（動作） > **Edit Inbound Rules**（編輯輸入規則） > **Add rule**（新增規則）。
5. 新增規則，針對連接埠範圍 3978 的自訂 TCP 規則，允許 NAT 閘道 IP 位址。
6. 按一下 **Save rules**（儲存規則）。

Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0
Custom TCP Rule	TCP	3978	
Custom TCP Rule	TCP	3978	
Custom TCP Rule	TCP	3978	

啟動應用程式範本

請完成下列程序來啟動應用程式範本。

STEP 1 | 建立您將從中啟動應用程式範本的 S3 貯體。

- 如果這是跨帳戶部署，則請建立新的貯體。
- 如果有一個帳戶，則您可以建立新貯體，或使用您稍早建立的 S3 貯體（您可以針對所有項目使用一個貯體）。

STEP 2 | 將 app.zip 檔案上傳至 S3 貯體。

STEP 3 | 選取您想要啟動的應用程式啟動範本。

1. 在 AWS 管理主控台中，選取 **CloudFormation** > **CreateStack**
2. 選取 [Upload a template to Amazon S3（將範本上傳至 Amazon S3）] 以選擇應用程式範本，將範本所啟動的資源部署至與防火牆相同的 VPC 內或不同的 VPC。按一下 **Open**（開啟）和 **Next**（下一步）。
3. 指定堆疊名稱。堆疊名稱可讓您唯一地識別所有使用此範本所部署的資源。

STEP 4 | 在 [Select list of AZ（AZ 選擇清單）] 中，選取您的設定將跨越的可用性區域 (AZ)。

STEP 5 | 輸入描述性 **VPC Name**（**VPC** 名稱）。

©2023 Palo Alto Networks, Inc.

STEP 6 | 設定 Lambda 的參數。

1. 輸入儲存 app.zip 的 S3 貯體名稱。
2. 輸入 zip 檔案名稱。

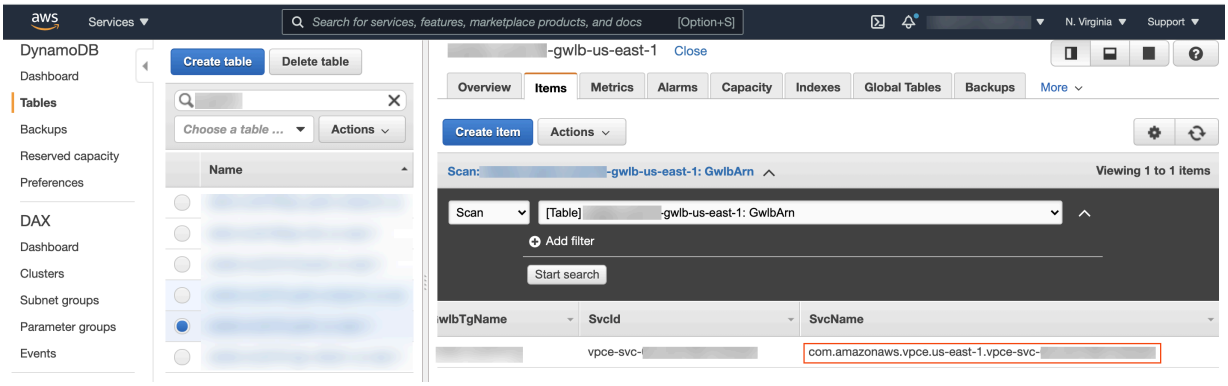
STEP 7 | 針對此範本啟動的 Ubuntu Web 伺服器，選取 EC2 實例類型。

STEP 8 | 輸入 Amazon EC2 金鑰配對。

©2023 Palo Alto Networks, Inc.

STEP 9 | 針對安全性 VPC 中的 GWLB 端點，輸入服務設定的名稱（服務名稱）。

1. 從 AWS 主控台的 **Services**（服務）下拉式清單中，選取 **DynamoDB**。
2. 選取 **Tables**（表格），找出您的安全性 VPC 表格。表格名稱將為 <stack name>-gwlb-<region>。例如—cft-deployment-gwlb-us-east-1。
3. 按一下 [Items（項目）] 頁籤，複製服務名稱。
4. 將服務名稱貼到應用程式範本設定參數中。



STEP 10 | 輸入傳輸閘道 ID。這是您在部署防火牆範本之前建立的同一個傳輸閘道。

©2023 Palo Alto Networks, Inc.

STEP 11 | 檢閱範本設定並啟動範本。

STEP 12 | 部署應用程式之後，您必須將路由新增至傳輸閘道路由表，才能啟用東西向和輸出流量檢查。

1. 登入 AWS VPC 主控台。
2. 選取 **Transit Gateway Route Tables**（傳輸閘道路由表），然後選擇您的傳輸閘道路由表。此路由表由範本建立，稱為 **<app-stack-name>-<region>-PANWAppAttRt**。
3. 選取 **Routes**（路由），然後按一下 **Create static route**（建立靜態路由）。
4. 在 **CIDR** 欄位中輸入 0.0.0.0/0。
5. 從 **Choose attachment**（選擇連接）下拉式清單中，選取 VM-Series 防火牆 VPC 連接。
6. 按一下 **Create static route**（建立靜態路由）。

STEP 13 | （選用）建立堡壘主機（又稱為跳箱），以存取應用程式範本建立的 Web 伺服器。

1. 在您的應用程式 VPC 中建立公開子網路。
2. 在此子網路中，新增從您的 IP 位址到網際網路閘道的路由。
3. 在公共子網路中，建立具有公共 IP 位址的新 EC2 實例。
4. 為此 EC2 實例建立安全性群組，以允許從您的 IP 位址執行 SSH。

©2023 Palo Alto Networks, Inc.

AWS 上 VM-Series 防火牆的高可用性

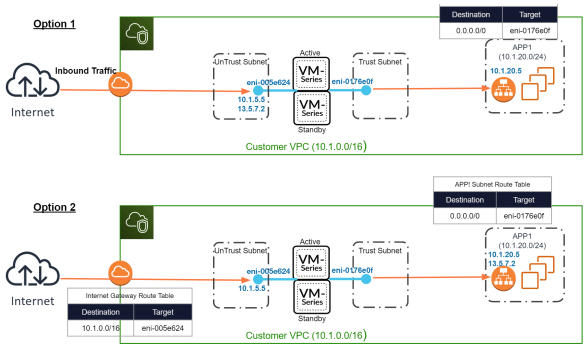
AWS 上的 VM-Series 防火牆僅支援主動/被動 HA；如果部署 Amazon 彈性負載平衡 (ELB)，則不支援 HA（在此情況下，ELB 提供容錯轉移功能）。

- AWS 上的 HA 概觀
- HA 的 IAM 角色
- HA 連結
- 活動訊號輪詢與您好訊息
- 裝置優先順序及先佔
- HA 計時器
- 使用次要 IP 在 AWS 上設定主動/被動 HA
- 使用介面移動在 AWS 上設定主動/被動 HA
- 在 AWS 上移轉主動/被動 HA

AWS 上的 HA 概觀

為確保備援，您可以在 AWS 上部署 VM-Series 防火牆，採用主動/被動高可用性 (HA) 組態。主動端點連續不斷地將其組態及工作階段資訊與設定相同的被動端點保持同步。如果主動設備關閉，兩部設備間的活動訊號連線可確保故障復原。有兩個選項可在 HA 中將 VM-Series 防火牆部署在 AWS—次要 IP 移動和資料平面介面 (ENI) 移動。

若要確保您網際網路型應用程式的所有流量都會通過防火牆，您有兩個選項。您可以在 VM-Series 防火牆的不受信任介面（上圖中的 E1/2）上設定應用程式的公用 IP 位址，或者，您可以設定 AWS 進入路由。AWS 進入路由功能可讓您建立路由表與 AWS 網際網路閘道的關聯，並新增透過 VM-Series 防火牆將應用程式流量重新導向的路由規則。這樣的重新導向可確保所有網際網路流量都會通過防火牆，且無需重新設定應用程式端點。

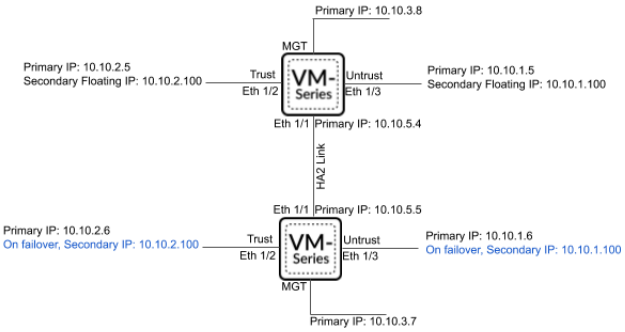


次要 IP 移動

當主動對等故障時，被動對等會偵測到此失敗狀況，並變成主動。此外，被動對等還會對 AWS 基礎結構觸發 API 呼叫，將已設定的次要 IP 位址從失敗對等的資料平面介面移給自己。此外，AWS 會更新路由表，以確保流量導向至主動防火牆實例。這兩個操作可確保容錯移轉之後還原輸入和輸出流量工作階段。此選項可讓您利用 DPDK 來改善 VM-Series 防火牆實例的效能，而且容錯移轉時間比介面移動 HA 更短，還支援介面移動提供的所有功能。

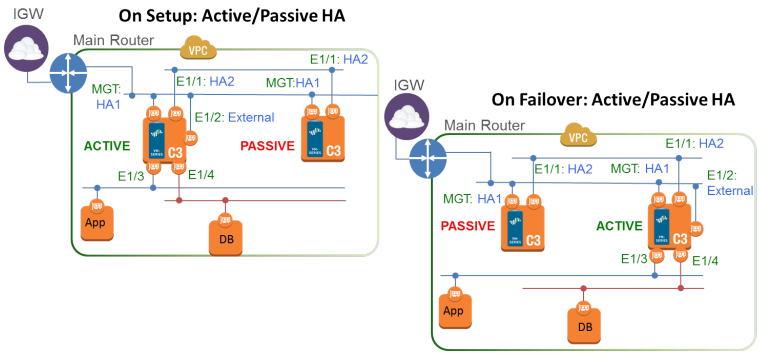
©2023 Palo Alto Networks, Inc.

次要 *IP* 移動 *HA* 需要 *VM-Series* 外掛程式 *2.0.1* 或更新版本。



資料平面介面移動

當主動對等故障時，被動對等會偵測到此失敗狀況，並變成主動。此外，被動對等還會對 AWS 基礎結構觸發 API 呼叫，將所有資料平面介面 (ENI) 從失敗對等移給自己。



HA 的 IAM 角色

AWS 要求所有 API 請求必須使用其簽發的憑證進行加密簽署。為了啟用 VM-Series 防火牆（部署為 HA 配對）的 API 權限，您必須建立原則，並在AWS 身分及存取管理 (IAM) 服務中將該原則附加至角色。角色必須在啟動時附加至 VM-Series 防火牆。此政策將權限給予 IAM 角色來起始必要的 API 動作，以便觸發容錯移轉時，將介面或次要 IP 位址從主動對等移至被動對等。

如需建立原則的詳細指示，請參閱 AWS 文件中的建立客戶管理的原則。如需建立 IAM 角色，定義哪些帳戶或 AWS 服務可承擔該角色，以及承擔角色後應用程式可使用哪些 API 動作及資源的詳細指示，請參閱 Amazon EC2 的 IAM 角色。

在 AWS 主控台設定的 IAM 原則必須（至少）擁有下列動作與資源：

啟用 *HA* 需要下列 *IAM* 動作、權限和資源。若要啟用 *AWS Cloudwatch* 監控，請參閱在 VM-Series 防火牆上啟用 CloudWatch 監控

以取得所需的 *IAM* 動作。

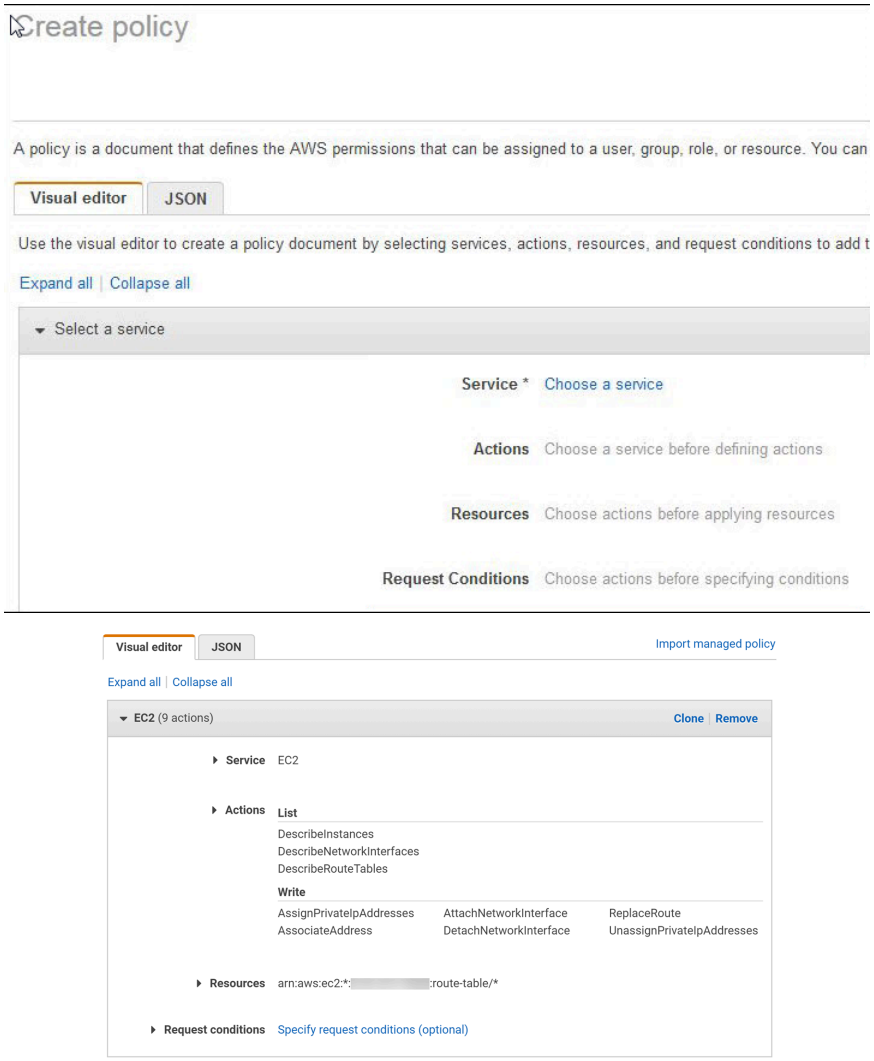
©2023 Palo Alto Networks, Inc.

IAM 動作、權限或資源	說明	介面移動	次要 IP 移動
AttachNetworkInterface	允許將 ENI 連接至實例。	✓	✓
DescribeNetworkInterfaces	擷取 ENI 參數以便將介面連接至實例。	✓	✓
DetachNetworkInterface	允許將 ENI 從 EC2 實例分離。	✓	✓
DescribeInstances	允許取得 VPC 中 EC2 實例的相關資訊。	✓	✓
AssociateAddress	允許將主要 IP 位址相關聯的公共 IP 位址，從被動介面移至主動介面。		✓
AssignPrivateIpAddresses	允許將次要 IP 位址和相關聯的公共 IP 位址，指派給被動對等的介面。		✓
DescribeRouteTables	允許擷取與 VM-Series 防火牆實例相關聯的所有路由表。		✓
ReplaceRoute	允許更新 AWS 路由表項目。		✓
GetPolicyVersion	允許擷取 AWS 政策版本資訊。		✓
GetPolicy	允許擷取 AWS 政策資訊。		✓
ListAttachedRolePolicies	允許擷取連接至特定 IAM 角色的所有受管理政策的清單。		✓
ListRolePolicies	允許擷取內嵌於特定 IAM 角色中的內嵌政策名稱清單。		✓
GetRolePolicy	允許擷取內嵌於特定 IAM 角色中的特定內嵌政策。		✓
policy	允許存取 IAM 政策 Amazon Resource Name (ARN)。		✓
role	允許存取 IAM 角色 ARN。		✓
route-table	允許存取路由表 Amazon Resource Name (ARN) 以便於容錯移轉時更新。		✓

©2023 Palo Alto Networks, Inc.

IAM 動作、權限或資源	說明	介面移動	次要 IP 移動
萬用字元 (*)	在 ARN 欄位中使用 * 作為萬用字元。	✓	✓

下列螢幕擷取畫面顯示以上針對次要 IP HA 所述 IAM 角色的存取管理設定：



介面移動 HA 需要的最低權限為：**{"Version":"2012-10-17","Statement":[{"Sid":"VisualEditor0","Effect":"Allow","Action":["ec2:AttachNetworkInterface","ec2:DetachNetworkInterface","ec2:DescribeInstance"*"}]}**

次要 IP 移動 HA 需要的最低權限為：{"Version":"2012-10-17","Statement":[{"Sid":"VisualEditor0","Effect":"Allow","Action":["ec2:AttachNetworkInterface","ec2:DetachNetworkInterface","ec2:DescribeInstances","ec2:DescribeNetworkInterfa “ec2:AssignPrivateIpAddresses”，“ec2:AssociateAddress”，“ec2:DescribeRouteTables”],"Resource":

©2023 Palo Alto Networks, Inc.

"*"}{"Sid":"VisualEditor1","Effect":"Allow","Action": "ec2:ReplaceRoute", "Resource": "arn:aws:ec2:*:*:route-table/*"}]}

HA 連結

HA 配對中的裝置使用 HA 連結來同步資料和維護狀態資訊。在 AWS 上，VM-Series 防火牆使用下列連接埠：

- 控制連結—HA1 連結用於交換 Hello、活動訊號及 HA 狀態資訊，以及管理路由和 User-ID 資訊的平面同步。此連結也用於隨端點同步主動或被動設備上的組態變更。

  用於 HA1 的管理連接埠。使用於明碼通訊的 TCP 連接埠 28769 和 28260，或使用於加密通訊的連接埠 28（TCP 上的 SSH）。
- 資料連結—HA2 連結可用於在 HA 配對中同步設備之間的執行階段、轉送表格、IPSec 安全性關聯和 ARP 表格。HA2 連結中的資料流永遠為單一方向性（HA2 保持運作除外）；其流向會從主動設備流往被動設備。

  Ethernet1/1 必須指派為 HA2 連結；如此才能在 HA 中將 VM-Series 防火牆部署在 AWS。HA 資料連結可設定為使用 IP（通訊協定編號 99）或 UDP（埠號 29281）作為傳輸用途。

AWS 上的 VM-Series 防火牆不支援用於 HA1 或 HA2 的備份連結。

活動訊號輪詢與您好訊息

防火牆使用您好訊息和活動訊號來驗證端點設備可回應及可操作。您好訊息會以設定的您好間隔在端點間傳送，以確認裝置的狀態。活動訊號是在控制連結上對 HA 端點的 ICMP ping，而該端點會回應 ping 以建立設備間的連線與回應。如需觸發容錯移轉的 HA 計時器的詳細資料，請參閱HA 計時器。（VM-Series 防火牆的 HA 計時器與 PA-5200 系列防火牆的 HA 計時器相同）。

裝置優先順序及先佔

可對 HA 配對中的裝置指定裝置優先順序值，以表示喜好的裝置在容錯移轉後可擔任主動角色及管理流量。若要在 HA 配對中使用特定設備來主動保護流量，您必須在兩個防火牆上啟用先佔行為並為每個設備指定設備優先順序。數值較小的設備就等於有較高的優先順序，表示將其指定為主動設備並管理所有網路上的流量。另一部設備則進入被動狀態，並與主動設備的設定和狀態資訊同步，以便隨時在發生故障時轉換為主動狀態。

依預設，防火牆上的先佔選項為停用，且必須在兩個設備上都啟用。啟用後，先佔行為允許優先順序較高（數值較小）的防火牆在故障復原後繼續擔任主動設備。出現先佔行為時，該事件會記錄在系統日誌中。

對於 ***AWS*** 上的 ***VM-Series*** 防火牆中的 ***HA***，不建議先佔。

HA 計時器

高可用性 (HA) 計時器是用來偵測防火牆失敗及觸發故障復原。若要減少設定 HA 計時器的複雜度，您可以從三個設定檔選取：**Recommended**（建議）、**Aggressive**（積極）和 **Advanced**（進階）。這些設定檔會自動填入最佳的 HA 計時器值，供特定的防火牆平台啟用更快速的 HA 部署。

 ©2023 Palo Alto Networks, Inc.

為一般的故障復原計時器設定使用 **Recommended**（建議）的設定檔，並為較快速的故障復原計時器設定使用 **Aggressive**（積極）設定檔。**Advanced**（進階）設定檔可讓您自訂計時器值以符合您的網路需求。

AWS 上 **VM-Series** 防火牆上的 **HA** 計時器	建議的/積極設定檔的預設值
提升保留時間	2000/500 毫秒
Hello 間隔	8000/8000 毫秒
活動訊號間隔	2000/1000 毫秒
最大擺動旗標數	3/3
先佔保留時間	1/1 分鐘
監控失敗維持時間	0/0 毫秒
其他主機維持時間	500/500 毫秒

使用次要 IP 在 AWS 上設定主動/被動 HA

完成下列程序，將新的 VM-Series 防火牆部署為具有次要 IP 位址的 HA 配對。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

©2023 Palo Alto Networks, Inc.

STEP 1 | 在為 HA 配對部署 VM-Series 防火牆之前，請確認以下事項：

- 請參閱 VPC 規劃工作表，確保為 VM-Series 防火牆備妥 VPC。
- 次要 IP 移動 HA 需要 VM-Series 外掛程式 2.0.1 或更新版本。
- HA 對等雙方都部署在相同的 AWS 可用性區域。

  從 VM-Series 外掛程式 2.0.3 開始，您可以將 HA 對等部署在不同的可用性區域。不過，在 HA 容錯移轉事件期間，路由表會更新，但次要 IP 不會移動。不建議採取這種部署。
- 部署實例時，建立 IAM 角色並將角色指派給 VM-Series 防火牆。
- 主動和被動防火牆至少必須各有四個介面—管理介面、HA2 介面、不受信任介面和信任介面。此外，必須指派次要 IP 位址給主動防火牆上的信任和不受信任介面。

  管理介面必須用作 HA1 介面。
- 確認網路與安全性元件已適當定義。
  - 啟用網際網路通訊。預設的 VPC 包含網際網路閘道，如果您在預設的子網路中安裝 VM-Series 防火牆，則該防火牆可存取網際網路。
  - 建立子網路。子網路是指派給 VPC 的 IP 位址範圍區段，您可以在該 VPC 中啟動 EC2 實例。VM-Series 防火牆必須屬於公共子網路，才能設定該防火牆存取網際網路。
  - 建立包含防火牆資料介面的資料安全性群組。此外，設定安全性來允許所有流量 (0.0.0.0/0)，以便防火牆強制執行安全性。必須如此，才能在容錯移轉期間維持現有工作階段。
  - 為私人子網路的路由表新增路由，以確定流量可在 VPC 中整個子網路與安全性群組之間路由（若適當的話）。
- 如果您在啟動防火牆，請建立必要的 S3 貯體，其中包含所需的啟動程序檔案。

©2023 Palo Alto Networks, Inc.

STEP 2 | 在 AWS 上部署 VM-Series 防火牆。

1. 如果您的 VM-Series 防火牆未安裝 VM-Series 外掛程式 2.0.1 或更新版本，請先升級外掛程式再繼續。
2. 在每個 HA 對等上，設定乙太網路 1/1 作為 HA2 介面。
   1. 開啟 Amazon EC2 主控台。
   2. 選取 [Network Interface（網路介面）]，然後選取您的網路介面。
   3. 選取 **Actions**（動作） > **Manage IP Addresses**（管理 **IP** 位址）。
   4. 將此欄位保留空白，以允許 AWS 動態指派 IP 位址，或輸入 VM-Series 防火牆子網路範圍內的 IP 位址。
   5. 按一下 **Yes**（是）和 **Update**（更新）。
   6. 選取 **Actions**（動作） > **Change Source/Dest.Check**（變更來源/目的地檢查），然後選取 **Disable**（停用）。
   7. 在第二個（成為被動）HA 對等上重複此程序。
3. 將次要 IP 位址新增至第一個（成為主動）HA 對等上的資料平面介面。
   1. 選取 **Network Interface**（網路介面），然後選取您的網路介面。
   2. 選取 **Actions**（動作） > **Manage IP Addresses**（管理 **IP** 位址） > **IPv4 Addresses**（**IPv4** 位址） > **Assign new IP**（指派新 **IP**）。
   3. 將此欄位保留空白，以允許 AWS 動態指派 IP 位址，或輸入 VM-Series 防火牆子網路範圍內的 IP 位址。
   4. 按一下 **Yes**（是）和 **Update**（更新）。
4. 將次要彈性（公共）IP 位址與主動對等的不受信任介面建立關聯。
   1. 選取 **Elastic IPs**（彈性 **IP**），然後選取要建立關聯的彈性 IP 位址。
   2. 選取 **Actions**（動作） > **Associate Elastic IP**（與彈性 **IP** 位址建立關聯）。
   3. 在 **Resource Type**（資源類型）下方，選取 **Network Interface**（網路介面）。
   4. 選擇要與彈性 IP 位址建立關聯的網路介面。
   5. 按一下 **Associate**（關聯）。
5. 若要檢查輸出流量，請在子網路路由表中新增項目，將下一個躍點設為防火牆信任介面。
   1. 選取 **VPC** > **Route Tables**（路由表）。
   2. 選擇子網路路由表。
   3. 選取 **Actions**（動作） > **Edit routes**（編輯路由） > **Add route**（新增路由）。
   4. 輸入 **Destination**（目的地） CIDR 區塊或 IP 位址。
   5. 在 **Target**（目標）中，輸入防火牆信任介面的網路介面。
   6. 按一下 **Save routes**（儲存路由）。
6. 若要使用 AWS 進入路由，請建立路由表，並將網際網路閘道與路由表建立關聯。然後，新增項目，將下一個躍點設為主動防火牆不受信任介面。
   1. 選取 **Route Tables**（路由表） > **Create route table**（建立路由表）。
   2. （選用）輸入路由表的描述性 **Name tag**（名稱標籤）。

©2023 Palo Alto Networks, Inc.

3. 按一下 **Create**（建立）。
4. 按一下您的路由表，選取 **Actions**（動作） > **Edit edge associations**（編輯邊緣關聯）。
5. 選取 **Internet gateways**（網際網路閘道），然後選擇您的 VPC 網際網路閘道。
6. 按一下 **Save**（儲存）。
7. 按一下您的路由表，選取 **Actions**（動作） > **Edit routes**（編輯路由）。
8. 在 **Target**（目標）中，選取 **Network Interface**（網路介面），然後選擇主動防火牆的不受信任介面。
9. 按一下 **Save routes**（儲存路由）。

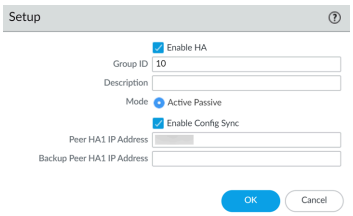
STEP 3 | 在防火牆上設定介面。您必須為不受信任和信任介面設定 HA2 資料連結，以及至少兩個 Layer 3 介面。請先在第一個 HA 對等完成此工作流程，再對第二個 HA 對等重複這些步驟。

1. 登入防火牆 Web 介面。
2. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後按一下您的不受信任介面。在此範例中，HA2 介面為 1/1、信任介面為乙太網路 1/2，不受信任介面為乙太網路 1/3。
3. 按一下 **Ethernet 1/1** 的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：**HA**
4. 按一下 **ethernet 1/2**（乙太網路 **1/2**）的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：**Layer3**
   - 在 **Config**（設定）頁籤上，將介面指派給預設路由器。
   - 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。定義新區域（例如 trust-zone），然後按一下 **OK**（確定）。
   - 在 **IPv4** 頁籤上，選取 **DHCP Client**（**DHCP** 用戶端）。
   - 勾選 **Enable**（啟用）。
   - 在不受信任的介面上，勾選 **Automatically create default route pointing to default gateway provided by server**（自動建立指向伺服器所提供之預設閘道的預設路由）。此選項指示防火牆建立指向預設閘道的靜態路由。
   - 針對乙太網路 1/3 重複這些步驟。
5. 在被動對等上重複上述步驟。

©2023 Palo Alto Networks, Inc.

STEP 4 | 啟用 HA。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般）。
2. 編輯 [Setup（設定）] 設定。
3. 在 **Peer HA1 IP address field**（對等 **HA1 IP** 位址欄位）中輸入被動對等的私人 IP 位址。
4. 按一下 **OK**（確定）。



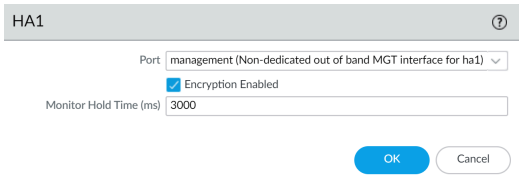
5. 編輯 **Election Settings**（選取設定），將特定防火牆指定為主動對等。在主動防火牆上輸入較低的 **Device Priority**（裝置優先順序）數值。如果兩個防火牆的裝置優先順序值相同，則 HA1 控制上 MAC 值最低的防火牆會成為主動防火牆。

   不建議啟用先佔。

6. 按一下 **OK**（確定）。
7. **Commit**（提交）您的變更。
8. 在被動對等上重複上述步驟。

STEP 5 | 將控制連結 (HA1) 設定為使用管理連接埠。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 [Control Link (HA1)（控制連結 (HA1)）] 區段。

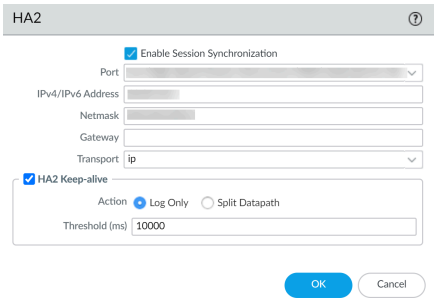


2. （選用）選取 **Encryption Enabled**（啟用加密），以保護對等之間的 HA 通訊安全。若要啟用加密，必須從設備中匯出 HA 金鑰再匯入對等設備。
   1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證）。
   2. 選取匯出 **Export HA key**（匯出 **HA** 金鑰）。將 HA 金鑰儲存至對等設備可存取的網路位置。
   3. 在對等裝置上，導覽至 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證），並選取 **Import HA key**（匯入 **HA** 金鑰）以瀏覽至金鑰儲存位置，然後將金鑰匯入到對等裝置。

©2023 Palo Alto Networks, Inc.

STEP 6 | 設定資料連結 (HA2) 以使用 ethernet1/1。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 [Data Link (HA2)（資料連結 (HA2)）] 區段。
2. 選取 **Port**（連接埠）ethernet1/1。
3. 輸入 ethernet1/1 的 IP 位址。此 IP 位址必須與指派給 EC2 儀表板上的 ENI 的 IP 位址相同。
4. 輸入 **Netmask**（網路遮罩）。
5. 如果 HA1 介面位於不同子網路，輸入 **Gateway**（閘道）IP 位址。
6. 選取 **IP** 或 **UDP** 作為 **Transport**（傳輸）用途。如果您需要 Layer 3 傳輸（IP 通訊協定編號 99）則使用 **IP**。如果您想要防火牆在完整封包而非僅僅是標頭上計算總和檢查碼，與 IP 選項相同（UDP 連接埠 29281），則使用 **UDP**。



7. （選用）修改 **HA2 Keep-alive**（**HA2** 保持活動）封包的 **Threshold**（閾值）。依預設，可啟用 **HA2 Keep-alive**（**HA2** 保持運作）對端點之間 HA2 資料連結進行監控。如果發生故障且超過此臨界值（預設值為 10000 毫秒），則會發生定義的動作。發生 HA2 keep-alive（HA2 保持運作）故障時，會產生重要系統日誌訊息。

> 您可以在兩個設備都設定 ***HA2 keep-alive***（***HA2*** 保持運作）選項，或僅設定 *HA* 配對中的一個設備。如果您在一部設備上啟用此選項，僅該設備會傳送保持運作訊息。

STEP 7 | 完成兩個防火牆的 HA 設定後，請確認配對的防火牆為主動/被動 HA。

1. 存取兩個防火牆上的 **Dashboard**（儀表板），然後檢視高可用性 Widget。
2. 在主動 HA 對等上，按一下 **Sync to peer**（同步處理至對等）。
3. 確認防火牆已配對並同步。
   - 在被動防火牆上：本機防火牆狀態應顯示為 **Passive**（被動），而 **Running Config**（執行中設定）應顯示為 Synchronized（已同步）。
   - 在主動防火牆上：本機防火牆狀態應顯示為 **Active**（主動），而執行中設定應顯示為 **synchronized**（已同步）。
4. 從防火牆 command line interface（命令列介面 - CLI），執行下列命令：
   - 確認容錯移轉備妥情況：

     ```
     show plugins vm_series aws ha state
     ```

   - 顯示次要 IP 對應：

     ```
     show plugins vm_series aws ha ips
     ```


©2023 Palo Alto Networks, Inc.

使用介面移動在 AWS 上設定主動/被動 HA

完成下列程序，使用介面移動模式設定主動-被動 HA。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 確定您具備下列先決條件：

如需在 AWS 雲端部署高可用性 (HA) VM-Series 防火牆，您必須確保執行下列步驟：

- 在 EC2 實例上啟動 VM-Series 防火牆時，選取您建立的 IAM 角色；您無法將角色指派給已在執行中的實例。請參閱 HA 的 IAM 角色

  。如需建立 IAM 角色，定義哪些帳戶或 AWS 服務可承擔該角色，以及承擔角色後應用程式可使用哪些 API 動作及資源的詳細指示，請參閱 AWS 文件。
- 在介面移動 HA 部署中，AWS 上的 VM-Series 防火牆不支援 DPDK。如果您在防火牆上有 VM-Series 外掛程式 2.0.1 或更新版本，則必須停用 DPDK。

  停用 DPDK 需要重新啟動防火牆。如果您使用啟動載入來部署 VM-Series 防火牆，您可以在 initi-cfg.txt 檔案中使用 **op-cmd-dpdk-pkt-io=off** 停用 DPDK，以避免重新啟動防火牆。如需詳細資訊，請參閱 在 AWS 上啟動 VM-Series 防火牆。
- HA 配對中的主動防火牆必須最少擁有三個 ENI：兩個資料平面介面與一個管理介面。

  HA 配對中的被動防火牆必須擁有一個 ENI 用於管理，以及一個 ENI 用作資料平面介面；您將資料平面設定為 HA2 介面。

  請勿將額外的資料平面附加至 *HA* 配對中的被動防火牆。在故障復原時，先前主動防火牆的資料平面介面將移至（卸除，然後連接）現在的主動防火牆（之前的被動防火牆）。
- 必須在相同的 AWS 可用性區域中部署 HA 端點。

STEP 2 | 在 AWS 上啟動 VM-Series 防火牆。

STEP 3 | （VM-Series 外掛程式 2.0.1 或更新版本）在主動和被動防火牆上停用 DPDK。DPDK 預設為啟用，但介面移動 HA 模式不支援 DPDK，所以必須停用，改以啟用封包 MMAP。

1. 登入被動防火牆 CLI。
2. 使用下列命令停用 DPDK。執行此命令會重新啟動防火牆。

   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

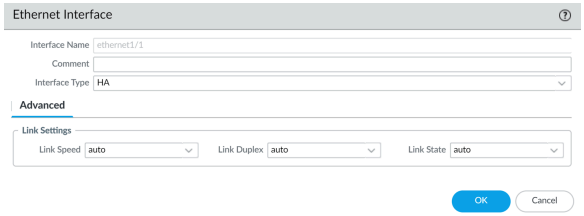
STEP 4 | 啟用 HA。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 [Setup（設定）] 區段。
2. 選取 **Enable HA**（啟用 **HA**）。

©2023 Palo Alto Networks, Inc.

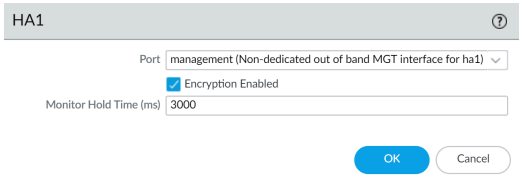
STEP 5 | 將 ethernet 1/1 設定為 HA 實例。此介面必須用於 HA2 通訊。

1. 選取 **Network**（網路） > **Interfaces**（介面）。
2. 確保 ethernet1/1 的連結狀態為啟動。
3. 按一下 ethernet1/1 的連結，然後將 **Interface Type**（介面類型）設定為 HA。



STEP 6 | 將控制連結 (HA1) 設定為使用管理連接埠。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 [Control Link (HA1)（控制連結 (HA1)）] 區段。

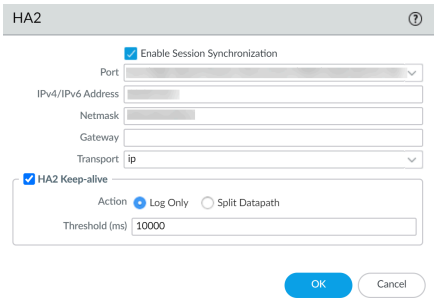


2. （選用）選取 **Encryption Enabled**（啟用加密），以保護對等之間的 HA 通訊安全。若要啟用加密，必須從設備中匯出 HA 金鑰再匯入對等設備。
   1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證）。
   2. 選取匯出 **Export HA key**（匯出 **HA** 金鑰）。將 HA 金鑰儲存至對等設備可存取的網路位置。
   3. 在對等裝置上，導覽至 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證），並選取 **Import HA key**（匯入 **HA** 金鑰）以瀏覽至金鑰儲存位置，然後將金鑰匯入到對等裝置。

©2023 Palo Alto Networks, Inc.

STEP 7 | 設定資料連結 (HA2) 以使用 ethernet1/1。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 [Data Link (HA2)（資料連結 (HA2)）] 區段。
2. 選取 **Port**（連接埠）ethernet1/1。
3. 輸入 ethernet1/1 的 IP 位址。此 IP 位址必須與指派給 EC2 儀表板上的 ENI 的 IP 位址相同。
4. 輸入 **Netmask**（網路遮罩）。
5. 如果 HA1 介面位於不同子網路，輸入 **Gateway**（閘道）IP 位址。
6. 選取 **IP** 或 **UDP** 作為 **Transport**（傳輸）用途。如果您需要 Layer 3 傳輸（IP 通訊協定編號 99）則使用 **IP**。如果您想要防火牆在完整封包而非僅僅是標頭上計算總和檢查碼，與 IP 選項相同（UDP 連接埠 29281），則使用 **UDP**。



7. （選用）修改 **HA2 Keep-alive**（**HA2** 保持活動）封包的 **Threshold**（閾值）。依預設，可啟用 **HA2 Keep-alive**（**HA2** 保持運作）對端點之間 HA2 資料連結進行監控。如果發生故障且超過此臨界值（預設值為 10000 毫秒），則會發生定義的動作。發生 HA2 keep-alive（HA2 保持運作）故障時，會產生重要系統日誌訊息。

> 您可以在兩個設備都設定 ***HA2 keep-alive***（***HA2*** 保持運作）選項，或僅設定 *HA* 配對中的一個設備。如果您在一部設備上啟用此選項，僅該設備會傳送保持運作訊息。

STEP 8 | 設定裝置優先順序及啟用先佔。

如果您想要確定特定設備是偏好的主動設備，則使用此設定。相關資訊，請參閱裝置優先順序及先佔。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 [Election Settings（選取設定）] 區段。
2. 設定 **Device Priority**（裝置優先順序）中的數值。請確定在要指定較高優先順序的設備上設定較小的數值。

> 如果兩個防火牆具備相同的設備優先順序值，則 *HA1* 控制連結上有最小 *MAC* 位址的防火牆會成為主動設備。

3. 選取 **Preemptive**（先佔）。

   您必須在主動與被動設備上啟用先佔。
4. 修改故障復原計時器。依預設，HA 計時器設定檔是設定為 **Recommended**（建議的）設定檔，並且適用於最近的 HA 部署。

©2023 Palo Alto Networks, Inc.

STEP 9 | （選用）修改在觸發容錯移轉之前的等候時間。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 [Active/Passive Settings（主動/被動設定）]。
2. 將 **Monitor fail hold up time**（監控失敗維持時間）修改為 1-60 分鐘之間的值；預設為 1 分鐘。此為防火牆在連結監控失敗後，將於其間保持使用中狀態的時間間隔。使用此設定，可避免由於相鄰設備偶而波動所致的 HA 故障復原。

STEP 10 | 設定 HA 對等的 IP 位址。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般），然後編輯 [Setup（設定）] 區段。
2. 根據端點輸入 HA1 的 IP 位址。這是指派給管理介面 (ethernet 0/0) 的 IP 位址，也是其他防火牆上的 HA1 連結。
3. 為 **Group ID**（群組 **ID**）設定 1 至 63 之間的數字。雖然該值不用於 AWS 上的 VM-Series 防火牆，但不能將此欄位保留空白。

STEP 11 | 設定其他端點。

在 HA 對等上重複 3 至 9。

STEP 12 | 完成兩個設備的設定後，請確認配對的設備為主動/被動 HA。

1. 存取兩個設備上的 **Dashboard**（儀表盤），然後檢視 **High Availability**（高可用性）Widget。
2. 在主動設備上，按一下 **Sync to peer**（同步處理至端點）連結。
3. 確認設備已配對並同步，如下圖所示：
   - 在被動設備上：本機裝置狀態應顯示為 **passive**（被動），且設定為 **synchronized**（已同步）。
   - 在主動設備上：本機裝置狀態應顯示為 **active**（主動），且設定為 **synchronized**（已同步）。

STEP 13 | 確認故障復原正常運作。

1. 確認 HA 模式。

   show plugins vm_series aws ha failover-mode
2. 確認封包 IO 模式設為封包 MMAP。

   show system setting dpdk-pkt-io
3. 關閉主動 HA 端點。

   1. 在 EC2 儀表板中，選取 **Instances**（實例）。

   2. 在清單中選取 VM-Series 防火牆，然後按一下 **Actions**（動作） > **Stop**（停止）。
4. 檢查被動端點承擔主動端點的角色，且資料背板介面已移至現在的主動 HA 端點。

©2023 Palo Alto Networks, Inc.

在 AWS 上移轉主動/被動 HA

兩種 high availability（高可用性 - HA）都支援，只要部署有需要，您就可以在每個模式之間移轉。因為介面移動模式不支援 DPDK，必須在 VM-Series 防火牆上停用，才能完成移轉。停用 DPDK 需要重新啟動 VM-Series 防火牆，這會影響主動防火牆的任何流量工作階段。

- 在 AWS 上將主動/被動 HA 移轉至次要 IP 模式
- 在 AWS 上將主動/被動 HA 移轉至介面移動模式

在 AWS 上將主動/被動 HA 移轉至次要 IP 模式

請完成下列程序，將現有的 VM-Series 防火牆 HA 配對從介面移動 HA 移轉至次要 IP HA。

次要 *IP* 移動 *HA* 需要 *VM-Series* 外掛程式 *2.0.1* 或更新版本。

STEP 1 | 在被動 HA 對等上升級 VM-Series 外掛程式，接著在主動對等上升級。

STEP 2 | 為主動對等上的所有資料介面建立次要 IP 位址。

1. 登入 AWS EC2 主控台。
2. 選取 **Network Interface**（網路介面），然後選取您的網路介面。
3. 選取 **Actions**（動作） > **Manage IP Addresses**（管理 **IP** 位址） > **IPv4 Addresses**（**IPv4** 位址） > **Assign new IP**（指派新 **IP**）。
4. 將此欄位保留空白，以允許 AWS 動態指派 IP 位址，或輸入 VM-Series 防火牆子網路範圍內的 IP 位址。
5. 按一下 **Yes**（是）和 **Update**（更新）。

STEP 3 | 將次要彈性（公共）IP 位址與主動對等的不受信任介面建立關聯。

1. 登入 AWS EC2 主控台。
2. 選取 **Elastic IPs**（彈性 **IP**），然後選取要建立關聯的彈性 IP 位址。
3. 選取 **Actions**（動作） > **Associate Elastic IP**（與彈性 **IP** 位址建立關聯）。
4. 在 **Resource Type**（資源類型）下方，選取 **Network Interface**（網路介面）。
5. 選擇要與彈性 IP 位址建立關聯的網路介面。
6. 按一下 **Associate**（關聯）。

STEP 4 | 建立路由表指向包含信任介面的子網路。

1. 選取 **Route Tables**（路由表） > **Create route table**（建立路由表）。
2. （選用）輸入路由表的描述性 **Name tag**（名稱標籤）。
3. 選取您的 **VPC**。
4. 按一下 **Create**（建立）。
5. 選取 **Subnet Associations**（子網路關聯） > **Edit subnet associations**（編輯子網路關聯）。
6. 針對包含信任介面的子網路，選取 **Associate**（關聯）核取方塊。
7. 按一下 **Save**（儲存）。

©2023 Palo Alto Networks, Inc.

STEP 5 | 以移轉至次要 IP 移動 HA 所需的額外動作和權限，更新 IAM 角色。

IAM 動作、權限或資源	說明
AssociateAddress	允許將主要 IP 位址相關聯的公共 IP 位址，從被動介面移至主動介面。
AssignPrivateIpAddresses	允許將次要 IP 位址和相關聯的公共 IP 位址，從被動介面移至主動介面。
UnassignPrivateIpAddress	允許從主動對等的介面取消指派次要 IP 位址和相關聯的公共 IP 位址。
DescribeRouteTables	允許擷取與 VM-Series 防火牆實例相關聯的所有路由表。
ReplaceRoute	允許更新 AWS 路由表項目。
GetPolicyVersion	允許擷取 AWS 政策版本資訊。
GetPolicy	允許擷取 AWS 政策資訊。
ListAttachedRolePolicies	允許擷取連接至特定 IAM 角色的所有受管理政策的清單。
ListRolePolicies	允許擷取內嵌於特定 IAM 角色中的內嵌政策名稱清單。
GetRolePolicy	允許擷取內嵌於特定 IAM 角色中的特定內嵌政策。
policy	允許存取 IAM 政策 Amazon Resource Name (ARN)。
role	允許存取 IAM 角色 ARN。
route-table	允許存取路由表 ARN。
萬用字元 (*)	在 ARN 欄位中使用 * 作為萬用字元。

©2023 Palo Alto Networks, Inc.

STEP 6 | 在與主動防火牆資料介面相同的子網路中，在被動防火牆上建立新的介面 (ENI)。

請勿將次要 *IP* 位址指派給這些新的介面。

1. 開啟 Amazon EC2 主控台。
2. 選取 **Network Interfaces**（網路介面） > **Create Network Interfaces**（建立網路介面）。
3. 輸入新介面的描述性 **Name**（名稱）。
4. 在 **Subnet**（子網路）下方，選取主動防火牆不受信任介面的子網路。
5. 在 **Private IP**（私人 **IP**）下方，將欄位保留空白以允許 AWS 動態指派 IP 位址，或輸入主動防火牆不受信任介面的子網路範圍內的 IP 位址。
6. 在 **Security groups**（安全性群組）下方，選取一個或多個安全性群組。
7. 選取 **Yes**（是）和 **Create**（建立）。
8. 選取 **Actions**（動作） > **Change Source/Dest.Check**（變更來源/目的地檢查），然後選取 **Disable**（停用）。
9. 針對主動防火牆不受信任介面的子網路，重複這些步驟。

STEP 7 | 將新的 ENI 連接至被動防火牆實例。您必須依正確順序將這些 ENI 連接至被動防火牆，因為次要 IP HA 方法是根據 AWS 指派的網路介面索引。例如，如果主動防火牆的 eth1/2 是子網路 A 的一部分，而 eth1/3 是子網路 B 的一部分，則您必須連接屬於子網路 A 的介面和屬於子網路 B 的介面。在此範例中，AWS 已指派索引值 2 給 eth1/2，並指派值 3 給 eth1/3。必須維護此索引編製，容錯移轉才會成功。

1. 若要連接上述建立的 ENI，請選取您建立的不受信任介面，然後按一下 **Attach**（連接）。
2. 選取被動防火牆的實例 ID，然後按一下 **Attach**（連接）。
3. 針對信任介面重複這些步驟。

STEP 8 | 登入被動防火牆，將介面設為透過 DHCP 取得其 IP 位址。

1. 登入被動 VM-Series 防火牆網頁介面。
2. 選取 **Network**（網路） > **Interfaces**（介面）。
3. 按一下第一個資料介面。
4. 選取 **IPv4**。
5. 選取 **DHCP Client**（**DHCP** 用戶端）。
6. 只在不受信任介面上，選取 **Automatically create default route pointing to default gateway provided by server**（自動建立指向伺服器所提供之預設閘道的預設路由）。
7. 按一下 [OK（確定）]。
8. 針對每個資料介面重複此程序。

©2023 Palo Alto Networks, Inc.

STEP 9 | 如果您在 VM-Series 防火牆上已設定任何 NAT 政策來參考資料介面的私人 IP 位址，則必須更新這些政策，改為參考新指派的次要 IP 位址。

1. 存取主動 VM-Series 防火牆的網頁介面。
2. 選取 **Policies**（政策） > **NAT**。
3. 按一下要修改的 NAT 政策規則，然後按一下 **Translated Packet**（轉譯的封包）。
4. 在 **Translated Address**（轉譯的位址）下方，按一下 [Add（新增）]，然後輸入 AWS 中建立的次要 IP 位址。
5. 刪除主要 IP 位址。
6. 按一下 **OK**（確定）。
7. 視需要重複這些步驟。
8. **Commit**（提交）您的變更。

STEP 10 | 啟用次要 IP HA 容錯移轉模式。

1. 在主動對等上存取 VM-Series 防火牆 CLI。
2. 執行下列命令。

   ```
   request plugins vm_series aws ha failover-mode secondary-ip
   ```

3. Commit（提交）您的變更。
4. 執行下列命令來確認 HA 模式。

   ```
   show plugins vm_series aws ha failover-mode
   ```

5. 在被動對等上重複此命令。

STEP 11 | 完成兩個防火牆的 HA 設定後，請確認配對的防火牆為主動/被動 HA。

1. 存取兩個防火牆上的 **Dashboard**（儀表板），然後檢視高可用性 Widget。
2. 在主動 HA 對等上，按一下 **Sync to peer**（同步處理至對等）。
3. 確認防火牆已配對並同步。
   - 在被動防火牆上：本機防火牆狀態應顯示為 **Passive**（被動），而 **Running Config**（執行中設定）應顯示為 Synchronized（已同步）。
   - 在主動防火牆上：本機防火牆狀態應顯示為 **Active**（主動），而執行中設定應顯示為 **synchronized**（已同步）。
4. 從防火牆 command line interface（命令列介面 - CLI），執行下列命令：
   - 確認容錯移轉備妥情況：

     ```
     show plugins vm_series aws ha state
     ```

   - 顯示次要 IP 對應：

     ```
     show plugins vm_series aws ha ips
     ```

在 AWS 上將主動/被動 HA 移轉至介面移動模式

請完成下列程序，將現有的 VM-Series 防火牆 HA 配對從次要 IP HA 移轉至介面移動 HA。

©2023 Palo Alto Networks, Inc.

STEP 1 | 在被動 HA 對等上停用 DPDK 支援。介面移動 HA 模式不支援 DPDK，所以必須停用，改以啟用封包 MMAP。

1. 登入被動防火牆 CLI。
2. 使用下列命令停用 DPDK。執行此命令會重新啟動防火牆。

   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

STEP 2 | 在主動 HA 對等上停用 DPDK 支援。

1. 登入主動防火牆 CLI。
2. 使用下列命令停用 DPDK。執行此命令會重新啟動防火牆。

   ```
   admin@PA-VM> set system setting dpdk-pkt-io off
   ```

   重新啟動防火牆會影響流量。

STEP 3 | 將主動對等上的 HA 模式從次要 IP 模式變更為介面移動模式。

1. 在主動對等上存取 VM-Series 防火牆 CLI。
2. 執行下列命令。

   ```
   request plugins vm_series aws ha failover-mode interface-move
   ```

3. Commit（提交）您的變更。
4. 執行下列命令來確認 HA 模式。

   ```
   show plugins vm_series aws ha failover-mode
   ```

5. 在被動對等上重複此命令。

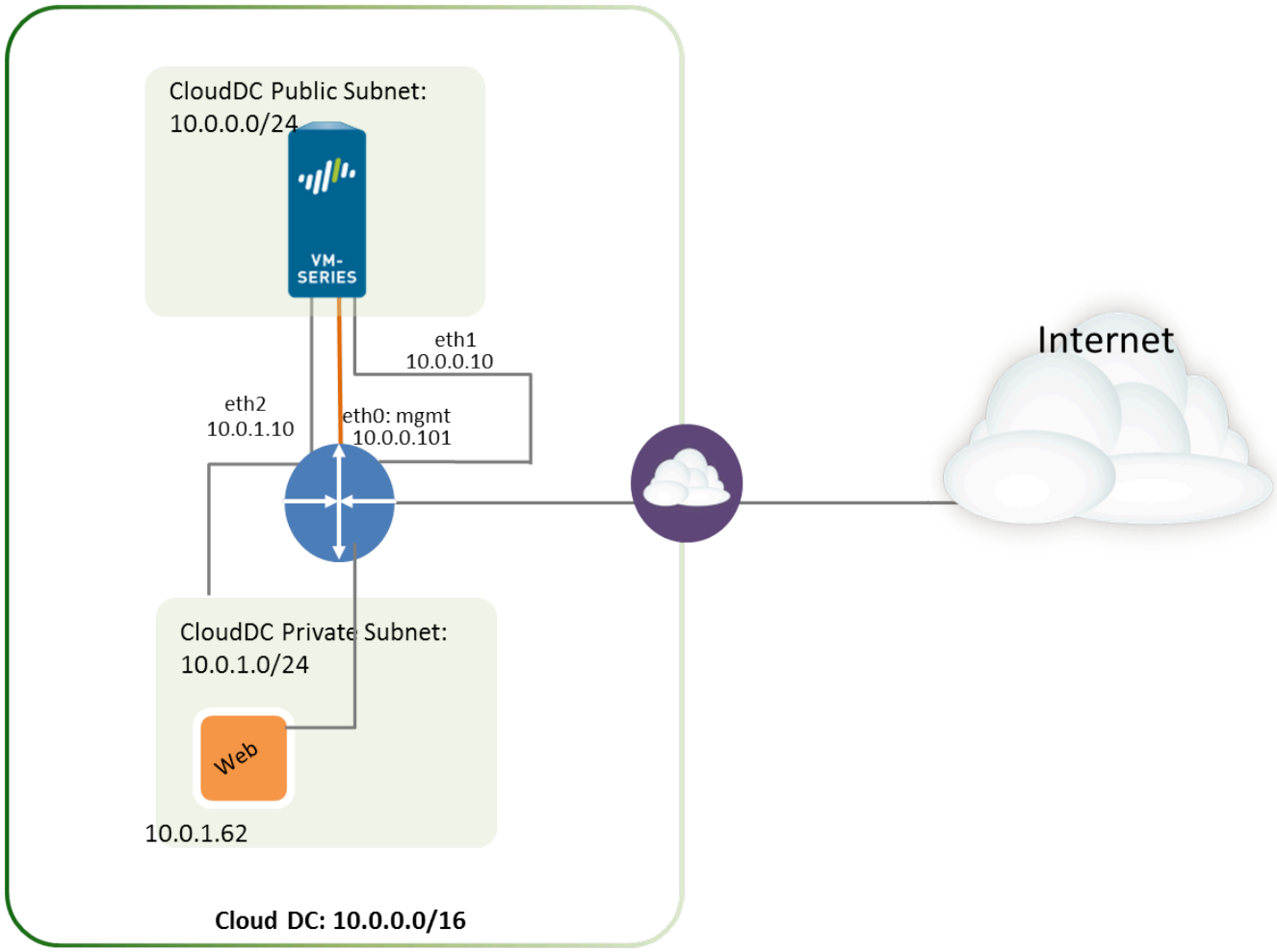
STEP 4 | 從被動防火牆實例刪除資料介面。

1. 登入 AWS EC2 主控台。
2. 選取 **Network Interfaces**（網路介面）。
3. 在被動防火牆實例上選取資料介面，然後按一下 **Delete**（刪除）。
4. 在 **Delete Network Interface**（刪除網路介面）視窗中，按一下 **Yes, Delete**（是，刪除）。
5. 針對被動防火牆實例上的每個資料介面，重複此程序。

©2023 Palo Alto Networks, Inc.

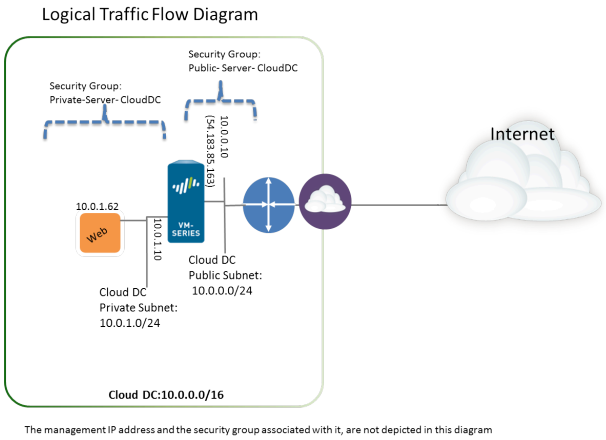
使用案例：保護 AWS 雲端中的 EC2 實例

在此範例中，VPC 部署在具有兩個 /24 子網路的 10.0.0.0/16 網路：10.0.0.0/24 與 10.0.1.0/24。VM-Series 防火牆將在網際網路閘道連接的 10.0.0.0/24 子網路中啟動。10.0.1.0/24 子網路是私人子網路，將代管必須由 VM-Series 防火牆保護的 EC2 實例；此私人子網路上的任何伺服器會為可路由的 IP 位址（為彈性 IP 位址）使用 NAT，以存取網際網路。使用為 AWS VPC 中的 VM-Series 規劃工作表在 VPC 內規劃設計；記錄 EC2 實例的子網路範圍、網路介面與相關聯的 IP 位址，及記錄安全性群組，將使用設定程序更容易、更有效率。



下圖說明流量在 Web 伺服器與網際網路之間往返的邏輯流向。進/出 Web 伺服器的流量會傳送至與私人子網路連接的 VM-Series 防火牆其資料介面。防火牆會套用傳入/傳出在 VPC 的網際網路閘道進/出之流量的原則與程序。該圖也顯示連接資料介面的安全性群組。

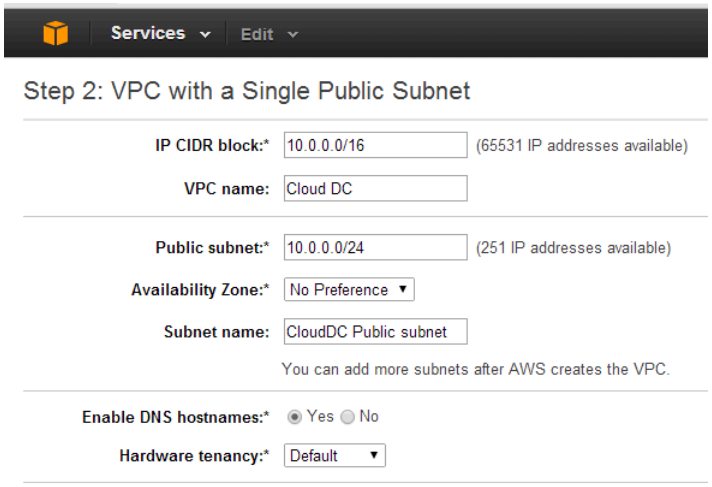
©2023 Palo Alto Networks, Inc.



STEP 1 | 建立含公共子網路的新 VPC（或選取現有的 VPC）。

1. 登入 AWS 主控台，然後選取 **VPC** 儀表板。
2. 確認您選取了正確的地理區域（AWS 地區）。VPC 將部署在目前所選的地區中。
3. 選取 **Start VPC Wizard**（啟動 **VPC** 精靈），然後選取 **VPC with a Single Public Subnet**（含單一公共子網路的 **VPC**）。

   在此範例中，VPC 的 IP CIDR 區塊為 10.0.0.0/16，VPC 名稱為 Cloud DC，公共子網路為 10.0.0.0/24，子網路名稱為 Cloud DC Public subnet。您將在建立 VPC 後建立私人子網路。



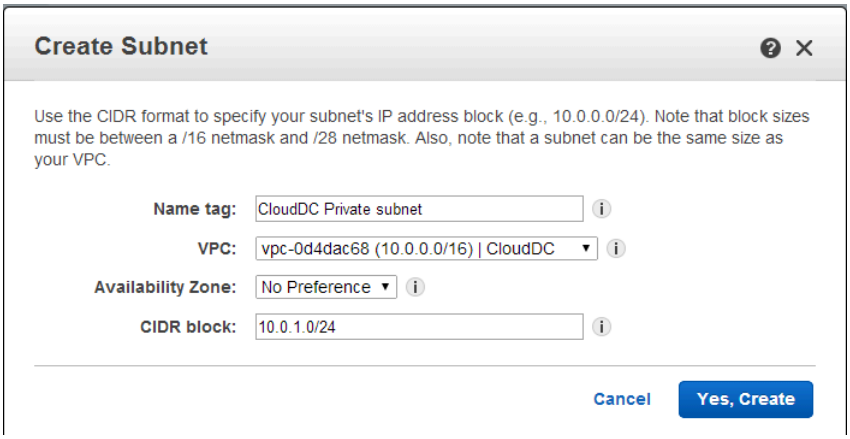
4. 按一下 **Create VPC**（建立 **VPC**）。

 ©2023 Palo Alto Networks, Inc.

STEP 2 | 建立私人子網路。

選取 **Subnets**（子網路），然後按一下 **Create a Subnet**（建立子網路）。填入資訊。

在此範例中，子網路的 **Name tag**（名稱標籤）是 Web/DB Server Subnet，此子網路建立在雲端資料中心 VPC 中，指派給子網路的 CIDR 區塊為 10.0.1.0/24。



©2023 Palo Alto Networks, Inc.

STEP 3 | 為每個子網路建立新路由表。



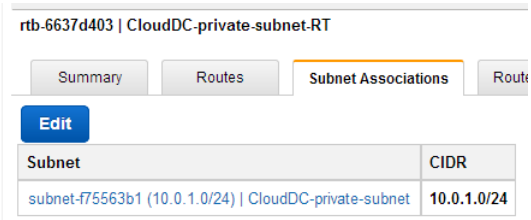
雖然系統會自動在 *VPC* 上建立主要路由表，但我們建議建立新的路由表，而不要修改現有的路由表。

為了導向每個子網路的輸出流量，您會在此工作流程的後面將路由新增至與每個子網路關聯的路由表。

1. 選取 **Route Tables**（路由表） > **Create Route Table**（建立路由表）。
2. 新增 **Name**（名稱），例如 CloudDC-public-subnet-RT，選取您在步驟 1 中建立的 **VPC**，然後按一下 **Yes, Create**（是，建立）。
3. 選取路由表，按一下 **Subnet Associations**（子網路關聯），然後選取公共子網路。



4. 選取 **Create Route Table**（建立路由表）。
5. 新增 **Name**（名稱），例如 CloudDC-private-subnet-RT，選取您在步驟 1 中建立的 **VPC**，然後按一下 **Yes, Create**（是，建立）。
6. 選取路由表，按一下 **Subnet Associations**（子網路關聯），然後選取私人子網路。



©2023 Palo Alto Networks, Inc.

STEP 4 | 建立安全性群組，將輸入/輸出網際網路的存取限制在 VPC 中的 EC2 實例。

依預設，AWS 禁止屬於同一個安全性群組的介面之間通訊。

選取 **Security Groups**（安全性群組），然後按一下 **Create Security Group**（建立安全性群組）按鈕。在此範例中，我們會使用下列輸入存取規則建立三個安全性群組：

- CloudDC-Management，指定可連接至 VM-Series 防火牆管理介面的通訊協定與來源 IP 位址。您至少需要 SSH 與 HTTPS。在此範例中，我們在連接至此安全性群組的網路介面上啟用 SSH、ICMP、HTTP 及 HTTPS。

  VM-Series 防火牆的管理介面 (eth 0/0) 將指派給 CloudDC-management-sg。

- Public-Server-CloudDC，指定可透過 VPC 內的 HTTP、FTP、SSH 連線的來源 IP 位址。此群組允許流量從外部網路流向至防火牆。

  VM-Series 防火牆的資料背板介面 eth1/1 將指派給 Public-Server-CloudDC。

- Private-Server-CloudDC，其存取權非常有限，僅允許同一個子網路上的其他 EC2 實例互相通訊，及與 VM-Series 防火牆通訊。

  VM-Series 防火牆的資料背板介面 eth1/2 及私人子網路中的應用程式將連接至此安全性群組。

  下列螢幕擷取畫面顯示了此使用案例的安全性群組。

Name tag	Group ID	Group Name	VPC	Description
CloudDC-private-subnet-sg	sg-6c32c409	Private-Server-CloudDC	vpc-0d4dac68 (10.0.0.0/16) |...	For Private Servers to comm...
CloudDC-public-subnet-sg	sg-6832c40d	Public-Server-CloudDC	vpc-0d4dac68 (10.0.0.0/16) |...	External Traffic to VM-Series
CloudDC-management-sg	sg-9735c3f2	CloudDC-Managment	vpc-0d4dac68 (10.0.0.0/16) |...	CloudDC-Management
	sg-1035c375	default	vpc-0d4dac68 (10.0.0.0/16) |...	default VPC security group

STEP 5 | 部署 VM-Series 防火牆。

在初始啟動期間，系統只會為防火牆連接與設定將作為管理介面的主要網路介面。在步驟 6 中將新增處理資料流量所需的網路介面。

請參閱在 AWS 上部署 VM-Series 防火牆的步驟 3。

©2023 Palo Alto Networks, Inc.

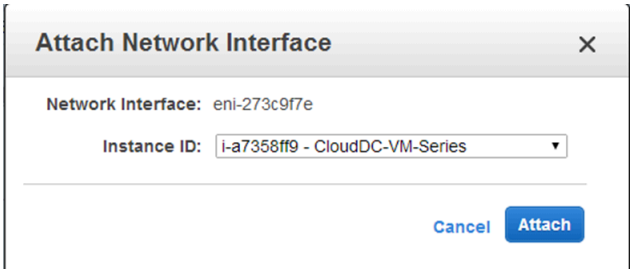
STEP 6 | 建立稱為 Elastic Network Interfaces（彈性網路介面 - ENI）的虛擬網路介面並連接至 VM-Series 防火牆。這些 ENI 用於處理進/出防火牆的資料流量。

1. 在 EC2 儀表板上，選取 **Network Interfaces**（網路介面），然後按一下 **Create Network Interface**（建立網路介面）。
2. 為介面輸入描述性名稱。
3. 選取子網路。使用子網路 ID 確定您已選取正確的子網路。您只能將 ENI 連接至同一個子網路中的實例。
4. 輸入要指派給介面的 **Private IP**（私人 **IP**） 位址，或選取 **Auto-assign**（自動指派）以自動指派所選子網路中可用 IP 位址內的 IP 位址。
5. 選取 **Security group**（安全性群組）以控制存取網路介面。
6. 按一下 **Yes, Create**（是，建立）。

   在此範例中，我們會以下列組態建立兩個介面：

Name	Network interfa	Subnet ID	VPC ID	Zone	Security group	Description	Instance ID
CloudDC-VM-Series-Untrust	eni-bcf355e5	subnet-ef5563a9	vpc-0d4dac68	us-west-1a	Public-Server-...	CloudDC-VM-Series-untrust	i-a7358ff9
CloudDC-VM-Series-Trust	eni-abf355f2	subnet-f75563b1	vpc-0d4dac68	us-west-1a	Private-Server-...	CloudDC-VM-Series-Trust	i-a7358ff9

   - 用於 Eth1/1 (VM-Series Untrust)
     - 子網路：10.0.0.0/24
     - 私人 IP：10.0.0.10
     - 安全性群組：Public-Server-CloudDC
   - 用於 Eth1/2 (VM-Series Trust)
     - 子網路：10.0.1.0/24
     - 私人 IP：10.0.1.10
     - 安全性群組：Private-Server-CloudDC
7. 若要將 ENI 連接至 VM-Series 防火牆，請選取您剛剛建立的介面，然後按一下 **Attach**（附加）。



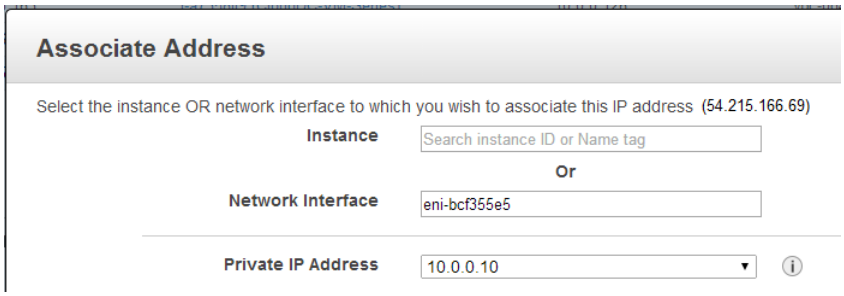
8. 選取 VM-Series 防火牆的 **Instance ID**（實例 **ID**），然後按一下 **Attach**（連接）。
9. 重複步驟 7 與 8 連接其他的網路介面。

©2023 Palo Alto Networks, Inc.

STEP 7 | 建立彈性 IP 位址並連接至需要直接網際網路存取的防火牆資料平面網路介面。

此範例中將 VM-Series _Untrust 指派給 EIP。與介面關聯的 EIP 是私人子網路中的 Web 伺服器可供公開存取的 IP 位址。

1. 選取 **Elastic IPs**（彈性 **IP**），然後按一下 **Allocate New Address**（配置新位址）。
2. 選取 **EC2-VPC**，然後按一下 **Yes, Allocate**（是，配置）。
3. 選取新配置的 EIP，然後按一下 **Associate Address**（建立位址關聯）。
4. 選取 **Network Interface**（網路介面）和與介面關聯的 **Private IP address**（私人 **IP** 位址），然後按一下 **Yes, Associate**（是，建立關聯）。



在此範例中，組態為：

Address	Instance	Private IP Address	Scope	Public DNS
54.183.85.163	i-a7358ff9 (CloudDC-VM-Series)	10.0.0.126	vpc-0d4dac68	ec2-54-183-85-163.us-west-...
54.215.166.69	i-a7358ff9 (CloudDC-VM-Series)	10.0.0.10	vpc-0d4dac68	ec2-54-215-166-69.us-west-...

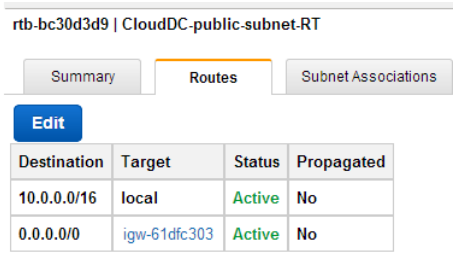
STEP 8 | 停用與 VM-Series 防火牆連接的每個網路介面上的來源/目的地檢查。停用此屬性可讓介面處理其目的地不是其 IP 位址的網路流量。

1. 選取 **Network Interfaces**（網路介面）頁籤中的網路介面。
2. 在 **Action**（動作）下拉式清單中選取 **Change Source/Dest. Check**（變更來源/目的地檢查）。
3. 按一下 **Disabled**（已停用），然後 **Save**（儲存）變更。
4. 針對額外的網路介面（在此範例中為 firewall-1/2）重複步驟 1-3。

©2023 Palo Alto Networks, Inc.

STEP 9 | 在與公共子網路關聯的路由表中（自步驟 3），將預設路由新增至 VPC 的網際網路閘道。

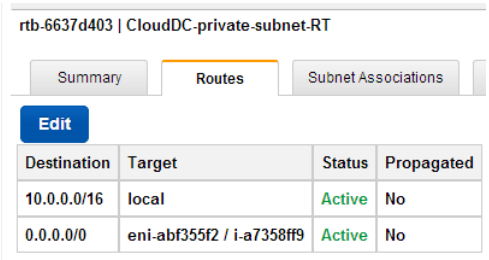
1. 從 VPC 儀表板中，選取 **Route Tables**（路由表），然後尋找與公共子網路關聯的路由表。
2. 選取路由表，選取 **Routes**（路由），然後按一下 **Edit**（編輯）。
3. 新增路由以將此子網路的封包轉送至網際網路閘道。在此範例中，0.0.0.0/0 表示進/出此子網路的所有流量將使用連接至 VPC 的網際網路閘道。



STEP 10 | 在與私人子網路關聯的路由表中新增預設路由，以將流量傳送至 VM-Series 防火牆。

新增此路由可將流量從此私人子網路中的 EC2 實例轉送至 VM-Series 防火牆。

1. 從 VPC 儀表板中，選取 **Route Tables**（路由表），然後尋找與私人子網路關聯的路由表。
2. 選取路由表，選取 **Routes**（路由），然後按一下 **Edit**（編輯）。
3. 新增路由將封包從此子網路轉送至位於同一個子網路的 VM-Series 防火牆網路介面。在此範例中，0.0.0.0/0 表示進/出此子網路的所有流量將使用 VM-Series 防火牆上的 eni-abf355f2（Ethernet 1/2，亦即 CloudDC-VM-Series -Trust）。



對於在私人子網路中的 *EC2* 實例上部署的每個 *Web* 或資料庫伺服器，您必須定義 *VM-Series* 防火牆 *IP* 位址的預設路由，使防火牆成為伺服器的預設閘道。

在 VM-Series 防火牆上執行步驟 11 到 16。

©2023 Palo Alto Networks, Inc.

STEP 11 | 設定防火牆的新管理密碼。

需要有如 ***PuTTY*** 等 ***SSH*** 工具才能存取防火牆上的 ***CLI*** 與變更預設管理密碼。您必須先執行 ***SSH***，再變更預設密碼，才能存取 ***Web*** 介面。

1. 使用您在防火牆上設定的公共 IP 位址，在 VM-Series 防火牆的命令行介面 (CLI) 中執行 SSH。

   需要使用您於在 AWS 上啟動 VM-Series 防火牆的步驟 3-12 中使用或建立的私人金鑰來存取 CLI。
2. 輸入下列命令登入防火牆：

   ssh-i <*private_key_name*> admin@<*public-ip_address*>
3. 使用下列命令設定新密碼，並依照畫面上的提示進行：

   configure

   set mgt-config users admin password

   提交
4. 終止 SSH 工作階段。

STEP 12 | 存取 VM-Series 防火牆的 Web 介面。

開啟網頁瀏覽器，然後輸入管理介面的 EIP。例如：https://54.183.85.163

STEP 13 | 啟動 VM-Series 防火牆上的授權。此步驟僅需要 BYOL 授權；自動啟動依使用授權。

請參閱啟動授權。

©2023 Palo Alto Networks, Inc.

STEP 14 | 在 VM-Series 防火牆上，將防火牆上的資料平面網路介面設定成第 3 層介面。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）。
2. 按一下 **Ethernet 1/1** 的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：**Layer3**
   - 選取 **Config**（設定）頁籤，然後將介面指派給預設路由器。
   - 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 New Zone（新增區域）。定義新地區，例如 untrust，然後按一下 OK（確定）。
   - 選取 IPv4，然後選取 **DHCP Client**（**DHCP** 用戶端）；將自動取得您在 AWS 管理主控台中指派給網路介面的私人 IP 位址。
   - 在 **Advanced**（進階） > **Other Info**（其他資訊）頁籤上，展開 Management Profile（管理設定檔）下拉式清單，然後選取 **New Management Profile**（新增管理設定檔）。
   - 輸入設定檔的 **Name**（名稱），例如 allow_ping，然後選取 Permitted Services（許可的服務）清單中的 **Ping**，然後按一下 **OK**（確定）。
   - 若要儲存介面設定，請按一下 **OK**（確定）。
3. 按一下 **ethernet 1/2**（乙太網路 **1/2**）的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：**Layer3**
   - 選取 **Config**（設定）頁籤，然後將介面指派給預設路由器。
   - 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。定義新區域，例如 trust，然後按一下 **OK**（確定）。
   - 選取 **IPv4**，然後選取 **DHCP Client**（**DHCP** 用戶端）。
   - 在 **IPv4** 頁籤上，清除 **Automatically create default route to default gateway provided by server**（自動建立伺服器所提供之預設閘道的預設路由）核取方塊。對於連接至 VPC 中私人子網路的介面，請停用此選項確定此介面處理的流量不會直接流至 VPC 上的 IGW。
   - 在 **Advanced**（進階） > **Other Info**（其他資訊）頁籤上，展開 Management Profile（管理設定檔）下拉式清單，然後選取您早先建立的 allow_ping 設定檔。
   - 按一下 **OK**（確定）儲存介面組態。
4. 按一下 **Commit**（提交）來儲存變更。確認介面的連結狀態為啟動 。 如果連結狀態不是啟動，請將防火牆重新啟動。

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Security Zone
ethernet1/1	Layer3	allow_ping		Dynamic-DHCP Client	default	untrust
ethernet1/2	Layer3	allow_ping		Dynamic-DHCP Client	default	trust

©2023 Palo Alto Networks, Inc.

STEP 15 | 在 VM-Series 防火牆上，建立「目的地 NAT」與「來源 NAT」規則，以允許在 VPC 內部署的應用程式進/出的輸入/輸出流量。

1. 選取 **Policies**（政策） > **NAT**。
2. 建立將流量從防火牆導向至 Web 伺服器的 Destination NAT（目的地 NAT）規則。
   1. 按一下 **Add**（新增），然後輸入規則的名稱。例如，NAT2WebServer。
   2. 在 **Original Packet**（原始封包）頁籤中，進行下列選取：
      - **Source Zone**（來源區域）：untrust（流量來源）
      - **Destination Zone**（目的地區域）：untrust（與 Web 伺服器的 EIP 關聯的防火牆資料背板介面區域）。
      - **Source Address**（來源位址）：任何
      - **Destination Address**（目的地位址）：10.0.0.10
      - 在 **Translated Packet**（轉譯的封包）頁籤中，選取 Destination Address Translation（目的地位址轉譯）核取方塊，並將 **Translated Address**（轉譯的位址）：設為 10.0.1.62，這是 Web 伺服器的私人 IP 位址。
   3. 按一下 **OK**（確定）。

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	NAT2WebServer	none	untrust	untrust	any	any	10.0.0.10	any	none	address: 10.0.1.62

3. 建立「Source NAT」（來源 NAT）規則以允許從 Web 伺服器流向網際網路的輸出流量。
   1. 按一下 **Add**（新增），然後輸入規則的名稱。例如，NAT2External。
   2. 在 **Original Packet**（原始封包）頁籤中，進行下列選取：
      - **Source Zone**（來源區域）：trust（流量來源）
      - **Destination Zone**（目的地區域）：untrust（與 Web 伺服器的 EIP 關聯的防火牆資料背板介面區域）。
      - **Source Address**（來源位址）：任何
      - **Destination Address**（目的地位址）：任何
   3. 在 **Translated Packet**（轉譯的封包）頁籤的 Source Address Translation（來源位址轉譯）區段中進行下列選取：
      - **Translation Type**（轉譯類型）：Dynamic IP and Port （動態 IP 及連接埠）
      - **Address Type**（位址類型）：轉譯的位址
      - **Translated Address**（轉譯的位址）：10.0.0.10（untrust 區域中的防火牆資料背板介面）。
   4. 按一下 **OK**（確定）。

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	NAT2WebServer	none	untrust	untrust	any	any	10.0.0.10	any	none	address: 10.0.1.62
2	NAT2External	none	trust	untrust	any	any	any	any	dynamic-ip-and-port 10.0.0.10	none

©2023 Palo Alto Networks, Inc.

4. 按一下 **Commit**（提交）儲存 NAT 原則。

STEP 16 | 在 VM-Series 防火牆上，建立安全性原則以管理流量。



請不要輸入 *Web* 伺服器的靜態 *IP* 位址，而是使用動態位址群組。動態位址群組允許您建立會自動調適變更的原則，因此當您在子網路中啟動額外的 *Web* 伺服器時，不需要更新原則。如需詳細資訊，請參閱使用案例：使用動態位址群組保護 VPC 中的新 EC2 實例。

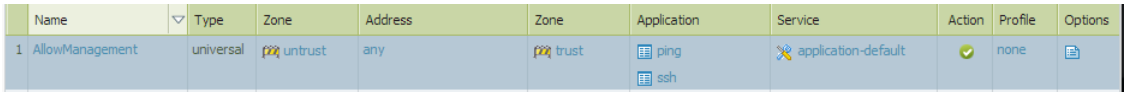
1. 選取 **Policies**（政策） > **Security**（安全性）。

   在此範例中，我們有四個規則。第一個規則允許管理對防火牆流量的存取；第二個規則允許輸入流量流入 Web 伺服器；第三個規則允許網際網路存取 Web 伺服器；最後一個規

©2023 Palo Alto Networks, Inc.

則允許修改預先定義的 interzone-default（內部網路區預設值）規則，以記錄遭拒絕的所有流量。

2. 建立規則以允許管理對防火牆的存取。
   1. 按一下 **Add**（新增），然後輸入規則的 **Name**（名稱）。確認 **Rule Type**（規則類型）為通用。
   2. 在 **Source**（來源）頁籤中，新增 untrust 作為 **Source Zone**（來源地區）。
   3. 在 **Destination**（目的地）頁籤中，新增 trust 作為 **Destination Zone**（目的地地區）。
   4. 在 **Applications**（應用程式）頁籤中，**Add**（新增） ping 與 ssh。
   5. 在 **Actions**（動作）頁籤中，將 **Actions**（動作）設定為 Allow（允許）。
   6. 按一下 **OK**（確定）。



3. 建立規則以允許輸入流量流入 Web 伺服器。
   1. 按一下 **Add**（新增），然後輸入規則的 **Name**（名稱），並確認 **Rule Type**（規則類型）為通用。
   2. 在 **Source**（來源）頁籤中，新增 untrust 作為 **Source Zone**（來源地區）。
   3. 在 **Destination**（目的地）頁籤中，新增 trust 作為 **Destination Zone**（目的地地區）。
   4. 在 **Applications**（應用程式）頁籤中 **Add**（新增） Web 瀏覽。
   5. 在 **Service/URL Category**（服務/URL 類別）頁籤中，確認將服務設定為 application-default（應用程式預設值）。
   6. 在 **Actions**（動作）頁籤中，將 **Actions**（動作）設定為 Allow（允許）。
   7. 在 **Actions**（動作）頁籤的 Profile Settings（設定檔設定）區段中，選取 **Profiles**（設定檔），然後附加防毒、反間諜軟體及漏洞保護的預設設定檔。
   8. 按一下 **OK**（確定）。



4. 建立規則以允許網際網路存取 Web 伺服器。
   1. 按一下 **Add**（新增），然後輸入規則的 **Name**（名稱），並確認 Rule Type（規則類型）為通用。
   2. 在 **Source**（來源）頁籤中，新增 trust 作為 **Source Zone**（來源地區）。
   3. 在 **Source**（來源）頁籤的 Source Address（來源位址）區段中，新增 10.0.1.62，然後新增 Web 伺服器的 IP 位址。
   4. 在 **Destination**（目的地）頁籤中，新增 untrust 作為 **Destination Zone**（目的地地區）。
   5. 在 **Service/URL Category**（服務/URL 類別）頁籤中，確認將服務設定為 **application-default**（應用程式預設值）。
   6. 在 **Actions**（動作）頁籤中，將 **Actions**（動作）設定為 Allow（允許）。

©2023 Palo Alto Networks, Inc.

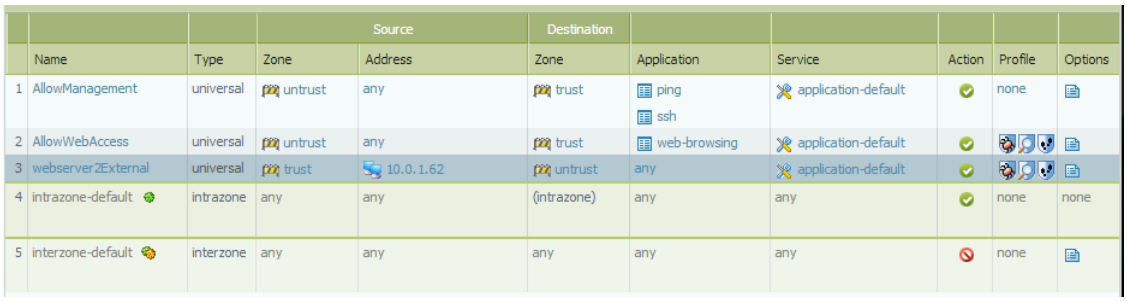
7. 在 **Actions**（動作）頁籤的 Profile Settings（設定檔設定）區段中，選取 **Profiles**（設定檔），然後附加防毒、反間諜軟體及漏洞保護的預設設定檔。
8. 按一下 **OK**（確定）。



5. 編輯「區域間預設值」規則，以記錄所有拒絕的流量。當沒有明確定義其他的規則以比對不同區域之間的流量時，系統會評估預先定義的區域間規則。
   1. 選取 **interzone-default**（內部網路區預設值）規則，然後按一下 **Override**（取代）。
   2. 在 **Actions**（動作）頁籤中，選取 **Log at session end**（同時連線結束時的日誌）。
   3. 按一下 **OK**（確定）。

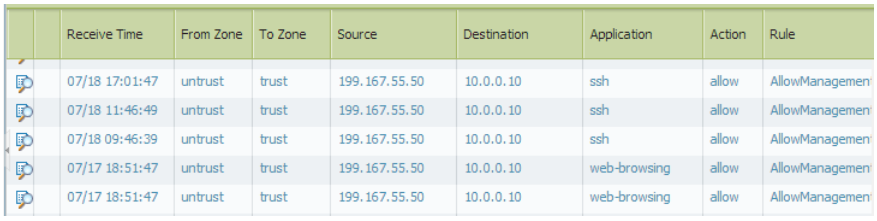


6. 複查在防火牆上定義的一組完整安全性規則。
7. 按一下 **Commit**（提交）儲存原則。



STEP 17 | 確認 VM-Series 防火牆正在保護流量。

1. 啟動網頁瀏覽器，然後輸入 Web 伺服器的 IP 位址。
2. 登入 VM-Series 防火牆的網頁介面，並在 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量）中確認您可看見工作階段的流量日誌。
   - 輸入至 Web 伺服器的流量（抵達 AWS VPC 中的 EC2 實例）：



   - 自 Web 伺服器輸出的流量（AWS VPC 中的 EC2 實例）：



您已成功將 VM-Series 防火牆部署成雲端閘道#

©2023 Palo Alto Networks, Inc.

使用案例：使用動態位址群組保護 VPC 中的新 EC2 實例

在如 AWS-VPC 等您可以視需求啟動新 EC2 的動態環境中，管理安全性原則中的管理負荷很難處理。在安全性原則中使用動態位址群組可使作業更加靈活，並能防止服務中斷或有防護漏洞。

在此範例中，您可在防火牆上使用 VM 資訊來源監控 VPC，並在安全性原則中使用動態位址群組，以探索與保護 EC2 實例。當您註冊 EC2 實例時，動態位址群組會對照符合為群組成員資格所定義準則的所有實例其 IP 位址，接著會為該群組套用安全性原則。此範例中的安全性原則允許網際網路存取群組的所有成員。



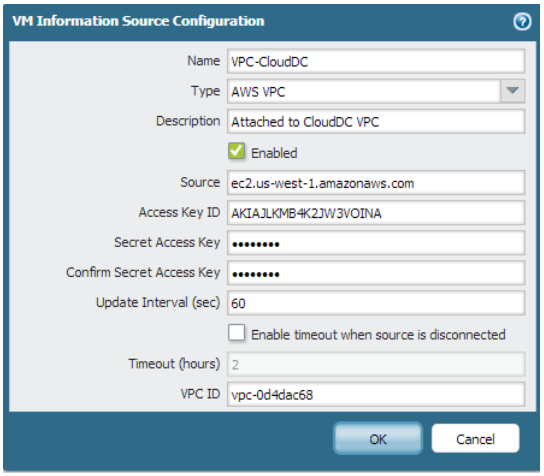
您可選擇使用 ***Panorama*** 作為與 ***VPC*** 通訊的中心點，而非使用防火牆上的 ***VM*** 資訊。在 ***Panorama*** 上使用 ***AWS*** 外掛程式，您可以擷取 ***IP*** 位址-至-標籤對應並註冊關於您設定通知的受管理防火牆的資訊。如需此選項的詳細資訊，請參閱 Panorama 上透過 AWS 外掛程式進行的 VM 監控。

下節中的這個工作流程假設您已建立 AWS VPC，並已在 EC2 實例中部署 VM-Series 防火牆與一些應用程式。如需為 VM-Series 設定 VPC 的指示，請參閱使用案例：保護 AWS 雲端中的 EC2 實例。

©2023 Palo Alto Networks, Inc.

STEP 1 | 設定防火牆以監控 VPC。

1. 選取 **Device**（裝置） > **VM Information Sources**（**VM** 資訊來源）。
2. 按一下 **Add**（新增）並輸入下列資訊：
   1. **Name**（名稱）用來識別您要監控的 VPC。例如，VPC-CloudDC。
   2. 將 **Type**（類型）設為 AWS VPC。
   3. 在 **Source**（來源）中，輸入 VPC 的 URI。語法是 **ec2.*<your_region>*.amazonaws.com**
   4. 新增防火牆所需的認證，以數位簽署對 AWS 服務的 API 呼叫。您必須執行下列操作：
      - **Access Key ID**（存取金鑰 **ID**）：輸入英數字文字字串以唯一識別擁有或授權存取 AWS 帳戶的使用者。
      - **Secret Access Key**（密碼存取金鑰）：輸入密碼並確認輸入。
   5. （選用）將 **Update interval**（更新間隔）修改成在 5-600 秒之間的值。依預設，防火牆每 5 秒會輪詢一次。系會將 API 呼叫排入佇列中並每隔 60 秒擷取這些呼叫，因此更新花費的時間為 60 秒加上所設定的輪詢間隔。



   6. 輸入 **VPC ID**，此 ID 會顯示在 AWS 管理主控台的 VPC 儀表板上。
   7. 按一下 **OK**（確定）並 **Commit**（交付）變更。
   8. 確認連線 **Status**（狀態）顯示為 已連線

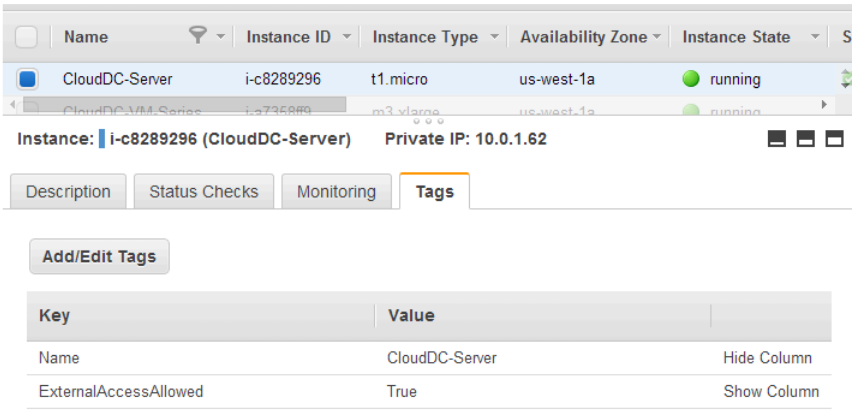
©2023 Palo Alto Networks, Inc.

STEP 2 | 在 VPC 中標記 EC2 實例。

如需 VM-Series 防火牆可監控的標籤清單，請參閱在 AWS VPC 上監控的屬性清單。

標籤為名稱-值配對。您可以在 AWS 管理主控台的 EC2 儀表板上標記 EC2 實例，或使用 AWS API 或 AWS CLI 標記 EC2 實例。

在此範例中，我們使用 EC2 儀表板新增標籤：

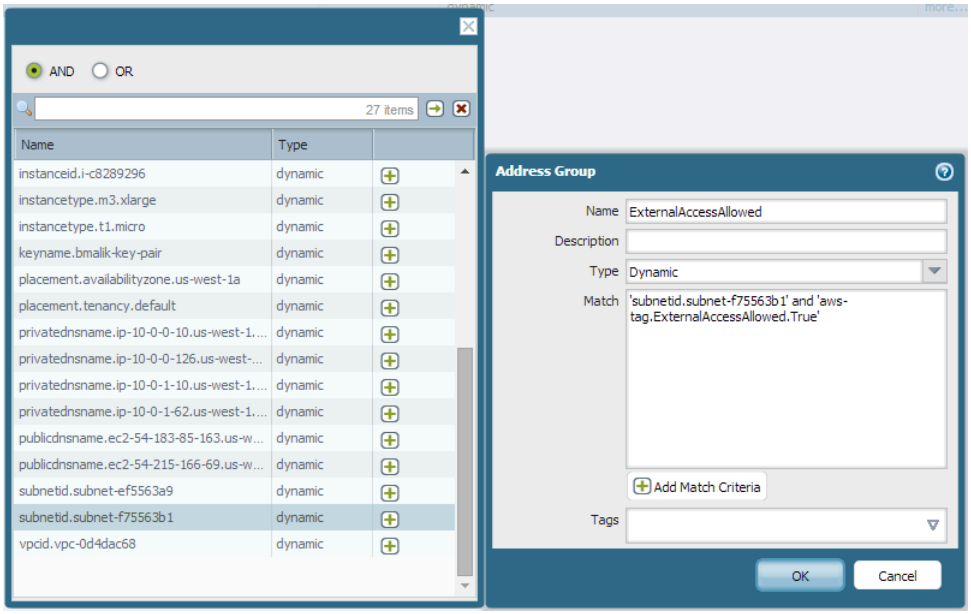


©2023 Palo Alto Networks, Inc.

STEP 3 | 在防火牆上建立動態位址群組。

如需該功能的概況檢視，請參閱教學課程。

1. 選取 **Object**（物件） > **Address Groups**（地址群組）。
2. 按一下 **Add**（新增），再輸入位址群組的 **Name**（名稱）和 **Description**（說明）。
3. 在 **Type**（類型）中選取 **Dynamic**（動態）。
4. 定義比對準則。
   1. 按一下 **Add Match Criteria**（新增比對準則），然後選取 **And** 運算子。
   2. 選取要篩選或比對的屬性。在此範例中，我們選取您剛剛建立的 ExternalAccessAllowed 標籤，以及 VPC 其私人子網路的子網路 ID。



5. 按一下 **OK**（確定）。
6. 按一下 **Commit**（交付）。

©2023 Palo Alto Networks, Inc.

STEP 4 | 在安全性原則中使用動態位址群組。

若要建立規則以允許網際網路存取任何屬於名為 ExternalServerAccess 之動態位址群組的 Web 伺服器。

1. 選取 **Policies**（政策） > **Security**（安全性）。
2. 按一下 **Add**（新增），然後輸入規則的 **Name**（名稱），並確認 **Rule Type**（規則類型）為通用。
3. 在 **Source**（來源）頁籤中，新增 trust 作為 **Source Zone**（來源地區）。
4. 在 **Source**（來源）頁籤的 Source Address（來源位址）區段中，**Add**（新增）您剛剛建立的 ExternalServerAccess 群組。
5. 在 **Destination**（目的地）頁籤中，新增 untrust 作為 **Destination Zone**（目的地地區）。
6. 在 **Service/URL Category**（服務/URL 類別）頁籤中，確認將服務設定為 **application-default**（應用程式預設值）。
7. 在 **Actions**（動作）頁籤中，將 **Actions**（動作）設定為 Allow（允許）。
8. 在 **Actions**（動作）頁籤的 Profile Settings（設定檔設定）區段中，選取 **Profiles**（設定檔），然後附加防毒、反間諜軟體及漏洞保護的預設設定檔。
9. 按一下 **OK**（確定）。

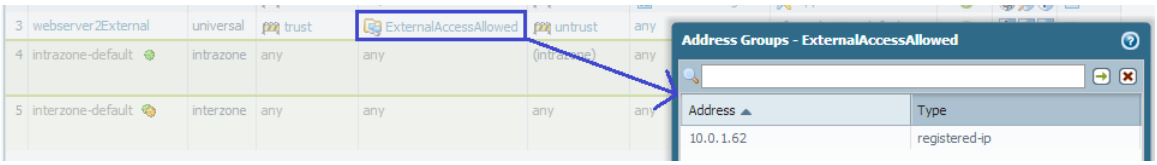


10. 按一下 **Commit**（交付）。

STEP 5 | 確認在防火牆上已填入動態位址群組的成員。

系統將針對屬於此位址群組的所有 IP 位址強制執行原則，並在此處顯示。

1. 選取 **Policies**（原則） > **Security**（安全性），然後選取規則。
2. 選取位址群組連結旁的下拉箭頭，再選取 **Inspect**（檢驗）。您也可以驗證比對準則是否正確。
3. 按一下 **more**（更多）連結，並確認出現已註冊的 IP 位址清單。



 ©2023 Palo Alto Networks, Inc.

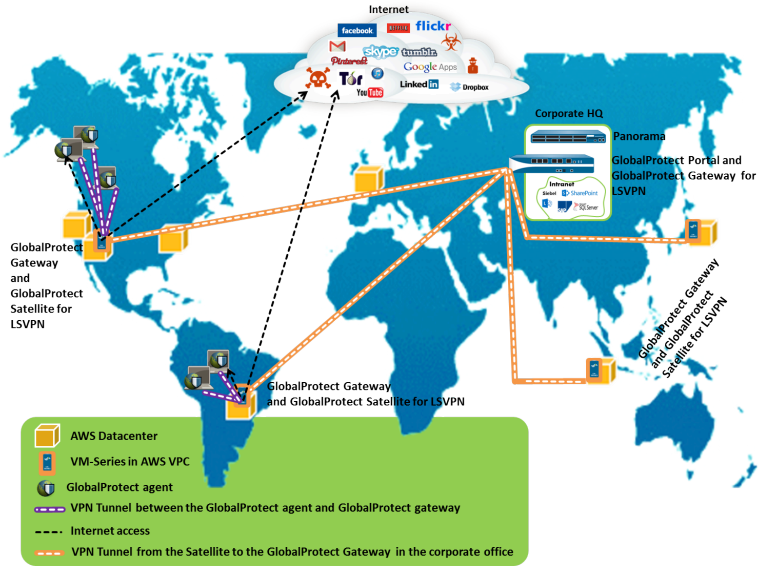
使用案例：將 VM-Series 防火牆作為 AWS 上的 GlobalProtect 閘道

要保護行動使用者不受威脅與高風險應用程式的危害，這並不簡單，通常需要取得與設定安全性和 IT 基礎結構，以滿足全球多個地點的頻寬與執行時間需求，同時在預算範圍內。

對於您所在區域之外的行動使用者所使用的裝置，AWS 上的 VM-Series 防火牆結合了能一致且可靠地保護這類裝置所需的安全性與 IT 物流。透過將 VM-Series 防火牆部署在 AWS 雲端中，您可以快速、輕鬆地在任何地區中部署 GlobalProtect™ 閘道，無須使用您自己資源設定此基礎結構時通常需要的費用或 IT 物流。

若要縮短延遲，請選取最接近您使用的 AWS 區域、在 EC2 實例上部署 VM-Series 防火牆，然後將防火牆設為 GlobalProtect 閘道。有了此解決方案，AWS 雲端中的 GlobalProtect 閘道會為網際網路流量強制實行安全性原則，因此不需要將該流量返回公司網路。此外，為存取公司網路上的資源，AWS 上的 VM-Series 防火牆會使用 LSVPN 功能建立可返回公司網路上防火牆的 IPSec 通道。

為輕鬆部署與集中管理此分散式基礎結構，請使用 Panorama 設定在此解決方案中使用的 GlobalProtect 元件。選取性地確保行動設備，例如智慧型手機與平板電腦，可安全地在網路上使用；請使用 Mobile Device Manager 設定與管理行動設備。



- GlobalProtect 基礎結構的元件
- 在 AWS 上部署 GlobalProtect 閘道

GlobalProtect 基礎結構的元件

為封鎖危險的應用程式並保護行動使用者免受惡意軟體威脅，您必須設定 GlobalProtect 基礎結構以包含 GlobalProtect 入口網站、GlobalProtect 閘道及 GlobalProtect 應用程式。此外，如需存取公司資源，您必須使用 LSVPN 設定在 AWS 上的 VM-Series 防火牆與公司總部防火牆之間的 IPSec VPN 連線（中樞與輻軸 VPN 部署）。

©2023 Palo Alto Networks, Inc.

- GlobalProtect 代理程式/應用程式安裝在每個可存取公司應用程式及資源的一般使用者系統上。代理程式會先連線至入口網站，以取得閘道資訊，然後建立與最接近 GlobalProtect 閘道的安全 VPN 連線。一般使用者系統與閘道之間的 VPN 連線可確保資料的隱私。
- GlobalProtect 入口網站提供 GlobalProtect 基礎結構的管理功能。每個用戶端系統都會收到入口網站的組態資訊，包括可用閘道的相關資訊，以及連線到 GlobalProtect 閘道可能需要的任何用戶端憑證。在此使用案例中，GlobalProtect 入口網站是部署在公司總部中的硬體式防火牆。
- GlobalProtect 閘道會根據應用程式、使用者、內容、設備及設備狀態傳遞行動威脅防禦與原則強制實施。在此使用案例中，AWS 上的 VM-Series 防火牆作為 GlobalProtect 閘道。GlobalProtect 閘道會掃描每個使用者要求中是否有惡意軟體與其他威脅，如果原則允許，則會透過 IPSec 通道將要求傳送至網際網路或公司網路（至 LSVPN 閘道）。
- 對於 LSVPN，您必須設定 GlobalProtect 入口網站、LSVPN 的 GlobalProtect 閘道（中樞），及 GlobalProtect 衛星（輻軸）。

  此使用案例中將公司辦公室的硬體式防火牆部署為 GlobalProtect 入口網站與 LSVPN 閘道，將 AWS 上的 VM-Series 防火牆設為 GlobalProtect 衛星，並設定 GlobalProtect 衛星與閘道以建立在閘道上終止的 IPSec 通道。當行動使用者要求位在公司網路上的應用程式或資源時，VM-Series 防火牆會透過 IPSec 通道路由要求。

在 AWS 上部署 GlobalProtect 閘道

為了保護行動使用者，除了在 AWS 上部署與設定 GlobalProtect 閘道外，您必須設定此整合式解決方案所需的其他元件。下表包含建議的工作流程：

在 AWS 上部署 VM-Series 防火牆。

請參閱在 AWS 上部署 VM-Series 防火牆。

在公司總部設定防火牆。

此使用案例中將防火牆設定為 GlobalProtect 入口網站與 LSVPN 閘道。

- 設定 GlobalProtect 入口網站。
- 設定 LSVPN 的 GlobalProtect 入口網站。
- 設定入口網站以驗證 LSVPN 衛星。
- 設定 LSVPN 的 GlobalProtect 閘道。

在 Panorama 上設定範本，藉此將 AWS 上的 VM-Series 防火牆設定為 GlobalProtect 閘道與 LSVPN 衛星。

若要輕鬆管理此分散式部署，請使用 Panorama 在 AWS 上設定防火牆。

- 在 Panorama 上建立範本。

接著使用下列連結在範本中定義組態。

- 將防火牆設為 GlobalProtect 閘道。
- 備妥衛星以加入 LSVPN。

©2023 Palo Alto Networks, Inc.

在 Panorama 上建立裝置群組，以定義網路存取原則與網際網路存取規則，並套用到 AWS 上的防火牆。

請參閱建立裝置群組。

將範本與裝置群組套用到 AWS 上的 VM-Series 防火牆，然後確認防火牆已正確設定。

部署 GlobalProtect 用戶端軟體。

每個一般使用者系統皆需要 GlobalProtect 代理程式或應用程式，才能連線至 GlobalProtect 閘道。

請參閱部署 GlobalProtect 用戶端軟體。

©2023 Palo Alto Networks, Inc.

AWS 上的資源監控

當您在 AWS 公共雲端中部署或終止資源時，可使用 AWS 專用 Panorama 外掛程式或使用防火牆上的 AWS 資源資訊來源，對這些工作負載一致地執行安全性政策規則。請參閱相容性矩陣，以取得 Panorama 外掛程式版本資訊。

AWS 專用 Panorama 外掛程式專為調整規模而建立，讓您可在 AWS 公共雲端上監控多達 1000 個 AWS VPC。有了此外掛程式，您可將 Panorama 作為錨點來輪詢 AWS 帳戶中的標籤，然後將中繼資料（IP 位址至標籤的對應）散佈至一個裝置群組的多個防火牆。由於 Panorama 會與您的 AWS 帳戶通訊以擷取 AWS 資源資訊，因此您可精簡對雲端環境發出的 API 呼叫次數。使用 Panorama 和 AWS 外掛程式時，您可集中管理標籤擷取和安全性原則，以確保混合和雲端原生架構的原則保持一致。請參閱在 Panorama 上透過 AWS 外掛程式監控 AWS 資源。

如果您沒有 Panorama 或您的部署較為簡單且需要監控的 VPC 在 10 個以下，則您可在防火牆（硬體或 VM-Series 防火牆）上使用 VM 資訊來源對 AWS 工作負載進行監控。您可在動態位址群組中使用防火牆擷取的中繼資料並在安全性原則中引用這些中繼資料來保護 VM 工作負載，因為工作負載會上下旋轉且 IP 位址經常變更。請參閱使用案例：使用動態位址群組保護 VPC 中的新 EC2 實例。

在 Panorama 上透過 AWS 外掛程式監控 AWS 資源

在 AWS 公共雲端部署或終止資源時，您需要設法在 Palo Alto Networks® 防火牆上同步更新安全性政策，才能保護這些 EC2 實例。若要從 Panorama 啟用此功能，您必須在 Panorama 上安裝 AWS 外掛程式並啟用 Panorama 和 AWS VPC 之間的 API 通訊。然後，Panorama 可以收集一組預先定義的屬性（或中繼資料元素）作為 AWS 資源的標籤，並將資訊註冊到 Palo Alto Networks® 防火牆。當您在動態位址群組中參照並在安全性原則規則中比對這些標籤時，可對部署在您的 AWS 帳戶內的所有資產一致地執行原則。

- 在 Panorama 上設定 AWS 外掛程式進行監控
- 在 AWS VPC 上監控的屬性清單

設定 Panorama 上透過 AWS 外掛程式進行的 VM 監控

若要找到您的組織在 AWS 公共雲端中部署的所有虛擬電腦工作負載，您需要在 Panorama 上安裝 AWS 外掛程式並設定監控定義，使 Panorama 能夠驗證 AWS VPC 並擷取有關工作負載的 VM 資訊。Panorama 將擷取正在執行的 VM 的 IP 位址— 公共 IP 位址和私人及次要私人 IP 位址—與相關標籤。如需 Panorama 支援的中繼資料元素清單，請參閱在 AWS VPC 上監控的屬性清單。

在 Panorama 擷取屬性後，若要從 Panorama 推送虛擬電腦資訊至防火牆，您必須將防火牆（硬體或 VM-Series）新增為在 Panorama 上受管理的裝置，並將防火牆分組至一個或多個裝置群組中。然後，您可指定哪些裝置群組屬於通知群組，通知群組是監控定義中的組態元素，Panorama 使用其註冊從 AWS 擷取的 IP 位址-至-標籤對應。

最後，若要在 EC2 實例中一致地執行安全性原則，您必須設定動態位址群組並在允許或拒絕向 VM 的 IP 位址傳送流量的原則規則中參照它們。若要簡化組態並從 Panorama 集中管理原則及物件，您可在 Panorama 上定義動態位址群組與安全性原則規則並將其推送至防火牆，而非在每個防火牆上本機管理動態位址群組和安全性原則規則。

©2023 Palo Alto Networks, Inc.

AWS 外掛程式 *2.0* 版可在 *AWS* 公共雲端、*AWS GovCloud* 和 *AWS China* 上用來監控最多 *1000* 個 *VPC* 的 *EC2* 實例。但由於 *Panorama* 無法部署在 *AWS China* 上，因此 *IAM* 角色不支援 *AWS China* 上的實例設定檔；您必須提供 *AWS* 認證。

- 規劃在 AWS 上進行 VM 監控的檢查清單
- Panorama 的 IAM 角色和權限
- 安裝或升級 AWS 外掛程式
- 設定 AWS 外掛程式以進行 VM 監控

規劃在 AWS 上進行 VM 監控的檢查清單

若要 Panorama 與 AWS API 互動並收集有關 EC2 實例的資訊，您需要建立 IAM 角色並指派授予所需權限的原則以驗證 AWS 並在 VPC 內存取 EC2 實例。您可以新增 100 個 IAM 角色，來管理 Panorama 上最多 1000 個 VPC。

- 收集 VPC ID。
- 在 AWS 上標記 EC2 實例。您可以在 AWS 管理主控台的 EC2 儀表板上標記（定義名稱-值配對） EC2 實例，或使用 AWS API 或 AWS CLI 標記 EC2 實例。如需支援的屬性清單，請參閱在 AWS VPC 上監控的屬性清單。
- 檢查您將啟動監控的 VPC 之間的重複 IP 位址。如果您在 AWS VPC 中有重複的 IP 位址，中繼資料將被附加在一起或進行交換，這可能會在原則執行中導致意外結果。

  重複的 *IP* 位址會寫入至可供您從 *Panorama* 上的 *CLI* 存取的 *plugin_aws_ret.log* 檔案。

- 檢閱 Panorama 和受管理防火牆的需求：
  - 最低系統需求—Panorama 虛擬設備或硬體型 Panorama 設備。

Panorama 的最低需求				
系統資源	記憶體	CPU	受監控的 VPC 數目	已註冊的標籤數目
	16GB	4	1-100	具有 AWS 外掛程式 2.0 版的 Panorama 9.1 已經過測試，可擷取 10,000 個各含 13 個標籤的 IP 位址，或 5000 個各含 25 個標籤的 IP 位址，並且可成功將其註冊至裝置群組內的防火牆。每個 EC2 實例的標籤長度（包括名稱與值）假定為每一標籤 64 位元組。例如，EC2 實例名稱標籤為 aws.ec2.tag.Name.prod-web-app-4523-lvss6j。
	32 GB	8	100-500	
	64 GB	16	500-1000	
Panorama 作業系統版本	9.1 或更新版本			

©2023 Palo Alto Networks, Inc.

Panorama 的最低需求	
AWS 外掛程式版本	2.0.0 或更新版本
授權	Panorama 上用來管理防火牆的有效支援授權和裝置管理授權。 新世代防火牆必須具有有效支援授權。
對 EC2 實例上的中繼資料進行擷取的角色和權限	請參閱 Panorama 的 IAM 角色和權限

- 您必須在 Panorama 上將防火牆新增為受管理的裝置並建立裝置群組以便您設定 Panorama 以通知這些群組其擷取的 VM 資訊。裝置群組可包括 VM-Series 防火牆或硬體防火牆上的虛擬系統。
- 如果您的 Panorama 設備採用高可用性組態，則您必須在兩個 Panorama 端點上手動安裝相同版本的 AWS 外掛程式。此外，如果您使用實例設定檔，則必須將相同的實例設定檔連接至兩個 Panorama 對等。

  您僅在主動 ***Panorama*** 端點上設定 ***AWS*** 外掛程式。提交時，組態將同步至被動 ***Panorama*** 端點。僅主動 ***Panorama*** 端點會輪詢您針對 ***VM*** 監控設定的 ***AWS*** 帳戶。

- 設定 Panorama 所需的認證/權限，以數位簽署對 AWS 服務的 API 呼叫。

  您可以選擇是否要提供長期認證（存取金鑰 ID 和密碼存取金鑰）以啟用存取每個 AWS 帳戶內的資源，或設定 AWS 上的承擔角色允許存取相同 AWS 帳戶或跨帳戶內定義的 AWS 資源。使用承擔角色，您必須設定信任關係並定義權限，同時建立角色本身。這特別適用於跨帳戶部署，而在跨帳戶部署中，查詢中帳戶沒有權限可以查看或處理來自所查詢帳戶的資料。若要讓 Panorama 外掛程式成功驗證 VPC 並擷取標籤，您必須設定承擔角色來使用任何 AWS 服務的 AWS Security Token Service (STS) API。而且查詢中帳戶的使用者必須具有 STS 權限才能查詢承擔角色，以及取得暫時安全性認證來存取資源。如果您的 Panorama 部署在 AWS 上，則您可以選擇使用實例設定檔，而要不提供 IAM 角色的 AWS 認證。實例設定檔包含角色資訊，以及 Panorama 對 AWS 服務的 API 呼叫進行數位簽署所需的相關認證。如需詳細資訊，請參閱Panorama 的 IAM 角色和權限。

Panorama 的 IAM 角色和權限

透過 AWS 外掛程式 2.0 版，您可以使用 IAM 角色或實例設定檔，讓 Panorama 對部署於您 AWS 帳戶內的資源驗證及擷取中繼資料。

- 如果您的 Panorama 不是部署在 AWS 上，您將有兩個選項。您可以為您要監控的 AWS 帳戶提供長期 IAM 認證，或設定 AWS 上的承擔角色，以允許存取相同 AWS 帳戶或跨帳戶內定義的 AWS 資源。建議以「承擔角色」作為較安全的選項。
- 如果您的 Panorama 部署在 AWS 上，則除了前述兩個選項以外，您也可以新增允許 IAM 角色傳至 EC2 實例的實例設定檔。您可以使用讓您所有受監控的資源和 Panorama 都代管於相同帳戶內的實例設定檔，或使用具有跨帳戶存取權之「承擔角色」的實例設定檔，讓 Panorama 和

©2023 Palo Alto Networks, Inc.

受監控的資源部署在不同的 AWS 帳戶。如果您使用實例設定檔，就無須在 Panorama 上輸入您的 AWS 認證。

選項 **1**：具有長期認證的 **IAM** 角色	
所需的角色和權限	與您監控的 VPC/EC2 實例所屬的 AWS 帳戶相關聯的 AWS 認證。 與具有長期認證的 IAM 角色相關聯的最低權限的 JSON 格式如下所示： `{"路徑": "/", "使用者名": "panorama_vm_programmatic", 「使用者 ID":"AIDAIZXXXXCR5JPII4XYZ", "Arn": "arn:aws:iam::412383210500:user/ panorama_vm_programmatic", "建立日期":"2018-07-06T19:14:31Z", "群組清單": [], "附加受管原則": [ { "原則名稱":"唯讀存取", "原則Arn": "arn:aws:iam::aws:policy/唯讀存取" } ] },`
Panorama 上的輸入	在 **Panorama** > **Plugins**（外掛程式） > **AWS** > **Setup**（設定） > **IAM Role**（**IAM** 角色）中，輸入使用者的 **Access Key ID**（存取金鑰 **ID**）和 **Secret Access Key**（密碼存取金鑰）。
選項 **2**：具有承擔角色的 **IAM** 角色	
所需的角色和權限	雖然此選項可用來在相同帳戶內或跨帳戶監控 VPC，但只有在需要藉由承擔角色讓您可存取您通常應可存取的資源，以啟用跨帳戶存取時，我們才會建議使用此選項。 若要從不同的帳戶承擔角色，您的 AWS 帳戶必須受到該角色的信任，且在其信任原則中定義為信任的實體。此外，想要存取不同帳戶中不同角色的使用者，必須具有以安全權杖服務 (STS) 存取權指定角色 ARN 的原則。 在您要監控的帳戶 **1** 上： · 建立具有必要權限的 IAM 角色。若要使用 VM 監控，您必須要有 AmazonEC2ReadOnlyAccess。 · 複製角色 ARN。 · 建立使用者，並將帳戶 2 的帳戶 ID 新增作為信任的實體。這可讓帳戶 2 有權使用此角色來存取帳戶 1 內的資源。 在需要存取帳戶 **1** 的帳戶 **2** 上 · 將下列原則連接至 STS 權限，並修改角色 ARN 以符合您在帳戶 1 中建立的內容。 **`{ "版本":"2012-10-17", "聲明": [ { "效果": "允許", "動作": "sts:承擔角色", "資源":"arn:aws:iam::012347211234:role/PAN-OS-assume-role" } }`**

©2023 Palo Alto Networks, Inc.

Panorama 上的輸入	· 在 **Panorama** > **Plugins**（外掛程式） > **AWS** > **Setup**（設定） > **IAM Role**（**IAM** 角色）中，輸入帳戶 2 使用者的 **Access Key ID**（存取金鑰 **ID**）和 **Secret Access Key**（密碼存取金鑰）。 · 在 **Panorama** > **Plugins**（外掛程式） > **AWS** > **Monitoring Definitions**（監控定義）中，為您要監控的 AWS 帳戶 1 輸入 **Role ARN**（角色 **ARN**）。
選項 **3**：實例設定檔	
所需的角色和權限	只有將 Panorama 部署為 AWS 上的 EC2 執行個體時 請注意，當您使用 *AWS* 管理主控台建立 *IAM* 角色時，主控台會自動建立與該角色名稱相同的執行個體設定檔。由於角色和執行個體設定檔具有相同的名稱，因此當您使用 *IAM* 角色啟動遊覽 *Panorama (EC2* 執行個體*)* 時，相同名稱的執行個體設定檔會與其相關聯。 當 Panorama 與您要監控的資源全都在單一 AWS 帳戶內時。 請建立具有 AmazonEC2ReadOnlyAccess 的 IAM 角色。
Panorama 上的輸入	在 **Panorama** > **Plugins**（外掛程式） > **AWS** > **Setup**（設定） > **IAM Role**（**IAM** 角色）中，選取 **Instance Profile**（實例設定檔）作為選項。
選項 **4**：具有承擔角色的執行個體設定檔	
所需的角色和權限	當 Panorama 與您要監控的資源部署於不同 AWS 帳戶時，請使用具有承擔角色的實例設定檔。 為達到 Panorama HA，請務必將相同的實例設定檔連接至兩個 Panorama 對等。 在已部署您的 **EC2** 實例的帳戶 **1** 上： · 建立 IAM 角色。 · 對這個角色新增已將您的 Panorama 部署為受信任實體的 AWS 帳戶 ID（帳戶 2）。 · 依照先前有關於 VM 監控的詳細說明，連接 JSON 原則。 · 複製角色 ARN。Panorama 必須以此角色來擷取您 EC2 實例或 EKS 叢集上的中繼資料。 在已部署 **Panorama** 的帳戶 **2** 上： · 建立 IAM 角色並連接 JSON 原則（連接至 STS 原則和您從帳戶 1 取得的資源 ARN）。 · 對於每個您額外要監控的 AWS 帳戶，請複製相同的 STS 原則，並修改角色 ARN。
Panorama 上的輸入	· 在 **Panorama** > **Plugins**（外掛程式） > **AWS** > **Setup**（設定） > **IAM Role**（**IAM** 角色）中，選取 **Instance Profile**（實例設定檔）作為選項

©2023 Palo Alto Networks, Inc.

- 在 **Panorama** > **Plugins**（外掛程式） > **AWS** > **Monitoring Definitions**（監控定義）中，為您要監控的 AWS 帳戶輸入 **Role ARN**（角色 **ARN**）。

  在此範例中為帳戶 1。

安裝或升級 **AWS** 外掛程式

若要開始在 AWS 上監控您的 EC2 實例，請參閱「相容性矩陣」，以瞭解支援 VM 監控所需的 AWS 專用 Panorama 外掛程式和 VM-Series 外掛程式版本。

若要將 AWS 專用 Panorama 外掛程式 1.0.1 版安裝升級至 2.0.x 版，您必先升級至 2.0.x 所需的 Panorama 和 VM-Series 外掛程式版本，再依照下列指示安裝以執行升級。



安裝 *AWS* 外掛程式 *2.0* 版後，將無法降級至 *1.0* 版。

如果您有 Panorama HA 設定，請在每個 Panorama 端點上重複安裝/升級程序。



請在規劃的維護期間安裝或解除安裝外掛程式。

如果您目前已安裝任何雲端平台的 Panorama 外掛程式，在安裝（或解除安裝）另一個外掛程式時，將必須重新啟動 Panorama 才能認可變更。

如果您在安裝了多個外掛程式的 HA 配對中安裝了一個獨立的 Panorama 或兩個 Panorama 設備，則在未設定一或多個外掛程式的情況下，外掛程式可能不會收到更新的 IP-Tag 資訊。發生這種情況是因為 Panorama 不會將 IP-Tag 資訊轉送到未設定的外掛程式。此外，如果一或多個 Panorama 外掛程式未處於「已註冊」或「成功」狀態（每個外掛程式的正狀態不同），則可能會出現此問題。在繼續或執行下述命令之前，請確保您的外掛程式處於正狀態。

如果遇到此問題，有兩種權宜方案：

- 解除安裝未設定的外掛程式。建議您不要安裝未打算立即設定的外掛程式
- 您可以使用以下命令來變通處理此問題。對每個 Panorama 實例上的每個未設定外掛程式執行以下命令，以防止 Panorama 等待傳送更新。否則，防火牆可能會遺失一些 IP-Tag 資訊。

  `request plugins dau plugin-name <plugin-name> unblock-device-push yes`

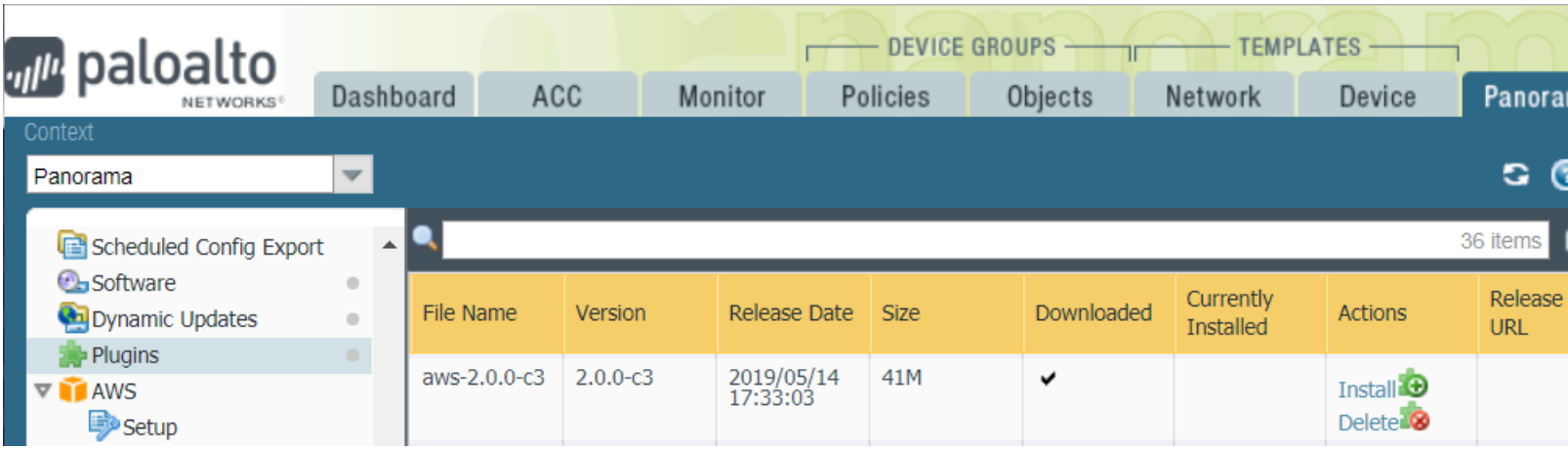
  您可以透過執行以下命令來取消此命令：

  `request plugins dau plugin-name <plugin-name> unblock-device-push no`

上述的命令在重新啟動後不會持續存在，並且必須在任何後續重新啟動時再次使用。對於 HA 配對中的 Panorama，必須在每個 Panorama 上執行命令。

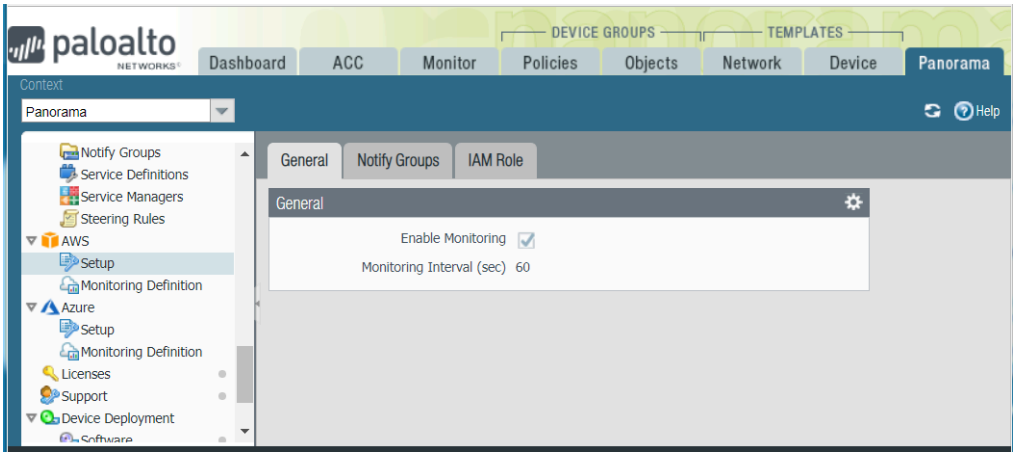
©2023 Palo Alto Networks, Inc.

STEP 1 | 登入 Panorama Web 介面，選取 **Panorama** > **Plugins**（外掛程式），然後按一下 **Check Now**（立即檢查），以取得支援 VM 監控的 **AWS** 外掛程式版本。



STEP 2 | **Download and Install**（下載並安裝）外掛程式。

在您成功安裝後，Panorama 會重新整理，而且 AWS 外掛程式會顯示於 **Panorama** > **Plugins**（外掛程式）頁籤上。



在 *Panorama* ***Dashboard***（儀表板）的 *[General Information*（一般資訊）*] Widget* 上，您可以確認已安裝的 *AWS* 專用 *Panorama* 外掛程式版本。

STEP 3 | （HA 中的 Panorama）**Commit**（認可） > **Commit to Panorama**（認可至 **Panorama**）。

如果您的 Panorama 屬於 HA，請將變更認可至 Panorama 設定，以確保在容錯移轉時會將標籤註冊至 Panorama 對等。

設定 AWS 外掛程式以進行 VM 監控

若要開始在您的 AWS 公共雲端部署中監控虛擬電腦，安裝 AWS 外掛程式後，您必須建立監控定義。此定義指定授權在您要監控的 AWS VPC 內存取 EC2 實例的 IAM 角色，及包含 Panorama 應將其擷取的所有 IP 位址-至-標籤對應推送至的防火牆之通知群組。為了執行原則，您之後必須建立動態位址群組並在安全性原則中引用它們。動態位址群組可讓您篩選要比對的標籤，以便防火牆可取得以每個標籤註冊的公共與私人 IP 位址，然後根據您定義的原則規則允許或拒絕存取傳入和傳出工作負載的流量。

©2023 Palo Alto Networks, Inc.

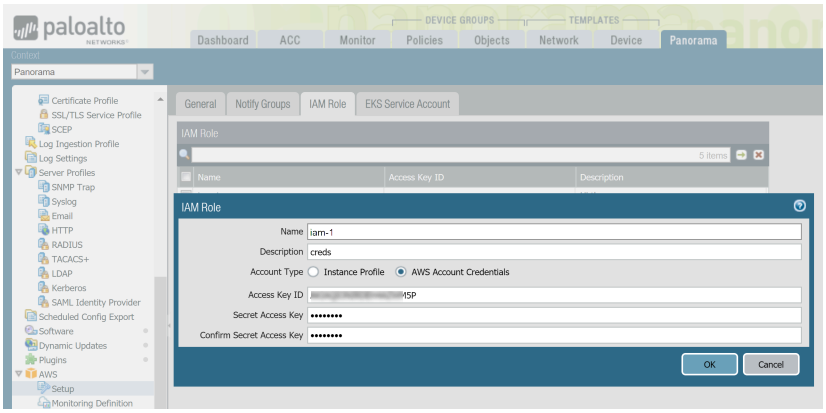
STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 設定下列物件以在 AWS 上啟用 VM 監控。

- 新增 IAM 角色。

  IAM 角色是可讓您委派存取權的實體，讓 Panorama 可以代表您向 AWS 資源（部署為 EC2 實例的虛擬機器）發出服務要求。

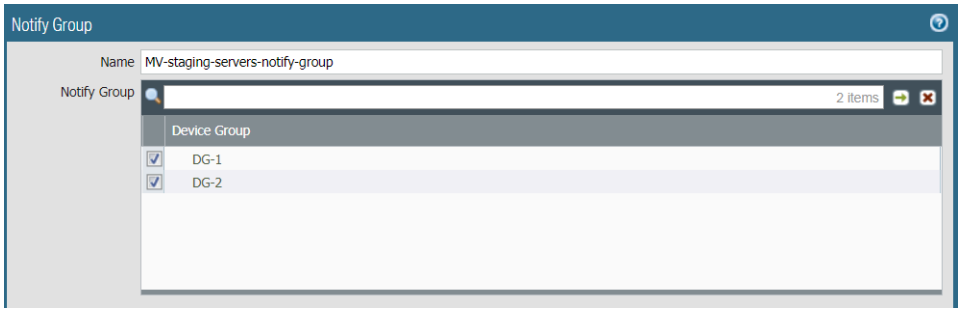
  1. 選取 **Panorama** > **Plugins**（外掛程式） > **AWS** > **Setup**（設定） > **IAM Role**（**IAM** 角色） > **Add**（新增）。

  2. 輸入 **Name**（名稱），然後選擇輸入 **Description**（說明）以識別 IAM 角色。
  3. 選取帳戶類型 — **Instance Profile**（實例設定檔）或 **AWS Account Credentials**（**AWS** 帳戶認證）。如果您的 Panorama 部署在 AWS 上，您可以選擇將具有正確權限的實例設定檔連接至 Panorama，或新增與 Panorama 上的 IAM 角色相關聯的認證。如果您的 Panorama 不是部署在 AWS 上，您就必須在 Panorama 的本機位置輸入 IAM 角色的認證。
  4. （僅適用於 AWS 帳戶認證）輸入 **Secret Access Key**（密碼存取金鑰），並再次輸入加以確認，然後按一下 **OK**（確定）。

- 新增通知群組。

  1. 選取 **Panorama** > **Plugins**（外掛程式） > **AWS** > **Setup**（設定） > **Notify Groups**（通知群組） > **Add**（新增）。

  2. 輸入 **Name**（名稱），以識別 Panorama 將所擷取的 VM 資訊推送至其中的防火牆群組。
  3. 選取 **Device Groups**（裝置群組），即一組 Panorama 將推送其從 AWS VPC 擷取的 VM 資訊（IP 位址-至-標籤對應）至的防火牆或虛擬系統。防火牆會使用此更新，決定構

©2023 Palo Alto Networks, Inc.

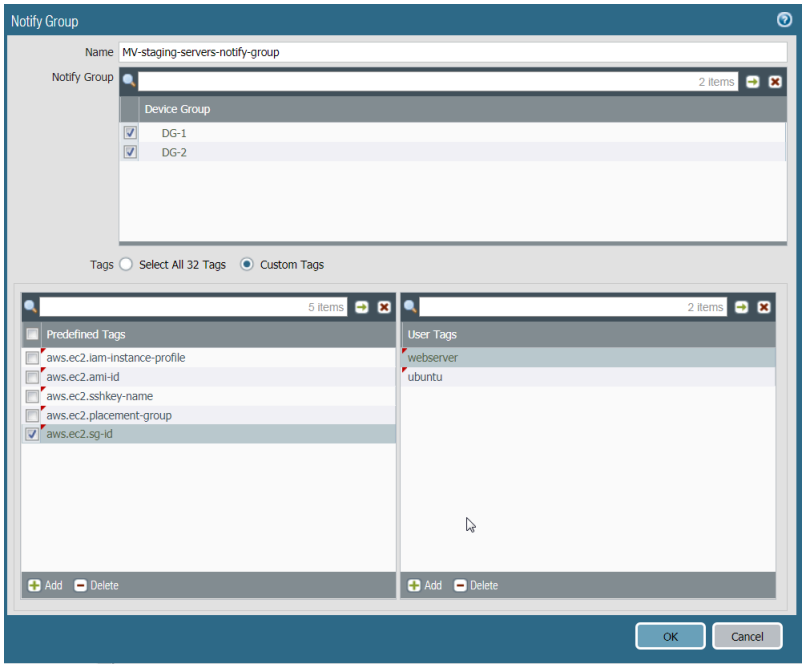
成原則中參照之動態位址群組的最新成員清單。如果您使用的是 Azure 和 AWS 專用 Panorama 外掛程式，您可以將兩種環境下的標籤用於相同的防火牆或虛擬系統。

仔細考慮您的裝置群組。

- 由於監控定義只能包含一個通知群組，因此請確保選取通知群組內的所有相關裝置群組。如果您要解除註冊 *Panorama* 推送至通知群組中所含防火牆的標籤，則必須刪除監控定義。
- 若要在已針對多個虛擬系統啟用的防火牆上註冊標籤至所有虛擬系統，您必須在 *Panorama* 上新增每個虛擬系統至單獨的裝置群組並將裝置群組指派給通知群組。如果您將所有虛擬系統指派給一個裝置群組，*Panorama* 將僅註冊標籤至一個虛擬系統。

4. 選取您要從 AWS VPC 擷取的標籤。

   您可以 **Select All 32 Tags**（選取所有 **32** 標籤）（預設值），或選取您要為實例擷取的 **Custom Tags**（自訂標籤）。使用 [Custom Tags（自訂標籤）] 選項，您可以 **Add**（新增）要用作安全性原則中比對準則的預先定義標籤和使用者定義標籤。如果您監控大量 EC2 實例，則減少您擷取的標籤數目可確保更有效率地使用 Panorama 上的 CPU 和記憶體容量。請參閱規劃在 AWS 上進行 VM 監控的檢查清單以取得相關指引。



- 確認監控已在外掛程式上啟用。必須啟用 Panorama 的此設定才能與 AWS 公共雲端通訊以進行 VM 監控。

  Enable Monitoring（啟用監控）的核取方塊在 **Panorama** > **Plugins**（外掛程式） > **AWS** > **Setup**（設定） > **General**（一般）上。

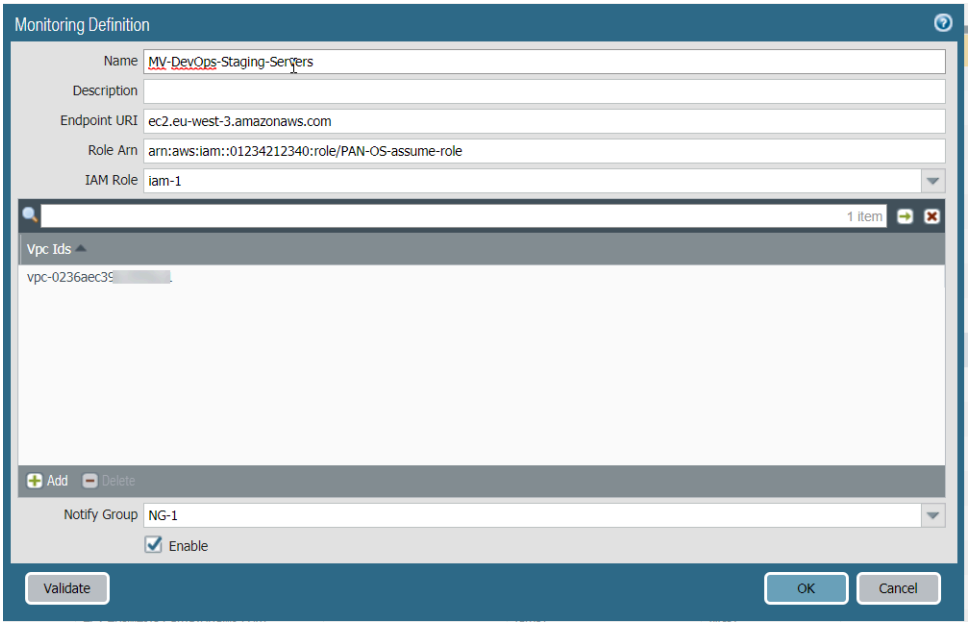
©2023 Palo Alto Networks, Inc.

STEP 3 | 為您要監控的每個 VPC 建立 **Monitoring Definition**（監控定義）。

當您新增監控定義時，其依預設會啟用。

- 選取 **Panorama** > **Plugins**（外掛程式） > **AWS** > **Monitoring Definition**（監控定義），以 **Add**（新增）新的定義。
- 輸入 **Name**（名稱），然後選擇輸入 **Description**（說明）以識別您使用此定義的 AWS VPC。
- 輸入 **Endpoint URI**（端點 **URI**）。語法是 ec2.<your_region>.amazonaws.com；

  對於 AWS 中國，則是 ec2.<your region>.amazonaws.com.cn。
- （選用）輸入 **Role ARN**（角色 **ARN**），如果您已設定角色鏈和具有暫時認證的 IAM 角色，而暫時認證有權使用 AWS STS API 利用相同的帳戶或跨帳戶來存取 AWS 資源。角色 ARN 必須屬於您要監控的 VPC。
- 選取 **IAM Role**（**IAM** 角色），並從 AWS 管理主控台的 [VPC Dashboard（VPC 儀表板）] 中 **Add**（新增）**VPC ID**，然後 **Notify Group**（通知群組）。



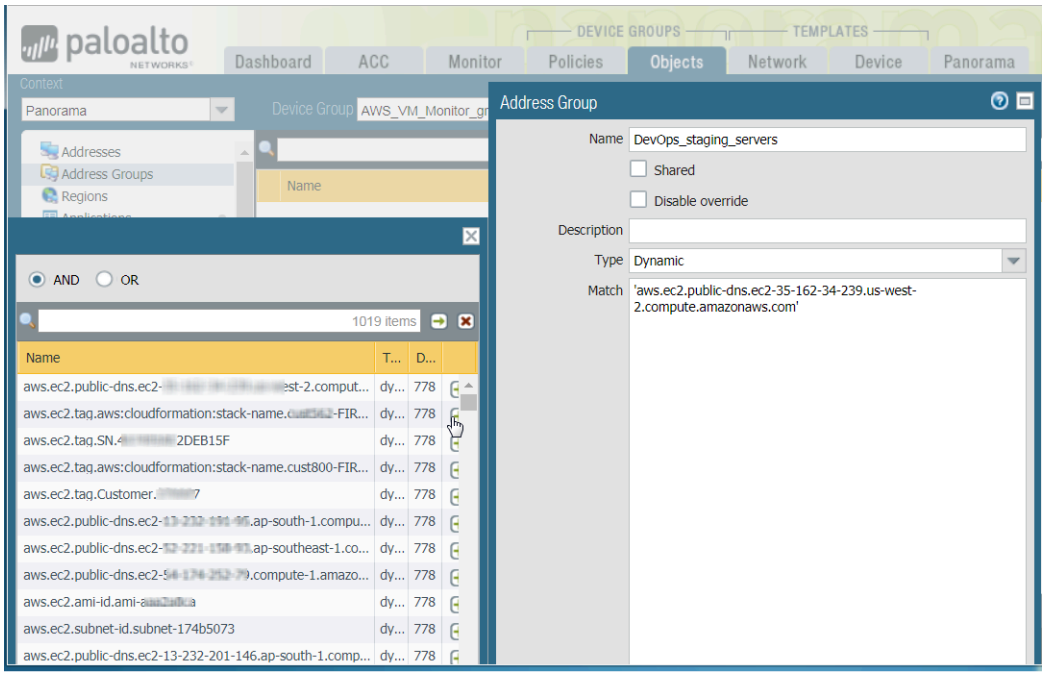
STEP 4 | 在 Panorama 上 **Commit**（提交）變更。

確認監控定義的狀態顯示為「成功」。如果失敗，請確認您已正確輸入 AWS VPC ID 並提供進行授權存取的正確金鑰和 ID。

按一下 ***Validate***（驗證），以確認 *Panorama* 可使用 *IAM* 角色和金鑰進行驗證，並且可與您在上方輸入的 *AWS VPC* 通訊。

©2023 Palo Alto Networks, Inc.

STEP 5 | 確認您可在 Panorama 上檢視 VM 資訊，並定義動態位址群組的比對準則。



HA 容錯移轉時，新的主動 *Panorama* 會嘗試重新連線至 *AWS* 雲端，並擷取所有監控定義的標籤。如果 *Panorama* 無法與您設定並啟用的任何監控定義重新連線，*Panorama* 將產生系統日誌訊息

HA 切換後無法處理帳號；需要使用者干預。

若發生此情況，您必須登入 *Panorama* 並驗證監控定義以修復無效認證或移除無效帳戶。雖然中斷 *Panorama* 與 *AWS* 雲端的連線，但是仍然會保留容錯移轉之前擷取的所有監控定義標籤，而且防火牆可以繼續向該 *IP* 位址清單強制執行政策。*Panorama* 只有在您刪除監控定義時才會移除所有與帳戶相關的標籤。監控此問題的最佳做法是，從 *Panorama* 設定動作導向的日誌轉送至 HTTPS 目的地，以便您立即採取措施。

©2023 Palo Alto Networks, Inc.

STEP 6 | 瞭解可在何處找到與 Panorama 上的 AWS 外掛程式有關的日誌，以進行疑難排解。

- 使用 CLI 命令 **less plugins-log** 檢視所有可用日誌的清單

  plugin_aws_ret.log 會顯示與 IP 位址和標籤擷取有關的日誌。

  plugin_aws_proc.log 會顯示處理已註冊的 IP 位址和標籤時的相關日誌。

  plugin_aws.log 會顯示與 AWS 外掛程式設定和精靈有關的日誌。

使用 **show plugins aws vm-mon-status** 可取得監控定義的狀態。

```
admin@Panorama> show plugins aws vm-mon-status Mon-
Def Name VPC Status Last Updated Time Error Msg
 ------------------------------------------------------------------------------
 MD-Ins-Prof-ARN vpc-07986b091 Success 2019-12-02T10:24:56.007000
 MD-gov vpc-7ea1cf1a Success 2019-12-02T10:24:56.008000 MD-IAM-ARN
 vpc-025a83c123 Success 2019-12-02T10:24:56.012000
```


©2023 Palo Alto Networks, Inc.

使用 Amazon ELB 服務自動調整 VM-Series 防火牆規模

AWS 的 Palo Alto Networks 自動調整規模範本可協助您設定和部署 VM-Series 防火牆，以保護部署於 AWS 中的應用程式。範本會利用 AWS 的擴充功能自動單獨調整在 AWS 中部署的 VM-Series 防火牆，以因應應用程式工作負載資源激增的需求。

- VM-Series 自動化功能包括 PAN-OS API 和啟動（針對 2.0 版使用啟動程序檔案，而針對 2.1 版使用 Panorama）。
- AWS 自動化技術包括 AWS 服務的 CloudFormation 範本和指令碼，例如 Lambda、自動調整規模群組 (ASG)、彈性負載平衡 (ELB)、S3 和 SNS。

您可以在 Palo Alto Networks GitHub 儲存庫（適用於 AWS 中的自動調整規模 VM-Series 防火牆）中取得範本：

- 2.0 版提供一個防火牆範本和一個應用程式範本。這些範本和支援指令碼會在單一 VPC 或多個 VPC 中部署多個 VM-Series 防火牆、一個網際網路連結的防火牆、一個內部防火牆，以及單一虛擬私人雲端 (VPC) 或多個 VPC 中的應用程式 ASG。

  在 2.0 版中，Palo Alto Networks 支援防火牆範本，且應用程式範本支援社群。如需部署詳細資料，請參閱 AWS 專用 VM-Series 自動調整規模範本 2.0 版。
- 2.1 版新增了對單一 VPC 中的部署的支援，以及新增負載平衡器分層式拓撲支援，可讓您將 VM-Series 防火牆部署至前端 VPC，並將後端應用程式部署至透過 VPC 對等或 AWS PrivateLink 所連線的一或多個應用程式 VPC。

  在 2.1 版中，您可以在 VPC 中同時實作應用程式負載平衡器 (ALB) 和網路負載平衡器 (NLB)。2.1 版包含兩個防火牆範本和五個應用程式範本。如需部署詳細資料，請參閱AWS 專用 VM-Series 自動調整規模範本 2.1 版。

如果您具有現有範本部署，則沒有移轉程序。

下表比較每個範本版本的一些高階功能。

功能/需求	版本 **2.0**	版本 **2.1**
以 Panorama 模式執行 PAN-OS 9.0.1 或更新版本的 Panorama。	（選用）如果您選擇使用 Panorama，則必須在 VM-Series 防火牆 VPC 與應用程式 VPC 之間設定 VPC 對等。對等的流量會周遊公共網際網路。	（必要）部署 2.1 版範本。

©2023 Palo Alto Networks, Inc.

功能/需求	版本 2.0	版本 2.1
不支援高可用性 *(HA)* 設定中的 *Panorama*。		在 *Panorama* 上，您必須手動安裝 *VM-Series* 外掛程式，讓 *VM-Series* 防火牆發佈 *PAN-OS* 度量以自動調整規模。
啟動載入	S3 貯體中的 `bootstrap.xml` 設定檔案。	Panorama 的 `init-cfg.txt` 檔案。
Palo Alto Networks S3 貯體範例	使用您自己的 S3 貯體，或使用 panw-aws-autoscale-v20-us-west-2 中的範例。	使用您自己的 S3 貯體來進行部署。
單一 VPC 或單獨 VPC（中樞和輻軸）	是	是
新 VPC	是	是
現有 VPC（棕色欄位）	否。	是
每個 VPC 的可用性區域	2	2-4
外部負載平衡器	僅限 ALB	ALB 或 NLB
內部負載平衡器	僅限 NLB	ALB 或 NLB
與 VM-Series 防火牆 VPC 和後端伺服器的 AWS PrivateLink 連線。	否。	是

如需範本的詳細資料，請參閱：

- AWS 專用 VM-Series 自動調整規模範本 2.0 版
- AWS 專用 VM-Series 自動調整規模範本 2.1 版

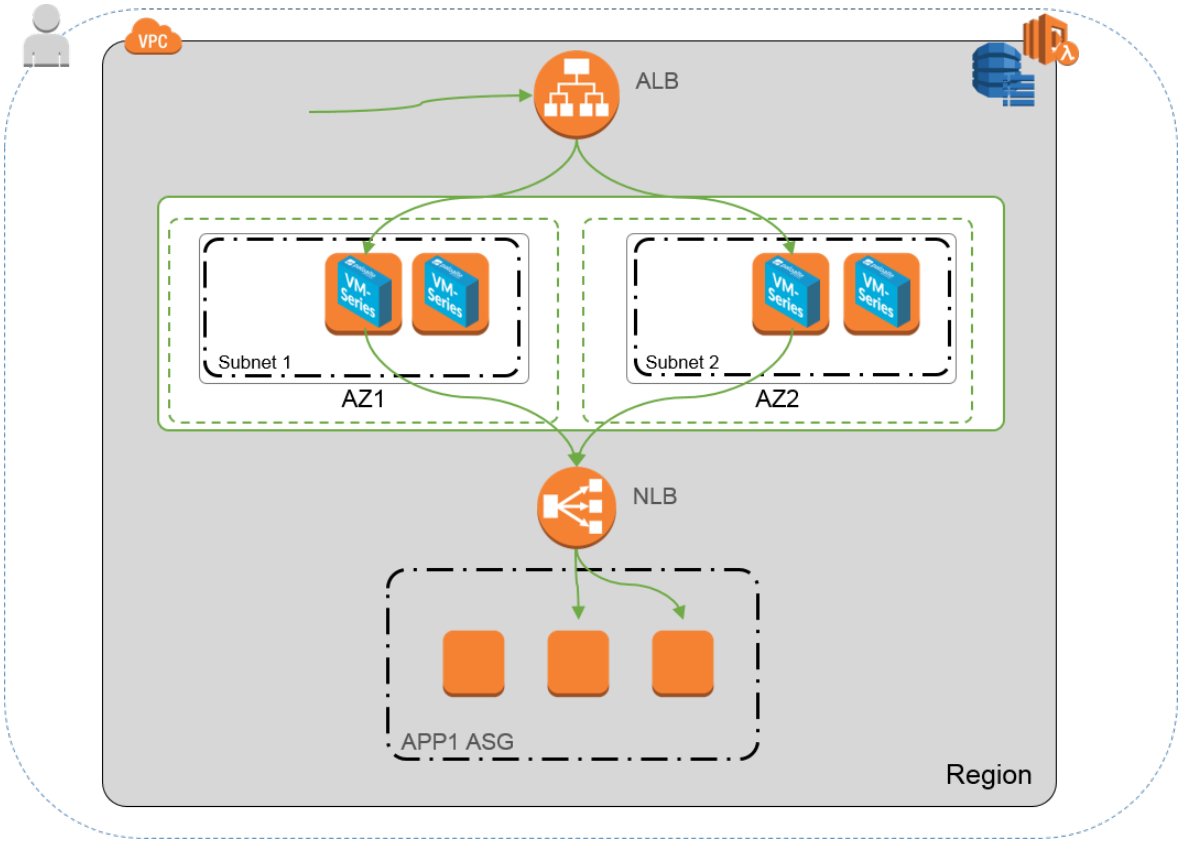
©2023 Palo Alto Networks, Inc.

AWS 專用 VM-Series 自動調整規模範本 2.0 版

為了協助您管理變大的應用程式規模，自動調整規模 VM-Series 防火牆範本 2.0 版提供中樞與輻軸架構來簡化部署。這一版的解決方案提供兩個範本，在單一 AWS 帳戶和多個 AWS 帳戶內，都支援單一和多重 VPC 部署。

- 防火牆範本—防火牆範本會部署一個應用程式負載平衡器 (ALB)，並將 VM-Series 防火牆部署在跨兩個 Availability Zone（可用性區域 - AZ）的自動調整規模群組內。此網際網路型應用程式 ALB 會將進入 VPC 的流量分散至 VM-Series 防火牆的集區。VM-Series 防火牆會自動發佈自訂 PAN-OS 度量，以允許自動調整規模。

  Palo Alto Networks 正式支援防火牆模板，並且具有有效的支援權利，您可以向 Palo Alto Networks 技術支援請求協助。



以下應用程式範本部署了上圖中描述的網路負載平衡器。

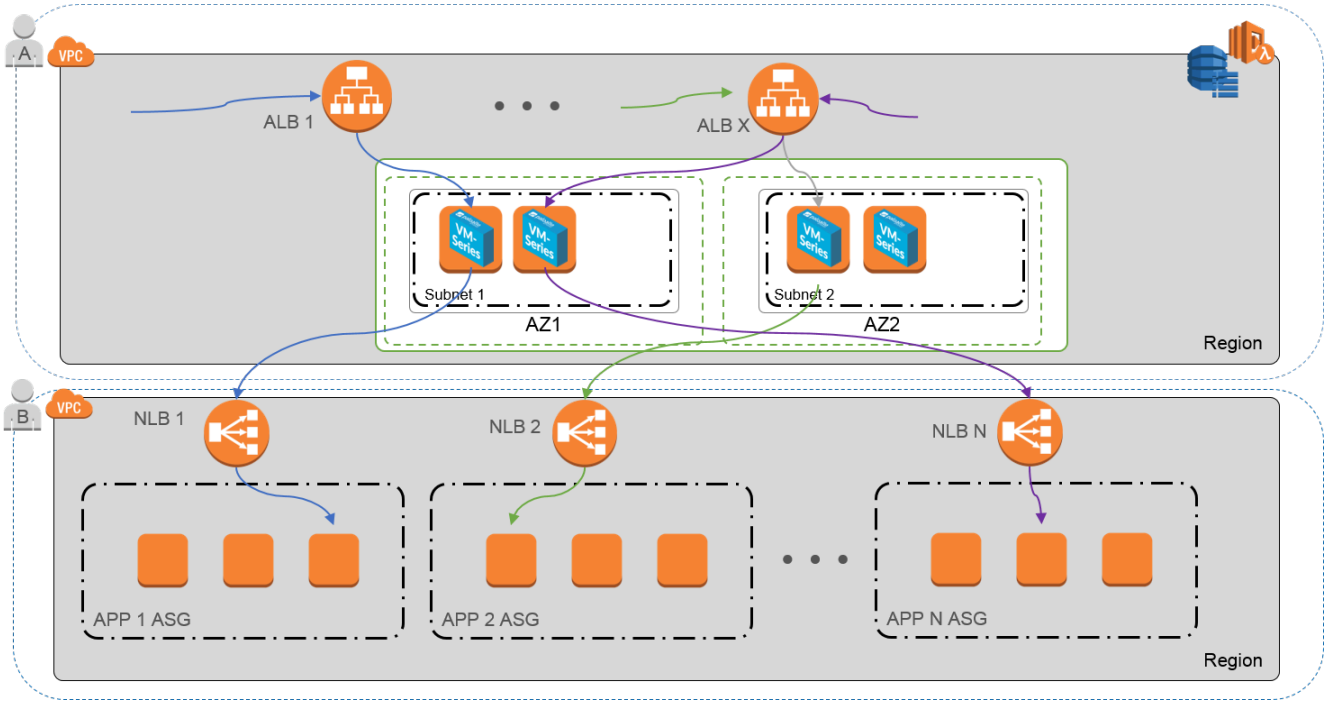
- 應用程式範本—應用程式範本會在每個 AZ 中，部署一個網路負載平衡器 (NLB) 和一個含有 Web 伺服器的自動調整規模群組 (ASG)。

  應用程式範本具備社群支援性質。此範本只是範例，可協助您開始使用基本 Web 應用程式。在生產環境中，您使用您自己的應用程式範本，或自訂此範本來符合您的需求。

這些範本可讓您部署具有網際網路型 ALB 和內部 NLB 的負載平衡器分層式拓撲。從網際網路可存取 ALB，它會將進入 VPC 的流量分散至一群 VM-Series 防火牆。接著，防火牆會利用 NAT 原則，將流量路由至 NLB，而這些平衡器再將流量分散至自動調整規模層的 Web 伺服器或應用程式伺服

©2023 Palo Alto Networks, Inc.

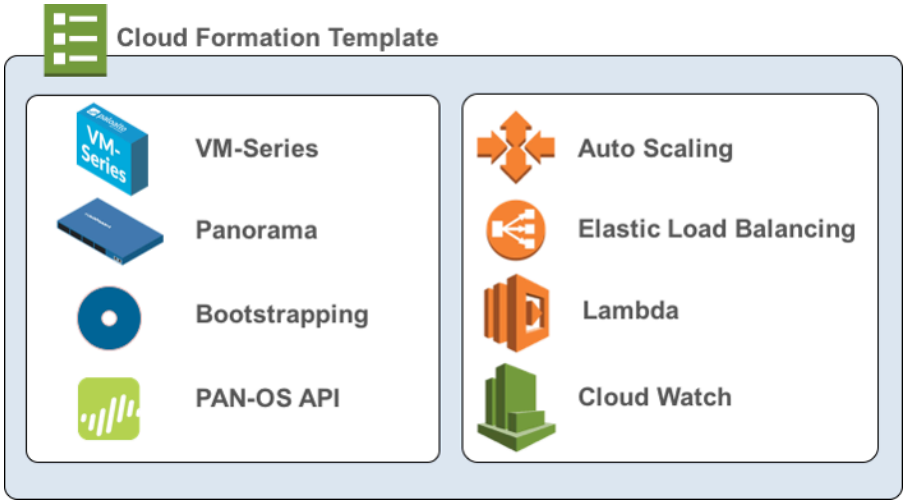
器。VM-Series 防火牆能夠將自訂 PAN-OS 度量發佈至 AWS CloudWatch，讓您監控 VM-Series 防火牆的健康情況和資源負載，然後會利用此資訊，在防火牆上的適當 ASG 中觸發調整規模事件。



- AWS 專用 VM-Series 自動調整規模範本（2.0 版）使用什麼元件？
- AWS 專用 VM-Series 自動調整規模範本（2.0 版）如何啟用動態自動調整規模？
- 規劃 AWS 專用 VM-Series 自動調整規模範本（2.0 版）
- 啟動之前自訂防火牆範本（2.0 版）
- 啟動 AWS 專用 VM-Series 自動調整規模範本（2.0 版）
- 自訂 Bootstrap.xml 檔案（2.0 版）
- 堆疊更新搭配 AWS 專用 VM-Series 自動調整規模範本（2.0 版）
- 修改管理員帳戶和更新堆疊

©2023 Palo Alto Networks, Inc.

AWS 專用 VM-Series 自動調整規模範本（2.0 版）使用什麼元件？



AWS 專用 VM-Series 自動調整規模範本包含下列建置區塊：

建置區塊	說明
防火牆範本 （Palo Alto Networks 正式支援的範本）	`firewall-v2.0.template` 會部署新的 VPC，此 VPC 具有子網路、路由表、AWS NAT 閘道、兩個可用性區域 (AZ)，以及在這些 AZ 之間路由流量所需的安全性群組。這個 2.0 版範本也會部署一個外部 ALB，以及一個 ASG，而每個 AZ 中都有一個 VM-Series 防火牆。 由於生產環境中的諸多變化，包括（但不限於）子網路、可用性區域、路由表、安全性群組等若干元件。您必須在新的 VPC 中部署 `firewall-v2.0.template`。 *AWS 專用 VM-Series 自動調整規模範本不會部署 Panorama，Panorama 是選用的。Panorama 支援輕鬆管理原則和集中的可視性。如果要使用 Panorama 來管理解決方案所部署的 VM-Series 防火牆，您可以使用公司網路內的 M-Series 設備或 Panorama 虛擬設備，或使用 AWS 上的 Panorama 虛擬設備。* 此解決方案包含 AWS NAT 閘道，供防火牆用來發出輸出要求，以擷取更新、連線至 Panorama，以及將度量發佈至 AWS CloudWatch。
應用程式範本 （社群支援的範本）	應用程式範本會部署一個 NLB 和一個 ASG，而每個 AZ 中都有一個 Web 伺服器。因為 NLB 的每個 AZ 都有唯一 IP 位址，且防火牆上的 NAT 原則規則必須參照單一 IP 位址，所以兩個 AZ 各有一個 ASG。ASG 中的所有防火牆都使用相同設定。 2.0 版的自動調整規模解決方案包含兩個應用程式範本： · `panw_aws_nlb-v2.0.template` 可讓您將應用程式範本資源部署在您已部署防火牆範本的同一個 VPC 內（相同的 AWS 帳戶）。

©2023 Palo Alto Networks, Inc.

建置區塊	說明
	· `panw_aws_nlb_vpcv-2.0.template` 可讓您使用相同的 AWS 帳戶或多個 AWS 帳戶，將應用程式範本資源部署在不同的 VPC 中。
Lambda 功能	AWS Lambda 提供穩健的事件驅動自動化，不需要複雜的協調運作軟體。在 `firewall-v2.0.template` 中，AWS Lambda 可監控 Simple Queue Service（簡易佇列服務 - SQS）來得知有發佈至佇列的 NLB。Lambda 功能偵測到新的 NLB 時，會建立新的 NAT 原則規則，並將其套用至 ASG 內的 VM-Series 防火牆。防火牆具有每個應用程式的 NAT 原則規則，而且防火牆會使用 NAT 原則規則（將連接埠對應至 NLB IP 位址），將流量轉送至應用程式 Web 伺服器前面的 NLB。 您需要建立安全性原則規則，以針對您的部署來允許或拒絕應用程式流量。範例 *`bootstrap.xml`* 檔案不包含任何安全性原則規則。您應使用 *Panorama* 集中管理防火牆，並且讓安全性原則規則更容易建立。 有一些額外的功能： · 在防火牆啟動或終止時新增或移除介面 (ENI)。 · 在您刪除堆疊或終止實例時刪除所有相關聯的資源。 · 在發生相應縮小事件時，將作為 Panorama 管理裝置的防火牆移除。 · 在相應縮小事件導致防火牆終止時停用 BYOL 授權。 若要深入瞭解 Lambda 功能，請參閱 **http://paloaltonetworks-aws-autoscale-2-0.readthedocs.io/en/latest/**
啟動程序檔案 GitHub 儲存庫中提供的 bootstrap.xml 檔案僅供測試和評估。在生產部署中，您必須在啟動之前修改 bootstrap.xml 中的範例認證。	此解決方案需要 init-cfg.txt 檔案和 bootstrap.xml 檔案，才能讓 VM-Series 防火牆有基本組態來處理流量。 · `init-cfg.txt` 檔案包含 mgmt-interface-swap 操作命令，可讓防火牆在其主要介面 (eth0) 上接收資料平面流量。此自動調整規模解決方案需要交換資料平面介面和管理介面，才能讓應用程式 ALB 將 Web 流量轉送至自動調整規模層的 VM-Series 防火牆。如需詳細資訊，請參閱搭配 Amazon ELB 使用的管理介面對應。 · `bootstrap.xml` 檔案可啟用防火牆網路介面的基本連線，還可讓防火牆連接至 AWS CloudWatch 命名空間，而此命名空間符合您在啟動範本時所輸入的堆疊名稱。

若要部署解決方案，請參閱啟動 AWS 專用 VM-Series 自動調整規模範本（2.0 版）。

AWS 專用 VM-Series 自動調整規模範本（2.0 版和 2.1 版）如何啟用動態調整規模？

VM-Series 防火牆會使用以自動調整規模範本部署的 VM-Series 防火牆，根據自訂 PAN-OS 度量進行相應縮小和相應放大。VM-Series 防火牆原本是將這些度量發佈至 Amazon CloudWatch 主控

©2023 Palo Alto Networks, Inc.

台，但您可以根據您為調整規模參數選取的度量，定義 CloudWatch 警報和原則來動態部署或終止實例，用以管理 AWS 部署中的應用程式流量。

防火牆會以每五分鐘一次的頻率（預設值）將度量發佈至 AWS CloudWatch。當受監控的度量在已定義的時間間隔內達到已設定的閾值時，CloudWatch 會觸發警報並發出自動調整規模事件。

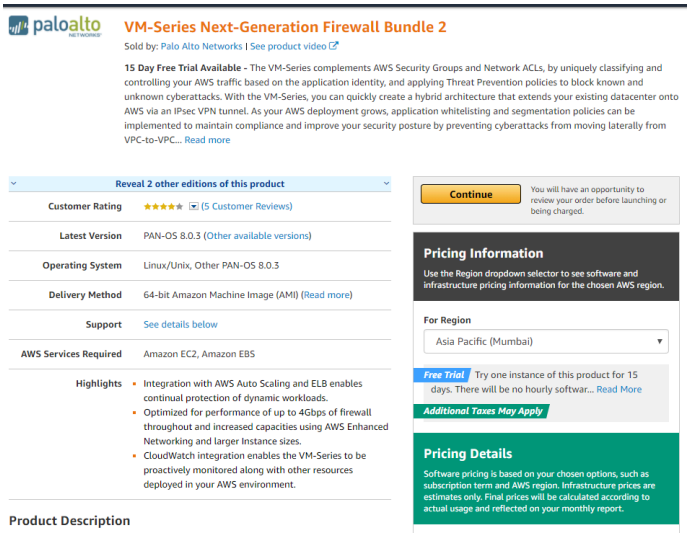
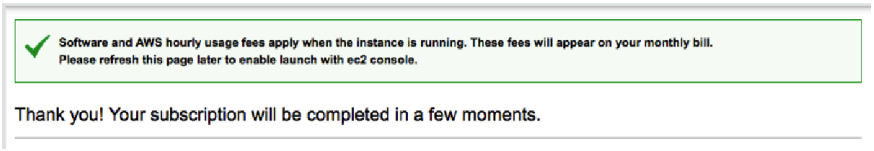
當自動調整模規事件觸發部署新的防火牆時，啟動時會有新的實例啟動載入，而 AWS lambda 功能會以 NAT 原則規則來設定防火牆。每個應用程式都會建立一個 NAT 原則規則，此規則會參照部署中每個網路負載平衡器的 IP 位址。當應用程式負載平衡器收到要求時，就會將此要求轉送至防火牆上指派的 TCP 連接埠。然後，防火牆會檢查流量，再轉送至對應的網路負載平衡器，平衡器再將要求轉送至其目標群組中的 Web 伺服器。

規劃 AWS 專用 VM-Series 自動調整規模範本（2.0 版和 2.1 版）

此檢查清單中的項目是您實作此解決方案時必須執行的動作和選取。

範本 2.0 版和 2.1 版的規劃檢查清單	
❑ 確認部署 VM-Series 自動調整規模範本的需求。	自動調整規模範本需要 AWS Lambda 和 S3 特徵碼第 2 版或第 4 版，且可以部署執行支援 PAN-OS 版本的 VM-Series 防火牆。您需要查詢支援的區域和 AMI ID 清單，以作為在防火牆範本中的輸入。
❑ 指派適當權限給 IAM 使用者角色。	部署 VM-Series 自動調整規模範本的使用者，必須具有管理權限或 iam-policy.json 中列出的權限，才能成功啟動此解決方案。請複製此檔案中的權限，並貼到新的 IAM 原則中，然後將原則附加至新的或現有 IAM 角色。 若為跨帳戶部署，為了存取不同 AWS 帳戶中的資源，部署應用程式範本的使用者的 IAM 角色必須具有完整 SQS 存取權限，也必須有信任關係，以授權她寫入屬於防火牆範本的 SQS 佇列。
❑ 收集跨帳戶部署所需的詳細資訊。	如果部署中的防火牆範本和應用程式範本分別在不同帳戶中，則託管防火牆範本資源的帳戶是信任帳戶，而託管應用程式範本資源的其他 AWS 帳戶是受信任帳戶。若要在跨帳戶部署中啟動應用程式範本，您需要下列資訊: · 您要在其中部署應用程式範本之帳戶的跨帳戶 Amazon Resource Name（Amazon 資源名稱 - ARN）。 · 外部 ID，這是您在建立 IAM 角色以授予完整 SQS 存取權給信任帳戶時所定義的 ID。 · 您打算在其中啟動應用程式範本的每個 AWS 帳戶的 10 位數帳戶號碼。因為託管防火牆範本資源的帳戶充當信任帳戶，且擁有應用程式範本的使用者需要的資源，您需要列出每個可存取防火牆資源的受信任帳戶的帳戶號碼。
❑ 建立支援帳戶在 Palo Alto Networks 支援入口網站上	您可以選擇 BYOL 或 PAYG 授權。 · 若為 BYOL，在啟動 VM-Series 自動調整規模範本之前，您必須將驗證碼註冊到 Palo Alto Networks 支援帳戶，並且在啟動程序套件中，

©2023 Palo Alto Networks, Inc.

範本 2.0 版和 2.1 版的規劃檢查清單	
（如果您尚無此帳戶）。	以 authcodes 為檔案名稱，將驗證碼新增至 `/license` 資料夾。如需詳細資料，請參閱啟動 AWS 專用 VM-Series 自動調整規模範本（2.0 版）或啟動防火牆範本（2.1 版）。 · 若為 PAYG，您必須註冊 VM-Series 防火牆，才能啟用支援權利。
❑ （僅適用於PAYG）檢閱並接受使用者授權合約 (EULA)。 首次在 AWS 帳戶中啟動 VM-Series 防火牆時為必要。	在 AWS Marketplace 中，搜尋 Palo Alto Networks，然後選取您打算使用的搭售包。對於您打算使用的搭售包，如果您未接受 EULA，VM-Series 防火牆無法部署。 · 如需範例，請搜尋 **VM-Series** 防火牆搭售包 **2**。  · 按一下 **Continue**（繼續），選取 **Manual Launch**（手動啟動）。檢閱合約，按一下 **Accept Software Terms**（接受軟體條款）以接受 EULA。  您現在可以關閉瀏覽器。
❑ 對於 AWS Lambda、Python 指令碼和範本，決定您打算使用公共 S3 貯體還是私人 S3 貯體。	在支援的區域清單包含的所有 AWS 區域中，Palo Alto Networks 提供公共 S3 貯體。這些 S3 貯體包含您需要的所有範本、AWS Lambda 指令碼和啟動程序檔案。 *Palo Alto Networks* 建議只將公共 *S3* 貯體中的啟動程序檔案用於評估此解決方案。在生產環境中，您必須為啟動程序套件建立私人 *S3* 貯體。

©2023 Palo Alto Networks, Inc.

範本 2.0 版和 2.1 版的規劃檢查清單	
	S3 貯體的命名慣例是 **panw-aws-autoscale-v20-*<region_name>***。例如，AWS 奧勒崗區域中的貯體是 panw-aws-autoscale-v20-us-west-2。 若要使用您的私人 S3 貯體，您必須下載範本、AWS Lambda 指令碼和啟動程序檔案，並複製到私人 S3 貯體。您可以將防火牆範本和應用程式範本的所有必要檔案放在一個 S3 貯體中，或放在分開的 S3 貯體中。
❑ 下載範本、AWS Lambda 指令碼和啟動程序檔案。	• 從 GitHub 儲存庫取得用於部署防火牆範本（應用程式負載平衡器和 VM-Series 防火牆）的檔案。 請勿跨越 *VM-Series* 自動調整規模範本版本來混合和搭配檔案。 • 範本和 Lambda 指令碼： • panw-aws.zip • firewall-v2.X.template • 啟動程序檔案： • init-cfg.txt • bootstrap.xml 此解決方案隨附的 bootstrap.xml 檔案是為了協助您開始使用，僅供測試和評估。在生產部署中，您必須在啟動之前修改 bootstrap.xml 檔案。 • iam-policy:部署 VM-Series 自動調整規模範本的使用者，必須具有管理權限或此檔案中列出的權限，才能成功啟動此解決方案。 此防火牆範本由 *Palo Alto Networks Techincal Supoort* 支援。 • 從 GitHub 儲存庫 2.0 或 2.1 版取得用於部署 NLB 和 Web 伺服器的檔案。 • 範本： • pan_aws_nlb-2.X.template — 使用此範本，將應用程式範本資源部署在您已部署防火牆範本的同一個 VPC 內（相同的 AWS 帳戶）。 • pan_aws_nlb_vpc-2.X.template — 使用此範本，將應用程式範本資源部署在不同的 VPC 中。此範本可讓您將資源部署在相

©2023 Palo Alto Networks, Inc.

範本 2.0 版和 2.1 版的規劃檢查清單	
	同 AWS 帳戶內或不同 AWS 帳戶中（只要您有適當權限可支援跨帳戶部署）。 · pan_nlb_lambda.template — 建立 AWS 網路負載平衡器，以分散流量，進而註冊相應放大的後端 Web 伺服器。 · Lambda 指令碼和 Python 指令碼。
❑ 針對您的生產環境自訂 bootstrap.xml 檔案。	為了確保生產環境的安全性，您必須在生產部署中以唯一的管理使用者名稱和密碼自訂 bootstrap.xml 檔案。預設的使用者名稱和密碼是 pandemo/demopassword。您也可以利用此機會，使用符合您的應用程式安全性需求的介面、區域和安全性原則規則，建立最佳防火牆組態。
❑ 決定是否要使用 Panorama 來集中進行記錄、報告和防火牆管理。	Panorama 是為了輕鬆管理而提供的選項，也是管理防火牆的最佳作法。不需要管理此解決方案中部署的自動調整規模層 VM-Series 防火牆。 如果要使用 Panorama，您可以使用 AWS 上的 Panorama 虛擬設備，或使用您公司網路內部的 M-Series 設備或 Panorama 虛擬設備。 ***Panorama*** 必須設定為 ***Panorama*** 模式，而非 ***Managment Only***（僅限管理）模式。 為了成功向 Panorama 註冊防火牆，您必須收集下列詳細資訊： · Panorama 的 API 金鑰 # 為了讓 AWS Lambda 向 Panorama 提出 API 要求，您必須在啟動 VM-Series 自動調整規模範本時提供 API 金鑰。就最佳作法而言，在生產環境中，請針對 API 呼叫建立個別的管理帳戶，並產生相關聯的 API 金鑰。 · Panorama IP 位址 # 您必須在組態 (init-cfg.txt) 檔案中必須包含此 IP 位址。防火牆必須能夠從 VPC 存取此 IP 位址；為了確保連線安全，請使用 direct connect 連結或 IPSec 通道。 · VM 驗證金鑰 # 可讓 Panorama 驗證防火牆，以便將每個防火牆新增為受管理的裝置。您必須在組態 (init-cfg.txt) 檔案中必須包含此金鑰。 整個部署留存期都需要 vm 驗證金鑰。如果連線要求中缺少有效金鑰，VM-Series 防火牆將無法向 Panorama 註冊。如需金鑰的詳細資訊，請參閱在 Panorama 上產生 VM 驗證金鑰。 · 指派給防火牆的範本堆疊名稱和裝置群組名稱 # 您必須先新增範本並指派給範本堆疊、在 Panorama 上建立裝置群組，然後在組態 (init-cfg.txt) 檔案中包含範本堆疊名稱和裝置群組名稱。

©2023 Palo Alto Networks, Inc.

範本 2.0 版和 2.1 版的規劃檢查清單	
	為了降低使用彈性 *IP* 位址時的成本和規模限制，防火牆沒有公共 *IP*。如果您不使用 *Panorama* 來管理防火牆，則必須部署跳躍伺服器（具有 *EIP* 位址的堡壘主機）來連接至 *VPC* 內的不受信任子網路，才能透過 *SSH* 和/或 *HTTPS* 存取 *VM-Series* 防火牆。依預設，此解決方案包含 *AWS NAT* 閘道，供防火牆用來發出輸出要求，以擷取更新、連線至 *Panorama*，以及將度量發佈至 *AWS CloudWatch*。
開始使用	啟動 AWS 專用 VM-Series 自動調整規模範本（2.0 版）。

啟動之前自訂防火牆範本（2.0 版和 2.1 版）

為了簡化部署工作流程，防火牆只會顯示一組有限的參數，您在啟動範本之前必須為這些參數提供輸入。如果您想要檢視和自訂範本所包含的其他選項，則在啟動 AWS 專用 VM-Series 自動調整規模範本 2.0 版或 2.1 之前，可以使用文字編輯工具（例如記事本或 Visual Studio Code）來指定您偏好的值。

請使用下表來檢視您在部署 AWS 的自動調整規模防火牆範本時，可自訂的參數清單。透過您已購買的支援選項，Palo Alto Networks 的官方支援原則允許您修改此清單中的參數。

參數	說明	預設值
VPC 的 CIDR 區塊	您想要用於 VPC 的 IP 位址空間。 您在下方修改的子網路必須屬於此 *VPC CIDR* 區域，而且唯一的。	192.168.0.0/16
管理子網路 CIDR 區塊	防火牆的管理子網路的 CIDR 區塊（逗號分隔清單）。	192.168.0.0/24, 192.168.10.0/24
不信任子網路 CIDR 區塊	不信任子網路的 CIDR 區塊（逗號分隔清單）。	192.168.1.0/24, 192.168.11.0/24
信任子網路 CIDR 區塊	信任子網路的 CIDR 區塊（逗號分隔清單）。	192.168.2.0/24, 192.168.12.0/24
NAT 閘道子網路 CIDR 區塊	AWS NAT 閘道的 CIDR 區塊（逗號分隔清單）。	192.168.100.0/24, 192.168.101.0/24
Lambda 子網路 CIDR 區塊	Lambda 功能的 CIDR 區塊（逗號分隔清單）。	192.168.200.0/24, 192.168.201.0/24

©2023 Palo Alto Networks, Inc.

參數	說明	預設值
防火牆實例大小	AWS 實例類型和您在部署中想要的 VM-Series 防火牆大小。	M4.xlarge
選取調整規模參數 您不需要針對調整規模參數而修改範本。對於您要觸發自訂調整規模的一或多個自訂 *PAN-OS* 度量，您可以在 *AWS* 主控台設定 AWS CloudWatch 警報。	該範本會將下列所有度量發佈到 AWS CloudWatch： · CPU—資料平面 CPU 使用率 · AS—作用中工作階段 · SU—工作階段使用率 · SSPU—SSL 代理使用率 · GPU—GlobalProtect 閘道使用率 · GPAT—GlobalProtect 閘道使用率 ActiveTunnels · DPB—資料平面封包緩衝區使用率	資料平面 CPU 使用率
選取 Scaling Period（調整規模期間）的時間（秒）	套用平均值統計資料的期間（秒）。必須是 60 的倍數。	900
VM-Series 實例數目上限	自動調整規模群組中的 VM-Series 防火牆數目上限。	3
VM-Series 實例數目下限	自動調整規模群組中的 VM-Series 防火牆數目下限。	1
ScaleDown 閾值（百分比/值）	觸發相應縮小的條件值。	20
ScaleUp 閾值（百分比/值）	觸發相應放大的條件值。	80

啟動 AWS 專用 VM-Series 自動調整規模範本（2.0 版）

您可以選取將防火牆範本部署於一個 VPC 中，以及在您部署防火牆的同一個 VPC 或不同 VPC 中，部署範例應用程式範本。

如果您要保護的應用程式屬於另一個 AWS 帳戶，範例應用程式範本包含跨帳戶部署的支援。解決方案支援中樞與輻軸架構，可讓您將防火牆範本部署於一個 AWS 帳戶，然後作為中樞來保護屬於相同或不同 AWS 帳戶的應用程式（輻軸）。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

· 啟動 VM-Series 防火牆範本

©2023 Palo Alto Networks, Inc.

- 啟動應用程式範本
- （只有在部署多個內部負載平衡器時才需要）啟用流向 ELB 服務的流量（2.0 版和 2.1 版）

啟動 **VM-Series** 防火牆範本

此工作流程說明如何使用防火牆範本來部署應用程式負載平衡器和 VM-Series 防火牆。

此防火牆範本包含 *AWS NAT* 閘道，供防火牆用來發出輸出要求，以擷取更新、連線至 *Panorama*，以及將度量發佈至 *AWS CloudWatch*。如果您不使用 *Panorama* 來管理防火牆，則必須部署跳躍伺服器（具有 *EIP* 位址的堡壘主機）來連接至 *VPC* 內的不受信任子網路，才能透過 *SSH* 和/或 *HTTPS* 存取 *VM-Series* 防火牆。因為 *VM-Series* 防火牆上的管理介面只有私人 *IP* 位址，所以需要此跳躍伺服器。

STEP 1 | 檢閱規劃 AWS 專用 VM-Series 自動調整規模範本（2.0 版）的檢查清單。

確定您已完成下列工作：

- （僅適用於 PAYG）檢閱並接受您打算使之 PAYG 搭售包的 EULA。
- （僅適用於 BYOL）取得驗證碼。您需要在啟動程序套件的 /license 資料夾中輸入此驗證碼。
- 從 GitHub 儲存庫下載啟動 VM-Series 自動調整規模範本所需的檔案。

©2023 Palo Alto Networks, Inc.

STEP 2 | 修改 init-cfg.txt 檔案。您必須將裝置憑證自動註冊 PIN 新增至 init-cfg.txt 檔案，才能在部署 VM-Series 防火牆實例時自動安裝裝置憑證。

vm-series-auto-registration-id=

vm-series-auto-registration-pin-value=

如需詳細資訊，請閱讀有關啟動程序和 init-cfg.txt 檔案。

如果您使用 Panorama 管理防火牆，請完成下列工作：

1. 在 Panorama 上產生 VM 驗證金鑰.在對 Panorama 發出的連線要求中，防火牆必須包含有效金鑰。將金鑰的存留期設為 8760 小時（1 年）。
2. 使用文字編輯器開啟 init-cfg.txt 檔案，例如記事本。切勿變更格式，因為這會導致部署 VM-Series 自動調整規模範本失敗。以名稱-值配對新增下列資訊：
   - 主要 Panorama 和（選用）次要 Panorama 的 IP 位址。輸入：

     panorama-server=

     panorama-server-2=
   - 指定您想要指派防火牆的範本堆疊名稱和裝置群組。輸入：

     tplname=

     dgname=
   - VM 驗證金鑰。輸入：

     vm-auth-key=
3. 確認您未刪除用於 AWS 的 VM-Series 防火牆上交換管理介面 (mgmt) 和資料平面介面 (ethernet 1/1) 的命令。例如，檔案必須包含名稱-值配對，如下所示：

   op-command-modes=mgmt-interface-swap

   vm-auth-key=755036225328715

   panorama-server=10.5.107.20

   panorama-server-2=10.5.107.21

   tplname=FINANCE_TG4

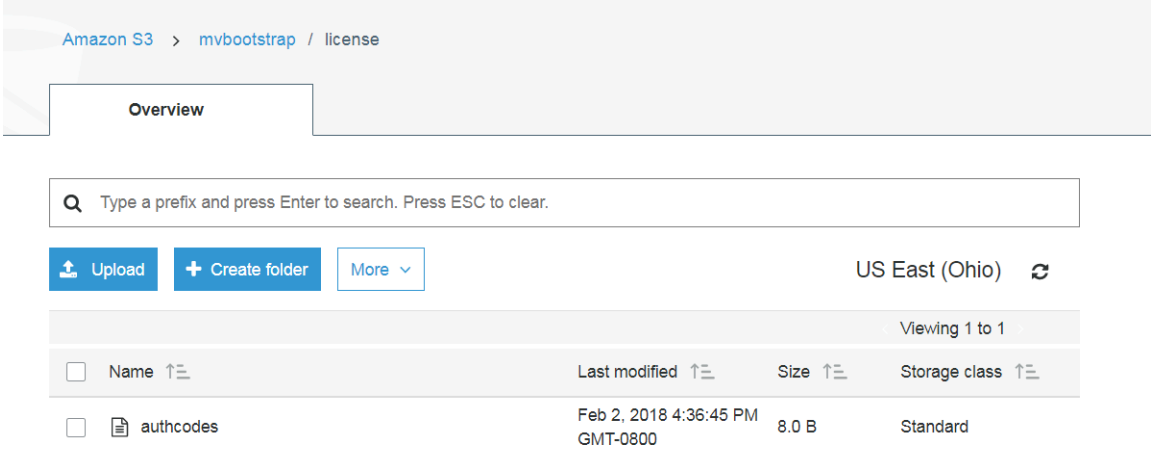
   dgname=finance_dg
4. 儲存並關閉檔案。

STEP 3 | （僅適用於 BYOL）在啟動程序套件的 /license 資料夾中輸入授權驗證碼。如需詳細資訊，請參閱準備啟動程序套件。

1. 使用文字編輯器建立新的 .txt 檔案，例如記事本。
2. 將 BYOL 授權的驗證碼新增至此檔案，然後使用驗證碼儲存此檔案（無副檔名）並上傳至 /license 資料夾。驗證碼必須支援您的部署可能需要的防火牆數目。您必須使用驗證碼包

©2023 Palo Alto Networks, Inc.

而非個別的驗證碼，以便防火牆可同步擷取與防火牆相關聯的所有授權金鑰。如果您使用個別的驗證碼而非驗證碼包，防火牆只會擷取檔案中包含的首個驗證碼的授權金鑰。



STEP 4 | 針對 bootstrap.xml 檔案中定義的 VM-Series 防火牆管理員帳戶，變更預設認證。

在生產環境中使用 VM-Series 自動調整規模範本需要如此。

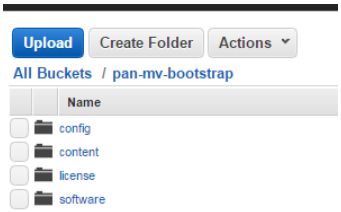
GitHub 儲存庫中的 bootstrap.xml 檔案僅供測試和評估。在生產部署中，您必須在啟動之前自訂 Bootstrap.xml 檔案（2.0 版）。

©2023 Palo Alto Networks, Inc.

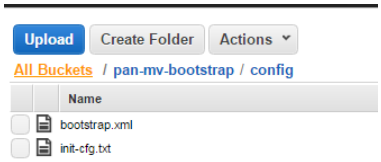
STEP 5 | 準備 Amazon Simple Storage (S3) 貯體，對生產環境啟動 VM-Series 自動調整規模範本。

確保在您打算部署範本的同一個區域中建立 *S3* 貯體；裝載於公共 *S3* 貯體中的啟動程序檔案只是為了讓您更輕鬆評估範本。

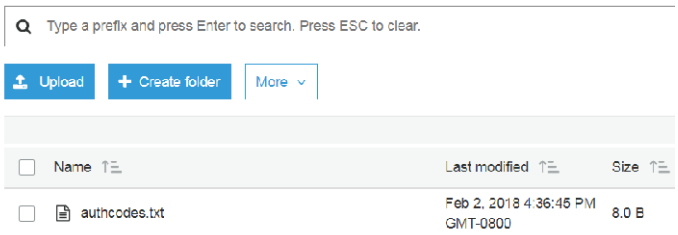
1. 為啟動程序檔案建立新的 S3 貯體。
   1. 登入 AWS 管理主控台並開啟 S3 主控台。
   2. 按一下 **Create Bucket**（建立貯體）。
   3. 輸入 **Bucket Name**（貯體名稱）和 **Region**（區域），然後按一下 **Create**（建立）。貯體必須在 S3 根層次。如果貯體深入巢狀，啟動會失敗，因為您無法指定啟動程序檔案位置的路徑。
2. 將啟動程序檔案上傳至 S3 貯體。啟動程序資料夾必須在 S3 貯體的根資料夾中。
   1. 按一下貯體名稱，然後按一下 **Create folder**（建立資料夾）。
   2. 為啟動程序建立下列資料夾結構：



   3. 按一下連結以開啟 **config** 資料夾。
   4. 選取 **Actions**（動作） > **Upload**（上傳）和 **Add Files**（新增檔案），瀏覽以選取 init-cfg.txt 檔案和 bootstrap.xml 檔案，然後按一下 **Open**（開啟）。
   5. 按一下 **Start Upload**（開始上傳），將檔案新增至 config 資料夾。此資料夾只能包含兩個檔案：init-cfg.txt 和 bootstrap.xml。



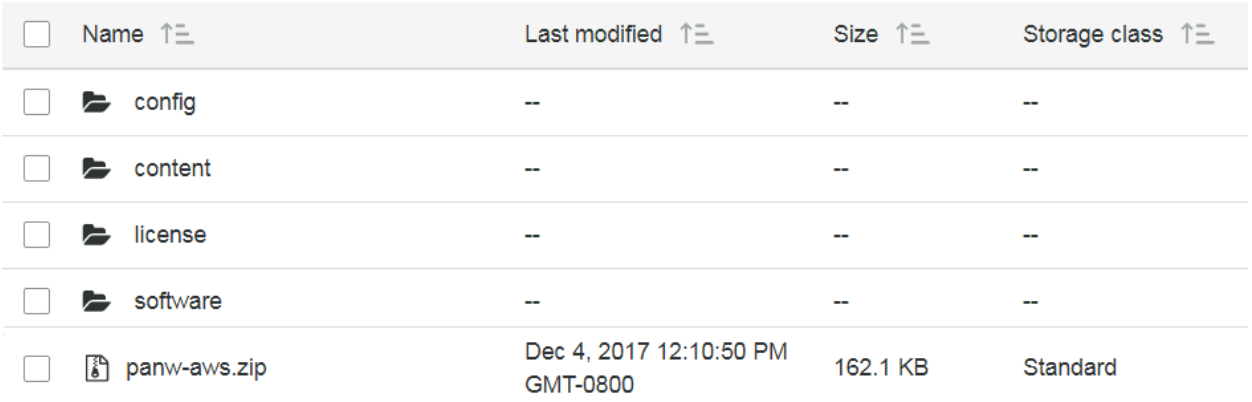
   6. （僅適用於 BYOL）按一下連結以開啟 **license** 資料夾並上傳 txt 檔案，其中含有授權 VM-Series 防火牆所需的驗證碼。



3. 將 AWS Lambda 指令碼（panw-aws.zip 檔案）上傳至 S3 貯體。在此範例中，AWS Lambda 指令碼位於啟動程序套件所在的同一個 S3 貯體中。

 ©2023 Palo Alto Networks, Inc.

1. 按一下貯體名稱。
2. 按一下 **Add Files**（新增檔案）選取 panw-aws.zip 檔案，然後按一下 **Open**（開啟）。
3. 按一下 **Start Upload**（開始上傳），將 zip 檔案新增至 S3 貯體。



Name	Last modified	Size	Storage class
config	--	--	--
content	--	--	--
license	--	--	--
software	--	--	--
panw-aws.zip	Dec 4, 2017 12:10:50 PM GMT-0800	162.1 KB	Standard

STEP 6 | 選取防火牆範本。

如果您需要在啟動之前自訂防火牆範本（2.0 版），請現在進行並選取已修改的範本。

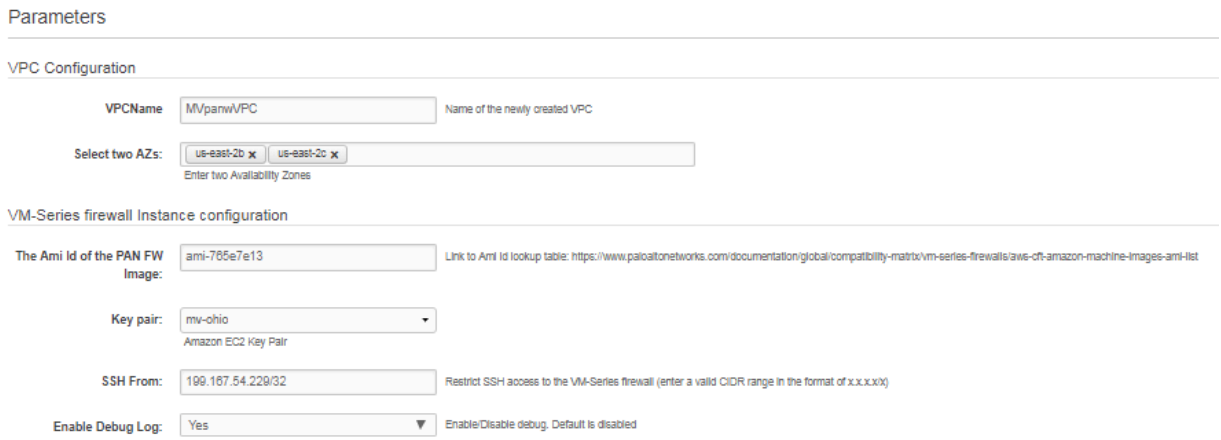
1. 在 AWS 管理主控台，選取 **CloudFormation** > **Create Stack**（建立堆疊）。
2. 選取 **Upload a template to Amazon S3**（將範本上傳至 **Amazon S3**），選取 firewall-v2.0.template，然後按一下 **Open**（開啟）和 **Next**（下一步）。
3. 指定 **Stack name**（堆疊名稱）。堆疊名稱可讓您唯一地識別此範本部署的所有資源。

STEP 7 | 設定 VPC 的參數。

1. 輸入 **VPC Configuration**（**VPC** 組態）的參數，如下所示：
   1. 輸入 **VPCName**。
   2. 在 **Select two AZs**（選取兩個 **AZ**）中，選取您的設定跨越的兩個可用性區域。

©2023 Palo Alto Networks, Inc.

STEP 8 | 選取 VM-Series 防火牆偏好設定。

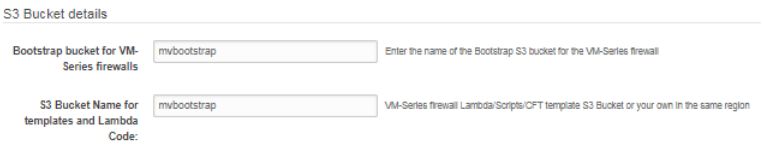


1. 針對 VM-Series 防火牆查詢 AMI ID 並輸入。確保 AMI ID 符合您選取使用的 AWS 區域、PAN-OS 版本和 BYOL 或 PAYG 授權選項。
2. 選取 EC2 **Key pair**（金鑰配對）（從下拉式清單）以啟動防火牆。若要登入防火牆，您必須提供此金鑰配對及其相關聯私密金鑰的名稱。
3. 限制以 SSH 存取防火牆的管理介面。確保您提供的 CIDR 區塊對應於您的專用管理 IP 位址或網路。請勿讓允許的來源網路範圍過大，也決不要將允許的來源設定為 0.0.0.0/0。在模範本上設定 IP 位址之前，請先確認 IP 位址，以確保不會封鎖您自己。
4. 如果您要 **Enable Debug Log**（啟用偵錯日誌），請選取 **Yes**（是）。啟用偵錯日誌會產生更詳細的日誌，這有助於部署問題的疑難排解。這些日誌是以堆疊名稱產生，並儲存在 AWS CloudWatch 中。

依預設，範本使用 CPU 使用率作為 VM-Series 防火牆的調整規模參數。自訂 PAN-OS 度量會自動發佈至與您稍早指定的堆疊名稱相符的 CloudWatch 命名空間。

STEP 9 | 指定 Amazon S3 貯體的名稱。

您可以使用一個 *S3* 貯體來存放啟動程序套件和 *zip* 檔案。

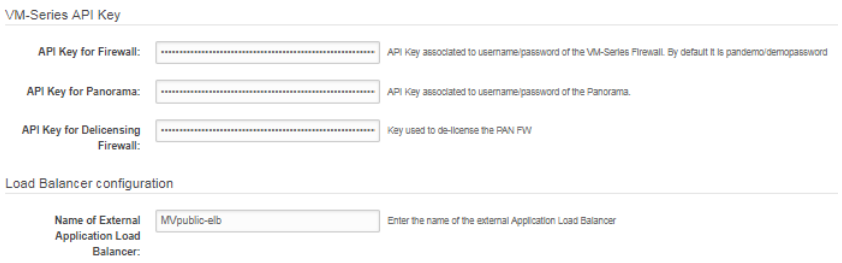


1. 輸入含有啟動程序套件的 S3 貯體的名稱。

   如果啟動程序貯體未適當設定，或貯體名稱輸入不正確，啟動程序會失敗，您也無法登入防火牆。負載平衡器的健康情況檢查也會失敗。
2. 輸入含有 panw-aws.zip 檔案的 S3 貯體的名稱。

©2023 Palo Alto Networks, Inc.

STEP 10 | 指定金鑰以允許 API 存取防火牆和 Panorama。



1. 輸入防火牆驗證 API 呼叫時必須使用的金鑰。預設金鑰是基於範例 bootstrap.xml 檔案，僅適用於測試和評估。在生產環境中，您必須針對 API 呼叫建立個別的 PAN-OS 登入，並產生相關聯的金鑰。
2. 如果您使用 Panorama 來集中管理，請輸入 API 金鑰，以允許 AWS Lambda 對 Panorama 發出 API 呼叫。在生產環境中，您應該針對 API 呼叫建立個別的登入，並產生相關聯的金鑰。
3. 複製並貼上您的帳戶的授權停用 API 金鑰。當相應縮小事件發生時，需要有此金鑰才能在防火牆上成功停用授權。若要取得此金鑰：
   1. 登入客戶支援入口網站。
   2. 選取 **Assets**（資產） > **API Key Management**（**API** 金鑰管理）。
   3. 複製 API 金鑰。

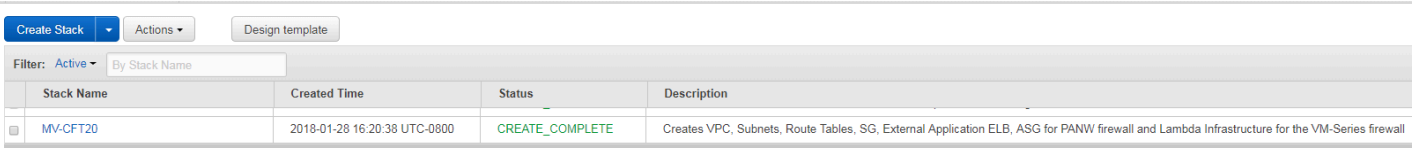
STEP 11 | 輸入應用程式負載平衡器的名稱。

STEP 12 | （選用）套用標籤，以識別與 VM-Series 自動調整規模範本相關聯的資源。

新增名稱-值配對，以識別和分類此堆疊中的資源。

STEP 13 | 檢閱範本設定並啟動範本。

1. 選取 **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**（我瞭解此範本可能導致 **AWS CloudFormation** 建立 **IAM** 資源）。
2. 按一下 **Create**（建立）來啟動範本。將會顯示 CREATE_IN_PROGRESS 事件。
3. 成功部署時，狀態會更新為 CREATE_COMPLETE。

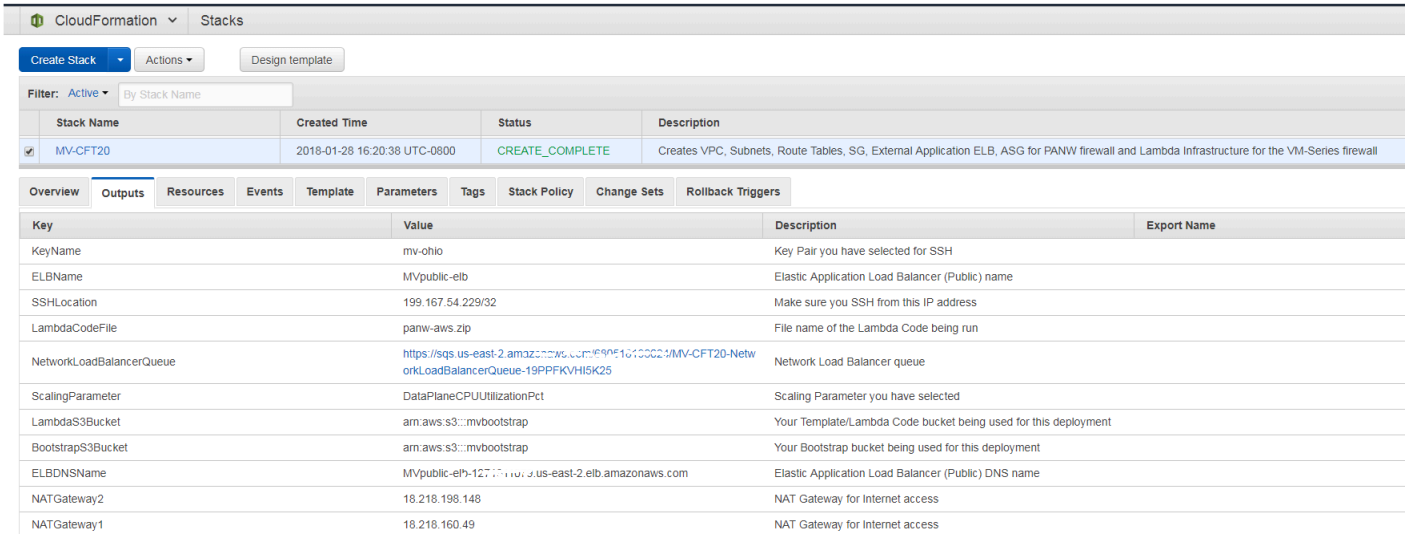


除非您自訂範本，否則 VM-Series 自動調整規模範本會啟動 ASG，其中在每個 AZ 中都包含一個位於應用程式負載平衡器後面的 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

STEP 14 | 確認範本已啟動所有必要資源。

1. 在 AWS 管理主控台上，選取堆疊名稱來檢視 **Output**（輸出）中的資源清單。



2. 在 EC2 儀表板上，選取 **Auto Scaling Groups**（自動調整規模群組）。在每個 AZ 中，確認 VM-Series 防火牆有一個 ASG，而每個 ASG 中各有一個防火牆。ASG 名稱首碼包含堆疊名稱。
3. 登入 VM-Series 防火牆。您必須部署跳躍伺服器或使用 Panorama，才能存取防火牆的 Web 介面。

- 可能需要長達 *20* 分鐘，防火牆才會完成啟動且能夠處理流量。
- 完成測試或生產部署時，完全刪除堆疊是確保停止收費的唯一辦法。關閉實例或將 *ASG* 最大值變更為 *0* 不夠。

STEP 15 | 儲存下列資訊。部署應用程式範本時，您需要提供這些值作為輸入。

- 每個 AZ 中 NAT 閘道的 IP 位址。如果您將應用程式部署在不同 VPC 中，則需要此 IP 位址來限制以 HTTP 存取 Web 伺服器。指定此 IP 位址可確保在不同 VPC 中存取您的應用程式時，防火牆能夠保護應用程式的安全，而且沒有任何人可以避開防火牆而直接存取 Web 伺服器。如果您未輸入 NAT 閘道 IP 位址，範例應用程式範本 (panw_aws_nlb_vpc-2.0.template) 會顯示範本驗證錯誤；您必須以逗號分隔的清單方式來輸入 IP 位址。
- 網路負載平衡器 SQS URL。防火牆堆疊中的一項 AWS Lambda 功能可監控此佇列，以瞭解您部署的任何網路負載平衡器，並在 VM-Series 防火牆上建立 NAT 原則規則（每個應用程式各一個），讓防火牆能夠將流量傳送至網路負載平衡器 IP 位址。

啟動應用程式範本

應用程式範本可讓您完成分層式拓撲，還可讓您評估自動調整規模解決方案。此應用程式範本會在 VM-Series 防火牆（利用防火牆來部署）的自動調整規模群組後面，部署網路負載平衡器和一對 Web 伺服器。此範本中的 Web 伺服器有公共 IP 位址可支援直接輸出存取，以擷取軟體更新。請使用此範本來評估解決方案，但建立您自己的範本來部署到生產環境。對於自訂範本，務必啟用應用程式範本和防火牆範本之間的 SQS 傳訊。

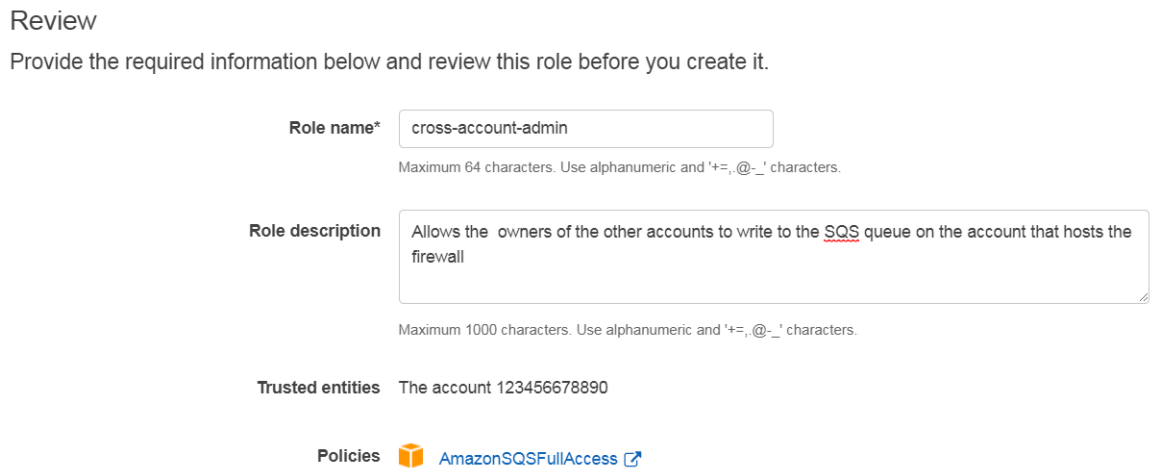
©2023 Palo Alto Networks, Inc.

啟動應用程式範本時，必須根據想要在您部署防火牆範本的同一個 VPC 內 (panw_aws_nlb-2.0.template)，還是在不同 VPC 中 (panw_aws_nlb_vpc-2.0.template) 部署應用程式範本，以選取範本。如果是不同 VPC，範本提供跨帳戶部署的支援。跨帳戶部署需要您建立 IAM 角色，並於信任 AWS 帳戶與受信任 AWS 帳戶之間啟用權限和信任關係，而且啟動範本時需要帳戶資訊作為輸入。

STEP 1 | （僅跨帳戶部署才需要）建立 IAM 角色。請參閱 AWS 文件。

此角色將存取權授予屬於不同 AWS 帳戶的使用者。此使用者需要權限來存取防火牆範本中的 Simple Queue Service（簡易佇列服務 - SQS）資源。防火牆會使用此佇列來瞭解您部署的每個網路負載平衡器，以便建立 NAT 原則將流量傳送至網路負載平衡器後面的 Web 伺服器。

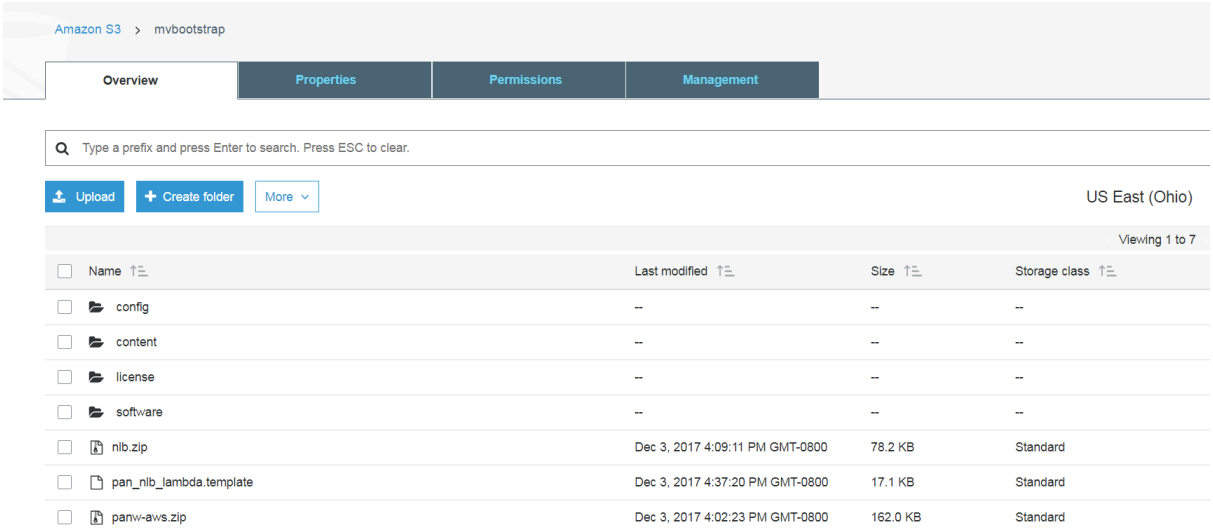
- 在 **Account ID**（帳戶 **ID**）中，輸入帳戶的 AWS 帳戶 ID，以準備將應用程式範本部署於此帳戶中。對於裝載防火牆範本資源的帳戶，指定該帳戶 ID 可讓您授權存取此帳戶中的資源。
- 選取 **Require external ID**（需要外部 **ID**），輸入共用密碼的值。指定外部 ID 可讓使用者只在要求包含正確時才擔任角色。
- 選取 **Permissons**（權限）以允許 **Amazon SQS Full Access**（**Amazon SQS** 完整存取）。



 ©2023 Palo Alto Networks, Inc.

STEP 2 | 使用 Palo Alto Networks 公共 S3 貯體或準備私人 (S3) 貯體，以啟動應用程式範本。

1. 使用 GitHub 儲存庫中的所有檔案建立 zip 檔案（不包括三個 .template 檔案），在下列螢幕擷取畫面中，名稱是 nlb.zip。
2. 將 zip 檔案上傳至您稍早建立的 S3 貯體或新貯體。



3. 將 pan_nlb_lambda 範本複製到您將 nlb.zip 檔案複製到的同一個貯體。

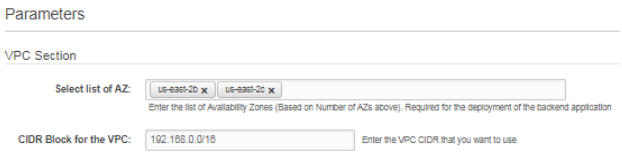
STEP 3 | 選取要啟動的應用程式範本。

1. 在 AWS 管理主控台，選取 **CloudFormation** > **Create Stack**（建立堆疊）。
2. 選取 **Upload a template to Amazon S3**（將範本上傳至 **Amazon S3**），然後選取 panw_aws_nlb-2.0.template，將範本啟動的資源部署於防火牆所在的相同 VPC 內，或選取 panw_aws_nlb_vpc-2.0.template，將資源部署到不同的 VPC。按一下 **Open**（開啟）和 **Next**（下一步）。
3. 指定 **Stack name**（堆疊名稱）。堆疊名稱可讓您唯一地識別所有使用此範本所部署的資源。

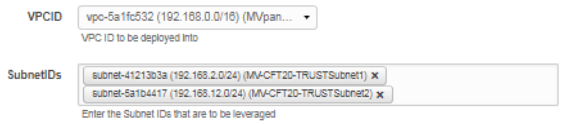
©2023 Palo Alto Networks, Inc.

STEP 4 | 設定 VPC 和網路負載平衡器的參數。

1. 在 **Select list of AZ**（選取 **AZ** 清單）中，選取您的設定將跨越的兩個可用性區域。如果部署在相同的 VPC 內，請確保您選取的可用性區域，與您為防火牆範本選取的可用性區域相同。
2. 輸入 **CIDR Block for the VPC**（**VPC** 的 **CIDR** 區塊）。預設 CIDR 為 192.168.0.0/16。



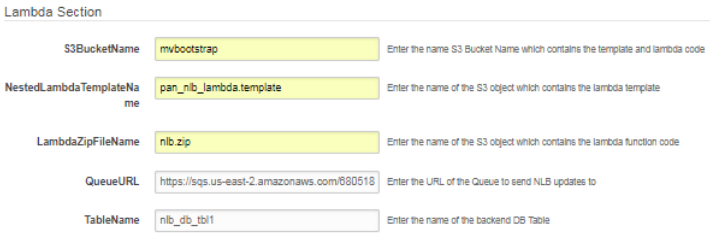
3. （僅當您使用 panw_aws_nlb-2.0.template 將應用程式部署在相同 VPC 內時）



選取與每個 AZ 中防火牆上的信任子網路相關聯的 **VPC ID** 和 **Subnet IDs**（子網路 **ID**）。網路負載平衡器會附加至防火牆上的信任子網路，以完成負載平衡器分層式拓撲。

4. 輸入網路負載平衡器的名稱。

STEP 5 | 設定 AWS Lambda 的參數。



1. 輸入 S3 貯體名稱，其中儲存 nlb.zip 和 pan_nlb_lambda.template。
2. 輸入 pan_nlb_lambda.template 的名稱和 zip 檔案名稱。
3. 貼上您稍早複製的 SQS URL。
4. 輸入唯一的 **TableName**。此表格儲存應用程式的連接埠和 IP 位址的對應，而這些應用程式與您的部署中的網路負載平衡器相關聯。

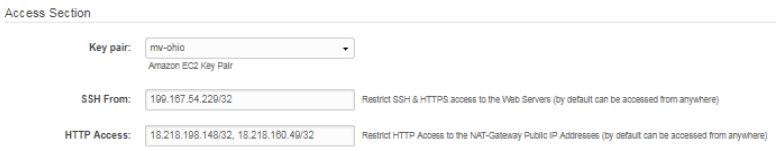
   刪除應用程式堆疊時也會刪除此表格。因此，如果網路負載平衡器的多個實例寫入相同表格，但此表格已刪除，則防火牆上的 NAT 規則就無法正常運作，應用程式流量可能會錯誤地轉送至錯誤的連接埠/網路負載平衡器。

STEP 6 | 請修改 Web 伺服器 EC2 實例類型，以符合您的部署需求。

STEP 7 | 選取 EC2 **Key pair**（金鑰配對）（從下拉式清單）以啟動 Web 伺服器。若要登入 Web 伺服器，您必須提供金鑰配對名稱及其相關聯的私密金鑰。

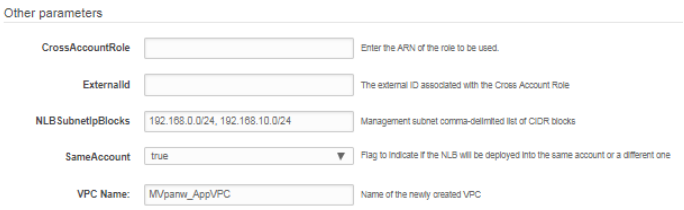
©2023 Palo Alto Networks, Inc.

STEP 8 | （僅當您使用 panw_aws_nlb_vpc-2.0.template 時）封鎖對 Web 伺服器的存取。



1. 限制以 **SSH From**（**SSH** 來源）存取 Web 伺服器。只您有列在這裡的 IP 位址才能登入 Web 伺服器。
2. 限制以 HTTP 存取 Web 伺服器。輸入來自防火牆範本輸出的 NAT 閘道的公共 IP 位址，並確定使用逗點分隔 IP 位址。輸入 NAT 閘道 IP 位址可讓您確保流向應用程式伺服器的所有 web 流量，都受到 VM-Series 防火牆保護。

STEP 9 | （僅當您使用 panw_aws_nlb_vpc-2.0.template 時）設定其他參數時，需要在不同 VPC 中啟動應用程式範本堆疊。

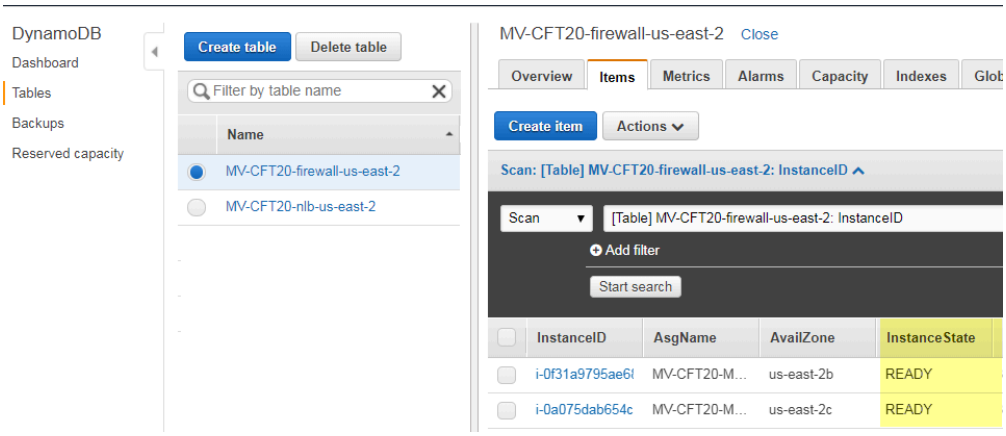


1. 如果您將此應用程式範本部署於防火牆範本所在的相同 AWS 帳戶內，請選取 SameAccount **true**，並將跨帳戶角色和外部 ID 留白；若為跨帳戶部署，請選取 **false**。

   若為跨帳戶部署，請在 **CrossAccountRole** 和 **ExternalId** 中，輸入您在（僅跨帳戶部署才需要）建立 IAM 角色中定義的 Amazon Resource Number（Amazon 資源號碼 - ARN）。請參閱 AWS 文件。您可以從 AWS 管理主控台的 **Support**（支援） > **Support Center**（支援中心） 取得 ARN。
2. 輸入您要在其中部署應程式範本資源的 **VPC Name**（**VPC** 名稱）。
3. 選用 變更網路負載平衡器管理子網路的 **NLBSubnetIPBlocks**。

STEP 10 | 檢閱範本設定並啟動範本。

STEP 11 | 確認網路負載平衡器已部署且處於就緒狀態。



©2023 Palo Alto Networks, Inc.

STEP 12 | 取得應用程式負載平衡器的 **DNS name**（**DNS** 名稱），並輸入到 web 瀏覽器中。

例如：http://MVpublic-elb-123456789.us-east-2.elb.amazonaws.com/

出現網頁時，表示您已成功啟動自動調整規模範本。

STEP 13 | 對於每個網路負載平衡器的 IP 位址，確認每個防火牆都有 NAT 原則規則。

當您部署應用程式範本來啟動網路負載平衡器和一對 Web 伺服器的另一個實例時，防火牆會去瞭解已配置給下一個網路負載平衡器實例的連接埠，然後建立另一個 NAT 原則規則。因此，如果您部署應用程式範本三次，防火牆會有三個 NAT 原則規則，分別用於連接埠 81、82 和 83。



STEP 14 | 如果您啟動應用程式範本一次以上，則需要 啟用流向 ELB 服務的流量。

啟用流向 **ELB** 服務的流量（**2.0** 版和 **2.1** 版）

如果您在部署中新增第二個或額外的內部負載平衡器 (ILB)，則必須完成其他設定，內部負載平衡器、VM-Series 防火牆自動調整規模群組和 Web 伺服器才能報告為健康情況良好，而所有 AWS 資源之間的流量也才會維持負載平衡。

在 *2.0* 版中，*ILB* 只能是網路負載平衡器。在 *2.1* 版中，*ILB* 可以是應用程式負載平衡器或網路負載平衡器。

STEP 1 | 在 AWS 管理主控台，在 DynamoDB 表格上確認配置給每個網路平衡器的連接埠。

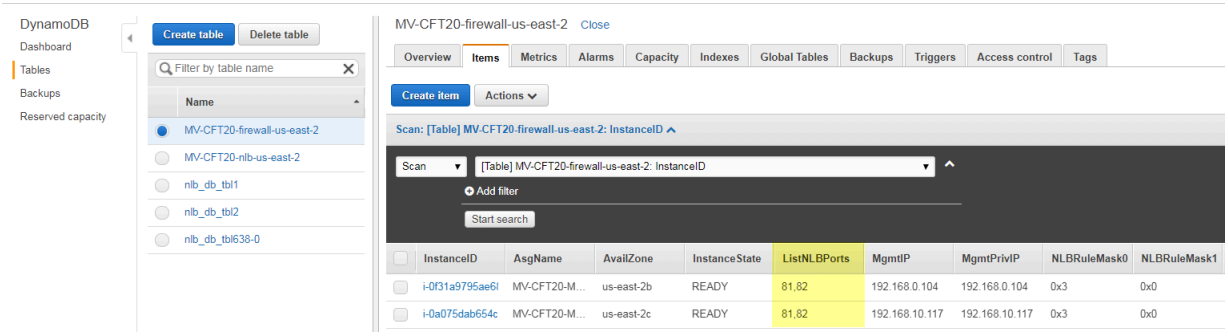
當您啟動新的內部負載平衡器時，應用程式範本必須將 SQS 訊息傳送至您啟動範本時提供作為輸入的 SQS URL。防火牆範本中的 AWS Lambda 功能可監控 SQS，並將連接埠對應新增至防火牆範本的 DynamoDB 表格。從連接埠 81 開始，針對您部署的每個額外內部負載平衡器所配置的連接埠會以 1 遞增。因此，第二個內部負載平衡器使用連接埠 82，第三個連接埠則使用連接埠 83。

1. 在 AWS 管理主控台，選取 **DynamoDB** 服務。

©2023 Palo Alto Networks, Inc.

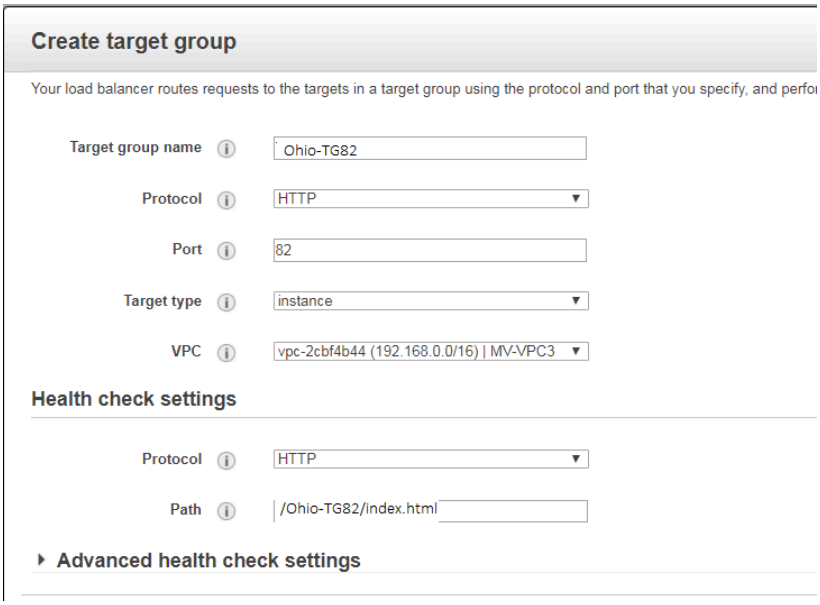
2. 選取 **Tables**（表格），按一下與您的防火牆範本的堆疊名稱相符的表格。例如，MV-CFT20-firewall-us-east-2。

   在 [Items（項目）清單] 中，檢視內部負載平衡器所使用的連接埠，這些平衡器正發佈至與防火牆範本相關聯的 SQS。



STEP 2 | 建立目標群組。內部負載平衡器會使用您為目標群組中的伺服器指定的連接埠和通訊協定，將要求傳送要已註冊的目標。

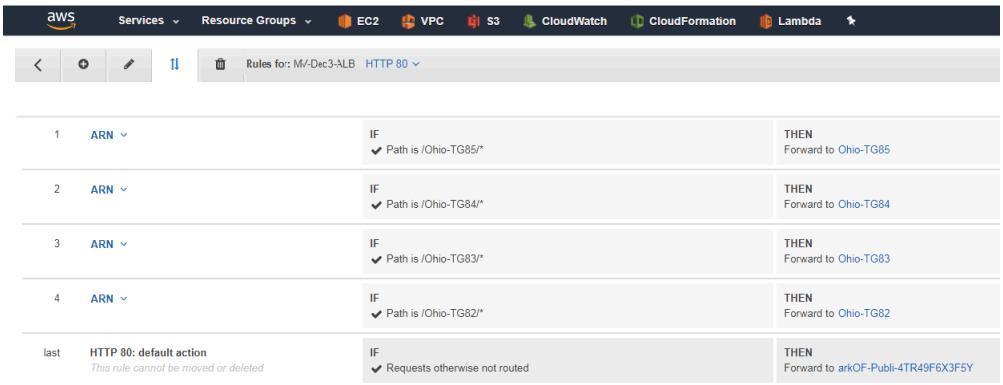
新增目標群組時，請使用您在 DynamoDB 表格上已確認的連接埠資訊。



©2023 Palo Alto Networks, Inc.

STEP 3 | 在內部負載平衡器上編輯接聽程式規則，將要求路由至目標 Web 伺服器。

1. 在 AWS 管理主控台上，於 [Load Balancing（負載平衡）] 區段中選取 **Load Balancers**（負載平衡器），並選取符合堆疊名稱的內部負載平衡器。
2. 選取 **View/edit rules**（檢視/編輯規則）以修改接聽程式的規則。
3. 選取 **Insert rule**（插入規則），並新增路徑式路由，將流量轉送至您在上方定義的目標群組，如下所示：



STEP 4 | 將目標群組附加至兩個 VM-Series 防火牆自動調整規模群組。

1. 在 Auto Scaling（自動調整規模）部分中，選取 **Auto Scaling Groups**（自動調整規模群組），並選取符合堆疊名稱的自動調整規模群組。
2. 選取 **Details**（詳細資料） > **Edit**（編輯），然後從 **Target Groups**（目標群組）下拉式清單中選取新的目標群組。



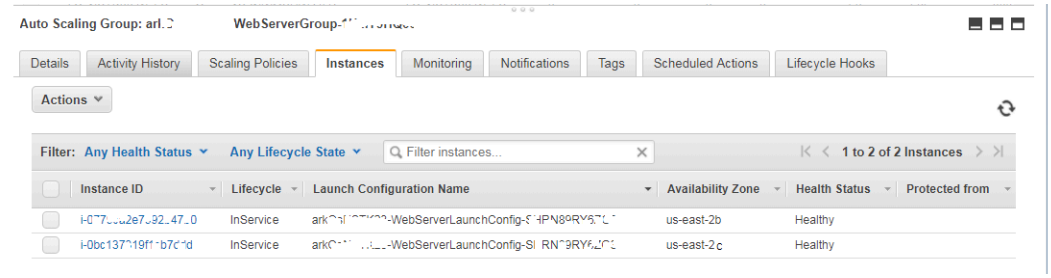
STEP 5 | 登入由應用程式範本所部署的每個 Web 伺服器，以目標群組名稱建立新的目錄，然後將 index.html 檔案複製到該目錄中。在您設定 index.html 檔案的路徑之前，此 Web 伺服器的健康情況檢查會報告為狀況不良。

```
sudo su
cd/var/www/html
mkdir <target-groupname>
cp index.html <target-groupname>
```

 ©2023 Palo Alto Networks, Inc.

STEP 6 | 驗證 Web 伺服器的健康情況。

選取 **Auto Scaling Groups**（自動調整規模群組），使用應用程式堆疊名稱來尋找 Web 伺服器自動調整規模群組，以確認 Web 伺服器報告為健康情況良好。



自訂 Bootstrap.xml 檔案（2.0 版）

對於防火牆管理員，GitHub 儲存庫中提供的 bootstrap.xml 檔案使用預設的使用者名稱和密碼。在生產環境中部署 VM-Series 自動調整規模範本之前，您至少必須為 VM-Series 防火牆的管理帳戶建立唯一的使用者名稱和密碼。（選用）您可以使用區域、原則規則和安全性設定檔來設定防火牆，並匯出最佳組態快照。然後，您就可以將此組態快照當作生產環境的 bootstrap.xml 檔案。

有兩種方法可以自訂適合生產環境使用的 bootstrap.xml 檔案。

- 選項 **1**：使用 GitHub 儲存庫中提供的啟動程序檔案，在 AWS 上啟動 VM-Series 防火牆，修改防火牆組態，然後匯出組態，為 VM-Series 自動調整規模範本建立新的 bootstrap.xml 檔案。請參閱使用 GitHub 啟動程序檔案作為種子。
- 選項 **2**：在 AWS 上啟動新的 VM-Series 防火牆（不使用啟動程序檔案），新增 NAT 原則規則以確保 VM-Series 防火牆適當地處理流量，然後匯出組態，為 VM-Series 自動調整規模範本建立新的 bootstrap.xml 檔案。請參閱從頭開始建立新的啟動程序檔案。

如果您已部署範本，而現在需要變更管理使用者的認證或新增管理使用者，並更新範本堆疊，請參閱修改管理員帳戶和更新堆疊。

從頭開始建立新的啟動程序檔案

使用支援 PAN-OS 版本的 AMI（請參閱 Panorama 外掛程式的相容性矩陣），在 AWS 上啟動新的 VM-Series 防火牆（不使用範例 bootstrap.xml 檔案），並匯出設定以建立新的 bootstrap.xml 檔案，與 VM-Series 自動調整規模範本 2.0 版搭配使用。

STEP 1 | 在 AWS 上部署 VM-Series 防火牆（不需要啟動程序），並使用公共 IP 位址透過 SSH 進入 VM-Series 防火牆的 Command Line Interface（命令行介面 - CLI）。您需要為防火牆設定新的管理密碼。

STEP 2 | 登入防火牆 Web 介面。

STEP 3 | （選用）設定防火牆。您可以設定資料平面介面、區域和原則規則。

STEP 4 | 在防火牆 **Commit**（提交）變更。

STEP 5 | 匯出組態檔案並命名為 **`bootstrap.xml`**。（**Device**（裝置） > **Setup**（設定） > **Operation**（操作） > **Export Named Configuration Snapshot**（匯出具名設定快照））。

©2023 Palo Alto Networks, Inc.

STEP 6 | 從 GitHub 儲存庫下載 bootstrap.xml 檔案，以文字編輯工具開啟，複製第 353 到 356 行。這幾行定義 AWS CloudWatch 命名空間，供防火牆在其中發佈自訂 PAN-OS 度量，而防火牆需要這些度量才能自動調整規模。

STEP 7 | 編輯您稍早匯出的組態檔案來包含 AWS CloudWatch 資訊。

在 `</management>`之後搜尋 `</management>` 並將 353 行貼到 356 行 。

```
352         </management>
353         <aws-cloudwatch>
354           <enabled>yes</enabled>
355           <name>autoscale-default-panw-asg-name</name>
356         </aws-cloudwatch>
357       </setting>
```

STEP 8 | 刪除管理介面組態。

1. 搜尋 `</service>`，並刪除後面的 IP 位址、網路遮罩和預設閘道。
2. 搜尋 `</type>`，並刪除後面的 IP 位址、網路遮罩、預設閘道和公共金鑰。

```
326         </service>
327         <ip-address>192.168.10.16</ip-address>
328         <netmask>255.255.255.0</netmask>
329         <default-gateway>192.168.10.1</default-gateway>
330         <hostname>PA-VM</hostname>
331       </system>
332       <setting>
333         <config>
334           <rematch>yes</rematch>
335         </config>
336         <management>
337           <hostname-type-in-syslog>FQDN</hostname-type-in-syslog>
338           <initcfg>
339             <type>
340               <dhcp-client>
341                 <send-hostname>yes</send-hostname>
342                 <send-client-id>no</send-client-id>
343                 <accept-dhcp-hostname>no</accept-dhcp-hostname>
344                 <accept-dhcp-domain>no</accept-dhcp-domain>
345               </dhcp-client>
346             </type>
347             <ip-address>192.168.10.16</ip-address>
348             <netmask>255.255.255.0</netmask>
349             <default-gateway>192.168.10.1</default-gateway>
350             <public-key>c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUFBREFRQUJBQUFCQVFDQTRCSjJwZFBSZlh0TjF2SDVqWW5GRUdYTVdvTmZlaU1FcCtBSlZRaVU4c2hEMHBmSUtOVTVSeHdGRFd4OVZZckRRRFVrLzQ5VDdkeThXcXorcXZ1em44dlFpamY1RDJVEeHB2WXk3ZWtiam1IallYdTVXUFR4MnZSaXdiMmVzcS91K3FXbm9hSlQ1cXdjU2srbHRxN0prVjlGcC9HSy9jQkRDT0FqOVhmSHMvWi8xQ0VZRk9uZ0UrNTd5L2VwSjFFWWtxZXlLczZuRTBvbWxRajBHSmNhb1FMcUlqZDZmQW5Dcm93dEZ4Y3c3YWVTR
351           </initcfg>
352         </management>
```

STEP 9 | 儲存檔案。您可以繼續啟動 AWS 專用 VM-Series 自動調整規模範本（2.0 版）。

使用 **GitHub** 啟動程序檔案作為種子

使用 GitHub 儲存庫中提供的啟動程序檔案，從 AWS Marketplace 在 AWS 上啟動 VM-Series 防火牆，依照您的生產環境來修改防火牆組態。然後，匯出組態來建立新的 bootstrap.xml 檔案，此檔案現在可用於 VM-Series 自動調整規模範本。

STEP 1 | 若要啟動防火牆，請參閱在 AWS 上啟動 VM-Series 防火牆。

STEP 2 | 新增 elastic network interface（彈性網路介面 - ENI）並指定相關聯的 elastic IP address（彈性 IP 位址 - EIP），讓您能夠存取 VM-Series 防火牆的網頁介面。如需詳細資訊，請參閱在 AWS 上啟動 VM-Series 防火牆。

STEP 3 | 使用 EIP 位址，並以 admin 當作使用者名稱和密碼，登入防火牆網頁介面。

STEP 4 | 為管理使用者帳戶新增安全密碼（**Device**（裝置） > **Local User Database**（本機使用者資料庫） > **Users**（使用者））。

STEP 5 | （選用）設定防火牆來保護生產環境的安全。

©2023 Palo Alto Networks, Inc.

STEP 6 | 在防火牆 **Commit**（提交）變更。

STEP 7 | 為管理員帳戶產生新的 API 金鑰。將這個新的金鑰複製到新檔案。啟動 VM-Series 自動調整規模範本時，您需要輸入此 API 金鑰；AWS 服務使用 API 金鑰來部署防火牆，以及發佈度量來自動調整規模。

STEP 8 | 匯出組態檔案並儲存為 **bootstrap.xml**。（**Device**（裝置） > **Setup**（設定） > **Operation**（操作） > **Export Named Configuration Snapshot**（匯出具名設定快照））。

STEP 9 | 使用文字編輯工具開啟 bootstrap.xml 檔案，並刪除管理介面組態。

```
326         </service>
327         <ip-address>192.168.10.16</ip-address>
328         <netmask>255.255.255.0</netmask>
329         <default-gateway>192.168.10.1</default-gateway>
330         <hostname>PA-VM</hostname>
331       </system>
332       <setting>
333         <config>
334           <rematch>yes</rematch>
335         </config>
336         <management>
337           <hostname-type-in-syslog>FQDN</hostname-type-in-syslog>
338           <initcfg>
339             <type>
340               <dhcp-client>
341                 <send-hostname>yes</send-hostname>
342                 <send-client-id>no</send-client-id>
343                 <accept-dhcp-hostname>no</accept-dhcp-hostname>
344                 <accept-dhcp-domain>no</accept-dhcp-domain>
345               </dhcp-client>
346             </type>
347             <ip-address>192.168.10.16</ip-address>
348             <netmask>255.255.255.0</netmask>
349             <default-gateway>192.168.10.1</default-gateway>
350             <public-key>c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUFBREFRQUJBQUFCQVFDQTRCSjJwZFBSZlh0TjF2SDVqWW5GRUdYTVdvTmZlaU1FcCtBSlZRaVU4c2hEMHBmSUtOVTVSeHdGRFd4OVZZckRRRFVrLzQ5VDdkeThXcXorcXZ1em44dlFpamY1RDJ4dldEaHFWQ3
                VEeHB2WXk3Zwtiam1IallYdTVXUFR4MnZSaXdiMmVzcS91K3FXbm9hSlQ1cXdjU2srbHRxN0prVjlGcC9HSy9jQkRDT0FqOVhmSHMvWi8xQ0VZRk9uZ0UrNTd5L2VwSjFFWWtxZXllLczZuRTBvbWxRajBHSmNhb1FMcUlqZDZmQW5Dcm93dEZ4Y3c3YWVTRnhZdDdXUlFY
351           </initcfg>
352         </management>
```

STEP 10 | （匯出 PAN-OS 8.0 組態時需要）確保用於驗證 Palo Alto Networks 伺服器的設定已停用。尋找 `<server-verification>no</server-verification>.`。

STEP 11 | 如果檢查是 `yes`，請變更為 **no**。

STEP 12 | 儲存檔案。您可以繼續啟動 AWS 專用 VM-Series 自動調整規模範本（2.0 版）。

應用程式範本和防火牆範本之間的 SQS 傳訊

因此，使用 firewall-v2.0.template 所部署的 VM-Series 防火牆，就能偵測流量並傳送至您要自動散佈傳入流量到其中的網路負載平衡器，此防火牆範本包含 lambda 功能來監控「簡易佇列服務」中的訊息。此訊息可讓 lambda 功能知道有新的網路負載平衡器，然後在防火牆上自動建立 NAT 原則規則，以將流量傳送到此網路負載平衡器的 IP 位址。為了在 AWS 基礎結構內適當路由流量，訊息還必須包含 DNS、VPC ID 和網路負載平衡器所屬的 AZ 的基本資訊。

如果您建立自己的應用程式範本，則必須設定應用程式範本將兩種訊息張貼至 SQS URL，供 VM-Series 自動調整規模範本 2.0 版中的防火牆範本使用，以瞭解它必須將您環境中的流量分散到哪些網路負載平衡器：

- ADD-NLB 訊息：有新的網路負載平衡器可用時通知防火牆。
- DEL-NLB 訊息：當網路負載平衡器已終止而不再可用時通知防火牆。

下列範例中的每一種訊息類型包含範例值。您需要以符合您的部署的值來修改這些訊息。

ADD-NLB 訊息

```
msg_add_nlb= { 'MSG-TYPE':'ADD-NLB', 'AVAIL-ZONES': [{'NLB-
IP':'192.168.2.101', 'ZONE-NAME':'us-east-2a', 'SUBNET-ID':
```

 ©2023 Palo Alto Networks, Inc.

```
 'subnet-2a566243'}, {'NLB-IP':'192.168.12.101', 'ZONE-NAME':'us-
east-2b', 'SUBNET-ID': 'subnet-2a566243 '}], 'DNS-NAME':
 'publicelb1-2119989486.us-east-2.elb.amazonaws.com', 'VPC-ID':
 'vpc-42ba9f2b', 'NLB-NAME': 'publicelb1' }
```

DEL-NLB 訊息

```
msg_del_nlb= { 'MSG-TYPE':'DEL-NLB', 'DNS-NAME':
 'publicelb1-2119989486.us-east-2.elb.amazonaws.com', }
```

請參閱 AWS 文件，以取得如何將訊息傳送至 Amazon SQS 佇列的詳細資訊，或檢閱範例應用程式範本套件中的 **describe_nlb_dns.py**，以瞭解應用程式範本如何建構訊息。

堆疊更新搭配 AWS 專用 VM-Series 自動調整規模範本（2.0 版）

堆疊更新可讓您修改 VM-Series 自動調整規模範本 (firewall-v2.0.template) 所部署的資源。不刪除現有部署並重新部署解決方案，而改以使用堆疊更新來修改下列參數：

- 授權—從 BYOL 切換至 PAYG（反之亦然），或從一個 PAYG 搭售包切換至另一個 PAYG 搭售包。
- 其他堆疊資源—變更啟動組態參數，例如自動調整規模群組的 Amazon Machine Image（Amazon 機器映像 - AMI）ID、AWS 實例類型、金鑰配對。您也可以更新與防火牆上的管理使用者帳戶相關聯的 API 金鑰。

變更 *AMI-ID* 可讓您搭配不同 *PAN-OS* 版本部署 *VM-Series* 防火牆的新實例。

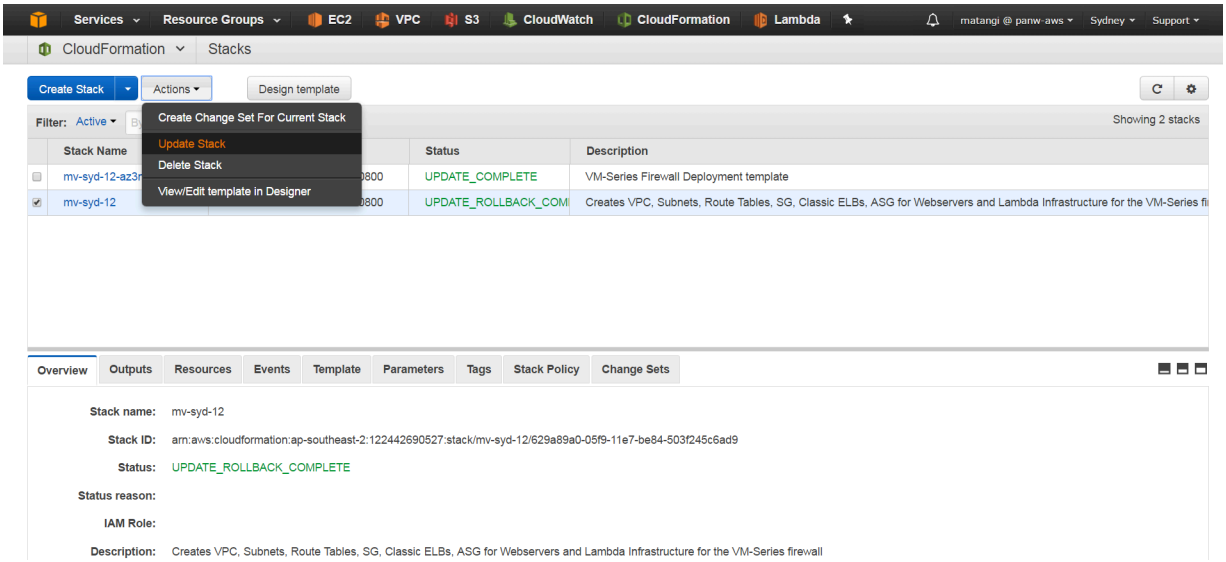
部署 VM-Series 自動調整規模範本時，將自動為您建立自動調整規模群組和啟動組態。啟動組態是自動調整規模群組用來啟用 EC2 實例的範本，可指定參數，例如自動調整規模群組的 AMI ID、實例類型、金鑰配對。若要以更新的參數啟動 VM-Series 防火牆，您必須先更新堆疊，然後刪除每個 AZ 中現有的自動調整規模群組。若要避免服務中斷，請先在一個 AZ 中刪除自動調整規模群組，並等待新的防火牆實例以更新的堆疊參數啟動。然後，確認防火牆已繼承您所做的更新，再繼續於其他 AZ 中完成變更。

對於重要的應用程式，請在維護時段執行堆疊更新。

您可以直接更新堆疊，或建立變更集。本文中的工作流程引導您手動更新堆疊。

©2023 Palo Alto Networks, Inc.

STEP 1 | 在 AWS CloudFormation 主控台，選取您要更新的上層堆疊，然後選取 **Actions**（動作） > **Update Stack**（更新堆疊）。



STEP 2 | 修改您要更新的資源。

- PAN-OS 版本—若要修改 PAN-OS 版本，請針對您要使用的版本查詢 AMI ID 並輸入 ID。
- 授權選取—從 BYOL 切換至 PAYG，或在 PAYG 搭售包 1 和 2 之間切換。

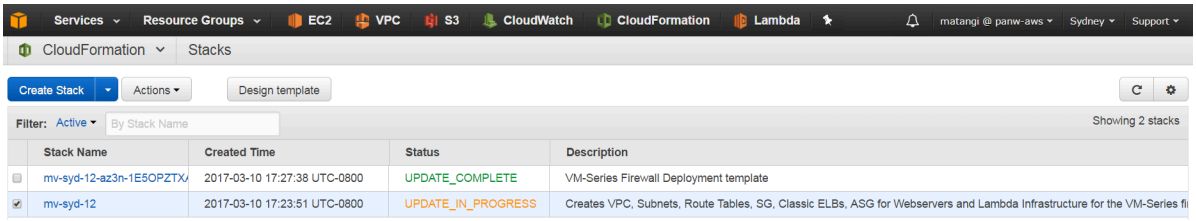
如果您要切換至 BYOL，請確保啟動程序套件包含驗證碼（請參閱步驟 3 和 5）。

如果您要在 PAYG 搭售包版本 1 和版本 2 之間切換，請針對 VM-Series 防火牆查詢 AMI ID。

- 其他堆疊資源—您可以修改堆疊資源的 AMI ID、實例類型、安全性群組、金鑰配對，或與防火牆上的管理使用者帳戶相關聯的 API 金鑰。

如果您建立新的管理使用者帳戶，或修改防火牆上現有管理員的認證，為了更新此堆疊，並以更新的 API 金鑰部署新的防火牆，您需要遵循修改管理帳戶和更新堆疊中的工作流程。

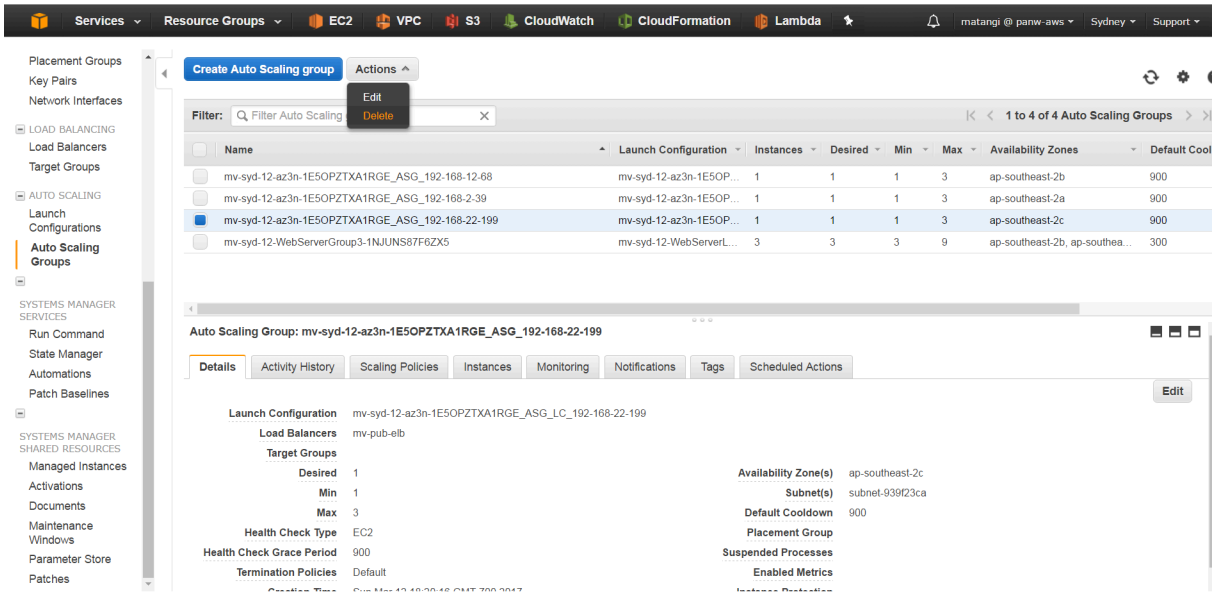
STEP 3 | 確認收到通知並檢閱變更，然後按一下 **Update**（更新）起始堆疊更新。



 ©2023 Palo Alto Networks, Inc.

STEP 4 | 在 **EC2 dashboard**（**EC2** 儀表板） > **Auto Scaling Groups**（自動調整規模群組）上，選取要刪除其中 ASG 的 AZ。

刪除 ASG 會自動觸發重新部署新的 ASG。新的 ASG 中的防火牆會使用更新的堆疊組態。



STEP 5 | 確認新的 ASG 中使用更新的參數用來啟動 VM-Series 防火牆。

使用階段式推出程序，完整測試新的 ASG，確保防火牆可適當處理流量。然後等待一小時，再繼續處理下一個 ASG。

STEP 6 | 重複步驟 4 和 5，取代其他 AZ 中的 ASG。

修改管理帳戶和更新堆疊（2.0 版）

如果您已部署範本，現在想要變更管理帳戶的密碼，或在 VM-Series 防火牆上建立新的管理使用者帳戶，您必須為管理使用者帳戶產生新的 API 金鑰，並以新的 API 金鑰更新範本堆疊。為了確保以更新的管理使用者帳戶來設定新的防火牆實例，您需要匯出防火牆組態，並重新命名為 bootstrap.xml，然後上傳至 VM-Series AutoScaling 範本使用的 S3 啟動程序資料夾。

STEP 1 | 登入防火牆的網頁介面，並變更現有管理使用者的認證，或建立新帳戶。

STEP 2 | 產生 API 金鑰。

STEP 3 | 匯出目前執行中的組態，並重新命名為 bootstrap.xml。

STEP 4 | 將此 bootstrap.xml 檔案上傳至 S3 啟動資料夾；請參閱自訂 Bootstrap.xml 檔案（2.0 版）。

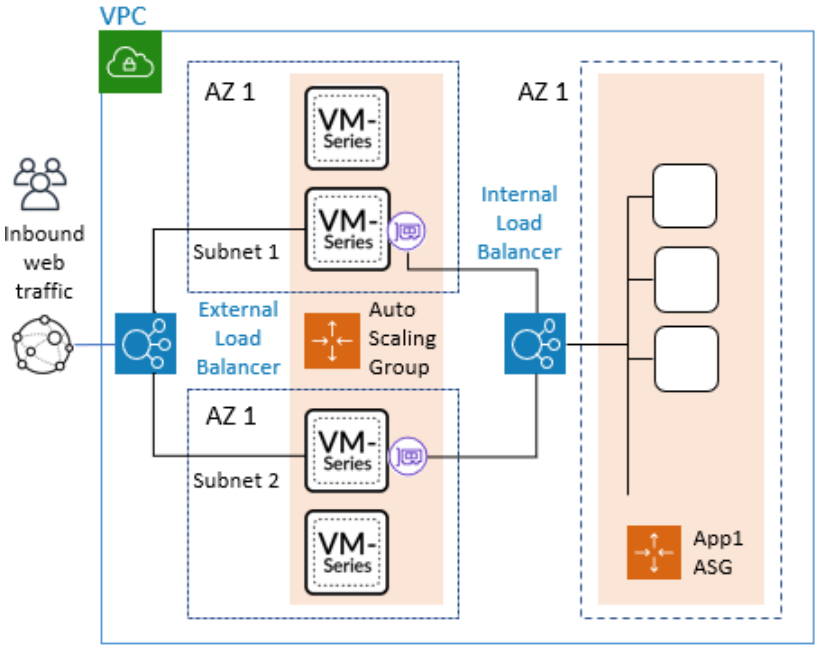
STEP 5 | 更新堆疊中的 API 金鑰，以確保新啟動的防火牆具有更新的管理員帳戶。

請參閱堆疊更新搭配 AWS 專用 VM-Series 自動調整規模範本（2.0 版）。

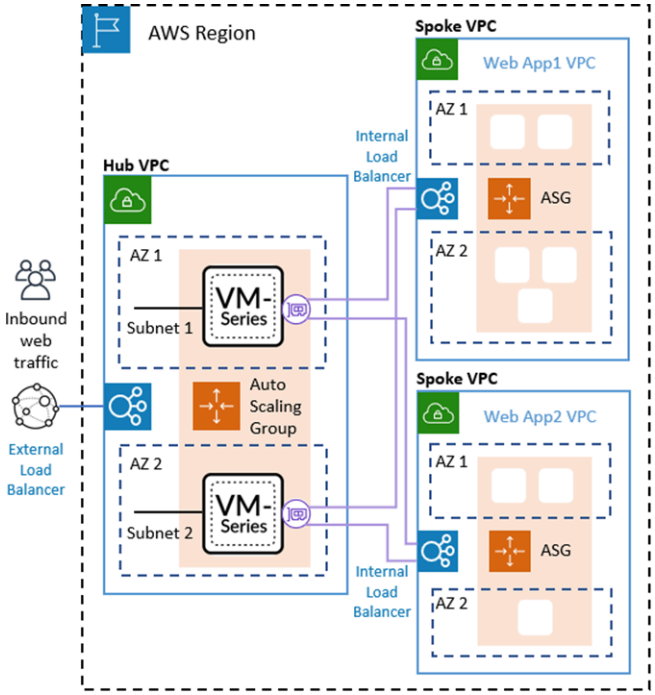
©2023 Palo Alto Networks, Inc.

AWS 專用 VM-Series 自動調整規模範本 2.1 版

VM-Series 自動調整規模範本可讓您部署 VM-Series 防火牆的單一自動調整規模群組 (ASG) 來保護從網際網路到 AWS 上您應用程式工作負載的輸入流量。您可以在單一 VPC 內部署 VM-Series 防火牆 ASG 和應用程式工作負載，如下所示。



您也可以在集中化 VPC 中部署防火牆 ASG，並在相同區域的單獨 VPC 中部署應用程式工作負載，以形成中樞和輻軸架構，如下所示。



 ©2023 Palo Alto Networks, Inc.

使用中樞和輻軸架構，您可以簡化傳遞具有許多應用程式、VPC 或帳戶之 AWS 部署的集中化安全性和連線。此架構可以增加靈活度。網路安全性管理員會管理防火牆 VPC，而 DevOps 管理員或應用程式開發人員可以管理應用程式 VPC。

確定應用程式 ***VPC*** 已連線至防火牆 ***VPC***、沒有網際網路閘道 ***(IGW)***，以及使用持續監控和安全性合規性服務，例如 Prisma Public Cloud。

您可以使用單一 AWS 帳戶或多個 AWS 帳戶，以監控和保護 VPC 與網際網路之間的流量。集中化單一 VPC 中的防火牆可以減少具有多個 VPC 和（或）多個帳戶之部署的成本。

為了提供彈性來保護應用程式工作負載，2.1 版可讓您針對前面有 VM-Series 防火牆 ASG 的外部負載平衡器與前面有應用程式工作負載的內部負載平衡器 (ILB)，部署應用程式負載平衡器或網路負載平衡器。

應用程式負載平衡器的前面有應用程式工作負載時，您可以將防火牆 VPC 連線至使用 VPC 對等的應用程式 VPC。NLB 的前面有應用程式工作負載時，您可以使用 VPC 對等或 AWS 私人連結來連線防火牆和應用程式 VPC，如下所摘要：

防火牆 **VPC LB**（外部）	應用程式 **VPC LB**（內部）	連線方法
ALB	NLB	AWS 私人連結
NLB	NLB	AWS 私人連結
NLB	ALB	VPC 對等
ALB	ALB	VPC 對等

如果您在單一 VPC 中進行部署，則可以使用前一張表格中的所有工作負載組合。

您可以使用 greenfield（新 VPC 和應用程式）和 brownfield（現有 VPC 和應用程式）使用案例來部署範本。

範本	新增	現有
防火牆	firewall-new-vpc-v2.1.template panw-aws-same-vpc-v2.1.template	firewall-existing-vpc-v2.1.template panw-aws-same-vpc-v2.1.template
應用程式	panw-aws-nlb-new-vpc-v2.1.template panw-aws-alb-new-vpc-v2.1.template	panw-aws-alb-existing-vpc-v2.1.template panw-aws-nlb-existing-vpc-v2.1.template

AWS 專用 VM-Series 自動調整規模範本（2.1 版）使用什麼元件？

AWS 專用 VM-Series 自動調整規模範本包含下列建置區塊。

- VM-Series 防火牆範本
- 應用程式範本

©2023 Palo Alto Networks, Inc.

- Lambda 功能
- Panorama
- 啟動程序檔案

VM-Series 防火牆範本

防火牆範本會在自動調整規模群組內部署一個網際網路連結的外部負載平衡器和多個 VM-Series 防火牆，而自動調整規模群組最少跨兩個可用性區域 (AZ)。外部負載平衡器會將傳入的 VPC 流量分散到 VM-Series 防火牆集區。它可以是應用程式負載平衡器 (ALB) 或網路負載平衡器 (NLB)。VM-Series 防火牆會自動發佈自訂 PAN-OS 度量，以允許自動調整規模。

範本	說明
firewall-new-vpc-v2.1.template	在新的 VPC 中部署具有兩個到四個可用性區域的防火牆堆疊。
firewall-existing-vpc-v2.1.template	在現有 VPC 中部署具有兩個到四個可用性區域的防火牆堆疊。 要在現有 VPC 中部署，您必須輸入： · VPC ID · 網際網路閘道 ID。這是現有閘道。 · 管理、不受信任、信任、NAT 閘道和 Lambda 子網路的子網路 CIDR 清單。此範本使用 CIDR 來建立這些子網路。 如果您選擇建立新的 ELB，則範本會將防火牆 ASG 連線至 ELB 後端集區。如果您使用現有 ELB，則必須手動將防火牆 ASG 連線至現有負載平衡器後端。

如需這些參數的詳細資訊，請參閱啟動之前自訂防火牆範本（2.0 版和 2.1 版）。

應用程式範本

應用程式範本會在每個可用性區域 (AZ) 中部署一個內部負載平衡器 (ILB) 和一個具有 Web 伺服器的自動調整規模群組。

範本	說明
panw-aws-same-vpc-v2.1.template	在與防火牆 VPC 相同的 VPC 中，部署應用程式。您可以選擇網路或應用程式負載平衡器。
panw-aws-alb-new-vpc-v2.1.template	使用 ALB 作為內部負載平衡器並在防火牆 VPC 與應用程式 VPC 之間使用 VPC 對等，以在新的 VPC 中部署應用程式。支援相同的帳戶和跨帳戶部署。 您必須提供下列參數： · 中樞帳戶 ID

©2023 Palo Alto Networks, Inc.

範本	說明
	· VPC 對等的中樞 VPC ID · 中樞 VPC 信任子網路 CIDR。在建立 VPC 對等之後，此範本會將這些項目用於路由表建構，即一個可用性區域一個 CIDR。 · StsAssumeRoleARN（來自中樞範本以進行 SQS 存取的輸出）
panw-aws-nlb-new-vpc-v2.1.template	使用 NLB 作為內部負載平衡器並在防火牆 VPC 與應用程式 VPC 之間使用 NLB 端點服務/介面進行通訊，以在新的 VPC 中部署應用程式。 您必須提供這些參數。 · 中樞帳戶 ID · StsAssumeRoleARN（來自中樞範本以進行 SQS 存取的輸出）
panw-aws-alb-existing-vpc-v2.1.template	在現有應用程式 VPC 中部署 ALB。您必須提供應用程式的 VPC ID 以及現有子網路 ID。 此範本會在應用程式 VPC 中部署負載平衡器，並建立 lambda 資源。您必須從任何現有負載平衡器卸除目標工作負載，並將它連線至新的負載平衡器。
panw-aws-nlb-existing-vpc-v2.1.template	在現有應用程式 VPC 中部署 NLB。使用 NLB 作為內部負載平衡器並在防火牆 VPC 與應用程式 VPC 之間使用 NLB 端點服務/介面進行通訊，以在新的 VPC 中部署應用程式。

Lambda 功能

AWS Lambda 提供穩健的事件驅動自動化，不需要複雜的協調運作軟體。AWS Lambda 會監控 Simple Queue Service (SQS)，以得知發佈至佇列的負載平衡器（ALB 或 NLB）。Lambda 功能偵測到新的負載平衡器時，會建立新的 NAT 政策規則，並將它套用至 ASG 內的 VM-Series 防火牆。防火牆具有每個應用程式的 NAT 政策規則，而且防火牆會使用 NAT 政策規則（將連接埠對應至負載平衡器 IP 位址），將流量轉送至應用程式 Web 伺服器前面的負載平衡器。

Lambda 功能也會刪除 Lambda 新增至 Panorama 中裝置群組和範本堆疊的所有設定項目。這包括 NAT 規則、位址物件，以及推送至 VM-Series 防火牆的靜態路由。Lambda 功能也會處理取消授權。

若要深入瞭解 Lambda 功能，請參閱 **Palo Alto Networks AWS** 自動調整規模文件。

Panorama

您必須具有處於 Panorama 模式的 Panorama 管理伺服器，才能設定自動調整規模 2.1 版。

©2023 Palo Alto Networks, Inc.

Panorama 管理伺服器可從單一位置集中監控和管理多個 Palo Alto Networks 新世代防火牆。Panorama 可讓您監控周遊您網路的所有應用程式、使用者和內容，然後使用此資訊來建立應用程式啟用政策，以保護和控制網路。如果您不熟悉 Panorama，則請參閱 Panorama 管理員指南。

受管理防火牆是使用 `init-config.txt` 檔案予以啟動。範例檔案包括在 GitHub 儲存庫中，以在現有 Panorama 中建立它們時複製範本堆疊和裝置群組中的設定。

Panorama 中所建立的不受信任和信任區域必須全部小寫。

在 Panorama 中，您必須使用 DHCP 來設定網路介面。

- 只有 eth1/1 才應該自動建立預設路由信任和不受信任區域。
- 安全性政策區域命名為 `untrust` 和 `trust`。

  所有區域名稱都必須是小寫。

- 這些範本會設定名為 `pandemo` 且密碼為 `demopassword` 的管理員帳戶。
- 使用命名慣例 VR-<*TemplateStackName*> 來建立虛擬路由器。在虛擬路由器 ECMP 頁籤上，啟用 ECMP。
- 若要在 Panorama 上設定 DNS 伺服器位址，請選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務）。將 **Primary DNS Server**（主要 **DNS** 伺服器）設定為 169.254.169.253、將 **Secondary DNS Server**（次要 **DNS** 伺服器）設定為 8.8.8.8，並將 **FQDN Refresh Time (sec)**（**FQDN** 重新整理時間（秒））設定為 60。Panorama 需要 AWS DNS 伺服器 IP 位址，才能解析 AWS 上內部負載平衡器的 FQDN。FQDN 重新整理時間是 Panorama 認可新偵測到內部負載平衡器的間隔。

啟動應用程式範本之後，Lambda 會在 Panorama 中填入下列資訊：

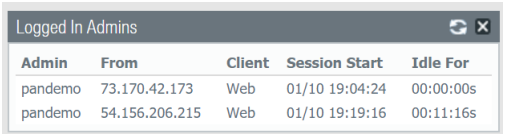
- NAT 政策
- 應用程式範本中 LB 的位址物件
- 虛擬路由器中的靜態路由
- Tcp81 服務物件

2.1 版防火牆範本包括 AWS NAT 閘道，供防火牆用來發出輸出要求以擷取更新、連線至 Panorama，以及將度量發佈至 AWS CloudWatch。NAT 閘道也會有每個區域與其連接的彈性 IP 位址。

您需要下列 Panorama 資源才能處理 AWS 專用自動調整規模範本。

Panorama API 金鑰	您需要 Panorama API 金鑰才能驗證 API。Lambda 使用您的 API 金鑰來自動設定範本和裝置群組選項。若要產生 API 金鑰，請參閱取得 API 金鑰。

©2023 Palo Alto Networks, Inc.

Panorama 授權停用金鑰	範本需要授權停用 API 金鑰並啟用 [Verify Update Server Identity（驗證更新伺服器識別）]，才能從 Panorama 停用授權金鑰。授權停用金鑰應取自 Palo Alto 客戶支援入口網站，如安裝授權 API 金鑰所述。
Panorama VM-Auth-Key	您需要有 vm-auth-key，才能讓啟動的防火牆連線至 Panorama，並接收其啟動程序設定。請參閱 在 Panorama 上產生 VM 驗證金鑰。
Panorama 管理介面存取	· 連接埠 **443 (HTTPS)**—初始部署防火牆範本時，請保持 HTTPS 的開啟狀態，讓 Lambda 可以連線至 Panorama。在 Panorama 中，等待接收下列連線確認：  Logged In Admins Admin From Client Session Start Idle For pandemo 73.170.42.173 Web 01/10 19:04:24 00:00:00s pandemo 54.156.206.215 Web 01/10 19:19:16 00:11:16s 當您保護連接埠 443 時，請指定從中允許連線的 IP 位址範圍，以及指派給 NAT 閘道的 EIP。有兩個 NAT 閘道和其相關聯的 EIP。若要在 AWS 中找到 NAT 閘道 EIP，請移至 **VPC** > **NAT Gateways**（**NAT** 閘道）。請記下進行 HTTPS 之安全性群組的 EIP 資訊。 · 連接埠 **3978**—連接埠 3978 必須可以接收來自任何 IP 位址的流量。

啟動程序檔案

GitHub 自動調整規模儲存庫包括 **`init-cfg.txt`** 檔案，讓 VM-Series 防火牆具有基本設定可以：

- 執行介面交換，讓 VM-Series 防火牆 **`untrust`** 流量針對 eth0 使用 AWS ENI。
- 與 Panorama 通訊以取得裝置群組和範本設定。

自動調整規模 GitHub 儲存庫具有基本設定可以開始使用。此自動調整規模解決方案需要交換資料平面和管理介面，才能讓負載平衡器將網頁流量轉送至 VM-Series 防火牆自動調整規模層。如需使用 Amazon ELB 的管理介面對應的詳細資料，請參閱搭配 Amazon ELB 使用的管理介面對應。

規劃部署 AWS 專用 VM-Series 自動調整規模範本（2.1 版）

開始部署之前，請檢閱下列資源。

- 如需範本功能和帳戶規劃的概觀，請參閱使用 Amazon ELB 服務自動調整 VM-Series 防火牆規模。
- 啟動之前自訂防火牆範本（2.0 版和 2.1 版）.本主題中的基本參數會套用至所有範本版本。
- AWS 專用 VM-Series 自動調整規模範本（2.0 版和 2.1 版）如何啟用動態調整規模？

  這些概念會套用至所有範本版本。

啟動防火牆範本（2.1 版）

您可以選擇在相同的 VPC 或單獨的 VPC 中部署防火牆和應用程式範本。

©2023 Palo Alto Networks, Inc.

這些範本支援中樞和輻軸架構，而您可以用來將防火牆範本部署於一個 AWS 帳戶，然後作為中樞來保護屬於相同或不同 AWS 帳戶的應用程式（輻軸）。

此工作流程說明如何使用防火牆範本來部署外部負載平衡器和 VM-Series 防火牆。在啟動此範本之前，必須先在 Panorama 上設定 vm-auth-key。

STEP 1 | 檢閱規劃部署 AWS 專用 VM-Series 自動調整規模範本（2.1 版）和規劃 AWS 專用 VM-Series 自動調整規模範本（2.0 版和 2.1 版）中的檢查清單。

確認您已完成下列工作：

- （僅適用於 PAYG）檢閱並接受您打算使用之 PAYG 搭售包的 EULA。
- （僅適用於 BYOL）取得搭售包的授權碼，而授權碼支援您部署可能需要的防火牆數目。您必須將此授權碼儲存至名為 **authcodes** 的文字檔案（無副檔名），並將 **authcodes** 檔案放在啟動程序套件的 **/license** 資料夾中。

  如果您使用個別授權碼，而非搭售包，則防火牆只會擷取檔案中第一個授權碼的授權金鑰。

- 從 GitHub 儲存庫，下載啟動 VM-Series 自動調整規模 2.1 版範本所需的檔案。

©2023 Palo Alto Networks, Inc.

STEP 2 | 修改 `init-cfg.txt` 檔案，並將它上傳至 `/config` 資料夾。

因為您使用 Panorama 啟動 VM-Series 防火牆，所以應該修改 `init-cfg.txt` 檔案，如下所示。不需要 `bootstrap.xml` 檔案。

```
type=dhcp-client
```

```
ip-address=
```

```
default-gateway=
```

```
netmask=
```

```
ipv6-address=
```

```
ipv6-default-gateway=
```

```
hostname=
```

```
vm-auth-key=
```

```
panorama-server=
```

```
panorama-server-2=
```

```
tplname=AWS-tmplspoke1
```

```
dgname=AWS-dgspoke1
```

```
dns-primary=169.254.169.253
```

```
dns-secondary=8.8.8.8
```

```
op-command-modes=mgmt-interface-swap
```

```
dhcp-send-hostname=yes
```


©2023 Palo Alto Networks, Inc.

```
dhcp-send-client-id=yes
```

```
dhcp-accept-server-hostname=yesdhcp-accept-server-domain=yes
```

```
vm-series-auto-registration-id=
```

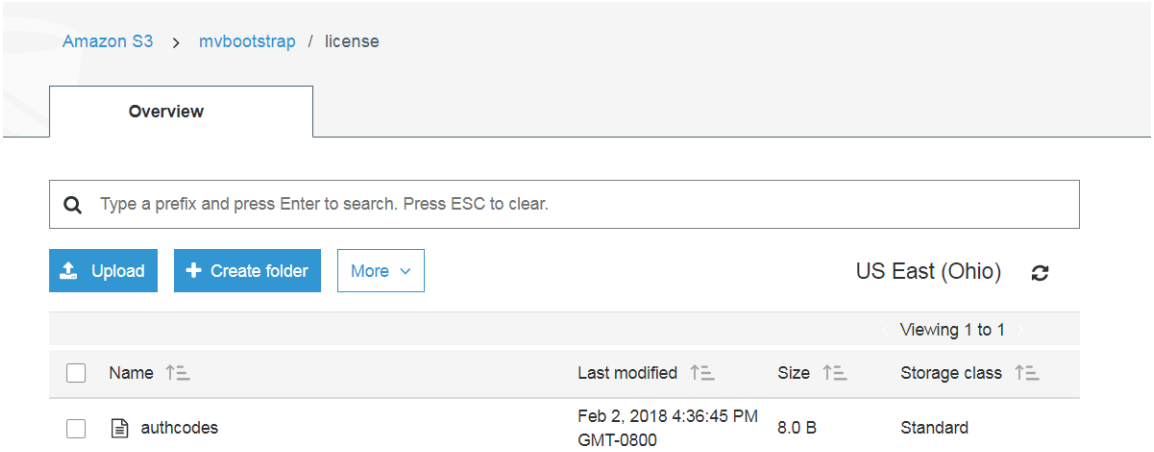
```
vm-series-auto-registration-pin-value=
```

確認 **op-command-modes=mgmt-interface-swap** 存在。此命令用於在 AWS 的 VM-Series 防火牆上交換管理介面 (mgmt) 和資料平面介面 (ethernet 1/1)。使用 AWS DNS 伺服器 IP 位址 169.254.169.253，更快速地重新解析負載平衡器 DNS 名稱。

您必須將裝置憑證自動註冊 PIN 新增至 init-cfg.txt 檔案，才能在部署 VM-Series 防火牆實例時自動安裝裝置憑證。

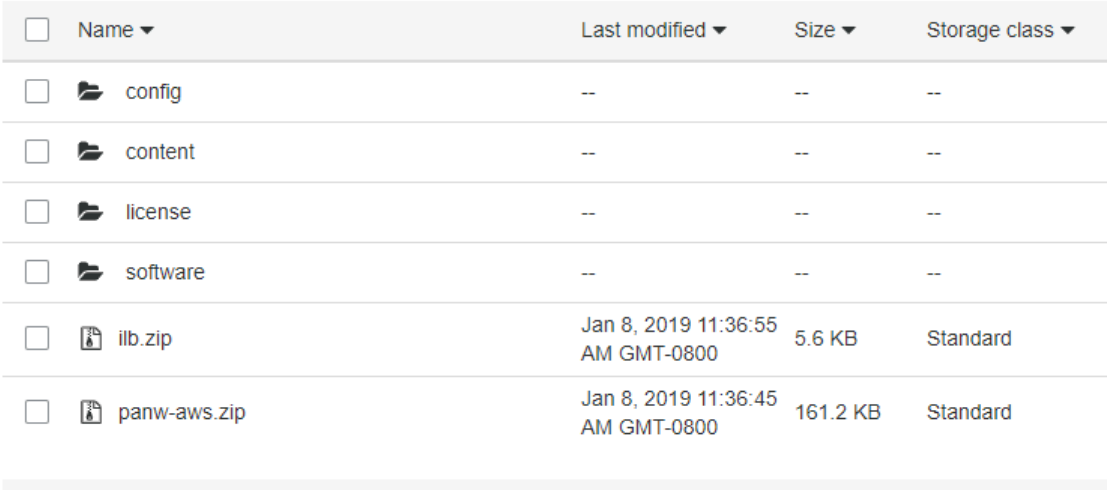
STEP 3 | （僅適用於 BYOL）在啟動程序套件的 **/license** 資料夾中新增授權碼。

1. 使用文字編輯器建立名為 **authcodes** 的新文字檔案（無副檔名）。
2. 將 BYOL 授權的授權碼新增至此檔案，並儲存。授權碼必須代表搭售包，而且必須支援您部署可能需要的防火牆數目。如果您使用個別授權碼，而非搭售包，則防火牆只會擷取檔案中第一個授權碼的授權金鑰。



 ©2023 Palo Alto Networks, Inc.

STEP 4 | 將防火牆範本 (`panw-aws-zip`) 和應用程式範本 (`ilb.zip`) 的 Lambda 程式碼上傳至 S3 貯體。您可以使用用於啟動的相同 S3 貯體。



Name	Last modified	Size	Storage class
config	--	--	--
content	--	--	--
license	--	--	--
software	--	--	--
ilb.zip	Jan 8, 2019 11:36:55 AM GMT-0800	5.6 KB	Standard
panw-aws.zip	Jan 8, 2019 11:36:45 AM GMT-0800	161.2 KB	Standard

如果透過與防火牆不同的帳戶來管理應用程式堆疊，則請使用應用程式帳戶以在與防火牆範本相同的 AWS 區域中建立另一個 s3 貯體，並將 `ilb.zip` 複製至該 s3 貯體。

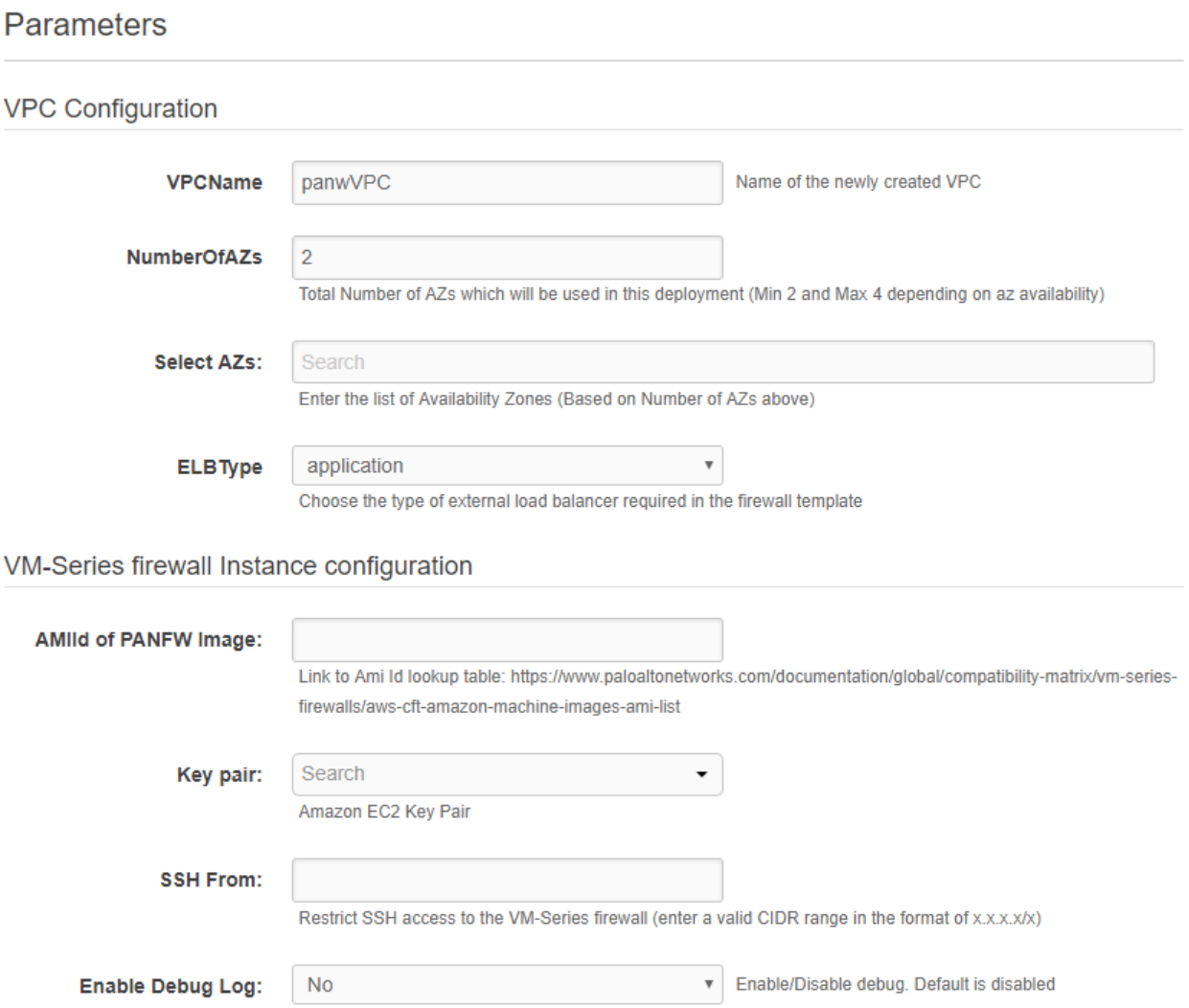
STEP 5 | 選取防火牆範本。

1. 在 AWS 管理主控台，選取 **CloudFormation** > **Create Stack**（建立堆疊）。
2. 選取 [Upload a template to Amazon S3（將範本上傳至 Amazon S3）] 以選擇應用程式範本，將範本所啟動的資源部署至與防火牆相同的 VPC 內或不同的 VPC。按一下 [Open（開啟）] 和 [Next（下一步）]。
3. 指定堆疊名稱。堆疊名稱可讓您唯一地識別所有使用此範本所部署的資源。

©2023 Palo Alto Networks, Inc.

STEP 6 | 設定 VPC 的參數。

1. 務必選取至少兩個可用性區域

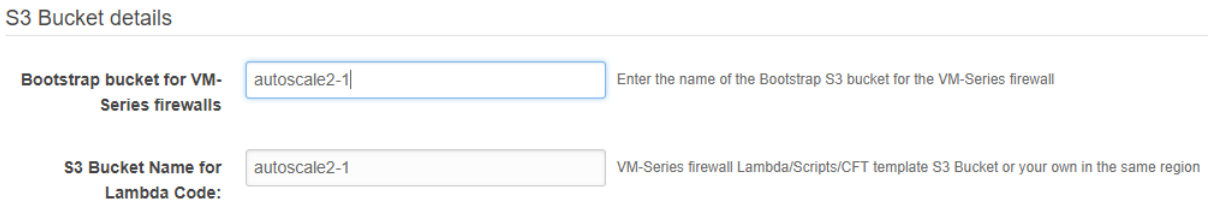


2. 查閱並輸入 VM-Series 防火牆的 AMI ID。確保 AMI ID 符合您選取使用的 AWS 區域、PAN-OS 版本和 BYOL 或 PAYG 授權選項。
3. 選取 EC2 **Key pair**（金鑰配對）（從下拉式清單）以啟動防火牆。若要登入防火牆，您必須提供此金鑰配對及其相關聯私密金鑰的名稱。
4. 針對 **SSH From**（**SSH** 來源）欄位，防火牆將由 Panorama 進行管理，而且沒有管理介面的 EIP。但有時您會決定指派要從中連線的 EIP 設定 IP 範圍。
5. 如果您想要 **Enable Debug Log**（啟用偵錯日誌），請選取 **Yes**（是）。啟用偵錯日誌會產生更詳細的日誌，這有助於部署問題的疑難排解。這些日誌是以堆疊名稱產生，並儲存在 AWS CloudWatch 中。

依預設，範本使用 CPU 使用率作為 VM-Series 防火牆的調整規模參數。 自訂 PAN-OS 度量會自動發佈至與您稍早指定的堆疊名稱相符的 CloudWatch 命名空間。

©2023 Palo Alto Networks, Inc.

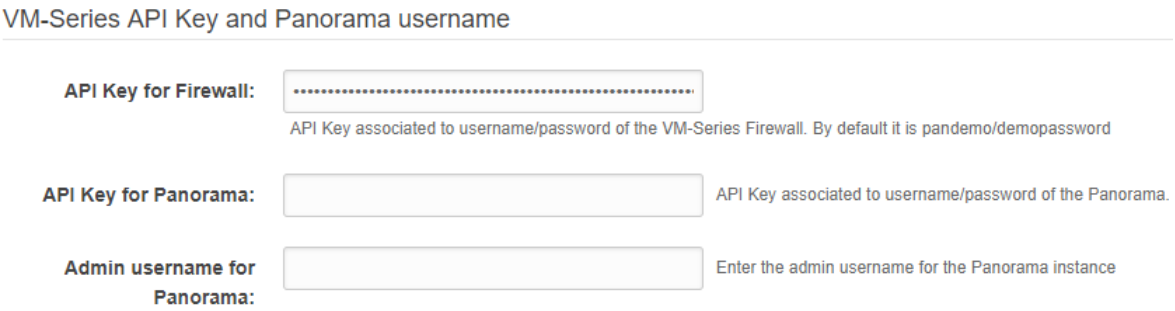
STEP 7 | 指定 Amazon S3 貯體的名稱。



1. 輸入含有啟動程序套件的 S3 貯體的名稱。

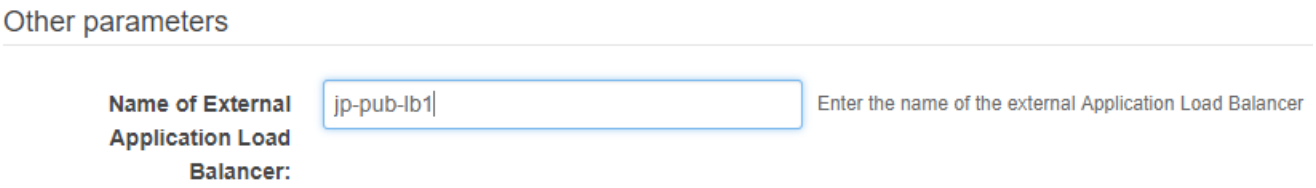
   如果啟動載入貯體未適當設定，或貯體名稱輸入不正確，啟動載入程序會失敗，您也無法登入防火牆。負載平衡器的健康情況檢查也會失敗。
2. 輸入含有 panw-aws.zip 檔案的 S3 貯體的名稱。如前所提及，您可以針對啟動程序和 Lambda 程式碼使用一個 S3 貯體。

STEP 8 | 指定金鑰以允許 API 存取防火牆和 Panorama。



1. 輸入防火牆驗證 API 呼叫時必須使用的金鑰。預設金鑰是以範例檔案為基礎，僅適用於測試和評估。在生產環境中，您必須針對 API 呼叫建立個別的 PAN-OS 登入，並產生相關聯的金鑰。
2. 輸入 API 金鑰，以允許 AWS Lambda 對 Panorama 發出 API 呼叫。在生產環境中，您應該針對 API 呼叫建立個別的登入，並產生相關聯的金鑰。

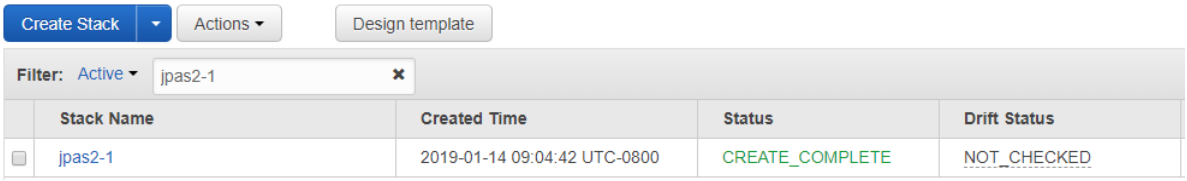
STEP 9 | 輸入應用程式負載平衡器的名稱。



©2023 Palo Alto Networks, Inc.

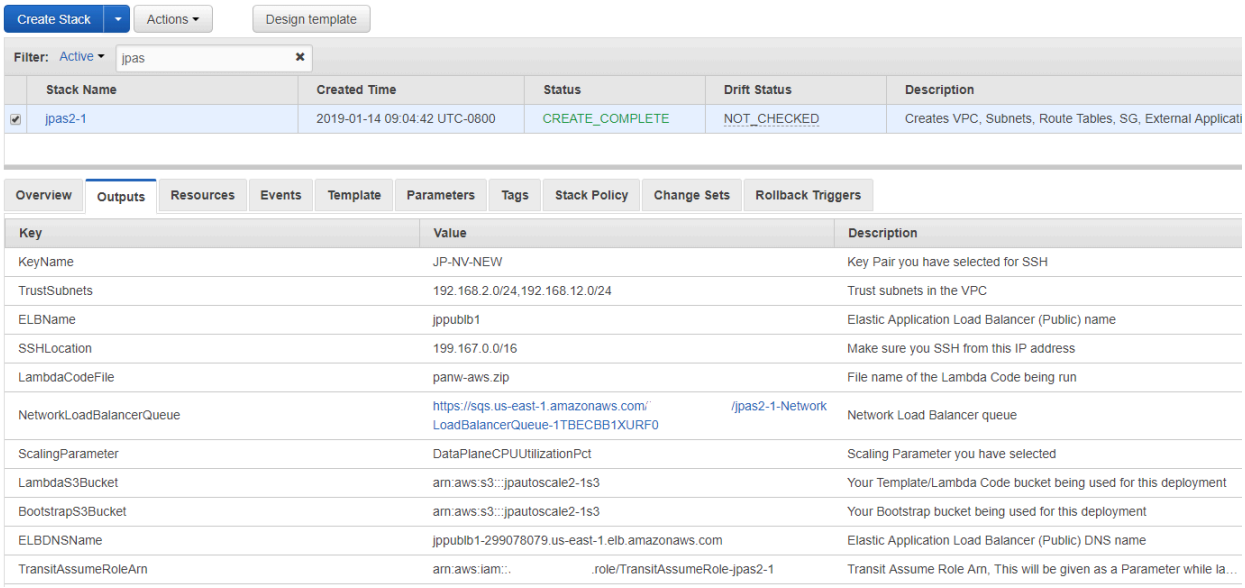
STEP 10 | 檢閱範本設定並啟動範本。

1. 選取 **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**（我瞭解此範本可能導致 **AWS CloudFormation** 建立 **IAM** 資源）。
2. 按一下 **Create**（建立）來啟動範本。將會顯示 CREATE_IN_PROGRESS 事件。
3. 成功部署時，狀態會更新為 CREATE_COMPLETE。



STEP 11 | 確認範本已啟動所有必要資源。

1. 在 [EC2 Dashboard（EC2 儀表板）] 上，選取 [Auto Scaling Groups（自動調整規模群組）]。在每個 AZ 中，確認 VM-Series 防火牆有一個 ASG。ASG 名稱首碼包含堆疊名稱。
2. 在 AWS 管理主控台上，選取堆疊名稱來檢視 [Output（輸出）] 中的資源清單。
3. 您的輸出應該與下圖中的輸出類似。
   - 請記下網路負載平衡器佇列名稱。
   - 請記下彈性負載平衡器公共 DNS 名稱。



可能需要長達 *20* 分鐘，防火牆才會完成啟動且能夠處理流量。

完成測試或生產部署時，完全刪除堆疊是確保停止收費的唯一辦法。關閉實例或將 *ASG* 最大值變更為 *0* 不夠。

©2023 Palo Alto Networks, Inc.

STEP 12 | 儲存下列防火牆範本資訊。部署應用程式範本時，您必須提供這些值作為輸入。

- 每個 **AZ** 中 **NAT** 閘道的 **IP** 位址—您需要此 IP 位址來限制 HTTPS 存取 Panorama，讓 Lambda 在必要時可使用 NAT 閘道的 EIP 與 Panorama 通訊。
- 網路負載平衡器 **SQS URL**—防火牆堆疊中的 Lambda 功能會監控此佇列，以瞭解您部署的任何網路負載平衡器，並在 Panorama 上建立 NAT 政策規則（一個應用程式一個），讓防火牆能夠將流量傳送至網路負載平衡器 IP 位址。

啟動應用程式範本（2.1 版）

應用程式範本可讓您完成分層式拓撲，還可讓您評估自動調整規模解決方案。此應用程式範本會在 VM-Series 防火牆（已使用防火牆範本進行部署）的自動調整規模群組後面，部署應用程式或網路負載平衡器和一對 Web 伺服器。

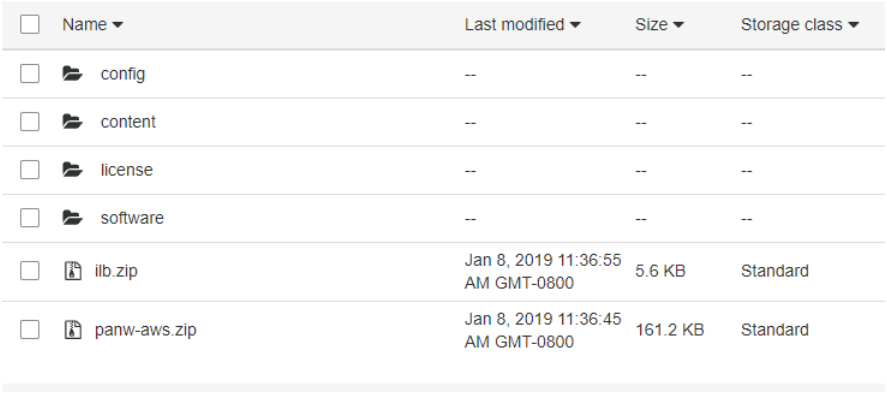
使用此範本來評估解決方案，但自訂您自己的範本來部署到生產環境。針對自訂範本，務必啟用應用程式範本與防火牆範本之間的 SQS 傳訊。

啟動應用程式範本時，必須根據想要在您部署防火牆範本的相同 VPC 內還是在不同的 VPC 中部署應用程式範本，來選取範本。請參閱 啟用流向 ELB 服務的流量（2.0 版和 2.1 版）。

STEP 1 | 建立您將從中啟動應用程式範本的 S3 貯體。

- 如果這是跨帳戶部署，則請建立新的貯體。
- 如果有一個帳戶，則您可以建立新貯體，或使用您稍早建立的 S3 貯體（您可以針對所有項目使用一個貯體）。

STEP 2 | 將 ilb.zip 檔案上傳至 S3 貯體。



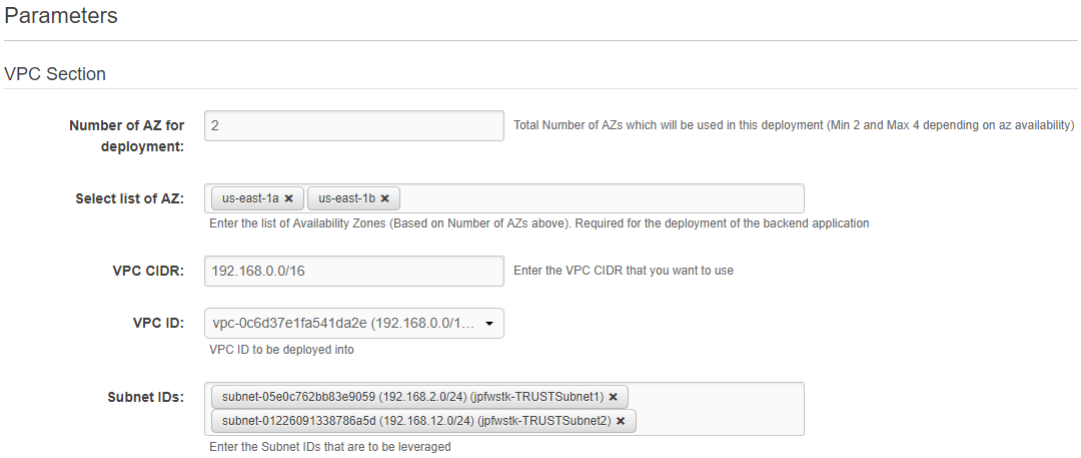
STEP 3 | 選取您想要啟動的應用程式啟動範本。

1. 在 AWS 管理主控台中，選取 **CloudFormation** > **CreateStack**
2. 選取 [Upload a template to Amazon S3（將範本上傳至 Amazon S3）] 以選擇應用程式範本，將範本所啟動的資源部署至與防火牆相同的 VPC 內或不同的 VPC。按一下 **Open**（開啟）和 **Next**（下一步）。
3. 指定堆疊名稱。堆疊名稱可讓您唯一地識別所有使用此範本所部署的資源。

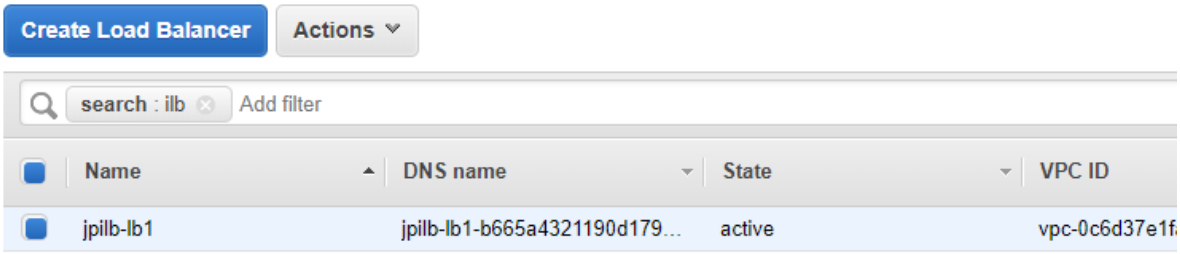
©2023 Palo Alto Networks, Inc.

STEP 4 | 設定 VPC 和網路負載平衡器的參數。

1. 在 [Select list of AZ（選取 AZ 清單）] 中，選取您的設定將跨越的兩個可用性區域。如果部署在相同的 VPC 內，請確保您選取的可用性區域，與您為防火牆範本選取的可用性區域相同。
2. 如果部署至新的 VPC，請輸入 VPC 的 CIDR 區塊。預設 CIDR 為 192.168.0.0/16。
3. 如果部署至相同的 VPC，則您將選取前一個 VPC，並使用信任子網路。

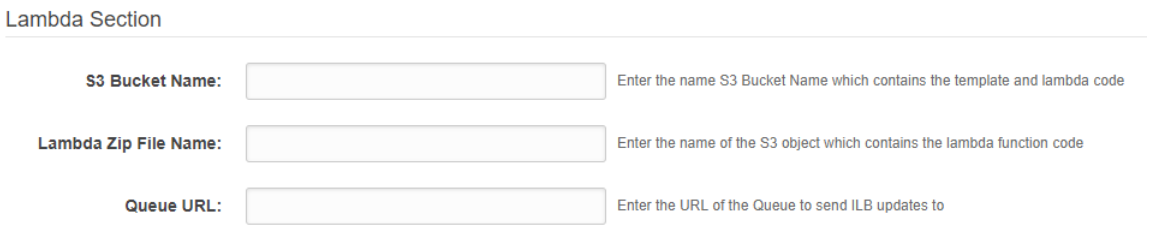


STEP 5 | 選取負載平衡器類型。



STEP 6 | 設定 Lambda 的參數。

1. 輸入 ilb.zip 儲存所在的 S3 貯體名稱。
2. 輸入 zip 檔案名稱。
3. 貼上您稍早複製的 SQS URL。



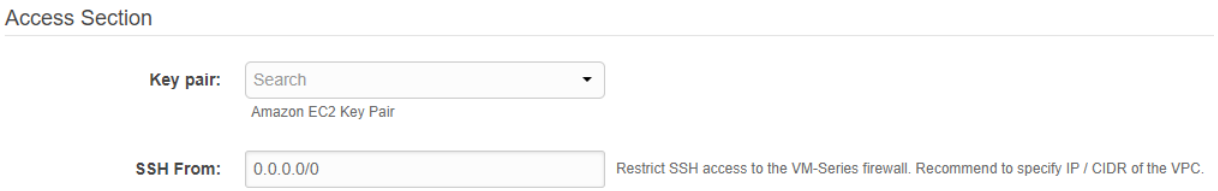
©2023 Palo Alto Networks, Inc.

STEP 7 | 修改 Web 伺服器 EC2 實例類型，以符合您的需求。



STEP 8 | 從下拉式清單中選取 [EC2 Key pair（EC2 金鑰配對）]，以啟動 Web 伺服器。若要登入 Web 伺服器，您必須提供金鑰配對名稱及其相關聯的私密金鑰。

STEP 9 | 僅針對管理存取，選取您將從中存取伺服器的網路的 IP 位址。網頁流量來自您在啟動防火牆範本時所複製的 ELBDNS 名稱。

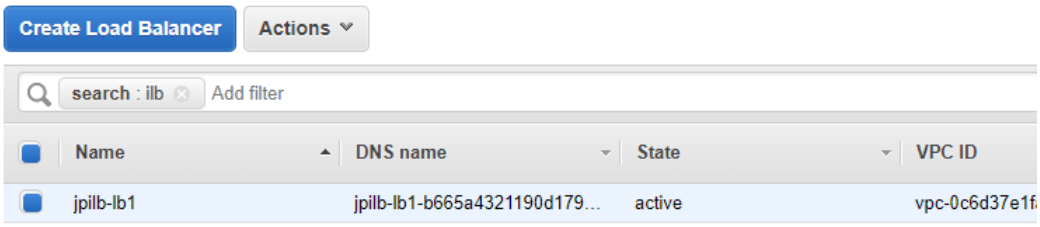


STEP 10 | 檢閱範本設定並啟動範本。

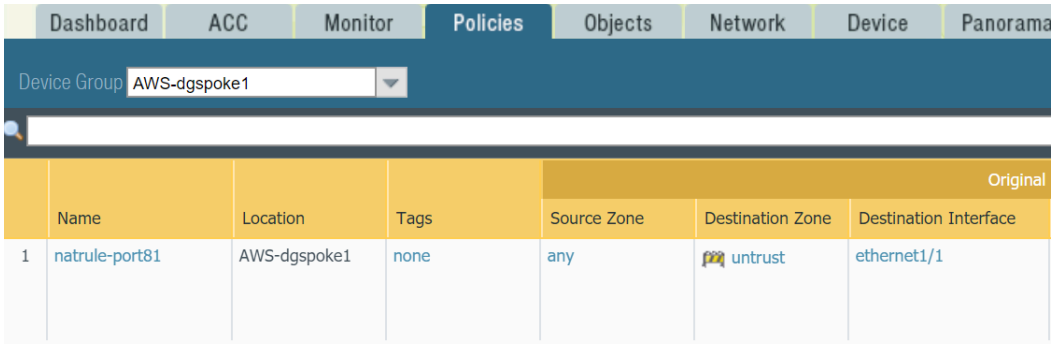
©2023 Palo Alto Networks, Inc.

STEP 11 | 完成應用程式範本之後，可能需要最多 20 分鐘，網頁才會作用。

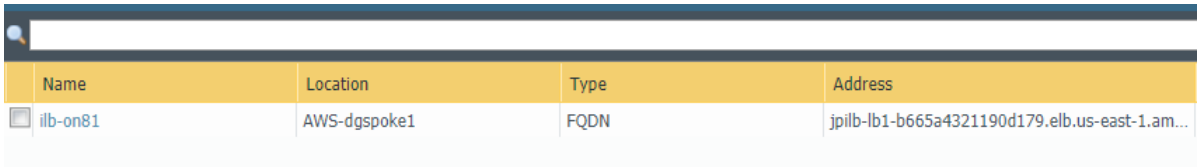
1. 確認將應用程式範本負載平衡器標示為使用中。



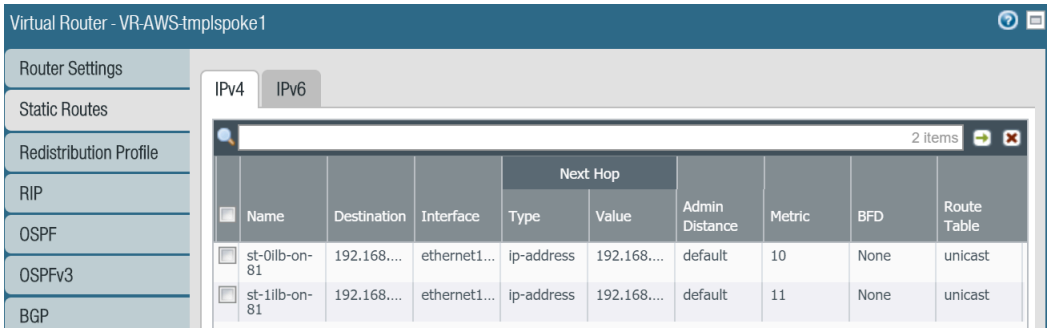
2. 確認 Panorama 在裝置群組中具有 NAT 物件。



3. 確認 Panorama 在裝置群組中具有位址物件。



4. 確認 Panorama 在範本堆疊中具有靜態路由。



STEP 12 | 取得您稍早針對應用程式負載平衡器所儲存的 DNS 名稱，並將它輸入至 Web 瀏覽器。

©2023 Palo Alto Networks, Inc.

STEP 13 | 成功啟動時，您的瀏覽器應該與此輸出類似。



Congratulations, you have successfully launched VM-Series ASG CloudFormation. This file is coming from Webserver Region: us-east-1

StackID: arn:aws:cloudformation:us-east-1: :stack/jpappstk1/1c197cb0-18f4-11e9-b92e-0ab87eb901cc

StackName: jpappstk1

建立自訂 Amazon 機器映像（2.1 版）

自訂 VM-Series AMI 可讓您使用您想要使用的 PAN-OS 版本，在網路上一致且彈性地部署 VM-Series 防火牆，而非限制為只能使用發佈至 AWS 公共 Marketplace 或 AWS GovCloud Marketplace 的 AMI。使用自訂 AMI 可加速使用所選擇的 PAN-OS 版本來部署防火牆的程序，因為它會減少下列操作的時間：使用 AWS 公共或 AWS GovCloud Marketplace 上所發佈的 AMI 來佈建防火牆，然後執行軟體升級來取得您想要在網路上使用的 PAN-OS 版本。此外，您還可以在自動調整規模 VM-Series 防火牆 CloudFormation 範本或您已建立的任何其他範本中使用自訂 AMI。

您可以使用 BYOL、搭售包 1 或搭售包 2 授權來建立自訂 AMI。建立自訂 AMI 的程序需要您移除防火牆中的所有設定，並執行私人資料重設，因此，在此工作流程中，您將從 AWS Marketplace 啟動新的防火牆實例，而非使用您已完全設定的現有防火牆。

使用防火牆的 *BYOL* 版本來建立自訂 *AMI* 時，您必須先在防火牆上啟動授權，才能存取與下載 *PAN-OS* 內容和軟體更新來升級防火牆，然後先停用防火牆上的授權，再執行私人資料重設並建立自訂 *AMI*。如果您未停用授權，則會遺失您在此防火牆實例上套用的授權。

STEP 1 | 從 Marketplace 啟動 VM-Series 防火牆。

請參閱啟動 VM-Series 防火牆。

STEP 2 | （僅適用於 BYOL）啟動授權。

STEP 3 | 在防火牆上安裝最新內容。

STEP 4 | （僅適用於 BYOL）停用授權。

©2023 Palo Alto Networks, Inc.

STEP 5 | 執行私人資料重設。

私人資料重設會移除所有日誌，並還原預設設定。

系統磁碟不會予以消除，因此步驟 4 中的內容更新會保持不變。

1. 存取防火牆 CLI。
2. 匯出設定的複本。
3. 移除所有日誌，並還原預設設定。

```
request system private-data-reset
```

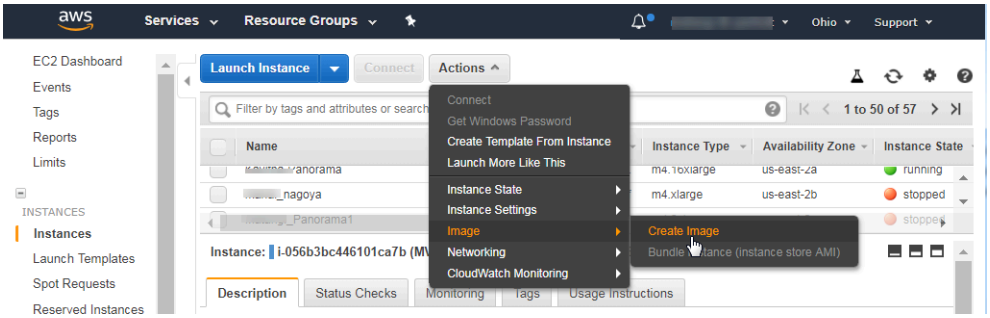
輸入 **y** 以確認。

防火牆會重新啟動以初始化預設設定。

©2023 Palo Alto Networks, Inc.

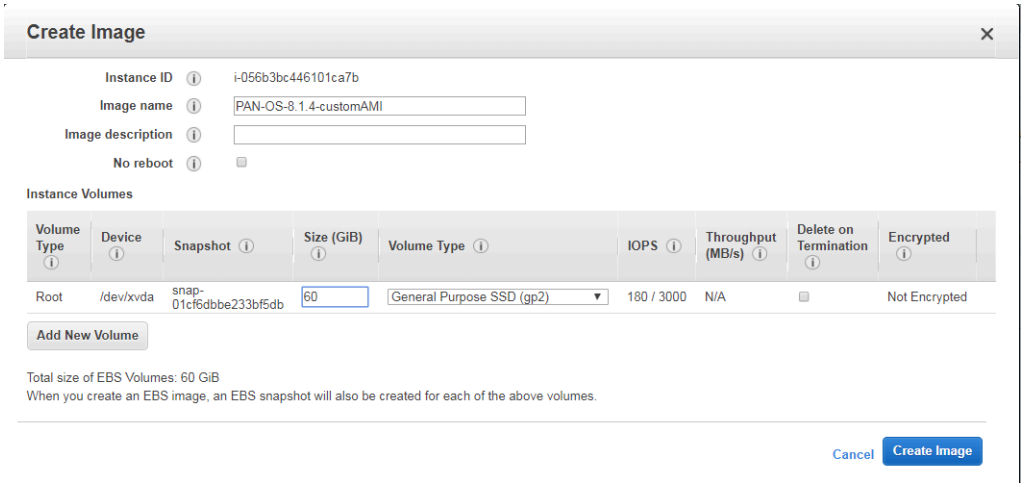
STEP 6 | 建立自訂 AMI。

1. 登入 AWS 主控台，並選取 [EC2 Dashboard（EC2 儀表板）]。
2. **Stop**（停止）VM-Series 防火牆。
3. 選取 VM-Series 防火牆實例，然後按一下 **Image**（映像） > **Create Image**（建立映像）。



4. 輸入自訂映像名稱，然後按一下 **Create Image**（建立映像）。

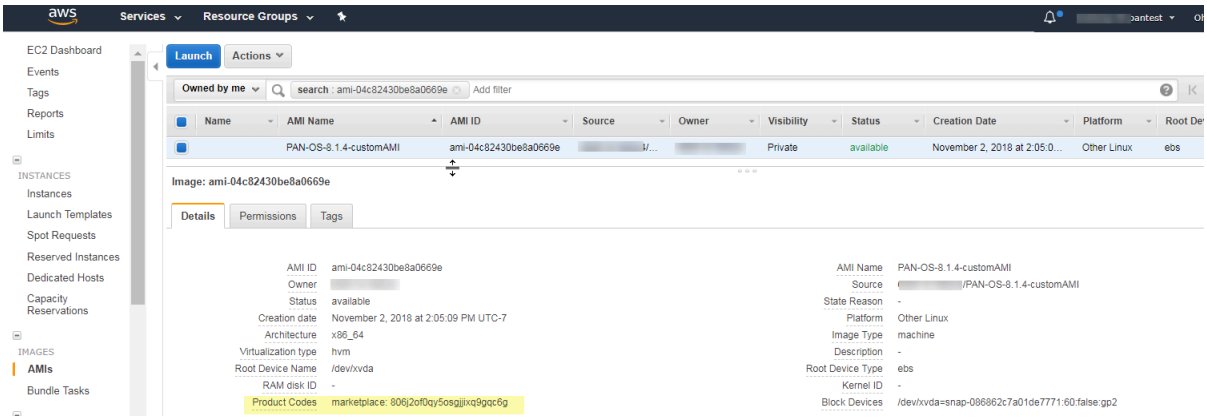
   60GB 的磁碟空間是最低需求。



5. 確認自訂 AMI 已建立並具有正確的產品代碼。

   1. 在 [EC2 Dashboard（EC2 儀表板）] 上，選取 **AMI**。
   2. 選取您剛剛建立的 AMI。根據您使用 BYOL、搭售包 1 還是搭售包 2 授權選項來選取 AMI，您應該會在詳細資料中看到下列其中一個 **Product Codes**（產品代碼）：
      - BYOL—6njl1pau431dv1qxipg63mvah
      - 搭售包 1—6kxdw3bbmdeda3o6i1ggqt4km
      - Bundle 2—806j2of0qy5osgjjixq9gqc6g

©2023 Palo Alto Networks, Inc.



STEP 7 | 在 AWS 上加密 VM-Series 防火牆的 EBS 磁碟區.

如果您計劃搭配使用自訂 AMI 與使用 Amazon ELB 服務自動調整 VM-Series 防火牆規模部署的 EBS 加密，則必須使用 AWS 帳戶的預設主要金鑰。

VM-Series 自動調整規模範本清除（2.1 版）

如果您已將範本部署為測試，則請刪除它們以節省資源並降低成本。

STEP 1 | 在 AWS 管理主控台中，選取 **Cloud Formation** > **Create Stack**（建立堆疊）。

STEP 2 | 找到您先前啟動的防火牆範本和應用程式範本，並刪除兩個範本。

如需刪除範本堆疊詳細資訊，請參閱何謂 AWS CloudFormation?

刪除範本堆疊失敗，會導致 *AWS* 費用。

應用程式範本與防火牆範本之間的 SQS 傳訊（2.1 版）

使用其中一個防火牆範本所部署的 VM-Series 防火牆可以偵測流量，並將其傳送至您要自動將傳入流量散佈到其中的負載平衡器。為了完成此操作，防火牆範本包含 lambda 功能來監控簡易佇列服務是否有訊息。訊息可讓 lambda 功能知道有新的負載平衡器，然後在防火牆上自動建立 NAT 原則規則，以將流量傳送至負載平衡器的 IP 位址。若要在 AWS 基礎結構內適當路由流量，訊息還必須包含 DNS、VPC ID 和負載平衡器所屬的 AZ 的基本資訊。

如果您要建立自己的應用程式範本，則必須設定應用程式範本以將 ADD 和 DEL 訊息張貼至 SQS URL，供防火牆範本用來瞭解必須將您環境中的流量分散到哪些負載平衡器：

- ADD-NLB 訊息：有新的網路負載平衡器可用時通知防火牆。
- DEL-NLB 訊息：當網路負載平衡器已終止而不再可用時通知防火牆。
- ADD-ALB 訊息：有新的應用程式負載平衡器可用時通知防火牆。
- DEL-ALB 訊息：當應用程式負載平衡器已終止而不再可用時通知防火牆。

下列範例中的每種訊息類型都包括範例值。您必須使用符合您部署的值來修改這些訊息。

ADD-NLB 訊息

©2023 Palo Alto Networks, Inc.

```
msg_add_nlb= {
       "MSG-TYPE":"ADD-NLB",
       "AVAIL-ZONES": [
       {
           "NLB-IP":"192.168.2.101",
           "ZONE-NAME":"us-east-2a",
           "SUBNET-ID": "subnet-2a566243"
       },
       {
           "NLB-IP":"192.168.12.101",
           "ZONE-NAME":"us-east-2b",
           "SUBNET-ID": "subnet-2a566243 "
       }
       ],
            "DNS-NAME": "publicelb1-2119989486.us-
east-2.elb.amazonaws.com",
           "VPC-ID": "vpc-42ba9f2b",
           "NLB-NAME": "publicelb1"
}
```


©2023 Palo Alto Networks, Inc.

DEL-NLB 訊息

```
msg_del_nlb= {
 "MSG-TYPE":"DEL-NLB",
 "DNS-NAME": "publicelb1-2119989486.us-east-2.elb.amazonaws.com",
}
```

ADD-ALB

```
{ "AVAIL-ZONES": [
       {
           "SUBNET-CIDR":"172.32.0.0/24",
           "SUBNET-ID": "subnet-0953a3a8e2a8208a9",
           "ZONE-NAME": "us-east-2a"
       },
       {
           "SUBNET-CIDR":"172.32.2.0/24",
           "SUBNET-ID": "subnet-0a9602e4fb0d88baa",
           "ZONE-NAME": "us-east-2c"
       },
       {
           "SUBNET-CIDR":"172.32.1.0/24",
```


©2023 Palo Alto Networks, Inc.

```
            "SUBNET-ID": "subnet-0b31ed16f308b3c4d",

            "ZONE-NAME": "us-east-2b"

        }

    ],

    "VPC-PEERCONN-ID": "pcx-0538bb05dbe2e1b8e",

    "VPC-CIDR":"172.32.0.0/16",

    "ALB-NAME": "appILB-908-0",

    "ALB-ARN":"arn:aws:elasticloadbalancing:us-
east-2:018147215560:loadbalancer/app/appILB-908-0/1997ed20eeb5bcef",

    "VPC-ID": "vpc-0d9234597da6d9147",

    "MSG-TYPE":"ADD-ALB",

    "DNS-NAME": "internal-appILB-908-0-484644265.us-
east-2.elb.amazonaws.com"

}
```

DEL-ALB 訊息

```
{

    "MSG-TYPE":"DEL-ALB",

    "DNS-NAME": "internal-appILB-908-0-484644265.us-
east-2.elb.amazonaws.com"

}
```

如需如何將訊息傳送至 Amazon SQS 佇列的詳細資料，請參閱 AWS 文件。

©2023 Palo Alto Networks, Inc.

堆疊更新搭配 AWS 專用 VM-Series 自動調整規模範本（2.1 版）

堆疊更新可讓您修改 VM-Series 自動調整規模範本防火牆範本所部署的資源。使用堆疊更新來修改啟動設定參數，而不刪除現有部署並重新部署解決方案。

您可以修改 AWS 實例類型、自動調整規模群組的金鑰配對，以及與防火牆上管理使用者帳戶相關聯的 API 金鑰。

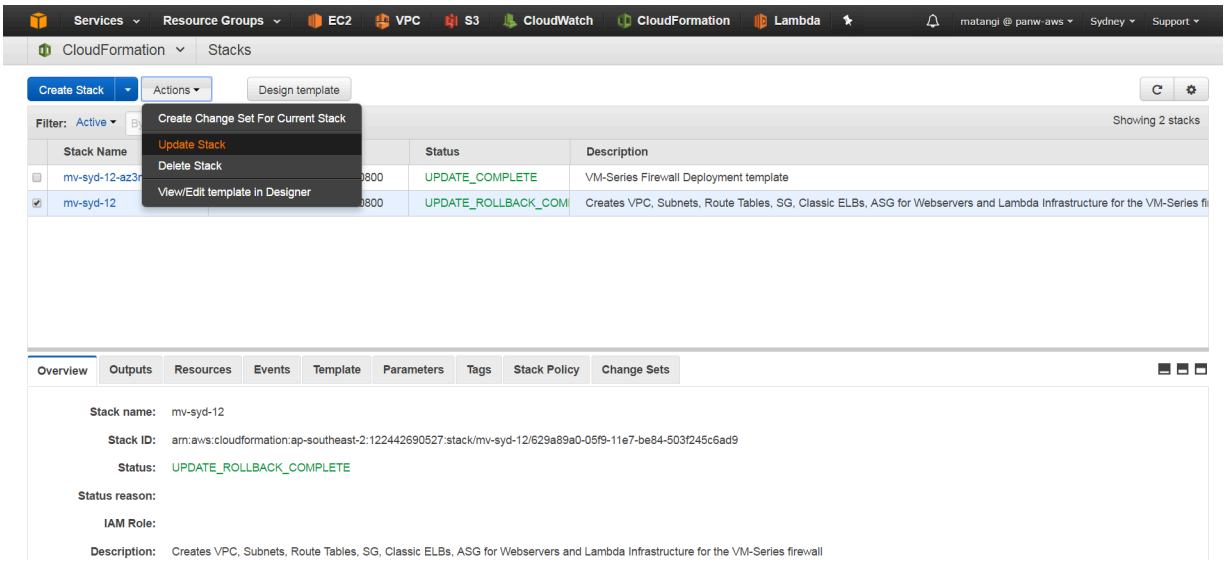
您不需要更新堆疊，即可修改預設通知或建立自動調整規模警報。請參閱變更調整規模參數和 CloudWatch 度量（2.1 版）。

部署 VM-Series 自動調整規模範本時，將自動為您建立自動調整規模群組和啟動組態。啟動設定是自動調整規模群組用來啟動 EC2 實例的範本，而且可以指定參數，例如實例類型、自動調整規模群組的金鑰配對，或與防火牆上管理使用者帳戶相關聯的 API 金鑰。

對於重要的應用程式，請在維護時段執行堆疊更新。

您可以直接更新堆疊或建立變更集合。本文中的工作流程引導您手動更新堆疊。

STEP 1 | 在 AWS CloudFormation 主控台，選取您要更新的上層堆疊，然後選取 **Actions**（動作） > **Update Stack**（更新堆疊）。



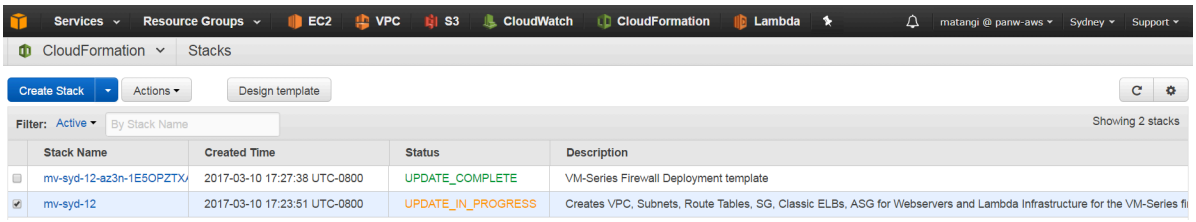
STEP 2 | 修改您要更新的資源。

您可以修改實例類型、安全性群組、堆疊資源的金鑰配對，或與防火牆上管理使用者帳戶相關聯的 API 金鑰。

如果您建立新的管理使用者帳戶，或修改防火牆上現有管理員的認證，則為了更新該堆疊，並使用更新的 API 金鑰來部署新的防火牆，您需要遵循修改管理帳戶（2.1 版）中的工作流程。

©2023 Palo Alto Networks, Inc.

STEP 3 | 確認收到通知並檢閱變更，然後按一下 **Update**（更新）起始堆疊更新。



修改管理帳戶（2.1 版）

如果您已部署範本，現在想要變更管理帳戶的密碼，或在 VM-Series 防火牆上建立新的管理使用者帳戶，您必須為管理使用者帳戶產生新的 API 金鑰，並以新的 API 金鑰更新範本堆疊。

STEP 1 | 登入防火牆的網頁介面，並變更現有管理使用者的認證，或建立新帳戶。

STEP 2 | 產生 API 金鑰。

STEP 3 | 更新堆疊中的 API 金鑰，以確保新啟動的防火牆具有更新的管理員帳戶。

請參閱堆疊更新搭配 AWS 專用 VM-Series 自動調整規模範本（2.0 版）。

變更調整規模參數和 CloudWatch 度量（2.1 版）

此工作說明如何使用自訂 PAN-OS 度量作為調整規模參數，來觸發自動調整規模動作。

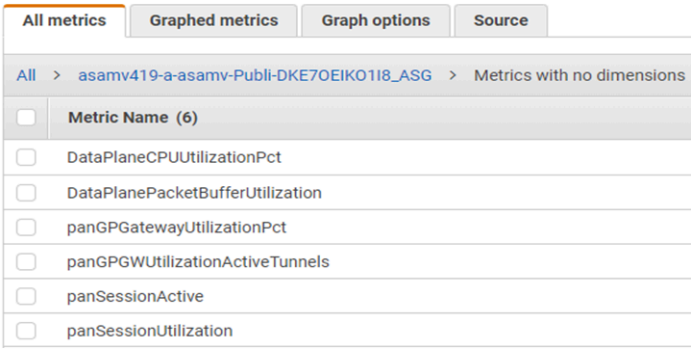
當您啟動防火牆範本時，範本會使用可用來定義自動調整規模動作的相應縮小和相應放大政策來建立命名空間。政策名稱包括命名空間，如下所示：

- <Custom Namespace>-scalein - 移除 1 個實例
- <Custom Namespace>-scaleout - 新增 1 個實例

每個 PAN-OS 度量都會有您可刪除和取代為自動調整規模動作的預設通知。針對每個度量，建立兩個動作：一個決定何時新增 VM-Series 防火牆，另一個則決定何時移除 VM-Series 防火牆。

STEP 1 | 在 AWS 中，選取 **Services**（服務） > **CloudWatch** > **Metrics**（度量）。

STEP 2 | 選擇 **Custom Namespace**（自訂命名空間）連結，然後選取度量連結以檢視自訂 PAN-OS 度量。



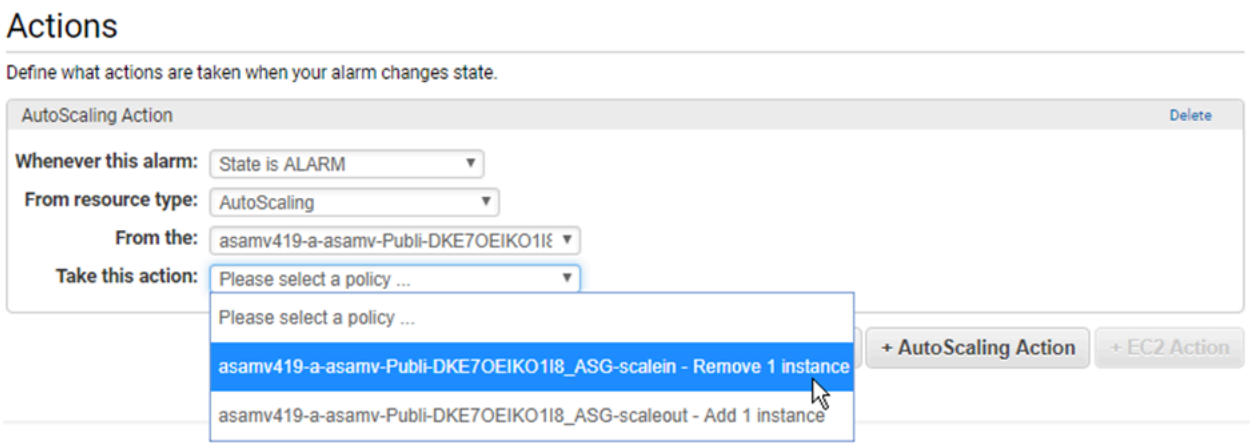
 ©2023 Palo Alto Networks, Inc.

STEP 3 | 核取方塊以選取度量，然後選取 **Graphed metrics**（圖形化度量）頁籤。

1. 在 **Statistics**（統計資料）欄中，選擇統計資料準則（例如平均值、最小值和最大值），然後選擇期間。
2. 在 **Actions**（動作）欄中，選取鈴（Create alarm（建立警報））。

STEP 4 | 定義一個警報，以在過了您設定的時間範圍後，CPU 使用率符合或低於您所設定的準則時移除防火牆。

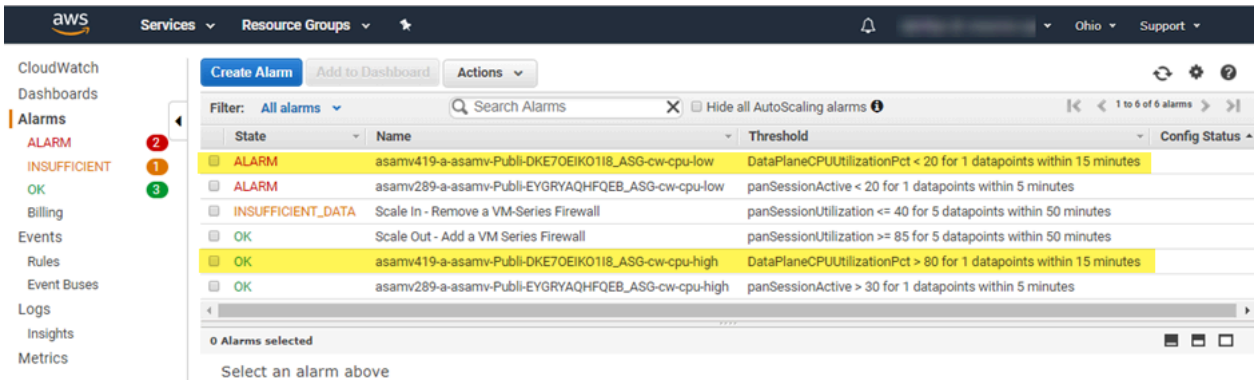
1. 選取 **Edit**（編輯），以變更圖形標題。
2. 在 **Alarm details**（警報詳細資料）下方，填寫 **Name**（名稱） 和 **Description**（描述），並選擇運算子，然後設定最小值來維護目前實例。如果未維護最小值，則會移除實例。
3. 在 **Actions**（動作）下方，**delete**（刪除）預設通知。
4. 選取 **+AutoScaling Action**（+自動調整規模動作）。
   - 使用 **From the**（從）清單來選取命名空間。
   - 從 **Take this action**（採取此動作）中，選取要移除實例的政策。



5. 選取 **Create Alarm**（建立警報）。

STEP 5 | 建立第二個警報，以在 CPU 使用率符合或超過您所設定的準則時新增防火牆。

STEP 6 | 若要檢視警報，請選取 **Services**（服務） > **CloudWatch** > **Alarms**（警報）。



若要從此視窗編輯警報，請核取警報旁邊的方塊，然後選取 **Action**（動作） > **Edit**（編輯）。

©2023 Palo Alto Networks, Inc.

在 AWS VPC 上監控的屬性清單

在 AWS VPC 中佈建或修改虛擬機器時，您有兩種方法可以監控這些實例並擷取標籤，用作動態位址群組中的比對準則。

- **VM** 資訊來源—在新世代防火牆上，您總共可監控多達 32 個標籤—14 個預先定義的標籤和 18 個使用者定義的鍵值組（標籤）。
- **Panorama** 上的 **AWS** 外掛程式—AWS 專用 Panorama 外掛程式可讓您將 Panorama 連線至公共雲端上的 AWS VPC，並擷取虛擬機器的 IP 位址與標籤對應。然後，Panorama 向已設定通知的受管理 Palo Alto Networks® 防火牆註冊 VM 資訊。透過該外掛程式，Panorama 可為每個虛擬機器共擷取 32 個標籤，11 個預先定義標籤和多達 21 個使用者定義標籤。



標籤-值的長度上限（包括名稱和值）必須是 *116* 個字元或更少。如果標籤長度超過 *116* 個字元，*Panorama* 則不會擷取此標籤並將其在防火牆上註冊。

AWS-VPC 上監控的屬性		防火牆上的 **VM** 資訊來源	**Panorama** 上的 **AWS** 外掛程式
AMI ID	映像 ID.<ImageId string>	是	是
架構	架構.<Architecture string>	是	否。
可用性區域	可用性區域.<string>	是	是
來賓 OS	來賓 OS.<guest OS name>	是	否。
IAM 實例設定檔	IAM 實例設定檔.<instanceProfileArn>	否。	是
執行個體 ID	執行個體 ID.<InstanceId string>	是	否。
執行個體狀態	執行個體狀態.<instance state>	是	否。
執行個體類型	執行個體類型.<instance type>	是	否。
金鑰名稱	金鑰名稱.<KeyName string>	是	是
擁有者 ID 從 ENI 擷取此屬性的值。	帳戶號碼.<OwnerId>	否。	是
位置 租用、群組名稱	位置.租用戶.<string> 位置.群組名稱.<string>	是	是

©2023 Palo Alto Networks, Inc.

AWS-VPC 上監控的屬性		防火牆上的 VM 資訊來源	Panorama 上的 AWS 外掛程式
私人 DNS 名稱	私人 DNS 名稱.<Private DNS Name>	是	否。
公開 DNS 名稱	公開 DNS 名稱.<Public DNS Name>	是	是
子網路 ID	子網路 ID.<subnetID string>	是	是
安全性群組 ID	Sg ID.<sg-xxxx>	否。	是
安全性群組名稱	Sg-名稱.<SecurityGroupName>	否。	是
VPC ID	VpcId.<VpcId string>	是	是
Tag (金鑰，值)	aws 標籤.<key>.<value>	是； 支援多達 18 個使用者定義標籤。使用者定義的標籤按字母順序排序，前 18 個標籤可用於防火牆。	是； 支援多達 21 個使用者定義標籤。使用者定義的標籤按字母順序排序，前 21 個標籤可用於 Panorama 及防火牆。

監控 AWS VPC 所需的 IAM 權限

若要啟用 VM 監控，繫結至 AWS 存取金鑰和密碼存取金鑰的使用者 AWS 憑證，必須擁有上列屬性的權限。這些權限允許防火牆啟動 API 叫用來監控 AWS VPC 中虛擬電腦。

與使用者關聯的 IAM 原則必須擁有全域唯讀存取權限，例如 AmazonEC2ReadOnlyAccess，或者必須包含所有受監控屬性的個人權限。下列 IAM 原則範例列示了啟動 API 動作來監控 AWS VPC 中的資源的權限：

```
{ "版本":"2012-10-17", "聲明": [ { "效果":"允許", "行動": ["ec2:描述可用區域", "ec2:描述映像", "ec2:描述實例", "ec2:描述狀態", "ec2:描述金鑰配對", "ec2:描述放置群組", "ec2:描述區域", "ec2:描述子網路", "ec2:描述標籤", "ec2:描述 VPC" ], "資源": [ "*" ] } ] }
```


©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

在 KVM 上設定 VM-Series 防火牆

核心式虛擬機器 (KVM) 是開放原始碼虛擬模組，適用於執行 Linux 發行版的伺服器。VM-Series 防火牆可部署在執行 KVM Hypervisor 的 Linux 伺服器上。

本指南假設您有使用 Linux 的現有 IT 基礎結構，並已有使用 Linux/Linux 工具的基礎。指南中的指示只於在 KVM 上部署 VM-Series 防火牆有關。

- KVM 上的 VM-Series—需求與先決條件
- KVM 上支援的部署
- 在 KVM 上安裝 VM-Series 防火牆
- KVM 專用 VM-Series 的效能調整
- 智慧流量卸載

KVM 上的 VM-Series—需求與先決條件

- 在網路上連接 VM-Series 的選項
- KVM 上 VM-Series 的先決條件

表 **2: KVM** 上的 **VM-Series**—系統需求

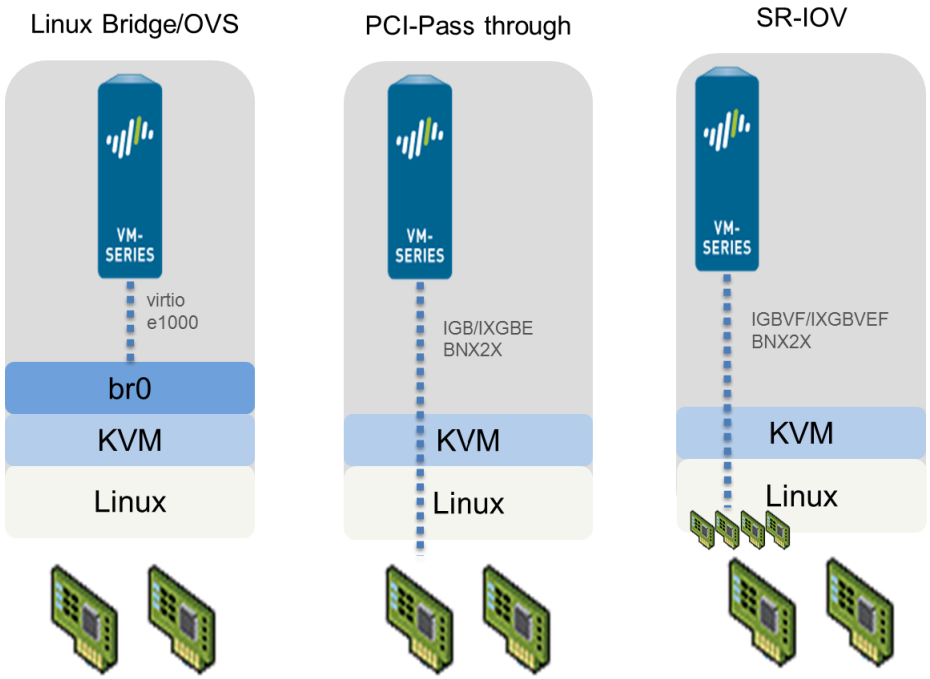
需求	說明
硬體資源	有關您的 VM-Series 型號的最低硬體需求，請參閱 VM-Series 系統需求。
軟體版本	請參閱「相容性矩陣」，以瞭解支援的 KVM 軟體版本。
SR-IOV 驅動程式	請參閱相容性矩陣中的 PacketMMAP 驅動程式版本驅動程式。
DPDK 驅動程式	請參閱相容性矩陣中的 DPDK 驅動程式版本。 如果您在 KVM 的 VM-Series 上使用其中一個支援的 NIC 驅動程式，則 DPDK 預設為啟用。
網路介面—網路介面卡與軟體橋接器	KVM 上的 VM-Series 總共 25 個介面 — 1 個管理介面，最多 24 個網路介面用於資料流量。 部署在 KVM 上的 VM-Series 支援軟體式虛擬交換器，例如 Linux 橋接器或 Open vSwitch 橋接器，並支援與 PCI 通道或 SR-IOV 纜線介面卡直接連線。 若您計劃使用 PCI 通道或 SR-IOV 建立連結，則不能在 SR-IOV 或 PCI 通道專用的實體連接埠上設定 vSwitch。若要與主機及其他在此網路上的虛擬電腦通訊，則 VM-Series 防火牆必須有實體連接埠的獨佔存取權，且與在該介面上的虛擬功能 (VF) 相關聯。 · 在 Linux 橋接器與 OVS 上支援 e1000 與 Virtio 驅動程式；不支援預設的驅動程式 rtl8139。

©2023 Palo Alto Networks, Inc.

需求	說明

	• 為了支援 PCI 通道/SR-IOV，已針對下列網路卡測試 VM-Series 防火牆：
	  • 採用 Intel 82576 的 1G NIC：所有受支援 Linux 發行版上的 SR-IOV 支援；PCI 通道支援。
	  • 採用 Intel 82599 的 10G NIC：所有受支援 Linux 發行版上的 SR-IOV 支援；PCI 通道支援。
	  • Intel X710 10G NIC：所有支援的 Linux 發行版上的 SR-IOV 支援；PCI 通道支援。
	  • Intel X722 10G NIC：所有支援的 Linux 發行版上的 SR-IOV 支援；PCI 通道支援。
	  • 採用 Broadcom 57112 與 578xx 的 10G NIC：所有支援的 Linux 發行版上的 SR-IOV 支援；不支援 PCI 通道。
	  • Mellanox ConnectX5 10G/25G/50G/100G NIC：所有受支援 Linux 發行版上的 SR-IOV 支援。
	  • 請參閱相容性矩陣中的 PacketMMAP 驅動程式版本
	
	指派給 *VM-Series* 防火牆且支援 *SR-IOV* 的介面必須設定成 *Layer 3* 介面或 *HA* 介面。

在網路上連接 VM-Series 的選項



- 透過 Linux 橋接器或 OVS，資料流量可使用軟體橋接器連接同一部主機上的來賓。對於外部連線，資料流量會使用連接橋接器的實體介面。

©2023 Palo Alto Networks, Inc.

- 透過 PCI 通道，資料流量會在來賓及其所連接的實體介面之間直接傳遞。當介面與來賓連接時，便無法供主機或主機上其他來賓使用。
- 透過 SR-IOV，資料流量會在來賓及其所連接的虛擬功能之間直接傳遞。

KVM 上 VM-Series 的先決條件

在 Linux 伺服器安裝 VM-Series 防火牆前，請先參閱以下幾節：

- 準備 Linux 伺服器
- 準備部署 VM-Series 防火牆

準備 **Linux** 伺服器

在 KVM 上安裝 VM-Series 防火牆之前，請確認您有正常運作的 Linux 環境，且網路基礎結構支援您所選擇的部署需要的連線。

- 驗證 Linux 支援
- 驗證網路基礎結構
- 安裝 Mellanox 軟體工具
- 在 KVM 的 VM-Series 防火牆上為 Mellanox CX5 NIC 啟用虛擬功能
- 確認主機設定

驗證 **Linux** 支援

確認您有正確的環境可支援安裝。

- 檢查 Linux 發行版。如需支援的版本清單，請參閱相容性矩陣中的 KVM 專用 VM-Series。
- 確認您已安裝與設定建立和管理虛擬機器所需的 KVM 工具與套件，例如 Libvirt。
- 如果您想要使用 SCSI 磁碟控制器存取 VM-Series 防火牆用來儲存資料的磁碟，則必須使用 virsh 將 virtio-scsi 控制器連接到 VM-Series 防火牆。接著您可以編輯 VM-Series 防火牆的 XML 範本以允許使用 virtio-scsi 控制器。相關指示請參閱啟用 SCSI 控制器。

  Ubuntu 12.04 上的 *KVM* 不支援 *virtio-scsi* 控制器。

驗證網路基礎結構

確認您已設定網路基礎結構，能夠在來賓與 VM-Series 防火牆之間引導流量，並確保您可以連線至外部伺服器或網際網路。VM-Series 防火牆可使用 Linux 橋接器、Open vSwitch、PCI 通道或支援 SR-IOV 的網路卡連線。

- 針對您打算使用的每個介面，確定其連結狀態皆為啟動—有時候您必須手動啟動介面。
- 如果使用 Linux 橋接器或 OVS，請確認您已設定傳送/接收進/出防火牆所需的橋接器。如果未使用，請先建立橋接器並確認其為啟動，再開始安裝防火牆。
- 如果使用 SR-IOV 或 PCI 通道，請確認所有介面的 PCI ID。若要檢視清單，請使用下列命令：

  Virsh nodedev-list –tree

  請參閱 驗證 VM-Series 防火牆上網路介面順序的 PCI-ID。

©2023 Palo Alto Networks, Inc.

- 如果使用 SR-IOV 或 PCI 通道，請在 BIOS 中確認虛擬延伸模組 (VT-d/IOMMU) 已啟用。例如，若要啟用 IOMMU，`/etc/grub.conf` 中必須定義 `intel_iommu=on`。請參閱系統廠商所提供文件中的指示。
- 如果使用 PCI 通道，確定 VM-Series 防火牆具有您計劃連接之介面的獨佔存取權。

  若要允許獨佔存取，您必須手動將介面從 Linux 伺服器分離。

  `Virsh nodedev-detach <pci id of interface>`

  例如：

  `Virsh nodedev-detach pci_0000_07_10_0`

  在某些情況下，您可能需要編輯 `/etc/libvirt/qemu.conf`，將 `relaxed_acs_check = 1` 取消註解。
- 如果使用的是 SR-IOV，請確認您計劃在網路卡上使用者的每個連接埠其虛擬功能已啟用。透過 SR-IOV，單一 Ethernet 連接埠（實體功能）可分割成多個虛擬功能。來賓可對應至一或多個虛擬功能。

  如下所示啟用虛擬功能：

  1. 在此位置建立新檔案：`/etc/modprobe.d/`
  2. 使用 vi 來編輯檔案，將功能變成持久啟用：

     `vim /etc/modprobe.d/igb.conf`
  3. 啟用所需的虛擬功能數目：

     `options igb max_vfs=4`

     在上述範例中，當您儲存變更並重新啟動 Linux 伺服器之後，每個介面（或實體功能）將有 4 個虛擬功能。

  有關支援的虛擬功能實際數目的詳細資訊，以及如何啟用虛擬功能的指示，請參閱網路廠商提供的文件。

安裝 **Mellanox** 軟體工具

如果您使用 Mellanox CX5 卡，請在主機上安裝 Mellanox 軟體工具。安裝之前，請驗證 Linux 支援和您的網路基礎結構。

STEP 1 | 在主機上，根據您的作業系統版本，從下列連結下載 Mellanox OpenFabric Enterprise Distribution for Linux (MLNX_OFED) 的套件：

https://www.mellanox.com/products/infiniband-drivers/linux/mlnx_ofed

STEP 2 | 執行安裝命令：

`mlnxofedinstall`

如果您已安裝所有必備套件，則上述命令會安裝所有 MLNX_OFED 套件。繼續步驟 3。

如果您的環境沒有所需的套件，安裝程式會列出您必須安裝的所有套件。安裝套件之後，請重新執行安裝命令，並繼續步驟 3。

STEP 3 | 重新啟動主機。

©2023 Palo Alto Networks, Inc.

STEP 4 | 檢查 Mellanox 軟體工具的狀態。

```
#mst statusMST 模組: ------------------------------------------
 ---------- MST PCI 模組未載入 MST PCI 配置模組載入 MST 裝置:
 ------------- ------------------------------------------------
 -- /dev/mst/mt4121_pciconf0 - PCI 配置循環存取。
 domain:bus:dev.fn=0000:3b:00.0 addr.reg=88 data.reg=92 晶片版本
為: 00
```

STEP 5 | 確保 PCI 清單上的 Mellanox 已更新:

```
#lspci | grep Mellanox3b:00.0 乙太網路控制器: Mellanox Technologies
 MT28800 系列 [ConnectX-5 Ex] 3b:00.1 乙太網路控制器: Mellanox
 Technologies MT28800 系列 [ConnectX-5 Ex]
```

在 KVM 的 VM-Series 防火牆上為 Mellanox CX5 NIC 啟用虛擬功能

在 Mellanox Cx5 NIC 上啟用虛擬功能之前，安裝 Mellanox 軟體工具。

STEP 1 | 確保 Mellanox Software Tools (mst) 已啟動。

STEP 2 | 啟用所需的虛擬功能數目。例如:

```
mlxconfig -d /dev/mst/mt4121_pciconf0 set SRIOV_EN=1 NUM_OF_VFS=4
```

在您儲存變更並重新啟動 Linux 伺服器後，上述範例中的每個介面（或實體功能）將有 4 個虛擬功能。有關支援的虛擬功能實際數目的詳細資訊，以及如何啟用虛擬功能的指示，請參閱網路廠商提供的文件。

在 *Mellanox Cx5 NIC* 上首次啟用虛擬功能時，您可能會看到下列錯誤訊息:

```
[ 1429.841162] mlx5_core 0000:3b:00.1:
 mlx5_port_module_event:1025:(pid 0):連接埠模組事件[錯誤]:
模組 1，電線錯誤，由於 PCIe 插槽上的電源不足/未通告的電源，一個
或多個網路連接埠已停電。請參閱卡片的使用者手冊了解電源規格，或聯繫
 Mellanox 支援
```

若要解決問題，請在 *Linux* 伺服器上輸入下列命令序列:

```
# mlxconfig -d <dev> set ADVANCED_POWER_SETTINGS=1 #
 mlxconfig -d <dev> set DISABLE_SLOT_POWER_LIMITER=1 #
 reboot
```


©2023 Palo Alto Networks, Inc.

STEP 3 | 檢查虛擬功能的狀態。

```
# cat /sys/class/net/enp59s0f1/device/sriov_numvfs
```

（選用）如果虛擬功能未正確設定（狀態為 0 或空白），請執行下列命令：

```
# echo 4 > /sys/class/net/enp59s0f1/device/sriov_numvfs
```

STEP 4 | 列出 PCI 裝置，準確比對 Mellanox 的各個實體功能上載入的虛擬功能數目：

```
#lspci | grep Mellanox3b:00.0 乙太網路控制器: Mellanox Technologies
 MT28800 系列 [ConnectX-5 Ex] 3b:00.1 乙太網路控制器: Mellanox
 Technologies MT28800 系列 [ConnectX-5 Ex] 3b:00.2 乙太網路控
制器: Mellanox Technologies MT28800 系列 [ConnectX-5 Ex 虛擬功
能] 3b:00.3 乙太網路控制器: Mellanox Technologies MT28800 系列
 [ConnectX-5 Ex 虛擬功能] 3b:00.4 乙太網路控制器: Mellanox Technologies
 MT28800 系列 [ConnectX-5 Ex 虛擬功能] 3b:00.5 乙太網路控制器: Mellanox
 Technologies MT28800 系列 [ConnectX-5 Ex 虛擬功能] 3b:00.6 乙太
網路控制器: Mellanox Technologies MT28800 系列 [ConnectX-5 Ex 虛
擬功能] 3b:00.7 乙太網路控制器: Mellanox Technologies MT28800 系列
 [ConnectX-5 Ex 虛擬功能] 3b:01.0 乙太網路控制器: Mellanox Technologies
 MT28800 系列 [ConnectX-5 Ex 虛擬功能] 3b:01.1 乙太網路控制器: Mellanox
 Technologies MT28800 系列 [ConnectX-5 Ex 虛擬功能]
```

確認主機設定

設定主機以發揮最大的 VM-Series 效能。如需有關設定以下每個選項的資訊，請參閱 KVM 專用 VM-Series 的效能調整。

- **Enable DPDK**（啟用 **DPDK**）。DPDK 可讓主機避開 Linux 核心來加速處理封包。反之，與 NIC 互動是透過驅動程式和 DPDK 程式庫。需要 Open vSwitch，DPDK 與 VM-Series 防火牆才能一起使用。
- **Enable SR-IOV**（啟用 **SR-IOV**）。Single root I/O virtualization（單一根 I/O 虛擬化 - SR-IOV）可讓單一根埠下的單一 PCIe 實體裝置，以多個單獨實體裝置呈現給 Hypervisor 或來賓。
- **Enable multi-queue support for NICs**（啟用 **NIC** 的多佇列支援）。多重佇列 virtio-net 可讓網路效能隨著 vCPU 數目而調整，還能建立多個 TX 和 RX 佇列來平行處理封包。
- 將 **CPU** 資源隔離在 **NUMA** 節點中。您可以將來賓 VM 的 CPU 資源隔離到單一非流一記憶體存取 (NUMA) 節點，以改善 KVM 上 VM-Series 的效能。

準備部署 VM-Series 防火牆

- 購買 VM-Series 型號並在 Palo Alto Networks 客戶支援網站上註冊驗證碼。請參閱建立支援帳戶和註冊 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

- 取得 qcow2 映像並儲存在 Linux 伺服器上。最佳作法是將該映像複製到下列資料夾：/var/lib/libvirt/qemu/images。

  如果您計畫為 VM-Series 防火牆部署多個實例，請為映像製作足量複本。VM-Series 防火牆的各實例均需使用 .qcow2 映像來維護連結，由於該映像正是用於部署防火牆的映像，因此為了防止發生任何資料損毀的問題，請確定每個映像都是獨立的，並由防火牆的單一實例使用。

©2023 Palo Alto Networks, Inc.

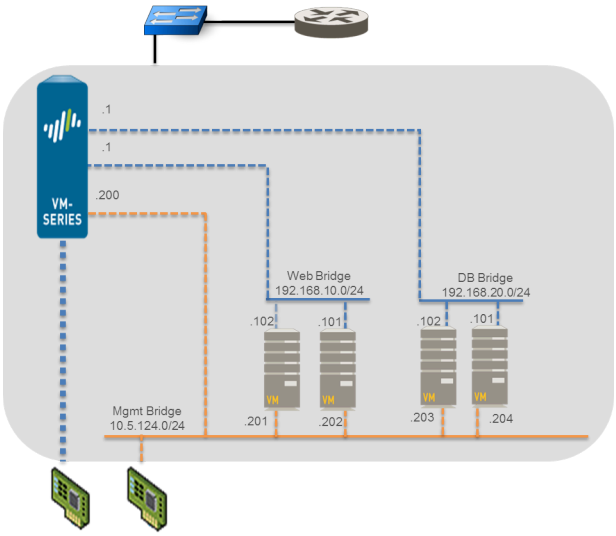
KVM 上支援的部署

您可以在 Linux 主機上部署各 Linux 主機（單一租用戶）其 VM-Series 防火牆的單一實例，或 VM-Series 防火牆的多個實例。可使用 Virtual Wire、iLayer 2 或 Layer 3 介面部署 VM-Series 防火牆。如果您計劃在 VM-Series 防火牆上使用支援 SR-IOV 的介面，您只能將該介面設定為 Layer 3 介面。

- 保護單一主機上的流量
- 保護 Linux 主機之間的流量

保護單一主機上的流量

若要保護 Linux 伺服器上來賓之間的東西向流量，則可使用 Virtual Wire、Layer 2 或 Layer 3 介面部署 VM-Series 防火牆。下圖顯示含 Layer 3 介面的防火牆，其中伺服器上的防火牆與其他來賓之間是使用 Linux 橋接器連接的。此部署透過防火牆路由 Web 伺服器與資料庫伺服器之間的所有流量；只在資料庫伺服器之間的流量及只在 Web 伺服器之間的流量由橋接器處理，不會透過防火牆路由。

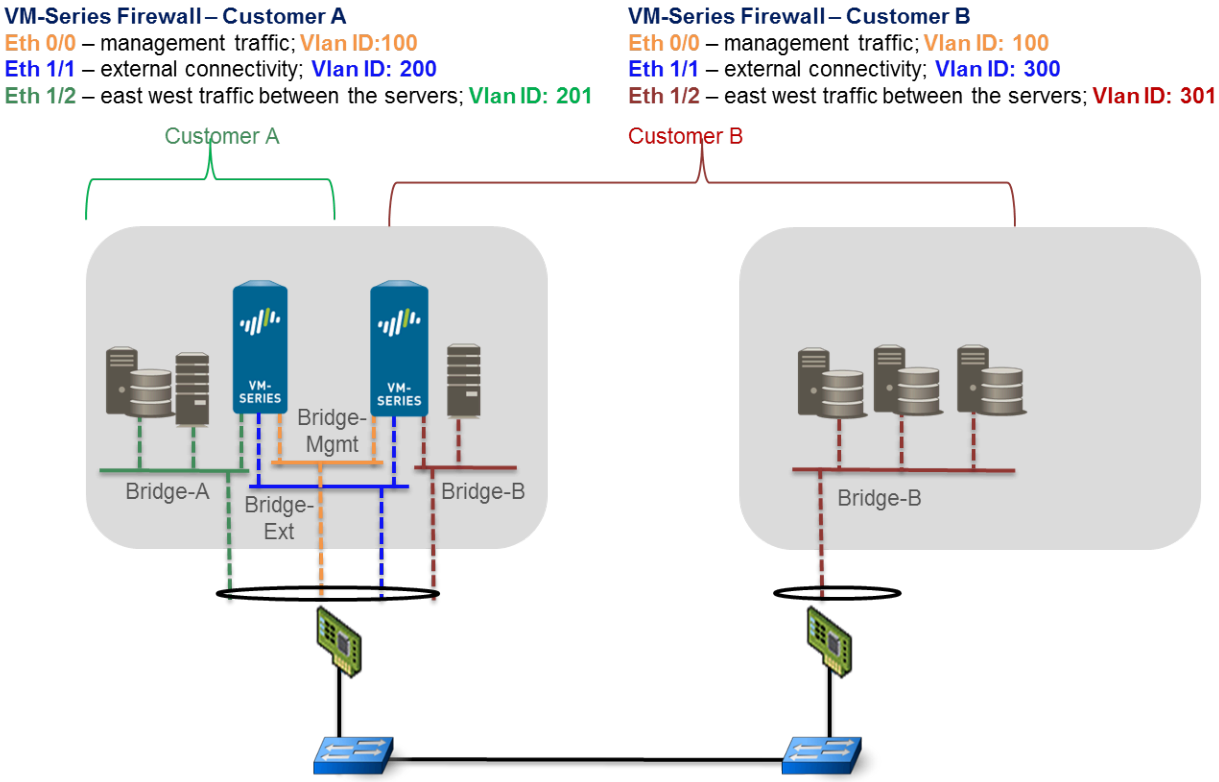


保護 Linux 主機之間的流量

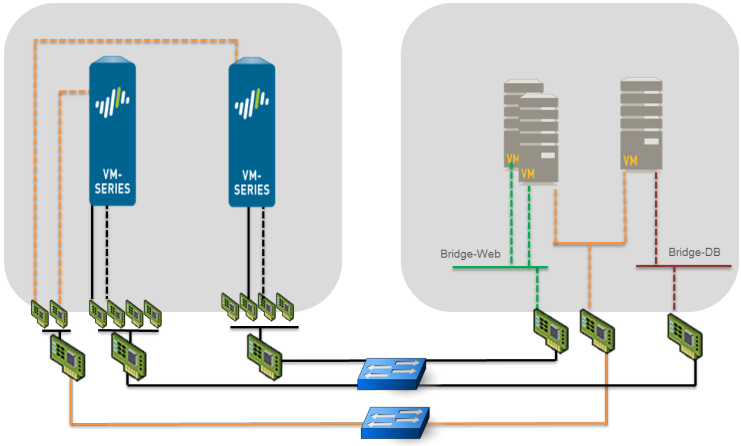
若要保護工作負載，可在 Linux 主機上部署 VM-Series 防火牆的多個實例。例如，如果您要隔離不同部門或客戶的流量，您可以使用 VLAN 標籤

邏輯隔離網路流量，並將流量路由至適當的 VM-Series 防火牆。在下列範例中，某個 Linux 主機為兩名客戶代管 VM-Series 防火牆：客戶 A 與客戶 B，而客戶 B 的流量遍佈在兩個伺服器之間。為了隔離流量並導向至為每個客戶設定的 VM-Series 防火牆，因此使用 VLAN。

©2023 Palo Alto Networks, Inc.



在此部署的另一個變化中，有一對 VM-Series 防火牆部署在高可用性設定中。下圖中的 VM-Series 防火牆部署在 Linux 伺服器上，伺服器使用支援 SR-IOV 的介面卡。透過 SR-IOV，單一 Ethernet 連接埠（實體功能）可分割成多個虛擬功能。每個連接至 VM-Series 防火牆的虛擬功能皆設定為 Layer 3 介面。HA 配對中的主動端點會保護從部署在不同 Linux 伺服器的來賓路由至該端點的流量。



©2023 Palo Alto Networks, Inc.

在 KVM 上安裝 VM-Series 防火牆

用來管理 KVM 的 libvirt API 包含大量的工具，可讓您建立與管理虛擬機器。若要將 VM-Series 防火牆安裝在 KVM 上，您可以使用下列任何方法。

- virt-manager—使用 virt-manager 虛擬機器管理員來部署 VM-Series。virt-manager 提供一個方便的精靈協助您完成安裝程序。
- virsh—使用 KVM 命令行來部署 VM-Series。建立可定義虛擬機器實例的 XML 檔案，以及可定義防火牆初始組態設定的啟動 XML 檔案。然後將 ISO 映像裝載為 CD-ROM，以安裝防火牆。
- virt-install—使用 KVM 命令行部署 VM-Series 防火牆的另一個選項。使用此選項，可建立並安裝 VM-Series 防火牆的定義。

本文件提供使用 virt-manager 和 virsh 在 KVM 上安裝 VM-Series 防火牆的步驟。

- 使用 Virt-Manager 安裝 VM-Series 防火牆
- 使用 ISO 安裝 VM-Series 防火牆
- 使用 VM-Series CLI 在 KVM 上交換管理介面
- 啟用 SCSI 控制器
- 驗證 VM-Series 防火牆上網路介面順序的 PCI-ID

使用 Virt-Manager 安裝 VM-Series 防火牆

下列程序使用 virt-manager 將 VM-Series 防火牆安裝在於 RHEL 上執行 KVM 的伺服器。

- 在 KVM 主機上佈建 VM-Series 防火牆
- 在 KVM 上執行 VM-Series 防火牆的初始組態

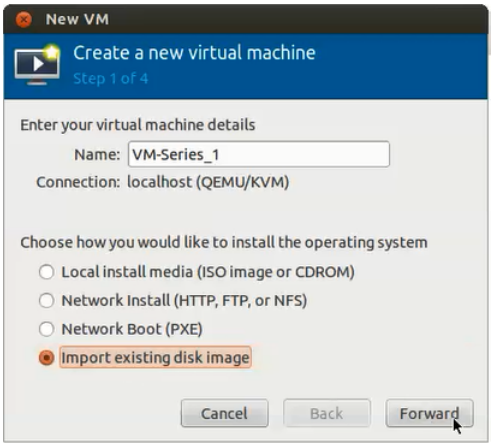
在 **KVM** 主機上佈建 **VM-Series** 防火牆

依照下列指示來佈建 VM-Series 防火牆的 KVM 主機。

©2023 Palo Alto Networks, Inc.

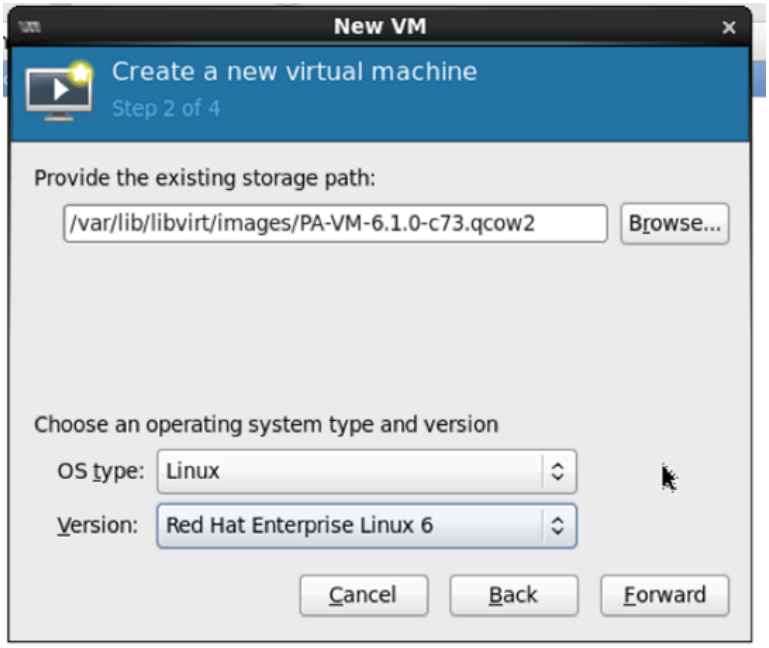
STEP 1 | 建立新的虛擬機器，並將 KVM 專用 VM-Series 防火牆映像新增至 virt-mgr。

1. 在 Virt-manager 上，選取 **Create a new virtual machine**（建立新虛擬機器）。
2. 為 VM-Series 防火牆新增描述性的 **Name**（名稱）。



3. 選取 **Import existing disk image**（匯入現有磁碟映像），然後設定 **OS Type**（作業系統類型）：Linux 與 **Version**（版本）：Red Hat Enterprise Linux 6。

   如果您願意，可以將 *OS Type*（作業系統類型）與 *Version*（版本）保留為 *Generic*（一般）。

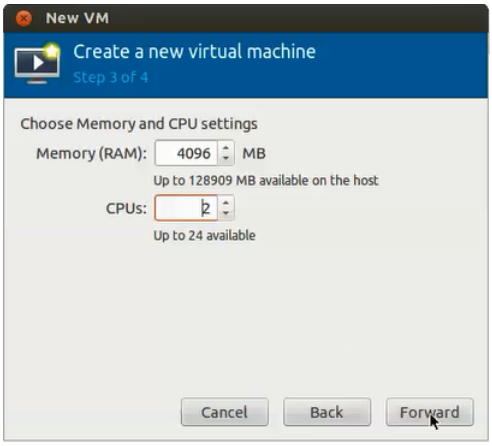


4. 若要為資料介面新增網路介面卡：

©2023 Palo Alto Networks, Inc.

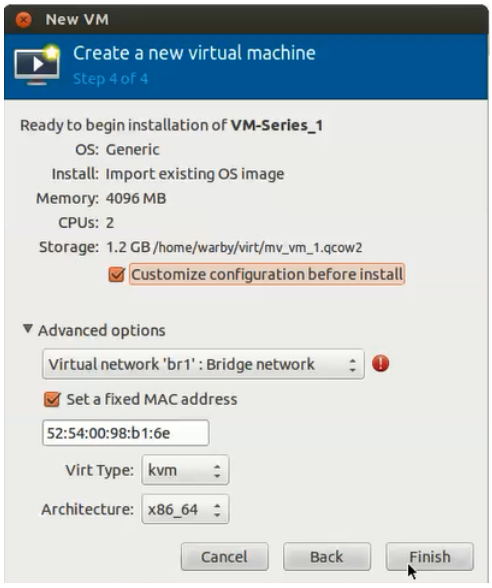
STEP 2 | 設定記憶體和 CPU 設定。

1. 根據您的 VM-Series 型號的 VM-Series 系統需求，將 **Memory**（記憶體）設為最少記憶體。
2. 根據您 VM-Series 型號的 VM-Series 系統需求，將 **CPU** 設定為最小 CPU。



STEP 3 | 啟用組態自訂，並選取管理介面橋接器。

1. 選取 **Customize configuration before install**（安裝前自訂組態）。
2. 在 Advanced（進階）選項下，為管理介面選取橋接器，然後接受預設設定。



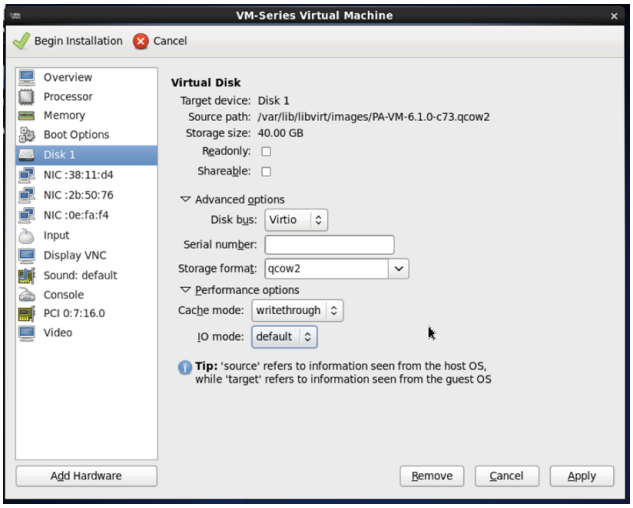
©2023 Palo Alto Networks, Inc.

STEP 4 | 設定虛擬磁碟的設定。

1. 選取 **Disk**（磁碟），展開 Advanced（進階）選項，然後選取 **Storage format**（儲存格式）—qcow2；**Disk Bus**（磁碟匯流排）—Virtio 或 IDE（視您的設定而定）。

   如果您要使用 *SCSI* 磁碟匯流排，請參閱啟用 SCSI 控制器。

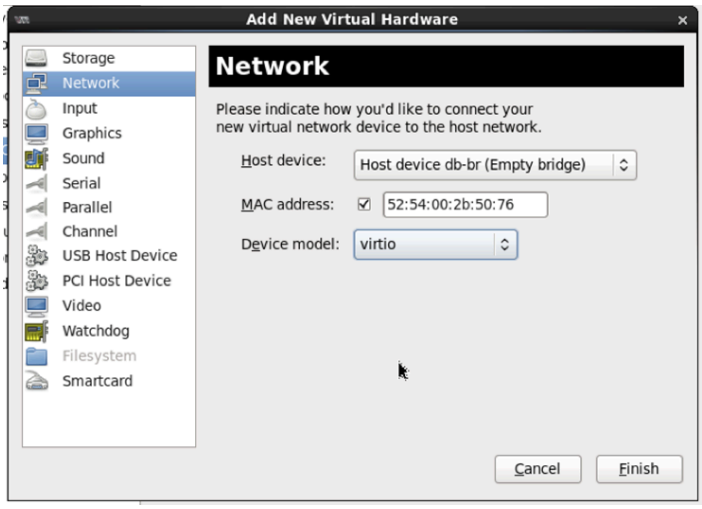
2. 展開 Performance（效能）選項，然後將 **Cache mode**（快取模式）設為 **writethrough**。此設定可改善 VM-Series 防火牆的安裝時間與執行速度。



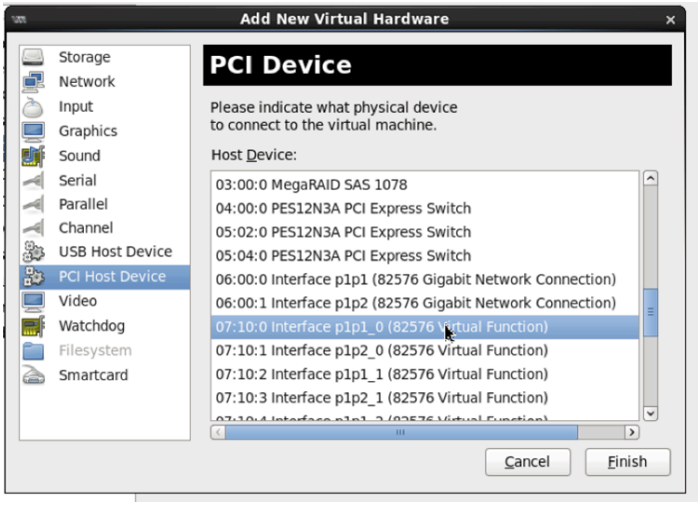
 ©2023 Palo Alto Networks, Inc.

STEP 5 | 設定網路介面卡。

1. 如果您使用的是如 Linux 橋接器或 Open vSwitch 等軟體橋接器，請選取 **Add Hardware**（新增硬體）> **Network**（網路）。
2. 對於 **Host Device**（主機設備）輸入橋接器名稱，或從下拉式清單中選取橋接器。
3. 若要指定驅動程式，請將 **Device Model**（設備模型）設為 e-1000 或 virtio。這些是唯一支援的虛擬介面類型。



4. 為 PCI-通道或支援 SR-IOV 的裝置選取 **Add Hardware**（新增硬體）> **PCI Host Device**（**PCI** 主機裝置）。



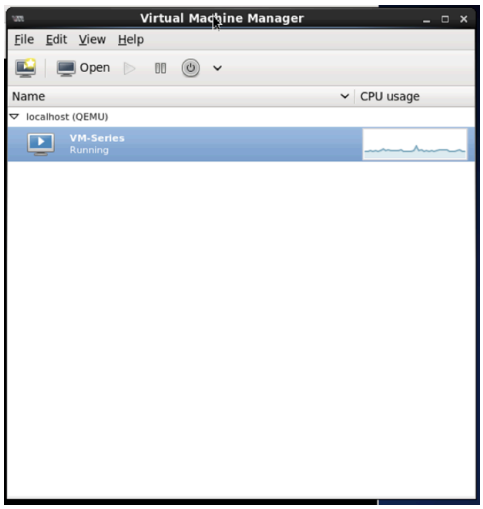
5. 在 **Host Device**（主機設備）清單中，選取卡片或虛擬功能上的介面。
6. 按一下 **Apply**（套用）或 **Finish**（完成）。

©2023 Palo Alto Networks, Inc.

STEP 6 | 按一下 **Begin Installation**（開始安裝） 

。等候 5-7 分鐘讓安裝完成。

依預設，會為 *VM-Series* 防火牆建立 *XML* 範本並儲存在 *etc/libvirt/qemu* 中。



STEP 7 | （選用）啟動 VM-Series 防火牆

如果您使用啟動程序在 KVM 上執行 VM-Series 防火牆的組態，請參閱在 KVM 上啟動 VM-Series 防火牆。如需啟動程序的詳細資訊，請參閱啟動 VM-Series 防火牆。

STEP 8 | 設定管理介面的網路存取設定。

1. 在主控台上開啟連線。
2. 使用以下的使用者名稱/密碼登入防火牆：admin/admin。
3. 使用下列命令，進入組態模式：

```
configure
```

4. 使用下列命令，設定管理介面：

1. ```
   set deviceconfig system type static
   ```

2. ```
   set deviceconfig system ip-address <Firewall-IP>
    netmask <netmask> default-gateway <gateway-IP> dns-setting
    servers primary <DNS-IP>
   ```

   其中，*<Firewall-IP>* 是要指定給管理介面的 IP 位址；*<netmask>* 是子網路遮罩；*<gateway-IP>* 是網路閘道的 IP 位址；*<DNS-IP>* 則是 DNS 伺服器的 IP 位址。

3. 提交

©2023 Palo Alto Networks, Inc.

STEP 9 | 確認主機上的哪些連接埠會對應到 VM-Series 防火牆上的介面。若要確認 Linux 主機上的介面順序，請參閱驗證 VM-Series 防火牆上網路介面順序的 PCI-ID。

若要確定流量是由正確的介面處理的，請使用下列命令識別主機上的哪些連接埠對應至 VM-Series 防火牆上的連接埠。

```
admin@PAN-VM> debug show vm-series interfaces all Phoenix_interface
 Base-OS_port Base-OS_MAC PCI-ID mgt                              eth0
 52:54:00:d7:91:52 0000:00:03.0 Ethernet1/1 eth1 52:54:00:fe:8c:80
 0000:00:06.0 Ethernet1/2 eth2 0e:c6:6b:b4:72:06 0000:00:07.0
 Ethernet1/3 eth3 06:1b:a5:7e:a5:78 0000:00:08.0 Ethernet1/4 eth4
 26:a9:26:54:27:a1 0000:00:09.0 Ethernet1/5 eth5 52:54:00:f4:62:13
 0000:00:10.2
```

STEP 10 | 存取 VM-Series 防火牆的 Web 介面並設定介面，然後定義安全性規則與 NAT 規則，以安全地啟用您想要保護的應用程式。

請參閱《PAN-OS 管理員指南》。

在 KVM 上執行 VM-Series 防火牆的初始組態

在 KVM 伺服器上使用虛擬設備主控台，以設定 VM-Series 防火牆的網路存取。依預設，VM-Series 防火牆使用 DHCP 取得管理介面的 IP 位址。不過，您可以指派靜態 IP 位址。完成初始組態之後，請存取網頁介面來完成進一步的組態設定工作。如果您使用 Panorama 執行中央管理，請參閱Panorama 管理員指南以取得使用 Panorama 管理裝置的詳細資訊。

如果要使用啟動載入在 KVM 上執行 VM-Series 防火牆的設定，請參閱在 KVM 上啟動載入 VM-Series 防火牆。

如需啟動程序的一般資訊，請參閱啟動 VM-Series 防火牆。

STEP 1 | 從網路管理員收集必要資訊。

- MGT 連接埠的 IP 位址
- 網路遮罩
- 預設閘道
- DNS 伺服器 IP 位址

STEP 2 | 存取 VM-Series 防火牆的主控台。

1. 在 KVM 伺服器上針對 VM-Series 防火牆選取 **Console**（主控台）頁籤，或在 VM-Series 防火牆上按一下滑鼠右鍵並選取 **Open Console**（開啟主控台）。
2. 按下 Enter 以存取登入畫面。
3. 輸入預設的使用者名稱/密碼 (admin/admin) 進行登入。
4. 輸入 **configure** 切換至組態模式。

©2023 Palo Alto Networks, Inc.

STEP 3 | 設定管理介面的網路存取設定。

輸入下列命令：

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> 網路遮罩 <netmask>
default-gateway <gateway-IP> dns-setting servers primary <DNS-IP>
```

STEP 4 | 提交您的變更並結束組態模式。

輸入 **commit** 。

輸入 **exit**。

使用 ISO 安裝 VM-Series 防火牆

手動建立 VM-Series 防火牆的 XML 定義，然後使用 virsh 將定義匯入為 ISO。Virsh 是最強大的工具，可完整管理虛擬機器。

- 使用 ISO 檔案部署 VM-Series 防火牆
- VM-Series 防火牆的範例 XML 檔

使用 ISO 檔案部署 VM-Series 防火牆

如果您要在開機時將指令碼傳遞到 VM-Series 防火牆，您可以插入含 ISO 檔的 CD-ROM。ISO 檔案可讓您定義啟動程序 XML 檔案，其中包括防火牆管理連接埠的初始組態參數。第一次開機時 VM-Series 防火牆會檢查 **bootstrap-networkconfig.xml** 檔案，並使用在該檔案上定義的值。

如果在剖析啟動程序檔案時發生單一錯誤，*VM-Series* 防火牆會拒絕此檔案中所有的組態，並以預設值開機。

STEP 1 | 建立 XML 檔案，並將它定義為虛擬機器實例。

如需範例檔案，請參閱VM-Series 防火牆的範例 XML 檔案。

在此範例中，VM-Series 防火牆名為 PAN_Firewall_DC1。

例如：

```
user-PowerEdge-R510:~/kvm_script$ sudo vi /etc/libvirt/qemu/
PAN_Firewall_DC1.xml user-PowerEdge-R510:~/kvm_script$ sudo
 virsh define/etc/libvirt/qemu/PAN_Firewall_DC1.xml Domain
 PAN_Firewall_DC1_bootstp defined from /etc/libvirt/qemu/
PAN_Firewall_DC1.xml user-PowerEdge-R510:~/kvm_script$
 sudo virsh -q attach-interface PAN_Firewall_DC1_bootstp
 bridge br1 --model=virtio --persistent user-PowerEdge-
R510:~/kvm_script$ virsh list --all Id Name State
 ---------------------------------------------- -
 PAN_Firewall_DC1_bootstp shut off
```


©2023 Palo Alto Networks, Inc.

STEP 2 | 建立啟動程序 XML 檔案。

您可以在此檔案中定義初始組態參數，並將它命名為 bootstrap-networkconfig。

如果您不想要包含參數，例如 *panorama-server-secondary*。將整行從檔案中刪除。如果您將 *IP* 位址欄位保留空白，將無法成功剖析此檔案。

使用下列範例作為 bootstrap-networkconfig 檔案的範本。bootstrap-networkconfig 檔案僅包含下列參數：

```
<vm-initcfg> <hostname>VM_ABC_Company</hostname> <ip-
address>10.5.132.162</ip-address> <netmask>255.255.254.0</
netmask> <default-gateway>10.5.132.1</default-gateway> <dns-
primary>10.44.2.10</dns-primary> <dns-secondary>8.8.8.8</dns-
secondary> <panorama-server-primary>10.5.133.4</panorama-server-
primary> <panorama-server-secondary>10.5.133.5</panorama-server-
secondary> </vm-initcfg>
```

STEP 3 | 建立 ISO 檔。在此範例中，我們使用 mkisofs。

將 *ISO* 檔案儲存在映像目錄 *(/var/lib/libvirt/image)* 或 *qemu* 目錄 *(/etc/libvirt/qemu)* 中，以確定防火牆具有 *ISO* 檔案的讀取存取權。

例如：

```
# mkisofs -J -R -v -V "Bootstrap" -A "Bootstrap" -ldots -l -
allow-lowercase -allow-multidot -o <iso-filename> bootstrap-
networkconfig.xml
```

STEP 4 | 將 ISO 檔附加至 CD-ROM。

例如：

```
# virsh -q attach-disk <vm-name> <iso-filename> sdc --type cdrom --
mode readonly  –persistent\
```

VM-Series 防火牆的範例 XML 檔

```
<?xml version="1.0"?> <domain type="kvm"> <name>PAN_Firewall_DC1</
name> <memory>4194304</memory> <currentMemory>4194304</currentMemory>
 <vcpu placement="static">2</vcpu> <os> <type arch="x86_64">hvm</
type> <boot dev="hd"/> </os> <features> <acpi/> <apic/> <pae/> </
features> <clock offset="utc"/> <on_poweroff>destroy</on_poweroff>
 <on_reboot>restart</on_reboot> <on_crash>restart</on_crash>
 <devices> <emulator>/usr/libexec/qemu-kvm</emulator> <disk
 type="file" device="disk"> <driver type="qcow2" name="qemu"/>
 <source file="/var/lib/libvirt/images/panos-kvm.qcow2"/> <target
 dev="vda" bus="virtio"/> </disk> <controller type="usb" index="0"/
> <controller type="ide" index="0"/> <controller type="scsi"
 index="0"/> <serial type="pty"> <source path="/dev/pts/1"/> <target
```


©2023 Palo Alto Networks, Inc.

```
 port="0"/> <alias name="serial0"/> </serial> <console type="pty"
 tty="/dev/pts/1"> <source path="/dev/pts/1"/> <target type="serial"
 port="0"/> <alias name="serial0"/> </console> <input type="mouse"
 bus="ps2"/> <graphics type="vnc" port="5900" autoport="yes"/> </
devices> </domain>
```

若要修改指派給 *VM-Series* 防火牆上的 *vCPU* 數目，請在此行 *XML* 檔案範例中將值從 ***2*** 變更為 ***4*** 或 ***8*** *vCPU*：

```
<vcpu placement="static">2</vcpu>
```

使用 VM-Series CLI 在 KVM 上交換管理介面

根據預設，VM-Series 防火牆會將第一個介面 (eth0) 指派為管理介面。不過，在某些部署中，第一個介面必須預先對應至公共 IP 位址。因此，管理介面必須指派給不同的介面。將公共 IP 位址指派給管理介面會有安全性風險。

或者，您可以在啟動載入時，在 init-cfg.txt 檔案元件 中啟用管理介面交換。

STEP 1 | 登入 VM-Series 防火牆 CLI 並輸入下列命令：

```
set system setting mgmt-interface-swap enable yes
```

STEP 2 | 確認您要交換介面並將 eth1 資料平面介面用作管理介面。

STEP 3 | 重新啟動防火牆以使交換生效。使用下列命令：

```
request restart system
```

STEP 4 | 確認介面已交換。使用下列命令：

```
debug show vm-series interfaces all Phoenix_interface   Base-
OS_port   Base-OS_MAC        PCI-ID         Driver mgt(interface-
swap) eth0   0e:53:96:91:ef:29   0000:00:04.0   ixgbevf Ethernet1/1
           eth1    0e:4d:84:5f:7f:4d       0000:00:03.0   ixgbevf
```

啟用 SCSI 控制器

如果您想要 VM-Series 防火牆使用 SCSI 類型的磁碟匯流排，以存取虛擬磁碟，請使用下列指示將 virtio scsi 控制器連接至防火牆，然後啟用 virtio-scsi 控制器的使用。

Ubuntu 12.04 上的 *KVM* 不支援 *virtio-scsi* 控制器；*virtio-scsi* 控制器只適用於在 *RHEL* 或 *CentOS* 上執行的 *VM* 系列防火牆。

此程序需要 *virsh*，因為 *Virt* 管理員不支援 *virtio-scsi* 控制器。

STEP 1 | 為 SCSI 控制器建立 XML 檔。在此範例中檔案名為 virt-scsi.xml。

©2023 Palo Alto Networks, Inc.

```
[root@localhost~]# cat /root/virt-scsi.xml <controller type='scsi'
 index='0' model='virtio-scsi'> <address type='pci' domain='0x0000'
 bus='0x00' slot='0x0b'function='0x0'/> </controller>
```

確定用於 *virtio-scsi* 控制器的插槽與另一個設備的插槽不衝突。

STEP 2 | 將此控制器與 VM-Series 防火牆的 XML 範本建立關聯。

```
[root@localhost~]# virsh attach-device --config <VM-Series_name> /
root/virt-scsi.xml 裝置附加成功
```

STEP 3 | 允許防火牆使用 SCSI 控制器。

```
[root@localhost~]# virsh attach-disk <VM-Series_name>/var/
lib/libvirt/images/PA-VM-6.1.0-c73.qcow2 sda --cache none --
persistent 磁碟附加成功
```

STEP 4 | 編輯 VM-Series 防火牆的 XML 範本。在 XML 範本中，您必須變更防火牆使用的目標磁碟與磁碟匯流排。

依預設，*XML* 範本儲存在 *etc/libvirt/qemu* 中。

```
<disk type='file' device='disk'> <driver name='qemu' type='qcow2'
 cache='writeback'/> <source file='/var/lib/libvirt/images/PA-
VM-7.0.0-c73.qcow2'/> <target dev='sda' bus='scsi'/> <address
 type='drive' controller='0' bus='0' target='0' unit='0'/> </disk>
```

驗證 VM-Series 防火牆上網路介面順序的 PCI-ID

無論您是使用虛擬介面（Linux/OVS 橋接器）或 PCI 設備（PCI 通道或支援 SR-IOV 的介面卡）與 VM-Series 防火牆連線，VM-Series 防火牆都會將介面視為 PCI 設備。系統會根據 PCI-ID 指派 VM-Series 防火牆上的介面；PCI-ID 是匯流排、設備或插槽，及介面的功能組成的值。介面從最低的 PCI-ID 開始排序，這表示防火牆的管理介面 (eth0) 會指派給 PCI-ID 最低的介面。

假設您將四個介面指派給 VM-Series 防火牆，其中三個是類型為 virtio 與 e1000 的虛擬介面，第四個是 PCI 設備。若要檢視每個介面的 PCI-ID，請在 Linux 主機上輸入 **virsh dumpxml $ domain *<name of the VM-Series firewall>*** 命令，以檢視連接至 VM-Series 防火牆的介面清單。在輸出結果中查看下列網路組態：

```
<interface type='bridge'> <mac address='52:54:00:d7:91:52'/> <source
 bridge='mgmt-br'/> <model type='virtio'/> <address type='pci'
 domain='0x0000' bus='0x00' slot='0x03' function='0x0'/> </interface>
 <interface type='bridge'> <mac address='52:54:00:f4:62:13'/>
 <source bridge='br8'/> <model type='e1000'/> <address type='pci'
 domain='0x0000' bus='0x00' slot='0x10' function='0x0'/> </interface>
```


©2023 Palo Alto Networks, Inc.

```
 <interface type='bridge'> <mac address='52:54:00:fe:8c:80'/>
 <source bridge='br8'/> <model type='e1000'/> <address type='pci'
 domain='0x0000' bus='0x00' slot='0x06' function='0x0'/> </interface>
 <hostdev mode='subsystem' type='pci' managed='yes'> <source>
 <address domain='0x0000' bus='0x08' slot='0x10' function='0x1'/> </
source> <address type='pci' domain='0x0000' bus='0x00' slot='0x07'
 function='0x0'/> </hostdev>
```

在此狀況下，每個介面的 PCI-ID 如下所示：

- 第一個虛擬介面 PCI-ID 是 00:03:00
- 第二個虛擬介面 PCI-ID 是 00:10:00
- 第三個虛擬介面 PCI-ID 是 00:06:00
- 第四個虛擬介面 PCI-ID 是 00:07:00

因此在 VM-Series 防火牆上，系統會指派 PCI-ID 為 00:03:00 的介面作為 eth0（管理介面）、指派 PCI-ID 為 00:06:00 的介面作為 eth1 (ethernet1/1)、PCI-ID 為 00:07:00 的介面作為 eth2 (ethernet1/2)，以及 PCI-ID 為 00:10:00 介面作為 eth3 (ethernet1/3)。

©2023 Palo Alto Networks, Inc.

KVM 專用 VM-Series 的效能調整

KVM 專用 VM-Series 防火牆是高效能裝備，但可能需要調整 Hypervisor，才能達到最佳結果。本節說明一些最佳作法和建議，有助於發揮 VM-Series 防火牆的最佳效能。

依預設，KVM 使用 linux 橋接器來連接 VM 網路。不過，虛擬環境中的最佳效能是透過專用 I/O 介面（PCI 通道或 SR-IOV）實現。如果需要虛擬交換器，請使用最佳效能的虛擬交換器（例如搭配 DPDK 的 Open vSwitch）。

- 在 Ubuntu 16.04.1 LTS 上安裝 KVM 和 Open vSwitch
- 在 KVM 上啟用 Open vSwitch
- 整合 Open vSwitch 與 DPDK
- 在 KVM 上啟用 SR-IOV
- 透過 SR-IOV 啟用 VLAN 存取模式
- 在 KVM 上啟用 NIC 的多佇列支援
- 在 KVM 上的 NUMA 節點中隔離 CPU 資源

在 Ubuntu 16.04.1 LTS 上安裝 KVM 和 Open vSwitch

為了簡單安裝，建議使用 Ubuntu 16.04.1 LTS 作為 KVM Hypervisor 平台。

STEP 1 | 安裝 KVM 和 OVS。

1. 登入 Ubuntu CLI。
2. 執行下列命令：

```
$ sudo apt-get install qemu-kvm libvirt-bin ubuntu-vm-builder
 bridge-utils $ sudo apt-get install openvswitch-switch
```

STEP 2 | 檢查和比較相關套件的版本。

執行下列命令：

```
$ virsh --version 1.3.1 $ libvirtd --version libvirtd (libvirt)
 1.3.1 $ /usr/bin/qemu-system-x86_64 --version QEMU emulator
 version 2.5.0 (Debian 1:2.5+dfsg-5ubuntu10.6), Copyright (c)
 2003-2008 Fabrice Bellard $ ovs-vsctl --version ovs-vsctl (Open
 vSwitch) 2.5.0 Compiled Mar 10 2016 14:16:49 DB Schema 7.12.1
```

在 KVM 上啟用 Open vSwitch

修改來賓 XML 定義網路設定來啟用 OVS。

修改來賓 XML 定義如下。

```
[...] <interface type='bridge'> <mac address='52:54:00:fb:00:01'/>
 <source bridge='ovsbr0'/> <virtualport type='openvswitch'/> <model
```


©2023 Palo Alto Networks, Inc.

```
type='virtio'/> <address type='pci' domain='0x0000' bus='0x00'
slot='0x03' function='0x0'/> </interface> [...]
```

整合 Open vSwitch 與 DPDK

若要整合 Open vSwitch (OVS) 與 DPDK，您必須安裝必要元件，然後設定 OVS。在 KVM 專用 VM-Series 防火牆上，依預設會啟用 DPDK。

- 在 Ubuntu 上安裝 QEMU、DPDK 和 OVS
- 在主機上設定 OVS 和 DPDK
- 編輯 VM-Series 防火牆組態檔案

在 Ubuntu 上安裝 QEMU、DPDK 和 OVS

您必須安裝 QEMU 2.5.0、DPDK 2.2.0 和 OVS 2.5.1，才能在 OVS 上啟用 DPDK。請完成下列程序來安裝元件。

STEP 1 | 登入 KVM 主機 CLI。

STEP 2 | 執行下列命令來安裝 QEMU 2.5.0：

```
apt-get install build-essential gcc pkg-config glib-2.0 libglib2.0-
dev libsdl1.2-dev libaio-dev libcap-dev libattr1-dev libpixman-1-
dev apt-get build-dep qemu apt-get install qemu-kvm libvirt-bin
 wget http://wiki.qemu.org/download/qemu-2.5.0.tar.bz2 tar xjvf
 qemu-2.5.0.tar.bz2 cd qemu-2.5.0 ./configure make make install
```

STEP 3 | 安裝 dpdk-2.2.0。

1. 執行下列命令：

   ```
   wget http://dpdk.org/browse/dpdk/snapshot/dpdk-2.2.0.tar.gz
    tar xzvf dpdk-2.2.0.tar.gz cd dpdk-2.2.0 vi config/
   common_linuxapp
   ```

2. 將 `CONFIG_RTE_APP_TEST=y` 變更為 **`CONFIG_RTE_APP_TEST=n`**
3. 將 `CONFIG_RTE_BUILD_COMBINE_LIBS=n` 變更為 **`CONFIG_RTE_BUILD_COMBINE_LIBS=y`**
4. 執行下列命令：

   ```
   vi GNUmakefile
   ```

5. 將 `ROOTDIRS-y := lib drivers app` 變更為 **`ROOTDIRS-y := lib drivers`**
6. 執行下列命令：

   ```
   make install T=x86_64-native-linuxapp-gcc
   ```


©2023 Palo Alto Networks, Inc.

STEP 4 | 執行下列命令來安裝 OVS 2.5.1：

```
wget http://openvswitch.org/releases/openvswitch-2.5.1.tar.gz
 tar xzvf openvswitch-2.5.1.tar.gz cd openvswitch-2.5.1 ./
configure –with-dpdk=”/root/dpdk-2.2.0/x86_64-native-linuxapp-
gcc/” make make install
```

在主機上設定 OVS 和 DPDK

安裝必要的元件來支援 OVS 和 DPDK 之後，您必須設定主機來使用 OVS 和 DPDK。

STEP 1 | 登入 KVM 主機 CLI。

STEP 2 | 如果您要取代或重新設定現有 OVS-DPDK 設定，請執行下列命令來重設任何先前的組態。對每個介面重複此命令。

```
rm /usr/local/var/run/openvswitch/<interface-name>
```

STEP 3 | 設定 OVS 的初始巨型分頁。

```
echo 16384 > /sys/kernel/mm/hugepages/hugepages-2048kB/nr_hugepages
```

STEP 4 | 裝載 QEMU 的巨型分頁：

```
mkdir /dev/hugepages mkdir /dev/hugepages/libvirt mkdir /dev/
hugepages/libvirt/qemu mount -t hugetlbfs hugetlbfs /dev/hugepages/
libvirt/qemu
```

STEP 5 | 使用下列命令來終止目前存在的任何 OVS 精靈。

```
killall ovsdb-server ovs-vswitchd
```

STEP 6 | 建立 OVS 精靈的目錄。

```
mkdir -p /usr/local/etc/openvswitch
mkdir -p /usr/local/var/run/openvswitch
```

STEP 7 | 清除舊目錄。

```
rm -f /var/run/openvswitch/vhost-user*
rm -f /usr/local/etc/openvswitch/conf.db
```

STEP 8 | 初始化組態資料庫。

```
ovsdb-tool create /usr/local/etc/openvswitch/conf.db\
/usr/local/share/openvswitch/vswitch.ovsschema
```


©2023 Palo Alto Networks, Inc.

STEP 9 | 建立 OVS DB 伺服器。

```
ovsdb-server --remote=punix:/usr/local/var/run/openvswitch/
db.sock \ --remote=db:Open_vSwitch,Open_vSwitch,manager_options
 \ --private-key=db:Open_vSwitch,SSL,private_key \ --
certificate=db:Open_vSwitch,SSL,certificate \ --bootstrap-ca-
cert=db:Open_vSwitch,SSL,ca_cert \ --pidfile --detach
```

STEP 10 | 初始化 OVS。

```
ovs-vsctl --no-wait init
```

STEP 11 | 啟動資料庫伺服器。

```
export DB_SOCK=/usr/local/var/run/openvswitch/db.sock
```

STEP 12 | 安裝 DPDK 的 igb_uio 模組（網路裝置驅動程式）。

```
cd ~/dpdk-2.2.0/x86_64-native-linuxapp-gcc/kmod modprobe uio insmod
 igb_uio.ko cd ~/dpdk-2.2.0/tools/
```

STEP 13 | 在介面上使用 PCI-ID 或介面名稱啟用 DPDK。

```
./dpdk_nic_bind.py --bind=igb_uio <your first data interface>
./dpdk_nic_bind.py --bind=igb_uio <your second data interface>
```

STEP 14 | 在 DPDK 模式中啟動 OVS 精靈。您可以變更 ovs-vswitchd 的核心數。將 -c 0x1 變更為 -c 0x3，就能在此精靈中執行兩個核心。

```
ovs-vswitchd --dpdk -c 0x3 -n 4 -- unix:$DB_SOCK --pidfile --
detach
echo 50000 > /sys/kernel/mm/hugepages/hugepages-2048kB/
nr_hugepages
```

STEP 15 | 建立 OVS 橋接器，然後將連接埠附加至 OVS 橋接器。

```
ovs-vsctl add-br ovs-br0 -- set bridge ovs-br0
 datapath_type=netdev
ovs-vsctl add-port ovs-br0 dpdk0 -- set Interface dpdk0 type=dpdk
ovs-vsctl add-br ovs-br1 -- set bridge ovs-br1
 datapath_type=netdev
ovs-vsctl add-port ovs-br1 dpdk1 -- set Interface dpdk1 type=dpdk
```


©2023 Palo Alto Networks, Inc.

STEP 16 | 建立 OVS 的 DPDK vhost 使用者連接埠。

```
ovs-vsctl add-port ovs-br0 vhost-user1 -- set Interface vhost-user1
 type=dpdkvhostuser
ovs-vsctl add-port ovs-br1 vhost-user2 -- set Interface vhost-user2
 type=dpdkvhostuser
```

STEP 17 | 設定主機使用的 NIC 硬體佇列數目。

```
ovs-vsctl set Open_vSwitch . other_config:n-dpdk-rxqs=8
ovs-vsctl set Open_vSwitch . other_config:n-dpdk-txqs=8
```

STEP 18 | 設定用於 OVS 的 CPU 遮罩。

```
ovs-vsctl set Open_vSwitch . other_config:pmd-cpu-mask=0xffff
```

STEP 19 | 設定 DPDK vhost 使用者連接埠的必要權限。在下列範例中，777 用來給予讀取、寫入和執行權限。

```
chmod 777 /usr/local/var/run/openvswitch/vhost-user1
chmod 777 /usr/local/var/run/openvswitch/vhost-user2
chmod 777 /dev/hugepages/libvirt/qemu
```

編輯 VM-Series 防火牆組態檔案

編輯 VM-Series 防火牆 XML 組態檔案來支援 OVS 和 DPDK。部署 VM-Series 防火牆之後，您可以存取 XML 組態檔案。如果是在部署防火牆之後這樣做，務必關閉防火牆，再進行任何變更。以下是範例值，您在每個參數中的值會根據您的 VM-Series 型號而有所不同。

STEP 1 | 登入 KVM 主機 CLI。

©2023 Palo Alto Networks, Inc.

STEP 2 | 編輯 VM-Series 防火牆的 XML 組態檔案。

1. 使用 **virsh edit $*<your-vm-series-name>*** 開啟 XML 設定檔案。
2. 設定支援巨型分頁的記憶體。確保提供足夠的記憶體來支援您在主機上要部署的 VM-Series 防火牆型號。如需詳細資訊，請參閱 VM-Series 系統需求。

```
<memory unit='KiB'>12582912</memory> <currentMemory
 unit='KiB'>6291456</currentMemory> <memoryBacking>
 <hugepages/>
```

3. 為 VM 設定必要的 CPU 旗標。

```
<cpu mode='host-model'>
```

4. 在 VM 和主機之間啟用記憶體共用。

```
<numa> <cell id='0' cpus='0,2,4,6' memory='6291456'
 unit='KiB' memAccess='shared'/> <cell id='1' cpus='1,3,5,7'
 memory='6291456' unit='KiB' memAccess='shared'/> </numa>
```

5. 將 DPDK vhost 使用者連接埠設為 VM-Series 防火牆的網路介面。此外，設定主機提供給 VM-Series 防火牆的 virtio 虛擬佇列數目。

```
<interface type='vhostuser'> <mac address='52:54:00:36:83:70'/
> <source type='unix' path='/usr/local/var/run/openvswitch/
vhost-user1' mode='client'/> <model type='virtio'/>
 <driver name=’vhost’ queues=’8’/> <address type='pci'
 domain='0x0000' bus='0x00' slot='0x04' function='0x0'/
> </interface> <interface type='vhostuser'> <mac
 address='52:54:00:30:d7:94'/> <source type='unix' path='/
usr/local/var/run/openvswitch/vhost-user2' mode='client'/>
 <model type='virtio'/> <driver name=’vhost’ qeueus=’8’>
 <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
 function='0x0'/> </interface>
```

在 KVM 上啟用 SR-IOV

Single root I/O virtualization（單一根 I/O 虛擬化 - SR-IOV）可讓單一根埠下的單一 PCIe 實體裝置，以多個單獨實體裝置呈現給 Hypervisor 或來賓。若要在 KVM 來賓上啟用 SR-IOV，請定義與實體 NIC 相關聯的虛擬功能 (VF) 裝置集區，並從集區自動將 VF 裝置指派到 PCI ID。

如果 SR-IOV 具有 Intel 10GB 網路介面（ixgbe 驅動程式），驅動程式版本必須是 4.2.5 或更新版本，才能支援每個 NIC 介面使用多重佇列。請參閱 PacketMMAP 和 DPDK 驅動程式支援的相容性矩陣（依 PAN-OS 版本分組）。

©2023 Palo Alto Networks, Inc.

STEP 1 | 定義 VF 集區的網路。

1. 使用類似下列範例的文字產生 XML 檔案。將 **pf dev** 的值變更為對應於 SR-IOV 裝置實體功能的 **ethdev**。

```
<network> <name>通道</name> <forward mode='hostdev'
 managed='yes'> <pf dev='eth3'/> </forward> </network>
```

2. 儲存 XML 檔案。
3. 執行下列命令：

```
$ virsh net-define <path to network XML file>  $ virsh net-
autostart passthrough $ virsh net-start passthrough
```

STEP 2 | 若要確保 VM-Series 防火牆會在 DPDK 模式中啟動，請編輯 KVM Hypervisor 上的來賓 VM XML 設定以新增下列項目：

```
<cpu mode='host-passthrough' check='none'/>
```

這可確保 CPU 旗標會公開。

若要確認 CPU 旗標公開於 VM 上：

```
cat /proc/cpuinfo
```

在 PAN-OS 10.2 或更新版本搭配 DPDK 18.11 的標幟輸出中，您需要 **AVX**，或 **AES** 和 **SSE** 標幟。

STEP 3 | 定義並啟動網路之後，修改來賓 XML 定義來指定網路。

```
<interface type='network'> <source network='passthrough'> </
interface>
```

當來賓啟動時，會自動將 VF 指派給來賓。

STEP 4 | 將多點傳送 MAC 位址新增至主機。

當啟用 SR-IOV 時，多點傳送流量將由 PF 進行篩選。此篩選會導致依賴於多點傳送的應用程式（如 OSPF）故障。若要防止此篩選，您必須使用下列命令手動新增多點傳送 MAC 位址至主機：

```
#ip maddress add <multicast-mac> dev <interface-name>
```

透過 SR-IOV 啟用 VLAN 存取模式

KVM 上的 VM-Series 防火牆可在 VLAN 存取模式中運作，以支援將其部署為虛擬網路功能 (VNF) 而在多租用戶雲端/資料中心環境中提供安全性即服務的使用案例。在 VLAN 存取模式中，每個 VNF 在每個網路都有專用的虛擬網路介面 (VNI)，且無需 VLAN 標籤即可傳送和接收送往/來自 SR-IOV 虛擬功能 (VF) 的封包；您可以在主機 Hypervisor 的實體和虛擬功能上啟用此功能。當您隨後在 VM-Series 防火牆上啟用 VLAN 存取模式時，防火牆無需 VLAN 標籤即可在其所有資料平面介

 ©2023 Palo Alto Networks, Inc.

面間傳送和接收流量。此外，如果您設定 QoS 原則，防火牆即會在存取介面上強制執行 QoS，並且以不同的方式處理多租用戶部署中的流量。

根據預設，*KVM* 上的 *VM-Series* 防火牆會在 *VLAN* 主幹模式中運作。

STEP 1 | 在主機系統上，設定要在 VLAN 存取模式中運作的實體和虛擬功能。

ip link set [inf_name] vf [vf_num] vlan [vlan_id]。

若要讓 *VM-Series* 防火牆發揮最佳效能，請務必：

- 啟用 *CPU* 釘選。請參閱 在 KVM 上的 NUMA 節點中隔離 CPU 資源。
- 停用重播防護（如果您已設定 *IPSec* 通道）。

  在防火牆 *Web* 介面上，選取 ***Network***（網路） **> *IPSec Tunnels***（***IPSec*** 通道），然後選取 *IPSec* 通道，再按一下 ***General***（一般）並選取 ***Show Advanced Options***（顯示進階選項），然後清除 ***Enable Replay Protection***（啟用重播防護）。

STEP 2 | 在 VM-Series 防火牆上存取 CLI。

STEP 3 | 啟用 VLAN 存取模式。

request plugins vm-series vlan-mode access-mode on

on 會啟用 VLAN 存取模式；若要使用 VLAN 主幹模式，請輸入 **request plugins vm-series vlan-mode access-mode off**。

STEP 4 | 重新啟動防火牆。

輸入 **request restart system**。

STEP 5 | 確認 VLAN 模式設定。

show plugins vm-series vlan-mode

在 KVM 上啟用 NIC 的多佇列支援

修改來賓 XML 定義來啟用多重佇列 virtio-net。多重佇列 virtio-net 可讓網路效能隨著 vCPU 數目而調整，還能建立多個 TX 和 RX 佇列來平行處理封包。

修改來賓 XML 定義。在 N 中插入 1 到 256 的值，以指定佇列數目。為了得到最佳結果，佇列數目必須符合 VM 上設定的資料平面核心數目。

```
<interface type='network'> <source network='default'/> <model
 type='virtio'/> <driver name='vhost' queues='N'/> </interface>
```


©2023 Palo Alto Networks, Inc.

在 KVM 上的 NUMA 節點中隔離 CPU 資源

您可以將來賓 VM 的 CPU 資源隔離到單一非流一記憶體存取 (NUMA) 節點，以改善 KVM 上 VM-Series 的效能。在 KVM 上，您可以檢視 NUMA 拓撲 **virsh**。下列範例來自雙節點 NUMA 系統：

STEP 1 | 檢視 NUMA 拓撲。在下列範例中，有兩個 NUMA 節點（通訊端），各有四核心 CPU 且啟用超執行緒。所有偶數編號 CPU ID 屬於一個節點，所有奇數編號 CPU ID 屬於另一個節點。

```
% virsh 功能 <…> <topology> <cells num='2'> <cell id='0'> <memory
 unit='KiB'>33027228</memory> <pages unit='KiB' size='4'>8256807</
pages> <pages unit='KiB' size='2048'>0</pages> <distances>
 <sibling id='0' value='10'/> <sibling id='1' value='20'/> </
distances> <cpus num='8'> <cpu id='0' socket_id='1' core_id='0'
 siblings='0,8'/> <cpu id='2' socket_id='1' core_id='1'
 siblings='2,10'/> <cpu id='4' socket_id='1' core_id='2'
 siblings='4,12'/> <cpu id='6' socket_id='1' core_id='3'
 siblings='6,14'/> <cpu id='8' socket_id='1' core_id='0'
 siblings='0,8'/> <cpu id='10' socket_id='1' core_id='1'
 siblings='2,10'/> <cpu id='12' socket_id='1' core_id='2'
 siblings='4,12'/> <cpu id='14' socket_id='1' core_id='3'
 siblings='6,14'/> </cpus> </cell> <cell id='1'> <memory
 unit='KiB'>32933812</memory> <pages unit='KiB' size='4'>8233453</
pages> <pages unit='KiB' size='2048'>0</pages> <distances>
 <sibling id='0' value='20'/> <sibling id='1' value='10'/> </
distances> <cpus num='8'> <cpu id='1' socket_id='0' core_id='0'
 siblings='1,9'/> <cpu id='3' socket_id='0' core_id='1'
 siblings='3,11'/> <cpu id='5' socket_id='0' core_id='2'
 siblings='5,13'/> <cpu id='7' socket_id='0' core_id='3'
 siblings='7,15'/> <cpu id='9' socket_id='0' core_id='0'
 siblings='1,9'/> <cpu id='11' socket_id='0' core_id='1'
 siblings='3,11'/> <cpu id='13' socket_id='0' core_id='2'
 siblings='5,13'/> <cpu id='15' socket_id='0' core_id='3'
 siblings='7,15'/> </cpus> </cell> </cells>
```

STEP 2 | 使用來賓 xml 定義中的 **cpuset** 屬性，將 KVM 來賓中的 vCPU 釘選到特定的實體 vCPU。在此範例中，全部 8 個 vCPU 都釘選到第一個 NUMA 節點中的實體 CPU。如果不想明確釘選 vCPU，您可以省略 **cputune** 區塊，在此情況下，所有 vCPU 會釘選到 cpuset 中指定的 CPU 範圍，但不會明確對應。

```
<vcpu cpuset='0,2,4,6,8,10,12,14'>8</vcpu> <cputune> <vcpupin
 vcpu='0' cpuset='0'/> <vcpupin vcpu='1' cpuset='2'/> <vcpupin
 vcpu='2' cpuset='4'/> <vcpupin vcpu='3' cpuset='6'/> <vcpupin
 vcpu='4' cpuset='8'/> <vcpupin vcpu='5' cpuset='10'/> <vcpupin
 vcpu='6' cpuset='12'/> <vcpupin vcpu='7' cpuset='14'/> </cputune>
```


©2023 Palo Alto Networks, Inc.

智慧流量卸載

智慧型流量卸載是 VM-Series 防火牆安全性訂閱，搭配 NVIDIA Bluefield-2 DPU 一起設定時，可增加 VM-Series 防火牆的容量輸送量。VM-Series 防火牆和 BlueField-2 DPU 必須安裝在執行 Ubuntu 18.04 且核心版本為 4.15.0-20 的 x86 實體主機上。VM-Series 防火牆必須在虛擬介接模式中部署。

Intelligent Traffic Offload（智慧型流量卸載；ITO）服務會將流量的前幾個封包路由至防火牆來檢查，以決定是否應該檢查或卸載流量中的其餘封包。此決定基於原則或基於是否可以檢查流量（例如，無法檢查加密流量） 透過只檢查可受益於安全性檢查的流程，防火牆的整體負載會大幅降低，VM-Series 防火牆效能也會提升，而不犧牲安全性。

目前的 NVIDIA BlueField-2 DPU 擴充性限制如下：

- 工作階段表格容量：500,000 個工作階段
- 工作階段表格更新率：7000 個工作階段/秒
- 每秒連線數：20,000
- 卸載急轉速率：1500 位元組封包約 90 Gbps

如果流量卸載至 BlueField D-2 DPU 超過每秒 7,000 個工作階段，或卸載工作階段表格已滿，則流量仍會流經 VM-Series 防火牆並接受檢查。當每秒工作階段數降到 7,000 以下時，智慧型流量卸載至 Bluefield-2 DPU 會重新開始。

在具有相同設定的實體主機上執行的 VM-Series 防火牆支援主動/被動 HA。

智慧型流量卸載不支援加速過時工作階段設定。

- 智慧型流量卸載需求
- 智慧型流量卸載介面
- high availability （高可用性）
- 安裝 BlueField-2 DPU
- 安裝 VM-Series 防火牆
- 檢查 BlueField-2 DPU 系統
- 啟用虛擬功能
- 安裝或升級 BlueField Bootstream 軟體
- 安裝或升級 Debian 套件
- 執行智慧型流量卸載
- BlueField-2 DPU 疑難排解
- PAN-OS 疑難排解
- 參考

©2023 Palo Alto Networks, Inc.

智慧型流量卸載需求

ITO 需要相同的 x86 實體主機上安裝一個 VM-Series 防火牆和一個 BlueField-2 DPU。支援 VM-Series 防火牆的主動/被動高可用性。

每個主機只能部署一個 ***VM-Series*** 防火牆和一個 ***BlueField-2 DPU***。

- 具有 2 個（HA 為 4 個）可用 100GB/s 連接埠的網路交換器。

  如果想要使用 VLAN，請確定您的交換器有能力。
- X86 實體主機硬體需求。
  - 至少 120GB 可用的 RAM（伺服器為 64GB，VM-Series 防火牆為 56GB）
  - 至少 18 個實體核心
  - Bluefield-2 SmartNIC MBF2M516A-CEEOT，具有兩個 100GB/s 連接埠安裝在 PCI-e 插槽 3 或 4。
  - 根據《NVIDIA BlueField 乙太網路 DPU 使用者指南》的建議，BlueField2 DPU 上的每個連接埠都有經認證的 100GigE SFP。
- X86 主機軟體需求。
  - Ubuntu 18.04，核心版本為 4.15.0-20。
  - Bluefield 二進位 bootstream 版本：5.3-1.0.0.1

    接受「使用者授權合約」以開始下載。
- VM-Series 防火牆的虛擬機器。
  - PAN-OS 10.2 或更新版本。
  - VM-Series 外掛程式 2.1.0 或更新版本。
  - 若要授權智慧型流量卸載，請為 10.0.4 和更新版本建立軟體 NGFW 部署設定檔，至少要有 18 個 vCPU 和智慧型流量卸載服務。設定檔可以包含其他安全性服務。

    對於 PAN-OS 10.1.1 或更新版本和 VM-Series 外掛程式 2.1.1 或更新版本，若要授權智慧型流量卸載，請為 10.0.4 和更新版本建立軟體 NGFW 部署設定檔，至少要有六 (6) 個 vCPU 和智慧型流量卸載服務。設定檔可以包含其他安全性服務。

智慧型流量卸載介面

智慧型流量卸載部署可連接三種介面：

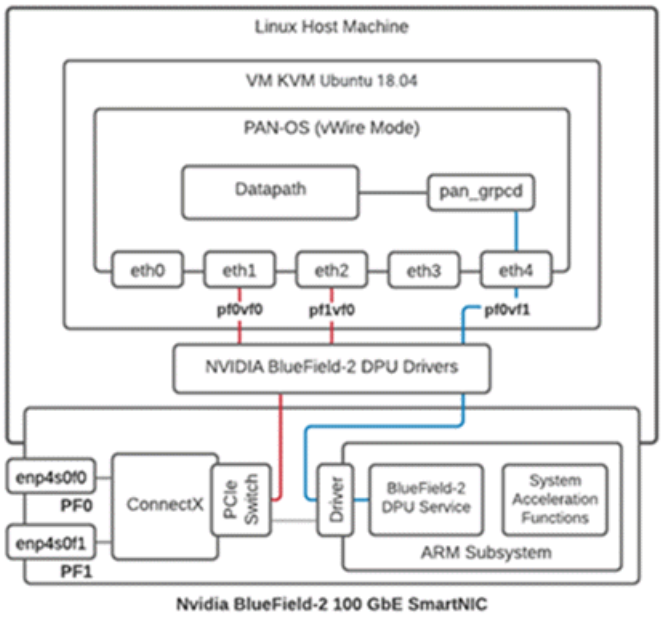
- PAN-OS 虛擬介面：
  - eth0：管理介面
  - eth1、eth2：資料平面
  - eth3：HA 介面
  - eth4：gRPC 介面
- BlueField-2 DPU 實體介面（從主機作業系統建立）。

©2023 Palo Alto Networks, Inc.

- BlueField-2 DPU 100GB 連接埠的主機實體介面（從主機作業系統建立）。

您可以透過您在實體主機上建立的 SR-IOV virtual function（虛擬功能；VF），將 PAN-OS 介面連線至 BlueField-2 DPU（請參閱啟用虛擬功能）。

在下圖中，兩個 BlueField-2 DPU 連接埠顯示為實體功能 PF0 和 PF1。從主機端可以觀察到這些 PF 為 enp4s0f0 和 enp4s0f1，並分割成多個 VF 來執行 SR-IOV 功能。



- 每個 PF 的第一個 VF 必須是資料連接埠 (eth1:pf0vf0)。
- gRPC 用戶端/伺服器介面的控制通道需要額外的 VF (eth4:pf0v1)。
- 來自主機端的 VF 如下：
  - enp4s0f0 在 BlueField-2 DPU 上以 pf0vf0 和 pf1vf0 表示，用於資料。
  - enp4s0f1 以 pf0vf1 表示，用於 gRPC 控制流量。

high availability （高可用性）

在實體主機上以 Vwire 模式部署的一對 VM-Series 防火牆支援主動/被動 HA。

- 防火牆必須安裝在依照智慧型流量卸載需求設定 BlueField-2 DPU 的實體主機上。
- 對於 HA2 介面（請參閱 主動封包流程 和 被動封包流程 中的圖表），在兩台主機上都使用相同的 Mellanox 介面（cx-3、cx-4 或 cx-5）。
- （選用）若要支援流量切換，主機必須位於不同的 VLAN 上，您才能使用 VLAN 標籤來選取主要，如保護 Linux 主機之間的流量所述。

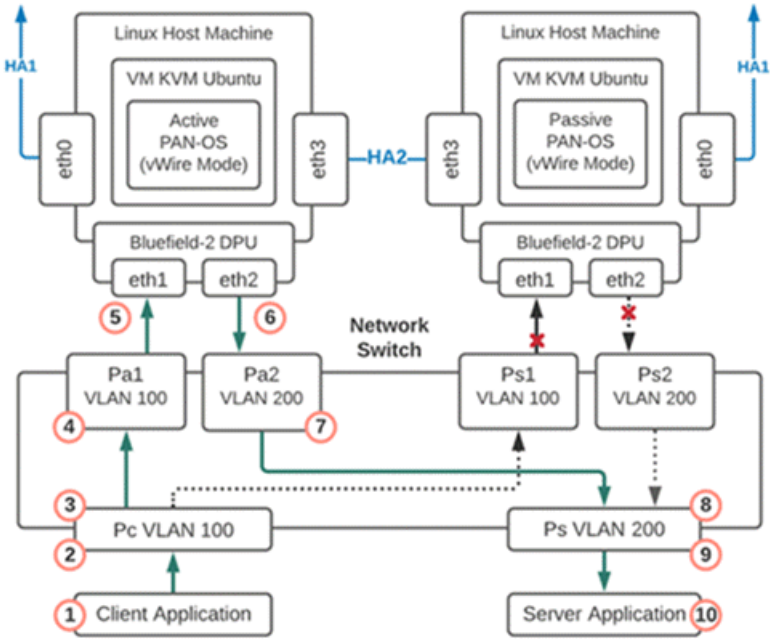
ITO H/A 著重於 VM-Series 防火牆可用性。每個防火牆各維護一個工作階段表格，每個 BlueField-2 DPU 各會維護一個流量表格。HA 設定會同步作用中工作階段表格，確保在執行階段鏡像到被動防火牆。工作階段表格儲存需要檢查的工作階段，以及標示為卸載的工作階段。

HA 使用 PAN-OS 介面 eth3（位於 VM-Series 防火牆的 NIC 上）。Eth3 用於選取主動防火牆，並同步主動/被動配對上的 VM-Series 防火牆工作階段表格。

©2023 Palo Alto Networks, Inc.

主動封包流程

下圖針對使用選用 VLAN 設定的 HA 設定，逐步說明主動封包流程。



1. 封包從用戶端應用程式傳送至網路交換器。
2. 封包到達交換器連接埠，該連接埠已設計為將 VLAN 100 標籤新增至封包。
3. 由於連接埠 Ps1 的介面故障，標記的封包只能移至連接埠 Pa1，因為防火牆處於被動模式。
4. 封包到達連接埠 Pa1，從封包中移除 VLAN 100，接著封包傳遞至防火牆 eth1。
5. 防火牆在 vWire 模式中執行，封包由防火牆處理，然後從 eth2 送出。
6. 封包到達連接埠 Pa2 並添加 VLAN 200。
7. 封包從連接埠 Pa2 送出，只能傳遞至連接埠 Ps，因為另一個 VLAN 200 連接埠 Ps2 故障。
8. 封包到達連接埠 Ps，移除 VLAN 200 標籤。
9. 封包從連接埠 Ps 送出，不含 VLAN 標籤
10. 封包傳遞至伺服器。

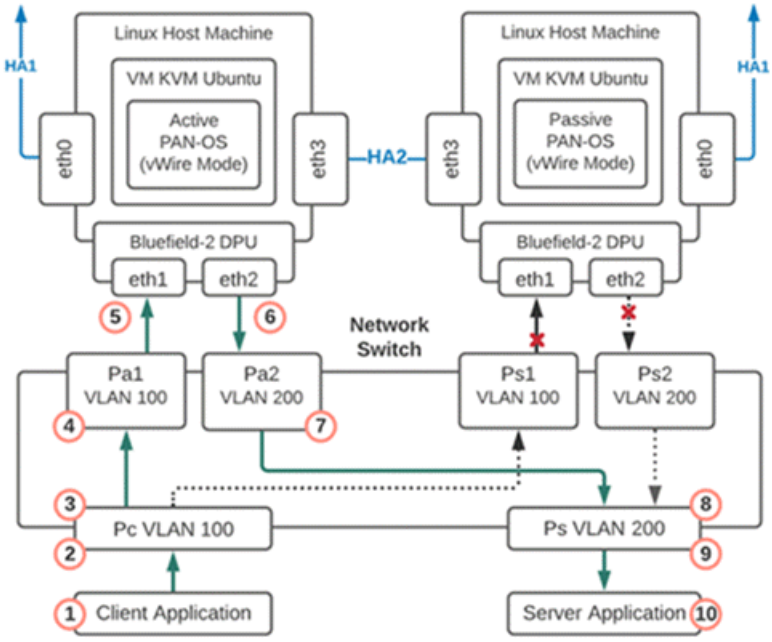
容錯移轉事件

當有主動 VM-Series 防火牆傳來通知，或被動防火牆偵測到主動沒有回應時，就會發生容錯移轉事件。發生這種情況時，Pa1 和 Pa2 連接埠的網路連線會中斷，連接埠 Ps1 和 Ps2 的網路連線會變成作用中。

被動封包流程

當 VM-Series 防火牆處於被動狀態時，被動成員上的 Bluefield-2 DPU 開始運作，但要等到容錯移轉且共置的 VM-Series 防火牆變為作用中，才會傳送流量。下圖針對使用選用 VLAN 設定的 HA 設定，逐步說明被動封包流程。

©2023 Palo Alto Networks, Inc.



1. 封包從用戶端應用程式傳送至網路交換器。
2. 封包到達交換器連接埠，該連接埠已設計為將 VLAN 100 標籤新增至封包。
3. 因為連接埠 Pa1 的介面故障，而且防火牆現在已從被動變成主動，標記的封包只能移至連接埠 Ps1。
4. 封包到達連接埠 Ps1，從封包中移除 VLAN 100，接著封包傳遞至防火牆 eth1。
5. 防火牆在 vWire 模式中執行，封包由防火牆處理，然後從 eth2 送出。
6. 封包到達連接埠 Ps2 並添加 VLAN 200。
7. 封包從連接埠 Ps2 送出，只能傳遞至連接埠 Ps，因為另一個 VLAN 200 連接埠 Pa2 故障。
8. 封包到達連接埠 Ps，移除 VLAN 200 標籤。
9. 封包從連接埠 Ps 送出，不含 VLAN 標籤。
10. 封包傳遞至伺服器。

安裝 BlueField-2 DPU

在安裝 VM-Series 防火牆之前，請先在實體主機上安裝 BlueField-2 DPU。如需 BlueField-2 DPU 的相關資訊，請參閱軟體文件：NVIDIA BLUEFIELD DPU 系列軟體 V3.5.0.11563 文件。

1. 依照《NVIDIA BlueField 乙太網路 DPU 使用者指南》的指示，在主機電腦上安裝 BlueField-2 DPU。
2. 依照《NVIDIA BlueField-2 DPU 軟體快速入門指南》的指示，安裝 BlueField 驅動程式。

安裝 VM-Series 防火牆

VM-Series 防火牆上的 KVM 標準安裝會安裝 PAN-OS。請遵循下列各節中的安裝步驟。

- KVM 上的 VM-Series—需求與先決條件
- 使用 Virt-Manager 安裝 VM-Series 防火牆或使用 ISO 安裝 VM-Series 防火牆

©2023 Palo Alto Networks, Inc.

啟用虛擬功能

如智慧型流量卸載介面所述，virtual function（虛擬功能；VF）會將 PAN-OS 介面連線至 BlueField-2 DPU。

每個連接埠的虛擬功能 VF 數目上限為 2。您總共需要三個 — 兩個用於資料路徑，一個用於管理介面。

STEP 1 | 在主機電腦上啟用虛擬功能。

- 根據預設，BlueField-2 DPU 會將第一個 VF 用於資料路徑，即下列範例中的 enp4s0f0v0 和 enp4s0f1v0。
- 另一個 VF (enp4s0f0v1) 用於 BlueField-2 卡上執行的服務專用的管理介面（不要與 VM-Series 防火牆管理介面混淆）。

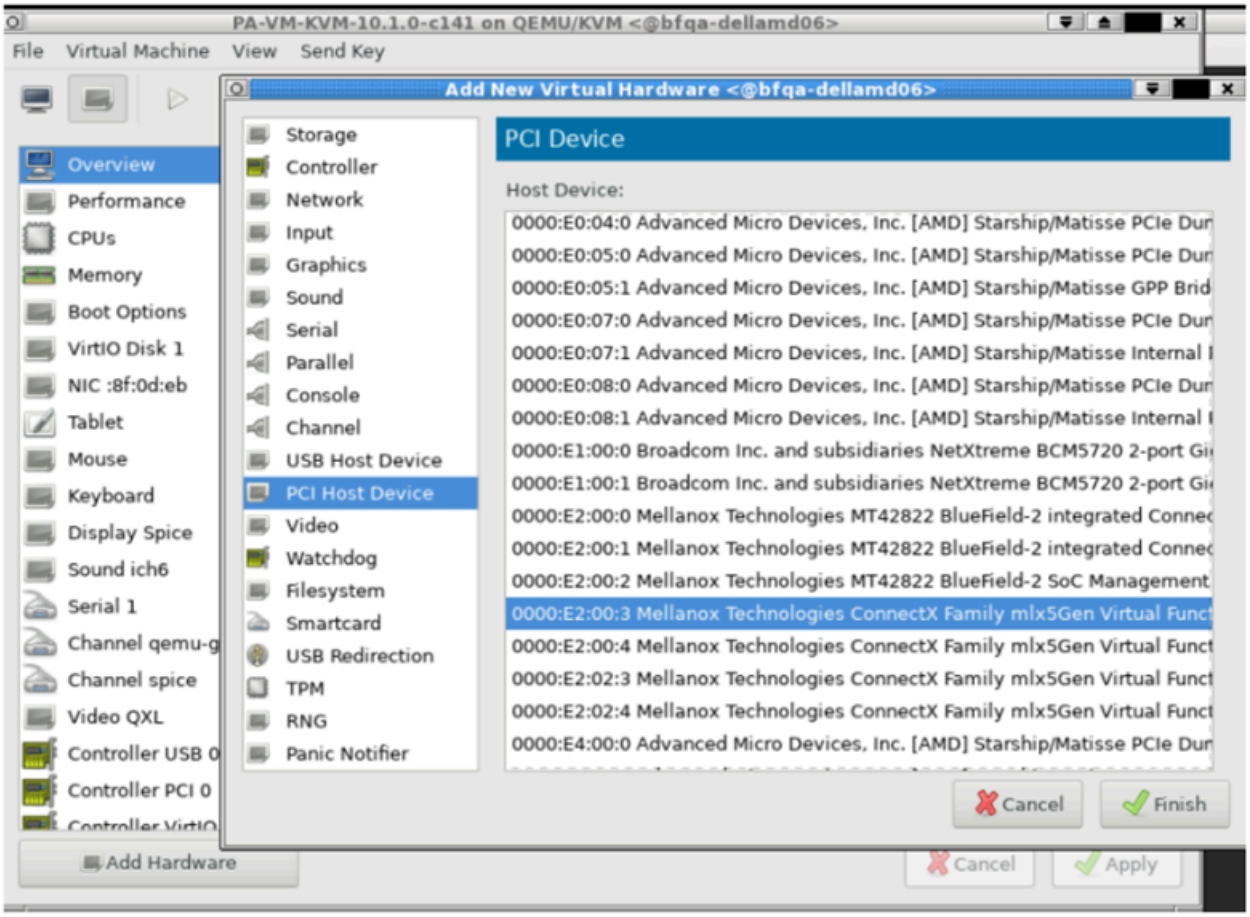
```
$ cat /sys/class/net/enp4s0f0/device/sriov_totalvfs
   8
$ echo 2 > /sys/class/net/enp4s0f0/device/sriov_numvfs
$ cat /sys/class/net/enp4s0f1/device/sriov_totalvfs
   8
$ echo 2 > /sys/class/net/enp4s0f1/device/sriov_numvfs
```


©2023 Palo Alto Networks, Inc.

STEP 2 | 從 KVM 超管理器將 VF 配置給 VM-Series 防火牆。

除非將 *VF* 配置給 *VM*，否則客體 *PAN-OS* 不會開機。

1. 關閉 VM。
2. 在 KVM 上，使用 virt-manager 將 VF 新增至 VM。
   - 選取 [Add Hardware（新增硬體）]，選取 PF1 的 VF0，然後按一下 [Finish（完成）]。
   - 選取 [Add Hardware（新增硬體）]，選取 PF0 的 VF0，然後按一下 [Finish（完成）]。
   - 選取 [Add Hardware（新增硬體）]，選取 PF0 的 VF1，然後按一下 [Finish（完成）]。



檢查 BlueField-2 DPU 系統

當主機上安裝 Rshim 驅動程式時，BlueField-2 DPU 會先與該主機通訊。Rshim 提供 tty（可透過 minicom 存取）介面和名為 tmfifo_net0 的網絡介面。tmfifo_net0 介面可讓您從主機以 ssh 進入 BlueField-2 DPU。Rshim 驅動程式在 x86 超管理器作業系統上執行，事實上，OFED 安裝預設會安裝 Rshim 驅動程式。

©2023 Palo Alto Networks, Inc.

STEP 1 | 登入主機電腦。

```
$ ssh user@<host-ip-address>
```

```
$ password:
```

STEP 2 | 如果 Rshim 驅動程式的主機網路介面沒有 IP 位址，您必須建立 IP 位址。

```
$ ip addr add dev tmfifo_net0 192.168.100.1/24
```

STEP 3 | 從主機電腦登入 BlueField-2 DPU 子系統。

```
$ ssh ubuntu@192.168.100.2
```

```
$ password: ubuntu
```

如果這是您第一次登入，系統會提示您以新密碼取代預設密碼。

STEP 4 | 在 BlueField-2 DPU 上變更預設密碼。

以初始使用者名稱 **ubuntu** 和密碼 **ubuntu** 登入 BlueField-2 DPU。

登入後，系統會提示您設定新密碼。

```
警告：您的密碼已過期。您必須立即變更密碼並重新登入#變更 ubuntu 的密碼。目前密碼：***** 新密碼：***** 重新輸入新密碼：***** passwd：密碼更新成功
```

登出，然後使用新密碼登入。

STEP 5 | 檢查軟體版本。

```
$ ofed_info -s
```

這應該會傳回以下版本或更新版本：

```
$ MLNX_OFED_LINUX-5.3-0.3.3
```

STEP 6 | 檢查 Bluefield 2 DPU 是否處於正確模式。

正確模式為內嵌式 CPU 功能所有權模式。如需有關檢查和設定模式的指示，請參閱嵌入式 CPU 功能所有權模式文件。

安裝或升級 BlueField Bootstream 軟體

依照下列步驟，確保 BlueField-2 DPU 有最新的 Bluefield bootstream (BFB) 軟體。BFB 包括 BlueField 作業系統和其他軟體，例如驅動程式和網路介面。

STEP 1 | 將 BFB 套件下載至 BlueField-2 DPU 的實體主機。

從 NVIDIA 網站，為 DPI ARM 核心上執行的作業系統取得最新版的驅動程式 — 您必須接受使用者授權合約才能下載。

©2023 Palo Alto Networks, Inc.

STEP 2 | 從實體主機上的 Rshim 開機位置安裝 BFB。

請注意，以下檔名（以 **DOCA** 開頭和以 **.bfb** 結尾的字串）不含空格。將下列命令輸入成一行。

```
$ cat DOCA_v1.0_BlueField_OS_Ubuntu_20.04-5.3-1.0.0.0-3.6.0.11699-1-aarch64.bfb > /dev/rshim0/boot
```

STEP 3 | 登入 BlueField-2 DPU。

使用您在檢查 BlueField-2 DPU 系統中建立的新密碼。

```
$ ssh ubuntu@192.168.100.2
```

```
$ password:
```

STEP 4 | 在 BlueField-2 DPU 上套用韌體升級。

將下列命令輸入成一行。

```
$ sudo /opt/mellanox/mlnx-fw-updater/firmware/mlxfwmanager_sriov_dis_aarch64_41686
```

STEP 5 | 重新啟動系統。

登出 BlueField-2 DPU，然後返回 Linux 主機。

```
$ ipmitool chassis power cycle
```

STEP 6 | 登入 BlueField-2 DPU。

```
$ ssh ubuntu@192.168.100.2
```

```
$ password:
```

STEP 7 | 在 BlueField-2 DPU 上啟動 opof（open offload；開放式卸載）服務。opof 目前是獨立服務。

VF 必須存在，您才能啟動 *opof*。請參閱 啟用虛擬功能。

```
$ opof_setup
$ service opof restart
```

STEP 8 | 確認 opof 服務正常運作。

```
$ service opof status
```

安裝或升級 Debian 套件

如果 Debian 套件版本早於 1.0.4，則必須升級。

©2023 Palo Alto Networks, Inc.

STEP 1 | 在 BlueField-2 DPU 上，檢查 opof 套件的版本。

```
$ opof -v
```

如果早於 1.0.4，則必須升級。

STEP 2 | 為套件新增 NVilDIA 儲存庫。

```
$ cd /etc/apt/sources.list.d
```

將每個 `wget` 命令全部輸入成一行。URL 中沒有空格：

```
wget https://linux.mellanox.com/public/repo/doca/1.0/ubuntu20.04/
doca.list
```

```
wget -qO - https://linux.mellanox.com/public/repo/doca/1.0/
ubuntu20.04/aarch64/GPG-KEY-Mellanox.pub | sudo apt-key add -
```

```
$ apt update
```

STEP 3 | 在 BlueField-2 DPU 上，檢查儲存庫中的 Debian 套件。

```
$ apt search opof
```

```
正在排序...完成全文搜尋...完成 opof/now 1.0.4 arm64 [已安裝，本地] Nvidia
 Firewall Open Offload Daemon
```

STEP 4 | 在 ARM 上，解除安裝過時的 Debian 套件。

```
$ apt remove opof
```

STEP 5 | 安裝新的 Debian 套件。

```
$ apt install opof
```

STEP 6 | 設定並重新啟動 opof 服務。

```
$ opof_setup
```

```
$ service opof restart
```

STEP 7 | 確認 opof 服務正常運作。

```
$ service opof status
```

執行智慧型流量卸載

此解決方案需要訂閱智慧型流量卸載軟體，以及至少 18 個實體核心，才能達到最佳效能/輸送量。根據預設，PAN-OS 會分配 2 個核心給智慧型流量卸載，4 個核心給管理程序，其餘 12 個核心給資料平面處理。

- 在 VM-Series 防火牆上設定智慧型流量卸載
- 在 BlueField-2 DPU 上設定智慧型流量卸載服務
- 啟動或重新啟動智慧型流量卸載服務

©2023 Palo Alto Networks, Inc.

- 取得服務狀態和健康情況

在 VM-Series 防火牆上設定智慧型流量卸載

請依照下列步驟在 PAN-OS 上啟用智慧型流量卸載。

STEP 1 | 啟動 PAN-OS VM。這假設您已建立 VM 實例且正在重新啟動。

```
$ virsh start <vm-name>
```

STEP 2 | 使用 SSH 登入 VM-Series 防火牆管理介面。

```
$ ssh admin@<panos-management-IP-address>
```

```
$ admin@PA-VM>
```

STEP 3 | 確認已安裝和授權智慧型流量卸載。

```
admin@PA-VM> show intelligent-traffic-offload
```

```
智慧型流量卸載:    設定                : 啟用    操作 啟用          : True
   最小數量封包          : 8    最小速率                  : 95    TCP 老
化                  : 12-    UDP 老化                 : 20
```

`Configuration:Enabled` 表示已授權智慧型流量卸載。

`Operation Enabled:True` 表示您已重新啟動已設定的裝置。

STEP 4 | 啟用智慧型流量卸載。

使用下列命令啟用 ITO，而不重新啟動系統。

```
admin@PA-VM> set session offload yes
```

您也可以使用 **set session offload no** 來停用 ITO，而不需要重新啟動系統。

STEP 5 | 驗證智慧型流量卸載。

```
admin@PA-VM> show session info | match offload
```

```
硬體工作階段卸載: True 硬體 UDP 工作階段卸載: True
```

若要檢視全域計數器，請使用下列命令：

```
admin@PA-VM> show counter global | match flow_offload
```

如需輸出編排的詳細資訊及每個計數器的說明，請參閱工作階段計數器。

在 BlueField-2 DPU 上設定智慧型流量卸載服務

必須依照在 VM-Series 防火牆上設定智慧型流量卸載所述建置服務。

©2023 Palo Alto Networks, Inc.

STEP 1 | 從主機電腦登入 BlueField-2 DPU 複合系統。

$ **ssh ubuntu@192.168.100.2**

```
$ password: ubuntu $ ubuntu> sudo -i
```

STEP 2 | 在 BlueField-2 DPU 作業系統中設定初步組態。

root@bf2SmartNIC:~# **opof_setup**

```
[ INFO ] 未指定巨型分頁，使用 2048 [ INFO ] 未指定 gRPC 連接埠，使用
 pf0vf1 設定 ovs fallback 為 pf0vf1 設定 grpc 保留 2048*2MB 巨型分頁
```

啟動或重新啟動智慧型流量卸載服務

如果 ITO 服務在 DPU 上執行，服務可能已自動啟動。若要檢查狀態，請執行下列命令：

$ service opof status

如果 opof 服務未執行，請輸入下列命令以啟動控制器：

$ service opof start

若要重新啟動服務，請執行下列命令：

$ service opof restart

取得服務狀態和健康情況

使用 opof 取得服務狀態和健康情況。每個命令都有自己的命令列說明，例如：**$ opof -h**

- 查詢工作階段：

  $ opof query -i <session_id>

- 查詢服務卸載統計資料：

  $ opof stats

BlueField-2 DPU 疑難排解

使用下列程序來重新啟動系統。

1. 若要重新啟動系統，請登出 BlueField-2 DPU，然後返回 Linux 主機作業系統。

   $ ipmitool chassis power cycle

2. 重新啟動後，如果介面沒有出現，請登入 BlueField-2 DPU 並輸入：

   $ /sbin/mlnx_bf_configure

3. 返回主機作業系統並輸入：

   $ sudo /etc/init.d/openibd restart

©2023 Palo Alto Networks, Inc.

PAN-OS 疑難排解

驗證流量

資料流量可以從用戶端產生，並由伺服器透過智慧型流量卸載設定來消耗。IPERF3 可用來產生流量，如執行 IPERF3 測試所述。流量開始後，流量的前幾個封包會傳送至 PA-VM，以決定是否需要卸載流量。

必須定義應用程式取代政策，以識別卸載的流量。TCP 流程會在控制封包上設定 FIN/RST 旗標，並傳送至 PA-VM。當 PA-VM 決定卸載流量時，請使用 show session all 來顯示卸載的流量。使用 **show session id <flowID>** 來提供流量狀態的相關資訊。卸載的流量為 `Offload: yes` 狀態。

當流量的後續封包處於卸載狀態，且正在通過 BlueField-2 DPU 時，不會更新流量計數器。流量結束後，卸載服務會觸發過時計時器（從 CLI 設定的 TCP 過時）。計時器到期時，該服務會收集更新的流量統計資料，並傳送至 VM-Series 防火牆。防火牆接著會更新流量工作階段計數器，且 **show session id <flowID>** 會傳回更新的值。

工作階段計數器

使用下列命令來檢視工作階段計數器。

admin@PA-VM > **show counter global | match flow_offload**

每個計數器的輸出欄如下：

Counter Name（計數器名稱）| Value（值）| Rate（比率）| Severity（嚴重性）| Category（類別）| Aspect（層面）| Description（說明）。

- Value（值）— 系統啟動以來的出現次數。
- Rate（比率）— 計數器變更的頻率。
- Severity（嚴重性）— Info（資訊）、Warning（警告）、Drop（捨棄）。用於技術支援。
- Category（類別）— Flow（流量）（工作階段的元件）。
- Aspect（層面）— 整個流量的卸載。

計數器名稱	說明
flow_offload_rcv_cpu	已卸載工作階段的 CPU 接收的封包數
flow_offload_session_update	工作階段需要更新的次數
flow_offload_session_insert	插入卸載裝置中的工作階段數目
flow_offload_session_delete	從卸載裝置刪除的工作階段數目
flow_offload_delete_msg_failed	傳送給失敗 GRPC 的 del 訊息數目
flow_offload_add_msg_failed	傳送給失敗 GRPC 的工作階段訊息數目
flow_offload_session_verify	傳送給卸載裝置的驗證訊息數目

©2023 Palo Alto Networks, Inc.

計數器名稱	說明
flow_offload_verify_msg_failed	傳送給失敗 GRPC 的驗證訊息數目
flow_offload_update_session_stat	HW 表示流量過時
flow_offload_missing_session_stat	找不到統計資料的工作階段
flow_offload_invalid_session	卸載無效的工作階段 ID
flow_offload_del_session_fail	卸載刪除無效的工作階段
flow_offload_add_session_fail	卸載新增工作階段失敗
flow_offload_get_session_fail	卸載取得工作階段失敗
flow_offload_grpc_fail	卸載 grpc 呼叫失敗
flow_offload_active_session	作用中卸載的工作階段數目
flow_offload_aged_session	過時卸載的工作階段數目
flow_offload_session	卸載的工作階段數目

執行 IPERF3 測試

Iperf3 是選用的簡單應用程式，用於產生有效的流量供執行資料流量測試。若要將伺服器當成服務執行，請使用 **iperf3 -s -D**。根據預設，應用程式會在 TCP/UDP 目的地連接埠 5201 上等待封包，但可以變更連接埠。

- 單一流程 — 對於單一 iperf3 流程，請輸入：

```
iperf3 -c <server-ip-address> -t 60
```

- 多重流程 — 若要持續 60 秒啟動 20 個並行流程，請輸入：

```
iperf3 -c <ip of server> -P 20 -t 60
```

驗證智慧型流量卸載

您可以使用 VM-Series 防火牆日誌，驗證防火牆上執行的 ITO 用戶端與 Bluefield-2 DPU 上的卸載服務之間的連線。成功卸載預期的日誌輸出如下所示。

admin@auto-pavm> **less mp-log pan_grpcd.log**

```
[PD] dec 可用清單 0xe0ff022000 DP 中的 RS LIB INIT# pan_fec_app_init:
 fec_data 0xe0feef1088, maxentries 120 [FEC] enc 可用清單 0xe0feef1100,
 dec 可用清單 0xe0feef10b8 Creating dp grpc ring buf Initializing dp
```


©2023 Palo Alto Networks, Inc.

```
 grpc ring buf 對應流量資料記憶體 找到卸載參數 心跳發現 1 已建立到卸載裝置的連
線
```

OPOF 疑難排解

您也可以檢視卸載服務日誌以驗證連線：

root@linux:~# **service opof status**

```
● opof.service - Nvidia 防火牆智慧型流量卸載精靈程式已載入：已載入（/
etc/systemd/system/opof.service；已停用；供應商預設：已啟用） 作用
中：自 2021 年 5 月 21 日星期五 18:40:38 UTC 起作用中（執行）；3 小
時 48 分鐘前文件：檔案/opt/mellanox/opof/README.md 程序：163906
 ExecStartPre=/usr/sbin/opof_pre_check (code=exited, status=0/
SUCCESS) 主 PID：163922 (nv_opof) 工作：30（限制：19085） 記憶體：50.7M
 CGroup: /system.slice/opof.service └─163922 /usr/sbin/nv_opof -n 1
 -a 0000:03:00.0,representor=[0] -a 0000:03:00.1,representor=[0] 5 月
 21 日 18:40:38 localhost.localdomain nv_opof[163922]：EAL：探查 PCI 驅
動程式：mlx5_pci (15b3:a2d6) 裝置：0000:03:00.0 (socket 0) 5 月 21 日
 18:40:38 localhost.localdomain nv_opof[163922]:EAL：無效的 NUMA 插槽，
預設為 0 May 21 18:40:38 localhost.localdomain nv_opof[163922]：EAL：
探查 PCI 驅動程式：mlx5_pci (15b3:a2d6) 裝置：0000:03:00.0 (socket 0)
 5 月 21 日 18:40:38 localhost.localdomain nv_opof[163922]:EAL：
無效的 NUMA 插槽，預設為 0 May 21 18:40:38 localhost.localdomain
 nv_opof[163922]：EAL：探查 PCI 驅動程式：mlx5_pci (15b3:a2d6) 裝
置：0000:03:00.1 (插槽 0) 5 月 21 日 18:40:38 localhost.localdomain
 nv_opof[163922]:EAL：無效的 NUMA 插槽，預設為 0 May 21 18:40:38
 localhost.localdomain nv_opof[163922]：EAL：探查 PCI 驅動程式：mlx5_pci
 (15b3:a2d6) 裝置：0000:03:00.1 (插槽 0) 5 月 21 日 18:40:39
 localhost.localdomain nv_opof[163922]:EAL：沒有舊版回撥，舊版插槽未建
立 5 月 21 日 18:40:39 localhost.localdomain nv_opof[163922]：EAL：
沒有舊版回撥，舊版插槽未建立 5 月 21 日 18:40:42 localhost.localdomain
 nv_opof[163922]：伺服器監聽：169.254.33.51:3443
```

日誌顯示，智慧型流量卸載正透過 **server listening on** IP 位址，與 VM-Series 防火牆 PA-VM 進行通訊，您會看到 VF 及 DPDK 參數的其他詳細資訊。另外附上新增卸載的 TCP 流程之後產生的日誌。

參考

- NVIDIA BlueField 乙太網路 DPU 使用者指南
- NVIDIA BLUEFIELD DPU 系列軟體 V3.5.0.11563 D
- Nvidia DPU 智慧型流量卸載精靈
- OpenOffload gRPC GITHUB
- PAN-OS 管理員指南

©2023 Palo Alto Networks, Inc.

在 Hyper-V 上設定 VM-Series 防火牆

VM-Series 防火牆可部署於執行 Microsoft Hyper-V 的伺服器上。Hyper-V 會封裝為獨立 Hypervisor 或 Windows Server 附加元件/角色。

- Hyper-V 上支援的部署
- Hyper-V 的系統需求
- Linux 整合服務
- 在 Hyper-V 上安裝 VM-Series 防火牆

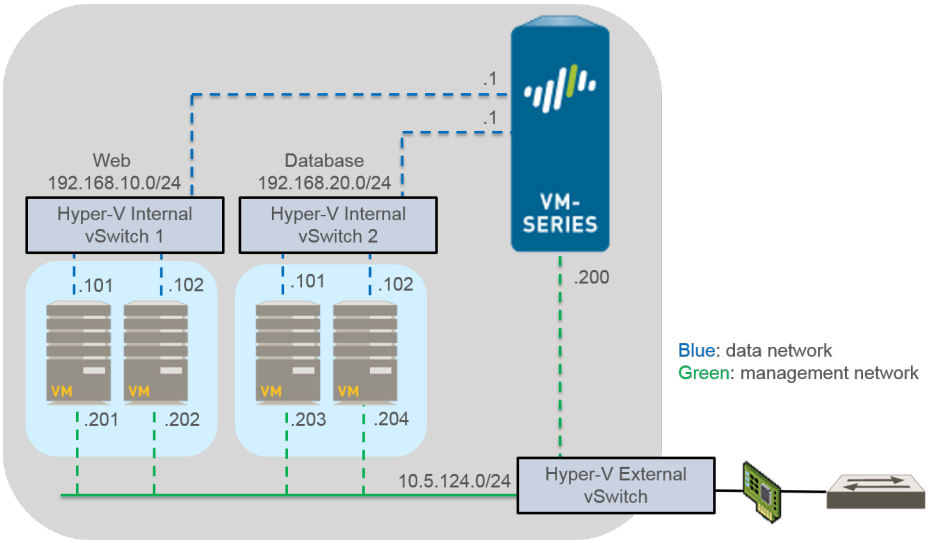
Hyper-V 上支援的部署

您可以在執行 Hyper-V 的主機上部署 VM-Series 的一或多個實例。部署 VM-Series 防火牆的位置視乎網路拓撲而定。VM-Series 支援旁接介面、Virtual Wire、Layer 2 及 Layer 3 介面部署。

- 保護單一 Hyper-V 主機上的流量
- 保護多個 Hyper-V 主機之間的流量

保護單一 Hyper-V 主機上的流量

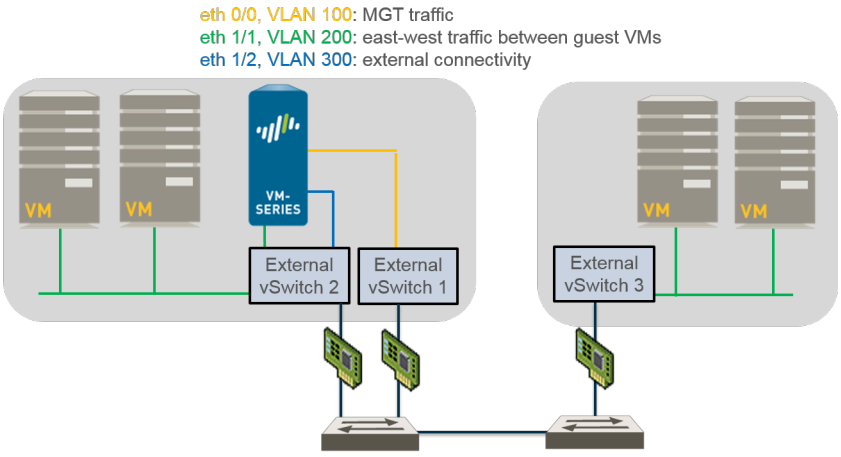
VM-Series 防火牆部署於單一 Hyper-V 主機以及其他來賓 VM 上在下例中，VM-Series 防火牆的 Layer 3 介面以及 VM-Series 和其他來賓 VM 透過 Hyper-V vSwitch 連接。Web 伺服器與資料庫伺服器之間的所有流量均透過防火牆進行路由。僅通過資料庫伺服器的流量或僅通過 Web 伺服器的流量由外部 vSwitch 進行處理，而非透過防火牆路由。



保護多個 Hyper-V 主機之間的流量

您可以部署 VM-Series 防火牆來保護多個 Hyper-V 主機的流量。在下例中，採用 Layer 2 模式部署 VM-Series ，保護來賓 VM 的傳入和傳出流量。單一 VM-Series 防火牆保護兩個 Hyper-V 主機間分佈的四個來賓 VM 之間的流量。VLAN 標籤用於以邏輯方式隔離流量並將流量導向至防火牆。此外，將管理流量置於其自身的外部 vSwitch，可與所有其他流量分離。

©2023 Palo Alto Networks, Inc.



©2023 Palo Alto Networks, Inc.

Hyper-V 的系統需求

VM-Series 需要在 Hyper-V 上進行最少資源配置，因此請確認符合下列要求以確保最佳效能。

- 主機 CPU 必須為具有虛擬化延伸的 64 位元 x86 型 Intel 或 AMD CPU。
- 有關您的 VM-Series 型號的最低硬體需求，請參閱 VM-Series 系統需求。
- 至少兩個網路介面卡。VM-Series 防火牆支援合成網路介面卡，相較模擬網路介面卡，該介面卡可提供更佳效能。Hyper-V 支援多達八個合成網路介面卡。
- 如需瞭解支援的 Windows Server 版本，請參閱相容性矩陣。

  Hyper-V Server 沒有原生圖形使用者介面；所有組態透過 PowerShell 完成。但是，您可使用遠端機器上執行的 Hyper-V 管理員來管理防火牆。如果您使用 Hyper-V 角色附加元件，則可使用 Hyper-V 管理員或 PowerShell 來管理防火牆。
- VM-Series 防火牆支援 SR-IOV/PCI 傳遞。

  僅 *Nvidia/Mellanox (MLX5) SRIOV* 裝置支援 *DPDK*。不支援主幹模式搭配 *SR-IOV*。

©2023 Palo Alto Networks, Inc.

Linux 整合服務

Linux 整合服務 (LIS) 是一個驅動程式及服務套件，可增強 Hyper-V 上 Linux 虛擬機器的效能。VM-Series 防火牆支援下列服務，以改善主機與虛擬機器之間的整合：

- 非失誤性關機—可讓您從 Hyper-V 管理介面的 VM-Series 防火牆執行非失誤性關機，而不必登入來賓。
- **Hyper-V Manager** 的活動訊號—從 Hyper-V 管理介面進行來賓 VM 執行狀態的活動訊號監控。
- **Firewall Management IP** 位址可視性—可讓您使用 Hyper-V Manager 來檢視指派給防火牆上管理介面的 IP 位址。

©2023 Palo Alto Networks, Inc.

在 Hyper-V 上安裝 VM-Series 防火牆

使用本節中的相關指示，在 Hyper-V 主機上部署 VM-Series 防火牆。Palo Alto Networks 支援下載 VHDX 映像檔案所需的帳戶及有效的 VM-Series 授權，以及在 Hyper-V 主機上安裝 VM-Series。如果您尚未使用您的支援帳戶，來註冊在訂購完成電子郵件中收到的容量驗證碼，請參閱註冊 VM-Series 防火牆。完成註冊後，請繼續下列工作：

- 開始之前
- Hyper-V 上的 VM-Series 防火牆的效能調整
- 在 Hyper-V 主機上使用 Hyper-V 管理員佈建 VM-Series 防火牆
- 在 Hyper-V 主機上使用 PowerShell 佈建 VM-Series 防火牆
- 在 VM-Series 防火牆上執行初始組態

開始之前

安裝和設定 VM-Series 防火牆之前，請在設定 VM-Series 防火牆時依需要瞭解並考量下列項目：

- Virtual Switch（虛擬交換器 - vSwitch）類型
- MAC 位址詐騙

Virtual Switch（虛擬交換器 - vSwitch）類型

在安裝 VM-Series 之前，您必須建立提供外部連線所需的 vSwitch，以便進行管理存取，以及對防火牆提供保護之虛擬電腦的輸入和輸出流量進行路由。Hyper-V 可讓您建立三類 vSwitches：

- 外部 **vSwitch**—連結虛擬網路介面卡並提供 vSwitch 對虛擬網路的存取權。
- 內部 **vSwitch**—在虛擬電腦與 Hyper-V 主機之間傳遞流量。此類 vSwitch 不提供虛擬網路連線。
- 私人 **vSwitch**—僅在 Hyper-V 主機上的虛擬電腦間傳遞流量。

管理 VM-Series 防火牆需要外部 vSwitch。其他連線至 VM-Series 防火牆的 vSwitch 可以是任何類型，且視乎網路拓撲而定。

MAC 位址詐騙

如果您部署啟用 Layer 3 模式介面的 VM-Series 防火牆，請確保啟用 Hypervisor 指派的 MAC 位址，以便 Hypervisor 及防火牆可適當處理封包。或者，使用 Hyper-V Manager 針對防火牆上的每個資料平面介面，在虛擬網路介面卡上啟用 MAC 位址詐騙。如需詳細資訊，請參閱 Hypervisor 指派的 MAC 位址。

如果部署啟用 Layer 2 模式或 Virtual-Wire 模式介面的 VM-Series 防火牆，您必須針對防火牆上的每個資料平面，在 Hyper-V 的虛擬網路介面卡上啟用 MAC 位址詐騙。必須進行此設定，以確保當來源 MAC 位址與連出介面 MAC 位址不符時，VM-Series 傳送的封包不會被虛擬網路介面卡丟棄。

©2023 Palo Alto Networks, Inc.

Hyper-V 上的 VM-Series 防火牆的效能調整

Hyper-V 專用 VM-Series 防火牆是高效能裝備，但可能需要調整 Hypervisor，才能達到最佳結果。本節說明一些最佳作法和建議，有助於發揮 VM-Series 防火牆的最佳效能。

- 停用 Virtual Machine（虛擬機器 - VM）佇列
- 在 NUMA 節點中隔離 CPU 資源

停用 **Virtual Machine**（虛擬機器 **- VM**）佇列

對於 Hyper-V 主機上的所有 NIC，Palo Alto Networks 建議停用虛擬機器佇列 (VMQ)。此選項容易引起組態錯誤，啟用時可能會導致網路效能降低。

STEP 1 | 登入 Hyper-V 管理員並選取您的 VM。

STEP 2 | 選取 **Settings**（設定） > **Hardware**（硬體） > **Network Adapter**（網路介面卡） > **Hardware Acceleration**（硬體加速）。

STEP 3 | 在 Virtual machine queue（虛擬機器佇列）下，取消勾選 **Enable virtual machine queue**（啟用虛擬機器佇列）。

STEP 4 | 按一下 **Apply**（套用）儲存您的變更，再按一下 **OK**（確定）結束 VM 設定。

在 **NUMA** 節點中隔離 **CPU** 資源

您可以將來賓 VM 的 CPU 資源隔離到單一非流一記憶體存取 (NUMA) 節點，以改善 Hyper-V 專用 VM-Series 的效能。您可以在 Hyper-V 管理員中選取 **Settings**（設定） > **Hardware**（硬體） > **Processor**（處理器） > **NUMA**，以檢視 VM 的 NUMA 設定。

在 Hyper-V 主機上使用 Hyper-V 管理員佈建 VM-Series 防火牆

使用這些指示在使用 Hyper-V Manager 的 Hyper-V 伺服器上部署 VM-Series 防火牆。

STEP 1 | 下載 VHDX 檔案。

註冊您的 VM-Series 防火牆，並取得 VHDX 檔案。

1. 移至 https://www.paloaltonetworks.com/services/support。
2. 依 **PAN-OS for VM-Series Base Images**（**VM-Series** 基礎映像的 **PAN-OS**） 篩選並下載 VHDX 檔案。例如，PA-VM-HPV-7.1.0.vhdx。

STEP 2 | 設定任何您需要的 vSwitch。

若要建立 vSwitch：

1. 從 Hyper-V 管理員中，選取主機並選取 **Action**（動作） > **Virtual Switch Manager**（虛擬交換器管理員），以開啟 Virtual Switch Manager（虛擬交換器管理員）視窗。
2. 在 **Create virtual switch**（建立虛擬交換器）項下，選取要建立的 vSwitch 的類型（external（外部）、internal（內部）或 private（私人）），然後按一下 **Create Virtual Switch**（建立虛擬交換器）。

©2023 Palo Alto Networks, Inc.

STEP 3 | 安裝防火牆。

1. 在 Hyper-V 管理員上，選取主機並選取 **Action**（動作） > **New**（新增） > **Virtual Machine**（虛擬機器）。在 New Virtual Machine Wizard（新建虛擬電腦 Wizard）中進行下列設定：
   1. 選取 VM-Series 防火牆的 **Name**（名稱）和 **Location**（位置）。VM-Series 防火牆在指定位置儲存 VHDX 檔案。
   2. 選取 **Generation 1**。這是預設選項及唯一支援的版本。
   3. 在 **Startup Memory**（啟動記憶體）中，根據您的 VM-Series 型號的 VM-Series 系統需求指派記憶體。

      請勿啟用動態記憶體；*VM-Series* 防火牆需要配置靜態記憶體。

   4. 設定 **Networking**（網路）。選取外部 vSwitch 以連線至防火牆上的管理介面。
   5. 若要連線 **Virtual Hard Disk**（虛擬硬碟），選取 **Use an existing virtual hard disk**（使用現有虛擬硬碟），然後瀏覽至您之前下載的 VHDX 檔案。
   6. 檢閱摘要並按一下 **Finish**（完成）。
2. 將虛擬 CPU 指派給防火牆。
   1. 選取您建立的 VM，然後導覽至 **Action**（動作） > **Settings**（設定）。
   2. 選取 **Processor**（處理器），根據您的 VM-Series 型號的 VM-Series 系統需求輸入 CPU 數目下限。
   3. 按一下 **OK**（確定）。

STEP 4 | 請為防火牆上的資料平面介面連線至少一個網路介面卡。

1. 選取 **Settings**（設定） > **Hardware**（硬體） > **Add Hardware**（新增硬體），然後選取網路介面卡的 **Hardware type**（硬體類型）。

   不支援傳統網路介面卡及 *SR-IOV*。若已選取，*VM-Series* 防火牆將啟動維護模式。

2. 按一下 **OK**（確定）。

STEP 5 | （選用）如果您不是使用由 Hypervisor 指派 MAC 位址的第 3 層，請在 Hyper-V 上啟用 MAC 位址詐騙。

1. 按兩下資料平面虛擬網路介面卡，然後按一下 **Advanced Settings**（進階設定）。
2. 按一下 **Enable MAC address spoofing**（啟用 **MAC** 位址詐騙）核取方塊，然後按一下 **Apply**（套用）。

STEP 6 | 開啟防火牆電源。

從 **Virtual Machines**（虛擬機器）清單中選取防火牆，然後導覽至 **Action**（動作） > **Start**（啟動）以啟動防火牆。

©2023 Palo Alto Networks, Inc.

在 Hyper-V 主機上使用 PowerShell 佈建 VM-Series 防火牆

使用這些指示在使用 PowerShell 的 Hyper-V 伺服器上部署 VM-Series 防火牆。

STEP 1 | 下載 VHDX 檔案。

註冊您的 VM-Series 防火牆，並取得 VHDX 檔案。

1. 移至 https://www.paloaltonetworks.com/services/support。
2. 依 **PAN-OS for VM-Series Base Images**（**VM-Series** 基礎映像的 **PAN-OS**） 篩選並下載 VHDX 檔案。例如，PA-VM-HPV-7.1.0.vhdx。

STEP 2 | 設定任何您需要的 vSwitch。

使用下列命令建立 vSwitch。為 vSwitch 提供名稱並選取交換器類型。

```
> New-VMSwitch -Name <"switch-name"> -SwitchType <switch-type>
```

STEP 3 | 安裝 VM-Series 防火牆。

1. 建立新的虛擬機器，並根據您的 VM-Series 型號的 VM-Series 系統需求來設定記憶體。

   ```
   > NEW-VM -Name <vm-name> -MemoryStartupBytes 4GB -
   VHDPath <file-path-to-vhdx>
   ```

2. 根據您的 VM-Series 型號的 VM-Series 系統需求來設定處理器數目。

   ```
   > SET-VMProcessor  -VMName <vm-name>  -Count 2
   ```

STEP 4 | 請為防火牆上的管理介面連線至少一個網路介面卡。

在 VM 建立期間，將預設網路介面卡連線至管理 vSwitch。

```
> connect-VMNetworkAdapter -vmname <vm-name> -Name <"network-
adapter-name"> -SwitchName <"management-vswitch">
```

STEP 5 | （選用）如果您不是使用由 Hypervisor 指派 MAC 位址的第 3 層，請在 Hyper-V 上啟用 MAC 位址詐騙。

```
> Set-VMNetworkAdapter -vmname <vm-name> -Name <"network-adapter-
name"> -MacAddressSpoofing On
```

STEP 6 | 開啟防火牆電源。

例如：

```
> Start-VM -vmname <vm-name>
```


©2023 Palo Alto Networks, Inc.

在 VM-Series 防火牆上執行初始組態

使用這些指示執行 VM-Series 防火牆的初始組態。依預設，VM-Series 防火牆使用 DHCP 取得管理介面的 IP 位址。不過，您可以指派靜態 IP 位址。完成初始組態之後，請存取網頁介面來完成進一步的組態設定工作。如果您使用 Panorama 執行中央管理，請參閱《Panorama 管理員指南》以取得使用 Panorama 管理裝置的詳細資訊。

如果您使用啟動程序在 Hyper-V 上執行 VM-Series 防火牆的組態，請參閱在 Hyper-V 上啟動 VM-Series 防火牆。如需啟動程序的一般資訊，請參閱啟動 VM-Series 防火牆。

STEP 1 | 從網路管理員收集必要資訊。

- 管理連接埠 IP 位址
- 網路遮罩
- 預設閘道
- DNS 伺服器 IP 位址

STEP 2 | 存取 VM-Series 防火牆的主控台。

1. 在 Hyper-V Manager 中，選取 VM-Series 防火牆，然後按一下 Actions（動作）清單中 **Connect**（連線）。
2. 使用預設使用者名稱及密碼登入防火牆：**admin/admin**
3. 使用下列命令，進入組態模式：**configure**

STEP 3 | 設定管理介面的網路存取設定。

輸入下列命令：

```
set deviceconfig system type static
```

```
set deviceconfig system ip-address <Firewall-IP> 網路遮罩 <netmask>
default-gateway <gateway-IP> dns-settingservers primary <DNS-IP>
```

其中，*<Firewall-IP>* 是要指定給管理介面的 IP 位址；*<netmask>* 是子網路遮罩；*<gateway-IP>* 是網路閘道的 IP 位址；*<DNS-IP>* 則是 DNS 伺服器的 IP 位址。

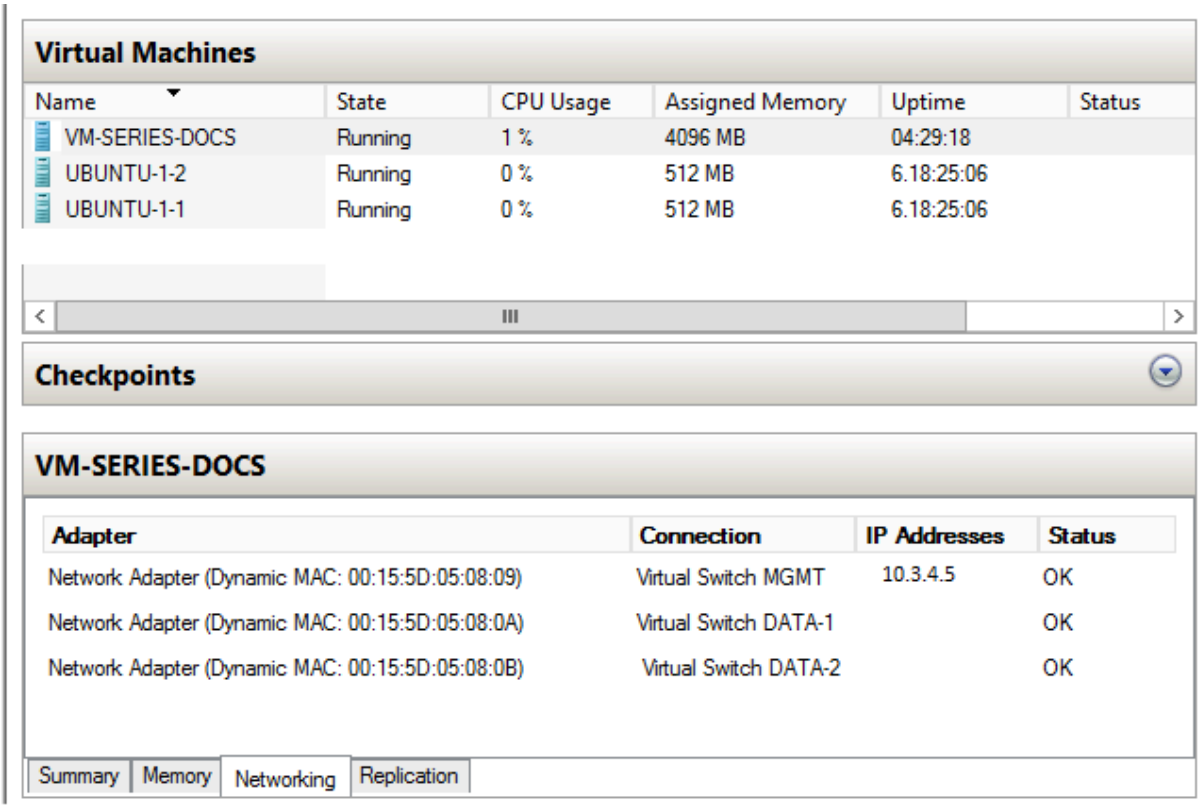
STEP 4 | 提交您的變更並結束組態模式。

1. 輸入 **commit** 。
2. 輸入 **exit**。

©2023 Palo Alto Networks, Inc.

STEP 5 | 確認您可以從 Hyper-V Manager 檢視管理介面 IP 位址。

1. 從 **Virtual Machines**（虛擬電腦）清單中選取 VM-Series 防火牆。
2. 選取 **Networking**（網路）。清單中顯示的第一個網路介面卡用於防火牆的管理存取；清單中的後續介面卡用作防火牆的資料平面介面。



STEP 6 | 驗證執行防火牆管理所需要的外部服務之網路存取權，例如 Palo Alto Networks 更新伺服器。

1. 使用 Ping 公用程式來確認與 Palo Alto Networks 更新伺服器的網路連線，如下列範例所示。確認是否進行了 DNS 解析並且回應中包含更新伺服器的 IP 位址；更新伺服器不會對偵測要求做出回應。

```
admin@PA-220 > ping host updates.paloaltonetworks.com
```

```
PING 更新.paloaltonetworks.com (10.101.16.13) 56(84) 位元組
資料。從 192.168.1.1 icmp_seq=1 無法存取目標主機 從 192.168.1.1
```


©2023 Palo Alto Networks, Inc.

```
 icmp_seq=2 無法存取目標主機 從 192.168.1.1 icmp_seq=3 無法存取目標主機 從 192.168.1.1 icmp_seq=4 無法存取目標主機
```

驗證 *DNS* 解析後，按下 *Ctrl+C* 停止偵測要求。

2. 使用以下 CLI 命令，從 Palo Alto Networks 更新伺服器擷取 防火牆支援權利的相關資訊：

```
request support check
```

如果您可以連線，則更新伺服器將回應防火牆的支援狀態。

STEP 7 | （選用）確認 VM-Series 巨型框架組態不超過 Hyper-V 上支援的最大 MTU。

啟用 Jumbo Frame 時，VM-Series 具有大小為 9216 位元組的預設 MTU。然而，視乎網路介面卡的功能，Hyper-V 主機實體網路介面卡支援的最大 MTU 大小為 9000 或 9014 位元組。若要驗證 Hyper-V 上已設定的 MTU：

1. 在 Windows Server 2012 R2 中，開啟 **Control Panel**（控制台），然後導覽至 **Network and Internet**（網路和網際網路） > **Network and Sharing Center**（網路和共用中心） > **View network status and tasks**（檢視網路狀態及工作）。
2. 按一下清單中的網路介面卡或虛擬交換器。
3. 按一下 **Properties**（屬性）。
4. 按一下 **Configure**（設定）。
5. 在 Advanced（進階）頁籤上，從清單中選取 **Jumbo Packet**。
6. 從 Value（值）下拉式清單中選取 9000 或 9014 位元組。
7. 按一下 **OK**（確定）。

如果您已在 Hyper-V 上啟用巨型框架，請在 VM-Series 防火牆上啟用巨型框架，並設定 MTU 大小以符合 Hyper-V 主機上的設定。

STEP 8 | 存取 VM-Series 防火牆的 Web 介面並設定介面，然後定義安全性規則與 NAT 規則，以安全地啟用您想要保護的應用程式。

請參閱《PAN-OS 管理員指南》。

©2023 Palo Alto Networks, Inc.

在 Azure 上設定 VM-Series 防火牆

Azure 上的 VM-Series 防火牆帶來 Palo Alto Networks 下一代防火牆的安全性功能，如同 Azure Marketplace 中的虛擬機器。VM-Series 防火牆提供了一組完整的安全性功能以確保您的虛擬電腦工作負載和資料受到保護，且防火牆支援的功能與本機安全性功能（如安全性群組、Web 應用程式防火牆與本機連接埠式防火牆）不同。

在 Azure 上，VM-Series 防火牆提供自帶授權 (BYOL) 模式或即付即用 (PAYG) 小時付費模式。Microsoft Azure 可讓您部署防火牆來保障雲端虛擬網路中的工作負載，因此，您可以部署一個公共雲端解決方案，或者延伸內部部署的 IT 基礎結構以建立混合解決方案。

- 關於 Azure 上的 VM-Series 防火牆
- Azure 上支援的部署
- 從 Azure Marketplace 部署 VM-Series 防火牆（解決方案範本）
- 從 Azure China Marketplace 部署 VM-Series 防火牆（解決方案範本）
- Azure 中的 Panorama 協調部署
- 建立 Azure 的自訂 VM-Series 映像
- 使用 Azure 安全性中心建議來保護您的工作負載
- 在 Azure Stack 上部署 VM 系列防火牆
- 啟用 VM-Series 防火牆上的 Azure Application Insights
- Azure 上的 VM 監控
- 在 Azure 上設定主動/被動 HA
- 使用 ARM 範本部署 VM-Series 防火牆
- 部署 VM-Series 和 Azure 應用程式閘道範本
- 保護 Azure 上的 Kubernetes 服務

關於 Azure 上的 VM-Series 防火牆

Azure 上的 VM-Series 防火牆必須使用 Resource Manager 模式部署於虛擬網路 (VNet) 中。在符合 DoD Impact Level 5 資料和 FedRAMP High 標準安全性需求的標準 Azure 公共雲端、Azure China 和 Azure Government（包括 Azure Government 上的 DoD）上，您可以部署 VM-Series 防火牆。

Marketplace 上 Azure 公共雲端、Azure Government 和 Azure DoD 區域的 VM-Series 防火牆，同時支援自帶授權 (BYOL) 模式和即付即用 (PAYG) 小時付費選項（依使用授權）。如需授權詳細資料，請參閱授權類型—VM-Series 防火牆，並請參閱可部署 VM-Series 防火牆的支援的 Azure 區域清單。

若為 Azure China，VM-Series 防火牆僅支援 BYOL 選項。請參閱從 Azure China Marketplace 部署 VM-Series 防火牆（解決方案範本）瞭解工作流程。

您還可在 Azure Stack 上部署 VM-Series 防火牆，Azure Stack 是 Microsoft 的私人雲端解決方案，可讓您使用組織資料中心內的 Azure 服務。有了 Azure Stack，您可構建一個混合雲端解決方案，將公共 Azure 部署與內部部署 Azure Stack 設定統一起來。您可從 Azure Marketplace 下載 VM-Series 防火牆 BYOL，並在 Azure Stack 上將其提供給您的租用戶。如需相關指示，請參閱在 Azure Stack 上部署 VM-Series 防火牆。

- Azure 網路和 VM-Series 防火牆
- Azure 安全中心整合
- Azure 上的 VM-Series 防火牆範本
- Azure 上的 VM-Series 最低系統需求
- 關於 Azure 上的 VM-Series 的高可用性支援

Azure 網路和 VM-Series 防火牆

Azure VNet 基礎結構不需要虛擬電腦針對各子網路配備網路介面。基礎結構包括內部路由表（稱為系統路由），其直接連線至 VNet 內的所有虛擬電腦，從而使流量自動轉送至任何子網路中虛擬電腦。對於不在 VNet 中的目的地 IP 位址，流量將傳送至預設網際網路閘道，或 VPN 閘道（若設定）。為了將流量路由至 VM-Series 防火牆，您必須建立使用者定義的路由 (UDR)，該路由指定流量離開子網路的下一個躍點。此路由將強制目的地為其他子網路的流量前往 VM-Series 防火牆，而非使用系統路由直接存取其他子網路中的虛擬電腦。例如，在具有 Web 層與資料庫層的兩層應用程式中，您可以設定 UDR 透過 VM-Series 防火牆將流量從 Web 子網路導向至 DB 子網路。

在 ***Azure*** 上，***UDR*** 僅用於離開子網路的流量。您無法建立使用者定義的路由來指定流量從網際網路進入子網路，或將流量路由至子網路內虛擬電腦的方式。***UDR*** 可讓您將輸出流量導向至 ***VM-Series*** 防火牆上的介面，一律確保防火牆也可保護流向網際網路的流量。

如需 ***Microsoft Azure*** 的相關文件，請參閱 https://azure.microsoft.com/en-us/documentation/。

部署 VM-Series 防火牆的解決方案範本（在 Azure Marketplace 中提供）有三個網路介面。若要在 Azure 上設定主動/被動 HA，您將需要為 HA2 連結新增其他介面。如果您想要自訂範本，請使用 GitHub 儲存庫中提供的 ARM 範本。

©2023 Palo Alto Networks, Inc.

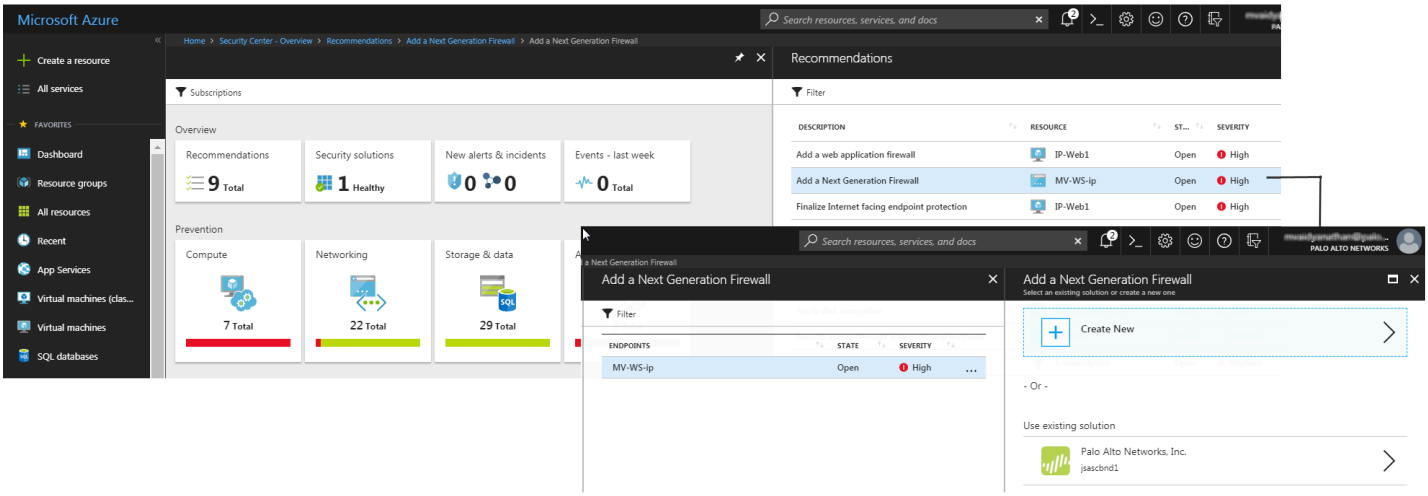
Azure 安全中心整合

Microsoft 已棄用 Azure 安全性中心對合作夥伴安全性解決方案的支援，並將其取代為 Azure Sentinel。

VM-Series 防火牆與 Azure 安全性中心整合，以為在您 Azure 工作負載的安全性角度上的監控和警報，提供統一的檢視。在 Azure 安全性中心上，VM-Series 防火牆可作為保護 Azure 工作負載遠離威脅以及減少任何在公共雲端中保護您企業和智慧財產缺口的合作夥伴安全性解決方案。若要啟用此整合並如同安全性警報一樣直接顯示在 Azure 安全性中心儀表板，則 Azure 上的 VM-Series 防火牆須包含一個日誌轉送設定檔。

若要開始進行，則您需要在 Azure 訂閱上啟用 Azure 安全性中心。接著您會有兩種可啟動此整合的方法：

- 根據 **Azure** 安全性中心儀表板中的建議部署 **VM-Series** 防火牆。



當 Azure 安全性中心儀表板建議您部署 VM-Series 防火牆以保護暴露於網際網路的工作負載時，您僅可將防火牆部署至新的資源群組或現有空的資源群組。這是因為 Azure 目前限制您在現有的資源群組中部署多 NIC 設備。因此，在您部署 VM-Series 防火牆之後，必須手動將其設定為處於您需要保護的工作負載流量的路徑中。

當您從 Azure 安全中心部署防火牆時，防火牆將使用三個網路介面（管理、對外（不信任）和對內（信任））和一個用戶定義的路由 (UDR) 啟動，該路由從信任子網路將所有輸出流量傳送到防火牆上的信任介面，以便防火牆一律檢查 Internet 綁定流量。預設設定包括兩個範例安全性政策規則—在使用預設防毒、反間諜軟體及弱點保護安全性設定檔來檢查流量之後，***outbound-default***（輸出預設）規則允許所有在應用程式預設連接埠上來自信任區域到不受信任區域的流量，而 ***inbound-default***（輸入預設）規則則允許所有來自不受信任區域到信任區域的網頁瀏覽流量。防火牆也會轉送所有使用輸入或輸出規則截獲的檔案至 WildFire 公共雲端以作為分析使用。兩種規則皆包含封鎖所有至 URL 目錄 copyright-infringement、dynamic-dns、extremism、malware, phishing 和 unknown 流量的 URL 篩選設定檔。除了這些安全性設定檔之外，還啟用了兩個安全性政策規則，以在工作階段結束時記錄並將威脅和 WildFire 提交日誌作為安全警示轉送到 Azure 安全中心儀表板。

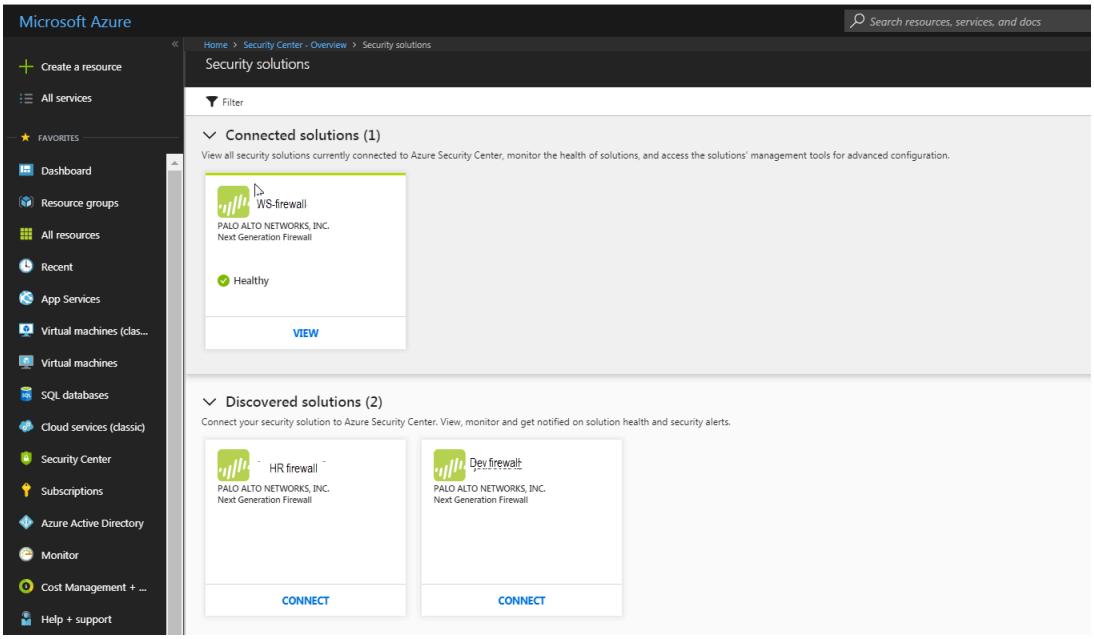
為了實際在與您要保護的工作負載相同的資源群組中使用這種整合和根據 Azure 安全性中心的建議部署 VM-Series 防火牆，您可以使用對 Internet 公開的公共 IP 位址暫存工作負載。當 Azure 安全性中心偵測到安全性風險時，其將觸發部署下一代防火牆的建議，然後您可將 VM-

©2023 Palo Alto Networks, Inc.

Series 防火牆部署至新的資源群組，且您之後可新增工作負載至此資源群組。之後您必須刪除佈置用於觸發建議的工作負載。

- 選取您已部署的 **VM-Series** 防火牆以保護您的工作負載。如果您有標準的 Azure 安全性中心訂閱層，Azure 安全性中心將發現並顯示您從 Azure Marketplace 部署或使用 Azure CLI、PowerShell 或 ARM 範本進行自訂部署的所有現有 VM-Series 防火牆。Azure 訂閱中的防火牆在 Azure 安全性中心儀表板上被分組到安全性解決方案中。

  Microsoft Azure 不支援透過免費層訂閱發現現有的防火牆。



至從 Azure 安全性中心連線現有的 VM-Series 防火牆，您必須設定 Linux 虛擬機器並設定 Syslog 轉送，以將常見事件格式的防火牆日誌作為警報轉送到 Azure 安全中心。其他組態可提供單一窗口檢視來監控您的所有 Azure 資產。

轉送大量日誌到 ***Azure*** 安全性中心可能會讓您有額外的訂閱成本。

Azure 上的 VM-Series 防火牆範本

您可以使用範本在 Azure 上部署 VM-Series 防火牆。Palo Alto Networks 提供兩類範本—解決方案範本與 ARM 範本。

©2023 Palo Alto Networks, Inc.

- **Azure Marketplace** 中的解決方案範本—解決方案範本可於 Azure Marketplace 下載，讓您能夠透過 Azure 入口網站部署 VM-Series 防火牆。在所有區域中（Azure China 除外），您可以使用現有資源群組及儲存帳戶（或建立新的）部署具有下列預設設定的 VM-Series 防火牆：
  - VNet CIDR 10.8.0.0/16；您可以將 CIDR 自訂為不同的私人 IP 位址範圍。
  - 三個子網路—10.8.0.0/24（管理）、10.8.1.0/24（不信任）、10.8.2.0/24（信任）
  - 三個網路介面，每個子網路中一個。如果您自訂 VNet CIDR，子網路範圍將對應至您的變更。

  若要使用解決方案範本，請參閱從 Azure Marketplace 部署 VM-Series 防火牆（解決方案範本），若為 Azure China，請參閱從 Azure China Marketplace 部署 VM-Series 防火牆（解決方案範本）。
- **GitHub** 儲存庫中的 **ARM** 範本—除了 Marketplace 部署，Palo Alto Networks 還在 GitHub 儲存庫中提供 Azure Resource Manager 範本，以簡化在 Azure 上部署 VM-Series 防火牆的程序。
  - 使用 ARM 範本部署 VM-Series 防火牆—ARM 範本包括兩個 JSON 檔案（範本檔案及參數檔案），可幫助您透過簡單、協調的操作部署及部署 VNet 中的所有資源。這些範本是依據按現況、盡全力的支援原則來提供。

    如果您想要使用 *Azure CLI* 來尋找 *Palo Alto Networks* 提供的所有映像，您需要下列詳細資訊來完成命令（顯示 *VM* 映像清單）：
    - 發佈者：*paloaltonetworks*
    - 供應項目：*vmseries-flex*
    - *SKU*：*byol*、*bundle1*、*bundle 2*
    - 版本：*10.0.0* 或最新版本
  - 部署 VM-Series 和 Azure 應用程式閘道範本來支援相應放大安全性架構，在一對（外部和內部）Azure 負載平衡器 VM-Series 和 Azure 應用程式閘道之間，使用兩個 VM-Series 伺服器，以保護您的網際網路型 web 應用程式。此範本目前不適用於 Azure China。
  - 使用 ARM 範本，將 VM-Series 防火牆部署至現有資源群組，例如您要在 Azure 上設定主動/被動 HA時。

除了 Palo Alto Networks 官方支援政策所涵蓋的上述 ARM 範本之外，Palo Alto Networks 還會在 Palo Alto Networks GitHub 儲存庫中提供社群支援的範本，使您能夠開始探索 Azure 上的雲端自動化和調整規模之旅中可用的解決方案。

Azure 上的 VM-Series 最低系統需求

您必須僅在 Azure Resource Manager (ARM) 模式中部署 VM-Series 防火牆；不支援經典模式（基於服務管理的部署）。Azure 上的 VM-Series 防火牆必須符合下列需求：

- 下列類型的 Azure Linux VM—支援的型號。

  這些類型包括 Accelerated Networking (SR-IOV) 支援。

©2023 Palo Alto Networks, Inc.

- 有關部署 VM-Series 防火牆所需的記憶體、磁碟和 CPU 核心數，請參閱 VM-Series 系統需求。

  您可以額外新增 40GB 到 8TB 的磁碟空間以用於日誌記錄。VM-Series 防火牆會在可用時使用 Azure 受管理的磁碟；但不使用 Azure 針對某些實例類型所提供的臨時磁碟。
- 最多八個網路介面 (NIC)。管理存取需要一個主要介面，資料流量最多需要七個介面。

  在 Azure 上，因為虛擬機器不需要每個子網路中都有網路介面，所以您可以設定具有三個網路介面的 VM-Series 防火牆（一個用於管理流量，兩個用於資料平面流量）。如果要在防火牆上建立基於區域的原則規則，除了管理介面，您還需要至少兩個資料平面介面，以便將一個資料平面介面指派給信任區域，另一個資料平面介面指派給不受信任區域。針對 HA 部署，您將需要另一個介面，以用於 HA 對等之間的 HA2 連結。

  由於 Azure VNet 是第 3 層網路，Azure 上的 VM-Series 防火牆僅支援第 3 層介面。

關於 Azure 上的 VM-Series 的高可用性支援

若要確定可用性，您可以使用工作階段同步處理在傳統設定中在 Azure 上設定主動/被動 HA，或是，對於小型和大型部署，請採用相應放大架構來使用雲端原生負載平衡器，例如 Azure 應用程式閘道或 Azure 負載平衡器，將流量分散至一組健康情況良好的防火牆實例。如需詳細資料，請參閱部署 VM-Series 和 Azure 應用程式閘道範本。

Azure Service 上的 VM-Series 的服務主體權限

若要讓 Panorama 與 Azure API 互動並收集工作負載的相關資訊，您需要建立 Azure Active Directory 和服務主體，且都必須有權限向 Azure AD 驗證並於您的訂閱內存取資源。

若要建立 Active Directory（主動式目錄 - AD）應用程式和服務主體，請遵循操作說明：使用入口網站建立可存取資源的 Azure AD 應用程式和服務主體中的指示。在產生應用程式的過程中，有一個步驟「將應用程式指派給角色和將「讀者」IAM 角色指派給應用程式。

如果您沒有必要權限來建立和註冊 AD 應用程式，請要求 Azure AD 或訂閱管理員建立服務主體。

註冊應用程式之後，請記錄這些值，供稍後在 Azure 專用 Panorama 外掛程式中輸入：

- 應用程式 ID
- 秘密金鑰（產生秘密金鑰時請記錄下來，離開頁面後就看不到秘密金鑰）。
- 租戶 ID

權限

下表列出所需的最低內建角色，以及可供您自訂角色的細微權限。

若要支援	權限
Azure 高可用性	請參閱 在 Azure 上設定主動/被動 HA。
Azure Application Insights	“**Microsoft.Authorization/*/read**”、 “**Microsoft.Network/networkInterfaces/***”、 “**Microsoft.Network/networkSecurityGroups/***”、

©2023 Palo Alto Networks, Inc.

若要支援	權限
啟用 VM-Series 防火牆上的 Azure Application Insights	“Microsoft.Network/virtualNetworks/*”、 “Microsoft.Compute/virtualMachines/read”
VM 監控 設定 Azure 外掛程式在 Panorama 上監控	服務主體需要的最低角色是**Reader**（讀者）。或者，您可以新增下列自訂權限： “Microsoft.Compute/virtualMachines/read”、 “Microsoft.Network/networkInterfaces/read”、 “Microsoft.Network/virtualNetworks/read”、 “Microsoft.Network/locations/serviceTags/read” "Microsoft.Network/loadBalancers/read"、 "Microsoft.Network/publicIPAddresses/read" "Microsoft.Resources/subscriptions/resourcegroups/read"、
Panorama 協調部署 建立自訂角色並與 Active Directory（主動式目錄 - AD）建立關聯	“Microsoft.Resources/subscriptions/resourcegroups/*”、 “Microsoft.Resources/deployments/write”、 “Microsoft.Resources/deployments/operationStatuses/read”、 “Microsoft.Resources/deployments/read”、 “Microsoft.Resources/deployments/delete”
	"Microsoft.Network/publicIPPrefixes/write"、 "Microsoft.Network/publicIPPrefixes/read"、 "Microsoft.Network/publicIPPrefixes/delete"、 "Microsoft.Network/publicIPAddresses/write"、 "Microsoft.Network/publicIPAddresses/read"、 "Microsoft.Network/publicIPAddresses/delete"、 "Microsoft.Network/publicIPAddresses/join/action"、
	"Microsoft.Network/natGateways/write"、 "Microsoft.Network/natGateways/read"、 "Microsoft.Network/natGateways/delete"、

©2023 Palo Alto Networks, Inc.

若要支援	權限
	"Microsoft.Network/natGateways/join/action"、
	"Microsoft.Network/virtualNetworks/read"、 **"Microsoft.Network/virtualNetworks/write"**、 **"Microsoft.Network/virtualNetworks/delete"**、 **"Microsoft.Network/virtualNetworks/subnets/write"**、 **"Microsoft.Network/virtualNetworks/subnets/read"**、 **"Microsoft.Network/virtualNetworks/subnets/delete"**、 **"Microsoft.Network/virtualNetworks/subnets/join/action"**、
	"Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read"、
	"Microsoft.Network/networkSecurityGroups/write"、 **"Microsoft.Network/networkSecurityGroups/read"**、 **"Microsoft.Network/networkSecurityGroups/delete"**、 **"Microsoft.Network/networkSecurityGroups/join/action"**、
	"Microsoft.Network/loadBalancers/write"、 **"Microsoft.Network/loadBalancers/read"**、 **"Microsoft.Network/loadBalancers/delete"**、 **"Microsoft.Network/loadBalancers/probes/join/action"**、 **"Microsoft.Network/loadBalancers/backendAddressPools/join/action"**、 **"Microsoft.Network/loadBalancers/frontendIPConfigurations/read"**、
	"Microsoft.Network/locations/serviceTags/read"、
	"Microsoft.Network/applicationGateways/read"、

©2023 Palo Alto Networks, Inc.

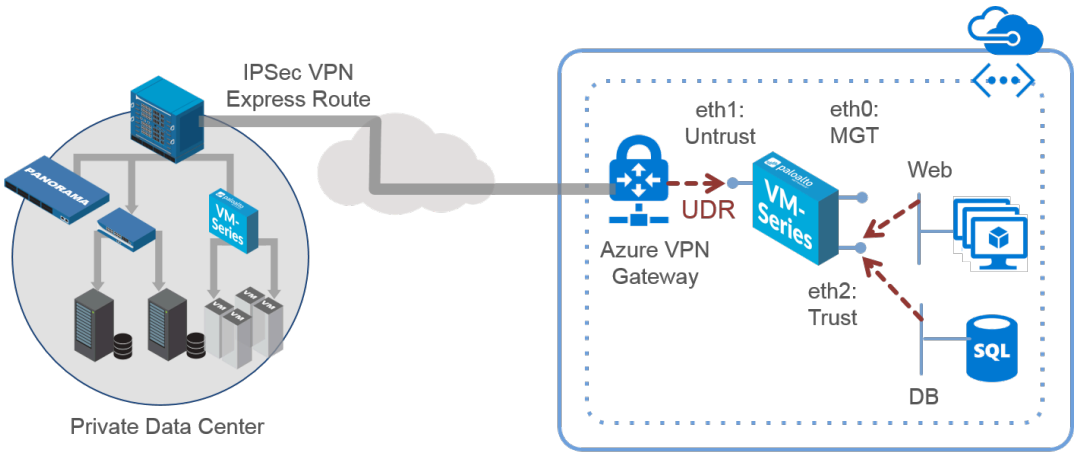
若要支援	權限
	"Microsoft.Network/networkInterfaces/read"、
	"Microsoft.Compute/virtualMachineScaleSets/write"、 **"Microsoft.Compute/virtualMachineScaleSets/read"**、 **"Microsoft.Compute/virtualMachineScaleSets/delete"**、 **"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read"**、
	"Microsoft.Compute/virtualMachines/read"、
	"Microsoft.Compute/images/read"、
	"Microsoft.insights/components/write"、 **"Microsoft.insights/components/read"**、 **"Microsoft.insights/components/delete"**、
	"Microsoft.insights/autoscalesettings/write"

©2023 Palo Alto Networks, Inc.

Azure 上支援的部署

在下列案例中，使用 Azure 上的 VM-Series 防火牆保障網路使用者：

- 混合及 **VNet** 至 **VNet** - Azure 上的 VM-Series 防火牆可讓您使用 IPSec 及 ExpressRoute 將實體資料中心/私人雲端安全地延伸至 Azure。如果您已將網路分段且在單獨的 VNet 中部署工作負載，為了增強資料中心的安全性，您可以使用 IPSec 通道和允許應用程式流量的政策，以保護 VNet 之間流動的流量。



- 子網路間—VM-Series 防火牆可將 VNet 中的防火牆置於前面，抵禦多層架構應用程式間子網路間流量的橫向威脅。
- 閘道—VM-Series 防火牆用作 VNet 閘道，以保護 Azure Virtual Network (VNet) 中的網際網路對向部署。VM-Series 防火牆可保障目的地為 VNet 中伺服器的流量，此外還可抵禦多層架構應用程式間子網路間流量的橫向威脅。
- **GlobalProtect**—使用 Azure 基礎結構快速、輕鬆地將 VM-Series 防火牆部署為 GlobalProtect™，並將閘道安全性原則延伸至遠端使用者及裝置，不受位置影響。

您可以繼續從 Azure Marketplace（解決方案範本）部署 VM-Series 防火牆、在 Azure Stack 上部署 VM-Series 防火牆，或在 Azure 中協調 VM-Series 防火牆部署。

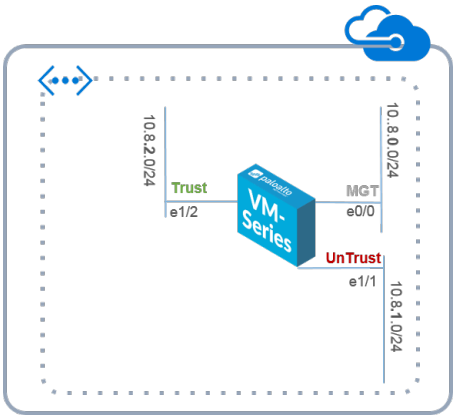
您也可以了解可用來部署防火牆的 Azure 上的 VM-Series 防火牆範本。

如需啟動程序的相關資訊，請參閱在 Azure 上啟動 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

從 Azure Marketplace 部署 VM-Series 防火牆（解決方案範本）

下列指示說明如何為可在 Azure® Marketplace 和 Azure Government Marketplace 下載的 VM-Series 防火牆部署解決方案範本。若要使用 GitHub 儲存庫中提供的可自訂 Azure Resoruce Manager (ARM) 範本，請參閱使用 ARM 範本部署 VM-Series 防火牆。



All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 設定 Azure 帳戶。

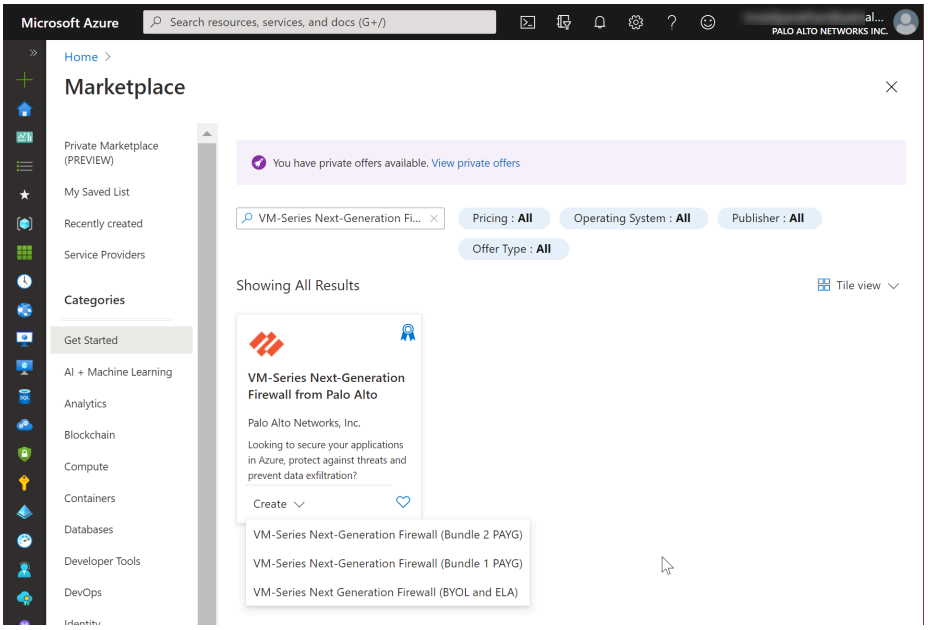
1. 若您沒有帳戶，請建立一個 Microsoft® 帳戶。
2. 使用您的 Microsoft 帳戶認證登入 Azure 入口網站（**`https://portal.azure.com`** 或 **`https://portal.azure.us`**）。

   如果您使用試用訂閱，則可能需要開啟支援要求（***Help + Support***（說明 + 支援） ***> New Support Request***（新增支援要求）），以增加配置的 *VM* 核心配額。

©2023 Palo Alto Networks, Inc.

STEP 2 | 在 Azure Marketplace 中尋找 VM-Series 解決方案範本。

1. 選取 **Marketplace** > **Virtual Machines**（虛擬機器）。
2. 搜尋 Palo Alto Networks®，VM-Series 防火牆產品清單即會顯示。對於 BYOL（自帶授權）與 PAYG（即付即用）型號的差異，請參閱 公共雲端專用 VM-Series 防火牆授權。



3. 選取產品並 **Create**（建立）新的 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

STEP 3 | 部署防火牆。

1. 設定好防火牆的基本設定。

   1. 選取 Azure **Subscription**（訂閱）。
   2. 建立新的資源群組或選取現有為空的資源群組。資源群組將保留與此部署中的 VM-Series 防火牆相關聯的所有資源。

      Azure 已不支援為啟用多個網路介面控制器 *(NIC)* 的 *Marketplace* 解決方案選取現有資源群組。若要將防火牆部署至現有資源群組，請使用 GitHub 儲存庫中的 *ARM* 範本，或使用您自己的自訂 *ARM* 範本。
   3. 選取您正在部署防火牆的 Azure **Region**（地區）。
   4. 輸入防火牆管理員的 **Username**（使用者名稱）。
   5. 選取 **Authentication type**（驗證類型）—密碼或 SSH 公共金鑰。

      如果您打算在 *FIPS-CC* 操作模式下使用防火牆，則必須啟用 *SSH* 金鑰驗證。雖然您可以利用使用者名稱和密碼來部署 *VM-Series* 防火牆，但將操作模式改為 *FIPS-CC* 之後，就無法以使用者名稱和密碼來驗證身分。重設為 *FIPS-CC* 模式之後，您必須使用 *SSH* 金鑰登入，才能設定使用者名稱和密碼，供後續用來登入防火牆網頁介面。如需有關建立 *SSH* 金鑰的詳細資訊，請參閱 Azure 文件。
   6. 輸入 **Password**（密碼）（最多 31 個字元）或複製並貼上 **SSH public key**（**SSH** 公開金鑰），以保護防火牆的管理存取安全。
2. 設定網路。

   1. 選取現有 Azure 虛擬網路 (VNet) 或建立新的 VNet，然後輸入 VNet 的 IP 位址空間。依預設，Classes Inter-Domain Routing（無類別區隔路由，CIDR）的 IP 位址為 10.8.0.0/16。
   2. 設定網路介面的子網路。

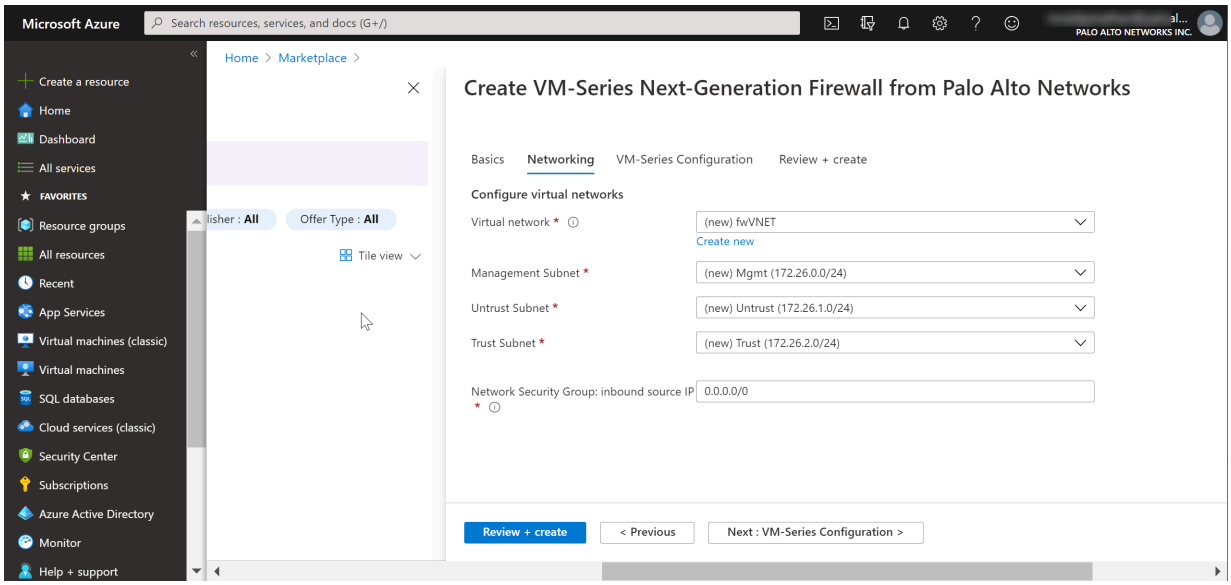
      若您使用預設子網路，則必須檢閱組態。如果您使用現有 VNet，則必須設定三個子網路：分別用於管理、信任和不受信任的介面。如果您建立新的 VNet，請驗證或變

©2023 Palo Alto Networks, Inc.

更每個子網路的首碼。預設子網路包括管理子網路 10.8.0.0/24、不受信任的子網路 10.8.1.0/24 和信任子網路 10.8.2.0/24。

3. 輸入可存取 VNet 的來源 IP 位址或 IP 範圍（包括 CIDR 區塊）。**Network Security Group: inbound source IP**（網路安全性群組：輸入來源 **IP**）可讓您限制 Azure VNet 的輸入存取。

   限制存取防火牆。確保您提供的 *CIDR* 區塊對應於您的專用管理 *IP* 位址或網路。請勿讓允許的來源網路範圍過大，也決不要將允許的來源設定為 *0.0.0.0/0*。在您於範本上設定 *IP* 位址之前，請先驗證 *IP* 位址，以確保不會封鎖您自己。



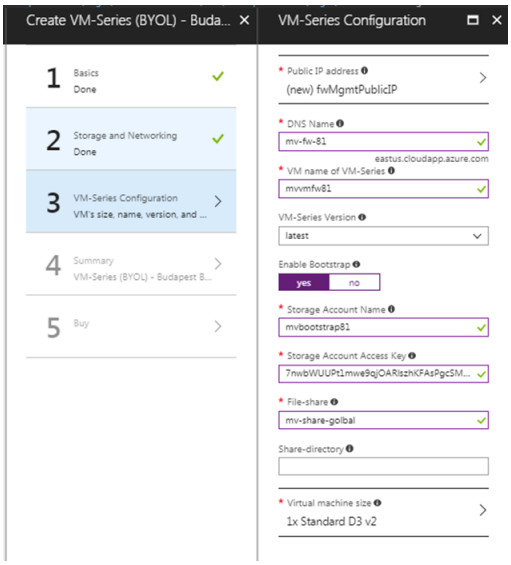
3. 定義防火牆的管理存取。

   1. 使用預設變數 ((new) fwMgmtPublicIP)) 將 **Public IP address**（公共 **IP** 位址）指派給防火牆的管理介面 (`eth0`)。

      管理介面上不支援 *Azure* 加速網路。

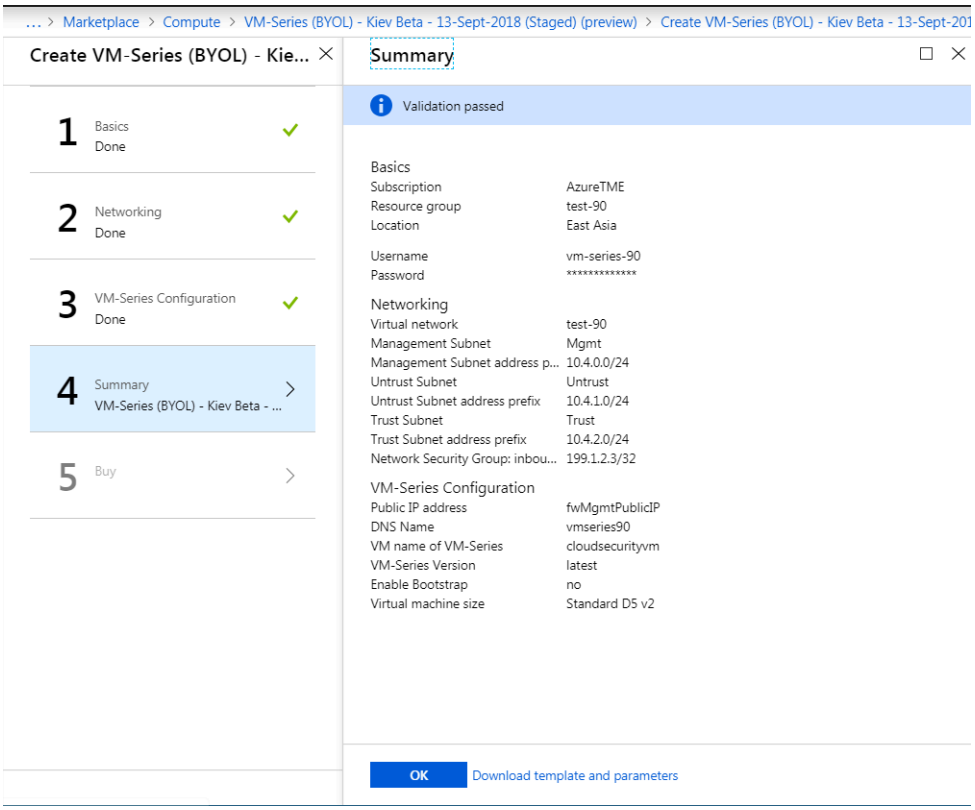
   2. 輸入首碼以使用 DNS 名稱存取防火牆。您必須將輸入的首碼與螢幕上顯示的尾碼組合在一起，才能存取防火牆的 Web 介面。例如：***<yourname><your-region>*.cloudapp.azure.com**
   3. 選取最新的 **VM-Series Version**（**VM-Series** 版本）。
   4. 輸入顯示名稱以識別資源群組中的 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.



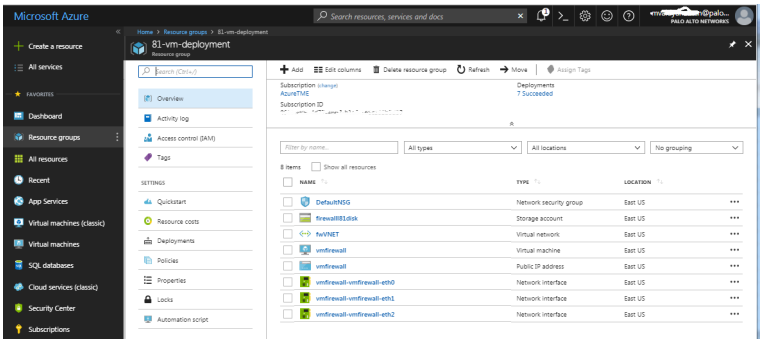
4. 新增此資料以在啟動時設定防火牆。請參閱 在 Azure 上啟動載入 VM-Series 防火牆。
   1. 選取 **yes**（是）以**Enable Bootstrap**（啟用啟動）。
   2. 輸入包含 啟動套件 的 **Storage Account Name**（儲存帳戶名稱）。
   3. 輸入**Storage Account Access Key**（儲存帳戶存取金鑰）。防火牆需要此存取金鑰以驗證儲存帳戶並存取其內儲存的檔案。
   4. 新增 **File share name**（檔案共享名稱），這是您必須在啟動防火牆時上傳的檔案。儲存帳戶必須位於您部署防火牆相同的地方，且必須有用來啟動的正確檔案夾架構。
   5. 根據您的需求選取 Azure 虛擬電腦層級及大小。使用 **Change size**（變更大小）連結以檢視支援的實例類型，以及檢閱 Azure 上的 VM-Series 最低系統需求。
5. 檢閱摘要，並按一下 **OK**（確定）。然後接受使用條款及隱私權政策，然後按一下 **Create**（建立）以啟動防火牆。

©2023 Palo Alto Networks, Inc.



6. 確認您已成功部署 VM-Series 防火牆。

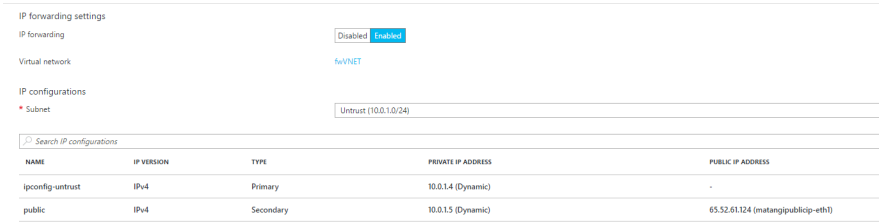
   1. 選取 **Dashboard**（儀表板） > **Resource Groups**（資源群組），然後選取資源群組。
   2. 選取您的資源群組並參閱 **Overview**（概觀）以瞭解資源成功部署的詳細狀態。



 ©2023 Palo Alto Networks, Inc.

STEP 4 | 附加公共 IP 位址給 VM-Series 防火牆的不受信任介面。當您建立新的公共 IP 位址時，您會從 Microsoft 擁有的大量 IP 位址中取得位址，因此，您無法選取特定的位址。可指派給介面的公共 IP 位址數目上限是根據您的 Azure 訂用帳戶。

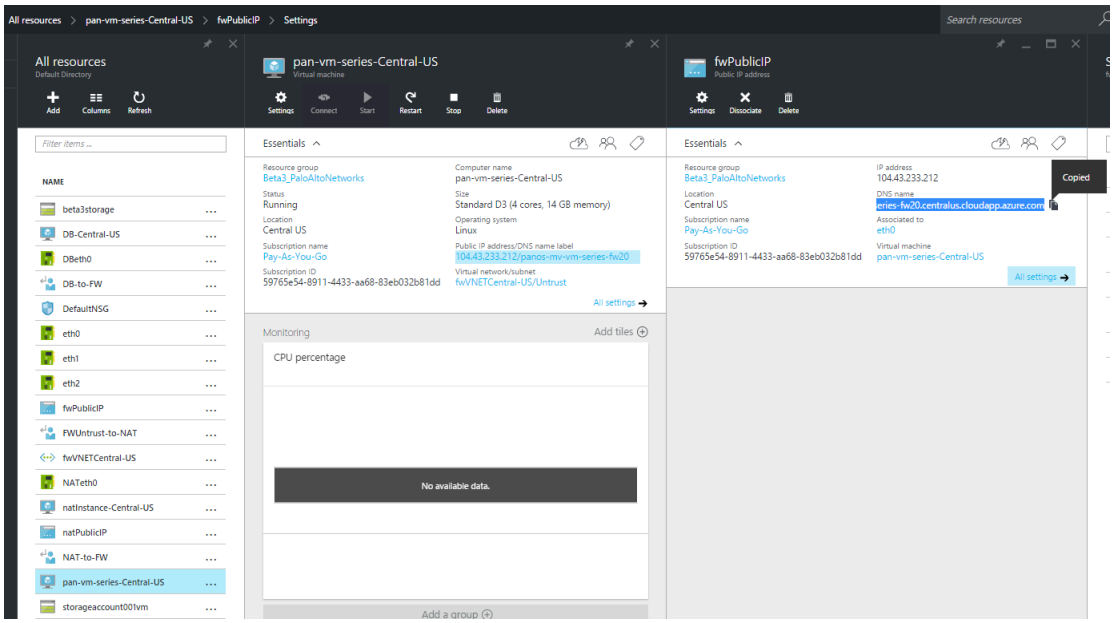
1. 在 Azure 入口網站上，選取您要新增公共 IP 位址的網路介面（例如 **eth1** 介面）。
2. 選取 **IP Configurations**（**IP** 設定） > **Add**（新增），並針對 [Public IP address（公共 IP 位址）] 選取 **Enabled**（已啟用）。建立新的公共 IP 位址，或選取您可用的公共 IP 位址。
3. 確認您可以檢視與介面相關聯的次要 IP 位址。



將次要 *IP* 位址附加至網路介面時，*VM-Series* 防火牆不會自動取得已指派給介面的私人 *IP* 位址。您需要利用 *VM-Series* 防火牆介面來手動設定私人 *IP* 位址。請參閱將資料平面網路介面設為防火牆上的第 3 層介面。

STEP 5 | 登入防火牆的網頁介面。

1. 在 Azure 入口網站的 **All Resources**（所有資源）中，選取 VM-Series 防火牆，然後檢視防火牆的完整 DNS 名稱。



1. 使用 Web 瀏覽器的安全連線 (https)，登入防火牆的 DNS 名稱。
2. 輸入您在參數檔案中定義的使用者名稱密碼。您將看到一則憑證警告，沒關係—繼續前往網頁。

©2023 Palo Alto Networks, Inc.

STEP 6 | 啟動 VM-Series 防火牆上的授權。

對於 **BYOL** 版本

1. 建立支援帳戶。
2. 註冊 VM-Series 防火牆（使用驗證碼）。
3. 在防火牆網頁介面上，選取 **Device**（裝置） > **Licenses**（授權），然後選取 **Activate feature using authentication code**（使用驗證碼啟動功能）。
4. 輸入您在支援入口網站上註冊的容量驗證碼 (*auth-code*)。防火牆將連線至更新伺服器 (`updates.paloaltonetworks.com`)，並自動下載授權及重新啟動。
5. 重新登入 Web 介面並在 **Dashboard**（儀表板）上確認下列各項：
   - **Serial#**（序號）中顯示有效的序號。

     如果顯示 `Unknown` 一詞，則意味防火牆未經授權。若要在防火牆上檢視流量日誌，您必須安裝有效的容量授權。
   - **VM Mode**（**VM** 模式）顯示為 Microsoft Azure。

對於 **PAYG** 版本

1. 建立支援帳戶。
2. 註冊依使用授權版公共雲端專用 VM-Series 防火牆（無驗證碼）。

STEP 7 | 將資料背板網路介面設為防火牆上的 Layer 3 介面。

如果您在單一伺服器上使用不同 IP 位址和 SSL 憑證來代管多個網站或服務，您可能需要在 VM-Series 防火牆介面上設定多個 IP 位址。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）。
2. 按一下 **ethernet 1/1**，然後依照以下所述設定：
   - 將 **Interface Type**（介面類型）設為**Layer3**（預設值）。
   - 在 **Config**（設定）頁籤上，將介面指派給預設路由器。
   - 另，在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。定義稱為 **`UnTrust`** 的新區域，然後按一下 **OK**（確定）。
   - 在 **IPv4** 頁籤上，若您在介面上僅計劃指派一個 IP 位址，則選取 **DHCP Client**（**DHCP** 用戶端）—防火牆將自動取得 ARM 範本內指派的私人 IP 位址。如果

©2023 Palo Alto Networks, Inc.

您打算指派多個 IP 位址，請選取 **Static**（靜態），並手動輸入在 Azure 入口網站上指派給介面的主要和次要 IP 位址。

- 停用（清除）**Automatically create default route to default gateway provided by server**（自動建立伺服器所提供之預設閘道的預設路由）以確保此介面所處理的流量不會直接流向 VNet 中的預設閘道。

3. 按一下 **ethernet 1/2**，然後依照以下所述設定：
   - 將 **Interface Type**（介面類型）設為**Layer3**（預設值）。
   - 將**Security Zone**（安全性區域）設定為**Trust**（信任）。
   - 設定 **IP address**（**IP** 位址） **DHCP Client**（**DHCP** 用戶端）或**Static**（靜態）。
   - 停用（清除）**Automatically create default route to default gateway provided by server**（自動建立伺服器所提供之預設閘道的預設路由）以確保此介面所處理的流量不會直接流向 VNet 中的預設閘道。
4. **Commit**（提交）您的變更並確認介面的連結狀態為啟動。
5. 在 VM-Series 防火牆的虛擬路由器上，為防火牆需要路由的任何網路新增靜態路由。

   例如，若要為防火牆保護的伺服器新增至目的地子網路的預設路由：
   - 選取 **Network**（網路） > **Virtual Router**（虛擬路由器） > **default**（預設） >
   - 選取 **Static Routes**（靜態路由） > **IPv4**，並為目的地伺服器新增下一躍點 IP 位址。您可將 x.x.x.1 設定為所有流量的下一躍點 IP 位址（從介面 ethernet1/1 流向 0.0.0.0/0）。

STEP 8 | 根據您的特定部署來設定防火牆。

- 閘道—在不受信任的區域前面部署第三方負載平衡器。
- 混合與 **Inter-VNet**—在不受信任的區域前面部署 Azure VPN 閘道或 NAT 虛擬機器。
- **Inter-Subnet**—在 VM 系列防火牆上，新增區域內安全性規則，以允許基於子網路的流量附加至 Trust（信任）介面。
- **GlobalProtect™**—在不信任區域前部署 NAT 虛擬電腦。

STEP 9 | 將流量導向至 VM-Series 防火牆。

1. 為了確保 VM-Series 防火牆可保護 Azure 資源群組內所有流量的安全，請在防火牆上設定靜態路由。
2. 設定使用者定義路由，將所有流量導向通過 VM-Series 防火牆上的介面。如需詳細資訊，請參閱有關 UDR 的 Azure 文件。

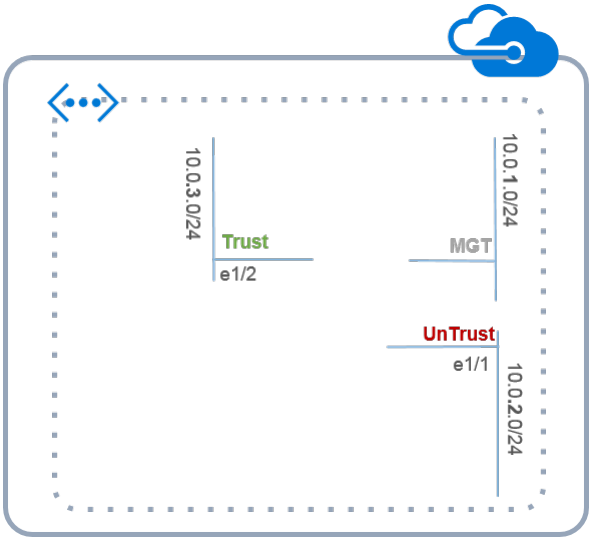
   內部子網路上的使用者定義路由必須透過 Trust（信任）介面傳送所有流量。不信任側上的使用者定義路由透過 VM-Series 防火牆上的不信任介面從網際網路導向所有流量。網際網路流量可能來自 Azure 應用程式閘道或 Azure 負載平衡器，或者，如果是在連線內部網路與 Azure 雲端的混合部署中，則可能是通過 Azure VPN 閘道而來。

STEP 10 | 若要將 PAN-OS® 度量發佈至 Azure Application Insight，請參閱 啟用 VM-Series 防火牆上的 Azure Application Insights。

©2023 Palo Alto Networks, Inc.

從 Azure China Marketplace 部署 VM-Series 防火牆（解決方案範本）

下列指示顯示如何為 Azure China Marketplace 中提供的 VM-Series 防火牆部署解決方案範本。Azure China Marketplace 僅支援 BYOL 模式的 VM-Series 防火牆。您可以將防火牆部署在空的現有資源群組中，或部署到新的資源群組。此範本中的預設 VNet 是 10.0.0.0/16，而所部署的 VM-Series 防火牆具有 3 個網路介面：一個管理介面和兩個資料平面介面，如下所示。若要使用 GitHub 儲存庫中提供的可自訂 ARM 範本，請參閱使用 ARM 範本部署 VM-Series 防火牆。



All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 設定 Azure 帳戶。

1. 建立 Microsoft 帳戶。
2. 使用您的 Microsoft 帳戶認證登入 Azure 入口網站 (**`https://portal.azure.com`**)。

   如果您使用試用訂閱，則可能需要開啟支援要求（***Help + Support***（說明 + 支援） > ***New Support Request***（新增支援要求）），以增加配置的 *VM* 核心配額。

©2023 Palo Alto Networks, Inc.

STEP 2 | 在 Azure Marketplace 中尋找 VM-Series 解決方案範本。

1. 在 Azure China Marketplace (https://market.azure.cn) 上搜尋 Palo Alto Networks。將會顯示 VM-Series 防火牆各種 PAN-OS 版本的供應項目。



2. 選取供應項目，然後按一下 **Immediate deployment of**（立即部署）。

STEP 3 | 部署防火牆。

1. 選取 Azure **Subscription**（訂閱）。
2. 選取資源群組來保留與此部署中的 VM-Series 防火牆相關聯的所有資源。

   您可以將 ***VM-Series*** 防火牆部署至新的資源群組，或現有空的資源群組。若要將防火牆部署至含有其他資源的現有資源群組，請使用 GitHub 儲存庫中的 ***ARM*** 範本，或您自己的自訂 ***ARM*** 範本。確保現有資源符合您在 ***ARM*** 範本中提供的參數值。

   1. 如果您建立新的資源群組，請輸入資源群組的名稱，並選取您要部署防火牆的 Azure China 區域。
   2. 如果您選取現有資源群組，請為此資源群組選取 Azure China 區域，並選取完整部署。

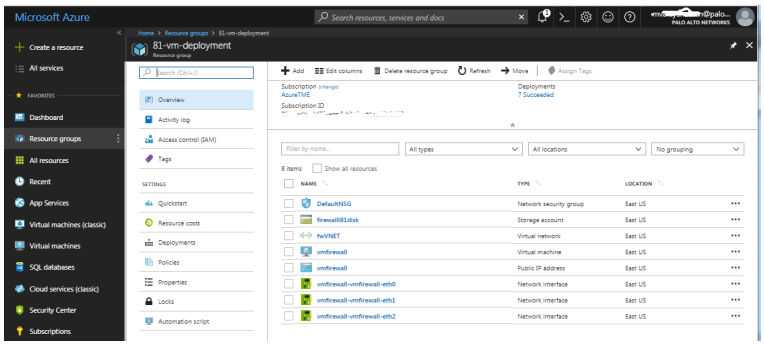
3. 設定好防火牆的基本設定。

   1. 輸入現有帳戶的儲存帳戶名稱，或建立新帳戶。
   2. 輸入 blob 儲存容器的名稱，防火牆 vhd 映像將複製並儲存到此容器中。
   3. 輸入 DNS 名稱，以存取防火牆的管理介面 (eth0) 上的公共 IP 位址。若要存取防火牆的網頁介面，必須結合您輸入的首碼和尾碼，例如 <yourDNSname><china_region>.cloudapp.azure.com。
   4. 輸入防火牆管理員的 **Username**（使用者名稱）。
   5. 輸入 **Password**（密碼）以保護防火牆的管理存取安全。
   6. 根據您的需求選取 Azure 虛擬電腦層級及大小。請參閱Azure 上的 VM-Series 最低系統需求。
   7. 輸入 **VmName**，這是在資源群組內用以識別 VM-Series 防火牆的顯示名稱。
   8. 使用 **PublicIPAddressName** 來標示資源群組內的防火牆管理介面。Microsoft Azure 會繫結您定義的 DNS 名稱與此名稱，讓您可以從公共網際網路存取防火牆的管理介面。
   9. 輸入 **VirtualNetworkName** 來識別 VNet。VNet 的預設 IP **Address Prefix**（位址首碼） 是 10.0.0.0/16。這可以變更以符合 IP 定址需求。
   10. 設定網路介面的子網路。如果您使用現有 VNet，則必須已定義三個子網路，分別用於管理、信任和不受信任的介面。如果您建立新的 VNet，請驗證或變更每個子網路的首

©2023 Palo Alto Networks, Inc.

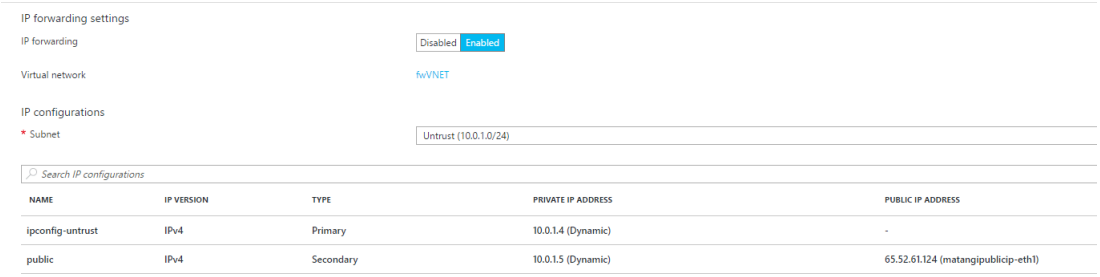
碼。預設子網路為 10.0.1.0/24、10.0.2.0/24 和 10.0.3.0/24。您可以依喜好將這些子網路配置給管理、信任和不受信任的介面。

4. 檢閱摘要，接受使用條款及隱私權原則，然後按一下 **Immediate deployment**（立即部署）以部署防火牆。部署可能需要 20 分鐘，您可以利用頁面上的連結來驗證進度。
5. 確認您已成功部署 VM-Series 防火牆。
   1. 使用您的 Microsoft 帳戶認證登入 Azure China 入口網站 (https://portal.azure.cn)。
   2. 選取 **Dashboard**（儀表板） > **Resource Groups**（資源群組），然後選取資源群組。
   3. 選取 **All Settings**（所有設定） > **Deployments**（部署） > **Deployment History**（部署歷程記錄），以瞭解詳細狀況。



STEP 4 | 附加公共 IP 位址給 VM-Series 防火牆的不受信任介面。這可讓您從公共網際網路存取此介面，對於任何網際網路型應用程式或服務很有用。

1. 在 Azure 入口網站上，選取您要新增公共 IP 位址的網路介面。例如 eth1 介面。
2. 選取 **IP Configurations**（**IP** 設定） > **Add**（新增），並針對 [Public IP address（公共 IP 位址）] 選取 **Enabled**（已啟用）。建立新的公共 IP 位址，或選取您可用的公共 IP 位址。
3. 確認您可以檢視與介面相關聯的次要 IP 位址。



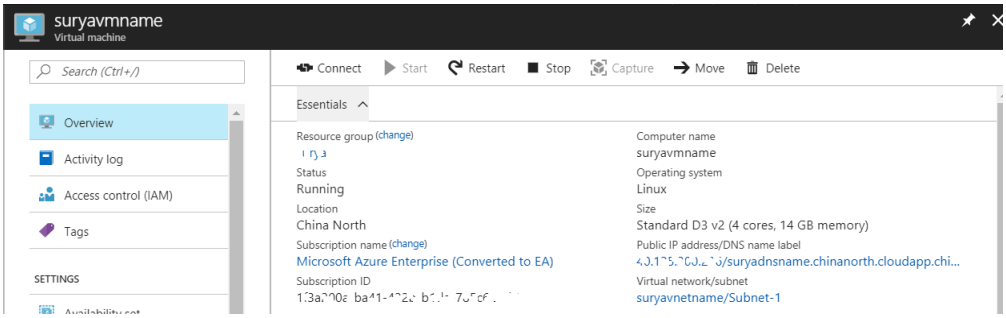
將次要 *IP* 位址附加至網路介面時，*VM-Series* 防火牆不會自動取得已指派給介面的私人 *IP* 位址。您需要利用 *VM-Series* 防火牆介面來手動設定私人 *IP* 位址。請參閱將資料平面網路介面設為防火牆上的第 3 層介面。

在 Azure 上的 VM-Series 防火牆，每個介面都有一個動態（預設）或靜態私人 IP 位址，以及多個相關聯的公共 IP 位址（靜態或動態）。可指派給介面的公共 IP 位址數目上限是根據您的 Azure 訂用帳戶。當您建立新的公共 IP 位址時，您會從 Microsoft 擁有的大量 IP 位址中取得位址，因此，您無法選取特定的位址。

©2023 Palo Alto Networks, Inc.

STEP 5 | 登入防火牆的網頁介面。

1. 在 Azure 入口網站的 **All Resources**（所有資源）中，選取 VM-Series 防火牆，然後檢視防火牆的完整 DNS 名稱。



2. 使用 Web 瀏覽器的安全連線 (https)，登入防火牆的 DNS 名稱。
3. 輸入您稍早定義的使用者名稱/密碼。您將看見憑證警告；此為正常現象。繼續開啟網頁。

STEP 6 | 啟動 VM-Series 防火牆上的授權。

1. 建立支援帳戶。
2. 註冊 VM-Series 防火牆（使用驗證碼）。
3. 在防火牆網頁介面上，選取 **Device**（裝置） > **Licenses**（授權），然後選取 **Activate feature using authentication code**（使用驗證碼啟動功能）。
4. 輸入您在支援入口網站上註冊的容量驗證碼。防火牆將連線至更新伺服器 (updates.paloaltonetworks.com)，並自動下載授權及重新啟動。
5. 重新登入 Web 介面並在 **Dashboard**（儀表板）上確認下列各項：
   - **Serial#**（序號）中顯示有效的序號。

     如果顯示 Unknown 一詞，則意味設備未經授權。若要在防火牆上檢視流量日誌，您必須安裝有效的容量授權。
   - **VM Mode**（**VM** 模式）顯示為 Microsoft Azure。

STEP 7 | 將資料背板網路介面設為防火牆上的 Layer 3 介面。

如果您在單一伺服器上使用不同 IP 位址和 SSL 憑證來代管多個網站或服務，您可能需要在 VM-Series 防火牆介面上設定多個 IP 位址。

1. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）。
2. 按一下 **Ethernet 1/1** 的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：第 3 層（預設值）。
   - 在設定頁籤上，將介面指派給預設路由器。
   - 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 New Zone（新增區域）。定義稱為 UnTrust 的新區域，然後按一下 OK（確定）。
   - 在 **IPv4** 頁籤上，如果您打算在介面上只指派一個 IP 位址，請選取 **DHCP Client**（**DHCP** 用戶端）。將會自動取得在 ARM 範本中指定的私人 IP 位址。如果您

©2023 Palo Alto Networks, Inc.

打算指派多個 IP 位址，請選取 **Static**（靜態），並手動輸入在 Azure 入口網站上指派給介面的主要和次要 IP 位址。

- 清除 **Automatically create default route to default gateway provided by server**（自動建立伺服器所提供之預設閘道的預設路由）核取方塊。停用此選項可確保此介面所處理的流量，不會直接流向 VNet 中的預設閘道。

3. 按一下 **ethernet 1/2**（乙太網路 **1/2**）的連結，然後依照以下所述設定：
   - 將 **Interface Type**（介面類型）設為 Layer3（預設值）。
   - **Security Zone**（安全性地區）：信任
   - **IP Address**（**IP** 位址）：選取 **DHCP Client**（**DHCP** 用戶端）或 **Static**（靜態）。
   - 清除 **Automatically create default route to default gateway provided by server**（自動建立伺服器所提供之預設閘道的預設路由）核取方塊。停用此選項可確保此介面所處理的流量，不會直接流向 VNet 中的預設閘道。
4. 按一下 **Commit**（交付）。確認介面的連結狀態為啟動。

STEP 8 | 根據您的特定部署來設定防火牆。

- 閘道#在不受信任的區域前面部署第三方負載平衡器。
- 混合和 VNet 間#在不受信任的區域前面部署 Azure VPN 閘道或 NAT 虛擬機器。
- 子網路間#在 VM-Series 防火牆上，新增內部網路區安全性原則規則，以基於附加至信任介面的子網路來允許流量。
- GlobalProtect#在不受信任的區域前面部署 NAT 虛擬機器。

STEP 9 | 將流量導向至 VM-Series 防火牆。

1. 為了確保 VM-Series 防火牆可保護 Azure 資源群組內所有流量的安全，請在防火牆上設定靜態路由。
2. 設定 UDR 將所有流量導向通過 VM-Series 防火牆上的介面。如需詳細資訊，請參閱有關 UDR 的 Azure 文件。

   內部子網路上的 UDR 必須透過 Trust（信任）介面傳送所有流量。UnTrust（不信任）側上的 UDR 透過 VM-Series 防火牆上的 UnTrust（不信任）介面從網際網路導向所有流量。網際網路流量可能來自 Azure 應用程式閘道或 Azure 負載平衡器，或者，如果是在連線內部網路與 Azure 雲端的混合部署中，則可能是通過 Azure VPN 閘道而來。

©2023 Palo Alto Networks, Inc.

Azure 中的 Panorama 協調部署

Azure 專用 Panorama 外掛程式可集中部署、設定和監控 Azure 雲端的安全狀態。可協調 Azure 網路中的 VM-Series 部署，以便您對受管理的防火牆啟用安全性政策。此外掛程式會連結至 Azure ARM 部署和 Azure 監視器頁面，讓您查看 VM-Series 防火牆的部署狀態、使用情況和效能。

在 Azure 中，此外掛程式協調 Azure 資源的部署，例如負載平衡器、子網路和 NAT 閘道，以及 VM-Series 防火牆自動調整規模集。在 Panorama 中，此外掛程式會自動設定 Panorama 裝置群組、範本堆疊和 NAT 政策。可讀取 Azure 資源中的標籤，然後在防火牆群組上集中啟用標籤型政策。

Panorama 外掛程式可以在 Azure 環境的一個或多個地區協調部署。部署可能包含中樞堆疊、輸入堆疊或兩者，取決於需要為部署保護的流量：

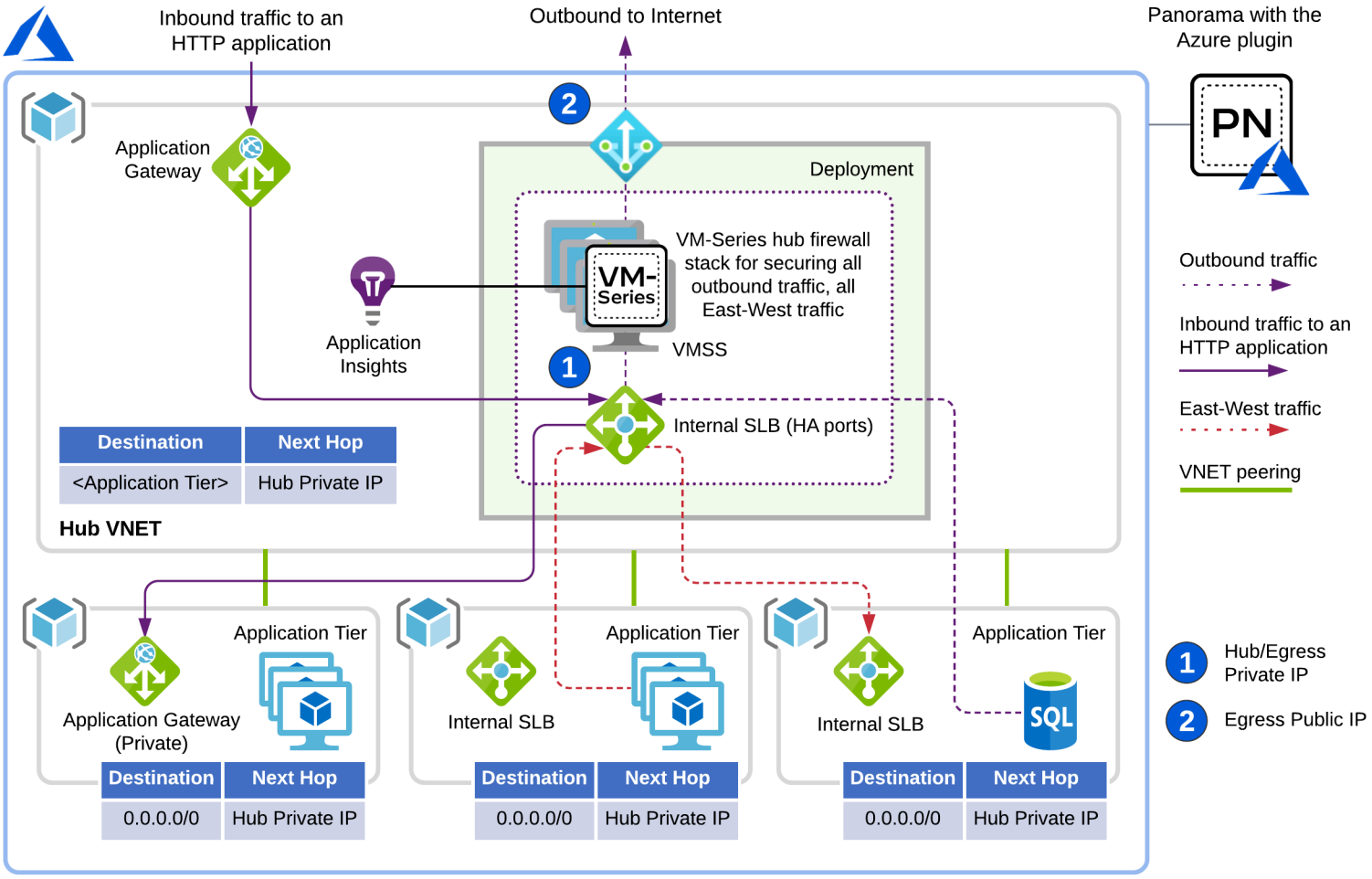
- 中樞防火牆堆疊保護應用程式工作負載之間的輸出流量和東西向流量。
- 輸入防火牆堆疊保護進出公開應用程式的流量。

您可以設定每個堆疊的防火牆數目。您可以選擇在部署中設定固定數量的防火牆，或設定一個範圍供 VMSS 用來調整規模。部署中的這兩個堆疊會建立 VM-Series 防火牆的 VMSS，各自可擴充到最多 25 個防火牆。

中樞堆疊

部署使用中樞堆疊，並利用 Azure 內部標準負載平衡器（具有 HA 連接埠），將一組防火牆調整規模和平衡負載。然後，您可以使用標準負載平衡器的私人 IP 位址（下圖的 **2**，“Hub/Egress Private IP”），將流量路由至防火牆進行檢查和威脅防護。中樞堆疊保護應用程式的輸出流量和東西向流量。

©2023 Palo Alto Networks, Inc.



若要保護輸出流量和東西向流量，請在應用程式 VNET 中新增路由規則，將流量重新導向至中樞堆疊來檢查。

輸入堆疊

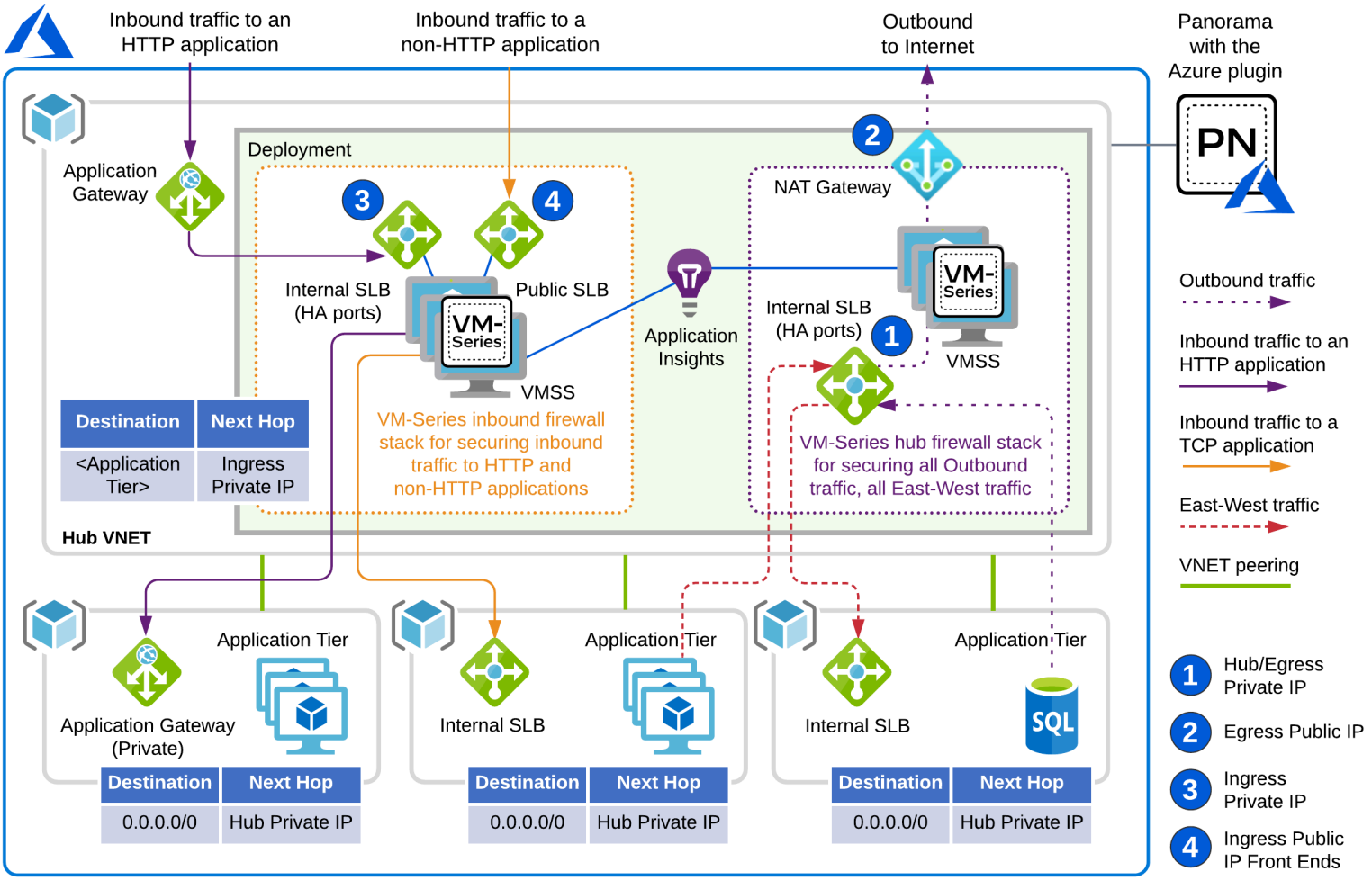
輸入防火牆堆疊可獨立調整規模，並提高應用程式輸入流量的可視性和安全性。

每個輸入堆疊最多可保護 *10* 個應用程式。

若要保護輸入 HTTP 流量，請在應用程式閘道的子網路路由表中新增 UDR，將所有流量路由至輸入堆疊（下圖的 **3**，Ingress Private IP）。若要保護非 HTTP 輸入流量，請使用 Panorama 外掛程式建立應用程式端點的前端入口（下圖的 **4**，Ingress Public IP Front Ends）。為了啟用檢查，Panorama 外掛程式會自動在 Azure 公共標準負載平衡器上建立負載平衡器規則，並自動在防火牆上建立 NAT 規則。

如果您只有 HTTP/HTTPS 輸入流量，則可以省略輸入堆疊，只使用中樞堆疊來保護該流量。

©2023 Palo Alto Networks, Inc.



請參閱為協調部署做好準備和在 Azure 中協調 VM-Series 防火牆部署。

為協調部署做好準備

在 Azure 上協調 VM-Series 防火牆之前，請完成下列工作。

- 設定先決條件
- 協調運作權限
- 建立自訂角色並與 Active Directory（主動式目錄 - AD）建立關聯
- 尋找您的 Azure 目錄網域名稱

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

設定先決條件

在 Panorama 和 Azure 上完成下列基本工作。

©2023 Palo Alto Networks, Inc.

- Azure
  - 建立服務主體讓外掛程式發出 API 呼叫。
  - 規劃特別專用於 VM-Series 防火牆傳輸 VNet 的 CIDR 區塊。外掛程式會管理此 CIDR 區塊，用以部署初始防火牆 VNet 並於未來升級至新的範本堆疊。

    CIDR 最小範圍是 /22。
- Panorama
  - 確保您在 Panorama 上已設定有效的授權 API 金鑰。這可讓外掛程式在相應縮小自動調整規模事件中管理取消授權。請參閱安裝授權停用 API 金鑰。
  - 在 Panorama 上安裝最新版的 VM-series 外掛程式，以允許將 Application Insight 設定新增至範本堆疊。
- 合格的 Azure 區域

  支援 VM-Series 防火牆的所有區域都支援 Panorama 協調部署。下列區域已合格；如果您部署在未列出的區域且遇到問題，請聯聯支援人員。
  - 美國西部
  - 美國西部 2
  - 美國中北部
  - 美國東部
  - 美國東部 2
  - 西歐
  - 德國中西部
  - UAE 北部
  - 印度西部
  - 澳大利亞東南部

規劃部署時，請注意如果您目前執行 Azure 專用 Panorama 外掛程式版本 2.x，則不允許升級至目前版本。除此之外，一旦安裝目前版本，就不允許降級至版本 2.x 外掛程式。請參閱相容性矩陣中的 Azure 專用 Panorama 外掛程式。

協調運作權限

此 JSON 範例檔案包含範本部署者角色的權限。在 **AssignableScopes** 區段中，請加入所有必須查詢的相關訂閱，包括部署的目標訂閱，以及含有應用程式 VNET（與存在受保護資源的 VM-Series 防火牆互連）的「每一個」訂閱。

```
{ "名稱":"範本部署", "為自訂": true, "說明":"管理範本部署.",    "動
作": [ "Microsoft.Resources/subscriptions/resourcegroups/*",
 "Microsoft.Resources/deployments/write", "Microsoft.Resources/
deployments/operationStatuses/read", "Microsoft.Resources/
deployments/read", "Microsoft.Resources/deployments/delete",
 "Microsoft.Network/publicIPPrefixes/write", "Microsoft.Network/
publicIPPrefixes/read", "Microsoft.Network/publicIPPrefixes/delete",
 "Microsoft.Network/publicIPAddresses/write", "Microsoft.Network/
```


©2023 Palo Alto Networks, Inc.

```
publicIPAddresses/read", "Microsoft.Network/publicIPAddresses/
delete", "Microsoft.Network/publicIPAddresses/join/action",
 "Microsoft.Network/natGateways/write", "Microsoft.Network/
natGateways/read", "Microsoft.Network/natGateways/delete",
 "Microsoft.Network/natGateways/join/action", "Microsoft.Network/
virtualNetworks/read", "Microsoft.Network/virtualNetworks/write",
 "Microsoft.Network/virtualNetworks/delete", "Microsoft.Network/
virtualNetworks/subnets/write", "Microsoft.Network/virtualNetworks/
subnets/read", "Microsoft.Network/virtualNetworks/subnets/
delete", "Microsoft.Network/virtualNetworks/subnets/join/action",
 "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/
read", "Microsoft.Network/networkSecurityGroups/write",
 "Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/
networkSecurityGroups/delete", "Microsoft.Network/
networkSecurityGroups/join/action", "Microsoft.Network/loadBalancers/
write", "Microsoft.Network/loadBalancers/read", "Microsoft.Network/
loadBalancers/delete", "Microsoft.Network/loadBalancers/probes/join/
action", "Microsoft.Network/loadBalancers/backendAddressPools/join/
action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/
read", "Microsoft.Network/locations/serviceTags/read",
 "Microsoft.Network/applicationGateways/read", "Microsoft.Network/
networkInterfaces/read", "Microsoft.Compute/virtualMachineScaleSets/
write", "Microsoft.Compute/virtualMachineScaleSets/read",
 "Microsoft.Compute/virtualMachineScaleSets/delete",
 "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
 "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/images/
read", "Microsoft.insights/components/write", "Microsoft.insights/
components/read", "Microsoft.insights/components/delete",
 "Microsoft.insights/autoscalesettings/write" ] "NotActions": [ ],
 "AssignableScopes": [ "/subscriptions/{deployment-subscription}",
 "/subscriptions/{app1-subscription}", "/subscriptions/{app2-
subscription}", . . . ] }
```

建立自訂角色並與 Active Directory（主動式目錄 - AD）建立關聯

STEP 1 | 若要在 Azure 中建立 Active Directory（主動式目錄 - AD），請導覽至 Azure Active Directory，然後按一下左側的 **App Registrations**（應用程式註冊）。使用外掛程式所需的權限建立自訂角色。

下方包含範例 JSON。

1. 按一下 **add**（新增）並提供名稱。選取從上述 JSON 檔案建立的角色，將 [Assign access to（指派存取給）] 保留為 Active Directory（主動式目錄 - AD）使用者，然後選取第一步建立的 Active Directory，並按一下 [Save（儲存）]。
2. 選取類型。

   [Redirect URI（重新導向 URI）] 下方完全不要修改。

©2023 Palo Alto Networks, Inc.

STEP 2 | 使用外掛程式所需的權限建立自訂角色。

請參閱 協調運作權限。

1. 登入 Azure CLI。

```
az login
```

2. 從 協調運作權限 中的檔案建立自訂角色。

```
az 角色定義建立 --role-definition <role-json-file>
```

STEP 3 | 將角色與您在步驟 1 建立的 Active Directory（主動式目錄 - AD）建立關聯。您可以使用主控台或 CLI。

針對 協調運作權限 中自訂角色的 ***assignableScope*** 區段所定義的每個訂閱，您必須重複此步驟。

主控台

1. 在 Azure 入口網站上，導覽至 **Subscriptions**（訂閱）並選取您的訂閱。
2. 在左側選取 **Access Control (IAM)**（存取控制 **(IAM)**），然後在頂端列選取 **Role Assignments**（角色指派）。
3. 選取 **Add**（新增），然後選擇 **add role assignment**（新增角色指派）。
   - 選取您在步驟 3 建立的角色，並將 [Assign access to（指派存取給）] 保留為 Active Directory（主動式目錄 - AD）使用者。
   - 選取步驟 1 建立的 Active Directory（主動式目錄 - AD），然後按一下 **Save**（儲存）。

CLI:

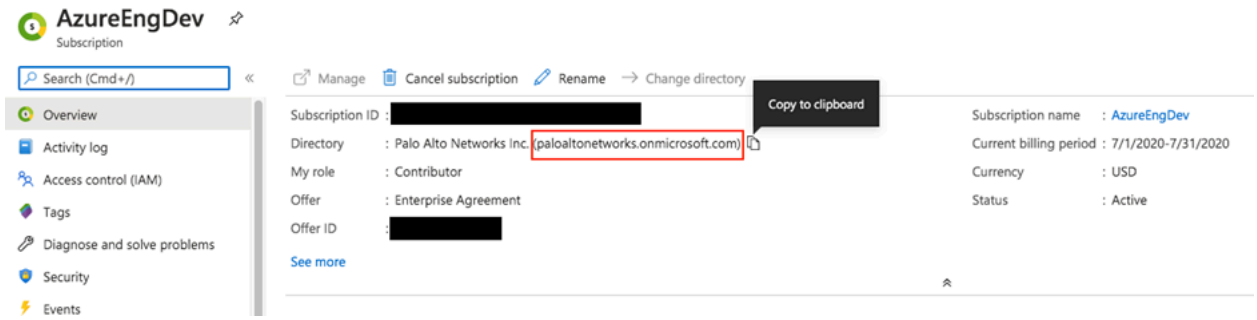
在下列命令中，**<role-name>** 是指先前 JSON 範例檔案中的名稱，亦即 **Template Deployment**。

```
az ad sp create-for-rbac --name <name-of-service-principal> --role
 <role-name> --output json
```

尋找您的 Azure 目錄網域名稱

為了讓外掛程式提供連結指向您的 Azure 部署和 Azure 入口網站中的 Application Insights 實例，您必須為訂閱識別目錄網域，如下所示：

©2023 Palo Alto Networks, Inc.



在 Azure 中協調 VM-Series 防火牆部署

您最多可以建立十個協調部署。此外，每個協調的部署最多支援 100 個前端應用程式。

不支援 *Azure China* 和 *Azure Government*。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

©2023 Palo Alto Networks, Inc.

STEP 1 | 建立服務主體。

使您建立的服務主體認證上線，以准許 Panorama 外掛程式發出必要的 API 呼叫來協調您的部署

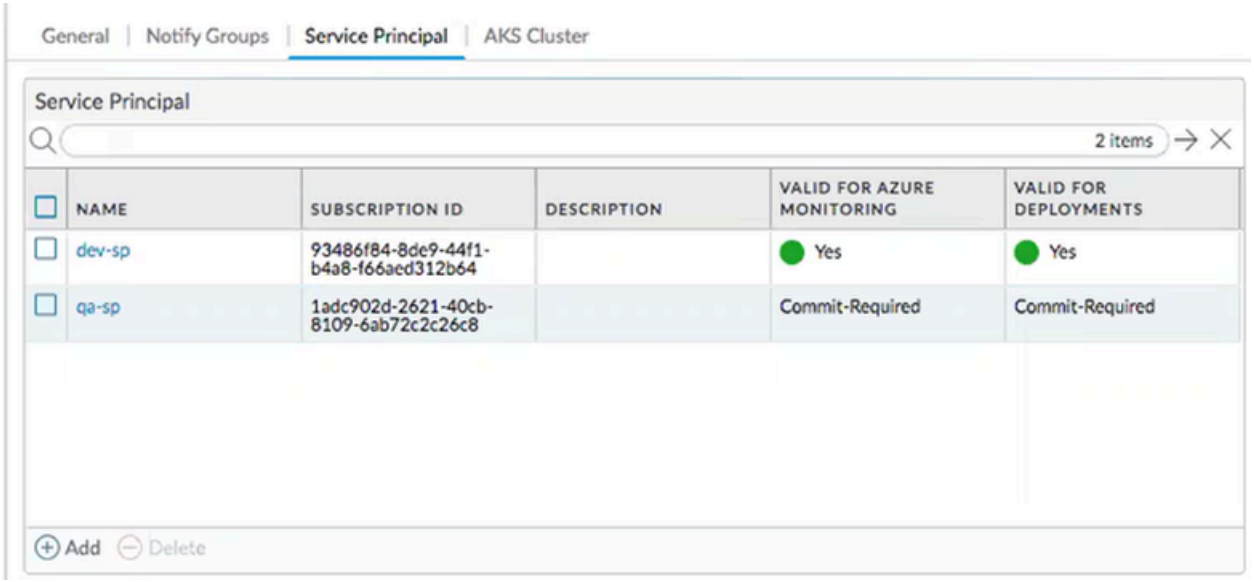
1. 選取 **Setup**（設定） > **Service Principal**（服務主體） > **Add**（新增）
2. 輸入 **Name**（名稱）和選用的 **Description**（說明），以識別服務帳戶。
3. 為您要監控的 Azure 訂閱輸入 **Subscription ID**（訂閱 **ID**）。

   您必須登入 Azure 入口網站才能取得此訂閱 ID。
4. 輸入 **Client ID**（用戶端 **ID**）。用戶端 ID 是與 Azure Active Directory 應用程式相關聯的應用程式 ID。
5. 輸入 **Client Secret**（用戶端密碼）並重新輸入以確認。
6. 輸入 **Tenant ID**（租用戶 **ID**）。

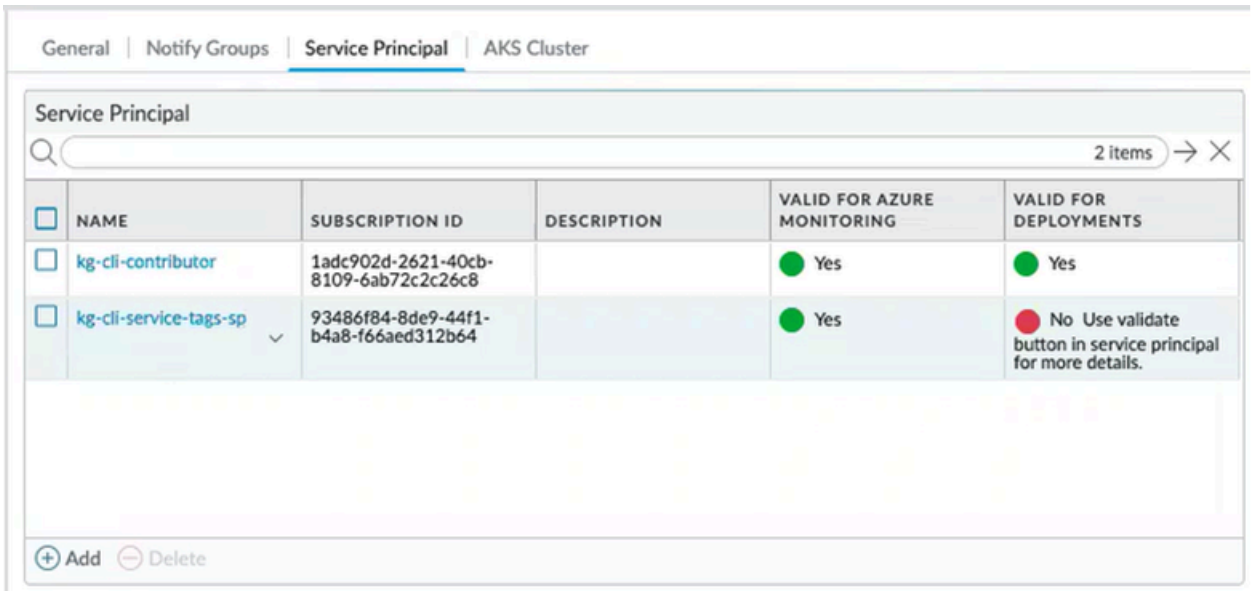
   租用戶 ID 為您在設定啟動目錄應用程式時儲存的目錄 ID。
7. 按一下 **Validate**（驗證）以確認您輸入的金鑰和 ID 有效，且 Panorama 可以使用 API 與 Azure 訂閱通訊。

   可能需要一分鐘來驗證。您可以更新頁面來檢查進度。
8. 當服務主體生效時，請提交變更。

   提交可確保您設定部署時有服務主體可用。



©2023 Palo Alto Networks, Inc.



©2023 Palo Alto Networks, Inc.

STEP 2 | 設定 Azure 部署。

1. 選取 **Deployments**（部署）並 **Add**（新增）設定。
2. 選取 **Build**（建置） > **General**（一般）。
   - 提供 **Name**（名稱）和選用 **Description**（說明）。
   - 從下拉式清單中選擇服務主體。

     您必須選取有效的服務主體才能啟用 **Azure** 索引標籤。

     如果沒看到您的服務主體，請返回 步驟 1，並確定服務主體有效且已提交。



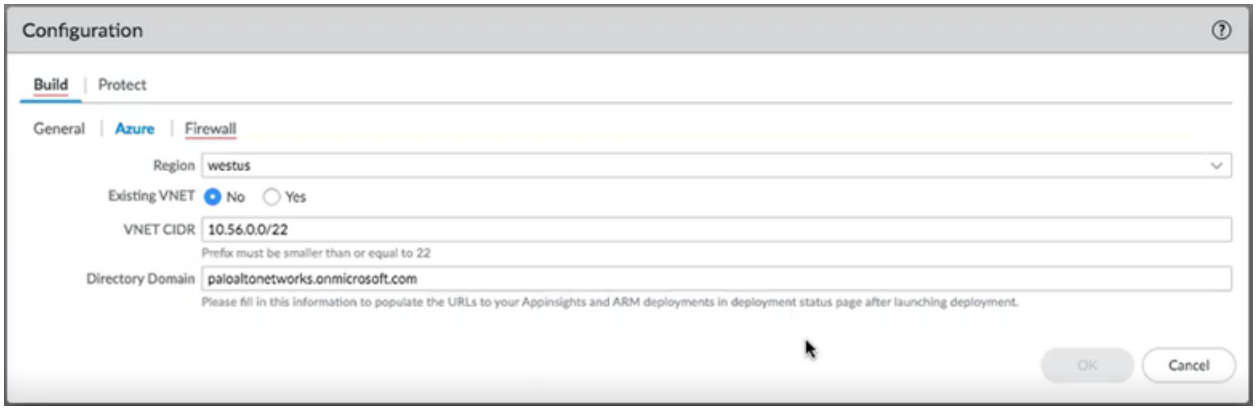
3. 在 **Build**（建置） > **Azure** 頁籤上，選取地區。

   下拉式清單是動態—列出具有 Palo Alto Networks VM-Series 新世代防火牆映像的所有地區。

   - **Existing VNET**（現有的 **VNET**）。
     - 選取否建立新的 VNET。

       外掛程式會使用 VNET CIDR 和目錄網域為您建立 VNET。

     - 選取 **Yes**（是）指出現有的 VNET。
   - **VNET CIDR**—輸入 CIDR 範圍。首碼必須小於或等於 /22。例如，192.168.0.0/22。
   - **Directory Domain**（目錄網域）—請參閱尋找您的 Azure 目錄網域名稱。此字串是訂閱中所有資源的一部分 URL，可協助外掛程式連結至您的部署。

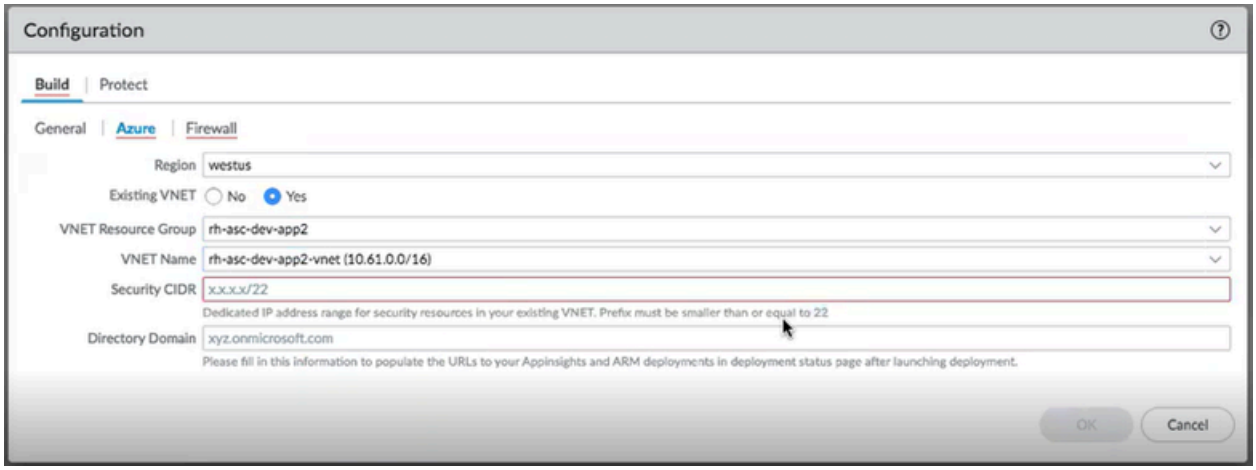


   如果您選取是，外掛程式會要求提供 VNET 資源群組、VNET 名稱、安全性 CIDR 和目錄網域。

©2023 Palo Alto Networks, Inc.

- **VNET Resource Group**（**VNET** 資源群組）—從您所選地區中所有資源群組的清單中選擇。
- **VNET Name**（**VNET** 名稱）—從您所選資源群組的 VNET 清單中選擇。
- **Security CIDR**（安全性 **CIDR**）—輸入 CIDR 範圍。首碼必須小於或等於 /22。例如，192.168.0.0/22。
- **Directory Domain**（目錄網域）—請參閱尋找您的 Azure 目錄網域名稱。此字串是訂閱中所有資源的一部分 URL，可協助外掛程式連結至您的部署。

VNET 資源群組和 VNET 名稱協助外掛程式找出您現有的 VNET。外掛程式部署的任何項目都會放到外掛程式所管理的資源群組內。



STEP 3 | 為您的部署設定 VM-Series 防火牆堆疊。

您可以部署中樞堆疊來保護輸出/東西向流量。您可以部署輸入堆疊來保護輸入流量。如果需要保護所有流量，這兩個堆疊也可以都部署。

這兩個堆疊的設定參數相同。

- **License Type**（授權類型）—選取 [BYOL]、[Bundle 1（搭售包 1）] 或 [Bundle 2（搭售包 2）]。
- **License Authcode**（授權驗證碼）—（僅限 BYOL）。輸入歡迎信中傳送的驗證碼。
- **VM Size**（**VM** 大小）
  - 此下拉式清單顯示與您輸入的驗證碼相關聯的 VM 大小。
  - Bundle1（搭售包 1）或 Bundle2（搭售包 2）—選擇任何 VM 大小。

Existing Device Group（現有的裝置群組）—在堆疊和部署之中，裝置群組都必須是唯一的。也就是說，針對每個部署中的每個堆疊，您需要單獨的專用裝置群組。

如果您選取 **No**（否），外掛程式會建立裝置群組。

如果您選取 **Yes**（是），請從下拉式清單中選取現有的裝置群組。

- **Min Firewalls**（最少防火牆）—在 VMSS 中介於 1 到 25 之間的值。
- **Max Firewalls**（最多防火牆）—在 VMSS 中介於 1 到 25 之間的值。

©2023 Palo Alto Networks, Inc.

STEP 4 | 選取 **Build**（建置） > **Firewall**（防火牆） > **Basic**（基本），以設定這兩個堆疊通用的資訊。

針對 **Image Type**（映像類型），選取 **Marketplace Image**（**Marketplace** 映像）或 **Custom Image**（自訂映像）。

- **Image Resource Group**（映像資源群組）— （僅限自訂映像）選擇包含自訂映像的資源群組。若為自訂映像，清單會顯示您在步驟 2.b 選取的地區中所有包含映像的資源群組。
- **Image**（映像）— （僅限自訂映像）此下拉式清單顯示您所選資源群組中的所有映像。
- **Software Version**（軟體版本）— （Marketplace 映像）只顯示有效的軟體版本。關於最低 PAN-OS 版本，請查閱相容性矩陣。
- **Username**（使用者名稱）—您所建立防火牆的管理員使用者名稱。對於 VM-Series 防火牆和 Azure，此名稱都必須合法。請參閱建立 VM 時的使用者名稱需求為何？
- **Password**（密碼）—您所建立防火牆的管理員密碼。密碼必須符合 VM-Series 防火牆與 Azure 的字元和長度需求（31 個字元）。請參閱建立 VM 時的密碼需求為何？。
- **Confirm Password**（確認密碼）—重新輸入密碼。
- **Primary Panorama IP**（主要 **Panorama IP**）—指定可供防火牆啟動時用來連接至 Panorama 的 Panorama IP 位址。請選擇下拉式清單中顯示的公共 IP 或私人 IP 位址，或輸入 Panorama IP 位址。
- **Secondary Panorama IP**（次要 **Panorama IP**）—（僅限 Panorama 在 HA 設定中）。指定可供防火牆啟動時用來連接至 Panorama 的次要 Panorama IP。請從下拉式清單中選擇，或輸入正確 IP。
- **Configure Device Certificate PIN**（設定裝置憑證 **PIN**）。因為這些值都加密，輸入每個值時必須確認。
  - **Device Certificate PIN ID**（裝置憑證 **PIN ID**）—裝置憑證 ID。
  - **Confirm Device Certificate PIN ID**（確認裝置憑證 **PIN ID**）
  - **Device Certificate PIN Value**（裝置憑證 **PIN** 值）—憑證 PIN 值。
  - **Confirm Device Certificate PIN Value**（確認裝置憑證 **PIN** 值）

STEP 5 | 選取 **Build**（建置） > **Firewall**（防火牆） > **Advanced**（進階）選用預設值。

勾選 **Advanced**（進階）以編輯預設值。

- **Autoscaling Metric**（自動調整規模度量）—預設值為 [Data Plane CPU Util Percent（資料平面 CPU 使用率百分比）]。
- **Scale In Threshold**（相應縮小閾值）—接受預設值，或定義相應縮小閾值。
- **Scale Out Threshold**（相應放大閾值）—接受預設值，或定義相應放大閾值。
- **Jumbo Frame**—預設為停用。

按一下 **OK**（確定）並交付變更。重新整理頁面直到看見 **Deploy**（部署）按鈕，然後按一下 **Deploy**（部署）開始部署。部署開始之後，資訊會寫入 **Deployments**（部署）頁面。

部署需要 *15-20* 分鐘才會完成。

©2023 Palo Alto Networks, Inc.

STEP 6 | 選取 **Azure** > **Deployments**（部署），以檢視部署狀態。

- [Resource Group（資源群組）] 欄會顯示外掛程式已建立的資源群組。
- 防火牆的管理介面會使用防火牆存取 IP 來連接至 Panorama。您必須將此位址列入白名單，以確保 Panorama 可以連接 Panorama 來取得所需的設定。

  如果 *Panorama* 部署在公共雲端，請務必將防火牆存取 *IP* 新增至 *Panorama* 安全性群組。

  請參閱用於 Panorama 的連接埠，以決定您需要開放來允許流量的連接埠。
- 如需每個堆疊的其他詳細資訊，請開啟 **Deployment Status**（部署狀態）欄中的連結。
  - **Hub-Stack**（中樞堆疊）—[Hub stack Public IP（中樞堆疊公共 IP）] 符合部署摘要中的 [Firewall Access IP（防火牆存取 IP）]，因為對於來自部署的輸出流量和來自防火牆的管理流量，NAT 閘道都相同。

    所有輸出流量和東西向流量都應該路由至 **Egress Private IP**（輸出私人 **IP**）接受檢查。如果您已設定 UDR，則可以將流量導向至這個位址。
  - **Inbound-Stack**（輸入堆疊）—[Private IP（私人 IP）] 是防火牆前方的 Azure 內部負載平衡器上的位址。如果您正在設定 UDR，則可以將流量導向至這個位址。
- 點選連結來檢視部署資訊及 Azure 的 Application Insights。
- 部署詳細資訊可能顯示成功、警告和失敗訊息。

©2023 Palo Alto Networks, Inc.

STEP 7 | 為後端 TCP/UDP 應用程式設定輸入保護。

位於輸入防火牆堆疊前方的公共負載平衡器，是任何後端 UDP 或 TCP 應用程式的進入點。新增下列設定，讓外掛程式管理必要的負載平衡器和防火牆設定，以路由至您的後端應用程式。

1. 選取 **Azure** > **Deployments**（部署），然後選取您的部署。
2. 選取 **Protect**（保護）頁籤，然後按一下 **Add**（新增）。
3. 提供應用程式 **Name**（名稱），並選擇 **Protocol**（通訊協定）。

   輸入保護詳細資料：

   - **Frontend IP Type**（前端 **IP** 類型）—選取 [New Public IP（新的公共 IP）]、[Existing Frontend（現有的前端）] 和 [Existing Public IP（現有的公共 IP）] 其中一個。

     如果您選取 [Existing Frontend（現有的前端）]，**Frontend Name**（前端名稱）會列出負載平衡器上所有已知的前端。
   - **Resource Group**（資源群組）—（僅限現有的公共 IP）從下拉式清單中，選取存在您所需前端 IP 位址的資源群組。
   - IP Name（IP 名稱）—（僅限現有的公共 IP）用來將 IP 對應至負載平衡器的前端、設定負載平衡器及建立 NAT 規則。
   - **Frontend Port**（前端連接埠）—新增應該設定成在公共負載平衡器接收流量的前端連接埠。
   - **Backend IP**（後端 **IP**）—新增後端應用程式的 IP 位址。
   - **Backend Port**（後端連接埠）—新增後端應用程式預期會接收流量的連接埠。

   按一下 **OK**（確定）。
4. **Commit**（提交）以在負載平衡器上新增設定，並推送至防火牆。

©2023 Palo Alto Networks, Inc.

建立 Azure 的自訂 VM-Series 映像

您可以建立自訂 VM-Series 防火牆映像，供以後用於 Azure 部署。自訂映像可讓您以想要使用的 PAN-OS 版本，靈活又一致地部署 VM-Series 防火牆，而不受限於只能使用從 Azure 市集取得的映像。此外，自訂映像可以包含最新內容和防毒更新。

您在建立 VHD 之前需要移除所有私人資料，才能建立自訂映像—使用者設定、使用者、外掛程式設定等。此外，請完成下列程序，以準備和建立自訂映像。

如果用來建立自訂映像的 ***VM-Series*** 防火牆是以進階磁碟類型部署，則使用自訂映像部署的任何 ***VM-Series*** 防火牆，都必須使用相同的進階磁碟類型來部署。不過，如果您使用以標準磁碟類型部署的防火牆建立映像，則可以使用標準或進階磁碟類型來部署防火牆。

STEP 1 | 登入 Azure。

STEP 2 | 從 Azure Marketplace 部署 VM-Series 防火牆。

STEP 3 | （僅限 BYOL 授權）啟動您的授權。

STEP 4 | 升級 VM-Series 防火牆至 PAN-OS 10.0.3。升級至 PAN-OS 10.0.3 也會將 VM-Series 外掛程式升級至 2.0.3。

STEP 5 | 使用 Azure Marketplace 範本中提供的使用者名稱和密碼，透過 SSH 存取 VM-Series 防火牆 command line interface（命令列介面 - CLI）。

STEP 6 | 確認 VM-Series 防火牆有正確的 PAN-OS、VM-Series 外掛程式、內容和防毒版本。

```
show system info
```

如果您使用的是 ***PAN-OS 10.1***，請確保將 ***VM-Series*** 外掛程式升級到 ***2.1.7*** 或更高版本，如果您使用的是 ***PAN-OS 10.2.0***，請確保您使用的 ***VM-Series*** 外掛程式為 ***3.0.3*** 或更高版本。

STEP 7 | （僅限 BYOL 授權）停用您的授權。

STEP 8 | 在 VM-Series 防火牆上執行私人資料重設。此命令需要重新啟動防火牆。您必須等待 VM-Series 防火牆完成重新啟動才能繼續；重新啟動可能需要五到七分鐘。

```
request system private-data-reset
```


©2023 Palo Alto Networks, Inc.

STEP 9 | 從 VM-Series 實例建立新的 VHD 映像。

1. 登入 Azure CLI。
2. 確認您使用正確的訂閱。

   ```
   az account set --subscription <subscription-id>
   ```

3. 執行下列命令將 VM 一般化，以便製成適合多個部署的映像，然後建立新的 VHD。

   ```
   az vm deallocate --resource-group <myResourceGroup> --name
   <myVM>
   ```

   ```
   az vm generalize --resource-group <myResourceGroup> --name
   <myVM>
   ```

STEP 10 | 從自訂映像建立新的 VM-Series 防火牆。

```
az image create --resource-group <myResourceGroup> --name <myImage>
--source <resource-id-of-VM>
```

STEP 11 | 以自訂映像部署 VM-Series 防火牆之後，確認您的部署。

1. 從自訂映像啟動虛擬機器時，您應該使用提供的認證登入防火牆。
2. 成功登入之後，確認防火牆執行正確的 PAN-OS 版本，且有正確的內容和防毒版本。

   ```
   show system info
   ```

STEP 12 | （選用）將自訂映像複製到另一個地區。

```
az image copy –source-resource-group <source-rg> –source-object-
name <pa-vm-image-name> –target-location <target-region> –target-
resource-group <destination-rg>
```

 ©2023 Palo Alto Networks, Inc.

使用 Azure 安全性中心建議來保護您的工作負載

Microsoft 已棄用 Azure 安全性中心對合作夥伴安全性解決方案的支援，並將其取代為 Azure Sentinel。

當您在已對 Azure 安全性中心啟用的 Azure 訂閱內部署新的工作負載時，Azure 安全性中心可讓您以兩種方式保護這些工作負載。在一個工作負載中，Azure 安全性中心將建議您部署 VM-Series 防火牆的新實例以保護網際網路型應用程式工作負載。在另一個工作負載中，Azure 安全性中心將發現您在 Azure 訂閱中部署的 VM-Series 防火牆（合作夥伴安全性解決方案），然後您必須執行其他組態才能將 VM-Series 防火牆連線至 Azure 安全性中心，以便您在儀表板上檢視警報。如需詳細瞭解各個工作流程的整合情況及優缺點，請參閱 Azure 安全性中心整合：

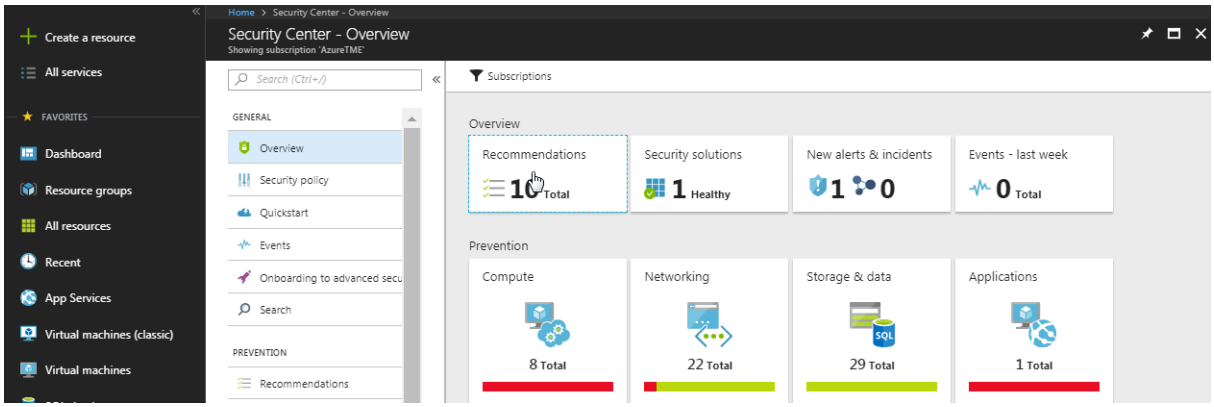
- 根據 Azure 安全性中心的建議部署 VM-Series 防火牆
- 從 Azure 安全性中心連線現有的 VM-Series 防火牆

根據 Azure 安全性中心的建議部署 VM-Series 防火牆

Azure 安全性中心將掃描您的 Azure 資源並為需要下一代防火牆的工作負載提供安全建議。建議將顯示在儀表板上，您可以從 Azure marketplace 部署 VM-Series 防火牆的新實例，或者使用 Azure CLI、Powershell 或 ARM 範本進行部署。使用 Azure CLI、Powershell 或 ARM 範本進行自訂部署的優點是，您可以在與您想要保護的工作負載相同的資源群組內部署 VM-Series 防火牆。當您使用 Azure marketplace 部署 VM-Series 防火牆時，Azure 要求您只能將防火牆部署至新的資源群組或空的資源群組。因此，marketplace 部署需要您確保將來自您要保護的工作負載的流量導向至屬於不同資源群組的防火牆。

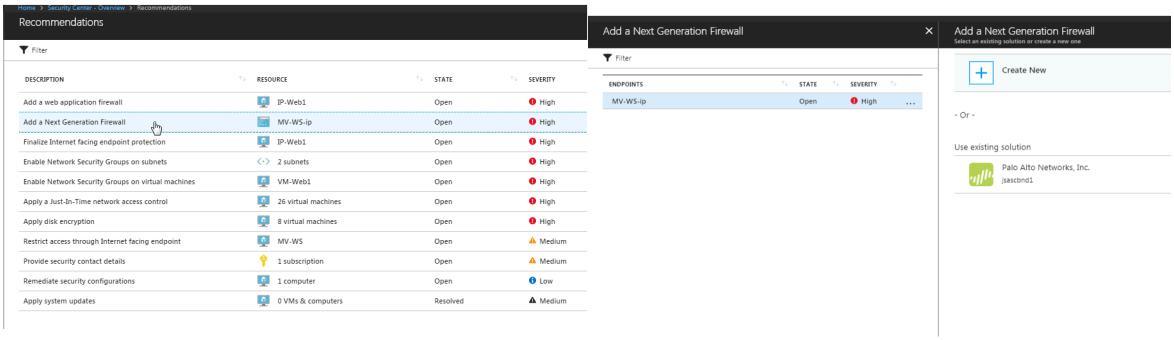
STEP 1 | 登入您的 Azure 入口網站並存取安全性中心儀表板。

STEP 2 | 選取 **Recommendations**（建議）。



 ©2023 Palo Alto Networks, Inc.

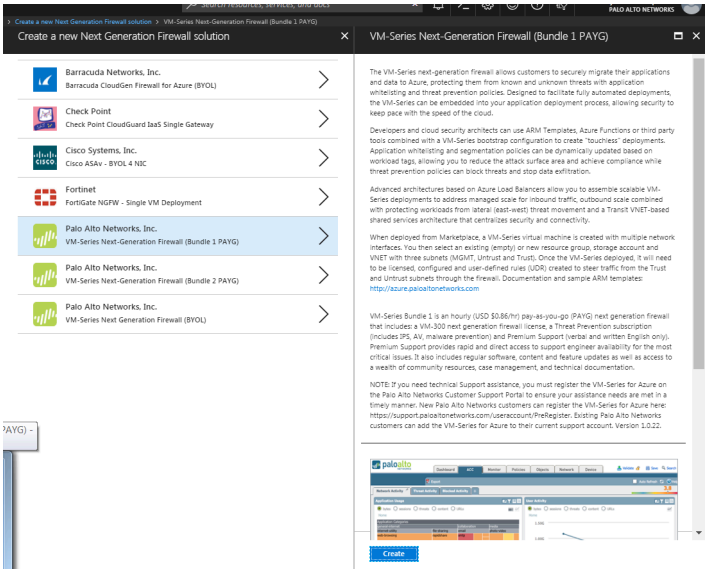
STEP 3 | 選取 **Add a Next Generation Firewall**（新增下一代防火牆），選取您要保護的工作負載。



STEP 4 | 選取您要部署 VM-Series 防火牆的新實例還是使用 VM-Series 防火牆的現有實例。

若要使用此工作流程，請透過暴露於網際網路的公共 IP 位址佈置工作負載，並部署新資源群組中 VM-Series 防火牆的實例。然後，刪除您已佈置的工作負載，並在您已部署防火牆的資源群組中部署生產工作負載。

- 若要 **Create New**（建立新的），請參閱從 Azure Marketplace 部署 VM-Series 防火牆（解決方案範本）。
- 若要 **Use existing solution**（使用現有解決方案），請選取您以前部署過的 VM-Series 防火牆。



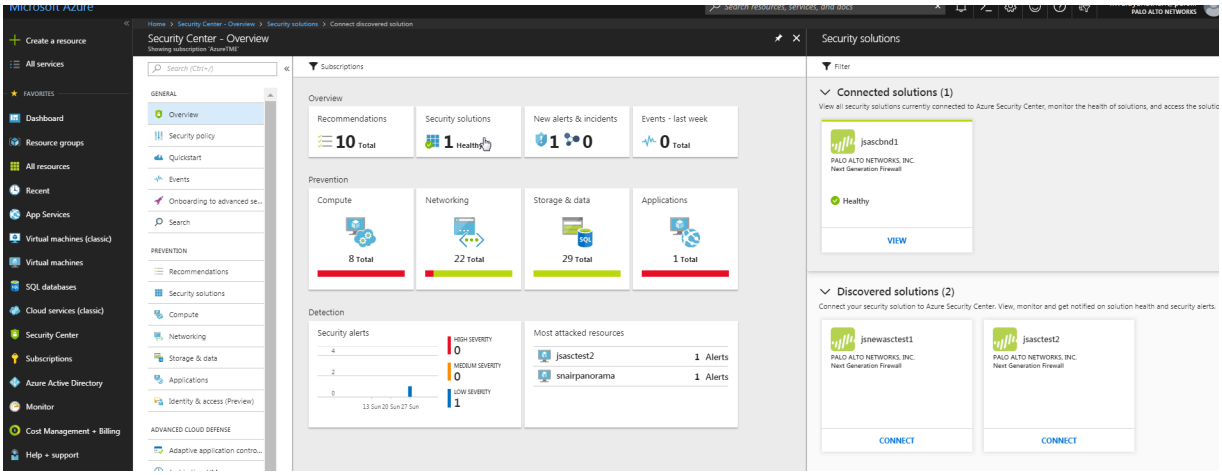
從 Azure 安全性中心連線現有的 VM-Series 防火牆

當 Azure 安全性中心偵測到您已在 Azure 訂閱中部署 VM-Series 防火牆時，其會將防火牆顯示為安全性解決方案。然後，您可以透過 Syslog 以普通事件格式 (CEF) 將 VM-Series 防火牆連線至安全性中心，並在安全性中心儀表板上將防火牆日誌作為警報進行檢視。

STEP 1 | 登入您的 Azure 入口網站並存取安全性中心儀表板。

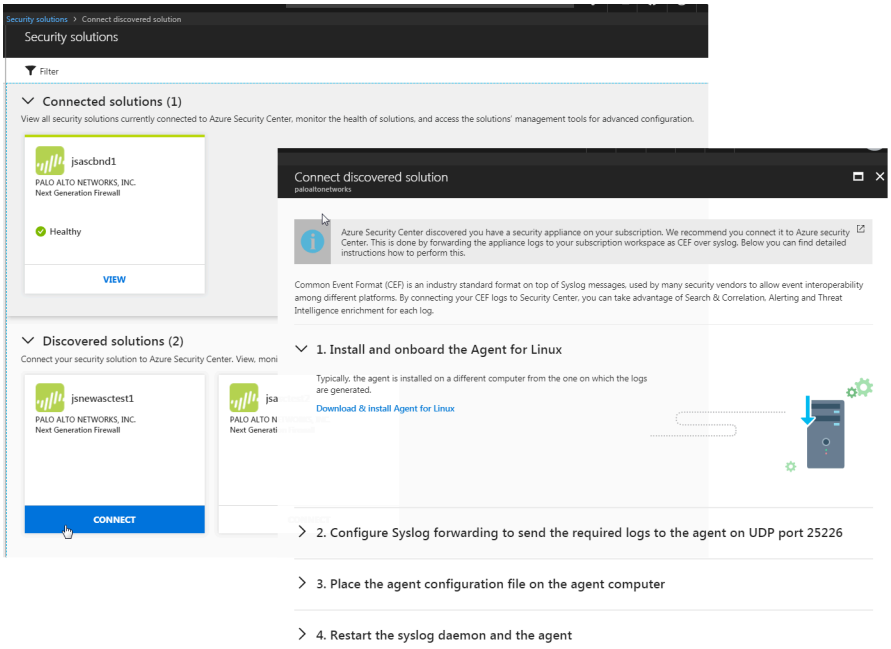
©2023 Palo Alto Networks, Inc.

STEP 2 | 選取安全性解決方案以檢視此 Azure 訂閱中的所有可用 VM-Series 防火牆。



STEP 3 | 展開已發現的解決方案，並選取與您想要保護的工作負載在相同資源群組中的 VM-Series 防火牆，然後按一下 **Connect**（連線）。

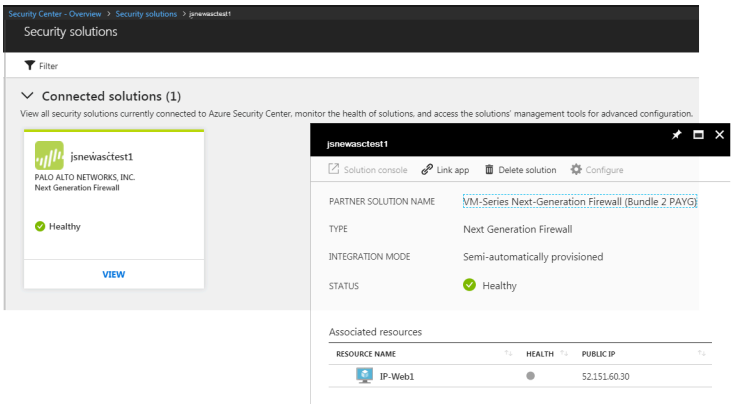
若要在 [Security Center（安全性中心）] 儀表板上將防火牆日誌作為警示進行檢視，您需要按照螢幕上顯示的四步程序操作。



©2023 Palo Alto Networks, Inc.

STEP 4 | 將 VM-Series 防火牆成功連線至安全性中心時，VM-Series 防火牆將顯示在連線的解決方案清單中。

按一下「檢視」以確認防火牆正在為您需要保護的工作負載提供保護。



使用 Panorama 將日誌轉送至 Azure 安全性中心

若您使用 Panorama 管理防火牆，則您可以使用範本與裝置群組以轉送防火牆日誌到 Azure 安全性中心。利用預設 Azure 安全性中心日誌轉送設定檔，防火牆產生的低、中、高或嚴重級別的威脅和 WildFire 提交日誌將作為安全性警報顯示於 Azure 安全性中心儀表板上。所以您可以更有效地集中並分流警報，您可以設定 精確日誌篩選器為僅轉送哪些您有興趣的日誌，或僅轉送高和嚴重級別的日誌。您也可以依據您的應用程式和安全性需求，選取性地附加一些日誌轉送檔案。

若要從 Panorama 啟用 Azure 安全性中心整合，請使用下列工作流程。

STEP 1 | 將防火牆新增為在 Panorama 上受管理的裝置。

STEP 2 | 從 Panorama 建立一個範本 與 一個裝置群組 以推送日誌，轉送設定到要轉送日誌到 Azure 安全性中心的防火牆。

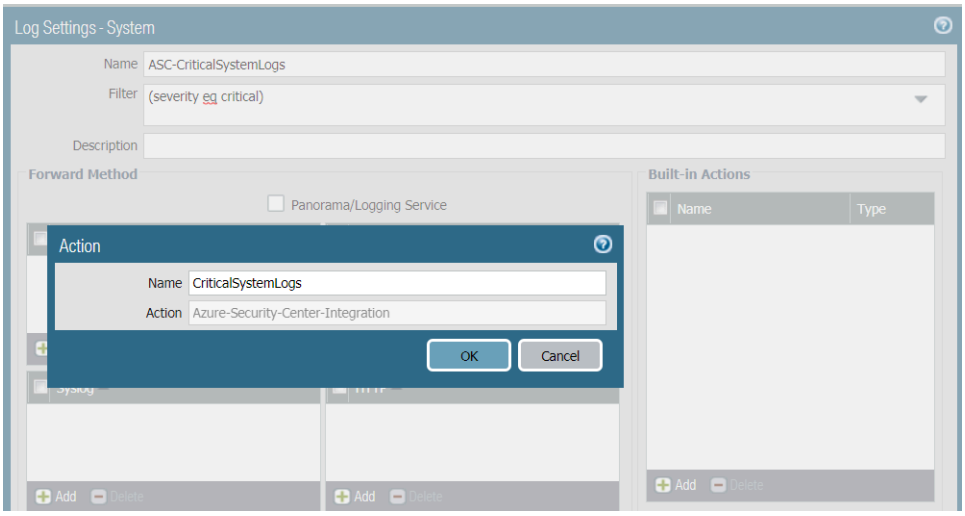
©2023 Palo Alto Networks, Inc.

STEP 3 | 指定日誌類型以轉送至日誌記錄服務。

您啟用轉送的方式需視日誌類型而定。對於依據規則比對而產生的日誌，您在裝置群組中使用日誌轉送設定檔，而對於其他日誌類型，您則使用範本內的日誌設定組態。

1. 設定系統、組態、User-ID 和 HIP 比對日誌的轉送。

   1. 選取 **Device**（裝置） > **Log Settings**（日誌設定）。
   2. 選取 **Template**（範本），其中包含您想要轉送日誌到日誌記錄服務的防火牆。
   3. 對於您要轉送到日誌記錄服務的每種日誌類型，請 **Add**（新增）一個比對清單篩選器。給它一個 **Name**（名稱），可選取定義一個 **Filter**（篩選器）。
   4. **Add**（新增） Built-in Actions（內建動作）並輸入一個 **Name**（名稱）。將自動選取 Azure-Security-Center-Integration 動作。按一下 **OK**（確定）。

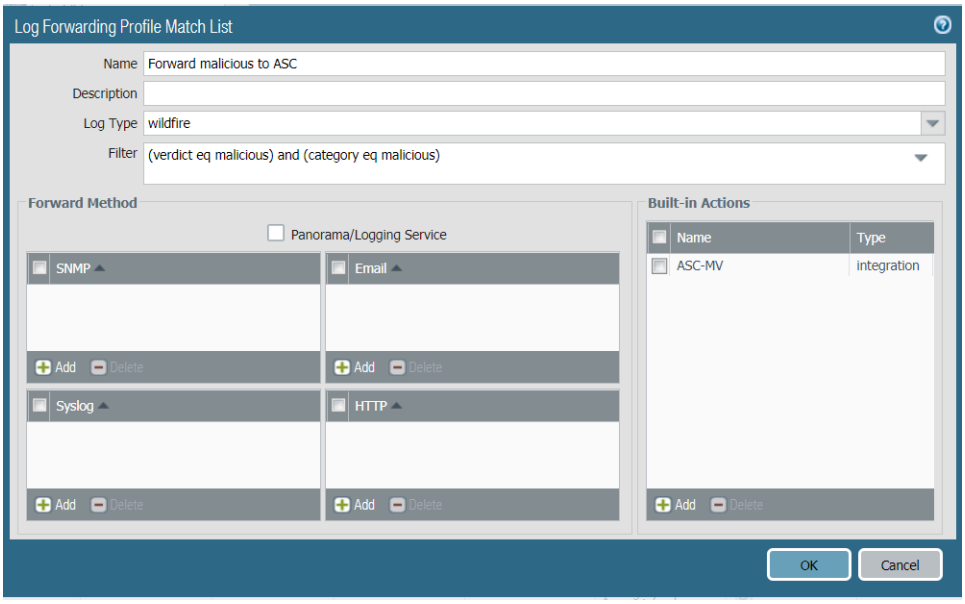
      

   5. 按一下 **OK**（確定）。

2. 設定在規則比對發生時，轉送所有生成的日誌類型，如：流量、威脅、WildFire 提交、URL 篩選、資料篩選及驗證日誌。若要轉送這些日誌，您必須建立並附加一個日誌轉送設定檔至每個您想要轉送日誌的原則規則上。

   1. 選取 **Device Group**（裝置群組），然後選取 **Objects**（物件） > **Log Forwarding**（日誌轉送）以**Add**（新增）一個設定檔。在日誌轉送設定檔比對清單中，新增您想要轉送的每一種日誌類型。
   2. 在 [Built-in Actions（內建動作）] 中選取 **Add**（新增）以在裝置群組中啟用防火牆，將日誌轉送至 Azure 安全性中心。

©2023 Palo Alto Networks, Inc.



3. 在您剛建立的裝置群組中建立基本安全性原則規則，並選取 **Actions**（動作）以附加您建立的日誌轉送設定檔，將日誌轉送至 Azure 安全性中心。在防火牆擁有介面和區域以及基本安全性規則之前，不會讓任何流量通過，且僅符合安全性原則規則的流量才會被日誌記錄（依預設）。
4. 對於您所建立的每條規則，請選取 **Actions**（動作）並選取允許防火牆將日誌轉送到 Azure 安全性中心的日誌轉送設定檔。

STEP 4 | 提交您的變更至 Panorama 並將其推送到您建立的範本和裝置群組中。

STEP 5 | 確定防火牆日誌已轉送至 Azure 安全性中心。

1. 登入 Azure 入口網站，選取 **Azure Security Center**（**Azure** 安全性中心）。
2. 確認您可在 Azure 安全性中心儀表板上如同安全性警告一樣看見防火牆日誌。

©2023 Palo Alto Networks, Inc.

在 Azure Stack 上部署 VM 系列防火牆

您可在 Azure Stack 上部署 VM-Series 防火牆以保護多層架構應用程式間子網路間流量及 Azure Stack 部署內伺服器的出埠流量。如果您想要使用 VM-Series 防火牆作為閘道來保護 Azure Stack 部署內目的地為伺服器的入埠流量，則必須在接收入埠流量並將其轉送至防火牆的防火牆之前部署 NAT 設備。必須使用 NAT 設備，因為在 Azure Stack 上，您無法將公共 IP 位址指派給虛擬電腦的非主要介面，例如 VM-Series 防火牆。

***Azure stack** 上的 **VM-Series** 防火牆不支援啟動程序、**Azure Application Insights** 或 **Azure** 安全性中心整合。*

與公共 Azure 不同，Azure Stack 上沒有用於部署 VM-Series 防火牆的解決方案範本。因此，您必須使用 ARM 範本部署 VM-Series 防火牆。若要開始部署，您可以使用 GitHub 上社群支援的範例 ARM 範本，然後開發您自己的生產部署 ARM 範本。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 從 Azure 下載 marketplace 項目至 AzureStack。

若要在 Azure Stack 上部署 VM-Series 防火牆，您需要存取 VM-Series 防火牆 PAN-OS 映像（8.1 或更新版本）的 BYOL。您可在連線的部署中將映像直接從 Azure Marketplace 下載至 Azure Stack。

STEP 2 | 存取 Azure Stack 入口網站。

您的 Azure Stack 營運商（服務供應商或您組織中的管理員）應當提供存取該入口網站的正確 URL。

STEP 3 | 部署 VM-Series 防火牆。

Azure Stack 上不提供 VM-Series 防火牆的解決方案範本。因此，您必須在 ARM 範本中參照上一步所下載的映像以部署 VM-Series 防火牆。若要開始，您可根據社群支援原則部署 GitHub 提供的範例 ARM 範本。

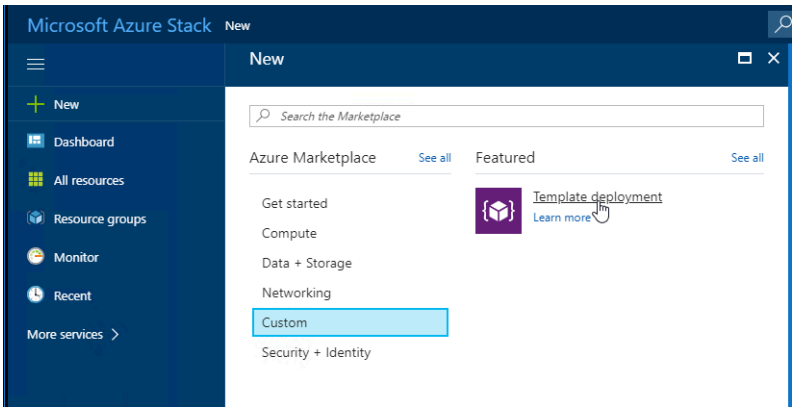
1. 取得範例 Azure Stack GitHub 範本。
   - 選取 azurestackdeploy.json 以檢視內容。
   - 按一下「原始」並複製 JSON 檔案的內容。
2. 部署範例 GitHub 範本。

   您可以將防火牆部署在空的現有資源群組中，或部署到新的資源群組。此範本中的預設 VNet 是 192.168.0.0/16，而所部署的 VM-Series 防火牆具有三個網路介面：一個

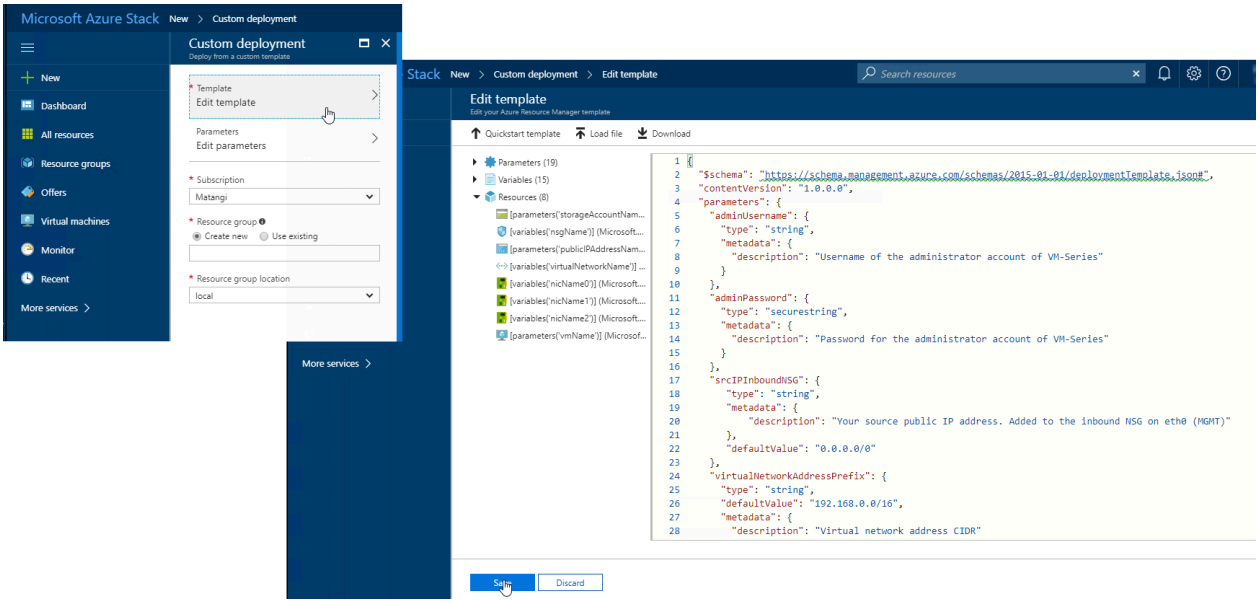
©2023 Palo Alto Networks, Inc.

192.168.0.0/24 子網路上的管理介面和 192.168.1.0/24 與 192.168.2.0/24 子網路上的兩個資料平面介面。您可自訂這些子網路以滿足您的需求。

- 登入 Azure Stack 入口網站。
- 選取 **New**（新增） > **Custom**（自訂） > **Template deployment**（範本部署）。

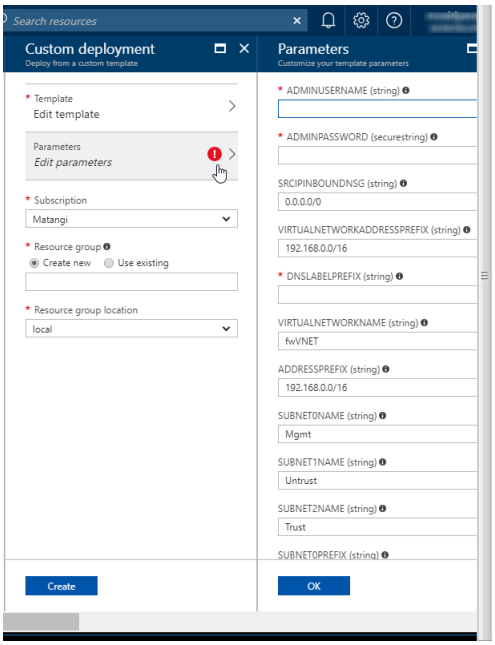


- **Edit template**（編輯範本），刪除範本中的所有現有內容，貼上您之前複製的 JSON 範本內容並 **Save**（儲存）。

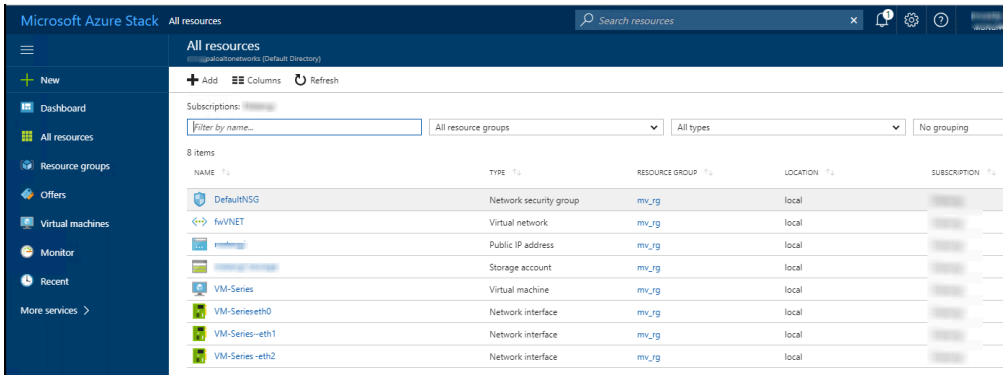


- **Edit parameters**（編輯參數），輸入必要參數的值，並在需要時修改預設值，然後按一下 **OK**（確定）。

©2023 Palo Alto Networks, Inc.



- 選取您想要使用的 **Subscription**（訂閱），然後按一下 **OK**（確定）。
- 選取現有為空的 **Resource Group**（資源群組）或建立新的資源群組，然後按一下 **OK**（確定）。
- 按一下 **Create**（建立）。儀表板上的一個新動態磚將顯示範本部署的進度。



©2023 Palo Alto Networks, Inc.

STEP 4 | 接下來的步驟：

1. 登入防火牆的網頁介面。

   使用 Web 瀏覽器的安全連線 (https)，登入防火牆的 DNS 名稱。輸入您稍早定義的使用者名稱/密碼。您將看見憑證警告；此為正常現象。繼續開啟網頁。

2. 啟動 VM-Series 防火牆上的授權。

   1. 建立支援帳戶和註冊 VM-Series 防火牆（使用驗證碼）。
   2. 在防火牆網頁介面上，選取 **Device**（裝置） > **Licenses**（授權），然後選取 **Activate feature using authentication code**（使用驗證碼啟動功能）。
   3. 輸入您在支援入口網站上註冊的容量驗證碼。防火牆將連線至更新伺服器 (updates.paloaltonetworks.com)，並自動下載授權及重新啟動。
   4. 在 **Dashboard**（儀表板）上重新登入 Web 介面，確認顯示有效的 **Serial#**（序號）。

      VM Mode（**VM** 模式）顯示為 Microsoft Azure。

      如果顯示 Unknown 一詞，則意味設備未經授權。若要在防火牆上檢視流量日誌，您必須安裝有效的容量授權。

STEP 5 | 7

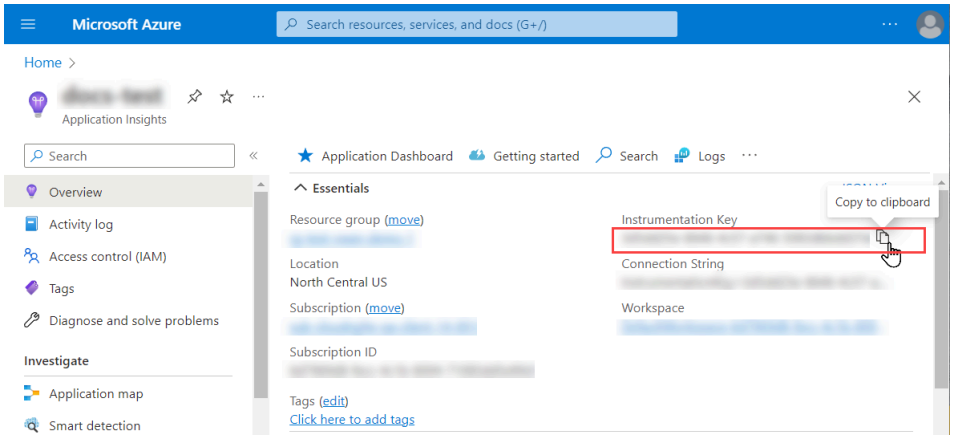
©2023 Palo Alto Networks, Inc.

啟用 VM-Series 防火牆上的 Azure Application Insights

Azure 上的 VM-Series 防火牆原本可發佈自訂 PAN-OS 度量至您可用來直接從 Azure 入口網站監控防火牆的 Azure Application Insights 中。這些度量可讓您評估效能和使用模式，您可據以設定警報並採取行動以將事件自動化，如啟動或結束 VM-Series 防火牆實例。請參閱作為監控使用發佈的自訂 PAN-OS 度量以瞭解可用度量的相關描述。

STEP 1 | 在 Azure 入口網站建立您的 Application Insights 實例以監控防火牆，並從 **Configure**（設定）> **Properties**（屬性）複製 **Instrumentation Key**（儀表金鑰）。

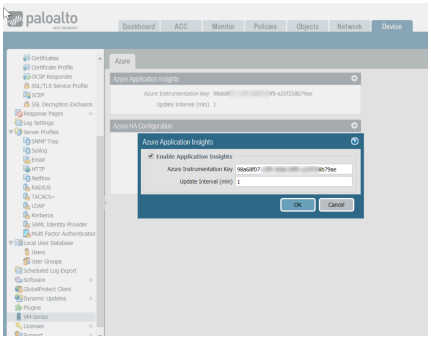
防火牆需要此金鑰以驗證 Application Insights 實例並向其發佈度量。關於所需的權限，請參閱Azure Service 上的 VM-Series 的服務主體權限。



STEP 2 | 啟用此防火牆以發佈度量至您的 Application Insights 實例。

1. 登入 Azure 上的 VM-Series 防火牆。
2. 選取 **Device**（裝置） > **VM-Series** > **Azure**。
3. 編輯 **Azure Application Insights** 並輸入您早先複製的儀表金鑰。

   發佈度量的預設間隔時間為五分鐘。您可以在 1 至 60 分鐘間變更此預設值。



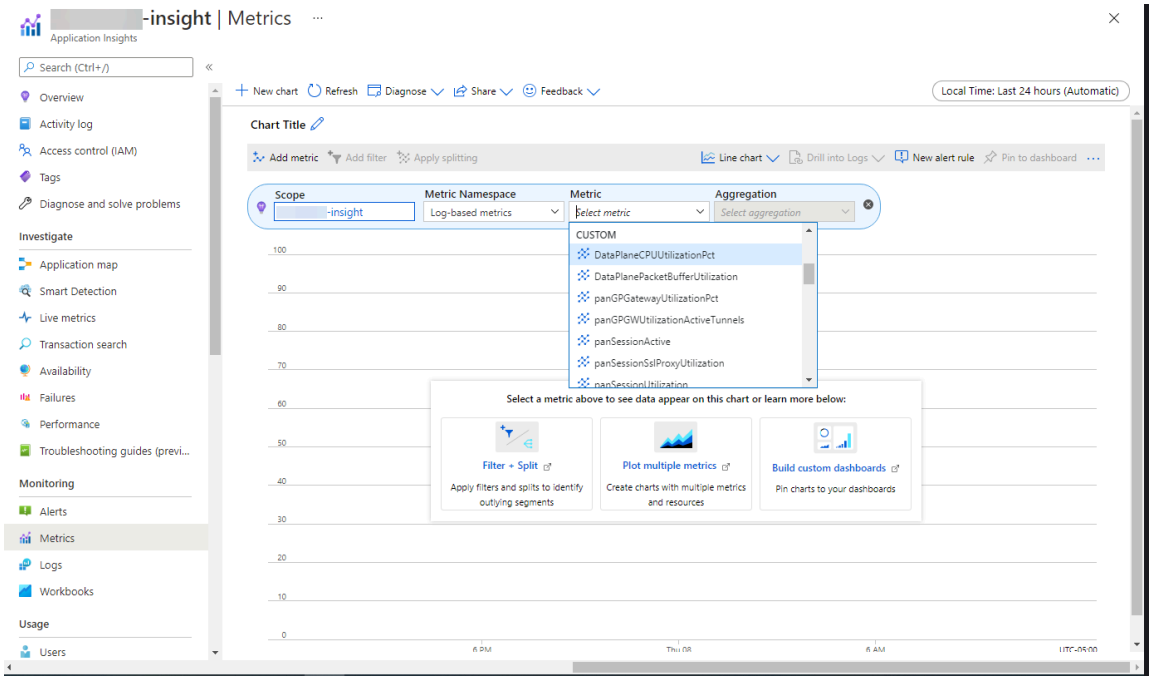
4. **Commit**（提交）您的變更。

   防火牆會對其產生系統日誌，記錄對 Azure Application Insights 的驗證是成功還是失敗。

©2023 Palo Alto Networks, Inc.

STEP 3 | 確認您可以檢視 Azure Application Insights 儀表板上的度量。

1. 在 Azure 入口網站上，選取 Application Insights 實例，然後選取 **Monitoring**（監控） > **Metrics**（度量），以檢視 PAN-OS 自訂度量。



2. 選取您想要監控的度量，以瞭解趨勢及觸發警報。參閱 Microsoft Azure 文件以瞭解探索在 Application Insights 上的度量的詳細內容。

 ©2023 Palo Alto Networks, Inc.

在 Azure 上監控

在 Microsoft® Azure® 上監控可讓您動態更新安全性政策規則，對您的 Azure 訂閱內部署的所有資產，一致地強制執行安全性政策。若要啟用此功能，您需要安裝 Azure 專用 Panorama 外掛程式，並啟用 Panorama 與 Azure 訂閱之間的 API 通訊。然後，Panorama 就可以收集所有 Azure 資產的 IP 位址至標籤對應，並將 Azure 資源推送或散佈到您的 Palo Alto Networks® 防火牆。

- 關於在 Azure 上監控
- 設定 Azure 外掛程式在 Panorama 上監控
- 在 Azure 上使用 Panorama 外掛程式監控的屬性

關於在 Azure 上監控

當您在 Azure 公共雲端中部署或終止虛擬機器時，可使用 Azure 專用 Panorama 外掛程式，對這些工作負載一致地強制執行安全性原則規則。

Azure 專用 Panorama 外掛程式專為調整規模而建立，讓您可在 Azure 公共雲端上監控多達 100 個 Azure 訂閱。有了此外掛程式，您可將 Panorama 作為錨點來輪詢標籤訂閱，然後將中繼資料（IP 位址-至-標籤對應）散佈至一個裝置群組的多個防火牆。由於 Panorama 會與 Azure 訂閱通訊以擷取 Azure 資源資訊，因此您可精簡對雲端環境發出的 API 呼叫次數。雖然您可以在防火牆上本機定義安全性原則，但使用 Panorama 和外掛程式可集中管理安全性原則，確保混合和雲端原生架構的原則保持一致。

請參閱「相容性矩陣」中的 Panorama 外掛程式版本資訊。

設定 Azure 外掛程式在 Panorama 上監控

若要找到您的組織在 Azure 雲端部署的所有工作負載，您需要在 Panorama 上安裝 Azure 外掛程式並設定監控定義，以便 Panorama 向您的 Azure 訂閱驗證並擷取 Azure 工作負載的相關資訊。Panorama 會擷取 Azure 資源的主要私人 IP 位址及相關標籤。如需 Panorama 支援的中繼資料元素清單，請參閱在 Azure 上使用 Panorama 外掛程式監控的屬性。

在 Panorama 擷取屬性後，若要將資源資訊從 Panorama 推送至防火牆，您必須將防火牆（硬體或 VM-Series）新增為 Panorama 上受管理的裝置，並將防火牆分組為一個或多個裝置群組。然後，您可指定哪些裝置群組屬於通知群組，通知群組是監控定義中的組態元素，Panorama 使用其註冊從 Azure 擷取的 IP 位址-至-標籤對應。

最後，若要在所有 Azure 工作負載上一致地強制執行安全性政策，您必須設定動態位址群組，並在允許或拒絕流量流向 Azure 資源 IP 位址的政策規則中參考這些群組。若要簡化組態並從 Panorama 集中管理原則及物件，您可在 Panorama 上定義動態位址群組與安全性原則規則並將其推送至防火牆，而非在每個防火牆上本機管理動態位址群組和安全性原則規則。

Azure 外掛程式用於監控 *Azure* 公共雲端的 *Azure* 資源。不支援 *Azure Government* 或 *Azure China*。

- 規劃使用 Azure 外掛程式進行 VM 監控的檢查清單
- 安裝 Azure 外掛程式

©2023 Palo Alto Networks, Inc.

- 設定 Azure 外掛程式以進行監控

規劃使用 Azure 外掛程式進行監控的檢查清單

- 設定啟動目錄應用程式與服務主體以啟用 API 存取—若要 Panorama 與 Azure API 互動並收集有關工作負載的資訊，您需要建立啟動目錄服務主體。此服務主體擁有驗證 Azure AD 和存取訂閱內資源所需的權限。

  若要完成此設定，您必須有權限向 Azure AD 租用戶註冊應用程式，並將應用程式指派給訂閱中的角色。如果您沒有必要權限，可要求 Azure AD 或訂閱管理員建立具有 IAM 讀者角色或 Azure Service 上的 VM-Series 的服務主體權限 中指定之自訂權限的服務主體。

- 請確保訂閱 ID 在服務主體中是唯一的。Panorama 僅允許您使用一個服務主體監控 Azure 訂閱。您可監控多達 100 個 Azure 訂閱，包含 100 個服務主體資源。從 Azure 版本 3.2.0 的 Panorama 外掛程式開始，您可以監控多達 500 個 Azure 訂閱。請注意下表中描述的處理時間。

	訂閱數量				
	100	**200**	**300**	**400**	**500**
系統資源利用率	• CPU：22% • 記憶體：0.025 MB	• CPU：23.8% • 記憶體：0.025 MB	• CPU：31.8% • 記憶體：0.025 MB	• CPU：28.6% • 記憶體：0.025 MB	• CPU：39.2% • 記憶體：0.025 MB
處理所有監控定義的平均時間	1 小時 15 分鐘	2 小時 30 分鐘	3 小時 30 分鐘	4 小時	5 小時
平均標籤更新處理時間	5 分鐘	10 分鐘	15 分鐘	20 分鐘	25 分鐘

上表中的資訊是在具有 *8* 個 *vCPU* 和 *32GB* 內存的實例上擷取。

©2023 Palo Alto Networks, Inc.

- Panorama 可將多達 8000 個 IP 位址-至-標籤對應推送至指派給裝置群組的防火牆或虛擬系統。檢閱 Panorama 和受管理防火牆的需求：
  - 最低系統需求（請參閱「相容性矩陣」中的 Panorama 外掛程式資訊）：

    執行 Panorama 8.1.3 或更新版本的 Panorama 虛擬設備或硬體型 Panorama 設備，且具有有效支援授權和裝置管理授權可管理防火牆。

    已授權且執行 PAN-OS 8.0 或 8.1 的新世代防火牆。
  - 您必須在 Panorama 上將防火牆新增為受管理的裝置，並建立裝置群組，以便設定 Panorama 將其擷取的資訊通知這些群組。裝置群組可包括 VM-Series 防火牆或硬體防火牆上的虛擬系統。
  - Panorama 外掛程式可擷取和註冊的標籤數目如下：

    Panorama 若執行 8.1.3 或更新版本，且管理執行 PAN-OS 8.1.3 或較低版本的防火牆，則裝置群組內包含的防火牆或虛擬系統可以具有 7000 個各含 10 個標籤的 IP 位址，或 6500 個各含 15 個標籤的 IP 位址。

    在對執行 PAN-OS 8.0.x 的防火牆進行管理的 Panorama 8.1.3 或更新版本上，具有 2500 個 IP 位址，每個包含 10 個標籤。
    - 如果您的 Panorama 設備採用高可用性組態，則您必須在兩個 Panorama 端點上手動安裝相同版本的 Azure 外掛程式。

      您僅在主動 ***Panorama*** 端點上設定 ***Azure*** 外掛程式。提交時，組態將同步至被動 ***Panorama*** 端點。僅主動 ***Panorama*** 對等會輪詢您設定要監控的 ***Azure*** 訂閱。

安裝 Azure 外掛程式

若要開始在 Azure 上監控，您需要下載 Azure 外掛程式並安裝在 Panorama。如果您有 Panorama HA 組態，請在每個 Panorama 端點上重複此安裝程序。

如果您目前已安裝 ***Panorama*** 外掛程式，安裝（或解除安裝）另一個外掛程式的程序需要重新啟動 ***Panorama*** 才能提交變更。因此，請在計畫性維護期間安裝額外的外掛程式。

如果您在安裝了多個外掛程式的 HA 配對中安裝了一個獨立的 Panorama 或兩個 Panorama 設備，則在未設定一或多個外掛程式的情況下，外掛程式可能不會收到更新的 IP-Tag 資訊。發生這種情況是因為 Panorama 不會將 IP-Tag 資訊轉送到未設定的外掛程式。此外，如果一或多個 Panorama 外掛程式未處於「已註冊」或「成功」狀態（每個外掛程式的正狀態不同），則可能會出現此問題。在繼續或執行下述命令之前，請確保您的外掛程式處於正狀態。

如果遇到此問題，有兩種權宜方案：

- 解除安裝未設定的外掛程式。建議您不要安裝未打算立即設定的外掛程式

©2023 Palo Alto Networks, Inc.

- 您可以使用以下命令來變通處理此問題。對每個 Panorama 實例上的每個未設定外掛程式執行以下命令，以防止 Panorama 等待傳送更新。否則，防火牆可能會遺失一些 IP-Tag 資訊。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以透過執行以下命令來取消此命令：

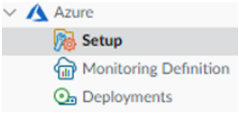
  request plugins dau plugin-name <plugin-name> unblock-device-push no

上述的命令在重新啟動後不會持續存在，並且必須在任何後續重新啟動時再次使用。對於 HA 配對中的 Panorama，必須在每個 Panorama 上執行命令。

STEP 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。

STEP 2 | 選取 **Download**（下載）並 **Install**（安裝）外掛程式。

在您成功安裝後，Panorama 將重新整理且 Azure 外掛程式將顯示於 **Panorama** 頁籤上。



STEP 3 | 重新啟動 Panorama。

選取 **Panorama** > **Setup**（設定） > **Operations**（操作） > **Reboot Panorama**（重新啟動 **Panorama**）

設定 Azure 外掛程式以進行監控

若要開始監控 Azure 公共雲端部署中的資源，在安裝 Azure 外掛程式後，您必須建立監控定義。此定義指定授權在您要監控的 Azure 訂閱內存取資源的服務主體，及包含 Panorama 應將其擷取的所有 IP 位址-至-標籤對應推送至的防火牆之通知群組。為了執行原則，您之後必須建立動態位址群組並在安全性原則中引用它們。動態位址群組可讓您篩選要比對的標籤，以便防火牆可取得為標籤註冊的主要私人 IP 位址，然後根據您定義的原則規則允許或拒絕存取傳入和傳出工作負載的流量。

STEP 1 | 登入 Panorama 網頁介面。

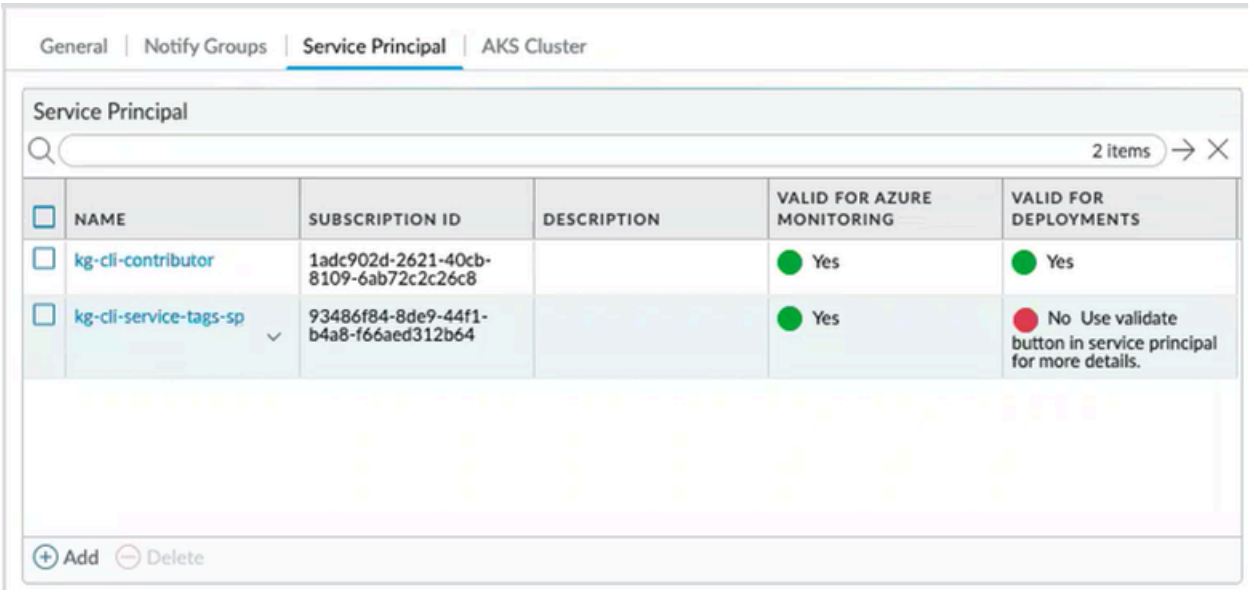
 ©2023 Palo Alto Networks, Inc.

STEP 2 | 設定下列物件以在 Azure 上啟用監控。

- 新增服務主體。

  服務主體為您在 Azure 入口網站建立的服務帳戶。此帳戶會連接至 Azure AD 且擁有存取和監控 Azure 訂閱中資源的有限權限。

  1. 選取 **Panorama** > **Plugins**（外掛程式） > **Azure** > **Setup**（設定） > **Service Principal**（服務主體） > **Add**（新增）。

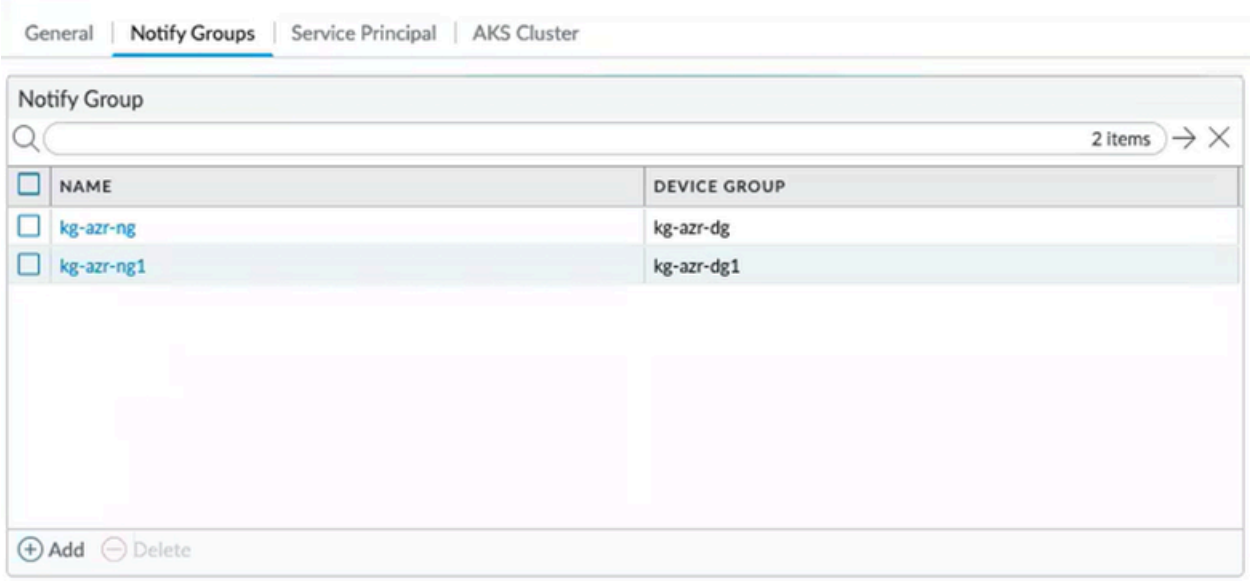


  2. 輸入**Name**（名稱），然後選擇輸入 **Description**（說明）以識別服務帳戶。
  3. 為您要監控的 Azure 訂閱輸入 **Subscription ID**（訂閱 **ID**）。您必須登入 Azure 入口網站才能取得此訂閱 ID。
  4. 輸入 **Client Secret**（用戶端密碼）並重新輸入以確認。
  5. 輸入 **Tenant ID**（租用戶 **ID**）。租用戶 ID 為您在設定啟動目錄應用程式時儲存的目錄 ID。
  6. 按一下 **Validate**（驗證）以確認您輸入的金鑰和 ID 有效，且 Panorama 可以使用 API 與 Azure 訂閱通訊。

- 新增通知群組。

  1. 選取 **Panorama** > **Plugins**（外掛程式） > **Azure** > **Setup**（設定） > **Notify Groups**（通知群組） > **Add**（新增）。

©2023 Palo Alto Networks, Inc.



2. 輸入 **Name**（名稱）和選用 **Description**（說明），以識別防火牆群組供 Panorama 推送其擷取的資訊。
3. 選取 **Device Groups**（裝置群組），這是一組防火牆或虛擬系統，可供 Panorama 推送從您的 Azure 訂閱擷取的資訊（IP 位址至標籤對應）。防火牆會使用此更新，決定構成原則中參照之動態位址群組的最新成員清單。

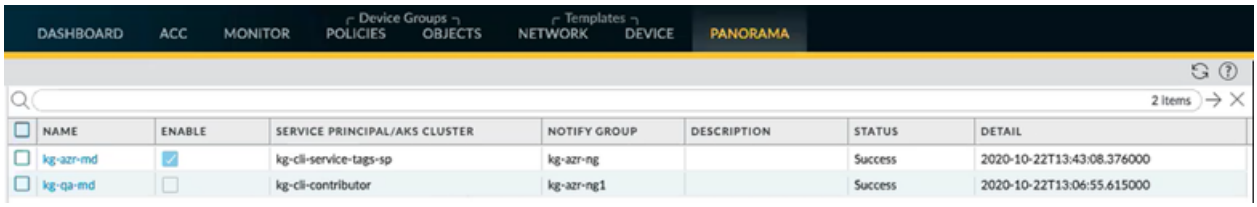
   仔細考慮您的裝置群組。

   - 由於監控定義只能包含一個通知群組，因此請確保選取通知群組內的所有相關裝置群組。如果您要取消註冊 Panorama 推送至通知群組中所包含防火牆的標籤，必須刪除監控定義。
   - 若要在已針對多個虛擬系統啟用的防火牆上註冊標籤至所有虛擬系統，您必須在 Panorama 上新增每個虛擬系統至單獨的裝置群組並將裝置群組指派給通知群組。如果您將所有虛擬系統指派給一個裝置群組，Panorama 將僅註冊標籤至一個虛擬系統。
4. 確認監控已在外掛程式上啟用。必須啟用此設定，Panorama 才能與 Azure 公共雲端通訊以進行監控。

   Enable Monitoring（啟用監控）的核取方塊在 **Panorama** > **Plugins**（外掛程式） > **Azure** > **Setup**（設定） > **General**（一般）上。

©2023 Palo Alto Networks, Inc.

STEP 3 | 建立 **Monitoring Definition**（監控定義）。



當您新增監控定義時，其依預設會啟用。

- 選取 **Panorama** > **Plugins**（外掛程式） > **Azure** > **Monitoring Definition**（監控定義），以 **Add**（新增）定義。
- 輸入 **Name**（名稱），然後選擇輸入 **Description**（說明）以識別您使用此定義的 Azure 訂閱。
- 選取 **Service Principal**（服務主體）和 **Notify Group**（通知群組）。

  Panorama 需要您在服務主體組態中指定的金鑰與 ID 以產生 Azure Bearer Token，用於在 API 呼叫標頭中收集關於工作負載的資訊。

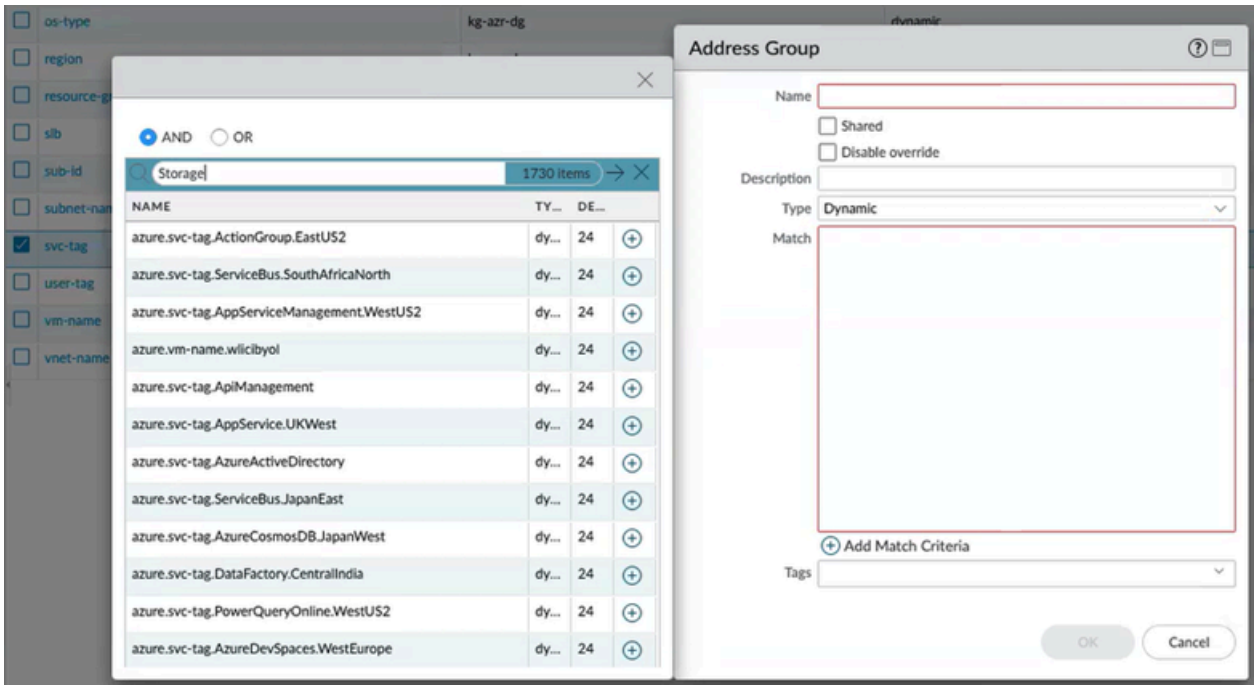
STEP 4 | 在 Panorama 上 **Commit**（提交）變更。

確認監控定義的狀態顯示為「成功」。如果失敗，請確認您已正確輸入 Azure 訂閱 ID 並提供了服務主體的正確金鑰與 ID。

©2023 Palo Alto Networks, Inc.

STEP 5 | 確認您可以在 Panorama 上檢視資訊，並定義動態位址群組的比對準則。

部分瀏覽器延伸可能會封鎖 *Panorama* 與 *Azure* 之間的 *API* 呼叫，進而防止 *Panorama* 接收比對準則。如果 *Panorama* 未顯示比對準則，而且您使用瀏覽器延伸，則請停用延伸，並 *[Synchronize Dynamic Objects*（同步處理動態物件）*]* 以填入 *Panorama* 可用的標籤。



發生 *HA* 故障時，新啟動的 *Panorama* 將嘗試重新連線至 *Azure* 雲端並擷取所有監控定義的標籤。如果在重新連接甚至一個監控定義時出現錯誤，*Panorama* 會生成一條系統日誌消息

> *HA* 切換後無法處理訂閱；需要使用者干預。

當您看到此錯誤時，您必須登入 *Panorama* 並修復問題，例如刪除無效訂閱或提供有效認證，並提交您的變更以使 *Panorama* 能夠重新連接並檢索所有監控定義的標籤。即使中斷 *Panorama* 與 *Azure* 雲端的連線，防火牆還是會有容錯移轉之前所擷取的所有標籤清單，因此可以繼續對該 *IP* 位址清單進行強制執行政策。*Panorama* 只有在您刪除監控定義時才會移除所有與訂閱相關的標籤。監控此問題的最佳做法是，從 *Panorama* 設定動作導向的日誌轉送至 HTTPS 目的地，以便您立即採取措施。

©2023 Palo Alto Networks, Inc.

在 Azure 上使用 Panorama 外掛程式監控的屬性

使用 Azure 專用 Panorama 外掛程式時，Panorama 可以收集以下 Microsoft® Azure® 部署內虛擬電腦上的中繼資料元素或屬性組。Panorama 可為每個 VM 擷取總共 32 個標籤，包括 11 個預定義的標籤和最多 21 個使用者定義的標籤。

標籤的最大長度為 *127* 個字元。如果標籤長度超過 *127* 個字元，*Panorama* 則不會擷取此標籤並將其在防火牆上註冊。此外，標籤不應包含非 *ASCII* 特殊字元，例如 *{* 或 *"*。

所有 Azure 專用 Panorama 外掛程式版本會監控下列屬性。

虛擬電腦

VM 監控	範例
VM 名稱	azure-tag.vm-name.web_server1
網路安全性群組名稱	azure-tag.nsg-name.myNSG
作業系統類型	azure-tag.os-type.Linux
作業系統發行商	azure-tag.os-publisher.Canonical
作業系統優惠	azure-tag.os-offer.UbuntuServer
作業系統 **SKU**	azure-tag.os-sku.14.04.5-LTS
子網路	azure-tag.subnet.webtier
VNet	azure-tag.vnet.untrustnet
Azure 區域	azure-tag.region.east-us
資源群組名稱	azure-tag.resource-group.myResourceGroup
訂閱 **ID**	azure.sub-id.93486f84-8de9-44f1-b4a8-f66aed312b64
使用者定義的標籤 支援多達 21 個使用者定義標籤。使用者定義的標籤按字母順序排序，前 21 個標籤可用於 Panorama 及防火牆。	azure-tag.mytag.value

負載平衡器

©2023 Palo Alto Networks, Inc.

對於每個應用程式閘道和標準負載平衡器（公共和私人 IP 位址），Azure 專用 Panorama 外掛程式版本 3.0 或更新版本支援標籤。每個負載平衡器已預先定義資源群組、負載平衡器和地區的標籤，支援最多 21 個專屬於負載平衡的使用者定義標籤。

負載平衡器標籤	範例
負載平衡器	azure.<type>.myLoadBalancer
Azure 區域	azure-tag.region.east-us
資源群組名稱	azure-tag.resource-group.myResourceGroup
使用者定義的標籤 支援多達 21 個使用者定義標籤。使用者定義的標籤按字母順序排序，前 21 個標籤可用於 Panorama 及防火牆。	azure-tag.mytag.value

子網路**/VNET**

對於訂閱中的每個子網路和 VNET，Azure 專用 Panorama 外掛程式版本 3.0 或更新版本支援標籤。每個子網路和 VNET 標籤都與完整的 IP CIDR 範圍相關聯，所以您可以根據 CIDR 範圍來建立政策，而非根據個別 IP 位址。此外掛程式會查詢訂閱中的每個子網路和 VNET，並為它們建立標籤。

子網路和 **VNET** 標籤	範例
子網路名稱	azure.subnet-name.web
VNET 名稱	azure.vnet-name.myvnet

服務標籤監控

Azure 專用 Panorama 外掛程式版本 3.0 支援服務標籤。

Azure 服務標籤簡化 Azure virtual machine（虛擬機器 - VM）和 Azure 虛擬網路的安全性，因為您可以將網路存取限於您想要使用的 Azure 服務。服務標籤代表特定 Azure 服務的一組 IP 位址首碼。例如，標籤可以代表所有儲存區 IP 位址。

此外掛程式每天呼叫 API (5:00 am UTC) 從 Azure 入口網站擷取所有服務標籤，剖析承載以產生 IP-服務對應，並將對應儲存在外掛程式資料庫中。對應會傳遞至 configd，再傳遞至 Panorama。如果 API 呼叫無法傳回服務資訊，則外掛程式會從 **`service_tags_public.json`** 的內容產生 IP-服務對應。外掛程式日誌會報告 IP-服務對應的來源，即每日擷取或 JSON 檔案。

此外掛程式也會隨著新安裝外掛程式、提交事件及監控定義新增或刪除，而更新服務標籤。

IP-服務對應範例如下所示：

©2023 Palo Alto Networks, Inc.

服務名稱：**AppServiceManagementazure.svc-tag.<service-name>**範例：**azure.svc-tag.AppServiceManagement.WestUS2 Public IP CIDRs: 13.166.40.0/26 54.179.89.0/18**

©2023 Palo Alto Networks, Inc.

在 Azure 上設定主動/被動 HA

您可以在採用主動/被動高可用性 (HA) 設定的 Azure 上設定一對 VM-Series 防火牆。針對 Azure 上的 HA，您必須在相同的 Azure 資源群組內部署兩個防火牆 HA 對等，且必須在兩個 HA 對等上安裝相同版本的 VM-Series 外掛程式。

- 在 Azure 上設定主動/被動 HA（南北向和東西向流量）—如果您已在 Azure 基礎結構中部署網際網路型應用程式，且需要保護南北向流量，您將需要以浮動 IP 位址保護容錯移轉的流量。此浮動 IP 位址支援外部連線，且一律會連接至主動對等。在容錯移轉時，卸除 IP 位址並將其重新連接至現行主動對等的程序，可能需要幾分鐘的時間。
- 在 Azure 上設定主動/被動 HA（僅限東西向流量）—如果您的應用程式存取和安全需求限於 Azure 基礎結構內，且您只需要保護東西向流量，則不需要浮動 IP 位址。反之，HA 實作會自動重新設定 Azure 路由表中的 UDR，以提供更快的容錯移轉速度。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

若要對 Azure 上的 VM-Series 防火牆啟用 HA，您必須建立 Azure Active Directory 應用程式和服務主體，其中包括下表列出的權限。

Azure HA 類型	權限	角色範圍

次要 IP 移動 HA	`"Microsift.Authorization/*/read""Microsift.Compute/virtualMachines/read""Microsift.Network/networkInterfaces/*""Microsift.Network/networkSecurityGroups/*""Microsift.Network/virtualNetworks/join/action""Microsift.Network/virtualNetworks/subnets/join/action"`
	只有在已指派公共 IP 位址給任何資料介面時，才需要以下權限。建議使用標準 SKU 介面。
	`"Microsift.Network/publicIPAddresses/join/action""Microsift.Network/publicIPAddresses/read""Microsift.Network/publicIPAddresses/write"`
		· 部署 VM 的虛擬網路
		· 兩個 VM-Series 防火牆
		· 兩個 VM-Series 防火牆的 NIC
		· 網路安全性群組
		· VM-Series 防火牆的公共 IP 位址

UDR HA	`"Microsift.Authorization/*/read""Microsift.Compute/virtualMachines/`	· 兩個 VM-Series 防火牆

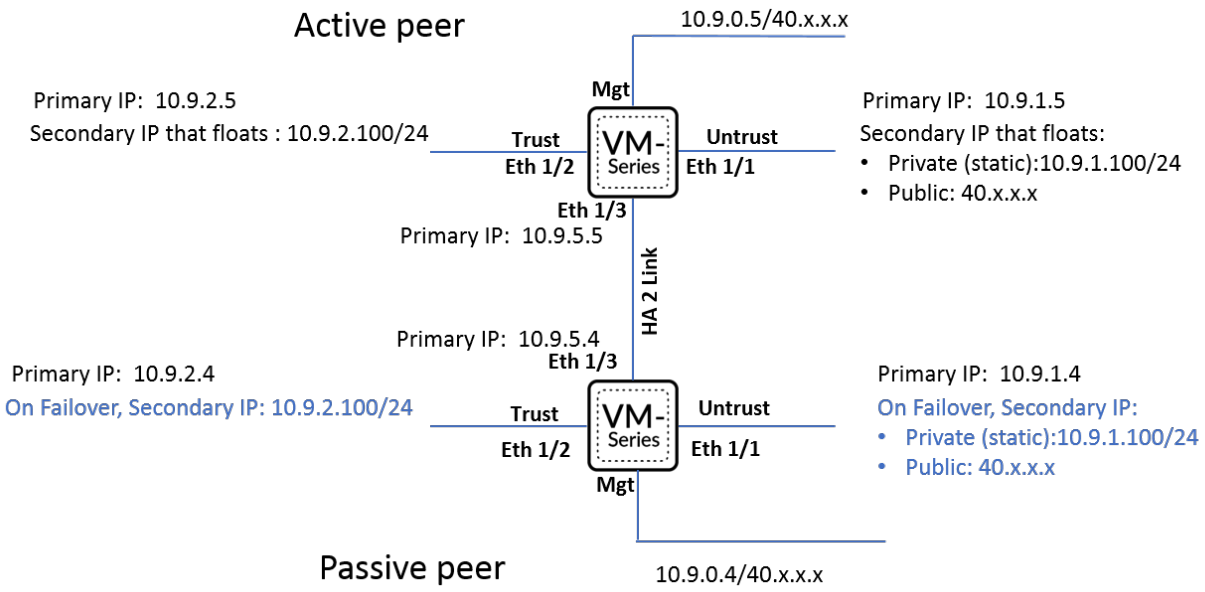
©2023 Palo Alto Networks, Inc.

Azure HA 類型	權限	角色範圍
	read""Microsift.Network/routeTables/*""Microsift.Network/networkInterfaces/*"	· 兩個 VM-Series 防火牆的 NIC · 與 UDR 相關聯的路由表
次要 IP 移動和 UDR	"Microsift.Authorization/*/read""Microsift.Compute/virtualMachines/read""Microsift.Network/networkInterfaces/*""Microsift.Network/networkSecurityGroups/*""Microsift.Network/routeTables/*""Microsift.Network/virtualNetworks/join/action""Microsift.Network/virtualNetworks/subnets/join/action" 只有在已指派公共 IP 位址給任何資料介面時，才需要以下權限。建議使用標準 SKU 介面。 "Microsift.Network/publicIPAddresses/join/action""Microsift.Network/publicIPAddresses/read""Microsift.Network/publicIPAddresses/write"	· 部署 VM 的虛擬網路 · 兩個 VM-Series 防火牆 · 兩個 VM-Series 防火牆的 NIC · 網路安全性群組 · VM-Series 防火牆的公共 IP 位址 · 與 UDR 相關聯的路由表

在 Azure 上設定主動/被動 HA（南北向和東西向流量）

如果您要保護 Azure 基礎結構中各個應用程式的南北向流量，請對可在不同的對等間快速移動的浮動 IP 位址使用此工作流程。因為您無法移動 Azure 上與防火牆主要介面相關聯的 IP 位址，所以需要指派可作為浮動 IP 位址的次要 IP 位址。主動防火牆關閉時，浮動 IP 位址會從主動防火牆移至被動防火牆，讓被動防火牆可以在變成主動對等時盡快無縫地保護流量安全。除了浮動 IP 位址之外，HA 對等也需要 HA 連結（控制連結 (HA1) 和資料連結 (HA2)）來同步處理資料與維護狀態資訊。

©2023 Palo Alto Networks, Inc.



- 設定防火牆以啟用 HA
- 設定 Azure 的 VM-Series 防火牆上的主動/被動 HA

設定防火牆以啟用 HA

收集下列詳細資料，以設定 Azure 的 VM-Series 防火牆的 HA。

設定 Active Directory 應用程式和服務主體，以程式設計方式存取 API。

- 若要讓防火牆與 Azure API 互動，您需要建立 Azure Active Directory 服務主體。服務主體具有驗證 Azure AD 與存取訂閱中資源所需的權限。若要完成此設定，您必須有權限向 Azure AD 租用戶註冊應用程式，並將應用程式指派給訂閱中的角色。如果您沒有必要權限，可要求 Azure AD 或訂閱管理員建立服務主體。有關所需權限，請參閱上表。複製下列詳細資料，稍後用於此工作流程：
  - 用戶端 **ID**—與 Active Directory 相關聯的應用程式 ID（在 Azure 入口網站上，按一下 **Home**（首頁） > **Azure Active Directory** > **App registrations**（應用程式註冊），選取應用程式並複製 ID）。
  - 租用戶 **ID**—與 Active Directory 相關聯的目錄 ID（在 Azure 入口網站上，按一下 **Home**（首頁） > **Azure Active Directory** > **Properties**（屬性） > **Directory ID**（目錄 **ID**），選取應用程式並複製 ID）。
  - **Azure Subscription ID**（**Azure** 訂閱 **ID**）—您已部署防火牆的 Azure 訂閱。您必須登入 Azure 入口網站才能取得此訂閱 ID。

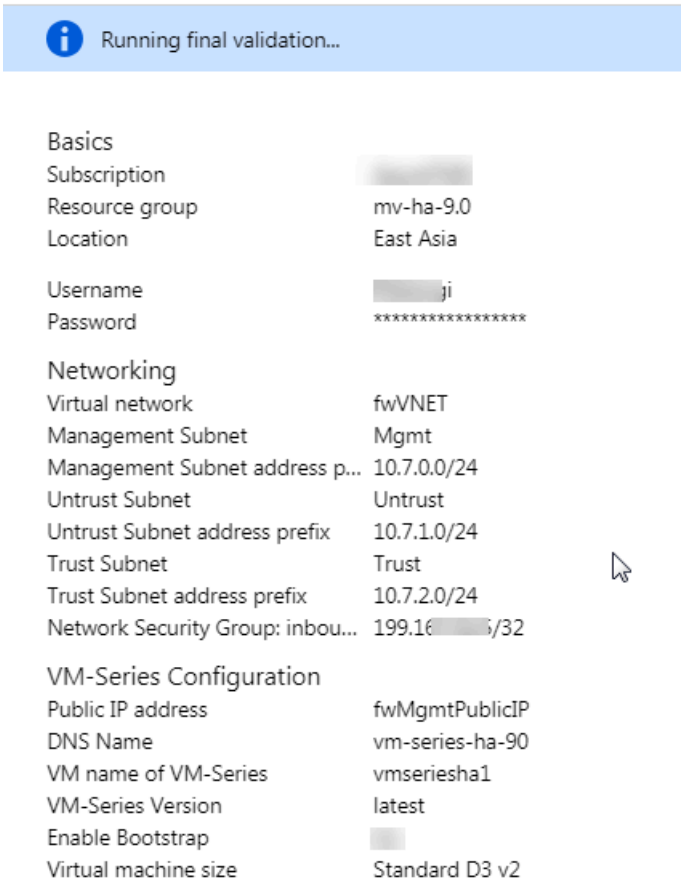
©2023 Palo Alto Networks, Inc.

- 資源群組名稱— 您已部署要設定為 HA 對等的防火牆的資源群組名稱。兩個防火牆都必須位於相同的資源群組中。
- 秘密金鑰—與 Active Directory 應用程式相關聯的驗證金鑰（在 Azure 入口網站上，按一下 **Home**（首頁） > **Azure Active Directory** > **Certificates & secrets**（憑證和機密），複製 **Client secrets**（用戶端密碼）下的 **Value**（值）。如果您沒有秘密金鑰，請先建立秘密金鑰，然後複製值）。若以應用程式形式登入，您必須同時提供金鑰值和應用程式 ID。

這樣就可知道從何處取得在相同 Azure 資源群組內部署 VM-Series 防火牆所需的範本。

針對 HA 設定，兩個 HA 對等都必須屬於相同的 Azure 資源群組。如果您從 Azure Marketplace 部署防火牆的第一個實例，而且必須使用自訂 ARM 範本或 Palo Alto Networks 範例 GitHub 範本將防火牆的第二個實例部署至現有資源群組。您需要自訂範本或 Palo Alto Networks 範例範本的原因是 Azure 不支援將防火牆部署至不是空的資源群組。

複製第一個防火牆實例的部署資訊。例如：



比對上方螢幕擷取畫面所顯示的 **VM Name of VM-Series firewall**（**VM-Series** 防火牆的 **VM** 名稱）與防火牆 Web 介面上的 **Hostname**（主機名稱）。您必須在 **Device**（裝置） > **Setup**（設定） > **Management**（管理）上新增相同的名稱，因為防火牆的主機名稱是用來觸發容錯移轉。

©2023 Palo Alto Networks, Inc.

規劃 Azure 的 VM-Series 防火牆上的網路介面設定。

若要設定 HA，您必須在相同的 Azure 資源群組內部署兩個 HA 對等，而且兩個防火牆的網路介面數目必須相同。每個 HA 對等最少都需要四個網路介面：

- 管理介面 **(eth0)**—與主要介面相關聯的私人和公共 IP 位址。公共 IP 位址會啟用對防火牆 Web 介面的存取與 SSH 存取。

  您可以使用管理介面上的私人 IP 介面作為 HA1 對等 IP 位址，以用於主動/被動 HA 對等之間的控制連結通訊。如果您想要專用的 HA1 介面，則必須連接每個防火牆上的其他網路介面，這表示每個防火牆上都需要五個介面。
- 不受信任介面 **(eth1/1)**—具有 /32 網路遮罩的主要私人 IP 位址，以及同時具有私人 IP 位址（任何網路遮罩）和公共 IP 位址的次要 IP 設定。

  容錯移轉時，如果被動對等轉換為主動狀態，則會從先前的主動對等卸除與次要 IP 設定相關聯的公共 IP 位址，並將其連接至目前的主動 HA 對等。
- 信任介面 **(eth1/2)**—主要和次要私人 IP 位址。容錯移轉時，如果被動對等轉換為主動狀態，則會從先前的主動對等卸除次要私人 IP 位址，並將其連接至目前的主動 HA 對等。
- **HA2 (eth 1/3)**—主要私人 IP 位址。HA2 介面是 HA 對等用於同步處理工作階段、轉送表格、IPSec 安全性關聯性和 ARP 表格的資料連結。

介面	主動防火牆對等	被動防火牆對等	說明
信任	次要 IP 位址	—	主動對等的信任介面需要容錯移轉時可浮動到其他對等的次要 IP 設定。信任介面上的這個次要 IP 設定必須是具有所保護安全的伺服器網路遮罩的私人 IP 位址。容錯移轉時，VM-Series 外掛程式會呼叫 Azure API 以從主動對等卸除此次要私人 IP 位址，並將其連接至被動對等。將此 IP 位址連接至目前的主動對等，確保防火牆可以透過不受信任介面上的浮動 IP 接收流量，並將它傳送至信任介面上的浮動 IP，再將它傳送至工作負載。
不信任	次要 IP 位址	—	防火牆的不受信任介面所需的次要 IP 設定包括一個具有不受信任子網路之網路遮罩的靜態私人 IP 位址，以及一個用於透過網際網路存取後端伺服器或工作負載的公共 IP 位址。容錯移轉時，VM-Series 外掛程式會呼叫 Azure API 以從主動對等卸除次要 IP 設定，並先將其連接至被動對等，再將其轉換為主動狀態。這個浮動次要 IP 設定的程序可讓目前的主動防火牆繼續處理流向工作負載的輸入流量。
HA2	從 Azure 管理主控台，將 NIC 新增至防火牆。	從 Azure 管理主控台，將 NIC 新增至防火牆。	在主動和被動對等上，新增專用 HA2 連結以啟用工作階段同步處理。 HA1 的預設介面是管理介面，而且您可以選擇使用管理介面，而不是將其他介面新增至防火牆。

©2023 Palo Alto Networks, Inc.

介面	主動防火牆對等	被動防火牆對等	說明
			若要啟用透過 HA2 連結的資料流程，您需要在 Azure 入口網站上新增其他網路介面，並設定防火牆上 HA2 的介面。

設定 Azure 的 VM-Series 防火牆上的主動/被動 HA

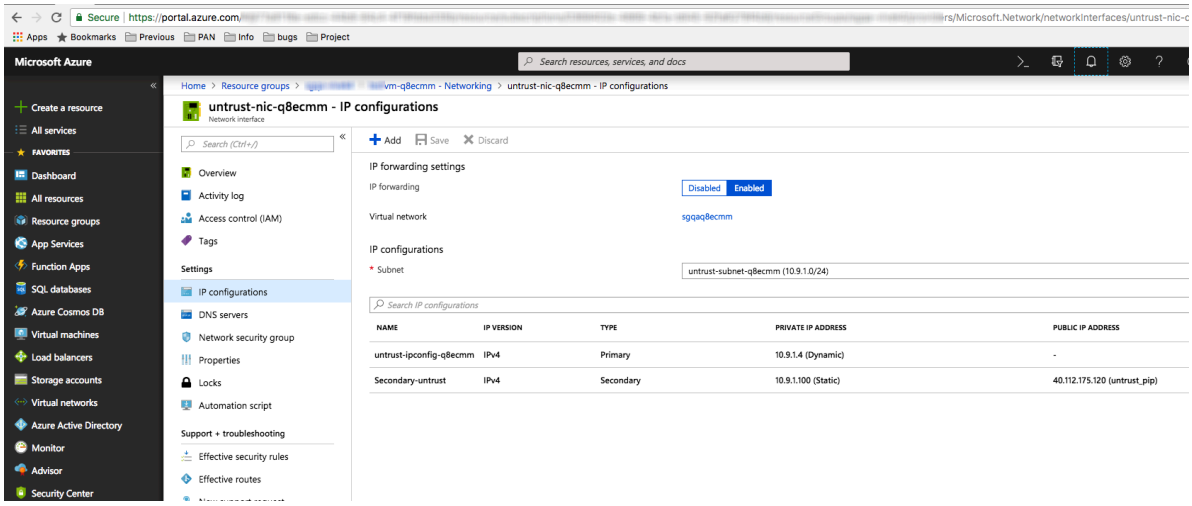
在此工作流程中，您可以使用 Azure Marketplace 中的 VM-Series 防火牆解決方案範本來部署 VM-Series 防火牆的第一個實例，以及使用範例 GitHub 範本的防火牆的第二個實例。

如果驗證金鑰（用戶端密碼）與透過 *HA* 設定來設定 *VM-Series* 防火牆所需的 *Active Directory* 應用程式相關聯，則會在防火牆和 *Panorama* 上使用 *VM-Series* 外掛程式 *1.0.4* 版予以加密。因為金鑰是透過 *VM-Series* 外掛程式 *1.0.4* 版予以加密，所以您必須在 *Panorama* 和受管理 *VM-Series* 防火牆上安裝相同版本的外掛程式，才能從 *Panorama* 集中管理防火牆。

©2023 Palo Alto Networks, Inc.

STEP 1 | 使用解決方案範本部署 VM-Series 防火牆，並針對 HA 設定網路介面。

1. 將次要 IP 設定新增至防火牆的不受信任介面。

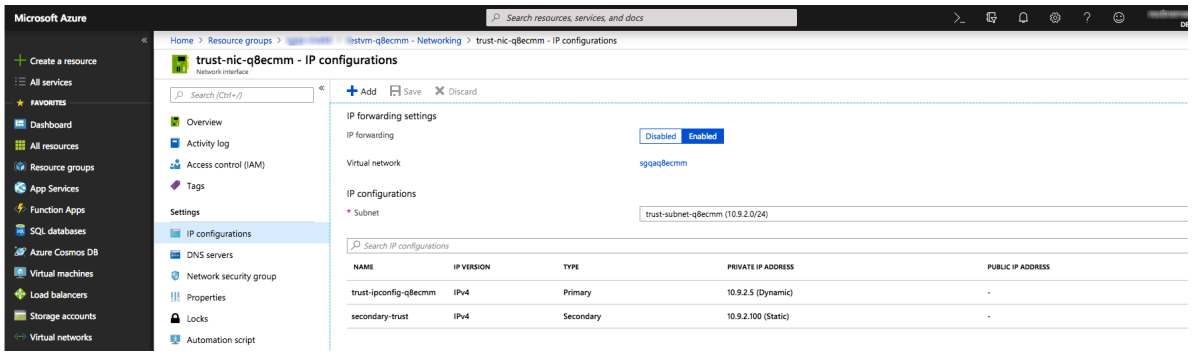


您必須將次要 IP 設定（具有私人 IP 位址（任何網路遮罩）和公共 IP 位址）連接至將指定為主動對等的防火牆。次要 IP 設定一律會隨附於主動 HA 對等，並在進行容錯移轉時從某個對等移至另一個對等。

在此工作流程中，會將此防火牆指定為主動對等。主動 HA 對等具有設定為防火牆上 HA 設定一部分的較低裝置優先順序數值，而且此值指出防火牆採用主動對等角色的偏好設定。

2. 將次要 IP 設定新增至防火牆的信任介面。

©2023 Palo Alto Networks, Inc.



信任介面的次要 IP 設定只需要靜態私人 IP 位址。容錯移轉時，此 IP 位址會從主動防火牆移至被動防火牆，因此流量會從不受信任介面流向信任介面，再流向防火牆所保護的目的地子網路。

3. 連接網路介面，以進行防火牆 HA 對等之間的 HA2 通訊。
   1. 在虛擬網路內新增子網路。
   2. 建立和連接網路介面至防火牆。
4. 在 Azure 上設定您的路由表。

   您的下一個躍點應指向浮動 IP 位址，如下所示：

©2023 Palo Alto Networks, Inc.

Routes

Search routes

Name	Address prefix	Next hop
database_server_to_frontend_server_route	10.9.3.0/24	10.9.2.100

Subnets

Search subnets

Name	Address range	Virtual network	Security group
database-server	10.9.4.0/24	vmq	-

Routes

Search routes

Name	Address prefix	Next hop
frontend_Server_to_Database_Server_route	10.9.4.0/24	10.9.1.100

Subnets

Search subnets

Name	Address range	Virtual network	Security group
frontend-server	10.9.3.0/24	vmq	-

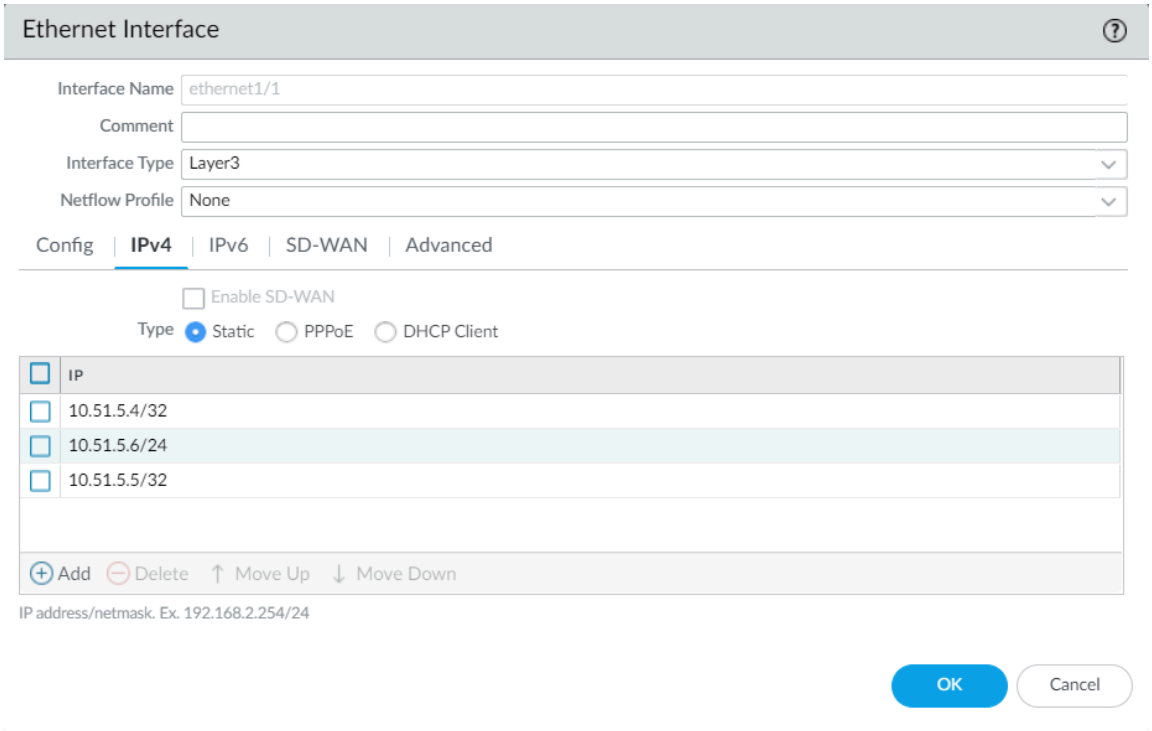
©2023 Palo Alto Networks, Inc.

STEP 2 | 在防火牆上設定介面。

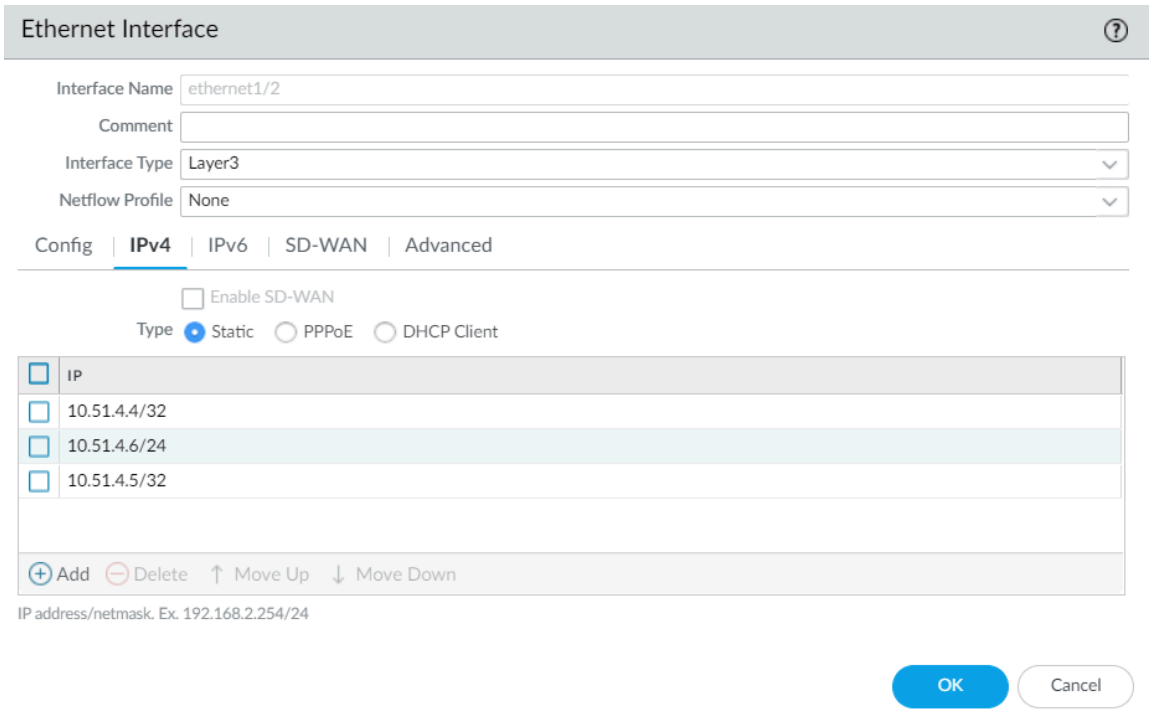
在您部署和設定被動 HA 對等之前，請在主動 HA 對等上完成這些步驟。

1. 登入防火牆 Web 介面。
2. 將乙太網路 1/1 設定為不受信任介面，並將乙太網路 1/2 設定為受信任介面。

   選取 **Network**（網路） > **Interfaces**（介面），並設定如下：



 ©2023 Palo Alto Networks, Inc.



3. 將乙太網路 1/3 設定為 HA 介面。

   若要設定 HA2 連結，請選取介面，並將 **Interface Type**（介面類型）設定為 **HA**。將連結速度和雙工設定為 auto（自動）。



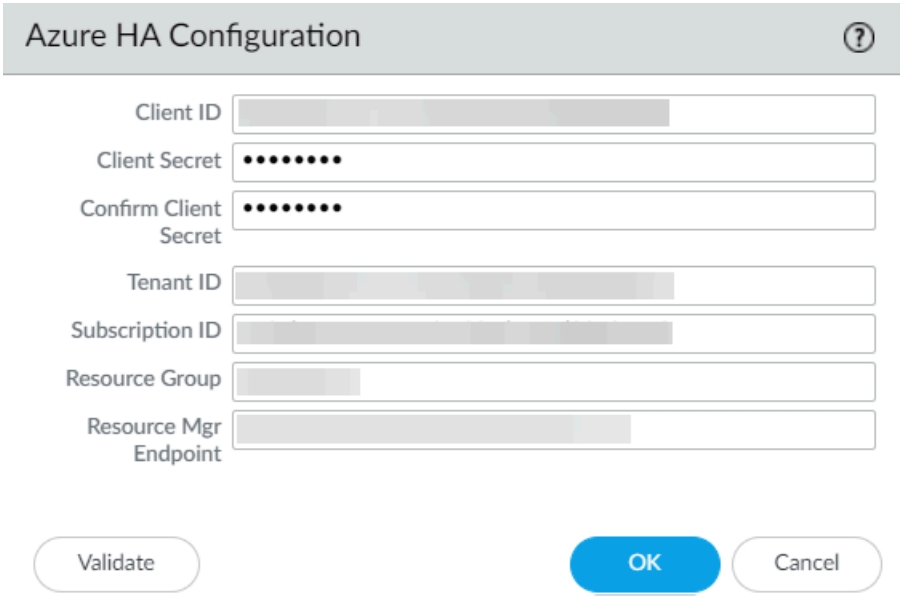
 ©2023 Palo Alto Networks, Inc.

STEP 3 | 設定 VM-Series 外掛程式，驗證您已在其中部署防火牆的 Azure 資源群組。

在 VM-Series 外掛程式上設定 Azure HA 設定。

若要加密用戶端密碼，請使用 VM-Series 外掛程式 1.0.4 版或更新版本。如果使用 Panorama 來管理防火牆，則您必須安裝 VM-Series 外掛程式 1.0.4 版或更新版本。

1. 選取 **Device**（裝置） > **VM-Series**，以在防火牆外掛程式與 Azure 資源之間透過程式設計方式存取。



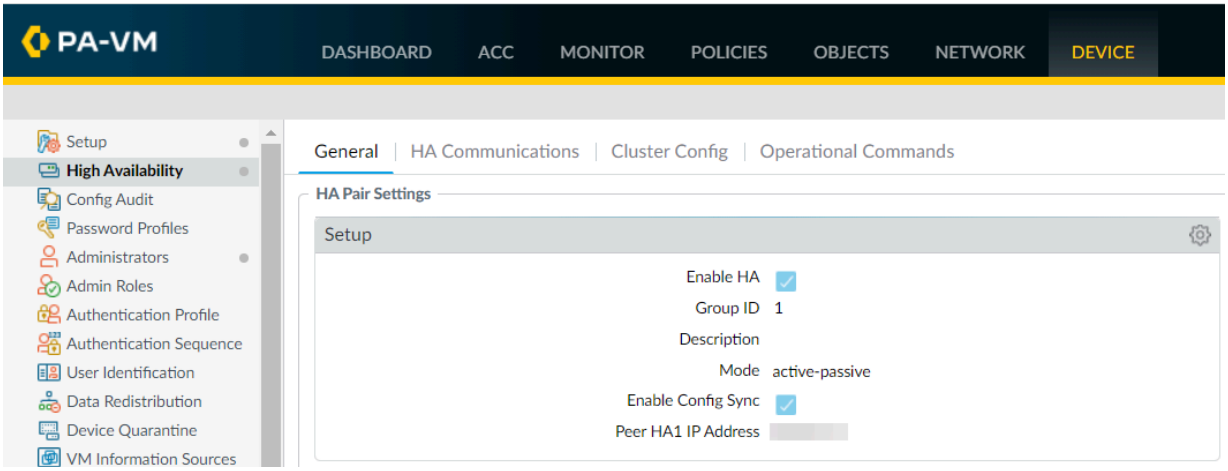
2. 輸入 **Client ID**（用戶端 **ID**）。用戶端 ID 是與 Azure Active Directory 應用程式相關聯的應用程式 ID。
3. 輸入 **Client Secret**（用戶端密碼）並重新輸入以確認。
4. 輸入 **Tenant ID**（租用戶 **ID**）。租用戶 ID 為您在設定啟動目錄應用程式時儲存的目錄 ID。
5. 為您要監控的 Azure 訂閱輸入 **Subscription ID**（訂閱 **ID**）。
6. 輸入 **Resource Group**（資源群組）名稱。
7. （僅限 Azure Stack 部署）輸入 **Resource Mgr Endpoint**（**Resource Mgr** 端點）URL。

   VM-Series 外掛程式 *2.1.2* 和更新版本有此欄位。

8. 按一下 **Validate**（驗證），確認您輸入的金鑰和 ID 有效，而且 VM-Series 外掛程式可以使用 API 成功與 Azure 資源進行通訊。

©2023 Palo Alto Networks, Inc.

STEP 4 | 啟用 HA。



1. 選取 **Device**（裝置） > **Setup**（設定） > **HA**。
2. 輸入 **Peer HA1 IP address**（對等 **HA1 IP** 位址）作為被動對等的私人 IP 位址。
3. （選用）編輯控制連結 (HA1)。如果您未計劃將管理介面用於控制連結，並已新增其他介面（例如乙太網路 1/4），則請編輯此區段來選取要用於 HA1 通訊的介面。
4. 編輯資料連結 (HA2) 以使用 **Port**（連接埠）乙太網路 1/3，並新增此對等的 IP 位址以及子網路的 **Gateway**（閘道） IP 位址。

STEP 5 | **Commit**（提交）變更。

©2023 Palo Alto Networks, Inc.

STEP 6 | 在相同 Azure 資源群組內設定被動 HA 對等。

1. 部署防火牆的第二個實例。
   - 從 GitHub 下載自訂範本和 parameters 檔案。
   - 登入 Azure 入口網站。
   - 搜尋 **custom template**（自訂範本），然後選取 **Deploy from a custom template**（從自訂範本部署）。
   - 選取 **Build your own template in the editor**（在編輯器中建立自己的範本） > **Load file**（載入檔案）。
   - 選取您稍早下載的 **azuredeploy.json**，並 **Save**（儲存）。
   - 完成輸入，並同意條款，然後 **Purchase**（購買）。

     請務必比對下列輸入與您已部署的防火牆實例的項目（Azure 訂閱、資源群組名稱、資源群組位置、您要在其中部署防火牆的現有 VNet 名稱、VNet CIDR、子網路名稱、子網路 CIDR），並啟動管理、信任和不受信任子網路的 IP 位址。
2. 重複步驟 1 和步驟 2 來設定介面，以及將防火牆設定為被動 HA 對等。
3. 略過步驟 3，並完成啟用 HA（步驟 5）。在步驟 4 中，適當地修改此被動 HA 對等的 IP 位址。

STEP 7 | 完成兩個防火牆的設定後，請確認配對的防火牆為主動/被動 HA。

1. 存取兩個防火牆上的 **Dashboard**（儀表板），然後檢視高可用性 Widget。
2. 在主動防火牆上，按一下 **Sync to peer**（同步處理至對等體）連結。
3. 確認防火牆已配對並同步，如下所示：
   - 在被動防火牆上：本機防火牆狀態應顯示為 **passive**（被動），而 **Running Config**（執行中設定）應顯示為 **synchronized**（已同步）。
   - 在主動防火牆上：本機防火牆狀態應顯示為 **active**（主動），而 **Running Config**（執行中設定）應顯示為 **synchronized**（已同步）。
4. 在被動對等上，確認立即同步處理 VM-Series 外掛程式設定。

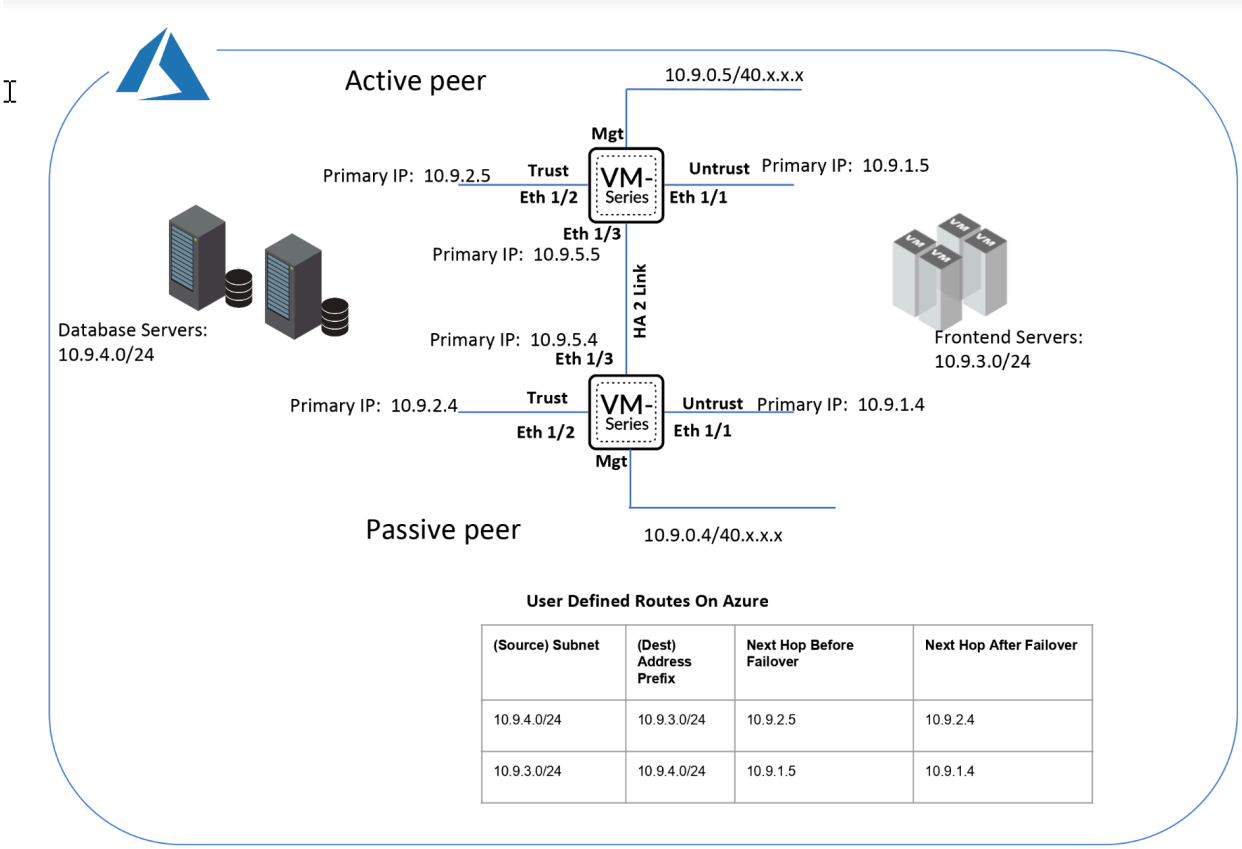
   選取 **Device**（裝置） > **VM-Series**，並驗證您可以檢視被動對等上已省略設定的 Azure HA 設定。

在 Azure 上設定主動/被動 HA（僅限東西向流量）

如果您的資源全都部署在 Azure 基礎結構內，且您不需要對 Azure VNet 的南北向流量強制執行安全性，則可以在主動/被動高可用性 (HA) 設定中部署一對 VM-Series 防火牆，而無須使用浮動 IP 位址。HA 對等將需要 HA 連結（控制連結 (HA1) 和資料連結 (HA2)）來同步處理資料與維護狀態資訊。

您必須具有 VM-Series 外掛程式 1.0.9 版或更新版本，且必須在相同的 Azure 資源群組內部署兩個防火牆 HA 對等。

©2023 Palo Alto Networks, Inc.



User Defined Routes On Azure

(Source) Subnet	(Dest) Address Prefix	Next Hop Before Failover	Next Hop After Failover
10.9.4.0/24	10.9.3.0/24	10.9.2.5	10.9.2.4
10.9.3.0/24	10.9.4.0/24	10.9.1.5	10.9.1.4

- 設定防火牆以啟用 HA
- 設定 Azure 的 VM-Series 防火牆上的主動/被動 HA

設定防火牆以啟用 HA

收集下列詳細資料，以設定 Azure 的 VM-Series 防火牆的 HA。

設定 Active Directory 應用程式和服務主體，以程式設計方式存取 API。

- 若要讓防火牆與 Azure API 互動，您需要建立 Azure Active Directory 服務主體。服務主體具有驗證 Azure AD 與存取訂閱中資源所需的權限。若要完成此設定，您必須有權限向 Azure AD 租用戶註冊應用程式，並將應用程式指派給訂閱中的角色。如果您沒有必要權限，可要求 Azure AD 或訂閱管理員建立服務主體。有關所需權限，請參閱上表。複製下列詳細資料，稍後用於此工作流程：
  - 用戶端 **ID**—與 Active Directory 相關聯的應用程式 ID（在 Azure 入口網站上，按一下 **Home**（首頁） > **Azure Active Directory** > **App registrations**（應用程式註冊），選取應用程式並複製 ID）。

©2023 Palo Alto Networks, Inc.

- 租用戶 **ID**—與 Active Directory 相關聯的目錄 ID（在 Azure 入口網站上，按一下 **Home**（首頁） > **Azure Active Directory** > **Properties**（屬性） > **Directory ID**（目錄 **ID**），選取應用程式並複製 ID）。

- **Azure Subscription ID**（**Azure** 訂閱 **ID**）—您已部署防火牆的 Azure 訂閱。您必須登入 Azure 入口網站才能取得此訂閱 ID。
- 資源群組名稱— 您已部署要設定為 HA 對等的防火牆的資源群組名稱。兩個防火牆都必須位於相同的資源群組中。
- 秘密金鑰—與 Active Directory 應用程式相關聯的驗證金鑰（在 Azure 入口網站上，按一下 **Home**（首頁） > **Azure Active Directory** > **Certificates & secrets**（憑證和機密），複製 **Client secrets**（用戶端密碼）下的 **Value**（值）。如果您沒有秘密金鑰，請先建立秘密金鑰，然後複製值）。若以應用程式形式登入，您必須同時提供金鑰值和應用程式 ID。

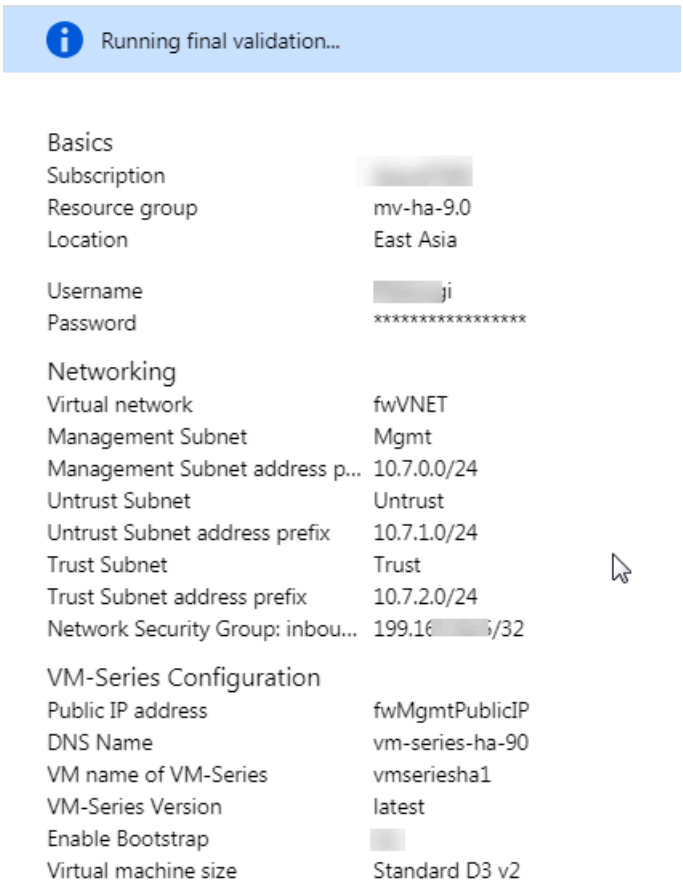
這樣就可知道從何處取得在相同 Azure 資源群組內部署 VM-Series 防火牆所需的範本。

針對 HA 設定，兩個 HA 對等都必須屬於相同的 Azure 資源群組。如果您從 Azure Marketplace 部署防火牆的第一個實例，而且必須使用自訂 ARM 範本或 Palo Alto Networks 範例 GitHub 範

©2023 Palo Alto Networks, Inc.

本將防火牆的第二個實例部署至現有資源群組。您需要自訂範本或 Palo Alto Networks 範例範本的原因是 Azure 不支援將防火牆部署至不是空的資源群組。

複製第一個防火牆實例的部署資訊。例如：



比對上方螢幕擷取畫面所顯示的 **VM Name of VM-Series firewall**（**VM-Series** 防火牆的 **VM** 名稱）與防火牆 Web 介面上的 **Hostname**（主機名稱）。您必須在 **Device**（裝置）> **Setup**（設定）> **Management**（管理）上新增相同的名稱，因為防火牆的主機名稱是用來觸發容錯移轉。

©2023 Palo Alto Networks, Inc.

規劃 Azure 的 VM-Series 防火牆上的網路介面設定。

若要設定 HA，您必須在相同的 Azure 資源群組內部署兩個 HA 對等，而且兩個防火牆的網路介面數目必須相同。每個 HA 對等最少都需要四個網路介面：

- 管理介面 **(eth0)**—與主要介面相關聯的私人和公共 IP 位址。公共 IP 位址會啟用對防火牆 Web 介面的存取與 SSH 存取。

  您可以使用管理介面上的私人 IP 介面作為 HA1 對等 IP 位址，以用於主動/被動 HA 對等之間的控制連結通訊。如果您想要專用的 HA1 介面，則必須連接每個防火牆上的其他網路介面，這表示每個防火牆上都需要五個介面。
- 不受信任介面 **(eth1/1)** — 具有 /32 網路遮罩的主要私人 IP 位址。

  容錯移轉時，如果被動對等轉換為主動狀態，VM-Series 外掛程式即會自動將流量傳送至被動對等的主要私人 IP 位址。Azure UDR 會啟用流量流程。
- 信任介面 **(eth1/2)** — 主要私人 IP 位址。容錯移轉時，如果被動對等轉換為主動狀態，VM-Series 外掛程式即會自動將流量傳送至被動對等的主要私人 IP 位址。
- **HA2 (eth 1/3)**—主要私人 IP 位址。HA2 介面是 HA 對等用於同步處理工作階段、轉送表格、IPSec 安全性關聯性和 ARP 表格的資料連結。

介面	主動防火牆對等	被動防火牆對等	說明
HA2	從 Azure 管理主控台，將 NIC 新增至防火牆。	從 Azure 管理主控台，將 NIC 新增至防火牆。	在主動和被動對等上，新增專用 HA2 連結以啟用工作階段同步處理。 HA1 的預設介面是管理介面，而且您可以選擇使用管理介面，而不是將其他介面新增至防火牆。若要啟用透過 HA2 連結的資料流程，您需要在 Azure 入口網站上新增其他網路介面，並設定防火牆上 HA2 的介面。

設定 Azure 的 VM-Series 防火牆上的主動/被動 HA

在此工作流程中，您可以使用 Azure Marketplace 中的 VM-Series 防火牆解決方案範本來部署 VM-Series 防火牆的第一個實例，以及使用範例 GitHub 範本的防火牆的第二個實例。

如果驗證金鑰（用戶端密碼）與透過 *HA* 設定來設定 *VM-Series* 防火牆所需的 *Active Directory* 應用程式相關聯，則會在防火牆和 *Panorama* 上使用 *VM-Series* 外掛程式 *1.0.9* 版予以加密。因為金鑰是透過 *VM-Series* 外掛程式 *1.0.9* 版予以加密，所以您必須在 *Panorama* 和受管理 *VM-Series* 防火牆上安裝相同版本的外掛程式，才能從 *Panorama* 集中管理防火牆。

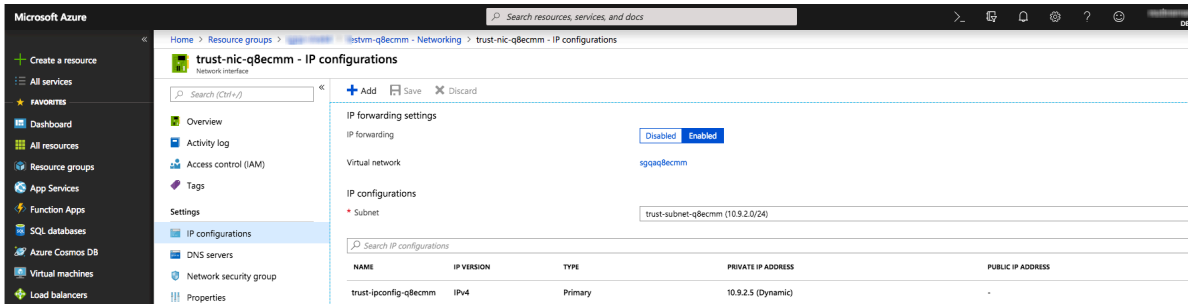
©2023 Palo Alto Networks, Inc.

STEP 1 | 使用解決方案範本部署 VM-Series 防火牆，並針對 HA 設定網路介面。

若要保護 Azure VNet 內的東西向流量，您只需要信任和不受信任防火牆介面的主要 IP 位址。進行容錯移轉時，UDR 將會變更，且路由會指向轉換為主動狀態之對等的主要 IP 位址。

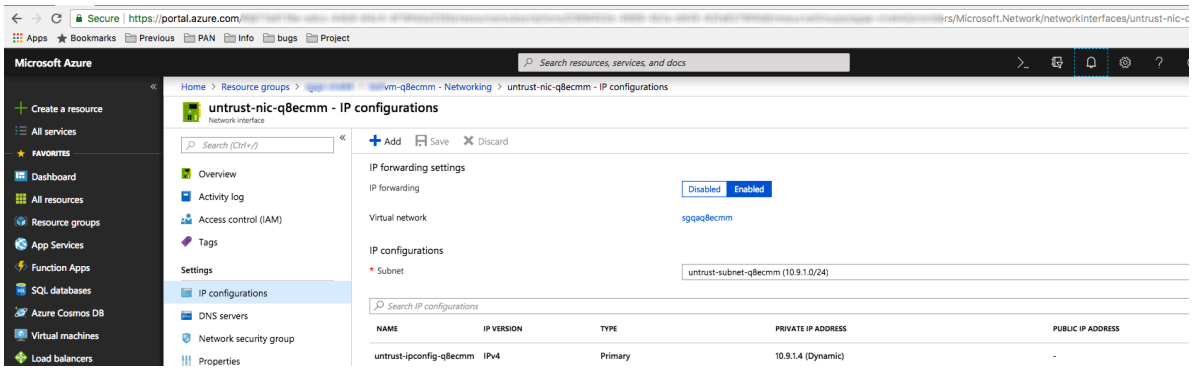
1. 將主要 IP 設定新增至主動防火牆對等的信任介面。

   在此工作流程中，會將此防火牆指定為主動對等。主動 HA 對等具有設定為防火牆上 HA 設定一部分的較低裝置優先順序數值，而且此值指出防火牆採用主動對等角色的偏好設定。



2. 將主要 IP 設定新增至主動防火牆對等的不受信任介面。

©2023 Palo Alto Networks, Inc.



3. 附加一個網路介面，用於防火牆 HA 對等體之間的 HA2 通信。
   1. 在虛擬網路內新增子網路。
   2. 建立和連接網路介面至防火牆。
4. 在 Azure 上設定您的路由表。

   對主動防火牆對等的信任和不受信任介面的主要 IP 位址建立下一個躍點的路由。

Example with Frontend Server to Database Server Route :

Routes

Search routes

Name	Address prefix	Next hop
frontend_Server_to_Database_Server_route	10.9.4.0/24	10.9.1.5

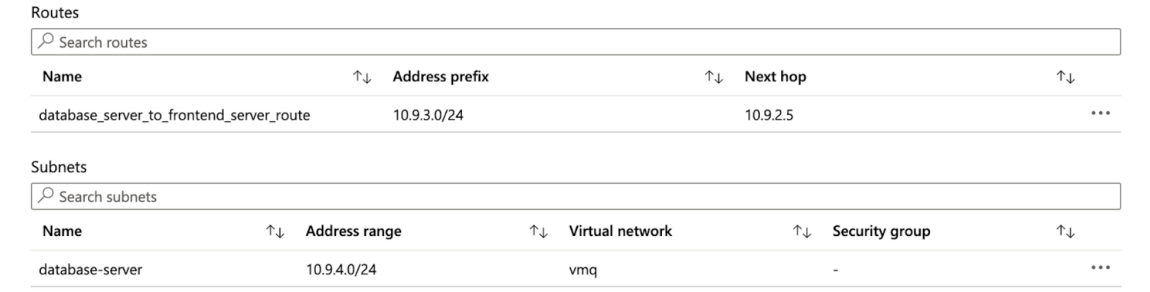
Subnets

Search subnets

Name	Address range	Virtual network	Security group
frontend-server	10.9.3.0/24	vmq	-

©2023 Palo Alto Networks, Inc.

Example with Database Server to Frontend Server route:



在容錯移轉後，資料庫伺服器至前端伺服器路由的下一個躍點將會從 10.9.2.5 變更為 10.9.2.4。同樣地，前端伺服器至資料庫伺服器路由的下一個躍點將會從 10.9.1.5 變更為 10.9.1.4。

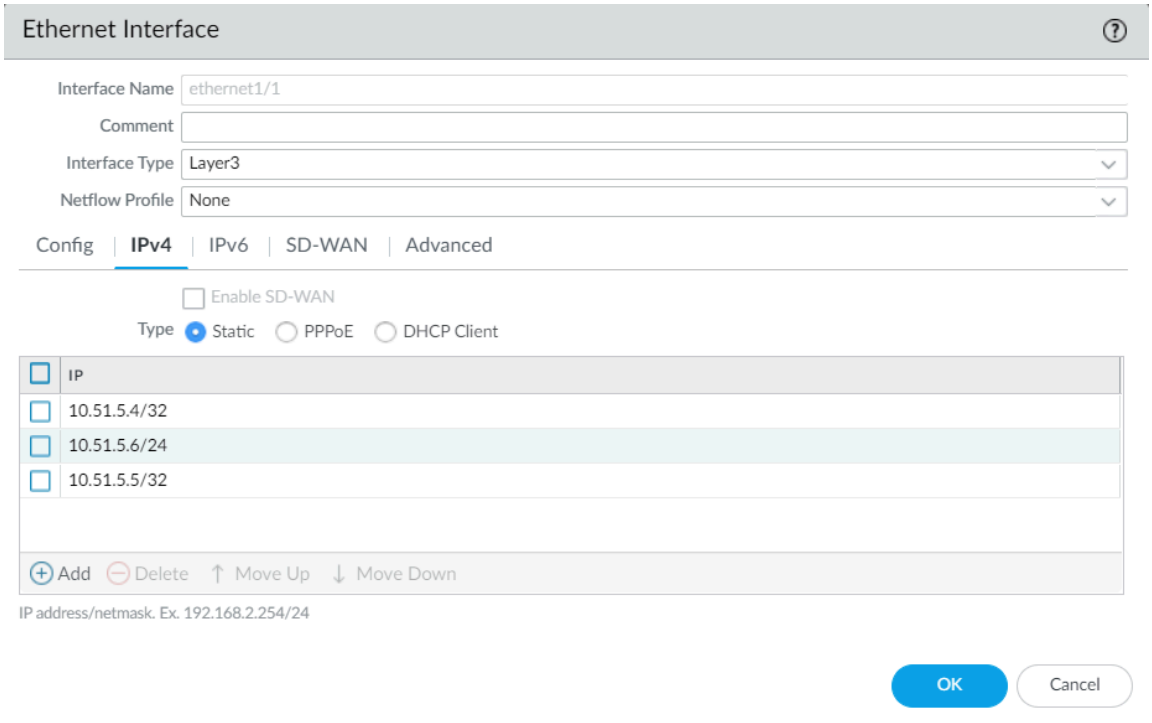
©2023 Palo Alto Networks, Inc.

STEP 2 | 在防火牆上設定介面。

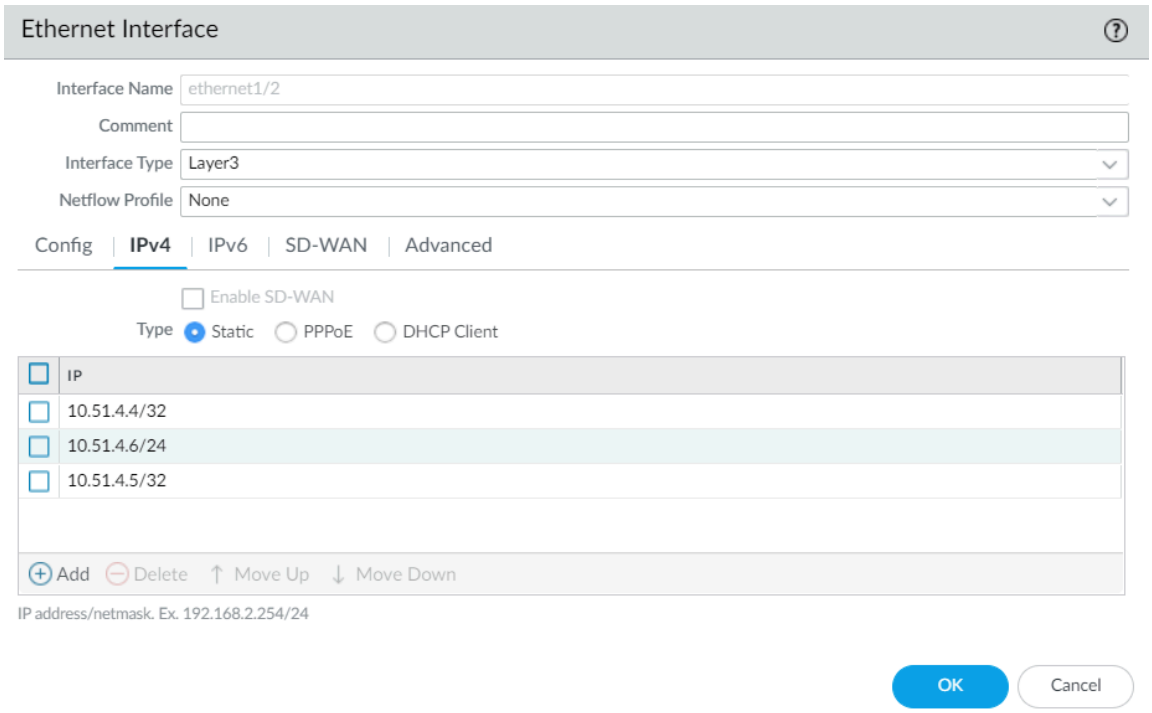
在您部署和設定被動 HA 對等之前，請在主動 HA 對等上完成這些步驟。

1. 登入防火牆 Web 介面。
2. 將乙太網路 1/1 設定為不受信任介面，並將乙太網路 1/2 設定為不受信任介面。

   選取 **Network**（網路） > **Interfaces**（介面），並設定如下：



©2023 Palo Alto Networks, Inc.



3. 將乙太網路 1/3 設定為 HA 介面。

   若要設定 HA2 連結，請選取介面，並將 **Interface Type**（介面類型）設定為 **HA**。將連結速度和雙工設定為 auto（自動）。



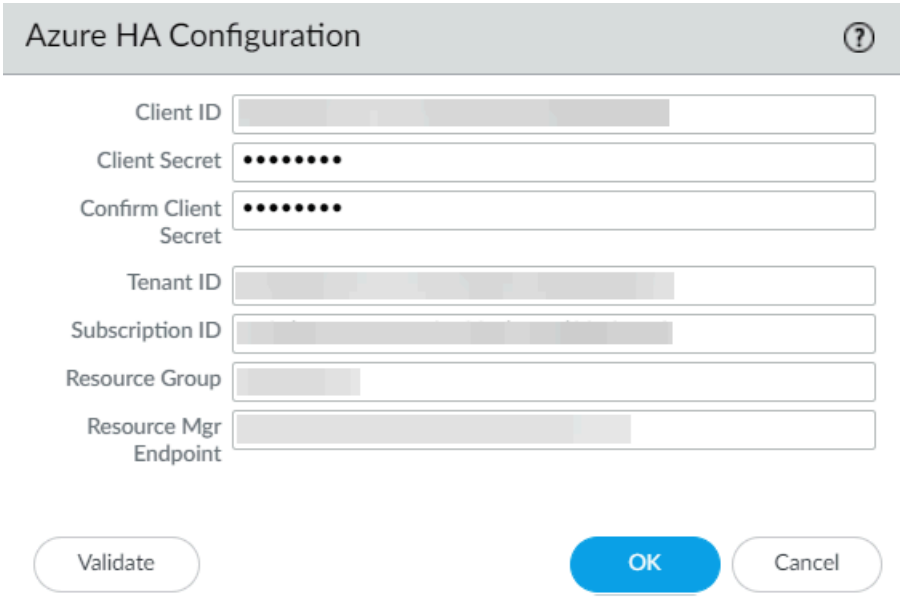
 ©2023 Palo Alto Networks, Inc.

STEP 3 | 設定 VM-Series 外掛程式，驗證您已在其中部署防火牆的 Azure 資源群組。

在 VM-Series 外掛程式上設定 Azure HA 設定。

若要加密用戶端密碼，請使用 VM-Series 外掛程式 1.0.4 版或更新版本。如果使用 Panorama 來管理防火牆，則您必須安裝 VM-Series 外掛程式 1.0.4 版或更新版本。

1. 選取 **Device**（裝置） > **VM-Series**，以在防火牆外掛程式與 Azure 資源之間透過程式設計方式存取。



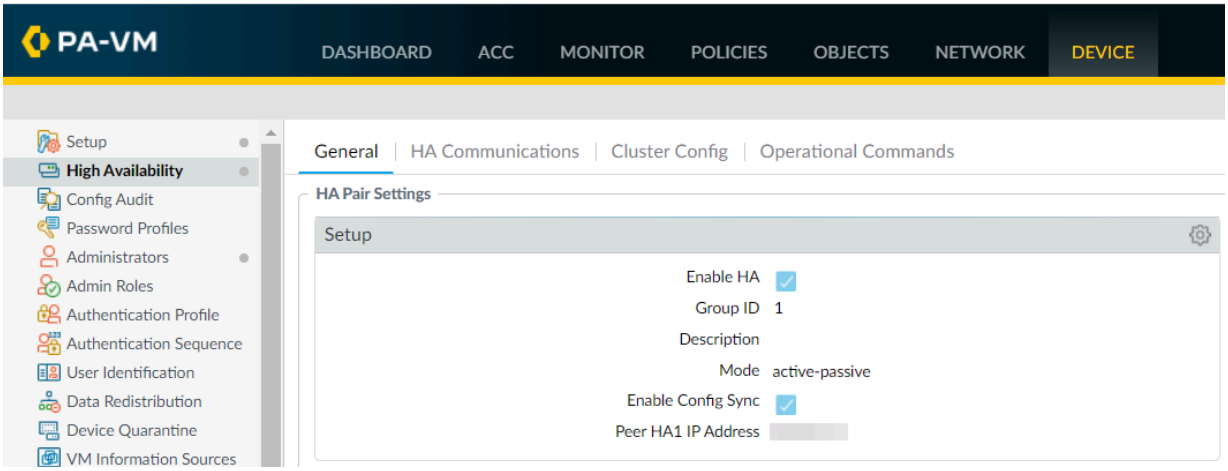
2. 輸入 **Client ID**（用戶端 **ID**）。用戶端 ID 是與 Azure Active Directory 應用程式相關聯的應用程式 ID。
3. 輸入 **Client Secret**（用戶端密碼）並重新輸入以確認。
4. 輸入 **Tenant ID**（租用戶 **ID**）。租用戶 ID 為您在設定啟動目錄應用程式時儲存的目錄 ID。
5. 為您要監控的 Azure 訂閱輸入 **Subscription ID**（訂閱 **ID**）。
6. 輸入 **Resource Group**（資源群組）名稱。
7. （僅限 Azure Stack 部署）輸入 **Resource Mgr Endpoint**（**Resource Mgr** 端點）URL。

   VM-Series 外掛程式 *2.1.2* 和更新版本有此欄位。

8. 按一下 **Validate**（驗證），確認您輸入的金鑰和 ID 有效，而且 VM-Series 外掛程式可以使用 API 成功與 Azure 資源進行通訊。

©2023 Palo Alto Networks, Inc.

STEP 4 | 啟用 HA。



1. 選取 **Device**（裝置） > **Setup**（設定） > **HA**。
2. 輸入 **Peer HA1 IP address**（對等 **HA1 IP** 位址）作為被動對等的私人 IP 位址。
3. （選用）編輯控制連結 (HA1)。如果您未計劃將管理介面用於控制連結，並已新增其他介面（例如乙太網路 1/4），則請編輯此區段來選取要用於 HA1 通訊的介面。
4. 編輯資料連結 (HA2) 以使用 **Port**（連接埠）乙太網路 1/3，並新增此對等的 IP 位址以及子網路的 **Gateway**（閘道） IP 位址。

STEP 5 | **Commit**（提交）變更。

©2023 Palo Alto Networks, Inc.

STEP 6 | 在相同 Azure 資源群組內設定被動 HA 對等。

1. 部署防火牆的第二個實例。
   - 從 GitHub 下載自訂範本和 parameters 檔案。
   - 登入 Azure 入口網站。
   - 搜尋 **custom template**（自訂範本），然後選取 **Deploy from a custom template**（從自訂範本部署）。
   - 選取 **Build your own template in the editor**（在編輯器中建立自己的範本） > **Load file**（載入檔案）。
   - 選取您稍早下載的 **azuredeploy.json**，並 **Save**（儲存）。
   - 完成輸入，並同意條款，然後 **Purchase**（購買）。

     請務必比對下列輸入與您已部署的防火牆實例的項目（Azure 訂閱、資源群組名稱、資源群組位置、您要在其中部署防火牆的現有 VNet 名稱、VNet CIDR、子網路名稱、子網路 CIDR），並啟動管理、信任和不受信任子網路的 IP 位址。
2. 重複步驟 1 和步驟 2 來設定介面，以及將防火牆設定為被動 HA 對等。
3. 略過步驟 3，並完成啟用 HA（步驟 5）。在步驟 4 中，適當地修改此被動 HA 對等的 IP 位址。

STEP 7 | 完成兩個防火牆的設定後，請確認配對的防火牆為主動/被動 HA。

1. 存取兩個防火牆上的 **Dashboard**（儀表板），然後檢視高可用性 Widget。
2. 在主動防火牆上，按一下 **Sync to peer**（同步處理至對等體）連結。
3. 確認防火牆已配對並同步，如下所示：
   - 在被動防火牆上：本機防火牆狀態應顯示為 **passive**（被動），而 **Running Config**（執行中設定）應顯示為 **synchronized**（已同步）。
   - 在主動防火牆上：本機防火牆狀態應顯示為 **active**（主動），而 **Running Config**（執行中設定）應顯示為 **synchronized**（已同步）。
4. 在被動對等上，確認立即同步處理 VM-Series 外掛程式設定。

   選取 **Device**（裝置） > **VM-Series**，並驗證您可以檢視被動對等上已省略設定的 Azure HA 設定。

©2023 Palo Alto Networks, Inc.

使用 ARM 範本部署 VM-Series 防火牆

除了基於 Marketplace 的部署，Palo Alto Networks 還提供載有範例 ARM 範本的 GitHub 儲存庫，您可以下載範本並根據您的需求自訂範本。ARM 範本為描述個別資源所需資源的 JSON 檔案，例如網路介面、完整的虛擬電腦，甚至是使用多部虛擬電腦的整個應用程式堆疊。

ARM 範本適用於進階使用者，而 Palo Alto Networks 則根據社群支援原則提供 ARM 範本。如需瞭解 ARM 範本，請參閱有關 ARM 範本的 Microsoft 文件。

為了簡化所有所需資源的部署，兩層範例範本 (https://github.com/PaloAltoNetworks/azure/tree/master/two-tier-sample) 包含兩個 JSON 檔案：

- 範本檔案—azureDeploy.json 是在資源群組中部署所有元件的主要資源檔案。
- 參數檔案—azureDeploy.parameters.json 檔案包含在 VNet 中成功部署 VM-Series 防火牆所需參數。它包含虛擬電腦層級與大小的詳細資訊、防火牆的使用者名稱與密碼、防火牆的儲存容器名稱。您可以針對 Azure VNet 部署自訂此檔案。

為了協助您將防火牆部署為網際網路型應用程式的閘道，此範本會佈建 VM-Series 防火牆、資料庫伺服器和 Web 伺服器。VNet 使用私人非路由 IP 位址空間 192.168.0.0/16。您可以修改範本以使用 172.16.0.0/12 或 10.0.0.0/8。

ARM 範本還提供必要的使用者定義規則及 IP 轉送旗標，讓 VM-Series 防火牆保護 Azure 資源群組的安全。對於範本中包含的五個子網路（Trust、Untrust、Web、DB 及 NAT），您設有五個路由表，每個具有使用者定義規則的子網路各使用一個，以便將流量路由至 VM-Series 防火牆及 NAT 虛擬電腦。

對於範本中包含的四個子網路（Trust、Untrust、Web 及 DB），您設有四個路由表，每個具有使用者定義規則的子網路各使用一個，以便將流量路由至 VM-Serie 防火牆。

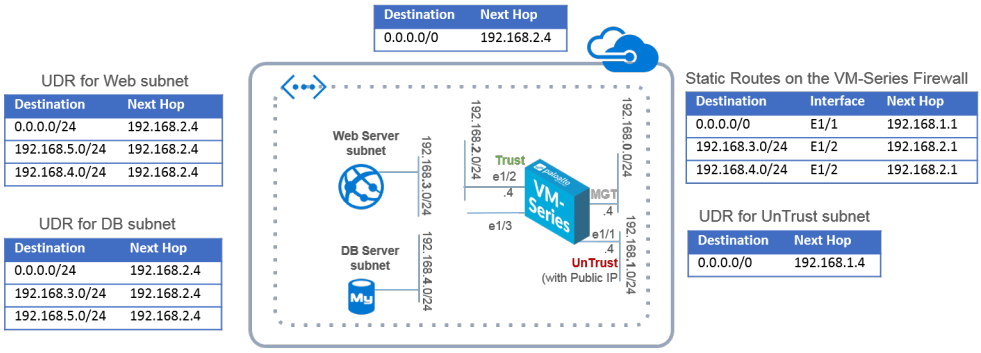


圖 **4:** 使用 **ARM** 範本部署 **VM-Series** 防火牆

STEP 1 | 從 GitHub 儲存庫下載兩層範例 ARM 範本。

下載檔案並儲存至本機用戶端：https://github.com/PaloAltoNetworks/azure/tree/master/two-tier-sample

©2023 Palo Alto Networks, Inc.

STEP 2 | 在 Azure 上建立資源群組。

1. 使用下列命令登入 Azure CLI：**azurelogin**

   如需協助，請參閱有關安裝 CLI 的 Azure 文件，或從 Azure 文件中取得如何在 Azure Government 或 Azure China 上存取 CLI 的詳細資訊。
2. 使用下列命令切換至 Resource Manager 模式：**azureconfig mode arm**
3. 建立資源群組。

©2023 Palo Alto Networks, Inc.

STEP 3 | 部署 ARM 範本。

1. 使用文字編輯器開啟參數檔案，並根據您的部署修改值：

   在 *Azure China* 中，您必須編輯儲存帳戶的路徑，此帳戶託管部署 *VM-Series* 防火牆所需的 *VHD* 映像。在範本檔案的變數部分中，找出稱為 ***userImageNameURI*** 的參數，以您儲存 *VHD* 映像的位置取代此值。

2. 在您建立的資源群組中部署範本。

```
azure group create -v -n “<YourResourceGroupName>” -
l “<YourAzureLocation>” -d “<GiveASmallDeploymentLabel>” -f
 azureDeploy.json -e azureDeploy.parameters.json
```

3. 透過 Azure CLI 檢查部署的進度/狀態：

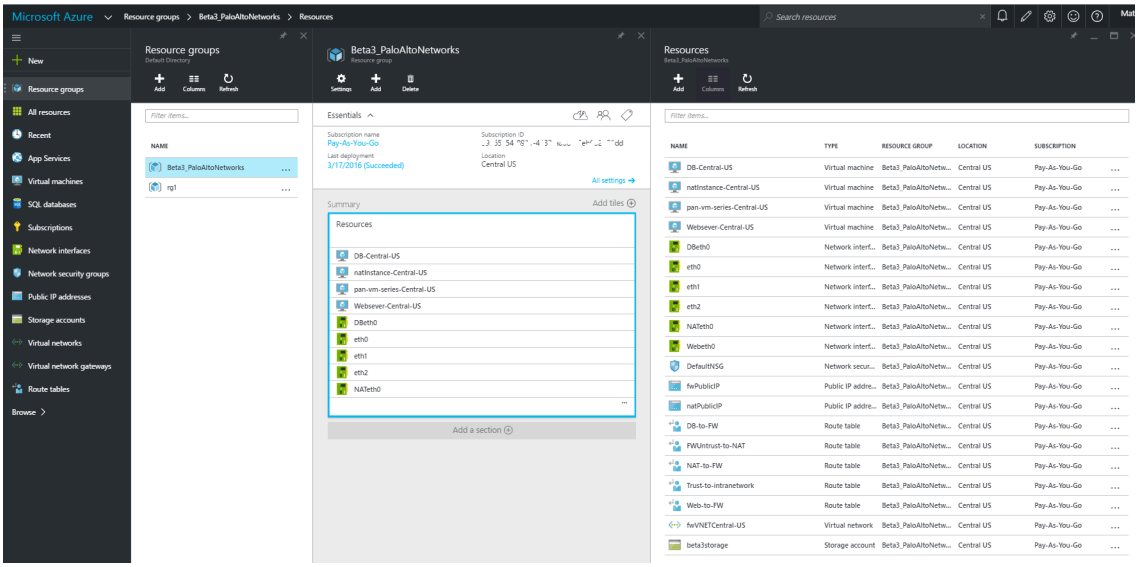
```
azure group deployment show
 "<YourResourceGroupName>" “<YourDeploymentLabel> “
```

   成功部署範本後，狀態為 `ProvisioningStateis Running`。

   如果狀態為 *`ProvisioningStateis Failed`*，您必須在 *Azure* 入口網站的 ***Resource Group***（資源群組）**>** ***Events***（事件）上檢查錯誤。僅僅篩選最近一小時的事件，選取最近的事件，然後深入探究以找出錯誤。

4. 確認您已成功部署 VM-Series 防火牆。

   1. 選取 **Dashboard**（儀表板） > **Resource Groups**（資源群組），然後選取資源群組。
   2. 選取 **All Settings**（所有設定） > **Deployments**（部署） > **Deployment History**（部署歷程記錄），以瞭解詳細狀況。



   VNet 中的位址空間使用首碼 *192.168*，在 *ARM* 範本中定義該首碼。

5. 將公共 IP 位址附加至防火牆的不受信任介面。

©2023 Palo Alto Networks, Inc.

STEP 4 | 將防火牆設定為 VNet 閘道以保護網際網路對向部署。

1. 登入防火牆的管理介面 IP 位址。
2. 將資料平面網路介面設定為防火牆上的第 3 層介面（**Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路））。
3. 新增統計規則至防火牆上的虛擬路由器。若要透過此範例中的防火牆路由流量，您需要防火牆上有三個靜態路由（**Network**（網路） > **Virtual Routers**（虛擬路由器），並選取路由器，然後按一下 **Static Routes**（靜態路由））：
   1. 透過 UnTrust 區域、ethernet1/1 將所有出埠流量路由至 Azure 路由器，位址為 192.168.1.1。
   2. 透過 UnTrust 區域、ethernet1/2 將目的地為 Web 伺服器子網路的所有入埠流量路由至 Azure 路由器，位址為 192.168.2.1。
   3. 透過 UnTrust 區域、ethernet1/2 將目的地為資料庫伺服器子網路的所有入埠流量路由至 Azure 路由器，位址為 192.168.2.1。
4. 建立安全性政策規則（**Policies**（政策） > **Security**（安全性）），以允許防火牆上的輸入與輸出流量。您還需要建立安全性原則規則，以允許從 Web 伺服器子網路傳送至資料庫伺服器（反之亦然）的相應流量。
5. 在防火牆 **Commit**（提交）變更。
6. 確認 VM-Series 防火牆正在保護流量（**Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量））。

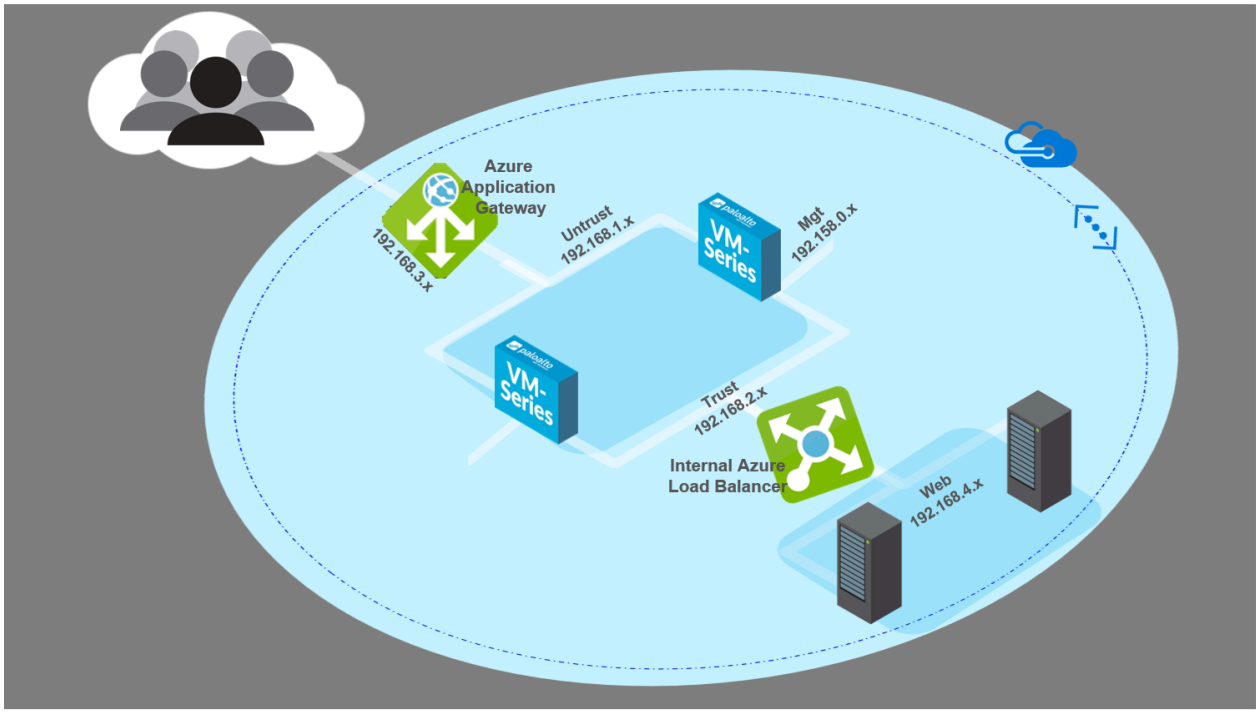
©2023 Palo Alto Networks, Inc.

部署 VM-Series 和 Azure 應用程式閘道範本

VM-Series 和 Azure 應用程式閘道範本是入門套件，可用來部署 VM-Series 防火牆，以針對 Microsoft Azure 上的網際網路型部署，保護 web 工作負載的安全（目前不適用於 Azure China）。

此範本會在一對 Azure 負載平衡器（外部和內部）之間部署兩個 VM-Series 防火牆。外部負載平衡器是 Azure 應用程式閘道，這是一個 HTTP（第 7 層）負載平衡器，也充當網際網路型閘道來接收流量，再透過 VM-Series 防火牆分送至內部負載平衡器。內部負載平衡器是面對著一對 Web 伺服器的 Azure 負載平衡器（第 4 層）。此範本支援 BYOL 和 Azure Marketplace 版本的 VM-Series 防火牆。

隨著 web 工作負載的需求增加，而且您也增加 Web 伺服器層的容量時，您可以手動部署額外的 VM-Series 防火牆來保護 Web 伺服器層的安全。

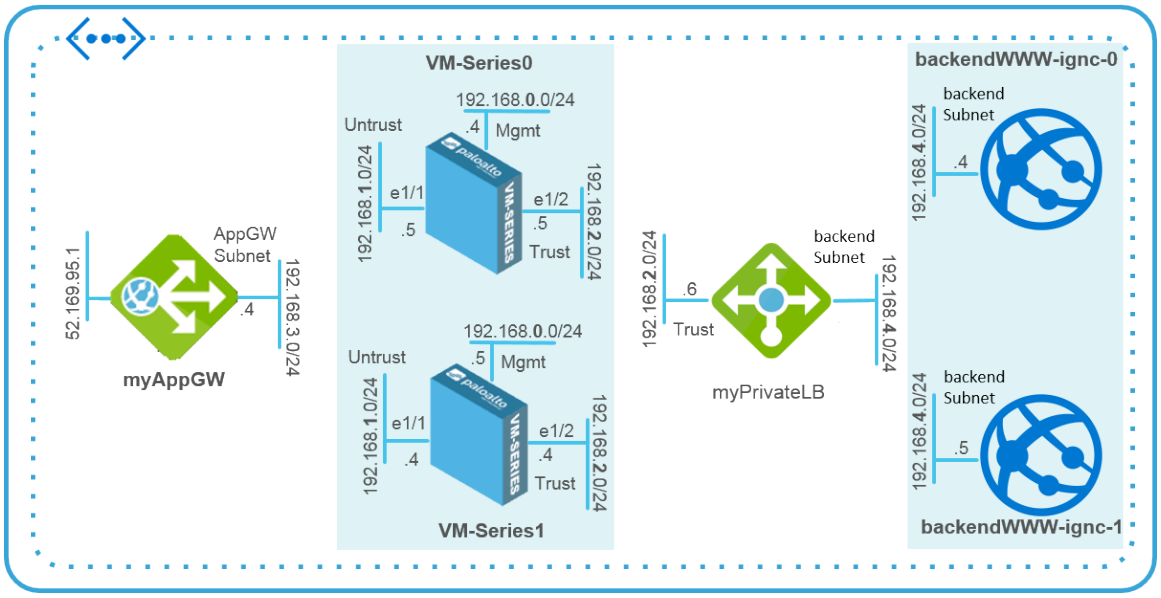


- VM-Series 和 Azure 應用程式閘道範本
- 開始使用 VM-Series 和 Azure 應用程式閘道範本

VM-Series 和 Azure 應用程式閘道範本

VM-Series 和 Azure 應用程式閘道範本會啟動 Azure 應用程式閘道（第 7 層負載平衡器）和 Azure（第 4 層）負載平衡器。在應用程式閘道和負載平衡器之間，有一對 VM-Series 防火牆內嵌在一個可用性設定組中，也有一對在 Ubuntu 上執行 Apache2 的範例 Web 伺服器內嵌在另一個可用性設定檔中。可用性設定組可預防計畫性和非計畫性停機。下列拓撲圖顯示範本所部署的資源：

©2023 Palo Alto Networks, Inc.



您可以使用新的或現有儲存帳戶或資源群組，在其中將此解決方案的所有資源部署在一個 Azure 位置內。這不提供資源群組名稱和儲存帳戶名稱的預設值，您必須輸入名稱。雖然您可以建立新的或使用現有 VNet，此範本會建立一個預設 VNet，名稱為 ***vnet-FW***，CIDR 區塊為 192.168.0.0/16，並配置五個子網路 (192.168.1.0/24 - 192.168.5.0/24)，以部署 Azure 應用程式閘道、VM-Series 防火牆、Azure 負載平衡器和 Web 伺服器。每個部署的 VM-Series 防火牆有三個網路介面 — Mgmt 子網路 (192.168.0.0/24) 中的 ethernet0/1、不受信任子網路 (192.168.1.0/24) 中的 ethernet1/1，以及受信任子網路 (192.168.2.0/24) 中的 ethernet1/2。

此範本會建立一個 Network Security Group（網路安全性群組 - NSG），在連接埠 80、443 和 22 上允許來自任何來源 IP 位址的輸入流量。還會將 VM-Series 防火牆配對和 Web 伺服器配對部署在其各自的可用性設定組中，以確保在計畫性或非計畫性維護期間，各配對至少有一個實例可用。每個可用性設定組都設定為使用三個容錯網域和五個更新網域。

Azure 應用程式閘道充當反向 Proxy 服務，可終止用戶端連線並將要求轉送至後端 Web 伺服器。Azure 應用程式閘道設有 HTTP 接聽程式，並使用預設建康情況探查來測試 VM-Series 防火牆 IP 位址（適用於 ethernet1/1）是否良好而且可接收流量。

此範本不提供自動調整規模解決方案；您必須規劃容量需求，然後部署其他資源，以針對您的部署來改寫範本。

VM-Series 防火牆不設定為接收和保護流向 Web 伺服器的 web 流量。因此，您至少必須為防火牆設定靜態路由，將流量從 VM-Series 防火牆傳送至預設路由器，設定目的地 NAT 原則將流量傳回至負載平衡器的 IP 位址，以及設定安全性原則規則。防火牆也需要 NAT 原則規則，才能將回應傳回給來自 Azure 應用程式閘道上 HTTP 接聽程式的健康情況查探。為了協助您完成基本的防火牆組態，GitHub 儲存庫包含範例組態檔案 ***appgw-sample.xml***，方便您開始使用。

開始使用 VM-Series 和 Azure 應用程式閘道範本

VM-Series 和 Azure 應用程式閘道範本會啟動所有必要的資源，讓您部署和保護 Microsoft Azure（不包括 Azure China）中連接網際網路的部署的 Web 工作負載。本節提供詳細資訊來說明

©2023 Palo Alto Networks, Inc.

如何部署此範本、設定防火牆來路由和保護以 Web 伺服器為目的地的流量，以及延伸此範本所提供的功能和資源，以滿足您的部署需求。

- 將範本部署至 Azure
- VM-Series 和 Azure 應用程式閘道範本參數
- 範例組態檔案
- 改寫範本

將範本部署至 Azure

使用下列指示將範本部署至 Azure。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 部署範本。

目前無法部署在 *Azure China*。

1. 從 https://github.com/PaloAltoNetworks/azure-applicationgateway 存取範本
2. 按一下 **Deploy to Azure**（部署至 **Azure**）。
3. 填寫詳細資訊以部署範本。如需每個參數的說明和預設值（若有的話），請參閱 VM-Series 和 Azure 應用程式閘道範本參數。

   對於 VM-Series 防火牆上的管理帳戶，您至少必須選取 **Azure Subscription**（**Azure** 訂用帳戶）、**Resource Group**（資源群組）、**Location**（位置）、**Storage Account**

©2023 Palo Alto Networks, Inc.

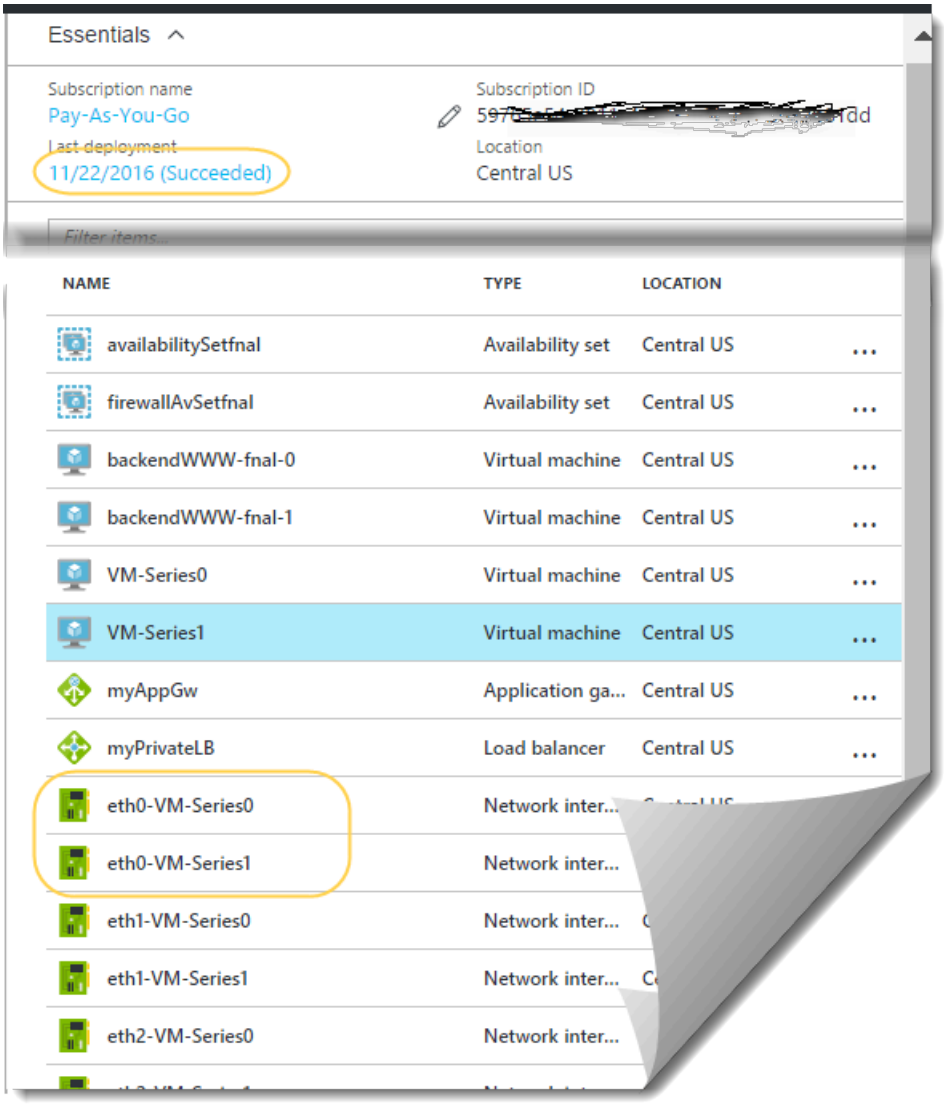
Name（儲存帳戶名稱）和 **Username/password**（使用者名稱/密碼）或 **SSH Key**（SSH 金鑰）。

4. 按一下 **Purchase**（購買）以接受條款並部署資源。

   如果發生驗證錯誤，請按一下以檢視詳細資訊，並修正錯誤。

5. 在 Azure 入口網站，確認您已成功部署範本資源，包括 VM-Series 防火牆。

   1. 選取 **Dashboard**（儀表板） > **Resource Groups**（資源群組），然後選取資源群組。
   2. 選取 **Overview**（概觀），檢閱所有已部署的資源。部署狀態應該顯示 **Succeeded**（成功）。



3. 請記下指派給 **eth0-VM-Series0** 和 **eth0-VM-Series1** 的公共 IP 位址或 DNS 名稱，以存取 VM-Series 防火牆的管理介面。

©2023 Palo Alto Networks, Inc.

STEP 2 | 登入防火牆。

1. 從 Web 瀏覽器使用安全連線 (https)，登入 eth0-VM-Series0 的 IP 位址，或防火牆的 DNS 名稱。
2. 輸入您在參數檔案中定義的使用者名稱/密碼。您將看見憑證警告；此為正常現象。繼續開啟網頁。

©2023 Palo Alto Networks, Inc.

STEP 3 | 設定 VM-Series 防火牆。

您可以手動設定防火牆，或匯入 GitHub 儲存庫中提供的範例組態檔案，並依照您的安全性需求來自訂。

- 手動設定防火牆—您至少必須執行下列動作：

1. 將資料平面網路介面設定為防火牆上的第 3 層介面（**Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路））。
2. 將靜態規則新增至防火牆上的虛擬路由器。針對任何以 ethernet1/1 為目的地的流量，此靜態規則指定防火牆的不受信任介面 IP 位址作為 nexthop 位址。（**Network**（網路） > **Virtual Routers**（虛擬路由器），選取路由器並按一下 **Static Routes**（靜態路由））。
3. 建立安全性政策規則（**Policies**（政策） > **Security**（安全性）），以允許防火牆上的輸入與輸出流量。
4. 新增 NAT 政策（**Policies**（政策） > **NAT**）。您必須在防火牆上建立目的地 NAT 和來源 NAT 規則，以便將流量傳送至 Web 伺服器並傳回至提出要求的用戶端。

   目的地 NAT 規則適用於所有到達防火牆不受信任介面的流量。需要此規則將封包上的目的地 IP 位址轉譯成內部負載平衡器的 IP 位址，才能將所有流量導向至內部負載平衡器，再導向至後端 Web 伺服器。

   來源 NAT 規則適用於所有來自後端 Web 伺服器並以防火牆不受信任介面為目的地的流量。此規則會將來源位址轉譯成防火牆上信任介面的 IP 位址。
5. **Commit**（提交）您的變更。

   - 匯入範例組態檔案：
6. 下載範例組態檔案檔案並儲存至本機用戶端。
7. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），並按一下 **Import named configuration snapshot**（匯入具名設定快照）、**Browse**（瀏覽）至您儲存在本機的設定檔案，然後按一下 **OK**（確定）。
8. 按一下 **Load named configuration snapshot**（載入具名組態快照），選取您剛才匯入的範例組態檔案的 **Name**（名稱），然後按一下 **OK**（確定）。
9. 變更位址物件和靜態路由的 IP 位址，以符合您使用的 CIDR 區塊中 IP 位址。更新位址物件來使用 eth1-VM-Series0 和 eth1-VM-Series1 的私人 IP 位址。
10. 重要#建立新的管理使用者帳戶。選取 **Device**（裝置） > **Administrators**（管理員），然後**Add**（新增）新帳戶。
11. 在 **Device**（裝置） > **Setup**（設定） > **Management**（管理）的 [General Settings（一般設定）] Widget 中，修改 **Hostname**（主機名稱）。
12. **Commit**（提交）變更並登出。提交會以範例組態檔案和您剛完成的更新，覆寫執行中的組態。提交時會覆寫您在部署範本時所指定的主機名稱和管理員使用者帳戶。現在，您需要以新的管理使用者帳戶和密碼登入。

    - 登入防火牆—使用您建立的認證，並刪除範例組態檔案中匯入的 pandemo 管理帳戶。

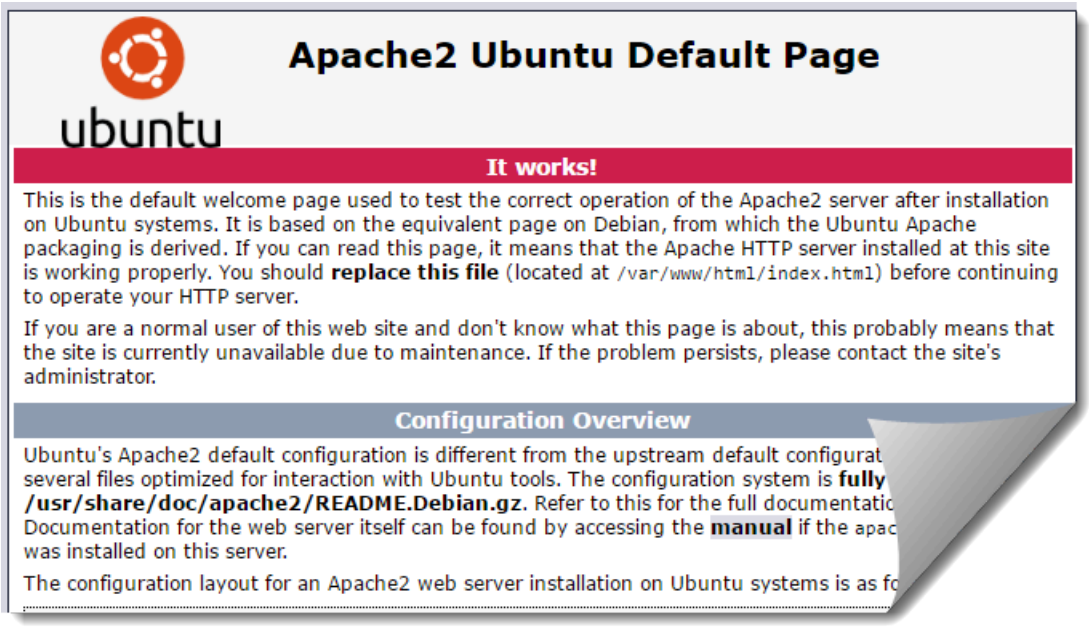
STEP 4 | 登入並設定 VM-Series 防火牆的其他實例。

請參閱步驟設定 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

STEP 5 | 確認您已適當地設定防火牆。

從 web 瀏覽器中，利用 http 存取應用程式閘道的 IP 位址或 DNS 名稱。您應該能夠檢視預設 Apache 2 Ubuntu 網頁。



如果您使用範例設定防火牆，請登入防火牆，然後在 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量）中檢視工作階段啟動時所產生的流量日誌。

VM-Series 和 Azure 應用程式閘道範本參數

下表列出必要和選用參數及預設值（若有的話）。

參數	說明
資源群組	建立新的或使用現有的（無預設值）。
訂閱	Azure 訂閱的類型，用於支付範本所部署之資源的成本。
位置	選取您要部署範本的 Azure 位置（無預設值）。
網路安全性群組	
網路安全性群組名稱	網路安全性群組限制從哪些來源 IP 位址可存取 VM-Series 防火牆和 Web 伺服器。 預設值：nsg-mgmt
網路安全性群組輸入來源 IP	這些來源 IP 位址可登入範本所部署的 VM 的 management port（管理連接埠 - MGT port）。

©2023 Palo Alto Networks, Inc.

參數	說明
	預設值 0.0.0.0/0 表示您可以從任何 IP 位址登入防火牆管理連接埠。
儲存帳戶	
儲存帳戶名稱	建立新的儲存帳戶，或輸入現有儲存帳戶的名稱（無預設值）。此名稱必須是全球唯一的。
儲存帳戶類型	選取標準或進階儲存體，以及本地備援、異地備援和讀取存取異地備援的資料複寫需求。 預設選項是 Locally Redundant Storage（本地備援儲存體 - LRS）。其他選項包括「標準 GRS」、「進階 LRS」和「標準 RAGRS」。
VNet	
虛擬網路	建立新的 VNet，或輸入現有 VNet 的名稱。 VNet 的預設名稱是 vnet-FW
虛擬網路位址首碼	192.168.0.0/16
Azure 應用程式閘道	
應用程式閘道名稱	myAppGw
應用程式閘道 DNS 名稱	輸入 Azure 應用程式閘道的全球唯一 DNS 名稱。
應用程式閘道子網路名稱和首碼	預設名稱是 AppGWSubnet，子網路首碼是 192.168.3.0/24。
Azure 負載平衡器和 Web 伺服器	
內部負載平衡器名稱	myPrivateLB
內部負載平衡器子網路名稱和首碼	預設名稱是 backendSubnet，子網路首碼是 192.168.4.0/24。
後端 Vm 大小	預設大小是「標準層 D1 Azure VM」。使用範本中的下拉式清單，檢視後端 Web 伺服器可用的其他 Azure VM 選項。
防火牆	
防火牆型號	選取 BYOL 或 PAYG（搭售包 1 或搭售包 2，每個搭售包都包含 VM-300 和一組訂閱）。

©2023 Palo Alto Networks, Inc.

參數	說明
防火牆 Vm 名稱和大小	防火牆的預設名稱是 VM-Series，預設大小是「標準層 D3 Azure VM」。 使用範本中的下拉式清單，檢視 VM-Series 防火牆可用的其他 Azure VM 選項。
管理子網路名稱和首碼	此解決方案中部署的 VM-Series 防火牆和 Web 伺服器的管理子網路。 預設名稱是 Mgmt，子網路首碼是 192.168.0.0/24。
管理公共 IP 位址名稱	輸入主機名稱以存取每個防火牆的管理介面。這些名稱必須是全球唯一的。
信任的子網路名稱和首碼	VM-Series 防火牆的 eth1/1 所連線的子網路；這個子網路將 VM-Series 防火牆連線至 Azure 應用程式閘道。防火牆在 eth1/1 接收流向 Web 伺服器的 web 流量。 預設名稱是 Trust，子網路首碼是 192.168.2.0/24。
不受信任的子網路名稱	VM-Series 防火牆的 eth1/2 所連線的子網路。防火牆在此介面上接收返回和輸出 web 流量。 預設名稱是 Untrust，子網路首碼是 192.168.1.0/24。此名稱必須是全球唯一的。
使用者名稱	輸入 VM-Series 防火牆和 Web 伺服器上管理帳戶的使用者名稱。
驗證類型	您必須輸入用於驗證的密碼，或使用 SSH 公開金鑰（無預設值）。

範例組態檔案

為了協助您開始使用，GitHub 儲存庫中有一個名為 ***appgw-sample.xml*** 的範例組態檔案，其中包含下列規則/物件：

- 位址物件—兩個位址物件：**`firewall-untrust-IP`** 和 **`internal-load-balancer-IP`**，需要修改以符合您的設定中的 IP 位址。您需要修改這些位址物件，以使用 Azure 入口網站上指派給 eth1-VM-Series0 和 eth1-VM-Series1 的私人 IP 位址。
- 靜態路由—防火牆上的預設虛擬路由器具有指向 192.168.1.1 的靜態路由，如果您使用預設範本值，則此 IP 位址正確。如果您變更不受信任的子網路 CIDR，則需要更新 IP 位址以符合您的設定。所有從後端 Web 伺服器至應用程式閘道的流程，都使用此 IP 位址作為下一個躍點，以將封包傳遞至防火牆上不受信任的介面。

©2023 Palo Alto Networks, Inc.

- **NAT** 原則規則—NAT 原則規則會啟用目的地 NAT 和來源 NAT。
  - 目的地 NAT 規則適用於所有到達防火牆不受信任介面 (ethernet1/2) 的流量，此介面是 firewall-untrust-IP 位址物件。此規則會將封包上的目的地 IP 位址轉譯成內部負載平衡器的 IP 位址，讓所有流量導向至內部負載平衡器，再導向至後端 Web 伺服器。
  - 來源 NAT 規則適用於所有從後端 Web 伺服器至防火牆上不受信任網路介面的流量。此規則會將來源位址轉譯成防火牆上信任介面的 IP 位址 (ethernet1/2)。
- 安全性原則規則—範例組態檔案中定義兩個安全性原則規則。第一個規則允許所有輸入網頁瀏覽流量，並於防火牆上啟動工作階段時產生日誌。第二個規則封鎖其他所有流量，並於防火牆上啟動和結束工作階段時產生日誌。您可以使用這些日誌，監控流向此部署中的 Web 伺服器的所有流量。
- 管理使用者認證—範例組態檔案包含用於登入防火牆的使用者名稱和密碼，已設為 pandemo/demopassword。匯入範例組態之後，您必須變更密碼並設為強式的自訂密碼，或建立新的管理員帳戶並刪除 pandemo 帳戶。

改寫範本

隨著需求演變，您可以界定容量需求的範圍，並針對您的部署案例來延伸範本。在入門範本上，您可以運用下列一些方法來符合規劃的容量需求：

- 在 Azure 應用程式閘道後方部署其他 VM-Series 防火牆。您可以手動將更多 VM-Series 防火牆安裝至相同的可用性設定組，或啟動新的可用性設定組，再手動部署其他 VM-Series 防火牆。
- 除了 GitHub 儲存庫中的範例組態檔案所提供的基本組態，部署超出此組態的 VM-Series 防火牆。
- 在 Azure 應用程式閘道上啟用 HTTPS 負載平衡（SSL 卸載）。如需詳細資訊，請參閱 Azure 文件。
- 新增或取代範本隨附的範例 Web 伺服器。

©2023 Palo Alto Networks, Inc.

保護 Azure 上的 Kubernetes 服務

若要保護 Azure Kubernetes 服務，您必須在 Panorama 上安裝 Azure 外掛程式，並設定 Azure 保護 Azure 上的 Kubernetes 服務 部署。Panorama 專用 Azure 外掛程式支援標籤型 VM 監控和 保護 Azure 上的 Kubernetes 服務，保護 Azure Kubernetes Services (AKS) 叢集的輸入流量，以及監控 AKS 叢集的輸出流量。Panorama 協調部署可讓您利用 Azure 自動調整規模度量及相應縮小和相應放大閾值，獨立調整 VM-Series 防火牆的規模，以應付應用程式工作負載資源激增的需求。

若要保護 AKS 叢集的輸入流量，您必須先保護 Azure 上的 Kubernetes 服務。Panorama 協調部署與 保護 Azure 上的 Kubernetes 服務 搭配運作，收集網路和資源的相關資訊，然後為任一保護 Azure 上的 Kubernetes 服務部署建立自動調整規模層的 VM-Series 防火牆。請參閱 Palo Alto Networks 相容性矩陣，以確認要保護 AKS 叢集所需的最低作業系統、外掛程式和範本版本。

Palo Alto Networks 提供可在新的 Azure VNet 中部署 Azure Kubernetes Service (AKS) 叢集的 AKS 範本。Panorama 上的 Azure 外掛程式可協助您設定能夠監控 Azure Kubernetes 叢集工作負載的連線，並取得您已註解為「內部負載平衡器」的服務，以及建立可用於動態位址群組中的標籤。您可以利用 Panorama 動態位址群組，在輸入流量路由至執行於 AKS 叢集上的服務時，對流量套用安全性原則。

- Azure 專用 Panorama 外掛程式如何保護 Kubernetes 服務？
- 保護 AKS 叢集

Azure 專用 Panorama 外掛程式如何保護 Kubernetes 服務？

您可以使用 VM-Series 防火牆來保護 Azure Kubernetes Service (AKS) 叢集的輸入流量。VM-Series 防火牆只能保護負載平衡器（例如 Azure 負載平衡器）已公開的服務。輸出流量只能受到監控。

本章將回顧可讓 Panorama 專用 Azure 外掛程式連線至 AKS 叢集的不同元件。

- 需求
- 用來保護 AKS 叢集的範例中樞-輻軸拓撲
- 使用者定義的路由
- AKS 叢集通訊
- 具有 Kubernetes 標籤的動態位址群組

需求

此解決方案需要下列元件。請參閱「相容性矩陣」中的 Panorama 外掛程式資訊，以瞭解最低版本需求。

- VM-Series 防火牆。
- Panorama — 您的 Panorama 版本必須高於或等於 VM-Series PAN-OS 版本。
- Azure 專用 Panorama 外掛程式。
- Panorama 協調部署。

©2023 Palo Alto Networks, Inc.

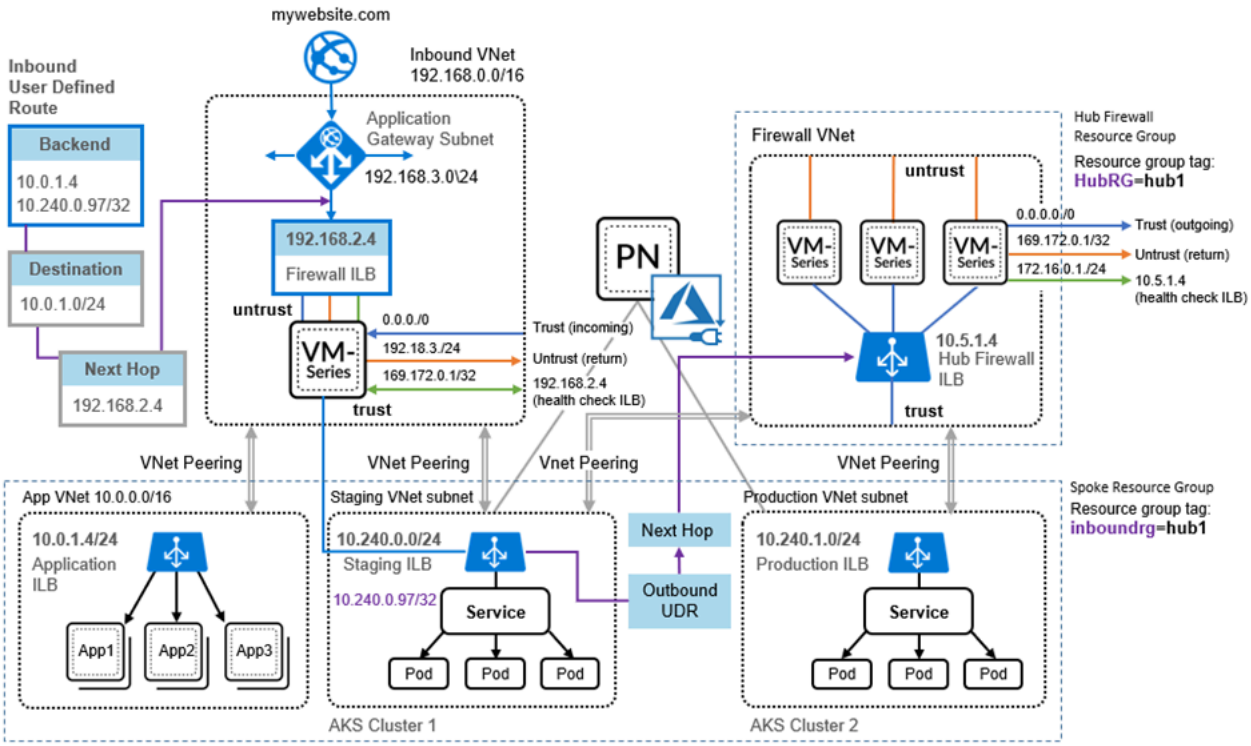
- Azure AKS 範本 1.0 版。此範本會建立 AKS 叢集。

  您必須為叢集啟用 AKS 進階網路 (CNI)。

  若要進行 AKS 部署，必須以進階網路設定中樞與輻軸的 VNet 對等互連（請參閱用來保護 AKS 叢集的範例中樞-輻軸拓撲）。

用來保護 AKS 叢集的範例中樞-輻軸拓撲

下圖顯示可為 Azure AKS 叢集保護輸入流量的範例自動調整規模部署。我們來回顧一下某些元件。



- 自動調整規模基礎結構 — Azure 自動調整規模範本可建立傳訊基礎結構以及基本中樞和輻軸架構。
- **AKS** 叢集 — Palo Alto Networks AKS 範本可在新的 VNet 中建立 AKS 叢集。指定輻軸資源群組的名稱後，範本會為 VNet 和 AKS 叢集標記輻軸資源群組名稱，讓 Panorama 專用 Azure 自動調整規模外掛程式能夠探索到該資源群組。Panorama 專用 Azure 外掛程式會對「預備 ILB」查詢服務 IP 位址，以瞭解 AKS 叢集服務。

只有一個輻軸防火牆擴展集可以與 *AKS* 叢集相關聯；如果您在單一 *AKS* 叢集上公開多個服務，這些服務必須受到相同輻軸的保護。

對於每個資源群組，請建立子網路型位址群組。以上圖為例，請建立 *10.240.0.0/24*（*AKS* 叢集 *1*）的位址群組。

©2023 Palo Alto Networks, Inc.

- **VNet** 對等互連 — 您必須手動設定 VNET 對等互連，以與相同區域中的其他 VNet 通訊。

  不支援跨區域對等互連。

  您可以使用其他自動化工具來部署 *AKS* 叢集。如果部署於現有的 *VNet* 中（例如中樞防火牆 *VNet*），您就必須手動設定與輸入和輸出中樞與輻軸資源群組的 *VNet* 對等互連，並手動為 *VNet* 和 *AKS* 叢集標記資源群組名稱。
- 使用者定義的路由和規則—您可以手動設定使用者定義的路由和規則（請參閱使用者定義的路由）。在上圖中，根據 UDR 規則，傳入的流量可重新導向至防火牆 ILB 以進行檢查。離開 AKS 叢集的輸出流量會根據 Azure 使用者定義路由 (UDR) 規則重新導向至中樞防火牆 ILB。此解決方案採用「全部允許」作為預設政策，讓 Kubernetes 協調依原狀運作，但若要套用政策，您可以使用允許清單或拒絕清單來允許或拒絕輸出流量。

使用者定義的路由

您必須手動建立使用者定義的路由和路由規則，來控管輸入或輸出流量。

輸入

在上圖中，應用程式閘道的輸入流量會導向至後端集區，並根據 UDR 規則重新導向至防火牆 ILB。例如，您可以建立指向 VNet 子網路的 UDR，讓 Kubernetes 服務的流量指向防火牆 ILB。

輸出

在中樞防火牆集上，若要讓每個 AKS 叢集受到保護，您必須建立叢集子網路 CIDR 的靜態路由，並將下一個躍點設為中樞 VNet 信任子網路的閘道位址。

AKS 叢集的所有輸出流量都會透過單一 UDR 規則導向至中樞防火牆集。

AKS 叢集通訊

Azure 專用 Panorama 外掛程式只能與指定 AKS 叢集的 AKS 控制器節點通訊。輸出 AKS 流量的下一個躍點為中樞防火牆 ILB。由於監控受到監控，因此您必須允許所有流量。下列主題主要說明有助於您建立連線的一般做法。在規劃您的網路和子網路時，請多加留意。

- 建立 AKS 叢集驗證
- 使用位址群組識別流量
- 將子網路位址群組新增至最上層原則
- 防止應用程式在工作負載與 AKS 叢集 VNets 對等互連時中斷

建立 **AKS** 叢集驗證

當您在 Panorama 專用 Azure 外掛程式中連接 AKS 叢集時，您必須輸入秘密授權權杖。請使用 Kubernetes 命令執行下列步驟。

STEP 1 | 建立 ClusterRole。

©2023 Palo Alto Networks, Inc.

STEP 2 | 建立 ClusterRoleBinding。

1. 建立 ClusterRoleBinding 的 `.yaml` 檔案。例如，建立名為 `crb.yaml` 的文字檔案。

   ```
   API 版本：rbac.authorization.k8s.io　kind：叢集角色連結　中繼資料：名稱：預設-檢視　角色參考：apiGroup：rbac.授權.k8s.io　kind：叢集角色　名稱：檢視主題：-kind：服務帳戶　名稱：預設　命名空間：預設
   ```

2. 使用 Azure Cloud Shell 套用 `crb.yaml` 角色繫結。

   kubectl apply -f crb.yaml

3. 檢視您剛剛建立的服務帳戶。

   kubectl get serviceaccounts

STEP 3 | 將服務帳戶認證儲存至 `.json` 檔案。

1. 在本機機器上，切換為您想要儲存認證的目錄。
2. 使用 kubectl 命令來建立權杖。

   MY_SA_TOKEN= ‘kubectl get serviceaccounts default -o jsonpath=’ {.secrets[0].name}’ ‘

3. 檢視權杖名稱。

   $ echo $MY_SA_TOKEN

4. 顯示認證。

   kubectl get secret $MY_SA_TOKEN -o json

當您在 Panorama 專用 Azure 外掛程式中連接 AKS 叢集時（在步驟 3.d 中），您需要權杖。

使用位址群組識別流量

若要為受監控的輸出流量產生一些細微性，請建立專用於 AKS 叢集 VNet 子網路的位址群組（例如上圖中的 10.240.0.97/32）。接著，您可以撰寫允許傳入流量或傳回流量的規則，而不使用「全部允許」。

如果您建立位址群組，請務必保有 AKS 連接器與任何工作節點之間的通訊。請參閱 將子網路位址群組新增至最上層原則。

如果通訊中斷，應用程式流量可能會遺失，或您的應用程式部署可能會有問題。

將子網路位址群組新增至最上層原則

若要維護連線，位址群組必須是 Panorama 中最上層原則的一部分。您可以設定叢集位址群組，或啟動載入叢集以設定叢集位址群組。

請在設定 *VNet* 對等互連或使用者定義的路由之前將位址群組新增至最上層原則。

©2023 Palo Alto Networks, Inc.

防止應用程式在工作負載與 **AKS** 叢集 **VNets** 對等互連時中斷

如果 AKS 叢集與執行於個別 VNet 中的 VM 工作負載共存，且 VNet 同時與工作負載輻軸（輸入）和中樞（輸出）對等互連，則您必須建立位址群組以區分工作負載和 AKS 流量，並將該位址群組新增至最上層原則，如前所述。

具有 Kubernetes 標籤的動態位址群組

在監控 AKS 叢集資源時，Azure 外掛程式會自動為 AKS 服務產生下列 IP 標籤。

```
aks.<aks cluster name>.<aks service name>
```

對於節點、*Pod* 或其他資源並不會產生標籤。

如果 AKS 服務有任何標籤 (label)，則會具有下列標籤 (tag)（每個 label 一個 tag）：

```
aks.<aks cluster name>.svc.<label>.<value>
```

如果為叢集定義了 labelSelector 標籤，外掛程式將會產生下列 IP 標籤：

```
aks_<labelSelector>.<aks cluster name>.<aks service name>
```

保護 AKS 叢集

若要讓 Panorama 連線至 Azure Kubernetes Services (AKS) 叢集中的負載平衡器，您必須在 Panorama 上啟用 Azure 外掛程式，以建立與 AKS 叢集的連線。然後，您必須設定防火牆所屬的裝置群組和範本，讓 Panorama 可以將設定物件和原則規則推送至受管理防火牆。

- 開始之前
- 使用範本部署 AKS 叢集
- 在 Panorama 專用 Azure 外掛程式中連接 AKS 叢集
- 設定 VNet 對等互連
- 將流量重新導向至防火牆 ILB
- 將原則套用至相關 AKS 服務
- 部署並保護 AKS 服務

開始之前

若要保護 AKS 的安全，您必須先部署 GitHub 上提供的 Azure 自動調整規模解決方案。

若要保護在 Kubernetes 叢集中作為服務執行的 Web 應用程式，您必須規劃 VNET、子網路和 UDR。VM-Series 防火牆和 Panorama 可讓您保護和檢視您的 Kubernetes 服務。

- 檢閱「Azure 專用 Panorama 外掛程式如何保護 Kubernetes 服務？」。
- 您必須具有 AKS 進階網路，才能使用 Palo Alto Networks AKS 範本。

©2023 Palo Alto Networks, Inc.

- 部署 AKS 叢集之前，請先設計您的 AKS 子網路。請檢閱用來保護 AKS 叢集的範例中樞-輻軸拓撲和AKS 叢集通訊。
  - 此範本會建立單一 AKS 叢集（服務）作為範例。您必須指定 VNet、VNet 子網路和服務的 CIDR 範圍。CIDR 範圍不可重疊
  - 根據您的需求調整子網路的大小。請避免非必要的過大範圍，這樣可能會影響到效能。
  - 請參閱使用者定義的路由。請指定特定的 UDR 路由，而非一般的子網路特定路由。
- 規劃您要如何讓 VNet 對等互連。如果您要讓 AKS 叢集對等互連，請務必閱讀AKS 叢集通訊。
- 考量您要用來識別流量的方式。
  - 如果您想要對輸出 AKS 流量使用位址群組，請參閱將子網路位址群組新增至最上層原則。
  - 如果您的服務名稱或標籤在命名空間中不是唯一的，請使用標籤選取器來篩選標籤和命名空間，以取得唯一的結果。

使用範本部署 AKS 叢集

Azure AKS 範本是可在新的 VNet 中佈建叢集的範例。

STEP 1 | 在 GitHub 上移至 PaloAltoNetworks/azure-aks，並在儲存庫中找出建置套件。

STEP 2 | 將建置套件解壓縮。編輯您本身的部署所需的 `azuredeploy.json` 和 `parameters.json` 檔案，並加以儲存。

STEP 3 | 發出下列 Azure CLI 命令以範本部署範本。

```
az group deployment validate --resource-group RG_NAME --template-
file azuredeploy.json --parameters @parameters.json
```

```
az group deployment create --name DEPLOYMENT_NAME --resource-
group RG_NAME --template-file azuredeploy.json --parameters
 @parameters.json
```

STEP 4 | 在 AKS 叢集上部署您的應用程式或服務。

1. 註解您的服務 YAML 檔案，使類型成為負載平衡器，並將其註解為 service.beta.kubernetes.io/azure-load-balancer-internal: "true"。例如：

```
  apiVersion: v1      kind:服務   中繼資料：名稱：azure-vote-front
    標籤：      服務："azure-vote-front"     層："stagingapp"      註
釋：     service.beta.kubernetes.io/azure-load-balancer-internal:
 "true" 規格：       類型：負載平衡器連接埠：-連接埠：80 選擇器：應用程
式：azure-vote-front
```

2. 若未這麼做，請先建立 AKS 叢集驗證，再繼續操作。

©2023 Palo Alto Networks, Inc.

3. 在 AKS 叢集上部署您的服務。

   例如，您可以透過 kubectl 來部署應用程式：

   ```
   kubectl apply -f myapplication.yaml
   ```

   例如，請參閱：https://github.com/Azure-Samples/azure-voting-app-redis/blob/master/azure-vote-all-in-one-redis.yaml

4. 使用 kubectl 取得已部署之服務的服務 IP。

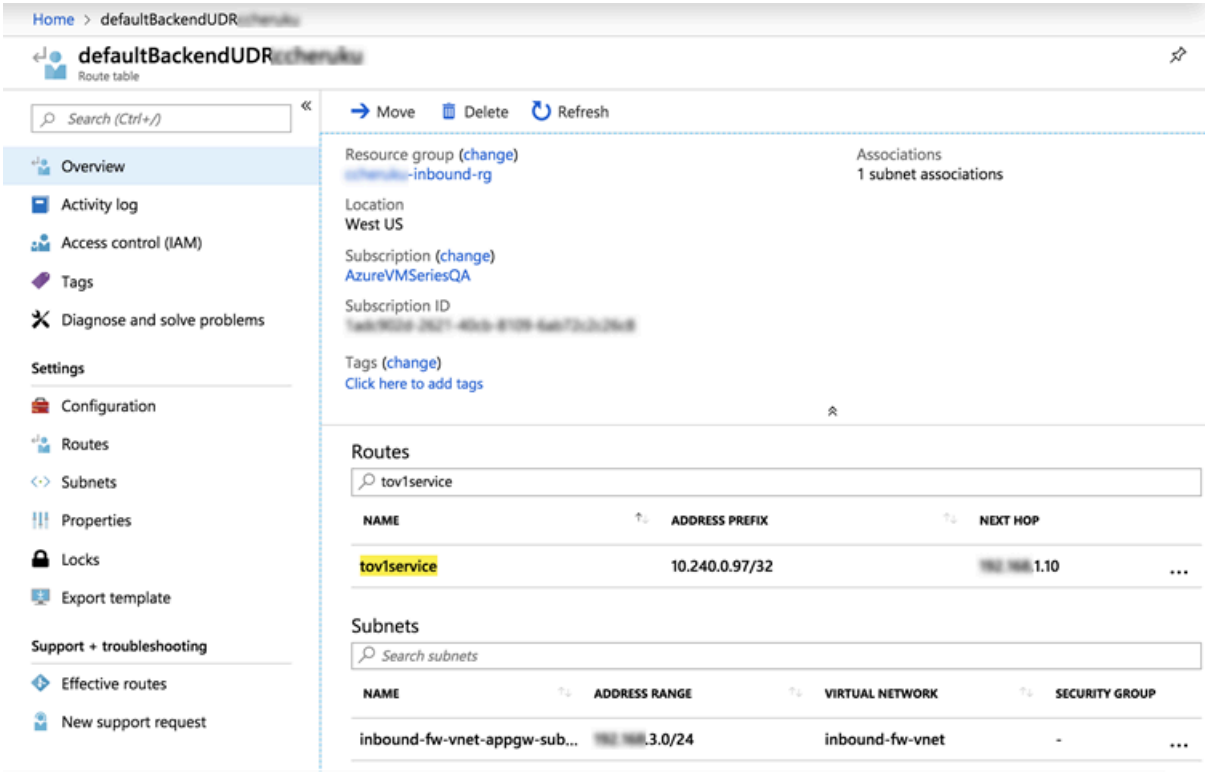
   ```
   kubectl get services -o wide
   ```

```
NAME               TYPE           CLUSTER-IP     EXTERNAL-IP   PORT(S)          AGE    SELECTOR
azure-vote-back    ClusterIP      10.0.77.21     <none>        6379/TCP         2d23h  app=azure-vote-back
azure-vote-front   LoadBalancer   10.0.18.189    10.240.0.97   80:31937/TCP     2d23h  app=azure-vote-front
kubernetes         ClusterIP      10.0.0.1       <none>        443/TCP          2d23h  <none>
```

   在 EXTERNAL-IP 欄中，根據您在步驟 a 中的註解，10.240.0.97 會用於 ILB。在 Azure 上使用服務 IP 建立路由定義的路由。

STEP 5 | 建立 UDR 規則，將您的服務指向位於應用程式閘道後方的防火牆 ILB。

在 Azure 中，移至您的輸入輻軸資源群組，並檢視路由表，然後根據目的地服務 IP 新增路由。在下列畫面中，tov1service **ADDRESS PREFIX**（位址首碼） 欄中的值為服務 IP。



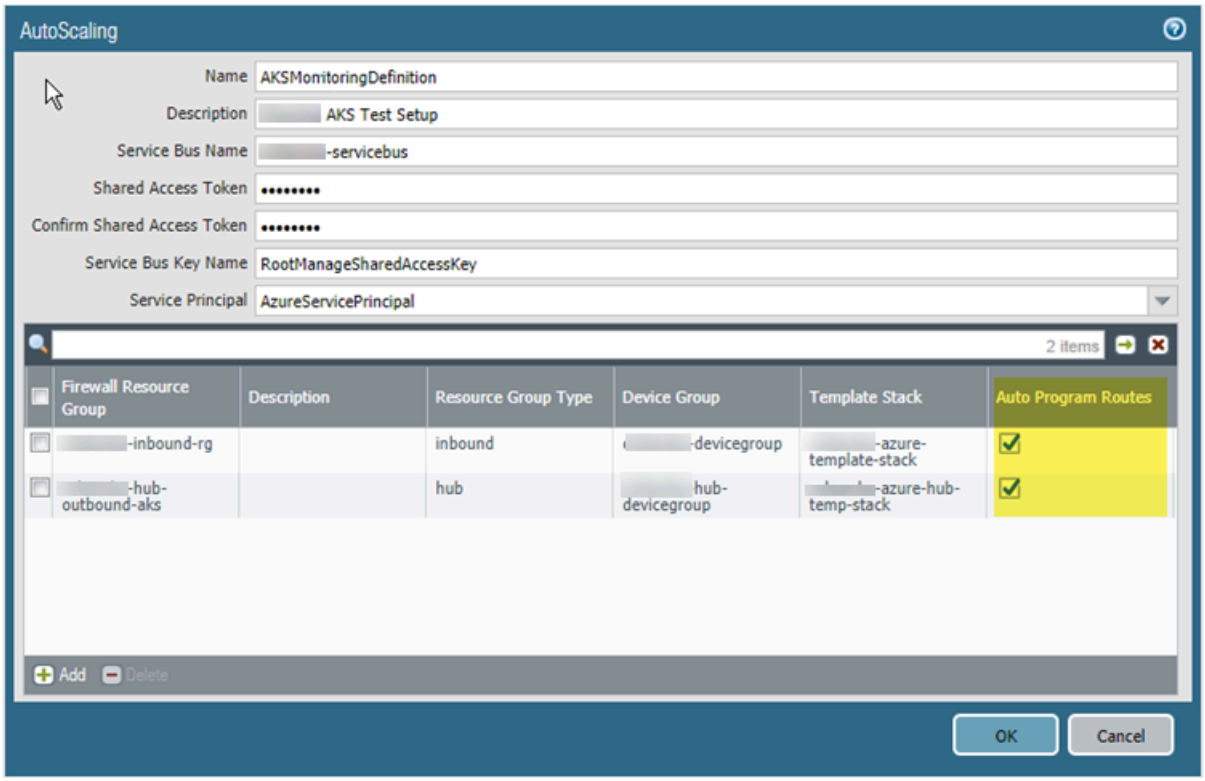
在 Panorama 專用 Azure 外掛程式中連接 AKS 叢集

此工作假設您已部署 Panorama 協調部署，也已建立範本、範本堆疊和裝置群組。

如需填寫各個表單的詳細資訊，請參閱 Panorama 線上說明。

©2023 Palo Alto Networks, Inc.

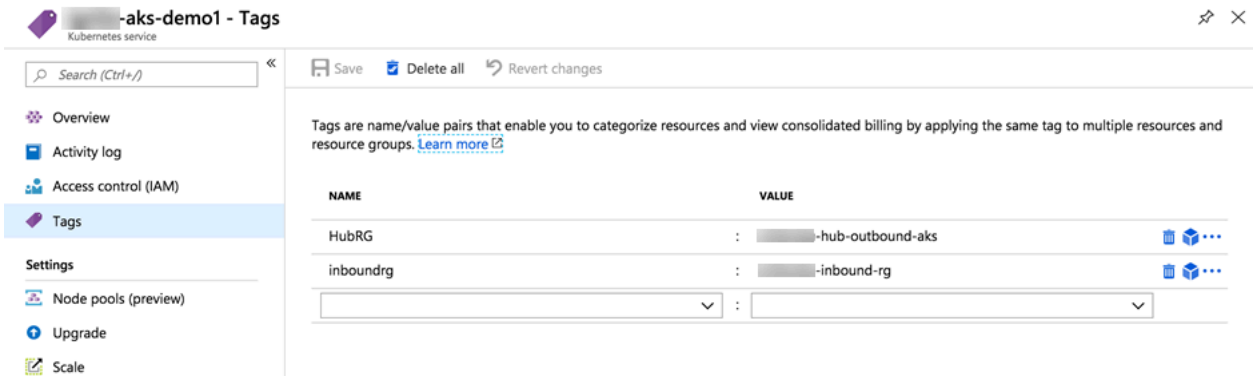
STEP 1 | 選取 **Panorama** > **Azure** > **Deployments**（部署），以檢視您設定部署時建立的監控定義。如下所示，如果 **Auto Program Routes**（自動程式路由）已啟用，系統就會為您設定防火牆路由。



 ©2023 Palo Alto Networks, Inc.

STEP 2 | 在 AKS 中，標記您的資源群組。標籤是名稱/值配對。

1. 選取 **Home**（首頁） > **Resource Groups**（資源群組），然後選擇資源群組。
2. 選取 **Tags**（標籤）並定義名稱/值配對。如下圖所示，標籤名稱必須是 inboundgrouprg 和 HubRG：
   - inboundgrouprg — 您的輻軸資源群組名稱
   - HubRG — 您的中樞資源群組名稱



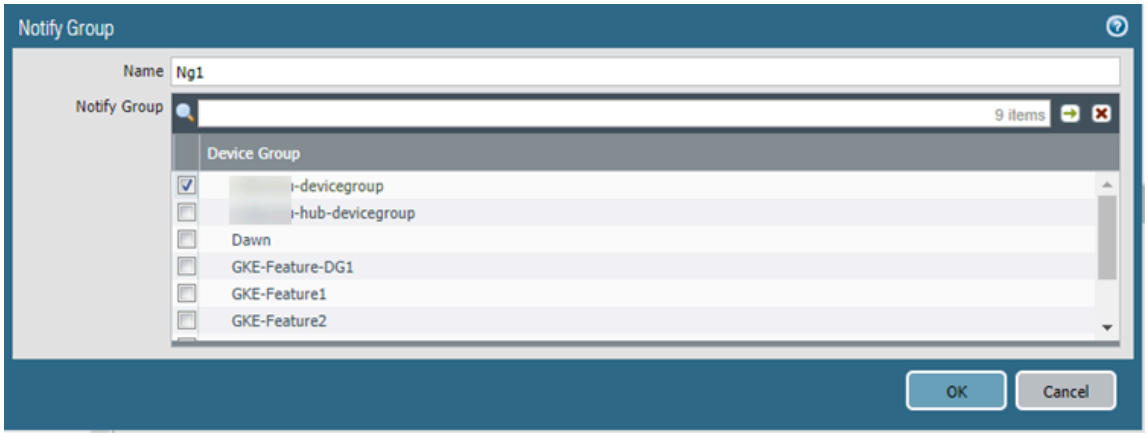
範本會以輻軸資源群組的名稱作為參數，並以輻軸資源群組名稱來標記 VNet 和 AKS 叢集，以便 Azure 專用 Panorama 外掛程式能夠探索到叢集。

範本會在個別的 *VNet* 中部署資源。如果您在輻軸防火牆所設定的相同 *VNet* 中手動部署 *AKS* 叢集，則必須手動為輻軸資源群組名稱建立標籤。

©2023 Palo Alto Networks, Inc.

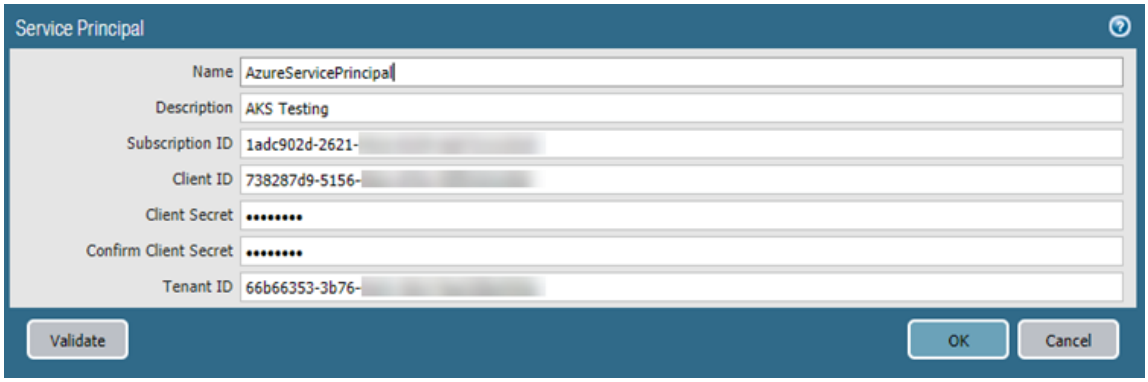
STEP 3 | 在 Panorama 中，選取 **Panorama** > **Azure** > **Setup**（設定）。

1. 在 **General**（一般）頁籤上，啟用監控。
2. 在 **Notify Groups**（通知群組）頁籤上 **Add**（新增） 通知群組，並選取要通知的裝置群組。



3. 在 **Service Principal**（服務主體）頁籤上，**Add**（新增）並 **Validate**（驗證）服務主體。

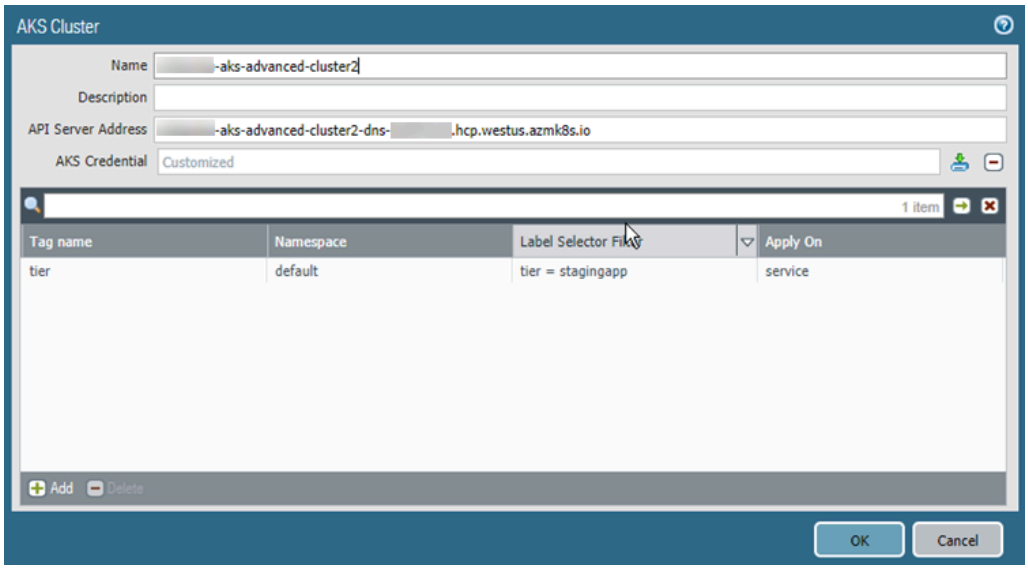
   請使用您為協調部署建立的服務主體。



4. 在 **AKS Cluster**（**AKS** 叢集）頁籤上，**Add**（新增）AKS 叢集。
   - 輸入 AKS 叢集的確切名稱。
   - 輸入 API 伺服器位址。若要在 Azure 中尋找位址，請檢視您的 AKS 服務，然後選取 [Overview（概要）]。
   - 上傳 AKS 認證 JSON 檔案（請參閱建立 AKS 叢集驗證）。
5. 填入其餘欄位，並 **Add**（新增）一或多個標籤。

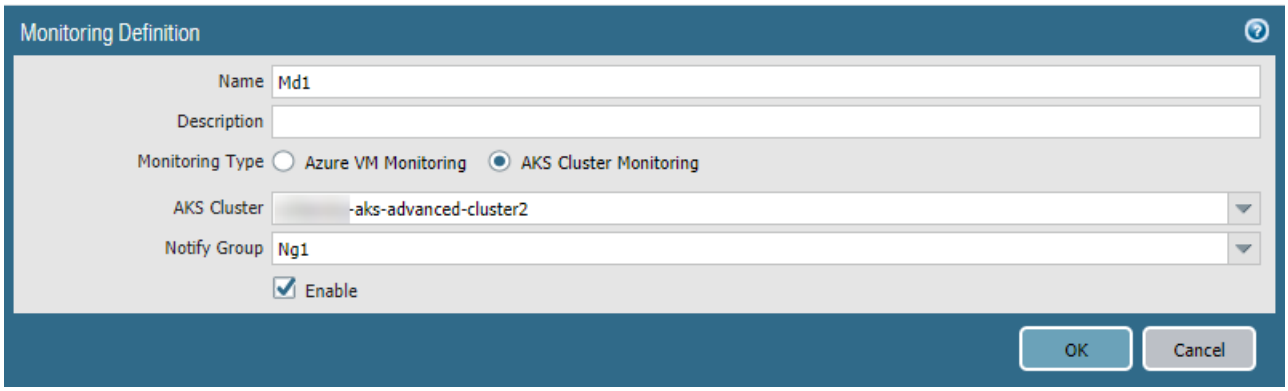
   如果您的服務名稱或標籤在命名空間中不是唯一的，請使用標籤選取器來篩選標籤和命名空間，以取得唯一的結果。

©2023 Palo Alto Networks, Inc.



STEP 4 | 選取 **Panorama** > **Azure** > **Monitoring Definition**（監控定義）

1. 新增監控定義。
2. 輸入名稱和說明，然後選取 **AKS Cluster Monitoring**（**AKS** 叢集監控）。
3. 選取 **AKS Cluster**（**AKS** 叢集）和 **Notify Group**（通知群組），勾選 **Enable**（啟用），然後按一下 **OK**（確定）。



設定 VNet 對等互連

如果您想要使用位址群組來識別流量，請務必先將子網路位址群組新增至您的最上層 Panorama 原則，再設定對等互連。

部署 AKS 叢集後，請設定叢輸入 VNet 到您的叢集，以及從您的叢集到防火牆 VNet 的 VNet 對等互連。

將流量重新導向至防火牆 ILB

您必須手動建立使用者定義路由 (UDR) 和路由規則，以將流量重新導向至特定 ILB。如需範例，請參閱「Azure 專用 Panorama 外掛程式如何保護 Kubernetes 服務？」中的圖表對輸入 UDR 的描述。

©2023 Palo Alto Networks, Inc.

STEP 1 | 建立將 Web 流量重新導向至適當後端集區的 URL 路由規則。

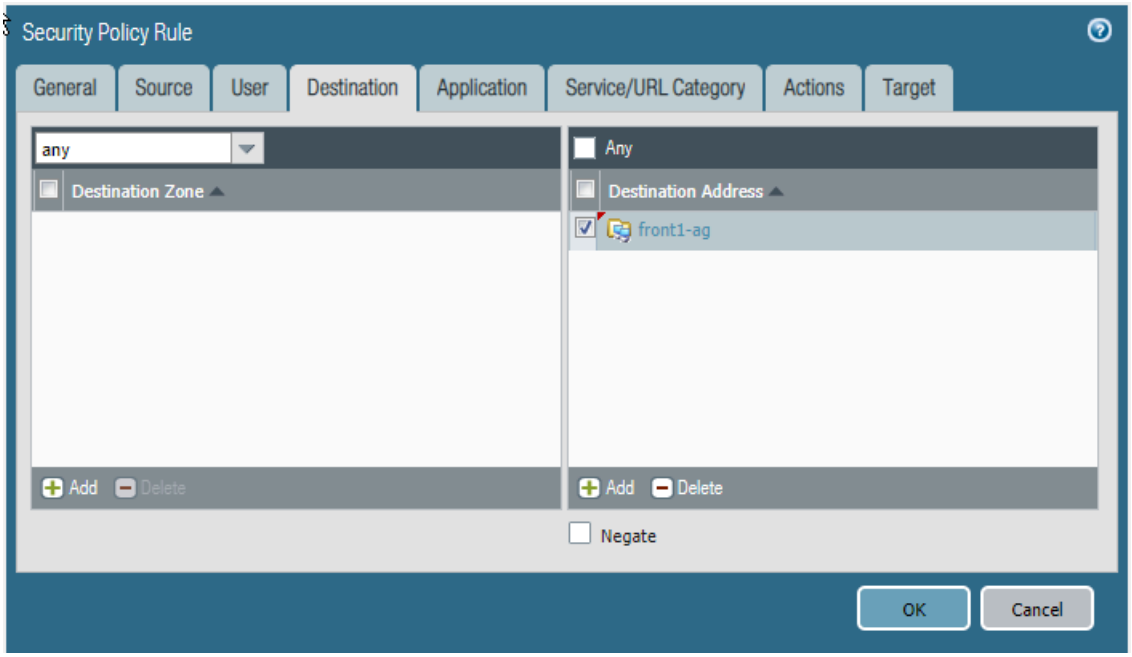
STEP 2 | 更新應用程式閘道的 UDR 規則，以新增服務 CIDR 的路由，並以輻軸防火牆資源群組中的輸入防火牆負載平衡器作為下一個躍點。

將原則套用至相關 AKS 服務

STEP 1 | 在 Panorama 中，選取 [Policies（原則）]。

STEP 2 | 在 **Device Group**（裝置群組）清單中，選擇 AKS 服務的裝置群組。

STEP 3 | **Add**（新增）安全性原則規則。填寫表單，然後在 **Destination**（目的地）頁籤上 **Add**（新增）目的地位址或位址群組。



部署並保護 AKS 服務

這些步驟說明如何使用 VM-Series 防火牆和 Panorama 專用 Azure 外掛程式來保護周遊至 Kubernetes 服務的輸入和輸出流量。

STEP 1 | 在應用程式部署環境中，建立應用程式的 YAML 檔案，或使用已存在的檔案。以下是範例應用程式 YAML 檔案：

```
apiVersion: apps/v1 kind: 部署中繼資料:     名稱: azure-vote-back 規格:
副本: 1 選擇器: 比對標籤: 應用程式: azure-vote-back 範本: 中繼資料: 標籤: 應
用程式: azure-vote-back 規範: 容器: -名稱: azure-vote-back 圖像: redis 資
源: 請求: CPU: 100m                記憶體: 128Mi                限制: CPU: 250m
                記憶體: 256Mi           連接埠: -容器連接埠: 6379 名稱: redis
 - API 版本: V1 kind: 服務中繼資料: 名稱: azure-vote-back 標籤: 服務:
後端 規格: 連接埠: -連接埠: 6379 選擇器: 應用程式: azure-vote-back -
API 版本: 應用程式/v1 kind: 部署中繼資料: 名稱:  azure-vote-front 規格:
複本: 5 選擇器: 比對標籤: 應用程式: azure-vote-front 範本: 中繼資料: 標
```

 ©2023 Palo Alto Networks, Inc.

```
籤：應用程式：azure-vote-front 規範：容器：-名稱：azure-vote-front 圖
像：microsoft/azure-vote-front:v1 資源：請求：CPU：100m              記
憶體：128Mi              限制：CPU：250m              記憶體：256Mi
          連接埠：-容器連接埠：80 環境：-名稱：REDIS              值:"azure-
vote-back"— API 版本：v1 kind:服務中繼資料：名稱：azure-vote-front 標
籤：服務："azure-vote-front" 類型：「生產」供應安全性：「是」a：「值」b：
「值」c：「值」層："stagingapp" 註釋：service.beta.kubernetes.io/azure-
load-balancer-internal「真」 規格：類型：負載平衡器連接埠：-連接埠：80    選
擇器：      應用程式：azure-vote-front
```

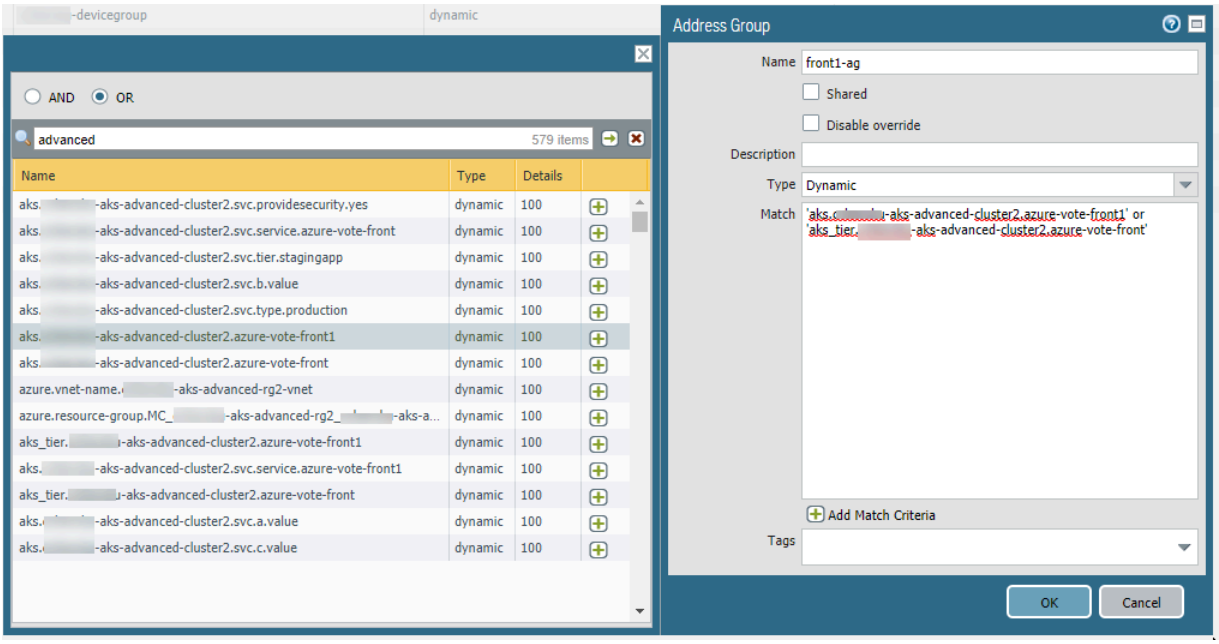
STEP 2 | 編輯您的 YAML 檔案，以標記 Kubernetes 服務。

標籤可讓您在使用 AKS 專用 Panorama 外掛程式連線至叢集時，建立對應標籤與 IP 之間的對應。例如，在上述範例檔案中，請在服務中繼資料中尋找應用程式標籤。這些標籤是：**azure-vote-back** 和 **azure-vote-front**。

STEP 3 | 在您的 AKS 叢集中，套用 YAML 檔案。

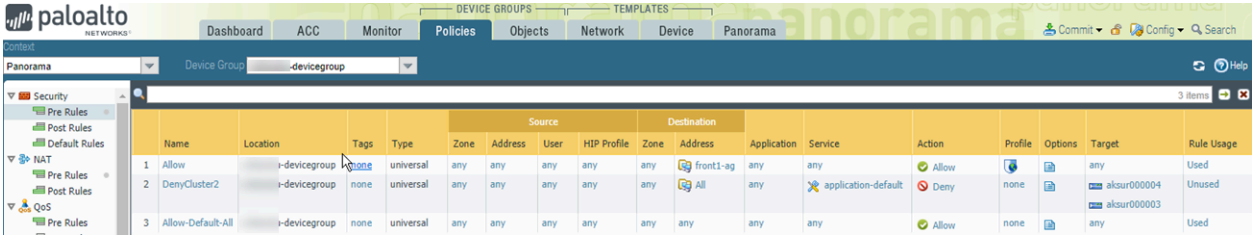
STEP 4 | 在 Panorama 中，使用資源群組標籤建立位址群組。

1. 在 **Objects**（物件）頁籤上，從 **Device Group**（裝置群組）清單中選取裝置群組。
2. 選取 **Address Groups**（位址群組），然後 **Add**（新增）位址群組。
   1. 指定名稱，然後選取 **Dynamic**（動態）類型。
   2. **Add**（新增）位址。新增後會產生一個視窗，列出偵測到的位址。填入清單可能需要幾分鐘的時間。
   3. 您可以為比對準則選擇一或多個位址。選取 AND 或 OR 作為準則關係。
   4. 如果您有許多位址，請在搜尋方塊中輸入字串以篩選輸出，如下圖所示。
   5. 在位址清單中按一下 +，在位址群組比對準則中加入位址。
   6. 在比對準則完成後，按一下 **OK**（確定）。



 ©2023 Palo Alto Networks, Inc.

STEP 5 | 顯示使用位址群組的原則。

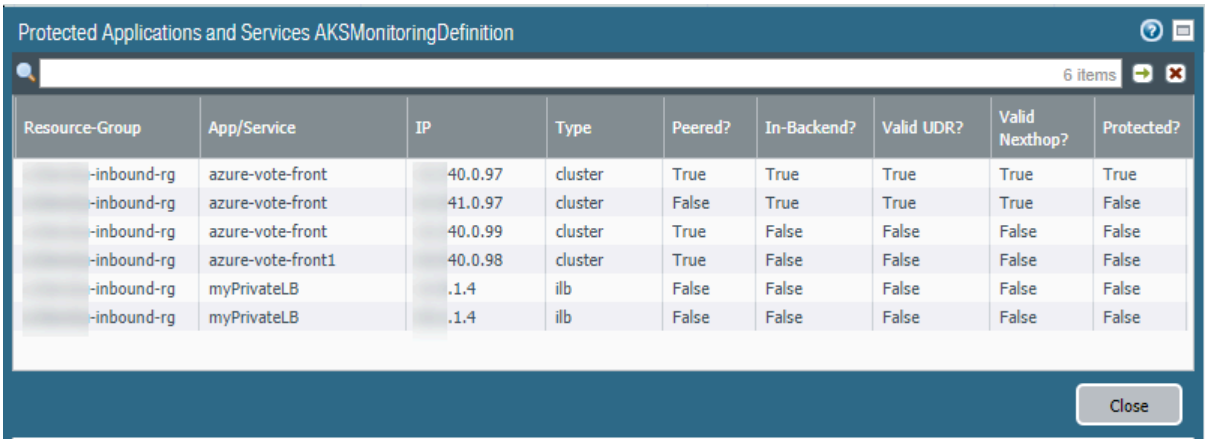


STEP 6 | 檢視受保護的 AKS 服務。

在 **Panorama** > **Azure** > **Deployments**（部署）中，檢視您的監控定義，並在 [Action（動作）] 欄中選取 **Protected Applications and Services**（受保護的應用程式和服務）連結。

Protected?（受保護?）欄會彙總資源群組的安全性狀態。填入視窗可能需要幾分鐘的時間。如果您有許多資源群組，請在搜尋方塊中輸入字串以篩選輸出。

此輸出會以 Azure 資源群組設定為基礎，而不會查詢裝置群組或範本堆疊成員資格。



 ©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

在 OpenStack 上設定 VM-Series 防火牆

OpenStack 專用 VM-Series 防火牆可讓您提供安全應用程式傳遞，以集網路安全性、效能和可視性。

- OpenStack 專用 VM-Series 防火牆
- OpenStack 專用 VM-Series 解決方案的元件
- 基本閘道部署的熱度範本
- 服務鏈結和服務調整規模的熱度範本
- 在基本閘道部署中安裝 VM-Series 防火牆
- 使用服務鏈結或調整規模安裝 VM-Series 防火牆

OpenStack 中的 VM-Series 部署

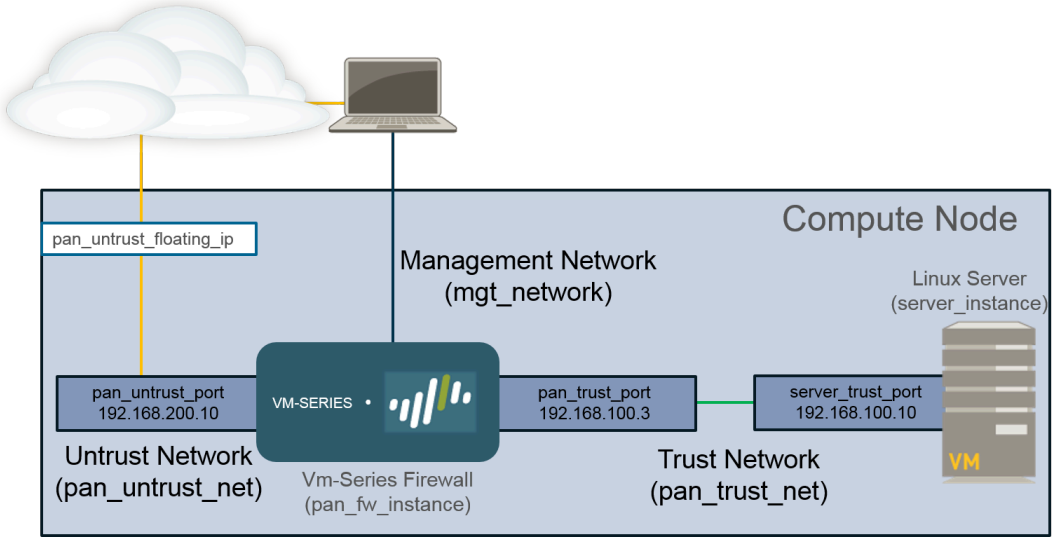
Palo Alto Networks 提供的熱度協調運作範本，可讓您個別地、透過服務鏈結，或利用服務調整規模動態地部署 VM-Series 防火牆。

- 基本閘道
- 服務鏈結和服務調整規模

基本閘道

OpenStack 專用 VM-Series 防火牆可讓您在 OpenStack 環境中的計算節點上執行的 KVM Hypervisor 上，部署 VM-Series 防火牆。此解決方案使用「熱度協調運作範本」和啟動程序來部署 VM-Series 防火牆和 Linux 伺服器。VM-Series 防火牆會檢查已部署的 Linux 伺服器上進出的流量，以保護伺服器。範例啟動程序檔案可讓 VM-Series 防火牆以基本組態啟動，以處理流量。

這些熱度範本檔案和啟動程序檔案結合起來，在類似下列的網路組態中建立兩個虛擬機器，即 VM-Series 防火牆和 Linux 伺服器。



服務鏈結和服務調整規模

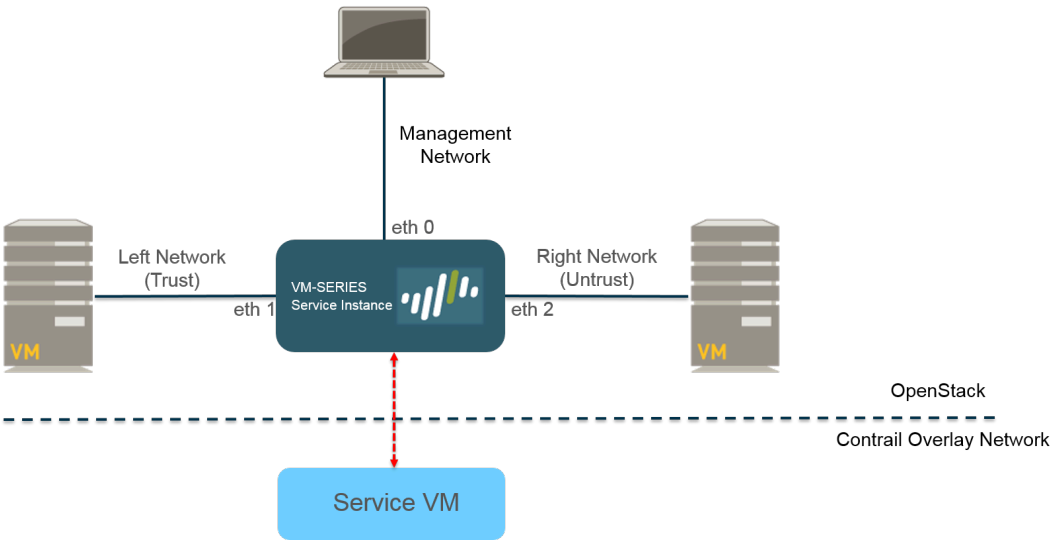
OpenStack Queens 不支援透過服務鏈結和服務調整規模來部署 *VM-Series* 防火牆。

服務鏈結是一項 Contrail 功能，可在 OpenStack 環境中將 VM-Series 防火牆部署為服務實例。服務鏈結是一組服務虛擬機器，例如防火牆或負載平衡器，服務鏈結中的每個虛擬機器都是一個服務實例。服務調整規模可讓您動態部署 VM-Series 防火牆的其他實例。OpenStack 會利用 Ceilometer 收集的 CPU 使用率或每秒傳入位元組度量，決定部署或關閉 VM-Series 防火牆的其他實例，以符合網路的目前需求。

OpenStack 解決方案中的 VM-Series 防火牆會利用熱度協調運作範本，以設定和部署服務鏈結和服務調整規模所需的元件。Palo Alto networks 提供的熱度範本會建立服務範本、服務實例和服務原

©2023 Palo Alto Networks, Inc.

則（將流量導向至 VM-Series 防火牆），以部署兩個 Linux 伺服器和它們之間的 VM-Series 防火牆服務實例。



©2023 Palo Alto Networks, Inc.

OpenStack 專用 VM-Series 解決方案的元件

OpenStack 環境中的 VM-Series 防火牆已搭配下列元件經過測試。

元件	說明
軟體	請參閱相容性矩陣，以深入瞭解支援的軟體版本。
VM-Series 硬體資源	有關您的 VM-Series 型號的最低硬體需求，請參閱 VM-Series 系統需求。 在 OpenStack 中，類別可定義計算實例的 CPU、記憶體和儲存容量。設定熱度範本時，選取的計算類別必須符合或超過 VM-Series 型號的硬體需求。
Fuel Master	Fuel 是 OpenStack 的 web UI 型部署和管理工具。
OpenStack 控制器	此節點執行大部分的 OpenStack 共用服務，例如 API 和排程。此外，Horizon UI 也在此節點上執行。
OpenStack 計算	計算節點包含 OpenStack 部署中的虛擬機器，包括 VM-Series 防火牆。VM-Series 所在的計算節點必須符合下列準則： · 實例類型 OS::Nova::Server · 允許設定至少三個介面 · 接受 VM-Series qcow2 映像 · 接受計算類別參數 請將 ***OpenStack*** 計算節點安裝在裸機伺服器，因為 ***VM-Series*** 防火牆不支援巢狀虛擬化。
Contrail 控制器	Contrail 控制器節點是軟體定義的網路控制器，用於管理、控制和分析虛擬網路。它提供路由資訊給計算節點和閘道節點。 此外，Contrail 控制器也為服務鏈結和服務調整規模提供必要的支援。
Contrail 閘道	Contrail 閘道節點提供從虛擬網路至外部網路的 IP 連線。始於虛擬機器的 MPLS over GRE 通道終止於閘道節點，在此節點上，封包解封並傳送至 IP 網路上的目的地。
Ceilometer（OpenStack 遙測）	就 OpenStack 專用 VM-Series 防火牆而言，Ceilometer 會監控 CPU 使用率，以調整服務的規模。當 CPU 使用率符合已定義的閾值時，就會部署或關閉 VM-Series 防火牆的新服務實例。

©2023 Palo Alto Networks, Inc.

元件	說明
熱度協調運作範本檔案	Palo Alto Networks 提供範例熱度範本來部署 VM-Series 防火牆。此範本由主要範本和環境範本構成。這些檔案會將一個 VM-Series 實例執行個體化為具有一個管理介面和兩個資料介面。 在基本閘道部署中，此範本會將 Linux 伺服器執行個體化為具有一個介面。伺服器的介面會連接至此範本所建立的私人網路。 在服務鏈結或服務調整規模部署中，此範本會將兩個 Linux 伺服器執行個體化，讓其中一個伺服器連接至防火牆的每個資料介面。
VM-Series 防火牆啟動程序檔案	VM-Series 防火牆啟動程序檔案由 init-cfg.txt 檔案、bootstrap.xml 檔案和 VM-Series 驗證碼組成。除了熱度範本檔案，Palo Alto Networks 還提供範例 init-cfg.txt 和 bootstrap.xml 檔案。您必須提供自己的驗證碼來授權 VM-Series 防火牆和啟動任何訂閱。如需 VM-Series 啟動程序檔案的詳細資訊，請參閱啟動 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

基本閘道部署的熱度範本

熱度範本檔案包含下列四個檔案，可協助您在 OpenStack 中啟動 KVM 上的 VM-Series 防火牆。部署 VM-Series 防火牆和 Linux 伺服器需要所有這四個檔案。

- **pan_basic_gw.yaml**—定義為了在計算節點上支援 VM-Series 防火牆和 Linux 伺服器而建立的資源，例如介面和 IP 位址。
- **pan_basic_gw_env.yaml**—定義 VM-Series 防火牆和 Linux 伺服器所在的環境。pan_basic_gw.yaml 檔案中有許多參數都參照此檔案中定義的參數，例如 VM-Series 和 Linux 伺服器的類別。
- **init-cfg.txt**—包含在防火牆管理介面上啟用 DHCP 的操作命令。
- **bootstrap.xml**—提供 VM-Series 防火牆的基本組態。bootstrap.xml 檔案會設定資料介面和 IP 位址。這些值必須符合 pan_basic_gw.yaml 檔案中相應的值。

  此外，bootstrap.xml 檔案還包含一個 NAT 規則，稱為 untrust2trust。此規則會將伺服器上的信任連接埠，轉譯為 VM-Series 防火牆上的不受信任連接埠。

有兩種方式可將啟動載入檔案傳至 OpenStack — 檔案插入（特質檔案）或使用者資料。

從 *OpenStack Queens* 開始已不再支援檔案插入；您必須改用使用者資料。

下表說明 pan_basic_gw.yaml 範本檔案建立的資源，並提供預設值（如適用）。

資源	說明
pan_fw_instance	具有一個管理介面和兩個資料介面的 VM-Series 防火牆。
server_instance	具有單一介面的 Linux 伺服器。
pan_trust_net	通向內部網路的連線，防火牆的信任介面和伺服器的信任介面都連接至此網路。
pan_trust_subnet	連接至防火牆的信任介面 (pan_trust_net) 且 CIDR 值為 192.168.100.0/24 的子網路。
pan_untrust_net	防火牆的不受信任連接埠所連接的不受信任網路。
pan_untrust_subnet	連接至防火牆的不受信任介面 (pan_untrust_net) 且 CIDR 值為 192.168.200.0/24 的子網路。
allow_ssh_https_icmp_secgrou	在連接埠 22 和 443 上允許 TCP 和允許 ICMP 流量的安全性群組。
pan_untrust_port	在第 3 層模式中部署的 VM-Series 防火牆的不受信任連接埠。熱度範本提供預設 IP 位址 192.168.200.10 給此連接埠。

©2023 Palo Alto Networks, Inc.

資源	說明
	如果您在熱度範本中變更此 IP 位址，則必須在 bootstrap.xml 檔案中變更 IP 位址。
pan_untrust_floating_ip	從 public_network 指派的浮動 IP 位址。
pan_untrust_floating_ip_assoc	這會將 pan_untrust_floating_ip 與 the pan_untrust_port 相關聯。
pan_trust_port	VM-Series 防火牆第 3 層模式的信任連接埠。
server_trust_port	Linux 伺服器第 3 層模式的信任連接埠。熱度範本提供預設 IP 位址 192.168.100.10 給此連接埠。 如果您在熱度範本中變更此 IP 位址，則必須在 bootstrap.xml 檔案中變更 IP 位址。

pan_basic_gw.yaml 檔案參照 pan_basic_gw_env.yaml 中的許多值，需要這些值才能建立部署 VM-Series 防火牆和 Linux 伺服器所需的資源。熱度範本環境檔案包含下列參數。

參數	說明
mgmt_network	VM-Series 防火牆管理介面會連接至此參數中指定的網路。此範本不會建立管理網路；您必須在部署熱度範本之前建立此網路。預設值是 mgmt_ext_net。
public_network	OpenStack 叢集和叢集中的虛擬機器用來與外部或公共網路通訊的位址。公共網路提供虛擬 IP 位址給公共端點，以用來連線至 OpenStack 服務 API。此範本不會建立公共網路；您必須在部署熱度範本之前建立此網路。預設值是 public_net。
pan_image	此參數指定在部署 VM-Series 防火牆時，熱度範本所使用的 VM-Series 基本映像。預設值是 pa-vm-7.1.4。
pan_flavor	此參數定義配置給 VM-Series 防火牆的硬體資源。預設值是 m1.medium。此值符合在 KVM 上設定 VM-Series 防火牆章節中說明的。
server_image	此參數讓熱度範本知道要用於 Linux 伺服器的映像。預設值是 Ubuntu-14.04。
server_flavor	此參數定義配置給 Linux 伺服器的硬體資源。預設值是 m1.small。
server_key	用於透過 ssh 存取 Linux 伺服器的伺服器金鑰。預設值是 server_key。您可以在環境檔案中輸入新伺服器金鑰來變更此值。

©2023 Palo Alto Networks, Inc.

服務鏈結和服務調整規模的熱度範本

OpenStack Queens 不支援透過服務鏈結和服務調整規模來部署 *VM-Series* 防火牆。

熱度範本環境檔案中定義的參數，都是針對透過服務鏈結或服務調整規模所部署的 VM-Series 防火牆實例而定義。環境檔案中定義的參數分成如下所述的區段。服務鏈結的熱度範本有兩個版本（vwire 和 L3），而服務調整規模則是一個版本。

服務鏈結需要熱度範本檔案和兩個啟動程序檔案，才能啟動 VM-Series 防火牆服務實例，以及左右網路中的兩個 Linux 伺服器。

- 範本檔案—此範本定義的資源是建立來支援 VM-Series 防火牆和兩個 Linux 伺服器，例如介面和 IP 位址。
  - service_chaining_template_vm.yaml，適用於 vwire 部署。
  - service_chaining_template_L3.yaml，適用於 L3 部署。
  - service_scaling_template.yaml，適用於服務調整規模部署。
- 環境檔案—此環境檔案定義 VM-Series 防火牆和 Linux 伺服器所在的環境。範本中有許多參數都參照此檔案中定義的參數，例如 VM-Series 的類別和 Linux 伺服器的名稱。
  - service_chaining_env_vm.yaml，適用於 vwire 部署。
  - service_chaining_env_L3.yaml，適用於 L3 部署。
  - service_scaling_env.yaml，適用於服務調整規模部署。
- **service_instance.yaml**—（僅限服務調整規模）這是巢狀熱度範本，由 Service_Scaling_template.yaml 參照來部署服務實例。其中提供針對調整規模事件而部署服務實例的必要資訊。
- **init-cfg.txt**—提供啟動 VM-Series 防火牆至少需要的資訊。提供的 init-cfg.txt 只包含在防火牆管理介面上啟用 DHCP 的操作命令。
- **<file_name>_bootstrap.xml**—提供 VM-Series 防火牆的基本設定。bootstrap.xml 檔案會設定資料介面。這些值必須符合熱度範本檔案中相應的值。

如需 init-cfg.txt 和 bootstrap.xml 檔案的詳細資訊，請參閱啟動程序組態檔案。

下表說明環境檔案的參數。

- 虛擬網路
- 虛擬電腦
- 服務範本
- 服務實例
- IPAM
- 服務原則
- 警報

©2023 Palo Alto Networks, Inc.

虛擬網路

熱度範本環境檔案中的虛擬網路組態參數可定義虛擬網路，以連線至熱度範本所部署的 VM-Series 防火牆和兩個 Linux 伺服器。

虛擬網路 (VN Config)	
management_network	VM-Series 防火牆管理介面會連接至此參數中指定的網路。
left_vn 或 left_network	左邊虛擬網路的名稱。
right_vn 或 right_network	右邊虛擬網路的名稱。
left_vn_fqdn	左邊虛擬網路的完全合格網域名稱。
right_vn_fqdn	右邊虛擬網路的完全合格網域名稱。
route_target	請編輯此值，以符合您的外部閘道的路由目標組態。

虛擬電腦

虛擬機器參數定義左邊和右邊 Linux 伺服器。連接埠元組的名稱在此定義，供熱度範本參照。在 Contrail 中，連接埠元組是連線至相同虛擬機器的一組已排序的虛擬機器介面。連接埠元組可讓您建立連接埠，並在建立服務實例時傳遞該資訊。熱度範本會建立左邊、右邊和管理連接埠，並新增至連接埠元組。然後，連接埠元組會連結至服務實例。使用熱度範本啟動服務實例時，連接埠元組會將服務虛擬機器對應至 OpenStack 中部署的虛擬機器。

虛擬機器 (VM Config)	
flavor	左邊和右邊虛擬機器的類別。預設值是 m1.small。
left_vm_image 或 right_vm_image 或 image	左邊和右邊虛擬機器的軟體映像名稱。請變更此值，以符合您上傳的映像的檔案名稱。 預設值是 TestVM，這是 OpenStack 提供的預設映像。
svm_name	套用至 VM-Series 防火牆的名稱。
left_vm_name 和 right_vm_name	左邊和右邊虛擬機器的名稱。
port_tuple_name	兩個 Linux 伺服器和 VM-Series 防火牆使用的連接埠元組名稱。
server_key	用於透過 SSH 存取虛擬機器的伺服器金鑰。預設值是 server_key。您可以在環境檔案中輸入新伺服器金鑰來變更此值。

©2023 Palo Alto Networks, Inc.

服務範本

服務範本定義服務實例的參數，例如軟體映像、虛擬機器類別、服務類型和介面。服務範本是在網域的範圍內設定，可用於指定之網域內的所有專案。

服務實例 (ST Config)	
S_Tmp_name	服務範本的名稱。
S_Tmp_version	服務範本版本。預設值是 2。請勿變更此參數，因為支援連接埠元組需要服務範本版本 2。
S_Tmp_service_mode	服務模式是 VM-Series 防火牆服務實例使用的網路模式。若為 L3 網路範本，預設值是 in-network。若為虛擬介接範本，預設值是 transparent。
S_Tmp_service_type	範本所部署的服務類型。預設值是 firewall，在部署 VM-Series 防火牆時不可變更。
S_Tmp_image_name	此參數指定在部署 VM-Series 防火牆時，熱度範本所使用的 VM-Series 基本映像。請編輯此參數，以符合上傳至 OpenStack 環境的 VM-Series 防火牆映像的名稱。
S_Tmp_flavor	此參數定義配置給 VM-Series 防火牆的硬體資源。預設值是 m1.large。
S_Tmp_interface_type_mgmt S_Tmp_interface_type_left S_Tmp_interface_type_right	這些參數定義管理、左邊和右邊介面的介面類型。
domain	此服務範本繫結的網域。預設值是 default-domain。

服務實例

熱度範本環境檔案的服務實例部分，提供由熱度範本和服務範本所部署的個別實例的名稱。

Service Instance (SI Config)	
S_Ins_name	服務實例名稱。這是 Contrail 中的 VM-Series 防火牆實例的名稱。
S_Ins_fq_name	服務實例的完全合格名稱。

IPAM

IP address management（IP 位址管理 - IPAM）為服務實例的介面提供 IP 位址資訊。將這些參數變更為最適合您的環境。

©2023 Palo Alto Networks, Inc.

IPAM (IPAM Config)	
NetIPam_ip_prefix_mgmt	VM-Series 防火牆上管理介面的 IP 首碼。預設值是 172.2.0.0。
NetIPam_ip_prefix_len_mgmt	VM-Series 防火牆上管理介面的 IP 首碼長度。預設值是 /24。
NetIPam_ip_prefix_left	VM-Series 防火牆上左邊介面的 IP 首碼。預設值是 10.10.1.0。
NetIPam_ip_prefix_len_left	VM-Series 防火牆上左邊介面的 IP 首碼長度。預設值是 /24。
NetIPam_ip_prefix_right	VM-Series 防火牆上右邊介面的 IP 首碼。預設值是 10.10.2.0。
NetIPam_ip_prefix_len_right	VM-Series 防火牆上右邊介面的 IP 首碼長度。預設值是 /24。
NetIPam_addr_from_start	此參數決定如何將 IP 位址指派給上述子網路上的 VM。若為 true，任何新的 VM 會取用下一個可用的 IP 位址。若為 false，則隨機指派 IP 位址給任何新的 VM。預設值是 true。

服務原則

服務政策定義流量重新導向規則和政策，讓左邊和右邊虛擬機器之間傳送的流量流向 VM-Series 防火牆服務實例。

服務政策 (Policy Config)	
policy_name	Contrail 中的服務政策的名稱，可將流量重新導向至 VM-Series 防火牆。若為 L3 範本，預設值是 PAN_SVM_policy-L3。若為虛擬介接範本，預設值是 PAN_SVM_policy-vw。
policy_fq_name	服務政策的完全合格名稱。
simple_action	Contrail 對流向 VM-Series 防火牆服務實例套用的預設動作。預設值為 pass，因為 VM-Series 防火牆會將其自己的安全性政策套用至流量。
protocol	Contrail 允許傳遞至 VM-Series 防火牆的通訊協定。預設值是 any。
src_port_end 和 src_port_start	使用此參數來指定應該與政策規則相關聯的來源連接埠。您可以輸入單一連接埠、以逗號分隔的連接埠清單，或 <port>-<port> 格式的連接埠範圍。 在提供的熱度範本中，預設值是 -1，表示任何來源連接埠。
direction	此參數定義 Contrail 允許傳遞至 VM-Series 防火牆的流量方向。預設值是 <> 或雙向流量。

©2023 Palo Alto Networks, Inc.

服務政策 (Policy Config)	
dst_port_end 和 dst_port_start	使用此參數來指定應該與政策規則相關聯的目的地連接埠。您可以輸入單一連接埠、以逗號分隔的連接埠清單，或 <port>-<port> 格式的連接埠範圍。 在提供的熱度範本中，預設值是 -1，表示任何目的地連接埠。

警報

警報參數用於服務調整規模，不包含在服務鏈結環境檔案中。這些參數定義閾值，供 Contrail 據以決定何時應該調整規模。這組參數僅供服務調整規模熱度範本使用。

在冷卻參數下設定的預設時間，是為了讓防火牆有足夠時間啟動。如果您變更冷卻值，請預留足夠時間讓每個新的防火牆實例啟動。

警報	
meter_name	由 Ceilometer 監控和 contrail 使用的度量，用以決定何時應該部署或關閉額外的 VM-Series 防火牆。熱度範本使用 CPU 使用率或每秒位元組，作為服務調整規模的度量。
cooldown_initial	在初始服務實例啟動之後，Contrail 在啟動額外服務實例之前等待的時間量。預設值是 1200 秒。
cooldown_scaleup	在第一個相應增加服務實例啟動之後，Contrail 在啟動其他服務實例之間等待的時間量。預設值是 1200 秒。
cooldown_scaledown	在第一個相應增加服務實例關閉之後，Contrail 在關閉其他服務實例之間等待的時間量。預設值是 1200 秒。
period_high	在觸發警報之前平均 CPU 負載計算為偏高的期間。預設值是 300 秒。
period_low	在觸發警報之前平均 CPU 負載計算為偏低的期間。預設值是 300 秒。
threshold_high	Contrail 在啟動相應增加事件之前所參照的 CPU 使用率值，以百分比或每秒位元組為單位。預設值是 40% CPU 使用率或每秒 2800 位元組。
threshold_low	Contrail 在啟動相應減少事件之前所參照的 CPU 使用率值，以百分比或每秒位元組為單位。預設值是 20% CPU 使用率或每秒 12000 位元組。

©2023 Palo Alto Networks, Inc.

在基本閘道部署中安裝 VM-Series 防火牆

完成下列步驟來準備熱度範本、啟動程序檔案和軟體映像，在 OpenStack 中部署 VM-Series 防火牆需要這些項目。備妥檔案後，部署 VM-Series 防火牆和 Linux 伺服器。

STEP 1 | 下載熱度範本和啟動程序檔案。

從 GitHub 儲存庫下載熱度範本套件。

STEP 2 | 下載 VM-Series 基本映像。

1. 登入 Palo Alto Networks 客戶支援入口網站。
2. 從 **Filter By**（篩選依據）下拉式清單中，選取 **Software Updates**（軟體更新）並選取 **PAN-OS for VM-Series KVM Base Images**（**PAN-OS for VM-Series KVM** 基本映像）。
3. 下載 KVM**qcow2** 檔案的 VM-Series。

STEP 3 | 下載 Ubuntu 14.04，將映像上傳至 OpenStack 控制器。

熱度範本需要 Ubuntu 映像才能啟動 Linux 伺服器。

1. 下載 Ubuntu 14.04。
2. 登入 Horizon UI。
3. 選取 **Project**（專案） > **Compute**（計算） > **Images**（映像） > **Create Image**（建立映像）。
4. 將映像的 **Name**（名稱）命名為 Ubuntu 14.04，以符合 pan_basic_gw_env.yaml 檔案中的參數。
5. 將 Image Source（映像來源）設為 **Image File**（映像檔案）。
6. 按一下 **Choose File**（選取檔案），並導覽至您的 Ubuntu 映像檔案。
7. 將 Format（格式）設為符合此 Ubuntu 映像的檔案格式。
8. 按一下 **Create Image**（建立映像）。

STEP 4 | 將 KVM 專用 VM-Series 基本映像上傳至 OpenStack 控制器。

1. 登入 Horizon UI。
2. 選取 **Project**（專案） > **Compute**（計算） > **Images**（映像） > **Create Image**（建立映像）。
3. 為此映像**Name**（命名）以比對在熱度範本中的映像名稱。
4. 將 Image Source（映像來源）設為 **Image File**（映像檔案）。
5. 按一下 **Choose File**（選取檔案），並導覽至您的 VM-Series 映像檔案。
6. 將 Format（格式）設為 **QCOW2-QEMU Emulator**（**QCOW2-QEMU** 模擬器）。
7. 按一下 **Create Image**（建立映像）。

©2023 Palo Alto Networks, Inc.

STEP 5 | 上傳啟動程序檔案。有兩種方式可將啟動載入檔案傳至 OpenStack — 檔案插入（特質檔案）或使用者資料。若要透過使用者資料傳遞啟動載入檔案，您必須將檔案放在 tar ball（.tgz 檔案）中，並以 base64 編碼該 tar ball。

從 *OpenStack Queens* 開始已不再支援檔案插入；您必須改用使用者資料。

- 進行檔案插入時，請將 init-cfg.txt、bootstrap.xml 和 VM-Series 驗證碼上傳至 OpenStack 控制器，或 OpenStack 控制器可存取的 Web 伺服器。
- 如果使用 **--user-data** 方法將啟動載入套件傳遞至 config-drive，您可以使用下列命令來建立 tar ball，並以 base64 編碼 tar ball (.tgz file)：

```
tar -cvzf <file-name>.tgz config/ license software content base64
 -i <in-file> -o <outfile>
```

STEP 6 | 編輯 pan_basic_gw.yaml 範本來指向啟動程序檔案和驗證碼。

- 如果您要使用特質檔案，請在 personality 底下，指定檔案位置的檔案路徑或 Web 伺服器位址。將您不使用的任何一行取消註解。

```
  pan_fw_instance: type:OS::Nova::Server properties: image:
 { get_param: pan_image } flavor: { get_param: pan_flavor }
 networks: - network: { get_param: mgmt_network } - port:
 { get_resource: pan_untrust_port } - port: { get_resource:
 pan_trust_port } user_data_format:RAW config_drive: true
 personality: /config/init-cfg.txt: {get_file: "/opt/pan_bs/
init-cfg.txt"} # /config/init-cfg.txt: { get_file: "http://
web_server_name_ip/pan_bs/init-cfg.txt" } /config/bootstrap.xml:
 {get_file: "/opt/pan_bs/bootstrap.xml"} # /config/bootstrap.xml:
 { get_file: "http://web_server_name_ip/pan_bs/bootstrap.xml" } /
license/authcodes: {get_file: "/opt/pan_bs/authcodes"} # /
license/authcodes: {get_file: "http://web_server_name_ip/pan_bs/
authcodes"}
```

- 如果您要使用「使用者資料」，請在 user_data 底下，指定檔案位置的檔案路徑或 Web 伺服器位址。如果您有多個

```
pan_fw_instance: type:OS::Nova::Server properties: image:
 { get_param: pan_image } flavor: { get_param: pan_flavor }
 networks: - port: { get_resource: mgmt_port } - port:
 { get_resource: pan_untrust_port } - port: { get_resource:
 pan_trust_port } user_data_format:RAW config_drive: true
 user_data: # get_file: http://10.0.2.100/pub/repository/panos/
images/openstack/userdata/boot.tgz get_file: /home/stack/newhot/
bootfiles.tgz
```


©2023 Palo Alto Networks, Inc.

STEP 7 | 編輯 pan_basic_gw_env.yaml 範本環境檔案來適合您的環境。確保管理和公共網路值符合您在 OpenStack 環境中建立的值。將 pan_image 設為符合您指派給 VM-Series 基本映像檔案的名稱。您也可以在這裡變更伺服器金鑰。

```
root@node-2:~# cat basic_gateway/pan_basic_gw_env.yaml parameters:
 mgmt_network: mgmt_ext_net public_network: public_net pan_image:
 pa-vm-image pan_flavor: m1.medium server_image:Ubuntu-14.04
 server_flavor: m1.small server_key: server_key
```

STEP 8 | 部署熱度範本。

1. 執行命令 **source openrc**
2. 執行命令 **heat stack-create *<stack-name>* -f *<template>* -e ./*<env-template>***

```
root@node-2:~# heat stack-create stack1 -f pan_basic_gw.yaml -e pan_basic_gw_env.yaml
+--------------------------------------+------------+--------------------+----------------------+--------------+
| id                                   | stack_name | stack_status       | creation_time        | updated_time |
+--------------------------------------+------------+--------------------+----------------------+--------------+
| ebe40f9d-2781-4bb2-b246-f15c761f9045 |   stack1   | CREATE_IN_PROGRESS | 2017-01-25T13:36:59 | None         |
+--------------------------------------+------------+--------------------+----------------------+--------------+
```

STEP 9 | 確認 VM-Series 防火牆已成功部署。

您可以使用下列命令來檢查堆疊的建立狀態。

- 使用 **heat stack-list** 來檢查堆疊狀態
- 使用 **heat event-list** 來檢視堆疊建立期間發生之事件的詳細清單
- 使用 **heat stack-show** 來檢視堆疊的詳細資訊

STEP 10 | 確認 VM-Series 防火牆會雙向檢查進入 Linux 伺服器的流量。

1. 登入防火牆。
2. 選取 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量）可檢視 SSH 工作階段。

©2023 Palo Alto Networks, Inc.

使用服務鏈結或調整規模安裝 VM-Series 防火牆

完成下列步驟來準備熱度範本、啟動程序檔案和軟體映像，部署 VM-Series 防火牆需要這些項目。備妥檔案後，部署 VM-Series 防火牆服務和兩個 Linux 伺服器。

OpenStack Queens 不支援透過服務鏈結和服務調整規模來部署 *VM-Series* 防火牆。

STEP 1 | 下載熱度範本和啟動程序檔案。

從 GitHub 儲存庫下載熱度範本套件。

STEP 2 | 下載 VM-Series 基本映像。

1. 登入 Palo Alto Networks 客戶支援入口網站。
2. 從 **Filter By**（篩選依據）下拉式清單中，選取 **Software Updates**（軟體更新）並選取 **PAN-OS for VM-Series KVM Base Images**（**PAN-OS for VM-Series KVM** 基本映像）。
3. 下載 KVM**qcow2** 檔案的 VM-Series。

STEP 3 | 下載 Ubuntu 14.04，將映像上傳至 OpenStack 控制器。

對於服務鏈結，您可以使用 OpenStack 提供的預設映像，稱為 TestVM。使用 TestVM 時，請跳過此步驟。服務調整規模需要 Ubuntu 映像。

1. 下載 Ubuntu 14.04。
2. 登入 Horizon UI。
3. 選取 **Project**（專案） > **Compute**（計算） > **Images**（映像） > **Create Image**（建立映像）。
4. 將映像的 **Name**（名稱）命名為 Ubuntu 14.04，以符合 pan_basic_gw_env.yaml 檔案中的參數。
5. 將 Image Source（映像來源）設為 **Image File**（映像檔案）。
6. 按一下 **Choose File**（選取檔案），並導覽至您的 Ubuntu 映像檔案。
7. 將 Format（格式）設為符合此 Ubuntu 映像的檔案格式。
8. 按一下 **Create Image**（建立映像）。

使用 *Ubuntu* 映像時需要伺服器金鑰。確保伺服器金鑰已新增至環境檔案。

©2023 Palo Alto Networks, Inc.

STEP 4 | 將 KVM 專用 VM-Series 基本映像上傳至 OpenStack 控制器。

1. 登入 Horizon UI。
2. 選取 **Project**（專案） > **Compute**（計算） > **Images**（映像） > **Create Image**（建立映像）。
3. 為此映像**Name**（命名）以比對在熱度範本中的映像名稱。
4. 將 Image Source（映像來源）設為 **Image File**（映像檔案）。
5. 按一下 **Choose File**（選取檔案），並導覽至您的 VM-Series 映像檔案。
6. 將 Format（格式）設為 **QCOW2-QEMU Emulator**（**QCOW2-QEMU** 模擬器）。
7. 按一下 **Create Image**（建立映像）。

STEP 5 | 上傳啟動程序檔案。檔案必須上傳至這裡說明的資料夾結構。熱度範本使用此資料夾結構來尋找啟動程序檔案。

1. 登入 OpenStack 控制器。
2. 建立下列資料夾結構：

   /root/bootstrap/config/

   /root/bootstrap/license/
3. 使用 SCP 或 FTP，將 init-cfg.txt 和 bootstrap.xml 檔案新增至 config 資料夾，並將 VM-Series 驗證碼新增至 license 資料夾。

STEP 6 | 編輯範本環境檔案來適合您的環境。確認環境檔案中的映像名稱，符合您上傳檔案時所指定的名稱。

```
參數: # VN 設定 management_network: 'mgmt_net' left_vn: 'left_net'
 right_vn: 'right_net' left_vn_fqdn: 'default-domain:admin:left_net'
 right_vn_fqdn: 'default-domain:admin:right_net'
 route_target: "target:64512:20000" # VM 設定 flavor: 'm1.small'
 left_vm_image: 'TestVM' right_vm_image: 'TestVM'
 svm_name: 'PAN_SVM_L3 left_vm_name: 'Left_VM_L3'
 right_vm_name: 'Right_VM_L3' port_tuple_name: 'port_tuple_L3'
 #ST 設定 S_Tmp_name: PAN_SVM_template_L3 S_Tmp_version: 2
 S_Tmp_service_mode: 'in-network' S_Tmp_service_type: '防火
牆' S_Tmp_image_name: 'PA-VM-8.0.0' S_Tmp_flavor: 'm1.large'
 S_Tmp_interface_type_mgmt: 'management'
 S_Tmp_interface_type_left: 'left'
 S_Tmp_interface_type_right: 'right' 網域: 'default-
domain' '# SI 設定 S_Ins_名稱: PAN_SVM_Instance_L3
 S_Ins_fq名稱: 'default-domain:admin:PAN_SVM_Instance_L3'
 #IPAM 設定 NetIPam_ip_prefix_mgmt: '172.2.0.0'
 NetIPam_ip_prefix_len_mgmt: 24 NetIPam_ip_prefix_left: '10.10.1.0'
 NetIPam_ip_prefix_len_left: 24 NetIPam_ip_prefix_right: '10.10.2.0'
 NetIPam_ip_prefix_len_right: 24 NetIPam_addr_from_start_true: true
 #原則設定 policy_name: 'PAN_SVM_policy-L3' policy_fq_name: 'default-
domain:admin:PAN_SVM_policy-L3' simple_action: 'pass'
 protocol: 'any' src_port_end: -1 src_port_start: -1 direction: '<
 >' dst_port_end: -1 dst_port_start: -1
```


©2023 Palo Alto Networks, Inc.

STEP 7 | 編輯範本檔案來指向啟動程序檔案和驗證碼。在 Personality 下，指定檔案位置的檔案路徑。將您不使用的任何一行取消註解。

```
Pan_Svm_instance 類型: OS::Nova::Server depends_on:
 [ mgmt_InstanceIp, left_InstanceIp, right_InstanceIp ] properties:
 name: {get_param: svm_name } image: { get_param:S_Tmp_image_name }
 flavor: { get_param:S_Tmp_flavor } networks: - port:
 { get_resource: mgmt_VirtualMachineInterface } -
 port: { get_resource: left_VirtualMachineInterface } -
 port: { get_resource: right_VirtualMachineInterface }
 user_data_format:RAW config_drive: true personality: /config/
init-cfg.txt: {get_file: "/root/bootstrap/config/init-cfg.txt"}
 # /config/init-cfg.txt: { get_file: "http://10.4.1.21/op_test/
config/init-cfg.txt" } /config/bootstrap.xml: {get_file: "/
root/bootstrap/config/Service_Chaining_bootstrap_L3.xml"} # /
config/bootstrap.xml: { get_file: "http://10.4.1.21/op_test/
config/Service_Chaining_bootstrap_L3.xml" } # /license/authcodes:
 {get_file: "/root/bootstrap/license/authcodes"} # /license/
authcodes: {get_file: "http://10.4.1.21/op_test/license/authcodes"}
```

STEP 8 | 上傳熱度範本檔案。

1. 登入 OpenStack 控制器。
2. 使用 SCP 或 FTP 新增熱度範本檔案和環境檔案。

STEP 9 | 部署熱度範本。

1. 執行命令 **source openrc**
2. 執行命令 **heat stack-create *<stack-name>* -f *<template>* -e ./*<env-template>***

STEP 10 | 確認 VM-Series 防火牆已成功部署。

您可以使用下列命令來檢查堆疊的建立狀態。

- 使用 **heat stack-list** 來檢查堆疊狀態
- 使用 **heat event-list** 來檢視堆疊建立期間發生之事件的詳細清單
- 使用 **heat stack-show** 來檢視堆疊的詳細資訊

STEP 11 | 確認 VM-Series 防火牆會雙向檢查 Linux 伺服器之間的流量。

1. 登入防火牆。
2. 選取 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量）可檢視 SSH 工作階段。

©2023 Palo Alto Networks, Inc.

在 Google Cloud Platform 上設定 VM-Series 防火牆

您可在 Google Cloud Platform 上的 Google Compute Engine 實例上部署 VM-Series 防火牆。

- 在 Google Cloud Platform 上受支援的部署
- 預備在 Google Cloud Platform 上設定 VM-Series 防火牆
- 在 Google Cloud Platform 上部署 VM-Series 防火牆
- 使用 GCP 專用 Panorama 外掛程式進行 VM 監控
- 在 Google Cloud Platform 上自動調整 VM-Series 防火牆規模

有關在 Google Cloud Platform 上的 VM-Series 防火牆

VM-Series 防火牆為 Google® Cloud Platform (GCP™) 帶來下一代的防火牆功能。

為使效能最大化，GCP 上的 VM-Series 防火牆支援 Data Plane Development Kit（資料平面開發套件 - DPDK）程式庫，並依據 VM-Series 防火牆授權與 Google Cloud Platform 虛擬電腦 (VM) 尺寸的特定結合，提供快速封包處理以及提升網路效能。

- Google Cloud Plaform 與 VM-Series 防火牆
- 防火牆上的 VM-Series 最低系統需求

Google Cloud Plaform 與 VM-Series 防火牆

透過整合 VM-Series 防火牆與 Google Cloud Platform (GCP)，您可以將 VM-Series 防火牆作為在 Google Compute Engine 實例上執行的虛擬電腦 (VM) 來部署。此程序在您 從 Google Cloud Platform Marketplace 部署 VM-Series 防火牆 時會簡化。

部署 VM-Series 防火牆之後，即可設定下列可選服務：

- 在 VM Series 防火牆上啟用 Google Stackdriver 監控—從防火牆，將 PAN-OS 度量推送至 Google Stackdriver 服務。
- 啟用 VM 監控以追蹤 VM 在 Google Cloud Platform 上的變動 — 設定監控包含您實例的特定 GCP 區域的 VM 資料來源。受監控的 VM 中繼資料可包含預定義的 GCP 屬性（如專案 ID） 與使用者定義的屬性（如標籤和網路標籤）。

防火牆上的 VM-Series 最低系統需求

您必須選取公共雲端專用 VM-Series 防火牆授權和授權方法：自帶授權 (BYOL) 或即付即用 (PAYG)。若要在 Google Compute Engine 實例上部署 VM-Series 防火牆，則必須針對您的授權，選取支援VM-Series 系統需求的電腦類型。

單一個 Google Compute Engine 實例可支援最多八個網路介面。若您想要設定八個介面，請選取 n1-standard-8 或更大的電腦類型。

功能	BYOL	搭售包 1 與 2	
		PAYG	Marketplace
VM-100 防火牆	✓		
VM-200 防火牆	✓		
VM-300 防火牆	✓	✓	✓
VM-1000-HV 防火牆	✓		

©2023 Palo Alto Networks, Inc.

功能	BYOL	搭售包 1 與 2	
		PAYG	Marketplace
VM-500 防火牆	✓		
VM-700 防火牆	✓		

VM-Series 防火牆支援下面列出的預先定義標準機器類型。您可以選取較高效能的電腦類型，或建立自己的自訂電腦類型，其所提供的資源需求與您的 VM-Series 防火牆授權相容。

- n1-standard-4
- n1-standard-8
- n1-standard-16
- n2-standard-4
- n2-standard-8
- n2-standard-16
- n2-standard-32

自訂機器類型：

- e2-standard-4
- e2-standard-8
- e2-standard-16
- e2-standard-32

©2023 Palo Alto Networks, Inc.

在 Google Cloud Platform 上受支援的部署

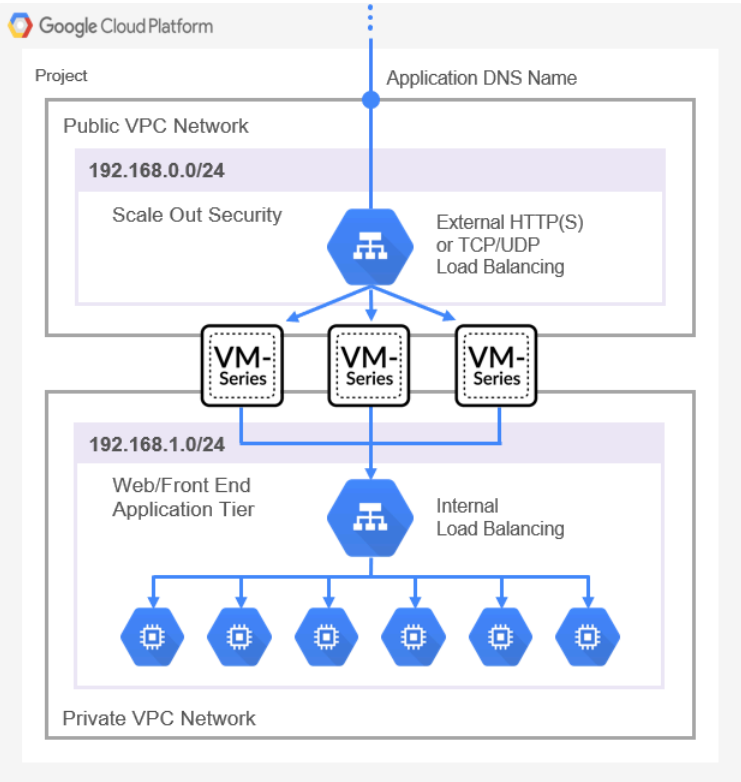
您可以在虛擬私人雲端 (VPC) 網路中的 Google® Compute Engine 實例上部署 VM-Series 防火牆。部署類型為：

- 網際網路閘道
- 區隔閘道
- 混合型 IPSec VPN

網際網路閘道

VM-Series 防火牆保護流向和來自網際網路的南/北流量，以保護應用程式遠離已知和未知的威脅。一個 Google 專案可以有最多五個 VPC 網路。有關網際網路閘道的典型範例，請參閱 Google 組態範例。

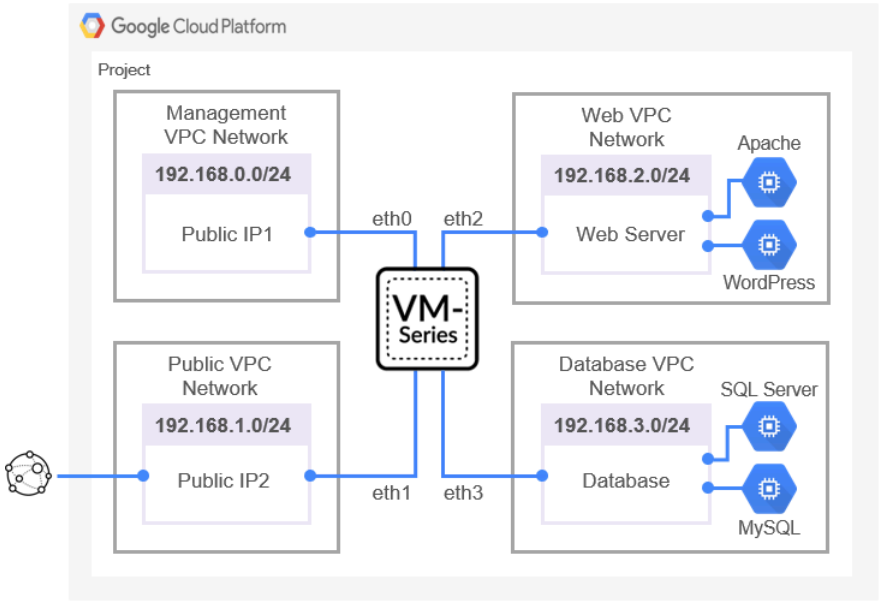
在公共雲端環境中，相較於較大、較高效能的 VM，使用放大架構更為常見（如下圖所示）。此架構（有時稱之為三明治式部署）能避免單點故障，並讓您可以在必要時新增或移除防火牆。



區隔閘道

區段閘道能保護虛擬私人雲端 (VPC) 間的東/西流量，以確保數據保護合規性與應用程式的存取。下圖顯示防火牆保護了北/南和東/西流量。

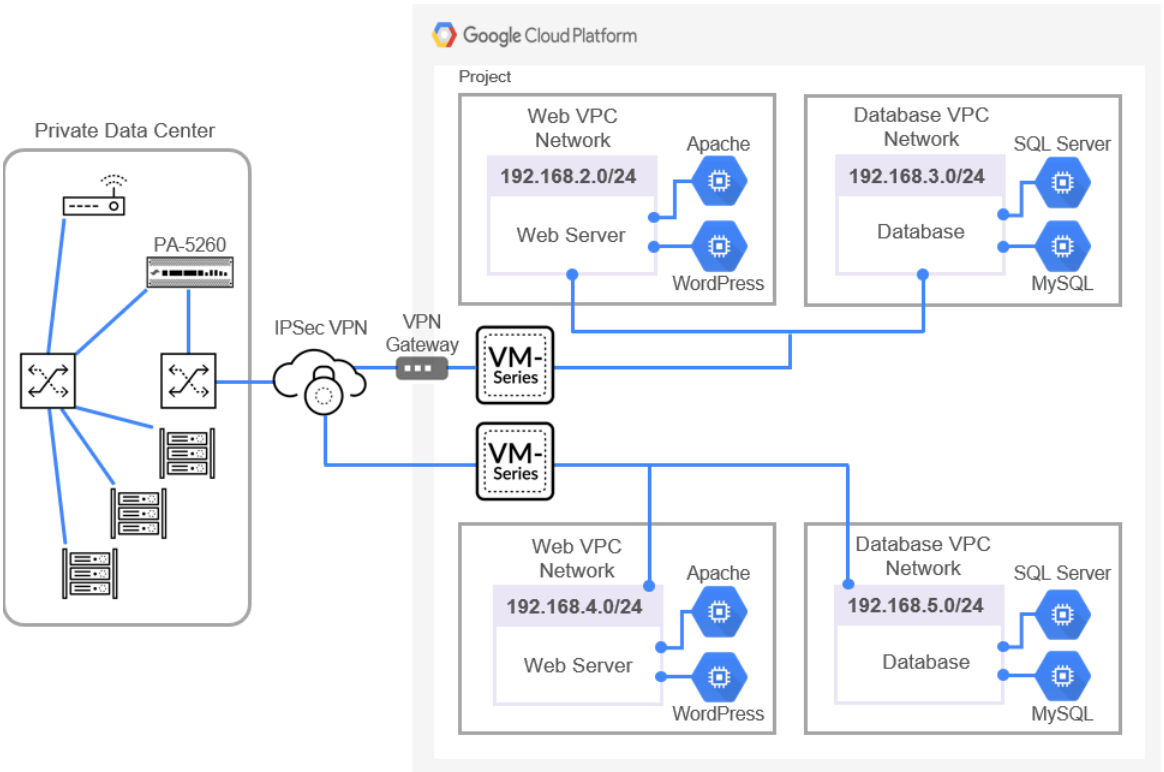
©2023 Palo Alto Networks, Inc.



混合型 IPSec VPN

VM-Series 防火牆作為 IPSec VPN 終點使用，可保護託管於 Google Cloud Platform (GCP) 上的設備其進出的通訊。

下圖中的部署顯示從內部部署網路到部署在 GCP 防火牆間的站對站 VPN，以及一個從內部部署網路到 Google Cloud VPN 閘道間的 IPSec 連線。



©2023 Palo Alto Networks, Inc.

預備在 Google Cloud Platform 上設定 VM-Series 防火牆

從 Google Cloud Platform Marketplace 部署 VM-Series 防火牆 的程序需要準備工作。

如果您使用 Google Marketplace 來部署，您必須建立專案網路和子網路，並事先為 VM-Series 防火牆介面規劃網路和 IP 位址指派。部署期間，您必須從現有的網路與子網路中進行選取。

在規您的部署時，請參閱下列主題：

- 一般需求
- 在 Panorama 上安裝 VM-Series 外挂程式
- 安裝 GCP 專用 Panorama 外掛程式
- 準備從 GCP Marketplace 部署

一般需求

此檢查清單中的元素常見於部署您直接或以 Panorama 管理的 VM-Series 防火牆。Panorama 外掛程式對某些服務有額外需求，例如 Stackdriver 監控、VM 監控、自動調整規模或保護 Kubernetes 部署。

如需公共雲端的 Panorama 外掛程式資訊，請務必查閱相容性矩陣。此版本需要下列軟體：

- **GCP** 帳戶—您必須有與電子郵件地址連結的 GCP 使用者帳戶，也必須知道該電子郵件地址的使用者名稱和密碼。
- **Google Cloud SDK**—如果尚未安裝 Google Cloud SDK（包含 Google Cloud API、gcloud 和其他命令列工具），請這麼做。您可以使用 command line interface（命令列介面 - CLI）來部署防火牆範本和其他範本。
- **GCP** 上 **VM-Series** 防火牆的 **PAN-OS**—從 Google Marketplace 所取得執行 PAN-OS 版本的 VM-Series 防火牆。
  - **VM-Series** 防火牆—必須使用來自 Google Marketplace 的 Palo Alto Networks 映像，將您想要從 Panorama 管理的 VM-Series 防火牆部署在 Google Cloud Platform。防火牆必須符合 防火牆上的 VM-Series 最低系統需求。
  - **VM-Series** 授權—您必須授權 VM-Series 防火牆來取得序號。需要序號才能將 VM-Series 防火牆新增為 Panorama 管理的裝置。如果您使用 GCP 專用 Panorama 外掛程式來部署 VM-Series 防火牆，則必須提供 BYOL 授權碼。Google Marketplace 會處理您的服務帳單，但防火牆會直接與 Palo Alto Networks 授權伺服器接觸。
  - 防火牆上的 **VM-Series** 外掛程式—執行 PAN-OS 9.0 和更新版本的 VM-Series 防火牆包含 VM-Series 外掛程式，負責管理與公共雲端和私人雲端的整合。如相容性矩陣所示，VM-Series 外掛程式有最低版本對應於每個 PAN-OS 版本。

    有主要 PAN-OS 升級時，VM-Series 外掛程式版本會自動升級。關於次要版本，由您決定是否需要 VM-Series 外掛程式升級，如果需要，請執行手動升級。請參閱 在 Panorama 上安裝 VM-Series 外挂程式。

©2023 Palo Alto Networks, Inc.

- 以管理模式執行的 **Panorama**—執行與受管理防火牆相同或更新 PAN-OS 版本的 Panorama 實體或虛擬設備。虛擬實例不需要部署在 GCP。
  - 您必須有 Panorama 授權版本。
  - Panorama 必須可從網路存取您想要管理的 VM 部署所在的 VPC。
  - 如果您想要管理 GCP 中部署的 VM，或設定自動調整規模之類的功能，則 PAN-OS 和 VM-Series 外掛程式版本，必須符合支援 GCP 專用 Panorama 外掛程式的公共雲端需求。
  - Panorama 上的 VM-Series 外掛程式。請參閱 在 Panorama 上安裝 VM-Series 外挂程式
- **GCP** 專用 **Panorama** 外掛程式版本 **2.0.0**—對於以 VM 監控或自動調整規模範本所部署的防火牆，GCP 外掛程式會管理授權、啟動和設定防火牆所需的互動。GCP 外掛程式結合 VM 監控或自動調整規模範本，使用 Panorama 範本堆疊和裝置群組以程式控制 NAT 規則，將流量導向至受管理的 VM-Series 防火牆。

  請參閱 安裝 GCP 專用 Panorama 外掛程式。

在 Panorama 上安裝 VM-Series 外挂程式

在 Panorama 上，安裝或升級到支援您想設定 GCP 功能的 VM-Series 外掛程式版本，詳述於公共雲端相容性矩陣表格。

初始安裝—因為 VM-Series 外掛程式在 Panorama 上為選項，首次安裝時，您必須從支援入口網站下載 VM-Series 外掛程式，然後前往 **Panorama** > **Device Deployment**（裝置部署） > **Plugins**（外掛程式）來上傳和安裝。

升級—前往 **Panorama** > **Device Deployment**（裝置部署） > **Plugins**（外掛程式），然後按一下 **Check Now**（立即檢查）。安裝符合公共雲端相容性矩陣表格所列需求的版本。

安裝 GCP 專用 Panorama 外掛程式

如果您想要管理以 Palo Alto Networks 範本建立的 VM 監控或自動調整規模部署，則需要 GCP 專用 Panorama 外掛程式。請安裝支援您想設定 GCP 功能的外掛程式版本，詳述於公共雲端相容性矩陣表格。

您無法將 *GCP* 專用 *Panorama* 外掛程式從版本 *1.0.0* 升級至版本 *2.0.x*。如果您已安裝版本 *1.0.0*，請先移除，再安裝 *2.0.x*。

如果您在安裝了多個外掛程式的 HA 配對中安裝了一個獨立的 Panorama 或兩個 Panorama 設備，則在未設定一或多個外掛程式的情況下，外掛程式可能不會收到更新的 IP-Tag 資訊。發生這種情況是因為 Panorama 不會將 IP-Tag 資訊轉送到未設定的外掛程式。此外，如果一或多個 Panorama 外掛程式未處於「已註冊」或「成功」狀態（每個外掛程式的正狀態不同），則可能會出現此問題。在繼續或執行下述命令之前，請確保您的外掛程式處於正狀態。

如果遇到此問題，有兩種權宜方案：

- 解除安裝未設定的外掛程式。建議您不要安裝未打算立即設定的外掛程式

©2023 Palo Alto Networks, Inc.

- 您可以使用以下命令來變通處理此問題。對每個 Panorama 實例上的每個未設定外掛程式執行以下命令，以防止 Panorama 等待傳送更新。否則，防火牆可能會遺失一些 IP-Tag 資訊。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以透過執行以下命令來取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

上述的命令在重新啟動後不會持續存在，並且必須在任何後續重新啟動時再次使用。對於 HA 配對中的 Panorama，必須在每個 Panorama 上執行命令。

STEP 1 | 驗證 Panorama 安裝。

在 Panorama 上，確保 PAN-OS 版本符合支援 GCP 自動調整規模的需求。

STEP 2 | 移除 GCP 專用 Panorama 外掛程式 1.0 版。

如果您已安裝 Panorama 外掛程式 1.0 版，則必須移除。

STEP 3 | 安裝 GCP 專用 Panorama 外掛程式。

選取 **Panorama** > **Plugins**（外掛程式），然後在搜尋列輸入 **gcp**。**Install**（安裝）支援您想設定功能的外掛程式版本（請參閱公共雲端相容性矩陣表格）。

安裝之後，您可以在 Panorama 儀表板 **General Information**（一般資訊）清單中看到外掛程式。檢視 **Panorama** > **Google Cloud Platform**，您會看到 **Setup**（設定）、**Monitoring Definition**（監控定義）和 **AutoScaling**（自動調整規模）介面。

STEP 4 | （選用）如果您的 Panorama 設備位於 high availability（高可用性 - HA）設定中，您必須在兩個 Panorama 端點上手動安裝相同版本的 Google 外掛程式。

只在主動 *Panorama* 對等上設定 *Google* 外掛程式。提交時，設定會同步至被動 *Panorama* 對等。只有主動 *Panorama* 對等會輪詢您設定為 *VM* 監控的 *Google VM*。

準備從 GCP Marketplace 部署

使用 Google Marketplace 在 Google Compute Engine (GCE) 實例上部署防火牆之前，請檢閱這些需求，以確保您有適當的帳戶和權限。

- 一般帳戶與權限
- 可用的 Google 資源
- Google 驗證方法
- SSH 金鑰配對

©2023 Palo Alto Networks, Inc.

一般帳戶與權限

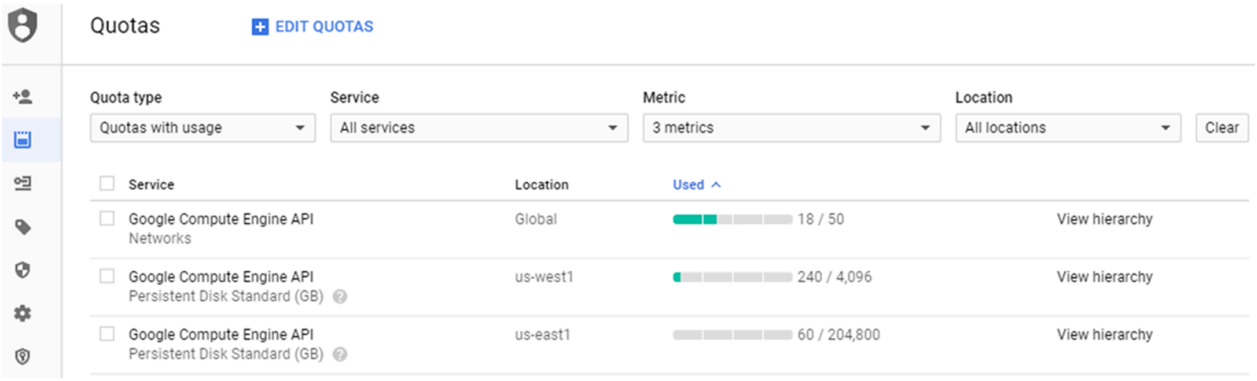
- 您和您允許的任何使用者都必須擁有下列最低權限的角色或等效的 Identity and Access Management (IAM) 權限才能連線至 VM-Series 防火牆：
  - **Compute** 檢視者—Compute 檢視者可讓您取得和列出計算引擎資源，但無法讀取儲存在這些資源上的資料。
  - **Storage Object Viewer**—讓您能夠在同一專案中使用 Google 貯體進行引導。

  > 您組織中的使用者可能具有 IAM 權限或比權限所需更寬鬆的預定義角色。請確保適當地限制 *VM-Series* 防火牆存取。

  您也可以限制服務帳戶的存取，如Google 驗證方法所述。
- 監控度量寫入器 — Stackdriver 要求。

可用的 Google 資源

您的專案必須有足夠的資源部署 VM-Series 防火牆作為 Google Compute 實例。若您正部署 GCP Marketplace 解決方案，請確定此解決方案除防火牆外，是否部署了其他 VM。在 Google Cloud Console 中，選取 **IAM & admin**（**IAM** 與管理員） > **Quotas**（配額），以檢閱專案的資源配額及耗用的網路和磁碟空間。如果您的資源即將用完，可要求 Google 為您的組織配置更多資源。



Google 驗證方法

GCP 支援採用多種方式連線至實例。您可使用服務帳戶或 SSH 金鑰配對進行驗證。

1. 服務帳戶—服務帳戶適用於應用程式或 VM，不適用於一般使用者。它們通常在您使用程式或指令碼，或存取自 gcloud 命令行存取防火牆時，作為控制存取使用。若您正使用 Google 服務

©2023 Palo Alto Networks, Inc.

帳戶 以驗證實例或應用程式，您必須知道該帳戶的電子郵件。請參閱建立並管理服務帳戶金鑰。

如果您想要從專案外部連線至 VM-Series 防火牆（從不同專案或從命令列），則必須使用服務帳戶。例如，如果您想要啟用實體下一代防火牆以監控 VM-Series 防火牆，則必須儲存 VM-Series 防火牆服務帳戶資訊至 JSON 檔案。在實體防火牆中，您可在設定連線時上載檔案。

1. 選取 **IAM & Admin**（**IAM** 與管理員） > **Service accounts**（服務帳戶），然後選擇 **+Create Service Account**（**+** 建立服務帳戶）。

   輸入服務帳戶名稱和說明，然後按一下 **Create**（建立）。
2. 從下拉式功能表中選取角色類型，然後在右側選取適當的存取層級。

   例如，選取 [Project（專案）] > [Editor（編輯者）]。您可以選取多個角色給一個服務帳戶。完成時按一下 **Continue**（繼續）。
3. 授與權限讓特定使用者存取此服務帳戶。從右側的 **Permissions**（權限）欄選取成員，給他們權限來存取上一步中的角色。

2. **SSH** 金鑰—如果您從 Marketplace 部署 VM-Series 防火牆，則必須為 Google Compute Engine 實例中繼資料以 RSA 格式提供一個 Open SSH 金鑰。

   VM-Series 防火牆在部署時僅接受一個金鑰。

   在部署時，請將公共金鑰貼至 Marketplace 部署，如SSH 金鑰配對所述。部署之後，您可在防火牆中使用 SSH 私密金鑰以設定管理員帳戶。若要新增使用者，請參閱管理防火牆管理員。

您有幾種驗證方式：

- 為實例建立服務帳戶—您可以為特定實例或實例群組建立服務帳戶，並授與特定權限，以進而授與使用者。
- 對您的專案使用預設服務帳戶—如果您使用 Google Cloud Platform (GCP™) 主控台，然後以電子郵件地址登入，則可以根據專案管理員為您的帳戶指派的任何權限或角色，以存取 GCE 實例。

  使用 Google Cloud Console 或 gcloud 命令行工具建立的每個 Google Compute Engine 實例都有一個預設服務帳戶，其名稱採用電子郵件地址格式：

  <project-number>

  `-compute@developer.gserviceaccount.com`

  若要查看防火牆實例的服務帳號名稱，請查看實例詳細資訊並滾動到底部（參閱 Compute Engine 預設服務帳號）。

  對於 VM-Series 防火牆所在相同專案中的 VM，預設服務帳戶可以管理對這些 VM 的驗證。存取範圍可讓防火牆對 Google Cloud 專案中的 VM 起始 API 呼叫。
- 使用 **IAM** 權限與 **Google API**—若您使用 Google SDK API 與 gcloud ，則您必須呼叫 API 進行驗證。
  - 當您自命令行管理防火牆，或執行指令碼設定防火牆時，通常使用 Google SDK。
  - 如果您連接的虛擬電腦有一個自訂映像含有需要 Google API 的應用程式，則您需要存取 Google API。

 ©2023 Palo Alto Networks, Inc.

SSH 金鑰配對

當您從 Google Marketplace 部署 VM-Series 防火牆時，您需要 SSH 金鑰配對，才能向 VM-Series 防火牆驗證。

根據您的金鑰產生器文件建立金鑰配對。請勿編輯公共金鑰檔案。編輯具有引入非法字元的風險。

VM-Series 防火牆管理驗證的方式與 GCE 實例不同。部署之後，請先以 **admin** 使用者登入。只會接受一次 VM-series 防火牆預設使用者名稱。成功登入後，請為 VM-Series 網頁介面設定管理員使用者名稱和密碼（請參閱從 Google Cloud Platform Marketplace 部署 VM-Series 防火牆）。

Google Marketplace 部署介面 **SSH key**（**SSH** 金鑰）欄位顯示下列預留位置：

admin:ssh-rsa your-SSH-key

admin 是首次登入防火牆所需的 VM-Series 防火牆管理員使用者名稱。當您從 Google Cloud Platform Marketplace 部署 VM-Series 防火牆時，請將 **admin:** 首碼新增至該 Marketplace 欄位。

當您將金鑰貼至 Marketplace **SSH** 金鑰欄位時，如果您未提供完整的公共金鑰，或金鑰包含非法字元，您將無法登入 VM-Series 防火牆。當您第一次在 VM-Series 防火牆中使用 SSH 時，公共金鑰將傳輸至防火牆。

如果公共金鑰損壞，您必須刪除部署並重新開始。任何網路和子網路都繼續存在，但必須重新建立防火牆規則。

STEP 1 | 建立 SSH 金鑰配對並將該 SSH 金鑰配對儲存於找到 SSH 金鑰中提到的作業系統的預設位置。

- **Linux** 或 **MacOS**—使用 `ssh-keygen` 在 .ssh 目錄中建立金鑰配對。
- **Windows**—使用 PuTTYgen 建立金鑰配對。

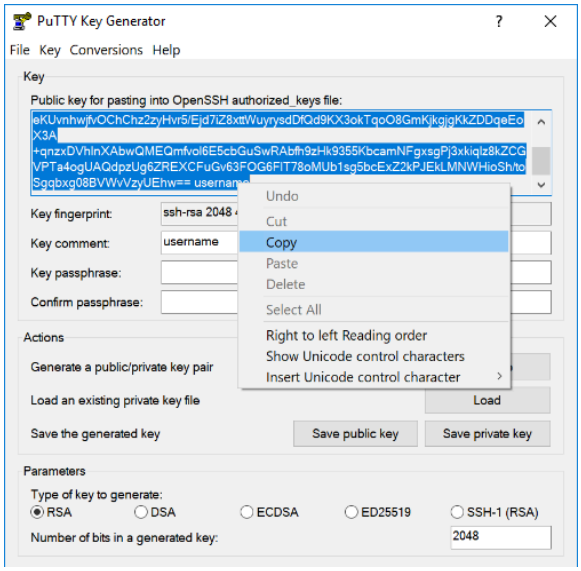
  Key comment（金鑰註解）欄位的內容不影響 VM-Series 防火牆；您可以接受預設值（金鑰建立日期）或輸入有助於您記住金鑰配對名稱的註解。使用 **Save private key**（儲存私密金鑰）按鈕在 .ssh 目錄中儲存私密金鑰。

©2023 Palo Alto Networks, Inc.

STEP 2 | 選取完整的公共金鑰。

- **Linux** 或 **MacOS**—在文字編輯器中開啟您的公共金鑰並複製該公共金鑰。
- **Windows**—您必須使用 PuTTY 金鑰產生器來檢視公共金鑰。啟動 PuTTYgen，按一下 **Load**（載入），並瀏覽至儲存於 .ssh 目錄中的私密金鑰。

  在 PuTTYgen 中，向下捲動以確保選取整個金鑰，按一下滑鼠右鍵，並選取「複製」。



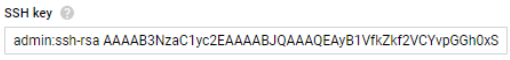
STEP 3 | 在 [SSH key（SSH 金鑰）] 欄位中輸入公共金鑰，詳述如下。

1. 在 Marketplace **SSH** 金鑰欄位中，刪除預留位置文字，並鍵入：

   admin:

   請確保冒號後面沒有多餘的空格。

2. 在 **admin:** 之後插入游標並選取 **Paste as plain text**（貼為純文字）。金鑰必須自成一行，如下所示。

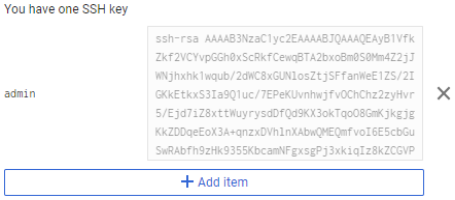
3. 將游標移至金鑰結尾，加上空格，然後輸入： **admin**

   SSH key（**SSH** 金鑰）欄位的最終內容必須為：

   admin:ssh-rsa [KEY] **admin**

STEP 4 | 檢查金鑰。

部署之後，在嘗試登入防火牆之前，請檢視管理實例，檢查金鑰是否有換行字元或多餘空格：



如果金鑰完全在一行上，且格式為 **admin:ssh-rsa** [KEY] **admin**，即表示您已完成。

©2023 Palo Alto Networks, Inc.

STEP 5 | （選用）如果出問題，則您必須更換金鑰。

1. 按一下 **X** 以刪除金鑰，然後按一下 **+ Add item**（**+** 新增項目）。
2. 輸入步驟 3 所述的金鑰。現在，**SSH key**（**SSH** 金鑰）欄位必須顯示：

   admin:ssh-rsa [KEY] **admin**
3. 按一下 **Save**（儲存）以部署更新的部署。
4. 重新檢查金鑰。

虛擬私人雲端 (VPC) 網路規劃

從 Google Market 部署之前，請規劃 VPC 網路（稱為網路）、子網路（也稱為子網）及 Google 防火牆規則。開始從 Google Cloud Platform Marketplace 部署 VM-Series 防火牆之前，您必須建立網路和子網路。

Marketplace 部署頁面僅顯示當您開始部署時存在的網路與子網路。如果網路連線中斷，您必須退出部署，建立網路，並重新開始。

- **VPC** 網路—您必須特別為每個 VM-Series 防火牆網路介面建立自訂網路。
  - 請參閱公共雲端專用 VM-Series 防火牆授權以依據 VM-Series 防火牆授權，決定所需網路介面的數量。最少需要設定三個 VPC 網路與子網路，以啟動 VM-Series 防火牆。
  - GCP 專案有使用預設組態與防火牆規則的預設網路；若未使用，您可刪除此預設網路。
  - 依預設，一個專案中最多有五個網路。您的 GCP 管理員可為您的專案請求額外的網路。
  - 若要連線至管理介面，您必須建立允許存取的 GCP 防火牆規則。如果您選取 **Enable GCP Firewall rule for connections to Management interface**（啟用管理介面連線的 **GCP** 防火牆規則），便可在部署期間執行此操作，然後為 **Source IP in GCP Firewall rule for connections to Management Interface**（管理介面連線的 **GCP** 防火牆規則中的來源 **IP**）提供 CIDR 區塊。

    確定您的網路包含您想要保護的所有實例。
- 子網路—一個計算引擎實例在單一介面上可支援最多八個 Layer 3 介面。管理、信任和不受信任的介面使用三個介面，且您最多可建立五個額外資料平面介面。資料平面介面通常表示應用程式網路。
- **IP** 位址—您在建立介面子網路時提供 IP 位址範圍，而在部署子網路時，您可以選擇啟用外部位址。
  - 當您建立網路子網路時，必須指定 IP 位址範圍。此範圍用於您的內部網路，因此不能與其他子網路重疊。
  - 於部署期間，在建立網路介面時，您可以選取啟用外部位址。依預設，您將收到一個暫時 IP 位址。您在部署期間無法提供保留的靜態 IP 位址，但可在部署程序完成時將暫時位址提升為靜態 IP 位址（請參閱提升暫時外部 IP 位址）。

©2023 Palo Alto Networks, Inc.

網路介面規劃

當您自 Google Cloud Platform Marketplace 部署時，預設的 VM-Series 防火牆部署會有三個介面：管理平面介面和不信任的與信任的資料平面介面。您可以依據您 VM 上可用的計算資源，來定義額外的資料平面實例；請參閱公共雲端專用 VM-Series 防火牆授權。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

部署期間，您能夠為這些介面命名。

介面次序

在您使用 Marketplace 部署時，網路介面的次序已預先定義完成。管理介面對應至 eth0、不受信任的介面對應至 eth1 以及受信任的介面對應至 eth2。Marketplace 會使用該次序，因為對應管理介面至 eth0 和不受信任的介面至 eth1 可確保您若因為負載平衡需要交換管理介面時可成功交換。

管理介面

您所新增的第一個網路介面對應至防火牆上的 eth0，且包含啟用 IP 轉送的可用選項。您可使用此網路介面來管理 VM-Series 防火牆。此介面通常有外部 IP 位址。

若資料平面介面附加至公開子網路，則只需要外部 ***IP***。在建立時，您可以收到一個暫時 ***IP*** 位址，然後在完成部署後將其提升為靜態 ***IP*** 位址（請參閱提升暫時外部 IP 位址）。

資料平面介面（不受信任的、受信任的）

在您從 Marketplace 部署時，您新增的網路介面順序已事先決定。

- 在管理介面後設定不受信任的介面。該次序表示不受信任的介面已對應至 eth1。不受信任的介面通常會附加至公共子網路，且有外部 IP 位址。

  若資料平面介面附加至公開子網路，則只需要外部 ***IP***。在建立時，您可以收到一個暫時 ***IP*** 位址，然後將其提升為靜態 ***IP*** 位址，如提升暫時外部 IP 位址中所述。
- 受信任的介面遵照不受信任的介面，並對應至 eth2。受信任的網路通常沒有外部 IP 位址。您可在信任的介面之後新增任何額外的資料平面介面。

其他資料平面介面

為您必須保護的應用程式規劃介面，如 Web 伺服器、資料庫及網路中的其他應用程式。除了啟動防火牆所需的三個介面外，您最多可建立五個額外的資料平面介面。請確保您想要保護的應用程式在連線至 VM-Series 防火牆的網路中。

©2023 Palo Alto Networks, Inc.

在 Google Cloud Platform 上部署 VM-Series 防火牆

若要使用 GCP 市集範本來部署 VM-Series 防火牆，您必須先針對防火牆上的每個介面建立 VPC 網路。從 Google Marketplace 部署防火牆之後，您可以登入防火牆來調整設定，以便在您的 GCP VPC 設定內起作用。您也可以啟用監控來收集度量，讓您改善資源管理，或建立安全性政策規則，以自動隨著應用程式環境的變化而調整。

- 從 Google Cloud Platform Marketplace 部署 VM-Series 防火牆
- 管理 Google Cloud Platform 負載平衡的介面交換
- 使用 VM-Series 防火牆 CLI 來交換管理介面
- 啟用在 VM Series 防火牆上的 Google Stackdriver 監控
- 啟用 VM 監控以追蹤在 Google Cloud Platform (GCP) 上的 VM 變更
- 使用動態位址群組保護 VPC 中的實例
- 使用自訂範本或 gcloud CLI 部署 VM-Series 防火牆

從 Google Cloud Platform Marketplace 部署 VM-Series 防火牆

您可以使用 Google® Cloud Platform Marketplace，依固定 vCPU 容量授權來部署 VM-Series 防火牆（VM-Series 型號）。可從公共雲端取得的授權映像如下：

- VM-Series 新世代防火牆搭售包 1
- VM-Series 新世代防火牆搭售包 2
- VM-Series 新世代防火牆 (BYOL)

如需這些授權選項的詳細資訊，請參閱從 Google Cloud Platform Marketplace 部署 VM-Series 防火牆。

Marketplace 使用最低一個管理介面和兩個資料平面介面（信任和不受信任）部署一個 VM-Series 防火牆實例。您可以在虛擬私人雲端 (VPC) 中為多達五個 Google Compute Engine 實例新增額外的資料平面介面。

部署 VM-Series 防火牆之前，必須在您的組織中建立或選取一項專案，然後建立任何將與防火牆連接的網路與子網路，如 VPC 網路規劃與網路介面規劃中所述。

您不能在相同的 VPC 網路上附加多個網路介面。您建立的每個介面必須包含具有至少一個子網路的專屬網路。確定您的網路包含任何您建立的額外資料平面實例。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 選擇啟動方法.

©2023 Palo Alto Networks, Inc.

STEP 2 | 找出在 Marketplace 中所列出的 VM-Series 防火牆。

1. 登入 Google Cloud 主控台。
2. 從產品與服務功能表中，選取 **Marketplace**。
3. 搜尋 **VM-Series**。
4. 選取 VM-Series 防火牆授權選項中的一個選項。

STEP 3 | 按一下 **Launch on Compute Engine**（在計算引擎上啟動）。

STEP 4 | 為此實例命名並選取資源。

1. 輸入**Deployment Name**（部署名稱）（此名稱會顯示在部署管理員中）。此名稱必須為唯一，且不能與其他在此專案中的部署相衝突。
2. 選取 **Zone**（區域）。如需支援的區域清單，請參閱地區與區域。
3. 依據您授權的VM-Series 系統需求和 Google Cloud Platform 上 VM-Series 的最低系統需求選取 **Machine Type**（電腦類型）。

STEP 5 | 指定實例中繼資料。

選項 **Bootstrap Bucket**（啟動程序貯體）和 **Interface Swap**（介面交換）影響 VM-Series 防火牆首次啟動時的初始組態。

1. **Bootstrap Bucket**（啟動程序貯體）（選用）—如果您打算使用啟動程序檔案，請輸入儲存貯體的名稱，或儲存貯體內的資料夾路徑，其中包含啟動套件。您需要權限才能存取儲存貯體。例如：

   vmseries-bootstrap-gce-storagebucket=<bucketname>

   或

   vmseries-bootstrap-gce-storagebucket=<bucketname/directoryname>

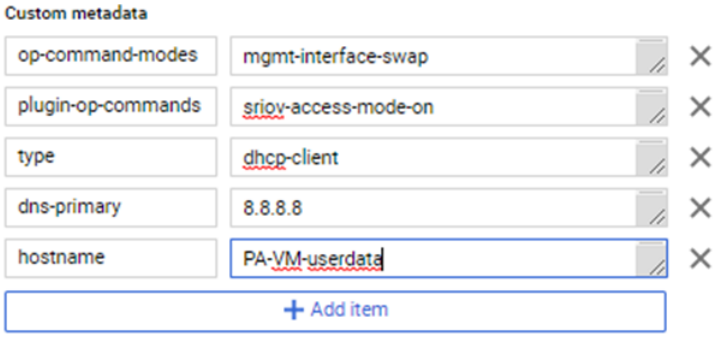
   如果您選擇以自訂中繼資料來啟動，請繼續步驟 6。
2. **Interface Swap**（介面交換）（選用）—部署時交換管理介面 (eth0) 與第一個資料平面介面 (eth1)。只有在將 VM-Series 防火牆部署在 Goolge Cloud Platform HTTP 負載平衡時才需要進行介面交換。如需詳細資訊，請參閱管理 Google Cloud Platform 負載平衡的介面交換。
3. **SSH key**（**SSH** 金鑰）—從 SSH 金鑰配對貼至公共金鑰內。依照SSH 金鑰配對中針對您的作業系統的指示建立、複製並貼上金鑰。Windows 使用者必須在 PuTTY 中檢視金鑰、從使用者介面複製，並貼至 Marketplace 部署。

   如果金鑰格式不正確，*VM-Series* 防火牆將不允許您登入。您必須刪除部署並重新開始。
4. 按一下 **More**（更多）以顯示其他中繼資料選項。選項 **blockProjectKeys** 與 **enableSerialConsole** 為實例的屬性；您可在成功部署後變更這些中繼資料值。
   - **blockProjectKeys**（選用）—如果封鎖專案金鑰，則僅可使用您提供的公共 SSH 金鑰來存取實例。
   - **enableSerialConsole**（選用）—與序列主控台互動讓您可以監控實例建立並執行互動式除錯工作。

©2023 Palo Alto Networks, Inc.

STEP 6 | 指定自訂中繼資料。

如果您選擇以自訂中繼資料來啟動，請新增您在步驟 5 中未新增的任何鍵值組。關於鍵值組清單，請參閱init-cfg.txt 檔案元件。例如：



STEP 7 | 設定開機磁碟。

1. **Boot disk type**（開機磁碟類型）—從 SSD 永久磁碟或標準永久磁碟中選取。請參閱儲存選項。
2. 輸入 **Boot disk size**（開機磁碟大小）—最小為 60GB。您可以稍後再編輯磁碟大小，但必須停止 VM 這麼做。

STEP 8 | 設定管理介面。

1. **Management VPC Network name**（管理 **VPC** 網路名稱）—選取現有網路
2. **Management Subnet name**（管理子網路名稱）—選取現有子網路。
3. **Enable External IP for Management interface**（啟用管理介面的外部 **IP**）（選用）—如果您啟用此選項，即可使用指派給 VM-Series 防火牆管理介面的 IP 位址，使用 SSH 存取 VM-Series 防火牆網路介面。
4. **Enable GCP Firewall rule for connections to Management interface**（啟用管理介面連線的 **GCP** 防火牆規則）（選用）—此選項可自動為您提供的外部來源 IP 位址建立 GCP 防火牆允許規則。
5. **Source IP in GCP Firewall rule for connections to Management Interface**（管理介面連線的 **GCP** 防火牆規則中的來源 **IP**）—如果您 **Enable GCP Firewall rule for connections to Management interface**（啟用管理介面連線的 **GCP** 防火牆規則），請輸入來源 IP 位址或 CIDR 區塊。
   - 請勿使用 0.0.0.0/0.請提供對應於您的專用管理 IP 位址或網路的 IP 位址或 CIDR 區塊。請勿讓來源網路範圍過大。
   - 請驗證位址以確保不會封鎖您自己。

STEP 9 | 設定不受信任的資料平面介面。

1. **Untrust VPC Network name**（不受信任的 **VPC** 網路名稱）—選取現有網路。
2. **Untrust Subnet name**（不受信任的子網路名稱）—選取現有子網路。
3. **Enable External IP for Untrust**（啟用不受信任的外部 **IP**）—啟用 GCP 以提供暫時 IP 位址，作為外部 IP 位址。

©2023 Palo Alto Networks, Inc.

STEP 10 | 設定受信任的資料平面介面。

1. **Trust VPC Network name**（信任的 **VPC** 網路名稱）—選取現有網路。
2. **Trust Subnet name**（信任的子網路名稱）—選取現有子網路。
3. **Enable External IP for Trust**（啟用信任的外部 **IP**）—啟用 GCP，以提供暫時 IP 位址作為外部 IP 位址。

STEP 11 | 設定額外的介面。您必須輸入要新增的資料平面介面數量；預設值為 0（無）。部署頁面總是顯示編號為 4 至 8 的額外五個資料平面的欄位。

1. **Additional Dataplane interfaces**（額外的資料平面介面）—輸入額外的資料平面實例數。

   如果此數為 *0*（預設），即便您填寫了介面欄位，編號為 *4* 至 *8* 的資料平面也會被忽略。例如，如果您指定 *2*，然後填寫三個介面的資訊，則只會建立前兩個。

2. **Additional Dataplane # VPC name**（額外的資料平面 **#** 子網路名稱）—選取現有網路。
3. **Dataplane # Subnet name**（資料平面 **#** 子網路名稱）—選擇存在的子網路。
4. **Enable External IP for dataplane # interface**（啟用資料平面 **#** 介面的外部 **IP**）—啟用 GCP 以提供暫時 IP 位址，作為外部 IP 位址。

STEP 12 | **Deploy**（部署）實例。

STEP 13 | 使用 Google 雲端部署管理員檢視並管理您的部署。

STEP 14 | 使用 CLI 以變更防火牆上的管理員密碼。

1. 從命令行登入 VM-Series 防火牆。在您的 SSH 工具中，連線至管理介面的外部 IP，並指定私密金鑰的路徑。

   Windows 使用者：使用 PuTTY 連線至 VM-Series 防火牆並發出命令行指示。若要指定私人金鑰的路徑，請選取 **Connection**（連線） > **SSH** > **Auth**（驗證）。在 **Private key file for authentication**（用於驗證的私密金鑰檔案）：按一下 **Browse**（瀏覽）以選取您的私密金鑰。

2. 進入組態模式：

   ```
   VMfirewall> configure
   ```

3. 輸入下列命令：

   ```
   VMfirewall# set mgt-config users admin password
   ```

4. 輸入管理員的新密碼並確認。
5. 提交您的新密碼：

   ```
   VMfirewall# 提交
   ```

6. 回到命令模式：

   ```
   VMfirewall# exit
   ```

7. （選用）如果您使用啟動程序檔案進行介面交換，可使用下列命令檢視介面對應：

   ```
   VMfirewall> debug show vm-series interfaces all
   ```


©2023 Palo Alto Networks, Inc.

STEP 15 | 存取 VM-Series 防火牆 Web 介面。

1. 在瀏覽器中，建立一個安全 (https) 連線到管理介面的 IP 位址。

   如果發生網路錯誤，請檢查您是否有允許建立此連線的 GCP 防火牆規則。
2. 提示時，輸入使用者名稱（管理員）以及您從 CLI 指定的管理員密碼。
3. （選用）如果已啟動，則驗證啟動程序完成。

   若您看到問題，可搜尋在 VM-Series 防火牆上的日誌資料。選擇 **Monitor**（監控）> **System**（系統），然後在手動搜尋欄位中，輸入 **`description contains 'bootstrap'`**，並在結果中尋找表示啟動成功的訊息。

在登入防火牆後，您可以新增管理員並建立介面、區域、NAT 規則與原則規則，如同實體防火牆一樣。

管理 Google Cloud Platform 負載平衡的介面交換

由於內部負載平衡只能將流量傳送至下一個躍點負載平衡 Google Compute Engine 實例的主要介面，VM-Series 防火牆必須能夠將 eth0 用於資料平面流量。

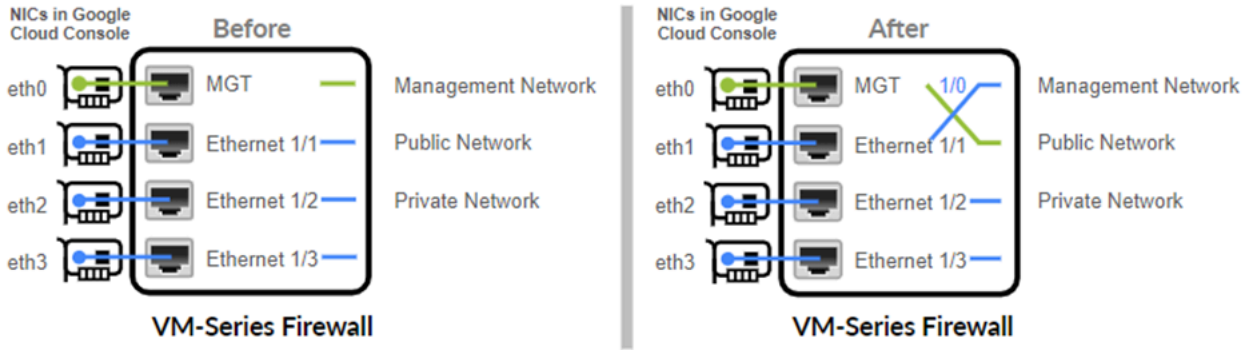
All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

若 VM-Series 防火牆位於 Google Cloud Platform 內部負載平衡介面之後，即可收到 eth0 上的資料平面流量。

- VM 系列防火牆對直接傳出至網際網路的流量提供保護，而無需使用 VPN 連結或 Direct Connect 連結返回公司網路。
- 每個防火牆只有一個後端伺服器時，例如 Web 伺服器，VM-Series 防火牆會對網際網路型應用程式提供保護。VM-Series 防火牆及 Web 伺服器可線性擴充、成對，以及部署在 Google 內部負載平衡位址之後。

為使防火牆傳送及接收 eth0 而非 eth1 上的資料流量，您必須在防火牆內交換內部負載平衡網路介面的對應，故 eth0 會對應至乙太網路 1/1，而 eth1 會對應至防火牆上的 MGT 介面。

若可行，請交換管理介面對應，然後再設定防火牆並定義原則規則。



交換介面的對應方式可讓 Google Cloud Platform 將流量散佈及路由至 VM 系列防火牆（位於相同或不同區域）上的健康實例。

©2023 Palo Alto Networks, Inc.

交換管理介面

您可以在…時交換介面，也可以在建立防火牆之後設定防火牆。

建立時— 當您部署 VM-Series 防火牆時，可使用兩種方法啟用介面交換。

- Google Cloud 主控台 — 在建立實例表中，在 **Metadata**（中繼資料）欄位中輸入金鑰值配對，其中 **mgmt-interface-swap** 為金鑰，而 **enable** 為值。
- 啟動檔案 — 建立包含啟動程序組態內 **mgmt-interface-swap** 操作命令的啟動檔案，如在 Google Cloud Platform 上啟動 VM-Series 防火牆中所述。在建立實例表中，在 **Metadata**（中繼資料）欄位中輸入金鑰值配對，以啟用啟動選項。

From the VM-Series firewall（來自 **VM-Series** 防火牆） - 登入防火牆並使用 VM-Series 防火牆 CLI 來交換管理介面。在操作模式中，簽發下列命令：

```
set system setting mgmt-interface-swap enable yes
```

- 選取指定介面交換設定的方法 - 啟動程序組態檔案、防火牆 *CLI* 或 *Google Compute Engine* 實例 ***Metadata***（中繼資料）欄位（在 *Google Cloud* 主控台上存取）。採用一種方法來確保防火牆上可預測的行為。

  無法從 *Google Cloud* 主控台確定您是否已交換 *eth0* 和 *eth1*。交換後，必須記得負載平衡是位於 *eth0* 上，且防火牆管理介面為 *eth1*，以便能適當地設定 *Google Cloud Platform* 負載平衡，並建立安全性政策規則，以保護一或多個 *VM-Series* 防火牆上的負載平衡。
- 如果您在交換前已設定 *VM-Series* 防火牆，檢查 *eth0* 及 *eth1* 的任何 *IP* 位址變更是否會影響原則規則。

使用 VM-Series 防火牆 CLI 來交換管理介面

此工作僅在您的架構將 *VM-Series* 防火牆放置於 *Google Cloud Platform* 內部負載平衡器後時才需要進行。

部署防火牆時，如果您沒有使用資料平面介面來指定要交換管理介面 (MGT) 的中繼資料，則可使用 CLI 來啟用防火牆，以在主要介面上接收資料平面流量。

STEP 1 | 從 Google Cloud Platform Marketplace 部署 VM-Series 防火牆.

繼續前，確認防火牆最少配備兩個網路介面（*eth0* 與 *eth1*）。如果啟動只配備一個介面的防火牆，介面交換命令會導致防火牆啟動維護模式。

STEP 2 | 在 Google Cloud 主控台上，檢視 VM 實例詳細內容以確認 eth1 介面的網路介面 IP 位址，並確定任何安全性規則都允許連線（HTTPS 和 SSH）至新的管理介面 (eth 1)。

STEP 3 | 登入 VM-Series 防火牆 CLI 並輸入下列命令：

```
set system setting mgmt-interface-swap enable yes
```

您可以從命令行介面檢視預設的對應。輸出與下列內容相似：

©2023 Palo Alto Networks, Inc.

```
> debug show vm-series interfaces all Interface_name Base-
OS_port   mgt              eth0   Ethernet1/1      eth1
   Ethernet1/2      eth2
```

STEP 4 | 確認您要交換介面（將 eth1 資料平面介面用作管理介面）。

STEP 5 | 重新啟動防火牆以使交換生效：

```
request restart system
```

STEP 6 | 確認介面已交換：

```
debug show vm-series interfaces all
```

啟用在 VM Series 防火牆上的 Google Stackdriver 監控

Google® Compute Engine 實例上的 VM-Series 防火牆可將自訂 PAN-OS 度量發佈至 Google Stackdriver。這些度量讓您可評估效能與使用模式，讓您可以據此管理防火牆資源。

- Google Stackdriver 權限
- 啟用 Google Stackdriver

Google Stackdriver 權限

視乎您是使用預設服務帳戶驗證，還是需要用 Google API 驗證，驗證需求可能有所差異。

您可以使用兩種方式驗證：

- 使用 **VM-Series** 防火牆實例的預設服務帳戶—如果您使用的是 Google Cloud Platform (GCP™) 主控台，則可使用電子郵件地址登入，並可根據專案管理員指派給帳戶的權限或角色存取實例。
- 使用 **IAM** 權限與 **Google API**—若您使用 Google SDK API 與 gcloud ，則您必須呼叫 API 進行驗證。當您自命令行管理防火牆，或執行指令碼設定防火牆時，通常使用 Google SDK。

透過 Google Cloud 主控台或 gcloud 命令行工具建立的每個 Google Compute Engine 實例，均有一個名稱為電子郵件地址格式的預設服務帳戶：

```
<project-number>-compute@developer.gserviceaccount.com
```

若要檢視防火牆實例的服務帳戶名稱，請檢視實例詳細資料並向下捲動至底部（請參閱 Compute Engine 預設服務帳戶）。

預設服務帳戶可以管理驗證，如同 VM-Series 防火牆一般監控相同專案內的 VM。

- 存取範圍讓防火牆能夠初始化 API 呼叫以監控 Google Cloud 專案中的 VM。
- 除非監控的虛擬電腦中有需要使用 Google API 設備的自訂映像，否則您不需要存取 Google API。

若您想要自實體防火牆或在不同專案內的 VM-Series 防火牆設定監控，則必須使用 Google API 驗證。有兩個必備條件：

©2023 Palo Alto Networks, Inc.

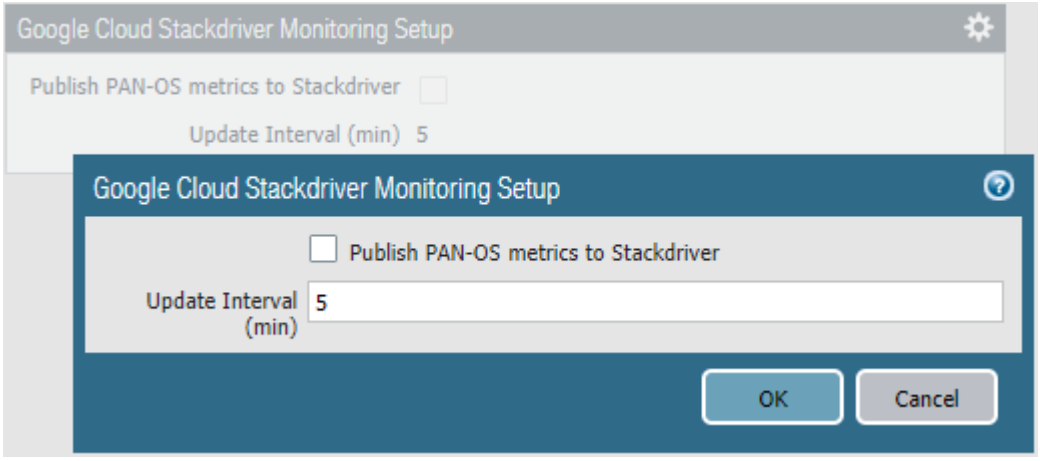
- 必須安裝 Google API。
- 您的帳戶必須具有監控度量寫入器和 Stackdriver 帳戶檢視器的角色。

啟用 Google Stackdriver

若需一份您可發佈至 Google Stackdriver 的 PAN-OS 度量相關說明，請參閱發佈自訂 PAN-OS 度量以作為監控使用。

STEP 1 | 從 Google Compute Engine 實例上的 VM-Series 防火牆推送 PAN-OS 度量至 Stackdriver。

1. 登入 VM-Series 防火牆的網頁介面。
2. 選取 **Device**（裝置） > **VM-Series**。在 Google Cloud Stackdriver 監控設定下，按一下 **Edit**（ ）。
   1. 查看 **Publish PAN-OS metrics to Stackdriver**（將 **PAN-OS** 度量推送至 **Stackdriver**）



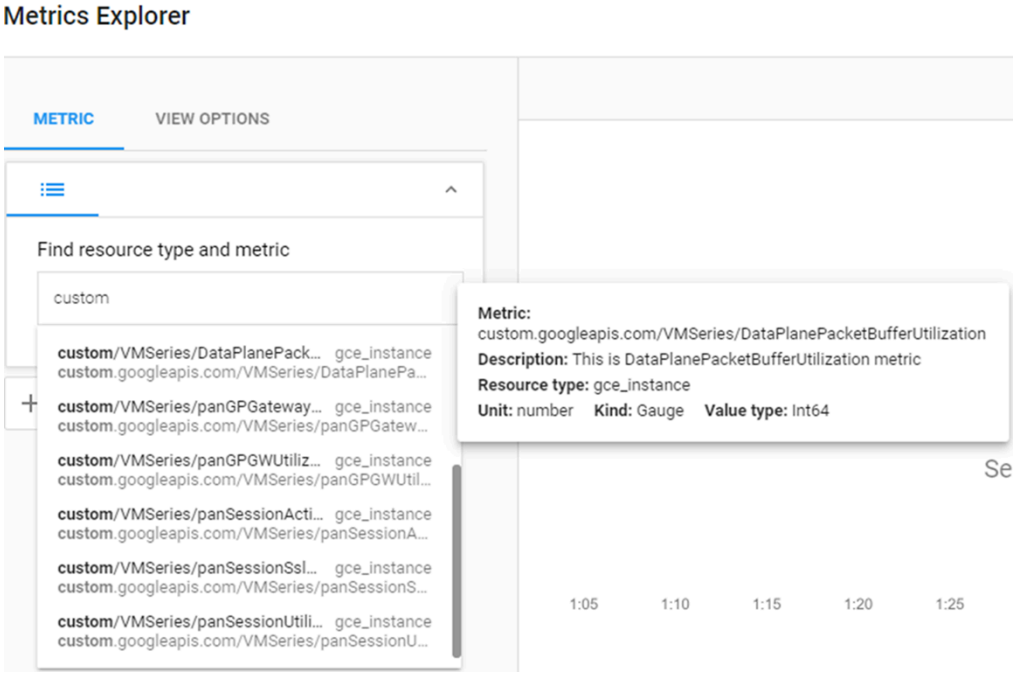
   2. 設定 **Update Interval**（更新間隔）（範圍是 1 - 60 分鐘；預設為 5）。這是防火牆將度量發佈至 Stackdriver 的頻率。
   3. 按一下 **OK**（確定）。
3. **Commit**（提交）您的變更。

   在您為 PAN-OS 度量設定警報之前，等待直到防火牆開始將度量發佈至 Stackdriver。

©2023 Palo Alto Networks, Inc.

STEP 2 | 確認您在 Stackdriver 上可以看見度量。

1. 在 Google Cloud 主控台中，選取 **Products and Services**（產品和服務） > **Monitoring**（監控）。
2. 在 Stackdriver 中，選取 **Resources**（資源） > **Metrics Explorer**。
3. 在尋找資源類型和度量區段中，於搜尋欄位輸入 **`custom`** 以篩選 PAN-OS 度量。



STEP 3 | 在 Stackdriver 上為 PAN-OS 度量設定警報和動作。請參閱 Google Compute Engine 快速入門與 Stackdriver 警報簡介。

啟用 VM 監控以追蹤在 Google Cloud Platform (GCP) 上的 VM 變更

您可以啟用任何執行 PAN-OS 9.0（虛擬或實體）的防火牆以監控部署在 Google Compute Engine Instance 上的應用程式工作負載。VM 監控讓您可以監控預定義的中繼資料元素組或在 VM-Series 防火牆上的屬性。在 PAN-OS 9.1 管理員指南中，請參閱在雲端平台中虛擬電腦上監控的屬性。

瞭解 Google VPC 中的虛擬電腦新增、移動和刪除操作，您即可建立安全性原則規則，以自動適應應用程式環境中的更改。當您部署或移動虛擬電腦時，防火牆會收集屬性（或中繼資料元素）。您可以使用此中繼資料作為規則比對，及定義動態位址群組（請參閱使用動態位址群組保護 VPC 中的實例）。

您可為每個防火牆或為具多虛擬系統功能的防火牆上的每個虛擬系統設定多達十個 VM 資訊來源。資料來源也可使用 Panorama 範本推送。

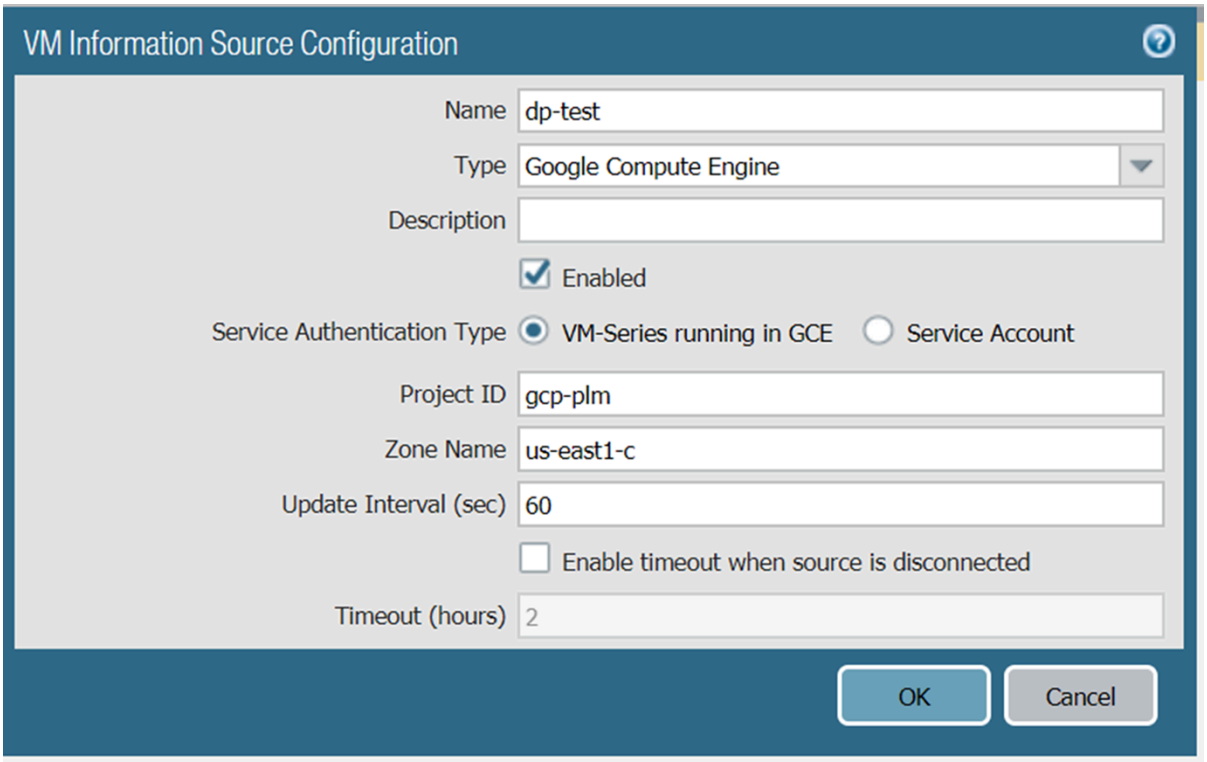
若要執行 VM 監控，您必須具有監控度量寫入器的 IAM 角色。

STEP 1 | 登入您已部署的防火牆。

©2023 Palo Alto Networks, Inc.

STEP 2 | 啟用 VM 監控。

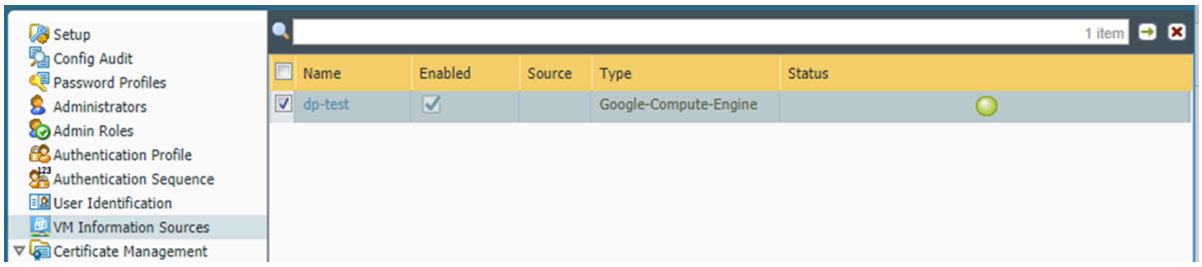
1. 選取 **Device**（裝置） > **VM Information Sources**（**VM** 資訊來源）。
2. **Add**（新增）VM 資訊來源並輸入以下資訊：
   - 指定 **Name**（名稱）用來識別您要監控的實例。
   - 選取 Google Compute Engine **Type**（類型）。
   - 選取 **Enabled**（已啟用）。
   - 選取 **Service Authentication Type**（服務驗證類型）。
     - 如果您選取 **VM-Series running in GCE**（在 **GCE** 中執行的 **VM-Series**），則會驗證建立實例時產生的預設服務帳戶。此為實例中繼資料之部分。
     - 如果您想要自目前專案之外的防火牆監控，請選取 **Service Account**（服務帳戶）。您必須上載 JSON 格式的服務帳戶認證。請參閱建立並管理服務帳戶金鑰。
   - （選用）將 **Update interval**（更新間隔）修改成在 5-600 秒之間的值。依預設，防火牆每 5 秒會輪詢一次。系統會將 API 呼叫排入佇列中並每隔 60 秒擷取這些呼叫，因此更新花費的時間為 60 秒加上所設定的輪詢間隔。



   - （選用）若要變更逾時之前的小時數，請核取 **Enable timeout when the source is disconnected**（當來源中斷連線時啟用逾時） 並輸入監控來源的連線關閉前的逾時（單位為小時；範圍是 2 至 10；預設為 2）。

     如果防火牆無法存取主機並已達到指定上限，防火牆將關閉與來源的連線。
   - 按一下 **OK**（確定）並 **Commit**（提交）變更。

©2023 Palo Alto Networks, Inc.



STEP 3 | 確認連線狀態。

如果連線狀態為擱置中或已中斷，請確認來源正在運作中，且防火牆也能存取來源。如果您使用非管理 (MGT) 連接埠的連接埠與受監控來源進行通訊，則必須變更服務路由（選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務），並按一下 **Service Route Configuration**（服務路由設定），然後修改 **VM Monitor**（**VM** 監控）服務的 **Source Interface**（來源介面））。

使用動態位址群組保護 VPC 中的實例

在如 Google® Cloud Platform (GCP™) 等您可以視需求啟動新實例的動態環境中，管理安全性原則中的管理負荷很難處理。使用在政策中使用動態位址群組可讓作業更加靈活，並能防止服務中斷或保護漏洞。

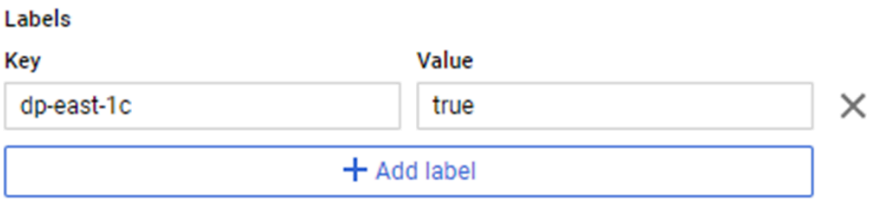
此工作流程假設您已部署 VM-Series 防火牆並已設定一些實例上的應用程式，以及啟用 Google Stackdriver 監控。

STEP 1 | 設定防火牆以監控 VPC。

STEP 2 | 在 VPC 中的標籤實例。

標籤為名稱-值配對。您可以標記來自 Google Cloud 主控台、Google API 呼叫或 Google Cloud Shell 的資源。在此工作中，我們會標示實例；不過，標籤可以套用至許多資源，如標記資源中所述。

您也可以從實例瀏覽器新增標籤。

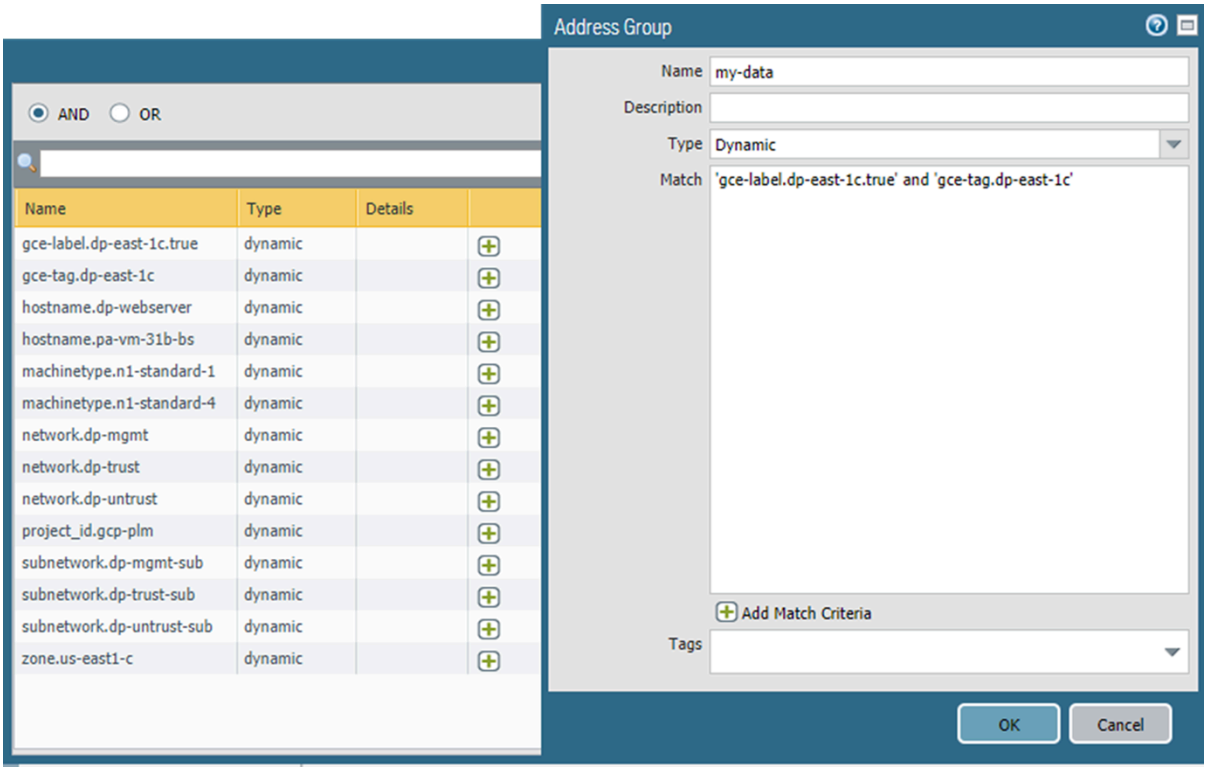


您建立的標籤支援您的原則，以對安全性政策有用的方式來區分您的資源。

 ©2023 Palo Alto Networks, Inc.

STEP 3 | 在防火牆上建立動態位址群組。

1. 選取 **Object**（物件） > **Address Groups**（位址群組）。
2. **Add**（新增）動態位址群組，並指定 **Name**（名稱）和 **Description**（描述）。
3. 將 **Type**（類型）設定為 **Dynamic**（動態）。
4. 定義比對準則。
   1. **Add Match Criteria**（新增比對準則），然後選取 **And** 運算子。
   2. 選取要篩選或比對的屬性。



5. 按一下 **OK**（確定）。
6. 按一下 **Commit**（交付）。

 ©2023 Palo Alto Networks, Inc.

STEP 4 | 在安全性政策規則中使用動態位址群組。

建立規則以允許網際網路存取任何屬於名為 my-data 之動態位址群組的 Web 伺服器。

1. 選取 **Policies**（政策） > **Security**（安全性）。
2. **Add**（新增）規則以及規則的 **Name**（名稱），並確認 **Rule Type**（規則類型）為 `universal`。
3. 在 **Source**（來源）頁籤中，新增 trust 作為 **Source Zone**（來源地區）。
4. 在 [Source Address（來源位址）] 區段中，**Add**（新增）新的 my-data 群組。
5. 在 **Destination**（目的地）頁籤中，新增 untrust 作為 **Destination Zone**（目的地地區）。
6. 在 **Service/URL Category**（服務/**URL** 類別）頁籤中，確認將服務設定為 **application-default**（應用程式預設值）。
7. 在 **Actions**（動作）頁籤中，將 **Actions**（動作）設定為 Allow（允許）。
8. 在 [Profile Settings（設定檔設定）] 中，將 **Profile Type**（設定檔類型）設定為 **Profiles**（設定檔），然後連接防毒、反間諜軟體和弱點保護的預設設定檔。
9. 按一下 **OK**（確定）。
10. 按一下 **Commit**（交付）。

STEP 5 | 確認在防火牆上已填入動態位址群組的成員。

將為此位址群組的所有 IP 位址強制執行政策，並在此處顯示。

1. 選取 **Policies**（政策） > **Security**（安全性），然後選取規則。
2. 從下拉式清單中，選取 **Inspect**（檢查）。您也可以驗證比對準則是否正確。
3. 按一下 **more**（更多），以確認顯示已註冊的 IP 位址清單。

使用自訂範本或 gcloud CLI 部署 VM-Series 防火牆

在 Google Cloud Platform Marketplace 上發佈的官方 VM-Series 映像可從 **paloaltonetworksgcp-public** 專案中取得。如果您要從 **gcloud** 命令行調用映像，或者在您編寫或改編的範本中參照映像，則您需要知道這些映像的安全路徑。

- BYOL: vmseries-byol-*<version>*
- PAYG Bundle 1: vmseries-bundle1-*<version>*
- PAYG Bundle 2: vmseries-bundle2-*<version>*

使用 gcloud CLI 尋找目前的映像名稱與專案：

```
  gcloud compute images list --project paloaltonetworksgcp-public
   --no-standard-images   NAME PROJECT FAMILY DEPRECATED STATUS
   vmseries-bundle1-810 paloaltonetworksgcp-public READY   vmseries-
bundle2-810 paloaltonetworksgcp-public READY   vmseries-byol-810
 paloaltonetworksgcp-public READY
```

新增 **--uri** 旗標，以查看映像路徑：

 ©2023 Palo Alto Networks, Inc.

```
gcloud compute images list --project paloaltonetworksgcp-public
 --no-standard-images --uri
```

```
https://www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-
public   /global/images/vmseries-bundle1-810   https://
www.googleapis.com/compute/v1/projects/paloaltonetworksgcp-public
   /global/images/vmseries-bundle2-810   https://www.googleapis.com/
compute/v1/projects/paloaltonetworksgcp-public   /global/images/
vmseries-byol-810
```

例如，從 https://github.com/PaloAltoNetworks 下載 gcp-two-tier 範本。

此範本將映像名稱（包括 PAN-OS 版本）與 URL 路徑分隔。在 `two-tier-template.py` 中，*image* 變數需要映像名稱；例如：*vmseries-byol-810*。`vm-series-template.py` 使用 *COMPUTE_URL_BASE* 和 *sourceImage* 的值來建立路徑。

©2023 Palo Alto Networks, Inc.

使用 GCP 專用 Panorama 外掛程式進行 VM 監控

Google Cloud Platform (GCP) 專用 Panorama 外掛程式版本 2.0.0 可讓您建立 VM 監控設定，以向 GCP 專案驗證，並監控 VM-Series 防火牆及其中部署的其他 VM。當您對專案建立連線後，此外掛程式可以擷取 Panorama 與 GCP 資產之間的「IP 位址至標籤對應」通訊。標籤可以是預先定義的屬性、VM 的使用者定義標籤及使用者定義的網路標籤（請參閱檢閱和建立標籤）。

GCP 專用 Panorama 外掛程式會從執行中 VM 擷取內部和外部 IP 位址，並定期從所連接 GCP VPC 中的 VM 擷取 IP 至標籤對應。

您可以使用標籤將 VM 組織成動態位址群組，然後在允許或拒絕流量流向特定 VM IP 位址的安全性政策規則中，參考您的標籤。若要一致地強制執行安全性政策，您可以將規則推送至 VM-Series 防火牆。

- 使用 GCP 專用 Panorama 外掛程式設定 VM 監控

使用 GCP 專用 Panorama 外掛程式設定 VM 監控

本主題說明為了 VM 監控而準備 GCP 資產的步驟、檢閱必要的 Panorama 元素，並說明如何在 Google Cloud Platform (GCP) 專用 Panorama 外掛程式中設定 VM 監控。

- 為了 VM 監控而設定 GCP 資產
- 檢閱和建立標籤
- 使用 GCP 專用 Panorama 外掛程式設定 VM 監控
  - 準備 Panorama 來設定 VM 監控
  - 設定 VM 監控

為了 **VM** 監控而設定 **GCP** 資產

您可以監控您從 GCP 市集部署的 VM-Series 防火牆、您以自動調整規模防火牆範本部署的防火牆、您從 GCP 主控台或 gcloud 命令列建立的 GCE 實例，或 GCP 中部署的其他 virtual machine（虛擬機器 - VM）。如果您從 Marketplace 部署 PAN-OS VM，請遵循在 Google Cloud Platform 上設定 VM-Series 防火牆中的指示。

檢閱 **IAM** 角色

確保您具有下列最低權限可執行 VM 監控工作：

- 在 GCP 主控台，為您的專案建立 服務帳戶，並授與專案擁有者或編輯者權限。

  無法自動建立服務帳戶。如果您沒有權限建立服務帳戶，您可以要求管理員建立，並指派適當角色給您。
- 檢視服務帳戶：唯讀。
- 檢視從 Google Marketplace 部署的 PAN-OS VM：計算檢視者。
- 指派使用者定義的標籤給實例：專案擁有者、編輯者或實例管理員。

©2023 Palo Alto Networks, Inc.

建立服務帳戶

在 Panorama 上使用 GCP 外掛程式設定 VM 監控之前，您必須使用 GCP 主控台建立服務帳戶，以授與權限來存取 GCP 專案、部署於其中的 VM-Series 防火牆、您希望 Panorama 管理的其他任何 VM，以及相關的網路和子網路。Panorama 專用 GCP 外掛程式會擷取 Google 資產預先定義的屬性、使用者定義的 VM 標籤和使用者定義的網路標籤。

每個專案都有一個建立專案時自動建立的預設服務帳戶。如果您特別為 VM 監控建立單獨的服務帳戶，則您對使用者及其角色有更大的控制權。每個專案最多可以設定 100 個服務帳戶。

STEP 1 | 在 Google Cloud Platform 主控台，選取您想要監控的專案。

STEP 2 | 選取 **IAM & Admin**（**IAM** 與管理員） > **Service accounts**（服務帳戶），然後選擇 **+Create Service Account**（**+** 建立服務帳戶）。

輸入服務帳戶名稱和說明，然後按一下 **Create**（建立）。

STEP 3 | 從下拉式功能表中選取角色類型，然後在右側選取適當的存取層級。

例如，選取 [Project（專案）] > [Editor（編輯者）]。您可以選取多個角色給一個服務帳戶。

完成時按一下 **Continue**（繼續）。

STEP 4 | 授與權限讓特定使用者存取此服務帳戶。從右側的 **Permissions**（權限）欄選取成員，給他們權限來存取上一步中的角色。

STEP 5 | （選用）按一下 **+CREATE KEY**（**+** 建立金鑰）建立認證，讓您以 Google Cloud CLI 驗證來存取 VM-Series 防火牆、網路及其他與此服務相關聯的 VM。

自動會下載此金鑰。務必存放在安全位置。產生的私密金鑰有如下的 JSON 格式：

```
{ "type": "service_account", "project_id": "gcp-xxx",
 "private_key_id":"252e1e7a2e9c84b5d4dbb6195b1de074594b6499",
 "private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDAd0i
+RMKCtrsO\n4KHnzTAPrgoBjRgpjyNcvQmdUqHr\n-----END PRIVATE
 KEY-----\n", "client_email": "dlp-vm-monit-svc-acct@gcp-
xxx.iam.gserviceaccount.com", "client_id":"108932514695821539229",
 "auth_uri": "https://accounts.google.com/o/oauth2/auth",
 "token_uri": "https://oauth2.googleapis.com/token",
 "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/
v1/certs", "client_x509_cert_url": "https://www.googleapis.com/
robot/v1/metadata/x509/dlp-vm-monit-svc-acct%40gcp-
xxx.iam.gserviceaccount.com" }
```

檢閱和建立標籤

預先定義的屬性、使用者定義的標籤及使用者定義的網路標籤，通稱為「標籤」。

- 對於 Google VM，自動會建立預先定義的標籤（屬性）。當您設定 VM 監控時，您可以選擇將 8 個預先定義的屬性全部監控，也可以建立一份自訂的屬性清單來監控。
- 您可以為 VM 標籤和網路標籤定義您自己的標籤。

©2023 Palo Alto Networks, Inc.

標記 VM 和網路以利於識別和分組，以便您建構規則來強制執行安全性政策。您可以標記 Google 專案中部署的任何 VM—例如，VM-Series 防火牆、Web 伺服器、應用程式伺服器或負載平衡器。

- 標籤必須與 VM 相關聯。這也適用於網路和子網路。
- 如果一個實例有多個相關聯的 IP 位址（例如，如果您標記 VM-Series 防火牆信任和不受信任介面），Panorama 會產生多組標籤資訊。

Panorama 可擷取和註冊的標籤總數，取決於 Panorama 執行的 PAN-OS 版本和受管理 VM-Series 防火牆的版本。

在具有多個介面的 VM 上，Google 區域、Google 地區、VPC 名稱和子網路名稱用來標記網路介面。專用於網路介面。

預先定義的屬性

Panorama 專用 Google Cloud Platform 外掛程式會從任何受管理的 VM，擷取下列預先定義的標籤：

- 專案 **ID**—例如：google.project-id.myProjectId。

  若要在 Google 主控台尋找您的專案資訊，請選取專案，然後選取 **IAM & Admin**（**IAM** 與管理員） > **Settings**（設定）。
- 服務帳戶—您的服務帳戶，採用電子郵件地址形式。例如：google.svc-accnt.sa-name@project-id.iam.gserviceaccount.com。

  若要尋找您的服務帳戶，請檢視 VM 實例詳細資訊。
- **VPC** 名稱—受管理 VM 的 VPC 網路名稱。例如：google.vpc-name.myvnet。
- 子網路名稱—您為受管理 VM 介面建立的子網路名稱。例如，對於 VM-Series 防火牆不受信任介面，您為不受信任介面建立的子網路名稱：google.subnet-name-untrust.web。
- **OS SKU**—您部署受管理 VM 時選擇的作業系統。例如：google.os-sku.centos-7。

  如果 *VM* 使用自訂映像，則不支援此屬性。
- **Google** 區域—您部署 VM 時選取的區域。例如：google.zone.us-east1-c。
- **Google** 地區—您選取的區域所在的地區。例如：google.region.us-east1。
- 實例群組名稱—例如：google.instance-group.myInstanceGroup。若要在 Google 主控台檢視或建立實例群組，請選取 **Compute Engine** > **Instance Group**（實例群組）。

使用者定義的標籤

Panorama 最多使用 16 個使用者定義的標籤。如果您有 16 個以上的標籤，Panorama 會依字母順序排序使用者定義的標籤，並使用前 16 個標籤。

檢閱標籤鍵值組的 Google 需求：鍵最短 1 個字元，最長 63 個字元，不得空白。值可以空白，最長 63 個字元。

若要在 GCP 主控台建立或檢視標籤，請前往 **Compute Engine** > **VM Instances**（**VM** 實例），然後選取 **Show Info Panel**（顯示資訊面板）。在 **Info Panel**（資訊面板）中，選取 **Labels**（標籤）。按一下 **+Add a label**（**+** 新增標籤），新增鍵和值，然後按一下 **Save**（儲存）。

©2023 Palo Alto Networks, Inc.

使用者定義的網路標籤

Panorama 最多使用 8 個使用者定義的網路標籤。如果您有 8 個以上的標籤，Panorama 會依字母順序排序使用者定義的標籤，並使用前 8 個標籤。

請注意，Google 限制網路標籤如下：

- 每個標籤最多 63 個字元。
- 您可以使用小寫字母、數字和破折號。標籤必須以小寫字母開頭，以數字或小寫字母結尾。

若要在 GCP 主控台建立或檢視網路標籤，請前往 **Compute Engine** > **VM Instances**（**VM** 實例），然後選取實例。**Edit**（編輯）實例，向下捲動至 **Network Tags**（網路標籤），輸入標籤（以逗號分隔），然後 **Save**（儲存）。請參閱設定網路標籤。

使用 GCP 專用 Panorama 外掛程式設定 VM 監控

標記 GCP 資產和建立服務帳戶之後，請將資產提供給 Panorama，以便您設定 VM 監控。

準備 **Panorama** 來設定 **VM** 監控

請依照下列步驟讓 Panorama 管理和監控 GCP 資產。部署於 GCP 的任何 VM 都可以是 Panorama 中受管理的裝置。

STEP 1 | 在 Panorama 中，將 VM-Series 防火牆及 GCP 專案相關聯的其他 VM 新增為受管理的裝置。

STEP 2 | 新增裝置群組並將受管理的裝置指派給群組。裝置群組是您想以群組形式管理的一組防火牆或 virtual system（虛擬系統 - vsys）。

> *VM* 只能是一個裝置群組的成員。請謹慎規劃裝置群組。

STEP 3 | 新增範本。命名範本並接受預設 VPC。

STEP 4 | 新增範本堆疊。**Add**（新增）堆疊，**Add**（新增）您剛建立的範本，然後選取您的裝置。

STEP 5 | Commit（提交）變更。

設定 **VM** 監控

STEP 1 | 如果尚未安裝 GCP 專用 Panorama 外掛程式，請這麼做。

STEP 2 | 登入 Panorama 網頁介面，然後選取 **Panorama** > **Google Cloud Platform**。

©2023 Palo Alto Networks, Inc.

STEP 3 | 設定 VM 監控。

1. 進行一般設定。

   1. 選取 **Panorama** > **Google Cloud Platform** > **Setup**（設定） > **General**（一般）。若要編輯設定，請按一下齒輪。

      - 勾選 **Enable Monitoring**（啟用監控），在您設定服務帳戶的所有專案上允許 VM 監控。
      - 輸入 **Monitoring Interval**（監控間隔）（以秒為單位）。這是標籤擷取事件之間的時間長度。

2. **Add**（新增）通知群組。通知群組是裝置群組清單，Panorama 會將「IP 位址至標籤」對應和更新推送至這些裝置群組。

   一個專案只能有一個通知群組。

   1. 選取 **Panorama** > **Google Cloud Platform** > **Setup**（設定） > **Notify Groups**（通知群組），然後按一下 **Add**（新增）。
   2. 輸入 **Name**（名稱）以識別防火牆群組，Panorama 會將擷取的 VM 資訊（IP 位址至標籤對應）推送至這組防火牆。
   3. 選取 **Device Groups**（裝置群組），Panorama 會將從您的專案擷取的 VM 資訊（IP 位址至標籤對應）推送至這些裝置群組。VM-Series 防火牆根據此更新，以決定安全性政策中所參考動態位址群組的最新成員清單。

      請謹慎規劃裝置群組。

   4. 選取預先定義的標籤或自訂標籤。

      - **Select All 8 Predefined Tags**（8 個預先定義的標籤全選）—選擇此選項可選取所有預先定義的屬性（標籤）。
      - **Custom Tags**（自訂標籤）—選擇此選項可以為預先定義的屬性、使用者定義的標籤及使用者定義的網路標籤，建立標籤清單。

   5. - 請確保所有相關的裝置群組都包含在單一通知群組中。
      - 如果您要取消註冊 Panorama 推送至通知群組中所包含防火牆的標籤，必須刪除監控定義。
      - 若要在已針對多個虛擬系統啟用的防火牆上註冊標籤至所有虛擬系統，您必須在 Panorama 上新增每個虛擬系統至單獨的裝置群組並將裝置群組指派給通知群組。

©2023 Palo Alto Networks, Inc.

如果您將所有虛擬系統指派給一個裝置群組，Panorama 將僅註冊標籤至一個虛擬系統。

3. **Add**（新增）GCP 服務帳戶認證。
   - 命名服務帳戶認證。
   - （選用）輸入服務帳戶的說明。
   - **Browse**（瀏覽）來上傳您建立服務帳戶時產生的 JSON 檔案。

   您必須使用 *Panorama* 網頁介面。您無法使用 *CLI* 來新增服務帳戶

   一個認證只能使用一個服務帳戶。請勿從單一 *JSON* 檔案建立多個認證。

新增服務帳戶認證之後，您可以從 Panorama 命令列來驗證認證：

```
request plugins gcp validate-service-account <svc-acct-credential-name>
```

STEP 4 | 建立 **Monitoring Definition**（監控定義）。

監控定義由專案的服務帳戶驗證及通知群組所組成。專案中的所有網路資產都受到監控，而擷取的標籤會推送至您列在監控定義中的裝置群組。當您新增監控定義時，其依預設會啟用。

一個專案只能有一個監控定義，一個監控定義只能包含一個通知群組。

1. 選取 **Panorama** > **Google Cloud Platform** > **Monitoring Definition**（監控定義），然後按一下 [Add（新增）]。
2. **Name**（命名）監控定義。
3. 對於您監控的專案和資產，輸入選用 **Description**（說明）。
4. 選取您在上一步建立的 **Service Account**（服務帳戶）認證。
5. 選取 **Notify Group**（通知群組）。
6. 對此服務帳戶相關聯的元素，**Enable**（啟用）監控。

STEP 5 | 在 Panorama 上 **Commit**（提交）變更。

確認監控定義的狀態顯示為「成功」。如果失敗，請確認您已正確輸入專案 ID，且為服務提供正確的金鑰和 ID。

©2023 Palo Alto Networks, Inc.

STEP 6 | 確認您可在 Panorama 上檢視 VM 資訊，並定義動態位址群組的比對準則。

HA 容錯移轉時，新近的主動 Panorama 會嘗試重新連線至 Google Cloud Platform，並擷取所有監控定義的標籤。即使一個監控定義在重新連線時發生錯誤，Panorama 也會產生系統日誌訊息：

HA 切換后無法處理訂閱；需要使用者干預。

如果您看到此錯誤，請在 Panorama 中解決問題。例如，移除無效訂閱或提供有效認證，並提交變更，以便 Panorama 重新連線並擷取所有監控定義的標籤。

即使 *Panorama* 與 *Google Cloud Platform* 中斷連線，防火牆仍有一份在容錯移轉之前已擷取的所有標籤，因此可以繼續對該 *IP* 位址清單強制執行政策。當您刪除監控定義時，*Panorama* 會移除與已註冊的 *VM* 相關聯的所有標籤。最佳做法是從 *Panorama* 設定動作導向的日誌轉送至 HTTPS 目的地，以便您立即採取行動。

©2023 Palo Alto Networks, Inc.

在 Google Cloud Platform 上自動調整 VM-Series 防火牆規模

Google Cloud Platform (GCP) 專用 Panorama 外掛程式版本 2.0.0 協助您在 GCP 部署 VM-Series 防火牆，還可讓 Panorama 管理 VM-Series 防火牆來保護 VM，以監控或自動調整 GCP 中的部署規模。使用 Panorama 執行集中式原則及防火牆管理，可更有效率地管理並維護防火牆的分散式網路。

由於 Panorama 維護 GCP 管理的實例群組，您可以建立應用程式支援政策，以保護和控制網路。

自動調整規模部署支援使用共用 VPC 網路設定或 VPC 網路對等，以建立通用 VPC 網路，其中，主機專案包含共用 VPC 網路和 VM-Series 防火牆，而服務專案包含基於 vm 或基於容器的應用程式部署（Kubernetes 叢集）。Palo Alto Networks提供範本，協助您在主機專案中部署 VM-Series 防火牆，在服務專案中部署選用範例應用程式。

BYOL 和 PAYG 授權可用於 VM-Series 防火牆。在授權期間，VM-Series 防火牆實例直接與 Palo Alto Networks 授權伺服器通訊。

如果您選擇 BYOL，則部署可能因為縮減規模事件而停用授權實例。如果 GCP 專用 Panorama 外掛程式中設定 VM-Series 防火牆的部署資訊，且已自動移除防火牆，則 Panorama 會偵測防火牆狀態，並自動取消註冊防火牆。

- Google Cloud Platform 專用自動調整規模元件
- 部署 GCP 自動調整規模範本 2

Google Cloud Platform 專用自動調整規模元件

一般 GCP 自動調整規模部署都使用主機專案和服務專案，並在兩者之間形成通用 VPC 網路。GCP 專用 Panorama 外掛程式可以在單一專案中搭配主機和服務 VPC，或在共用 VPC 或對等 VPC 網路設定中的主機和服務專案中，保護自動調整規模部署，其中主機專案包含 VM-Series 防火牆和共用 VPC 網路，而服務專案包含應用程式部署。如果應用程式部署在 Kubernetes 叢集，則需要對等 VPC。

- 自動調整規模需求
- 準備部署自動調整規模範本

自動調整規模需求

- 一般需求—請確定您的環境符合基本需求。
- **GCP** 專用 **Panorama** 外掛程式—如果尚未這麼做，請安裝 GCP 專用 Panorama 外掛程式。

  如果您先前已安裝 *GCP* 專用 *Panorama* 外掛程式版本 *1.0.0*，請先移除，再安裝 *2.0.X*。您無法升級。

- **Palo Alto Networks** 自動調整規模範本版本 **1.0**—Palo Alto Networks 提供範本，讓您在主機專案中部署 VM-Series 防火牆實例，在服務專案中設定和部署範例應用程式。如需範本的詳細資訊，請參閱關於自動調整規模範本。

  從 GitHub 下載範本。Zip 檔案包含防火牆範本和應用程式範本各自的 zip 檔案。

©2023 Palo Alto Networks, Inc.

準備部署自動調整規模範本

在部署自動調整規模範本之前，請完成下列工作。

- 準備主機專案和必要的服務帳戶
- 取得授權 API 金鑰
- 設定 GCP 專用 Panorama 外掛程式來保護自動調整規模部署
- 為自動調整規模準備 VM-Series 防火牆啟動套件

準備主機專案和必要的服務帳戶

您需要主機專案和服務專案，才能產生支援防火牆範本和應用程式範本的共用 VPC 拓撲。您可以建立新主機專案，或準備現有專案當作主機。

若要設定共用 VPC，組織管理員必須將共用 VPC 管理員角色授與主機專案管理員。共用 VPC 管理員可以啟用專案當作主機，並將服務專案管理員角色授與服務專案管理員。請檢閱有關管理員和 IAM 角色的 GCP 文件。

STEP 1 | 在 GCP 主控台，建立 GCP 專案當作主機。如果您想要使用現有專案，請跳至下一步。

若要建立新專案，請選取您的組織或 **No organization**（無組織），然後按一下 **New Project**（新專案）並填寫專案資訊。這注意，這是您 **EDIT**（編輯）專案 ID 的唯一機會。

必須安裝和設定 *Google Cloud SDK*，您才能從 *CLI* 向主機專案驗證。您將使用 *command line interface*（命令列介面 - *CLI*）部署防火牆範本和應用程式範本，並將服務專案連接至主機專案。

©2023 Palo Alto Networks, Inc.

STEP 2 | 啟用自動調整規模所需的 API 和服務。需要的 API 如下：

- 雲端發佈/訂閱 API
- 雲端部署管理員 API
- 雲端儲存 API
- Compute Engine API
- Google Compute Engine 實例群組管理員 API
- Google Compute Engine 實例群組更新者 API
- Google Compute Engine 實例群組 API
- Kubernetes 引擎 API
- Stackdriver API
- Stackdriver 日誌記錄 API
- Stackdriver 監控 API

您可以從 GCP 主控台或 GCP CLI 啟用 API，如下所示。

從 **GCP** 主控台啟用 **API**

1. 選取主機專案，從導覽功能表中選取 **APIs & Services**（**API** 與服務）。
2. 搜尋和檢視每個需要的 API。
3. **ENABLE**（啟用）任何不顯示「啟用 API」狀態的 API。

從 **CLI** 啟用 **API**

1. 在 CLI 中，檢視設定以確保您在正確專案中。

```
gcloud config list
```

否則，請如下設定專案：

```
gcloud config set project <project-name>
```

2. 發出下列命令以啟用需要的 API。

```
gcloud services enable pubsub.googleapis.com gcloud
 services enable deploymentmanager.googleapis.com
 gcloud services enable storage-component.googleapis.com
 gcloud services enable compute.googleapis.com gcloud
 services enable replicapool.googleapis.com gcloud
 services enable replicapoolupdater.googleapis.com gcloud
 services enable resourceviews.googleapis.com gcloud
 services enable container.googleapis.com gcloud services
 enable stackdriver.googleapis.com gcloud services
```


©2023 Palo Alto Networks, Inc.

```
enable logging.googleapis.com gcloud services enable
monitoring.googleapis.com
```

3. 確認需要的 API 已啟用。

```
gcloud services list --enabled
```


©2023 Palo Alto Networks, Inc.

STEP 3 | 建立用於部署 VM-Series 防火牆的服務帳戶，並指派自動調整服務或 Kubernetes 叢集規模所需的 IAM 角色。

當您設定防火牆範本時，您會將此服務帳戶的電子郵件新增至 VM-Series 防火牆 `.yaml` 檔案。在主機專案內，範本使用此服務帳戶的認證建立含子網路的主機 VPC、在 VPC 中部署 VM-Series 防火牆、設定 Stackdriver 自訂度量、建立發佈/訂閱主題等。

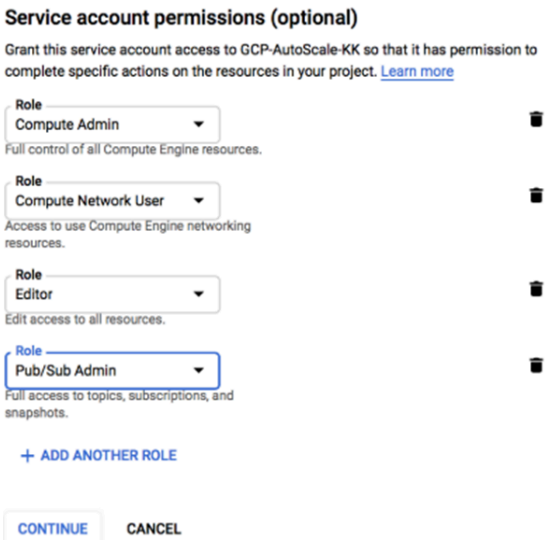
1. 在 GCP 主控台，選取 **IAM & Admin**（**IAM** 與管理員） > **Service accounts**（服務帳戶），然後選取 **+CREATE SERVICE ACCOUNT**（**+** 建立服務帳戶）。

   填寫服務帳戶詳細資訊，然後按一下 **CREATE**（建立）。

2. 將服務帳戶權限給予此專案中的自動調整規模資源。

   從下拉式功能表中選取角色類型，然後在右側選取適當的存取層級。例如，選取 [Project（專案）] > [Editor（編輯者）]。您可以選取多個角色給一個服務帳戶。

   - Compute Engine > Compute Admin（Compute 管理員）
   - Compute Engine > Compute Network User（Compute 網路使用者）
   - Pub/Sub（發佈/訂閱） > Admin（管理員）
   - Monitoring（監控） > Monitoring Metric Writer（監控度量撰寫者）
   - Stackdriver > Stackdriver Accounts Editor（Stackdriver 帳戶編輯者）
   - Storage（儲存區） > Storage Admin（儲存區管理員）
   - （僅限 GKE）Kubernetes > Kubernetes Engine Cluster Admin（Kubernetes 引擎叢集管理員）
   - （僅限 GKE）Kubernetes > Kubernetes Engine Viewer（Kubernetes 引擎檢視者）

   當您完成新增角色時 **Continue**（繼續）。

3. 按一下 **+CREATE KEY**（**+** 建立金鑰），為主機服務帳戶建立金鑰。
   - （選用）新增電子郵件地址，將其他使用者或管理員存取授與此服務帳戶。
   - 按一下 JSON，以 JSON 格式下載私密金鑰。
   - 將金鑰存放在安全位置。當您部署 GCP 自動調整規模範本時，會需要此金鑰。

 ©2023 Palo Alto Networks, Inc.

4. 按一下 **DONE**（完成）。

STEP 4 | 建立服務帳戶，讓 Panorama 管理員可以用來與此主機專案互動。

1. 在 GCP 主控台，選取 **IAM & Admin**（**IAM** 與管理員） > **Service accounts**（服務帳戶），然後選取 **+CREATE SERVICE ACCOUNT**（**+** 建立服務帳戶）。
2. 填寫服務帳戶詳細資訊，然後按一下 **CREATE**（建立）。
3. 授與服務帳戶存取。

   從下拉式功能表中選取角色類型，然後在右側選取適當的存取層級。例如，選取 [Project（專案）] > [Editor（編輯者）]。您可以選取多個角色給一個服務帳戶。

   - Compute Engine > Compute Viewer（Compute 檢視者）
   - Deployment Manager（部署管理員） > Viewer（檢視者）
   - Pub/Sub（發佈/訂閱） > Admin（管理員）

   按一下 **CONTINUE**（繼續）。
4. 按一下 **+CREATE KEY**（**+** 建立金鑰），為主機服務帳戶建立金鑰。
   - （選用）新增電子郵件地址，將其他使用者或管理員存取授與此服務帳戶。
   - 選取 JSON，以 JSON 格式下載私密金鑰。
   - 將金鑰存放在安全位置。當您設定 GCP 專用 Panorama 外掛程式來保護自動調整規模部署時，會需要此金鑰。

STEP 5 | （選用）在 CLI 中，確保您可以與新主機專案通訊。

1. 將專案設定為您剛建立的主機專案。

   ```
   gcloud set project <your-autoscale-host-project-name>
   ```
2. 建立用於自動調整規模的設定。除非您停用啟動，否則新設定會自動啟動。

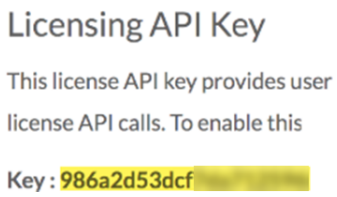
   ```
   gcloud config configurations create <CONFIGURATION_NAME> gcloud config list
   ```

取得授權 **API** 金鑰

您需要授權 API 金鑰，Panorama 才能授權和取消授權 GCP 中的受管資產。

STEP 1 | 登入支援入口網站，選取 **Assets**（資產） > **Licensing API**（授權 **API**），然後按一下 **Enable**（啟用）。出現金鑰。

只有超級使用者才能看到 *[Enable*（啟用）*]* 連結來產生此金鑰。請參閱如何啟用、重新產生、延長授權 API 金鑰。



STEP 2 | 選取金鑰並複製。

©2023 Palo Alto Networks, Inc.

STEP 3 | 從 CLI，以 SSH 進入 Panorama 並發出下列命令，將 <key> 換成從支援入口網站複製的 API 金鑰：

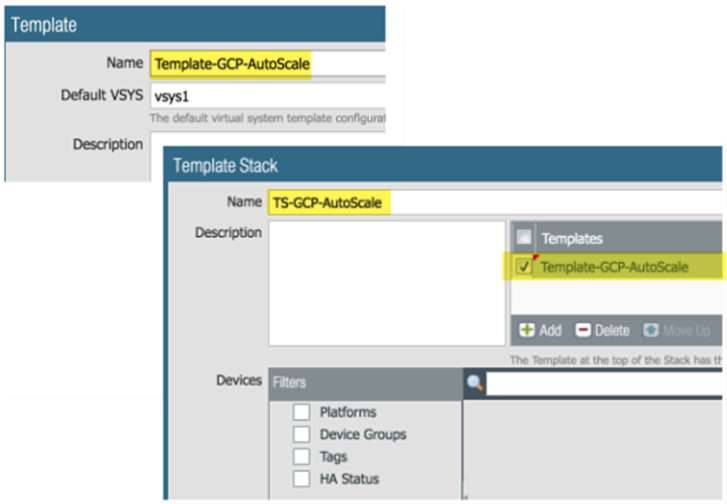
```
request license api-key set key <key>
```

```
API Key 設定成功
```

設定 **GCP** 專用 **Panorama** 外掛程式來保護自動調整規模部署

在 Panorama 中，建立資產來支援自動調整規模防火牆部署。

STEP 1 | 建立範本及包含該範本的範本堆疊，然後 **Commit**（提交）變更。



STEP 2 | 在 **Network**（網路）脈絡中，選取範本或範本堆疊。選取 **Virtual Routers**（虛擬路由器），然後 **Add**（新增）虛擬路由器。

當防火牆範本建立靜態路由時，這些路由會新增至此虛擬路由器。

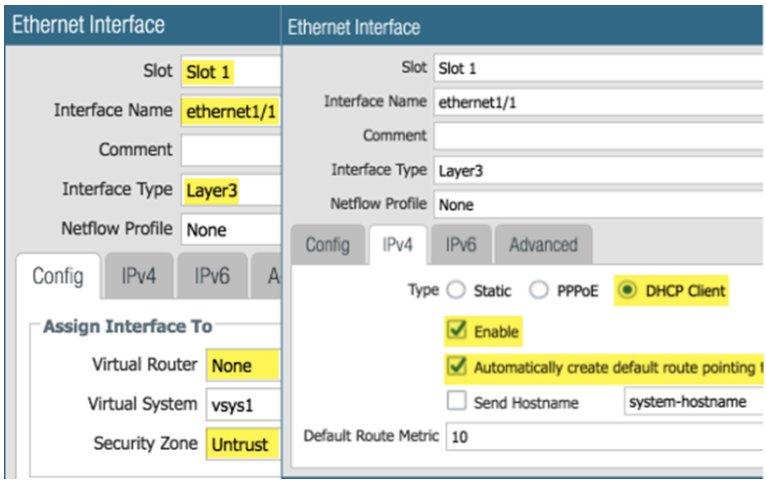
對於自動調整規模部署，只定義一個路由器。



 ©2023 Palo Alto Networks, Inc.

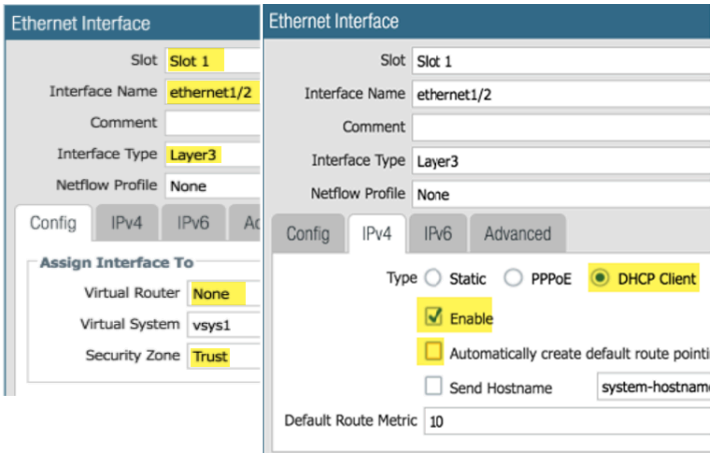
STEP 3 | 在 **Network**（網路）脈絡中，選取您建立的範本，然後選取 **Interfaces**（介面）和 **Add Interface**（新增介面）。

- 在 [Config（設定）] 頁籤上，選取插槽，選取 **Interface name**（介面名稱），然後選取 Layer3 **Interface Type**（介面類型）。從 **Security Zone**（安全性區域）功能表，選取 **New Zone**（新增區域），將區域命名為 Untrust，然後按一下 **OK**（確定）。
- 在 **IPv4** 頁籤上，啟用 **DHCP Client**（**DHCP** 用戶端）和 **Automatically create default route pointing to default gateway provided by server**（自動建立指向伺服器所提供之預設閘道的預設路由）（預設情況下啟用），然後按一下 **OK**（確定）。



STEP 4 | 新增 ethernet1/2 (Trust) 第三層介面。

- 在 [Config（設定）] 頁籤上，選擇與上一步相同的插槽，選取 **Interface name**（介面名稱）(ethernet1/2)，然後選取 Layer3 **Interface Type**（介面類型）。從 **Security Zone**（安全性區域）功能表，選取 **New Zone**（新增區域），將區域命名為 Trust，然後按一下 **OK**（確定）。
- 在 **IPv4** 頁籤上，啟用 **DHCP Client**（**DHCP** 用戶端），停用 **Automatically create default route pointing to default gateway provided by server**（自動建立指向伺服器所提供之預設閘道的預設路由），然後按一下 **OK**（確定）。



©2023 Palo Alto Networks, Inc.

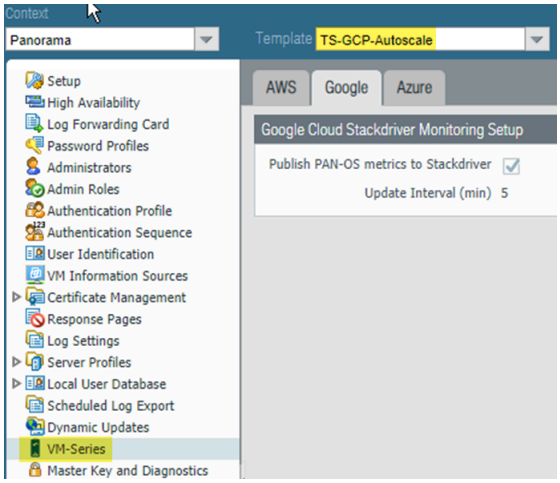
STEP 5 | 返回您稍早建立的範本堆疊和虛擬路由器。將 untrust 和 trust 介面（ethernet1/1 和 ethernet1/2）放入虛擬路由器中，然後按一下 **OK**（確定）。



STEP 6 | 設定自動調整部署規模的 Stackdriver。

您必須有 Panorama 上的 VM-Series 外掛程式，才能設定 Stackdriver。

1. 在 **Device**（裝置）脈絡中，從 [Template（範本）] 下拉式功能選取您稍早建立的範本堆疊。
2. 選取 **Device**（裝置） > **VM-Series** > **Google**，然後按一下 [Edit（編輯）] 齒輪 ( )。啟用 **Publish PAN-OS metrics to Stackdriver**（將 **PAN-OS** 度量發佈至 **Stackdriver**）。



3. Commit（提交）您的變更。

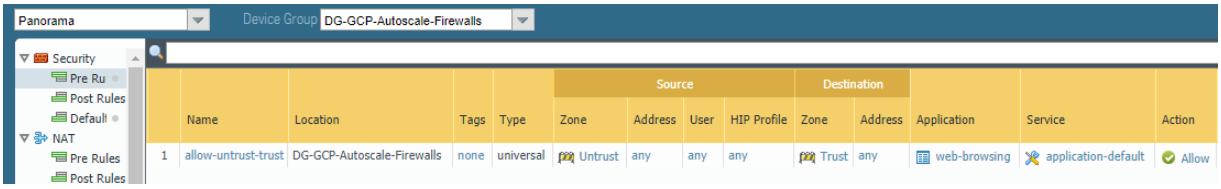
©2023 Palo Alto Networks, Inc.

STEP 7 | 建立裝置群組，該群組參考您在步驟 1 建立的範本或範本堆疊。

此裝置群組將包含您以防火牆範本建立的 VM-Series 防火牆。

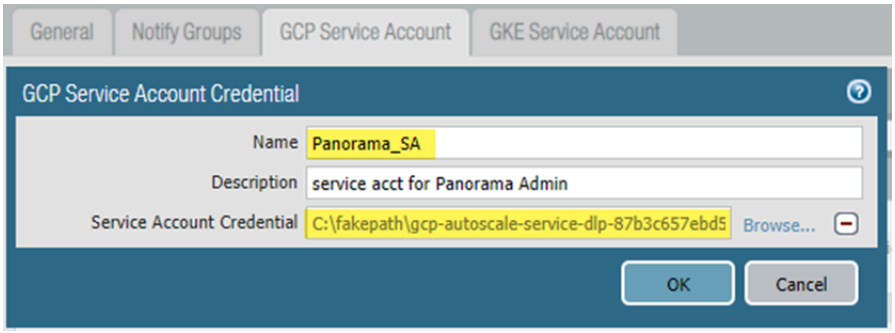
1. 新增安全性政策，以允許從 Untrust 至 Trust 的網頁瀏覽流量。

   在 [Policies（政策）] 脈絡中，選取您剛建立的裝置群組。選取 **Security**（安全性） > **Pre Rules**（預先規則），然後 **Add**（新增）下列安全性政策。



STEP 8 | 為主機專案設定 GCP 服務帳戶。

1. 在 Panorama 脈絡中，展開 Google Cloud Platform，選取 **Setup**（設定），然後按一下 **Add**（新增）。
2. 對您在步驟 4 建立的主機服務帳戶，提供名稱和說明。
3. 上傳您在步驟 4.4 建立的 JSON 認證檔案。



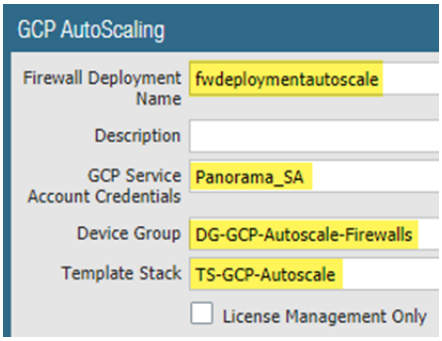
新增服務帳戶認證之後，您可以從 Panorama 命令列來驗證認證（無法從網頁介面來驗證）：

```
request plugins gcp validate-service-account
 gcp_service_account <svc-acct-credential-name>
```


©2023 Palo Alto Networks, Inc.

STEP 9 | 在 GCP 專用 Panorama 外掛程式上設定自動調整規模。

1. 在 Panorama 脈絡中，展開 Google Cloud Platform，選取 [AutoScaling （自動調整規模）]，然後按一下 **Add**（新增）。
2. 對部署提供防火牆部署名稱和選用說明。
3. 對 GCP 服務帳戶認證，提供步驟 8 中的 GCP 服務帳戶名稱。



4. 選擇您在步驟 7 建立的裝置群組，以及您在步驟 1 建立的範本堆疊。
5. 停用 **License Management Only**（僅限授權管理），以確保流量安全。

STEP 10 | Commit（提交）您的變更。

為自動調整規模準備 **VM-Series** 防火牆啟動套件

在啟動載入過程中，防火牆的初始要求會提供主機 IP 位址、序號和 VM 驗證金鑰，以便 Panorama 確認 VM 驗證金鑰，並將防火牆新增為受管理的裝置。然後，Panorama 可以將防火牆指派給適當的裝置群組和範本，以便您使用 Panorama 集中設定及管理防火牆。

在此情況下，您必須在 Panorama 上產生 VM 驗證金鑰，並將金鑰加入用於啟動載入的 init-cfg.txt 檔案中。VM 驗證金鑰可讓 Panorama 驗證新啟動的 VM-Series 防火牆。啟動套件必須包含。

- 在 /config 目錄中，init-cfg.txt 檔案（包含 Panorama IP 位址）。
- 在 /license 目錄中，名為 authcodes 的檔案包含 VM 驗證金鑰。

  金鑰的使用期限介於 1 小時至 8760 小時（1 年）之間。指定時間過後，金鑰將過期，若在此連線請求中沒有提供有效的驗證金鑰，Panorama 將不會註冊 VM-Series 防火牆。

STEP 1 | 設定 Google 儲存貯體，其中提供在 Google Cloud Platform 上啟動 VM-Series 防火牆所需的資料夾。您可以使用現有的啟動套件，或建立新的啟動套件，以提供這些資料夾。

STEP 2 | 編輯 `init-cfg.txt` 範例檔案中的值，依照您的環境自訂此檔案。

防火牆範本包含 `init-cfg.txt` 範例檔案。

參數	值	備註
type	dhcp-client	
hostname	<pa-vm>	您準備主機專案時指派的選用名稱。只有當需要特定主機

©2023 Palo Alto Networks, Inc.

參數	值	備註
		且 dhcp-send-hostname 是 no 時，才需要此參數。
vm-auth-key	<vmauthkey>	Panorama 將防火牆新增為受管理的裝置之前必須驗證的金鑰。請參閱在 Panorama 上產生 VM 驗證金鑰。
panorama-server	<panorama-ip>	您在設定 GCP 專用 Panorama 外掛程式來保護自動調整規模部署中所設定 Panorama 管理裝置的 IP 位址。
tplname	<template-stack-name>	您在設定 GCP 專用 Panorama 外掛程式來保護自動調整規模部署中建立的範本堆疊。
dgname	<dg-name>	您在 GCP 專用 Panorama 外掛程式中所建立裝置群組的名稱。
dns-primary		主要 DNS 伺服器。
dns-secondary		次要 DNS 伺服器。
dhcp-send-hostname	yes	保留原狀。
dhcp-send-client-id	yes	保留原狀。
dhcp-accept-server-hostname	yes	保留原狀。
dhcp-accept-server-domain	yes	保留原狀。

STEP 3 | 將您編輯過的 **`init-cfg.txt`** 檔案上傳至啟動套件中的 **`/config`** 資料夾。

STEP 4 | 如果您使用 BYOL，請建立名為 **`authcodes`** 的文字檔案（無副檔名），新增驗證碼，然後將檔案上傳至 **`/license`** 資料夾。

部署 GCP 自動調整規模範本

- 關於自動調整規模範本
- 部署防火牆範本
- 準備服務專案
- 設定共用 VPC
- 部署應用程式範本

©2023 Palo Alto Networks, Inc.

- 使新的應用程式上線
- 範例 GKE 服務範本

關於自動調整規模範本

從 https://github.com/PaloAltoNetworks/GCP-AutoScaling 下載 Palo Alto Networks 自動調整規模範本。Zip 檔案包含防火牆範本和應用程式範本各自的 zip。每個 zip 是含有多個檔案的範本目錄，但您只需要編輯 YAML 檔案。

- 防火牆範本
- 應用程式範本

防火牆範本

防火牆目錄檔案建立 VM-Series 防火牆及其他部署資源。這些檔案會為 VM-Series 防火牆建立新的網路和常見的子網路：管理、不受信任和信任。還會部署雲端發佈/訂閱傳訊服務，將資訊從 GCP 轉送至 GCP 專用 Panorama 外掛程式。此基礎結構備妥後，外掛程式可以利用動態位址群組，對輸入流量（路由至 GCP 上執行的服務）套用安全性政策，還可以根據自動調整規模度量來部署 VM-Series 防火牆，以滿足越來越需要應用程式工作負載資源的情況，或剔除不再需要的防火牆。

若要設定負載平衡器，請編輯外部應用程式負載平衡器 (ALB) 或網路負載平衡器 (NLB) 的 `.yaml` 檔案。

- **ALB**（HTTP 外部負載平衡器）

  若要自訂 ALB，請編輯 `vm-series-fw-alb.yaml`。

  HTTP 外部負載平衡器是基於 proxy 的負載平衡器，可對來自網際網路的輸入流量執行 SNAT 和 DNAT。HTTP 負載平衡器設計為僅支援 80 和 8080 TCP 連接埠。

  在負載平衡器分層式架構下，為了使用 HTTP 負載平衡器來支援多個應用程式，我們可以使用 GCP HTTP 負載平衡器 *urlMap* 和 *namedPort*，將不同 URL 對應至負載平衡器中的不同連接埠。接著，VM-Series 防火牆可以將連接埠轉譯為不同的應用程式，各以每個應用程式各一個內部負載平衡器來表示。

- **NLB**（TCP 負載平衡器）

  若要自訂 NLB，請編輯 `vm-series-fw-nlb.yaml`。

  TCP 負載平衡器是不基於 proxy 的負載平衡器，這表示不會對來自網際網路的輸入流量執行 NAT。

  GCP 中的 TCP 負載平衡器允許以任意連接埠新增多個前端 IP 位址，也就可能支援多個應用程式。

  TCP 負載平衡器還有一個優點是保留原始用戶端 IP 位址，這很適合某些應用程式。

應用程式範本

應用程式目錄提供範例應用程式。您可以設定和部署內部負載平衡器 (ILB)，讓應用程式伺服器訂閱「發佈/訂閱」服務，並與 VM-Series 防火牆及 Panorama 上的 GCP 外掛程式通訊。

若要自訂應用程式範本，請編輯 `apps.yaml`，如部署防火牆範本和應用程式範本所述。

©2023 Palo Alto Networks, Inc.

部署防火牆範本

從主機專案編輯防火牆範本。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

©2023 Palo Alto Networks, Inc.

STEP 1 | 編輯 `vm-series-fw-nlb.yaml` 或 `vm-series-fw-alb.yaml` 環境變數，以反映您的雲端環境。

此工作流程中的範例適用於 NLB。如需範本參數的進一步說明，請參閱vm-series-fw-nlb.yaml和vm-series-fw-alb.yaml。

```
屬性:      地區: us-east1      區域:      -us-east1-b      # 請勿修改 lb-類型欄位。      lb-類型: nlb      cloud-nat: yes      轉送規則連接埠:80
```

```
# 只允許一個應用程式      urlPath-namedPort-maps:      - appName: app1
```

```
# ssh 金鑰公用:      - 可選
```

在自動調整規模防火牆範本中，您需要以單引號括住輸入的值，鍵的前面要加上 **admin:** 並緊接一個空格。這與 Google Marketplace 範本採用的慣例相同，如SSH 金鑰配對所述。例如：

```
    sshkey: 'admin: ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDe0gJHd8okxPGWXsmdTdcZBJNI6ONT/NSz6INs2CNtKW
[redacted]
oTKXL8t0SRnOKaKV73NR5KnfpsNfwGxG8aQtEkeMCZIxX+6WOnRf/N4K3
yourname@[redacted].paloaltonetworks.local'
```

```
    bootstrap-bucket: bootstrap-autoscale
```

```
    image: vmseries-byol-814      machine-type: n1-standard-4
```

對於 service-account，提供您稍早（步驟 3）所建立主機專案服務帳戶的電子郵件地址。

```
      服務帳戶: sa-pan@gcp-autoscale-kk.iam.gserviceaccount.com
```

fw-instance-tag 值是部署中的受管理實例群組名稱。

```
     fw-instance-tag: vm-series-fw
```

為自動調整規模選擇一個度量。可能的值為：panSessionActive、panSessionUtilization、DataPlaneCPUUtilizationPct、DataPlanePacketBufferUtilizatio或 panSessionUtilization。

```
metric: custom.googleapis.com/VMSeries/panSessionActive
```

```
max-size:2 min-size:1 target-type:GAUGE util-target:100
```


©2023 Palo Alto Networks, Inc.

```
# Greenfield deployment mgmt-network-cidr:172.22.2.0/24 untrust-
network-cidr:172.22.1.0/24 trust-network-cidr:172.22.3.0/24 mgmt-
network-access-source-range: - 199.167.54.229/32 - 199.167.52.5/32
 mgmt-network-access-ports: - 22 - 443
```

STEP 2 | 部署防火牆範本。

```
gcloud deployment-manager deployments create <your-template> --
config apps.yaml --automatic-rollback-on-error
```

請記下部署之後 CLI 列印的輸出—子網路名稱、部署名稱和 Panorama 發佈/訂閱主題名稱。您需要這些值來設定共用 VPC 及用於應用程式範本部署。

在 GCP 專用 Panorama 外掛程式自動調整規模定義中，必須設定防火牆部署名稱。

準備服務專案

為應用程式建立單獨的服務專案，或選擇現有的專案。

若要進一步了解共用 VPC 中的主機專案和服務專案，請參閱共用 VPC 概觀，並檢閱管理員和 IAM 角色。主機專案管理員必須具有適當角色，才能設定共用 VPC，還有將應用程式專案變成主機專案的服務專案。請參閱佈建共用 VPC 中的指示。

©2023 Palo Alto Networks, Inc.

STEP 1 | 從 GCP 主控台或 CLI 啟用服務專案。

需要的 API 如下：

- 雲端部署管理員 API
- 雲端發佈/訂閱 API
- Compute Engine API

從 **GCP** 主控台啟用 **API**

1. 選取服務專案，從導覽功能表中選取 **APIs & Services**（**API** 與服務）。
2. 搜尋和檢視每個需要的 API。
3. **ENABLE**（啟用）任何不顯示「啟用 API」狀態的 API。

從 **CLI** 啟用 **API**

1. 在 CLI 中，檢視設定以確保您在正確專案中。

```
gcloud config list
```

否則，請如下設定專案：

```
gcloud config set project <project-name>
```

2. 發出下列命令以啟用需要的 API。

```
gcloud services enable deploymentmanager.googleapis.com gcloud
 services enable pubsub.googleapis.com gcloud services enable
 compute.googleapis.com
```

3. 確認需要的 API 已啟用。

```
gcloud services list --enabled
```

STEP 2 | 將應用程式專案變成主機專案的服務專案。

從服務/應用程式專案管理員新增服務帳戶，成為主機專案中具有下列角色的成員：

- Compute 網路使用者
- 發佈/訂閱管理員

STEP 3 | 選擇 VPC 設定。

- 如果服務專案在主機專案中會共用網路，請繼續設定共用 VPC。
- 如果服務專案有自己的 VPC 網路可用於應用程式部署，請繼續設定對等 VPC。

©2023 Palo Alto Networks, Inc.

設定共用 VPC

在主機專案中部署防火牆範本之後，請設定支援應用程式的服務專案。具備共用 VPC 認證的管理員會從主機專案執行這些工作。若要進一步了解共用 VPC 脈絡中的主機專案和服務專案，請參閱共用 VPC 概觀。

STEP 1 | 使用您部署防火牆範本時建立的信任 VPC，建立共用 VPC。

為主機（防火牆）專案設定共用 VPC：

```
gcloud compute shared-vpc enable HOST_PROJECT_ID
```

STEP 2 | 將服務/應用程式專案連接至主機專案。

```
gcloud compute shared-vpc associated-projects add
[SERVICE_PROJECT_ID]--host-project [HOST_PROJECT_ID]
```

有額外選項可讓您只共用特定的子網路，而非主機專案中的所有子網路。

STEP 3 | 如果您想要使用範例應用程式範本來部署應用程式，請繼續部署應用程式範本。

如果您已部署應用程式，且想要在自動調整規模部署中保護此應用程式，請前往手動使應用程式上線到現有的自動調整規模部署。

如果您已在 GKE 叢集部署服務，請繼續在共用 VPC 中使 GKE 叢集上線。

設定對等 VPC

兩個 VPC 之間必須建立 VPC 網路對等連線。如果 VPC 位於兩個不同專案中，則兩個專案中都必須建立連線。

STEP 1 | 在主機專案中，將防火牆部署的信任 VPC 網路與應用程式 VPC 互連。

```
gcloud beta compute networks peerings create [PEERING-NAME] \
     --network=[MY-LOCAL-NETWORK] \     --peer-project [SERVICE-
PROJECT-ID] \     --peer-network [PEER-NETWORK-NAME] \    [--
import-custom-routes] \    [--export-custom-routes]
```

STEP 2 | 在服務專案中，將應用程式部署的信任 VPC 網路與防火牆部署的信任 VPC 網路互連。

```
gcloud beta compute networks peerings create [PEERING-NAME] \
     --network=[MY-LOCAL-NETWORK] \     --peer-project [HOST-
PROJECT-ID] \     --peer-network [PEER-NETWORK-NAME] \    [--
import-custom-routes] \     [--export-custom-routes]
```

STEP 3 | 如果您想要使用範例應用程式範本來部署應用程式，請繼續部署應用程式範本。

如果您已部署應用程式，且想要在自動調整規模部署中保護此應用程式，請前往手動使應用程式上線到現有的自動調整規模部署。

如果您已在 GKE 叢集部署服務，請繼續在對等 VPC 中使 GKE 叢集上線。

©2023 Palo Alto Networks, Inc.

部署應用程式範本

服務專案管理員從服務專案部署應用程式範本。

STEP 1 | 建立單獨的應用程式專案（服務專案）來部署應用程式（請參閱準備服務專案）。

STEP 2 | 準備 `apps.yaml` 檔案，如apps.yaml中所述。

STEP 3 | 使用應用程式範本來部署新的應用程式，並定義具名連接埠的標籤。

```
gcloud deployment-manager deployments create <your-template> --
config apps.yaml --automatic-rollback-on-error
```

繼續在 GCP 專用 Panorama 外掛程式中檢視已上線的應用程式。

使新的應用程式上線

當您使用應用程式範本來部署應用程式時，它會負責連線至主機專案。對於您未以應用程式範本部署的應用程式，只要是部署在具有準備服務專案所述功能的服務專案中，一樣可受保護。

- 手動使應用程式上線到現有的自動調整規模部署
- 使 GKE 叢集上線

手動使應用程式上線到現有的自動調整規模部署

若要保護您使用外部負載平衡器和自動調整規模 VM-Series 防火牆部署所部署的應用程式，請遵循下列步驟。對於每個上線的應用程式，您必須提供應用程式名稱、具名連接埠和路徑。

STEP 1 | 準備將新的具名連接埠和 URL 路徑，新增至您部署防火牆範本時建立的 HTTP 外部負載平衡器。

STEP 2 | 以額外服務名稱和連接埠值更新所有實例群組 named-ports。下列範例使應用程式 `app2` 和 `app3` 上線。

```
gcloud compute instance-groups set-named-ports fw-template2-fw-igm-
us-east1-b --zone us-east1-b --named-ports=app1:80,app2:81,app3:82
 gcloud compute instance-groups set-named-ports fw-
template2-fw-igm-us-east1-c --zone us-east1-c --named-
ports=app1:80,app2:81,app3:82
```

STEP 3 | 建立新的 http-health-check。

```
gcloud compute backend-services create fw-template2-backend-app3 --
protocol="HTTP" --port-name=app3 --http-health-checks=fw-template2-
healthcheck-app3 --load-balancing-scheme="EXTERNAL" --global
```


©2023 Palo Alto Networks, Inc.

STEP 4 | 以稍早在 HTTP 外部負載平衡器上建立的 port-name，建立新的後端服務。

```
gcloud compute backend-services create fw-template2-backend-app3 --
protocol="HTTP" --port-name=app3 --http-health-checks=fw-template2-
healthcheck-app3 --load-balancing-scheme="EXTERNAL" --global
```

檢查是否看得見新的後端服務。

```
gcloud compute backend-services list
```

STEP 5 | 編輯 url-maps 並新增路徑規則。例如：

```
- paths:     - /app3     - /app3/*service:     https://
www.googleapis.com/compute/v1/projects/<project-name>/global/
backendServices/fw-template2-backend-app3
```

```
gcloud compute url-maps edit fw-template2-ext-loadbalancer
```

STEP 6 | 若要使用 VM-Series 防火牆保護此應用程式，請透過 gcloud CLI 手動觸發發佈/訂閱訊息。這樣會傳送訊息給防火牆範本中建立的主題。

```
gcloud pubsub topics publish   projects/topics/hj-asg-891ca3-gcp-
pavmqa-panorama-apps-deployment   --attribute ilb-ip=172.22.9.34,
     app-deployment-name=hj-asg-891ca3-app1,     ilb-port=80,
     named-port=81,     network-cidr=172.22.9.0/24,     fw-
deployment-name=hj-asg-891ca3,     host-project=gcp-pavmqa,
     type=ADD-APP   --message "ADD-APP"
```

STEP 7 | 在 GCP 專用 Panorama 外掛程式中檢視已上線的應用程式.

STEP 8 | （選用）若要更新應用程式屬性，例如 ilb-ip、ilb-port 或 named-port，請發出 pubsub 命令：

```
gcloud pubsub topics publish projects/gcp-pavmqa/topics/hj-
asg-891ca3-gcp-pavmqa-panorama-apps-deployment   --attribute
 ilb-ip=172.22.9.34,     app-deployment-name=hj-asg-891ca3-
app1,     ilb-port=80,     named-port=81,     network-
cidr=172.22.9.0/24,     fw-deployment-name=hj-asg-891ca3,     host-
project=gcp-pavmqa,     type=UPDATE-APP   --message "UPDATE-APP"
```

STEP 9 | （選用）若要停止保護應用程式，請發出下列命令：

```
gcloud pubsub topics publish projects/gcp-pavmqa/topics/hj-
asg-891ca3-gcp-pavmqa-panorama-apps-deployment   --attribute ilb-
ip=172.22.3.20,app-deployment-name=fw-templ-3-app-1,     ilb-
port=80,     named-port=80,     fw-deployment-name=hj-asg-891ca3,
     type=DEL-APP   --message "DEL-APP"
```


©2023 Palo Alto Networks, Inc.

使 **GKE** 叢集上線

若要使私人 GKE 叢集上線，Panorama 專用 GCP 外掛程式需要下列資訊。

- 在 GCP 中，向 GKE 服務公開叢集的 ELB 前端，以便 VM-Series 防火牆取得服務的具名連接埠資訊。
- 叢集 API 伺服器位址。
- 部署叢集所在服務的服務帳戶認證（JSON 格式）。

GKE 叢集名稱不可超過 *24* 個字元。如果您在對等 *VPC* 設定中部署自動調整規模，這確保靜態路由名稱不超過 *31* 個字元。

- 在共用 VPC 中使 GKE 叢集上線
- 在對等 VPC 中使 GKE 叢集上線
- 在 GCP 專用 Panorama 外掛程式中檢視已上線的應用程式
- 從 CLI 檢視部署狀態

在共用 *VPC* 中使 *GKE* 叢集上線

若要使 GKE 叢集上線，必須與服務專案共用主機專案信任網路 VPC。請參閱 設定共用 VPC。

基於安全考量，自動調整規模部署中應該只使用私人叢集。請參閱建立私人叢集。

STEP 1 | 設定主機專案 ID。

```
gcloud config set project [HOST_PROJECT_ID]
```

STEP 2 | （選用）設定叢集的計算區域或地區。

如果叢集是區域性，請輸入下列命令：

```
gcloud config set compute/zone [COMPUTE_ZONE]
```

如果叢集是地區性，請輸入下列命令：

```
gcloud config set compute/region [COMPUTE_REGION]
```

STEP 3 | 在主機專案中，更新信任 VPC 子網路中的次要範圍。

```
gcloud compute networks subnets update [TRUST_SUBNETWORK_NAME]   --
add-secondary-ranges   [PODS_IP_RANGE_NAME] = [POD_RANGE_CIDR],
   [SERVICE_IP_RANGE_NAME]=[SERVICE_RANGE_CIDR]
```

Pod 和服務 *IP* 範圍必須在：*10.0.0.0/8*、*172.16.0.0/12* 或 *192.168.0.0/16* 之內，且不得與子網域中現有的 *IP* 範圍發生衝突。

©2023 Palo Alto Networks, Inc.

STEP 4 | 在服務專案中，在共用 VPC 中建立私人叢集。

1. 設定服務專案 ID。

```
gcloud config set project [SERVicE_PROJECT_ID]
```

2. 在共用 VPC 中建立私人叢集。

```
gcloud container clusters create  [CLUSTER_NAME]   --project
 [SERVICE_PROJECT_ID]   --zone=[ZONE_NAME]   --enable-
ip-alias   --enable-private-nodes   --network projects/
[HOST_PROJECT_ID]/global/networks/[NETWORK_NAME]   --
subnetwork projects/[HOST_PROJECT_ID]/regions/[REGION_NAME] /
subnetworks/[TRUST_SUBNETWORK_NAME]   --cluster-secondary-
range-name=[PODS_IP_RANGE_NAME]   --services-secondary-
range-name=[SERVICE_IP_RANGE_NAME]   --master-ipv4-
cidr=[MASTER_IPV4_CIDR]   --enable-master-authorized-networks
   --master-authorized-networks=[PANORAMA_MANAGEMENT_IP/32],
   [MY_MANAGEMENT_IP/32]
```

STEP 5 | 檢查目前叢集脈絡：

```
kubectl config current-context
```

STEP 6 | 檢查所有叢集脈絡。

```
kubectl config get-context
```

STEP 7 | 切換至另一個叢集。

```
kubectl config use-context [CONTEXT_NAME]
```

如果您已在 GCP 主控台建立叢集，請產生 kubeconfig 項目：

```
gcloud container clusters get-credentials [CLUSTER_NAME]
```

STEP 8 | 在 `.yaml` 檔案中建立叢集角色—例如，`gke_cluster_role.yaml`。

```
apiVersion: rbac.authorization.k8s.io/v1beta1 kind:ClusterRole
 metadata:   name: gke-plugin-role rules:   - apiGroups:       - ""
     resources:       - services     verbs:       - list
```

STEP 9 | 套用叢集角色。

```
kubectl apply -f gke_cluster_role.yaml
```


©2023 Palo Alto Networks, Inc.

STEP 10 | 在 .yaml 檔案中建立叢集角色繫結—例如，gke_cluster_role_binding.yaml。

```
kind:ClusterRoleBinding apiVersion: rbac.authorization.k8s.io/
v1beta1 metadata:   name: gke-plugin-role-binding subjects:   -
 kind:ServiceAccount     name: [SERVICEACCOUNT_NAME]     namespace:
 default roleRef:   kind:ClusterRole   name: gke-plugin-role
   apiGroup: rbac.authorization.k8s.io
```

STEP 11 | 套用叢集角色繫結。

```
kubectl apply -f gke_cluster_role_binding.yaml
```

STEP 12 | 建立服務帳戶。

```
kubectl create serviceaccount [SERVICEACCOUNT_NAME]
```

STEP 13 | 以 JSON 格式匯出服務帳戶秘密權杖。

```
MY_TOKEN=`kubectl get serviceaccounts [SERVICEACCOUNT_NAME] -o
 jsonpath='{.secrets[0].name}'` kubectl get secret $MY_TOKEN -o
 json > [FILE_NAME].json
```

STEP 14 | 取得 API 伺服器位址。

```
kubectl config view --minify | grep server | cut -f 2- -d ":" | tr
 -d " "
```

STEP 15 | 在 GCP 專用 Panorama 外掛程式中，新增服務帳戶資訊。

選取 **Panorama** > **Google Cloud Platform** > **Setup**（設定）。

命名認證，輸入說明，然後輸入步驟 14 的 **API** 伺服器位址，對於 **GKE** 服務帳戶認證，上傳您在步驟 13 匯出的 JSON 檔案。

新增服務帳戶認證之後，您可以從 Panorama 命令列來驗證認證（無法從網頁介面來驗證）：

```
request plugins gcp validate-service-account gke_service_account
 <svc-acct-credential-name>
```

 ©2023 Palo Alto Networks, Inc.

STEP 16 | 在 GCP 專用 Panorama 外掛程式上設定自動調整規模。

1. 在 Panorama 脈絡中，展開 Google Cloud Platform，選取 [AutoScaling （自動調整規模）]，然後按一下 **Add**（新增）。
2. 對部署提供 **Firewall Deployment Name**（防火牆部署名稱）和選用說明。
3. 對於 **GCP Service Account Credential**（**GCP** 服務帳戶認證），提供準備主機專案和必要的服務帳戶的步驟 4 建立的 GCP 服務帳戶名稱。
4. 選擇您設定 Panorama 外掛程式時建立的裝置群組和範本堆疊。
5. 停用 **License Management Only**（僅限授權管理），以確保流量安全。
6. 輸入確切的 **GKE Cluster Name**（**GKE** 叢集名稱）。
7. （選用）輸入 GKE 叢集的 **Description**（說明）。
8. 輸入 GKE 叢集的 **Network CIDR**（網路 **CIDR**）。
9. 選取對應於 GKE 叢集的 **GKE Service Account**（**GKE** 服務帳戶）。

STEP 17 | Commit（提交）您的變更。

STEP 18 | （選用）根據使用範例 GKE 服務範本建立和部署服務範本，或在 GCP 主控台部署 GKE 服務。

在對等 *VPC* 中使 *GKE* 叢集上線

若要使 GKE 叢集上線，您必須建立服務 VPC 並與主機專案中的防火牆信任網路互連，如設定對等 VPC所述。

基於安全考量，自動調整規模部署中應該只使用私人叢集。請參閱建立私人叢集。

STEP 1 | 設定專案 ID。

```
gcloud config set project [PROJECT_ID]
```

STEP 2 | 設定叢集的計算區域或地區。

如果叢集是區域性，請輸入下列命令：

```
gcloud config set compute/zone [COMPUTE_ZONE]
```

如果叢集是地區性，請輸入下列命令：

```
gcloud config set compute/region [COMPUTE_REGION]
```

STEP 3 | 以 Pod 和服務的次要 IP 範圍更新服務專案 VPC 網路。

```
gcloud compute networks subnets update [GKE_PEERED_VPC_SUBNETWORK]
 --region=[REGION] --add-secondary-ranges PODS_IP_RANGE_NAME=[ip
 cidr], SERVICE_IP_RANGE_NAME=[ip cidr]
```


©2023 Palo Alto Networks, Inc.

STEP 4 | 啟用雲端 NAT。

需要雲端 *NAT* 才能部署私人叢集。

```
gcloud compute routers create [ROUTER_NAME]   --network
 [NETWORK_NAME]   --region [REGION_NAME]
```

```
gcloud compute routers nats create [NAT_CONFIG_NAME]   --router-
region [REGION_NAME]   --router [ROUTER_NAME]   --nat-all-subnet-
ip-ranges   --auto-allocate-nat-external-ip
```

STEP 5 | 在服務 VPC 中建立新的私人叢集。

```
gcloud container clusters create [CLUSTER_NAME]   --
project [SERVICE_PROJECT_ID]   --zone=[ZONE_NAME]   --
enable-ip-alias   --network [NETWORK_NAME]   --subnetwork
 [SUBNETWORK_NAME]   --enable-private-nodes   --cluster-
secondary-range-name=[PODS_IP_RANGE_NAME]   --services-
secondary-range-name=[SERVICE_IP_RANGE_NAME]   --master-ipv4-
cidr=[MASTER_IPV4_CIDR]   --enable-master-authorized-networks
   --master-authorized-networks=[PANORAMA_MANAGEMENT_IP/32],
   [MY_MANAGEMENT_IP/32]
```

STEP 6 | 檢查目前叢集脈絡：

```
kubectl config current-context
```

STEP 7 | 檢查所有叢集脈絡。

```
kubectl config get-context
```

STEP 8 | 切換至另一個叢集。

```
kubectl config use-context [CONTEXT_NAME]
```

如果您已在 GCP 主控台建立叢集，請產生 kubeconfig 項目：

```
gcloud container clusters get-credentials [CLUSTER_NAME]
```

STEP 9 | 在 `.yaml` 檔案中建立叢集角色—例如，`gke_cluster_role.yaml`。

```
apiVersion: rbac.authorization.k8s.io/v1beta1 kind:ClusterRole
 metadata:   name: gke-plugin-role rules:   - apiGroups:       - ""
     resources:       - services     verbs:       - list
```


©2023 Palo Alto Networks, Inc.

STEP 10 | 套用叢集角色。

```
kubectl apply -f gke_cluster_role.yaml
```

STEP 11 | 在 .yaml 檔案中建立叢集角色繫結—例如，gke_cluster_role_binding.yaml。

```
kind:ClusterRoleBinding apiVersion: rbac.authorization.k8s.io/
v1beta1 metadata:   name: gke-plugin-role-binding subjects:   -
 kind:ServiceAccount     name: [SERVICEACCOUNT_NAME]     namespace:
 default roleRef:   kind:ClusterRole   name: gke-plugin-role
   apiGroup: rbac.authorization.k8s.io
```

STEP 12 | 套用叢集角色繫結。

```
kubectl apply -f gke_cluster_role_binding.yaml
```

STEP 13 | 建立服務帳戶。

```
kubectl create serviceaccount [SERVICEACCOUNT_NAME]
```

STEP 14 | 以 JSON 格式匯出服務帳戶秘密權杖。

```
MY_TOKEN=`kubectl get serviceaccounts [SERVICEACCOUNT_NAME] -o
 jsonpath='{.secrets[0].name}'` kubectl get secret $MY_TOKEN -o
 json >[FILE_NAME].json
```

STEP 15 | 取得 API 伺服器位址。

```
kubectl config view --minify | grep server | cut -f 2- -d ":" | tr
 -d " "
```

STEP 16 | 在 GCP 專用 Panorama 外掛程式中，新增服務帳戶資訊。

選取 **Panorama** > **Google Cloud Platform** > **Setup**（設定）。

命名認證，輸入步驟 15 中的 **API** 伺服器位址，然後上傳您在步驟 14 匯出的 JSON 檔案。

新增服務帳戶認證之後，您可以從 Panorama 命令列來驗證認證：

```
request plugins gcp validate-service-account <svc-acct-credential-
name>
```


©2023 Palo Alto Networks, Inc.

STEP 17 | 在 GCP 專用 Panorama 外掛程式上設定自動調整規模。

1. 在 Panorama 脈絡中，展開 Google Cloud Platform，選取 [AutoScaling （自動調整規模）]，然後按一下 **Add**（新增）。
2. 對部署提供 **Firewall Deployment Name**（防火牆部署名稱）和選用說明。
3. 對 **GCP Service Account Credential**（**GCP** 服務帳戶認證），提供步驟 16 中的 GCP 服務帳戶名稱。
4. 選擇您設定 Panorama 外掛程式時建立的裝置群組和範本堆疊。
5. 停用 **License Management Only**（僅限授權管理），以確保流量安全。
6. 輸入確切的 **GKE Cluster Name**（**GKE** 叢集名稱）。
7. （選用）輸入 GKE 叢集的 **Description**（說明）。
8. 輸入 GKE 叢集的 **Network CIDR**（網路 **CIDR**）。
9. 選取對應於 GKE 叢集的 **GKE Service Account**（**GKE** 服務帳戶）。

STEP 18 | （選用）在服務專案中，根據使用範例 GKE 服務範本建立和部署 GKE 範本，或使用 GCP 主控台部署 GKE 服務。使 GKE 叢集上線

在 *GCP* 專用 *Panorama* 外掛程式中檢視已上線的應用程式

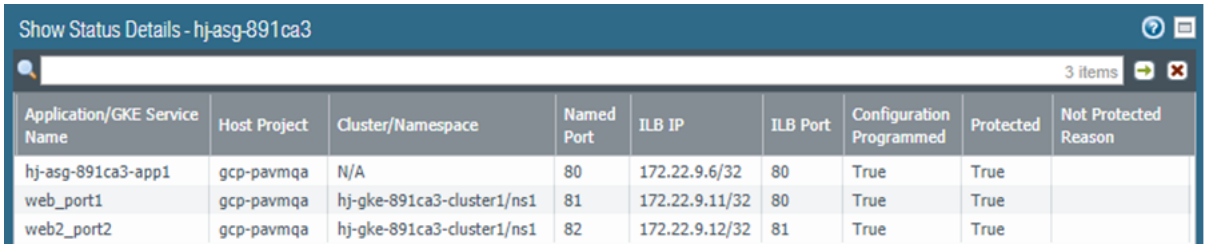
選取 **Panorama** > **Google Cloud Platform** > **Autoscaling**（自動調整規模），檢視已上線的應用程式。僅當您有已上線的應用程式時，才能看到 **Details**（詳細資料）欄。

Firewall Deployment Name	Project ID	Device Group	Template Stack	Details
gcp-asg-fw-peerbrown0	gcp-pavmqa	GCP_ASG_DG_peerbrown0	GCP_ASG_TS_peerbrown0	Show Status Delicense Inactive VMs Trigger GKE Services Sync
hj-nlb-n642wb	gcp-autoscale-host-250622	gcp-autoscale-dg2	gcp-autoscale-ts2	Show Status Delicense Inactive VMs Trigger GKE Services Sync
hj-asg-891ca3	gcp-pavmqa	gcp-autoscale-dg-891ca3	gcp-autoscale-ts-891ca3	Show Status Delicense Inactive VMs Trigger GKE Services Sync
hj-asg-y892bl	gcp-pavmqa	gcp-autoscale-dg-y892bl	gcp-autoscale-ts-y892bl	Show Status Delicense Inactive VMs Trigger GKE Services Sync

[Details（詳細資料）] 欄中的每個連結都會觸發動作。

©2023 Palo Alto Networks, Inc.

- **Show Status**（顯示狀態）— 針對上線到 GCP VM-Series 防火牆部署的應用程式，檢視其詳細資訊。



Application/GKE Service Name	Host Project	Cluster/Namespace	Named Port	ILB IP	ILB Port	Configuration Programmed	Protected	Not Protected Reason
hj-asg-891ca3-app1	gcp-pavmqa	N/A	80	172.22.9.6/32	80	True	True	
web_port1	gcp-pavmqa	hj-gke-891ca3-cluster1/ns1	81	172.22.9.11/32	80	True	True	
web2_port2	gcp-pavmqa	hj-gke-891ca3-cluster1/ns1	82	172.22.9.12/32	81	True	True	

下列欄位顯示從選取的部署取得的資訊。您在發佈/訂閱訊息中或透過 GKE 叢集服務輪詢指定這些值。

- **Application/GKE Service Name**（應用程式/**GKE** 服務名稱）—應用程式部署名稱，或 GKE 服務的名稱。
- **Host Project**（主機專案）—主機專案的名稱。
- **Cluster/Namespace**（叢集/命名空間）—GKE 叢集名稱，後面接著命名空間，例如 **`mycluster/namespace9`**。
- **Named Port**（名稱連接埠）—此連接埠批派給服務的具名連接埠。
- **ILB IP**—ILB IP 位址。
- **ILB Port**（**ILB** 連接埠）—ILB 連接埠號碼。

  關於自動調整應用程式的規模，此屬性是 `apps.yaml` 中的 **`ilb-port`**。

  關於保護 GKE 叢集，此值是 GKE 叢集的連接埠號碼，在您於叢集中部署服務時所使用的 `.yaml` 檔案中指定。
- **Configuration Programmed**（以程式控制設定）—如果 NAT 規則存在，則為 Ture，否則為 False。
- **Protected**（受保護）—應用程式成功上線時為 True，上線失敗時為 False。若為 False，請查看 **Not Protected Reason**（未受保護的原因）欄中的說明。
- **Not Protected Reason**（未受保護的原因）—如果 **Protected**（受保護）為 False，則顯示應用程式未受保護的原因。常見的一些原因如下：
  - **Configuration Programmed**（以程式控制設定）—如果 NAT 規則存在，則為 Ture，否則為 False。
  - **Protected**（受保護）—應用程式成功上線時為 True，上線失敗時為 False。若為 False，請查看 **Not Protected Reason**（未受保護的原因）欄中的說明。
  - **Not Protected Reason**（未受保護的原因）—如果 **Protected**（受保護）為 False，則顯示應用程式未受保護的原因。常見的一些原因如下：
    - 您在 GKE 叢集中部署 UDP 服務。
    - 您指定的具名連接埠已在使用中。只有一個應用程式可以監聽特定的具名連接埠。
    - 由於您選擇 **License management only**（僅限授權管理）選項，因此我們不以程式控制設定。
    - GKE 服務沒有相符的標籤。

©2023 Palo Alto Networks, Inc.

- **Delicense Inactive VMs**（取消授權非作用中 **VM**）—回答 **Yes**（是），對非作用中 VM 觸發取消授權功能。
- 觸發 **GKE** 服務同步—回答 **Yes**（是），以輪詢叢集上執行的服務，必要時以程式控制 NAT、位址、服務物件和靜態路由。根據預設，Panorama 於前一次論詢之後 10 分鐘自動輪詢。

從 *CLI* 檢視部署狀態

您可以使用 Panorama CLI 管理已部署的應用程式。命令列動作與在 GCP 專用 Panorama 外掛程式中檢視已上線的應用程式中所述的動作相同。在下列命令中，**autoscaling_name** 是您在自動調整規模設定中輸入的防火牆部署名稱。

- 列出上線（受保護）的應用程式。

```
show plugins gcp show-protected-apps autoscaling_name <fw-deployment-name>
```

- 對所指定部署中的防火牆觸發取消授權功能。

```
request plugins gcp force-delicensing autoscaling_name <fw-deployment-name>
```

- 對於 GKE 部署，強制外掛程式讀取發佈-訂閱訊息，並同步基於發佈-訂閱訊息而以程式控制的 NAT 規則。

```
request plugins gcp gke-service-discovery autoscaling_name <fw-deployment-name>
```

GCP 專用自動調整規模範本中的參數

您可以從 https://github.com/PaloAltoNetworks/GCP-AutoScaling 下載 `.zip` 檔案。`.zip` 檔案包含目錄來支援網路負載平衡器和應用程式負載平衡器設定的防火牆範本，以及應用程式範本。

範本 YAML 檔案具有下列通用格式：

```
#商標與授權資訊。      :      : 匯入:                          <do not change>
     :      : 資源:      -名稱: vm-series-fw      <do not change>      -類型:vm-series-fw.py    <do not change
    -properties:
    :
    :
outputs:                        <do not change>     :      :
```

在所有 `.yaml` 檔案中，請依照的部署來自訂資源屬性。請勿變更 `imports` 或 `outputs` 區段。

- 防火牆範本
- 應用程式範本

防火牆範本

下列段落詳述 NLB 和 ALB `.yaml` 檔案的參數。

©2023 Palo Alto Networks, Inc.

- vm-series-fw-nlb.yaml
- vm-series-fw-alb.yaml

vm-series-fw-nlb.yaml

在 `vm-series-fw-nlb.yaml` 範本中，編輯 `-properties`。

參數	範例值	備註
地區	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <list of zones>	zones- us-central1-a	如適用，如下列出多個區域： zones- us-central1-a- us-central1-b- us-central1-c- us-central1-f
lb-type	nlb	請勿變更。
cloud-nat	yes	請勿變更。
forwarding-rule-port	80	80 或 8080
urlPath-namedPort-maps-appname	`urlPath-namedPort-maps -MyApplication`	輸入您的應用程式名稱。
sshkey	'admin:ssh-rsa <PASTE KEY>'	檢閱SSH 金鑰配對。以單引號括住來輸入 **admin:** 並緊接一個空格，然後貼到鍵中。這與 Google Marketplace 範本採用的慣例相同。
bootstrap-bucket	bootstrap-autoscale	啟動程序檔案所在 GCP 貯體的名稱。
image	vm-series-byol-814	目前從 Google 市集取得的 BYOL 映像。 如果您使用 PAYG 或其他授權模式，映像可能不同。
machine-type	n1-standard-4	n1-standard-4 是 BYOL 的預設值。 如果授權允許，您可以使用防火牆上的 VM-Series 最低系統需求中的任何電腦類型。

©2023 Palo Alto Networks, Inc.

參數	範例值	備註
service-account		主機專案的唯一服務帳戶名稱。
fw-instance-tag	vm-series-fw	您在 GCP 中提供的實例標籤。
metric	custom.googleapis.com/VMSeries/panSessionActive	VM-Series 的自訂 API 路徑，加上您選擇的自動調整規模度量。 僅限提供下列其中一個度量。 `panSessionActive panSessionUtilization DataPlaneCPUUtilizationPct DataPlanePacketBufferUtilization panSessionUtilization`
max-size	2	
min-size	1	
target-type	GAUGE	目前只有 GAUGE 是有效類型。
util-target	100	
若要部署 VM-Series 防火牆，防火牆的管理、不受信任和信任介面需要有專用的網路和子網路。請填寫綠地部署（設定範本來建立新網路）或棕地部署（使用現有網路）的資訊。務必將您不使用的網路部署參數移除或變成註解。		
綠地部署：輸入值為防火牆建立管理、不受信任及信任網路和子網路。		
mgmt-network-cidr	172.22.2.0/24	
untrust-network-cidr	172.22.1.0/24	
trust-network-cidr	172.22.3.0/24	
mgmt-network-access-source-range- <permitted-ip-range>	`mgmt-network-access-source-range - <permitted-ip-range-1> - <permitted-ip-range-2>`	

©2023 Palo Alto Networks, Inc.

參數	範例值	備註
mgmt-network-access-ports-<port-number>	`mgmt-network-access -ports - 22 - 443`	
棕地部署：輸入每個現有網路或子網路的名稱		
mgmt-network	my-mgmt-network	
mgmt-subnet	my-mgmt-subnet	
trust-network	my-trust-network	
trust-subnet	my-trust-subnet	
untrust-network	my-untrust-network	
untrust-subnet	my-untrust-subnet	

vm-series-fw-alb.yaml

在 `vm-series-fw-alb.yaml` 範本中，編輯 `-properties`。

參數	範例值	備註
地區	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <list of zones>	zones- us-central1-a	如適用，如下列出多個區域： zones- us-central1-a- us-central1-b- us-central1-c- us-central1-f
lb-type	alb	請勿變更。
cloud-nat	yes	請勿變更。
forwarding-rule-port	80	80
connection-draining-timeout	300	逾時值（以秒為單位）。
`urlPath-namedPort-maps: - appname: namedPort: urlMapPaths: - '/app1' - '/app1/*'`	`urlPath-namedPort-maps: - appName: app1 namedPort:80 urlMapPaths: - '/app1' - '/app1/*' - appName: app2`	列出應用程式及對應的具名連接埠

©2023 Palo Alto Networks, Inc.

參數	範例值	備註
	namedPort:81 urlMapPaths: - '/app2' - '/app2/*'	
sshkey	'admin:ssh-rsa <PASTE KEY>'	檢閱SSH 金鑰配對。以單引號括住來輸入 **admin:** 並緊接一個空格，然後貼到鍵中。這與 Google Marketplace 範本採用的慣例相同。
bootstrap-bucket	bootstrap-bucket-name	啟動程序檔案所在 GCP 貯體的名稱。
image	vm-series-byol-814	目前從 Google 市集取得的 BYOL 映像。 如果您使用 PAYG 或其他授權模式，映像可能不同
machine-type	n1-standard-4	n1-standard-4 是 BYOL 的預設值。 如果授權允許，您可以使用防火牆上的 VM-Series 最低系統需求中的任何電腦類型。
service-account	服務專案的唯一服務帳戶名稱。	
fw-instance-tag	vm-series-fw	您在 GCP 中提供的實例標籤。
metric	custom.googleapis.com/VMSeries/panSessionActive	VM-Series 的自訂 API 路徑，加上您選擇的自動調整規模度量。 僅限提供下列其中一個度量。 panSessionActive panSessionUtilization DataPlaneCPUUtilizationPct DataPlanePacketBufferUtilization panSessionUtilization
max-size	2	
min-size	1	

©2023 Palo Alto Networks, Inc.

參數	範例值	備註
target-type	GAUGE	目前只有 GAUGE 是有效類型。
util-target	100	輸入自動調整規模的目標使用率目標值。
綠地部署：輸入值為防火牆建立管理、不受信任及信任網路和子網路。		
mgmt-network-cidr	192.168.12.0/24	
untrust-network-cidr	192.168.11.0/24	
trust-network-cidr	192.168.11.0/24	
mgmt-network-access-source-range- <permitted-ip-range>	`mgmt-network-access-source-range- <permitted-ip-range-1>- <permitted-ip-range-2>`	
mgmt-network-access-ports-<port-number>	`mgmt-network-access-ports- 22- 443`	
棕地部署：輸入每個現有網路或子網路的名稱		
mgmt-network	existing-vpc-mgmt	
mgmt-subnet	existing-subnet-mgmt	
trust-network	existing-vpc-trust	
trust-subnet	existing-subnet-trust	
untrust-network	existing-vpc-untrust	
untrust-subnet	existing-subnet-untrust	

應用程式範本
apps.yaml

此應用程式範本在主機專案（包含 VM-Series 防火牆）與服務專案（包含防火牆部署保護的應用程式或服務）之間建立連線。

參數	範例值	備註
host-project	your-host-project-name	含有 VM-Series 防火牆部署的專案名稱。

©2023 Palo Alto Networks, Inc.

參數	範例值	備註
fw-deployment-name	my-vm-series-firewall-name	
地區	us-central1	https://cloud.google.com/compute/docs/regions-zones
zones - <list of zones>	zones- us-central1-a	如適用，如下列出多個區域： `zones- us-central1-a - us-central1-b- us-central1-c- us-central1-f`
app-machine-type	n1-standard-2	執行應用程式或服務的 VM 電腦類型。如果授權允許，您可以使用防火牆上的 VM-Series 最低系統需求中的任何電腦類型。
app-instance-tag	web-app-vm	您在 GCP 中套用此標籤。
sshkey	'admin:ssh-rsa <PASTE KEY>'	檢閱SSH 金鑰配對。以單引號括住來輸入 **admin:** 並緊接一個空格，然後貼到鍵中。這與 Google Marketplace 範本採用的慣例相同。
trust-network	<project-name>/<vpc-network-name>	若為共用 VPC，<project-name> 是主機項目名稱。 若為對等 VPC，<project-name> 是服務專案名稱。
trust-subnet	<project-name>/<subnet-name>	若為共用 VPC，<project-name> 是主機項目名稱。 若為對等 VPC，<project-name> 是服務專案名稱。
trust-subnet-cidr	10.2.0.0/24	若為綠地部署，指主機專案信任子網路 CIDR（防火牆範本中的 trust-network-cidr 參數）。 若為棕地部署，指信任網路的 CIDR。

©2023 Palo Alto Networks, Inc.

參數	範例值	備註
vm-series-fw-template-topic	<pubsub-topic>	輸入防火牆部署建立的主題名稱。此應用程式範本將訊息張貼到主題，以程式控制防火牆設定來轉送流量。
ilb-port	80	輸入應用程式 internal-load-balancer-port 輸出的連接埠號碼。
urlPath-namedPort	83	輸入 urlPath-namedPort 輸出的連接埠號碼。

範例 GKE 服務範本

這些範例範本示範如何將 GKE 服務設定成由 VM-Series 防火牆保護。關於建立您自己的叢集服務的基本知識，請參閱建立私人叢集。

- 使用範例 GKE 服務範本
- gke_cluster_role.yaml
- gke_cluster_role_binding.yaml
- web-deployment.yaml
- web-service.yaml
- web-deployment-v2.yaml
- web-service-v2.yaml
- 一個服務中多個連接埠

使用範例 **GKE** 服務範本

您可以根據接下來 `.yaml` 檔案中的範例內容建立服務範本。您通常只建立單一 `.yaml` 檔案。

若要將叢集中的服務交由 VM-Series 防火牆保護，必須標示為「panw-named-port=<named_port>」，如 web-service.yaml 或 web-service-v2.yaml 所示。

1. 部署 `.yaml` 檔案，如下所示：

```
kubectl apply -f [FILE_NAME].yaml
```

2. 設定 VPC 部署。
   - 在共用 VPC 部署中，啟動共用 VPC 中的 GKE 叢集，如設定共用 VPC所述。
   - 在對等 VPC 部署中，將 GKE 叢集 VPC 與主機專案信任網路互連。請參閱 設定對等 VPC。

部署之後，您可以刪除服務範本 *`.yaml`* 檔案中部署的所有服務，如下所示：

```
kubectl delete -f [FILE_NAME].yaml
```


©2023 Palo Alto Networks, Inc.

gke_cluster_role.yaml

```
apiVersion: rbac.authorization.k8s.io/v1beta1 kind:ClusterRole
 metadata:   name: gke-plugin-role rules:   - apiGroups:       - ""
     resources:       - services     verbs:       - list
```

gke_cluster_role_binding.yaml

```
kind:ClusterRoleBinding apiVersion: rbac.authorization.k8s.io/
v1beta1 metadata:   name: gke-plugin-role-binding subjects:
   - kind:ServiceAccount     name: hj-gke-891ca3-cluster1-sa
     namespace: default roleRef:   kind:ClusterRole   name: gke-
plugin-role   apiGroup: rbac.authorization.k8s.io
```

web-deployment.yaml

```
apiVersion: extensions/v1beta1 kind:Deployment metadata:   name:
 web   namespace: default spec:   selector:    matchLabels:     run:
 web   template:    metadata:     labels:       run: web    spec:
     containers:     - image: gcr.io/google-samples/hello-app:1.0
       imagePullPolicy:IfNotPresent       name: web       ports:
       - containerPort:8080        protocol:  TCP
```

web-service.yaml

```
apiVersion: v1 kind:服務中繼資料: 名稱: Web 命名空間: 預設註
釋: cloud.google.com/load-balancer-type: "內部"    標籤:     panw-named-
port-port1: “80” 規格:  連接埠:  # 此服務應在其上提供服務的連接埠 - 名稱:
 port1 連接埠: 80     通訊協定:TCP     targetPort:8080 選擇器: 執行:
 Web 型態:LoadBalancer
```

web-deployment-v2.yaml

```
apiVersion: extensions/v1beta1 kind:部署中繼資料:  名稱:  web2 命名空
間:  預設規格:  選擇器:  比對標籤:  執行:  web2 範本:  中繼資料:  標籤:  執
行:  web2 規格:  容器:  - 影像: gcr.io/google-samples/hello-app:2.0
        imagePullPolicy: IfNotPresent        名稱:  web2         連接
埠:          - 容器連接埠: 8080          通訊協定: TCP
```

web-service-v2.yaml

```
apiVersion: v1 kind: 服務中繼資料: 名稱: Web 2 命名空間: 預設註
釋: cloud.google.com/load-balancer-type: "內部"     標籤:       panw-
named-port-port2: "81" 規格:  連接埠:  # 此服務應在其上提供服務的連接埠 - 名
稱:  port2 連接埠: 81     通訊協定: TCP     targetPort: 8080 選擇器:  執行:
 web2 類型: LoadBalancer
```


©2023 Palo Alto Networks, Inc.

一個服務中多個連接埠

如果一個服務中有多個連接埠，請編輯標籤，以 panw-named-port-*<service-spec-port-name>* 格式來對應目標連接埠名稱和號碼，如下列範例所示。

```
apiVersion: v1 kind:服務中繼資料：名稱：購物車    預設註
釋：cloud.google.com/load-balancer-type："內部"    標籤：        panw-
named-port-carts-http："6082"     panw-named-port-carts-https："6083"
   命名空間：預設規格：  類型：負載平衡器連接埠：  # 此服務應在其上服務的埠 - 名
稱：  carts-http 協定：TCP      連接埠：80     targetPort：80    - 名稱：  購
物車-https 通訊協定：TCP     連接埠：443     targetPort：443 選擇器：
     名稱：  購物車
```


©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

在 Cisco ENCS Network 上設定 VM-Series 防火牆

如果您已使用 Cisco 5400 Series Enterprise Network Compute System (ENCS) 設備來虛擬化分公司或遠端辦公室的傳統設備型網路基礎結構，則可以使用 Enterprise NFV Infrastructure Software (NFVIS) 在 Cisco 網路內部署 VM-Series 防火牆。VM-Series 防火牆即具有新世代防火牆功能的虛擬網路功能 (VNF)，可安全地啟用所有應用程式，並保護分公司或遠端辦公室使用者和網路免受威脅。

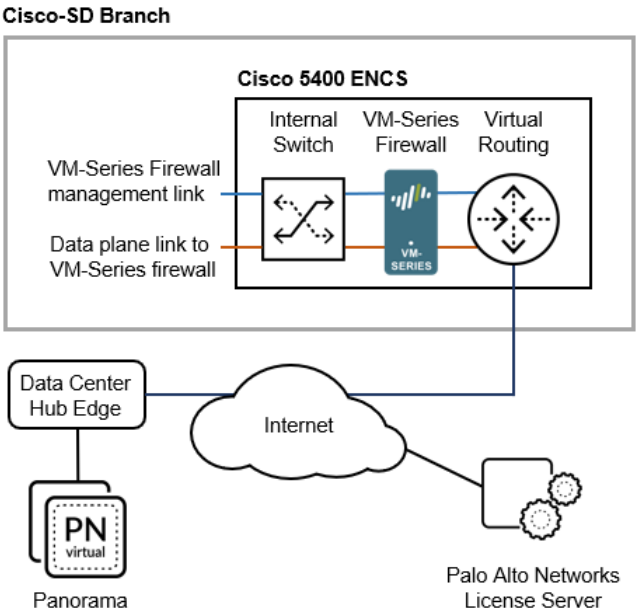
Cisco Enterprise Network Compute System (ENCS) 設備結合 Cisco Integrated Services Virtual Routers (ISRV) 和 NFVIS 軟體，以支援 Software-Defined Branch (SD-Branch) 網路架構。

- 規劃 Cisco ENCS 部署
- 準備 Cisco ENCS 的 VM-Series 防火牆映像
- 在 Cisco ENCS 上部署 VM-Series 防火牆

規劃 Cisco ENCS 部署

在 Cisco SD-Branch 中，將 Cisco ENCS 設備上的 VM-Series 防火牆部署為 VNF，以提供新世代防火牆功能來保護分公司的應用程式和使用者。您可以使用虛擬介接、第 2 層或第 3 層部署以及高可用性設定來部署防火牆。

若要管理 VM-Series 防火牆，可以在內部部署或雲端中部署 Panorama 設備。下列拓撲顯示分公司邊緣的 VM-Series 防火牆。



Cisco ENCS 需求

若要瞭解支援的 NFVIS 版本和硬體平台，請參閱 Palo Alto Networks 相容性矩陣。

- 在 NFVIS 中，設定網路和橋接器。
  - 建立虛擬 NIC，並將它們連接至虛擬橋接器，讓 ENCS 設備可以透過 VM-Series 防火牆導向流量。

    在 Cisco ENCS 設備上，VM-Series 防火牆最多支援 8 個資料平面介面。

    Cisco ENCS 上 *VM-Series* 防火牆的資料平面介面僅支援 *Virtio* 模式；不支援 *ENCS SR-IOV* 和 *PCI* 通道模式。
  - 設定進行 VM-Series 防火牆管理存取的網路連線。如果您使用 Panorama，請確定 Panorama 具有管理所部署防火牆的網路存取權。
- Python 2.7。如果您使用命令行進行轉換，則在本機機器上為必要項目。

©2023 Palo Alto Networks, Inc.

VM-Series 防火牆和 **Panorama** 需求

- VM-Series 防火牆—建議使用 VM-50 和 VM-100。也支援 VM-300、VM-500 和 VM-700，但前提是 ENCS 硬體具有可指派給 VM-Series 防火牆的足夠資源。請參閱VM-Series 系統需求，確定 Cisco ENCS 設備具有足夠的資源可以支援您選擇的 VM-Series 型號。
  - PAN-OS 9.1 或更新版本的 qcow2 檔案（VM-Series KVM 專用 PAN-OS 基礎映像）。請參閱從圖形使用者介面轉換 qcow2 檔案，步驟 2 或從命令行介面轉換 qcow2 檔案，步驟 2。
  - 符合您需求的 VM-Series 防火牆容量授權和訂閱授權碼。請參閱 VM-Series 型號授權類型。您在 NFVIS 使用者介面中輸入授權碼，或在轉換資料夾的 **authcodes** 文字檔案中包括授權碼，如從命令行介面轉換 qcow2 檔案的步驟 4 所述。
  - 透過 PAN-OS 9.1，Cisco ENCS 上的 VM-Series 防火牆可支援依預設啟用 DPDK 模式的 Virtio。
- Panorama 硬體或虛擬設備。雖然您可以在 Cisco SD-Branch 網路中部署單一 VM-Series 防火牆，但較常見的做法是在多個分公司中部署防火牆，並使用 Panorama 集中管理它們。
  - Panorama 9.1 版或更新版本。版本必須等於或高於您 VM-Series 防火牆上的版本。
  - Panorama 上產生的 VM 授權金鑰。此金鑰允許 VM-Series 防火牆向 Panorama 驗證。

©2023 Palo Alto Networks, Inc.

準備 Cisco ENCS 的 VM-Series 防火牆映像

您可以從 NFVIS 圖形使用者介面或命令行介面轉換 PAN-OS qcow2 檔案。

- 從圖形使用者介面轉換 qcow2 檔案
- 從命令行介面轉換 qcow2 檔案

從圖形使用者介面轉換 qcow2 檔案

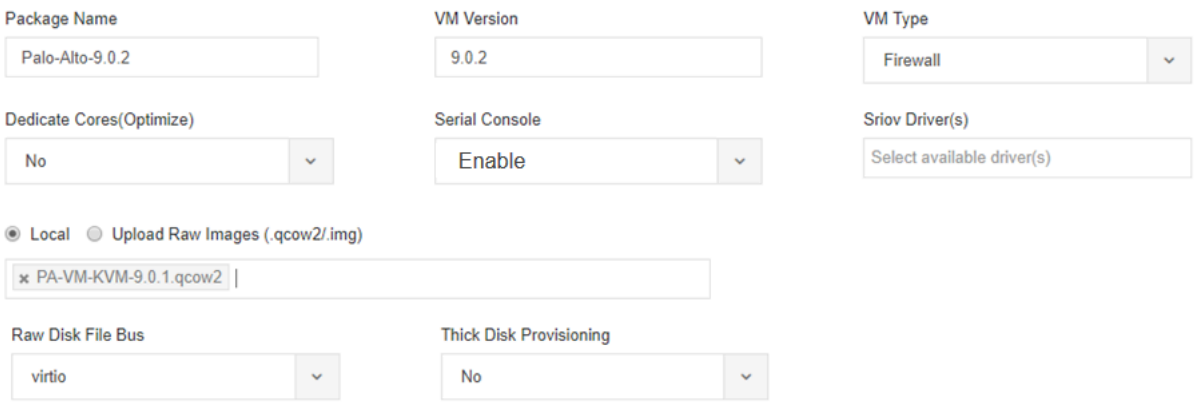
使用 NFVIS 圖形使用者介面來輸入映像包裝和啟動程序資訊。

STEP 1 | 在 NFVIS 中，移至 **VM Life Cycle**（**VM** 生命週期） > **Image Repository**（映像儲存庫） > **Image Packaging**（映像包裝）。

STEP 2 | 填寫套件資訊，如下所示，並提供您自己的值。

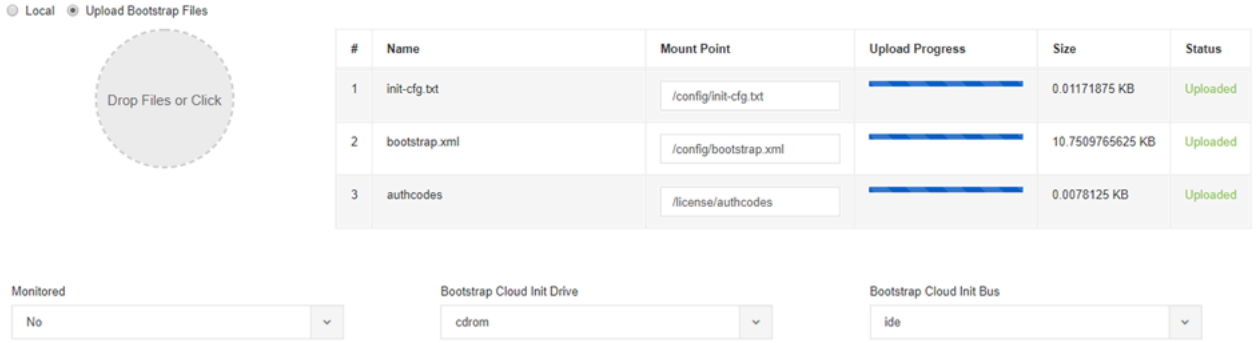
1. 輸入 **Package Name**（套件名稱）和 **VM Version**（**VM** 版本），並針對 **VM Type**（**VM** 類型）選擇 **Firewall**（防火牆）。
2. **Enable**（啟用） **Serial Console**（序列主控台）。
3. 將 **Sriov Driver(s)**（**Sriov** 驅動程式）欄位空白，因為不支援 SR-IOV。
4. 選取 **Local**（本機）以選擇您先前上傳的 qcow2 檔案，或按一下 **Upload Raw Images**（上傳原始映像）以上傳 qcow2 檔案。
   - 登入 Palo Alto Networks 客戶支援入口網站。

     如果您尚未這麼做，請建立支援帳戶並註冊 VM-Series 防火牆。
   - 選取 **Support**（支援） > **Software Updates**（軟體更新），並從 **Filter By**（篩選依據）下拉式清單中選取 **Pan OS for VM-Series KVM Base Image**（**VM-Series KVM** 專用 **Pan OS** 基礎映像），例如 9.1 版。
   - 下載 qcow2 映像。

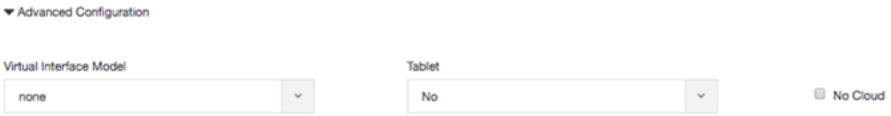


©2023 Palo Alto Networks, Inc.

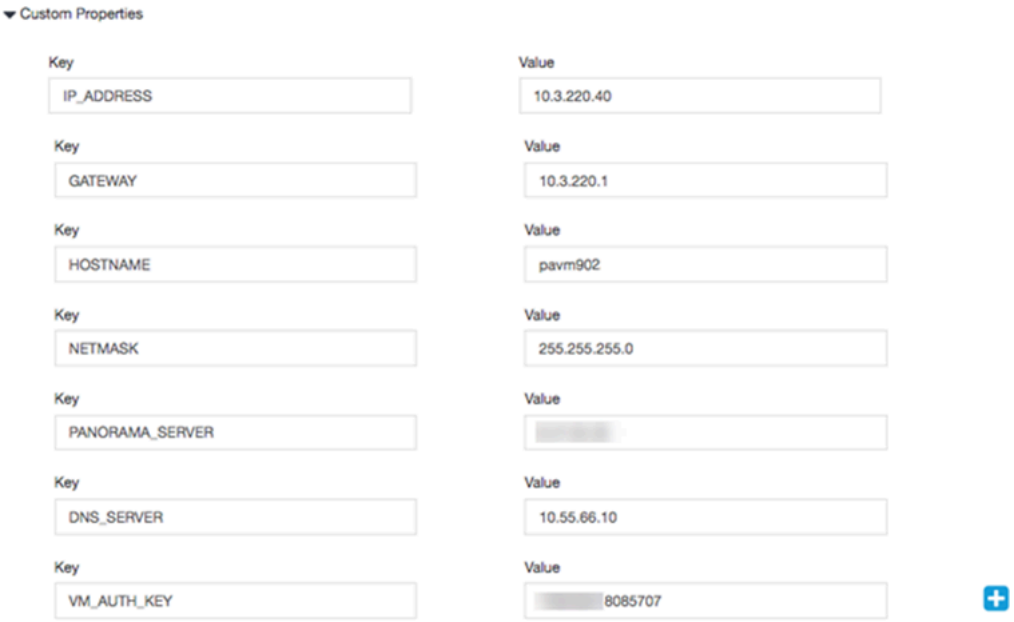
STEP 3 | 上傳啟動程序檔案。



STEP 4 | 設定 **Advanced Configuration**（進階設定）。



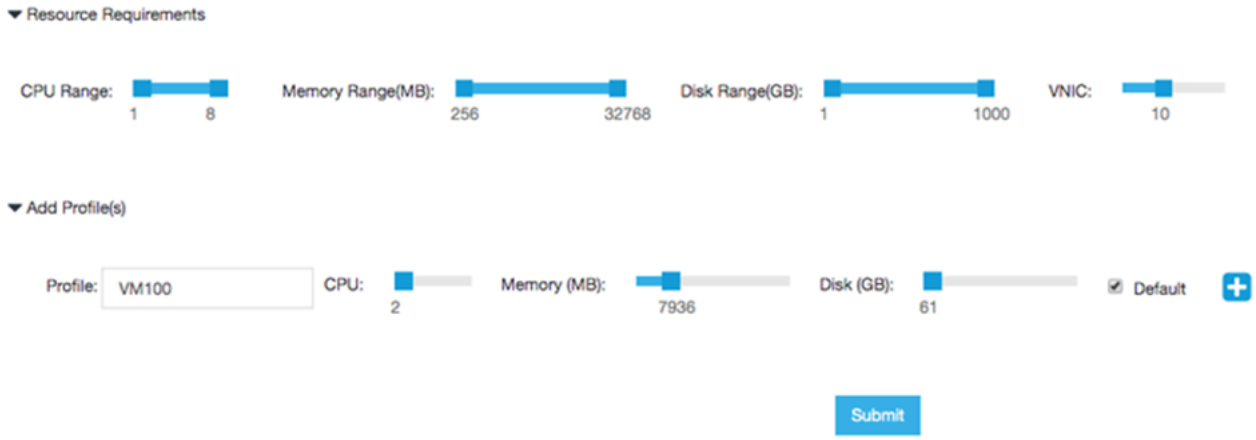
STEP 5 | 輸入 **Custom Properties**（自訂屬性）的值。



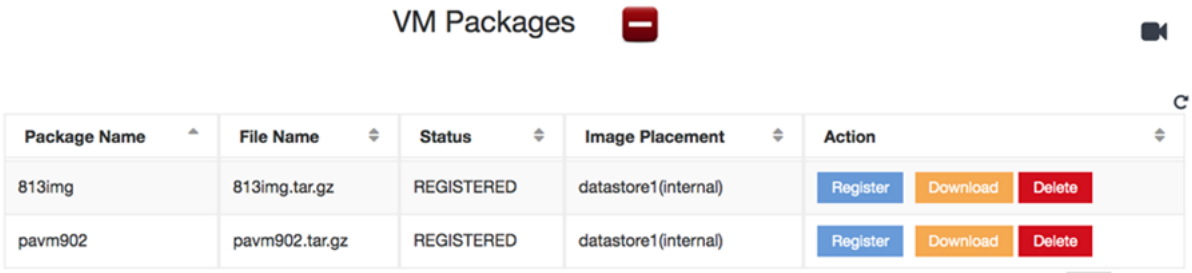
©2023 Palo Alto Networks, Inc.

STEP 6 | 設定資源需求的值，並選擇預設設定檔，或新增目前設定的設定檔。

按一下 **Submit**（提交），以儲存套件。



STEP 7 | 按一下 **Register**（註冊），以註冊新映像。



從命令行介面轉換 qcow2 檔案

若要從命令行介面建立啟動程序檔案，請建立檔案 `image_properties_template.xml`，然後使用 VM 映像包裝公用程式來建立 `.tar` 檔案，而使用 `nfvpt.py` 指令碼可以轉換此檔案。輸出為可從 NFVIS 使用者介面上傳的 `tar.gz` 檔案。

STEP 1 | 建立或選擇本機機器上的資料夾（轉換資料夾），而在其中，您想要下載和儲存將 VM-Series 防火牆 qcow2 映像轉換為 Cisco ENCS 格式所需的檔案。

STEP 2 | 取得 VM-Series 防火牆 qcow2 映像。

1. 登入 Palo Alto Networks 客戶支援入口網站。

   如果您尚未這麼做，請建立支援帳戶並註冊 VM-Series 防火牆。
2. 選取 **Support**（支援） > **Software Updates**（軟體更新），並從 **Filter By**（篩選依據）下拉式清單中選取 **Pan OS for VM-Series KVM Base Image**（**VM-Series KVM** 專用 **Pan OS** 基礎映像），例如 9.1 版。
3. 將 qcow2 映像下載至轉換資料夾。

STEP 3 | 在轉換資料夾中，建立下列 init-cfg.txt 檔案。

```
type=static ip-address=${IP_ADDRESS} default-gateway=${GATEWAY}
 netmask=${NETMASK} ipv6-address=  ipv6-default-gateway=
```


©2023 Palo Alto Networks, Inc.

```
 hostname=${HOSTNAME} vm-auth-key=${VM_AUTH_KEY} panorama-server=
${PANORAMA_SERVER} panorama-server-2=  tplname=  dgname=  dns-
primary=${DNS_SERVER} dns-secondary=  op-command-modes=jumbo-
frame, mgmt-interface-swap** dhcp-send-hostname=yes dhcp-send-
client-id=yes dhcp-accept-server-hostname=yes dhcp-accept-server-
domain=yes
```

STEP 4 | 建立名為 `authcodes`（無副檔名）的文字檔案，並輸入 VM-Series 防火牆容量和訂閱的授權碼。在轉換資料夾中儲存檔案。

STEP 5 | 在轉換資料夾中建立下列 `image_properties_template.xml` 檔案，並提供部署的值：

```
<image_properties> <vnf_type>FIREWALL</vnf_type>
 <name>pafw</name> <version>9.1.0</version> <bootup_time>-1</
bootup_time> <root_file_disk_bus>virtio</root_file_disk_bus>
 <root_image_disk_format>qcow2</root_image_disk_format>
 <vcpu_min>2</vcpu_min> <vcpu_max>8</vcpu_max>
 <memory_mb_min>4096</memory_mb_min> <memory_mb_max>16384</
memory_mb_max> <vnic_max>8</vnic_max> <root_disk_gb_min>32</
root_disk_gb_min> <root_disk_gb_max>60</root_disk_gb_max>
 <console_type_serial>true</console_type_serial>
 <sriov_supported>true</sriov_supported> <pcie_supported>false</
pcie_supported> <monitoring_supported>false</monitoring_supported>
 <monitoring_methods>ICMPPing</monitoring_methods>
 <low_latency>true</low_latency> <privileged_vm>true</
privileged_vm> <custom_property> <HOSTNAME> </HOSTNAME> </
custom_property> <custom_property> <IP_ADDRESS> </IP_ADDRESS>
 </custom_property> <custom_property> <NETMASK> </NETMASK>
 </custom_property> <custom_property> <GATEWAY> </GATEWAY>
 </custom_property> <custom_property> <PANORAMA_SERVER> </
PANORAMA_SERVER> </custom_property> <custom_property> <DNS_SERVER>
 </DNS_SERVER> </custom_property> <custom_property> <VM_AUTH_KEY>
 </VM_AUTH_KEY> </custom_property> <default_profile>VM-50</
default_profile> <profiles> <profile> <name>VM-50</name>
 <description>VM-50 profile</description> <vcpus>2</
vcpus> <memory_mb>5120</memory_mb> <root_disk_mb>60000</
root_disk_mb> </profile> <profile> <name>VM-100-n-200</name>
 <description>VM-100 and VM-200 profile</description> <vcpus>2</
vcpus> <memory_mb>7168</memory_mb> <root_disk_mb>60000</
root_disk_mb> </profile> <profile> <name>VM-300</name>
 <description>VM-300 profile</description> <vcpus>2</vcpus>
 <memory_mb>9216</memory_mb> <root_disk_mb>60000</root_disk_mb> </
profile> <profile> <name>VM-1000-HV</name> <description>VM-1000-
HV profile</description> <vcpus>4</vcpus> <memory_mb>9216</
memory_mb> <root_disk_mb>60000</root_disk_mb> </profile>
 <profile> <name>VM-500</name> <description>VM-500 profile</
description> <vcpus>4</vcpus> <memory_mb>16384</memory_mb>
 <root_disk_mb>60000</root_disk_mb> </profile> </profiles>
 <cdrom>true</cdrom> <bootstrap_file_1>/config/init-cfg.txt</
bootstrap_file_1> <bootstrap_file_2>/config/bootstrap.xml</
bootstrap_file_2> <bootstrap_file_3>/license/authcodes</
bootstrap_file_3> </image_properties>
```


©2023 Palo Alto Networks, Inc.

STEP 6 | 下載映像包裝公用程式。

1. 登入 Enterprise NFVIS 使用者介面，並選取 **VM Life Cycle**（**VM** 生命週期） > **Image Repository**（映像儲存庫）。
2. 按一下 **Browse Datastore**（瀏覽資料存放）頁籤，並導覽至 **data**（資料） > **intdatastore** > **uploads**（上傳） > **vmpackagingutility**。
3. 將 `nfvisvmpackagingtool.tar` 下載至轉換資料夾。
4. 將檔案解壓縮：

```
tar -xvf nfvisvmpackagingtool.tar
```

STEP 7 | 在包含 qcow2、`init-config.txt` 和 `authcodes` 檔案的轉換資料夾中，執行 `nfvpt.py` 指令碼。請參閱 `nfvpt.py` 映像包裝公用程式文件。

下列範例會建立映像檔案 Palo-Alto-9.1.0 和 VM-100 設定檔。選項是以空格區隔（此範例將選項顯示在單獨一行，只是為了方便查看），而自訂選項是具有冒號分隔符號的鍵值配對。

```
./nfvpt.py -o Palo-Alto-9.1.0 -i PA-VM-KVM-9.1.0.qcow2 -n
 PAN902 -t FIREWALL -r 9.1.0 --monitored false --privileged
 true --bootstrap /config/init-cfg.txt:init-cfg.txt,/license/
authcodes:authcodes --min_vcpu 2 --max_vcpu 8 --min_mem 4096
 --max_mem 16384 --min_disk 10 --max_disk 70 --vnic_max 8 --
optimize true --console_type_serial true --profile VM-100,"VM-100
 profile",2,7168,61440 --default_profile VM-100 --custom
 HOSTNAME:hello --custom IP_ADDRESS:10.2.218.24 --custom
 NETMASK:255.255.255.0 --custom GATEWAY:10.2.218.1 --custom
 DNS_SERVER:10.55.66.10 --custom PANORAMA_SERVER:0.10.10.0 --custom
 VM_AUTH_KEY:123451234512345
```

STEP 8 | 上傳已轉換的映像。

1. 在 NFVIS 使用者介面中，選取 **VM Life Cycle**（**VM** 生命週期） > **Image Repository**（映像儲存庫），然後按一下藍色 Images（映像）圖示來顯示 **Drop Files or Click**（丟棄檔案或按一下）圓圈。
2. 將已轉換的檔案拖曳至該圓圈，或按一下以瀏覽並選取檔案。
3. 在 [Status（狀態）] 欄中，按一下 **Start**（開始）。

   上傳完成時，會註冊映像，而且您上傳的檔案會顯示在 **Image Registration**（映像註冊）頁籤的 **Images**（映像）清單中。

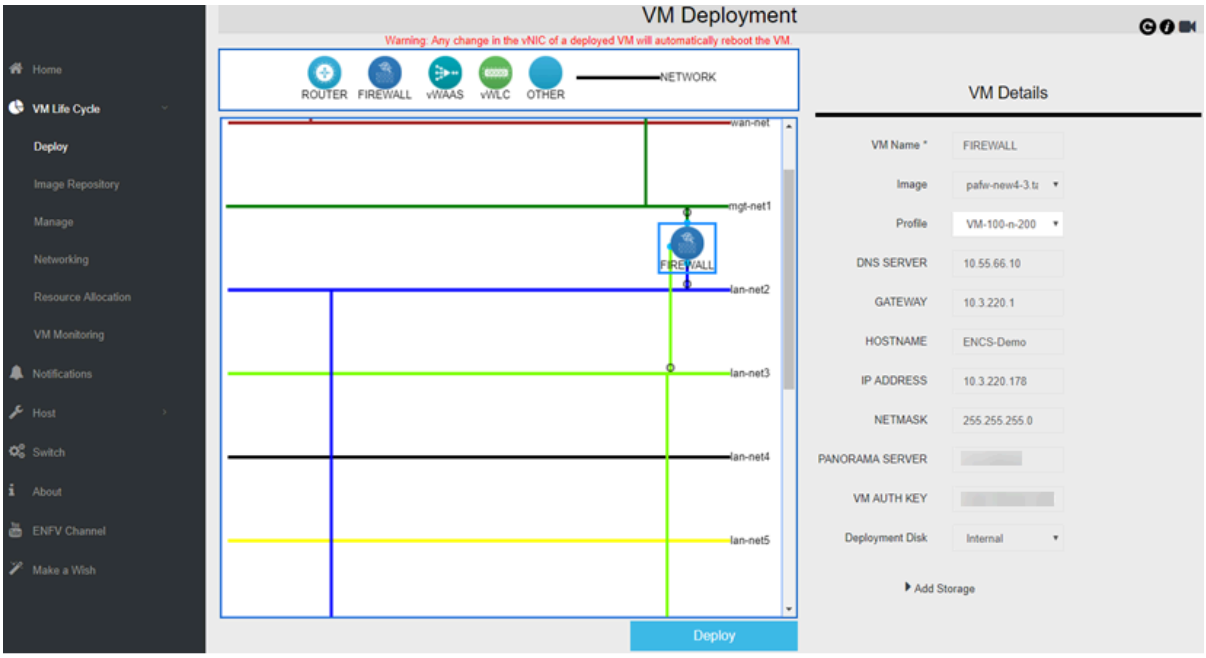
©2023 Palo Alto Networks, Inc.

在 Cisco ENCS 上部署 VM-Series 防火牆

開始部署防火牆之前，請確定您已建立網路連線來管理 VM-Series 防火牆的存取權。如果您要使用 Panorama，請確定 Panorama 具有防火牆的管理連線。

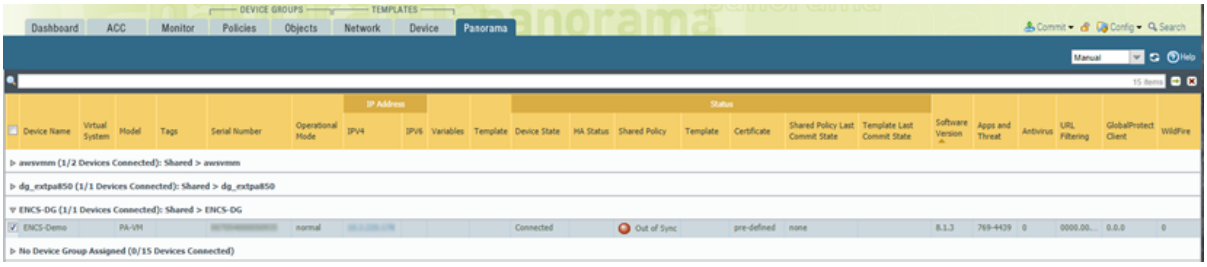
STEP 1 | 部署 VM-Series 防火牆。

1. 在 Enterprise NFVIS 中，按一下 **VM Life Cycle**（**VM** 生命週期） > **Deploy**（部署）。
2. 將防火牆圖示拖曳至適當的網路。在此範例中，防火牆會連線至管理網路和 LAN 網路。



3. **Deploy**（部署）VM-Series 防火牆。

   如果您要使用 Panorama 來管理防火牆，則在 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要） 上，防火牆會顯示為 **Connected**（已連線）。如果防火牆未連線至 Panorama，則請確認您已提供正確的 Panorama IP 位址，而且裝置可以透過網路進行通訊。

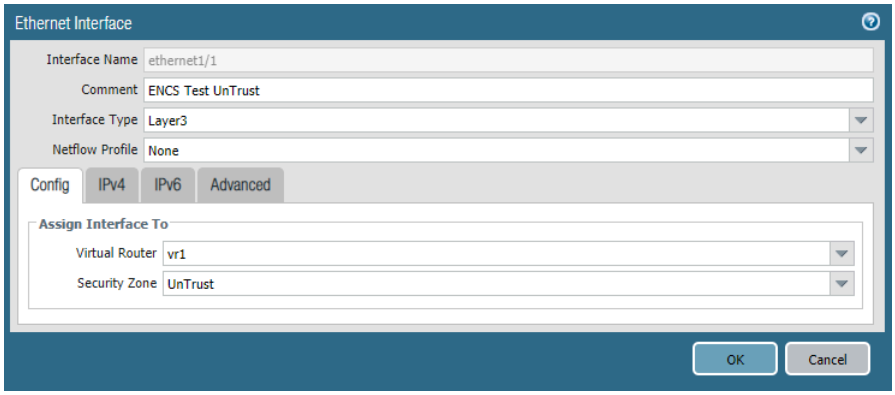


 ©2023 Palo Alto Networks, Inc.

STEP 2 | 設定 VM-Series 防火牆資料平面介面。

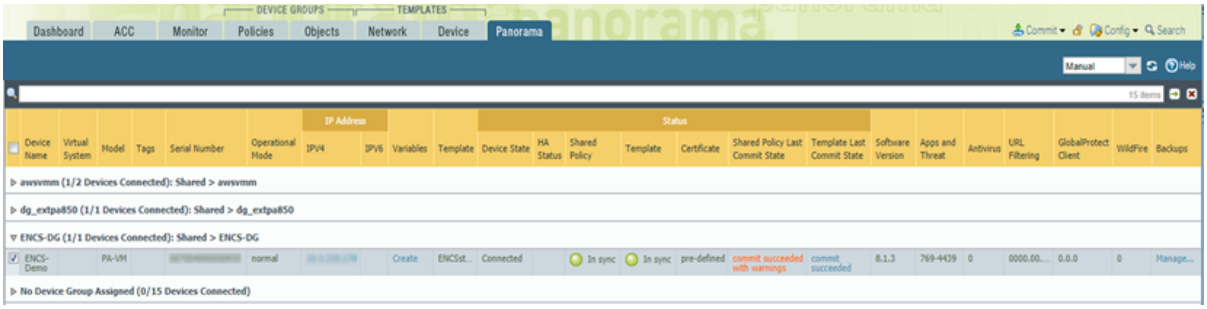
請參閱設定第 3 層介面、設定第 2 層介面或設定虛擬介接。如果使用 Panorama，則下列步驟會顯示如何設定第 3 層部署的防火牆。

1. 新增範本並將防火牆指派給範本。
2. 選取 **Network**（網路），並在 [Template（範本）] 下拉式清單中選取您已建立的範本。
3. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）。
4. 按一下 **ethernet 1/1**，然後依照以下所述設定：
   - 將 **Interface Type**（介面類型）設定為 **Layer3**。
   - 在 **Config**（設定）頁籤上，將介面指派給預設路由器。
   - 另，在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。例如，定義稱為 **UnTrust** 的新區域，然後按一下 **OK**（確定）。
   - 在 **IPv4** 頁籤上，選取 **DHCP Client**（**DHCP** 用戶端）或 **Static**（靜態）。如果您選擇 static（靜態），則請輸入 IP 位址。



5. 針對每個網路介面，重複 b-e。
6. **Commit**（認可） > **Commit and Push**（認可並推送），以將所有設定變更認可到 Panorama 和受管理防火牆。

   確認防火牆介面的連結狀態為啟動。

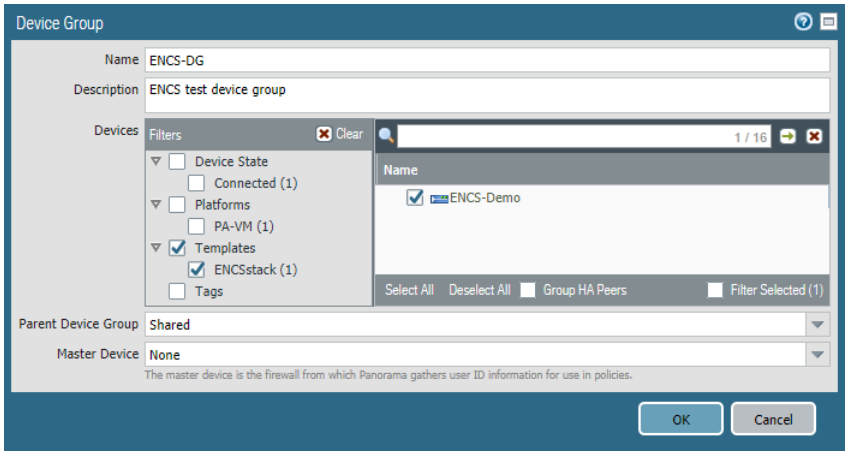


 ©2023 Palo Alto Networks, Inc.

STEP 3 | 設定安全性政策，以在網路上安全地啟用應用程式和使用者。

如果使用 Panorama，則下列步驟會顯示如何使用裝置群組來集中管理受管理防火牆的政策規則。

1. 新增裝置群組，並將受管理防火牆指派給裝置群組。



2. 設定裝置群組的安全性政策。

STEP 4 | 確認 VM-Series 防火牆正在保護網路上的流量。

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

在 Oracle Cloud Infrastructure 上設定 VM-Series 防火牆

在 Oracle Cloud Infrastructure (OCI) 雲端上部署 VM-Series 防火牆。使用 OCI 上的 VM-Series，您可以保護和細分工作負載來防止進階威脅，以及改善應用程式在您移至雲端時的可見度。

OCI 是一種公共雲端計算服務，可讓您在 Oracle 所提供的高可用性託管環境中執行應用程式。您可以部署 VM-Series 防火牆來保護執行 OCI 環境的應用程式和服務。

- OCI 形狀類型
- OCI 上支援的部署
- 準備在 OCI 上設定 VM-Series 防火牆
- 從 Oracle Cloud Marketplace 部署 VM-Series 防火牆
- 在 OCI 上設定主動/被動 HA

OCI 形狀類型

VM-Series 防火牆支援下列 OCI VM 形狀。如需 VM 形狀的詳細資訊，請參閱 Oracle Cloud Infrastructure 文件。

VM-Series 型號	最低 OCI 形狀
• VM-100 • 軟體 NGFW 積分型 VM-Series	VM.Standard2.4
• VM-300 • 軟體 NGFW 積分型 VM-Series	VM.Standard2.4
• VM-500 • 軟體 NGFW 積分型 VM-Series	VM.Standard2.8
• VM-700 • 軟體 NGFW 積分型 VM-Series	VM.Standard2.16
• VM-100、VM-300、VM-500 和 VM-700 • 軟體 NGFW 積分型 VM-Series	VM.Optimized3.Flex

您可以在資源高於最低 VM-Series 系統需求 的 OCI 實例上部署 VM-Series 防火牆。如果您為 VM-Series 防火牆型號選擇較大的形狀大小。雖然防火牆只會使用系統需求頁面上列出的最大 vCPUs 核心和記憶體，但是確實會利用較大形狀所提供的更快速網路效能。

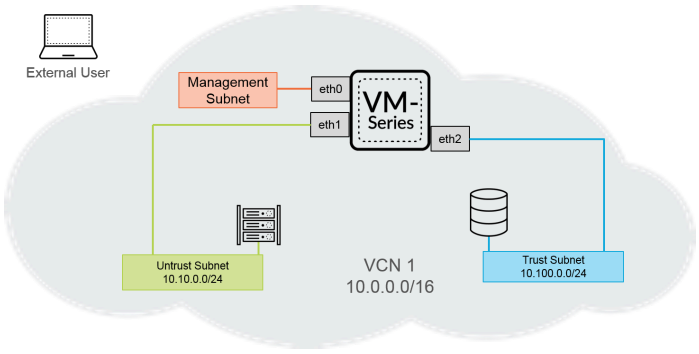
©2023 Palo Alto Networks, Inc.

OCI 上支援的部署

在下列情況下，使用 OCI 上的 VM-Series 防火牆來保護雲端環境：

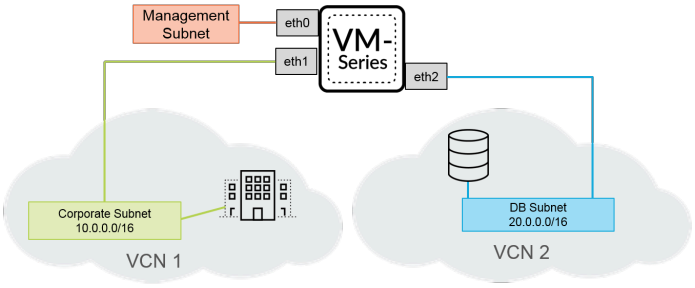
- 南北向流量—您可以使用 VM-Series 防火牆來保護來自不受信任來源且進入您雲端網路的流量，或離開您雲端網路以到達不受信任來源的流量。對任一種類型的流量，您都必須在防火牆的虛擬雲端網路 (VCN) 和 NAT 原則規則中設定路由表規則。

  在此範例中，輸出流量會離開您 VCN 中的信任子網路。您必須設定轉譯為公共 IP 位址的來源位址轉譯政策，以及將該流量重新導向至防火牆的路由表規則。路由規則會將傳出流量指向 VCN 信任子網路中防火牆的介面。防火牆接收此流量時，會對流量執行來源位址轉譯，並套用您已設定的任何其他安全性政策。



- VCN 間流量（東西向）— VM-Series 防火牆可讓您保護雲端環境內在 VCN 之間移動的流量。每個子網路都必須屬於不同的 VCN，因為依預設不會使用路由規則來啟用 VCN 內的流量。在此情況下，您將在連線至每個 VCN 中子網路的防火牆上設定介面。

  在下面範例中，信任子網路中的使用者想要存取 DB 子網路中的資料。在 OCI 上設定可到達 DB 子網路 CIDR 下一個躍點的路由，而此躍點指向 VM-Series 防火牆上的介面信任子網路。



如需詳細資訊，請參閱 使用彈性網路的 Palo Alto Networks VM-Series 防火牆保護工作負載。

©2023 Palo Alto Networks, Inc.

準備在 OCI 上設定 VM-Series 防火牆

進行在 Oracle Cloud Infrastructure 上部署 VM-Series 防火牆的程序時，必須完成準備工作。

- 虛擬雲端網路
- SSH 金鑰
- 初始設定使用者資料

虛擬雲端網路

虛擬雲端網路 (VCN) 是您在 OCI 環境中設定的虛擬私人網路。若要在 OCI 中部署 VM-Series 防火牆，您的 VCN 至少必須要有三張虛擬網路介面卡 (VNIC)，供管理介面和兩個資料介面使用。

OCI 使用一系列的路由表將流量送出 VCN，並為每個子網路新增一個路由表。子網路是您 VCN 的分區。若未指定路由表，子網路將會使用 VCN 的預設路由表。針對任何符合 CIDR 的流量，每個路由表規則都會指定一個目的地 CIDR 區塊和下一個躍點（目標）。只有在目的地 IP 位址位在 VCN 的指定 CIDR 區塊外部時，OCI 才會使用子網路的路由表；不需要路由規則，即可啟用 VCN 內的流量。而且，如果流量具有重疊規則，則 OCI 會使用路由表中的最特定規則來路由流量。

如果沒有路由規則符合將嘗試離開 ***VCN*** 的流量，則會丟棄流量。

每個子網路都需要一個路由表，而且您將路由表新增至子網路之後，就無法變更路由表。不過，在建立路由表之後，您可以新增、移除或編輯其中的規則。

SSH 金鑰

在首次登入防火牆時，您必須建立 SSH 金鑰配對。首次登入時，您無法使用預設使用者名稱和密碼存取防火牆。在防火牆首次啟動後，您必須透過 CLI 存取防火牆，並建立新的使用者名稱和密碼。

1. 建立 SSH 金鑰配對，並將該 SSH 金鑰配對儲存於作業系統的預設位置。
   - 在 Linux 或 MacOS 上，使用 `ssh-keygen` 在 .ssh 目錄中建立金鑰配對。
   - 在 Windows 上，使用 PuTTYgen 建立金鑰配對。

     Key comment（金鑰註解）欄位的內容不影響 VM-Series 防火牆；您可以接受預設值（金鑰建立日期）或輸入有助於您記住金鑰配對名稱的註解。使用 **Save private key**（儲存私密金鑰）按鈕在 .ssh 目錄中儲存私密金鑰。

©2023 Palo Alto Networks, Inc.

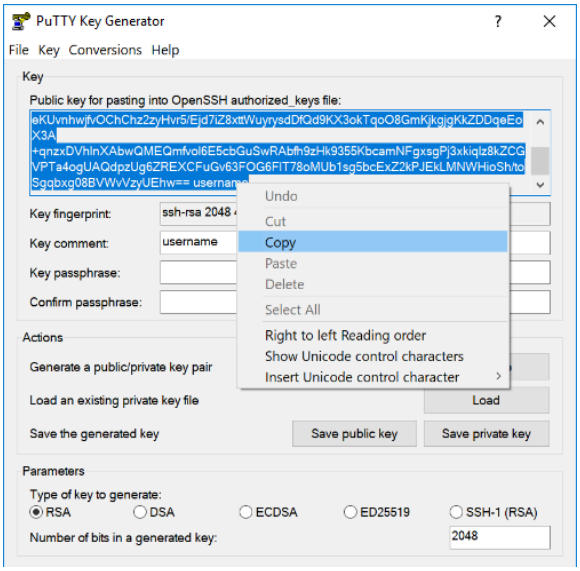
2. 選取完整的公共金鑰。

   - Linux or MacOS:（Linux 或 MacOS：）

     在文字編輯器中開啟您的公共金鑰並複製該公共金鑰。

   - Windows：您必須使用 PuTTY 金鑰產生器來檢視公共金鑰。啟動 PuTTYgen，按一下「載入」，並瀏覽儲存於 .ssh 目錄中的私密金鑰。

     在 PuTTYgen 中，向下捲動以確保選取整個金鑰，按一下滑鼠右鍵，並選取「複製」。



初始設定使用者資料

在設定 VM-Series 防火牆實例時，您必須提供下列啟動載入參數。OCI 會使用這項資訊執行防火牆的初始設定，對防火牆提供主機名稱和授權，並將防火牆連線至 Panorama（如果適用）。

如果您具有 ***Panorama*** 設備，且想要使用 ***Panorama*** 來管理 ***VM-Series*** 防火牆，才需要使用 ***Panorama*** 相關欄位。

欄位	說明
hostname=	防火牆的主機名稱。
vm-auth-key=	用來將防火牆註冊至 Panorama 的虛擬機器驗證金鑰。
panorama-server=	主要 Panorama 伺服器的 IPv4 或 IPv6 位址。這不是必要欄位，但為了集中管理防火牆，仍建議指定。
panorama-server-2=	次要 Panorama 伺服器的 IPv4 或 IPv6 位址。此欄位非必填但建議。

©2023 Palo Alto Networks, Inc.

欄位	說明
tplname=	Panorama 範本堆疊名稱。如果您新增 Panorama 伺服器 IP 位址，最佳作法是在 Panorama 上將防火牆指定給範本堆疊，並在此欄位中輸入範本堆疊名稱，如此就能集中管理組態設定並推送至防火牆。
dgname=	Panorama 裝置群組名稱。如果您新增 Panorama 伺服器 IP 位址，最佳作法是在 Panorama 上建立裝置群組，並在此欄位中輸入裝置群組名稱，如此就能分乎邏輯地分組防火牆，並將原則規則推送至防火牆。
authcodes=	用來透過 Palo Alto Networks 授權伺服器為 VM-Series 防火牆授權。
op-command-modes=jumbo-frame	用來在 VM-Series 防火牆上啟用 Jumbo Frame 模式。由於 OCI 依預設會以 Jumbo 模式部署 VM 實例，建議您以 Jumbo 模式啟動 VM-Series 防火牆，以達到最理想的輸送量。

以下列格式將啟動載入參數貼到 OCI 主控台中。

hostname=<*fw-hostname*>

vm-auth-key=<*auth-key*>

panorama-server=<*panorama-ip*>

panorama-server-2=<*panorama2-ip*>

tplname=<*template-stack-name*>

dgname=<*device-group-name*>

authocodes=<*firewall-authcode*>

op-command-modes=jumbo-frame

©2023 Palo Alto Networks, Inc.

從 Oracle Cloud Marketplace 部署 VM-Series 防火牆

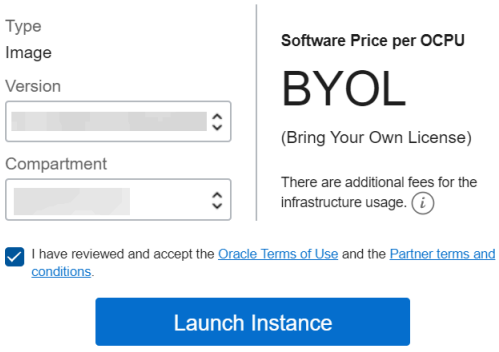
完成下列程序，以從 Oracle Cloud Marketplace 部署 OCI 中的 VM-Series 防火牆。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 登入 Oracle Cloud Marketplace。

STEP 2 | 在 Oracle Cloud Marketplace 中找出 VM-Series 防火牆應用程式。

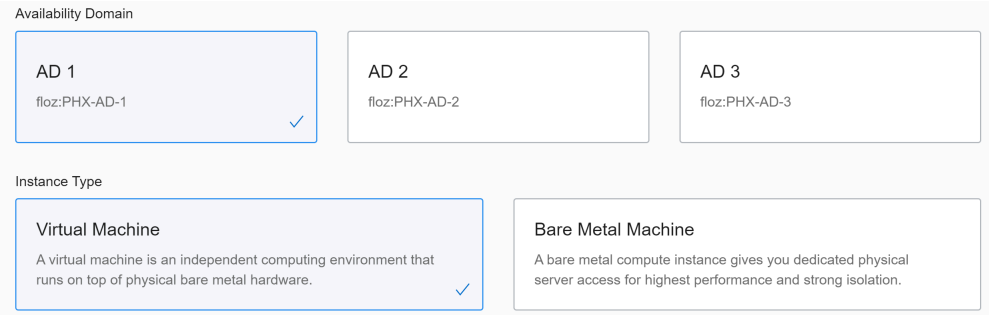
1. 搜尋 Palo Alto Networks，VM-Series 防火牆產品清單即會顯示。
2. 選取供應項目。
3. 按一下 **Get App**（取得應用程式）。
4. 選取您的 **Region**（區域），然後按一下 **Sign In**（登入）。
5. 選取 **Version**（版本）和 **Compartment**（區間）。
6. 接受 Oracle 和合作夥伴條款。
7. 按一下 **Launch Instance**（啟動實例）。



STEP 3 | 輸入 VM-Series 防火牆實例的描述性 **Name**（名稱）。

STEP 4 | 選取 **Availability Domain**（可用性網域）。

STEP 5 | 選取 **Shape Type**（形狀類型）下方的 **Virtual Machine**（虛擬機器）。



©2023 Palo Alto Networks, Inc.

STEP 6 | 選取形狀，其具有 VM-Series 防火牆型號所需的 CPU 數目、RAM 數量和介面數目。如需不同計算形狀所提供的資源數量，請參閱計算形狀頁面。如需每個 VM-Series 防火牆型號所需資源的詳細資訊，請參閱，請參閱VM-Series 系統需求。



STEP 7 | 在 [Networking（網路）] 下方，選取管理介面的 **Virtual cloud network compartment**（虛擬雲端網路區間）、**Virtual cloud network**（虛擬雲端網路）、**Subnet compartment**（子網路區間）和 **Subnet**（子網路）。您在建立 VM-Series 防火牆實例時只能新增一個介面。您可以在稍後新增其他介面。

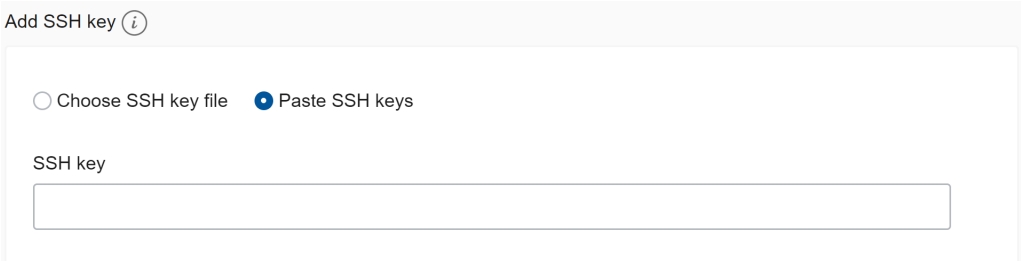


STEP 8 | （選用）將開機磁碟區設定為大於預設值的大小。開機磁碟區會預設為 60 GB。如果您需要更大的開機磁碟區來支援連接日誌之類的功能，請完成下列程序。

1. 選取 **Custom boot volume size (in GB)**（自訂開機磁碟區大小（以 **GB** 為單位））。
2. 輸入 60 或更大的值。60 GB 是 VM-Series 防火牆所需的最小硬碟大小。

STEP 9 | 新增您的 SSH 金鑰。

1. 在 **Add SSH Key**（新增 **SSH** 金鑰）底下，選取 **Paste SSH Key**（貼上 **SSH** 金鑰）。
2. 將您的 SSH 金鑰貼到提供的欄位中。



 ©2023 Palo Alto Networks, Inc.

STEP 10 | 新增啟動載入參數。

1. 按一下 **Show Advanced Options**（顯示進階選項）。
2. 在 **User data**（使用者資料）底下，選取 **Paste cloud-init script**（貼上 **cloud-init** 指令碼）。
3. 將啟動載入參數貼到提供的欄位中。

   hostname=<*fw-hostname*>

   vm-auth-key=<*auth-key*>

   panorama-server=<*panorama-ip*>

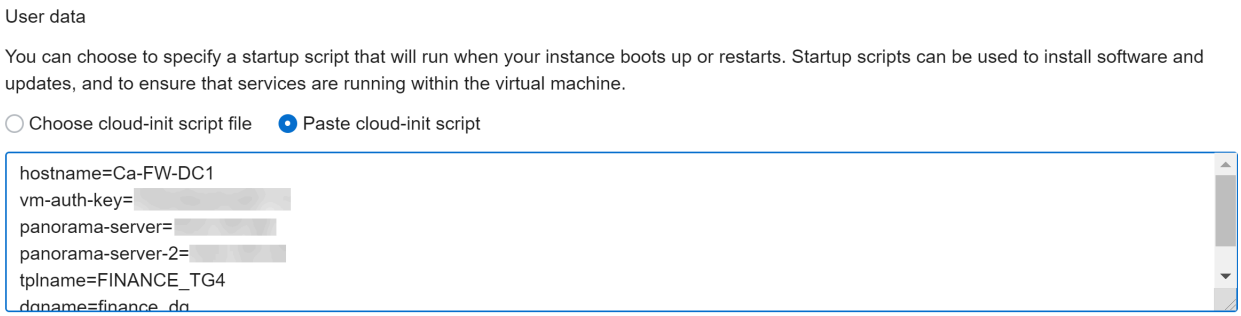
   panorama-server-2=<*panorama2-ip*>

   tplname=<*template-stack-name*>

   dgname=<*device-group-name*>

   authcodes=<*firewall-authcode*>

   op-command-modes=jumbo-frame



STEP 11 | 按一下 **Create**（建立）。

當 VM-Series 防火牆啟動時，OCI 會建立主要 VNIC 並將其連接至實例。此 VNIC 位於您在實例網路設定中指定的子網路內，且會連線至 VM-Series 防火牆的管理介面。

STEP 12 | 設定防火牆的新管理密碼。

1. 使用管理 IP 位址，透過 SSH 進入 VM-Series 防火牆的命令行介面 (CLI) 中。
2. 輸入下列命令登入防火牆：

   ssh-i <*private_key.pem*> admin@<*public-ip_address*>
3. 使用下列命令設定新密碼，並依照畫面上的提示進行：

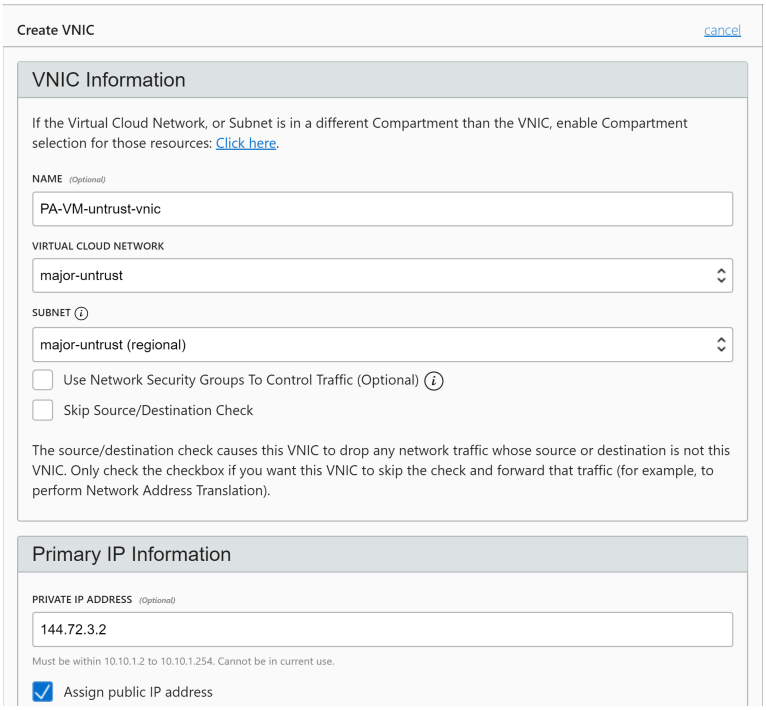
   configure

   set mgt-config users admin password

 ©2023 Palo Alto Networks, Inc.

STEP 13 | 將 vNIC 連接至每個資料介面的 VM-Series 防火牆實例。您必須將至少兩個資料介面連接至防火牆實例 — 不受信任和信任。

1. 選取新啟動的 VM-Series 防火牆實例，並選取 **Attached VNICs**（連接的 **VNIC**） > **Create VNIC**（建立 **VNIC**）。
2. 輸入 vNIC 的描述性 **Name**（名稱）。
3. 從 **Virtual Cloud Network**（虛擬雲端網路）下拉式清單中，選取 VCN。
4. 從 **Subnet**（子網路）下拉式清單中，選取子網路。
5. 指定 **Private IP Address**（私人 **IP** 位址）。只有在您想要選擇 vNIC 的特定 IP 時，才需要此項目。如果您未指定 IP，則 OCI 會指派來自您指派給子網路的 CIDR 區塊的 IP 位址。
6. 選取公共 vNIC（例如不受信任子網路）的 **Assign Public IP Address**（指派公共 **IP** 位址）。
7. 按一下 **Create VNIC**（建立 **VNIC**）。
8. 針對您部署所需的每個 vNIC，重複此程序。



 ©2023 Palo Alto Networks, Inc.

STEP 14 | 將資料背板網路介面設為防火牆上的 Layer 3 介面。

1. 登入防火牆。
2. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）。
3. 按一下 **Ethernet 1/1** 的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：**Layer3**
   - 在 **Config**（設定）頁籤上，將介面指派給預設路由器。
   - 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。定義新區域（例如 untrust-zone），然後按一下 **OK**（確定）。
   - 在 **IPv4** 頁籤上，選取 **Static**（靜態）。
   - 按一下 IP 區段中的 **Add**（新增），然後輸入介面的 IP 位址和網路遮罩。確定 IP 位址符合您指派給 VCN 中相應子網路的 IP 位址。例如，如果您將此介面新增至不受信任區域，則請確定指派 VCN 中所設定的不受信任 vNIC IP 位址。
4. 針對 VCN 中所設定的每個 vNIC（管理 vNIC 除外），重複此程序。

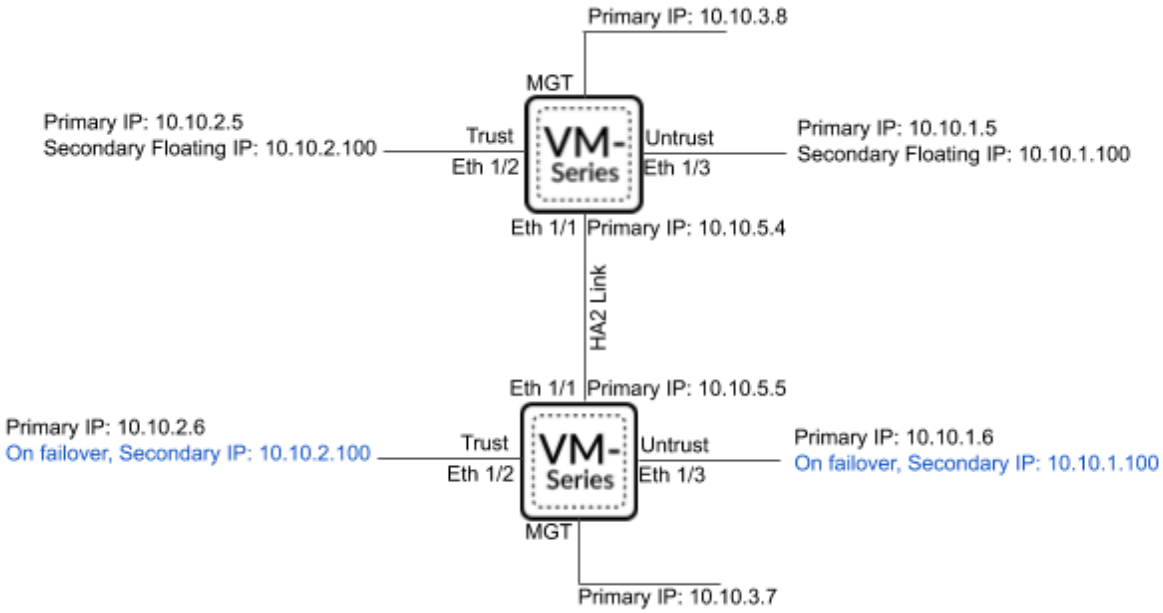
一律只刪除介面清單底端的介面。依錯誤順序刪除防火牆介面，會導致防火牆與 *OCI* 之間的介面不符。例如，假設您有五個資料介面，則請刪除防火牆上的介面二，並在底端新增新的介面。重新啟動防火牆之後，最新新增的介面會代替刪除的介面二，而非代替清單底端的介面。

©2023 Palo Alto Networks, Inc.

在 OCI 上設定主動/被動 HA

您可以在採用主動/被動高可用性 (HA) 設定的 OCI 上設定一對 VM-Series 防火牆。為了確保 OCI 上的 HA 設定中的執行時間，您必須建立可在不同對等間快速移動的浮動 IP 位址。主動防火牆關閉時，浮動 IP 位址會從主動防火牆移至被動防火牆，讓被動防火牆可以在變成主動對等時盡快無縫地保護流量安全。除了浮動 IP 位址之外，HA 對等也需要 HA 連結（控制連結 (HA1) 和資料連結 (HA2)）來同步處理資料與維護狀態資訊。

FIPS 模式下的 *OCI* 專用 *VM-Series* 防火牆不支援高可用性。



若要讓防火牆能夠在容錯移轉時移動浮動 IP 位址，您必須將防火牆實例設置於 OCI 上的動態群組中。動態雲組可讓您將防火牆實例分組為主要角色，並建立允許動態群組中的實例對 OCI 服務進行 API 呼叫的原則。您將使用比對規則將 HA 對等實例新增至動態群組，然後建立在不同 VNIC 間移動之浮動 IP 的原則。

HA 配對中的兩個 VM-Series 防火牆必須具有相同數量的網路介面。每個防火牆至少需要四個介面 — 管理、不受信任、信任和 HA。您可以在部署需要時設定其他資料介面。

- 管理介面 — 與主要介面相關聯的私人和公用 IP 位址。您可以使用管理介面上的私人 IP 位址，作為對等之間的 HA1 介面的 IP 位址。如果您想要有專用的 HA 介面，則必須將其他介面連接至每個防火牆，每個防火牆各五個介面。
- 不受信任和信任介面 — 主動 HA 對等上的這些資料介面都需要主動和次要 IP 位址。容錯移轉時，如果被動 HA 對等轉換為主動狀態，則會從先前的主動對等卸除次要私人 IP 位址，並將其連接至目前的主動 HA 對等。
- **HA2** 介面 — 此介面具有 HA 對等上的單一私人 IP 位址。HA2 介面是對等用來同步處理工作階段、轉送表格、IPsec 安全性關聯性和 ARP 表格的資料連結。

©2023 Palo Alto Networks, Inc.

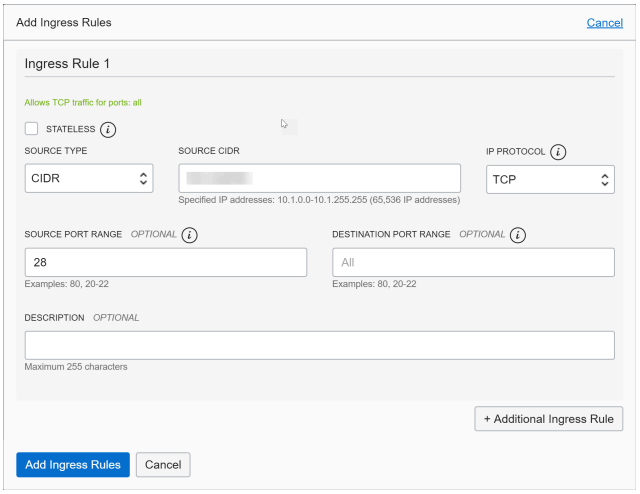
STEP 1 | 從 Oracle Cloud Marketplace 部署 VM-Series 防火牆並設定 HA 的網路介面。

1. （選用）在每個 HA 對等上設定專用 HA1 介面。
   1. 在 OCI 主控台中，選取 **Compute**（計算） > **Instances**（實例），然後按一下主動對等實例的名稱。
   2. 選取 **Attached VNICs**（連接的 **VNIC**），然後按一下 **Create VNIC**（建立 **VNIC**）。
   3. 輸入 HA1 介面的描述性名稱。
   4. 選取 VCN 和子網路。
   5. 輸入私人 IP 位址。
   6. 按一下 **Create VNIC**（建立 **VNIC**）。
   7. 對您的被動對等實例重複此程序。
2. 在每個 HA 對等上設定 HA2 介面。
   1. 在 OCI 主控台中，選取 **Compute**（計算） > **Instances**（實例），然後按一下主動對等實例的名稱。
   2. 選取 **Attached VNICs**（連接的 **VNIC**），然後按一下 **Create VNIC**（建立 **VNIC**）。
   3. 輸入 HA2 介面的描述性名稱。
   4. 選取 VCN 和子網路。HA2 介面應位於與資料介面不同的子網路上。
   5. 輸入私人 IP 位址。
   6. 按一下 **Create VNIC**（建立 **VNIC**）。
   7. 對您的被動對等實例重複此程序。
3. 將次要 IP 位址新增至主動對等上的資料平面介面。
   1. 在 OCI 主控台中，選取 **Compute**（計算） > **Instances**（實例），然後按一下主動對等實例的名稱。
   2. 選取 **Attached VNICs**（連接的 **VNIC**），然後按一下您的不受信任 VNIC。
   3. 選取 **IP Addresses**（**IP** 位址），然後按一下 **Assign Private IP Address**（指派私人 **IP** 位址）。
   4. 輸入 IP 位址，然後按一下 **Assign**（指派）。
   5. 對主動對等上的每個資料平面介面重複此程序。

©2023 Palo Alto Networks, Inc.

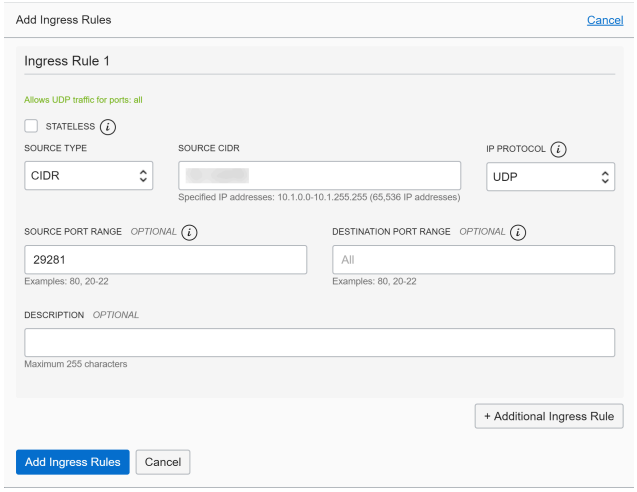
STEP 2 | 建立允許 HA 對等同步處理資料及維護狀態資訊的安全性規則。根據預設，OCI 僅允許 ICMP 流量。您必須開啟必要的 HA 連接埠。

1. 開啟 HA1 介面的連接埠。
   1. 在 OCI 主控台中，選取 **Networking**（網路） > **Virtual Cloud Networks**（虛擬雲端網路），然後選取您的 VCN。
   2. 選取 **Subnets**（子網路），然後選取包含 HA1 介面的子網路。
   3. 選取 **Security Lists**（安全性清單），然後按一下預設安全性清單加以編輯。
   4. 按一下 **Add Ingress Rule**（新增進入規則）。
   5. 輸入包含 HA 對等 HA1 連接埠 IP 位址的 **Source CIDR**（來源 **CIDR**）。
   6. 從 **IP Protocol**（**IP** 通訊協定）下拉式清單中，選取 **TCP**。
   7. 按一下 **+Additional Ingress Rule**（**+** 其他進入規則）。您需要為 TCP 連接埠 28260 和 28769 建立兩個額外的規則。
   8. 如果您的 VM-Series 防火牆已為 HA1 連結啟用加密，請為 ICMP 和 TCP 連接埠 28 建立額外的規則。
   9. 按一下 **Add Ingress Rules**（新增進入規則）。



2. 開啟 HA2 介面的連接埠。
   1. 在 OCI 主控台中，選取 **Networking**（網路） > **Virtual Cloud Networks**（虛擬雲端網路），然後選取您的 VCN。
   2. 選取 **Subnets**（子網路），然後選取包含 HA2 介面的子網路。
   3. 選取 **Security Lists**（安全性清單），然後按一下預設安全性清單加以編輯。
   4. 按一下 **Add Ingress Rule**（新增進入規則）。
   5. 輸入包含 HA 對等 HA2 連接埠 IP 位址的 **Source CIDR**（來源 **CIDR**）。
   6. 從 **IP Protocol**（**IP** 通訊協定）下拉式清單中，選取 **UDP** 或 **IP**。
   7. 如果傳輸模式為 UDP，請在 **Source Port Name**（來源連接埠名稱）中輸入 **29281**。如果傳輸模式為 IP，請在 **Source Port Name**（來源連接埠名稱）中輸入 **99**。
   8. 按一下 **Add Ingress Rules**（新增進入規則）。

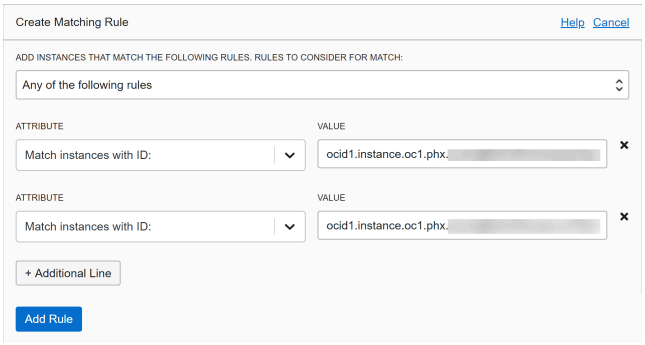
©2023 Palo Alto Networks, Inc.



©2023 Palo Alto Networks, Inc.

STEP 3 | 將兩個 HA 對等都新增至動態群組中，並建立允許 HA 對等移動浮動 IP 位址的原則。您必須具有每個 HA 對等實例的 OCID 以建置動態群組比對規則，將這些項目備妥以貼入規則建立器中。

1. 建立動態群組。
   1. 在 OCI 主控台中，選取 **Identity**（識別） > **Dynamic Groups**（動態群組） > **Create Dynamic Group**（建立動態群組）。
   2. 為您的動態群組輸入描述性 **Name**（名稱）。
   3. 按一下 **Rule Builder**（規則建立器）。
   4. 從第一個下拉式清單中選取 **Any of the following rules**（下列任何規則）。
   5. 從 **Attributes**（屬性）下拉式清單中選取 **Match instances with ID:**（比對具有下列 **ID** 的實例：），然後將對等 OCID 貼入 **Value**（值） 欄位中。
   6. 按一下 **+Additional Line**（+ 其他行）。
   7. 從 **Attributes**（屬性）下拉式清單中選取 **Match instances with ID:**（比對具有下列 **ID** 的實例：），然後將其他對等 OCID 貼入 **Value**（值） 欄位中。
   8. 按一下 **Add Rule**（新增規則）。

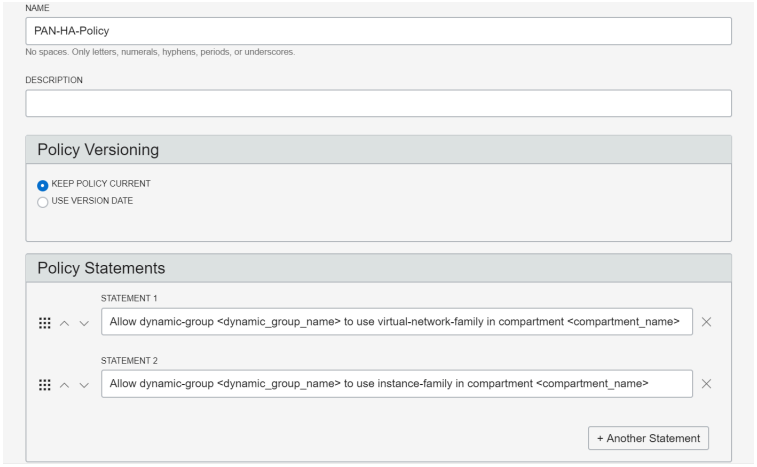


   9. 按一下 **Create Dynamic Group**（建立動態群組）。
2. 建立原則規則。
   1. 在 OCI 主控台中，選取 **Identity**（識別） > **Policies**（原則） > **Create Policy**（建立原則）。
   2. 輸入原則的描述性 **Name**（名稱）。
   3. 輸入第一個原則陳述式。

      ```
      Allow dynamic-group <dynamic_group_name> to use virtual-
      network-family in compartment <compartment_name>
      ```
   4. 按一下 **+Another Statement**（+ 其他陳述式）。
   5. 輸入第二個原則陳述式。

      ```
      Allow dynamic-group <dynamic_group_name> to use instance-
      family in compartment <compartment_name>
      ```
   6. 按一下 **Create**（建立）。

©2023 Palo Alto Networks, Inc.



 ©2023 Palo Alto Networks, Inc.

STEP 4 | 在防火牆上設定介面。您必須為不受信任和信任介面設定 HA2 資料連結，以及至少兩個 Layer 3 介面。請先在第一個 HA 對等完成此工作流程，再對第二個 HA 對等重複這些步驟。

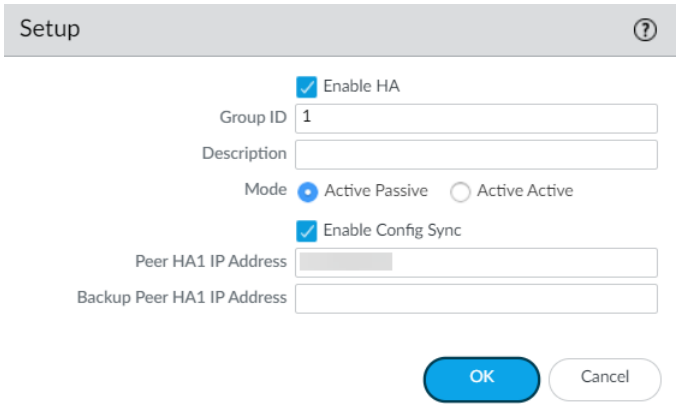
1. 登入防火牆 Web 介面。
2. （選用）如果您以管理介面作為 HA1，則必須將介面 IP 類型設定為靜態，並設定 DNS 伺服器。
   1. 選取 **Device**（裝置） > **Setup**（設定） > **Interfaces**（介面） > **Management**（管理）。
   2. 將 **IP Type**（**IP** 類型）設定為 **Static**（靜態）。
   3. 輸入 VM-Series 防火牆實例之主要 VNIC 的私人 **IP address**（**IP** 位址）。
   4. 按一下 **OK**（確定）。
   5. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務）。
   6. 按一下 **Edit**（編輯）。
   7. 輸入 Primary DNS Server（主要 **DNS** 伺服器）的 IP 位址。
   8. 按一下 **OK**（確定）。
   9. **Commit**（提交）您的變更。
3. 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後按一下您的不受信任介面。在此範例中，HA2 介面為 1/1、信任介面為乙太網路 1/2，不受信任介面為乙太網路 1/3。
4. 按一下 **Ethernet 1/1** 的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：**HA**
5. 按一下 **ethernet 1/2**（乙太網路 **1/2**）的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：**Layer3**
   - 在 **Config**（設定）頁籤上，將介面指派給預設路由器。
   - 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。定義新區域（例如 trust-zone），然後按一下 **OK**（確定）。
   - 在 **IPv4** 頁籤上，選取 **Static**（靜態）。
   - 按一下 IP 區段中的 **Add**（新增），然後輸入介面的主要 IP 位址和網路遮罩。確定 IP 位址符合您指派給 VCN 中相應子網路的 IP 位址。例如，如果您將此介面新增至受信任區域，則請確定指派 VCN 中所設定的受信任 vNIC IP 位址。
   - 按一下 IP 區段中的 **Add**（新增），然後輸入浮動 IP 位址和網路遮罩。
6. 按一下 **ethernet 1/3**（乙太網路 **1/3**）的連結，然後依照以下所述設定：
   - **Interface Type**（介面類型）：**Layer3**
   - 在 **Config**（設定）頁籤上，將介面指派給預設路由器。
   - 在 **Config**（設定）頁籤上，展開 **Security Zone**（安全性區域）下拉式清單並選取 **New Zone**（新增區域）。定義新區域（例如 untrust-zone），然後按一下 **OK**（確定）。
   - 在 **IPv4** 頁籤上，選取 **Static**（靜態）。

©2023 Palo Alto Networks, Inc.

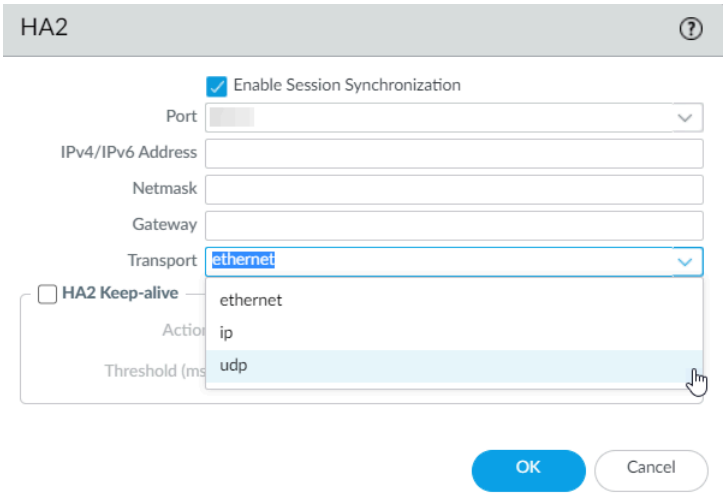
- 按一下 IP 區段中的 **Add**（新增），然後輸入介面的主要 IP 位址和網路遮罩。確定 IP 位址符合您指派給 VCN 中相應子網路的 IP 位址。例如，如果您將此介面新增至不受信任區域，則請確定指派 VCN 中所設定的不受信任 vNIC IP 位址。
- 按一下 IP 區段中的 **Add**（新增），然後輸入浮動 IP 位址和網路遮罩。

STEP 5 | 啟用 HA。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **General**（一般）。
2. 編輯 [Setup（設定）] 設定。
3. 在 **Peer HA1 IP address field**（對等 **HA1 IP** 位址欄位）中輸入被動對等的私人 IP 位址。
4. 按一下 **OK**（確定）。



5. （選用）編輯控制連結 (HA1)。如果您未計劃將管理介面用於控制連結，並已新增其他介面（例如乙太網路 1/4），則請編輯此區段來選取要用於 HA1 通訊的介面。
6. 編輯資料連結 (HA2) 以使用 **Port**（連接埠）乙太網路 1/1，並新增主動對等的 IP 位址以及子網路的 **Gateway**（閘道） IP 位址。
7. 從 Transport（傳輸）下拉式清單中選取 **IP** 或 **UDP**。不支援乙太網路。



8. 按一下 **OK**（確定）。

STEP 6 | **Commit**（提交）您的變更。

©2023 Palo Alto Networks, Inc.

STEP 7 | 對被動 HA 對等重複步驟 4 和步驟 5。

STEP 8 | 完成兩個防火牆的 HA 設定後，請確認配對的防火牆為主動/被動 HA。

1. 存取兩個防火牆上的 **Dashboard**（儀表板），然後檢視高可用性 Widget。
2. 在主動 HA 對等上，按一下 **Sync to peer**（同步處理至對等）。
3. 確認防火牆已配對並同步。
   - 在被動防火牆上：本機防火牆狀態應顯示為 **Passive**（被動），而 **Running Config**（執行中設定）應顯示為 Synchronized（已同步）。
   - 在主動防火牆上：本機防火牆狀態應顯示為 **Active**（主動），而執行中設定應顯示為 **synchronized**（已同步）。

©2023 Palo Alto Networks, Inc.

在 Alibaba Cloud 上設定 VM-Series 防火牆

在 Alibaba Cloud 上部署 VM-Series 防火牆會保護您在 Alibaba Cloud 內建立的網路。您可以部署 VM-Series 防火牆來保護面向網際網路的應用程式和混合雲端部署。

- Alibaba Cloud 上的 VM-Series 防火牆
- Alibaba Cloud 上的 VM-Series 防火牆最低系統需求
- 準備在 Alibaba Cloud 上部署 VM-Series 防火牆
- 在 Alibaba Cloud 上部署 VM-Series 防火牆

Alibaba Cloud 上的 VM-Series 防火牆

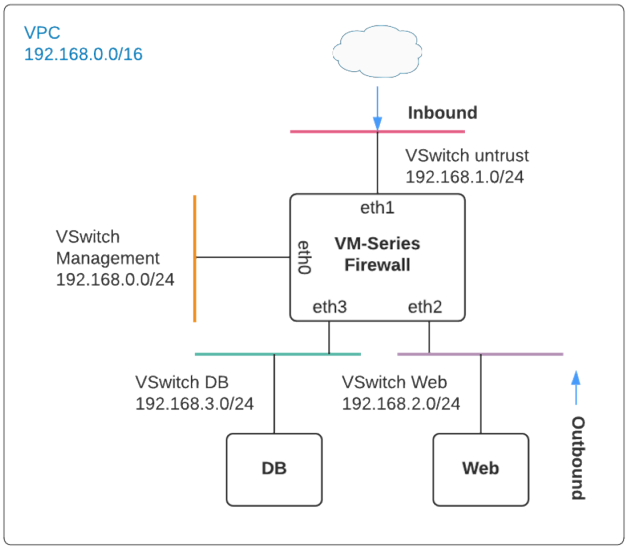
您可以在 Alibaba Cloud 部署 VM-Series 防火牆，以保護輸入和輸出南北向流量。

因為 ***Alibaba Cloud*** 不支援子網路路由，所以不支援保護相同 ***VPC*** 內的東西向流量。

Alibaba Cloud 上的 VM-Series 防火牆在 KVM 超管理器上執行，且當您選取具有足夠資源的 Alibaba Cloud 實例時，最多支援 8 個網路介面（請參閱Alibaba Cloud 上的 VM-Series 防火牆最低系統需求）。

Alibaba Cloud 上的 VM-Series 防火牆支援 BYOL 授權，(BYOL) 以及 Alibaba Cloud 國際區域和中國大陸上的 VM-Series ELA。目前不支援 PAYG 授權。

在 Alibaba Cloud 中，VPC 在邏輯上隔離您的虛擬網路。建立 VPC 之後，您可以建立 VSwitch，以進一步將 virtual private network（虛擬私人網路 - VPN）分段，如下圖所示。若要保護輸入流量，必須同時在防火牆上設定 DNAT 和 SNAT。



輸入流量源自 VPC 外部的用戶端，並前往 VM-Series 防火牆不受信任介面。防火牆會檢查流量，並透過信任介面傳送至應用程式。從應用程式返回的流量必須通過 VM-Series 防火牆信任介面，而防火牆會檢查流量，並透過不受信任介面送出。

輸出流量通常源自外部應用程式。一般而言，您會將 VPC 內面向網際網路的流量路由至 NAT 閘道（已連接 EIP）。若要這樣做，請在 VPC 路由表中新增預設閘道路由，並以應用程式子網路的 VM-Series 防火牆 IP 位址為下一個躍點。使用不受信任介面 IP 來設定 SNAT，以確保源自網際網路的流量會經過 VM-Series 防火牆傳回。

如需範例設定，請參閱保護 Alibaba Cloud 上的南北向流量的安全。

©2023 Palo Alto Networks, Inc.

Alibaba Cloud 上的 VM-Series 防火牆最低系統需求

在 Alibaba Cloud 上，您可以在 KVM 超管理器上部署 VM-Series 防火牆（請參閱VM-Series 部署）。

- VM-Series 防火牆軟體需求
- VM-Series 防火牆的 Alibaba Cloud 實例類型建議
- Alibaba Cloud CLI

VM-Series 防火牆軟體需求

確保您具有在 Alibaba Cloud 上完成 VM-Series 部署所需的軟體和授權。

- 若要在 Alibaba Cloud 上部署 VM-Series 防火牆，必須使用您從 Alibaba Marketplace 取得的 VM-Series 映像。此映像包含 PAN-OS 版本 10.0.3 和 VM-Series 外掛程式版本 2.0.3。
- 部署之前，請選擇 VM-Series ELA 或 BYOL 授權、容量授權和訂閱搭售包。請參閱 VM-Series 型號授權類型。
- 您必須能夠以 SSH 進入 VM-Series 防火牆，才能完成部署。如果您的作業系統不支援 SSH，請安裝第三方軟體，例如 Putty。

VM-Series 防火牆的 Alibaba Cloud 實例類型建議

建立 VM-Series 防火牆之前，您必須選擇支援 VM-Series 型號最低系統需求的 Elastic Compute Service (ECS) 實例類型。檢閱實例類型文件，確定 ECS 實例類型具有可保護網路設定的資源。

VM-Series 型號	Elastic Compute Service 實例類型
VM-100	ecs.g5.xlarge、ecs.sn2ne.xlarge
VM-300	ecs.g5.xlarge、ecs.sn2ne.xlarge
VM-500	ecs.g5.2xlarge, ecs.sn2ne.2xlarge
VM-700	ecs.g5.4xlarge, ecs.sn2ne.4xlarge

Alibaba Cloud CLI

Aliyun 3.0.4 版或更高版本。請參閱 準備使用 Aliyun 命令行介面。

©2023 Palo Alto Networks, Inc.

準備在 Alibaba Cloud 上部署 VM-Series 防火牆

此工作使用 Aliyun CLI 來建立 VM-Series 防火牆的 VPC 和 VSwitch，不過，您應該先規劃網路再開始。評估您想要保護的應用程式，並決定在何處部署 VM-Series 防火牆以檢查和保護南北向流量。

- 選擇授權與規劃網路
- 準備使用 Aliyun 命令行介面

選擇授權與規劃網路

評估您需要保護的應用程式，以及建立允許 VM-Series 防火牆檢驗輸入和輸出應用程式流量的網路。

STEP 1 | 規劃和設計 VPC。

1. 規劃網路，包括 VPC 和 VSwitch 的 CIDR 區塊。

   如需範例程序，請參閱建立 VPC 並設定網路。
2. 規劃 IP 位址。如果您需要特定位址或位址範圍，請參閱 Elastic IP Address 使用者指南。
3. 規劃安全性群組。

STEP 2 | 評估應用程式和網路設定，以及計算您需要保護應用程和網路的防火牆容量。

STEP 3 | 取得 VM-Series 防火牆授權。

雖然您不需要授權就能安裝 VM-Series 防火牆（您可以在安裝之後啟動授權），但必須先選擇適當的 VM-Series 型號和 ECS 實例類型，再部署防火牆。

1. 選擇 VM-Series 型號。

   VM-Series 防火牆支援最多 *8* 個介面，前提是 ***VM-Series*** 型號和 ***Alibaba Cloud*** 實例有足夠的資源。您可以使用型號

   使用您已選擇的 VM-Series 模型以選擇VM-Series 防火牆的 Alibaba Cloud 實例類型建議的其中一個。
2. 選擇符合您需求的 VM-Series 容量授權。
3. 購買 BYOL 訂閱搭售包（如果還沒有的話）。您會收到 VM-Series 訂閱的授權碼，在部署期間必須提供此授權碼。

STEP 4 | 規劃如何設定 Alibaba 帳戶和權限來存取 VM-Series 防火牆。首先，請參閱安全性常見問答集，並了解執行個體 RAM 角色。

準備使用 Aliyun 命令行介面

本章的重點在 ECS 主控台，不過，您在 ECS 主控台執行的所有操作，都可以從 Aliyun command line interface（命令列介面 - CLI）完成。如果您想要使用 VM-Series 防火牆保護 Alibaba Cloud 上的負載平衡，則需要 CLI。

©2023 Palo Alto Networks, Inc.

安裝和設定 Aliyun 的最新版本（Alibaba Cloud 命令行介面）。

STEP 1 | 建立存取金鑰，並將存取金鑰 ID 和密碼儲存至安全位置。

STEP 2 | 從 https://github.com/aliyun/aliyun-cli 下載所支援版本的 Aliyun。

STEP 3 | 安裝 Aliyun。

STEP 4 | 設定 Aliyun。

設定會提示您輸入存取金鑰資訊和其他資訊。

如果您的部署使用儲存貯體，則地區必須符合您的貯體地區。

```
aliyun configure 正在以驗證模式設定設定檔...存取金鑰 ID
 [******************8rq]: ************8rq 存取金鑰秘密 [************
 ***************tM2]:*************************tM2 預設區域 ID
 [ us-west-1]: us-west-1 預設輸出格式 [json]: json (僅支援 json)) 預設
語言 [zh|en] en: en 正在儲存設定檔[] ...完成。可用地區: ...
```


©2023 Palo Alto Networks, Inc.

在 Alibaba Cloud 上部署 VM-Series 防火牆

VM-Series 防火牆採用最少三個介面：管理、不受信任和信任。當您建立 Alibaba Cloud VPC 時，邏輯上會將它隔離。若要將虛擬私人網路細分為子網路，請建立數個 VSwitch，其各有自己的 CIDR 區塊。因為 VM-Series 防火牆具有多個介面，所以可以檢查所有子網路上的流量。

一般而言，外部輸入流量會遇到 VM-Series 防火牆不受信任介面。防火牆會檢查輸入流量，並透過信任介面將它傳送至應用程式。來自應用程式的傳回流量會前往防火牆的信任介面，然後由防火牆檢查傳回流量，並透過不受信任介面送出。

下列工作示範如何使用主控台建立 VM-Series 防火牆基礎結構。

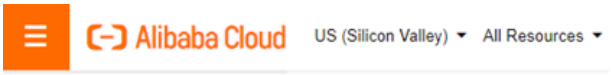
- 建立 VPC 並設定網路
- 建立並設定 VM-Series 防火牆
- 保護 Alibaba Cloud 上的南北向流量的安全
- 設定 Alibaba Cloud 上的負載平衡

建立 VPC 並設定網路

使用 Alibaba Cloud 主控台來建立 VPC、VSwitch、安全性群組和安全性群組規則。

All VM-Series firewall interfaces must be assigned an IPv4 address when deployed in a public cloud environment. IPv6 addresses are not supported.

STEP 1 | 開啟 VPC 主控台，並從功能表中選取區域。請注意，您選取的地區必須提供 Palo Alto Networks 支援的其中一個實例類型。



STEP 2 | 從 Alibaba Cloud 主控台首頁，選取 **Products and Services**（產品與服務） > **Networking**（網路） > **Virtual Private Cloud**（虛擬私人雲端 - **VPC**）。

STEP 3 | **Create a VPC**（建立 **VPC**）。

在此步驟中，您將建立 VPC 以及管理、不受信任和信任 VSwitch。ECS 主控台使用相同表單建立 VPC 和交換器。

1. 選取 **Create VPC**（建立 **VPC**）。

   指定 VPC 名稱、IPv4 CIDR 區塊和說明。請參閱建立 VPC。

屬性	值
名稱	由您選擇
IPV4 CIDR 區塊	由您選擇。請參閱 CIDR 區塊常見問答集。

©2023 Palo Alto Networks, Inc.

屬性	值
資源群組	由您選擇。

2. 選取 **Create vSwitch**（建立 **vSwitch**）。
   - 將 VSwitch 命名為 **Management**。
   - 選擇 **Zone**（區域），指定 **IPv4 CIDR Block**（**IPv4 CIDR** 區塊）（您指定給 VPC 的區塊子集），然後指定 **Description**（說明）。
   - 在底部，按一下 **Add**（新增）以新增另一個 vSwitch（直到您新增所有 vSwitch 才按一下 **OK**（確定））。

   請參閱建立 vSwitch。
3. 以相同方式 **Add**（新增）不受信任 VSwitch。
4. **Add**（新增）信任 VSwitch。
5. 按一下 **OK**（確定）。

   檢視 VPC 詳細資訊，進行任何變更之後按一下 **Complete**（繼續）。

STEP 4 | 建立安全性群組和安全性群組規則。

- 從 Alibaba Cloud 主控台首頁，選取 **Elastic Compute Service** > **Networking & Security**（網路與安全性） > **Security Groups**（安全性群組）。
- 在右上角，按一下 **Create Security Group**（建立安全性群組）。

1. 建立管理安全性群組。

   請參閱建立安全性群組來填寫下列欄位。

屬性	值
範本	自訂
安全性群組名稱	管理
Security Group Type（安全性群組類型）	Basic（基本）
網路類型	VPC
VPC	選取稍早建立的 VPC。

©2023 Palo Alto Networks, Inc.

屬性	值
資源群組	由您選擇

- 完成表單，然後按一下 **OK**（確定）。

  ECS 主控台會提示您建立此安全性群組的規則。此工作說明可讓您強化 VM-Series 防火牆的一些基本安全性群組規則。您可以建立更多規則來強制網路安全性需求。

2. 選取 **Create Rules Now**（立即建立規則），為 HTTPS 和 SSH 建立規則。

   選取 Inbound（輸入）頁籤，按一下 **Add Security Group Rule**（新增安全性群組規則）。

   - 建立輸入規則，以允許此安全性群組中使用 HTTPS。例如：

屬性	值
Rule Direction（規則方向）	輸入
動作	允許
Protocol Type（通訊協定類型）	HTTPS (443)
優先順序	100
Authorization Type（授權類型）	請參閱 新增安全性群組規則。
Authorization Object（授權物件）	

   - 按一下 **Add Security Group Rule**（新增安全性群組規則）建立輸入規則，以允許在管理介面上使用 SSH。

屬性	值
Rule Direction（規則方向）	輸入
動作	允許
Protocol Type（通訊協定類型）	Customized TCP（自訂的 TCP）
Port Range（連接埠範圍）	1/65535
Authorization Type（授權類型）	請參閱 新增安全性群組規則。
Authorization Object（授權物件）	

   按一下 **OK**（確定），然後選取 **Back**（返回），回到 [Security Groups（安全性群組）] 頁面。

©2023 Palo Alto Networks, Inc.

3. 選取 **Create Security Group**（建立安全性群組），建立不受信任安全性群組。

   出現提示時，請為不受信任安全性群組建立規則。

屬性	值
Rule Direction（規則方向）	輸入
動作	允許
Protocol Type（通訊協定類型）	Custom TCP（自訂 TCP）
Port Range（連接埠範圍）	1/65535
優先順序	100
Authorization Type（授權類型）	請參閱 新增安全性群組規則。
Authorization Object（授權物件）	

   按一下 **OK**（確定），然後選取 **Back**（返回），回到 [Security Groups（安全性群組）] 頁面。

4. 建立信任安全性群組。

   出現提示時，按一下 **Add Security Group Rule**（新增安全性群組規則），複製不受信任規則。

   繼續建立並設定 VM-Series 防火牆。

建立並設定 VM-Series 防火牆

此工作使用 ECS 主控台，建立至少具有三個介面的 VM-Series 防火牆實例：管理、不受信任和信任。依預設，ECS 實例支援單一 NIC，並會自動將彈性網路介面 (ENI) 與其連接。若要支援 VM-Series 防火牆，您必須單獨建立不受信任和信任彈性網路介面 (ENI)，並將它們連接至您的實例。

STEP 1 | 從 Alibaba Cloud 主控台首頁，選取 **Elastic Compute Service** > **Instances & Images**（實例與映像） > **Instances**（實例），然後按一下右上角的 **Create Instance**（建立實例）。

STEP 2 | 選取 **Custom Launch**（自訂啟動）。

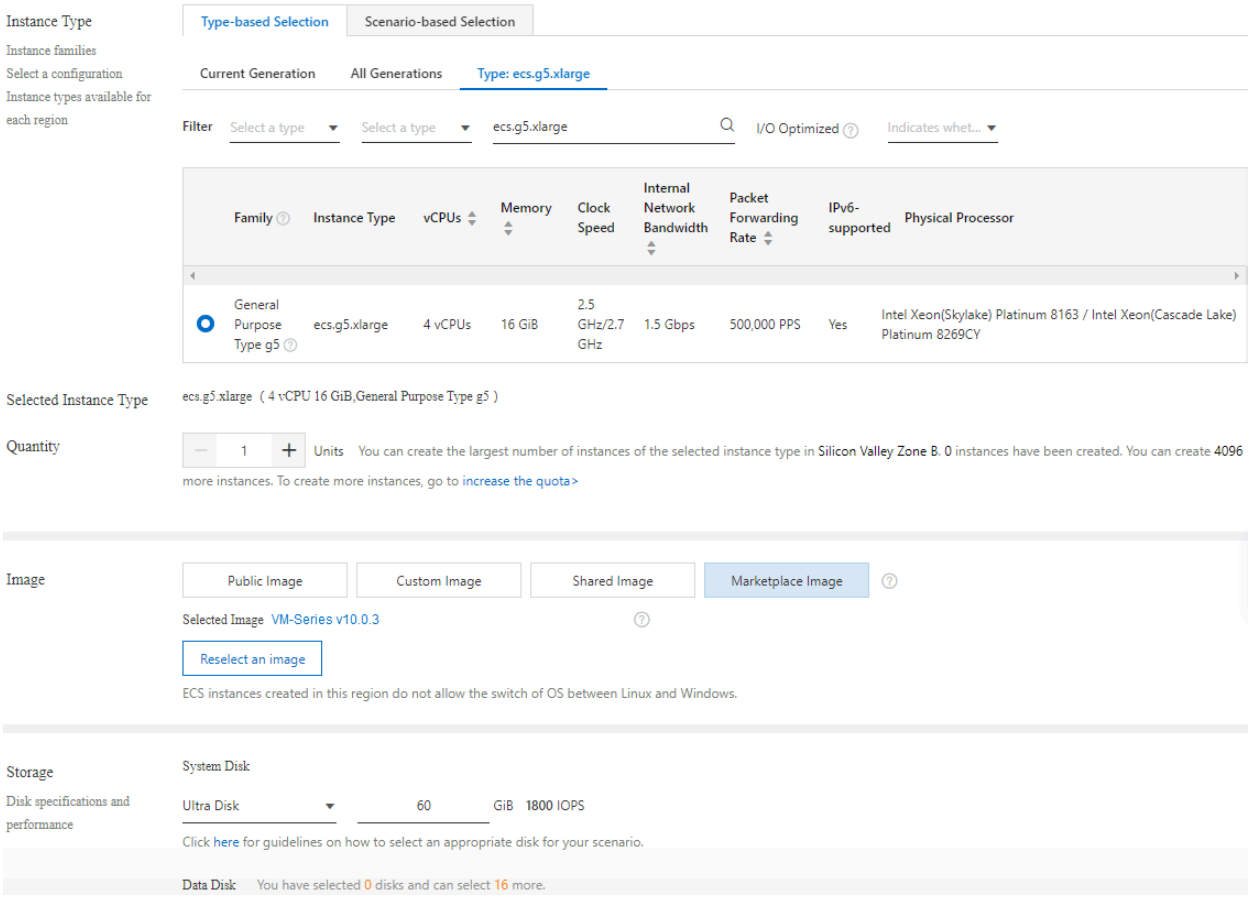
STEP 3 | 基本設定。

1. 填寫下列值。例如：

屬性	值
付費方法	Subscription（訂閱）。

 ©2023 Palo Alto Networks, Inc.

屬性	值
地區	由您選擇。您也可以選取區域。您選取的地區必須提供其中一個必要的實例類型。
執行個體類型	VM-Series 防火牆的 Alibaba Cloud 實例類型建議的其中一種類型。您可以使用 [Type-based Selection（基於類型的選擇）] 搜尋實例類型。
影像	選取 **Marketplace Image**（**Marketplace** 映像），在 Alibaba Marketplace 搜尋 “VM-Series”。此映像結合作業系統與 VM-Series 防火牆。
儲存區	選擇磁碟類型並指定 60 GB。
Snapshot（快照）	由您選擇。
持續時間	由您選擇。



2. 選取 **Next:Networking**（下一步：網路）。

©2023 Palo Alto Networks, Inc.

STEP 4 | 在 [Networking（網路）] 頁面上，提供下列值。

1. Network（網路）（選取 VPC）。
   - 選擇您在建立 VPC 並設定網路中建立的 VPC。
   - 選擇管理 VSwitch。
2. Public IP Address（公共 IP 位址）。

   如果您沒有公共 IP 位址，請啟用 **Assign Public IP address**（指派公共 **IP** 位址），系統會配置位址。如果您必須使用特定的 IP 位址，或特定範圍內的位址，則可以要求自訂 IP 位址。請參閱 Elastic IP Address 使用者指南。
3. Security Group（安全性群組）。

   選取 [Management security group（管理安全性群組）]。
4. 彈性網路介面。

   管理介面已連接至 eth0。
5. 選取 **Next:System Configurations**（下一步：系統設定）。

STEP 5 | 在 [System Configurations（系統設定）] 頁面上，填寫下列值。

1. Logon Credentials（登入認證）：選取 **Key Pair**（金鑰配對）。

   不支援密碼驗證。
2. 命名 VM-Series 防火牆實例並提供主機名稱。

   進行任何更正。

   選取 **Preview**（預覽）以檢視到目前為止的設定。
3. 在 **Advanced (based or instance RAM roles or cloud-init)**（進階（基於實例 **RAM** 角色或 **cloud-init**））後面，按一下 **Show**（顯示）。
   - RAM 角色為選用。
   - 在 [User Data（使用者資料）] 欄位中，以鍵值組輸入基本啟動程序資訊（以換行符號分隔）。請參閱 以使用者資料輸入基本設定（公共雲端）。例如，在 **User Data**（使用者資料）欄位中輸入下列資訊。

```
type=dhcp-client hostname=Ca-FW-DC1 vm-auth-
key=7550362253**** panorama-server=10.*.*.20 panorama-
server-2=10.*.*.21 tplname=FINANCE_TG4 dgname=finance_dg op-
cmd-dpdk-pkt-io=on dhcp-send-hostname=yes dhcp-send-client-
id=yes dhcp-accept-server-hostname=yes dhcp-accept-server-
domain=yes authcodes=I7115398 vm-series-auto-registration-
```


©2023 Palo Alto Networks, Inc.

```
pin-id=abcdefgh1234**** vm-series-auto-registration-pin-
value=zyxwvut-0987****
```

Alibaba Cloud 不支援 ***op-command-modes***（*mgmt-interface-swap* 和 *jumbo frame*）。

op-cmd-dpdk-pkt-io=on 支援 *DPDK*。如果您要指定 *PacketMMAP*，請指定 *op-cmd-dpdk-pkt-io=off*

分組為選用。訂購之前，選取 **Preview**（預覽）來檢視設定。

STEP 6 | 檢視服務條款，然後選取 **Create Order**（建立訂單），以建立 VM-Series 防火牆實例。

檢視採購單，然後選取 **Subscribe**（訂閱）。

STEP 7 | 從主控台首頁中，選擇 > **Elastic Compute Service**（彈性計算服務） > **Networks and Security**（網路與安全性） > **ENI**，然後選取右上角的 **Create ENI**（建立 **ENI**）。為不受信任和信任介面建立彈性網路介面。

1. 建立不受信任 ENI。

   在 **Actions**（動作）欄中，選取 **Bind to Instance**（繫結至實例），然後選取您剛建立的實例。

2. 建立信任 ENI 並繫結至實例。

STEP 8 | 配置彈性 IP (EIP) 位址。

配置 VM-Series 防火牆管理介面和不受信任網路介面的 EIP 位址。在此範例中，信任介面不會公開到網際網路，因此您不需要第三個 IP 位址。

如果您已有兩個 EIP，則請移至下一個步驟。

1. 建立 EIP 與 VM-Series 防火牆管理介面的關聯。
2. 建立 EIP 與 VM-Series 防火牆不受信任網路介面的關聯。

   您連接的第二個介面會指派給 VM-Series 防火牆上的網路介面 1。

STEP 9 | 重新啟動實例，以連接新的網路介面。

在 [Instances（實例）] 清單上，選取您的實例，選取 **Manage**（管理），然後選取右上角的 **Restart**（重新啟動）。

STEP 10 | 以安全性金鑰透過 SSH 進入 VM-Series 防火牆，然後設定管理員密碼：

```
developer1$ ssh -i dev1-vpc1.pem admin@18.***.145.153 Welcome
 admin. admin> configure Entering configuration mode [edit]
 admin# set mgt-config users admin password 輸入密碼：<password>確認密
碼：<password> [edit] admin# commit
```

STEP 11 | 存取 VM-Series 防火牆 Web 介面。

開啟 Web 瀏覽器，並輸入管理介面的 EIP。

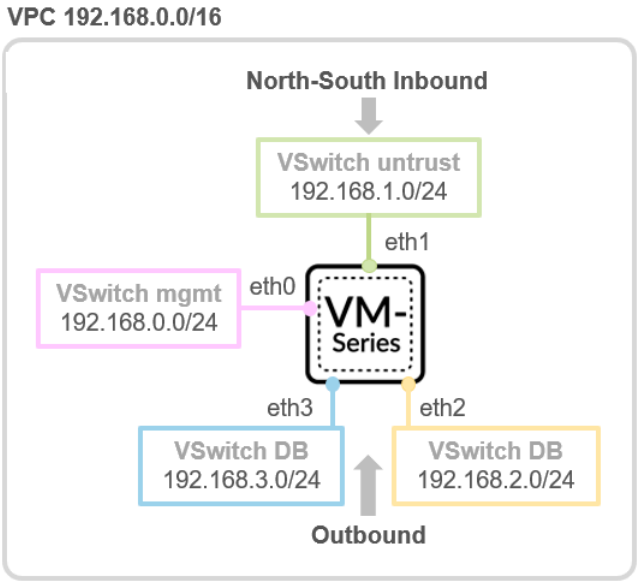
©2023 Palo Alto Networks, Inc.

保護 Alibaba Cloud 上的南北向流量的安全

建立 VPC 之後，您可以建立 VSwitch 以將虛擬私人網路細分為子網路。此範例以 CIDR 為 192.168.0.0/16 的 VPC 為例子，您可以輸入自己的值。四個 VSwitch 會建立四個子網路。

VSwitch 名稱	介面	範例 CIDR
mgmt	eth0	192.168.0.0/24
不信任	eth1	192.168.1.0/24
web	eth2	192.168.2.0/24
db	eth3	192.168.3.0/24

在下圖中，VM-Series 防火牆連接至兩個信任的子網路：web 和 db。外部用戶端存取 VM-Series 防火牆的不受信任介面時會起始輸入流量。防火牆會檢查流量，並將它傳送至應用程式。例如，防火牆會透過信任介面將流量傳送至 Web 伺服器。從 Web 伺服器傳回的流量必須到達 VM-Series 防火牆的信任介面。防火牆會檢查傳回流量流程，並透過不受信任介面傳送它。



若要保護輸入流量，必須同時在防火牆上設定 DNAT 和 SNAT。

STEP 1 | 建立輸入流量的 NAT 規則。

以下範例說明輸入流量保護的 NAT 規則。

```
          <nat> <rules> <entry name="inbound_web"> <source-
translation> <dynamic-ip-and-port> <interface-address>
 <interface>ethernet1/2</interface> </interface-address>
 </dynamic-ip-and-port> </source-translation> <destination-
translation> <translated-address>web_server</translated-address>
 </destination-translation> <to> <member>untrust</member> </to>
 <from> <member>any</member> </from> <source> <member>any</member>
```


©2023 Palo Alto Networks, Inc.

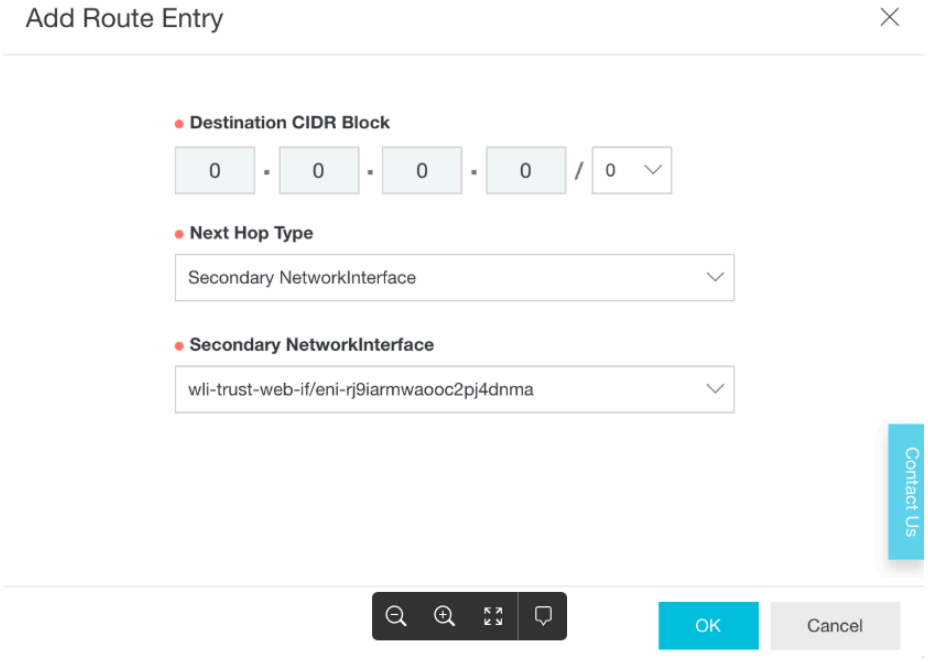
```
 </source> <destination> <member>fw_untrust</member> </destination>
 <service>any</service> <to-interface>ethernet1/1</to-interface>
 </entry> </rules> </nat> <address> <entry name="fw_untrust"> <ip-
netmask>192.168.1.4</ip-netmask> </entry> <entry name="fw_trust">
 <ip-netmask>192.168.2.201</ip-netmask> </entry> <entry
 name="web_server"> <ip-netmask>192.168.2.203</ip-netmask> </entry>
 </address>
```


©2023 Palo Alto Networks, Inc.

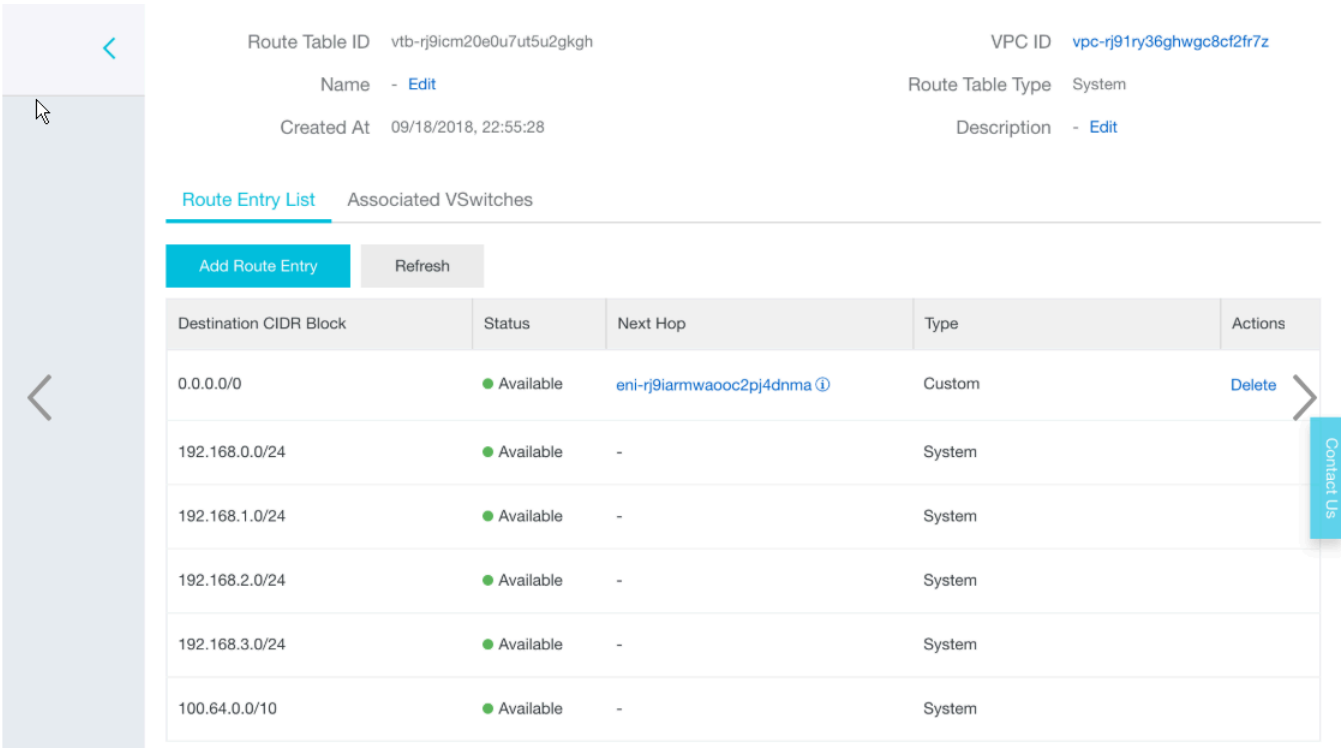
STEP 2 | 保護輸出流量。

如上圖所示，應用程式會起始輸出流量。例如，Web 伺服器必須執行 **`yum install`** 以更新 rpm 套件。一般而言，VPC 內的網際網路連結流量會路由至 NAT 閘道（已連接 EIP）。若要保護輸出流量，您必須強制輸出流量經過 VM-Series 防火牆。

1. 在 VPC 路由表中新增預設閘道路由，並以 Web 伺服器子網路中的防火牆 IP 為下一個躍點。



2. 檢視路由表中的項目。



©2023 Palo Alto Networks, Inc.

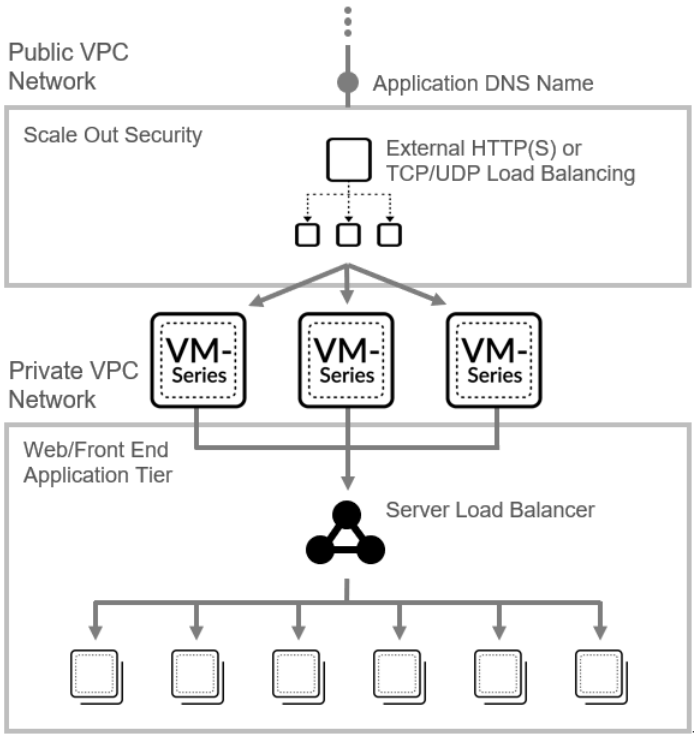
3. 使用不受信任介面 IP 來設定 SNAT 規則，以確定從網際網路傳回的流量經過 VM-Series 防火牆。

   此下範例說明 SNAT 設定。

```
            <nat> <rules> <entry name="outbound_web">
 <source-translation> <dynamic-ip-and-port> <interface-
address> <interface>ethernet1/1</interface> </interface-
address> </dynamic-ip-and-port> </source-translation> <to>
 <member>untrust</member> </to> <from> <member>trust</member>
 </from> <source> <member>any</member> </source> <destination>
 <member>any</member> </destination> <service>any</service>
 <to-interface>any</to-interface> </entry> </rules> </nat>
```

設定 Alibaba Cloud 上的負載平衡

在 Alibaba Cloud 上，您可以在負載平衡器分層式設定中部署 VM-Series 防火牆，而在此設定中，防火牆部署於公共網路與私人網路之間，如下所示。



建立 VPC 並設定網路時，您已建立不受信任和信任 ENI，並將它們連接至 VM-Series 防火牆實例，以作為次要 ENI。

當您使用主控台將多個後端伺服器新增至 Alibaba 伺服器負載平衡器 (SLB) 時，SLB 會將流量傳送至下一個躍點後端伺服器的主要 ENI。因為主要 ENI 是管理介面，所以流量必須流向不受信任介面（次要 ENI）來進行檢查。

若要確定網際網路流量流向資料平面介面，而非管理介面，請使用 Alibaba CLI 將 VM-Series 防火牆不受信任 ENI 連接至 SLB 實例。

©2023 Palo Alto Networks, Inc.

您必須安裝 Aliyun command line interface（命令列介面 - CLI），才能使用下列 *CLI* 命令。

STEP 1 | 建立負載平衡器分層式設定的公共和私人 VPC，並部署 VM-Series 防火牆。

其餘步驟是您可以調整以符合環境的範例 CLI 命令。

STEP 2 | 建立負載平衡器。

```
slb CreateLoadBalancer --RegionId us-west-1 --LoadBalancerName
 wli-slb --VpcId vpc-rj91ry36ghwgc8cf2fr7z --LoadBalancerSpec
 slb.s1.small --AddressType internet --MasterZoneId us-west-1a
 --SlaveZoneId us-west-1b { "網路類型": "classic", "負載平衡器
名稱": "**********", "位址": "**********, "資源群組 ID": "rg-
**********ofi", "要求 ID":"0B8BA2AA-E837-****-****-B82A8A1D5FBB",
 "位址 IP 版本": "ipv4", "負載平衡器 ID": "lb-*****************mvz",
 "VSwitchId": "", "VpcId": "vpc-*****************r7z" }
```

STEP 3 | 新增後端伺服器。

使用 *CLI*，逐一新增介面。介面的新增順序可決定接收介面的 *NIC*。

```
aliyun slb AddBackendServers --LoadBalancerId lb-
*****************mvz --BackendServers '[ { "ServerId":"eni-
*****************bzw", "Type":"eni","Weight":"100" } ]'
```

STEP 4 | 建立可執行健康檢查的 HTTP 接聽程式。

```
aliyun slb CreateLoadBalancerHTTPListener --LoadBalancerId lb-
*****************mvz --ListenerPort 80 --StickySession on --
HealthCheck on --HealthCheckURI '/'
```


©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

在 Cisco ACI 中設定防火牆

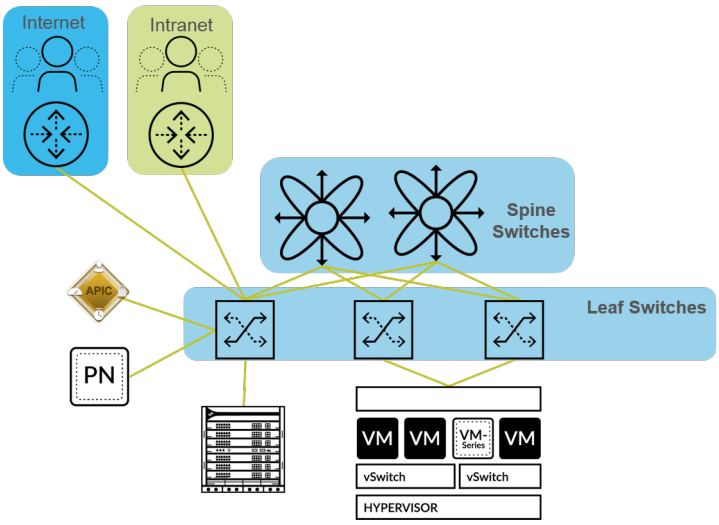
Palo Alto Networks 以服務形式與 Cisco Application-Centric Infrastructure（以應用程式為主的基礎結構 - ACI）整合。ACI 是 software-defined networking（軟體定義的網路 - SDN）解決方案，可輕鬆部署新的工作負載和網路服務。有一個稱為 Cisco Application Policy Infrastructure Controller（應用程式原則基礎結構控制器 - APIC）的 SDN 控制器，可讓您在 Endpoint Groups（端點群組 - EPG）之間部署防火牆服務。EPG 充當應用程式或應用程式層的容器。將防火牆設置於 EPG 之間時，防火牆上設定的安全性原則即可保護 EPG 之間的流量安全。APIC 提供單一窗口來管理整個資料中心的網路拓撲、網路原則和連線，還支援插入 L4 - L7 裝置，例如硬體型或 VM-Series 防火牆。需要 Panorama 才能集中管理安全性。

- Palo Alto Networks 防火牆與 Cisco ACI 整合
- 準備 ACI 環境進行整合
- 以網路政策模式整合防火牆與 Cisco ACI
- Cisco ACI 中的端點監控

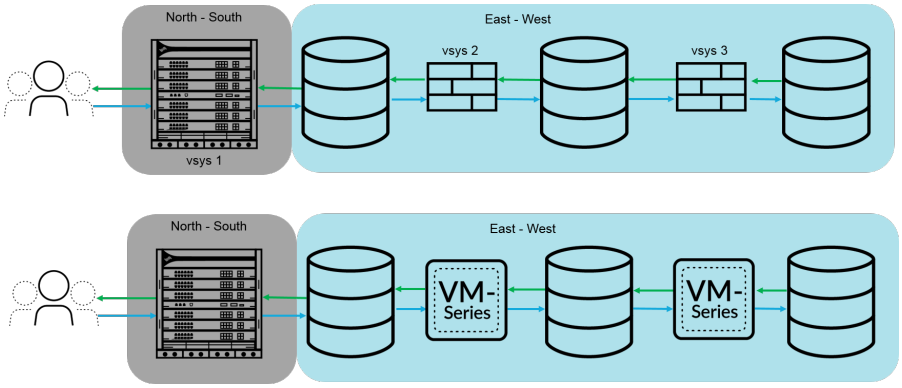
Palo Alto Networks 防火牆與 Cisco ACI 整合

Palo Alto Networks 與 Cisco ACI 整合可讓您在 EPG 之間插入防火牆，當作第 4 層到第 7 層服務。然後，防火牆就可在這些 EPG 內保護應用程式層之間的東西向流量安全，或使用者和應用程式之間的南北向流量安全。

下圖顯示實體 ACI 部署的範例，其中包括整合的 Palo Alto Network 防火牆。ACI 網狀架構中的所有實體都會連線至分葉交換器，這些分葉交換器又會連線至更大的骨幹交換器。當使用者存取應用程式時，ACI 網狀架構會將流量移至正確目的地。為了保護應用程式層之間的流量安全，網路管理員會在每個 EPG 之間插入 Palo Alto Networks 防火牆，當作 L4 至 L7 服務，並建立服務圖形來定義 L4 至 L7 裝置所提供的服務。



部署防火牆服務之後，流量現在的流動就合乎邏輯，如下所示。流量往返於使用者和應用程式中的各層，而不論每個實體實際上從何處及如何連線至網路。



防火牆與 Cisco ACI 整合時，流量會依照 policy-based redirect（基於政策的重新導向；PBR）傳送至防火牆。此外，防火牆的設定和 APIC 的設定完全不同。網路政策模式未依賴防火牆與 APIC 之間的任何其他設定整合，因此提供更大的彈性來設定和部署防火牆。

針對東西向流量，在防火牆的 ACI 網狀架構中定義橋接器網域和子網路。設定 EPG 之間使用 PBR 將流量傳送至防火牆的合約。PBR 會根據包含防火牆 IP 和 MAC 位址的政策，以將流量轉送至防火牆。防火牆介面一律處於第 3 層模式，而且會接收流量並將其路由回 ACI 網狀架構。您可以為

©2023 Palo Alto Networks, Inc.

客戶和提供者連線設定單獨介面，或為進入和輸出流量設定單一介面。本文件中的程序使用單一介面，因為它會簡化整合；您不需要設定最多介面、IP 位址或 VLAN。不過，使用單一介面時，您在定義安全性政策時無法使用區域資訊，而且您必須修改防火牆上的預設內部網路區政策來拒絕流量。

針對南北向流量，您必須使用稱為 L3Out 的專用原則。L3Out 包含租用戶連線至外部路由裝置以及存取外部網路所需的資訊。L3Out 連線所包含的外部網路 EPG 代表可透過 L3Out 政策存取的網路。就像 L3Out 可以將所有外部網路群組到單一 EPG，您也可以使用 vzAny 物件 ACI 來代表 VRF 中的所有 EPG。使用 vzAny 物件時可簡化輸出流量合約的應用，因為只要將新的 EPG 新增至 VRF，就會自動套用合約。在此情況下，外部網路會提供合約，而 vzAny 物件（所有內部 EPG）會使用它。

下節提供構成新世代防火牆與 Cisco ACI 之間整合的元件和概念的其他詳細資料。

- 服務圖形範本
- 多重內容部署

服務圖形範本

防火牆是透過服務圖形來部署於 Cisco ACI。服務圖形可讓您將第 4 層到第 7 層裝置（例如防火牆）整合至流量流程，而不需要 L4-L7 裝置作為 ACI 網狀架構中伺服器的預設閘道。

在 ACI 網狀架構中，防火牆會呈現為您在 APIC 中設定為裝置叢集的 L4-L7 裝置。單一防火牆或部署為 HA 配對的兩個防火牆會設定為裝置叢集。每個裝置叢集都會有一個或多個邏輯介面可說明裝置叢集的介面資訊，以及對應具有實體或虛擬機器監控 (VMM) 網域中 VLAN 的成員防火牆路徑。

服務圖形範本會定義您插入至 EPG 間之流量流程的防火牆裝置叢集。此外，服務圖形範本會定義防火牆的整合方式，以及指派給客戶和提供者 EPG 的邏輯介面。建立服務圖形範本之後，請將它指派給 EPG 和合約。因為服務圖形範本未繫結至特定 EPG 或 合約，所以您可以在多個 EPG 之間重複使用它。APIC 接著會部署服務圖形範本，方法是將它連線至 EPG 之間的橋接器網域。

多重內容部署

Cisco ACI 整合支援劃分成脈絡的實體防火牆，由 ACI 視為個別防火牆來管理。在防火牆上，這些脈絡是防火牆上的虛擬系統 (vsys)，每一個防火牆都獲得授權，可支援一定數量的 vsys 實例。在 ACI 中部署多重 vsys 防火牆時，您必須在租用戶中設定底座管理員，並指派給防火牆服務。

©2023 Palo Alto Networks, Inc.

準備 ACI 環境進行整合

您必須完成下列步驟來準備 Cisco ACI 環境，才能整合防火牆與裝置套件。

STEP 1 | 部署 Panorama。

STEP 2 | 部署防火牆。

- 實體防火牆—將防火牆的頻外管理連接埠連線至一個分葉交換器連接埠，並將至少一個防火牆資料介面連線至交換器。實體防火牆上的防火牆介面是以 VLAN 來設定，以確保連線至正確網路。根據平台專用安全指南來部署防火牆。
- VM-Series 防火牆 # 設定 VM-Series 防火牆的虛擬硬體時，請設定管理介面的連接埠群組。每個連線至網路的 VM-Series 防火牆需要其自己的 NIC。根據您的 Hypervisor 來部署 VM-Series 防火牆。

STEP 3 | 在每個防火牆和 Panorama 上設定管理 IP 位址。

在下列位置執行初始組態：

- 硬體型防火牆
- VM-Series 防火牆
- Panorama

STEP 4 | 新增防火牆給 Panorama 作為受管理的裝置。

STEP 5 | 在防火牆上安裝功能授權。

- 在實體防火牆上註冊和啟動授權。
- 在 VM-Series 防火牆上註冊和啟動 VM-Series 型號授權。
- 使用 Panorama 管理防火牆授權。

STEP 6 | 建立 Cisco ACI 網狀架和管理連線。

在此組態設定過程中，建立實體網域和 VLAN 命名空間。確保任何實體防火牆的資料介面是實體網域的一部分。

STEP 7 | 建立 Cisco ACI VMM 網域設定檔。

如果您使用虛擬機器或 VM-Series 防火牆，請為 VMware vSphere 環境建立 virtual machine monitor（虛擬機器監控器 - VMM）網域設定檔。VMM 網域指定 vSphere 與 ACI 網狀架構之間的連線原則。

©2023 Palo Alto Networks, Inc.

以網路政策模式整合防火牆與 Cisco ACI

以網路政策模式，您會使用政策型重新導向至單一邏輯 HA 介面，以將處於高可用性 (HA) 的一對防火牆整合到東西向或南北向流量。防火牆和 ACI 網狀架構會分開設定，而且防火牆上的位址物件會對應至 ACI 網狀架構中的 EPG。

您可以使用網路原則模式，部署 Palo Alto Networks 防火牆來保護東西向或南北向流量。

- 以網路政策模式部署防火牆來保護東西向流量
- 以網路政策模式部署防火牆來保護南北向流量

以網路政策模式部署防火牆來保護東西向流量

下列程序說明如何部署 Palo Alto Networks 防火牆，以搭配使用不受管理模式與基於原則的重新導向來保護 Cisco ACI 環境中的東西向流量。此程序假設您已完成下列操作：

- 防火牆可操作，並連線至 Cisco ACI 環境中的分葉交換器。此外，必須可透過 APIC 到達每個防火牆的管理介面。
- 防火牆是以主動/被動 HA 模式進行部署。此程序未涵蓋 HA 網路設定，並假設您已事先完成此操作。

若要保護東西向流量，請在防火牆的 ACI 網狀架構中定義橋接器網域和子網路。設定 EPG 之間使用 PBR 將流量傳送至防火牆的合約。PBR 會根據包含防火牆 IP 和 MAC 位址的政策，以將流量轉送至防火牆。防火牆介面一律處於第 3 層模式，而且會接收流量並將其路由回 ACI 網狀架構。您可以為客戶和提供者連線設定單獨介面，或為進入和輸出流量設定單一介面。本文件中的程序使用單一介面，因為它會簡化整合；您不需要設定最多介面、IP 位址或 VLAN。不過，使用單一介面時，您在定義安全性政策時無法使用區域資訊，而且您必須修改防火牆上的預設內部網路區政策來拒絕流量。

此程序會以 one-arm 模式部署防火牆。在 one-arm 模式中，流量會透過單一介面進入和離開防火牆。此通用防火牆介面用於服務圖形範本中的客戶和提供者介面。使用單一介面可藉由減少您必須設定的 IP 位址、VLAN 和介面數目，來簡化與防火牆的整合。不過，one-arm 部署模型是 intrazone（內部網路區），因此您無法使用區域資訊來定義安全性政策。

在防火牆上：

- 建立虛擬路由器和安全性區域
- 設定網路介面
- 設定靜態預設路由
- 建立 EPG 的位址物件
- 建立安全性政策規則

在 Cisco APIC 上：

- 建立 VLAN 集區和網域
- 設定東西向流量的 LLDP 和 LACP 介面政策
- 建立防火牆與 ACI 網狀架構之間的連線

©2023 Palo Alto Networks, Inc.

- 建立 VRF 和橋接器網域
- 建立 L4-L7 裝置
- 建立基於政策的重新導向
- 建立和套用服務圖形範本

建立虛擬路由器和安全性區域

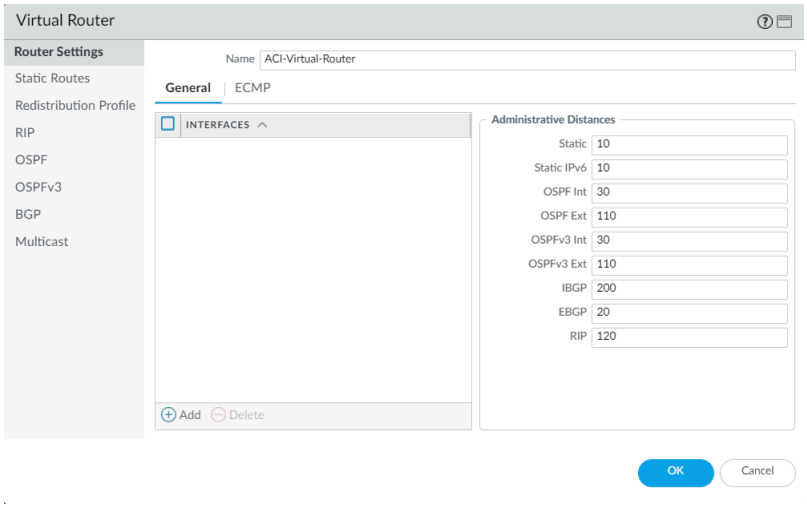
針對租用戶中的每個 VRF，在防火牆上設定虛擬路由器和區域。

STEP 1 | 登入防火牆。

STEP 2 | 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後按一下 **Add**（新增）。

STEP 3 | 為虛擬路由器指定描述性 **Name**（名稱）。

STEP 4 | 按一下 **OK**（確定）。



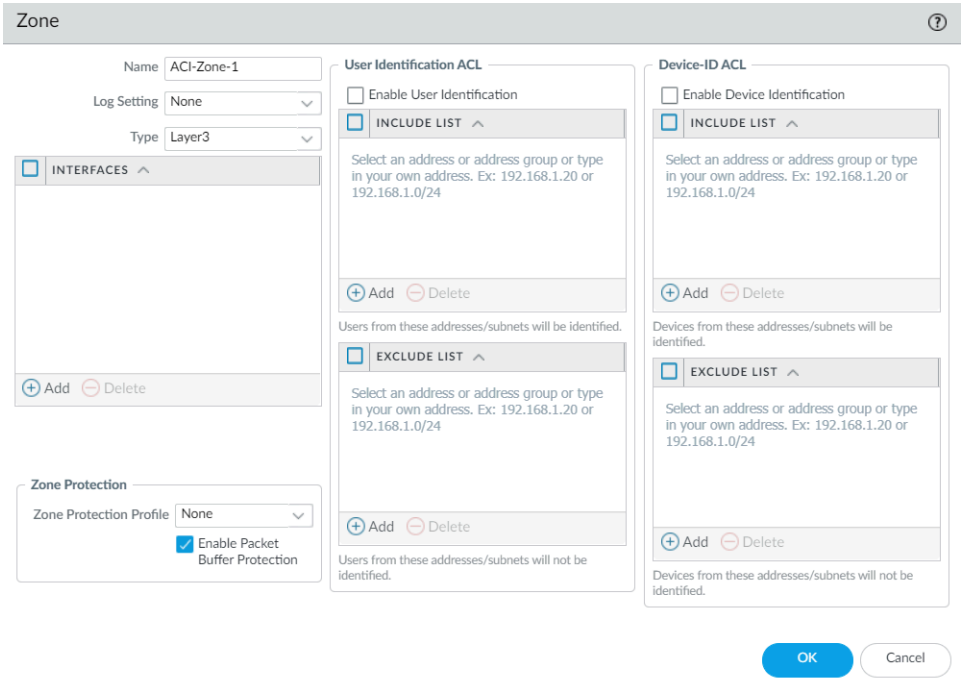
STEP 5 | 選取 **Network**（網路） > **Zones**（區域），然後按一下 **Add**（新增）。

STEP 6 | 為區域指定描述性 **Name**（名稱）。

STEP 7 | 從 **Type**（類型）下拉式清單中，選擇 Layer 3（第三層）。

©2023 Palo Alto Networks, Inc.

STEP 8 | 按一下 **OK**（確定）。



STEP 9 | **Commit**（提交）您的變更。

設定網路介面

設定將防火牆連線至 ACI 分葉交換器的乙太網路介面。此設定中使用的 VLAN ID 號碼應該是 ACI 中指派給防火牆的 VLAN 集區成員。

VM-Series 防火牆不支援彙總乙太網路群組。

STEP 1 | 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後按一下 **Add Aggregate Group**（新增彙總群組）。

STEP 2 | 在第二個 **Interface Name**（介面名稱）欄位中，輸入彙總群組數目。

STEP 3 | 從 **Interface Type**（介面類型）下拉式清單中，選取 [Layer 3（第三層）]。

STEP 4 | 選取 **LACP** 頁籤，然後按一下 **Enable LACP**（啟用 **LACP**）。

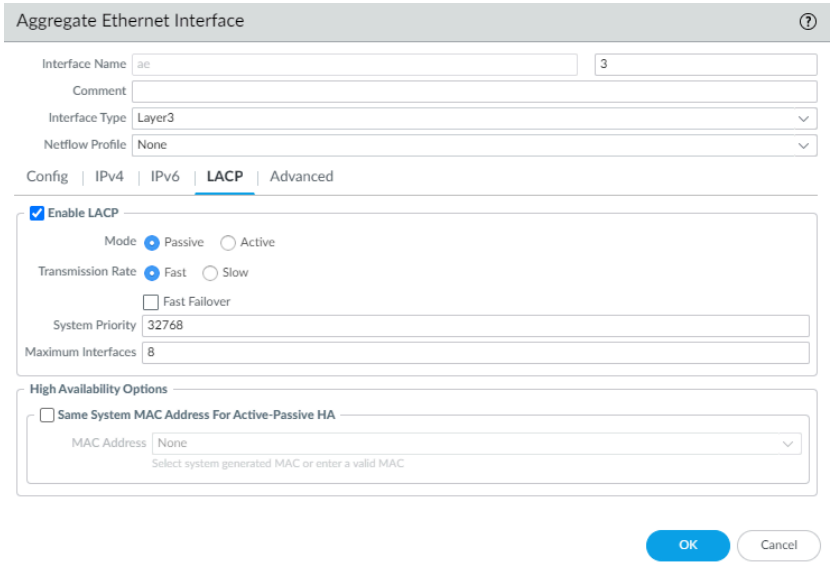
STEP 5 | 選取 **Fast**（快速）作為 **Transmission Rate**（傳輸速率）。

STEP 6 | 在 [High Availability Options（高可用性選項）] 下方，選取 **Enable in HA Passive State**（以 **HA** 被動狀態啟用）。

請不要選取 ***Same System MAC Address for Active-Passive HA***（主動-被動 ***HA*** 的系統 ***MAC*** 位址相同）。此選項讓防火牆配對顯示為交換器的單一裝置，因此流量將流向兩個防火牆，而不只是主動防火牆。

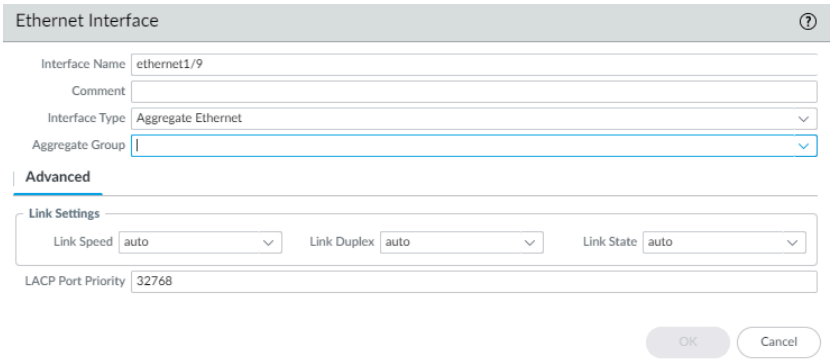
©2023 Palo Alto Networks, Inc.

STEP 7 | 按一下 **OK**（確定）。



STEP 8 | 按一下乙太網路介面名稱進行設定，並將它新增至彙總群組。

1. 從 [Interface Type（介面類型）] 下拉式清單中，選取 **Aggregate Ethernet**（彙總乙太網路）。
2. 選取您在彙總乙太網路群組設定中定義的介面。
3. 按一下 **OK**（確定）。
4. 針對彙總乙太網路群組的每個其他成員介面，重複此步驟。



 ©2023 Palo Alto Networks, Inc.

STEP 9 | 在彙總乙太網路介面上新增租用戶和 VRF 的子介面。

1. 選取彙總乙太網路群組的列，然後按一下 **Add Subinterface**（新增子介面）。
2. 在第二個 **Interface Name**（介面名稱）欄位中，輸入用來識別子介面的數值尾碼。
3. 在 **Tag**（標籤）欄位中，輸入子介面的 VLAN 標籤。
4. 從 **Virtual Router**（虛擬路由器）下拉式清單中，選取您先前設定的虛擬路由器。
5. 從 **Zone**（區域）下拉式清單中，選取您先前設定的區域。
6. 選取 **IPv4** 頁籤。
7. 選取 **Static Type**（靜態類型）。
8. 按一下 **Add**（新增），並以 CIDR 標記法輸入子介面 IP 位址和網路遮罩。
9. 按一下 **OK**（確定）。

設定靜態預設路由

設定靜態預設路由，以將流量從乙太網路子介面導向至子網路路由器。

STEP 1 | 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後按一下您先前在此程序中建立的虛擬路由器。

STEP 2 | 選取 **Static Routes**（靜態路由） > **IPv4**，然後按一下 **Add**（新增）。

STEP 3 | 輸入描述性的 **Name**（名稱）。

STEP 4 | 在 **Destination**（目的地）欄位中，輸入 0.0.0.0/0。

STEP 5 | 從 **Interface**（介面）下拉式清單中，選取您先前在此程序中建立的彙總乙太網路群組。

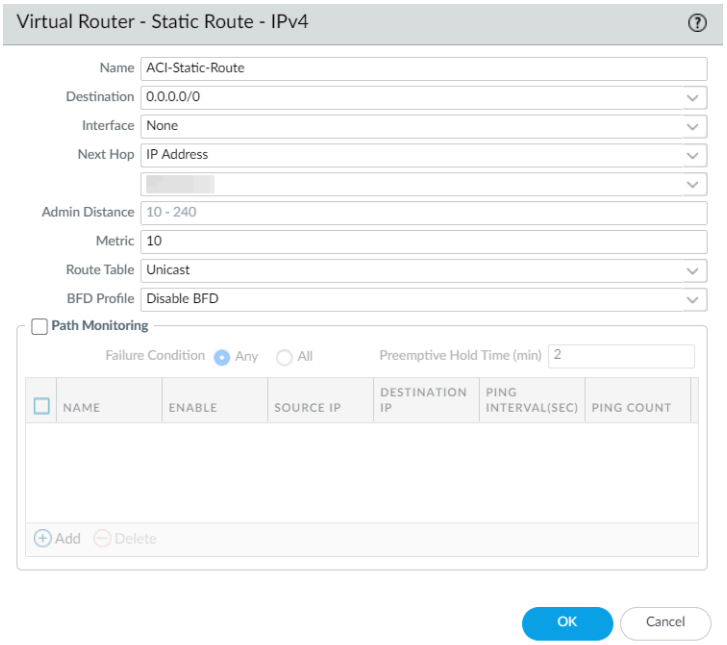
STEP 6 | 從 **Next Hop**（下一個躍點）下拉式清單中選取 [IP Address（IP 位址）]，然後輸入下一個躍點路由器的 IP 位址。

STEP 7 | 按一下 **OK**（確定）。

STEP 8 | 再按一下 **OK**（確定）。

©2023 Palo Alto Networks, Inc.

STEP 9 | **Commit**（提交）您的變更。



建立 EPG 的位址物件

您必須定義位址物件，並將它們對應至要在安全性政策中使用的端點群組 (EPG)。位址群組是使用端點 IP 位址範圍將安全性群組對應至伺服器群組的最佳方式。為每個 EPG 都建立一個位址物件。

STEP 1 | 選取 **Objects**（物件） > **Address**（位址），然後按一下 **Add**（新增）。

STEP 2 | 輸入位址物件的描述性名稱。

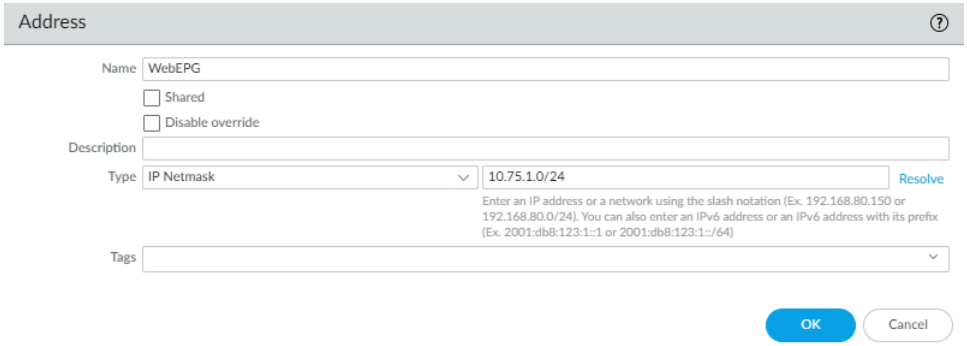
STEP 3 | 從 **Type**（類型）下拉式清單中，選取 [IP Netmask（IP 網路遮罩）]。

STEP 4 | 輸入 IP 網路遮罩。

STEP 5 | 按一下 **OK**（確定）。

STEP 6 | 針對每個 EPG 重複此程序。

STEP 7 | **Commit**（提交）您的變更。



 ©2023 Palo Alto Networks, Inc.

建立安全性政策規則

建立安全性政策規則，以控制 EPG 之間移動的流量。依預設，防火牆允許所有內部網路區流量。因此，因為 EPG 位於相同的區域，所以允許這些 EPG 之間的所有流量。建立新的規則之前，請先將預設內部網路區規則從 allow（允許）變更為 deny（拒絕）。

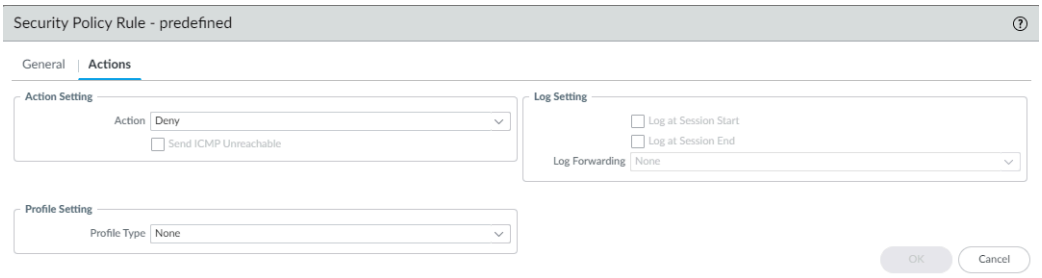
STEP 1 | 選取 **Policies**（政策） > **Security**（安全性）。

STEP 2 | 按一下 intrazone-default（內部網路區預設）以反白顯示該列，然後按一下 **Override**（覆寫）。

STEP 3 | 選取 **Action**（動作）頁籤。

STEP 4 | 從 **Action**（動作）下拉式清單中，選取 [Deny（拒絕）]。

STEP 5 | 按一下 **OK**（確定）。



STEP 6 | 使用您為 EPG 建立的位址物件和區域，根據需要來設定其他安全性政策規則。

建立 VLAN 集區和網域

設定 VLAN 集區，以在您將介面連接至 EPG 的 ACI 基礎結構時用來將 VLAN 配置至防火牆。防火牆的 VLAN 提取應該具有靜態 VLAN 範圍。

設定防火牆的專用網域。需要有防火牆的網域，才能將 VLAN 對應至 EPG。建立實體防火牆的實體網域，並建立 VM-Series 防火牆的 VMM 網域。

STEP 1 | 建立 VLAN 集區。

1. 登入 APIC。
2. 選取 **Fabric**（網狀架構） > **Access Policies**（存取政策） > **Pools**（集區） > **VLAN**。
3. 以滑鼠右鍵按一下 **VLAN**，然後選取 **Create VLAN Pool**（建立 **VLAN** 集區）。
4. 輸入 VLAN 集區的描述性 **Name**（名稱）。
5. 針對 [Allocation Mode（配置模式）]，選取 **Dynamic Allocation**（動態配置）。
6. 按一下 **Encap Blocks**（**Encap** 區塊）右側的加號 (+) 按鈕。
7. 在 **VLAN Range**（**VLAN** 範圍）欄位中，輸入 VLAN 範圍。
8. 從 [Allocation Mode（配置模式）] 下拉式清單中，選取 **Static Allocation**（靜態配置）。
9. 按一下 **OK**（確定）。
10. 按一下 **Submit**（提交）。

©2023 Palo Alto Networks, Inc.

STEP 2 | （僅限實體防火牆）建立實體網域。

1. 選取 **Fabric**（網狀架構） > **Access Policies**（存取政策） > **Physical and External Domains**（實體和外部網域） > **Physical Domains**（實體網域）。
2. 以滑鼠右鍵按一下 **Physical Domain**（實體網域），然後選取 **Create Physical Domain**（建立實體網域）。
3. 輸入實體網域的描述性 **Name**（名稱）。
4. 從 [VLAN Pool（VLAN 集區）] 清單中，選取您在前一個程序中建立的 VLAN 集區。
5. 按一下 **Submit**（提交）。

STEP 3 | （僅限 VM-Series 防火牆）建立 VMM 網域。

1. 選取 **Virtual Networking**（虛擬網路） > **VMM Domains**（**VMM** 網域） > **VMware**。
2. 以滑鼠右鍵按一下 **VMware**，然後選取 **Create vCenter Domain**（建立 **vCenter** 網域）。
3. 輸入 VMM 網域的描述性 **Name**（名稱）。
4. 從 **Virtual Switch**（虛擬交換器）下拉式清單中，選取 **VMware vSphere Distributed Switch**（**VMware vSphere** 分散式交換器）。
5. 從 **Encapsulation**（封裝）下拉式清單中，選取 **VLAN**。
6. 從 **VLAN Pool**（**VLAN** 集區）下拉式清單中，選取 VLAN 集區。
7. 按一下 **vCenter Credentials**（**vCenter** 認證）右側的加號 (+) 按鈕。
8. 輸入描述性 **Profile Name**（設定檔名稱） 和 vCenter 登入資訊。
9. 按一下 **vCenter** 右側的加號 (+) 按鈕。
10. 輸入描述性的 **Name**（名稱）。
11. 從 [Type（類型）] 下拉式清單中，選取 vCenter。
12. 在 **IP/Hostname**（**IP/**主機名稱） 下方，輸入 vCenter IP 位址。
13. 從 **Associated Credential**（相關聯的認證）下拉式清單中，選取您剛才建立的 vCenter 認證設定檔。
14. 按一下 **Submit**（提交）。

設定東西向流量的 LLDP 和 LACP 介面政策

建立政策，以在連線至防火牆的 ACI 介面上啟用 LLDP 和 LACP。

需要有 LLDP，才能在 ACI 環境中正確轉送；ACI 不會在分葉交換器上部署子網路路由器介面，除非在需要該介面的交換器上偵測到端點。LLDP 可協助判斷是否需要子網路路由器介面。

連結失敗時，LACP 提供較大的回復性和復原速度。

©2023 Palo Alto Networks, Inc.

STEP 1 | 建立 LLDP 介面政策。

1. 選取 **Fabric**（網狀架構） > **Access Policies**（存取政策） > **Interface Policies**（介面政策） > **Policies**（政策） > **LLDP Interface**（**LLDP** 介面）。
2. 以滑鼠右鍵按一下 **LLDP Interface**（**LLDP** 介面），然後選取 **Create LLDP Interface Policy**（建立 **LLDP** 介面政策）。
3. 輸入 LLDP 介面政策的描述性 **Name**（名稱）。
4. 針對 **Receive State**（接收狀態），選取 **Enabled**（已啟用）。
5. 針對 **Transmit State**（傳輸狀態），選取 **Enabled**（已啟用）。
6. 按一下 **Submit**（提交）。

STEP 2 | 建立連接埠通道政策以啟用 LACP。

1. 選取 **Fabric**（網狀架構） > **Access Policies**（存取政策） > **Interface Policies**（介面政策） > **Policies**（政策） > **Port Channel**（連接埠通道）。
2. 以滑鼠右鍵按一下 **Port Channel**（連接埠通道），然後選取 **Create Port Channel Policy**（建立連接埠通道政策）。
3. 輸入連接埠通道政策的描述性 **Name**（名稱）。
4. 從 **Mode**（模式）下拉式清單中，選取 **LACP Active**（**LACP** 主動）。
5. 按一下 **Submit**（提交）。

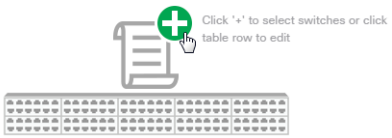
建立防火牆與 ACI 網狀架構之間的連線

使用您稍早在此程序中設定的防火牆的乙太網路介面（或彙總乙太網路群組），透過 VPC 連線將防火牆連接至分葉交換器。將一個或多個介面連線至分葉交換器上的相同連接埠。

STEP 1 | 選取 **Fabric**（網狀架構） > **Access Policies**（存取政策） > **Quick Start**（快速入門）。

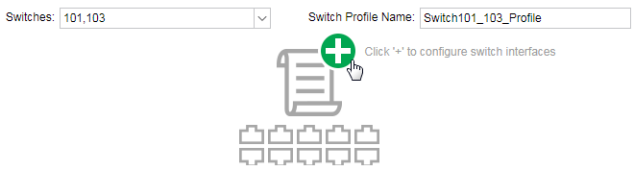
STEP 2 | 按一下 **Configure an interface, PC, and VPC**（設定介面、**PC** 和 **VPC**）。

STEP 3 | 按一下綠色和白色加號 (+)。



STEP 4 | 從 **Switches**（交換器）下拉式清單中，選取防火牆所連線的一個或多個分葉交換器。

STEP 5 | 按一下綠色和白色加號 (+)。



STEP 6 | 選取 [VPC] 作為 **Interface Type**（介面類型）。

STEP 7 | 在 **Interfaces**（介面）欄位中，輸入您防火牆用來連線至分葉交換器的介面數目。

©2023 Palo Alto Networks, Inc.

STEP 8 | 在 **Interface Selector Name**（介面選取器名稱）欄位中，輸入描述性名稱。

STEP 9 | 從 **LLDP Policy**（**LLDP** 政策）下拉式清單中，選取 **LLDP-Enabled**（已啟用 **LLDP**）。

STEP 10 | 從 **Port Channel Policy**（連接埠通道政策）下拉式清單中，選取 **LACP Active**（**LACP** 主動）。

STEP 11 | 從 **Attached Device Type**（連接的裝置類型）下拉式清單中，為實體防火牆選取 **Bare Metal**，或為 VM-Series 選取 **ESX Hosts**（**ESX** 主機）。

STEP 12 | 針對 **Domain**（網域），選取 **Choose One**（選擇一個）。

STEP 13 | 從 **Domain**（網域）下拉式清單中，選取您先前在此程序中建立的實體網域或 VMM 網域。

STEP 14 | 按一下 **Save**（儲存）。

STEP 15 | 按一下 **Save**（儲存），然後按一下 **Submit**（提交）。

STEP 16 | 針對 HA 配對中的第二個防火牆，重複此程序。

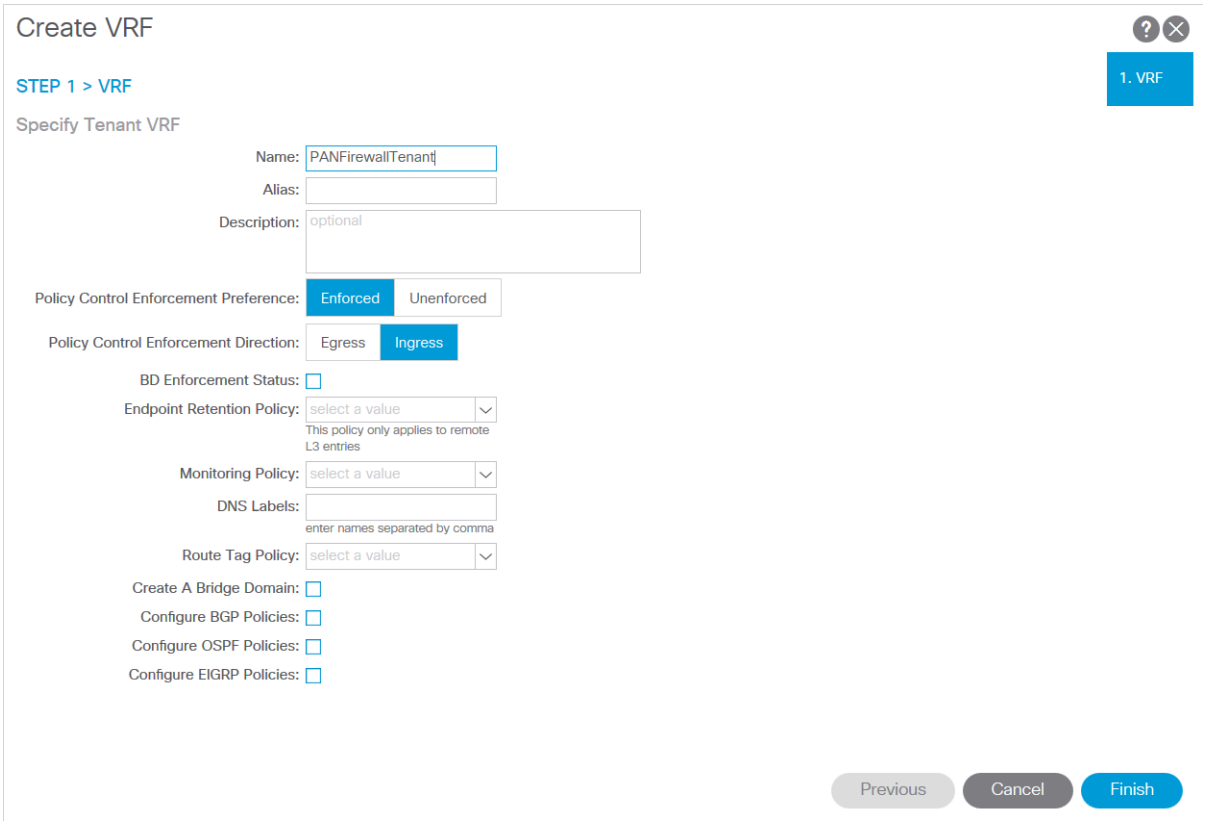
建立 **VRF** 和橋接器網域

租用戶需要一個用於所有橋接器網域和子網路的 VRF。在此範例中，您將建立用於防火牆和端點的單一通用 VRF。然後設定防火牆的專用橋接器網域，並停用資料平面學習。需要停用資料平面學習，才能在橋接器網域中使用基於政策的重新導向。

©2023 Palo Alto Networks, Inc.

STEP 1 | 建立 VRF。

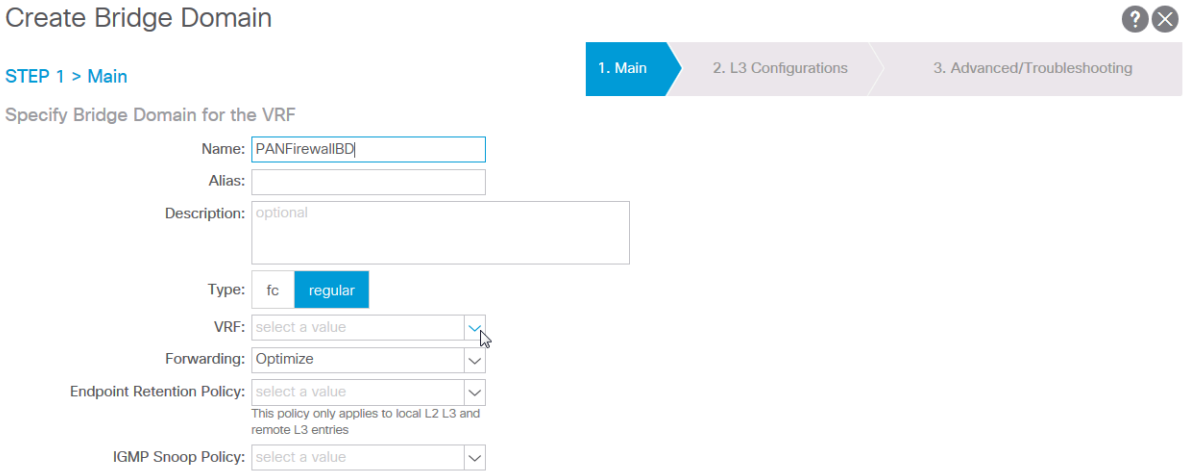
1. 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱。
2. 選取 **Networking**（網路） > **VRFs (VRF)**。
3. 以滑鼠右鍵按一下 **VRFs (VRF)**，然後選取 **Create VRF**（建立 **VRF**）。
4. 輸入 VRF 的描述性 **Name**（名稱）。
5. 清除 **Create A Bridge Domain**（建立橋接器網域）核取方塊。
6. 按一下 **Finish**（完成）。



©2023 Palo Alto Networks, Inc.

STEP 2 | 建立防火牆的橋接器網域。

1. 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱。
2. 選取 **Networking**（網路） > **Bridge Domains**（橋接器網域）。
3. 以滑鼠右鍵按一下 **Bridge Domains**（橋接器網域），然後選取 **Create Bridge Domain**（建立橋接器網域）。
4. 輸入橋接器網域的描述性 **Name**（名稱）。
5. 從 **VRF** 下拉式清單中，選取您在前一個程序中建立的 VRF。
6. 按一下 **Next**（下一步）。



建立 L4-L7 裝置

您必須將防火牆定義為 APIC 中的 L4-L7 裝置，讓 ACI 可以將它插入至流量流程。您可以將 APIC 中的 L4-L7 裝置設定為裝置叢集，而裝置叢集代表單一防火牆或作為單一裝置的防火牆 HA 配對的建構。裝置叢集具有一個或多個邏輯介面可定義具有實體網域中 VLAN 的成員防火牆路徑。

STEP 1 | 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱。

STEP 2 | 選取 **Services**（服務） > **L4-L7** > **Devices**（裝置）。

STEP 3 | 以滑鼠右鍵按一下 **Devices**（裝置），然後選取 **Create L4-L7 Device**（建立 **L4-L7** 裝置）。

STEP 4 | 清除 **Managed**（受管理）核取方塊。

STEP 5 | 輸入 L4-L7 裝置的描述性 **Name**（名稱）。

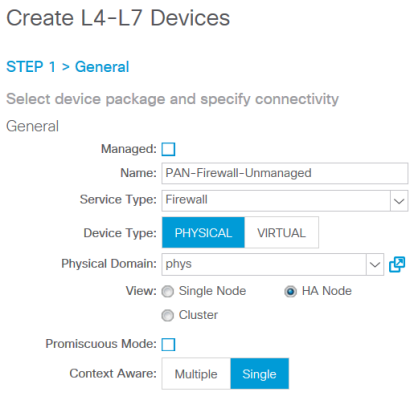
STEP 6 | 從 **Service Type**（服務類型）下拉式清單中，選取 **Firewall**（防火牆）。

STEP 7 | 從 **Device Type**（裝置類型）下拉式清單中，針對實體防火牆選取 **Physical**（實體），或針對 VM-Series 防火牆選取 **Virtual**（虛體）。

STEP 8 | 從 **Domain**（網域）下拉式清單中，選取您先前建立的實體或 VMM 網域。

©2023 Palo Alto Networks, Inc.

STEP 9 | 針對 **View**（檢視），選取 [HA Node（HA 節點）]。



STEP 10 | 在 **Device 1**（裝置 **1**）下方，按一下 **Device Interfaces**（裝置介面）右側的加號 (+) 圖示。

STEP 11 | 輸入此介面的描述性 **Name**（名稱）。

STEP 12 | 在 **Path**（路徑）下方，選取 HA 配對中主要防火牆的路徑。

STEP 13 | 按一下 **Update**（更新）。

STEP 14 | 在 **Device 2**（裝置 **2**）下方，按一下 **Device Interfaces**（裝置介面）右側的加號 (+) 圖示。

STEP 15 | 輸入此介面的描述性 **Name**（名稱）。

STEP 16 | 在 **Path**（路徑）下方，選取 HA 配對中次要防火牆的路徑。

STEP 17 | 按一下 **Update**（更新）。

STEP 18 | 在 **Cluster**（叢集）下方，按一下 **Cluster Interfaces**（叢集介面）右側的加號 (+) 圖示。

STEP 19 | 輸入叢集的描述性 **Name**（名稱）。

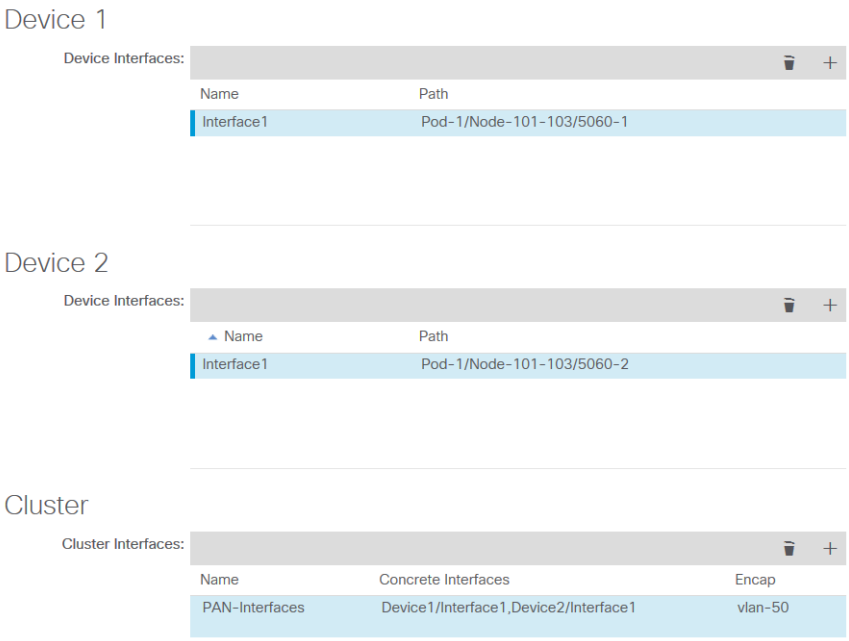
STEP 20 | 從 **Concrete Interface**（實體介面）下方的清單中，選取您在上面設定的兩個介面。APIC 需要您設定兩個介面。不過，因為防火牆與 ACI 網狀架構之間只有一個連線，所以只會使用其中一個介面。

STEP 21 | 在 **Encap** 下方，輸入您稍早建立之靜態 VLAN 集區中的 VLAN。流量將會重新導向至這裡所指派的 VLAN 上的防火牆。

STEP 22 | 按一下 **Update**（更新）。

©2023 Palo Alto Networks, Inc.

STEP 23 | 按一下 **Finish**（完成）。



建立基於政策的重新導向

設定基於政策的重新導向，以將 EPG 之間的流量傳送至防火牆。基於政策的重新導向會利用防火牆上介面的 MAC 位址。在 APIC 上設定 PBR 設定之前，您必須從防火牆取得 MAC 位址。

STEP 1 | 取得防火牆的 MAC 位址。

1. 登入防火牆 CLI。
2. 使用 **`command show interface all`** 顯示所設定介面的 MAC 位址。
3. 複製將接收重新導向流量的介面的 MAC 位址。

STEP 2 | 建立 L4-L7 基於政策的重新導向。

1. 登入 APIC。
2. 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱。
3. 選取 **Policies**（政策） > **Protocol**（通訊協定） > **L4-L7 Policy Based Redirect**（**L4-L7** 基於政策的重新導向）。
4. 以滑鼠右鍵按一下 **L4-L7 Policy Based Redirect**（**L4-L7** 基於政策的重新導向），然後選取 **Create L4-L7 Policy Based Redirect**（建立 **L4-L7** 基於政策的重新導向）。
5. 輸入基於政策的重新導向的描述性 **Name**（名稱）。
6. 按一下 **Destinations**（目的地）右側的加號 (+) 圖示。
7. 在 **IP** 欄位中，輸入將接收重新導向流量的介面的 IP 位址。
8. 在 **MAC** 欄位中，輸入從防火牆 CLI 複製的 MAC 位址。
9. 按一下 **OK**（確定）。
10. 按一下 **Submit**（提交）。

©2023 Palo Alto Networks, Inc.

建立和套用服務圖形範本

建立服務圖形範本，以使用代表基於政策的重新導向整合中防火牆的裝置叢集。建立服務圖形之後，您必須將它套用至 EPG，以保護流量。合約和合約篩選規則會定義可轉送至防火牆的流量。

STEP 1 | 建立服務圖形範本。

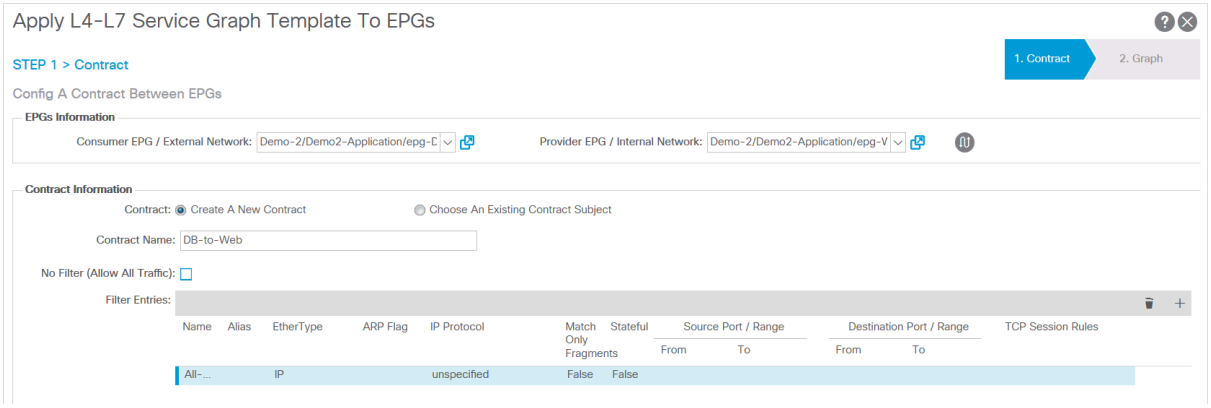
1. 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱。
2. 選取 **Services**（服務） > **L4-L7** > **L4-L7 Service Graph Templates**（**L4-L7** 服務圖形範本）。
3. 以滑鼠右鍵按一下 **L4-L7 Service Graph Template**（**L4-L7** 服務圖形範本），然後選取 **Create L4-L7 Service Graph Template**（建立 **L4-L7** 服務圖形範本）。
4. 輸入服務圖形範本的描述性 **Graph Name**（圖形名稱）。
5. 針對 **Graph Type**（圖形類型），選取 **Create a New One**（建立新的）。
6. 按一下並拖曳您在前一個程序中於客戶與提供者 EPG 之間建立的 L4-L7 裝置。
7. 針對 **Firewall**（防火牆），選取 **Routed**（已路由）。
8. 選取 **Routed Redirect**（路由重新導向）。
9. 按一下 **Submit**（提交）。



©2023 Palo Alto Networks, Inc.

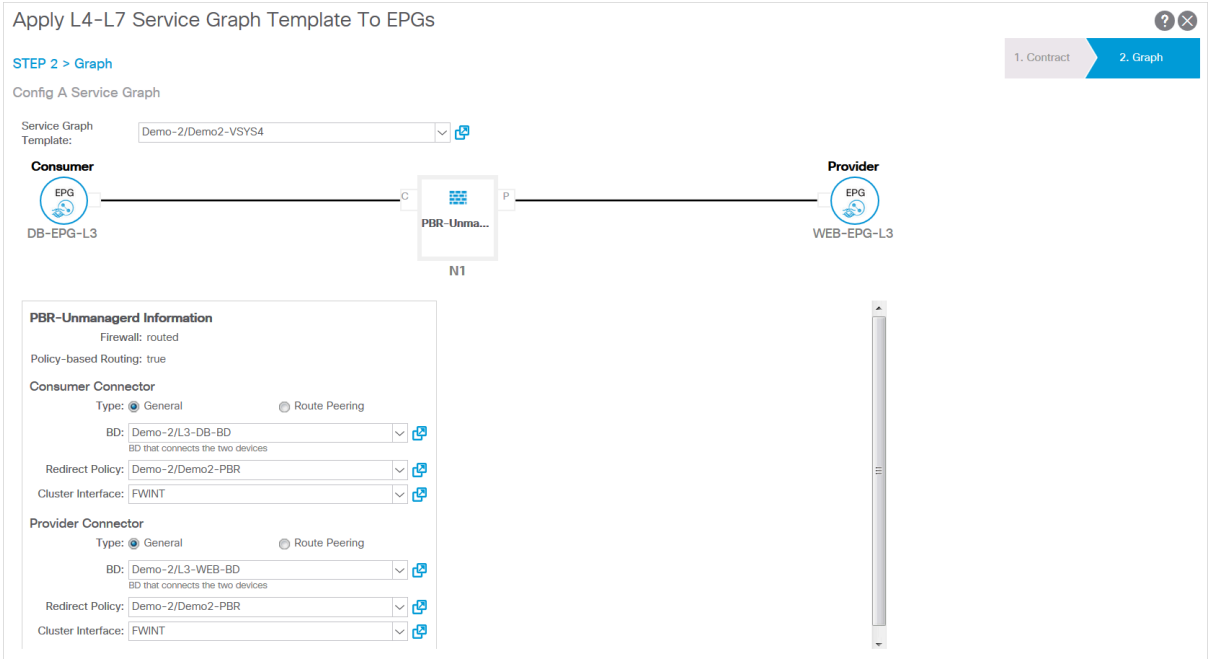
STEP 2 | 套用服務圖形範本。

1. 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱。
2. 選取 **Services**（服務） > **L4-L7**。
3. 在 **EPGs Information**（**EPG** 資訊）窗格中，從 **Consumer EPG**（客戶 **EPG**）和 **Provider EPG**（提供者 **EPG**）下拉式清單中選取客戶和提供者 EPG。
4. 選取 **Create a New Contract**（建立新合約）。
5. 輸入描述性 **Contract Name**（合約名稱）。
6. 清除 [No Filter（無篩選）] **(Allow All Traffic)**（允許所有流量）。不建議使用此選項。若要允許將 EPG 之間的所有流量重新導向至防火牆，建議您建立可執行此操作的篩選。
7. 按一下 **Filter Entries**（篩選項目）右側的加號 (+) 圖示。
8. 建立一個或多個規則來定義允許在 EPG 之間傳遞的流量，並將其重新導向至防火牆。
9. 按一下 **Next**（下一步）。



10. 從 **Service Graph Template**（服務圖形範本）下拉式清單中，選取您在前一個程序中建立的服務圖形範本。
11. 在客戶和提供者窗格中，從 **BD** 下拉式清單中選取包含您防火牆的橋接器網域。
12. 從 **Redirect Policy**（重新導向政策）下拉式清單中，選取您先前建立的基於政策的重新導向。
13. 從 **Cluster Interface**（叢集介面）下拉式清單中，選取您使用 L4-L7 裝置所建立的叢集介面。

©2023 Palo Alto Networks, Inc.



以網路政策模式部署防火牆來保護南北向流量

使用網路原則模式，以搭配使用未受管理模式與基於原則的重新導向來保護進入和離開您資料中心的南北向流量。此程序假設您已完成下列操作：

- 防火牆可操作，並連線至 Cisco ACI 環境中的分葉交換器。此外，必須可透過 APIC 到達每個防火牆的管理介面。
- 防火牆是以主動/被動 HA 模式進行部署。此程序未涵蓋 HA 網路設定，並假設您已事先完成此操作。

若要建立與 ACI 網狀架構外部網路的外部連線，您必須設定 L3Out。而且 L3Out 是專用政策，內含將外部路由裝置連線至租用戶所需的參數。此外，L3Out 所包含的外部 EPG（在 APIC UI 中稱為外部網路）代表可透過 L3Out 存取的網路。外部 EPG 不會動態填入並遵循零信任模型，因此您必須定義 EPG 中的網路。若要更輕鬆地設定，您可以設定網路 0.0.0.0/0，以將所有網路指派給外部 EPG。

若要保護輸入流量，請將 HA 配對中的一個或多個防火牆連線至邊界分葉交換器。邊界分葉交換器是提供與外部路由器之第 3 層連線的分葉交換器。防火牆會使用 vPC 配對中每個分葉交換器上所設定的開放最短路徑優先 (OSPF) 通訊協定以與邊界分葉交換器對等，並使用交換器虛擬介面 (SVI) 以與防火牆通訊。在防火牆上，您將設定連線至您資料中心的介面專用的虛擬路由器。此外，此程序還包括

針對輸出流量，防火牆會使用 OSPF 以向邊界分葉交換器公告外部網路。此外，外部網路 EPG 還會設定成允許防火牆公告到該 EPG 的所有網路。您在 vzAny 受管理物件與外部網路 EPG 之間建立合約，以允許來自 VRF 內任何 EPG 的流量透過防火牆到達外部網路。vzAny 受管理物件可讓您將 VRF 中的所有 EPG 都合併至一個或多個合約，而非建立每個 EPG 的單獨合約。vzAny 受管理物件中所收集的 EPG 會使用外部 EPG 所提供的聯絡人。

與服務管理員模式不同，如果 ACI 基礎結構與防火牆各自完成，則為管理。

在 APIC 上—

©2023 Palo Alto Networks, Inc.

- 建立 VLAN 集區和外部路由網域
- 設定南北向流量的 LLDP 和 LACP 介面政策
- 建立外部路由網路
- 設定要公告至外部防火牆的子網路
- 建立輸出合約
- 建立輸入網頁合約
- 將輸出和輸入合約套用至 EPG

在防火牆上—

- 建立南北向流量的虛擬路由器和安全性區域
- 設定網路介面
- 設定路由重新分配和 OSPF
- 設定外部連線的 NAT

建立 VLAN 集區和外部路由網域

建立 VLAN 集區，以在將介面連接至基礎結構以支援 ACI 網狀架構中的 EPG 時將 VLAN 配置給防火牆。您應該使用防火牆的靜態 VLAN 範圍。

此外，您還必須建立將 VLAN 對應至 EPG 的實體網域。下列程序建立防火牆專用的實體網域。

STEP 1 | 建立 VLAN 集區。

1. 登入 APIC。
2. 選取 **Fabric**（網狀架構） > **Access Policies**（存取政策） > **Pools**（集區） > **VLAN**。
3. 以滑鼠右鍵按一下 **VLAN**，然後選取 **Create VLAN Pool**（建立 **VLAN** 集區）。
4. 輸入 VLAN 集區的描述性 **Name**（名稱）。
5. 針對 [Allocation Mode（配置模式）]，選取 **Dynamic Allocation**（動態配置）。
6. 按一下 **Encap Blocks**（**Encap** 區塊）右側的加號 (+) 按鈕。
7. 在 **VLAN Range**（**VLAN** 範圍）欄位中，輸入 VLAN 範圍。
8. 從 [Allocation Mode（配置模式）] 下拉式清單中，選取 **Static Allocation**（靜態配置）。
9. 按一下 **OK**（確定）。
10. 按一下 **Submit**（提交）。

STEP 2 | 建立外部路由網域。

1. 選取 **Fabric**（網狀架構） > **Access Policies**（存取政策） > **Physical and External Domains**（實體和外部網域） > **External Domains**（外部網域）。
2. 以滑鼠右鍵按一下 **External Routed Domain**（外部路由網域），然後選取 **Create Layer 3 Domain**（建立第三層網域）。
3. 輸入實體網域的描述性 **Name**（名稱）。
4. 從 [VLAN Pool（VLAN 集區）] 清單中，選取您在前一個程序中建立的 VLAN 集區。
5. 按一下 **Submit**（提交）。

©2023 Palo Alto Networks, Inc.

設定南北向流量的 LLDP 和 LACP 介面政策

建立政策，以在連線至防火牆的 ACI 介面上啟用 LLDP 和 LACP。

需要有 LLDP，才能在 ACI 環境中正確轉送；ACI 不會在分葉交換器上部署子網路路由器介面，除非在需要該介面的交換器上偵測到端點。LLDP 可協助判斷是否需要子網路路由器介面。

連結失敗時，LACP 提供較大的回復性和復原速度。

STEP 1 | 建立 LLDP 介面政策。

1. 選取 **Fabric**（網狀架構） > **Access Policies**（存取政策） > **Interface Policies**（介面政策） > **Policies**（政策） > **LLDP Interface**（**LLDP** 介面）。
2. 以滑鼠右鍵按一下 **LLDP Interface**（**LLDP** 介面），然後選取 **Create LLDP Interface Policy**（建立 **LLDP** 介面政策）。
3. 輸入 LLDP 介面政策的描述性 **Name**（名稱）。
4. 針對 **Receive State**（接收狀態），選取 **Enabled**（已啟用）。
5. 針對 **Transmit State**（傳輸狀態），選取 **Enabled**（已啟用）。
6. 按一下 **Submit**（提交）。

STEP 2 | 建立連接埠通道政策以啟用 LACP。

1. 選取 **Fabric**（網狀架構） > **Access Policies**（存取政策） > **Interface Policies**（介面政策） > **Policies**（政策） > **Port Channel**（連接埠通道）。
2. 以滑鼠右鍵按一下 **Port Channel**（連接埠通道），然後選取 **Create Port Channel Policy**（建立連接埠通道政策）。
3. 輸入連接埠通道政策的描述性 **Name**（名稱）。
4. 從 **Mode**（模式）下拉式清單中，選取 **LACP Active**（**LACP** 主動）。
5. 按一下 **Submit**（提交）。

建立外部路由網路

防火牆會透過第 3 層 OSPF 網路將 IP 路由資訊傳遞給 ACI。ACI 搭配使用分葉交換器上的交換器虛擬介面 (SVI) 與每個交換器上的 IP 位址，以取得連線回復。使用 OSPF，建立第 3 層路由網路以與防火牆成為對等。

STEP 1 | 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱。

STEP 2 | 選取 **Networking**（網路） > **External Routed Networks**（外部路由網路）。

STEP 3 | 以滑鼠右鍵按一下 **External Routed Networks**（外部路由網路），並選取 **Create Routed Outside**（建立外部路由）。

STEP 4 | 輸入 **External Routed Network**（外部路由網路）的描述性 **Name**（名稱）。

STEP 5 | 從 **VRF** 下拉式清單中，選取具有外部連線的 VRF。

STEP 6 | 從 **External Routed Domain**（外部路由網域）下拉式清單中，選取您先前建立的外部路由網域。

©2023 Palo Alto Networks, Inc.

STEP 7 | 選取 **OSPF**。

STEP 8 | 輸入 **OSPF Area ID**（**OSPF** 區域 **ID**）。區域 ID 可以使用十進位數字或小數點十進位形式表示。例如，區域 1 與區域 0.0.0.1 相同，或區域 271 與區域 0.0.1.15 相同。區域 ID 範圍是 0 (0.0.0.0) 到 4294967295 (255.255.255.255)。

STEP 9 | 針對 **OSPF Area Type**（**OSPF** 區域類型），選取 **Regular Area**（一般區域）。

STEP 10 | 按一下 **Nodes and Interface Profiles**（節點和介面設定檔）右側的加號 (+) 按鈕，以使用連線至防火牆的邊界分葉交換器的節點來建立節點設定檔。

STEP 11 | 輸入 **Node Profile**（節點設定檔）的描述性 **Name**（名稱）。

STEP 12 | 將節點連接至節點設定檔。

1. 按一下 **Nodes**（節點）右側的加號 (+) 按鈕。這會開啟 **Select Node**（選取節點）視窗。
2. 從 **Node ID**（節點 **ID**）下拉式清單中，選取防火牆所連線的節點。
3. 在 **Router ID**（路由器 **ID**）中，輸入連接至分葉交換器的路由器的 IP 位址。
4. 按一下 **OK**（確定）。
5. 按一下 **Nodes and Interface Profiles**（節點和介面設定檔）右側的加號 (+) 按鈕。
6. 輸入 **Node Profile**（節點設定檔）的描述性 **Name**（名稱）。
7. 按一下 **Nodes**（節點）右側的加號 (+) 按鈕。這會開啟 **Select Node**（選取節點）視窗。
8. 從 **Node ID**（節點 **ID**）下拉式清單中，選取次要 HA 防火牆所連線的節點。
9. 在 **Router ID**（路由器 **ID**）中，輸入連接至第二個分葉交換器的路由器的 IP 位址。
10. 按一下 **OK**（確定）。

©2023 Palo Alto Networks, Inc.

STEP 13 | 連接節點設定檔的 OSPF 介面設定檔。

1. 輸入 OSPF 介面設定檔的描述性 **Name**（名稱）。
2. 按一下 **Next**（下一步）。
3. 從 [OSPF Policy（OSPF 政策）] 下拉式清單中，選取 **Create OSPF Interface Policy**（建立 **OSPF** 介面政策）。
4. 輸入 OSPF 介面政策的描述性 **Name**（名稱）。
5. 選取 **MTU Ignore**（**MTU** 忽略）。
6. 按一下 **Submit**（提交）。
7. 按一下 **Next**（下一步）。
8. 按一下 **SVI**。
9. 按一下 **SVI Interfaces**（**SVI** 介面）右側的加號 (+) 按鈕。這會開啟 **Select SVI**（選取 **SVI**）視窗。
10. 按一下 **Virtual Port Channel**（虛擬連接埠通道）。
11. 選取防火牆連線至分葉交換器之連接埠和連接埠通道介面的路徑。
12. 在 **Encap** 中，輸入用於設定檔外部第 3 層的 VLAN 封裝。
13. 針對 [Mode（模式）]，選取 **Trunk**（中繼）。
14. 在 **Side A IPv4 Primary Address**（**A** 端 **IPv4** 主要位址）欄位中，輸入連接至設定檔外部第 3 層之路徑的主要 IP 位址。
15. 在 **Side B IPv4 Primary Address**（**B** 端 **IPv4** 主要位址）欄位中，輸入連接至設定檔外部第 3 層之路徑的次要 IP 位址。
16. 按一下 **OK**（確定）。

STEP 14 | 按一下 **OK**（確定），以關閉 [Create Interface Profile（建立介面設定檔）] 視窗。

STEP 15 | 按一下 **OK**（確定），以關閉 [Create Node Profile（建立節點設定檔）] 視窗。

STEP 16 | 按一下 **Next**（下一步）。

STEP 17 | 按一下 **External EPG Networks**（外部 **EPG** 網路）右側的加號 (+) 按鈕。這會開啟 **Create Routed Outside**（建立外部路由）視窗。

STEP 18 | 輸入外部網路的描述性 **Name**（名稱）。

STEP 19 | 將子網路新增至外部網路。

1. 按一下 **Subnets**（子網路）右側的加號 (+) 按鈕。
2. 輸入子網路預設閘道的 IP 位址和遮罩。
3. 選取 **Export Route Control Subnet**（匯出路由控制子網路）。
4. 選取 **External Subnets for External EPG**（外部 **EPG** 的外部子網路）。
5. 按一下 **OK**（確定）。

STEP 20 | 按一下 **Finish**（完成）。

©2023 Palo Alto Networks, Inc.

設定要公告至外部防火牆的子網路

依預設，不會將 ACI 網狀架構中的子網路公告至外部網路。您必須設定要在外部公告的子網路。

STEP 1 | 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱。

STEP 2 | 選取 **Networking**（網路） > **Bridge Domains**（橋接器網域） > **<your bridge domain>**。

STEP 3 | 按一下 **L3 Configurations**（**L3** 設定）。

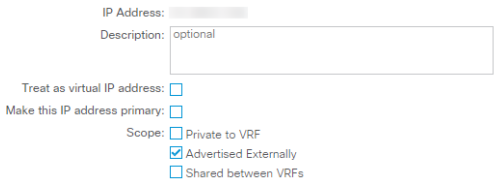
STEP 4 | 按一下 **Associated L3 Outs**（相關聯的 **L3** 輸出）右側的加號 (+) 按鈕。

STEP 5 | 從 **L3 Out**（**L3** 輸出）下拉式清單中，選取您在前一個程序中建立的第三層外部路由網路連線。

STEP 6 | 按一下 **Update**（更新）。

STEP 7 | 選取 **Networking**（網路） > **Bridge Domains**（橋接器網域） > **<your bridge domain>** > **Subnets**（子網路） > **<externally advertised subnet>**。

STEP 8 | 將 [Scope（範圍）] 設定為 **Advertised Externally**（外部公告）。



STEP 9 | 按一下 **Submit**（提交）。

建立輸出合約

建立篩選可允許 DNS、NTP、HTTP 和 HTTPS 流量的合約。您將使用此合約來允許 VRF 中的所有端點連線外部網路，但限制傳送至防火牆的流量。

STEP 1 | 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱。

STEP 2 | 選取 **Contracts**（合約） > **Filters**（篩選）

STEP 3 | 以滑鼠右鍵按一下 **Filters**（篩選），然後選取 **Create Filter**（建立篩選）。

STEP 4 | 輸入篩選的描述性 **Name**（名稱）。

STEP 5 | 建立 UDP 流量的篩選項目。

1. 按一下 **Entries**（項目）右側的加號 (+) 按鈕。
2. 輸入 **UDP** 篩選的描述性 **Name**（名稱）。
3. 從 **EtherType** 下拉式清單中，選取 **IP**。
4. 從 **IP Protocol**（**IP** 通訊協定）下拉式清單中，選取 **udp**。
5. 從 **Destination Port From**（目的地連接埠來源）下拉式清單中，選取 **dns**。
6. 按一下 **Update**（更新）。

©2023 Palo Alto Networks, Inc.

STEP 6 | 建立 TCP 流量的篩選項目。

1. 按一下 **Entries**（項目）右側的加號 (+) 按鈕。
2. 輸入 **TCP** 篩選的描述性 **Name**（名稱）。
3. 從 **EtherType** 下拉式清單中，選取 **IP**。
4. 從 **IP Protocol**（**IP** 通訊協定）下拉式清單中，選取 **tcp**。
5. 從 **Destination Port From**（目的地連接埠來源）下拉式清單中，選取 **dns**。
6. 按一下 **Update**（更新）。

STEP 7 | 建立 NTP 流量的篩選項目。

1. 按一下 **Entries**（項目）右側的加號 (+) 按鈕。
2. 輸入 **NTP** 篩選的描述性 **Name**（名稱）。
3. 從 **EtherType** 下拉式清單中，選取 **IP**。
4. 從 **IP Protocol**（**IP** 通訊協定）下拉式清單中，選取 **udp**。
5. 在 **Destination Port From**（目的地連接埠來源）欄位中，輸入 123。
6. 按一下 **Update**（更新）。

STEP 8 | 建立 HTTP 流量的篩選項目。

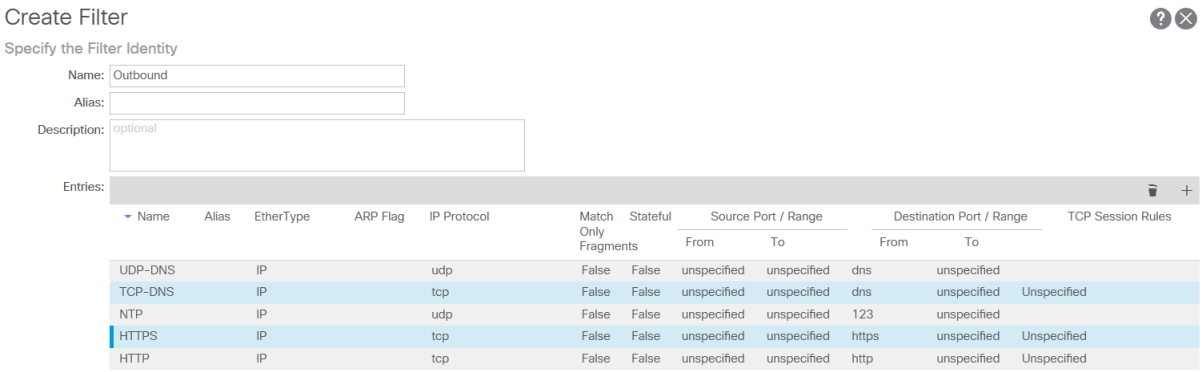
1. 按一下 **Entries**（項目）右側的加號 (+) 按鈕。
2. 輸入 **HTTP** 篩選的描述性 **Name**（名稱）。
3. 從 **EtherType** 下拉式清單中，選取 **IP**。
4. 從 **IP Protocol**（**IP** 通訊協定）下拉式清單中，選取 **tcp**。
5. 從 **Destination Port From**（目的地連接埠來源）下拉式清單中，選取 **http**。
6. 按一下 **Update**（更新）。

STEP 9 | 建立 HTTPS 流量的篩選項目。

1. 按一下 **Entries**（項目）右側的加號 (+) 按鈕。
2. 輸入 **HTTP** 篩選的描述性 **Name**（名稱）。
3. 從 **EtherType** 下拉式清單中，選取 **IP**。
4. 從 **IP Protocol**（**IP** 通訊協定）下拉式清單中，選取 **tcp**。
5. 從 **Destination Port From**（目的地連接埠來源）下拉式清單中，選取 **https**。
6. 按一下 **Update**（更新）。

©2023 Palo Alto Networks, Inc.

STEP 10 | 按一下 **Submit**（提交）。



STEP 11 | 建立輸出流量的合約。

1. 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱，然後選取 **Contracts**（合約）。
2. 以滑鼠右鍵按一下 **Contracts**（合約），然後選取 **Create Contract**（建立合約）。
3. 輸入 **Contract**（合約）的描述性 **Name**（名稱）。
4. 按一下 **Subjects**（主體）右側的加號 (+) 按鈕。
5. 輸入 **Subject**（主體）的描述性 **Name**（名稱）。
6. 在 [Filter Chain（篩選鏈）] 下方，按一下 **Filters**（篩選）右側的加號 (+) 按鈕。
7. 從下拉式清單中，選取您先前建立的篩選。
8. 按一下 **OK**（確定）。

STEP 12 | 按一下 **Submit**（提交）。

建立輸入網頁合約

您也必須建立一個合約和多個篩選，以允許輸入流量到達受防火牆保護的伺服器。下列程序說明如何建立一個合約和多個篩選，以允許 HTTP 和 HTTPS 網頁流量存取受防火牆保護的資源。

STEP 1 | 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱。

STEP 2 | 選取 **Contracts**（合約） > **Filters**（篩選）

STEP 3 | 以滑鼠右鍵按一下 **Filters**（篩選），然後選取 **Create Filter**（建立篩選）。

STEP 4 | 輸入篩選的描述性 **Name**（名稱）。

STEP 5 | 建立 HTTP 流量的篩選項目。

1. 按一下 **Entries**（項目）右側的加號 (+) 按鈕。
2. 輸入 **HTTP** 篩選的描述性 **Name**（名稱）。
3. 從 **EtherType** 下拉式清單中，選取 **IP**。
4. 從 **IP Protocol**（IP 通訊協定）下拉式清單中，選取 **tcp**。
5. 從 **Destination Port From**（目的地連接埠來源）下拉式清單中，選取 **http**。
6. 按一下 **Update**（更新）。

©2023 Palo Alto Networks, Inc.

STEP 6 | 建立 HTTPS 流量的篩選項目。

1. 按一下 **Entries**（項目）右側的加號 (+) 按鈕。
2. 輸入 **TCP** 篩選的描述性 **Name**（名稱）。
3. 從 **EtherType** 下拉式清單中，選取 **IP**。
4. 從 **IP Protocol**（**IP** 通訊協定）下拉式清單中，選取 **tcp**。
5. 從 **Destination Port From**（目的地連接埠來源）下拉式清單中，選取 **https**。
6. 按一下 **Update**（更新）。

STEP 7 | 按一下 **Submit**（提交）。

STEP 8 | 建立輸入網頁流量的合約。

1. 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱，然後選取 **Contracts**（合約）。
2. 以滑鼠右鍵按一下 **Contracts**（合約），然後選取 **Create Contract**（建立合約）。
3. 輸入 **Contract**（合約）的描述性 **Name**（名稱）。
4. 按一下 **Subjects**（主體）右側的加號 (+) 按鈕。
5. 輸入 **Subject**（主體）的描述性 **Name**（名稱）。
6. 在 [Filter Chain（篩選鏈）] 下方，按一下 **Filters**（篩選）右側的加號 (+) 按鈕。
7. 從下拉式清單中，選取您先前建立的篩選。
8. 按一下 **OK**（確定）。

STEP 9 | 按一下 **Submit**（提交）。

將輸出和輸入合約套用至 EPG

現在，您必須將輸入和輸出合約套用至適當的 EPG。

針對 VRF 內要將流量傳送至外部目的地的所有 EPG（EPG 集合），每個內部 EPG 都必須與外部 EPG 設定合約。一般而言，您需要在每個內部 EPG 與外部 EPG 之間建立單獨合約。不過，使用 vzAny 物件，您可以動態將相同的合約套用至所有 EPG。EPG 集合會使用合約，而外部 EPG 會提供合約。您可以在合約中設定特定流量設定檔，或將所有流量傳送至防火牆，並允許它控制離開資料中心的流量。此外，任何加入 VRF 的新 EPG 都會自動套用合約。

套用輸入合約，因此內部 EPG 是提供者，而外部 EPG 是客戶。會先根據合約檢查流向內部 EPG 的流量，接著防火牆會視需要進一步保護任何允許的流量。

©2023 Palo Alto Networks, Inc.

STEP 1 | 將輸出合約套用至 VRF 中的所有 EPG。

1. 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱。
2. 選取 **Networking**（網路） > **VRFs (VRF)** > **<you VRF>** > **EPG Collection for VRF**（**VRF** 的 **EPG** 集合）。
3. 按一下 **Consumed Contracts**（耗用的合約）右側的加號 (+) 按鈕。
4. 從 **Name**（名稱）下拉式清單中，選取輸出合約。
5. 按一下 **Update**（更新）。
6. 選取 **Networking**（網路） > **External Routed Networks**（外部路由網路） > **<your external routed network>** > **Networks**（網路） > **External**（外部）。
7. 按一下 **Provided Contracts**（提供的合約）右側的加號 (+) 按鈕。
8. 從 **Name**（名稱）下拉式清單中，選取輸出合約。
9. 按一下 **Update**（更新）。

STEP 2 | 套用輸入合約，因此內部 EPG 會將它提供給外部 EPG。

1. 在 **Tenants**（租用戶）頁籤上，按兩下租用戶名稱。
2. 選取 **Application Profiles**（應用程式設定檔） > **<your application profile>** > **Application EPGs**（應用程式 **EPG**） > **<your application EPG>** > **Contracts**（合約）。
3. 以滑鼠右鍵按一下 **Contracts**（合約），然後選取 **Add Provided Contract**（新增提供的合約）。
4. 從 **Contract**（合約）下拉式清單中，選取輸入合約。
5. 按一下 **Submit**（提交）。
6. 在同一租用戶上，選取 **Networking**（網路） > **External Routed Networks**（外部路由網路） > **<your external routed network>** > **Networks**（網路） > **External**（外部）。
7. 在 [Contracts（合約）] 頁籤上，按一下 **Consumed Contracts**（耗用的合約）右側的加號 (+) 按鈕。
8. 從 **Name**（名稱）下拉式清單中，選取輸入合約。
9. 按一下 **Update**（更新）。

建立南北向流量的虛擬路由器和安全性區域

在防火牆上建立虛擬路由器和安全性區域，以符合 ACI 上的租用戶和 VRF。

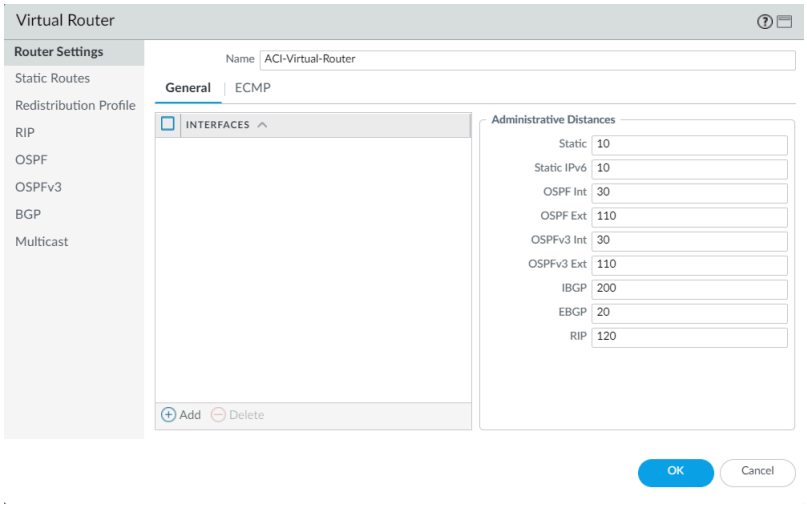
STEP 1 | 登入防火牆。

STEP 2 | 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後按一下 **Add**（新增）。

STEP 3 | 為虛擬路由器指定描述性 **Name**（名稱）。

©2023 Palo Alto Networks, Inc.

STEP 4 | 按一下 **OK**（確定）。

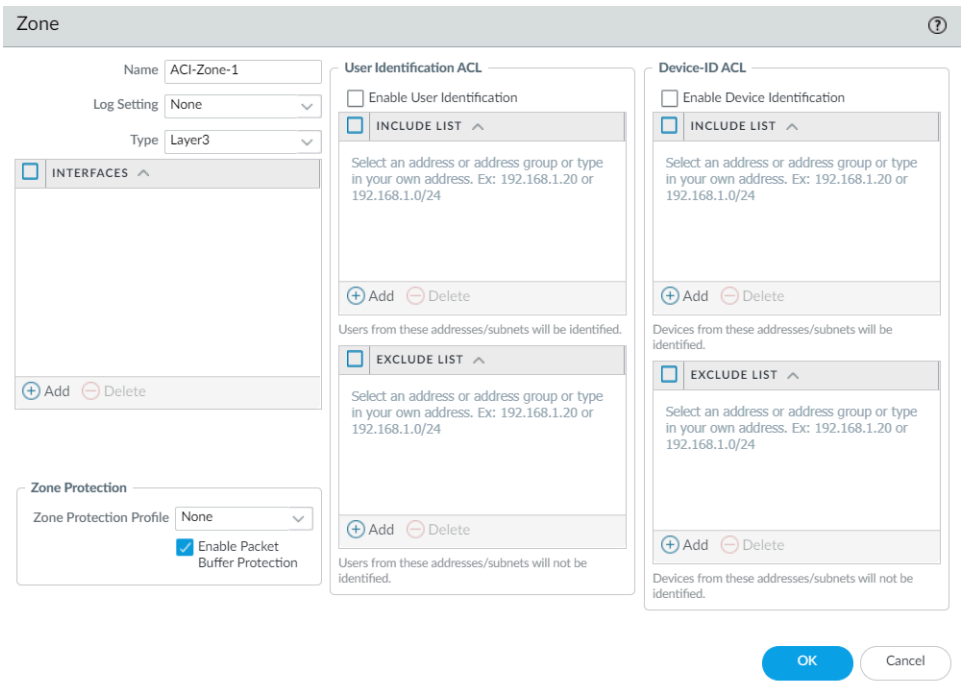


STEP 5 | 選取 **Network**（網路） > **Zones**（區域），然後按一下 **Add**（新增）。

STEP 6 | 為區域指定描述性 **Name**（名稱）。

STEP 7 | 從 **Type**（類型）下拉式清單中，選擇 Layer 3（第三層）。

STEP 8 | 按一下 **OK**（確定）。



STEP 9 | **Commit**（提交）您的變更。

設定網路介面

設定防火牆用來連線至 ACI 分葉交換器的彙總乙太網路介面、成員介面和子介面。如果您要使用 VM-Series 防火牆，則請使用預估介面，而非彙總介面。

©2023 Palo Alto Networks, Inc.

VM-Series 防火牆不支援彙總乙太網路群組。

STEP 1 | 選取 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路），然後按一下 **Add Aggregate Group**（新增彙總群組）。

STEP 2 | 在第二個 **Interface Name**（介面名稱）欄位中，輸入彙總群組數目。

STEP 3 | 從 **Interface Type**（介面類型）下拉式清單中，選取 [Layer 3（第三層）]。

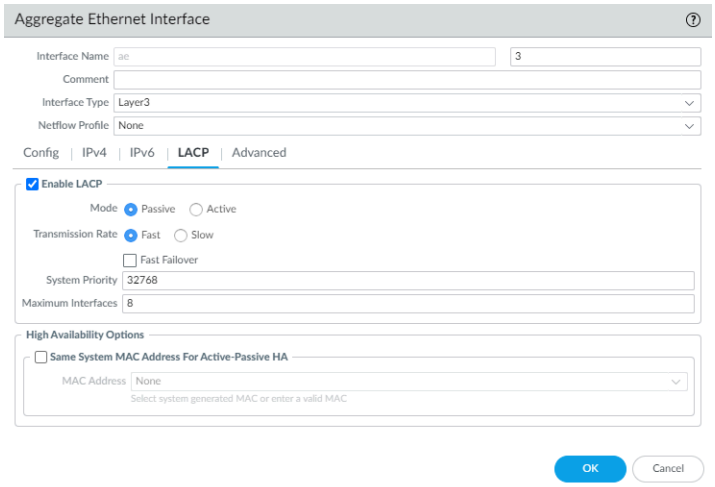
STEP 4 | 選取 **LACP** 頁籤，然後按一下 **Enable LACP**（啟用 **LACP**）。

STEP 5 | 選取 **Fast**（快速）作為 **Transmission Rate**（傳輸速率）。

STEP 6 | 在 [High Availability Options（高可用性選項）] 下方，選取 **Enable in HA Passive State**（以 **HA** 被動狀態啟用）。

請不要選取 ***Same System MAC Address for Active-Passive HA***（主動-被動 ***HA*** 的系統 ***MAC*** 位址相同）。此選項讓防火牆配對顯示為交換器的單一裝置，因此流量將流向兩個防火牆，而不只是主動防火牆。

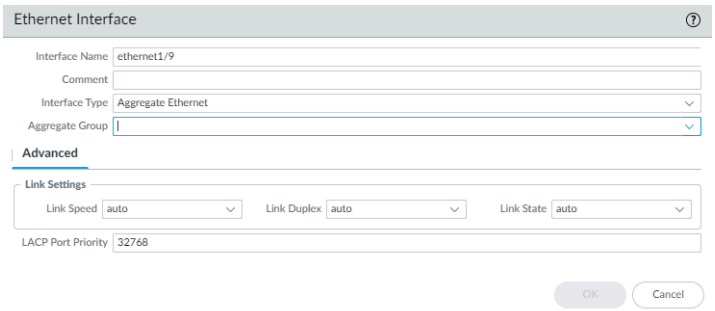
STEP 7 | 按一下 **OK**（確定）。



©2023 Palo Alto Networks, Inc.

STEP 8 | 按一下乙太網路介面名稱進行設定，並將它新增至彙總群組。

1. 從 [Interface Type（介面類型）] 下拉式清單中，選取 **Aggregate Ethernet**（彙總乙太網路）。
2. 選取您在彙總乙太網路群組設定中定義的介面。
3. 按一下 **OK**（確定）。
4. 針對彙總乙太網路群組的每個其他成員介面，重複此步驟。



STEP 9 | 在彙總乙太網路介面上新增租用戶和 VRF 的子介面。

1. 選取彙總乙太網路群組的列，然後按一下 **Add Subinterface**（新增子介面）。
2. 在第二個 **Interface Name**（介面名稱）欄位中，輸入用來識別子介面的數值尾碼。
3. 在 **Tag**（標籤）欄位中，輸入子介面的 VLAN 標籤。
4. 從 **Virtual Router**（虛擬路由器）下拉式清單中，選取您先前設定的虛擬路由器。
5. 從 **Zone**（區域）下拉式清單中，選取您先前設定的區域。
6. 選取 **IPv4** 頁籤。
7. 選取 **Static Type**（靜態類型）。
8. 按一下 **Add**（新增），並以 CIDR 標記法輸入子介面 IP 位址和網路遮罩。
9. 按一下 **OK**（確定）。

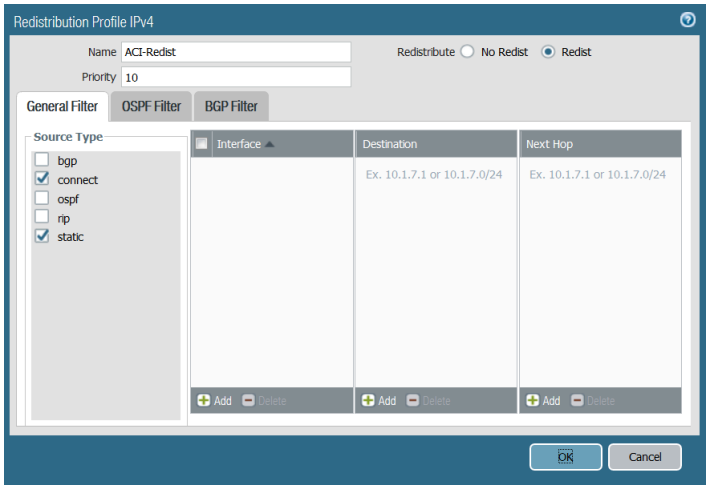
設定路由重新分配和 OSPF

設定路由重新分配，讓來自防火牆的路由資訊可用於連接至分葉交換器的對外路由器。然後，在防火牆上設定 OSPF，並指派 router-id、區域號碼和介面來形成相鄰項。

©2023 Palo Alto Networks, Inc.

STEP 1 | 設定路由重新分配。

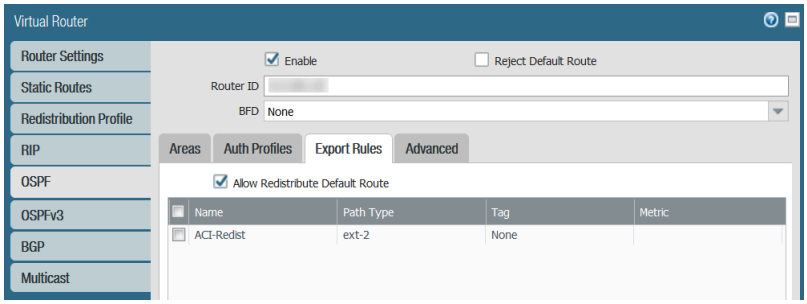
1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後按一下您稍早建立的虛擬路由器。
2. 選取 **Redistribution Profile**（重新分配設定檔） > **IPv4** > **Add**（新增）。
3. 輸入重新分配設定檔的描述性 **Name**（名稱）。
4. 輸入優先順序。
5. 針對 **Redistribute**（重新分配），選取 **Redist**（重新分配）。
6. 在 **General Filters**（一般篩選）下方，核取 **connect**（連線）和 **static**（靜態）。
7. 按一下 **OK**（確定）。



©2023 Palo Alto Networks, Inc.

STEP 2 | 設定 OSPF。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器），然後按一下您稍早建立的虛擬路由器。
2. 選取 **Router Settings**（路由器設定） > **ECMP**，然後選取 **Enable**（啟用）。
3. 選取 **OSPF**，然後選擇 **Enable**（啟用）。
4. 輸入 OSPF **Router ID**（路由器 **ID**）。
5. 在 **Area**（區域）下方，按一下 **Add**（新增）。
6. 輸入 **Area ID**（區域 **ID**）。此值必須符合您在 APIC 上建立外部路由網路時所指派的值。在防火牆上，這必須以小數點十進位形式輸入。例如，如果您在 APIC 中輸入區域 ID 10，則防火牆上的對等項目為 0.0.0.10。
7. 選取 **Interface**（介面） > **Add**（新增）。
8. 輸入連線至外部網路 EPG 的介面，然後按一下 **OK**（確定）。
9. 選取 **Export Rules**（匯出規則） > **Add**（新增）。
10. 從 **Name**（名稱）下拉式清單中選取您上面建立的重新分配設定檔，然後按一下 **OK**（確定）。
11. 選取 **Allow Redistribute Default Route**（允許重新分配預設路由）。
12. 按一下 **OK**（確定）。



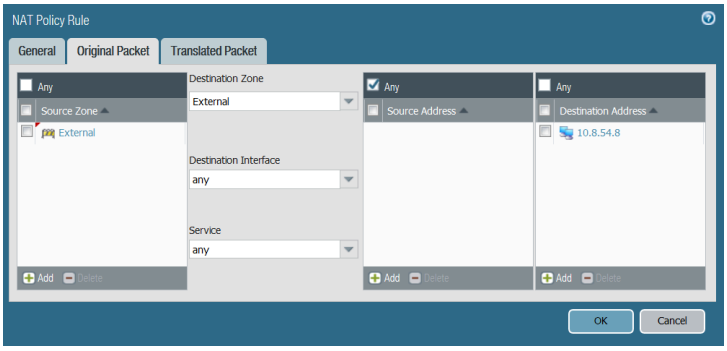
設定外部連線的 NAT

如果防火牆具有外部介面可用於連線至資料中心外部的網路，則您只需要設定 NAT。雖然不需要 NAT，但是您可以使用此程序將資料中心內的私人 IP 位址轉譯為外部的公共 IP 位址。針對進入資料中心內 EPG 的伺服器的流量設定位址轉譯，以開始設定 NAT。然後，設定 NAT 政策，以將來自任何 EPG 之輸出流量的來源位址轉譯為外部介面 IP 位址。

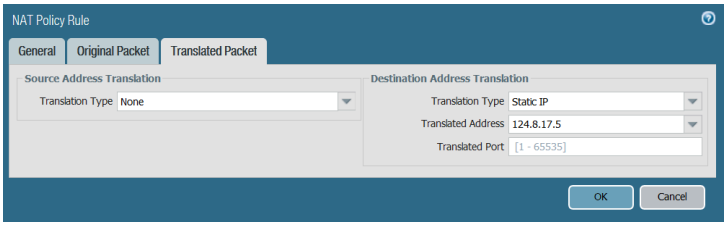
©2023 Palo Alto Networks, Inc.

STEP 1 | 針對進入資料中心內 EPG 的流量設定位址轉譯。

1. 選取 **Policies**（政策） > **NAT**，然後按一下 **Add**（新增）。
2. 輸入 NAT 政策規則的描述性 **Name**（名稱）。
3. 選取 **Original Packet**（原始封包），然後按一下 **Source Zone**（來源區域）下方的 **Add**（新增）。
4. 從下拉式清單中，選取來源區域。
5. 從 **Destination Zone**（目的地區域）下拉式清單中，選取目的地區域。
6. 針對 **Source Address**（來源位址），選取 **Any**（任何）。
7. 按一下 **Destination Address**（目的地位址）下方的 **Add**（新增），然後輸入外部 IP 位址。



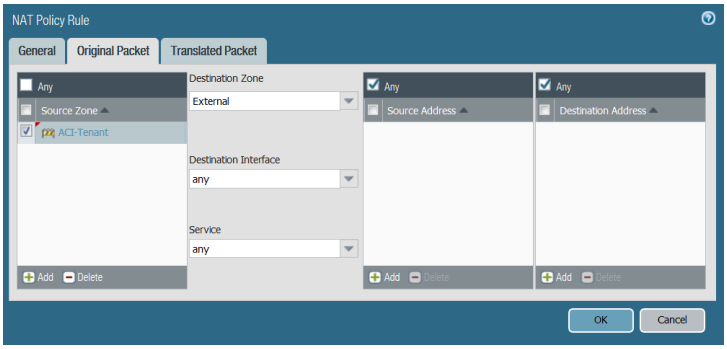
8. 在 **Translated Packet**（轉譯的封包）頁籤上，選取 **Destination Address Translation**（目的地位址轉譯）下方的 **Translation Type**（轉譯類型）。
9. 從 **Translated Address**（轉譯的位址）下拉式清單中，選取位址。
10. 按一下 **OK**（確定）。



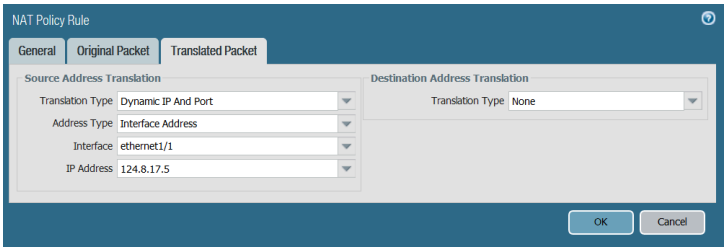
©2023 Palo Alto Networks, Inc.

STEP 2 | 設定輸出流量的位址轉譯。

1. 選取 **Policies**（政策） > **NAT**，然後按一下 **Add**（新增）。
2. 輸入輸出 NAT 政策的描述性 **Name**（名稱）。
3. 選取 **Original Packet**（原始封包），然後按一下 **Source Zone**（來源區域）下方的 **Add**（新增）。
4. 選取與 ACI 租用戶和 VRF 相符的區域。
5. 從 **Destination Zone**（目的地區域）下拉式清單中，選取外部區域。



6. 在 **Translated Packet**（轉譯的封包）頁籤上，選取 **Source Address Translation**（來源位址轉譯）下方的 **Translation Type**（轉譯類型）。
7. 輸入其他必要位址資訊。
8. 按一下 **OK**（確定）。



STEP 3 | **Commit**（提交）您的變更。

©2023 Palo Alto Networks, Inc.

Cisco ACI 中的端點監控

Panorama 專用 Cisco ACI 外掛程式可讓您使用動態位址群組 來建立 Cisco ACI 網狀架構的安全性原則。外掛程式會監控 Cisco ACI 環境中的應用程式政策基礎結構控制器 (APIC) 網狀架構變更，並與 Panorama 共用該資訊。每個已安裝 Cisco ACI 外掛程式的 Panorama 都可以支援最多 16 個 APIC 叢集。而且每個監控定義都有一個叢集和一個通知群組。

Cisco ACI 外掛程式可監控的端點數目與配置給 Panorama 的記憶體數量無關。如果您具有 Panorama 虛擬設備，則請確定指派環境中端點所需的記憶體數量。如需準備虛擬 Panorama 的詳細資訊，請參閱 Panorama 管理員指南。

Panorama 記憶體	端點
8GB	10,000
16GB	20,000

Cisco ACI 外掛程式會處理端點資訊，並將它轉換為一組標籤，而這組標籤可以用作將 IP 位址放入動態位址群組的比對準則。標籤會以下列格式建構：

cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.{epg_<EPG> | uepg_<micro-EPG>}

- **cisco.cl_<cluster>**—此標籤會根據 Cisco ACI 叢集來將 IP 位址群組為動態位址群組，並顯示您叢集的名稱。
- **cisco.cl_<cluster>.tn_<tenant>**—此標籤會根據租用戶來將 IP 位址群組為動態位址群組，並顯示您叢集和租用戶的名稱。
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>**—此標籤會根據應用程式設定檔來將 IP 位址群組為動態位址群組，並顯示您叢集、租用戶和應用程式設定檔的名稱。
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.epg_<EPG>**—此標籤會根據 EPG 來將 IP 位址群組為動態位址群組，並顯示您叢集、租用戶、應用程式設定檔和 EPG 的名稱。
- **cisco.cl_<cluster>.tn_<tenant>.ap_<app-profile>.uepg_<micro-EPG>**—此標籤會根據微 EPG 來將 IP 位址群組為動態位址群組，並顯示您叢集、租用戶、應用程式設定檔和微 EPG 的名稱。
- **cisco.cl_<cluster>.tn_<tenant>.l2out_<L2-external-endpoint>**—此標籤會根據 L2 外部端點將 IP 位址分組為動態位址群組，並顯示您的叢集、租用戶和 L2 外部端點的名稱。
- **cisco.cl_<cluster>.tn_<tenant>.bd_<bridge-domain>.subnet_<subnet>**—此標籤會根據子網路將 IP 位址分組為動態位址群組，並顯示您的叢集、租用戶、橋接器網域和子網路的名稱。

若要擷取端點 IP 位址到標籤的對應資訊，您必須設定 Cisco ACI 環境中每個 APIC 網狀架構的監控定義。監控定義會指定允許 Panorama 連線至 APIC 的使用者名稱和密碼。它也指定裝置群組，以及包含 Panorama 將標籤推送至其中的防火牆的相應通知群組。設定監控定義而且 Cisco ACI 外掛程式擷取標籤之後，就可以建立動態位址群組，以及新增標籤作為比對準則。

Cisco ACI 外掛程式會使用兩個間隔，以從 APIC 擷取資訊。第一個是監控間隔。

- 監控間隔—此監控間隔是外掛程式在查詢網狀架構中的變更之前等待的時間量。如果未發生變更，則會重設監控間隔。如果偵測到變更，則外掛程式會先處理變更，再重設監控間隔。預設監控間隔是 60 秒。您可以設定 60 秒到一天（86,400 秒）的監控間隔。

©2023 Palo Alto Networks, Inc.

- 完全同步間隔—完全同步間隔是外掛程式在更新所有網狀架構中的動態物件（不論是否發生任何變更）之前等待的時間量。這確保外掛程式與網狀架構同步，即使監控間隔遺漏變更事件也是一樣。預設完全同步間隔為 10 分鐘。您可以設定 600 秒（10 分鐘）到 86,400 秒（一天）的完全同步間隔。

  您必須透過 Panorama CLI 設定完全同步間隔。

如果您所設定監控間隔的值大於完全同步間隔的值，則會忽略完全同步間隔，而且在每個監控間隔執行完全同步處理。

如果 Panorama 中斷與 APIC 的連線，則 Panorama 將嘗試重新連線五次。五次失敗的嘗試之後，Panorama 會停止監控您叢集中的變更，並顯示系統日誌中的重新連線嘗試。若要復原並再次開始監控叢集，您必須對 Panorama 執行認可。

- 安裝 Cisco ACI 專用 Panorama 外掛程式
- 設定 Cisco ACI 外掛程式
- Cisco ACI 專用 Panorama 外掛程式儀表板

安裝 Cisco ACI 專用 Panorama 外掛程式

若要開始在 Cisco ACI 上監控端點，請在 Panorama 下載並安裝 Cisco ACI 外掛程式。

如果您有 Panorama HA 組態，請在每個 Panorama 端點上重複此安裝程序。在 Panoramas 上以 HA 對等安裝外掛程式時，請先將外掛程式安裝於被動對等，再安裝於主動對等。安裝外掛程式安裝於被動對等之後會轉換為非運作狀態。將外掛程式安裝於主動對等會將被動對等恢復為運作狀態。

如果您在安裝了多個外掛程式的 HA 配對中安裝了一個獨立的 Panorama 或兩個 Panorama 設備，則在未設定一或多個外掛程式的情況下，外掛程式可能不會收到更新的 IP-Tag 資訊。發生這種情況是因為 Panorama 不會將 IP-Tag 資訊轉送到未設定的外掛程式。此外，如果一或多個 Panorama 外掛程式未處於「已註冊」或「成功」狀態（每個外掛程式的正狀態不同），則可能會出現此問題。在繼續或執行下述命令之前，請確保您的外掛程式處於正狀態。

如果遇到此問題，有兩種權宜方案：

- 解除安裝未設定的外掛程式。建議您不要安裝未打算立即設定的外掛程式
- 您可以使用以下命令來變通處理此問題。對每個 Panorama 實例上的每個未設定外掛程式執行以下命令，以防止 Panorama 等待傳送更新。否則，防火牆可能會遺失一些 IP-Tag 資訊。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以透過執行以下命令來取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

上述的命令在重新啟動後不會持續存在，並且必須在任何後續重新啟動時再次使用。對於 HA 配對中的 Panorama，必須在每個 Panorama 上執行命令。

STEP 1 | 確認虛擬 Panorama 有足夠的記憶體可以支援 ACI 環境中的端點數目。

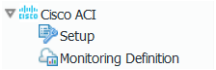
STEP 2 | 選取 **Panorama** > **Plugins**（外掛程式）。

©2023 Palo Alto Networks, Inc.

STEP 3 | 選取 **Check Now**（立即檢查） 以擷取可用更新清單。

STEP 4 | 選取 Action（動作）欄中的 **Download**（下載）以下載外掛程式。

STEP 5 | 選取外掛程式版本，在 Action（動作）欄中按一下 **Install**（安裝）來安裝外掛程式。安裝完成時，Panorama 會通知您。



設定 Cisco ACI 外掛程式

安裝外掛程式之後，您必須設定監控間隔、設定通知群組，以及建立 Panorama 與 APIC 網狀架構之間的連線。

STEP 1 | （選用）設定完全同步間隔。

1. 登入 Panorama CLI。
2. 進入設定模式。

   admin@Panorama> configure
3. 使用下列命令，以設定完全同步間隔。預設間隔為 600 秒（10 分鐘）。範圍為 600 秒到 86,400 秒（一天）。

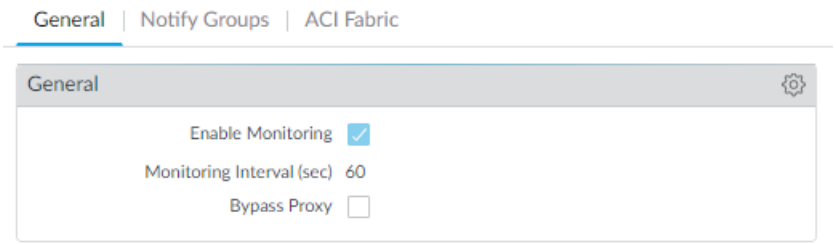
   admin@Panorama# **set plugins cisco full-sync-interval <interval-in-seconds>**

STEP 2 | 登入 Panorama 網頁介面。

STEP 3 | 您必須在 Panorama 上將防火牆新增為受管理的裝置並建立裝置群組以便您設定 Panorama 以通知這些群組其擷取的 VM 資訊。裝置群組可包括 VM-Series 防火牆或硬體防火牆上的虛擬系統。

STEP 4 | 啟用監控、設定監控間隔，並啟用繞過 Proxy。

1. 選取 **Panorama** > **Cisco ACI** > **Setup**（設定） > **General**（一般）。
2. 選取 **Enable Monitoring**（啟用監控）。這會監控部署中的所有叢集。
3. 設定 **Monitoring Interval**（監控間隔），單位為秒。監控間隔是 Panorama 從 APIC 擷取已更新網路資訊的頻率。預設值為 60 秒，而且範圍為 60 秒到 86,400 秒（一天）。
4. （選用）選取 [Bypass Proxy（繞過 Proxy）]，以繞過用於 Panorama 與 APIC 之間通訊的 Proxy 伺服器設定，在 Panorama 上設定於 **Panorama** > **Setup**（設定） > **Services**（服務） > **Proxy Server**（**Proxy** 伺服器）下方。此命令可讓 Panorama 直接與 APIC 通訊，同時維護其他服務的 Proxy 通訊。



 ©2023 Palo Alto Networks, Inc.

STEP 5 | 建立通知群組。

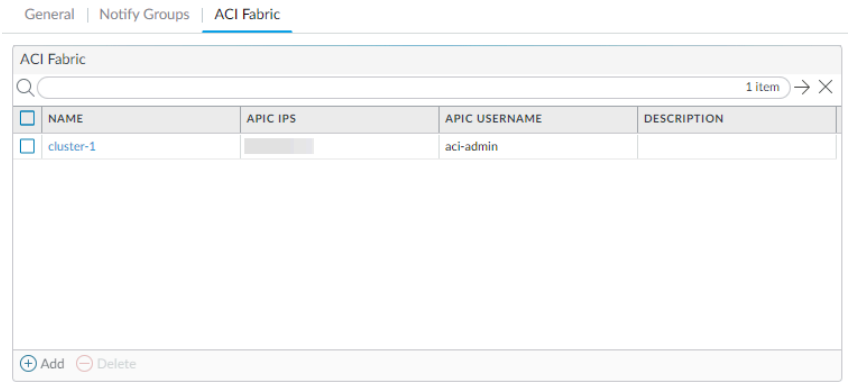
1. 選取 **Panorama** > **Cisco ACI** > **Setup**（設定） > **Notify Groups**（通知群組）。
2. 按一下 **Add**（新增）。
3. 輸入通知群組的描述性 **Name**（名稱）。
4. 選取 ACI 部署中的裝置群組。

STEP 6 | 新增 ACI 網狀架構資訊。

1. 選取 **Panorama** > **Cisco ACI** > **Setup**（設定） > **ACI Fabric**（**ACI** 網狀架構）。
2. 輸入叢集的描述性 **Name**（名稱）。
3. 以逗號區隔清單形式，輸入叢集中每個 APIC 的 IP 位址或 FQDN。

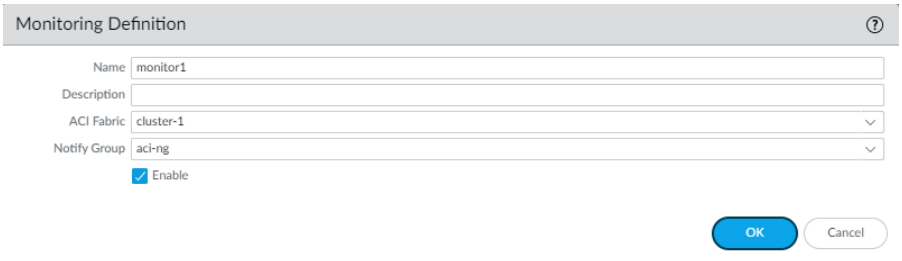
   使用 *FQDN* 時，請不要在 *URL* 中加入 *https://*。

4. 輸入 APIC 使用者名稱。
5. 輸入並確認 APIC 密碼。
6. 按一下 **OK**（確定）。



STEP 7 | 設定監控定義。

1. 選取 **Panorama** > **Cisco ACI** > **Monitoring Definition**（監控定義），然後按一下 **Add**（新增）。
2. 輸入描述性 **Name**（名稱），並選擇性地輸入說明以識別您要使用此定義的 Cisco ACI 叢集。
3. 選取 **Cluster Info**（叢集資訊）和 **Notify Group**（通知群組）。
4. 按一下 **OK**（確定）。



 ©2023 Palo Alto Networks, Inc.

STEP 8 | **Commit**（提交）您的變更。

STEP 9 | 確認您可在 Panorama 上檢視 EPG 資訊，並定義動態位址群組的比對準則。

部分瀏覽器延伸可能會封鎖 *Panorama* 與 *APIC* 之間的 *API* 呼叫，進而防止 *Panorama* 接收比對準則。如果 *Panorama* 未顯示比對準則，而且您使用瀏覽器延伸，則請停用延伸，並 *[Synchronize Dynamic Objects*（同步處理動態物件）*]* 以填入 *Panorama* 可用的標籤。

Panorama 不會立即處理新的監控定義以及填入動態位址可用的比對準則。您應該先等待所設定監控間隔的持續時間，再驗證該 *EPG* 資訊。

STEP 10 | 確認 EPG 中的位址已新增至動態位址群組。

1. 選取 **Panorama** > **Objects**（物件） > **Address Groups**（位址群組）。
2. 在動態位址群組的 [Addresses（位址）] 欄中，按一下 **More**（更多）。

   Panorama 會根據您指定的比對準則，顯示已新增至該動態位址群組的 IP 位址清單。

STEP 11 | 在原則中使用動態位址群組。

1. 選取 **Policies**（政策） > **Security**（安全性）。
2. 按一下 **Add**（新增），然後輸入原則的 **Name**（名稱）和 **Description**（說明）。
3. 新增 **Source Zone**（來源區域）以指定流量來源於哪個區域。
4. 新增流量將終止於哪個 **Destination Zone**（目的地區域）。
5. 對於 **Destination Address**（目的地位址），請選取您剛才建立的動態位址群組。
6. 針對流量指定動作—**Allow**（允許）或 **Deny**（拒絕），並選擇性地將預設安全性設定檔附加至規則。
7. 重複步驟 1 到 6，建立另一個原則規則。
8. 按一下 **Commit**（交付）。

   如需詳細資訊，請參閱在政策中使用動態位址群組。

©2023 Palo Alto Networks, Inc.

STEP 12 | 同步處理動態物件，即可隨時更新 APIC 中的動態物件。同步處理動態物件可讓您在虛擬環境中維護變更內容，並可讓您自動更新政策規則中使用的動態位址群組，以啟用應用程式。

1. 選取 **Panorama** > **Cisco ACI** > **Monitoring Definition**（監控定義）。
2. 按一下 **Synchronize Dynamic Objects**（同步處理動態物件）。

HA 容錯移轉時，新的主動 *Panorama* 會嘗試重新連線至 *APIC*，並擷取所有監控定義的標籤。即使一個監控定義在重新連線時發生錯誤，*Panorama* 也會產生系統日誌訊息

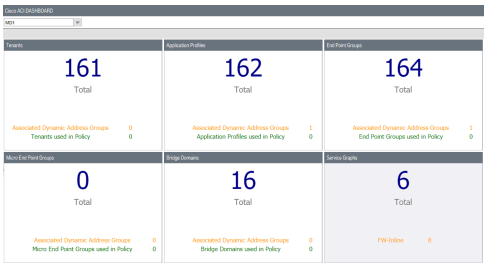
HA 切換后無法處理訂閱；需要使用者干預。

看到此錯誤時，您必須登入 *Panorama* 並修正問題，例如移除無效 *APIC IP* 或提供有效認證，並認可變更，讓 *Panorama* 重新連線並擷取所有監控定義的標籤。即使中斷 *Panorama* 與 *APIC* 的連線，防火牆還是會有容錯移轉之前所擷取的所有標籤清單，因此可以繼續對該 *IP* 位址清單進行強制執行政策。如果您在解決容錯移轉錯誤之前執行認可，則新的主動 *Panorama* 將不會推送任何 *IP* 到標籤對應資訊，並從防火牆清除對應資訊。監控此問題的最佳做法是，從 *Panorama* 設定動作導向的日誌轉送至 HTTPS 目的地，以便您立即採取措施。

Cisco ACI 專用 Panorama 外掛程式儀表板

Cisco ACI 專用 Panorama 外掛程式儀表板可讓您詳盡檢視受到外掛程式監控的 ACI 基礎結構。此儀表板包含兩個頁面 — 第一個頁面會在一組可點按的圖格上大致列出由外掛程式監控的各種物件，按一下圖格後，您就會進入第二個頁面，其中進一步提供圖格上顯示之物件的相關資訊。

安裝外掛程式後，您可以藉由選取 **Panorama** > **Cisco ACI** > **Dashboard**（儀表板）來存取儀表板。



儀表板只會查詢在 *Panorama* 上設定的預先規則安全性原則並對其計數；其中不包含後續規則、預設規則或 *NAT* 規則。

儀表板圖格	說明
Tenant Tags（租用戶標籤）	顯示 Panorama 從 APIC 擷取的租用戶總數。此外也會顯示與租用戶相關聯的動態位址群組數目，以及原則中使用的租用戶數目。

©2023 Palo Alto Networks, Inc.

儀表板圖格	說明
如果租用戶在 *APIC* 上的健康情況評分為零 *(0)*，*Panorama* 就不會擷取該租用戶的相關資訊。因此，*Panorama* 上的租用戶計數將與 *APIC* 上的總計不符。	按一下圖格以深入檢視，並檢視以下幾欄。 · **Tenant Name**（租用戶名稱）— 列出 Panorama 所擷取的所有租用戶。 · **Tenant Tag**（租用戶標籤）— 與各個租用戶相關聯的 Panorama 標籤。 · **Dynamic Address Group**（動態位址群組）— 顯示與所列標籤相關聯的動態位址群組。 · **In Policy**（在原則中）— 如果列出的動態位址群組使用於原則中，則會顯示。
Application Profiles（應用程式設定檔）	顯示 Panorama 從 APIC 擷取的應用程式設定檔總數。此外也會顯示與應用程式設定檔相關聯的動態位址群組數目，以及原則中使用的應用程式設定檔數目。 按一下圖格以深入檢視，並檢視以下幾欄。 · **Application Profile Name**（應用程式設定檔名稱）— 列出 Panorama 所擷取的所有應用程式設定檔。 · **Tenant Name**（租用戶名稱）— 顯示與列出的應用程式設定檔相關聯的租用戶。 · **Application Profile Tag**（應用程式設定檔標籤）— 與各個應用程式設定檔相關聯的 Panorama 標籤。 · **Dynamic Address Group**（動態位址群組）— 顯示與所列標籤相關聯的動態位址群組。

©2023 Palo Alto Networks, Inc.

儀表板圖格	說明
	· **In Policy**（在原則中）— 如果列出的動態位址群組使用於原則中，則會顯示。
End Point Groups（端點群組）	顯示 Panorama 從 APIC 擷取的端點群組 (EPG) 總數。此外也會顯示與 EPG 相關聯的動態位址群組數目，以及原則中使用的 EPG 數目。 按一下圖格以深入檢視，並檢視以下幾欄。 · **EPG Name**（**EPG** 名稱）— 列出 Panorama 所擷取的所有 EPG。 · **Application Profile Name**（應用程式設定檔名稱）— 列出與 EPG 相關聯的應用程式設定檔。 · **Tenant Name**（租用戶名稱）— 顯示與列出的應用程式設定檔相關聯的租用戶。 · **EPG Tag**（**EPG** 標籤）— 與各個 EPG 相關聯的 Panorama 標籤。 · **Dynamic Address Group**（動態位址群組）— 顯示與所列標籤相關聯的動態位址群組。 · **In Policy**（在原則中）— 如果列出的動態位址群組使用於原則中，則會顯示。
Micro End Point Groups（微端點群組）	顯示 Panorama 從 APIC 擷取的微端點群組 (EPG) 總數。此外也會顯示與微 EPG 相關聯的動態位址群組數目，以及原則中使用的微 EPG 數目。 按一下圖格以深入檢視，並檢視以下幾欄。 · **Micro EPG Name**（微 **EPG** 名稱）— 列出 Panorama 所擷取的所有 EPG。 · **Application Profile Name**（應用程式設定檔名稱）— 列出與微 EPG 相關聯的應用程式設定檔。 · **Tenant Tag**（租用戶標籤）— 顯示與列出的應用程式設定檔相關聯的租用戶。 · **Micro EPG Tag**（微 **EPG** 標籤）— 與各個微 EPG 相關聯的 Panorama 標籤。 · **Dynamic Address Group**（動態位址群組）— 顯示與所列標籤相關聯的動態位址群組。 · **In Policy**（在原則中）— 如果列出的動態位址群組使用於原則中，則會顯示。
Bridge Domains（橋接器網域）	顯示 Panorama 從 APIC 擷取的橋接器網域總數。此外也會顯示與橋接器網域相關聯的動態位址群組數目，以及原則中使用的橋接器網域數目。 按一下圖格以深入檢視，並檢視以下幾欄。 · **Bridge Domain Name**（橋接器網域名稱）— 列出 Panorama 所擷取的所有橋接器網域。

©2023 Palo Alto Networks, Inc.

儀表板圖格	說明
	· **Tenant Name**（租用戶名稱）— 顯示與列出的橋接器網域相關聯的租用戶。 · **Bridge Domain Tag**（橋接器網域標籤）— 與各個橋接器網域相關聯的 Panorama 標籤。 · **Dynamic Address Group**（動態位址群組）— 顯示與所列標籤相關聯的動態位址群組。 · **In Policy**（在原則中）— 如果列出的動態位址群組使用於原則中，則會顯示。
Service Graphs（服務圖形）	顯示外掛程式所監控的服務圖形總數，和以受監控的服務圖形為準的防火牆數目。 按一下圖格以深入檢視，並檢視以下幾欄。 · **Service Graph Name**（服務圖形名稱）— 列出 Panorama 所擷取的所有服務圖形。 · **Producer EPG**（產生者 **EPG**）— 顯示與服務圖形相關聯的產生者 EPG。 · **FW InLine** — 顯示與服務圖形相關聯的防火牆。

©2023 Palo Alto Networks, Inc.

在 Cisco CSP 上設定 VM-Series 防火牆

您可以將 VM-Series 防火牆部署為 Cisco Cloud Security Platform (CSP) 上的網路虛擬服務。因為 Cisco CSP 是 RHEL KVM 平台，所以會使用 KVM 專用 VM-Series 防火牆基本映像來部署 VM-Series 防火牆。

透過 Cisco CSP 上的 VM-Series 防火牆，您可以保護工作負載、防止進階威脅，以及改善虛擬網路上的應用程式可見度。

- Cisco CSP 上的 VM-Series 系統需求
- 在 Cisco CSP 上部署 VM-Series 防火牆

Cisco CSP 上的 VM-Series 系統需求

您可以在 Cisco CSP 上建立和部署 VM-Series 防火牆的多個實例（獨立或 HA 配對）。

VM-Series 防火牆具有下列要求：

- 請參閱相容性矩陣，以瞭解支援的 CSP 和 PAN-OS 版本。
- 啟動套件 已轉換為 ISO 檔案
- 如需 VM-Series 型號的最低硬體需求，請參閱VM-Series 系統需求。
- 至少兩個網路介面 (vNIC)。一個是管理介面專用的 vNIC，一個用於資料介面。對於資料流量，您最多可新增八個額外的 vNIC。
- Cisco CSP 上的 VM-Series 防火牆支援 VM-50 以外的所有 VM-Series 型號。
- 僅限 SR-IOV 和封包 MMAP 模式；不支援 DPDK。

©2023 Palo Alto Networks, Inc.

在 Cisco CSP 上部署 VM-Series 防火牆

完成下列程序，以在 Cisco CSP 上部署 VM-Series 防火牆。

STEP 1 | 從客戶支援入口網站下載 VM-Series qcow2 基本映像檔案。

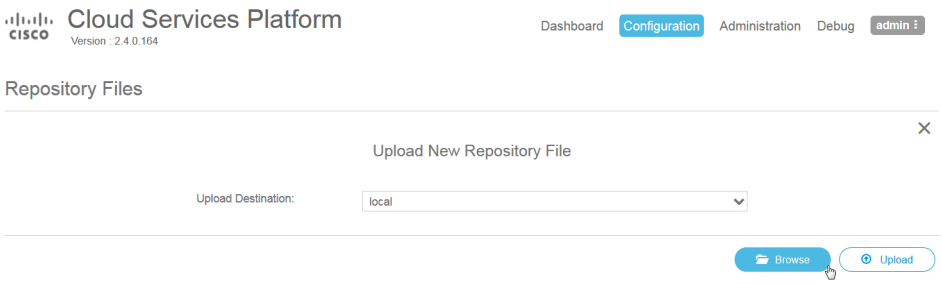
STEP 2 | 建立 VM-Series 防火牆的啟動 ISO 檔案。

1. 建立 VM-Series 防火牆的啟動套件。
2. 使用偏好的工具，建立包含啟動套件的 ISO 檔案。

STEP 3 | 登入 Cisco CSP 網頁介面。

STEP 4 | 上傳 VM-Series 防火牆 qcow2 映像和 ISO 檔案。

1. 選取 **Configuration**（設定） > **Repository**（儲存庫）。
2. 按一下加號 (+) 圖示。
3. 按一下 **Browse**（瀏覽），並導覽至 qcow2 檔案。
4. 按一下 **Upload**（上傳）。
5. 按一下 **Browse**（瀏覽），並導覽至 ISO 檔案。
6. 按一下 **Upload**（上傳）。



©2023 Palo Alto Networks, Inc.

STEP 5 | 建立 VM-Series 防火牆服務。

1. 輸入 VM-Series 防火牆的描述性 **Name**（名稱）。
2. 從下拉式清單中，選取 **Target Host Name**（目標主機名稱）。
3. 從 **Image Name**（映像名稱）下拉式清單中，選取您上傳的 qcow2 檔案。



4. 選取 [Day Zero Config（零日設定）]。
   1. 按一下 **Day Zero Config**（零日設定）加號 (+) 圖示。
   2. 從 **Source File Name**（來源檔案名稱）下拉式清單中，選取啟動 ISO 檔案。
   3. 按一下 **Submit**（提交）。



5. 配置 VM-Series 防火牆型號所需的核心數目和記憶體。
6. 新增足夠的 vNIC，以支援啟動 ISO 檔案中所設定的 VM-Series 介面數目。

如需建立和部署服務實例的詳細資訊，請參閱 Cisco Cloud Service Platform 文件。

STEP 6 | 啟動程序完成之後，請使用您在啟動 ISO 檔案中指定的管理 IP 位址來登入 VM-Series 防火牆。

應該會根據您在啟動套件中定義的參數啟動和設定防火牆。

©2023 Palo Alto Networks, Inc.

Cisco TrustSec 的端點監控

安裝和設定 Cisco TrustSec 專用 Panorama 外掛程式，以擷取環境中端點的 IP 位址，並使用動態位址群組建立這些端點的安全性原則。

- Cisco TrustSec 專用 Panorama 外掛程式
- 安裝 Cisco TrustSec 專用 Panorama 外掛程式
- 設定 Cisco TrustSec 專用 Panorama 外掛程式
- 對 Cisco TrustSec 專用 Panorama 外掛程式進行疑難排解

Cisco TrustSec 專用 Panorama 外掛程式

Cisco TrustSec 專用 Panorama 外掛程式可讓您使用動態位址群組建立 TrustSec 環境的安全性原則。此外掛程式會監控 TrustSec 安全性群組中的變更，並將該資訊註冊至 Panorama，並且將 IP 資訊轉送至防火牆，讓 Panorama 可將正確的原則套用至對應的端點。Cisco TrustSec 專用 Panorama 外掛程式最多可支援 16 個 pxGrid (Cisco ISE) 伺服器。

Cisco TrustSec 專用 *Panorama* 外掛程式目前支援動態物件，但不支援靜態物件。

Panorama 外掛程式會處理端點資訊，並將其轉換為一組標籤，供您作為將 IP 位址放入動態位址群組的比對準則。Panorama 會為您 pxGrid 伺服器上的每個安全性群組標籤 (SGT) 建立一個標籤。標籤會以下列格式建構：

cts.svr_<pxgrid-server-name>.sgt_<SGT-name>

若要擷取端點 IP 位址到標籤的對應資訊，您必須設定環境中每個 pxGrid 伺服器的監控定義。pxGrid 伺服器設定會指定使用者名稱和密碼，並且供允許 Panorama 連線至 pxGrid 的監控定義參照。此外，您也可以設定外掛程式，以透過 Panorama 上的憑證設定檔來驗證 pxGrid 伺服器識別。它也指定裝置群組，以及包含 Panorama 將標籤推送至其中的防火牆的相應通知群組。設定監控定義，且外掛程式擷取標籤後，就可以建立動態位址群組，以及新增標籤作為比對準則。

Cisco TrustSec 專用 Panorama 外掛程式版本 1.0.2 和更新版本支援大量同步和發佈訂閱監控模式。此外掛程式根據 Panorama 版本來選取模式—如果 Panorama 版本是 10.0.0 之前，則選取大量同步模式，而在 Panorama 10.0.0 和更新版本上，則選取發佈訂閱模式。使用者介面會顯示預設監控模式的設定選項。

- 大量同步
- 發佈訂閱

大量同步

大量同步模式使用兩種間隔從 pxGrid 伺服器擷取資訊—監控間隔和完全同步間隔。當 Cisco TrustSec 專用 Panorama 外掛程式版本 1.0.2 或更新版本安裝在 10.0.0 之前的 Panorama 版本時，此模式為預設值。10.0.0 之前的 Panorama 版本支援每 10 秒向 configd 更新一次 IP 表格。

- 監控間隔—此監控間隔是外掛程式在查詢變更之前等待的時間量。如果未發生變更，則會重設監控間隔。如果有變更，則外掛程式會先處理變更，再重設監控間隔。預設監控間隔是 60 秒。您可以設定 10 秒到一天（86,400 秒）的監控間隔。

  安裝 *Cisco TrustSec* 專用 *Panorama* 外掛程式 *1.0.0* 時，最低監控間隔為 *30* 秒。

- 完全同步間隔—完全同步間隔是外掛程式在更新所有 pxGrid 伺服器中的動態物件（不論是否發生任何變更）之前等待的時間量。這可確保外掛程式與 pxGrid 伺服器同步，即使監控間隔遺漏變更事件也是一樣。您可以設定 600 秒（10 分鐘）到 86,400 秒（一天）的完全同步間隔。您必須從 Panorama CLI 設定完全同步間隔。

如果監控間隔大於完全同步間隔，則會忽略完全同步間隔，而且在每個監控間隔執行完全同步處理。

©2023 Palo Alto Networks, Inc.

發佈訂閱

發佈訂閱模式直接監控 Cisco ISE 伺服器的通知（訂閱精靈）、剖析 IP 標籤，並將相關資訊傳送至標籤處理精靈 (tag-proc)。當 Cisco TrustSec 專用 Panorama 外掛程式版本 1.0.2 或更新版本安裝在 Panorama 版本 10.0.0 或更新版本時，發佈訂閱為預設模式。Panorama 版本 10.0.0 或更新版本支援每 100 毫秒向 configd 更新一次 IP 表格。

- **Push interval**（推送間隔）—推送間隔是推送之間的時間量。如果上一次推送花太多時間，則完成時會立刻觸發下一次推送。推送間隔最短 100 毫秒（0 秒），最長 60 秒。預設推送間隔為 0 秒。
- 啟用完全同步—啟用此選項可觸發完整更新。如果您啟用完全同步，則可以設定完全同步間隔。預設值為 [no（否）]。
- 完全同步間隔—完全同步間隔是外掛程式在更新所有 pxGrid 伺服器中的動態物件（不論是否發生任何變更）之前等待的時間量。預設完全同步間隔為 10 分鐘。您可以設定 600 秒（10 分鐘）到 86,400 秒（一天）的完全同步間隔。您必須從 Panorama CLI 設定完全同步間隔。
- **Reconnection interval**（重新連線間隔）—初始重新連線間隔為 1 秒，如果上一次重新連線失敗，則間隔會變成兩倍。重新連線間隔最長 64 秒。重新連線嘗試次數沒有限制。

©2023 Palo Alto Networks, Inc.

安裝 Cisco TrustSec 專用 Panorama 外掛程式

若要開始在 Cisco TrustSec 進行端點監控，請在下載並安裝 Panorama 上的 Cisco TrustSec 外掛程式。關於外掛程式版本與 Panorama 版本的相關性，請參閱相容性矩陣中的 Panorama 外掛程式。

需要提交才能升級或降級 *Cisco TrustSec* 外掛程式。

如果您有 Panorama HA 組態，請在每個 Panorama 端點上重複此安裝程序。在 HA 對等中的 Panorama 設備上安裝外掛程式時，請先將外掛程式安裝於被動對等，再安裝於主動對等。安裝外掛程式安裝於被動對等之後會轉換為非運作狀態。將外掛程式安裝於主動對等會將被動對等恢復為運作狀態。

如果您在安裝了多個外掛程式的 HA 配對中安裝了一個獨立的 Panorama 或兩個 Panorama 設備，則在未設定一或多個外掛程式的情況下，外掛程式可能不會收到更新的 IP-Tag 資訊。發生這種情況是因為 Panorama 不會將 IP-Tag 資訊轉送到未設定的外掛程式。此外，如果一或多個 Panorama 外掛程式未處於「已註冊」或「成功」狀態（每個外掛程式的正狀態不同），則可能會出現此問題。在繼續或執行下述命令之前，請確保您的外掛程式處於正狀態。

如果遇到此問題，有兩種權宜方案：

- 解除安裝未設定的外掛程式。建議您不要安裝未打算立即設定的外掛程式
- 您可以使用以下命令來變通處理此問題。對每個 Panorama 實例上的每個未設定外掛程式執行以下命令，以防止 Panorama 等待傳送更新。否則，防火牆可能會遺失一些 IP-Tag 資訊。

  `request plugins dau plugin-name <plugin-name> unblock-device-push yes`

  您可以透過執行以下命令來取消此命令：

  `request plugins dau plugin-name <plugin-name> unblock-device-push no`

上述的命令在重新啟動後不會持續存在，並且必須在任何後續重新啟動時再次使用。對於 HA 配對中的 Panorama，必須在每個 Panorama 上執行命令。

STEP 1 | 選取**Panorama** > 外掛程式 。

STEP 2 | 按一下 **Check Now**（立即檢查），以取得最新版的外掛程式。

STEP 3 | 選取 Action（動作）欄中的 **Download**（下載）以下載外掛程式。

STEP 4 | 選取外掛程式版本，在 Action（動作）欄中按一下 **Install**（安裝）來安裝外掛程式。安裝完成時，Panorama 會通知您。

©2023 Palo Alto Networks, Inc.

設定 Cisco TrustSec 專用 Panorama 外掛程式

安裝外掛程式後，您還必須將通知群組指派給 Cisco TrustSec 外掛程式設定。通知群組是一個裝置群組清單，其中包含 Panorama 應將其從 pxGrid 伺服器擷取到的所有標籤推送到的目標防火牆。

每個已安裝 Cisco TrustSec 外掛程式的 Panorama，最多可支援 16 個 pxGrid 伺服器和 16 個監控定義。而且每個監控定義都有一個 pxGrid 伺服器和一個通知群組。

Cisco TrustSec 專用 *Panorama* 外掛程式目前支援動態物件，但不支援靜態物件。

下列設定指示涵蓋大量同步和發佈訂閱監控模式；部分使用者介面功能是根據監控模式而啟用或可見。

STEP 1 | 如果您想要變更為預設值 600 秒（10 分鐘）以外的設定，請設定完全同步間隔。

1. 登入 Panorama CLI。
2. 進入設定模式。

   ```
   admin@Panorama> configure
   ```
3. 使用下列命令，以設定完全同步間隔。範圍為 600 秒到 86,400 秒（一天）。

   ```
   admin@Panorama# set plugins cisco_trustsec full-sync-interval
   <interval-in-seconds>
   ```

STEP 2 | 登入 Panorama 網頁介面。

STEP 3 | 您必須在 Panorama 上將防火牆新增為受管理的裝置並建立裝置群組以便您設定 Panorama 以通知這些群組其擷取的 VM 資訊。裝置群組可包括 VM-Series 防火牆或硬體防火牆上的虛擬系統。

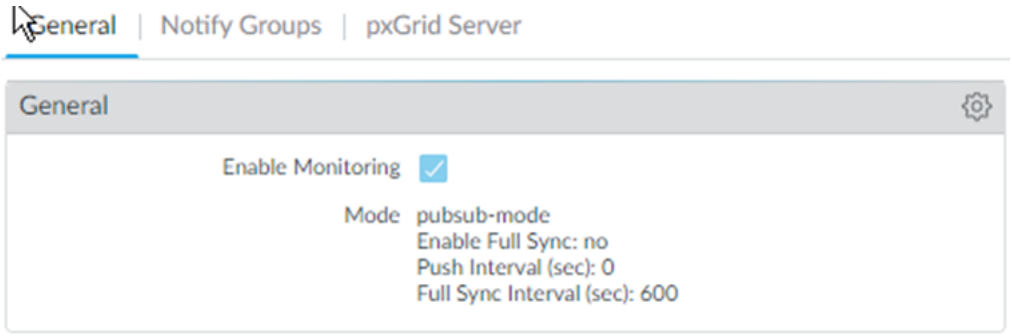
©2023 Palo Alto Networks, Inc.

STEP 4 | 設定 Cisco TrustSec 監控。

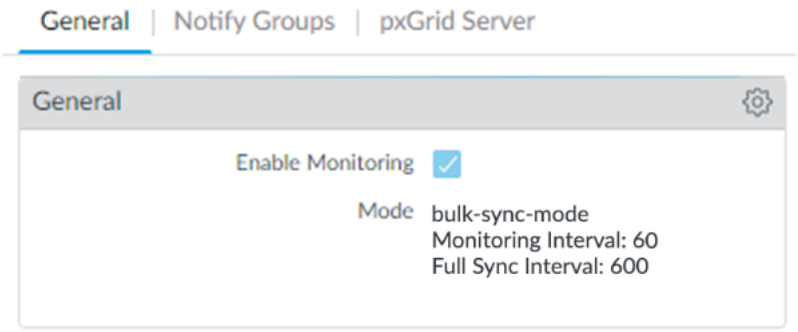
1. 選取 **Panorama** > **Cisco TrustSec** > **Setup**（設定） > **General**（一般）。

   Enable Cisco TrustSec Monitoring（啟用 **Cisco TrustSec** 監控）預設為啟用。這會監控部署中的所有叢集。

   如果 Cisco TrustSec 專用 Panorama 外掛程式 1.0.2 或更新版本安裝在 Panorama 10.0.0 或更新版本上，則使用者介面會選取發佈訂閱監控模式：

   外掛程式安裝在 10.0.0 之前的 Panorama 版本時會選取大量同步模式：

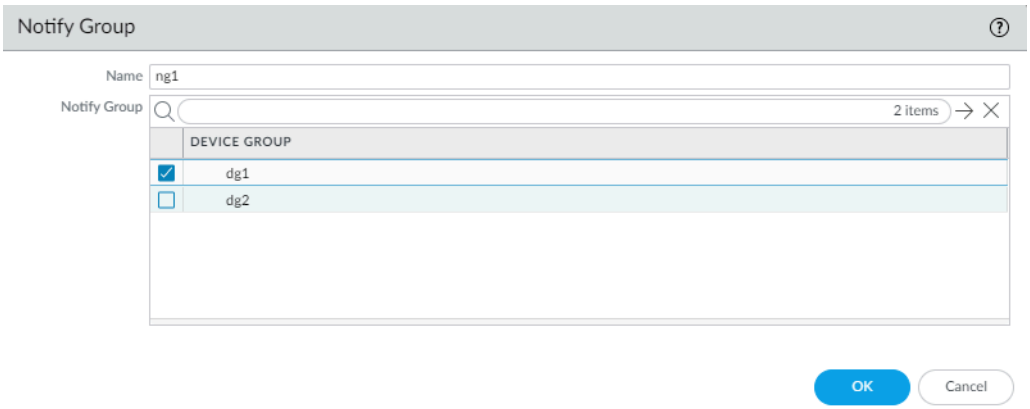
   

2. 按一下齒輪來編輯設定參數。
   - 推送間隔（僅限發佈訂閱）—最短 0 秒，最長 60 秒，預設值為 0（100 毫秒）。
   - 啟用完全同步（僅限發佈訂閱，選用）—選取此選項可啟用完全同步。預設值為 [no（否）]。
   - 完全同步間隔。
     - 發佈訂閱—如果選取 [Enable Full Sync（啟用完全同步）]，您可以設定完全同步間隔（以秒為單位）。範圍是 600 秒到 86400 秒（一天），預設值為 600
     - 大量同步—在大量同步模式下預設為啟用。範圍是 600 秒到 86400 秒（一天），預設值為 600。
   - 監控間隔（僅限大量同步）—10 到 86400 秒，預設值為 60—設定 Panorama 向 pxGrid 伺服器查詢端點位址資訊的輪詢間隔。此為監控事件結束與下一個事件開始之間的間隔時間。

©2023 Palo Alto Networks, Inc.

STEP 5 | 建立通知群組。

1. 選取 **Panorama** > **Cisco TrustSec** > **Setup**（設定） > **Notify Groups**（通知群組）。
2. 按一下 **Add**（新增）。
3. 輸入通知群組的描述性 **Name**（名稱）。
4. 選取您先前建立的裝置群組。



STEP 6 | （選用）若要啟用 pxGrid 伺服器的伺服器識別驗證，請在 Panorama 上設定憑證設定檔。

STEP 7 | 建立、啟動並核准 pxGrid 用戶端名稱和用戶端密碼。

1. 登入 Panorama CLI。
2. 執行下列命令以建立用戶端名稱。
   - 如果您有憑證設定檔，請如下建立用戶端名稱：

     admin@Panorama> request plugins cisco_trustsec create-account client-name <client-name> host <ise-server-ip>
   - 如果您略過步驟 6，也沒有憑證，請輸入：

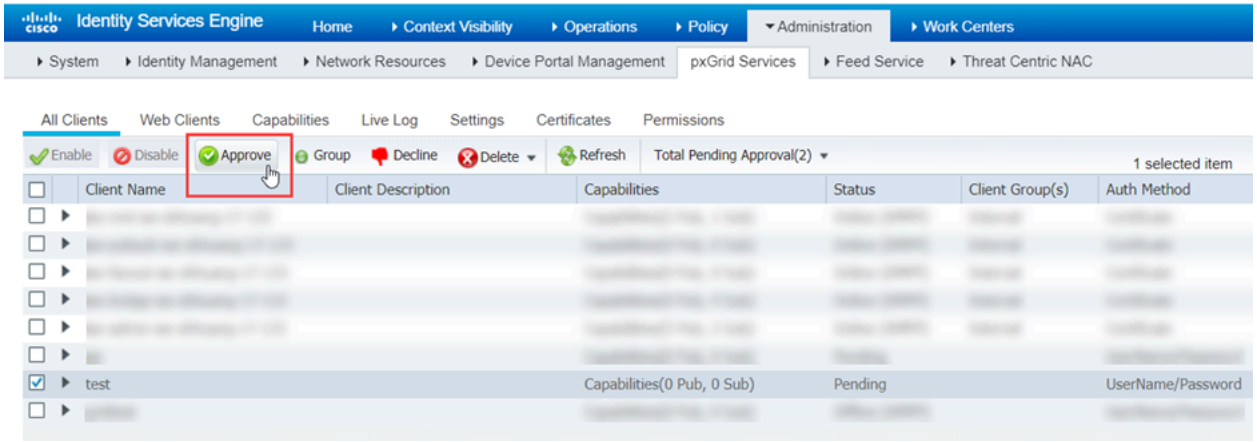
     request plugins cisco_trustsec create-account server-cert-verification-enabled no client-name <client-name>host <host-name>
3. 執行下列命令以建立用戶端名稱。

```
admin@Panorama> request plugins cisco_trustsec create-
account client-name test host 10.10.10.15 AccountCreate in
 progress...AccountCreate successful.   client nodename:
```


©2023 Palo Alto Networks, Inc.

```
test client password:PmVKBmPgf63Hypq AccountActivate in
progress...AccountActivate 成功。請在伺服器上核准該帳戶。
```

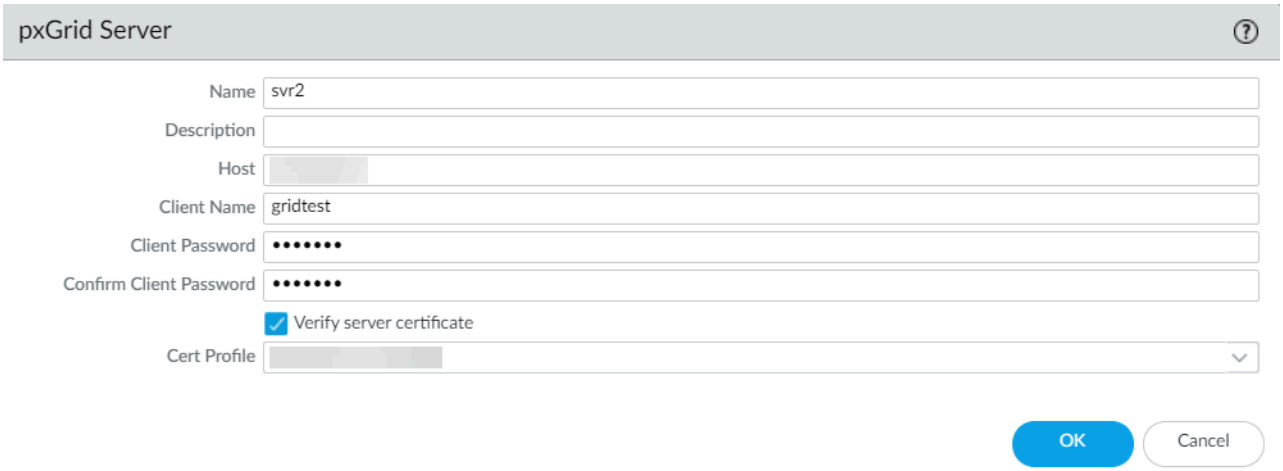
4. 登入您的 Cisco ISE 伺服器以核准帳戶。
5. 選取 **Administration**（管理） > **pxGrid Services**（**pxGrid** 服務） > **All Clients**（所有用戶端）。
6. 選取您在 Panorama 上建立的用戶端名稱。
7. 按一下 **Approve**（核准）。



©2023 Palo Alto Networks, Inc.

STEP 8 | 新增 pxGrid 伺服器資訊。Cisco TrustSec 專用 Panorama 外掛程式最多可支援 16 個 pxGrid (Cisco ISE) 伺服器。

1. 選取 **Panorama** > **Cisco TrustSec** > **Setup**（設定） > **pxGrid Server**（**pxGrid** 伺服器）。
2. 輸入 pxGrid 伺服器的描述性 **Name**（名稱）。
3. 在 **Host**（主機）欄位中，輸入 pxGrid 伺服器的 IP 位址或 FQDN。
4. 輸入您在先前的步驟中建立的用戶端名稱。
5. 輸入您在先前的步驟中產生的用戶端密碼，並加以確認。
6. 驗證 pxGrid 伺服器識別。
   1. 選取 **Verify server certificate**（驗證伺服器憑證）。
   2. 從 **Cert Profile**（憑證設定檔）下拉式清單中選取您的憑證設定檔。
7. 按一下 **OK**（確定）。



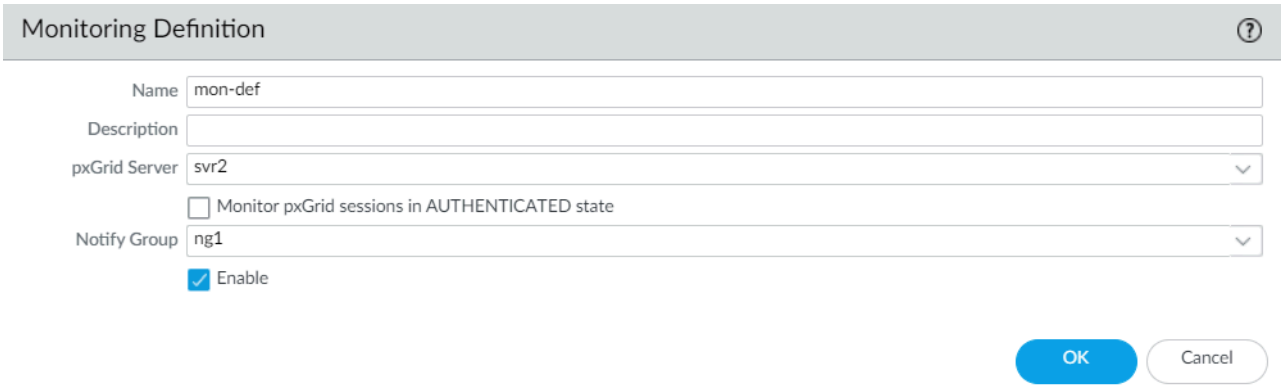
STEP 9 | 設定監控定義。

1. 選取 **Panorama** > **Cisco TrustSec** > **Monitoring Definition**（監控定義），然後按一下 **Add**（新增）。
2. 輸入描述性 **Name**（名稱），並選擇性地輸入 **Description**（說明）以識別監控定義。
3. 選取 **pxGrid Server**（**pxGrid** 伺服器）。
4. （選用）將 Panorama 設定為 **Monitor pxGrid sessions in AUTHENTICATED state**（監控處於已驗證狀態的 **pxGrid** 工作階段）。根據預設，Panorama 會從處於「已啟動」狀態

©2023 Palo Alto Networks, Inc.

的工作階段擷取 IP-標籤對應。ISE 工作階段有相應的計費開始封包時，表示處於「已啟動」狀態。如果工作階段沒有計費開始封包，則工作階段狀態為「已驗證」。

5. 選取 **Notify Group**（通知群組）。
6. 按一下 **OK**（確定）。



STEP 10 | **Commit**（提交）您的變更。

STEP 11 | 建立作用中 ISE 工作階段，以便 Panorama 取得動態位址群組定義的 SGT 標籤。若要建立作用中工作階段，請使用 ISE 來驗證裝置。

Panorama 不會在 ISE 上收集預設 SGT 標籤。

©2023 Palo Alto Networks, Inc.

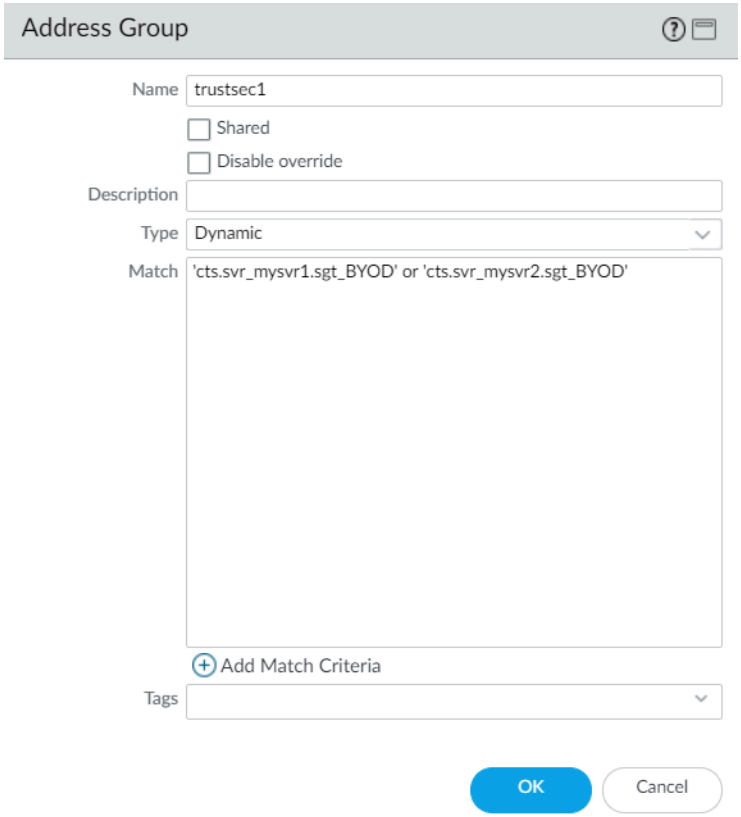
STEP 12 | 建立動態位址群組，並確認位址已新增至動態位址群組。

1. 選取 **Object**（物件） > **Address Groups**（位址群組）。
2. 從 **Device Group**（裝置群組）下拉式清單中，選取您在 Cisco TrustSec 環境中為監控端點建立的裝置群組。
3. 按一下 **Add**（新增），然後輸入動態位址群組的 **Name**（名稱）和 **Description**（說明）。

   動態位址組命名約定為：**`cts.svr_<server-name>.sgt_<SGT-name>`**
4. 在 **Type**（類型）中選取 **Dynamic**（動態）。
5. 按一下 **Add Match Criteria**（新增比對準則）。
6. 選取 **And** 或 **Or** 運算子，然後按一下安全性群組名稱旁的加號 (+) 圖示，以將它新增至動態位址群組。

   Panorama 只能顯示從作用中工作階段取得的安全性群組標籤。即時工作階段中的安全性群組標籤會出現在比對規則清單中。
7. 選取 **Panorama** > **Objects**（物件） > **Address Groups**（位址群組）。
8. 在動態位址群組的 [Addresses（位址）] 欄中，按一下 **More**（更多）。

   Panorama 會根據您指定的比對準則來顯示已新增至該動態位址群組的 IP 位址清單。



 ©2023 Palo Alto Networks, Inc.

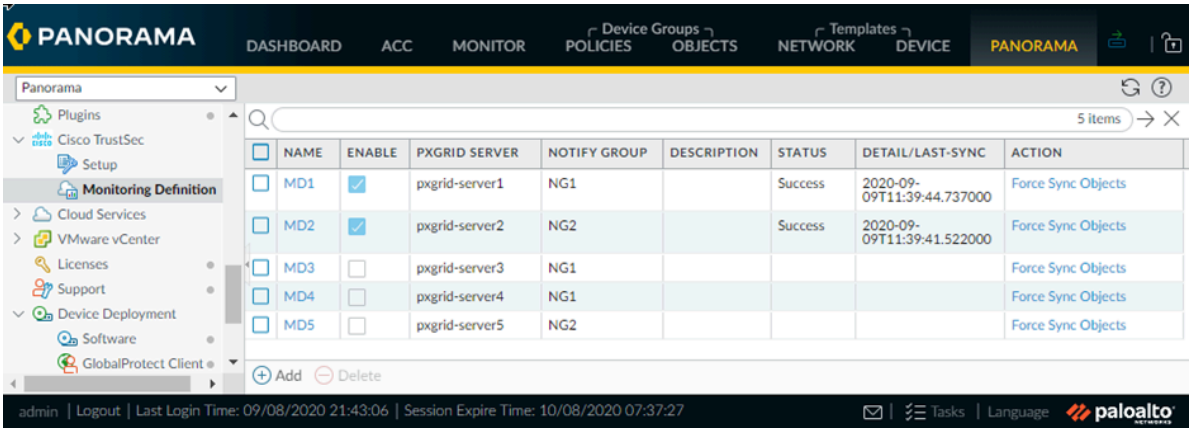
STEP 13 | 在原則中使用動態位址群組。

動態位址群組在連接至政策之前為空白。在政策使用動態位址群組之前，您在其中看不到任何 *IP* 位址。

1. 選取 **Policies**（政策） > **Security**（安全性）。
2. 按一下 **Add**（新增），然後輸入原則的 **Name**（名稱）和 **Description**（說明）。
3. 新增 **Source Zone**（來源區域）以指定流量來源於哪個區域。
4. 新增流量將終止於哪個 **Destination Zone**（目的地區域）。
5. 對於 **Destination Address**（目的地位址），請選取您剛才建立的動態位址群組。
6. 針對流量指定動作—**Allow**（允許）或 **Deny**（拒絕），並選擇性地將預設安全性設定檔附加至規則。
7. 重複步驟 1 到 6，建立另一個原則規則。
8. 按一下 **Commit**（交付）。

STEP 14 | （選用）同步處理動態物件，以隨時更新 pxGrid 伺服器中的動態物件。同步處理動態物件可讓您在虛擬環境中維護變更內容，並可讓您自動更新政策規則中使用的動態位址群組，以啟用應用程式。

1. 選取 **Panorama** > **Cisco TrustSec** > **Monitoring Definition**（監控定義）。
2. 按一下 **Synchronize Dynamic Objects**（同步處理動態物件）。



©2023 Palo Alto Networks, Inc.

對 Cisco TrustSec 專用 Panorama 外掛程式進行疑難排解

- 外掛程式狀態命令
- 偵錯命令
- 偵錯日誌

外掛程式狀態命令

- 清除計數器：

```
clear plugins cisco_trustsec counters
```

- 顯示監控狀態：

```
show plugins cisco_trustsec status
```

- 顯示計數器：

```
show plugins cisco_trustsec counters
```

偵錯命令

- 檢查動態位址群組中的 IP 位址。

```
show object registered-ip tag <tag>
```

```
show object registered-ip all
```

- 從伺服器擷取 IP 位址的標籤。擷取的 ip-標籤對應會記錄在 `plugin_cisco_trustsec.log` 中。Ip-標籤對應不會推送至與伺服器相關聯的通知群組。如果失敗，不會重試。

```
debug plugins cisco_trustsec query pxgrid-server $server-name ip
 $ip-address
```

- 強制與一個伺服器同步，並將對應推送至 configd 程序。如果失敗，不會重試。

```
request plugins cisco_trustsec synchronize-dynamic-objects name
 $server-name
```

- 強制與所有伺服器同步，並將對應推送至 configd 程序。如果失敗，不會重試。

```
 request plugins cisco_trustsec synchronize-dynamic-objects all
```


©2023 Palo Alto Networks, Inc.

- 強制將對應從 configd 程序同步至 VM-Series 防火牆。如果失敗，不會重試。

```
request plugins cisco_trustsec sync
```

偵錯日誌

日誌位於磁碟上的以下位置：

```
/opt/plugins/var/log/pan/plugin_cisco_trustsec.log /opt/plugins/
var/log/pan/plugin_cisco_trustsec_sub.log /opt/plugins/var/
log/pan/plugin_cisco_trustsec_ret.log /opt/plugins/var/log/pan/
plugin_cisco_trustsec_proc.log
```

日誌檔案（Panorama 裝置上安裝的所有外掛程式共用）的大小限制是 1 千萬 byte（位元組）。一個日誌檔案可以接受 93,000 個工作階段登入。如果您設定日誌輪換，則備份日誌可以支援 186,000 個工作階段登入。

- 變更外掛程式偵錯層級。

```
request plugins debug level $level plugin-name cisco_trustsec
```

  - **off**：無偵錯日誌。
  - **low**：只傾印基本偵錯日誌。
  - **medium**：傾印詳細偵錯日誌。
  - **high**：傾印一切，包括伺服器的要求/回應訊息。
- 將日誌合併成單一日誌檔案：

```
request plugins cisco_trustsec merge-logs
```

- 在 CLI 中顯示偵錯日誌：
  - Cisco TrustSec 外掛程式版本 1.0.2 或更新版本安裝在 10.0.0 版之前的 Panorama 版本：

```
tail mp-log plugin_cisco_trustsec_merged.log
```

  - Cisco TrustSec 外掛程式版本 1.0.2 或更新版本安裝在 Panorama 版本 10.0.0 或更新版本：

```
tail follow yes plugins-log
```


©2023 Palo Alto Networks, Inc.

在 Nutanix AHV 上設定 VM-Series 防火牆

Nutanix AHV 專用 VM-Series 防火牆可讓您在能夠執行 Nutanix Acropolis Hypervisor 的裝置上部署 VM-Series 防火牆。如果您使用 Panorama 來管理 Nutanix AHV 上的 VM-Series 防火牆，則可以使用 Nutanix 專用 Panorama 外掛程式執行 VM 監控。這可讓您以動態方式向防火牆通知您的 Nutanix 環境有所變更，並確保虛擬機器會在加入您的網路後套用原則。

- 在 Nutanix AHV 上部署 VM-Series 防火牆
- Nutanix 上的 VM 監控

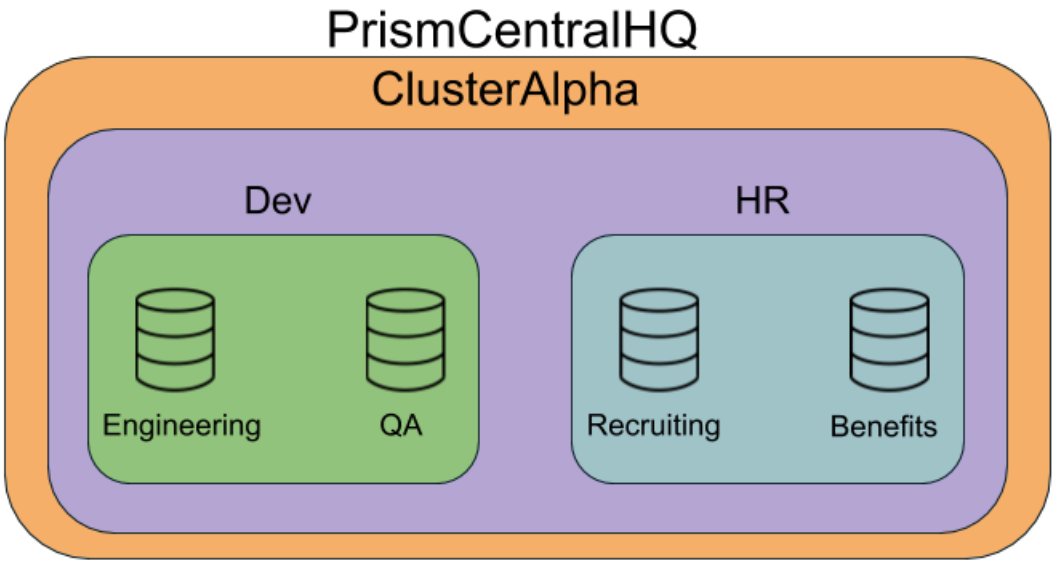
Nutanix 上的 VM 監控

安裝和設定 Nutanix 專用 Panorama 外掛程式，以監控 Nutanix 環境中的變更，並動態位址群組建立原則。

- 關於 Azure 上的 VM 監控
- 安裝 Nutanix 專用 Panorama 外掛程式
- 設定 Nutanix 專用 Panorama 外掛程式

關於 Azure 上的 VM 監控

Nutanix 專用 Panorama 外掛程式可監控您 環境中的虛擬機器，以利使用動態位址群組。Prism Central 可依類別將 Nutanix 環境中的實體分組，並進一步依值加以篩選。Panorama 可根據您在 Prism Central 中定義的類別和值建立標籤。當虛擬機器設置於某個類別中，並獲得指派的值時，Panorama 就會將對應的標籤套用至虛擬機器的 IP 位址。接著，您可以使用標籤作為 Panorama 中的動態位址群組的比對準則，以建立安全性原則。



在上述範例中，我們有 Dev 和 HR 兩個類別，其中分別包含兩個值。這些類別位於叢集內，而該叢集位於 Prism Central 中。當您開始監控 Nutanix 環境時，Panorama 就會使用值、叢集和 Prism Central 形成標籤。當您檢視動態位址群組的比對準則時，標籤會以下列格式列出。

ntnx.PC-<prism-central-name>.CL-<cluster-name>.<category>.<value>

透過上述範例中的資訊，Panorama 會建立下列標籤。

```
ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.Dev.Engineering
ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.Dev.QA
ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.HR.Recruiting
ntnx.PC-PrismCentralHQ.CL-ClusterAlpha.HR.Benefits
```


©2023 Palo Alto Networks, Inc.

若要保護這些類別中的工作負載，請使用這類標籤作為動態位址群組中的比對準則。然後，您可以使用動態位址群組作為安全性原則規則中的來源和目的地位址群組。當虛擬機器加入動態位址群組時，就會自動套用您所建立的原則。

安裝 Nutanix 專用 Panorama 外掛程式

若要開始在 Nutanix 上監控端點，請下載並安裝 Nutanix 專用 Panorama 外掛程式。

如果您有 Panorama HA 組態，請在每個 Panorama 端點上重複此安裝程序。在 Panoramas 上以 HA 對等安裝外掛程式時，請先將外掛程式安裝於被動對等，再安裝於主動對等。安裝外掛程式安裝於被動對等之後會轉換為非運作狀態。將外掛程式安裝於主動對等會將被動對等恢復為運作狀態。

如果您在安裝了多個外掛程式的 HA 配對中安裝了一個獨立的 Panorama 或兩個 Panorama 設備，則在未設定一或多個外掛程式的情況下，外掛程式可能不會收到更新的 IP-Tag 資訊。發生這種情況是因為 Panorama 不會將 IP-Tag 資訊轉送到未設定的外掛程式。此外，如果一或多個 Panorama 外掛程式未處於「已註冊」或「成功」狀態（每個外掛程式的正狀態不同），則可能會出現此問題。在繼續或執行下述命令之前，請確保您的外掛程式處於正狀態。

如果遇到此問題，有兩種權宜方案：

- 解除安裝未設定的外掛程式。建議您不要安裝未打算立即設定的外掛程式
- 您可以使用以下命令來變通處理此問題。對每個 Panorama 實例上的每個未設定外掛程式執行以下命令，以防止 Panorama 等待傳送更新。否則，防火牆可能會遺失一些 IP-Tag 資訊。

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  您可以透過執行以下命令來取消此命令：

  request plugins dau plugin-name <plugin-name> unblock-device-push no

上述的命令在重新啟動後不會持續存在，並且必須在任何後續重新啟動時再次使用。對於 HA 配對中的 Panorama，必須在每個 Panorama 上執行命令。

STEP 1 | 登入 Panorama 使用者介面。

STEP 2 | 選取 **Panorama** > **Plugins**（外掛程式）。

STEP 3 | 選取 **Check Now**（立即檢查） 以擷取可用更新清單。

STEP 4 | 選取 Action（動作）欄中的 **Download**（下載）以下載外掛程式。

STEP 5 | 選取外掛程式版本，在 Action（動作）欄中按一下 **Install**（安裝）來安裝外掛程式。安裝完成時，Panorama 會通知您。

設定 Nutanix 專用 Panorama 外掛程式

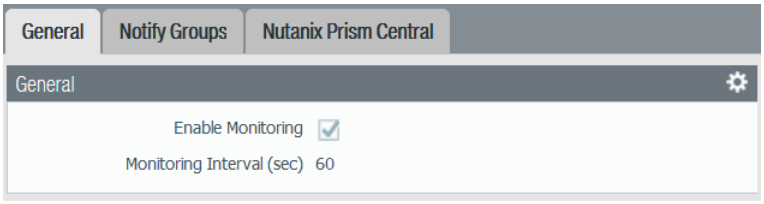
安裝外掛程式之後，請完成下列程序，以建立 Panorama 與 Prism Central 之間的連線。

STEP 1 | 登入 Panorama 網頁介面。

©2023 Palo Alto Networks, Inc.

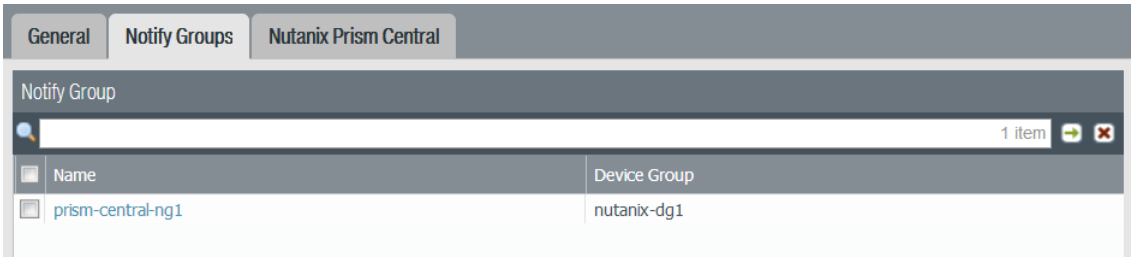
STEP 2 | 啟用監控，並設定監控間隔。

1. 選取 **Panorama** > **Nutanix** > **Setup**（設定） > **General**（一般）。
2. 選取 **Enable Monitoring**（啟用監控）。
3. 設定 **Monitoring Interval**（監控間隔），單位為秒。監控間隔是 Panorama 從 Prism Central 擷取已更新網路資訊的頻率。



STEP 3 | 建立通知群組。

1. 選取 **Panorama** > **Nutanix** > **Setup**（設定） > **Notify Groups**（通知群組）。
2. 按一下 **Add**（新增）。
3. 輸入通知群組的描述性 **Name**（名稱）。
4. 選取 Nutanix 部署中的裝置群組。



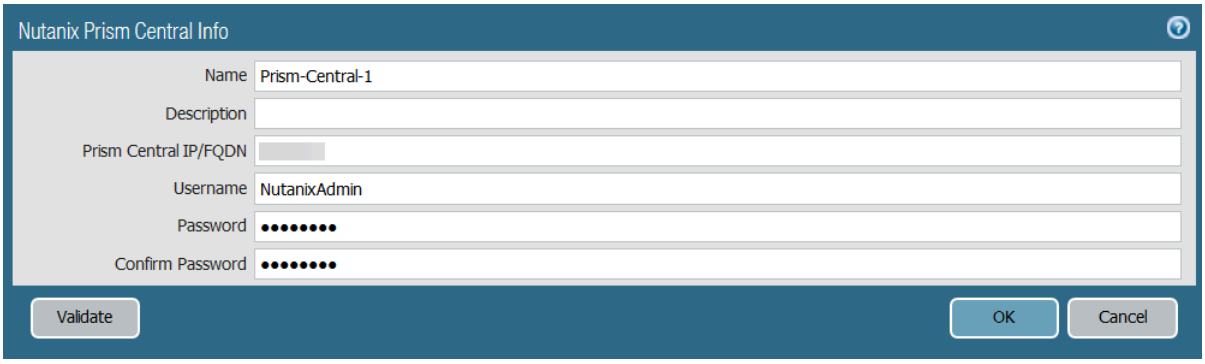
©2023 Palo Alto Networks, Inc.

STEP 4 | 新增 Prism Central 資訊。

1. 選取 **Panorama** > **Nutanix** > **Setup**（設定） > **Nutanix Prism Central**。
2. 按一下 **Add**（新增）。
3. 輸入 Prism Central 的描述性 **Name**（名稱）。
4. 輸入 Prism Central 的 IP 位址或 FQDN。
5. 輸入您的 Prism Central 使用者名稱。
6. 輸入並確認 Prism Central 密碼。
7. 按一下 **Validate**（驗證），以確認您已正確輸入 Prism Central 認證。

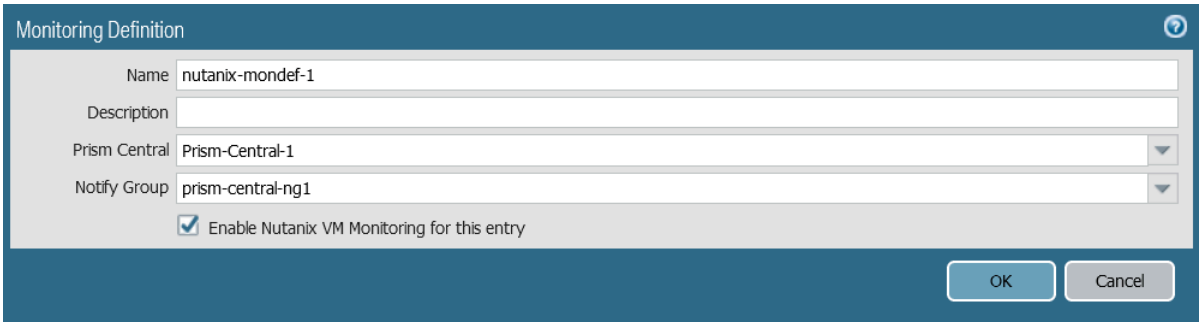
   如果您在按一下 *[OK*（確定）*]* 後返回 *[Nutanix Prism Central Info*（*Nutanix Prism Central* 資訊）*]* 視窗，此時若按一下 *[Validate*（驗證）*]* 按鈕，將會傳回認證驗證錯誤訊息。這是預期中的行為。雖然 *Panorama* 在密碼欄位中顯示點，但欄位是空的；這會導致即便 *Panorama* 成功連線至 *Prism Central*，驗證仍將失敗。

8. 按一下 **OK**（確定）。



STEP 5 | 設定監控定義。

1. 選取 **Panorama** > **Nutanix** > **Monitoring Definition**（監控定義），然後按一下 **Add**（新增）。
2. 輸入描述性 **Name**（名稱），並選擇性地輸入說明以識別您要使用此定義的 Prism Central。
3. 選取 **Prism Central** 和 **Notify Group**（通知群組）。
4. 按一下 **OK**（確定）。

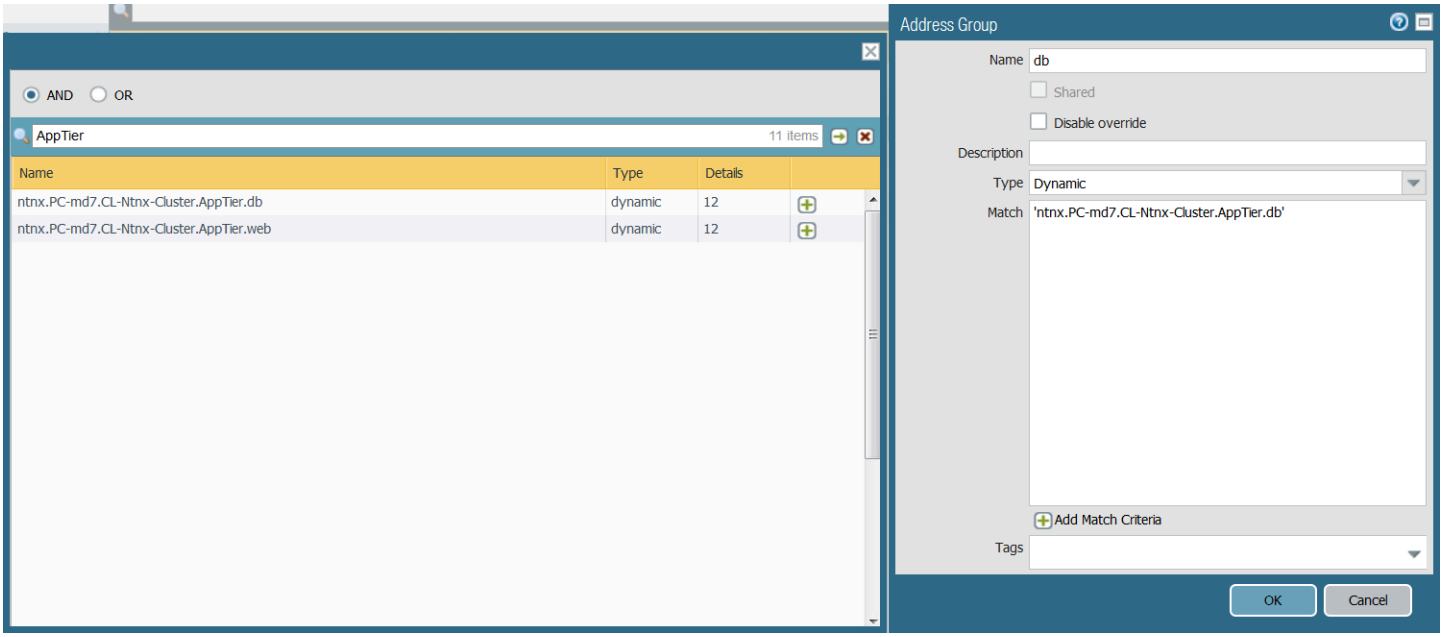


STEP 6 | **Commit**（提交）您的變更。

©2023 Palo Alto Networks, Inc.

STEP 7 | 確認您可在 Panorama 上檢視 VM 資訊，並定義動態位址群組的比對準則。

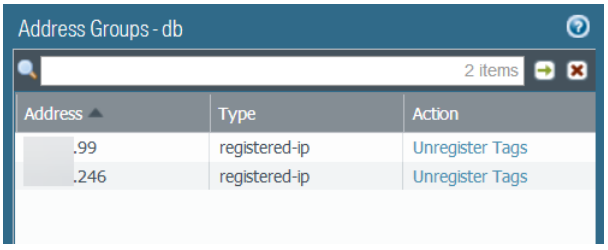
1. 選取 **Panorama** > **Objects**（物件） > **Address Groups**（位址群組），然後按一下 **Add**（新增）。
2. 為您的動態位指群組輸入描述性 **Name**（名稱）。
3. 從 [Type（類型）] 下拉式清單中，選取 **Dynamic**（動態）。
4. 按一下 **Add Match Criteria**（新增比對準則）。您可以選取動態標籤作為比對準則，以填入群組的成員。選取 **And** 或 **Or** 運算子，選取您在篩選或比對時要對照的屬性，然後按一下 **OK**（確定）。
5. **Commit**（提交）您的變更。



STEP 8 | 確認 VM 中的位址已新增至動態位址群組。

1. 選取 **Panorama** > **Objects**（物件） > **Address Groups**（位址群組）。
2. 在動態位址群組的 [Addresses（位址）] 欄中，按一下 **More**（更多）。

   Panorama 會根據您指定的比對準則，顯示已新增至該動態位址群組的 IP 位址清單。



©2023 Palo Alto Networks, Inc.

STEP 9 | 在原則中使用動態位址群組。

1. 選取 **Policies**（政策） > **Security**（安全性）。
2. 按一下 **Add**（新增），然後輸入原則的 **Name**（名稱）和 **Description**（說明）。
3. 新增 **Source Zone**（來源區域）以指定流量來源於哪個區域。
4. 新增流量將終止於哪個 **Destination Zone**（目的地區域）。
5. 對於 **Destination Address**（目的地位址），請選取您剛才建立的動態位址群組。
6. 針對流量指定動作—**Allow**（允許）或 **Deny**（拒絕），並選擇性地將預設安全性設定檔附加至規則。
7. 重複步驟 1 到 6，以建立另一個原則規則。
8. 按一下 **Commit**（交付）。

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.

啟動 VM-Series 防火牆

啟動程序可讓您建立一個在網路上部署新 VM-Series 防火牆的可重複且精簡的程序，因為它允許您為網路建立一個具有模型組態的套件，然後使用該套件隨時隨地部署 VM-Series 防火牆。

您可以使用完整設定來啟動防火牆，讓防火牆在啟動時就完整設定，您也可以從基本設定開始，這是可讓您啟動防火牆的最小初始設定，隨後再向 Panorama 註冊來完成設定。

如果您選擇基本設定，且在 AWS、Azure 或 GCP 上部署，則可以使用啟動套件和 `init-cfg.txt` 檔案。或者，您可以利用使用者資料來啟動。您不需要在檔案中提供啟動程序設定參數，而是在啟動 VM-Series 防火牆時，以鍵值組直接輸入到 AWS 或 GCP 使用者介面中。Azure 有類似的程序，可讓您在 Azure CLI 存取的範本或其他文字檔案中，提供啟動程序參數。

如果您建立啟動套件，請從外部裝置（例如虛擬磁碟、虛擬光碟）或雲端儲存裝置（例如貯體）傳遞套件。

- 選擇啟動方法
- VM-Series 防火牆啟動工作流程
- 啟動套件
- 啟動程序組態檔案
- 在 Panorama 上產生 VM 驗證金鑰
- 建立 init-cfg.txt 檔案
- 建立 bootstrap.xml 檔案
- 準備啟動程序授權
- 準備啟動程序套件
- 在 AWS 上啟動 VM-Series 防火牆
- 在 Azure 上啟動 VM-Series 防火牆
- 在 ESXi 上啟動 VM-Series 防火牆
- 在 Google Cloud Platform 上啟動 VM-Series 防火牆
- 在 Hyper-V 上啟動 VM-Series 防火牆
- 在 KVM 上啟動 VM-Series 防火牆
- 驗證啟動程序完成
- 啟動程序錯誤

選擇啟動方法

您可以使用基本設定或完整設定來啟動 VM-Series 防火牆。

完整設定使用啟動套件，且包含啟動時完整設定防火牆所需的一切資料。其中包括設定參數（在 init-cfg.txt 中）、內容更新和軟體版本。完整設定可以同時包含 init-cfg.txt 和 bootstrap.xml 檔案。

設定方法	設定位置	備註
在啟動套件的 /config/bootstrap.xml 中指定完整設定資訊。	公共雲端儲存 AWS S3 貯體、Azure 儲存帳戶或 Google 儲存貯體。	· 完整啟動套件在儲存貯體中。 · 需要雲端存取和 IAM 角色才能存取。

基本設定是可讓您啟動、授權和註冊 VM-Series 防火牆的最少設定。基本設定不支援外掛程式、內容、軟體映像或 bootstrap.xml。

啟動防火牆之後，您可以連接 Panorama 來完成設定，也可以登入防火牆來手動更新內容和軟體。下表簡單對照可用來儲存和存取基本設定的三種方法：

設定方法	設定位置	備註
init-cfg.txt 在啟動套件的 config/init-cfg.txt 中以鍵值組儲存基本設定參數。	公共雲端儲存 · AWS S3 貯體 · Azure 儲存帳戶 · GCP 儲存貯體	· 需要雲端存取和 IAM 角色才能存取。還必須將貯體的存取權授與 Panorama 管理員。
使用者資料 在公共雲端使用者介面中以鍵值組輸入設定參數。	**VM** 實例 · Alibaba：使用者資料 · AWS：使用者資料 · Azure：自訂資料 · GCP：GCP 中繼資料 · Oracle Cloud Infrastructure：使用者資料	· 初始設定參數隨 VM 一起儲存。 · 不需要另外儲存和相關聯的 IAM 角色。
AWS Secret Manager 在 AWS Secret Manager 中以鍵值組輸入設定參數。	在 AWS Secret Manager 中加密。	· 您需要 IAM 角色才能建立機密。可授權其他人取得機密。 · 若要取得機密，請以使用者資料傳遞機密名稱。

請參閱 VM-Series 防火牆啟動工作流程，以比較基本和完整設定的工作流程。

©2023 Palo Alto Networks, Inc.

- 基本設定
- 完成設定。

基本設定

基本設定包含初始設定和授權。您可以使用啟動套件傳遞初始設定的鍵值組，也可以輸入啟動程序參數鍵值組當成使用者資料。

如果不使用 Panorama，您可以使用初始設定來啟動防火牆，然後登入並手動完整設定。如果您使用 Panorama，則初始設定必須包含 Panorama 伺服器 IP 位址及 VM 驗證金鑰的啟動程序參數，以便啟動的防火牆向 Panorama 註冊和完成完整設定。

- 將基本設定新增至啟動套件
- 以使用者資料輸入基本設定（公共雲端）
- 在 AWS Secrets Manager 中儲存基本設定

將基本設定新增至啟動套件

初始設定是可讓您啟動、授權和註冊 VM-Series 防火牆及連接 Panorama（如適用）的最少設定。您需要在啟動套件中提供設定 (init-cfg.txt)。

以使用者資料輸入基本設定（公共雲端）

當您從公共雲端使用者介面部署 VM-Series 防火牆時，您可以在啟動/部署過程中以使用者資料輸入設定參數。如果您有足夠權限從雲端帳戶部署防火牆及存取 Panorama（如果使用），則可以略過建立啟動套件、建立設定檔案，以及雲端儲存相關的啟動工作（儲存貯體、IAM 角色，或授權外部存取儲存的服務帳戶）。

設定參數包括init-cfg.txt 檔案元件中的值，還有以下只當作使用者資料的額外值：

- **authcodes**—用來註冊 VM-Series 防火牆的驗證碼。例如，**authcodes=I7115398**。
- **mgmt-interface-swap**—在 AWS 或 GCP 部署中，當 VM-Series 防火牆位於負載平衡器後方時，用來交換管理介面。例如，**mgmt-interface-swap=enable**。

您可以在 Alibaba、AWS、GCP 或 OCI 使用者介面中，直接以鍵值組輸入設定參數。您也可以從文字檔案或雲端原生範本中定義設定，例如 AWS Cloud Formation 範本、Azure ARM 範本、GCP YAML 檔案或 Terraform 範本。

每個雲端各以不同術語描述使用者資料，且在啟動程序參數之間使用不同的分隔符號。

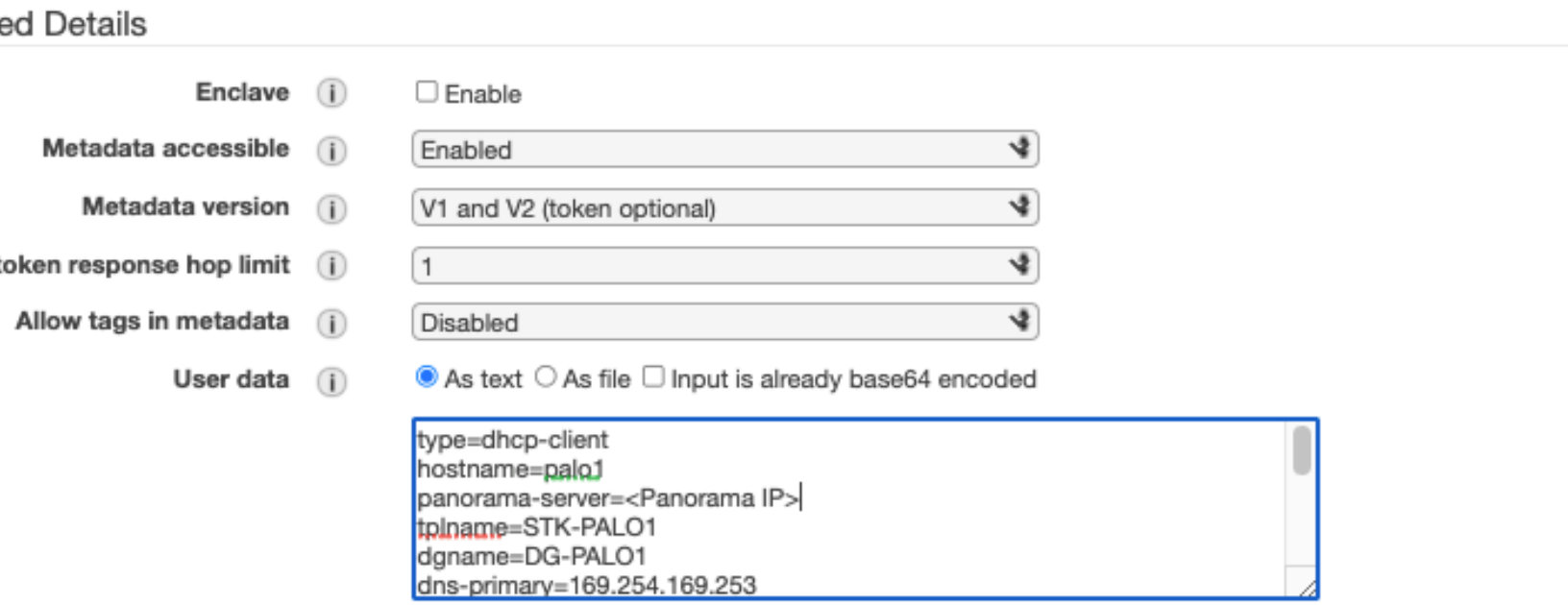
- **Alibaba Cloud** 使用者資料 —每個參數使用換行符號 (\n)，如果參數有多個選項，請使用逗號來分隔。
- **AWS** 使用者資料 — 使用分號或換行符號 (\n)。如果參數有一個以上的選項，請以逗號來分隔選項。例如：

```
  type=dhcp-client hostname=palo1 panorama-server=<PANORAMA-1 IP>
 panorama-server-2=<PANORAMA-2 IP> tplname=STK-NGFW-01 dgname=DG-
NGFW-01 dns-primary=169.254.169.253 dns-secondary=8.8.8.8 op-
command-modes=mgmt-interface-swap dhcp-send-hostname=yes dhcp-send-
client-id=yes dhcp-accept-server-hostname=yes dhcp-accept-server-
```


©2023 Palo Alto Networks, Inc.

```
domain=yes vm-auth-key= <YOUR AUTH KEY HERE> authcodes= <<YOUR AUTH
 CODE HERE>
```

如果您選擇在 AWS Secrets Manager 中儲存基本設定，請在使用者資料欄位中以鍵值組輸入機密名稱。例如：



- **Azure** 自訂資料 — 使用分號。如果參數有一個以上的選項，請以逗號來分隔選項。例如：

```
type=dhcp-client; op-command-modes=jumbo-frame; plugin-op-
commands=numa-perf-optimize:enable,set-dp-cores:30 vm-series-auto-
registration-pin-id=abcdefgh1234****; vm-series-auto-registration-
pin-value=zyxwvut-0987****
```

- **GCP** 自訂中繼資料—在檔案中，例如 YAML 檔案或 Terraform 範本，每個參數使用換行符號 (\n)，如果參數有多個選項，請使用逗號來分隔。例如：

```
type=dhcp-client op-command-modes=mgmt-interface-swap,jumbo-frame
 plugin-op-commands=numa-perf-optimize:enable,set-dp-cores:30 vm-
series-auto-registration-pin-id=abcdefgh1234**** vm-series-auto-
registration-pin-value=zyxwvut-0987****
```

- **Oracle Cloud Infrastructure** 使用者資料—每個參數使用換行符號 (\n)，如果參數有多個選項，請使用逗號來分隔。

在 AWS Secrets Manager 中儲存基本設定

您可以使用 AWS Secrets Manager 將基本設定儲存為機密，然後利用使用者資料以機密中儲存的參數啟動 VM。若要執行此工作，您需要有使用 Secrets Manager 的權限。

©2023 Palo Alto Networks, Inc.

- 機密建立者必須有 Secrets Manager 管理員完整權限。Secrets Manager 管理員可以允許其他人使用機密，如 AWS Secrets Manager 的身分驗證與存取控制所述。

  例如，下列政策陳述式可讓您取得機密值：

```
{ "版本":"2012-10-17", { "效果":"允許", "動
作": "secretsmanager:GetSecretValue", "資源":
 "arn:aws:secretsmanager:us-east-1:688382******:secret:My_bts-
******" } }
```

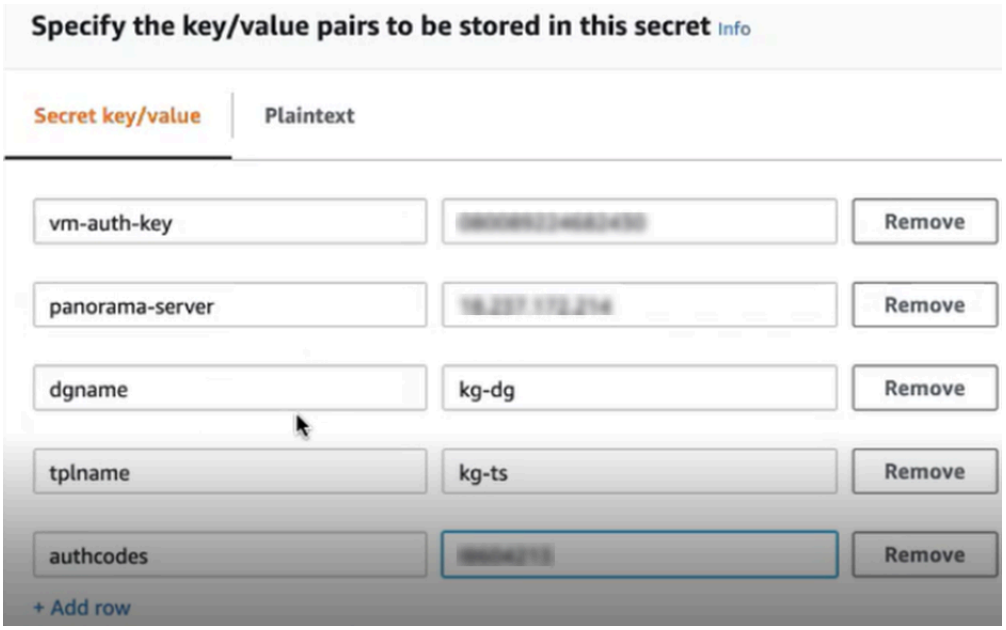
  請參閱您在 AWS Secrets Manager 的 IAM 政策或機密政策中可以使用的動作、資源和內容金鑰，以了解需要權限的動作，例如列出、取得和輪換機密。

- （選用）若要加密機密，您可以從 AWS Secrets Manager 使用 DefaultEncryptionKey。

STEP 1 | 登入 AWS 主控台，在 [Security, Identity and Compliance（安全、身分和合規）] 下方，選取 **Secrets Manager**，然後選取 **Store a new secret**（儲存新的機密）。

STEP 2 | 選取 **other type of secrets**（其他類型的機密）。

1. 輸入鍵值組來定義基本設定。



   mgmt-interface-swap 在 *AWS* 機密中不是以鍵值組輸入。必須輸入為：***op-command-modes=mgmt-interface-swap***

2. 選取 DefaultEncryptionKey，然後按 **Next**（下一步）。

STEP 3 | 提供機密名稱和說明。

1. 編輯資源權限，以透過 AWS 帳戶安全地存取機密。例如：

```
{ "版本":"2012-10-17", "聲明": [ { "Sid":"VisualEditor0","效
果":"允許", "動作": "s3:ListBucket", "資源": "arn:aws:s3:::sn-
bootstrap" }, { "Sid":"VisualEditor1","效果":"允許", "動作":
```


©2023 Palo Alto Networks, Inc.

```
 "s3:GetObject", "資源": "arn:aws:s3:::sn-bootstrap/*" },
 { "效果":"允許", "動作": "secretsmanager:GetSecretValue",
 "資源": "arn:aws:secretsmanager:us-east-1:688382******:
 secret:My_bootstrap" } ] }
```

2. （選用）您可以從命令列檢查機密（如果您有權限）。例如：

```
# aws secretsmanager get-secret-value --secret-id My_bootstrap
 { "ARN": "arn:aws:secretsmanager:us-east-1:688382******:
 secret:My_bootstrap", "名稱":"My_bootstrap", "版本
 ID":"01b6853d-e187-479f-**********", "密碼字串": "{\"mgmt-
interface-swap\":\"enable\", \"vm-auth-key\":\"AAA\",
\"panorama-server\":\"10.*.*.1\", \"panorama-server-2\":
\"10.*.*.2\",\"dgname\":\"dg-s0000h\", \"tplname\":\"tpl-
santosh\",\"license-authcode\":\"AAAA\"}", "版本階段":
 [ "AWSCURRENT" ], "建立日期":1581018411.847 }
```

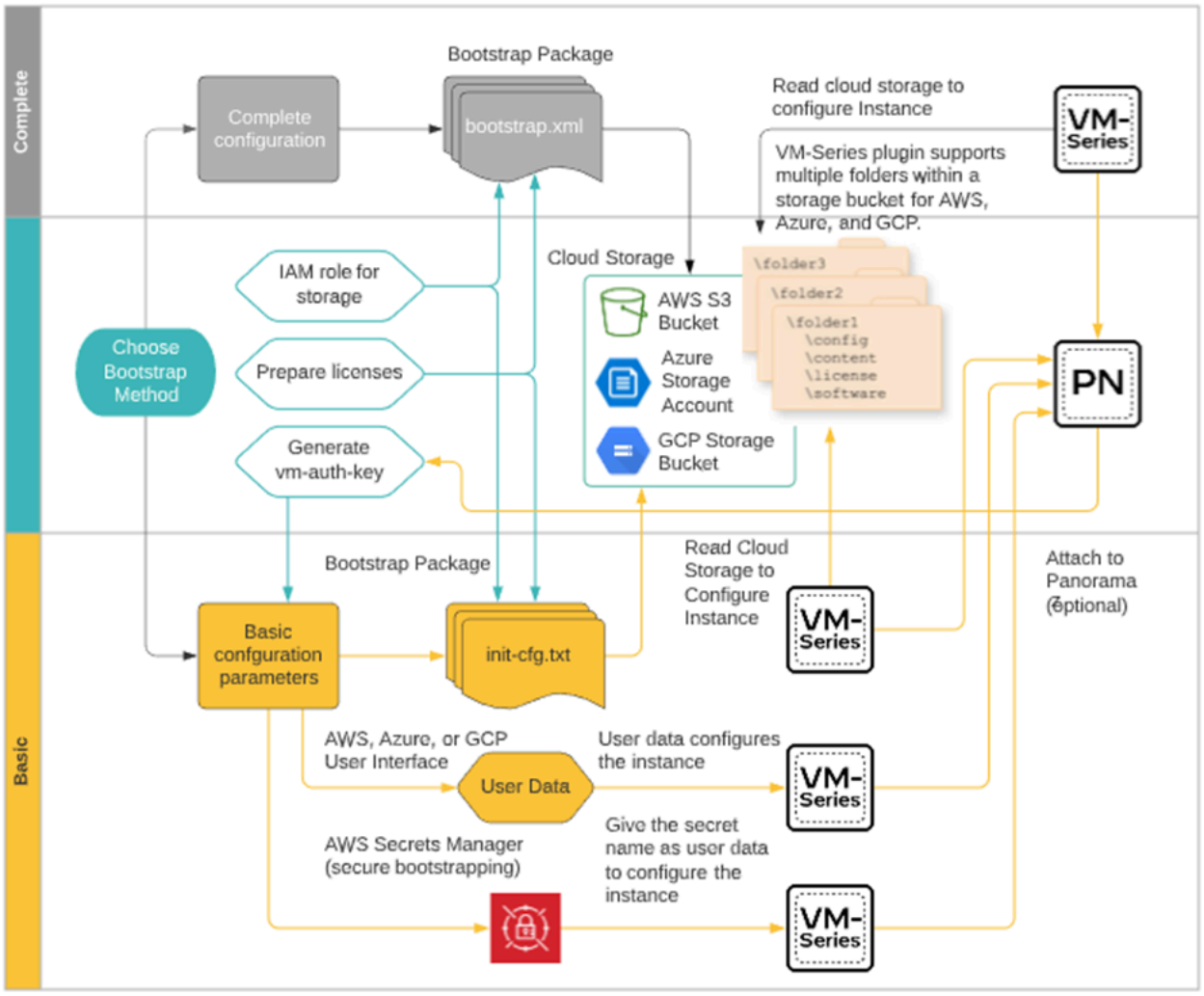
完成設定。

完整設定可確保防火牆在啟動時完整設定。bootstrap.xml 檔案包含初始設定、授權、軟體、內容和一個版本的 VM-Series 外掛程式。您可以手動建立 **bootstrap.xml**，也可以匯出現有設定，如建立 bootstrap.xml 檔案所述。

©2023 Palo Alto Networks, Inc.

VM-Series 防火牆啟動工作流程

使用下列工作流程來啟動 VM-Series 防火牆。如需完整和基本啟動載入程序的概觀，請參閱下圖。



STEP 1 | （選用）基於安全考量，您只能啟動處於原廠預設狀態的防火牆。如果您想要使用啟動套件來啟動先前設定的 VM-Series 防火牆，請將防火牆重設為原廠預設設定。

STEP 2 | 選擇啟動方法。

當您熟悉啟動套件之後，請評估您想要使用完整設定還是基本設定，然後可選擇使用 Panorama 來管理所啟動的防火牆。

如果您選擇基本設定，請決定是否使用啟動套件，或在使用者資料中以鍵值組輸入設定參數。

STEP 3 | （選用）如果您想使用 Panorama 來管理要啟動的 VM-Series 防火牆，請在 Panorama 上產生 VM 授權金鑰。您必須將此金鑰加入 `init-cfg.txt` 檔案 (**`vm-auth-key`**)，或以使用者資料輸入鍵值組。

STEP 4 | 準備啟動程序授權。

©2023 Palo Alto Networks, Inc.

STEP 5 | 如果您選擇基本設定且打算以使用者資料來啟動，請跳至步驟 7。

如果您打算使用基本設定和啟動套件，請建立 init-cfg.txt 檔案並準備啟動套件。

如果您選擇完整設定，請建立 bootstrap.xml 檔案並準備完整的啟動套件。

STEP 6 | 準備啟動套件，並以您的超管理器適合的傳遞格式儲存啟動套件。

STEP 7 | 啟動 VM-Series 防火牆。

- 在 AWS 上啟動 VM-Series 防火牆
- 在 Azure 上啟動 VM-Series 防火牆
- 在 ESXi 上啟動 VM-Series 防火牆
- 在 Google Cloud Platform 上啟動 VM-Series 防火牆
- 在 Hyper-V 上啟動 VM-Series 防火牆
- 在 KVM 上啟動 VM-Series 防火牆

STEP 8 | 驗證啟動程序完成。

©2023 Palo Alto Networks, Inc.

啟動套件

當防火牆處於原廠預設狀態時，僅在首次啟動時初始化啟動程序。

- 啟動套件結構
- 啟動套件傳遞

啟動套件結構

啟動套件必須包含 `/config`、`/license`、`/software` 和 `/content` 資料夾（即使是空的）。`/plugins` 是選用資料夾。如需範例，請參閱準備啟動程序套件。

- **/config folder**—包含組態檔案。此資料夾可包含兩個檔案：`init-cfg.txt` 和 `bootstrap.xml`。如需詳細資訊，請參閱啟動程序設定檔案。

  如果您打算使用啟動程序向 *Panorama* 預先註冊 *VM-Series* 防火牆，則必須在 *Panorama* 上產生 *VM* 驗證金鑰，並將產生的金鑰加入 ***`init-cfg.txt`*** 檔案中。請參閱在 Panorama 上產生 VM 驗證金鑰。

- **/license folder**—包含您打算在防火牆上啟動的授權金鑰或授權及訂閱的驗證碼。如果防火牆未連線網際網路，您必須從 Palo Alto Networks 支援入口網站手動取得授權金鑰，或使用授權 API 取得金鑰，然後將每個金鑰儲存在此資料夾。如需詳細資訊，請參閱準備啟動授權

  必須包含驗證碼包而非個別的驗證碼，以便防火牆或協調運作服務可同步擷取與防火牆關聯的所有授權金鑰。如果您使用個別的驗證碼而非驗證碼包，防火牆將只會擷取檔案中包含的首個驗證碼的授權金鑰。

- **/software folder**—包含將新佈建的 VM-Series 防火牆升級至網路所需 PAN-OS 版本的必要軟體映像。必須包含目前版本與 VM-Series 防火牆要升級為最終 PAN-OS 軟體版本之間的所有中繼軟體版本。請參閱相容性矩陣中的 VM-Series 防火牆超管理器支援。
- **/content folder**—包含應用程式與威脅更新、WildFire 更新及 BrightCloud URL 篩選資料庫，以取得 VM-Series 防火牆的有效訂閱。必須包含您所希望 PAN-OS 版本所需的最低內容版本。如果您沒有 PAN-OS 版本相關聯的最低必要內容版本，則 VM-Series 防火牆無法完成軟體升級。
- **/plugins** 資料夾—選用資料夾包含單一 VM-Series 外掛程式映像。

啟動套件傳遞

將啟動套件傳送至 VM-Series 防火牆所用檔案的類型因 Hypervisor 而異。使用下表決定超管理器或雲端廠商支援的檔案類型。

用於啟動的外部設備（啟動套件格式）	AWS	Azure	ESXi	Google	Hyper-V	KVM
CD-ROM（ISO 映像）	—	—	是	—	是	是
區塊儲存裝置	—	—	是	—	是	是

©2023 Palo Alto Networks, Inc.

用於啟動的外部設備（啟動套件格式）	AWS	Azure	ESXi	Google	Hyper-V	KVM
儲存帳戶	—	是	—	—	—	—
貯體	是	—	—	是	—	—

當您將儲存裝置連接至防火牆時，防火牆會掃描是否有啟動套件，如果找到，防火牆會使用該啟動套件中定義的設定。

如果檔案中包含 Panorama 伺服器 IP 位址，防火牆將會連線 Panorama。如果防火牆已連線網際網路，則會連線授權伺服器以更新 UUID 並取得授權金鑰及訂閱。防火牆隨後會新增為 Palo Alto Networks 支援入口網站中的資產。如果防火牆未連線網際網路，則會使用您在啟動套件中包含的授權金鑰，或連線至 Panorama 來擷取適當授權，並將授權部署至受管理的防火牆。

©2023 Palo Alto Networks, Inc.

啟動程序組態檔案

啟動套件必須在 **config/init-cfg.txt** 中包含基本設定。完整設定（在 **/config/bootstrap.xml** 檔案）為選用。

當啟動套件包含 **init-cfg.txt** 檔案和 **bootstrap.xml** 檔案時，防火牆會合併這些檔案的設定，而如果任何設定重疊，防火牆會使用 **init-cfg.txt** 檔案中定義的值。

- init-cfg.txt
- bootstrap.xml

init-cfg.txt

包含在防火牆上設定管理介面所需的基本資訊，例如 IP 位址類型（靜態或 DHCP）、IP 位址（僅 IPv4，或 IPv4 和 IPv6 兩者）、網路遮罩及預設閘道。DNS 伺服器 IP 位址、Panorama IP 位址和設備群組及範本堆疊參數為可選用。

您可以使用一般名稱 **init-cfg.txt**，或更為具體在檔案名稱前面加上每個防火牆的 UUID 或序號（例如：**0008C100105-init-cfg.txt**）。

防火牆啟動時會搜尋符合 UUID 或序號的文字檔案，如果找不到，則會使用一般檔案名稱 **init-cfg.txt** 來搜尋。如需範例檔案，請參閱建立 init-cfg.txt 檔案。

若您使用 *Panorama* 管理啟動的 *VM-Series* 防火牆：

- 您必須在 *Panorama* 上產生 *VM* 驗證金鑰，並將金鑰加入 ***init-cfg.txt*** 檔案中。如需詳細資訊，請參閱在 Panorama 上產生 VM 驗證金鑰。
- 管理防火牆的 *Panorama* 設備必須設定為 *Panorama* 模式。如果您以僅限管理模式使用 *Panorama* 設備，則會捨棄防火牆日誌，因為僅限管理模式下的 *Panorama* 沒有日誌收集器群組可儲存防火牆日誌。

bootstrap.xml

選用 **bootstrap.xml** 檔案包含防火牆的完整設定。如果您不使用 Panorama 集中管理防火牆，**bootstrap.xml** 檔案提供方法來自動部署啟動時設定的防火牆。

您可以手動定義設定，或從現有防火牆匯出執行中的設定 (**running-config.xml**)，並將檔案儲存為 **bootstrap.xml**。如果您匯出 **bootstrap.xml** 檔案，請確保從您的部署所在相同平台或超管理器上部署的防火牆匯出 XML 檔案。請參閱建立 bootstrap.xml 檔案。

©2023 Palo Alto Networks, Inc.

在 Panorama 上產生 VM 驗證金鑰

如果您要使用 Panorama 來管理您正在啟動的 VM-Series 防火牆，必須在 Panorama 上產生 VM 驗證金鑰，並在基本組態 (init-cfg.txt) 檔案中包含該金鑰。VM 驗證金鑰可讓 Panorama 驗證新啟動的 VM-Series 防火牆。因此，若要使用 Panorama 管理防火牆，必須包含 Panorama 的 IP 位址，且在基本組態檔案中包含 VM 驗證金鑰，而啟動程序套件的 /license 資料夾中必須包含授權驗證碼。防火牆隨後可在其首次請求連線 Panorama 時提供 IP 位址、序號和 VM 驗證金鑰，以便 Panorama 確認 VM 驗證金鑰的有效性，並將防火牆新增為受管理的設定。如果您在基本組態檔案中提供設備群組及範本，Panorama 會將防火牆指派給相應的設備群組及範本，以便您使用 Panorama 集中設定及管理防火牆。

金鑰的使用期限介於 1 小時至 8760 小時（1 年）之間。指定時間過後，金鑰將過期，若在此連線請求中沒有提供有效的驗證金鑰，Panorama 將不會註冊 VM-Series 防火牆。

STEP 1 | 登入 Panorama CLI 或存取 API：

- 在 CLI 中，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: 2015/12/29 12:03:52
  ```

- 在 API 中，使用下列 URL：

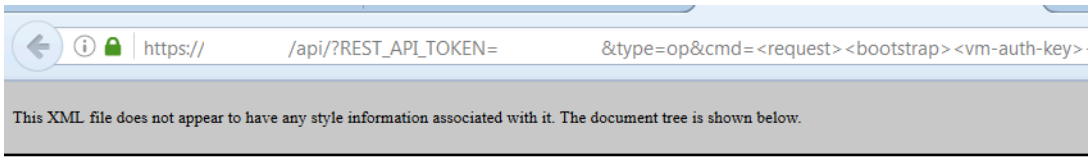
  ```
  https://<Panorama_IP_address>/api/?
  type=op&cmd=<request><bootstrap><vm-auth-
  key><generate><lifetime><number-of-hours></lifetime></generate></
  vm-auth-key></bootstrap></request>
  ```

  其中，lifetime 是 VM 驗證金鑰有效的小時數。

©2023 Palo Alto Networks, Inc.

STEP 2 | 確認在 Panorama 上產生的 VM 驗證金鑰的有效期限。確保有效期限的設定可讓防火牆在 Panorama 上的註冊時間足夠。

```
https://<Panorama_IP_address>/api/?
type=op&cmd=<request><bootstrap><vm-auth-key><show></show></vm-
auth-key></bootstrap></request>
```



This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
- <response status="success">
  - <result>
    - <bootstrap-vm-auth-keys>
      - <entry>
          <vm-auth-key>085812955845977</vm-auth-key>
          <expiry-time>2016/03/17 08:35:05</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>136387033275034</vm-auth-key>
          <expiry-time>2016/05/20 14:12:59</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>178644792323541</vm-auth-key>
          <expiry-time>2016/06/10 16:25:36</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>221348425464173</vm-auth-key>
          <expiry-time>2016/05/20 13:54:25</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>245832696687351</vm-auth-key>
          <expiry-time>2015/12/22 17:53:48</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>386239691539160</vm-auth-key>
          <expiry-time>2016/03/02 11:09:46</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>420246530153909</vm-auth-key>
          <expiry-time>2016/03/09 00:57:01</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>431216710324086</vm-auth-key>
          <expiry-time>2016/03/09 00:57:09</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>445486056501180</vm-auth-key>
          <expiry-time>2016/05/20 14:12:52</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>633795692572911</vm-auth-key>
          <expiry-time>2016/03/09 14:50:38</expiry-time>
        </entry>
      - <entry>
          <vm-auth-key>798346857952985</vm-auth-key>
          <expiry-time>2016/05/20 14:08:14</expiry-time>
        </entry>
      </bootstrap-vm-auth-keys>
    </result>
  </response>
```


STEP 3 | 將產生的 VM 驗證金鑰新增至基本組態 (init-cfg.txt) 檔案。請參閱建立 init-cfg.txt 檔案

©2023 Palo Alto Networks, Inc.

建立 init-cfg.txt 檔案

需要 **init-cfg.txt** 檔案才能啟動 VM-Series 防火牆。此檔案提供防火牆連線至網路所需的基本資訊。

- init-cfg.txt 檔案元件
- 範例 init-cfg.txt 檔案

請完成下列程序來建立 **init-cfg.txt** 檔案。

STEP 1 | 建立新文字檔案。

使用文字編輯器，例如 Notepad、EditPad 或其他純文字編輯器建立文字檔案。

STEP 2 | 在防火牆上新增管理介面的網路組態。



如果此檔案中缺少任何必要參數，防火牆將結束啟動程序，並使用預設 ***IP*** 位址 *192.168.1.1* 啟動。您可以檢視防火牆上的系統記錄，找出啟動失敗的原因。關於錯誤，請參閱授權 API。



各欄位金鑰與值之間沒有任何空格。請勿新增空格，因為這會導致管理員伺服器解析期間發生故障。

- 若要使用靜態 IP 位址設定管理介面，您必須指定 IP 位址、位址類型、預設閘道及網路遮罩。IPv4 位址是必要，IPv6 位址是選用。關於語法，請參閱範例 init-cfg.txt 檔案。
- 若要將管理介面設定為 DHCP 用戶端，您必須僅指定位址的類型。如果在管理介面上啟用 DHCP 用戶端，防火牆將略過 IP 位址、預設閘道、網路遮罩、IPv6 位址及檔案中定義的 IPv6 預設閘道值。關於語法，請參閱範例 init-cfg.txt 檔案。

在管理介面上啟用 DHCP 後，防火牆將連線 DHCP 指派的 IP 位址，且可在整個網路存取。您可以在儀表盤的 General Information（一般資訊）Widget 上檢視 DHCP 指派的 IP 位址，或使用 CLI 命令 **show system info**。然而，預設靜態管理 IP 位址 192.168.1.1 將保留在防火牆上正在執行的組態中 (**show config running**)。如果 DHCP 無法存取防火牆，此靜態 IP 位址確保您可以隨時還原防火牆連線。

STEP 3 | 新增 VM 驗證金鑰，以在 Panorama 上註冊 VM-Series 防火牆。

若要在 Panorama 上新增 VM-Series 防火牆，必須將您在 Panorama 上產生的 VM 驗證金鑰新增至基本設定 (**init-cfg.txt**) 檔案。如需有關產生金鑰的詳細資訊，請參閱在 Panorama 上產生 VM 驗證金鑰。

STEP 4 | 新增存取 Panorama 的詳細資訊。

- 新增主要與次要 Panorama 伺服器的 IP 位址。
- 指定您想要指派防火牆的範本與設備群組。

STEP 5 | （建議）新增 VM-Series 註冊 PIN 和值來安裝裝置憑證。

如果想要在 VM-Series 防火牆啟動時安裝裝置憑證，您必須在 CSP 上產生 VM-Series 註冊 PIN ID 並加入 **init-cfg.txt** 檔案中。此 PIN 和值也會套用任何使用 PAYG 授權的網站授權。

©2023 Palo Alto Networks, Inc.

STEP 6 | （選用）包含防火牆的其他參數。

- 新增主要與次要 DNS 伺服器的 IP 位址。
- 新增防火牆的主機名稱。
- 啟用 Jumbo Frame 或多個虛擬系統（或兩者）
- 對 AWS 或 GCP 上的 VM-Series 防火牆上啟用管理介面交換 (mgmt) 和資料平面介面 (ethernet 1/1)。如需有關變更管理介面的詳細資訊，請參閱搭配 Amazon ELB 使用的管理介面對應或管理 Google Cloud Platform 負載平衡的介面交換。
- 啟用或停用 DPDK。

init-cfg.txt 檔案元件

下表說明 **init-cfg.txt** 檔案中的啟動程序參數。

欄位	說明
type=	管理 IP 位址的類型：靜態或 DHCP 用戶端。此欄位為必填。
ip-address=	IPv4 位址。如果類型為 DHCP 用戶端，則略過此欄位。如果類型為靜態，則需要 IPv4 位址；ipv6-address 欄位是選用，可以包括在內。 您無法在 AWS 及 Azure 中指定 VM-Series 防火牆的管理 IP 位址與網路遮罩組態。如果已定義，防火牆將略過您指定的值。
default-gateway=	管理介面的 IPv4 預設閘道如果類型為 DHCP 用戶端，則略過此欄位。如果類型為靜態，則使用 IP 位址，此欄位為必填。
netmask=	IPv4 網路遮罩。如果類型為 DHCP 用戶端，則略過此欄位。如果類型為靜態，則使用 IP 位址，此欄位為必填。
ipv6-address=	（選用）管理介面的 IPv6 位址及 /prefix 長度。如果類型為 DHCP 用戶端，則略過此欄位。如果類型為靜態，則除了必要的 ip-address 欄位，還可以指定此欄位。
ipv6-default-gateway=	管理介面的 IPv6 預設閘道如果類型為 DHCP 用戶端，則略過此欄位。如果類型為靜態，則使用 IPv6 位址，此欄位為必填。
hostname=	防火牆的主機名稱。
panorama-server=	主要 Panorama 伺服器的 IPv4 或 IPv6 位址。這不是必要欄位，但為了集中管理防火牆，仍建議指定。
panorama-server-2=	次要 Panorama 伺服器的 IPv4 或 IPv6 位址。此欄位非必填但建議。

©2023 Palo Alto Networks, Inc.

欄位	說明
tplname=	Panorama 範本堆疊名稱。如果您新增 Panorama 伺服器 IP 位址，最佳作法是在 Panorama 上將防火牆指定給範本堆疊，並在此欄位中輸入範本堆疊名稱，如此就能集中管理組態設定並推送至防火牆。
dgname=	Panorama 裝置群組名稱。如果您新增 Panorama 伺服器 IP 位址，最佳作法是在 Panorama 上建立裝置群組，並在此欄位中輸入裝置群組名稱，如此就能分乎邏輯地分組防火牆，並將原則規則推送至防火牆。
cgname=	Panorama 收集器群組名稱。如果您要引導防火牆將日誌傳送至 Panorama 收集器群組，則必須先在 Panorama 上設定收集器群組，然後將防火牆設定為將日誌轉送至 Panorama。 在 M-Series 設備上，已預先定義預設收集器群組，且其中已包含本機日誌收集器當作成員。在 Panorama 虛擬設備上，您必須新增收集器群組，並將本機日誌收集器新增為成員。
dns-primary=	主要 DNS 伺服器的 IPv4 或 IPv6 位址。
dns-secondary=	次要 DNS 伺服器的 IPv4 或 IPv6 位址。
vm-auth-key=	Panorama 的虛擬電腦驗證金鑰（請參閱在 Panorama 上產生 VM 驗證金鑰）。啟動硬體防火牆時會略過此欄位。
op-command-modes=	允許下列值：multi-vsys、jumbo-frame、mgmt-interface-swap如果您輸入多個值，請使用空格或逗號分隔項目。 · **multi-vsys**—（僅限基於硬體的防火牆）啟用多個虛擬系統。 · **jumbo-frame**—將所有第三層介面的預設 MTU 大小設為 9192 位元組。 · **mgmt-interface-swap**—（僅限 AWS、Google、ESXi 和 KVM 上的 VM-Series 防火牆）部署防火牆時，允許您將管理介面 (MGT) 與資料平面介面 (ethernet 1/1) 互換。如需詳細資訊，請參閱 · 搭配 Amazon ELB 使用的管理介面對應 · 管理 Google Cloud Platform 負載平衡的介面交換 · 使用 VM-Series CLI 在 ESXi 上交換管理介面 · 使用 VM-Series CLI 在 KVM 上交換管理介面
op-cmd-dpdk-pkt-io=	值 **on** 或 **off** 可讓您在防火牆支援 DPDK 的環境中，啟用或停用 Data Plane Development Kit（資料平面開發套件 - DPDK）。DPDK 可讓主機略過 Linux 核心以加速處理封包；與 NIC 之間的互動是利用驅動程式和 DPDK 程式庫來執行。
plugin-op-commands=	指定 VM-Series 外掛程式操作命令。

©2023 Palo Alto Networks, Inc.

欄位	說明
	多個命令必須輸入成一份清單，以逗號分隔，不能有空格。 · **sriov-access-mode-on**—此命令只對 ESXi 和 KVM 超管理器上的 VM-Series 防火牆有效。 僅限 KVM，如果您啟用 **sriov-access-mode-on**，請勿啟用 **op-command-modes=jumbo-frame**。 · **aws-gwlb-inspect:enable**—啟用 VM-Series 與 AWS 閘道負載平衡器整合。 · **aws-gwlb-associate-vpce**: **<vpce-id>@ethernet<subinterface>**—可讓您將 VPC 端點與 VM-Series 介面建立關聯，或與防火牆上的子介面建立關聯。指定的介面會指派給安全性地區。 · **aws-gwlb-overlay-routing:enable**—與 AWS GWLB 整合時，使用此命令對 AWS 上的 VM-Series 啟用覆疊路由。 · **set-dp-cores:<#-cores>**—針對執行 PAN-OS 10.2 或更新版本並以軟體 NGFW 授權部署的 VM-Series 防火牆，自訂資料平面 vCPU 數目。NSX-T 不支援此選項。如需詳細資訊，請參閱 自訂資料平面核心。 · **numa-perf-optimize:enable**—在已安裝 VM-Series 外掛程式 2.1.2 或更新版本的 VM-Series 防火牆上，啟用 NUMA 效能最佳化。如需詳細資訊，請參閱 在 VM-Series 上啟用 NUMA 效能最佳化。
dhcp-send-hostname=	DHCP 伺服器的 yes 或 no 值。如果為 yes，防火牆將傳送其主機名稱至 DHCP 伺服器。此欄位僅當類型為 DHCP 用戶端時才關聯。
dhcp-send-client-id=	DHCP 伺服器的 yes 或 no 值。如果為 yes，防火牆將傳送其用戶端 ID 至 DHCP 伺服器。此欄位僅當類型為 DHCP 用戶端時才關聯。
dhcp-accept-server-hostname=	DHCP 伺服器的 yes 或 no 值。如果為 yes，防火牆將從 DHCP 伺服器接受其主機名稱。此欄位僅當類型為 DHCP 用戶端時才關聯。
dhcp-accept-server-domain=	DHCP 伺服器的 yes 或 no 值。如果為 yes，防火牆將從 DHCP 伺服器接受其 DNS 伺服器。此欄位僅當類型為 DHCP 用戶端時才關聯。
vm-series-auto-registration-pin-id 與 vm-series-auto-registration-pin-value	用於 VM-Series 防火牆上安裝裝置憑證的 VM-Series 註冊 PIN ID 和值。此 PIN ID 和值也可讓您在防火牆的 PAYG 實例上，自動為 AutoFocus 和 Cortex Data Lake 啟動網站授權。 您必須在 Palo Alto Networks CSP 上產生此註冊 PIN ID 和值。如需有關產生 PIN ID 和值的資訊，請參閱在 VM-Series 防火牆上安裝裝置憑證。

©2023 Palo Alto Networks, Inc.

範例 init-cfg.txt 檔案

下列範例基本設定檔案顯示檔案中支援的所有參數；必要參數以粗體顯示。

範例 **init-cfg.txt** 檔案（靜態 **IP** 位址）	範例 **init-cfg.txt** 檔案（**DHCP** 用戶端）
type=static	**type=dhcp-client**
ip-address=10.*.*.19	ip-address=
default-gateway=10.*.*.1	default-gateway=
netmask=255.255.255.0	netmask=
ipv6-address=2001:400:f00::1/64	ipv6-address=
ipv6-default-gateway=2001:400:f00::2*	ipv6-default-gateway=
hostname=Ca-FW-DC1	hostname=Ca-FW-DC1
vm-auth-key=7550362253****	vm-auth-key=7550362253****
panorama-server=10.*.*.20	panorama-server=10.*.*.20
panorama-server-2=10.*.*.21	panorama-server-2=10.*.*.21
tplname=FINANCE_TG4	tplname=FINANCE_TG4
dgname=finance_dg	dgname=finance_dg
dns-primary=10.5.6.6	dns-primary=10.5.6.6
dns-secondary=10.5.6.7	dns-secondary=10.5.6.7
op-command-modes=jumbo-frame,mgmt-interface-swap**	op-command-modes=jumbo-frame,mgmt-interface-swap**
op-cmd-dpdk-pkt-io=***	op-cmd-dpdk-pkt-io=***
plugin-op-commands=	plugin-op-commands=
dhcp-send-hostname=no	dhcp-send-hostname=yes
dhcp-send-client-id=no	dhcp-send-client-id=yes
dhcp-accept-server-hostname=no	dhcp-accept-server-hostname=yes
dhcp-accept-server-domain=no	dhcp-accept-server-domain=yes
vm-series-auto-registration-pin-id=abcdefgh1234**	**vm-series-auto-registration-pin-id=abcdefgh1234****
vm-series-auto-registration-pin-value=zyxwvut-0987**	**vm-series-auto-registration-pin-value=zyxwvut-0987****

©2023 Palo Alto Networks, Inc.

對於 *AWS* 上的 *VM-Series* 防火牆，您無法指定管理 *IP* 位址和網路遮罩設定。如果定義，防火牆將略過您指定的值，因為 *AWS* 使用後端中繼資料檔案指派管理 *IP* 位址及網路遮罩。

*如果您包含 *IPv6* 位址，則需要 *IPv6* 預設閘道。

***`mgmt-interface-swap`* 操作命令僅適用於 *AWS* 或 *GCP* 中的 *VM-Series* 防火牆。

****`op-cmd-dpdk-pkt-io=off`* 用於 *ESXi*、*KVM* 和 *GCP* 上停用 *VM-Series* 防火牆的 *DPDK*（*DPDK* 預設為啟用）。

*****有兩個使用案例需要 *`vm-series-auto-registration-pin-id`* 和 *`vm-series-auto-registration-pin-value`*：

- 採用 *VM-Series* 防火牆的即付即用 *(PAYG)* 授權選項啟動網站授權—*AutoFocus* 或 *Cortex Data Lake*。
- 擷取裝置憑證並安裝在 *VM-Series* 防火牆上。

©2023 Palo Alto Networks, Inc.

建立 bootstrap.xml 檔案

參考這些指示，從目標部署所在相同平台或超管理器上執行的防火牆匯出設定。

STEP 1 | 從防火牆匯出組態。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作）。
2. 選取您要匯出的組態檔案。
   - 若要匯出執行中的組態，請在 Configuration Management（組態管理）部分，**Export named configuration snapshot**（匯出命名的組態快照），然後從下拉式清單中選取 **running config.xml**。
   - 若要匯出上一版本的防火牆組態，在 Configuration Management（組態管理）部分，**Export configuration version**（匯出組態版本），然後在下拉式清單中選取相應的組態版本。

STEP 2 | 重新命名設定檔案並儲存。

1. 將檔案重新命名為 `bootstrap.xml`。

   為確保成功執行啟動程序，檔案名稱（區分大小寫）必須完全相符。
2. 將 `bootstrap.xml` 檔案儲存在 `init-cfg.txt` 檔案所在的相同位置。

©2023 Palo Alto Networks, Inc.

準備啟動程序授權

若要在啟動程序執行對防火牆授權，您必須購買驗證碼並在 Palo Alto Networks 支援入口網站上註冊授權及訂閱，再開始啟動程序。

對於執行 BYOL（不適用於依使用授權—PAYG）的 VM-Series 防火牆，必須具有包含功能驗證碼、支援訂閱及任何所需其他訂閱的驗證碼包。準備啟動授權的程序取決於防火牆啟動時是否可存取網際網路。

- 直接接入網際網路—防火牆直接連線至網際網路。
- 間接接入網際網路—防火牆由 Panorama 管理，其直接接入網際網路，且能夠代表防火牆擷取授權金鑰。
- 沒有接入網際網路—防火牆使用協調運作服務或自訂指令碼代表防火牆擷取授權金鑰。

對於接入網際網路的 VM-Series 防火牆：

當您準備啟動程序套件時，請輸入 `/license` 資料夾中的驗證碼。

對於間接接入網際網路的 VM-Series 防火牆：

1. 在 Palo Alto Networks 支援入口網站上註冊驗證碼。
   1. 前往支援入口網站，登入，然後選取 **Assets**（資產） > **Register New Device**（註冊新裝置） > **Register device using Serial Number or Authorization Code**（使用序號或驗證碼註冊裝置）。
   2. 請依照下列步驟以註冊 VM-Series 防火牆。
   3. 按一下 **Submit**（提交）。
2. 在 Palo Alto Networks 支援入口網站上啟動驗證碼以產生授權金鑰。
   1. 前往 支援入口網站，登入，然後選取 **Assets**（資產）頁籤。
   2. 對於每個序號，按一下 **Action**（動作）連結。
   3. 選取 **Activate Auth-Code**（啟動驗證碼）按鈕。
   4. 輸入 **Authorization code**（驗證碼），然後按一下 **Agree**（同意）和 **Submit**（提交）。
   5. 下載授權金鑰並將其儲存至本機資料夾。
   6. 繼續準備啟動程序套件；必須新增您已下載至啟動套件 `\license` 資料夾中的授權金鑰。

對於自訂指令碼或可代表防火牆接入網際網路的協調運作服務：

指令碼或服務必須從已部署防火牆的 Hypervisor 中擷取 CPU ID 及 UUID，並使用 CPU ID、UUID、API 金鑰及驗證碼存取 Palo Alto Networks 支援入口網站以取得所需金鑰。請參閱 授權 API。

©2023 Palo Alto Networks, Inc.

準備啟動程序套件

在 AWS、Azure 或 GCP 上，您可以在公共雲端儲存中建立啟動套件。

- VM-Series 外掛程式版本 1.0.13 和更早版本，以及版本 2.0.0 和 2.0.1，支援每個儲存貯體各一個啟動套件。
- VM-Series 外掛程式版本 2.0.2 和更新版本也支援公共雲端儲存貯體內的子資料夾。在貯體內，您可以建立多個資料夾和子資料夾，各包含一個啟動套件。資料夾通常代表一組 VM 的設定，例如 Panorama 裝置群組。

  若要存取啟動套件，請指定啟動程序資料夾的完整路徑。例如：`my-storage/my-firewalls/bootstrap-2020-10-15`

使用下列程序準備代理程式套件。

STEP 1 | 建立啟動程序套件的頂層目錄結構。

在本機用戶端或筆記型電腦，或在公共雲端儲存貯體中，建立下列資料夾：

```
/config
/content
/software
/license
/plugins
```

您可以將資料夾空白，但必須有 **/config**、**/license**、**/software** 和 **/content** 資料夾。**/plugins** 是選用資料夾，只有在您升級 VM-Series 外掛程式（與 PAN-OS 版本無關）時才需要。

請勿在啟動程序結構中放入任何其他檔案或資料夾。新增其他檔案或資料夾將會導致啟動載入失敗。

```
/my-storage                                  /my-firewalls
       /internal      /external                  /config        /config
         /content        /content                /license       /license
         /plugins        /plugins                /software      /software
```

STEP 2 | 在每個資料夾中新增內容。

如需程序概要介紹，請參閱啟動程序套件。如需 **/config** 資料夾中檔案的詳細資料，請參閱啟動設定檔案。

```
/config
  0008C100105-init-cfg.txt
  0008C100107-init-cfg.txt
  bootstrap.xml
/content
  panupv2-all-contents-488-2590
  panup-all-antivirus-1494-1969
  panup-all-wildfire-54746-61460
```

```
/software
  PanOS_vm-10.0.0
/license
  授權碼
  0001A100110-url3.key
  0001A100110-threats.key
  0001A100110-url3-wildfire.key
/plugins
  vm_series-2.0.2
```

- 如果您將金鑰儲存至 ***license*** 資料夾，則可以使用適合的檔案命名慣例，但檔案名稱中必須保留 ***.key*** 副檔名。針對授權碼，建立名稱為 ***authcodes*** 的文字檔（無副檔名），並將授權碼新增至該檔案，然後將它儲存至 ***license*** 資料夾。
- 使用包含驗證碼包而非個別的驗證碼，以便防火牆或協調運作服務可同步擷取與防火牆關聯的所有授權金鑰。如果您使用個別的驗證碼而非驗證碼包，防火牆將只會擷取檔案中包含的首個驗證碼的授權金鑰。
- 在 ***/plugins*** 資料夾中，只提供一個 *VM-Series* 外掛程式二進位檔。請不要提供多個外掛程式版本。

STEP 3 | 建立啟動程序套件。

對於 VM-Series 防火牆，為 Hypervisor 建立相應格式的映像。請參閱 啟動套件傳遞。

©2023 Palo Alto Networks, Inc.

在 AWS 上啟動 VM-Series 防火牆

STEP 1 | 選擇啟動方法。

- 若要將基本設定新增至啟動套件，請繼續步驟 2。
- 若要以使用者資料輸入基本設定，或利用使用者資料從 AWS 機密取得基本設定，請繼續步驟 3。

STEP 2 | 準備 S3 貯體和 IAM 角色來啟用讀取存取。

若要使用檔案來啟動，您必須熟悉完成此程序所需的 AWS S3 和 IAM 權限。如需建立原則的詳細指示，請參閱 AWS 文件中的建立客戶管理的原則。

VM-Series 防火牆的管理介面必須能夠存取 S3 貯體，才能完成啟動程序。您可以將公共 IP 位址或彈性 IP 位址指派給管理介面，以便能夠透過網際網路存取 S3 貯體。或者，如果您偏好在 VPC 和 S3 貯體之間建立私人連線，而不想在防火牆管理介面上啟用網際網路存取，則您可以 S3 貯體所在的同一區域建立 AWS VPC 端點。如需詳細資訊，請參閱 AWS 文件中的設定 VPC 端點。

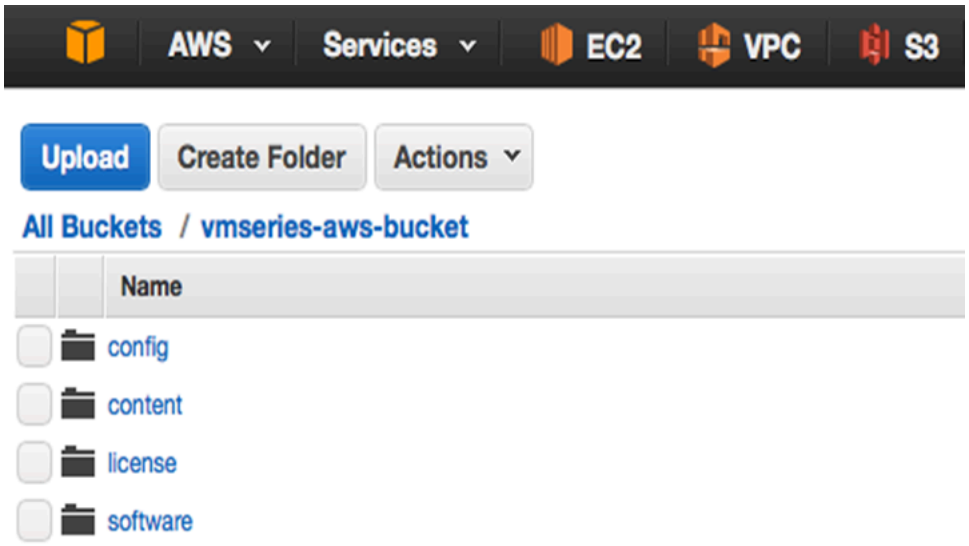
1. 運用內聯原則建立 IAM 角色，以啟用 S3 貯體 [ListBucket, GetObject] 的讀取權限。如需建立 IAM 角色，定義哪些帳戶或 AWS 服務可承擔該角色，以及承擔角色後應用程式可使用哪些 API 動作及資源的詳細指示，請參閱 Amazon EC2 的 IAM 角色。啟動 VM-Series 防火牆時，您必須附加此角色，以啟用貯體中 S3 貯體及物件的存取權，以便成功啟動程序。
2. 在 AWS 主控台上，建立 Amazon Simple Storage Service (S3) 貯體，或在現有 S3 貯體中建立子目錄。

   下列範例中的 S3 貯體 (vmseries-aws-bucket) 位於 [All Buckets（所有貯體）] 根資料夾層級。

```
{    "版本":"2012-10-17",    "聲明": [    {        "效
果":"允許",        "動作": ["s3:ListBucket"],        "資
源": ["arn:aws:s3:::<bucketname>"]    },    {        "效
果":"允許",        "動作": ["s3:GetObject"],        "資源":
 ["arn:aws:s3:::<bucketname>/*"]       }    ] }
```


©2023 Palo Alto Networks, Inc.

3. 在 S3 貯體內建立資料夾，如準備啟動程序套件所述。
   - 直接在 S3 貯體中建立結構。



   - （選用）在每個資料夾中新增內容。您可以讓資料夾空白，但 \config、\license、\software 和 \content 資料夾必須全部存在。\plugins 是選用資料夾。

如果您在 *Amazon S3* 中已啟用日誌記錄，則會在 *S3* 貯體中自動建立日誌資料夾。日誌資料夾有助於排解 *S3* 貯體的存取問題。

©2023 Palo Alto Networks, Inc.

STEP 3 | 在 AWS 上啟動 VM-Series 防火牆。選擇下列其中一項。

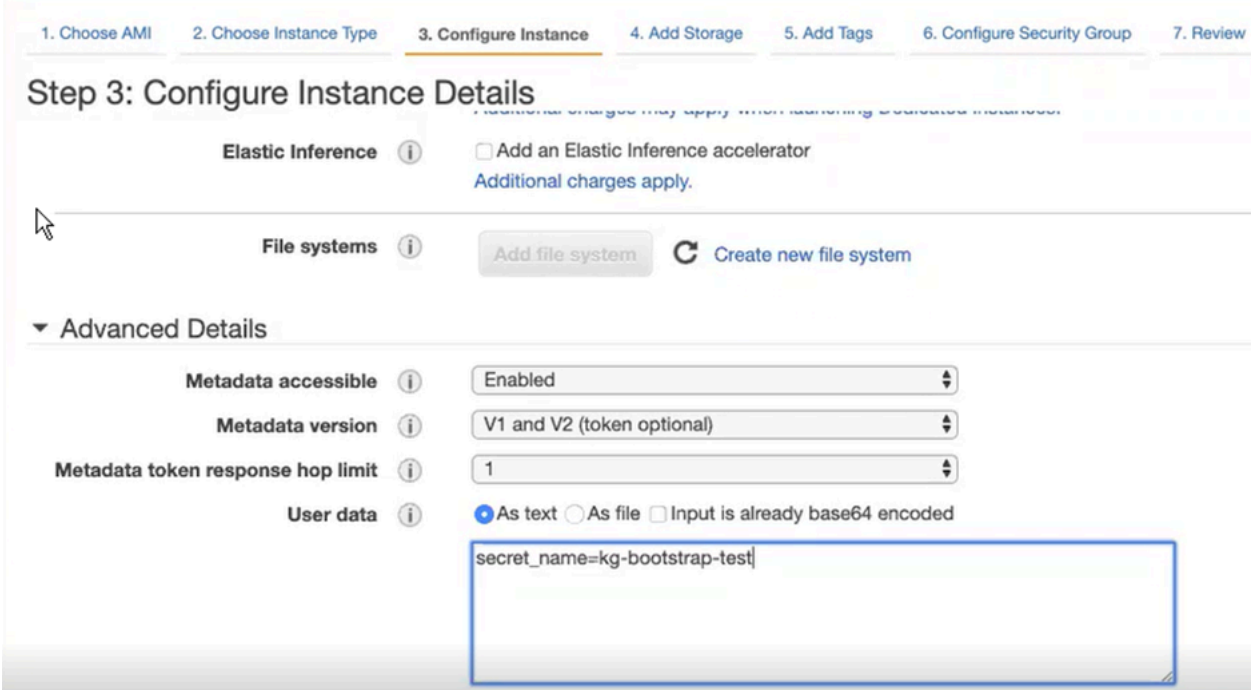
- **`init-cfg.txt`**—如果您使用檔案來設定防火牆，請連接您在步驟 2.1 建立的 IAM 角色，展開 **Advanced Details**（進階詳細資料）區段，然後在 **User Data**（使用者資料）欄位中，指定 S3 貯體、目錄或子目錄的路徑。例如，

  ```
  vmseries-bootstrap-aws-s3bucket=<bucketname>
  ```

  或

  ```
  vmseries-bootstrap-aws-s3bucket=<bucketname/directoryname>
  ```

- 使用者資料—如果您利用使用者資料來設定防火牆，請展開 **Advanced Details**（進階詳細資料）區段，然後在 **User Data**（使用者資料）欄位中輸入初始啟動程序參數，如以使用者資料輸入基本設定（公共雲端）所述。
- **AWS Secrets Manager**—如果您如在 AWS Secrets Manager 中儲存基本設定所述儲存基本設定，請展開 **Advanced Details**（進階詳細資料）區段，然後在 **User Data**（使用者資料）欄位中選擇 **As text**（以文字），以鍵值組輸入機密名稱。例如：

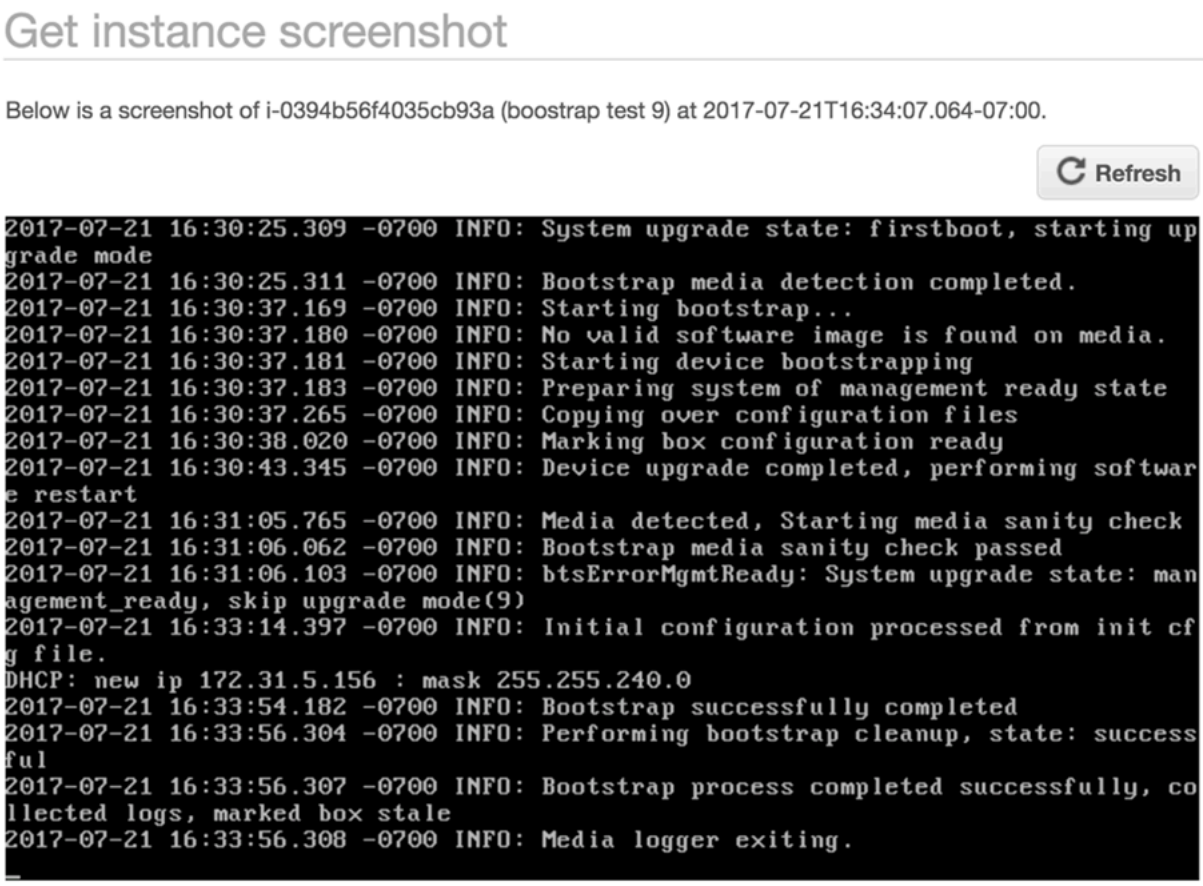


選取 **Review and Launch**（複查並啟動）。如需詳細資訊，請參閱在 AWS 上啟動 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

STEP 4 | 驗證啟動程序完成。在 AWS 管理主控台上選取防火牆實例，然後選擇 **Actions**（動作） > **Instance Settings**（實例設定） > **Get Instance Screenshot**（取得實例螢幕擷取畫面）。

- 螢幕擷取畫面顯示啟動載入進行中。下方顯示成功啟動：



- 如果您使用 S3 貯體，但 S3 貯體沒有正確權限，或 S3 貯體中的四個資料夾未全部存在，您會看到下列錯誤訊息：



 ©2023 Palo Alto Networks, Inc.

在 Azure 上啟動 VM-Series 防火牆

Azure 上的 VM-Series 防火牆支援***Azure Files***（***Azure*** 檔案）服務的啟動。

STEP 1 | 選擇啟動方法。

- 若要將基本設定新增至啟動套件，請繼續步驟 2。

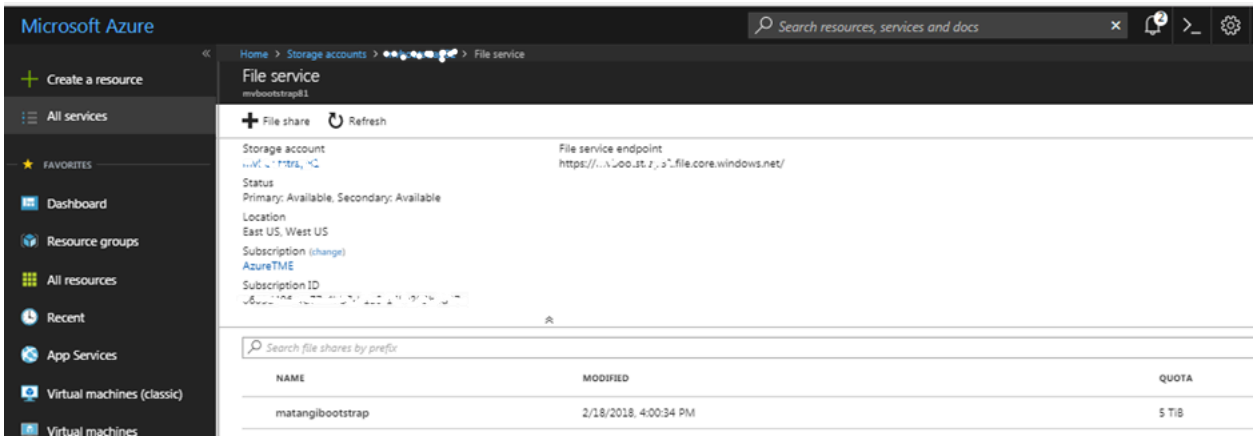
  若要管理 Azure 上的 VM-Series 防火牆啟動封包，則必須熟悉 Azure 上的儲存帳戶，並瞭解如何建立檔案共享與包含啟動封包所需檔案架構的目錄物件。您可以在許多虛擬電腦上共用 Azure 檔案，讓所有部署在相同區域，作為託管檔案共用儲存帳戶的防火牆可以同時存取檔案。

  VM-Series 防火牆的管理介面也必須能存取持有此啟動封包的檔案共用，才能完成啟動。
- 若要以使用者資料輸入基本設定（公共雲端），請繼續步驟 3.2。

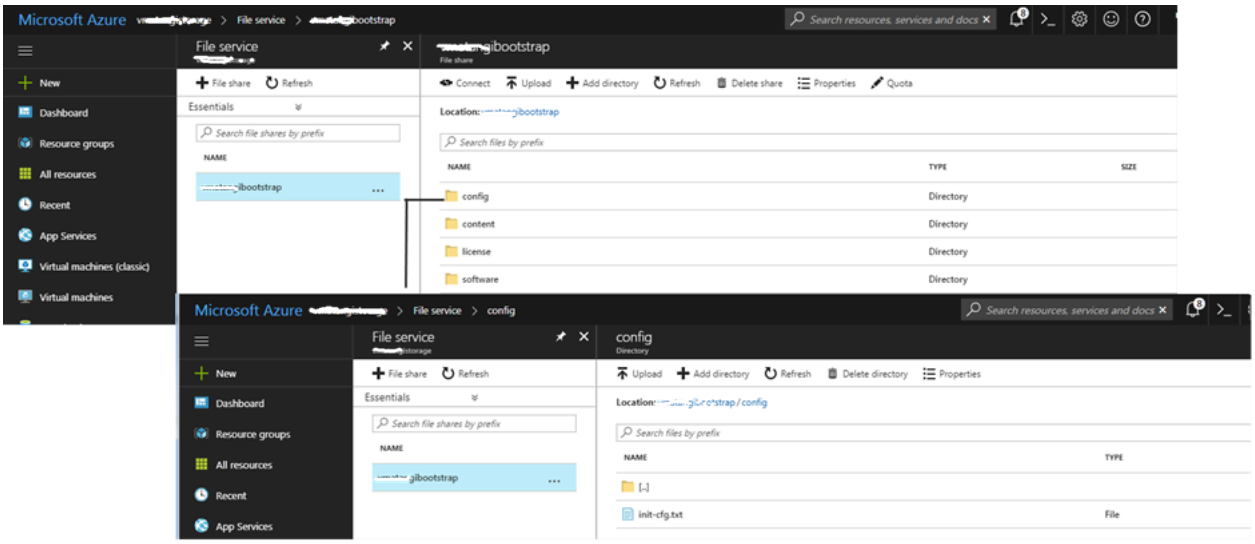
©2023 Palo Alto Networks, Inc.

STEP 2 | 使用 Azure 檔案服務設定啟動封包。

1. 在 Azure 入口網站上，選取或建立一個儲存帳戶。
2. 在 Azure 檔案服務內建立檔案共用。



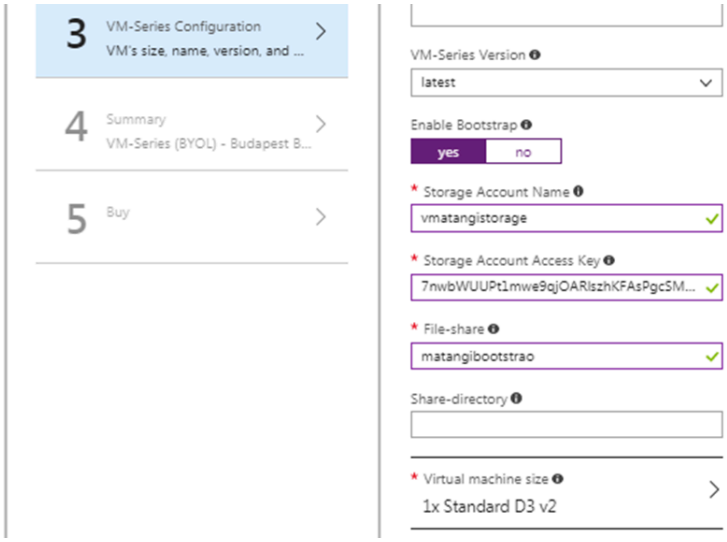
3. 在儲存帳戶內建立資料夾。
   - 直接在根資料夾中為啟動套件建立最上層目錄結構，並為每個啟動程序設定各建立一個子資料夾。
   - 在每個資料夾中新增內容資料夾。您可以讓資料夾空白，但在上層資料夾中，四個資料夾必須全部存在（config、license、software 和 content）。在下列快照中，您可以看到 **config** 檔案夾中已上傳 **init-cfg.txt** 檔案。



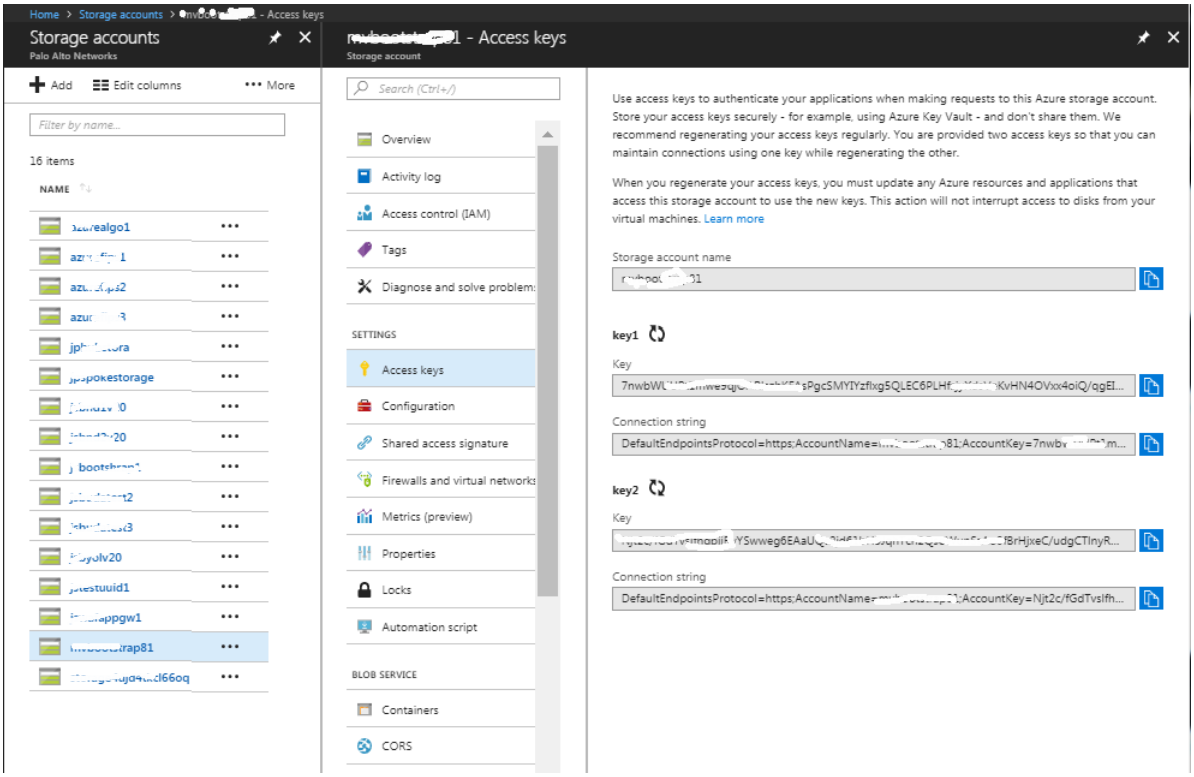
 ©2023 Palo Alto Networks, Inc.

STEP 3 | 從 Azure Marketplace 部署 VM-Series 防火牆（解決方案範本）。

- 如果您使用檔案來設定防火牆，請繼續步驟 3.1
- 如果您使用自訂資料來設定防火牆，請繼續步驟 3.2。



1. 如果您選擇使用啟動套件，請選取 **Enable Bootstrap:Yes**（啟用啟動：是），並提供存取檔案共用（保留啟動程序檔案）時所需的資訊。
   1. 儲存帳戶名稱—這是一個 Azure 儲存帳戶，您為啟動檔案夾建立檔案共用的地方。
   2. 儲存帳戶存取金鑰—防火牆需要此存取金鑰以驗證儲存帳戶並存取其內儲存的檔案。若要複製此存取金鑰，請選取儲存帳戶名稱，然後選取 **Setttings**（設定） > **Access Keys**（存取金鑰）



 ©2023 Palo Alto Networks, Inc.

。

3. **File-share**（檔案共用）—含有啟動套件的檔案共用名稱。
4. （選用）**Share-directory**（共用目錄）—檔案共用內的子資料夾路徑。如果您有通用的檔案共用作為儲存庫，存放不同設定的啟動程序設定，則可以使用共用目錄來建立資料夾階層，並存取通用檔案共用內的一組特定的子資料夾。

2. 以自訂資料輸入設定參數。關於鍵值組，請參閱以使用者資料輸入基本設定（公共雲端）。請以分號分隔每個鍵值。例如：

```
type=dhcp-client; op-command-modes=jumbo-frame; vm-series-
auto-registration-pin-id=abcdefgh1234****; vm-series-auto-
registration-pin-value=zyxwvut-0987****
```

使用 Azure 虛擬機器上的自訂資料和 Cloud-Init 的其中一個方法提供自訂資料。

STEP 4 | 驗證啟動程序完成。

©2023 Palo Alto Networks, Inc.

在 ESXi 上啟動 VM-Series 防火牆

您可以使用 ISO 映像或虛擬硬碟來啟動 VM-Series 防火牆。

- 使用 ISO 在 ESXi 上啟動 VM-Series 防火牆
- 使用區塊儲存裝置在 ESXi 上啟動 VM-Series 防火牆

使用 ISO 在 ESXi 上啟動 VM-Series 防火牆

根據這些指示，在 ESXi 伺服器上使用 ISO 啟動 VM-Series 防火牆。

STEP 1 | 建立 ISO 映像並將其上載至虛擬電腦檔案系統 (VMFS) 資料存放或網路檔案系統 (NFS) 磁碟區。

1. 準備啟動程序套件.
2. 建立 ISO 映像。您用於建立映像的工具因用戶端作業系統而異。
3. 將 ISO 映像上載至 VMFS 資料存放或可存取 ESX/ESXI 主機的 NFS 磁碟區。

STEP 2 | 部署防火牆。

1. 在 ESXi 伺服器上佈建 VM-Series 防火牆.

   依預設，防火牆部署兩個網路介面—一個用於管理流量，一個用於資料流量。確保防火牆上的第一個乙太網路介面（其管理介面）已連線至指派進行設備管理的虛擬交換器連接埠群組。
2. 請勿開啟防火牆電源。

STEP 3 | 將啟動程序映像附加至防火牆。

1. 從 **Inventory**（詳細目錄）清單中選取 VM-Series 防火牆。
2. 按一下 **Edit Settings**（編輯設定），然後選取 **Virtual Hardware**（虛擬硬體）。
3. 在 **CD DVD drive**（**CD DVD** 磁碟機）下拉式清單中，選取 **Datastore iso file**（資料存放 **ISO** 檔案），然後 **browse**（瀏覽） ISO 映像。
4. 開啟防火牆電源。防火牆將開始啟動程序，這需要幾分鐘時間。程序啟動成功或失敗的狀態訊息會顯示在主控台上。
5. 驗證啟動程序完成.

使用區塊儲存裝置在 ESXi 上啟動 VM-Series 防火牆

根據這些指示，在 ESXi 伺服器上使用區塊儲存裝置來啟動 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

STEP 1 | 建立啟動程序套件和虛擬硬碟。

1. 建立啟動程序套件。
2. 部署 Linux 虛擬機器。
3. 在 Linux 電腦上，準備啟動程序套件。您可以將資料夾留空，但必須有所有四個資料夾。
4. 將小於 39 GB 的新資料磁碟連接至 Linux 虛擬機器。
5. 分割磁碟並將檔案系統格式設定為 ext3。
6. 設定新檔案系統的目錄，並將磁碟安裝至 Linux 虛擬電腦。
7. 將啟動程序套件的內容複製到磁碟。
8. 卸載磁碟。
9. 從 Linux 虛擬機器卸除磁碟。記下 Disk File（磁碟檔案），其中描述您建立的啟動程序磁碟；它會顯示磁碟的資料存放名稱和路徑。此外，請勿勾選 Delete Files From Datastore（從資料存放刪除檔案）核取方塊；這樣做會刪除磁碟。

STEP 2 | 部署防火牆。

1. 在 ESXi 伺服器上佈建 VM-Series 防火牆.
2. 請勿開啟防火牆電源。

STEP 3 | 將啟動程序套件附加至防火牆。

1. 從詳細目錄清單中選取 VM-Series 防火牆。
2. 按一下 **Edit Settings**（編輯設定），然後選取 **Virtual Hardware**（虛擬硬體）。
3. 從 New Device（新裝置）下拉式清單中，選取 **Existing Hard Disk**（現有硬碟）。根據先前記下的資料存放和路徑，選取啟動程序磁碟。
4. 開啟防火牆電源。防火牆將開始啟動程序，這需要幾分鐘時間。程序啟動成功或失敗的狀態訊息會顯示在主控台上。
5. 驗證啟動程序完成.

©2023 Palo Alto Networks, Inc.

在 Google Cloud Platform 上啟動 VM-Series 防火牆

STEP 1 | 選擇啟動方法。

STEP 2 | 登入Google Cloud 主控台。

- 若要將基本設定新增至啟動套件，請如準備啟動套件所述建立啟動程序檔案，然後繼續步驟 3。
- 若要以自訂中繼資料輸入基本設定，請跳至步驟 4。

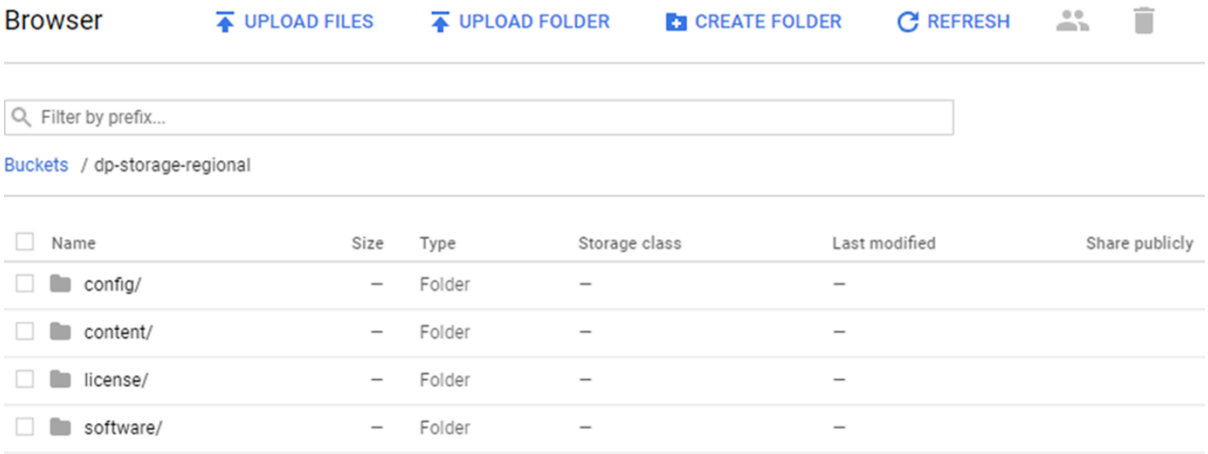
STEP 3 | 選取 **Storage**（儲存） > **Browser**（瀏覽器），然後按一下**Create Bucket**（建立貯體）。

當您從 Google Cloud Platform Marketplace 部署 VM-Series 防火牆時，您可以使用此貯體啟動防火牆。

若您希望使用同專案裡的 Google 貯體啟動，則必須擁有 devstorage.read_only IAM 權限。

您可以在最上層建立並填入貯體，也可以建立含有子資料夾的貯體，讓許多啟動套件共用相同貯體。

1. 輸入貯體名稱、選取預設儲存類別，然後選取位置。請注意，在貯體內的位置必須與您為計算引擎實例指定的區域相容。
2. 按一下 **Create**（建立）。
3. 在儲存瀏覽器中，按一下貯體名稱可將其開啟。
4. 按一下 **Create Folder**（建立檔案夾） 並將其命名為 `config`。按一下 **Create**（建立）。
5. 重覆步驟，為 `content`、`license` 和 `software` 建立檔案夾，如下所示。必須出示所有檔案夾，就算內容為空也一樣。



6. （選用）如果您建立 **`init-cfg.txt`** 檔案，請開啟 `config` 資料夾。按一下 **Upload Files**（上傳檔案），瀏覽以選取您的 **`init-cfg.txt`** 檔案，然後按一下 **Open**（開啟）。
7. 開啟 `license` 檔案夾並上傳 **`authcodes`** 檔案。
8. 繼續直到您已上傳所有啟動檔案。

©2023 Palo Alto Networks, Inc.

STEP 4 | 以中繼資料新增初始設定參數。**Add**（新增）每個鍵值組，如以使用者資料輸入基本設定（公共雲端）所述。

STEP 5 | 如需部署詳細資料，請參閱從 Google Cloud Platform Marketplace 部署 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

在 Hyper-V 上啟動 VM-Series 防火牆

您可以使用 ISO 映像或虛擬硬碟來啟動 VM-Series 防火牆。

- 使用 ISO 在 Hyper-V 上啟動 VM-Series 防火牆
- 使用區塊儲存裝置在 Hyper-V 上啟動 VM-Series 防火牆

使用 ISO 在 Hyper-V 上啟動 VM-Series 防火牆

根據這些指示，在 Hyper-V 伺服器上使用 ISO 啟動 VM-Series 防火牆。

STEP 1 | 建立 ISO 映像。

1. 準備啟動程序套件.
2. 建立 ISO 映像。您用於建立映像的工具因用戶端作業系統而異。
3. 上載 ISO 映像至可存取 Hyper-V 主機的位置。

STEP 2 | 部署防火牆。

1. 在 Hyper-V 主機上使用 Hyper-V 管理員佈建 VM-Series 防火牆.

   依預設，防火牆部署兩個網路介面—一個用於管理流量，一個用於資料流量。確保防火牆上的第一個乙太網路介面（其管理介面），已連線至指派來管理裝置的 vSwitch。
2. 請勿開啟防火牆電源。

STEP 3 | 將啟動程序映像附加至防火牆。

1. 在 Hyper-V 管理員中，從 **Virtual Machines**（虛擬機器）清單中選取 VM-Series 防火牆。
2. 按一下 **Settings**（設定） > **Hardware**（硬體） > **IDE Controller**（**IDE** 控制器） > **DVD Drive**（**DVD** 光碟機）。

   如果您有多個 *DVD* 光碟機，則 *ISO* 映像必須套用至第一個光碟機。
3. 在 Media（媒體）項下，按一下 **Image file**（映像檔案）選項按鈕。
4. 按一下 **Browse**（瀏覽），然後選取上載的 ISO 映像。
5. 按一下 **Apply**（套用），然後按一下 **OK**（確定）以結束虛擬機器設定。
6. 開啟防火牆電源。防火牆將開始啟動程序，這需要幾分鐘時間。程序啟動成功或失敗的狀態訊息會顯示在主控台上。
7. 驗證啟動程序完成.

使用區塊儲存裝置在 Hyper-V 上啟動 VM-Series 防火牆

根據這些指示，在 Hyper-V 伺服器上使用區塊儲存裝置來啟動 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

STEP 1 | 建立啟動程序套件和虛擬硬碟。

1. 部署 Linux 虛擬機器。
2. 在 Linux 電腦上，準備啟動程序套件。您可以將資料夾留空，但必須有所有四個資料夾。
3. 將小於 39 GB 的新資料磁碟連接至 Linux 虛擬機器。
   1. 關閉 Linux 虛擬機器電源。
   2. 在 Hyper-V 中，從 Virtual Machines（虛擬機器）清單中選取 Linux 虛擬機器。
   3. 選取 **Settings**（設定） > **Hardware**（硬體） > **IDE Controller**（**IDE** 控制器）。
   4. 選取 **Hard Drive**（硬碟），按一下 **Add**（新增）。
   5. 選取 **Virtual Hard Disk**（虛擬硬碟），按一下 **New**（新增）。
   6. 依照畫面上的指示建立新 VHD。請注意新 VHD 的名稱和路徑。
   7. 按一下 **Apply**（套用），然後按一下 **OK**（確定）以結束虛擬機器設定。
   8. 開啟 Linux 虛擬機器電源。
4. 連接至 Linux 虛擬機器的 CLI。
5. 分割磁碟並將檔案系統格式設定為 ext3。
6. 設定新檔案系統的目錄，並將磁碟安裝至 Linux 虛擬電腦。
7. 將啟動程序套件的內容複製到磁碟。
8. 卸載磁碟。
9. 從 Linux 虛擬機器卸除磁碟。
   1. 關閉 Linux 虛擬機器電源。
   2. 從 Virtual Machines（虛擬機器）清單中選取 Linux 虛擬機器。
   3. 選取 **Settings**（設定） > **Hardware**（硬體） > **IDE Controller**（**IDE** 控制器）。
   4. 選取您建立的 VHD。
   5. 按一下 **Remove**（移除）。這會卸除 VHD，但不會刪除它。

STEP 2 | 部署防火牆。

1. 在 Hyper-V 主機上使用 Hyper-V 管理員佈建 VM-Series 防火牆.
2. 請勿開啟防火牆電源。

STEP 3 | 將啟動程序磁碟映像附加至防火牆。

1. 從 Virtual Machines（虛擬機器）清單中選取防火牆。
2. 選取 **Settings**（設定） > **Hardware**（硬體） > **IDE Controller**（**IDE** 控制器）。
3. 選取 **Hard Drive**（硬碟），按一下 **Add**（新增）。
4. 選取 **Virtual Hard Disk**（虛擬硬碟），按一下 **Browse**（瀏覽）。
5. 瀏覽至您建立的啟動程序 VHD，選取它，然後按一下 **Open**（開啟）。
6. 按一下 **Apply**（套用），然後按一下 **OK**（確定）以結束虛擬機器設定。
7. 開啟防火牆電源。防火牆將開始啟動程序，這需要幾分鐘時間。程序啟動成功或失敗的狀態訊息會顯示在主控台上。
8. 驗證啟動程序完成.

©2023 Palo Alto Networks, Inc.

在 KVM 上啟動 VM-Series 防火牆

您可以在 KVM 上使用 ISO 映像或虛擬硬碟來啟動 VM-Series 防火牆。

- 使用 ISO 在 KVM 上啟動 VM-Series 防火牆
- 使用區塊儲存裝置在 KVM 上啟動 VM-Series 防火牆

使用 ISO 在 KVM 上啟動 VM-Series 防火牆

根據這些指示，在 KVM 伺服器上使用 ISO 啟動 VM-Series 防火牆。

STEP 1 | 建立 ISO 映像。

1. 準備啟動程序套件。
2. 建立 ISO 映像。您用於建立映像的工具因用戶端作業系統而異。
3. 上載 ISO 映像至可存取 KVM 主機的位置。

STEP 2 | 部署防火牆。

1. 在 KVM 上安裝 VM-Series 防火牆。

   依預設，防火牆部署兩個網路介面—一個用於管理流量，一個用於資料流量。確保防火牆上的第一個乙太網路介面（其管理介面）已連線至指派進行設備管理的虛擬交換器連接埠群組。
2. 請勿開啟防火牆電源。

STEP 3 | 將啟動程序映像附加至防火牆。

1. 在 virt-manager 中，按兩下 VM-Series 防火牆以開啟主控台。
2. 導覽至 **View**（檢視） > **Details**（詳細資訊）可檢視 VM 硬體詳細資訊。
3. 按一下 **Add Hardware**（新增硬體）可開啟 Add New Virtual Hardware（新增虛擬硬體）功能表。
4. 將設備類型變更為 IDE CDROM。
5. 按一下 **Select managed or other existing storage**（選取受管理的儲存空間或其他現有儲存空間）選項按鈕，然後按一下 **Browse**（瀏覽）。尋找您建立的 ISO 映像，然後按一下 **Choose Volume**（選取磁碟區）。
6. 按一下 **Finish**（完成）以結束 Add New Virtual Hardware（新增虛擬硬體）功能表。
7. 導覽至 **Virtual Machine**（虛擬機器） > **Run**（執行）可開啟防火牆。防火牆將開始啟動程序，這需要幾分鐘時間。程序啟動成功或失敗的狀態訊息會顯示在主控台上。
8. 驗證啟動程序完成。

使用區塊儲存裝置在 KVM 上啟動 VM-Series 防火牆

根據這些指示，在 KVM 伺服器上使用區塊儲存裝置來啟動 VM-Series 防火牆。

©2023 Palo Alto Networks, Inc.

STEP 1 | 建立啟動程序套件和虛擬硬碟。

1. 建立啟動程序套件。
2. 建立小於 39 GB 的新磁碟映像，劃分磁碟的分割區，並將檔案系統格式化為 ext3。用於完成此程序的工具因用戶端作業系統而異。
3. 裝載磁碟映像檔案，並將備妥的啟動程序套件複製到磁碟映像檔案。
4. 將啟動程序套件的內容複製到磁碟。
5. 卸載磁碟映像。
6. 將磁碟映像檔案上載至 KVM 主機可存取的位置。

STEP 2 | 部署防火牆。

1. 在 KVM 上安裝 VM-Series 防火牆。
2. 請勿開啟防火牆電源。

STEP 3 | 將啟動程序磁碟映像附加至防火牆。

1. 在 virt-manager 中，按兩下 VM-Series 防火牆以開啟主控台。
2. 選取 **View**（檢視） > **Details**（詳細資訊）可檢視 VM 硬體詳細資訊。
3. 按一下 **Add Hardware**（新增硬體）可開啟 Add New Virtual Hardware（新增虛擬硬體）功能表。
4. 選取 **Storage**（儲存空間），然後選取 **Select or create custom storage**（選取或建立自訂儲空間）。
5. 按一下 **Manage**（管理）按鈕開啟 **Choose Storage Volume**（選取儲存磁碟區）對話方塊，然後選取您先前建立的磁碟映像檔案。
6. 按一下 Choose Volume（選取磁碟區）。
7. 確定裝置類型為 Disk Device（磁碟裝置），不要變更 Bus Type（匯流排類型）。
8. 按一下 Finish（完成）。
9. 開啟防火牆電源。防火牆將開始啟動程序，這需要幾分鐘時間。程序啟動成功或失敗的狀態訊息會顯示在主控台上。
10. 驗證啟動程序完成。

©2023 Palo Alto Networks, Inc.

驗證啟動程序完成

您可以在啟動期間在主控台上查看基本狀態，並且可驗證程序是否完成。

STEP 1 | 如果 `init-cfg.txt` 檔案包含 **`panorama-server`**、**`tplname`** 及 **`dgname`**，請檢查 Panorama 管理的裝置、裝置群組和範本名稱。

STEP 2 | 驗證一般系統設定及組態。存取網頁介面並選取 **Dashboard**（儀表板） > **Widgets** > **System**（系統），或使用 CLI 操作命令 **`show system info`** 及 **`show config running`**。

STEP 3 | 驗證授權安裝。選取 **Device**（裝置） > **Licenses**（授權），或使用 CLI 操作命令 **`request license info`**。

STEP 4 | 如果設定了 Panorama，可從 Panorama 管理內容版本及軟體版本。如果未設定 Panorama，則使用 Web 介面來管理內容版本及軟體版本。

©2023 Palo Alto Networks, Inc.

啟動程序錯誤

如果在啟動程序執行過程中收到錯誤訊息，請參見下表瞭解詳細資訊。

錯誤訊息（嚴重性）	原因
啟動映像錯誤（高）	· 啟動套件沒有偵測到外部設備。 或者 · 從外部設備上的映像引導時發生嚴重錯誤。啟動程序已中止。
外部設備上沒有啟動程序組態檔案（高）	外部設備沒有啟動程序組態檔案。
啟動程序組態檔案中的強制連網資訊錯誤或沒有參數（高）	啟動程序所需的連網參數不正確或缺失。錯誤訊息列示導致啟動失敗的值（IP 位址、網路遮罩、預設閘道）。
無法安裝檔案 <license-key-filename> 的授權金鑰（高）	無法套用授權金鑰。此錯誤指示所用授權金鑰無效。輸出包含無法套用的授權金鑰名稱。
無法使用驗證碼 <authcode> 安裝授權金鑰（高）	無法套用授權驗證碼。此錯誤指示所用授權驗證碼無效。輸出包含無法套用的授權驗證碼名稱。
內容更新提交失敗（高）	未成功套用內容更新。
使用指定搭售包準備 USB 媒體成功（資訊）	啟動映像已成功套用於 USB 快閃設備。<username>：使用搭售包 <bundlename> 成功準備 USB
啟動成功（資訊）	使用啟動程序組態檔案佈建防火牆成功。輸出包含已安裝的授權金鑰及啟動組態的檔案名稱。僅在 VM-Series 防火牆上，還會顯示 PAN-OS 版本及內容更新版本。

閱讀有關啟動套件以及如何準備啟動程序套件的資訊。

©2023 Palo Alto Networks, Inc.

©2023 Palo Alto Networks, Inc.